Automatic Detection of Speculative Execution Combinations

Xaver Fabian
Cispa Helmholtz Center for Information Security
Saarbrücken, Germany
xaver.fabian@cispa.de

Marco Guarnieri
IMDEA Software Institute
Madrid, Spain
marco.guarnieri@imdea.org

Marco Patrignani
University of Trento
Trento, Italy
marco.patrignani@unitn.it

ABSTRACT

Modern processors employ different speculation mechanisms to speculate over different kinds of instructions. Attackers can exploit these mechanisms *simultaneously* in order to trigger leaks of speculatively-accessed data. Thus, sound reasoning about such speculative leaks requires accounting for *all* potential speculation mechanisms. Unfortunately, existing formal models only support reasoning about fixed, hard-coded speculation mechanisms, with no simple support to extend said reasoning to new mechanisms.

In this paper, we develop a framework for reasoning about composed speculative semantics that capture speculation due to different mechanisms and implement it as part of the Spectector verification tool. We implement novel semantics for speculating over store and return instructions and combine them with the semantics for speculating over branch instructions. Our framework yields speculative semantics for speculating over any combination of these instructions that are secure by construction, i.e., we obtain these security guarantees for free. The implementation of our novel semantics in Spectector let us verify programs that are vulnerable to Spectre v1, Spectre v4, and Spectre v5 vulnerabilities as well as new snippets that are only vulnerable to their compositions.

CCS CONCEPTS

• **Security and privacy** → **Formal security models**; **Systems security**.

KEYWORDS

Spectre; Speculative Execution; Speculative information flows; Speculative non-interference; Combinations of speculative semantics

1 INTRODUCTION

Speculative execution avoids pipeline stalls by predicting intermediate results and by speculatively executing instructions based on such predictions. When a prediction turns out to be incorrect, the processor squashes the speculative instructions, thereby rolling back their effect on the architectural state. Speculative instructions, however, leave footprints in microarchitectural components (like caches) that persist even after speculative execution terminates. As shown by Spectre [24], attackers can exploit these side effects to leak information about speculatively accessed data.

Modern general-purpose processors have different speculation mechanisms (branch predictors, memory disambiguators, etc.) that are used to speculate over different kinds of instructions: conditional branching [24], indirect jumps [24], store and load operations [23], and return instructions [25]. While well-known attacks target only individual speculation mechanism (e.g., Spectre-PHT [24] targets branch predictors), some speculative leaks only arise due to the interaction of multiple mechanisms.

Listing 1: Speculative leak arising from speculation over branch and store instructions combined.

```
1  x = 0;
2  p = &secret;
3  p = &public;
4  if (x != 0)
5      temp &= A[*p];
```

For example, the code in Listing 1 can speculatively leak the value of `&secret` in Line 5 whenever (1) the memory write to `p` in Line 3 is predicted to have a different address then the memory read `*p` on Line 5, and (2) the branch instruction on Line 4 is mispredicted as taken. This leak, therefore, arises from the *combination* of two speculation mechanisms: branch prediction and memory disambiguation prediction. Hence, leaks like the one in Listing 1 are missed by *sound* analyses for speculative leaks that consider speculation over only one of these speculation mechanisms.

Sound reasoning about speculative leaks requires accounting for *all* potential speculation mechanisms. However, existing formal models (also called *speculative semantics*) support multiple speculation mechanisms poorly. Some of them support only fixed speculation mechanisms: branch prediction [20, 21, 38–40] and (in addition) memory disambiguation prediction [9, 14, 32]. Furthermore, the different speculation mechanisms are *hard-coded* into the formal semantics [9, 14, 21]. Extending these semantics with new speculation mechanisms (e.g., speculation over return addresses or value prediction) requires changes to the formal model and to any security proof relying on it. This is not a scalable approach for developing comprehensive formal models and analyses for speculative leaks.

In this paper we develop a framework for composing speculative semantics that capture speculation due to different mechanisms and implement it as part of the Spectector verification tool. The combination yields a single operational semantics that can be used to reason about leaks involving *all* speculation mechanisms of the components (as in Listing 1). Our framework lets us define the speculative semantics of each mechanism independently, which leads to simpler formalisation. Additionally, the security of the composed semantics is derived automatically from the security of its sub-parts, maximising proof reuse. Finally, the composed semantics can be easily implemented in Spectector, which can be used to verify the absence of leaks like those in Listing 1.

Concretely, this paper makes the following contributions:

- It introduces $\mathcal{A}_{\mathtt{S}}$ and $\mathcal{A}_{\mathtt{R}}$, two novel semantics for speculation over store and return instructions (Section 3).
- It defines the framework for composing different speculative semantics and formalises its key properties: if the individual semantics fulfil some (expected) security conditions (which we prove for all the semantics we combine), then the composed semantics is also secure (Section 4).
- It instantiates the framework with $\mathcal{A}_{\mathtt{S}}$, $\mathcal{A}_{\mathtt{R}}$ and $\mathcal{A}_{\mathtt{B}}$, the semantics for speculation over branch instructions from [21], creating all the possible compositions ($\mathcal{A}_{\mathtt{B+S}}$, $\mathcal{A}_{\mathtt{S+R}}$, $\mathcal{A}_{\mathtt{B+R}}$, and $\mathcal{A}_{\mathtt{B+S+R}}$) and proving their security (Section 5). All these semantics are mechanised in Coq, and we write 🐓 to indicate when traces are calculated mechanically.
- It extends the Spectector verification tool with all these semantics and validates this extension on both existing benchmarks (for speculation on store and return instructions) as well as on new snippets (for combined speculation) that we define (Section 6).

The rest of the paper first presents background notions, such as the security notion we rely on, and the formal language we extend with the novel speculative semantics (Section 2) and then related work (Section 8) and conclusions (Section 9).

Additional material: Full details of the semantics and proofs can be found in the technical report available at [18]. The extended version of Spectector is available at [16], whereas the mechanisation of our speculative semantics in Coq are available at [17].

2 BACKGROUND: μASM, SPECULATIVE SEMANTICS AND SECURITY DEFINITION

This section first describes the attacker model and the security definition we consider (Section 2.1). Then, it presents the syntax (Section 2.2) and the semantics (Section 2.3) of μAsm, a simple assembly-style language, followed by $\mathcal{A}_{\mathtt{B}}$, the semantics for speculation over branch instructions (Section 2.4). Most of the notions that we overview next are taken from Guarnieri et al. [21].

2.1 Attacker Model and Security Definition

We adopt a commonly-used attacker model [3, 9, 14, 19–21, 31, 38]: a passive attacker observing the execution of a program through events τ. These events, which we call *observations*, model timing leaks through cache and control flow while abstracting away low-level microarchitectural details.

$$\begin{array}{lll} \mathit{Obs} ::= \mathtt{load}\ n \mid \mathtt{store}\ n \mid \mathtt{pc}\ n \mid \mathtt{call}\ f \mid \mathtt{ret}\ n & & \tau ::= \varepsilon \mid \mathit{Obs} \\ \quad \mid \mathtt{start}_x\ n \mid \mathtt{rlb}_x\ n & & \overline{\tau} ::= \emptyset \mid \overline{\tau} \cdot \tau \end{array}$$

The $\mathtt{store}\ n$ and $\mathtt{load}\ n$ events denote read and write accesses to memory location n, so they model cache leakage. In contrast, $\mathtt{pc}\ n$, $\mathtt{call}\ f$, and $\mathtt{ret}\ n$ events record the control-flow of the program. The $\mathtt{start}_x\ n$ and $\mathtt{rlb}_x\ n$ observations denote the start and the finish of a *speculative transaction* [21] (with identifier n) produced by the speculative semantics x (we use x and y to range over the speculative semantics we define later).

An observation τ is either an event Obs or the empty observation ε. Traces $\overline{\tau}$ are sequences of observations; we indicate sequences of elements $[e_1; \cdots; e_n]$ as $\bar{e}$, and adding an element e to $\bar{e}$ as $\bar{e} \cdot e$.

The *non-speculative projection* $\restriction_{ns}$ [21] of a trace $\overline{\tau}$ deletes all speculative observations by removing all sub-traces enclosed between $\mathtt{start}_x\ n$ and $\mathtt{rlb}_x\ n$. The remaining trace, then, captures all non-speculative observations.

Speculative Non-Interference: With this trace model we can define the security property we use in this paper: *Speculative Non-Interference* (SNI) [21]. Intuitively, SNI requires that programs do not leak more information under the speculative semantics than under the non-speculative semantics.

SNI is parametric in a policy ϕ, which describes public/low information for the program, and in the used speculative semantics x, which models how the program executes. Following Guarnieri et al. [21], a policy ϕ consists of a list of public registers and public memory locations. Two configurations σ^1, σ^2 are called *low-equivalent* for a policy ϕ, written $\sigma^1 \backsim_\phi \sigma^2$, if they agree on all register and memory locations in ϕ. The *speculative semantics* x defines how (speculative) traces describing the program behaviour are generated. We indicate that program p generates trace $\overline{\tau}$ from state σ with semantic x as $\mathit{Beh}_x^{\mathcal{A}}(p, \sigma) = \overline{\tau}$. We formalise multiple speculative semantics in later sections, each one instantiating $\mathit{Beh}_x^{\mathcal{A}}(p, \sigma)$.

A program p satisfies SNI (Definition 1) for a speculative semantics x if any pair of low-equivalent initial configurations σ^1 and σ^2 that generate the same observations without speculative events also generate the same observations with speculative events too.

Definition 1 (SNI). *Program p satisfies SNI (denoted $p \vdash_x$ SNI) if for all σ^1, σ^2, if $\sigma^1 \backsim_\phi \sigma^2$ and $\mathit{Beh}_x^{\mathcal{A}}(p, \sigma^1)\restriction_{ns} = \mathit{Beh}_x^{\mathcal{A}}(p, \sigma^2)\restriction_{ns}$ then $\mathit{Beh}_x^{\mathcal{A}}(p, \sigma^1) = \mathit{Beh}_x^{\mathcal{A}}(p, \sigma^2)$.*

2.2 μAsm

$$\begin{array}{ll} \text{(Programs) } p ::= n : i \mid p_1; p_2 & \text{(Functions) } \mathcal{F} ::= \varnothing \mid \mathcal{F}; f \mapsto n \\ \text{(Registers) } x \in \mathit{Regs} & \text{(Values) } n, l \in \mathit{Vals} = \mathbb{N} \cup \{\bot\} \\ \text{(Expressions) } e ::= n \mid x \mid \ominus e \mid e_1 \otimes e_2 & \\ \text{(Instructions) } i ::= \mathbf{skip} \mid x \leftarrow e \mid \mathbf{load}\ x, e \mid \mathbf{store}\ x, e \mid \mathbf{jmp}\ e & \\ \quad \mid \mathbf{beqz}\ x, l \mid x \xleftarrow{e'?} e \mid \mathbf{spbarr} \mid \mathbf{call}\ f \mid \mathbf{ret} & \end{array}$$

μAsm is an assembly-like language whose syntax is presented above. Programs p in μAsm are sequences of mappings from natural numbers n (i.e., the instruction address) to instructions i or $\bot$. Instructions include skipping, register assignments, loads, stores, indirect jumps, conditional branches, conditional assignments, speculation barriers, calls, and returns. Instructions can refer to expressions, which are constructed by combining registers and values with unary and binary operators. Registers come from the set Regs, containing register identifiers and designated registers **pc** and **sp** modelling the program counter and stack pointer respectively, while values come from the set Vals, which includes natural numbers and $\bot$.

In the following, we use instruction keywords to denote the set of all instructions of a given type. For instance, **beqz** is the set of all branch instructions, i.e., $\mathbf{beqz} = \{\mathbf{beqz}\ x, l \mid x \in \mathit{Regs} \wedge l \in \mathit{Vals}\}$.

2.3 Non-speculative Semantics of μAsm

μAsm has a small-step operational non-speculative semantics $\rightarrow$ that describes how programs execute without speculative execution. The judgment for this semantics is $\langle p, \sigma\rangle \xrightarrow{\tau} \langle p, \sigma'\rangle$ and it reads: "*a*

program state $\langle p, \sigma\rangle$ steps to a new program state $\langle p, \sigma'\rangle$ producing observation τ". Program states $\langle p, \sigma\rangle$ consist of the program p and the configuration σ. The program p is used to look up the current instruction, whereas the configuration $\sigma = \langle m, a\rangle$ is used to read from/write to the memory m and register file a. Memories map addresses (which are natural numbers) to values, whereas register files map register identifiers to values.

Most of the rules of the semantics are standard and thus omitted; we present selected rules below (see [21] for all rules). The rules rely on the evaluation of expressions (indicated as $[\![e]\!](a) = n$) where expression e is evaluated to value n under register file a. In the rules, $a[x \mapsto n]$, where $x \in Regs \cup \mathbb{N}$ and $n \in Vals$, denotes the update of a map (memory or registers), whereas $a(x)$ denotes reading from a map. Finally, $\sigma(x)$, where $x \in Regs$ and $\sigma = \langle m, a\rangle$, denotes $a(x)$.

$$\frac{\text{(Store)}\quad p(a(\mathbf{pc})) = \mathbf{store}\ x, e \qquad n = [\![e]\!](a)}{\langle p, \langle m, a\rangle\rangle \xrightarrow{\texttt{store}\ n} \langle p, \langle m[n \mapsto a(x)], a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1]\rangle\rangle}$$

$$\frac{\text{(Beqz-Sat)}\quad p(a(\mathbf{pc})) = \mathbf{beqz}\ x, \ell \qquad a(x) = 0}{\langle p, \langle m, a\rangle\rangle \xrightarrow{\texttt{pc}\ \ell} \langle p, \langle m, a[\mathbf{pc} \mapsto \ell]\rangle\rangle}$$

$$\frac{\text{(Call)}\quad \begin{array}{ll} p(\sigma(\mathbf{pc})) = \mathbf{call}\ f & \mathcal{F}(f) = n \\ a' = a[\mathbf{pc} \mapsto n, sp \mapsto a(sp) - 8] & m' = [a'(sp) \mapsto a(\mathbf{pc}) + 1]\end{array}}{\langle p, \langle m, a\rangle\rangle \xrightarrow{\texttt{call}\ f} \langle p, \langle m', a'\rangle\rangle}$$

$$\frac{\text{(Return)}\quad \begin{array}{ll} p(\sigma(\mathbf{pc})) = \mathbf{ret} & l = m(a(sp)) \\ a' = a[pc \mapsto l, sp \mapsto a(sp) + 8] & \end{array}}{\langle p, \langle m, a\rangle\rangle \xrightarrow{\texttt{ret}\ l} \langle p, \langle m, a'\rangle\rangle}$$

Branch instructions emit observations recording the outcome of the branch (Rule Beqz-Sat), while memory operations emit observations recording the accessed memory (Rule Store). A call to function f is a jump to the function's starting line number n, as indicated by the function map $\mathcal{F}$. A call stores the return address on the stack at the value of the stack pointer **sp** and decreases **sp** (Rule Call). A return does the inverse: it looks up the return address via the stack pointer **sp** and then increases the stack pointer (Rule Return).

The *non-speculative behaviour* $Beh_{NS}(p)$ of a program p is the set of all traces generated from an initial state until termination using the reflexive-transitive-closure of the non-speculative semantics.

2.3.1 Symbolic semantics. Following [21], we introduce a *symbolic* non-speculative semantics $\rightarrow^{\mathcal{S}}$ that is at the basis of Spectector's analysis. This symbolic semantics differs from $\rightarrow$ in two key ways: (1) concrete configurations σ are replaced with symbolic configurations $\sigma^{\mathcal{S}}$, and (2) path condition constraints are generated in the standard way and they are encoded as part of the symbolic trace $\overline{\tau}$. Given a symbolic trace $\overline{\tau}$, $\mu(\overline{\tau})$ denotes the set of all concrete traces that can be obtained by concretising $\overline{\tau}$ with values consistent with $\overline{\tau}$'s path condition. The *symbolic non-speculative behavior* $Beh^{\mathcal{S}}_{NS}(p)$ of a program p consists of all symbolic traces derived by applying $\rightarrow^{\mathcal{S}}$, and $\mu(Beh^{\mathcal{S}}_{NS}(p))$ is the set of all concrete traces derived from p's symbolic traces. As proved by Guarnieri et al. [21], $Beh_{NS}(p) = \mu(Beh^{\mathcal{S}}_{NS}(p))$.

2.4 $\mathcal{B}$: Speculating Over Branch Instructions

To model and reason about the effects of speculation over branch instructions, Guarnieri et al. [21] propose three related semantics: an always-mispredict semantics (Section 2.4.1), an oracle semantics (Section 2.4.2), and a symbolic semantics (Section 2.4.3). The always-mispredict semantics, our main focus, is a safe overapproximation of the oracle semantics, which explicitly models the behavior of the branch predictor using a prediction oracle. Finally, the symbolic semantics, which is used in the Spectector program analysis tool, is the symbolic version of the always-mispredict semantics. We summarize the properties of these semantics in Section 2.4.4. With a slight abuse of notation, $\mathcal{B}$ indicates both the three speculative semantics, and the AM one alone (since it is the most relevant one).

2.4.1 Always-mispredict (AM) Semantics. At every branch instruction, the always-mispredict semantics first speculatively executes the wrong branch for a fixed number of steps and then continues with the correct one. As a result, this semantics is deterministic and agnostic to implementation details of the branch predictor [21].

The state $\Sigma_{\mathcal{B}}$ of the AM semantics is a stack of speculative instances $\Phi_{\mathcal{B}}$ where reductions happen only on top of the stack. Whenever we start speculating, a new instance is pushed on top of the stack (Rule B:AM-branch). The instance is then popped when speculation ends (Rule B:AM-Rollback). Each instance $\Phi_{\mathcal{B}}$ contains the program p, a counter *ctr* that uniquely identifies the speculation instance, a configuration σ, and the remaining speculation window n describing the number of instructions that can still be executed speculatively (or $\perp$ when no speculation is happening). Throughout the paper, we fix the maximal speculation window, i.e., the maximum number of speculative instructions, to a global constant ω.

$$\textit{Spec. States}\ \Sigma_{\mathcal{B}} ::= \overline{\Phi}_{\mathcal{B}} \qquad \textit{Spec. Instances}\ \Phi_{\mathcal{B}} ::= \langle p, ctr, \sigma, n\rangle$$

This judgement for the AM semantics is: $\Sigma_{\mathcal{B}} \overset{\tau}{\rightsquigarrow}_{\mathcal{B}} \Sigma'_{\mathcal{B}}$.

$$\frac{\begin{array}{c}\text{(B:AM-branch)}\quad p(\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell \qquad \langle p, \sigma\rangle \xrightarrow{\tau} \langle p, \sigma'\rangle \qquad j = min(\omega, n) \\ \sigma'' = \sigma[\mathbf{pc} \mapsto l'] \qquad \overline{\tau} = \tau \cdot \texttt{start}_{\mathcal{B}}\ ctr \cdot \texttt{pc}\ l \\ l' = \begin{cases}\sigma(\mathbf{pc}) + 1 & \text{if } \sigma'(\mathbf{pc}) = l \\ l & \text{if } \sigma'(\mathbf{pc}) \neq l\end{cases}\end{array}}{\langle p, ctr, \sigma, n+1\rangle \overset{\overline{\tau}}{\rightsquigarrow}_{\mathcal{B}} \langle p, ctr, \sigma', n\rangle \cdot \langle p, ctr+1, \sigma'', j\rangle}$$

$$\frac{\text{(B:AM-NoSpec)}\quad p(\sigma(\mathbf{pc})) \notin \mathbf{beqz} \cup Z_{\mathcal{B}} \qquad \langle p, \sigma\rangle \xrightarrow{\tau} \langle p, \sigma'\rangle}{\langle p, ctr, \sigma, n+1\rangle \overset{\tau}{\rightsquigarrow}_{\mathcal{B}} \langle p, ctr, \sigma', n\rangle}$$

$$\frac{\text{(B:AM-Rollback)}\quad n' = 0 \text{ or p is stuck}}{\langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle \xrightarrow{\texttt{rlb}_{\mathcal{B}}\ ctr}_{\mathcal{B}} \langle p, ctr', \sigma, n\rangle}$$

As mentioned, Rule B:AM-branch pushes a new speculative state with the wrong branch, followed by the state with the correct one. When speculation ends, Rule B:AM-Rollback pops the related state. All other instructions are handled by delegating back to the non-speculative semantics (Rule B:AM-NoSpec).

Rule B:AM-NoSpec differs slightly from [21]: it applies to instructions that are not branch instructions (as in [21]) and are not in

the metaparameter Z_B (in gray). The latter is a set of instructions and is part of our composition framework (which we explain in Section 4.1). Instantiating Z_B allows us to restrict when to apply non-speculative steps in composed semantics. When we consider λ_B in isolation, Z_B is the empty set (so, Rule B:AM-NoSpec applies to everything except branch instructions as in [21]). However, we will instantiate Z_B in different manners when building the composed semantics. In the following, we write $\lambda_B^{Z_B}$ to stress the value of Z_B when needed but we often omit Z_B for simplicity.

The always-mispredict behaviour $Beh_B^{\mathcal{A}}(p)$ of a program p is the set of all traces generated from an initial state until termination using the reflexive-transitive closure of $\xrightarrow{}\!\!\!\!\!\!\lambda_B$.

2.4.2 Oracle Semantics. The oracle semantics explicitly models the branch predictor using an oracle O_B that relies on the branching history h of the program p to predict branch outcomes.

Here, we quickly summarize the key differences with the AM semantics; see [21] for the full definition. First, speculative instances are extended to track the branching history h, which records the outcomes of prior branch instructions. Second, when executing a **beqz** instruction, the oracle predicts the branch outcome (based on the branching history h) and a new speculative instance is pushed on top of the stack. Finally, whenever the speculation window of an instance anywhere on the stack reaches 0, the execution needs to be rolled back or committed. Rolling back deletes all the instances above the rolled back instance, whereas committing updates the configuration, the counter and the branching history h of the instance below and the committed instance is deleted.

As before, the behaviour $Beh_B^{O}(p)$ of a program p under the oracle semantics is the set of all its traces until termination.

2.4.3 Symbolic Semantics. The symbolic speculative semantics $\lambda_B^{\mathcal{S}}$ works on symbolic speculative states $\Sigma_B^{\mathcal{S}}$, and it is used in Spectector [21]. The only two differences w.r.t. the AM semantics are that (1) concrete states Σ_B are replaced with symbolic states $\Sigma_B^{\mathcal{S}}$, which store symbolic configurations $\sigma^{\mathcal{S}}$ instead of concrete configurations σ, and (2) the semantics uses the symbolic non-speculative semantic instead of the concrete one. The rules of the symbolic semantics look like those of the AM one, and the behaviour $Beh_B^{\mathcal{S}}(p)$ of a program p is defined as for the AM semantics.

2.4.4 Properties of λ_B. Guarnieri et al. [21] prove several properties relating the three semantics we presented above, which were instrumental in proving Spectector's security. We recap these properties in a single definition (Definition 2), which we will prove for all semantics in this paper. In the definition we indicate that a program p satisfies SNI w.r.t. the oracle semantics as $p \vdash_B^O$ SNI.

Definition 2 (Secure Speculative Semantics). *A speculative semantics λ_x is secure (denoted $\vdash \lambda_x$ SSS) if:*

- *Oracle Overapproximation: $p \vdash_x$ SNI iff $\forall O.\ p \vdash_x^O$ SNI*
- *Symbolic Consistency: $Beh_x^{\mathcal{A}}(p) = \mu(Beh_x^{\mathcal{S}}(p))$*
- *NS Consistency: $Beh_x^{\mathcal{A}}(p)\restriction_{ns} = Beh_{NS}(p) = Beh_x^{O}(p)\restriction_{ns}$*

Intuitively, a secure speculative semantics is made of three components: an AM semantics, an oracle semantics, and a symbolic semantics. First, the AM semantics must overapproximate the oracle semantics (for any oracle), so it is enough to check a program p for SNI w.r.t. the AM semantics [21, Theorem 1]. Then, since Spectector uses the symbolic semantics in the implementation, the symbolic semantics must be consistent w.r.t. the AM one [21, Proposition 2]. Finally, both the AM and the Oracle semantics can recover the non-speculative behaviour of a program p by applying the non-speculative projection on their traces [21, Propositions 1,3]. So we can execute p only once to get the (non-)speculative behaviour of that program run.

Theorem 1 states that λ_B is a secure speculative semantics.

Theorem 1 (λ_B is *SSS* [21]). $\vdash \lambda_B$ *SSS*

3 SPECULATION ON STORES AND RETURNS

This section defines λ_S and λ_R, two novel speculative semantics that model the effects of speculative execution over **store** instructions (Section 3.1) and **ret** instructions (Section 3.2). Similarly to λ_B, for each speculation mechanism we define three semantics: an always-mispredict semantics, an oracle semantics, and a symbolic semantics. As before, we will mostly focus on the always-mispredict semantics, which safely over-approximates the oracle one, and we will use its symbolic version to reason about leaks using Spectector. Most formal details, as well as proofs, can be found in the companion technical report [18].

3.1 λ_S: Speculation on Store Instructions

Modern processors write **store**s to main memory asynchronously to reduce delays caused by the memory subsystem. For this, processors employ a *Store Queue* where not-yet-committed **store** instructions are stored before being permanently written to memory. When executing a **load** instruction, the processor first inspects the store queue for a matching memory address. If there is a match, the value is retrieved from the store queue (called *store-to-load forwarding*), and otherwise the memory request is issued to the memory subsystem. To speed up computation, processors employ memory disambiguation predictors to predict if memory addresses of loads and stores match. Since the prediction can be incorrect, processors may speculatively bypass a **store** instruction in the store queue leading to a **load** instruction retrieving a stale value.

Example 1 (Store Speculation Vulnerability). Consider the example in Listing 2:

Listing 2: Code vulnerable to store speculation.

```
1 store secret, p
2 store public, p
3 load eax, p
4 load edx, B + eax
```

Assume that the **store** instructions in Line 1 and Line 2 are still in the *store queue* and not yet committed to main memory. A misprediction of the memory disambiguator for the **load** instruction in Line 3 causes it to bypass the **store** instruction in Line 2 and retrieve the value from the stale **store** instruction in Line 1. The speculative access of the memory is then leaked into the microarchitectural state by the array access into B in Line 4.

This section first introduces the extended trace model required to talk about speculation over **store** instructions (Section 3.1.1).

Next, it presents the speculative AM semantics (Section 3.1.2) and the corresponding oracle semantics (Section 3.1.3) and symbolic semantics (Section 3.1.4). This semantics is a secure speculative semantics (Theorem 2).

Theorem 2 ($\mathcal{L}_S$ is *SSS*). $\vdash \mathcal{L}_S$ *SSS*

3.1.1 Extended Trace Model. We extend the trace model *Obs* with $\texttt{start}_S\ n$ and $\texttt{rlb}_S\ n$ observations to mark start and end of a speculative transaction n started by a store bypass. Furthermore, we add a $\texttt{bypass}\ n$ observation denoting that the **store** instruction at program counter n was speculatively bypassed.

$$Obs_S ::= Obs \mid \texttt{start}_S\ n \mid \texttt{rlb}_S\ n \mid \texttt{bypass}\ n$$

3.1.2 Speculative Semantics. The overall structure of the $\mathcal{L}_S$ semantics is similar to that of $\mathcal{L}_B$: speculative execution is modeled using a stack of speculative states, instructions that do not start speculative transactions are executed by delegating back to the non-speculative semantics, and speculative transactions are rolled back whenever the speculative window reaches 0. The key difference between $\mathcal{L}_S$ and $\mathcal{L}_B$ is the differing source of speculation: **beqz** instructions for $\mathcal{L}_B$ and **store** instructions for $\mathcal{L}_S$.

The states used in $\mathcal{L}_S$ are similar to those of $\mathcal{L}_B$:

$$\textit{Spec. States}\ \Sigma_S ::= \overline{\Phi}_S \qquad \textit{Spec. Instance}\ \Phi_S ::= \langle p, ctr, \sigma, n\rangle$$

Judgement $\Sigma_S \overset{\tau}{\rightharpoonup\!\!\!\!\!\!\mathcal{L}_S} \Sigma'_S$ describes how Σ_S steps to Σ'_S emitting observation τ. As in $\mathcal{L}_B$, reductions only happen on top of the stack.

$$\frac{\begin{array}{c}p(\sigma(\mathbf{pc})) = \mathbf{store}\ x, e \qquad \langle p, \sigma\rangle \xrightarrow{\tau} \langle p, \sigma'\rangle \qquad j = min(\omega, n)\\ \sigma'' = \sigma[\mathbf{pc} \mapsto \sigma(\mathbf{pc}) + 1] \qquad \tau' = \tau \cdot \texttt{bypass}\ \sigma(\mathbf{pc}) \cdot \texttt{start}\ ctr\end{array}}{\langle p, ctr, \sigma, n+1\rangle \overset{\tau'}{\rightharpoonup\!\!\!\!\!\!\mathcal{L}_S} \langle p, ctr, \sigma', n\rangle \cdot \langle p, ctr+1, \sigma'', j\rangle}\ \text{(S:AM-Store)}$$

$$\frac{p(\sigma(\mathbf{pc})) \notin \mathbf{store} \cup Z_S \qquad \langle p, \sigma\rangle \xrightarrow{\tau} \langle p, \sigma'\rangle}{\langle p, ctr, \sigma, n+1\rangle \overset{\tau}{\rightharpoonup\!\!\!\!\!\!\mathcal{L}_S} \langle p, ctr, \sigma', n\rangle}\ \text{(S:AM-NoSpec)}$$

To model the effect of bypassing a **store** instruction, Rule S:AM-Store bypasses the **store** instruction by increasing the program counter without updating the memory and starts a new speculative transaction by pushing a new speculative instance on top of the state. A **load** instruction loading from the same memory location as the bypassed **store** instruction, therefore, retrieves a stale value.

Similarly to $\mathcal{L}_B$, all instructions that are not **store** instructions (and are not in Z_S) are handled by delegating back to the non-speculative semantics (Rule S:AM-NoSpec) and when the speculation window reaches 0, a roll back occurs that pops the topmost speculative instance from the stack.

The set $Beh_S^{\mathcal{A}}(p)$ contains all traces generated from an initial state until termination using the reflexive-transitive closure of $\overset{\tau}{\rightharpoonup\!\!\!\!\!\!\mathcal{L}_S}$.

3.1.3 Oracle Semantics. Instead of bypassing every **store** instruction, the oracle semantics employs an oracle O that decides if the **store** instruction should be speculatively bypassed or not. As before, the behaviour $Beh_S^O(p)$ of a program p is the set of all traces starting from an initial state until termination using the reflexive-transitive closure of the oracle semantics.

3.1.4 Symbolic Semantics. Similarly to $\mathcal{L}_B^S$, the symbolic speculative semantics $\mathcal{L}_S^S$ requires two changes w.r.t. the always-mispredict one: concrete configurations σ and the non-speculative semantics are replaced by symbolic configurations σ^S and the symbolic non-speculative semantics respectively. The behaviour $Beh_S^S(p)$ of a program p is the set of all its symbolic traces.

3.2 $\mathcal{L}_R$: Speculation on Return Instructions

The return-stack-buffer (RSB) is a small stack used by the CPU to save return addresses upon **call** instructions. These saved return addresses are speculatively used when the function returns, because accessing the RSB is faster than looking up the return address on the stack (stored in main memory). This works well because return addresses rarely change during function execution. However, mispredictions can be exploited by an attacker.

Example 2 (Return Speculation Vulnerability)**.** Consider the example in Listing 3 and recall that register **sp** is used to find return addresses saved on the stack.

Listing 3: A program exploiting RSB speculation.

```
1  Manip_Stack:
2      sp ← sp + 8
3      ret
4  Speculate:
5      call Manip_Stack
6      load eax, secret
7      load edx, eax
8      ret
9  Main:
10     call Speculate
11     skip
```

Each function call pushes a return address on the stack and decrements the **sp** register. After reaching the function *Manip_Stack*, the **sp** register is incremented (line 2). Thus, **sp** points to the previous return address on the stack (i.e., line 11), and the non-speculative execution continues in *Main* and terminates. However, the return address of the call in line 5 is line 6 and it is on top of the RSB. Thus, the CPU speculatively executes lines 6–7 and leaks the secret.

This section describes the AM semantics (Section 3.2.1), the oracle semantics (Section 3.2.2), and the symbolic semantics (Section 3.2.3). Then, it discusses formalising different implementations of the RSB in the CPU (Section 3.2.4). This semantics is a secure speculative semantics (Theorem 3).

Theorem 3 ($\mathcal{L}_R$ is *SSS*). $\vdash \mathcal{L}_R$ *SSS*

3.2.1 Speculative Semantics. Unlike before, the state of $\mathcal{L}_R$ contains a model of the RSB which is used to retrieve return addresses instead of relying on the stack. Thus, speculative instances of $\mathcal{L}_R$ are extended with an additional entry $\mathbb{R}$ for tracking the RSB, whose size is limited by a global constant $\mathbb{R}_{size}$ denoting the maximal RSB size. A speculative instance Φ_R now consists of the program p, the counter ctr, the configuration σ, the speculation window ω and the RSB $\mathbb{R}$. As before, a state Σ_R is a stack of speculative instances $\overline{\Phi}_R$.

$$\textit{Spec. States}\ \Sigma_R ::= \overline{\Phi}_R \qquad \textit{Spec. Instance}\ \Phi_R ::= \langle p, ctr, \sigma, \mathbb{R}, n\rangle$$

As before, in $\Sigma_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \Sigma_{\mathsf{R}}$ reductions happen on the top of the stack.

$$\frac{\begin{array}{ccc} p(\sigma(\mathbf{pc})) = \mathbf{ret} & \sigma = \langle m, a\rangle & \langle p, \sigma\rangle \xrightarrow{\tau} \langle p, \sigma'\rangle \\ \mathbb{R} = \mathbb{R}' \cdot l & j = min(\omega, n) & l \neq m(a(\mathbf{sp})) \\ \sigma'' = \sigma[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto a(\mathbf{sp}) + 8] & & \overline{\tau} = \tau \cdot \mathtt{start}_{\mathsf{R}}\ ctr \cdot \mathtt{ret}\ l \end{array}}{\langle p, ctr, \sigma, \mathbb{R}, n+1\rangle \overset{\overline{\tau}}{\rightsquigarrow}_{\mathsf{R}} \langle p, ctr, \sigma', \mathbb{R}', n\rangle \cdot \langle p, ctr+1, \sigma'', \mathbb{R}', j\rangle}\ (\mathsf{R}\text{:AM-Ret-Spec})$$

$$\frac{\begin{array}{cc} p(\sigma(\mathbf{pc})) = \mathbf{call}\ f & \langle p, \sigma\rangle \xrightarrow{\tau} \langle p, \sigma'\rangle \\ \mathbb{R}' = \mathbb{R} \cdot \langle a(\mathbf{pc}) + 1\rangle & |\mathbb{R}| < \mathbb{R}_{size} \end{array}}{\langle p, ctr, \sigma, \mathbb{R}, n+1\rangle \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \langle p, ctr, \sigma', \mathbb{R}', n\rangle}\ (\mathsf{R}\text{:AM-Call})$$

During **call** instructions (Rule R:AM-Call), the return address is pushed on top of the RSB (if there is space available) and during **ret** instructions, the return address stored on the RSB is used if the entry on top of the RSB is different from the one stored on the stack (Rule R:AM-Ret-Spec). Then, the rule creates a new speculative instance that uses the return address from the RSB $\mathbb{R}$. Note that speculation only happens when the return address from the RSB differs from the one on the stack (stored in $m(a(\mathbf{sp}))$).

Here, we overview how our semantics behaves with empty and full RSB; full formalisation is available in the technical report [18]. Whenever the RSB is empty, executing a **ret** instruction does not cause speculation and we return to the address pointed by **sp**. In contrast, whenever the RSB is full, executing a **call** instruction does not add entries to the RSB, i.e., we model an *acyclic* RSB.[1]

The behaviour $Beh^{\mathcal{A}}_{\mathsf{R}}(p)$ is the set of all traces generated from an initial state until termination using $\rightsquigarrow_{\mathsf{R}}$.

3.2.2 Oracle Semantics. Unlike before, the oracle cannot decide the outcome of the **ret** instruction, because the CPU always uses the return address stored in the RSB (if there is one) and it does not speculate otherwise [9]. The only thing the oracle decides here is the size of the speculation window ω.

3.2.3 Symbolic Semantics. Just as before, the symbolic speculative semantics $\rightsquigarrow^{\mathcal{S}}_{\mathsf{R}}$ replaces concrete configurations and the non-speculative semantics with symbolic configurations and the symbolic non-speculative semantics respectively. We remark that the program counter **pc** is *always* concrete in the symbolic non-speculative semantics [21]. As a result, the RSB only contains concrete values (and return addresses). The behaviour $Beh^{\mathcal{S}}_{\mathsf{R}}(p)$ of a program p is the set of all traces starting from an initial state until termination using the reflexive-transitive closure of the symbolic semantics.

3.2.4 Different Behaviours of Empty and Full RSBs. Modern CPUs use different RSB implementations that differ in the way they handle underflows and overflows, i.e., when the RSB is empty or full [27]. For example, cyclic RSB implementations overwrite old entries when the RSB is full. Alternatively, CPUs can fallback to other predictors (like the indirect branch predictor) to predict return addresses whenever the RSB is empty.

In our model, the RSB is not cyclic and there is no speculation when the RSB is empty (Rule R:AM-Ret-Empty).

[1] We follow the way AMD processors handle this kind of speculation [27].

$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{ret} \qquad \langle p, \sigma\rangle \xrightarrow{\tau} \langle p, \sigma'\rangle}{\langle p, ctr, \sigma, \emptyset, n+1\rangle \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \langle p, ctr, \sigma', \emptyset, n\rangle}\ (\mathsf{R}\text{:AM-Ret-Empty})$$

We remark that extending $\rightsquigarrow_{\mathsf{R}}$ to support different RSBs implementations can be done with minimal effort.

4 A FRAMEWORK FOR COMPOSING SPECULATIVE SEMANTICS

The presented speculative semantics allow us to verify programs for violations of SNI but they do not capture the vulnerability in Listing 1, as the traces of Example 3 show.

Example 3 (SNI for Listing 1). The traces generated are:

$$\overline{\tau}^1_{\mathsf{B}} = \overline{\tau}^2_{\mathsf{B}} := \mathtt{store}\ p \cdot \mathtt{store}\ p \cdot \mathtt{start}_{\mathsf{B}}\ 0 \cdot \mathtt{load}\ p \cdot \mathtt{load}\ A + public \cdot \mathtt{rlb}_{\mathsf{B}}\ 0 \cdot \mathtt{pc}\ 9$$

$$\overline{\tau}^1_{\mathsf{S}} = \overline{\tau}^2_{\mathsf{S}} := \ldots \cdot \mathtt{store}\ p \cdot \mathtt{start}_{\mathsf{S}}\ 1 \cdot \mathtt{bypass}\ 1 \cdot \mathtt{pc}\ \bot \cdot \mathtt{rlb}_{\mathsf{S}}\ 1 \cdot \mathtt{pc}\ \bot$$

The program in Listing 1 seems secure since there is no secret value leaked in the speculative transaction; thus the program satisfies SNI for $\rightsquigarrow_{\mathsf{B}}$ and $\rightsquigarrow_{\mathsf{S}}$ in isolation. However, this program speculatively leaks when considering speculation over **beqz** and **store** instructions, but we need our combined semantics to detect this vulnerability; see Section 5.3.

The vulnerability only appears when the branch predictor (Section 2.4.1) and the memory disambiguator (Section 3.1.2) are used *together*. Intuitively, we know that CPUs use all the speculation mechanisms described here (and many others as well) at the same time. Thus, we should not only focus on these different speculation mechanisms in *isolation* but we need to look at their *combinations* as well. That is, we need a way to compose the different semantics into new semantics that can reason about these "combined" leaks.

This section presents a novel, general framework for composing two speculative semantics x and y, each one capturing the effects of a single speculation mechanism, to allow for speculation from both mechanisms x and y. The semantics x and y are also called the *source* semantics of the composition. Next, we first introduce the new composed semantics, which consists of an always-mispredict semantics, an oracle semantics, and a symbolic semantics (Section 4.1). Then, we present the notion of *well-formed* composition which we use to study the properties of composed semantics (Section 4.2).

New Notation. The states Σ_{xy}, instances Φ_{xy}, and the trace model Obs_{xy} are defined as the union of the source parts. Furthermore, we define a projection function $\upharpoonright_{xy}$ and two projections $\upharpoonright^{x}_{xy}$ and $\upharpoonright^{y}_{xy}$ that return the first and second projection of the pair from $\upharpoonright_{xy}$. These functions are lifted to states by applying them pointwise:

$$Obs_{xy} := Obs_x \cup Obs_y \qquad \Phi_{xy} := \Phi_x \cup \Phi_y \qquad \Sigma_{xy} := \Sigma_x \cup \Sigma_y$$

$$\upharpoonright_{xy} \colon \Phi_{xy} \mapsto (\Phi_x, \Phi_y) \qquad \upharpoonright^{x}_{xy} \colon \Phi_{xy} \mapsto \Phi_x \qquad \upharpoonright^{y}_{xy} \colon \Phi_{xy} \mapsto \Phi_y$$

For example, the $\Phi_{\mathsf{S+R}}$ state resulting from the union of Φ_{S} and Φ_{R} states (from Section 3.1.2 and Section 3.2.1 respectively) is $\langle p, ctr, \sigma, \mathbb{R}, n\rangle$, as it contains all common elements (the program p, the counter ctr, the state σ, and the speculation count n) plus the

return stack buffer $\mathbb{R}$ from Φ_R only. Taking the $\cdot\restriction^S_{S+R}$ of a Φ_{S+R} state returns the Φ_S subpart, i.e., all but the return stack buffer.

We overload $\restriction^x_{xy}$ and $\restriction^y_{xy}$ to also work on traces $\overline{\tau}$. The projection $\tau\restriction^x_{xy}$ deletes all speculative transactions (marked by $\texttt{start}_y\ id$ and $\texttt{rlb}_y\ id$) not generated by the source semantics x. The definition of $\restriction^y_{xy}$ is similar by replacing x with y:

$$\varepsilon\restriction^x_{xy} = \varepsilon \qquad (\tau\cdot\overline{\tau})\restriction^x_{xy} = \tau\cdot(\overline{\tau})\restriction^x_{xy}$$
$$(\texttt{start}_y\ id\cdot\cdots\texttt{rlb}_y\ id\cdot\overline{\tau})\restriction^x_{xy} = \overline{\tau}\restriction^x_{xy}$$

We indicate source semantics for x and y as $\mathcal{A}_x$ and $\mathcal{A}_y$ respectively and use $\mathcal{A}_{xy}$ to indicate the composed semantics.

4.1 Combined Speculative Semantics

The combined semantics delegates back to the source semantics of x and y to model the effects of both speculation mechanisms (modeled by x and y). This is captured in the two core rules below:

$$\text{(AM-x-step)}\quad \frac{\Phi_{xy}\restriction^x_{xy} \overset{\tau}{\dashrightarrow}_x^{Z_{xy}\restriction^x_{xy}} \overline{\Phi}'_{xy}\restriction^x_{xy}}{\Phi_{xy} \overset{\tau}{\dashrightarrow}_{xy}^{Z_{xy}} \overline{\Phi}'_{xy}}$$

$$\text{(AM-y-step)}\quad \frac{\Phi_{xy}\restriction^y_{xy} \overset{\tau}{\dashrightarrow}_y^{Z_{xy}\restriction^y_{xy}} \overline{\Phi}'_{xy}\restriction^y_{xy}}{\Phi_{xy} \overset{\tau}{\dashrightarrow}_{xy}^{Z_{xy}} \overline{\Phi}'_{xy}}$$

The combined semantics does a step by either delegating back to the x source semantics (Rule AM-x-step) or to the y one (Rule AM-y-step).[2] The rules rely on metaparameter Z_{xy}, which is a pair of two metaparameters $Z_{xy} := (Z_x, Z_y)$ — one for x and one for y. We overload the projections $\restriction^x_{xy}$ and $\restriction^y_{xy}$ to extract the corresponding metaparameter from Z_{xy}, e.g., $Z_{xy}\restriction^x_{xy} = Z_x$.

The role of Z is central to making the composed semantics work as expected. It restricts how the combined semantics delegates execution to the components to ensure that the correct rule is applied.

With $Z = (\emptyset, \emptyset)$, consider the execution of the **beqz** instruction in Line 4 in Listing 1. The combined semantics $\mathcal{A}_{B+S}$ can use Rule AM-x-step to delegate back to $\mathcal{A}_B$ for **beqz** instructions, creating a new speculative transaction (Rule B:AM-branch). However, $\mathcal{A}_{B+S}$ can also use Rule AM-y-step, because **beqz** instructions are also handled by $\mathcal{A}_S$. Unfortunately, this does not start speculation, which happens only on **store** instructions (Rule S:AM-NoSpec).

Intuitively, $\mathcal{A}_{B+S}$ should delegate back to $\mathcal{A}_B$, so Rule AM-y-step should not be applicable. This can be obtained by instantiating $Z_{B+S} = (\textbf{store}, \textbf{beqz})$, so that its projections are $Z_B = \textbf{store}$ and $Z_S = \textbf{beqz}$. Now, $\mathcal{A}_{B+S}$ can only apply Rule AM-x-step on the **beqz** of Line 4, because Z_S ensures that $\mathcal{A}_S$ cannot execute **beqz** instructions, as depicted in the full rule for $\mathcal{A}_S^{\textbf{beqz}}$ below (where we indicate the instructions derived from $Z_S = \textbf{beqz}$ in blue):

$$\text{(S:AM-NoSpec)}\quad \frac{p(\sigma(\textbf{pc})) \notin \textbf{store} \cup \textbf{beqz} \qquad \langle p,\sigma\rangle \xrightarrow{\tau} \langle p,\sigma'\rangle}{\langle p, ctr, \sigma, n+1\rangle \overset{\tau}{\dashrightarrow}_S^{\textbf{beqz}} \langle p, ctr, \sigma', n\rangle}$$

[2] To simplify notation, we omit that the $\Phi_x \setminus \Phi_y$ parts of state Φ_{xy} in x-step (similar $\Phi_y \setminus \Phi_x$ in y-step) do not change between Φ_{xy} and $\overline{\Phi}'_{xy}$.

Having clarified the intuition behind the semantics, we can define the behaviour $Beh^{\mathcal{A}}_{xy}$ as the set of all traces generated from initial states until termination using $\dashrightarrow_{xy}$.

4.1.1 Oracle Combination. Instead of using one oracle, the combination uses a pair of oracles, one from each source semantics. When delegating back to either source, the correct oracle of the source is handed over to the source semantics.

4.1.2 Symbolic Combination. Instead of using the AM semantics for delegation, the combined symbolic semantics $\mathcal{A}^S_{xy}$ uses the symbolic source semantics for delegation. Furthermore, the new notation (union, projections) is lifted to the symbolic combination to create the symbolic states Σ^S_{xy}. The behaviour $Beh^S_{xy}(p)$ of program p is the set of all traces generated using the symbolic semantics.

4.2 Properties of Composition

We now illustrate the benefits of our composition framework. For this, we first introduce a notion of well-formed composition (Section 4.2.1), which intuitively tells when a combined semantics "makes sense". Then, we show that for well-formed compositions, if the source semantics are *SSS*, so is the combined semantics (Section 4.2.2). Since we proved this property for *any* well-formed composition in our framework, all (well-formed) compositions we present in Section 5 are *SSS for free*. This proof reuse and extensibility is our framework's key advantage over having ad-hoc semantics combining multiple speculation mechanisms, which requires one to manually prove the *SSS* results we instead obtain for free.

4.2.1 Well-formed Compositions. The well-formedness conditions for the composition ensures that the delegation is done properly (Definition 3), they are the *minimal* set of assumptions that let us derive *SSS* of the combined semantics for free:

Definition 3 (Well-formed composition)**.** *A composition $\mathcal{A}_{xy}$ of two speculative semantics $\mathcal{A}_x$ and $\mathcal{A}_y$ is* well-formed*, written $\vdash \mathcal{A}_{xy}$: WFC, if:*

(1) (Confluence) *Whenever $\Sigma_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma'_{xy}$ and $\Sigma_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma''_{xy}$, then $\Sigma'_{xy} = \Sigma''_{xy}$.*

(2) (Projection preservation) *For all p, $Beh^{\mathcal{A}}_x(p) = Beh^{\mathcal{A}}_{xy}(p)\restriction^x_{xy}$ and $Beh^{\mathcal{A}}_y(p) = Beh^{\mathcal{A}}_{xy}(p)\restriction^y_{xy}$.*

(3) (Relation preservation) *If $\Sigma_{xy} \approx_{xy} X_{xy}$ and $\Sigma_{xy} \overset{\overline{\tau}}{\dashrightarrow}^*_{xy} \Sigma'_{xy}$ then $X_{xy} \overset{\overline{\tau}, O_{xy}}{\rightsquigarrow}{}^*_{xy} X'_{xy}$ and $\Sigma'_{xy} \approx_{xy} X'_{xy}$.*

(4) (Symbolic preservation) *If $\Sigma^S_{xy} \overset{\tau_S}{\dashrightarrow}_{xy} \Sigma^S_{xy}$ and $\mu(\Sigma^S_{xy}) = \Sigma_{xy}$, then there is Σ'_{xy} s.t. $\Sigma_{xy} \overset{\mu(\tau_S)}{\dashrightarrow}_{xy} \Sigma'_{xy}$ and $\mu(\Sigma^{S'}_{xy}) = \Sigma'_{xy}$.*

Next, we explain the well-formedness conditions:

- Confluence (point 1) ensures that the non-determinism of the combined semantics (that non-deterministically delegates back to its sources) is not harmful. Consider the assignment in Line 1 in Listing 1. $\mathcal{A}_{B+S}$ can delegate to either $\mathcal{A}_B$ or $\mathcal{A}_S$ to reduce the assignment. If the combined semantics is *confluent*, then it does not matter which source rule executes the assignment in Line 1 in Listing 1, the semantics reaches the same state either way.

• Projection preservation (point 2) ensures that the combined semantics is not hiding or forgetting traces of its sources. Any observable emitted by a source semantics must be propagated to the combined one, this is also the reason why Obs_{xy} is defined as the union of the source *Obs*.

• To explain relation preservation (point 3), we need to mention a technical detail: the state relation (denoted $\approx_{xy}$ and defined in our technical report) between the AM states (Σ_{xy}) and the Oracle ones (X_{xy}). Intuitively, two states are related if they are the same or if one is waiting on a speculation of the other to end. Then, point (3) ensures that whenever we start from related states ($\Sigma_{xy} \approx_{xy} X_{xy}$) and we do one or more steps of the AM composed semantics ($\Sigma_{xy} \xrightarrow{\overline{\tau}} \mathcal{L}^{*}_{xy} \Sigma'_{xy}$), then we can *always* find a related state ($\Sigma'_{xy} \approx_{xy} X'_{xy}$) that is reachable by performing one or more steps of the composed oracle semantics ($X_{xy} \xrightarrow{\overline{\tau}', O_{xy}}{}^{*}_{xy} X'_{xy}$). This fact is used when proving that SNI of a program under the composed AM semantics implies SNI under the composed oracle semantics (point 1 of Definition 2). Thus, it is not important for the AM and the Oracle semantics to produce the same traces, just that the two AM traces and the two Oracle traces are pairwise equivalent – which follows from the state relation.

• Finally, symbolic preservation (point 4) ensures that any step of the always-mispredict composed semantics corresponds to the concretization of a step of the symbolic composed semantics (and vice versa[3]). Note that proving symbolic preservation is almost trivial whenever both source semantics enjoy the same property (like our semantics $\mathcal{L}_B$, $\mathcal{L}_S$, and $\mathcal{L}_R$).

4.2.2 SSS preservation. The key result of our framework is that well-formed compositions whose sources are secure speculative semantics (*SSS*) are also *SSS* (Theorem 4). Note that our proof of Theorem 4, available in the companion technical report [18], holds for *any* well-formed composition in our framework and, therefore, it applies *for free* to all the compositions in Section 5.

Theorem 4 ($\mathcal{L}_{xy}$ is *SSS*). *If* $\vdash \mathcal{L}_x$ *SSS and* $\vdash \mathcal{L}_y$ *SSS and* $\vdash \mathcal{L}_{xy}$: *WFC then* $\vdash \mathcal{L}_{xy}$ *SSS.*

As a corollary of Theorem 4, we obtain that the security of well-formed compositions is related to the security of their components (Theorem 5). In particular, whenever a program is insecure w.r.t. one of the components, then it is insecure w.r.t. the composed semantics. Dually, if a program is secure w.r.t. the composed semantics, then it is secure w.r.t. the single components. Note, however, that there are programs that are secure for the single components but insecure w.r.t. the composed semantics like Listing 1.

Theorem 5 (Combined SNI Preservation). *If* $\vdash \mathcal{L}_{xy}$: *WFC and* $p \nvdash_x$ *SNI or* $p \nvdash_y$ *SNI, then* $p \nvdash_{xy}$ *SNI.*

If $\vdash \mathcal{L}_{xy}$: *WFC and* $p \vdash_{xy}$ *SNI, then* $p \vdash_x$ *SNI and* $p \vdash_y$ *SNI.*

These results have an immediate practical impact on Spectector: (1) Spectector's security analysis relies on the (symbolic) speculative semantics, (2) the source semantics $\mathcal{L}_B$, $\mathcal{L}_S$, and $\mathcal{L}_R$ are *SSS*, (3) well-formed compositions are also *SSS*, and (4) the composition of $\mathcal{L}_B$, $\mathcal{L}_S$, and $\mathcal{L}_R$ are well-formed. So, the Spectector security analysis equipped with any combination of the $\mathcal{L}_B$, $\mathcal{L}_S$, and $\mathcal{L}_R$ produces sound results, i.e., whenever the tool proves that a program is leak-free then the program satisfies SNI. So, the next section describes all the compositions and proves they are well-formed (this implies that they are *SSS* thanks to Theorem 4), whereas the section thereafter describes their implementation in Spectector.

[3]For space reasons, Definition 3 only reports one direction (with a simplified notation).

5 INSTANTIATING OUR FRAMEWORK

This section describes all combinations of the speculative semantics $\mathcal{L}_B$, $\mathcal{L}_S$, and $\mathcal{L}_R$: $\mathcal{L}_{S+R}$ (Section 5.1), $\mathcal{L}_{B+R}$ (Section 5.2), $\mathcal{L}_{B+S}$ (Section 5.3), and $\mathcal{L}_{B+S+R}$ (Section 5.4). For each one, we overview the combined AM semantics using examples (whose traces we computed using our Coq executable composed semantics) and we prove that the combined semantics is well-formed, i.e., it satisfies Definition 3. In the following, we describe in detail how the $\mathcal{L}_{S+R}$ semantics can be instantiated as part of our framework; the other combinations can be instantiated similarly and we only provide a higher-level description. Full details and well-formedness proofs are available in the companion technical report [18].

5.1 $\mathcal{L}_{S+R}$ Composition

To combine semantics using our framework, we need to define the states, observations, and metaparameter Z_{S+R} for the composed semantics $\mathcal{L}_{S+R}$. The combined state Σ_{S+R} is the union of the states Σ_S and Σ_R; thus it contains the RSB $\mathbb{R}$ as well.

Spec. States $\Sigma_{S+R} ::= \overline{\Phi}_{S+R}$ *Spec. Instance* $\Phi_{S+R} ::= \langle p, ctr, \sigma, \mathbb{R}, n \rangle$

The union Obs_{S+R} of the trace models Obs_S and Obs_R is defined as:

$Obs_{S+R} ::= \texttt{start}_S\ n \mid \texttt{start}_R\ n \mid \texttt{rlb}_S\ n \mid \texttt{rlb}_R\ n \mid \texttt{bypass}\ n \mid \ldots$

To define the metaparameter Z_{S+R}, we need to identify, for each component semantics, the instructions that are related with speculative execution. For $\mathcal{L}_S$, the only instruction associated with speculative execution is **store**, since the semantics can only speculatively bypass stores. For $\mathcal{L}_R$, even though the semantics speculates only over **ret** instructions, **call** instructions also affect speculative execution since $\mathcal{L}_R$ pushes return addresses onto the $\mathbb{R}$ when executing **call**s. Therefore, we set the metaparameter Z_{S+R} to (**call**∪**ret**, **store**). This ensures that in $\mathcal{L}_{S+R}$, **store** instructions are only executed by delegating back to $\mathcal{L}_S^{\textbf{call}\cup\textbf{ret}}$ whereas **call** and **ret** instructions are only executed by delegating back to $\mathcal{L}_R^{\textbf{store}}$.

Theorem 6 states the combination of $\mathcal{L}_S$ and $\mathcal{L}_R$ described above is well-formed. Given that $\mathcal{L}_S$ and $\mathcal{L}_R$ are *SSS* (Theorem 2 and Theorem 3), we can derive "for free" that $\mathcal{L}_{S+R}$ is *SSS* (Theorem 4).

Theorem 6 ($\mathcal{L}_{S+R}$ is well-formed). $\vdash \mathcal{L}_{S+R}$: *WFC*

Listing 4 presents a program that contains a leak that can be detected only by $\mathcal{L}_{S+R}$ but not by its components $\mathcal{L}_S$ and $\mathcal{L}_R$.

Listing 4: $\mathcal{L}_{S+R}$ example

```
1 Manip_Stack:
2     sp ← sp + 8
3     ret
4 Speculate:
5     call Manip_Stack
6     store secret, p
7     store pub, p
8     load eax, p
```

```
9       load edi, eax
10      ret
11  Main:
12      call Speculate
13      skip
```

In Listing 4, execution starts on Line 12 by calling the function *Speculate* and it continues at Line 5. Next, the function *Manip_Stack* is called and the stack pointer **sp** is incremented (Line 2). This modifies the return address of the function *Manip_Stack* to now point to Line 13 (the return address of the **call** to *Speculate*). Under $\mathcal{A}_R$, mispredicting the return address of *Manip_Stack* using the RSB leads to continuing the execution at Line 6. However, the **store** instructions in Line 7 overwrites the secret value stored in Line 6. Then, the **load** instructions in Line 8 and Line 9 emit only public values. As a result, no secret is leaked and speculation ends. Similarly, under $\mathcal{A}_S$, speculation over store bypasses has no effect in Listing 4 because the **store** instruction in Line 6 is never reached and function *Manip_Stack* returns to Line 13. Therefore, the leak is missed under $\mathcal{A}_S$ and $\mathcal{A}_R$, i.e., Listing 4 $\vdash_S$ SNI and Listing 4 $\vdash_R$ SNI.

However, under the combined semantics $\mathcal{A}_{S+R}$, the **store** instruction on Line 7 is now speculatively bypassed and when returning from function *Manip_Stack* the execution speculatively continues from Line 8. Now, the **load** instructions are executed and the secret is leaked, as shown in the traces below. Since *secret* is a high value, there are low-equivalent configurations σ^1, σ^2 that differ in the value of *secret*. Thus, there are two traces ($\lightning$) that differs in the observation load *secret* (highlighted in gray). Hence, the program is not secure under the combined semantics, i.e., Listing 4 $\not\vdash_{S+R}$ SNI.

$$\tau^2_{S+R} \neq \tau^1_{S+R} \stackrel{\text{def}}{=} \texttt{call}\ \textit{Speculate} \cdots \texttt{start}_R\ 0 \cdots \texttt{start}_S\ 1 \cdots \texttt{rlb}_S\ 1 \cdots \texttt{start}_S\ 2 \cdot \texttt{bypass}\ 7 \cdot \texttt{load}\ p \cdot \boxed{\texttt{load}\ \textit{secret}} \cdots$$

The relation between the source semantics and their composition is visualised in Figure 1, which shows the insecure programs (with respect to SNI) detected under the different semantics. The combined semantics encompasses all vulnerable programs of $\mathcal{A}_S$ and $\mathcal{A}_R$ *and* additional programs like Listing 4. These additional programs are the reason why the semantics $\mathcal{A}_{S+R}$ is "stronger than the sum of its parts" $\mathcal{A}_S$ and $\mathcal{A}_R$.

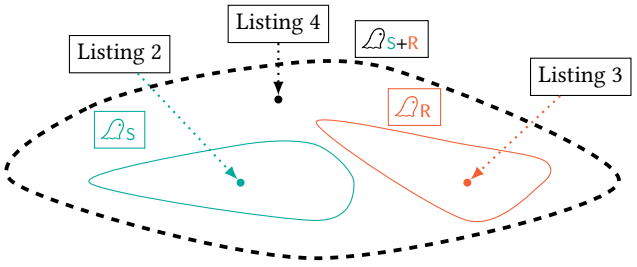


Figure 1: Relating $\mathcal{A}_S$, $\mathcal{A}_R$ and $\mathcal{A}_{S+R}$ wrt SNI.

5.2 $\mathcal{A}_{B+R}$ Composition

In this combination, the instructions that influence speculative execution are **call** and **ret** ($\mathcal{A}_R$) and **beqz** ($\mathcal{A}_B$). Thus, we set Z_{B+R} = (**call** ∪ **ret**, **beqz**) to account for this and to allow speculation from both sources.

Theorem 7 states that $\mathcal{A}_{B+R}$ is well-formed. This allows us to derive "for free" that $\mathcal{A}_{B+R}$ is *SSS* by applying Theorem 4.

Theorem 7 ($\mathcal{A}_{B+R}$ is well-formed). $\vdash \mathcal{A}_{B+R} : \mathit{WFC}$

Listing 5: $\mathcal{A}_{B+R}$ example

```
1   Manip_Stack:
2       sp <- sp + 8
3       ret
4   Speculate:
5       call Manip_Stack
6       x <- 0
7       beqz x, L2
8       load eax, secret
9   L2:
10      ret
11  Main:
12      call Speculate
13      skip
```

Listing 5 presents a leak that can be detected only under $\mathcal{A}_{B+R}$. The execution proceeds similarly to Listing 4 until the **ret** instruction in Line 3 is reached. Under $\mathcal{A}_R$, mispredicting the return address leads to function *Manip_Stack* returning to Line 6. However, the **beqz** instructions in Line 7 jumps to Line 10 (since x is 0) and speculation ends without leaking. Under $\mathcal{A}_B$, the **beqz** instruction in Line 7 is never executed and the function *Manip_Stack* returns to Line 13 without leaking. Hence, Listing 5 is secure (i.e., it satisfies SNI) when considering $\mathcal{A}_R$ and $\mathcal{A}_B$ in isolation.

Under the combined semantics $\mathcal{A}_{B+R}$, function *Manip_Stack* returns to Line 6 and the **beqz** instruction is then mispredicted. This leads to executing the **load** instructions in Line 8, which leaks secret information. The resulting traces ($\lightning$) are given below, where we highlight the secret-dependent observations. Given the length of the trace, we present only the most relevant parts, i.e., that both kinds of speculations need to have started for the leak to appear.

$$\tau^2_{B+R} \neq \tau^1_{B+R} \stackrel{\text{def}}{=} \texttt{call}\ \textit{Speculate} \cdots \texttt{start}_R\ 0 \cdots \texttt{start}_B\ 1 \cdot \texttt{pc}\ 8 \cdot \boxed{\texttt{load}\ \textit{secret}} \cdot \texttt{rlb}_B\ 1 \cdot \texttt{rlb}_R\ 0$$

Again, the two traces differ in the observation in the grey box and we have Listing 5 $\not\vdash_{B+R}$ SNI.

5.3 $\mathcal{A}_{B+S}$ Composition

In this combination,speculation happens on **beqz** instructions ($\mathcal{A}_B$) and on **store** instructions ($\mathcal{A}_S$). Thus, we set Z_{B+S} = (**store**, **beqz**). Therefore, in the combined semantics $\mathcal{A}_{B+S}$, **beqz** instructions are only executed by delegating back to $\mathcal{A}_B^{\textbf{store}}$ and **store** instructions are only executed by delegating back to $\mathcal{A}_S^{\textbf{beqz}}$. This semantics is also a well-formed composition (Theorem 8) and *SSS*.

Theorem 8 ($\mathcal{A}_{B+S}$ is well-formed). $\vdash \mathcal{A}_{B+S} : \mathit{WFC}$

Listing 1 from Section 1 contains a leak that can only be detected by $\mathcal{A}_{B+S}$ but not by its components. The traces associated with the code ($\lightning$) are given below, where secret-dependent observations

are highlighted in gray:

$$\bar{\tau}^2_{B+S} \neq \bar{\tau}^1_{B+S} \stackrel{\text{def}}{=} \cdots \mathtt{start}_S\ 1 \cdot \mathtt{bypass}\ 1 \cdots \mathtt{start}_B\ 2 \cdot \mathtt{pc}\ 5 \cdot \mathtt{load}\ p \cdot \boxed{\mathtt{load}\ A + secret} \cdot \mathtt{rlb}_B\ 2 \cdot \mathtt{rlb}_S\ 1 \cdots$$

The program is not secure under $\mathcal{A}_{B+S}$, i.e., Listing 1 $\not\sim_{B+S}$ SNI.

5.4 $\mathcal{A}_{B+S+R}$ Composition

We conclude this section by combining all three semantics $\mathcal{A}_B$, $\mathcal{A}_S$, and $\mathcal{A}_R$. Our framework (Section 4) allows only combining a pair of source semantics into a combined one. For simplicity, we present $\mathcal{A}_{B+S+R}$ as a direct combination of the three source semantics (technically, we obtain $\mathcal{A}_{B+S+R}$ by combining $\mathcal{A}_{B+S}$ with $\mathcal{A}_R$). The metaparameter Z_{B+S+R} (which we represent as a triple of values) is (**call** ∪ **ret** ∪ **store**, **call** ∪ **ret** ∪ **beqz**, **beqz** ∪ **store**). As a result, the combined semantics $\mathcal{A}_{B+S+R}$ can only delegate to the corresponding speculative semantics for the appropriate speculation sources.

As before, $\mathcal{A}_{B+S+R}$ is a well-formed composition (Theorem 9) and we get that $\mathcal{A}_{B+S+R}$ is *SSS* by applying Theorem 4.

Theorem 9 ($\mathcal{A}_{B+S+R}$ is well-formed). $\vdash \mathcal{A}_{B+S+R} : WFC$

Listing 6: $\mathcal{A}_{B+S+R}$ example

```
1  Manip_Stack:
2      sp <- sp + 8
3      ret
4  Speculate:
5      call Manip_Stack
6      x <- 0
7      beqz x, L2
8      load eax, p
9      load edi, eax
10 L2:
11     ret
12 Main:
13     store secret, p
14     store pub, p
15     call Speculate
```

Listing 6 depicts a leaky program that can be detected only under $\mathcal{A}_{B+S+R}$, since the program satisfies SNI under $\mathcal{A}_B$, $\mathcal{A}_S$ and $\mathcal{A}_R$. Under $\mathcal{A}_{B+S+R}$, the **store** instruction in Line 14 is bypassed Therefore, when returning from *Manip_Stack*, the program mispredicts the return address and speculatively returns to Line 6. Here, the **beqz** instruction in Line 7 is mispredicted and the **load** instructions are executed, which now leaks the secret value.

The resulting traces (🐓) are given below:

$$\tau^2_{B+S+R} \neq \tau^1_{B+S+R} \stackrel{\text{def}}{=} \cdots \mathtt{start}_S\ 1 \cdot \mathtt{bypass}\ 14 \cdot \mathtt{call}\ Speculate \cdots \cdot \mathtt{start}_R\ 2 \cdot \mathtt{ret}\ 6 \cdot \mathtt{start}_B\ 3 \cdot \mathtt{pc}\ 8 \cdot \mathtt{load}\ p \cdot \boxed{\mathtt{load}\ secret} \cdot \mathtt{rlb}_B\ 3 \cdot \mathtt{rlb}_R\ 2 \cdot \cdot \mathtt{rlb}_S\ 1 \cdots$$

Thus, the program is not secure, i.e., Listing 6 $\not\sim_{B+S+R}$ SNI.

6 IMPLEMENTATION AND EVALUATION

This section describes how our combined semantics can be used to detect leaks introduced by the interaction of multiple speculation mechanisms. For this, we extended Spectector, a symbolic analysis tool for speculative leaks against $\mathcal{A}_B$, with the semantics for $\mathcal{A}_S$ and $\mathcal{A}_R$ and for all the combinations from Section 5 (Section 6.1). Using Spectector, we analyze a corpus of 49 microbenchmarks containing speculative leaks generated by different speculation mechanisms (Section 6.2). With these experiments, we aim to show that (1) our $\mathcal{A}_S$ and $\mathcal{A}_R$ speculative semantics can correctly identify speculative leaks associated with speculation over store-bypasses and return instructions, and (2) our combined semantics can detect novel leaks that are otherwise undetectable when considering single speculation mechanisms in isolation.

6.1 Implementation

We implemented all our semantics (the symbolic versions of $\mathcal{A}_S$ and $\mathcal{A}_R$ plus all compositions from Section 5) as an extension of Spectector [21]. The implementation of compositions closely follows the structure of our framework. As in Section 5, selecting one of the composed semantics in Spectector sets the metaparameter Z, which is used to delegate back to the correct individual semantics. Spectector then uses symbolic execution together with self-composition [6] and an SMT solver to check for SNI against $\mathcal{A}_x$. Due to this setup, we inherit all limitations of Spectector's speculative analysis, e.g., path explosion due to symbolic execution and limitations in the translation from x86 to μAsm. We refer to [21] for an in-depth discussion of such limitations.

6.2 Experiments

Benchmarks: We analyze 49 snippets of code containing leaks resulting from speculation over branch, **store**/**load**, and **ret** instructions (and their combinations):

- **Spectre-STL:** 13 programs are variants of the Spectre-STL vulnerability. They exploit speculation over memory disambiguation, and they have been used as benchmarks in prior work [14, 32]. For each program, we also analyze a patched version where a manually inserted lfence instruction stops speculation over store-bypasses and prevents the leak.
- **Spectre-RSB:** 5 programs are variants of the Spectre-RSB vulnerability. They exploit speculation over return instructions, and they are obtained from the `safeside` [1] and `transientfail` [8] projects[4]. For each program, we also analyze manually patched versions obtained by (1) inserting lfences after call instructions (i.e., at the instruction address where **ret** speculatively returns), and (2) using the modified `retpoline` defense proposed in [27, Section 6.1].
- **Spectre-Comb:** 4 programs contain leaks that arise from combining speculation mechanisms. These are the programs depicted in listing 1, listing 5, listing 4, and listing 6 and discussed in Section 5. For each program, we also analyze a manually patched version where `lfence` instructions prevent the speculative leaks.

Experimental setup: The benchmarks for **Spectre-STL** and **Spectre-RSB** are implemented in C and compiled with Gcc 11.1.0 and we manually inserted `lfence`/`retpoline` countermeasures in the

[4]Out of the three Spectre-RSB examples from `safeside` [1], we analyze the only one that works against an acyclic RSB like the one supported by $\mathcal{A}_R$. Programs *ca_ip*, *ca_oop*, and *sa_ip* from `transientfail` [8] rely on concurrent execution. Since Spectector does not support concurrency, we hardcode the worst-case interleaving in terms of speculative leakage in our benchmark.

Test case		λ_S None	λ_S Fence
case01	(I)	○	●
case02	(I)	○	●
case03	(S)	●	●
case04	(I)	○	●
case05	(I)	○	●
case06	(I)	○	●
case07	(I)	○	●
case08	(I)	○	●
case09	(S)	●	●
case10	(I)	○	●
case11	(I)	○	●
case12	(S)	●	●
case13	(I)	○	●

(a) Results for the Spectre-STL programs under the λ_S semantics against unpatched programs (column "None") and programs patched with `lfence` (column "Fence")

Test case		λ_R None	λ_R Fence	λ_R Retpoline
ret2spec_c_d	(I)	○	●	●
ca_ip	(I)	○	●	●
ca_oop	(I)	○	●	●
sa_ip	(I)	○	●	●
sa_oop	(I)	○	●	●

(b) Results for the Spectre-RSB programs under the λ_R semantics against unpatched programs (column "None"), programs patched with `lfence` (column "Fence"), and programs patched with the modified `retpoline` defense proposed in [27, S6.1] (column "Retpoline")

Figure 2: Result of the analysis of our benchmarks for λ_S and λ_R. For each program, ○ denotes that Spectector finds a violation of SNI under the corresponding semantics, whereas ● denotes that Spectector proves the program secure under the semantics. Next to each program, we report if the program is Secure or Insecure in its unpatched version.

patched versions. The benchmarks for **Spectre-Comb** are directly formalised in μAsm. We run all our experiments on a laptop with a Dual Core Intel Core i5-7200U CPU and 8GB of RAM.

Spectre-STL: Figure 2a reports the results of analysing the programs in the **Spectre-STL** benchmark[5]. Using the λ_S semantics, Spectector successfully detected leaks (i.e., violations of SNI) in all unpatched programs, except programs 03, 09, and 12 which do not contain speculative leaks (consistently with other analysis results [14, 32]). Observe that Binsec/Haunted [14] flags program 13 as secure since the program can *only* speculatively leak initial values from the stack, which Binsec/Haunted treats as public by default [2]. Since we assume initial memory values to be secret (like Ponce de León and Kinder [32]), Spectector correctly detected the leak in program 13. Spectector also successfully proved that all patched programs (where an `lfence` is added between **store** instructions) satisfy SNI and are free of speculative leaks.

Spectre-RSB: Figure 2b reports the analysis results on the **Spectre-RSB** programs. Using λ_R, Spectector successfully detected leaks in all unpatched programs. Moreover, Spectector successfully proved that the patched programs where a `lfence` instruction is added after every **call** satisfy SNI, i.e., they are free of speculative leaks. Spectector also successfully proved secure the programs patched using the modified `retpoline` defense proposed by Maisuradze and Rossow [27], which replaces return instructions with a construct that traps the speculation in an infinite loop.

Spectre-Comb: Figure 3a reports the results of our analysis on the **Spectre-Comb** programs, which involve leaks arising from a combination of multiple speculation mechanisms. Spectector equipped with the single semantics λ_B, λ_S, and λ_R is not able to detect the speculative leaks in any of the 4 programs and, therefore, proves them secure. This is expected since the programs contain leaks that arise from a combination of semantics. Spectector can successfully identify leaks in listing 1, listing 5, listing 4 when using, respectively, the semantics λ_{B+S}, λ_{S+R}, and λ_{B+R}. Each semantics, however, fail in detecting leaks in the other programs, and all of them fail in detecting a leak in listing 6 as expected. Finally, Spectector is able to successfully detect leaks in all programs when using the λ_{B+S+R} semantics that combines all speculation mechanisms studied in this paper.

We also analyzed programs manually patched with `lfence` statements ("listing 1 Fence", "listing 5 Fence", "listing 4 Fence", and "listing 6 Fence" in Figure 3a). As before, Spectector successfully prove the security of patched programs. Even for leaks that arise from multiple speculation mechanisms, it is often sufficient to insert a single `lfence` to secure the entire program, e.g., an `lfence` after the **beqz** instruction in Listing 5 is enough to make the program SNI with respect to λ_{B+S+R}.

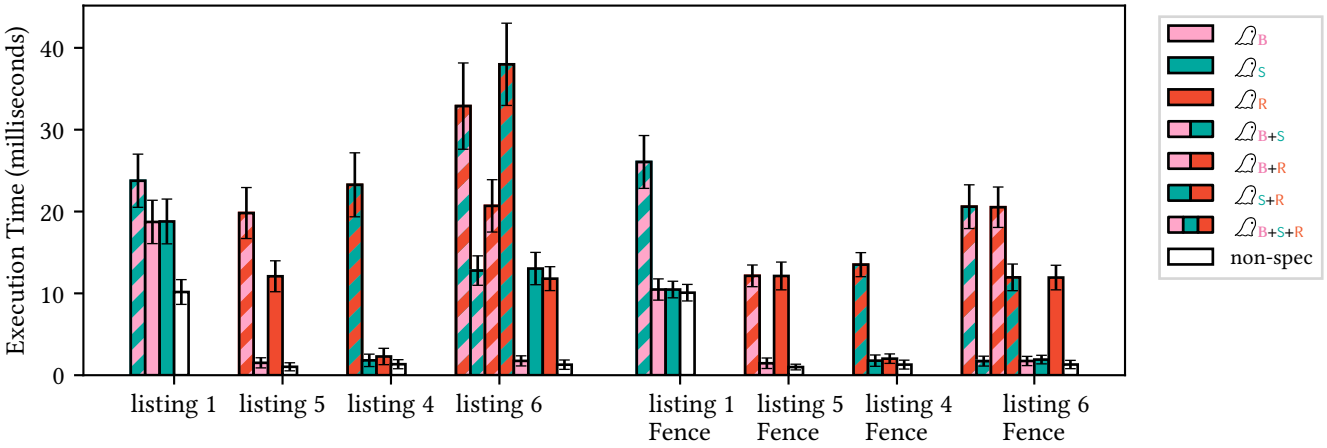
Figure 3b reports the average execution time (for 1000 executions) of Spectector's analysis for the **Spectre-Comb** programs under the different semantics. We highlight the following findings:

- For the programs patched with `lfence`, Spectector's execution time under a combined semantics is larger than Spectector's execution times under the corresponding source semantics. This follows from the combined semantics exploring (a) everything explored by the source semantics as well as (b) additional statements resulting from extra interactions between the source semantics. Note that the placement of `lfences` influence execution time. For instance, the execution time for "listing 5 Fence" under λ_R and λ_{B+R} is similar because the `lfence` is placed just after the branch instruction of Line 7, thereby stopping λ_B-speculation.
- For most of the unpatched programs, execution time under a combined semantics is again larger than the execution times under

[5]We had to slightly modify programs 02, 05, and 06 due to limitations of Spectector's x86 front-end when dealing with global values (programs 05 and 06) and 32-bit addressing (program 02). We had to limit the speculation window, due to vanilla Spectector's limitations in symbolic execution, when analyzing program 09, which contains a loop.

Test case		$\mathcal{A}_{B}$	$\mathcal{A}_{S}$	$\mathcal{A}_{R}$	$\mathcal{A}_{B+S}$	$\mathcal{A}_{S+R}$	$\mathcal{A}_{B+R}$	$\mathcal{A}_{B+S+R}$
listing 1	(I)	•	•	•	○	•	•	○
listing 5	(I)	•	•	•	•	○	•	○
listing 4	(I)	•	•	•	•	•	○	○
listing 6	(I)	•	•	•	•	•	•	○
listing 1 Fence	(S)	•	•	•	•	•	•	•
listing 5 Fence	(S)	•	•	•	•	•	•	•
listing 4 Fence	(S)	•	•	•	•	•	•	•
listing 6 Fence	(S)	•	•	•	•	•	•	•

(a) Results of the analysis. For each program, ○ denotes that Spectector finds a violation of SNI whereas • denotes that Spectector proves the program secure under the corresponding semantics. Next to each program, we report if it is Secure or Insecure w.r.t. $\mathcal{A}_{B+S+R}$.



(b) Average execution time for Spectector's analysis for the code snippets in the Spectre-Comb benchmark (over 1000 samples) for the relevant individual and composed speculative semantics. The white bar ("non-spec") represents the analysis time w.r.t. μAsm non-speculative semantics.

Figure 3: Results of the Spectre-Comb benchmark, where "listing x Fence" is the patched version (using `lfence`) of "listing x".

the source semantics. This is, however, not always the case. For instance, Spectector's execution time for listing 6 and $\mathcal{A}_{S+R}$ is larger than its execution time for $\mathcal{A}_{B+S+R}$. This is due to Spectector's terminating early after finding a violation of SNI, which happens under $\mathcal{A}_{B+S+R}$ but not under $\mathcal{A}_{S+R}$ (see also Figure 3a).

7 DISCUSSION

Scope of the models: Lifting the results of the security analysis for our speculative semantics to real-world CPUs is only possible to the extent that these semantics capture the information flows in the target system. Thus, Spectector's result may incorrectly classify programs as secure (if our semantics do not capture information flows happening in real-world CPUs) or insecure (if our semantics admit speculations that are impossible on real systems).

Other speculation mechanisms: There are many speculation mechanisms beyond those modeled in $\mathcal{A}_{B}$, $\mathcal{A}_{S}$, and $\mathcal{A}_{R}$:

- Speculation over indirect jumps [24] can be modeled as an always-mispredict semantics (similarly to $\mathcal{A}_{B}$) where mispredicted paths can start from any other statement. This, however, makes automated reasoning challenging due to the large number of speculative paths. Mechanisms like Intel Control-Flow-Integrity [34] can improve the situation by restricting potential jump targets.
- CPUs speculate over **ret** instructions in different ways. For instance, there are many different ways of implementing return stack buffers (e.g., cyclic versus acyclic RSBs [27] or RSBs that fall back to indirect branch prediction [41]). Some ARM processors, moreover, use straight-line speculation that allows CPUs to speculatively bypass a **ret** instruction and execute the instructions following it. Both kinds of speculation can be modeled by modifying the Rule R:AM-Ret-Spec rule in $\mathcal{A}_{R}$.
- Many proposals for value prediction over different kinds of instructions exist [26, 29, 35]. While naive speculative semantics might have to explore *all* possible values as prediction, semantics that model specific prediction mechanisms might restrict the set of predicted values (thereby leading to a more tractable analysis).

We expect that most of these mechanisms can be modeled as speculative semantics satisfying our well-formedness conditions. Hence, they could work with our composition framework.

Limitations of composition: Our composition framework has two main limitations:

(1) The metaparameter Z is expressed in terms of μAsm instructions, i.e., the smallest unit of computation in our framework. Since Z restricts how the composed semantics delegates execution to its sources, this limit the expressiveness of composed semantics. For

instance, $\mathcal{A}_{S+R}$ cannot speculate over the *implict* **store** writing the return address to the stack that happens as part of **call** instructions.

(2) Our framework does not support combinations where a single instruction perform speculation-relevant changes in both source semantics. For instance, consider a combination of $\mathcal{A}_R$ with a semantics modeling straight-line speculation. Here, both semantics start different speculative transactions on executing **ret** instructions. However, instantiating Z as $(\emptyset, \emptyset)$, which enables both speculations, violates the confluence well-formedness condition for the composed semantics, whereas setting $Z = (x, y)$ so that only one of x and y is **ret** would only capture one of the two speculation mechanisms.

We leave addressing both limitations as future work.

8 RELATED WORK

Speculative execution attacks: After Spectre [24] has been disclosed to the public in 2018, researchers have identified many other speculative execution attacks [4, 7, 25, 27, 42]. These attacks differ in the exploited speculation sources [23, 25, 27], the covert channels [33, 36, 37] used, or the target platforms [12]. We refer the reader to Canella et al. [8] for a survey of existing attacks.

Security conditions for speculative leaks: Researchers have proposed many program-level properties for security against speculative leaks, which can be classified in three main groups [10]:

(1) Non-interference definitions ensure the security of speculative *and* non-speculative instructions. For instance, speculative constant-time [9] (used also in [3, 14, 38]) extends the constant-time security condition to account also for transient instructions.

(2) Relative non-interference definitions [11, 19, 21, 22] ensure that transient instructions do not leak more information than what is leaked by non-transient instructions. For instance, speculative non-interference [21], which we build on, (used also in [20, 31]) restricts the information leaked by speculatively executed instructions (without constraining what can be leaked non-speculatively).

(3) Definitions that formalise security as a safety property [31, 32], which may over-approximate definitions from the groups above.

Operational semantics for speculative leaks: In the last few years, there has been a growing interest in developing formal models and principled program analyses for detecting leaks caused by speculatively executed instructions. We refer the reader to [10] for a comprehensive survey on the topic. In the following, we discuss the approaches that are more relevant to our paper.

Our speculative semantics $\mathcal{A}_S$ and $\mathcal{A}_R$ capture the effects of transient instructions at a rather high-level, and they are inspired by the always-mispredict $\mathcal{A}_B$ semantics from [21]. Our $\mathcal{A}_S$ semantics is also similar to the CT-BPAS speculation contract used by the Revizor testing tool [30]. In contrast, other approaches, which we overview next, explicitly model microarchitectural components like multiple pipeline stages, caches, and branch predictors.

For instance, KLEESpectre [39] and SpecuSym [22] consider a semantics that explicitly model the cache, which enable reasoning about the cache content. McIlroy et al. [28] go a step further and model a multi-stage pipeline with explicit cache and branch predictor. Their semantics can only model speculation over branch instructions since it lacks store-forwarding or RSB.

Cauligi et al. [9]'s semantics model speculation over branch instructions, store-bypasses, and return instructions. Differently from our semantics, their 3-stage pipeline semantics explicitly models several microarchitectural components like a reorder buffer and an RSB. Their tool detects violations of speculative constant-time induced by speculation over branch instructions and store-bypasses.

Binsec/Haunted [14] detect violations of speculative constant-time due to speculation over store-bypasses and branch instructions. For this, they explicitly model the store buffer, which $\mathcal{A}_S$ abstracts away. Barthe et al. [5] extend the Jasmin [3] cryptographic verification framework to reason about speculative constant-time and supports speculation over store-bypasses and branch instructions.

While several of these models support multiple speculation mechanisms, these mechanisms are *hard-coded* and no existing approach provides a composition framework or extensible ways of extending the main theoretical results to new mechanisms "for free". Moreover, while we could have used other semantics as a basis for our framework, this would have resulted in more difficult proofs (since semantics like the one in [9] are significantly more complex than ours).

Axiomatic semantics for speculative leaks: A few approaches formalise the effects of speculatively executed instructions using axiomatic semantics inspired by work on weak memory models. For instance, Colvin and Winter [13] and Disselkoen et al. [15] capture the effects of branch speculation but both lack program analyses.

Ponce de León and Kinder [32] illustrate how one can model leaks resulting from speculation over branch instructions and store-bypasses using the CAT modeling language for memory consistency, and they present a bounded model checking analysis for detecting speculative leaks. Interestingly, they talk about composing several of theirs semantics [32, SIV.F], which should allow them to detect vulnerabilities like Listing 1 (which we detect under $\mathcal{A}_{B+S}$). However, they do not formally characterize compositions and, therefore, they cannot derive interesting results "for free" about the composed semantics (like we do in Theorem 4). Moreover, even though they state that composability is an advantage of axiomatic models, our framework (and tool implementation) shows that composability can be done with operational semantics as well.

9 CONCLUSION AND FUTURE WORK

This paper presented new speculative semantics for speculation on store and return instructions. It also defined a general framework to reason about the composition of different speculative semantics and instantiated the framework with our new speculative semantics $\mathcal{A}_S$ and $\mathcal{A}_R$ and the semantics by Guarnieri et al. [21]. Our framework yields security of the composed semantics (almost) for free, given the security of its parts. All the new semantics have been implemented in the Spectector program analysis tool, which correctly detects all vulnerabilities in existing and novel benchmarks.

Acknowledgments: This work was partially supported by the Madrid regional government under the project S2018/TCS-4339 BLOQUES-CM, by the Spanish Ministry of Science, Innovation, and University under the project RTI2018-102043-B-I00 SCUM, by the Italian Ministry of Education under the Rita Levi Montalcini grant (2019 call), by the German Ministry for Education and Research under the project CISPA-Stanford Center for Cybersecurity (funding number: 16KIS0761), and by a gift from Intel Corporation.

REFERENCES

[1] 2019. SafeSide. https://github.com/google/safeside

[2] 2021. Result of case_13. https://github.com/binsec/haunted_bench/issues/2.

[3] José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Arthur Blot, Benjamin Grégoire, Vincent Laporte, Tiago Oliveira, Hugo Pacheco, Benedikt Schmidt, and Pierre-Yves Strub. 2017. Jasmin: High-Assurance and High-Speed Cryptography. In *Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*. ACM.

[4] Enrico Barberis, Pietro Frigo, Marius Muench, Herbert Bos, and Cristiano Giuffrida. 2022. Branch history injection: On the effectiveness of hardware mitigations against cross-privilege Spectre-v2 attacks. In *Proceedings of the 31st USENIX Security Symposium (USENIX Security '22)*. USENIX Association.

[5] Gilles Barthe, Sunjay Cauligi, Benjamin Grégoire, Adrien Koutsos, Kevin Liao, Tiago Oliveira, Swarn Priya, Tamara Rezk, and Peter Schwabe. 2021. High-Assurance Cryptography in the Spectre Era. In *Proceedings of the 42nd IEEE Symposium on Security and Privacy (S&P '21)*. IEEE.

[6] Gilles Barthe, Pedro R D'argenio, and Tamara Rezk. 2004. Secure information flow by self-composition. In *Proceedings of the 17th IEEE Computer Security Foundations Workshop (CSF '04)*. IEEE.

[7] Atri Bhattacharyya, Alexandra Sandulescu, Matthias Neugschwandtner, Alessandro Sorniotti, Babak Falsafi, Mathias Payer, and Anil Kurmus. 2019. SMoTherSpectre: Exploiting Speculative Execution through Port Contention. In *Proceedings of the 26th ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*. ACM.

[8] Claudio Canella, Jo Van Bulck, Michael Schwarz, Moritz Lipp, Benjamin von Berg, Philipp Ortner, Frank Piessens, Dmitry Evtyushkin, and Daniel Gruss. 2019. A Systematic Evaluation of Transient Execution Attacks and Defenses. In *Proceedings of the 28th USENIX Security Symposium (USENIX Security '19)*. USENIX Association.

[9] Sunjay Cauligi, Craig Disselkoen, Klaus v. Gleissenthall, Dean Tullsen, Deian Stefan, Tamara Rezk, and Gilles Barthe. 2020. Constant-Time Foundations for the New Spectre Era. In *Proceedings of the 41st ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI '20)*. ACM.

[10] Sunjay Cauligi, Craig Disselkoen, Daniel Moghimi, Gilles Barthe, and Deian Stefan. 2022. SoK: Practical Foundations for Software Spectre Defenses. In *Proceedings of the 43rd IEEE Symposium on Security and Privacy (S&P '22)*. IEEE.

[11] Kevin Cheang, Cameron Rasmussen, Sanjit Seshia, and Pramod Subramanyan. 2019. A Formal Approach to Secure Speculation. In *Proceedings of the 32nd IEEE Computer Security Foundations Symposium (CSF '19)*. IEEE.

[12] Guoxing Chen, Sanchuan Chen, Yuan Xiao, Yinqian Zhang, Zhiqiang Lin, and Ten H. Lai. 2019. Stealing Intel Secrets from SGX Enclaves via Speculative Execution. In *Proceedings of the 4th IEEE European Symposium on Security and Privacy (EuroS&P '19)*. IEEE.

[13] Robert J. Colvin and Kirsten Winter. 2019. An Abstract Semantics of Speculative Execution for Reasoning About Security Vulnerabilities. In *Proceedings of the 19th Refinement Workshop (Refine '19)*. Springer.

[14] Lesly-Ann Daniel, Sébastien Bardin, and Tamara Rezk. 2021. Hunting the Haunter — Efficient relational symbolic execution for Spectre with Haunted RelSE. In *Proceedings of the 28th Annual Network and Distributed System Security Symposium (NDSS '21)*. The Internet Society.

[15] Craig Disselkoen, Radha Jagadeesan, Alan Jeffrey, and James Riely. 2019. The Code That Never Ran: Modeling Attacks on Speculative Evaluation. In *Proceedings of the 40th IEEE Symposium on Security and Privacy (S&P '19)*. IEEE.

[16] Xaver Fabian, Marco Guarnieri, and Marco Patrignani. 2022. https://github.com/XFabian/Spectector-Combined

[17] Xaver Fabian, Marco Guarnieri, and Marco Patrignani. 2022. https://github.com/XFabian/Spectecoq

[18] Xaver Fabian, Marco Guarnieri, and Marco Patrignani. 2022. Automatic Detection of Speculative Execution Combinations. (2022). arXiv:2209.01179

[19] Roberto Guanciale, Musard Balliu, and Mads Dam. 2020. InSpectre: Breaking and Fixing Microarchitectural Vulnerabilities by Formal Analysis. In *Proceedings of the 27th ACM SIGSAC Conference on Computer and Communications Security (CCS '20)*. ACM.

[20] Marco Guarnieri, Boris Köpf, Jan Reineke, and Pepe Vila. 2021. Hardware-Software Contracts for Secure Speculation. In *Proceedings of the 42nd IEEE Symposium on Security and Privacy (S&P '21)*. IEEE.

[21] Marco Guarnieri, Boris Köpf, José F. Morales, Jan Reineke, and Andrés Sánchez. 2020. Spectector: Principled Detection of Speculative Information Flows. In *Proceedings of the 41st IEEE Symposium on Security and Privacy (S&P '20)*.

[22] Shengjian Guo, Yueqi Chen, Peng Li, Yueqiang Cheng, Huibo Wang, Meng Wu, and Zhiqiang Zuo. 2020. SpecuSym: Speculative Symbolic Execution for Cache Timing Leak Detection. In *Proceedings of the 42nd ACM/IEEE International Conference on Software Engineering (ICSE '20)*. ACM.

[23] J. Horn. 2018. Speculative execution, variant 4: Speculative store bypass. https://bugs.chromium.org/p/project-zero/issues/detail?id=1528. Accessed: 2021-04-11.

[24] Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom. 2019. Spectre Attacks: Exploiting Speculative Execution. In *Proceedings of the 40th IEEE Symposium on Security and Privacy (S&P '19)*.

[25] Esmaeil Mohammadian Koruyeh, Khaled N. Khasawneh, Chengyu Song, and Nael Abu-Ghazaleh. 2018. Spectre Returns! Speculation Attacks Using the Return Stack Buffer. In *Proceedings of the 12th USENIX Workshop on Offensive Technologies (WOOT'18)*. USENIX Association.

[26] Mikko H. Lipasti, Christopher B. Wilkerson, and John Paul Shen. 1996. Value locality and load value prediction. In *Proceedings of the 7th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '96)*. ACM.

[27] Giorgi Maisuradze and Christian Rossow. 2018. Ret2spec: Speculative Execution Using Return Stack Buffers. In *Proceedings of the 25th ACM SIGSAC Conference on Computer and Communications Security (CCS '18)*. ACM.

[28] Ross McIlroy, Jaroslav Sevcík, Tobias Tebbi, Ben L. Titzer, and Toon Verwaest. 2019. Spectre is here to stay: An analysis of side-channels and speculative execution. (2019). arXiv:1902.05178

[29] Sparsh Mittal. 2017. A survey of value prediction techniques for leveraging value locality. *Concurrency and computation: practice and experience* (2017).

[30] Oleksii Oleksenko, Christof Fetzer, Boris Köpf, and Mark Silberstein. 2022. Revizor: Testing Black-Box CPUs against Speculation Contracts. In *Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '22)*. ACM.

[31] Marco Patrignani and Marco Guarnieri. 2021. Exorcising Spectres with Secure Compilers. In *Proceedings of the 28th ACM Conference on Computer and Communications Security (CCS '21)*. ACM.

[32] Hernán Ponce de León and Johannes Kinder. 2022. Cats vs. Spectre: An Axiomatic Approach to Modeling Speculative Execution Attacks. In *Proceedings of the 43rd IEEE Symposium on Security and Privacy (S&P '22)*. IEEE.

[33] Michael Schwarz, Martin Schwarzl, Moritz Lipp, Jon Masters, and Daniel Gruss. 2019. NetSpectre: Read Arbitrary Memory over Network. In *Proceedings of the 24th European Symposium on Research in Computer Security (ESORICS '19)*. Springer.

[34] Vedvyas Shanbhogue, Deepak Gupta, and Ravi Sahita. 2019. Security Analysis of Processor Instruction Set Architecture for Enforcing Control-Flow Integrity. In *Proceedings of the 8th International Workshop on Hardware and Architectural Support for Security and Privacy (HASP '19)*. ACM.

[35] Rami Sheikh, Harold W. Cain, and Raguram Damodaran. 2017. Load value prediction via path-based address prediction: Avoiding mispredictions due to conflicting stores. In *Proceedings of the 50th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO '17)*. ACM.

[36] Julian Stecklina and Thomas Prescher. 2018. LazyFP: Leaking FPU Register State using Microarchitectural Side-Channels. *CoRR* (2018). arXiv:1806.07480

[37] Caroline Trippel, Daniel Lustig, and Margaret Martonosi. 2018. MeltdownPrime and SpectrePrime: Automatically-Synthesized Attacks Exploiting Invalidation-Based Coherence Protocols. *CoRR* (2018). arXiv:1802.03802

[38] Marco Vassena, Craig Disselkoen, Klaus von Gleissenthall, Sunjay Cauligi, Rami Gökhan Kıcı, Ranjit Jhala, Dean Tullsen, and Deian Stefan. 2021. Automatically Eliminating Speculative Leaks from Cryptographic Code with Blade. *Proceedings of the ACM on Programming Languages* 5, POPL (2021).

[39] Guanhua Wang, Sudipta Chattopadhyay, Arnab Kumar Biswas, Tulika Mitra, and Abhik Roychoudhury. 2020. KLEESpectre: Detecting Information Leakage through Speculative Cache Attacks via Symbolic Execution. *ACM Transactions on Software Engineering and Methodology* 29, 3 (2020).

[40] Guanhua Wang, Sudipta Chattopadhyay, Ivan Gotovchits, Tulika Mitra, and Abhik Roychoudhury. 2021. oo7: Low-Overhead Defense Against Spectre Attacks via Program Analysis. *IEEE Transactions on Software Engineering* 47, 11 (2021).

[41] Johannes Wikner and Kaveh Razavi. 2022. RETBLEED: Arbitrary Speculative Code Execution with Return Instructions. In *Proceedings of the 31st USENIX Security Symposium (USENIX Security '22)*. USENIX Association.

[42] Tao Zhang, Kenneth Koltermann, and Dmitry Evtyushkin. 2020. Exploring Branch Predictors for Constructing Transient Execution Trojans. In *Proceedings of the 25th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '20)*. ACM.

A PREFACE

There are some notational differences between the paper and technical report.

(1) In the technical report, The maximum speculation window ω is a parameter of the semantics instead of a constant.
(2) In the technical report, we use $\Downarrow_1^{\overline{\tau}}$ to indicate the reflexive-transitive closure of the corresponding semantics
(3) In the technical report, we use ω instead of $\mathcal{A}$ to indicate AM notation.
(4) In the technical report we use `bypass` n instead of *bypass* n
(5) In the technical report Z is a list of instructions [Z] instead of a set.

B REDEFINITONS

We start by reviewing μAsm and the non-speculative semantics as it was defined in Spectector.

Basic Types

(Registers)	x	$\in$	$Regs$
(Values)	n, l	$\in$	$Vals = \mathbb{N} \cup \{\bot\}$

Syntax

(Expressions)	e	$::=$	$n \mid x \mid \ominus e \mid e_1 \otimes e_2$
(Instructions)	i	$::=$	$\textbf{skip} \mid x \leftarrow e \mid \textbf{load}\ x, e \mid$
			$\textbf{store}\ x, e \mid \textbf{jmp}\ e \mid \textbf{beqz}\ x, l \mid$
			$x \xleftarrow{e'?} e \mid \textbf{spbarr} \mid \textbf{call}\ f \mid \textbf{ret}$
(Programs)	p	$::=$	$n : i \mid p_1; p_2$
(Functions)	$\mathcal{F}$	$::=$	$\varnothing \mid \mathcal{F}; f \mapsto n$

Figure 4: Syntax of μAsm.

A μAsm program p is defined as a sequence of pairs $n : i$ where i is an instruction and $n \in \mathbb{N}$ is a label. We will use p as a partial function from natural numbers to instructions, where $p(n)$ either returns the instruction if the label exists in p or $\bot$. In addition, we add a map $\mathcal{F}$ mapping function names f to line numbers n in p.

Definition 4. *A Configuration σ is a triple $\langle m, a\rangle$, where $m \in Mem$ models the memory and $a \in Assgn$ models the register assignments. Memories m and register assignments a are functions mapping memory addresses $m \in N$ respectively register identifiers $a \in Regs$ to values in Vals. The set $Mem \times Assgn$ of all configurations is called Conf.*

We use the register **sp** to point to the top of the software stack for call and returns. It works as a stack pointer. The adversary is modeled by exposing observations during program execution.

Definition 5. *A observation is defined as*

$$\tau ::= \texttt{load}\ n \mid \texttt{store}\ n \mid \texttt{pc}\ n \mid \texttt{call}\ f \mid \texttt{ret}\ n \mid$$

We call this set Obs.

Judgements

$\sigma \xrightarrow{\tau} \sigma'$	*Configuration σ small-steps to σ' and emits observation τ.*
$\sigma \Downarrow_{\overline{\tau}} \sigma'$	*Configuration σ big-steps to σ' and emits a list of observations $\overline{\tau}$.*
$(p, \sigma) \text{ß}^{O}_{NS}\ \overline{\tau}$	*Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.*

Expression evaluation

$[\![n]\!](a) = n \qquad [\![x]\!](a) = a(x) \qquad [\![\ominus e]\!](a) = \ominus[\![e]\!](a) \qquad [\![e_1 \otimes e_2]\!](a) = [\![e_1]\!](a) \otimes [\![e_2]\!](a)$

$\sigma \xrightarrow{\tau} \sigma$

$$\frac{p(a(\textbf{pc})) = \textbf{skip}}{\langle m, a\rangle \rightarrow \langle m, a[\textbf{pc} \mapsto a(\textbf{pc}) + 1]\rangle}\ (\text{Skip})$$

$$\frac{p(a(\textbf{pc})) = \textbf{spbarr}}{\langle m, a\rangle \rightarrow \langle m, a[\textbf{pc} \mapsto a(\textbf{pc}) + 1]\rangle}\ (\text{Barrier})$$

$$\frac{p(a(\textbf{pc})) = x \leftarrow e \qquad x \neq \textbf{pc}}{\langle m, a\rangle \rightarrow \langle m, a[\textbf{pc} \mapsto a(\textbf{pc}) + 1, x \mapsto [\![e]\!](a)]\rangle}\ (\text{Assign})$$

$$\text{(ConditionalUpdate-Sat)}\quad \frac{p(a(\mathbf{pc})) = x \xleftarrow{e'?} e \qquad [\![e']\!](a) = 0 \qquad x \neq \mathbf{pc}}{\langle m, a\rangle \to \langle m, a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1, x \mapsto [\![e]\!](a)]\rangle}$$

$$\text{(ConditionalUpdate-Unsat)}\quad \frac{p(a(\mathbf{pc})) = x \xleftarrow{e'?} e \qquad [\![e']\!](a) \neq 0 \qquad x \neq \mathbf{pc}}{\langle m, a\rangle \to \langle m, a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1]\rangle}$$

$$\text{(Terminate)}\quad \frac{p(a(\mathbf{pc})) = \bot}{\langle m, a\rangle \to \langle m, a[\mathbf{pc} \mapsto \bot]\rangle}$$

$$\text{(Load)}\quad \frac{p(a(\mathbf{pc})) = \mathbf{load}\ x, e \qquad x \neq \mathbf{pc} \qquad n = [\![e]\!](a)}{\langle m, a\rangle \xrightarrow{\texttt{load}\ n} \langle m, a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1, x \mapsto m(n)]\rangle}$$

$$\text{(Store)}\quad \frac{p(a(\mathbf{pc})) = \mathbf{store}\ x, e \qquad n = [\![e]\!](a)}{\langle m, a\rangle \xrightarrow{\texttt{store}\ n} \langle m[n \mapsto a(x)], a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1]\rangle}$$

$$\text{(Beqz-Sat)}\quad \frac{p(a(\mathbf{pc})) = \mathbf{beqz}\ x, \ell \qquad a(x) = 0}{\langle m, a\rangle \xrightarrow{\texttt{pc}\ \ell} \langle m, a[\mathbf{pc} \mapsto \ell]\rangle}$$

$$\text{(Beqz-Unsat)}\quad \frac{p(a(\mathbf{pc})) = \mathbf{beqz}\ x, \ell \qquad a(x) \neq 0}{\langle m, a\rangle \xrightarrow{\texttt{pc}\ a(\mathbf{pc})+1} \langle m, a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1]\rangle}$$

$$\text{(Jmp)}\quad \frac{p(a(\mathbf{pc})) = \mathbf{jmp}\ e \qquad \ell = [\![e]\!](a)}{\langle m, a\rangle \xrightarrow{\texttt{pc}\ \ell} \langle m, a[\mathbf{pc} \mapsto \ell]\rangle}$$

$$\text{(Call)}\quad \frac{p(a(\mathbf{pc})) = \mathbf{call}\ f \qquad \mathcal{F}(f) = n \qquad a' = a[\mathbf{pc} \mapsto n, \mathbf{sp} \mapsto a(\mathbf{sp}) - 8] \qquad m' = m[a'(\mathbf{sp}) \mapsto a(\mathbf{pc}) + 1]}{\langle m, a\rangle \xrightarrow{\texttt{call}\ f} \langle m', a'\rangle}$$

$$\text{(Ret)}\quad \frac{p(a(\mathbf{pc})) = \mathbf{ret} \qquad l = m(a(\mathbf{sp})) \qquad a' = a[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto a(\mathbf{sp}) + 8]}{\langle m, a\rangle \xrightarrow{\texttt{ret}\ l} \langle m, a'\rangle}$$

The evaluation relation $\to$ captures individual steps in the execution of a μAsm program.
Further, we define some shorthand notation for common interactions:

Definition 6. *We will write the shorthand $a[x \mapsto y]$ with $x \in Regs$ and $y \in Vals$ for the assignment $a' \in Assgn$ that satisfies $a'(x) = y$ and otherwise behaves similar to a. This updates a single register.*
We will do the same for memories and lift this to configurations in the obvious way with $\sigma = \langle m, a\rangle$:

$$\langle m, a\rangle[x \mapsto y] := \langle m, a[x \mapsto y]\rangle \text{ with } x \in Regs\ y \in Vals$$
$$\langle m, a\rangle(l \mapsto y) := \langle m(l \mapsto y), a\rangle \text{ with } l \in Vals\ y \in Vals$$

Definition 7. *Sequences of elements $e_1, \cdots, e_n$ are indicated as $\bar{e}$ and $\bar{e} \cdot e$ denotes a stack with top element e and rest of the stack $\bar{e}$.*

We now define the behaviour of the non-speculative semantics We add rules to define a run of the program

$$\boxed{\sigma \Downarrow_{\bar{\tau}} \sigma'}$$

$$\text{(NS-Reflection)}\quad \frac{}{\sigma \Downarrow_{\varepsilon} \sigma} \qquad \text{(NS-Single)}\quad \frac{\sigma \Downarrow_{\bar{\tau}} \sigma'' \qquad \sigma'' \xrightarrow{\tau} \sigma'}{\sigma \Downarrow_{\bar{\tau}\cdot\tau} \sigma'}$$

$$\boxed{p \times InitConf \ \text{👻}^{O}_{S}\ \bar{\tau}}$$

$$\frac{\exists \sigma' \quad \sigma' \in \mathit{FinalConf} \quad \sigma \Downarrow_{\overline{\tau}} \sigma'}{(p,\sigma) \,\text{👻}^{O}_{NS}\, \overline{\tau}} \text{(NS-Trace)} \qquad \frac{}{\mathit{Beh}_{NS}(p) = \{\overline{\tau} \mid \forall \sigma \in \mathit{InitConf}.\ (p,\sigma) \,\text{👻}^{O}_{NS}\, \overline{\tau}\}} \text{(NS-Beh)}$$

We define the behaviour of a program p, written $\mathit{Beh}_{NS}(p)$, as the set of traces that are generated starting from an initial configuration σ.

B.1 Symbolic Non-Speculative Semantics

We use the symbolic non-speculative semantics of Spectector and extend it with additional rules for **call** and **ret**:

We assume **sp** to be concrete. The symbolic state $\sigma_{\mathcal{S}}$ consists of a symbolic memory sm, symbolic assignments sa and a stack for the symbolic path condition $\delta^{\mathcal{S}}$. We extend it with additional rules for **call** and **ret**.

$$\frac{p(sa(\mathbf{pc})) = \mathbf{call}\ f \quad \mathcal{F}(f) = n \quad sa' = sa[\mathbf{pc} \mapsto n, \mathbf{sp} \mapsto sa(\mathbf{sp}) - 8] \quad sm' = \mathbf{write}(sm, sa(\mathbf{pc}) + 1, sa'(\mathbf{sp}))}{\langle sm, sa, \delta^{\mathcal{S}} \rangle \xrightarrow{\texttt{call}\ f} \langle sm', sa', \delta^{\mathcal{S}} \cdot \texttt{symPc}(\top) \rangle} \text{(Call-Symb)}$$

$$\frac{p(a(\mathbf{pc})) = \mathbf{ret} \quad l = \mathbf{read}(sm, sa(\mathbf{sp})) \quad l \in \mathit{Vals} \quad s' = sa[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto sa(\mathbf{sp}) + 8]}{\langle sm, sa, \delta^{\mathcal{S}} \rangle \xrightarrow{\texttt{ret}\ l} \langle sm, sa', \delta^{\mathcal{S}} \cdot \texttt{symPc}(\top) \rangle} \text{(Ret-Concr)}$$

$$\frac{p(a(\mathbf{pc})) = \mathbf{ret} \quad l = \mathbf{read}(sm, sa(\mathbf{sp})) \quad l \notin \mathit{Vals} \quad sa' = sa[\mathbf{pc} \mapsto l', \mathbf{sp} \mapsto sa(\mathbf{sp}) + 8] \quad l' \in \mathit{Vals}}{\langle sm, sa, \delta^{\mathcal{S}} \rangle \xrightarrow{\texttt{ret}\ l'} \langle sm, sa', \delta^{\mathcal{S}} \cdot \texttt{symPc}(l = l') \rangle} \text{(Ret-Symb)}$$

Note that we pushed the symbolic path condition `symPc()` into its own structure $\delta^{\mathcal{S}}$. This is done for all other rules not shown here as well. This stack $\delta^{\mathcal{S}}$ is just deleted by the concretization function $\mu()$.

Here is a short review of the rules of B

$\boxed{\Sigma_B \overset{\tau}{\dashrightarrow}_B \Sigma'_B}$

$$\frac{\Phi_B \overset{\tau}{\dashrightarrow}_B \overline{\Phi}'_B}{\overline{\Phi}_B \cdot \Phi_B \overset{\tau}{\dashrightarrow}_B \overline{\Phi}_B \cdot \overline{\Phi}'_B}\ \text{(B:AM-Context)}$$

$$\frac{n' = 0 \text{ or p is stuck}}{\overline{\Phi}_B \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle \overset{\mathtt{rlb}_B\ ctr}{\dashrightarrow}_B \overline{\Phi}_B \cdot \langle p, ctr', \sigma, n\rangle}\ \text{(B:AM-Rollback)}$$

$\boxed{\Phi_B \overset{\tau}{\dashrightarrow}_B \overline{\Phi}'_B}$

$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \quad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, \bot\rangle \overset{\tau}{\dashrightarrow}_B \langle p, ctr, \sigma', \bot\rangle}\ \text{(B:AM-barr)} \qquad \frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \quad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, n+1\rangle \overset{\tau}{\dashrightarrow}_B \langle p, ctr, \sigma', 0\rangle}\ \text{(B:AM-barr-spec)}$$

$$\frac{p(\sigma(\mathbf{pc})) \neq \mathbf{beqz}\ x, l, \mathbf{spbarr}, Z \quad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, n+1\rangle \overset{\tau}{\dashrightarrow}_B \langle p, ctr, \sigma', n\rangle}\ \text{(AM-NoBranch)} \qquad \frac{\tau = \mathtt{pc}\ n \mid \mathtt{start}_B\ n}{\Phi_B \overline{\rho} \cdot \tau \overset{\tau}{\dashrightarrow}_B \Phi_B \overline{\rho}}\ \text{(B:AM-General)}$$

$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell \quad (p,\sigma) \xrightarrow{\tau} (p,\sigma') \quad j = min(\omega, n) \quad \sigma'' = \sigma[\mathbf{pc} \mapsto l'] \quad l' = \begin{cases} \sigma(\mathbf{pc}) + 1 & \text{if } \sigma'(\mathbf{pc}) = l \\ l & \text{if } \sigma'(\mathbf{pc}) \neq l \end{cases}}{\langle p, ctr, \sigma, n+1\rangle_{\overline{\rho}} \overset{\tau}{\dashrightarrow}_B \langle p, ctr, \sigma', n\rangle_{\overline{\rho}} \cdot \langle p, ctr+1, \sigma'', j\rangle_{\overline{\rho} \cdot \mathtt{pc}\ \sigma''(\mathbf{pc}) \cdot \mathtt{start}_B\ ctr}}\ \text{(B:AM-Spec)}$$

$\boxed{\Sigma_B \Downarrow_B^{\overline{\tau}} \Sigma'_B}$

$$\frac{}{\Sigma_B \Downarrow_B^{\epsilon} \Sigma_B}\ \text{(B:AM-Reflection)} \qquad \frac{\Sigma_B \Downarrow_B^{\overline{\tau}} \Sigma''_B \quad \Sigma''_B \overset{\tau}{\dashrightarrow}_B \Sigma'_B}{\Sigma_B \Downarrow_B^{\overline{\tau} \cdot \tau} \Sigma'_B}\ \text{(B:AM-Single)}$$

$\boxed{p \times InitConf \Subset_B^{\omega} \overline{\tau}}$

$$\frac{\exists \Sigma'_B \quad \vdash \Sigma'_B : fin \quad \Sigma_B^{init} p, \sigma \Downarrow_B^{\overline{\tau}} \Sigma'_B}{(p,\sigma) \Subset_B^{\omega} \overline{\tau}}\ \text{(B:AM-Trace)} \qquad \frac{}{Beh_B^{\mathcal{A}}(p) = \{\overline{\tau} \mid \forall \sigma \in InitConf.\ (p,\sigma) \Subset_B^{\omega} \overline{\tau}\}}\ \text{(B:AM-Beh)}$$

C SEMANTICS FOR V4

We use a stack $\overline{\rho}$ to declutter our semantics such that only one action is emitted per rule.

$$\overline{\rho} ::= \varepsilon \mid \overline{\rho} \cdot \tau \text{ where } \tau \in Obs$$

It is a stack of observations that is either empty or has an observation τ at the top that will be emitted next. If we do not write a stack $\overline{\rho}$ besides a speculative instance then it is empty.

Furthermore, we have the metaparameter Z which is a list of instructions i. We will later instantiate this Z to define the combined semantics.

C.1 Always Mispredict V4

Speculative program states Σ_S are defined as stacks of Speculative instances $\overline{\Phi}_S$. A speculation instance $\Phi_S = \langle p, ctr, \sigma, n\rangle$ contains the program p, a $ctr \in \mathbb{N}$ to count the transactions, the current configuration σ and the speculation window n. The speculation window n is a natural number n or $\bot$ when there is no specualtive transaction ongoing.

Note that we define $n + 1$ to match $\bot$ as well.

$$\begin{aligned} \textit{Speculative States } \Sigma_S &::= \overline{\Phi}_S \\ \textit{Speculative Instance } \Phi_S &::= \langle p, ctr, \sigma, n\rangle_{\overline{\rho}} \\ \tau &::= \texttt{bypass}\ n \mid \texttt{start}_S\ ctr \mid \texttt{rlb}_S\ ctr \end{aligned}$$

Notice that $\texttt{start}\ ctr$ and $\texttt{rlb}\ ctr$ are now indexed by the speculative semantics they came from

Judgements

$\Sigma_S \overset{\tau}{\dashrightarrow}_S \Sigma'_S$	State Σ_S small-steps to Σ'_S and emits observation τ.
$\Phi_S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_S$	Speculative instance Φ_S small-steps to $\overline{\Phi}_S{}'$ and emits observation τ.
$\Sigma_S \Downarrow^{\overline{\tau}}_S \Sigma'_S$	State Σ_S big-steps to Σ'_S and emits a list of observations $\overline{\tau}$.
$p \times \mathit{InitConf} \overset{\omega}{\curvearrowright}_S \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$\Sigma_S \overset{\tau}{\dashrightarrow}_S \Sigma'_S$

$$\frac{\Phi_S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_S}{\overline{\Phi}_S \cdot \Phi_S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}_S \cdot \overline{\Phi}'_S}\ \text{(S:AM-Context)}$$

$$\frac{n' = 0 \text{ or p is stuck}}{\overline{\Phi}_S \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle \overset{\texttt{rlb}_S\ ctr}{\dashrightarrow}_S \overline{\Phi}_S \cdot \langle p, ctr', \sigma, n\rangle}\ \text{(S:AM-Rollback)}$$

$\Phi_S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_S$

$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, \bot\rangle \overset{\tau}{\dashrightarrow}_S \langle p, ctr, \sigma', \bot\rangle}\ \text{(S:AM-barr)}$$

$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, n+1\rangle \overset{\tau}{\dashrightarrow}_S \langle p, ctr, \sigma', 0\rangle}\ \text{(S:AM-barr-spec)}$$

$$\frac{p(\sigma(\mathbf{pc})) \neq \mathbf{store}\ x, e, \mathbf{spbarr}, Z \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, n+1\rangle \overset{\tau}{\dashrightarrow}_S \langle p, ctr, \sigma', n\rangle}\ \text{(S:AM-NoBranch)}$$

$$\frac{\tau = \texttt{bypass}\ n \mid \texttt{start}_S\ n}{\Phi_S{}_{\overline{\rho}\cdot\tau} \overset{\tau}{\dashrightarrow}_S \Phi_S{}_{\overline{\rho}}}\ \text{(S:AM-General)}$$

$$\frac{\begin{array}{c} p(\sigma(\mathbf{pc})) = \mathbf{store}\ x, e \qquad \sigma \xrightarrow{\tau} \sigma' \\ \sigma'' = \sigma[\mathbf{pc} \mapsto \sigma(\mathbf{pc}) + 1] \qquad j = min(\omega, n) \end{array}}{\langle p, ctr, \sigma, n+1\rangle_{\overline{\rho}} \overset{\tau}{\dashrightarrow}_S \langle p, ctr, \sigma', n\rangle_{\overline{\rho}} \cdot \langle p, ctr+1, \sigma'', j\rangle_{\overline{\rho}\cdot\texttt{bypass}\ \sigma(\mathbf{pc})\cdot\texttt{start}_S\ ctr}}\ \text{(S:AM-Store-Spec)}$$

For now it is easiest to think of Z as the empty list of instructions. Later on we will use a different value for Z to combine the semantics.

$\Sigma_S \Downarrow^{\overline{\tau}}_S \Sigma'_S$

$$\frac{}{\Sigma_S \Downarrow_S^{\varepsilon} \Sigma_S}\ \text{(S:AM-Reflection)} \qquad \frac{\Sigma_S \Downarrow_S^{\overline{\tau}} \Sigma_S'' \quad \Sigma_S'' \xrightarrow{\tau}_S \Sigma_S'}{\Sigma_S \Downarrow_S^{\overline{\tau}\cdot\tau} \Sigma_S'}\ \text{(S:AM-Single)}$$

Let us define what it means for a state to be initial or final.

Helpers

$$\frac{\Sigma_S = \langle p, 0, \sigma, \bot\rangle \quad \sigma \in \mathit{InitConf}}{\vdash \Sigma_S : \mathit{init}}\ \text{(S:AM-Init)} \qquad \frac{\Sigma_S = \langle p, \mathit{ctr}, \sigma, \bot\rangle \quad \sigma(\mathbf{pc}) = \bot}{\vdash \Sigma_S : \mathit{fin}}\ \text{(S:AM-Fin)}$$

$$\frac{}{\Sigma_S^{\mathit{init}} p, \sigma := \langle p, 0, \sigma, \bot\rangle}\ \text{(S:AM-Initial-State)}$$

$p \times \mathit{InitConf}\ \text{🕱}_S^{\omega}\ \overline{\tau}$

$$\frac{\exists \Sigma_S' \quad \vdash \Sigma_S' : \mathit{fin} \quad \Sigma_S^0(p,\sigma) \Downarrow_S^{\overline{\tau}} \Sigma_S'}{p, \sigma\ \text{🕱}_S^{\omega}\ \overline{\tau}}\ \text{(S:AM-Trace)} \qquad \frac{}{\mathit{Beh}_S^{\mathcal{A}}(p) = \{\overline{\tau} \mid \forall \sigma \in \mathit{InitConf}.\ p, \sigma\ \text{🕱}_S^{\omega}\ \overline{\tau}\}}\ \text{(S:AM-Beh)}$$

We define the behaviour of a program p, written $\mathit{Beh}_S^{\mathcal{A}}(p)$, as the set of traces that are generated starting from an initial configuration σ.

C.2 Oracle Semantics for V4

We use an oracle O to decide if a **store** instruction should be skipped or not as well as a new speculation window ω for that transaction. So $O(p, n, h)$ returns $(\{\text{true}, \text{false}\}, \omega)$. We keep track of the history h of decisions. Our speculation instances are now defined as:

$$\begin{aligned} \textit{Speculative States } X_S &::= \overline{\Psi}_S \\ \textit{Speculative Instance } \Psi_S &::= \langle p, \mathit{ctr}, \sigma, h, n\rangle_{\rho}^{b} \text{ where } b \in \{\text{true}, \text{false}, \varepsilon\} \\ \tau &::= .. \mid \texttt{commit}_S\ \mathit{ctr} \end{aligned}$$

Here ε is used as annotations for all speculative instances with $n = \bot$. If a rule does not change the value of b we will omit this annotation. The oracle semantics uses the same trace model as the AM semantics extended with $\texttt{commit}_S\ \mathit{ctr}$ observation. The ctr is used to annotate traces so one can find $\texttt{start}_S\ \mathit{ctr}$, $\texttt{rlb}_S\ \mathit{ctr}$ and $\texttt{commit}_S\ \mathit{ctr}$ pairs.

We use two helper functions $\mathit{decr}(\overline{\Psi}_S)$ and $\mathit{zeroes}(\overline{\Psi}_S)$ to decrease the window of all speculative instances during execution.

Definition 8 (Decrease function V4)**.**

$$\begin{aligned} \mathit{decr}() : X_S &\mapsto X_S \\ \mathit{decr}(\varepsilon) &= \varepsilon \\ \mathit{decr}(\overline{\Psi}_S \cdot (p, \mathit{ctr}, \sigma, h, n+1)) &= \mathit{decr}(\overline{\Psi}_S) \cdot \langle p, \mathit{ctr}, \sigma, h, n\rangle \\ \mathit{decr}(\overline{\Psi}_S \cdot \langle p, \mathit{ctr}, \sigma, h, n\rangle) &= \mathit{decr}(\overline{\Psi}_S) \cdot \langle p, \mathit{ctr}, \sigma, h, n\rangle \ \mathit{if}\ n = 0\ \mathit{or}\ n = \bot \end{aligned}$$

Definition 9 (Zeroes function V4)**.**

$$\begin{aligned} \mathit{zeroes}() : X_S &\mapsto X_S \\ \mathit{zeroes}(\varepsilon) &= \varepsilon \\ \mathit{zeroes}(\overline{\Psi}_S \cdot (p, \mathit{ctr}, \sigma, h, n+1)) &= \mathit{zeroes}(\overline{\Psi}_S) \cdot \langle p, \mathit{ctr}, \sigma, h, 0\rangle \\ \mathit{zeroes}(\overline{\Psi}_S \cdot \langle p, \mathit{ctr}, \sigma, h, n\rangle) &= \mathit{zeroes}(\overline{\Psi}_S) \cdot \langle p, \mathit{ctr}, \sigma, h, n\rangle \ \mathit{if}\ n = 0\ \mathit{or}\ n = \bot \end{aligned}$$

Judgements

$X_S \overset{\tau}{\rightsquigarrow}_S^{O} X_S'$	State X_S small-steps to X_S' and emits observation τ.
$\Phi_S \overset{\tau}{\rightsquigarrow}_S^{O} \overline{\Phi}_S'$	Speculative instance Ψ_S small-steps to $\overline{\Psi}_S{}'$ and emits observation τ.
$X_S \overset{O}{\Downarrow}_{\overline{\tau}}^{S} X_S'$	State X_S big-steps to X_S' and emits a list of observations $\overline{\tau}$.
$p \times \mathit{InitConf}\ \text{🕱}_S^{O}\ \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$X_S \overset{\tau}{\rightsquigarrow}_S^O X_S'$

(S:SE-Context)
$$\frac{\Psi_S \overset{\tau}{\rightsquigarrow}_S^O \overline{\Psi}_S' \qquad \Psi_S = \langle p, ctr, \sigma, h, n\rangle \qquad \text{if } p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \text{ then } \overline{\Psi}_{S1} = zeroes(\overline{\Psi}_S) \text{ else } \overline{\Psi}_{S1} = decr(\overline{\Psi}_S)}{\overline{\Psi}_S \cdot \Psi_S \overset{\tau}{\rightsquigarrow}_S^O \overline{\Psi}_{S1} \cdot \overline{\Psi}_S'}$$

(S:Rollback)
$$\frac{n' = 0 \text{ or p is stuck}}{\overline{\Psi}_S \cdot \langle p, ctr, \sigma, h, n\rangle \cdot \langle p, ctr', \sigma', h', n'\rangle^{true} \cdot \overline{\Psi}_S' \overset{\texttt{rlb}\ ctr}{\rightsquigarrow}_S^O \overline{\Psi}_S \cdot \langle p, ctr', \sigma, h, n\rangle}$$

(S:Commit)
$$\frac{}{\overline{\Psi}_S \cdot \langle p, ctr, \sigma, h, n\rangle^b \cdot \langle p, ctr', \sigma', h', 0\rangle^{false} \cdot \overline{\Psi}_S' \overset{\texttt{commit}_S\ ctr}{\rightsquigarrow}_S^O \overline{\Psi}_S \cdot \langle p, ctr', \sigma', h', n\rangle^b \cdot \overline{\Psi}_S'}$$

(S:General)
$$\frac{\tau = \texttt{bypass}\ n \mid \texttt{start}\ n}{\overline{\Psi}_S \cdot \Psi_{S\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}_S^O \overline{\Psi}_S \cdot \Psi_{S\overline{\rho}}}$$

$\Psi_S \overset{\tau}{\rightsquigarrow}_S^O \Psi_S'$

(S:barr)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, h, \bot\rangle \overset{\tau}{\rightsquigarrow}_S^O \langle p, ctr, \sigma', h, \bot\rangle}$$

(S:barr-spec)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, h, n+1\rangle \overset{\tau}{\rightsquigarrow}_S^O \langle p, ctr, \sigma, h, 0\rangle}$$

(S:NoBranch)
$$\frac{p(\sigma(\mathbf{pc})) \neq \mathbf{store}\ x, e, \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, h, n+1\rangle \overset{\tau}{\rightsquigarrow}_S^O \langle p, ctr, \sigma', h, n\rangle}$$

(S:Store-Skip)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{store}\ x, e \qquad \sigma \xrightarrow{\tau} \sigma' \qquad O(p, n, h) = (true, \omega) \qquad l = \sigma(\mathbf{pc}) + 1 \qquad \sigma'' = \sigma[\mathbf{pc} \mapsto l] \qquad h' = h \cdot \langle \sigma(\mathbf{pc}), true\rangle}{\langle p, ctr, \sigma, h, n+1\rangle \overset{\tau}{\rightsquigarrow}_S^O \langle p, ctr, \sigma', h', n\rangle \cdot \langle p, ctr+1, \sigma'', h', \omega\rangle^{true}_{\texttt{bypass}\ \sigma(\mathbf{pc})\cdot\texttt{st}\ (ctr)}}$$

(S:Store-Exe)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{store}\ x, e \qquad \sigma \xrightarrow{\tau} \sigma' \qquad O(p, n, h) = (false, \omega) \qquad h' = h \cdot \langle \sigma(\mathbf{pc}), false\rangle}{\langle p, ctr, \sigma, h, n+1\rangle \overset{\tau}{\rightsquigarrow}_S^O \langle p, ctr, \sigma', h, n\rangle \cdot \langle p, ctr+1, \sigma', h', \omega\rangle^{false}_{\texttt{st}\ (ctr)}}$$

In commit we forget the previous state because the committed state is the new one. We carry b because the previous state could have been created by speculation.

We add rules to define a run of the program

$X_S \overset{O}{\Downarrow}_{\overline{\tau}}^S X_S'$

(S:Reflection)
$$\frac{}{X_S \overset{O}{\Downarrow}_{\varepsilon}^S X_S}$$

(S:Single)
$$\frac{X_S \overset{O}{\Downarrow}_{\overline{\tau}}^S X_S'' \qquad X_S'' \overset{\tau}{\rightsquigarrow}_S^O X_S'}{X_S \overset{O}{\Downarrow}_{\overline{\tau}\cdot\tau}^S X_S'}$$

where $X_S \overset{O}{\Downarrow}_{\overline{\tau}}^S X_S'$ denotes a program run for program p starting in the speculative state X_S, terminating in the state X_S' creating the observations $\overline{\tau}$.

Let us define what it means for a state to be initial or final.

Helpers

(S:SE-Init)
$$\frac{X_S = \langle p, 0, \sigma, \varepsilon, \bot\rangle \qquad \sigma \in InitConf}{\vdash X_S : init}$$

(S:SE-Fin)
$$\frac{X_S = \langle p, ctr, \sigma, h, \bot\rangle \qquad \sigma(\mathbf{pc}) = \bot}{\vdash X_S : fin}$$

(S:SE-Initial-State)
$$\frac{}{X_S^{init}(p, \sigma) := \langle p, 0, \sigma, \varepsilon, \bot\rangle}$$

$p \times InitConf \; \text{👻}^{O}_{S} \; \overline{\tau}$

(S:SE-Trace)
$$\frac{\exists X'_S \quad \vdash X'_S : fin \qquad X^{init}_S(p,\sigma) \overset{O}{\Downarrow}{}^{S}_{\overline{\tau}} X'_S}{p, \sigma \; \text{👻}^{O}_{S} \; \overline{\tau}}$$

(S:SE-Beh)
$$\frac{}{Beh^{O}_{S}(p) = \{\overline{\tau} \mid \forall \sigma \in InitConf \,.\, p, \sigma \; \text{👻}^{O}_{S} \; \overline{\tau}\}}$$

We define the behaviour of a program p, written $Beh^{O}_{S}(p)$, as the set of traces that are generated starting from an initial configuration σ.

C.3 Symbolic Semantics

The symbolic semantics is similar to the AM semantics. Instead of concrete configurations σ and the non-speculative semantics, it uses symbolic configurations $\sigma_{\mathcal{S}}$ and the symbolic non-speculative semantics $\rightarrow^{\mathcal{S}}$. The symbolic states $\Sigma^{\mathcal{S}}_{S}$.

$\Sigma^{\mathcal{S}}_{S} \overset{\tau}{\dashrightarrow}{}^{\mathcal{S}}_{S} \Sigma^{\mathcal{S}\prime}_{S}$

(S:Sym-Context)
$$\frac{\Phi^{\mathcal{S}}_{S} \overset{\tau}{\dashrightarrow}{}^{\mathcal{S}}_{S} \overline{\Phi}'_{S_{\mathcal{S}}}}{\overline{\Phi}_{S_{\mathcal{S}}} \cdot \Phi^{\mathcal{S}}_{S} \overset{\tau}{\dashrightarrow}{}^{\mathcal{S}}_{S} \overline{\Phi}_{S_{\mathcal{S}}} \cdot \overline{\Phi}'_{S_{\mathcal{S}}}}$$

(S:Sym-Rollback)
$$\frac{n' = 0 \text{ or p is stuck}}{\overline{\Phi}_{S_{\mathcal{S}}} \cdot \langle p, ctr, \sigma_{\mathcal{S}}, n\rangle \cdot \langle p, ctr', \sigma'_{\mathcal{S}}, n'\rangle_{\overline{\rho}} \overset{\texttt{rlb}_S \; ctr}{\dashrightarrow}{}^{\mathcal{S}}_{S} \overline{\Phi}_{S_{\mathcal{S}}} \cdot \langle p, ctr', \sigma_{\mathcal{S}}, n\rangle_{\overline{\rho} \cdot \texttt{pc}} \, \sigma_{\mathcal{S}}(\mathbf{pc})}$$

$\Phi^{\mathcal{S}}_{S} \overset{\tau}{\dashrightarrow}{}_{S} \overline{\Phi}'_{S_{\mathcal{S}}}$

(S:Sym-barr)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma_{\mathcal{S}} \overset{\tau}{\rightarrow}{}^{\mathcal{S}} \sigma'_{\mathcal{S}}}{\langle p, ctr, \sigma_{\mathcal{S}}, \bot\rangle \overset{\tau}{\dashrightarrow}{}^{\mathcal{S}}_{S} \langle p, ctr, \sigma'_{\mathcal{S}}, \bot\rangle}$$

(S:Sym-barr-spec)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma_{\mathcal{S}} \overset{\tau}{\rightarrow}{}^{\mathcal{S}} \sigma'_{\mathcal{S}}}{\langle p, ctr, \sigma_{\mathcal{S}}, n+1\rangle \overset{\tau}{\dashrightarrow}{}^{\mathcal{S}}_{S} \langle p, ctr, \sigma'_{\mathcal{S}}, 0\rangle}$$

(S:Sym-NoBranch)
$$\frac{p(\sigma(\mathbf{pc})) \neq \mathbf{store}\; x, e, \mathbf{spbarr}, Z \qquad \sigma_{\mathcal{S}} \overset{\tau}{\rightarrow}{}^{\mathcal{S}} \sigma'_{\mathcal{S}}}{\langle p, ctr, \sigma_{\mathcal{S}}, n+1\rangle \overset{\tau}{\dashrightarrow}{}^{\mathcal{S}}_{S} \langle p, ctr, \sigma'_{\mathcal{S}}, n\rangle}$$

(S:Sym-General)
$$\frac{\tau = \texttt{bypass}\; n \mid \texttt{start}_S \; n}{\Phi^{\mathcal{S}}_{S} \, \overline{\rho \cdot \tau} \overset{\tau}{\dashrightarrow}{}^{\mathcal{S}}_{S} \Phi^{\mathcal{S}}_{S} \, \overline{\rho}}$$

(S:Sym-Store-Spec)
$$\frac{\begin{array}{c} p(\sigma(\mathbf{pc})) = \mathbf{store}\; x, e \qquad \sigma_{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\longrightarrow}{}^{\mathcal{S}} \sigma'_{\mathcal{S}} \\ \sigma''_{\mathcal{S}} = \sigma[\mathbf{pc} \mapsto \sigma(\mathbf{pc}) + 1] \qquad \sigma''_{\mathcal{S}} = \sigma'_{\mathcal{S}}.\delta^{\mathcal{S}} \qquad j = min(\omega, n) \end{array}}{\langle p, ctr, \sigma_{\mathcal{S}}, n+1\rangle_{\overline{\rho}} \overset{\tau}{\dashrightarrow}{}^{\mathcal{S}}_{S} \langle p, ctr, \sigma'_{\mathcal{S}}, n\rangle_{\overline{\rho}} \cdot \langle p, ctr+1, \sigma'', j\rangle_{\overline{\rho} \cdot \texttt{bypass}\; \sigma(\mathbf{pc}) \cdot \texttt{start}_S \; ctr}}$$

$\Sigma^{\mathcal{S}}_{S} \; \alpha \Downarrow^{\overline{\tau}}_{S} \Sigma^{\mathcal{S}\prime}_{S}$

(S:Sym-Reflection)
$$\frac{}{\Sigma^{\mathcal{S}}_{S} \; \alpha \Downarrow^{\varepsilon}_{S} \Sigma^{\mathcal{S}}_{S}}$$

(S:Sym-Single)
$$\frac{\Sigma_S \; \alpha \Downarrow^{\overline{\tau}}_{S} \Sigma''_S \qquad \Sigma''_S \overset{\tau}{\dashrightarrow}{}^{\mathcal{S}}_{S} \Sigma'_S}{\Sigma^{\mathcal{S}}_{S} \; \alpha \Downarrow^{\overline{\tau} \cdot \tau_S}_{S} \Sigma^{\mathcal{S}\prime}_{S}}$$

Let us define what it means for a state to be initial or final.

Helpers

(S:Sym-Init)
$$\frac{\Sigma^{\mathcal{S}}_{S} = \langle p, 0, \sigma_{\mathcal{S}}, \bot\rangle \qquad \sigma_{\mathcal{S}} \in InitConf}{\vdash \Sigma^{\mathcal{S}}_{S} : init}$$

(S:Sym-Fin)
$$\frac{\Sigma^{\mathcal{S}}_{S} = \langle p, ctr, \sigma_{\mathcal{S}}, \bot\rangle \qquad \sigma_{\mathcal{S}}(\mathbf{pc}) = \bot}{\vdash \Sigma^{\mathcal{S}}_{S} : fin}$$

(S:Sym-Initial-State)
$$\frac{}{\Sigma^{init}_{S} p, \sigma_{\mathcal{S}} := \langle p, 0, \sigma_{\mathcal{S}}, \bot\rangle}$$

$(p \times InitConf) \; _{\alpha}\text{👻}^{\omega}_{S} \; \overline{\tau}$

$$\frac{\exists \Sigma'_{\mathsf{S}} \quad \vdash \Sigma'_{\mathsf{S}} : \mathit{fin} \qquad \Sigma^0_{\mathsf{S}}(p,\sigma)\ {}_{\alpha}\Downarrow^{\overline{\tau}}_{\mathsf{S}}\ \Sigma'_{\mathsf{S}}}{(p,\sigma_{\mathcal{S}})\ {}_{\alpha}\text{🕮}^{\omega}_{\mathsf{S}}\ \overline{\tau}}\ (\text{S:Sym-Trace}) \qquad \frac{}{\mathit{Beh}^{\mathcal{S}}_{\mathsf{S}}(p) = \{\overline{\tau} \mid \forall \sigma_{\mathcal{S}} \in \mathit{InitConf}.\ (p,\sigma)\ {}_{\alpha}\text{🕮}^{\omega}_{\mathsf{S}}\ \overline{\tau}\}}\ (\text{S:Sym-Beh})$$

We define the behaviour of a program p, written $\mathit{Beh}^{\mathcal{S}}_{\mathsf{S}}(p)$, as the set of traces that are generated starting from an initial configuration $\sigma_{\mathcal{S}}$.

D SPECTRE V5

We change Speculation instances to contain the RSB $\mathbb{R}$. The RSB is a stack containing return addresses.

$$\begin{aligned} \textit{Speculative State } \Sigma_R &::= \Phi_R \\ \textit{Speculative Instance } \Phi_R &::= \langle p, ctr, \sigma, \mathbb{R}, n\rangle_{\overline{\rho}} \\ \tau &::= \texttt{start}_R\ ctr \mid \texttt{rlb}_R\ ctr \end{aligned}$$

Judgements

$\Sigma_R \overset{\tau}{\dashrightarrow}_R \Sigma'_R$	State Σ_R small-steps to Σ'_R and emits observation τ.
$\Phi_R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_R$	Speculative instance Φ_R small-steps to $\overline{\Phi}'_R$ and emits observation τ.
$\Sigma_R \Downarrow_R^{\overline{\tau}} \Sigma'_R$	State Σ_R big-steps to Σ'_R and emits a list of observations $\overline{\tau}$.
$p \times \mathit{InitConf} \curvearrowright_R^{\omega} \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$\Sigma_R \overset{\tau}{\dashrightarrow}_R \Sigma'_R$

(R:AM-Context)
$$\frac{\Phi_R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_R}{\overline{\Phi}_R \cdot \Phi_R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}_R \cdot \overline{\Phi}'_R}$$

(R:AM-Rollback)
$$\frac{n' = 0 \text{ or p is stuck}}{\overline{\Phi}_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}, n'\rangle \overset{\texttt{rlb}_R\ ctr}{\dashrightarrow}_R \overline{\Phi}_R \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}$$

$\Phi_R \overset{\tau}{\dashrightarrow}_R \Sigma'_R$

(R:AM-barr)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, \mathbb{R}, \bot\rangle \overset{\tau}{\dashrightarrow}_R \langle p, ctr, \sigma', \mathbb{R}, \bot\rangle}$$

(R:AM-barr-spec)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, \mathbb{R}, n+1\rangle \overset{\tau}{\dashrightarrow}_R \langle p, ctr, \sigma', \mathbb{R}, n\rangle}$$

(R:AM-NoBranch)
$$\frac{p(\sigma(\mathbf{pc})) \neq \mathbf{ret}, \mathbf{spbarr}, \mathbf{call}\ f, Z \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, \mathbb{R}, n+1\rangle \overset{\tau}{\dashrightarrow}_R \langle p, ctr, \sigma', \mathbb{R}, n\rangle}$$

(R:AM-Ret-Spec)
$$\frac{\begin{array}{ccc} p(\sigma(\mathbf{pc})) = \mathbf{ret} & \sigma \xrightarrow{\tau} \sigma' & \mathbb{R} = \mathbb{R}' \cdot l \\ l \neq m(a(sp)) & \sigma'' = \sigma[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto a(\mathbf{sp}) + 8] & j = min(\omega, n) \end{array}}{\langle p, ctr, \sigma, \mathbb{R}, n+1\rangle \overset{\tau}{\dashrightarrow}_R \langle p, ctr, \sigma', \mathbb{R}', n\rangle \cdot \langle p, ctr+1, \sigma'', \mathbb{R}', j\rangle_{\texttt{ret}\ l \cdot \texttt{start}_R\ ctr}}$$

(R:AM-Ret-Same)
$$\frac{\begin{array}{cc} p(\sigma(\mathbf{pc})) = \mathbf{ret} & \sigma \xrightarrow{\tau} \sigma' \qquad \mathbb{R} = \mathbb{R}'; l \\ l = m(a(sp)) & \end{array}}{\langle p, ctr, \sigma, \mathbb{R}, n+1\rangle \overset{\tau}{\dashrightarrow}_R \langle p, ctr, \sigma', \mathbb{R}, n\rangle}$$

(R:AM-Ret-Empty)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{ret} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, \emptyset, n+1\rangle \overset{\tau}{\dashrightarrow}_R \langle p, ctr, \sigma', \emptyset, n\rangle}$$

(R:AM-Call-Full)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{call}\ f \qquad \sigma \xrightarrow{\tau} \sigma' \qquad |\mathbb{R}| \geq RSB_{size}}{\langle p, ctr, \sigma, \mathbb{R}, n+1\rangle \overset{\tau}{\dashrightarrow}_R \langle p, ctr, \sigma', \mathbb{R}, n\rangle}$$

(R:AM-Call)
$$\frac{\begin{array}{cc} p(\sigma(\mathbf{pc})) = \mathbf{call}\ f & \sigma \xrightarrow{\tau} \sigma' \\ \mathbb{R}' = \mathbb{R} \cdot (a(\mathbf{pc}) + 1) & |\mathbb{R}| < RSB_{size} \end{array}}{\langle p, ctr, \sigma, \mathbb{R}, n+1\rangle \overset{\tau}{\dashrightarrow}_R \langle p, ctr, \sigma', \mathbb{R}', n\rangle}$$

(R:AM-General)
$$\frac{\tau = \texttt{ret}\ n \mid \texttt{start}_R\ n}{\Phi_{R\overline{\rho} \cdot \tau} \overset{\tau}{\dashrightarrow}_R \Phi_{R\overline{\rho}}}$$

$\boxed{\Sigma_R \Downarrow_R^{\overline{\tau}} \Sigma'_R}$

$$\frac{}{\Sigma_R \Downarrow_R^{\epsilon} \Sigma_R}\ (R{:}AM\text{-}Reflection) \qquad \frac{\Sigma_R \Downarrow_R^{\overline{\tau}} \Sigma''_R \quad \Sigma''_R \xrightarrow{\tau}_R \Sigma'_R}{\Sigma_R \Downarrow_R^{\overline{\tau}\cdot\tau} \Sigma'_R}\ (R{:}AM\text{-}Single)$$

Let us define what it means for a state to be initial or final.

Helpers

$$\frac{\Sigma_R = \langle p, 0, \sigma, \varepsilon, \bot\rangle \quad \sigma \in InitConf}{\vdash \Sigma_R : init}\ (R{:}AM\text{-}Init) \qquad \frac{\Sigma_R = \langle p, ctr, \sigma, \mathbb{R}, \bot\rangle \quad \sigma(\mathbf{pc}) = \bot}{\vdash \Sigma_R : fin}\ (R{:}AM\text{-}Fin)$$

$$\frac{}{\Sigma_R^{init} p, \sigma := \langle p, 0, \sigma, \varepsilon, \bot\rangle}\ (R{:}AM\text{-}Initial\text{-}State)$$

$\boxed{p \times InitConf \Subset_R^{\omega} \overline{\tau}}$

$$\frac{\exists \Sigma'_R \quad \vdash \Sigma'_R : fin \quad \Sigma_R^{init}(p,\sigma) \Downarrow_R^{\overline{\tau}} \Sigma'_R}{p, \sigma \Subset_R^{\omega} \overline{\tau}}\ (R{:}AM\text{-}Trace) \qquad \frac{}{Beh_R^{\mathcal{A}}(p) = \{\overline{\tau} \mid \forall \sigma \in InitConf.\ p, \sigma \Subset_R^{\omega} \overline{\tau}\}}\ (R{:}AM\text{-}Beh)$$

We define the behaviour of a program p, written $Beh_R^{\mathcal{A}}(p)$, as the set of traces that are generated starting from an initial configuration σ.

D.1 Oracle Semantics for V5

The oracle is defined as $O(p, n)$ and returns a speculation window size n. The reason being, that speculation of return addresses is deterministic in nature. We annotate speculation instances with a boolean b to annotate if the prediction was correct or not.

$$\begin{aligned} \textit{Speculative State } X_R &::= \Psi_R \\ \textit{Speculative Instance } \Psi_R &::= \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle^{\frac{b}{\rho}}\ b \in \{true, false, \varepsilon\} \\ \tau &::= .. \mid \texttt{commit}_R\ ctr \end{aligned}$$

Here ε is used as annotations for all speculative instances with $n = \bot$ and we will omit this annotation.

We use two helper functions $decr(X_R)$ and $zeroes(X_R)$

Definition 10 (Decrease function V5)**.**

$$\begin{aligned} decr() : X_R &\mapsto X_R \\ decr(\varepsilon) &= \varepsilon \\ decr(\overline{\Psi}_R \cdot (p, ctr, \sigma, \mathbb{R}, h, n+1)) &= decr(\overline{\Psi}_R) \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \\ decr(\overline{\Psi}_R \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle) &= decr(\overline{\Psi}_R) \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \ \textit{if } n = 0 \textit{ or } n = \bot \end{aligned}$$

Definition 11 (Zeroes function V5)**.**

$$\begin{aligned} zeroes() : X_R &\mapsto X_R \\ zeroes(\varepsilon) &= \varepsilon \\ zeroes(\overline{\Psi}_R \cdot (p, ctr, \sigma, \mathbb{R}, h, n+1)) &= zeroes(\overline{\Psi}_R) \cdot \langle p, ctr, \sigma, \mathbb{R}, h, 0\rangle \\ zeroes(\overline{\Psi}_R \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle) &= zeroes(\overline{\Psi}_R) \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \ \textit{if } n = 0 \textit{ or } n = \bot \end{aligned}$$

Judgements

$X_R \overset{\tau}{\rightsquigarrow}_R^{O} X'_R$	State X_R small-steps to X'_R and emits observation τ.
$\Psi_R \overset{\tau}{\rightsquigarrow}_R^{O} \overline{\Psi}'_R$	Speculative instance Ψ_R small-steps to $\overline{\Psi}'_R$ and emits observation τ.
$X_R \overset{O}{\Downarrow}_{\overline{\tau}}^{R} X'_R$	State X_R big-steps to X'_R and emits a list of observations $\overline{\tau}$.
$p \times InitConf \Subset_R^{O} \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$X_R \overset{\tau}{\rightsquigarrow}_R^O X'_R$

(R:SE-Context)
$$\frac{\Psi_R \overset{\tau}{\rightsquigarrow}_R^O \overline{\Psi}_R' \qquad \Psi_R = \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \qquad \text{if } p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \text{ then } \overline{\Psi}_{R1} = zeroes(\overline{\Psi}_R) \text{ else } \overline{\Psi}_{R1} = decr(()\overline{\Psi}_R)}{\overline{\Psi}_R \cdot \Psi_R \overset{\tau}{\rightsquigarrow}_R^O \overline{\Psi}_R \cdot \overline{\Psi}_R'}$$

(R:SE-Rollback)
$$\frac{n' = 0 \text{ or p is stuck}}{\overline{\Psi}_R \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}, h', n'\rangle^{false} \cdot \overline{\Psi}_R' \overset{\mathtt{rlb}_R\ ctr}{\rightsquigarrow}_R^O \overline{\Psi}_R \cdot \langle p, ctr', \sigma, \mathbb{R}, h, n\rangle}$$

(R:SE-Commit)
$$\frac{\sigma(\mathbf{pc}) = l'}{\overline{\Psi}_R \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle^b \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0\rangle^{true} \cdot \overline{\Psi}_R' \overset{\mathtt{commit}_R\ ctr}{\rightsquigarrow}_R^O \overline{\Psi}_R \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n\rangle^b \cdot \overline{\Psi}_R'}$$

(R:SE-General)
$$\frac{\tau = \mathtt{ret}\ n \mid \mathtt{start}_R\ n}{\overline{\Psi}_R \cdot \Psi_{R\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}_R^O \overline{\Psi}_R \cdot \Psi_{R\overline{\rho}}}$$

$\Psi_R \overset{\tau}{\rightsquigarrow}_R^O \Psi'_R$

(R:SE-barr)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, \mathbb{R}, h, \bot\rangle \overset{\tau}{\rightsquigarrow}_R^O \langle p, ctr, \sigma', \mathbb{R}, h, \bot\rangle}$$

(R:SE-barr-spec)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, \mathbb{R}, h, n+1\rangle \overset{\tau}{\rightsquigarrow}_R^O \langle p, ctr, \sigma', \mathbb{R}, h, 0\rangle}$$

(R:SE-NoBranch)
$$\frac{p(\sigma(\mathbf{pc})) \neq \mathbf{ret}, \mathbf{spbarr}, \mathbf{call}\ f \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, \mathbb{R}, h, n+1\rangle \overset{\tau}{\rightsquigarrow}_R^O \langle p, ctr, \sigma', \mathbb{R}, h, n\rangle}$$

(R:SE-Ret)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{ret} \qquad \sigma \xrightarrow{\tau} \sigma' \qquad \mathbb{R} = \mathbb{R}' \cdot l \qquad O(p, \sigma(\mathbf{pc})) = \omega \qquad \sigma'' = \sigma'[\mathbf{pc} \mapsto l] \qquad h' = h \cdot \langle \sigma(\mathbf{pc}), \omega\rangle)}{\langle p, ctr, \sigma, h, n+1\rangle \overset{\tau}{\rightsquigarrow}_R^O \langle p, ctr, \sigma', \mathbb{R}', h', n\rangle \cdot \langle p, ctr+1, \sigma'', \mathbb{R}', h', \omega\rangle^{m(a(\mathbf{sp}))==l}_{\mathtt{ret}\ l\cdot \mathtt{start}_R\ ctr}}$$

(R:SE-Ret-Empty)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{ret} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, \emptyset, h, n+1\rangle \overset{\tau}{\rightsquigarrow}_R^O \langle p, ctr, \sigma', \emptyset, h, n\rangle}$$

(R:SE-Call-Full)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{call}\ f \qquad \sigma \xrightarrow{\tau} \sigma' \qquad |\mathbb{R}| \geq RSB_{size}}{\langle p, ctr, \sigma, \mathbb{R}, h, n+1\rangle \overset{\tau}{\rightsquigarrow}_R^O \langle p, ctr, \sigma', \mathbb{R}, h, n\rangle}$$

(R:SE-Call)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{call}\ f \qquad \sigma \xrightarrow{\tau} \sigma' \qquad \mathbb{R}' = \mathbb{R} \cdot (a(\mathbf{pc}) + 1) \qquad |\mathbb{R}| < RSB_{size}}{\langle p, ctr, \sigma, \mathbb{R}, n+1\rangle \overset{\tau}{\not\rightsquigarrow}_R \langle p, ctr, \sigma', \mathbb{R}', n\rangle}$$

$\Sigma_R \overset{O}{\downarrow}{}^R_{\overline{\tau}} \Sigma'_R$

(R:SE-Reflection)
$$\frac{}{\Sigma_R \overset{O}{\downarrow}{}^R_{\varepsilon} \Sigma_R}$$

(R:SE-Single)
$$\frac{\Sigma_R \Downarrow_R^{\overline{\tau}} \Sigma''_R \qquad \Sigma''_R \overset{\tau}{\rightsquigarrow}_R^O \Sigma'_R}{\Sigma_R \overset{O}{\downarrow}{}^R_{\overline{\tau}\cdot\tau} \Sigma'_R}$$

Let us define what it means for a state to be initial or final.

Helpers

(R:SE-Init)
$$\frac{X_R = \overline{\Psi}_R \cdot \Psi_R \qquad \overline{\Psi}_R = \varepsilon \qquad \Psi_R = \langle p, 0, \sigma, \varepsilon, \varepsilon, \bot\rangle \qquad \sigma \in InitConf}{\vdash X_R : init}$$

(R:SE-Fin)
$$\frac{X_R = \overline{\Psi}_R \cdot \Psi_R \qquad \overline{\Psi}_R = \varepsilon \qquad \Psi_R = \langle p, ctr, \sigma, \mathbb{R}, h, \bot\rangle \qquad \sigma(\mathbf{pc}) = \bot}{\vdash X_R : fin}$$

(R:SE-Initial-State)
$$\frac{}{X_R^{init}(p, \sigma) := \langle p, 0, \sigma, \varepsilon, \varepsilon, \bot\rangle}$$

$$\boxed{p \times \mathit{InitConf} \;\text{🕮}^{O}_{\mathsf{R}}\; \overline{\tau}}$$

(R:SE-Trace)

$$\frac{\exists X'_{\mathsf{R}} \quad \vdash X'_{\mathsf{R}} : \mathit{fin} \quad X^{\mathit{init}}_{\mathsf{R}}(p,\sigma) \overset{O}{\Downarrow}{}^{\mathsf{R}}_{\overline{\tau}} \Psi'_{\mathsf{R}}}{p, \sigma \;\text{🕮}^{O}_{\mathsf{R}}\; \overline{\tau}}$$

(R:SE-Beh-V4)

$$\frac{}{\mathit{Beh}^{O}_{\mathsf{R}}(p) = \{\overline{\tau} \mid \forall \sigma \in \mathit{InitConf}.\ (p,\sigma) \;\text{🕮}^{O}_{\mathsf{R}}\; \overline{\tau}\}}$$

We define the behaviour of a program p, written $\mathit{Beh}^{O}_{\mathsf{R}}(p)$, as the set of traces that are generated starting from an initial configuration σ.

D.2 Symbolic semantics

Again the only difference to the AM semantics are the symbolic configurations and the symbolic non-speculative semantics.

$$\boxed{\Sigma^{\alpha}_{\mathsf{R}} \overset{\tau_{\mathcal{S}}}{=\!\!=\!\!\text{🕮}^{\alpha}_{\mathsf{R}}} \Sigma^{\alpha\prime}_{\mathsf{R}}}$$

(R:Sym-Context)

$$\frac{\Phi^{\alpha}_{\mathsf{R}} \overset{\tau}{=\!\!\text{🕮}^{\alpha}_{\mathsf{R}}} \overline{\Phi^{\mathcal{S}}}'_{\mathsf{R}}}{\overline{\Phi^{\mathcal{S}}}_{\mathsf{R}} \cdot \Phi^{\alpha}_{\mathsf{R}} \overset{\tau_{\mathcal{S}}}{=\!\!=\!\!\text{🕮}^{\alpha}_{\mathsf{R}}} \overline{\Phi^{\mathcal{S}}}_{\mathsf{R}} \cdot \overline{\Phi^{\mathcal{S}}}'_{\mathsf{R}}}$$

(R:Sym-Rollback)

$$\frac{n' = 0 \text{ or p is stuck}}{\overline{\Phi^{\mathcal{S}}}_{\mathsf{R}} \cdot \langle p, ctr, \sigma_{\mathcal{S}}, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma'_{\mathcal{S}}, \mathbb{R}, n'\rangle^{l} \overset{\mathtt{rlb}_{\mathsf{R}}\ ctr}{=\!\!=\!\!=\!\!\text{🕮}^{\alpha}_{\mathsf{R}}} \overline{\Phi^{\mathcal{S}}}_{\mathsf{R}} \cdot \langle p, ctr', \sigma_{\mathcal{S}}, \mathbb{R}, n\rangle}$$

$$\boxed{\Phi^{\alpha}_{\mathsf{R}} \overset{\tau}{=\!\!\text{🕮}^{\alpha}_{\mathsf{R}}} \Sigma^{\alpha\prime}_{\mathsf{R}}}$$

(R:Sym:AM-barr)

$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \quad \sigma_{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\longrightarrow}{}^{\mathcal{S}} \sigma'_{\mathcal{S}}}{\langle p, ctr, \sigma_{\mathcal{S}}, \mathbb{R}, \bot\rangle \overset{\tau}{=\!\!\text{🕮}^{\alpha}_{\mathsf{R}}} \langle p, ctr, \sigma'_{\mathcal{S}}, \mathbb{R}, \bot\rangle}$$

(R:Sym-barr-spec)

$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \quad \sigma_{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\longrightarrow}{}^{\mathcal{S}} \sigma'_{\mathcal{S}}}{\langle p, ctr, \sigma_{\mathcal{S}}, \mathbb{R}, n+1\rangle \overset{\tau}{=\!\!\text{🕮}^{\alpha}_{\mathsf{R}}} \langle p, ctr, \sigma'_{\mathcal{S}}, \mathbb{R}, n\rangle}$$

(R:Sym-NoBranch)

$$\frac{p(\sigma(\mathbf{pc})) \neq \mathbf{ret}, \mathbf{spbarr}, \mathbf{call}\ f, Z \quad \sigma_{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\longrightarrow}{}^{\mathcal{S}} \sigma'_{\mathcal{S}}}{\langle p, ctr, \sigma_{\mathcal{S}}, \mathbb{R}, n+1\rangle \overset{\tau}{=\!\!\text{🕮}^{\alpha}_{\mathsf{R}}} \langle p, ctr, \sigma'_{\mathcal{S}}, \mathbb{R}, n\rangle}$$

(R:Sym-Ret-Spec)

$$\frac{\begin{array}{ccc} p(\sigma(\mathbf{pc})) = \mathbf{ret} & \sigma_{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\longrightarrow}{}^{\mathcal{S}} \sigma'_{\mathcal{S}} & \mathbb{R} = \mathbb{R}' \cdot l \\ l \neq \mathbf{read}(sm, sa(\mathbf{sp})) \quad \sigma'' = \sigma[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto a(\mathbf{sp}) + 8] & \sigma''.\delta^{\mathcal{S}} = \sigma'_{\mathcal{S}}.\delta^{\mathcal{S}} & j = \mathit{min}(\omega, n) \end{array}}{\langle p, ctr, \sigma_{\mathcal{S}}, \mathbb{R}, n+1\rangle \overset{\tau}{=\!\!\text{🕮}^{\alpha}_{\mathsf{R}}} \langle p, ctr, \sigma'_{\mathcal{S}}, \mathbb{R}', n\rangle \cdot \langle p, ctr+1, \sigma''_{\mathcal{S}}, \mathbb{R}', j\rangle_{\mathtt{ret}\ l \cdot \mathtt{start}_{\mathsf{R}}\ ctr}}$$

(R:Sym-Ret-Same)

$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{ret} \quad \sigma_{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\longrightarrow}{}^{\mathcal{S}} \sigma'_{\mathcal{S}} \quad \mathbb{R} = \mathbb{R}'; l \quad l = \mathbf{read}(sm, sa(\mathbf{sp})))}{\langle p, ctr, \sigma, \mathbb{R}, n+1\rangle \overset{\tau}{=\!\!\text{🕮}^{\alpha}_{\mathsf{R}}} \langle p, ctr, \sigma', \mathbb{R}, n\rangle}$$

(R:Sym-Ret-Empty)

$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{ret} \quad \sigma_{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\longrightarrow}{}^{\mathcal{S}} \sigma'_{\mathcal{S}}}{\langle p, ctr, \sigma_{\mathcal{S}}, \emptyset, n+1\rangle \overset{\tau}{=\!\!\text{🕮}^{\alpha}_{\mathsf{R}}} \langle p, ctr, \sigma'_{\mathcal{S}}, \emptyset, n\rangle}$$

(R:Sym-Call-Full)

$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{call}\ f \quad \sigma_{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\longrightarrow}{}^{\mathcal{S}} \sigma'_{\mathcal{S}} \quad |\mathbb{R}| \geq \mathit{RSB}_{\mathit{size}}}{\langle p, ctr, \sigma_{\mathcal{S}}, \mathbb{R}, n+1\rangle \overset{\tau}{=\!\!\text{🕮}^{\alpha}_{\mathsf{R}}} \langle p, ctr, \sigma'_{\mathcal{S}}, \mathbb{R}, n\rangle}$$

(R:Sym-Call)

$$\frac{\begin{array}{cc} p(\sigma(\mathbf{pc})) = \mathbf{call}\ f & \sigma_{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\longrightarrow}{}^{\mathcal{S}} \sigma'_{\mathcal{S}} \\ \mathbb{R}' = \mathbb{R} \cdot (\sigma_{\mathcal{S}}(\mathbf{pc}) + 1) & |\mathbb{R}| < \mathit{RSB}_{\mathit{size}} \end{array}}{\langle p, ctr, \sigma_{\mathcal{S}}, \mathbb{R}, n+1\rangle \overset{\tau_{\mathcal{S}}}{=\!\!\text{🕮}^{\alpha}_{\mathsf{R}}} \langle p, ctr, \sigma'_{\mathcal{S}}, \mathbb{R}', n\rangle}$$

(R:Sym-General)

$$\frac{\tau = \mathtt{ret}\ n \mid \mathtt{start}_{\mathsf{R}}\ n}{\Phi^{\alpha}_{\mathsf{R}\,\overline{\rho_{\mathcal{S}}} \cdot \tau} \overset{\tau_{\mathcal{S}}}{=\!\!\text{🕮}^{\alpha}_{\mathsf{R}}} \Phi^{\alpha}_{\mathsf{R}\,\overline{\rho_{\mathcal{S}}}}}$$

$$\boxed{\Sigma^{\alpha}_{\mathsf{R}}\ \alpha \Downarrow^{\overline{\tau}}_{\mathsf{R}} \Sigma^{\alpha\prime}_{\mathsf{R}}}$$

$$\frac{}{\Sigma_{\mathrm{R}}^{\alpha}\ \alpha\Downarrow_{\mathrm{R}}^{\varepsilon}\ \Sigma_{\mathrm{R}}^{\alpha}}\ \text{(R:Sym-Reflection)} \qquad \frac{\Sigma_{\mathrm{R}}^{\alpha}\ \alpha\Downarrow_{\mathrm{R}}^{\overline{\tau_\alpha}}\ \Sigma_{\mathrm{R}}^{\alpha\prime\prime} \qquad \Sigma_{\mathrm{R}}^{\alpha\prime\prime}\ \overset{\tau}{\dashrightarrow}_{\mathrm{R}}^{\alpha}\ \Sigma_{\mathrm{R}}^{\alpha\prime}}{\Sigma_{\mathrm{R}}^{\alpha}\ \alpha\Downarrow_{\mathrm{R}}^{\overline{\tau_\alpha}\cdot\tau_{\mathcal{S}}}\ \Sigma_{\mathrm{R}}^{\alpha\prime}}\ \text{(R:Sym-Single)}$$

Let us define what it means for a state to be initial or final.

Helpers

$$\frac{\Sigma_{\mathrm{R}}^{\alpha} = \langle p, 0, \sigma_{\mathcal{S}}, \mathbb{R}, \bot\rangle \qquad \sigma_{\mathcal{S}} \in \mathit{InitConf}}{\vdash \Sigma_{\mathrm{R}}^{\alpha} : \mathit{init}}\ \text{(R:Sym-Init)} \qquad \frac{\Sigma_{\mathrm{R}}^{\alpha} = \langle p, \mathit{ctr}, \sigma, \mathbb{R}, \bot\rangle \qquad \sigma_{\mathcal{S}}(\mathbf{pc}) = \bot}{\vdash \Sigma_{\mathrm{R}}^{\alpha} : \mathit{fin}}\ \text{(R:Sym-Fin)}$$

$$\frac{}{\Sigma_{\mathrm{R}}^{\alpha\,\mathit{init}}(p,\sigma) := \langle p, 0, \sigma_{\mathcal{S}}, \varepsilon, \bot\rangle}\ \text{(R:Sym-Initial-State)}$$

$p \times \mathit{InitConf}\ \text{👻}_{\mathrm{R}}^{\omega}\ \overline{\tau}$

$$\frac{\exists \Sigma'_{\mathrm{R}} \qquad \vdash \Sigma'_{\mathrm{R}} : \mathit{fin} \qquad \Sigma_{\mathrm{R}}^{\alpha\,\mathit{init}}(()p,\sigma)\ {}_{\alpha}\!\Downarrow_{\mathrm{R}}^{\overline{\tau}}\ \Sigma_{\mathrm{R}}^{\alpha\prime}}{(p,\sigma_{\mathcal{S}})\ {}_{\alpha}\!\text{👻}_{\mathrm{R}}^{\omega}\ \overline{\tau}}\ \text{(R:Sym-Trace)} \qquad \frac{}{\mathit{Beh}_{\mathrm{R}}^{\mathcal{S}}(p) = \{\overline{\tau} \mid \forall \sigma_{\mathcal{S}} \in \mathit{InitConf}.\ (p,\sigma_{\mathcal{S}})\ {}_{\alpha}\!\text{👻}_{\mathrm{R}}^{\omega}\ \overline{\tau}\}}\ \text{(R:Sym-Beh)}$$

E FRAMEWORK DEFINITION

We define a general framework on how to combine different semantics.

E.1 Union of States

The states Σ_{xy} are defined as the union of the state of its parts

$$\Sigma_{xy} ::= \Sigma_x \cup \Sigma_y$$
$$\Phi_{xy} ::= \Phi_x \cup \Phi_y$$

E.2 Unified Trace Model

Similar to the states Σ_{xy}, the observations are defined as the union of the trace models

$$Obs_{xy} ::= \ Obs_x \cup Obs_y$$

E.3 Join and Projection on instances / states

We define the a join operator $\sqcup_{xy}$ on instances:

$$\sqcup_{xy} \colon (\Phi_x, \Phi_y) \mapsto \Phi_{xy}$$

Note, that the join operations is only defined iff all the components c in $\Phi_x \cap \Phi_y$ are equal, i.e. $\forall c \in \Phi_x \cap \Phi_y.\ \Phi_x.c = \Phi_y.c$.

Furthermore, we define projection functions $\restriction_{xy}$ as the inverse of the join function:

$$\restriction_{xy} \colon \Phi_{xy} \mapsto (\Phi_x, \Phi_y)$$

We require that

$$\sqcup_{xy}(\Phi_{xy}\restriction_{xy}) = \Phi_{xy}$$
$$(\sqcup_{xy}(\Phi_x, \Phi_y))\restriction_{xy} = (\Phi_x, \Phi_y)$$

Next, we will define two more specific projection $\restriction^x_{xy}$ and $\restriction^y_{xy}$:

$$\restriction^x_{xy} \colon \Phi_{xy} \mapsto \Phi_x$$
$$\restriction^y_{xy} \colon \Phi_{xy} \mapsto \Phi_y$$

They are defined as the first and second projection of the generated pair from $\restriction_{xy}$.

E.4 AM Semantics

$$\boxed{\Sigma_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma'_{xy}}$$

$$\frac{\Phi_{xy} \overset{\tau}{\dashrightarrow}_{xy} \overline{\Phi}'_{xy}}{\overline{\Phi}_{xy} \cdot \Phi_{xy} \overset{\tau}{\dashrightarrow}_{xy} \overline{\Phi}_{xy} \cdot \overline{\Phi}'_{xy}}\ \text{(AM-Context-xy)}$$

$$\frac{\begin{array}{cc} n' = 0 \text{ or p is stuck} & \overline{\Phi}_{xy} \cdot \Phi_{xy} \cdot \Phi'_{xy}\restriction^x_{xy} \overset{\mathtt{rlb}_x\ ctr}{\dashrightarrow}_x \overline{\Phi}_{xy} \cdot \Phi''_{xy}\restriction^x_{xy} \\ \Phi''_{xy} = \Phi_{xy} & \Phi''_{xy}.ctr = \Phi'_{xy}.ctr \end{array}}{\overline{\Phi}_{xy} \cdot \Phi_{xy} \cdot \Phi'_{xy} \overset{\mathtt{rlb}_x\ ctr}{\dashrightarrow}_{xy} \overline{\Phi}_{xy} \cdot \Phi''_{xy}}\ \begin{array}{c}\text{(AM-x-Rollback-xy)}\\ \\ \end{array}$$

$$\frac{\begin{array}{cc} \Phi'_{xy}.n = 0 \text{ or p is stuck} & \overline{\Phi}_{xy} \cdot \Phi_{xy} \cdot \Phi'_{xy}\restriction^y_{xy} \overset{\mathtt{rlb}_y\ ctr}{\dashrightarrow}_y \overline{\Phi}_{xy} \cdot \Phi''_{xy}\restriction^y_{xy} \\ \Phi''_{xy} = \Phi_{xy} & \Phi''_{xy}.ctr = \Phi'_{xy}.ctr \end{array}}{\overline{\Phi}_{xy} \cdot \Phi_{xy} \cdot \Phi'_{xy} \overset{\mathtt{rlb}_y\ ctr}{\dashrightarrow}_{xy} \overline{\Phi}_{xy} \cdot \Phi''_{xy}}\ \begin{array}{c}\text{(AM-y-Rollback-xy)}\\ \\ \end{array}$$

$$\boxed{\Phi_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Phi'_{xy}}$$

$$\frac{\Phi_{xy}\restriction^x_{xy} \overset{\tau}{\dashrightarrow}^{Z_{xy}\restriction^x_{xy}}_x \overline{\Phi}'_{xy}\restriction^x_{xy}}{\Phi_{xy} \overset{\tau}{\dashrightarrow}_{xy} \overline{\Phi}'_{xy}}\ \text{(AM-x-step)} \qquad \frac{\Phi_{xy}\restriction^y_{xy} \overset{\tau}{\dashrightarrow}^{Z_{xy}\restriction^y_{xy}}_y \overline{\Phi}'_{xy}\restriction^y_{xy}}{\Phi_{xy} \overset{\tau}{\dashrightarrow}_{xy} \overline{\Phi}'_{xy}}\ \text{(AM-y-step)}$$

To simplify notation, we omit that the $\Phi_x \setminus \Phi_y$ parts of state Φ_{xy} in x-step (similar $\Phi_y \setminus \Phi_x$ in y-step) do not change between Φ_{xy} and $\overline{\Phi}'_{xy}$.

$\boxed{\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}}$

$$\frac{}{\Sigma_{xy} \Downarrow^{\varepsilon}_{xy} \Sigma_{xy}}\ \text{(AM-Reflection-xy)} \qquad \frac{\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma''_{xy} \quad \Sigma''_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma'_{xy}}{\Sigma_{xy} \Downarrow^{\overline{\tau}\cdot\tau}_{xy} \Sigma'_{xy}}\ \text{(AM-Single-xy)}$$

E.5 Symbolic Semantics

$\boxed{\Sigma^{\mathcal{S}}_{xy} \overset{\tau}{\dashrightarrow}^{\mathcal{S}}_{xy} \Sigma^{\mathcal{S}\prime}_{xy}}$

$$\frac{\Phi^{\mathcal{S}}_{xy} \overset{\tau_S}{\dashrightarrow}^{\mathcal{S}}_{xy} \overline{\Phi^{\mathcal{S}}_{xy}}'}{\overline{\Phi^{\mathcal{S}}_{xy}} \cdot \Phi^{\mathcal{S}}_{xy} \overset{\tau_S}{\dashrightarrow}^{\mathcal{S}}_{xy} \overline{\Phi^{\mathcal{S}}_{xy}} \cdot \overline{\Phi^{\mathcal{S}}_{xy}}'}\ \text{(Sym-Context-xy)}$$

$$\frac{n' = 0 \text{ or p is stuck} \quad \overline{\Phi^{\mathcal{S}}_{xy}} \cdot \Phi^{\mathcal{S}}_{xy} \cdot {\Phi^{\mathcal{S}}_{xy}}' \restriction^{x}_{xy} \overset{\mathtt{rlb}_x\ ctr}{\dashrightarrow}_{x_S} \overline{\Phi^{\mathcal{S}}_{xy}} \cdot {\Phi^{\mathcal{S}}_{xy}}^{\dagger} \restriction^{x}_{xy} \quad {\Phi^{\mathcal{S}}_{xy}}^{\dagger} = \Phi^{\mathcal{S}}_{xy} \quad {\Phi^{\mathcal{S}}_{xy}}^{\dagger}.ctr = {\Phi^{\mathcal{S}}_{xy}}'.ctr}{\overline{\Phi^{\mathcal{S}}_{xy}} \cdot \Phi^{\mathcal{S}}_{xy} \cdot {\Phi^{\mathcal{S}}_{xy}}' \overset{\mathtt{rlb}_x\ ctr}{\dashrightarrow}^{\mathcal{S}}_{xy} \overline{\Phi^{\mathcal{S}}_{xy}} \cdot {\Phi^{\mathcal{S}}_{xy}}^{\dagger}}\ \text{(Sym-x-Rollback-xy)}$$

$$\frac{\Phi'_{xy}.n = 0 \text{ or p is stuck} \quad \overline{\Phi^{\mathcal{S}}_{xy}} \cdot \Phi^{\mathcal{S}}_{xy} \cdot {\Phi^{\mathcal{S}}_{xy}}' \restriction^{y}_{xy} \overset{\mathtt{rlb}_y\ ctr}{\dashrightarrow}_{y_S} \overline{\Phi^{\mathcal{S}}_{xy}} \cdot {\Phi^{\mathcal{S}}_{xy}}^{\dagger} \restriction^{y}_{xy} \quad {\Phi^{\mathcal{S}}_{xy}}^{\dagger} = \Phi^{\mathcal{S}}_{xy} \quad {\Phi^{\mathcal{S}}_{xy}}^{\dagger}.ctr = {\Phi^{\mathcal{S}}_{xy}}'.ctr}{\overline{\Phi^{\mathcal{S}}_{xy}} \cdot \Phi^{\mathcal{S}}_{xy} \cdot {\Phi^{\mathcal{S}}_{xy}}' \overset{\mathtt{rlb}_y\ ctr}{\dashrightarrow}^{\mathcal{S}}_{xy} \overline{\Phi^{\mathcal{S}}_{xy}} \cdot {\Phi^{\mathcal{S}}_{xy}}^{\dagger}}\ \text{(Sym-y-Rollback-xy)}$$

$\boxed{\Phi^{\mathcal{S}}_{xy} \overset{\tau_S}{\dashrightarrow}^{\mathcal{S}}_{xy} {\Phi^{\mathcal{S}}_{xy}}'}$

$$\frac{\Phi^{\mathcal{S}}_{xy} \restriction^{x}_{xy} \overset{\tau_S}{\dashrightarrow}^{Z_{xy}\restriction^{x}_{xy}}_{x_S} \overline{\Phi^{\mathcal{S}}_{xy}}' \restriction^{x}_{xy}}{\Phi^{\mathcal{S}}_{xy} \overset{\tau_S}{\dashrightarrow}^{\mathcal{S}}_{xy} \overline{\Phi^{\mathcal{S}}_{xy}}'}\ \text{(Sym-x-step)} \qquad \frac{\Phi^{\mathcal{S}}_{xy} \restriction^{y}_{xy} \overset{\tau_S}{\dashrightarrow}^{Z_{xy}\restriction^{y}_{xy}}_{y_S} \overline{\Phi^{\mathcal{S}}_{xy}}' \restriction^{y}_{xy}}{\Phi^{\mathcal{S}}_{xy} \overset{\tau}{\dashrightarrow}^{\mathcal{S}}_{xy} \overline{\Phi^{\mathcal{S}}_{xy}}'}\ \text{(Sym-y-step)}$$

$\boxed{\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}}$

$$\frac{}{\Sigma^{\mathcal{S}}_{xy}\ {}_{\mathcal{S}}\Downarrow^{\varepsilon}_{xy}\ \Sigma^{\mathcal{S}}_{xy}}\ \text{(Sym-Reflection-xy)} \qquad \frac{\Sigma^{\mathcal{S}}_{xy}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau}}_{xy}\ \Sigma^{\mathcal{S}\prime}_{xy} \quad \Sigma^{\mathcal{S}\prime}_{xy} \overset{\tau_S}{\dashrightarrow}^{\mathcal{S}}_{xy} \Sigma^{\mathcal{S}'}_{xy}}{\Sigma^{\mathcal{S}}_{xy}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau}\cdot\tau_S}_{xy}\ \Sigma^{\mathcal{S}'}_{xy}}\ \text{(Sym-Single-xy)}$$

E.6 Oracle semantics

$\boxed{X_{xy} \overset{\tau}{\rightsquigarrow}^{O_{xy}}_{xy} X'_{xy}}$

$$\frac{\Psi_{xy} \overset{\tau}{\rightsquigarrow}^{O_{xy}}_{xy} \overline{\Psi}'_{xy} \quad \Psi_{xy} = \langle p, ctr, \sigma, \mathbb{R}, h, n+1\rangle \quad \text{if } p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \text{ then } \overline{\Psi}_{xy}'' = zeroes(\overline{\Psi}_{xy}) \text{ else } \overline{\Psi}_{xy}'' = decr(\overline{\Psi}_{xy})}{\overline{\Psi}_{xy} \cdot \Psi_{xy} \overset{\tau}{\rightsquigarrow}^{O_{xy}}_{xy} \overline{\Psi}_{xy}'' \cdot \overline{\Psi}'_{xy}}\ \text{(SE-Context)}$$

$$\frac{\overline{\Psi}_{xy} \cdot \Psi_{xy\overline{\rho}\cdot\tau} \restriction^{x}_{xy} \overset{\tau}{\rightsquigarrow}^{O_x}_{x} \overline{\Psi}_{xy} \cdot \Psi_{xy\overline{\rho}} \restriction^{x}_{xy}}{\overline{\Psi}_{xy} \cdot \Psi_{xy\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}^{O_{xy}}_{xy} \overline{\Psi}_{xy} \cdot \Psi_{xy\overline{\rho}}}\ \text{(SE-x-General)} \qquad \frac{\overline{\Psi}_{xy} \cdot \Psi_{xy\overline{\rho}\cdot\tau} \restriction^{y}_{xy} \overset{\tau}{\rightsquigarrow}^{O_y}_{y} \overline{\Psi}_{xy} \cdot \Psi_{xy\overline{\rho}} \restriction^{y}_{xy}}{\overline{\Psi}_{xy} \cdot \Psi_{xy\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}^{O_{xy}}_{xy} \overline{\Psi}_{xy} \cdot \Psi_{xy\overline{\rho}}}\ \text{(SE-y-General)}$$

$$\frac{\begin{array}{c}n' = 0 \text{ or } p \text{ is stuck} \quad \Psi_{xy} \cdot \Psi'_{xy} \cdot \overline{\Psi}'_{xy}\restriction^{x}_{xy} \overset{\tau}{\rightsquigarrow}_{x}^{O_x} \Psi''_{xy}\restriction^{x}_{xy} \quad \text{(SE-x-Rollback)}\\ \Psi''_{xy} = \Psi_{xy} \qquad \Psi''_{xy}.ctr = \Psi'_{xy}.ctr\end{array}}{\overline{\Psi}_{xy} \cdot \Psi_{xy} \cdot \Psi'_{xy} \cdot \overline{\Psi}'_{xy} \overset{\tau}{\rightsquigarrow}_{xy}^{O_{xy}} \overline{\Psi}_{xy} \cdot \Psi''_{xy}}$$

$$\frac{\begin{array}{c}n' = 0 \text{ or } p \text{ is stuck} \quad \Psi_{xy} \cdot \Psi'_{xy} \cdot \overline{\Psi}'_{xy}\restriction^{y}_{xy} \overset{\tau}{\rightsquigarrow}_{y}^{O_y} \Psi''_{xy}\restriction^{y}_{xy} \quad \text{(SE-y-Rollback)}\\ \Psi''_{xy} = \Psi_{xy} \qquad \Psi''_{xy}.ctr = \Psi'_{xy}.ctr\end{array}}{\overline{\Psi}_{xy} \cdot \Psi_{xy} \cdot \Psi'_{xy} \cdot \overline{\Psi}'_{xy} \overset{\tau}{\rightsquigarrow}_{xy}^{O_{xy}} \overline{\Psi}_{xy} \cdot \Psi''_{xy}}$$

$$\frac{\begin{array}{c}\Psi_{xy} \cdot \Psi'_{xy}\restriction^{x}_{xy} \overset{\tau}{\rightsquigarrow}_{x}^{O_x} \Psi'_{xy}\restriction^{x}_{xy} \quad \text{(SE-x-Commit)}\\ \Psi''_{xy} = \Psi'_{xy} \qquad \Psi''_{xy}.\boldsymbol{n} = \Psi_{xy}.\boldsymbol{n}\end{array}}{\overline{\Psi}_{xy} \cdot \Psi_{xy} \cdot \Psi'_{xy} \cdot \overline{\Psi}_{xy}\prime \overset{\tau}{\rightsquigarrow}_{xy}^{O_{xy}} \overline{\Psi}_{xy} \cdot \Psi''_{xy} \cdot \overline{\Psi}_{xy}\prime}$$

$$\frac{\begin{array}{c}\Psi_{xy} \cdot \Psi'_{xy}\restriction^{y}_{xy} \overset{\tau}{\rightsquigarrow}_{y}^{O_y} \Psi''_{xy}\restriction^{y}_{xy} \quad \text{(SE-y-Commit)}\\ \Psi''_{xy} = \Psi'_{xy} \qquad \Psi''_{xy}.\boldsymbol{n} = \Psi_{xy}.\boldsymbol{n}\end{array}}{\overline{\Psi}_{xy} \cdot \Psi_{xy} \cdot \Psi'_{xy} \cdot \overline{\Psi}_{xy}\prime \overset{\tau}{\rightsquigarrow}_{xy}^{O_{xy}} \overline{\Psi}_{xy} \cdot \Psi''_{xy} \cdot \overline{\Psi}_{xy}\prime}$$

$\boxed{\Psi_{xy} \overset{\tau}{\rightsquigarrow}_{xy}^{O_{xy}} \Psi'_{xy}}$

$$\frac{O_{xy} = (O_x, O_y) \quad \Psi_{xy}\restriction^{x}_{xy} \overset{\tau}{\rightsquigarrow}_{x}^{O_x} \overline{\Psi}'_{xy}\restriction^{x}_{xy}}{\Psi_{xy} \overset{\tau}{\rightsquigarrow}_{xy}^{O_{xy}} \overline{\Psi}'_{xy}} \text{(SE-x-step)} \qquad \frac{O_{xy} = (O_x, O_y) \quad \Psi_{xy}\restriction^{y}_{xy} \overset{\tau}{\rightsquigarrow}_{y}^{O_y} \overline{\Psi}'_{xy}\restriction^{y}_{xy}}{\Psi_{xy} \overset{\tau}{\rightsquigarrow}_{xy}^{O_{xy}} \overline{\Psi}'_{xy}} \text{(SE-y-step)}$$

$\boxed{X_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}}$

$$\frac{}{X_{xy} \overset{O_{xy}}{\Downarrow^{xy}_{\varepsilon}} X_{xy}} \text{(SE-Reflection-xy)} \qquad \frac{X_{xy} \overset{O_{xy}}{\Downarrow^{xy}_{\overline{\tau}}} X''_{xy} \qquad X''_{xy} \overset{\tau_S}{\rightsquigarrow}_{xy}^{O_{xy}} X'_{xy}}{X_{xy} \overset{O_{xy}}{\Downarrow^{xy}_{\overline{\tau}\cdot\tau_S}} X'_{xy}} \text{(SE-Single-xy)}$$

Let us define what it means for a state to be initial or final.

$\boxed{Helpers}$

$$\frac{X_{xy} = \Psi_{xy} \quad \Psi_{xy}\restriction_{xy} = (\Psi_x, \Psi_y) \quad \vdash \Psi_x : init \quad \vdash \Psi_y : init}{\vdash X_{xy} : init} \text{(Comb-SE:Init)} \qquad \frac{X_{xy} = \Psi_{xy} \quad \Psi_{xy}\restriction_{xy} = (\Psi_x, \Psi_y) \quad \vdash \Psi_x : fin \quad \vdash \Psi_y : fin}{\vdash X_{xy} : fin} \text{(Comb-SE:Fin)}$$

$$\frac{}{X^{init}_{xy}(p, \sigma) := \sqcup_{xy}(X^{init}_{x}(p, \sigma), X^{init}_{y}(p, \sigma))} \text{(Comb-SE-Initial-State)}$$

E.7 Main definitions from the paper

Here we restate the main definitions of the paper in their full form.

Definition 12 (Secure Speculative Semantics). *A semantics $\mathcal{A}_x$ is secure (denoted $\vdash \mathcal{A}_x$ SSS) if:*

- *Oracle Overapproximation: $\forall O.\ p \vdash^{O}_{x}$ SNI iff $p \vdash_x$ SNI*
- *Symbolic Consistency: $Beh^{\mathcal{A}}_{x}(p) = \mu(Beh^{\mathcal{S}}_{x}(p))$*
- *NS Consistency: $Beh^{\mathcal{A}}_{x}(p)\restriction_{ns} = Beh_{NS}(p) = Beh^{O}_{x}(p)\restriction_{ns}$*

Definition 13 (Well-formed composition). *A composition $\mathcal{A}_{xy}$ of two speculative semantics $\mathcal{A}_x$ and $\mathcal{A}_y$ is well-formed, denoted with $\vdash \mathcal{A}_{xy}$: WFC if:*

(1) (Confluence) Whenever $\Sigma_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma'_{xy}$ and $\Sigma_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma''_{xy}$, then $\Sigma'_{xy} = \Sigma''_{xy}$.

(2) (Projection preservation) For all programs p, $Beh^{\mathcal{A}}_{x}(p) = Beh^{\mathcal{A}}_{xy}(p)\restriction^{x}_{xy}$ and $Beh^{\mathcal{A}}_{y}(p) = Beh^{\mathcal{A}}_{xy}(p)\restriction^{y}_{xy}$.

(3) *(Relation preservation) If* $\Sigma_{xy} \approx_{xy} X_{xy}$ *and* $\Sigma_{xy} \overset{\overline{\tau}}{=\!=\!\!\Rightarrow}{}^{*}_{xy} \Sigma'_{xy}$ *then* $X_{xy} \overset{\overline{\tau}'}{\rightsquigarrow}{}^{O_{xy}*}_{xy} X'_{xy}$ *and* $\Sigma'_{xy} \approx_{xy} X'_{xy}$.[6]

(4) *(Symbolic Preservation) If* $\Sigma^{\mathcal{S}}_{xy} \overset{\tau_{\mathcal{S}}}{=\!=\!\!\Rightarrow}{}^{\mathcal{S}}_{xy} \Sigma^{\mathcal{S}'}_{xy}$ *and* $\mu(\Sigma^{\mathcal{S}}_{xy}) = \Sigma_{xy}$ *and* $\mu \vDash pthCnd(\tau_{\mathcal{S}})$ *Then there exists* Σ'_{xy} *such that* $\Sigma_{xy} \overset{\mu(\tau)}{=\!=\!\!\Rightarrow}{}_{xy} \Sigma'_{xy}$ *and* $\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$. *Furthermore, if* $\Sigma_{xy} \overset{\tau}{=\!=\!\!\Rightarrow}{}_{xy} \Sigma'_{xy}$ *and* $\mu(\Sigma^{\mathcal{S}}_{xy}) = \Sigma_{xy}$ *then* $\Sigma^{\mathcal{S}}_{xy} \overset{\tau'}{=\!=\!\!\Rightarrow}{}^{\mathcal{S}}_{xy} \Sigma^{\mathcal{S}'}_{xy}$, $\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$, $\mu \vDash pthCnd(\tau')$ *and* $\mu(\tau') = \tau$

E.8 Main result

Here is the main result of the paper again.

Theorem 10 ($\mathcal{N}_{xy}$ is *SSS*). *if* $\vdash \mathcal{N}_x$ *SSS and* $\vdash \mathcal{N}_y$ *SSS and* $\vdash \mathcal{N}_{xy} : WFC$ *then* $\vdash \mathcal{N}_{xy}$ *SSS.*

Proof. Immediate from Theorem 12 (NS Consistency) and Theorem 11 (Symbolic Consistency).
Note that the last of *SSS* is missing (overapproximation of oracle). Since this is technical, we delay the presentation and refer the reader to each of the combinations and to the end □

We want to note that if one is not interested in for example the oracle semantics, one could drop the (3) from the well-formedness condition and Oracle Overapproximation from SSS and one could still prove the main result for this weaker definition of SSS. It depends on what the user needs.
Now here is one of the main results for the general case that follows from just well-formedness:

Corollary 1 (SNI of combined preserves SNI of parts)**.** *Let* $\vdash \mathcal{N}_{xy} : WFC$ *and let* p *be a program and* ω *be a speculation window. If* $p \vdash_{xy} SNI$ *then* $p \vdash_x SNI$ *and* $p \vdash_y SNI$.

Proof. Assume $p \vdash_{xy}$ SNI and that there are $\sigma, \sigma' \in InitConf$ with $\sigma \sim_P \sigma'$ for some policy P and (p, σ) $\mathcal{N}^{O}_{NS}$ $\overline{\tau}'$, (p, σ') $\mathcal{N}^{O}_{NS}$ $\overline{\tau}'$.
We need to show that

(1) (p, σ) $\mathcal{N}^{\omega}_{x}$ $\overline{\tau}_x$, (p, σ') $\mathcal{N}^{\omega}_{x}$ $\overline{\tau}_x$
(2) (p, σ) $\mathcal{N}^{\omega}_{y}$ $\overline{\tau}_y$, (p, σ') $\mathcal{N}^{\omega}_{y}$ $\overline{\tau}_y$

We show the proof for 1) via the projection to x. The proof for 2) is analogous using the projection to y. Both of these projections we get from $\vdash \mathcal{N}_{xy} : WFC$
Unfolding the definition of $p \vdash_{xy}$ SNI we get:

(1) if $\sigma \sim_P \sigma'$ and (p, σ) $\mathcal{N}^{O}_{NS}$ $\overline{\tau}$, (p, σ') $\mathcal{N}^{O}_{NS}$ $\overline{\tau}$, then (p, σ) $\mathcal{N}^{\omega}_{xy}$ $\overline{\tau}_{xy}$, (p, σ') $\mathcal{N}^{\omega}_{xy}$ $\overline{\tau}_{xy}$

After initialization we have (p, σ) $\mathcal{N}^{\omega}_{xy}$ $\overline{\tau}_{xy}$, (p, σ') $\mathcal{N}^{\omega}_{xy}$ $\overline{\tau}_{xy}$.
By the projection to x assumption we have (p, σ) $\mathcal{N}^{\omega}_{x}$ $\overline{\tau}_{xy}\restriction^{x}_{xy} \in Beh^{\mathcal{A}}_{x}(p)$ and (p, σ') $\mathcal{N}^{\omega}_{x}$ $\overline{\tau}_{xy}\restriction^{x}_{xy} \in Beh^{\mathcal{A}}_{x}(p)$, which is what we needed to show.

□

We leave the proof for Oracle overapproximation to the end of the TR because we need to introduce a few more concepts.

E.9 Proofs: Combination of Proper Composition to Symbolic

Theorem 11 (Symbolic Consistency). *If* $\vdash \mathcal{N}_{xy} : WFC$, *then* $\forall p.\ Beh^{\mathcal{A}}_{xy}p = \mu(Beh^{\mathcal{S}}_{xy}(p))$.

Proof. We prove the two directions separately:

⇐ Assume that $(p, \sigma_{\mathcal{S}})$ $\mathcal{N}^{\mathcal{S}}_{xy}$ $\overline{\tau} \in Beh^{\mathcal{S}}_{xy}(p)$. We thus know there exists $\vdash \Sigma^{\mathcal{S}'}_{xy} : fin$ such that $\Sigma^{init}_{xy}((p, \sigma_{\mathcal{S}}))\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau}}_{xy} \Sigma^{\mathcal{S}'}_{xy}$ and $\mu \vDash pthCnd(\overline{\tau_\alpha})$.
We now apply Lemma 1 (Soundness Symbolic Combination) on $\Sigma^{init}_{xy}((p, \sigma_{\mathcal{S}}))\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau}}_{xy} \Sigma^{\mathcal{S}'}_{xy}$ and get $\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}$, $\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$ and $\mu(\overline{\tau_\alpha}) = \overline{\tau}$
Since $\vdash \Sigma^{\mathcal{S}'}_{xy} : fin$ and $\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$ we have $\vdash \Sigma'_{xy} : fin$ as well.
Thus, $(p, \mu(\sigma_{\mathcal{S}}))$ $\mathcal{N}^{\omega}_{xy}$ $\mu(\overline{\tau_\alpha}) \in Beh^{\mathcal{A}}_{xy}p$.

⇒ Assume that (p, σ) $\mathcal{N}^{\omega}_{xy}$ $\overline{\tau} \in Beh^{\mathcal{A}}_{xy}p$. We thus know there exists $\vdash \Sigma'_{xy} : fin$ such that $\Sigma^{init}_{xy}((p, \sigma)) \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}$.

[6] We note that there is a very technical addition to Relatin Preservation that is needed in the proofs. We defer to that addition in Appendix N.7. It essentially characterizes the lockstep behaviour between AM and Oracle steps. For example, when no specualtin is happening and we have the same state, we expect the oracle and the AM semantics to do the same step and end up in the same state emitting the same trace.

We now apply Lemma 2 (Completeness Symbolic Combination) on $\Sigma^{init}_{xy}((p,\sigma)) \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}$ and get

$$\begin{aligned} \Sigma^{init}_{xy}((p,\sigma)) =& \mu(\Sigma^{\mathcal{S}}_{xy}) \\ \Sigma^{\mathcal{S}}_{xy}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau}'}_{xy}\ \Sigma^{\mathcal{S}'}_{xy} & \\ \Sigma'_{xy} =& \mu(\Sigma^{\mathcal{S}'}_{xy}) \\ \overline{\tau} =& \mu(\overline{\tau}') \\ \mu \ \vDash & \ pthCnd(\overline{\tau}') \end{aligned}$$

Since $\vdash \Sigma'_{xy} : fin$ and $\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$ we have $\vdash \Sigma^{\mathcal{S}'}_{xy} : fin$ as well.
Thus, $(p, \sigma_{\mathcal{S}})$ $\text{Ω}^{\mathcal{S}}_{xy}$ $\overline{\tau_\alpha} \in Beh^{\mathcal{S}}_{xy}(p)$ and we are done, since $(p, \mu(\sigma_{\mathcal{S}}))$ $\text{Ω}^{\mathcal{S}}_{xy}$ $\mu(\overline{\tau_\alpha}) = (p, \sigma)$ Ω^{ω}_{xy} $\overline{\tau}$.

□

Lemma 1 (Soundness Symbolic Combination)**.** *If*

(1) $\Sigma^{\mathcal{S}}_{xy}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau_\alpha}}_{xy}\ \Sigma^{\mathcal{S}'}_{xy}$ *and*
(2) $\mu(\Sigma^{\mathcal{S}}_{xy}) = \Sigma_{xy}$
(3) $\mu \ \vDash pthCnd(\overline{\tau_\alpha})$
(4) $\vdash \text{Ω}_{xy} : WFC$

Then

I $\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}$ *and*
II $\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$ *and* $\mu(\overline{\tau_\alpha}) = \overline{\tau}$

Proof. We proceed by induction on $\Sigma^{\mathcal{S}}_{xy}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau_\alpha}}_{xy}\ \Sigma^{\mathcal{S}'}_{xy}$

Rule Sym-Reflection-xy Then we have $\Sigma^{\mathcal{S}}_{xy}\ {}_{\mathcal{S}}\Downarrow^{\varepsilon}_{xy}\ \Sigma^{\mathcal{S}'}_{xy}$ with $\Sigma^{\mathcal{S}'}_{xy} = \Sigma^{\mathcal{S}}_{xy}$ and by Rule AM-Reflection-xy we have:
I $\Sigma_{xy} \Downarrow_{\varepsilon} \Sigma'_{xy}$ with $\Sigma'_{xy} = \Sigma_{xy}$.
It is trivially to see that we fulfill all conditions.

Rule Sym-Single-xy We have $\Sigma^{\mathcal{S}}_{xy}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau_\alpha}'\cdot\tau_{\mathcal{S}}}_{xy}\ \Sigma^{\mathcal{S}'}_{xy}$ and by Rule Sym-Single-xy we get $\Sigma^{\mathcal{S}}_{xy}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau_\alpha}'}_{xy}\ \Sigma^{\mathcal{S}''}_{xy}$ and $\Sigma^{\mathcal{S}''}_{xy} \overset{\tau_{\mathcal{S}}}{\dashrightarrow} \text{Ω}^{\mathcal{S}}_{xy}\ \Sigma^{\mathcal{S}'}_{xy}$.
We need to prove
I $\Sigma_{xy} \Downarrow^{\overline{\tau}\cdot\tau}_{xy} \Sigma'_{xy}$ and
II $\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$ and $\mu(\overline{\tau_\alpha}\cdot\tau_{\mathcal{S}}) = \overline{\tau}\cdot\tau$ and
We apply the IH on $\Sigma^{\mathcal{S}}_{xy}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau_\alpha}'}_{xy}\ \Sigma^{\mathcal{S}''}_{xy}$ and have a Σ''_{xy} such that:
(1) $\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma''_{xy}$ and
(2) $\mu(\Sigma^{\mathcal{S}''}_{xy}) = \Sigma''_{xy}$ and $\mu(\overline{\tau_\alpha}) = \overline{\tau}$ and
We use Symbolic Preservation (In lemma form here: Lemma 5 (Comb: Soundness single step symbolic)) from $\vdash \text{Ω}_{xy} : WFC$ on $\Sigma^{\mathcal{S}''}_{xy} \overset{\tau_{\mathcal{S}}}{\dashrightarrow} \text{Ω}^{\mathcal{S}}_{xy}\ \Sigma^{\mathcal{S}'}_{xy}$ and get $\Sigma''_{xy} \overset{\tau}{\dashrightarrow} \text{Ω}_{xy}\ \Sigma'_{xy}$ and $\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$ and $\mu(\tau_{\mathcal{S}}) = \tau$.
We now use Rule AM-Single-xy on $\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma''_{xy}$ and $\Sigma''_{xy} \overset{\tau}{\dashrightarrow} \text{Ω}_{xy}\ \Sigma'_{xy}$ and get the desired result.

□

Lemma 2 (Completeness Symbolic Combination)**.** *If*

(1) $\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}$ *and*
(2) $\vdash \text{Ω}_{xy} : WFC$

Then there is a valuation $\mu()$*, a symbolic trace* $\overline{\tau}'$ *and a final state* $\Sigma^{\mathcal{S}'}_{xy}$ *such that*

I $\Sigma_{xy} = \mu(\Sigma^{\mathcal{S}}_{xy})$ *and*
II $\Sigma^{\mathcal{S}}_{xy}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau_\alpha}}_{xy}\ \Sigma^{\mathcal{S}'}_{xy}$ *and*
III $\Sigma'_{xy} = \mu(\Sigma^{\mathcal{S}'}_{xy})$ *and* $\overline{\tau} = \mu(\overline{\tau_\alpha})$ *and*
IV $\mu \ \vDash pthCnd(\overline{\tau_\alpha})$

Proof. We proceed by induction on $\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}$

Rule AM-Reflection-xy Then we have $\Sigma_{xy} \Downarrow^{\varepsilon}_{xy} \Sigma'_{xy}$ with $\Sigma'_{xy} = \Sigma'_{xy}$.
I - IV By Rule Sym-Reflection-xy we have $\Sigma^{\mathcal{S}}_{xy}\ {}_{\mathcal{S}}\Downarrow^{\varepsilon}_{xy}\ \Sigma_{xy}$. By construction we are finished.

Rule AM-Single-xy We have $\Sigma_{xy} \Downarrow_{xy}^{\overline{\tau}' \cdot \tau} \Sigma'_{xy}$ and by Rule AM-Single-xy we get $\Sigma_{xy} \Downarrow_{xy}^{\overline{\tau_\alpha}'} \Sigma''_{xy}$ and $\Sigma''_{xy} \overset{\tau}{\dashrightarrow}_{xy}^{\mathcal{S}} \Sigma'_{xy}$.

We need to prove

I $\Sigma_{xy} = \mu(\Sigma_{xy}^{\mathcal{S}})$ and

II $\Sigma_{xy}^{\mathcal{S}}{}_{\mathcal{S}} \Downarrow_{xy}^{\overline{\tau_\alpha}' \cdot \tau_S} \Sigma_{xy}^{\mathcal{S}'}$ and

III $\Sigma'_{xy} = \mu(\Sigma_{xy}^{\mathcal{S}'})$ and $\overline{\tau}' \cdot \tau = \mu(\overline{\tau_\alpha}' \cdot \tau_{\mathcal{S}})$ and

IV $\mu \vDash pthCnd(\overline{\tau_\alpha}' \cdot \tau_{\mathcal{S}})$

We apply the IH on $\Sigma_{xy} \Downarrow_{xy}^{\overline{\tau_\alpha}'} \Sigma''_{xy}$ and have a $\Sigma_{xy}^{\mathcal{S}''}$ such that:

(1) $\Sigma_{xy} = \mu(\Sigma_{xy}^{\mathcal{S}})$ and

(2) $\Sigma_{xy}^{\mathcal{S}}{}_{\mathcal{S}} \Downarrow_{xy}^{\overline{\tau_\alpha}'} \Sigma_{xy}^{\mathcal{S}''}$ and

(3) $\Sigma''_{xy} = \mu(\Sigma_{xy}^{\mathcal{S}''})$ and $\overline{\tau}' = \mu(\overline{\tau_\alpha}')$ and

(4) $\mu \vDash pthCnd(\overline{\tau_\alpha}')$

We use Symbolic Preservation (In lemma form here: Lemma 6 (Comb: Completeness single step)) from $\vdash \mathcal{A}_{xy} : WFC$ on $\Sigma''_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma'_{xy}$ and get $\Sigma_{xy}^{\mathcal{S}''} \overset{\tau_S}{\dashrightarrow}_{xy}^{\mathcal{S}} \Sigma_{xy}^{\mathcal{S}'}$ and $\mu(\Sigma_{xy}^{\mathcal{S}'}) = \Sigma'_{xy}$ and $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu \vDash pthCnd(\tau_{\mathcal{S}})$.
By definition, we have $\mu \vDash pthCnd(\overline{\tau_\alpha}')$ since $\mu \vDash pthCnd(\tau'_{\mathcal{S}})$ and $\mu \vDash pthCnd(\overline{\tau_\alpha}')$.

We now use Rule Sym-Single-xy on $\Sigma_{xy}^{\mathcal{S}}{}_{\mathcal{S}} \Downarrow_{xy}^{\overline{\tau_\alpha}'} \Sigma_{xy}^{\mathcal{S}''}$ and $\Sigma_{xy}^{\mathcal{S}''} \overset{\tau_S}{\dashrightarrow}_{xy}^{\mathcal{S}} \Sigma_{xy}^{\mathcal{S}'}$ and get the desired result.

□

E.10 Proving Symbolic Preservation for a combination

> Furthermore, it is trivial to derive the 4th condition of WFC if you know it holds for both source semantics. We can then do a general proof using these assumptions (Lemma 3 and Lemma 4 below) to prove the Symbolic Preservation of the combination. We note that the assumptions used here were also used to derive Symbolic Consistency for SSS for the source semantics V4, V5 and even V1 (see Lemma 9 in Spectector). These assumptions relate single steps of the AM-semantics with single steps in the symbolic semantics. Thus, if you have proven SSS for a new semantics then you most likely have proven these single step assumptions as well and can use the general lemma below to derive Symbolic Consistency of a new combination automatically.

Assume these two Assumptions are available in all the following proofs of the subsection (and for y as well).

Lemma 3 (Assumption 1)**.** *If*

(1) $\Sigma_x \overset{\tau}{\dashrightarrow}_x \Sigma'_x$ *and*
(2) $\mu(\Sigma_{x_\alpha}) = \Sigma_x$ *and*
(3) $\mu \vDash pthCnd(\tau_{\mathcal{S}})$

Then

(1) $\Sigma_{x_\alpha} \overset{\tau_S}{\dashrightarrow}_{x_S} \Sigma'_{x_\alpha}$ *and*
(2) $\mu(\Sigma'_{x_\alpha}) = \Sigma'_x$ *and*
(3) $\mu(\tau_{\mathcal{S}}) = \tau$

Lemma 4 (Assumption 2)**.** *If*

(1) $\Sigma_{x_\alpha} \overset{\tau_S}{\dashrightarrow}_{x_S} \Sigma'_{x_\alpha}$ *and*
(2) $\mu(\Sigma_{x_\alpha}) = \Sigma_x$

Then

(1) $\Sigma_x \overset{\tau}{\dashrightarrow}_x \Sigma'_x$ *and*
(2) $\mu(\Sigma'_{x_\alpha}) = \Sigma'_x$ *and*
(3) $\mu(\tau_{\mathcal{S}}) = \tau$ *and*
(4) $\mu \vDash pthCnd(\tau_{\mathcal{S}})$

Lemma 5 (Comb: Soundness single step symbolic)**.** *If*

(1) $\Sigma_{xy}^{\mathcal{S}} \overset{\tau_S}{\dashrightarrow}_{xy}^{\mathcal{S}} \Sigma_{xy}^{\mathcal{S}'}$ *and*
(2) $\mu(\Sigma_{xy}^{\mathcal{S}}) = \Sigma_{xy}$
(3) $\mu \vDash pthCnd(\tau_{\mathcal{S}})$

Then there exists Σ'_{xy} *such that*

I $\Sigma_{xy} \overset{\tau}{\Longrightarrow}_{xy} \Sigma'_{xy}$ *and*
II $\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$ *and*
III $\mu(\tau_{\mathcal{S}}) = \tau$

Proof. We proceed by inversion on $\Sigma^{\mathcal{S}}_{xy} \overset{\tau_{\mathcal{S}}}{\Longrightarrow}_{xy} \Sigma^{\mathcal{S}'}_{xy}$:

Rule Sym-x-Rollback-xy Since $\mu()$ does not change the speculation window and *ctr* and $\mu(\Sigma^{\mathcal{S}}_{xy}) = \Sigma_{xy}$, we have $\Sigma_{xy}.n = \Sigma^{\mathcal{S}}_{xy}.n = 0$ and $\Sigma_{xy}.ctr = \Sigma^{\mathcal{S}}_{xy}.ctr$.

$\Sigma_{xy} \overset{\tau'}{\Longrightarrow}_{xy} \Sigma'_{xy}$ We can use the same rule Rule AM-x-Rollback-xy in the semantics to derive $\Sigma^{\mathcal{S}}_{xy} \overset{\tau'}{\Longrightarrow}_{x_{\mathcal{S}}} \Sigma^{\mathcal{S}'}_{xy}$.

$\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$ **and** $\mu(\tau_{\mathcal{S}}) = \tau$ The rule only deletes the topmost instance and changes the *ctr* of the instance below. Since $\Sigma_{xy}.ctr = \Sigma^{\mathcal{S}}_{xy}.ctr$, we have $\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$ and $\mu(\tau_{\mathcal{S}}) = \tau$.

Rule Sym-y-Rollback-xy Analogous to case Rule Sym-x-Rollback-xy.

Rule Sym-Context-xy We then have $\Phi^{\mathcal{S}}_{xy} \overset{\tau_{\mathcal{S}}}{\Longrightarrow}_{xy} \overline{\Phi^{\mathcal{S}}_{xy}}'$. We proceed by inversion on $\Phi^{\mathcal{S}}_{xy} \overset{\tau_{\mathcal{S}}}{\Longrightarrow}_{xy} \overline{\Phi^{\mathcal{S}}_{xy}}'$:

Rule Sym-x-step Then we have $\Phi^{\mathcal{S}}_{xy}\restriction^x_{xy} \overset{\tau_{\mathcal{S}}}{\Longrightarrow}^{Z_{xy}\restriction^x_{xy}}_{x_{\mathcal{S}}} \overline{\Phi^{\mathcal{S}}_{xy}}'\restriction^x_{xy}$. Note that $\mu(\Phi^{\mathcal{S}}_{xy}\restriction^x_{xy}) = \Phi_{xy}\restriction^x_{xy}$ because of $\mu(\Sigma^{\mathcal{S}}_{xy}) = \Sigma_{xy}$.
Furthermore, we have $\Phi^{\mathcal{S}}_{xy}.\sigma_{\mathcal{S}}(\mathbf{pc}) = \Phi_{xy}.\sigma(\mathbf{pc})$ since the **pc** is concrete. That means the same instruction is executed.
Now we use Lemma 3 (Assumption 1) and get $\Phi_{xy}\restriction^x_{xy} \overset{\tau}{\Longrightarrow}_x \overline{\Phi}'_{xy}\restriction^x_{xy}$ with $\mu(\overline{\Phi^{\mathcal{S}}_{xy}}'\restriction^x_{xy}) = \overline{\Phi}'_{xy}\restriction^x_{xy}$ and $\mu(\tau_{\mathcal{S}}) = \tau$.
From $\mu(\overline{\Phi^{\mathcal{S}}_{xy}}'\restriction^x_{xy}) = \overline{\Phi}'_{xy}\restriction^x_{xy}$ and $\mu(\Sigma^{\mathcal{S}}_{xy}) = \Sigma_{xy}$ we get $\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$.
Next, we use Rule AM-x-step (up to Confluence) using $\Phi_{xy}\restriction^x_{xy} \overset{\tau}{\Longrightarrow}_x \overline{\Phi}'_{xy}\restriction^x_{xy}$ and get $\Phi_{xy} \overset{\tau}{\Longrightarrow}_{xy} \overline{\Phi}'_{xy}$ and are finsihed.

Rule Sym-y-step Then we have $\Phi^{\mathcal{S}}_{xy}\restriction^y_{xy} \overset{\tau_{\mathcal{S}}}{\Longrightarrow}^{Z_{xy}\restriction^y_{xy}}_{y_{\mathcal{S}}} \overline{\Phi^{\mathcal{S}}_{xy}}'\restriction^y_{xy}$. Note that $\mu(\Phi^{\mathcal{S}}_{xy}\restriction^y_{xy}) = \Phi_{xy}\restriction^y_{xy}$ because of $\mu(\Sigma^{\mathcal{S}}_{xy}) = \Sigma_{xy}$.
The proof is analogous to the case above using Lemma 3 (Assumption 1).

□

Lemma 6 (Comb: Completeness single step)**.** *If*

(1) $\Sigma_{xy} \overset{\tau}{\Longrightarrow}_{xy} \Sigma'_{xy}$ *and*
(2) $\mu(\Sigma^{\mathcal{S}}_{xy}) = \Sigma_{xy}$

Then

I $\Sigma^{\mathcal{S}}_{xy} \overset{\tau'}{\Longrightarrow}^{\mathcal{S}}_{xy} \Sigma^{\mathcal{S}'}_{xy}$ *and*
II $\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$ *and*
III $\mu \vDash pthCnd(\tau')$ *and* $\mu(\tau') = \tau$

Proof. We proceed by inversion on $\Sigma_{xy} \overset{\tau}{\Longrightarrow}_{xy} \Sigma'_{xy}$:

Rule AM-x-Rollback-xy Since $\mu()$ does not change the speculation window and *ctr* and $\mu(\Sigma^{\mathcal{S}}_{xy}) = \Sigma_{xy}$, we have $\Sigma_{xy}.n = \Sigma^{\mathcal{S}}_{xy}.n = 0$ and $\Sigma_{xy}.ctr = \Sigma^{\mathcal{S}}_{xy}.ctr$.

$\Sigma^{\mathcal{S}}_{xy} \overset{\tau'}{\Longrightarrow}^{\mathcal{S}}_{xy} \Sigma^{\mathcal{S}'}_{xy}$ We can use the same rule in the symbolic semantics to derive $\Sigma^{\mathcal{S}}_{xy} \overset{\tau'}{\Longrightarrow}_{x_{\mathcal{S}}} \Sigma^{\mathcal{S}'}_{xy}$.

$\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$ The rule only deletes the topmost instance and changes the *ctr* of the instance below. Since $\Sigma_{xy}.ctr = \Sigma^{\mathcal{S}}_{xy}.ctr$, we have $\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$

$\mu \vDash pthCnd(\tau')$ **and** $\mu(\tau') = \tau$ Since the $\Sigma_{xy}.ctr = \Sigma^{\mathcal{S}}_{xy}.ctr$ we already have $\mu(\tau') = \tau$, since $\tau = \texttt{rlb}_x\ ctr$.
Furthermore since $\tau_{\mathcal{S}} = \texttt{rlb}_x\ ctr$, we have $\mu \vDash pthCnd(\tau') = \top$ by definition.

Rule AM-y-Rollback-xy Analogous to case Rule AM-x-Rollback-xy.

Rule AM-Context-xy We then have $\Phi_{xy} \overset{\tau}{\Longrightarrow}_{xy} \overline{\Phi}'_{xy}$. We proceed by inversion on $\Phi_{xy} \overset{\tau}{\Longrightarrow}_{xy} \overline{\Phi}'_{xy}$:

Rule AM-x-step Then we have $\Phi_{xy}\restriction^x_{xy} \overset{\tau}{\Longrightarrow}^{Z_{xy}\restriction^x_{xy}}_{x} \overline{\Phi}'_{xy}\restriction^x_{xy}$. Note that $\mu(\Phi^{\mathcal{S}}_{xy}\restriction^x_{xy}) = \Phi_{xy}\restriction^x_{xy}$ because of $\mu(\Sigma^{\mathcal{S}}_{xy}) = \Sigma_{xy}$.
Furthermore, we have $\Phi^{\mathcal{S}}_{xy}.\sigma_{\mathcal{S}}(\mathbf{pc}) = \Phi_{xy}.\sigma(\mathbf{pc})$ since the **pc** is concrete. That means the same instruction is executed.
Now we use Lemma 4 (Assumption 2) and get $\Phi^{\mathcal{S}}_{xy}\restriction^x_{xy} \overset{\tau_{\mathcal{S}}}{\Longrightarrow}_{x_{\mathcal{S}}} \overline{\Phi^{\mathcal{S}}_{xy}}'\restriction^x_{xy}$ with $\mu(\overline{\Phi^{\mathcal{S}}_{xy}}'\restriction^x_{xy}) = \overline{\Phi}'_{xy}\restriction^x_{xy}$ and $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu \vDash pthCnd(\tau_{\mathcal{S}})$.
From $\mu(\overline{\Phi^{\mathcal{S}}_{xy}}'\restriction^x_{xy}) = \overline{\Phi}'_{xy}\restriction^x_{xy}$ and $\mu(\Sigma^{\mathcal{S}}_{xy}) = \Sigma_{xy}$ we get $\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$.

Next, we use Rule Sym-x-step (up to Confluence) using $\Phi^{\mathcal{S}}_{xy}\restriction^{x}_{xy} \overset{\tau}{\dashrightarrow}_{\mathcal{S}_{xS}} \overline{\Phi^{\mathcal{S}}_{xy}}' \restriction^{x}_{xy}$ and get $\Phi^{\mathcal{S}}_{xy} \overset{\tau_S}{\dashrightarrow}^{\mathcal{S}}_{xy} \overline{\Phi^{\mathcal{S}}_{xy}}'$ and are finished.

Rule AM-y-step Analogous to the case above using Lemma 4 (Assumption 2) for the y-step.

□

E.11 NS Consistency for the general combination

We now prove one of the preconditions of $\vdash \mathcal{A}_{xy}$ *SSS* for the general combination.

Theorem 12 (NS Consistency). *If*

(1) $\vdash \mathcal{A}_{xy}$: *WFC and*

(2) $Beh_{NS}(p) = Beh^{\mathcal{A}}_{x}(p)\restriction_{ns}$, *and*

(3) $Beh_{NS}(p) = Beh^{\mathcal{A}}_{y}(p)\restriction_{ns}$

Then

I $Beh_{NS}(p) = Beh^{\mathcal{A}}_{xy}p\restriction_{ns}$.

Proof. By definition we get $\overline{\tau}\restriction_{ns} = \overline{\tau}\restriction^{y}_{xy}\restriction^{x}_{xy}$ (also commutative).

From $\vdash \mathcal{A}_{xy}$: *WFC*, we have that $Beh^{\mathcal{A}}_{xy}p\restriction^{y}_{xy} = Beh^{\mathcal{A}}_{y}(p)$.

Again by definition, we get $Beh^{\mathcal{A}}_{y}(p)\restriction^{x}_{xy} = Beh^{\mathcal{A}}_{y}(p)\restriction_{ns}$ ($Beh^{\mathcal{A}}_{y}(p)$ only has transactions of type y).

By assumption, we know that $Beh^{\mathcal{A}}_{y}(p)\restriction_{ns} = Beh_{NS}(p)$.

Combining these facts we get:

$$\begin{aligned} & Beh^{\mathcal{A}}_{xy}p\restriction_{ns} \\ &= Beh^{\mathcal{A}}_{xy}p\restriction^{y}_{xy}\restriction^{x}_{xy} \\ &= Beh^{\mathcal{A}}_{y}(p)\restriction^{x}_{xy} \\ &= Beh^{\mathcal{A}}_{y}(p)\restriction_{ns} \\ &= Beh_{NS}(p) \end{aligned}$$

and are finished. □

E.12 Why the behaviour of the source semantics is not strong enough

Here we give some intuition why we need 3) and 4) of the WFC of the combination. For example, one could think that we could rely on Symbolic Consistency of the source: $Beh^{\mathcal{A}}_{x}(p) = \mu(Beh^{\mathcal{S}}_{x}(p))$ and Oracle over approximation : $\forall O.\, p \vdash^{O}_{x}$ SNI iff $p \vdash_{x}$ SNI in the proofs for the combination.

However, this does not work. Consider this small example and the combination of V1 and V4 into V14 from the main paper restated here.

Listing 7: Speculative leak arising from speculation over branch and store instructions combined.

```
1  x = 0;
2  p = &secret;
3  p = &public;
4  if (x != 0)
5      temp &= A[*p];
```

We showed that this snippet is vulnerable in V14. Now consider you want to proof that every time you do a step in the combined AM semantics a step in the combined symbolic semantics should be made as well. As assumptions, we only assume Symbolic Consistency of the source semantics. However, when we try to execute the store instruction in line 5, we need to use the V4 semantics to do the step in the combination. But line 5 is never executed under the V4 semantics so it is also not in the behaviour of V4! This means we cannot rely on Symbolic Consistency of V4 to find a symbolic step here.

While the assumptions look similar, they are a little bit stronger. Lemma 3 (Assumption 1) is stated for a general single step and most importantly, this step does not have to be in the behaviour of V4. This makes it stronger than the behaviour.

That is also similar for the Oracle overapproximation because the behaviour does not account for speculative interactions in the combination and that is why we have 3) and 4) in the well-formedness condition of the combination.

F COMBINED SEMANTICS

With the new approach to the semantics we want to change the combined versions as well.

F.1 Combined Semantics V4 V5

Let us first define a speculative state and a speculative instance. Speculative instances are the union of their parts.

So here $\Phi_{S+R} \in \Phi_S \cup \Phi_R$.

$$\textit{Speculative States } \Sigma_{S+R} ::= \overline{\Phi}_{S+R}$$
$$\textit{Speculative Instance } \Phi_{S+R} ::= \langle p, ctr, \sigma, \mathbb{R}, n \rangle_{\overline{\rho}}$$

Definition 14 (Projection to V5). *We define a projection function* $\restriction^R : \Phi_{S+R} \to \Phi_R$ *as:*

$$\langle p, ctr, \sigma, \mathbb{R}, n \rangle \restriction^R = \langle p, ctr, \sigma, \mathbb{R}, n \rangle$$

We lift the function to speculative states Σ_{S+R} *in the following way:*

$$\varepsilon \restriction^R = \varepsilon$$
$$\overline{\Phi}_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \restriction^R = \overline{\Phi}_{S+R} \restriction^R \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle$$

Definition 15 (Projection to V4). *We define a projection function* $\restriction^S : \Phi_{S+R} \to \Phi_S \times \mathbb{R}$ *as:*

$$\langle p, ctr, \sigma, \mathbb{R}, n \rangle \restriction^S = (\langle p, ctr, \sigma, n \rangle, \mathbb{R}) \tag{1}$$

We lift the function to speculative states Σ_{S+R} *in the following way:*

$$\varepsilon \restriction^S = \varepsilon$$
$$\overline{\Phi}_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \restriction^S = \overline{\Phi}_{S+R} \restriction^S \cdot (\langle p, ctr, \sigma, n \rangle, \mathbb{R})$$

Judgements

$\Sigma_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Sigma'_{S+R}$	State Σ_{S+R} small-steps to Σ'_{S+R} and emits observation τ.
$\Phi_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}'_{S+R}$	Speculative instance Φ_{S+R} small-steps to $\overline{\Phi}_{S+R}{}'$ and emits observation τ.
$\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma'_{S+R}$	State Σ_{S+R} big-steps to Σ'_{S+R} and emits a list of observations $\overline{\tau}$.
$p \times \mathit{InitConf} \overset{\omega}{\Subset}_{S+R} \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$\Sigma_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Sigma'_{S+R}$

$$\frac{\Phi_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}'_{S+R}}{\overline{\Phi}_{S+R} \cdot \Phi_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}_{S+R} \cdot \overline{\Phi}'_{S+R}} \text{(AM-Context-V45)}$$

$$\frac{\begin{array}{c} n' = 0 \text{ or p is stuck} \quad \Phi_{S+R} \restriction^S = (\overline{\Phi}_S, \overline{\mathbb{R}}) \cdot (\langle p, ctr, \sigma, n \rangle, \mathbb{R}) \cdot (\langle p, ctr', \sigma', n' \rangle, \mathbb{R}') \\ \overline{\Phi}_S \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle \overset{\mathtt{rlb}_S \ ctr}{\dashrightarrow}_S \overline{\Phi}_S \cdot \langle p, ctr', \sigma, n \rangle \\ \overline{\Phi}_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n \rangle \restriction^S = (\overline{\Phi}_S, \overline{\mathbb{R}}) \cdot (\langle p, ctr', \sigma, n \rangle, \mathbb{R}) \end{array}}{\overline{\Phi}_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle \overset{\mathtt{rlb}_S \ ctr}{\dashrightarrow}_{S+R} \overline{\Phi}_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n \rangle} \text{(AM-v4-Rollback-V45)}$$

$$\frac{\begin{array}{c} n' = 0 \text{ or p is stuck} \quad \Phi_{S+R} \restriction^R = \overline{\Phi}_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle \\ \overline{\Phi}_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle \overset{\mathtt{rlb}_R \ ctr}{\dashrightarrow}_R \overline{\Phi}_R \cdot \langle p, ctr', \sigma, \mathbb{R}, n \rangle \\ \overline{\Phi}_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n \rangle \restriction^R = \overline{\Phi}_R \cdot \langle p, ctr', \sigma, \mathbb{R}, n \rangle \end{array}}{\overline{\Phi}_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle \overset{\mathtt{rlb}_R \ ctr}{\dashrightarrow}_{S+R} \overline{\Phi}_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n \rangle} \text{(AM-v5-Rollback-V45)}$$

$\Phi_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Phi'_{S+R}$

$$\frac{\Phi_{S+R}\restriction^S = (\Phi_S, \mathbb{R}) \quad \Phi_S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_S \quad \overline{\Phi}'_{S+R}\restriction^S = (\overline{\Phi}'_S, \mathbb{R})}{\Phi_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}'_{S+R}}\ \text{(AM-v4-step-V45)} \qquad \frac{\Phi_{S+R}\restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_R \quad \overline{\Phi}'_{S+R}\restriction^R = \overline{\Phi}'_R}{\Phi_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}'_{S+R}}\ \text{(AM-v5-step-V45)}$$

$$\boxed{\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma'_{S+R}}$$

$$\frac{}{\Sigma_{S+R} \Downarrow^{\epsilon}_{S+R} \Sigma_{S+R}}\ \text{(AM-Reflection-V45)} \qquad \frac{\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma''_{S+R} \quad \Sigma''_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Sigma'_{S+R}}{\Sigma_{S+R} \Downarrow^{\overline{\tau}\cdot\tau}_{S+R} \Sigma'_{S+R}}\ \text{(AM-Single-V45)}$$

Let us define what it means for a state to be initial or final.

$$\boxed{\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma'_{S+R}}$$

$$\frac{\Sigma_{S+R} = \langle p, 0, \sigma, \epsilon, \bot\rangle \quad \sigma \in \mathit{InitConf}}{\vdash \Sigma_{S+R} : \mathit{init}}\ \text{(AM-Init-V45)} \qquad \frac{\Sigma_{S+R} = \langle p, \mathit{ctr}, \sigma, \mathbb{R}, \bot\rangle \quad \sigma(\mathbf{pc}) = \bot}{\vdash \Sigma_{S+R} : \mathit{fin}}\ \text{(AM-Fin-V45)}$$

$$\frac{}{\Sigma^{\mathit{init}}_{S+R}(p, \sigma) := \langle p, 0, \sigma, \epsilon, \bot\rangle}\ \text{(R:Initial-State)}$$

$$\boxed{p \times \mathit{InitConf}\ \text{🕮}^{\omega}_{S+R}\ \overline{\tau}}$$

$$\frac{\exists \Sigma'_{S+R} \quad \vdash \Sigma'_{S+R} : \mathit{fin} \quad \Sigma^{\mathit{init}}_{S+R}(p, \sigma) \Downarrow^{\overline{\tau}}_{S+R} \Sigma'_{S+R}}{(p, \sigma)\ \text{🕮}^{\omega}_{S+R}\ \overline{\tau}}\ \text{(AM-Trace-V45)} \qquad \frac{}{\mathit{Beh}^{S+R}_{\mathcal{A}}(p) = \{\overline{\tau} \mid \forall \sigma \in \mathit{InitConf}.\ (p, \sigma)\ \text{🕮}^{\omega}_{S+R}\ \overline{\tau}\}}\ \text{(AM-Beh-V45)}$$

We define the behaviour of a program p, written $\mathit{Beh}^{S+R}_{\mathcal{A}}(p)$, as the set of traces that are generated starting from an initial configuration σ.

F.2 Combined oracle semantics V4 V5

Note that we now need our labels l and b again since the semantics can predict correctly again. We use identifiers i to mark from where the state was created from

$$\text{Spec. States } X_{S+R} ::= \overline{\Psi}_{S+R}$$

$$\text{Spec. Instance } \Psi_{S+R} ::= \langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, n\rangle^{(i,b+l)}_{\overline{\rho}} \text{ with } b = \{\mathit{true}, \mathit{false}, \epsilon\} \text{ and } l \in \mathbb{N} \cup \{\epsilon\} \text{ and } i \in \{S, R\}$$

Our oracle O_{S+R} is a pair of oracles (O_S, O_R)

Definition 16 (Projection to V5). *We define a projection function* $\restriction^R : \Psi_{S+R} \to \Psi_R$ *as:*

$$\langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, n\rangle\restriction^R = \langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, n\rangle$$

We lift the function to speculative states X_{S+R} *in the following way:*

$$\epsilon\restriction^R = \epsilon$$
$$\overline{\Psi}_{S+R} \cdot \langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, n\rangle\restriction^R = \overline{\Psi}_{S+R}\restriction^R \cdot \langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, n\rangle$$

Definition 17 (Projection to V4). *We define a projection function* $\restriction^S : \Psi_{S+R} \to \Psi_S \times \mathbb{R}$ *as:*

$$\langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, n\rangle\restriction^S = (\langle p, \mathit{ctr}, \sigma, h, n\rangle, \mathbb{R}) \tag{2}$$

We lift the function to speculative states X_{S+R} *in the following way:*

$$\epsilon\restriction^S = \epsilon$$
$$\overline{\Psi}_{S+R} \cdot \langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, n\rangle\restriction^S = \overline{\Psi}_{S+R}\restriction^S \cdot (\langle p, \mathit{ctr}, \sigma, h, n\rangle, \mathbb{R})$$

We use two helper functions $\mathit{decr}(\overline{\Psi}_{S+R})$ and $\mathit{zeroes}(\overline{\Psi}_{S+R})$ to decrease the stack of speculative instances during execution.

Definition 18 (V45:Decrease function)**.**

$$\begin{aligned} decr() &: X_{S+R} \mapsto X_{S+R} \\ decr(\varepsilon) &= \varepsilon \\ decr(\overline{\Psi}_{S+R} \cdot (p, ctr, \sigma, \mathbb{R}, h, n+1)) &= decr(\overline{\Psi}_{S+R}) \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n \rangle \\ decr(\overline{\Psi}_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n \rangle) &= decr(\overline{\Psi}_{S+R}) \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n \rangle \text{ if } n = 0 \text{ or } n = \bot \end{aligned}$$

Definition 19 (V45:Zeroes function)**.**

$$\begin{aligned} zeroes() &: X_{S+R} \mapsto X_{S+R} \\ zeroes(\varepsilon) &= \varepsilon \\ zeroes(\overline{\Psi}_{S+R} \cdot (p, ctr, \sigma, \mathbb{R}, h, n+1)) &= zeroes(\overline{\Psi}_{S+R}) \cdot \langle p, ctr, \sigma, \mathbb{R}, h, 0 \rangle \\ zeroes(\overline{\Psi}_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n \rangle) &= zeroes(\overline{\Psi}_{S+R}) \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n \rangle \text{ if } n = 0 \text{ or } n = \bot \end{aligned}$$

Judgements

$X_{S+R} \overset{\tau}{\rightsquigarrow}_{S+R}^{O_{S+R}} X'_{S+R}$	State X_{S+R} small-steps to X'_{S+R} and emits observation τ.
$\Psi_{S+R} \overset{\tau}{\rightsquigarrow}_{S+R}^{O_{S+R}} \overline{\Psi}'_{S+R}$	Speculative instance Ψ_{S+R} small-steps to $\overline{\Psi}_{S+R}{}'$ and emits observation τ.
$X_{S+R} \overset{O_{S+R}}{\Downarrow}_{\overline{\tau}}^{S+R} X'_{S+R}$	State X_{S+R} big-steps to X'_{S+R} and emits a list of observations $\overline{\tau}$.
$p \times InitConf \overset{O}{\Downarrow}_{S+R} \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$X_{S+R} \overset{\tau}{\rightsquigarrow}_{S+R}^{O_{S+R}} X'_{S+R}$

(V45-SE-Context)

$$\frac{\Psi_{S+R} \overset{\tau}{\rightsquigarrow}_{S+R}^{O_{S+R}} \overline{\Psi}'_{S+R} \qquad \Psi_{S+R} = \langle p, ctr, \sigma, \mathbb{R}, h, n+1 \rangle \qquad \text{if } p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \text{ then } \overline{\Psi}_{S+R}{}'' = zeroes(\overline{\Psi}_{S+R}) \text{ else } \overline{\Psi}_{S+R}{}'' = decr(\overline{\Psi}_{S+R})}{\overline{\Psi}_{S+R} \cdot \Psi_{S+R} \overset{\tau}{\rightsquigarrow}_{S+R}^{O_{S+R}} \overline{\Psi}_{S+R}{}'' \cdot \overline{\Psi}'_{S+R}}$$

(V45-SE:v4-General)

$$\frac{\overline{\Psi}_{S+R} \cdot \Psi_{S+R\overline{\rho} \cdot \tau} \restriction^{S} \overset{\tau}{\rightsquigarrow}_{S}^{O_S} \overline{\Psi}_{S+R} \cdot \Psi_{S+R\overline{\rho}} \restriction^{S}}{\overline{\Psi}_{S+R} \cdot \Psi_{S+R\overline{\rho} \cdot \tau} \overset{\tau}{\rightsquigarrow}_{S+R}^{O_{S+R}} \overline{\Psi}_{S+R} \cdot \Psi_{S+R\overline{\rho}}}$$

(V45-SE:v5-General)

$$\frac{\overline{\Psi}_{S+R} \cdot \Psi_{S+R\overline{\rho} \cdot \tau} \restriction^{R} \overset{\tau}{\rightsquigarrow}_{R}^{O_R} \overline{\Psi}_{S+R} \cdot \Psi_{S+R\overline{\rho}} \restriction^{R}}{\overline{\Psi}_{S+R} \cdot \Psi_{S+R\overline{\rho} \cdot \tau} \overset{\tau}{\rightsquigarrow}_{S+R}^{O_{S+R}} \overline{\Psi}_{S+R} \cdot \Psi_{S+R\overline{\rho}}}$$

(V45-SE:v4-Rollback)

$$\frac{n' = 0 \text{ or } p \text{ is stuck} \qquad \langle p, ctr, \sigma, \mathbb{R}, h, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n' \rangle^{true} \restriction^{S} \overset{\tau}{\rightsquigarrow}_{S}^{O_S} \langle p, ctr', \sigma, \mathbb{R}, h, n \rangle \restriction^{S}}{\overline{\Psi}_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n' \rangle^{(S,true)} \cdot \overline{\Psi}'_{S+R} \overset{\tau}{\rightsquigarrow}_{S+R}^{O_{S+R}} \overline{\Psi}_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, h, n \rangle}$$

(V45-SE:v5-Rollback)

$$\frac{n' = 0 \text{ or } p \text{ is stuck} \qquad \langle p, ctr, \sigma, \mathbb{R}, h, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n' \rangle^{m} \restriction^{R} \overset{\tau}{\rightsquigarrow}_{R}^{O_R} \langle p, ctr', \sigma, \mathbb{R}, h, n \rangle \restriction^{R}}{\overline{\Psi}_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n' \rangle^{(R,m)} \cdot \overline{\Psi}'_{S+R} \overset{\tau}{\rightsquigarrow}_{S+R}^{O_{S+R}} \overline{\Psi}_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, h, n \rangle}$$

(V45-SE:v4-Commit)

$$\frac{\langle p, ctr, \sigma, \mathbb{R}, h, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0 \rangle^{false} \restriction^{S} \overset{\tau}{\rightsquigarrow}_{S}^{O_S} \langle p, ctr', \sigma', \mathbb{R}', h', n \rangle \restriction^{S}}{\overline{\Psi}_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0 \rangle^{(S,false)} \cdot \overline{\Psi}_{S+R}{}' \overset{\tau}{\rightsquigarrow}_{S+R}^{O_{S+R}} \overline{\Psi}_{S+R} \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n \rangle \cdot \overline{\Psi}_{S+R}{}'}$$

(V45-SE:v5-Commit)

$$\frac{\langle p, ctr, \sigma, \mathbb{R}, h, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0 \rangle^{m} \restriction^{R} \overset{\tau}{\rightsquigarrow}_{R}^{O_R} \langle p, ctr', \sigma', \mathbb{R}', h', n \rangle \restriction^{R}}{\overline{\Psi}_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0 \rangle^{(R,m)} \cdot \overline{\Psi}_{S+R}{}' \overset{\tau}{\rightsquigarrow}_{S+R}^{O_{S+R}} \overline{\Psi}_{S+R} \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n \rangle \cdot \overline{\Psi}_{S+R}{}'}$$

$\Psi_{S+R} \overset{\tau}{\rightsquigarrow}_{S+R}^{O_{S+R}} \Psi'_{S+R}$

(V45-SE:v4-step)

$$\frac{O_{S+R} = (O, O_R) \qquad \Psi_{S+R} \restriction^{S} \overset{\tau}{\rightsquigarrow}_{S}^{O_S} \overline{\Psi}'_{S+R} \restriction^{S}}{\Psi_{S+R} \overset{\tau}{\rightsquigarrow}_{S+R}^{O_{S+R}} \overline{\Psi}'_{S+R}}$$

(V45-SE:v5-step)

$$\frac{O_{S+R} = (O_S, O) \qquad \Psi_{S+R} \restriction^{R} \overset{\tau}{\rightsquigarrow}_{R}^{O_R} \overline{\Psi}'_{S+R} \restriction^{S}}{\Psi_{S+R} \overset{\tau}{\rightsquigarrow}_{S+R}^{O_{S+R}} \overline{\Psi}'_{S+R}}$$

$X_{S+R} \overset{O_{S+R}}{\Downarrow}_{\overline{\tau}}^{S+R} X'_{S+R}$

$$\frac{}{X_{S+R} \overset{O_{S+R}}{\Downarrow}_{\varepsilon}^{S+R} X_{S+R}} \text{(SE-Reflection-V45)} \qquad \frac{X_{S+R} \overset{O_{S+R}}{\Downarrow}_{\overline{\tau}}^{S+R} X''_{S+R} \quad X''_{S+R} \overset{\tau}{\rightsquigarrow}_{S+R}^{O_{S+R}} X'_{S+R}}{X_{S+R} \overset{O_{S+R}}{\Downarrow}_{\overline{\tau}\cdot\tau}^{S+R} X'_{S+R}} \text{(SE-Single-V45)}$$

Let us define what it means for a state to be initial or final.

Helpers

$$\frac{X_{S+R} = \langle p, 0, \sigma, \varepsilon, \varepsilon, \bot \rangle \quad \sigma \in InitConf}{\vdash X_{S+R} : init} \text{(SE-Init-V45)} \qquad \frac{X_{S+R} = \langle p, ctr, \sigma, \mathbb{R}, h, \bot \rangle \quad \sigma(\mathbf{pc}) = \bot}{\vdash X_{S+R} : fin} \text{(SE-Fin-V45)}$$

$$\frac{}{X^{init}_{S+R}(p, \sigma) \coloneqq \langle p, 0, \sigma, \varepsilon, \varepsilon, \bot \rangle} \text{(S + R:SE-Initial-State)}$$

$$p \times InitConf \text{ } \text{🕱}^{O}_{S+R} \overline{\tau}$$

$$\frac{\exists X'_{S+R} \quad \vdash X'_{S+R} : fin \quad X^{init}_{S+R}(p, \sigma) \overset{O_{S+R}}{\Downarrow}_{\overline{\tau}}^{S+R} X'_{S+R}}{(p, \sigma) \text{ } \text{🕱}^{O}_{S+R} \overline{\tau}} \text{(SE-Trace-V45)} \qquad \frac{}{Beh^{S+R}_{\mathcal{A}}(p) = \{\overline{\tau} \mid \forall \sigma \in InitConf.\ (p, \sigma) \text{ } \text{🕱}^{O}_{S+R} \overline{\tau}\}} \text{(SE-Beh-V45)}$$

We define the behaviour of a program p, written $Beh^{S+R}_{\mathcal{A}}(p)$, as the set of traces that are generated starting from an initial configuration σ.

F.3 Combined Semantics V1 V4

$$\textit{Speculative States } \Sigma_{B+S} ::= \overline{\Phi}_{B+S}$$
$$\textit{Speculative Instance } \Phi_{B+S} ::= \langle p, ctr, \sigma, n\rangle_{\overline{\rho}}$$

Definition 20 (Projection to V1). *We define a projection function* $\restriction^B : \Phi_{B+S} \to \Phi_B$ *as:*

$$\langle p, ctr, \sigma, n\rangle \restriction^B = \langle p, ctr, \sigma, n\rangle$$

We lift the function to speculative states Σ_{B+S} *in the following way:*

$$\varepsilon \restriction^B = \varepsilon$$
$$\overline{\Phi}_{B+S} \cdot \langle p, ctr, \sigma, n\rangle \restriction^B = \overline{\Phi}_{B+S} \restriction^B \cdot \langle p, ctr, \sigma, n\rangle$$

Definition 21 (Projection to V4). *We define a projection function* $\restriction^S : \Phi_{B+S} \to \Phi_S$ *as:*

$$\langle p, ctr, \sigma, n\rangle \restriction^S = \langle p, ctr, \sigma, n\rangle$$

We lift the function to speculative states Σ_{B+S} *in the following way:*

$$\varepsilon \restriction^S = \varepsilon$$
$$\overline{\Phi}_{B+S} \cdot \langle p, ctr, \sigma, n\rangle \restriction^S = \overline{\Phi}_{B+S} \restriction^S \cdot \langle p, ctr, \sigma, n\rangle$$

Judgements

$\Sigma_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \Sigma'_{B+S}$	State Σ_{B+S} small-steps to Σ'_{B+S} and emits observation τ.
$\Phi_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \overline{\Phi}'_{B+S}$	Speculative instance Φ_{B+S} small-steps to $\overline{\Phi}_{B+S}{}'$ and emits observation τ.
$\Sigma_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma'_{B+S}$	State Σ_{B+S} big-steps to Σ'_{B+S} and emits a list of observations $\overline{\tau}$.
$p \times \mathit{InitConf} \overset{\omega}{\Longrightarrow}_{B+S} \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$\Sigma_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \Sigma'_{B+S}$

(AM-Context-V14)
$$\frac{\Phi_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \overline{\Phi}'_{B+S}}{\overline{\Phi}_{B+S} \cdot \Phi_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \overline{\Phi}_{B+S} \cdot \overline{\Phi}'_{B+S}}$$

(AM-v4-Rollback-V14)
$$\frac{\begin{array}{c} n' = 0 \text{ or p is stuck} \qquad \Phi_{B+S} \restriction^S = \overline{\Phi}_S \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle) \\ \overline{\Phi}_S \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle \overset{\mathrm{rlb}_S\ ctr}{\dashrightarrow}_S \overline{\Phi}_S \cdot \langle p, ctr', \sigma, n\rangle \\ \overline{\Phi}_{B+S} \cdot \langle p, ctr', \sigma, n\rangle \restriction^S = \overline{\Phi}_S \cdot \langle p, ctr', \sigma, n\rangle \end{array}}{\overline{\Phi}_{B+S} \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle \overset{\mathrm{rlb}_S\ ctr}{\dashrightarrow}_{B+S} \overline{\Phi}_{B+S} \cdot \langle p, ctr', \sigma, n\rangle}$$

(AM-v1-Rollback-V14)
$$\frac{\begin{array}{c} n' = 0 \text{ or p is stuck} \qquad \Phi_{B+S} \restriction^B = \overline{\Phi}_B \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle \\ \overline{\Phi}_B \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle \overset{\mathrm{rlb}_B\ ctr}{\dashrightarrow}_B \overline{\Phi}_B \cdot \langle p, ctr', \sigma, n\rangle \\ \overline{\Phi}_{B+S} \cdot \langle p, ctr', \sigma, n\rangle \restriction^B = \overline{\Phi}_B \cdot \langle p, ctr', \sigma, n\rangle \end{array}}{\overline{\Phi}_{B+S} \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle \overset{\mathrm{rlb}_B\ ctr}{\dashrightarrow}_{B+S} \overline{\Phi}_{B+S} \cdot \langle p, ctr', \sigma, n\rangle}$$

$\Phi_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \Phi'_{B+S}$

(AM-v4-step-V14)
$$\frac{\Phi_{B+S} \restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_S \qquad \overline{\Phi}'_{B+S} \restriction^S = \overline{\Phi}'_S}{\Phi_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \overline{\Phi}'_{B+S}}$$

(AM-v1-step-V14)
$$\frac{\Phi_{B+S} \restriction^B \overset{\tau}{\dashrightarrow}_B \overline{\Phi}'_B \qquad \overline{\Phi}'_{B+S} \restriction^B = \overline{\Phi}'_B}{\Phi_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \overline{\Phi}'_{B+S}}$$

$\Sigma_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma'_{B+S}$

$$\frac{}{\Sigma_{B+S} \Downarrow^{\varepsilon}_{B+S} \Sigma_{B+S}}\ \text{(AM-Reflection-V14)} \qquad \frac{\Sigma_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma''_{B+S} \quad \Sigma''_{B+S} \overset{\tau}{\rightarrow}_{B+S} \Sigma'_{B+S}}{\Sigma_{B+S} \Downarrow^{\overline{\tau}\cdot\tau}_{B+S} \Sigma'_{B+S}}\ \text{(AM-Single-V14)}$$

Let us define what it means for a state to be initial or final.

Helpers

$$\frac{\Sigma_{B+S} = \langle p, 0, \sigma, \varepsilon, \bot\rangle \quad \sigma \in \mathit{InitConf}}{\vdash \Sigma_{B+S} : \mathit{init}}\ \text{(AM-Init-V14)} \qquad \frac{\Sigma_{B+S} = \langle p, \mathit{ctr}, \sigma, \mathbb{R}, \bot\rangle \quad \sigma(\mathbf{pc}) = \bot}{\vdash \Sigma_{B+S} : \mathit{fin}}\ \text{(AM-Fin-V14)}$$

$$\frac{}{\Sigma^{\mathit{init}}_{B+S}(p,\sigma) \coloneqq \langle p, 0, \sigma, \varepsilon, \bot\rangle}\ \text{(B + S:AM-Initial-State)}$$

$p \times \mathit{InitConf}\ \text{Ω}^{\omega}_{B+S}\ \overline{\tau}$

$$\frac{\exists \Sigma'_{B+S} \quad \vdash \Sigma'_{B+S} : \mathit{fin} \quad \Sigma^{\mathit{init}}_{B+S}(p,\sigma) \Downarrow^{\overline{\tau}}_{B+S} \Sigma'_{B+S}}{p, \sigma\ \text{Ω}^{\omega}_{B+S}\ \overline{\tau}}\ \text{(AM-Trace-V14)} \qquad \frac{}{\mathit{Beh}^{B+S}_{\mathcal{A}}(p) = \{\overline{\tau} \mid \forall \sigma \in \mathit{InitConf}.\ p, \sigma\ \text{Ω}^{\omega}_{B+S}\ \overline{\tau}\}}\ \text{(AM-Beh-V14)}$$

We define the behaviour of a program p, written $\mathit{Beh}^{B+S}_{\mathcal{A}}(p)$, as the set of traces that are generated starting from an initial configuration σ.

F.4 Combined oracle semantics B + S

Judgements

$X_{B+S} \overset{\tau}{\rightsquigarrow}^{O_{B+S}}_{B+S} X'_{B+S}$	State X_{B+S} small-steps to X'_{B+S} and emits observation τ.
$\Psi_{B+S} \overset{\tau}{\rightsquigarrow}^{O_{B+S}}_{B+S} \overline{\Psi}'_{B+S}$	Speculative instance Ψ_{B+S} small-steps to $\overline{\Psi}_{B+S}{}'$ and emits observation τ.
$X_{B+S} \overset{O_{B+S}}{\Downarrow}{}^{B+S}_{\overline{\tau}} X'_{B+S}$	State X_{B+S} big-steps to X'_{B+S} and emits a list of observations $\overline{\tau}$.
$p \times \mathit{InitConf}\ \text{Ω}^{O}_{B+S}\ \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$X_{B+S} \overset{\tau}{\rightsquigarrow}^{O_{B+S}}_{B+S} X'_{B+S}$

$$\frac{\Psi_{B+S} \overset{\tau}{\rightsquigarrow}^{O_{B+S}}_{B+S} \overline{\Psi}'_{B+S} \qquad \Psi_{B+S} = \langle p, \mathit{ctr}, \sigma, h, n+1\rangle \qquad \text{if } p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \text{ then } \overline{\Psi}_{B+S}{}'' = \mathit{zeroes}(\overline{\Psi}_{B+S}) \text{ else } \overline{\Psi}_{B+S}{}'' = \mathit{decr}(\overline{\Psi}_{B+S})}{\overline{\Psi}_{B+S} \cdot \Psi_{B+S} \overset{\tau}{\rightsquigarrow}^{O_{B+S}}_{B+S} \overline{\Psi}_{B+S}{}'' \cdot \overline{\Psi}'_{B+S}}\ \text{(V14-SE-Context)}$$

$$\frac{\overline{\Psi}_{B+S} \cdot \Psi_{B+S\overline{\rho}\cdot\tau}\restriction^{S} \overset{\tau}{\rightsquigarrow}^{O_S}_{S} \overline{\Psi}_{B+S} \cdot \Psi_{B+S\overline{\rho}}\restriction^{S}}{\overline{\Psi}_{B+S} \cdot \Psi_{B+S\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}^{O_{B+S}}_{B+S} \overline{\Psi}_{B+S} \cdot \Psi_{B+S\overline{\rho}}}\ \text{(V14-SE:v4-General)} \qquad \frac{\overline{\Psi}_{B+S} \cdot \Psi_{B+S\overline{\rho}\cdot\tau}\restriction^{B} \overset{\tau}{\rightsquigarrow}^{O_B}_{1} \overline{\Psi}_{B+S} \cdot \Psi_{B+S\overline{\rho}}\restriction^{B}}{\overline{\Psi}_{B+S} \cdot \Psi_{B+S\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}^{O_{B+S}}_{B+S} \overline{\Psi}_{B+S} \cdot \Psi_{B+S\overline{\rho}}}\ \text{(V14-SE:v1-General)}$$

$$\frac{n' = 0 \text{ or } p \text{ is stuck} \qquad \langle p, \mathit{ctr}, \sigma, h, n\rangle \cdot \langle p, \mathit{ctr}', \sigma', h', n'\rangle^{\mathit{true}}\restriction^{S} \overset{\tau}{\rightsquigarrow}^{O_S}_{S} \langle p, \mathit{ctr}', \sigma, h, n\rangle\restriction^{S}}{\overline{\Psi}_{B+S} \cdot \langle p, \mathit{ctr}, \sigma, h, n\rangle \cdot \langle p, \mathit{ctr}', \sigma', h', n'\rangle^{(S,\mathit{true})} \cdot \overline{\Psi}'_{B+S} \overset{\tau}{\rightsquigarrow}^{O_{B+S}}_{B+S} \overline{\Psi}_{B+S} \cdot \langle p, \mathit{ctr}', \sigma, h, n\rangle}\ \text{(V14-SE:v4-Rollback)}$$

$$\frac{n' = 0 \text{ or } p \text{ is stuck} \qquad \langle p, \mathit{ctr}, \sigma, h, n\rangle \cdot \langle p, \mathit{ctr}', \sigma', h', n'\rangle^{m}\restriction^{B} \overset{\tau}{\rightsquigarrow}^{O_B}_{1} \langle p, \mathit{ctr}', \sigma, h, n\rangle\restriction^{B}}{\overline{\Psi}_{B+S} \cdot \langle p, \mathit{ctr}, \sigma, h, n\rangle \cdot \langle p, \mathit{ctr}', \sigma', h', n'\rangle^{(B,m)} \cdot \overline{\Psi}'_{B+S} \overset{\tau}{\rightsquigarrow}^{O_{B+S}}_{B+S} \overline{\Psi}_{B+S} \cdot \langle p, \mathit{ctr}', \sigma, h, n\rangle}\ \text{(V14-SE:v1-Rollback)}$$

$$\frac{\langle p, \mathit{ctr}, \sigma, h, n\rangle \cdot \langle p, \mathit{ctr}', \sigma', h', 0\rangle^{\mathit{false}}\restriction^{S} \overset{\tau}{\rightsquigarrow}^{O_S}_{S} \langle p, \mathit{ctr}', \sigma', h', n\rangle\restriction^{S}}{\overline{\Psi}_{B+S} \cdot \langle p, \mathit{ctr}, \sigma, h, n\rangle \cdot \langle p, \mathit{ctr}', \sigma', h', 0\rangle^{(S,\mathit{false})} \cdot \overline{\Psi}_{B+S}{}' \overset{\tau}{\rightsquigarrow}^{O_{B+S}}_{B+S} \overline{\Psi}_{B+S} \cdot \langle p, \mathit{ctr}', \sigma', h', n\rangle \cdot \overline{\Psi}_{B+S}{}'}\ \text{(V14-SE:v4-Commit)}$$

$$\frac{\langle p, \mathit{ctr}, \sigma, h, n\rangle \cdot \langle p, \mathit{ctr}', \sigma', h', 0\rangle^{m}\restriction^{B} \overset{\tau}{\rightsquigarrow}^{O_B}_{1} \langle p, \mathit{ctr}', \sigma', h', n\rangle\restriction^{B}}{\overline{\Psi}_{B+S} \cdot \langle p, \mathit{ctr}, \sigma, h, n\rangle \cdot \langle p, \mathit{ctr}', \sigma', h', 0\rangle^{(B,m)} \cdot \overline{\Psi}_{B+S}{}' \overset{\tau}{\rightsquigarrow}^{O_{B+S}}_{B+S} \overline{\Psi}_{B+S} \cdot \langle p, \mathit{ctr}', \sigma', h', n\rangle \cdot \overline{\Psi}_{B+S}{}'}\ \text{(V14-SE:v1-Commit)}$$

$\boxed{\Psi_{B+S} \overset{\tau, O_{B+S}}{\rightsquigarrow}_{B+S} \Psi'_{B+S}}$

(V14-SE:v1-step)
$$\frac{O_{B+S} = (O_B, O_S) \qquad \Psi_{B+S} \restriction^B \overset{\tau, O_B}{\rightsquigarrow}_1 \overline{\Psi}'_{B+S} \restriction^B}{\Psi_{B+S} \overset{\tau, O_{B+S}}{\rightsquigarrow}_{B+S} \overline{\Psi}'_{B+S}}$$

(V14-SE:v4-step)
$$\frac{O_{B+S} = (O_B, O_S) \qquad \Psi_{B+S} \restriction^S \overset{\tau, O_S}{\rightsquigarrow}_S \overline{\Psi}'_{B+S} \restriction^S}{\Psi_{B+S} \overset{\tau, O_{B+S}}{\rightsquigarrow}_{B+S} \overline{\Psi}'_{B+S}}$$

$\boxed{X_{B+S} \overset{O_{B+S}}{\Downarrow}_{\overline{\tau}}^{B+S} X'_{B+S}}$

(V14-SE:Reflection)
$$\frac{}{X_{B+S} \overset{O_{B+S}}{\Downarrow}_{\varepsilon}^{B+S} X_{B+S}}$$

(V14-SE:Single)
$$\frac{X_{B+S} \overset{O_{B+S}}{\Downarrow}_{\overline{\tau}}^{B+S} X''_{B+S} \qquad X''_{B+S} \overset{\tau, O_{B+S}}{\rightsquigarrow}_{B+S} X'_{B+S}}{X_{B+S} \overset{O_{B+S}}{\Downarrow}_{\overline{\tau}\cdot\tau}^{B+S} X'_{B+S}}$$

Let us define what it means for a state to be initial or final.

Helpers

(V14-SE:Init)
$$\frac{X_{B+S} = \langle p, 0, \sigma, \varepsilon, \bot \rangle \qquad \sigma \in \mathit{InitConf}}{\vdash X_{B+S} : \mathit{init}}$$

(V14-SE:Fin)
$$\frac{X_{B+S} = \langle p, \mathit{ctr}, \sigma, h, \bot \rangle \qquad \sigma(\mathbf{pc}) = \bot}{\vdash X_{B+S} : \mathit{fin}}$$

(B + S:SE-Initial-State)
$$\frac{}{X^{\mathit{init}}_{B+S}(p, \sigma) \coloneqq \langle p, 0, \sigma, \varepsilon, \bot \rangle}$$

$\boxed{p \times \mathit{InitConf} \; \text{🕮}^{O}_{B+S} \; \overline{\tau}}$

(V14-SE:Trace)
$$\frac{\exists X'_{B+S} \qquad \vdash X'_{B+S} : \mathit{fin} \qquad X^{\mathit{init}}_{B+S}(p, \sigma) \overset{O_{B+S}}{\Downarrow}_{\overline{\tau}}^{B+S} X'_{B+S}}{p, \sigma \; \text{🕮}^{O}_{B+S} \; \overline{\tau}}$$

(V14-SE:Beh)
$$\frac{}{\mathit{Beh}^{B+S}_{\mathcal{A}}(p) = \{\overline{\tau} \mid \forall \sigma \in \mathit{InitConf}.\; p, \sigma \; \text{🕮}^{O}_{B+S} \; \overline{\tau}\}}$$

F.5 Combined Semantics V1 V5

$$\textit{Speculative States } \Sigma_{B+R} ::= \overline{\Phi}_{B+R}$$
$$\textit{Speculative Instance } \Phi_{B+R} ::= \langle p, ctr, \sigma, \mathbb{R}, n\rangle_{\overline{\rho}}$$

Definition 22 (Projection to V5). *We define a projection function* $\restriction^R : \Phi_{B+R} \to \Phi_R$ *as:*

$$\langle p, ctr, \sigma, \mathbb{R}, n\rangle \restriction^R = \langle p, ctr, \sigma, \mathbb{R}, n\rangle$$

We lift the function to speculative states Σ_{B+R} *in the following way:*

$$\varepsilon \restriction^R = \varepsilon$$
$$\overline{\Phi}_{B+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \restriction^R = \overline{\Phi}_{B+R} \restriction^R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle$$

Definition 23 (Projection to V1). *We define a projection function* $\restriction^B : \Phi_{B+R} \to \Phi_B \times \mathbb{R}$ *as:*

$$\langle p, ctr, \sigma, \mathbb{R}, n\rangle \restriction^B = (\langle p, ctr, \sigma, n\rangle, \mathbb{R}) \tag{3}$$

We lift the function to speculative states Σ_{B+R} *in the following way:*

$$\varepsilon \restriction^B = \varepsilon$$
$$\overline{\Phi}_{B+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \restriction^B = \overline{\Phi}_{B+R} \restriction^B \cdot (\langle p, ctr, \sigma, n\rangle, \mathbb{R})$$

Judgements

$\Sigma_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \Sigma'_{B+R}$	State Σ_{B+R} small-steps to Σ'_{B+R} and emits observation τ.
$\Phi_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \overline{\Phi}'_{B+R}$	Speculative instance Φ_{B+R} small-steps to $\overline{\Phi}_{B+R}{}'$ and emits observation τ.
$\Sigma_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma'_{B+R}$	State Σ_{B+R} big-steps to Σ'_{B+R} and emits a list of observations $\overline{\tau}$.
$p \times \mathit{InitConf} \overset{\omega}{\dashrightarrow}_{B+R} \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$\Sigma_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \Sigma'_{B+R}$

(AM-Context-V15)
$$\frac{\Phi_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \overline{\Phi}'_{B+R}}{\overline{\Phi}_{B+R} \cdot \Phi_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \overline{\Phi}_{B+R} \cdot \overline{\Phi}'_{B+R}}$$

(AM-v1-Rollback-V15)
$$\frac{\begin{array}{c} n' = 0 \text{ or p is stuck} \quad \Phi_{B+R}\restriction^B = (\overline{\Phi}_B, \overline{\mathbb{R}}) \cdot (\langle p, ctr, \sigma, n\rangle, \mathbb{R}) \cdot (\langle p, ctr', \sigma', n'\rangle, \mathbb{R}') \\ \overline{\Phi}_B \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle \overset{\mathrm{rlb}_B\ ctr}{\dashrightarrow}_B \overline{\Phi}_B \cdot \langle p, ctr', \sigma, n\rangle \\ \overline{\Phi}_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\restriction^B = (\overline{\Phi}_B, \overline{\mathbb{R}}) \cdot (\langle p, ctr', \sigma, n\rangle, \mathbb{R}) \end{array}}{\overline{\Phi}_{B+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n'\rangle \overset{\mathrm{rlb}_B\ ctr}{\dashrightarrow}_{B+R} \overline{\Phi}_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}$$

(AM-v5-Rollback-V15)
$$\frac{\begin{array}{c} n' = 0 \text{ or p is stuck} \quad \Phi_{B+R}\restriction^R = \overline{\Phi}_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n'\rangle \\ \overline{\Phi}_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n'\rangle \overset{\mathrm{rlb}_R\ ctr}{\dashrightarrow}_R \overline{\Phi}_R \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \\ \overline{\Phi}_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\restriction^R = \overline{\Phi}_R \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \end{array}}{\overline{\Phi}_{B+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n'\rangle \overset{\mathrm{rlb}_R\ ctr}{\dashrightarrow}_{B+R} \overline{\Phi}_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}$$

$\Phi_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \Phi'_{B+R}$

(AM-v1-step-V15)
$$\frac{\Phi_{B+R}\restriction^B = (\Phi_B, \mathbb{R}) \quad \Phi_B \overset{\tau}{\dashrightarrow}_B \overline{\Phi}'_B \quad \overline{\Phi}'_{B+R}\restriction^B = (\overline{\Phi}'_B, \mathbb{R})}{\Phi_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \overline{\Phi}'_{B+R}}$$

(AM-v5-step-V15)
$$\frac{\Phi_{B+R}\restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_R \quad \overline{\Phi}'_{B+R}\restriction^R = \overline{\Phi}'_R}{\Phi_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \overline{\Phi}'_{B+R}}$$

$\Sigma_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma'_{B+R}$

$$\frac{}{\Sigma_{B+R} \Downarrow^{\varepsilon}_{B+R} \Sigma_{B+R}}\ \text{(AM-Reflection-V15)} \qquad \frac{\Sigma_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma''_{B+R} \quad \Sigma''_{B+R} \xrightarrow{\tau}_{B+R} \Sigma'_{B+R}}{\Sigma_{B+R} \Downarrow^{\overline{\tau}\cdot\tau}_{B+R} \Sigma'_{B+R}}\ \text{(AM-Single-V15)}$$

Let us define what it means for a state to be initial or final.

Helpers

$$\frac{\Sigma_{B+R} = \langle p, 0, \sigma, \varepsilon, \bot\rangle \quad \sigma \in \mathit{InitConf}}{\vdash \Sigma_{B+R} : \mathit{init}}\ \text{(AM-Init-V15)} \qquad \frac{\Sigma_{B+R} = \langle p, \mathit{ctr}, \sigma, \mathbb{R}, \bot\rangle \quad \sigma(\mathbf{pc}) = \bot}{\vdash \Sigma_{B+R} : \mathit{fin}}\ \text{(AM-Fin-V15)}$$

$$\frac{}{\Sigma^{\mathit{init}}_{B+R}(p, \sigma) \coloneqq \langle p, 0, \sigma, \varepsilon, \bot\rangle}\ \text{(V15:AM-Initial-State)}$$

$p \times \mathit{InitConf} \Subset^{\omega}_{B+R} \overline{\tau}$

$$\frac{\exists \Sigma'_{B+R} \quad \vdash \Sigma'_{B+R} : \mathit{fin} \quad \Sigma^{\mathit{init}}_{B+R}(p, \sigma) \Downarrow^{\overline{\tau}}_{B+R} \Sigma'_{B+R}}{p, \sigma \Subset^{\omega}_{B+R} \overline{\tau}}\ \text{(AM-Trace-V15)} \qquad \frac{}{\mathit{Beh}^{B+R}_{\mathcal{A}}(p) = \{\overline{\tau} \mid \forall \sigma \in \mathit{InitConf}.\ p, \sigma \Subset^{\omega}_{B+R} \overline{\tau}\}}\ \text{(AM-Beh-V15)}$$

We define the behaviour of a program p, written $\mathit{Beh}^{B+R}_{\mathcal{A}}(p)$, as the set of traces that are generated starting from an initial configuration σ.

F.6 Combined oracle semantics B + R

Definition 24 (V15:Decrease function)**.**

$$\begin{aligned}
\mathit{decr}() : X_{B+R} &\mapsto X_{B+R} \\
\mathit{decr}(\varepsilon) &= \varepsilon \\
\mathit{decr}(\overline{\Psi}_{B+R} \cdot (p, \mathit{ctr}, \sigma, \mathbb{R}, h, n+1)) &= \mathit{decr}(\overline{\Psi}_{B+R}) \cdot \langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, n\rangle \\
\mathit{decr}(\overline{\Psi}_{B+R} \cdot \langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, n\rangle) &= \mathit{decr}(\overline{\Psi}_{B+R}) \cdot \langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, n\rangle \ \mathit{if}\ n = 0\ \mathit{or}\ n = \bot
\end{aligned}$$

Definition 25 (V15:Zeroes function)**.**

$$\begin{aligned}
\mathit{zeroes}() : X_{B+R} &\mapsto X_{B+R} \\
\mathit{zeroes}(\varepsilon) &= \varepsilon \\
\mathit{zeroes}(\overline{\Psi}_{B+R} \cdot (p, \mathit{ctr}, \sigma, \mathbb{R}, h, n+1)) &= \mathit{zeroes}(\overline{\Psi}_{B+R}) \cdot \langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, 0\rangle \\
\mathit{zeroes}(\overline{\Psi}_{B+R} \cdot \langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, n\rangle) &= \mathit{zeroes}(\overline{\Psi}_{B+R}) \cdot \langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, n\rangle \ \mathit{if}\ n = 0\ \mathit{or}\ n = \bot
\end{aligned}$$

Judgements

$X_{B+R} \overset{\tau}{\rightsquigarrow}^{O_{B+R}}_{B+R} X'_{B+R}$	State X_{B+R} small-steps to X'_{B+R} and emits observation τ.
$\Psi_{B+R} \overset{\tau}{\rightsquigarrow}^{O_{B+R}}_{B+R} \overline{\Psi}'_{B+R}$	Speculative instance Ψ_{B+R} small-steps to $\overline{\Psi}_{B+R}{}'$ and emits observation τ.
$X_{B+R} \overset{O_{B+R}}{\Downarrow}{}^{B+R}_{\overline{\tau}} X'_{B+R}$	State X_{B+R} big-steps to X'_{B+R} and emits a list of observations $\overline{\tau}$.
$p \times \mathit{InitConf} \Subset^{O}_{B+R} \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$X_{B+R} \overset{\tau}{\rightsquigarrow}^{O_{B+R}}_{B+R} X'_{B+R}$

$$\frac{\Psi_{B+R} \overset{\tau}{\rightsquigarrow}^{O_{B+R}}_{B+R} \overline{\Psi}'_{B+R} \qquad \Psi_{B+R} = \langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, n+1\rangle \quad \text{if } p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \text{ then } \overline{\Psi}_{B+R}{}'' = \mathit{zeroes}(\overline{\Psi}_{B+R}) \text{ else } \overline{\Psi}_{B+R}{}'' = \mathit{decr}(\overline{\Psi}_{B+R})}{\overline{\Psi}_{B+R} \cdot \Psi_{B+R} \overset{\tau}{\rightsquigarrow}^{O_{B+R}}_{B+R} \overline{\Psi}_{B+R}{}'' \cdot \overline{\Psi}'_{B+R}}\ \text{(V15-SE-Context)}$$

$$\frac{\overline{\Psi}_{B+R} \cdot \Psi_{B+R\overline{\rho}\cdot\tau}\restriction^{B} \overset{\tau}{\rightsquigarrow}_1^{O_B} \overline{\Psi}_{B+R} \cdot \Psi_{B+R\overline{\rho}}\restriction^{B}}{\overline{\Psi}_{B+R} \cdot \Psi_{B+R\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}^{O_{B+R}}_{B+R} \overline{\Psi}_{B+R} \cdot \Psi_{B+R\overline{\rho}}}\ \text{(V15-SE:v1-General)} \qquad \frac{\overline{\Psi}_{B+R} \cdot \Psi_{B+R\overline{\rho}\cdot\tau}\restriction^{R} \overset{\tau}{\rightsquigarrow}_R^{O_R} \overline{\Psi}_{B+R} \cdot \Psi_{B+R\overline{\rho}}\restriction^{R}}{\overline{\Psi}_{B+R} \cdot \Psi_{B+R\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}^{O_{B+R}}_{B+R} \overline{\Psi}_{B+R} \cdot \Psi_{B+R\overline{\rho}}}\ \text{(V15-SE:v5-General)}$$

$$\frac{n' = 0 \text{ or } p \text{ is stuck} \quad \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n'\rangle^{m} \restriction^{B} \overset{\tau}{\rightsquigarrow}_{1}^{O_B} \langle p, ctr', \sigma, \mathbb{R}, h, n\rangle \restriction^{B}}{\overline{\Psi}_{B+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n'\rangle^{(B,false)} \cdot \overline{\Psi}'_{B+R} \overset{\tau}{\rightsquigarrow}_{B+R}^{O_{B+R}} \overline{\Psi}_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, h, n\rangle} \text{ (V15-SE:v1-Rollback)}$$

$$\frac{n' = 0 \text{ or } p \text{ is stuck} \quad \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n'\rangle^{m} \restriction^{R} \overset{\tau}{\rightsquigarrow}_{R}^{O_R} \langle p, ctr', \sigma, \mathbb{R}, h, n\rangle \restriction^{R}}{\overline{\Psi}_{B+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n'\rangle^{(R,false)} \cdot \overline{\Psi}'_{B+R} \overset{\tau}{\rightsquigarrow}_{B+R}^{O_{B+R}} \overline{\Psi}_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, h, n\rangle} \text{ (V15-SE:v5-Rollback)}$$

$$\frac{\langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0\rangle^{m} \restriction^{B} \overset{\tau}{\rightsquigarrow}_{1}^{O_B} \langle p, ctr', \sigma', \mathbb{R}', h', n\rangle \restriction^{B}}{\overline{\Psi}_{B+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0\rangle^{(B,true)} \cdot \overline{\Psi}_{B+R}{}' \overset{\tau}{\rightsquigarrow}_{B+R}^{O_{B+R}} \overline{\Psi}_{B+R} \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n\rangle \cdot \overline{\Psi}_{B+R}{}'} \text{ (V15-SE:v1-Commit)}$$

$$\frac{\langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0\rangle^{m} \restriction^{R} \overset{\tau}{\rightsquigarrow}_{R}^{O_R} \langle p, ctr', \sigma', \mathbb{R}', h', n\rangle \restriction^{R}}{\overline{\Psi}_{B+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0\rangle^{(R,true)} \cdot \overline{\Psi}_{B+R}{}' \overset{\tau}{\rightsquigarrow}_{B+R}^{O_{B+R}} \overline{\Psi}_{B+R} \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n\rangle \cdot \overline{\Psi}_{B+R}{}'} \text{ (V15-SE:v5-Commit)}$$

$\boxed{\Psi_{B+R} \overset{\tau}{\rightsquigarrow}_{B+R}^{O_{B+R}} \Psi'_{B+R}}$

$$\frac{O_{B+R} = (O_B, O_R) \quad \Psi_{B+R} \restriction^{B} \overset{\tau}{\rightsquigarrow}_{1}^{O_B} \overline{\Psi}'_{B+R} \restriction^{B}}{\Psi_{B+R} \overset{\tau}{\rightsquigarrow}_{B+R}^{O_{B+R}} \overline{\Psi}'_{B+R}} \text{ (V15-SE:v1-step)} \qquad \frac{O_{B+R} = (O_B, O_R) \quad \Psi_{B+R} \restriction^{R} \overset{\tau}{\rightsquigarrow}_{R}^{O_R} \overline{\Psi}'_{B+R} \restriction^{R}}{\Psi_{B+R} \overset{\tau}{\rightsquigarrow}_{B+R}^{O_{B+R}} \overline{\Psi}'_{B+R}} \text{ (V15-SE:v5-step)}$$

$\boxed{X_{B+R} \overset{O_{B+R}}{\Downarrow}_{\overline{\tau}}^{B+R} X'_{B+R}}$

$$\frac{}{X_{B+R} \overset{O_{B+R}}{\Downarrow}_{\varepsilon}^{B+R} X_{B+R}} \text{ (V15-SE:Reflection)} \qquad \frac{X_{B+R} \overset{O_{B+R}}{\Downarrow}_{\overline{\tau}}^{B+R} X''_{B+R} \quad X''_{B+R} \overset{\tau}{\rightsquigarrow}_{B+R}^{O_{B+R}} X'_{B+R}}{X_{B+R} \overset{O_{B+R}}{\Downarrow}_{\overline{\tau}\cdot\tau}^{B+R} X'_{B+R}} \text{ (V15-SE:Single)}$$

Let us define what it means for a state to be initial or final.

Helpers

$$\frac{X_{B+R} = \langle p, 0, \sigma, \varepsilon, \varepsilon, \bot\rangle \quad \sigma \in InitConf}{\vdash X_{B+R} : init} \text{ (V15-SE:Init)} \qquad \frac{X_{B+R} = \langle p, ctr, \sigma, \mathbb{R}, h, \bot\rangle \quad \sigma(\mathbf{pc}) = \bot}{\vdash X_{B+R} : fin} \text{ (V15-SE:Fin)}$$

$$\frac{}{X^{init}_{B+R}(p, \sigma) := \langle p, 0, \sigma, \varepsilon, \varepsilon, \bot\rangle} \text{ (V15:SE-Initial-State)}$$

$\boxed{p \times InitConf \text{ } \text{🕮}^{O}_{B+R} \overline{\tau}}$

$$\frac{\exists X'_{B+R} \quad \vdash X'_{B+R} : fin \quad X^{init}_{B+R}(p, \sigma) \overset{O_{B+R}}{\Downarrow}_{\overline{\tau}}^{B+R} X'_{B+R}}{p, \sigma \text{ } \text{🕮}^{O}_{B+R} \overline{\tau}} \text{ (V15-SE:Trace)}$$

$$\frac{}{Beh^{B+R}_{\mathcal{A}}(p) = \{\overline{\tau} \mid \forall \sigma \in InitConf.\ p, \sigma \text{ } \text{🕮}^{O}_{B+R} \overline{\tau}\}} \text{ (V15-SE:Beh)}$$

F.7 Combined Semantics V1 V4 V5

$$\textit{Speculative States } \Sigma_{B+S+R} ::= \overline{\Phi}_{B+S+R}$$
$$\textit{Speculative Instance } \Phi_{B+S+R} ::= \langle p, ctr, \sigma, \mathbb{R}, n\rangle_{\overline{\rho}}$$

Definition 26 (Projection to V5). *We define a projection function* $\restriction^R : \Phi_{B+S+R} \to \Phi_R$ *as:*

$$\langle p, ctr, \sigma, \mathbb{R}, n\rangle \restriction^R = \langle p, ctr, \sigma, \mathbb{R}, n\rangle$$

We lift the function to speculative states Σ_{B+S+R} *in the following way:*

$$\varepsilon \restriction^R = \varepsilon$$
$$\overline{\Phi}_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \restriction^R = \overline{\Phi}_{B+S+R} \restriction^R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle$$

Definition 27 (Projection to V4). *We define a projection function* $\restriction^S : \Phi_{B+S+R} \to \Phi_S \times \mathbb{R}$ *as:*

$$\langle p, ctr, \sigma, \mathbb{R}, n\rangle \restriction^S = (\langle p, ctr, \sigma, n\rangle, \mathbb{R}) \tag{4}$$

We lift the function to speculative states Σ_{B+S+R} *in the following way:*

$$\varepsilon \restriction^S = \varepsilon$$
$$\overline{\Phi}_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \restriction^S = \overline{\Phi}_{B+S+R} \restriction^S \cdot (\langle p, ctr, \sigma, n\rangle, \mathbb{R})$$

Definition 28 (Projection to V1). *We define a projection function* $\restriction^B : \Phi_{B+S+R} \to \Phi_B \times \mathbb{R}$ *as:*

$$\langle p, ctr, \sigma, \mathbb{R}, n\rangle \restriction^B = (\langle p, ctr, \sigma, n\rangle, \mathbb{R}) \tag{5}$$

We lift the function to speculative states Σ_{B+S+R} *in the following way:*

$$\varepsilon \restriction^B = \varepsilon$$
$$\overline{\Phi}_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \restriction^B = \overline{\Phi}_{B+S+R} \restriction^B \cdot (\langle p, ctr, \sigma, n\rangle, \mathbb{R})$$

Judgements

$\Sigma_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \Sigma'_{B+S+R}$	State Σ_{B+S+R} small-steps to Σ'_{B+S+R} and emits observation τ.
$\Phi_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \overline{\Phi}'_{B+S+R}$	Speculative instance Φ_{B+S+R} small-steps to $\overline{\Phi}_{B+S+R}{}'$ and emits observation τ.
$\Sigma_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma'_{B+S+R}$	State Σ_{B+S+R} big-steps to Σ'_{B+S+R} and emits a list of observations $\overline{\tau}$.
$p \times \mathit{InitConf} \; \Omega^{\omega}_{B+S+R} \; \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$\Sigma_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \Sigma'_{B+S+R}$

$$\frac{\text{(AM-Context-V145)}\quad \Phi_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \overline{\Phi}'_{B+S+R}}{\overline{\Phi}_{B+S+R} \cdot \Phi_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \overline{\Phi}_{B+S+R} \cdot \overline{\Phi}'_{B+S+R}}$$

$$\frac{\begin{array}{c}\text{(AM-v1-Rollback-V145)}\\ n' = 0 \text{ or p is stuck} \qquad \Phi_{B+S+R}\restriction^B = (\overline{\Phi}_B, \overline{\mathbb{R}}) \cdot (\langle p, ctr, \sigma, n\rangle, \mathbb{R}) \cdot (\langle p, ctr', \sigma', n'\rangle, \mathbb{R}')\\ \overline{\Phi}_B \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle \overset{\mathrm{rlb}_B \; ctr}{\dashrightarrow}_B \overline{\Phi}_B \cdot \langle p, ctr', \sigma, n\rangle\\ \overline{\Phi}_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \restriction^B = (\overline{\Phi}_B, \overline{\mathbb{R}}) \cdot (\langle p, ctr', \sigma, n\rangle, \mathbb{R})\end{array}}{\overline{\Phi}_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n'\rangle \overset{\mathrm{rlb}_B \; ctr}{\dashrightarrow}_{B+S+R} \overline{\Phi}_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}$$

$$\frac{\begin{array}{c}\text{(AM-v4-Rollback-V145)}\\ n' = 0 \text{ or p is stuck} \qquad \Phi_{B+S+R}\restriction^S = (\overline{\Phi}_S, \overline{\mathbb{R}}) \cdot (\langle p, ctr, \sigma, n\rangle, \mathbb{R}) \cdot (\langle p, ctr', \sigma', n'\rangle, \mathbb{R}')\\ \overline{\Phi}_S \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle \overset{\mathrm{rlb}_S \; ctr}{\dashrightarrow}_S \overline{\Phi}_S \cdot \langle p, ctr', \sigma, n\rangle\\ \overline{\Phi}_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \restriction^S = (\overline{\Phi}_S, \overline{\mathbb{R}}) \cdot (\langle p, ctr', \sigma, n\rangle, \mathbb{R})\end{array}}{\overline{\Phi}_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n'\rangle \overset{\mathrm{rlb}_S \; ctr}{\dashrightarrow}_{B+S+R} \overline{\Phi}_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}$$

(AM-v5-Rollback-V145)

$$\frac{n' = 0 \text{ or p is stuck} \quad \Phi_{B+S+R}\restriction^R = \overline{\Phi}_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n'\rangle \quad \overline{\Phi}_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n'\rangle \xrightarrow{\mathtt{rlb}_R\ ctr} \overline{\Phi}_R \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \quad \overline{\Phi}_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\restriction^R = \overline{\Phi}_R \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}{\overline{\Phi}_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n'\rangle \xrightarrow{\mathtt{rlb}_R\ ctr} \overline{\Phi}_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}$$

$$\boxed{\Phi_{B+S+R} \xrightarrow{\tau} \Phi'_{B+S+R}}$$

(AM-v1-step-V145)

$$\frac{\Phi_{B+S+R}\restriction^B = (\Phi_B, \mathbb{R}) \quad \Phi_B \xrightarrow{\tau} \overline{\Phi}'_B \quad \overline{\Phi}'_{B+S+R}\restriction^B = (\overline{\Phi}'_B, \mathbb{R})}{\Phi_{B+S+R} \xrightarrow{\tau} \overline{\Phi}'_{B+S+R}}$$

(AM-v4-step-V145)

$$\frac{\Phi_{B+S+R}\restriction^S = (\Phi_S, \mathbb{R}) \quad \Phi_S \xrightarrow{\tau} \overline{\Phi}'_S \quad \overline{\Phi}'_{B+S+R}\restriction^S = (\overline{\Phi}'_S, \mathbb{R})}{\Phi_{B+S+R} \xrightarrow{\tau} \overline{\Phi}'_{B+S+R}}$$

(AM-v5-step-V145)

$$\frac{\Phi_{B+S+R}\restriction^R \xrightarrow{\tau} \overline{\Phi}'_R \quad \overline{\Phi}'_{B+S+R} = \overline{\Phi}'_R\restriction^R}{\Phi_{B+S+R} \xrightarrow{\tau} \overline{\Phi}'_{B+S+R}}$$

$$\boxed{\Sigma_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma'_{B+S+R}}$$

(AM-Reflection-V145)

$$\frac{}{\Sigma_{B+S+R} \Downarrow^{\varepsilon}_{B+S+R} \Sigma_{B+S+R}}$$

(AM-Single-V145)

$$\frac{\Sigma_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma''_{B+S+R} \quad \Sigma''_{B+S+R} \xrightarrow{\tau} \Sigma'_{B+S+R}}{\Sigma_{B+S+R} \Downarrow^{\overline{\tau}\cdot\tau}_{B+S+R} \Sigma'_{B+S+R}}$$

Let us define what it means for a state to be initial or final.

$$\boxed{\textit{Helpers}}$$

(AM-Init-V145)

$$\frac{\Sigma_{B+S+R} = \varepsilon \cdot \langle p, 0, \sigma, \varepsilon, \bot\rangle \quad \sigma \in \textit{InitConf}}{\vdash \Sigma_{B+S+R} : \textit{init}}$$

(AM-Fin-V145)

$$\frac{\Sigma_{B+S+R} = \varepsilon \cdot \langle p, ctr, \sigma, \mathbb{R}, \bot\rangle \quad \sigma(\mathbf{pc}) = \bot}{\vdash \Sigma_{B+S+R} : \textit{fin}}$$

(V15:SE-Initial-State)

$$\frac{}{\Sigma^{\textit{init}}_{B+S+R}(p, \sigma) \coloneqq \langle p, 0, \sigma, \varepsilon, \bot\rangle}$$

$$\boxed{p \times \textit{InitConf} \Subset^{\omega}_{B+S+R} \overline{\tau}}$$

(AM-Trace-V145)

$$\frac{\exists \Sigma'_{B+S+R} \quad \vdash \Sigma'_{B+S+R} : \textit{fin} \quad \Sigma^{\textit{init}}_{B+S+R}(p, \sigma) \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma'_{B+S+R}}{p, \sigma \Subset^{\omega}_{B+S+R} \overline{\tau}}$$

(AM-Beh-V145)

$$\frac{}{\textit{Beh}^{B+S+R}_{\mathcal{A}}(p) = \{\overline{\tau} \mid \forall \sigma \in \textit{InitConf}.\ p, \sigma \Subset^{\omega}_{B+S+R} \overline{\tau}\}}$$

We define the behaviour of a program p, written $\textit{Beh}^{B+S+R}_{\mathcal{A}}(p)$, as the set of traces that are generated starting from an initial configuration σ.

F.8 Combined oracle semantics B + S + R

Note that we 'unfolded' the semantics. So instead of a pair of a pair ad a singleton, it really is 3 singletons.

$$\boxed{\textit{Judgements}}$$

$X_{B+S+R} \overset{\tau}{\rightsquigarrow}^{O_{B+S+R}}_{B+S+R} X'_{B+S+R}$	State X_{B+S+R} small-steps to X'_{B+S+R} and emits observation τ.
$\Psi_{B+S+R} \overset{\tau}{\rightsquigarrow}^{O_{B+S+R}}_{B+S+R} \overline{\Psi}'_{B+S+R}$	Speculative instance Ψ_{B+S+R} small-steps to $\overline{\Psi}_{B+S+R}{}'$ and emits observation τ.
$X_{B+S+R} \overset{O_{B+R}}{\Downarrow}{}^{B+S+R}_{\overline{\tau}} X'_{B+S+R}$	State X_{B+S+R} big-steps to X'_{B+S+R} and emits a list of observations $\overline{\tau}$.
$p \times \textit{InitConf} \Subset^{O}_{B+S+R} \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$$\boxed{X_{B+S+R} \overset{\tau}{\rightsquigarrow}^{O_{B+S+R}}_{B+S+R} X'_{B+S+R}}$$

(V145-SE-Context)

$$\frac{\Psi_{B+S+R} \overset{\tau}{\rightsquigarrow}^{O_{B+S+R}}_{B+S+R} \overline{\Psi}'_{B+S+R} \quad \Psi_{B+S+R} = \langle p, ctr, \sigma, \mathbb{R}, h, n+1\rangle \quad \text{if } p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \text{ then } \overline{\Psi}_{B+S+R}{}'' = \textit{zeroes}(\overline{\Psi}_{B+S+R}) \text{ else } \overline{\Psi}_{B+S+R}{}'' = \textit{decr}(\overline{\Psi}_{B+S+R})}{\overline{\Psi}_{B+S+R} \cdot \Psi_{B+S+R} \overset{\tau}{\rightsquigarrow}^{O_{B+S+R}}_{B+S+R} \overline{\Psi}_{B+S+R}{}'' \cdot \overline{\Psi}'_{B+S+R}}$$

$$\frac{\overline{\Psi}_{B+S+R} \cdot \Psi_{B+S+R\overline{\rho}\cdot\tau} \restriction^{B} \overset{\tau}{\rightsquigarrow}_{1}^{O_B} \overline{\Psi}_{B+S+R} \cdot \Psi_{B+S+R\overline{\rho}} \restriction^{B}}{\overline{\Psi}_{B+S+R} \cdot \Psi_{B+S+R\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}_{B+S+R}^{O_{B+S+R}} \overline{\Psi}_{B+S+R} \cdot \Psi_{B+S+R\overline{\rho}}} \text{(V145-SE:v1-General)}$$

$$\frac{\overline{\Psi}_{B+S+R} \cdot \Psi_{B+S+R\overline{\rho}\cdot\tau} \restriction^{S} \overset{\tau}{\rightsquigarrow}_{S}^{O_S} \overline{\Psi}_{B+S+R} \cdot \Psi_{B+S+R\overline{\rho}} \restriction^{S}}{\overline{\Psi}_{B+S+R} \cdot \Psi_{B+S+R\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}_{B+S+R}^{O_{B+S+R}} \overline{\Psi}_{B+S+R} \cdot \Psi_{B+S+R\overline{\rho}}} \text{(V145-SE:v4-General)}$$

$$\frac{\overline{\Psi}_{B+S+R} \cdot \Psi_{B+S+R\overline{\rho}\cdot\tau} \restriction^{R} \overset{\tau}{\rightsquigarrow}_{R}^{O_R} \overline{\Psi}_{B+S+R} \cdot \Psi_{B+S+R\overline{\rho}} \restriction^{R}}{\overline{\Psi}_{B+S+R} \cdot \Psi_{B+S+R\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}_{B+S+R}^{O_{B+S+R}} \overline{\Psi}_{B+S+R} \cdot \Psi_{B+S+R\overline{\rho}}} \text{(V145-SE:v5-General)}$$

$$\frac{n' = 0 \text{ or } p \text{ is stuck} \qquad \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n'\rangle^{m} \restriction^{B} \overset{\tau}{\rightsquigarrow}_{1}^{O_B} \langle p, ctr', \sigma, \mathbb{R}, h, n\rangle \restriction^{B}}{\overline{\Psi}_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n'\rangle^{(B,m)} \cdot \overline{\Psi}'_{B+S+R} \overset{\tau}{\rightsquigarrow}_{B+S+R}^{O_{B+S+R}} \overline{\Psi}_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, h, n\rangle} \text{(V145-SE:v1-Rollback)}$$

$$\frac{n' = 0 \text{ or } p \text{ is stuck} \qquad \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n'\rangle^{true} \restriction^{S} \overset{\tau}{\rightsquigarrow}_{S}^{O_S} \langle p, ctr', \sigma, \mathbb{R}, h, n\rangle \restriction^{S}}{\overline{\Psi}_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n'\rangle^{(S,true)} \cdot \overline{\Psi}'_{B+S+R} \overset{\tau}{\rightsquigarrow}_{B+S+R}^{O_{B+S+R}} \overline{\Psi}_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, h, n\rangle} \text{(V145-SE:v4-Rollback)}$$

$$\frac{n' = 0 \text{ or } p \text{ is stuck} \qquad \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n'\rangle^{m} \restriction^{R} \overset{\tau}{\rightsquigarrow}_{R}^{O_R} \langle p, ctr', \sigma, \mathbb{R}, h, n\rangle \restriction^{R}}{\overline{\Psi}_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n'\rangle^{(R,m)} \cdot \overline{\Psi}'_{B+S+R} \overset{\tau}{\rightsquigarrow}_{B+S+R}^{O_{B+S+R}} \overline{\Psi}_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, h, n\rangle} \text{(V145-SE:v5-Rollback)}$$

$$\frac{\langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0\rangle^{m} \restriction^{B} \overset{\tau}{\rightsquigarrow}_{1}^{O_B} \langle p, ctr', \sigma', \mathbb{R}', h', n\rangle \restriction^{B}}{\overline{\Psi}_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0\rangle^{(B,m)} \cdot \overline{\Psi}_{B+S+R}{}' \overset{\tau}{\rightsquigarrow}_{B+S+R}^{O_{B+S+R}} \overline{\Psi}_{B+S+R} \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n\rangle \cdot \overline{\Psi}_{B+S+R}{}'} \text{(V145-SE:v1-Commit)}$$

$$\frac{\langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0\rangle^{false} \restriction^{S} \overset{\tau}{\rightsquigarrow}_{S}^{O_S} \langle p, ctr', \sigma', \mathbb{R}', h', n\rangle \restriction^{S}}{\overline{\Psi}_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0\rangle^{(S,false)} \cdot \overline{\Psi}_{B+S+R}{}' \overset{\tau}{\rightsquigarrow}_{S+R}^{O_{S+R}} \overline{\Psi}_{B+S+R} \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n\rangle \cdot \overline{\Psi}_{B+S+R}{}'} \text{(V145-SE:v4-Commit)}$$

$$\frac{\langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0\rangle^{m} \restriction^{R} \overset{\tau}{\rightsquigarrow}_{R}^{O_R} \langle p, ctr', \sigma', \mathbb{R}', h', n\rangle \restriction^{R}}{\overline{\Psi}_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0\rangle^{(R,m)} \cdot \overline{\Psi}_{B+S+R}{}' \overset{\tau}{\rightsquigarrow}_{B+S+R}^{O_{B+S+R}} \overline{\Psi}_{B+S+R} \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n\rangle \cdot \overline{\Psi}_{B+S+R}{}'} \text{(V145-SE:v5-Commit)}$$

$$\boxed{\Psi_{B+S+R} \overset{\tau}{\rightsquigarrow}_{B+S+R}^{O_{B+S+R}} \Psi'_{B+S+R}}$$

$$\frac{O_{B+S+R} = (O_B, O_S, O_R) \qquad \Psi_{B+S+R} \restriction^{B} \overset{\tau}{\rightsquigarrow}_{1}^{O_B} \overline{\Psi}'_{B+S+R} \restriction^{B}}{\Psi_{B+S+R} \overset{\tau}{\rightsquigarrow}_{B+S+R}^{O_{B+S+R}} \overline{\Psi}'_{B+S+R}} \text{(V145-SE:v1-step)}$$

$$\frac{O_{B+S} = (O_B, O_S, O_R) \qquad \Psi_{B+S} \restriction^{S} \overset{\tau}{\rightsquigarrow}_{S}^{O_S} \overline{\Psi}'_{B+S} \restriction^{S}}{\Psi_{B+S} \overset{\tau}{\rightsquigarrow}_{B+S}^{O_{B+S}} \overline{\Psi}'_{B+S}} \text{(V145-SE:v4-step)}$$

$$\frac{O_{B+S+R} = (O_B, O_S, O_R) \qquad \Psi_{B+S+R} \restriction^{R} \overset{\tau}{\rightsquigarrow}_{R}^{O_R} \overline{\Psi}'_{B+S+R} \restriction^{R}}{\Psi_{B+S+R} \overset{\tau}{\rightsquigarrow}_{B+S+R}^{O_{B+S+R}} \overline{\Psi}'_{B+S+R}} \text{(V145-SE:v5-step)}$$

$$\boxed{X_{B+S+R} \overset{O_{B+R}}{\Downarrow}_{\overline{\tau}}^{B+S+R} X'_{B+S+R}}$$

$$\frac{}{X_{B+S+R} \overset{O_{B+R}}{\Downarrow}_{\varepsilon}^{B+S+R} X_{B+S+R}} \text{(V145-SE:Reflection)}$$

$$\frac{X_{B+S+R} \overset{O_{B+R}}{\Downarrow}_{\overline{\tau}}^{B+S+R} X''_{B+S+R} \qquad X''_{B+S+R} \overset{\tau}{\rightsquigarrow}_{B+S+R}^{O_{B+S+R}} X'_{B+S+R}}{X_{B+S+R} \overset{O_{B+R}}{\Downarrow}_{\overline{\tau}\cdot\tau}^{B+S+R} X'_{B+S+R}} \text{(V145-SE:Single)}$$

Let us define what it means for a state to be initial or final.

Definition 29 (V145-SE: initial speculative state). *A speculative state X_{B+S+R} is initial, written $\vdash X_{B+S+R} : init$, iff*

$$\frac{X_{B+S+R} = \overline{\Psi}_{B+S+R} \cdot \Psi_{B+S+R} \qquad \overline{\Psi}_{B+S+R} = \varepsilon \qquad \Psi_{B+S+R} = \langle p, 0, \sigma, \varepsilon, \varepsilon, \bot\rangle \qquad \sigma \in InitConf}{\vdash X_{B+S+R} : init} \text{(V145-SE:Init)}$$

Definition 30 (V145-SE: Final speculative state). *A speculative state X_{B+S+R} is final, written $\vdash X_{B+S+R} : fin$, iff*

$$\frac{X_{\mathrm{B+S+R}} = \overline{\Phi}_{\mathrm{B+S+R}} \cdot \Psi_{\mathrm{B+S+R}} \qquad \overline{\Psi}_{\mathrm{B+S+R}} = \varepsilon \qquad \Psi_{\mathrm{B+S+R}} = \langle p, ctr, \sigma, \mathbb{R}, h, \bot \rangle \qquad \sigma(\mathbf{pc}) = \bot}{\vdash X_{\mathrm{B+S+R}} : fin} \text{(V145-SE:Fin)}$$

Definition 31 (V145-SE: Creating initial states)**.** *We define a function* $X^{init}_{\mathrm{B+S+R}}() : p \times \sigma \to \Sigma_{\mathrm{B+S+R}}$ *that creates an initial speculative state from a program* p *and initial configuration* $\sigma \in InitConf$

$$X^{init}_{\mathrm{B+S+R}}(p, \sigma) := \langle p, 0, \sigma, \varepsilon, \varepsilon, \bot \rangle$$

By definition we have $\forall p, \sigma \in InitConf . \vdash X^{init}_{\mathrm{B+S+R}}(p, \sigma) : init$

$$\frac{}{\boxed{p \times InitConf \; \text{👻}^{O}_{\mathrm{B+S+R}} \; \overline{\tau}}} \qquad \frac{\exists X'_{\mathrm{B+S+R}} \qquad \vdash X'_{\mathrm{B+S+R}} : fin \qquad X^{init}_{\mathrm{B+S+R}}(p, \sigma) \; {}^{O_{\mathrm{B+R}}}\!\!\downarrow^{\mathrm{B+S+R}}_{\overline{\tau}} \; X'_{\mathrm{B+S+R}}}{p, \sigma \; \text{👻}^{O}_{\mathrm{B+S+R}} \; \overline{\tau}} \text{(V145-SE:Trace)}$$

$$\frac{}{Beh^{\mathrm{B+S+R}}_{\mathcal{A}}(p) = \{\overline{\tau} \mid \forall \sigma \in InitConf . \; p, \sigma \; \text{👻}^{O}_{\mathrm{B+S+R}} \; \overline{\tau}\}} \text{(V145-SE:Beh)}$$

We define more fine grained projection functions $\restriction^R$, $\restriction^S$ and $\restriction^B$ on traces:

Definition 32 (Trace projection of V1)**.**

$$
\begin{aligned}
\varepsilon\restriction^B &= \varepsilon \\
\overline{\tau}\cdot \mathtt{start_S}\ i\restriction^B &= \overline{\tau}\restriction^B \\
\overline{\tau}\cdot \mathtt{start_R}\ i\restriction^B &= \overline{\tau}\restriction^B \\
\overline{\tau}\cdot \mathtt{rlb_S}\ i\restriction^B &= helper_B(\overline{\tau}, i) \\
\overline{\tau}\cdot \mathtt{rlb_R}\ i\restriction^B &= helper_B(\overline{\tau}, i) \\
\overline{\tau}\cdot \tau\restriction^B &= \overline{\tau}\restriction^B\cdot\tau \ otherwise
\end{aligned}
$$

$$
\begin{aligned}
helper_B(\varepsilon, id) &= \varepsilon \\
helper_B(\overline{\tau}\cdot \mathtt{start_S}\ id, id) &= \overline{\tau}\restriction^B \\
helper_B(\overline{\tau}\cdot \mathtt{start_R}\ id, id) &= \overline{\tau}\restriction^B \\
helper_B(\overline{\tau}\cdot o, id) &= helper_B(\overline{\tau}, id)\ otherwise
\end{aligned}
$$

Definition 33 (Trace projection of V4)**.**

$$
\begin{aligned}
\varepsilon\restriction^S &= \varepsilon \\
\overline{\tau}\cdot \mathtt{start_B}\ i\restriction^S &= \overline{\tau}\restriction^S \\
\overline{\tau}\cdot \mathtt{start_R}\ i\restriction^S &= \overline{\tau}\restriction^S \\
\overline{\tau}\cdot \mathtt{rlb_B}\ i\restriction^S &= helper_S(\overline{\tau}, i) \\
\overline{\tau}\cdot \mathtt{rlb_R}\ i\restriction^S &= helper_S(\overline{\tau}, i) \\
\overline{\tau}\cdot \tau\restriction^S &= \overline{\tau}\restriction^S\cdot\tau \ otherwise
\end{aligned}
$$

$$
\begin{aligned}
helper_S(\varepsilon, id) &= \varepsilon \\
helper_S(\overline{\tau}\cdot \mathtt{start_B}\ id, id) &= \overline{\tau}\restriction^S \\
helper_S(\overline{\tau}\cdot \mathtt{start_R}\ id, id) &= \overline{\tau}\restriction^S \\
helper_S(\overline{\tau}\cdot o, id) &= helper_S(\overline{\tau}, id)\ otherwise
\end{aligned}
$$

Definition 34 (Trace projection of V5)**.**

$$
\begin{aligned}
\varepsilon\restriction^R &= \varepsilon \\
\overline{\tau}\cdot \mathtt{start_B}\ i\restriction^R &= \overline{\tau}\restriction^R \\
\overline{\tau}\cdot \mathtt{start_S}\ i\restriction^R &= \overline{\tau}\restriction^R \\
\overline{\tau}\cdot \mathtt{rlb_B}\ i\restriction^R &= helper_R(\overline{\tau}, i) \\
\overline{\tau}\cdot \mathtt{rlb_S}\ i\restriction^R &= helper_R(\overline{\tau}, i) \\
\overline{\tau}\cdot \tau\restriction^R &= \overline{\tau}\restriction^R\cdot\tau \ otherwise
\end{aligned}
$$

$$
\begin{aligned}
helper_R(\varepsilon, id) &= \varepsilon \\
helper_R(\overline{\tau}\cdot \mathtt{start_B}\ id, id) &= \overline{\tau}\restriction^R \\
helper_R(\overline{\tau}\cdot \mathtt{start_S}\ id, id) &= \overline{\tau}\restriction^R \\
helper_R(\overline{\tau}\cdot o, id) &= helper_R(\overline{\tau}, id)\ otherwise
\end{aligned}
$$

We define a projection function on traces that deletes all speculative transactions:

Definition 35 (Non-speculative projection). *We define the non-speculative projection mutually recursive as*

$$\begin{aligned}
\varepsilon\restriction_{ns} &= \varepsilon \\
\overline{\tau}\cdot \texttt{commit}_x\ n\restriction_{ns} &= \overline{\tau}\restriction_{ns} \\
\overline{\tau}\cdot \texttt{start}_x\ n\restriction_{ns} &= \overline{\tau}\restriction_{ns} \\
\overline{\tau}\cdot \texttt{rlb}_x\ id\restriction_{ns} &= helper(\overline{\tau}, id) \\
\overline{\tau}\cdot o\restriction_{ns} &= \overline{\tau}\restriction_{ns}\cdot o\ otherwise
\end{aligned}$$

The $helper()$ is defined as

$$\begin{aligned}
helper(\varepsilon, id) &= \varepsilon \\
helper(\overline{\tau}\cdot \texttt{start}\ id, id) &= \overline{\tau}\restriction_{ns} \\
helper(\overline{\tau}\cdot o, id) &= helper(\overline{\tau}, id)\ otherwise
\end{aligned}$$

Now some facts about these trace projections that follow from their definitions.

Lemma 7 (V45: Commutativity of speculative projections). *Let $\overline{\tau}$ be a trace generated by a program run. Then $\overline{\tau}\restriction^S\restriction^R = \overline{\tau}\restriction^R\restriction^S$*

Lemma 8 (V14: Commutativity of speculative projections). *Let $\overline{\tau}$ be a trace generated by a program run. Then $\overline{\tau}\restriction^S\restriction^B = \overline{\tau}\restriction^B\restriction^S$*

Lemma 9 (V15: Commutativity of speculative projections). *Let $\overline{\tau}$ be a trace generated by a program run. Then $\overline{\tau}\restriction^B\restriction^R = \overline{\tau}\restriction^R\restriction^B$*

We can relate for each combined semantics a combination of these projections to the non-speculative projection. All of these properties follow from the definitions of the projections functions.

Lemma 10 (V45: Relating speculative projections to non-speculative projection). *Let $(p,\sigma)\ \text{👻}^{\omega}_{\text{S+R}}\ \overline{\tau}$. Then $\overline{\tau}\restriction^S\restriction^R = \overline{\tau}\restriction_{ns}$.*

Lemma 11 (V14: Relating speculative projections to non-speculative projection). *Let $(p,\sigma)\ \text{👻}^{\omega}_{\text{B+S}}\ \overline{\tau}$. Then $\overline{\tau}\restriction^S\restriction^B = \overline{\tau}\restriction_{ns}$.*

Lemma 12 (V15: Relating speculative projections to non-speculative projection). *Let $(p,\sigma)\ \text{👻}^{\omega}_{\text{B+R}}\ \overline{\tau}$. Then $\overline{\tau}\restriction^B\restriction^R = \overline{\tau}\restriction_{ns}$.*

Lemma 13 (V145 Relating speculative projections to non-speculative projection). *Let $(p,\sigma)\ \text{👻}^{\omega}_{\text{B+S+R}}\ \overline{\tau}$. Then $\overline{\tau}\restriction^S\restriction^R\restriction^B = \overline{\tau}\restriction_{ns}$.*

Note that applying to different speculative projections will always result in the non-speculative projection

Lemma 14. *Let $\overline{\tau}$ be trace generated by a program run from one of our semantics. Then $\overline{\tau}\restriction^S\restriction^R\restriction^B = \overline{\tau}\restriction^R\restriction^B$.*

Some more Lemmas relating the behaviour of the speculative projection functions to the non-speculative one.

Lemma 15 (V4: speculative-projections equal to non-speculative Projections). *Let $(p,\sigma)\ \text{👻}^{\omega}_{\text{S}}\ \overline{\tau}$. Then $\overline{\tau}\restriction^R = \overline{\tau}\restriction_{ns}$ and $\overline{\tau}\restriction^B = \overline{\tau}\restriction_{ns}$.*

Lemma 16 (V5: speculative-projections equal to non-speculative Projections). *Let $(p,\sigma)\ \text{👻}^{\omega}_{\text{R}}\ \overline{\tau}$. Then $\overline{\tau}\restriction^B = \overline{\tau}\restriction_{ns}$ and $\overline{\tau}\restriction^S = \overline{\tau}\restriction_{ns}$.*

G PROOFS

H RELATION SYMBOLIC AND CONCRETE NON-SPECULATIVE SEMANTICS

We need to extend the Soundness (Lemma 8) and Completeness (Lemma 10) proofs of Spectector to include the new rules for call and return.

H.0.1 Soundness. We define the short hand notation $\mu(\sigma_{\mathcal{S}}) = \langle \mu(sm), \mu(sa)\rangle$ where $\sigma_{\mathcal{S}} = \langle sm.sa, \delta^{\mathcal{S}}\rangle$.

Lemma 17 (Non-spec: Soundness to symbolic)**.** *If*

(1) $\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}{}^{\mathcal{S}} \sigma'_{\mathcal{S}}$ *and*
(2) $\mu \vDash pthCnd(\tau_{\mathcal{S}})$

Then

I $\mu(\sigma) \xrightarrow{\mu(\tau_{\mathcal{S}})} \mu(\sigma'_{\mathcal{S}})$ *and*

Proof. We proceed by inversion on $\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}{}^{\mathcal{S}} \sigma'_{\mathcal{S}}$:

Rule Call-Symb Then $p(sa(pc)) = \textbf{call}\ f$ and since **pc** and function names f are always concrete $p(\mu(\sigma_{\mathcal{S}})) = \textbf{call}\ f$ as well. Furthermore, $sa' = sa[\textbf{pc} \mapsto n, \textbf{sp} \mapsto sa(\textbf{sp}) - 8]$ and $sm' = \textbf{write}(sm, sa(\textbf{pc}) + 1, sa'(\textbf{sp}))$ with $\mathcal{F}(f) = n$ with $\tau_{\mathcal{S}} = \texttt{call}\ f$
Now, we apply Rule Call on $\mu(\sigma_{\mathcal{S}})$ and get $\mu(\sigma_{\mathcal{S}}) \xrightarrow{\texttt{call}\ f} \langle p, \langle m', a'\rangle\rangle$ with $a' = \mu(sa)[\textbf{pc} \mapsto n, \textbf{sp} \mapsto \mu(sa)(\textbf{sp}) - 8]$.
From this and the fact that **sp** is always concrete we have $\mu(sa') = a'$.
Now, $m' = \mu(sm')[\mu(sa')(\textbf{sp}) \mapsto \mu(sa)(\textbf{pc}) + 1]$ which again follows from **sp** and **pc** to be concrete.

Rule Ret-Concr Then $p(sa(pc)) = \textbf{ret}$ and since **pc** is always concrete $p(\mu(\sigma_{\mathcal{S}}) = \textbf{ret}$ as well.
We have $l = \textbf{read}(sm, sa(\textbf{sp}))$ and $l \in Vals$ and $sa' = sa[\textbf{pc} \mapsto l, \textbf{sp} \mapsto sa(\textbf{sp}) + 8]$ and $\texttt{symPc}(\top)$. Let $\mu()$ be an arbitrary valuation (since $\mu \vDash pthCnd(\tau_{\mathcal{S}}) = \top$).
We can apply Rule Ret and get $\mu(\sigma_{\mathcal{S}}) \xrightarrow{\texttt{ret}\ l'} \sigma'$.
First note that $l = l'$, since **sp** is concrete and thus $\mu(sa') = \mu(sa)[\textbf{pc} \mapsto l, \textbf{sp} \mapsto \mu(sa)(\textbf{sp})]$
We now have $\sigma' = \langle p, \langle \mu(sm), \mu(sa')\rangle\rangle$ and are finished.

Rule Ret-Symb Then $p(sa(pc)) = \textbf{ret}$ and since **pc** is always concrete $p(\mu(\sigma_{\mathcal{S}}) = \textbf{ret}$ as well.
We have $l = \textbf{read}(sm, sa(\textbf{sp}))$ and $l \notin Vals$ and $sa' = sa[\textbf{pc} \mapsto l', \textbf{sp} \mapsto sa(\textbf{sp}) + 8]$ and $\texttt{symPc}(l = l')$, where $l' \in Vals$.
We can apply Rule Ret and get $\mu(\sigma_{\mathcal{S}}) \xrightarrow{\mu(\texttt{ret}\ l')} \sigma'$.
Since $\mu(l) = l'$ we can proceed analogously to the case above and are finished.

□

H.0.2 Completeness.

Lemma 18 (Non-spec : Completeness to symbolic)**.** *If*

(1) $\sigma \in InitConf$ *and*
(2) $\sigma \xrightarrow{\tau} \sigma'$ *and*
(3) $\mu(sm) = m$ *and* $\mu(sa) = a$

Then

I $\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}{}^{\mathcal{S}} \sigma'_{\mathcal{S}}$ *and*
II $\sigma'_{\mathcal{S}} = \langle sm', sa'\rangle$ *and*
III $\mu(sm') = \sigma'.m$ *and* $\mu(sa') = \sigma'.a$ *and* $\mu(\tau_{\mathcal{S}}) = \tau$ *and*
IV $\mu \vDash pthCnd(\tau_{\mathcal{S}})$

Proof. We proceed by inversion on $\sigma \xrightarrow{\tau} \sigma'$.

Rule Call Then $p(a(\textbf{pc})) = \textbf{call}\ f, \mathcal{F}(f) = n, a' = a[\textbf{pc} \mapsto n, \textbf{sp} \mapsto a(\textbf{sp}) - 8]$ and $m' = m[a'(\textbf{sp}) \mapsto a(\textbf{pc}) + 1]$.
Since **pc** is always concrete, $p(sa(\textbf{pc})) = \textbf{call}\ f$ as well.
We use Rule Call-Symb to derive a step $\langle p, \langle sm, sa\rangle\rangle \xrightarrow{\texttt{call}\ f}{}^{\mathcal{S}} \sigma'_{\mathcal{S}}$ with $sa' = sa[\textbf{pc} \mapsto n, \textbf{sp} \mapsto sa(\textbf{sp}) - 8]$ and $sm' = \textbf{write}(sm, sa(\textbf{pc}) + 1, sa'(\textbf{sp}))$ and $\mu \vDash pthCnd(\sigma'_{\mathcal{S}}) = \top$.
Now applying Lemma 7 from Spectector we get $\mu(sa') = \mu(sa)[\textbf{pc} \mapsto \mu(sa(\textbf{pc}+1))] = a[\textbf{pc} \mapsto a(\textbf{pc})+1]$. Now, again using Lemma 7, $\mu(sm') = \mu(\textbf{write}(sm, sa(\textbf{pc}) + 1, sa'(\textbf{sp}))) = \mu(sm)[\mu(sa'\textbf{sp}) \mapsto \mu(sa(\textbf{pc}) + 1)] = m[a'(\textbf{sp}) \mapsto a(\textbf{pc}) + 1]$

Rule Ret Then $p(a(\textbf{pc})) = \textbf{ret}, l = m(a(\textbf{sp}))$ and $a' = a[\textbf{pc} \mapsto l, \textbf{sp} \mapsto a(\textbf{sp}) + 8]$.
Since **pc** is always concrete, $p(sa(\textbf{pc})) = \textbf{ret}$ as well.
There are two cases now:

$l' = sm(sa(\mathbf{sp})) \in \mathit{Vals}$ We proceed by applying Rule Ret-Concr and get $\langle p, \langle sm, sa\rangle\rangle \xrightarrow{\texttt{call}\ f}^{\mathcal{S}} \sigma'_{\mathcal{S}}$ with $sa' = sa[\mathbf{pc} \mapsto l', \mathbf{sp} \mapsto sa(\mathbf{sp}) + 8]$ and $\texttt{symPc}(\top)$; thus $\mu \vDash \mathit{pthCnd}(\sigma'_{\mathcal{S}}) = \top$.
Observe that $\mathbf{read}(sm, sa(\mathbf{sp}) = l' = l$ since $\mu(sm) = m$ and $\mu(sa) = a$. Then $\mu(sa') = \mu(sa)[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto sa(\mathbf{sp}) + 8] = a[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto sa(\mathbf{sp}) + 8] = a'$ (using Lemma 7 of Spectector) From $m' = m$, $\mu(m) = sm$ and $sm = sm'$ we get $\mu(sm') = m'$.

$l' = sm(sa(\mathbf{sp})) \notin \mathit{Vals}$ We proceed by applying Rule Ret-Symb where we pick l as the target label and get $\langle p, \langle sm, sa\rangle\rangle \xrightarrow{\texttt{call}\ f}^{\mathcal{S}} \sigma'_{\mathcal{S}}$ with $sa' = sa[\mathbf{pc} \mapsto l', \mathbf{sp} \mapsto sa(\mathbf{sp}) + 8]$ and $\texttt{symPc}(l' = l)$
Then $\mu(sa') = \mu(sa)[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto sa(\mathbf{sp}) + 8] = a[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto sa(\mathbf{sp}) + 8] = a'$ (using Lemma 7 of Spectector) From $m' = m$, $\mu(m) = sm$ and $sm = sm'$ we get $\mu(sm') = m'$.
Since $\mu \vDash \mathit{pthCnd}(\sigma'_{\mathcal{S}}) = \texttt{symPc}(sm(sa(\mathbf{sp}) = l)$ (unfolding symread), we need to show $\mu(sm(sa(\mathbf{sp}))) = l$. Applying Lemma 7 and using the assumptions, we end at $m(a(\mathbf{sp})) = l$ and are finished.

□

I GENERAL FACTS

These definitions are just written with S in mind. But talk about general facts of speculation. Since there is no insight gained by copying these, we omit them here.

Definition 36 (Dot notation)**.** *In the following, we use a dot notation to refer to components of a speculative instance Ψ_S/Φ_S. For example, we write $\Psi_S.ctr$ to refer to ctr inside the instance Ψ_S.*

We lift this notation to speculative states X_S and Σ_S in the following way: we write $\Sigma_S \cdot \sigma$ to denote the configuration σ of the topmost speculative instance Φ_S of the speculative state Σ_S. For example if $\Sigma_S = \overline{\Phi}_S \cdot \Phi_S$ then $\Sigma_S.\sigma$ refers to $\Phi_S.\sigma$.

Definition 37 (No ongoing transactions that will be rolled back)**.** *A speculative state X_S has no ongoing transactions that will be rolled back, iff*

(SE-V4-no-ongoing-transaction-rolled)

$$\frac{\begin{array}{c}\exists X'_S \quad \vdash X'_S : \mathit{fin} \quad X_S {\overline{\rho}}^{O}\!\downarrow^{S}_{\overline{\tau}} X'_S \\ \forall \texttt{rlb}\ i \in \overline{\tau}.\ \exists \texttt{start}\ i \in \overline{\tau} \\ \nexists \texttt{start}\ id \in \overline{\rho}.\ \texttt{rlb}\ id \in \overline{\tau}\end{array}}{\vdash_O X_S \overline{\rho} : \mathit{noongoing}}$$

The last premise tells us that all started speculative transactions that will be rolled back were created in the execution $X_S \, {}^{O}\!\downarrow^{S}_{\overline{\tau}} X'_S$. Since X'_S is a final state, there are no more ongoing transactions. In conclusion, we know that there are no more unfinished transactions that will be rolled in X_S because we did not find a rlb *i for that transaction in the trace $\overline{\tau}$. Note that the final state is unique by Lemma 19 (Uniqueness final state).*

Definition 38 (Ongoing transactions that will be rolled back)**.** *A speculative execution $X_S \, {}^{O}\!\downarrow^{S}_{\overline{\tau}} X''_S$ has ongoing transactions that will be rolled back, iff*

(SE-V4-ongoing-transaction-rolled-closed)

$$\frac{\begin{array}{c}\exists X'_S \quad \vdash X'_S : \mathit{fin} \quad X''_S \, {}^{O}\!\downarrow^{S}_{\overline{\tau}'} X'_S \\ \exists.\ \texttt{rlb}\ id' \in \overline{\tau}.\ \forall \texttt{start}\ id \in \overline{\tau}'\ id \neq id'\end{array}}{\vdash_O X_S \, {}^{O}\!\downarrow^{S}_{\overline{\tau}} X''_S : \mathit{ongoingtransactionrolledback}}$$

By Lemma 19 (Uniqueness final state) the state X'_S is unique for the given oracle O.

Definition 39 (Oldest ongoing transaction that will be rolled back)**.** *A speculative state X_S has an oldest ongoing transaction that will be rolled back, iff*

(SE-V4-ongoing-transaction-rolled-closed-oldest)

$$\frac{\begin{array}{c}\exists X'_S \quad \vdash X'_S : \mathit{fin} \quad X''_S \, {}^{O}\!\downarrow^{S}_{\overline{\tau}'} X'_S \\ \exists.\ \texttt{rlb}\ id' \in \overline{\tau}.\ \forall \texttt{start}\ id \in \overline{\tau}'\ id \neq id' \\ \forall\ \texttt{rlb}\ j \nexists \texttt{start}\ j\ \exists\ \texttt{rlb}\ i \nexists \texttt{start}\ i \wedge i \leq j\end{array}}{\vdash^{i}_{O} X_S : \mathit{biggestongoingtransactionirolledback}}$$

has to exist because traces are finite.

Definition 40 (Case when $\restriction_{ns}$ is linear)**.**

$$\overline{\tau}\restriction_{ns} \cdot \overline{\tau}'\restriction_{ns} = \overline{\tau} \cdot \overline{\tau}'\restriction_{ns}$$

iff, $\forall.\ \texttt{rlb}\ id \in \overline{\tau}'.\ \texttt{start}\ id \in \overline{\tau}'$.

Definition 41 (Cases when Helper is linear). *Let $\overline{\tau} = \overline{\tau}' \cdot \tau$ be a trace. Then*

$$helper(\overline{\tau}', i) \cdot helper(\tau, i) = helper(\overline{\tau}' \cdot \tau, i)$$

iff, $\tau \neq$ `rlb` id forall $id \in \mathbb{N}$.

Definition 42. *If $\overline{\tau}'$ is a prefix of $\overline{\tau}$ and $X_S \overset{O}{\downarrow}_{\overline{\tau}} X'_S$, then there exists X^1_S such that $X_S \overset{O}{\downarrow}_{\overline{\tau}'} X^1_S \overset{O}{\downarrow}_{\overline{\tau}''} X'_S$, where $\overline{\tau} = \overline{\tau}' \cdot \overline{\tau}''$.*

Definition 43. *A speculative state X_S either has no ongoing transactions that need to be rolled back or it has ongoing transactions that need to be rolled back.*

Definition 44 (Well orderedness of rollback and start). *If there are* `start` *i*, `rlb` *$i \in \overline{\tau}$, Then $\overline{\tau} = \overline{\tau}' \cdot$* `rlb` *$i\overline{\tau}''$, the* `start` *$i \in \overline{\tau}'$.*
The `start` *i appears before the corresponding* `rlb` *i in the trace.*

Definition 45 (low-equivalent configurations w.r.t policy P). *Two configurations σ, σ' are indistinguishable with respect to a policy P, written $\sigma \sim_P \sigma'$, iff they agree on all registers and memory locations in P.*

Lemma 19 (Uniqueness final state). *If*

(1) X_S is a speculative state and
(2) O is an oracle and
(3) There exists X'_S, X''_S and
(4) $\vdash X'_S$: fin and $\vdash X''_S$: fin and
(5) $X_S \overset{O}{\downarrow}_{\overline{\tau}} X'_S$ and $X_S \overset{O}{\downarrow}_{\overline{\tau}'} X''_S$

Then

I $X'_S = X''_S$

Proof. Since $\vdash X'_S$: *fin* and $\vdash X''_S$: *fin* we know by definition that $X'_S = \langle p, ctr', \sigma', h', \bot\rangle$ and $X''_S = \langle p, ctr'', \sigma'', h'', \bot\rangle$. We need to show

I $ctr' = ctr''$ and
II $h' = h''$ and
III $\sigma' = \sigma''$

I Since the program p is the same, we know that the same amount of **store** x, e instructions are executed. For each **store** , instruction we use either Rule S:Store-Skip or Rule S:Store-Exe and both increase the ctr by 1. Since execution started in the same state X_S and we encounter the same amount of store instructions in $X_S \overset{O}{\downarrow}_{\overline{\tau}} X'_S$ and $X_S \overset{O}{\downarrow}_{\overline{\tau}'} X''_S$ we have that $ctr' = ctr''$.

II Because the oracle used is the same for both executions $X_S \overset{O}{\downarrow}_{\overline{\tau}} X'_S$ and $X_S \overset{O}{\downarrow}_{\overline{\tau}'} X''_S$, we make the same decisions at each **store** , instruction. Since we encounter the same amount of **store** , instructions and we started execution from the same initial state X_S, we have $h' = h''$

III Because the oracle used is the same for both executions $X_S \overset{O}{\downarrow}_{\overline{\tau}} X'_S$ and $X_S \overset{O}{\downarrow}_{\overline{\tau}'} X''_S$ and the executions start from the same state X_S, we have that the exact same steps are taken in both executions. From this we have $\sigma' = \sigma''$.

□

Lemma 20 (Commits do not change the topmost configuration). *If*

(1) $X_S \overset{O}{\downarrow}_{\overline{\tau}} X'_S$ and
(2) $\overline{\tau} =$ `commit` *$id_1 \cdot \cdots \cdot$* `commit` *id_n for some $n \geq 1$*

Then

I $X_S.\sigma = X'_S.\sigma$ and
II $\overline{\tau}\restriction_{ns} = \varepsilon$

Proof. We have

(1) $X_S \overset{O}{\downarrow}_{\overline{\tau}} X'_S$ and
(2) $\overline{\tau} =$ `commit` $id_1 \cdot \cdots \cdot$ `commit` id_n for some n

We now need to proof that $X_S.\sigma = X'_S.\sigma$ and $\overline{\tau}\restriction_{ns} = \varepsilon$.

I $X_S.\sigma = X'_S.\sigma$ For $X_S.\sigma = X'_S.\sigma$ notice that $X'_S.\sigma$ is the configuration for the topmost instance in the state X'_S. We now do a case analysis if that state was committed or not

topmost instance was not committed If the instance is not committed, then it will still be at the top, because Rule S:Commit only changes the instance before the previous instance.

topmost instance was committed If the topmost instance in X'_S is committed, then the configuration $X'_S.\sigma$ is still at the top, because the Rule S:Commit only updates the previous instance with the configuration σ, h and the ctr of the committed instance. We thus preserve $X'_S.\sigma$.

II $\overline{\tau}\restriction_{ns} = \varepsilon$ Follows from the definition of $\restriction_{ns}$.
This completes the proof. □

Lemma 21 (V4: Reaching Final state from final configuration)**.** *If*

(1) $X_S.\sigma \in FinalConf$ *and*
(2) $\vdash X_S : nounfinishedtransactionsrolledback$ *and*
(3) $|X_S| \geq 1$

Then

I $X_S \overset{O}{\Downarrow_{\overline{\tau}}^{S}} X'_S$ *and*
II $\forall \tau \in \overline{\tau}.\, \tau = \texttt{commit}\ id$ *for some* $id \in \mathbb{N}$ *and*
III $\vdash X'_S : fin$
IV $X_S.\sigma = X'_S.\sigma$

Proof. Induction on the size of $|X_S|$.

$|X_S| = 1$ **I** Then we derive $X_S \overset{O}{\Downarrow_{\overline{\tau}}^{S}} X'_S$ by Rule S:Reflection and have $X'_S = X_S$.
II Trivial, since $\overline{\tau} = \varepsilon$.
III Since $|X_S| = 1$, we have $X_S.n = \bot$. We can now derive $\vdash X_S : fin$, since $X_S.\sigma \in FinalConf$.
Because $X_S = X'_S$, we have $\vdash X'_S : fin$ and are finished.
IV Trivial, since $X_S = X'_S$.

$|X_S| = n + 1$ **with** $n > 0$ By $|X_S| > 1$ and $\vdash X_S : nounfinishedtransactionsrolledback$ we know that there are transactions that still need to be committed.
Since $X_S.\sigma \in FinalConf$, we know that the only rule that applies is Rule S:Commit. Thus, $X_S \overset{\texttt{commit}\ id}{\rightsquigarrow_S^O} X''_S$
Applying Rule S:Commit does not change topmost configuration (Lemma 20 (Commits do not change the topmost configuration)). So, we have $X''_S.\sigma = X_S.\sigma$.
We now apply IH on X''_S, since $|X''_S| = n$. We get

(1) $X''_S \overset{O}{\Downarrow_{\overline{\tau}'}^{S}} X'_S$ and
(2) $\forall \tau \in \overline{\tau}'.\, \tau = \texttt{commit}\ id$ for some $id \in \mathbb{N}$ and
(3) $\vdash X'_S : fin$

I We construct an execution $X_S \overset{O}{\Downarrow_{X'_S}^{S}}$ by Rule S:Single with $X_S \overset{\texttt{commit}\ id}{\rightsquigarrow_S^O} X''_S$ and $X''_S \overset{O}{\Downarrow_{\overline{\tau}'}^{S}} X'_S$.
II Here $\overline{\tau} = \texttt{commit}\ id \cdot \overline{\tau}'$. By IH we know that $\overline{\tau}'$ fulfills the condition. Thus, $\overline{\tau}$ trivially fulfills condition as well.
III By IH.
IV By Lemma 20 (Commits do not change the topmost configuration).

□

Definition 46 (Counting transaction that will be committed)**.** *We define a function* $count()$. *that counts all transaction that will be committed with a speculation window of* 0.

$$count() : X_S \mapsto \mathbb{N}$$
$$count(\varepsilon) = 0$$
$$count(\overline{\Psi}_S \cdot (p, ctr, \sigma, h, 0)^{false}) = count(\overline{\Psi}_S) + 1$$
$$count(\overline{\Psi}_S \cdot (p, ctr, \sigma, h, n) = count(\overline{\Psi}_S)$$

Lemma 22 (V4: Executing a chain of commits)**.** *If*

(1) no transaction that will be rolled back with speculation window 0 *in* X_S

Then there exists X'_S *such that*

(1) $X_S \overset{O}{\Downarrow_{\overline{\tau}}^{S}} X'_S$
(2) $minWndw(X'_S) > 0$
(3) $\forall \tau \in \overline{\tau}.\, \tau = \texttt{commit}\ id$ *for some* $id \in \mathbb{N}$
(4) $X_S.\sigma = X'_S.\sigma$

Proof. The proof proceeds in a similar fashion to Lemma 21 (V4: Reaching Final state from final configuration). By induction on the size of $count(X_S)$.

$count(X_S) = 0$ **I** Then we derive $X_S \overset{O}{\Downarrow_{\overline{\tau}}^{S}} X'_S$ by Rule S:Reflection and have $X'_S = X_S$.
II Because $\vdash_O X'_S : noongoing$ and $count(X'_S) = 0$, there cannot be a transaction with speculation window 0.

III Trivial, since $\overline{\tau} = \varepsilon$.
IV Trivial, since $X_S = X'_S$.

$count(X_S) = n + 1$ By $count(X_S) > 0$ we know that there are transactions that still need to be committed.

Then $minWndw(X_S) = 0$ and we know that the only rule that applies is Rule S:Commit. Thus, $X_S \xrightarrow{\texttt{commit}\ id}_S{}^{O} X''_S$
Applying Rule S:Commit does not change topmost configuration (Lemma 20 (Commits do not change the topmost configuration)). So, we have $X''_S.\sigma = X_S.\sigma$.
We now apply IH on X''_S, since $count(X''_S) = n$. We get

(1) $X''_S \overset{O}{\Downarrow}_{\overline{\tau}'}{}^{S} X'_S$ and
(2) $minWndw(X'_S) > 0$
(3) $\forall \tau \in \overline{\tau}'.\ \tau = \texttt{commit}\ id$ for some $id \in \mathbb{N}$ and
(4) $X_S.\sigma = X'_S.\sigma$

I We construct an execution $X_S \overset{O}{\Downarrow}_{X'_S}{}^{S}$ by Rule S:Single with $X_S \xrightarrow{\texttt{commit}\ id}_S{}^{O} X''_S$ and $X''_S \overset{O}{\Downarrow}_{\overline{\tau}'}{}^{S} X'_S$.
II By IH 2).
III Here $\overline{\tau} = \texttt{commit}\ id \cdot \overline{\tau}'$. By IH we know that $\overline{\tau}'$ fulfills the condition. Thus, $\overline{\tau}$ trivially fulfills condition as well.
IV By Lemma 20 (Commits do not change the topmost configuration).

□

Lemma 23 (V45: Executing a chain of commits). *If*

(1) no transaction that will be rolled back with speculation window 0 *in* X_{S+R}

Then there exists X'_S *such that*

(1) $X_{S+R} \overset{O_{S+R}}{\Downarrow}_{\overline{\tau}}{}^{S+R} X'_{S+R}$
(2) $minWndw(X'_{S+R}) > 0$
(3) $\forall \tau \in \overline{\tau}.\ \tau = \texttt{commit}_S\ id \vee \tau = \texttt{commit}_R\ id$ *for some* $id \in \mathbb{N}$
(4) $X_{S+R}.\sigma = X'_{S+R}.\sigma$

Proof. Analogous to Lemma 22 (V4: Executing a chain of commits). □

Lemma 24 (V15: Executing a chain of commits). *If*

(1) no transaction that will be rolled back with speculation window 0 *in* X_{B+R}

Then there exists X'_S *such that*

(1) $X_{B+R} \overset{O_{B+R}}{\Downarrow}_{\overline{\tau}}{}^{B+R} X'_{B+R}$
(2) $minWndw(X'_{B+R}) > 0$
(3) $\forall \tau \in \overline{\tau}.\ \tau = \texttt{commit}_B\ id \vee \tau = \texttt{commit}_R\ id$ *for some* $id \in \mathbb{N}$
(4) $X_{B+R}.\sigma = X'_{B+R}.\sigma$

Proof. Analogous to Lemma 22 (V4: Executing a chain of commits). □

Lemma 25 (V14: Executing a chain of commits). *If*

(1) no transaction that will be rolled back with speculation window 0 *in* X_{B+S}

Then there exists X'_S *such that*

(1) $X_{B+S} \overset{O_{B+S}}{\Downarrow}_{\overline{\tau}}{}^{B+S} X'_{B+S}$
(2) $minWndw(X'_{B+S}) > 0$
(3) $\forall \tau \in \overline{\tau}.\ \tau = \texttt{commit}_B\ id \vee \tau = \texttt{commit}_S\ id$ *for some* $id \in \mathbb{N}$
(4) $X_{B+S}.\sigma = X'_{B+S}.\sigma$

Proof. Analogous to Lemma 22 (V4: Executing a chain of commits). □

Lemma 26 (V14: Executing a chain of commits). *If*

(1) no transaction that will be rolled back with speculation window 0 *in* X_{B+S+R}

Then there exists X'_S *such that*

(1) $X_{B+S+R} \overset{O_{B+R}}{\Downarrow}_{\overline{\tau}}{}^{B+S+R} X'_{B+S+R}$
(2) $minWndw(X'_{B+S+R}) > 0$
(3) $\forall \tau \in \overline{\tau}.\ \tau = \texttt{commit}_B\ id \vee \tau = \texttt{commit}_S\ id \vee \tau = \texttt{commit}_R\ id$ *for some* $id \in \mathbb{N}$
(4) $X_{B+S+R}.\sigma = X'_{B+S+R}.\sigma$

Proof. Analogous to Lemma 22 (V4: Executing a chain of commits). □

Definition 47 (pc-similar). *Two configurations $\sigma, \sigma' \in Conf$ are* **pc**-*similar, written $\sigma \sim_{\mathbf{pc}} \sigma'$, iff $\sigma(\mathbf{pc}) = \sigma'(\mathbf{pc})$.*

Definition 48 (Next-step agreeing configurations). *Two configurations $\sigma, \sigma' \in Conf$ are next-step agreeing, written $\sigma \sim_{next} \sigma'$, iff there are $\sigma_1, \sigma_1' \in Conf$ such that $\sigma \xrightarrow{\tau} \sigma_1$, $\sigma' \xrightarrow{\tau} \sigma_1'$ and $\sigma_1 \sim_{\mathbf{pc}} \sigma_1'$*

Definition 49 (AM V4 similar speculative instances). *Two speculative instances $\langle p, ctr, \sigma, n\rangle^b$ and $\langle p', ctr', \sigma', n'\rangle^{b'}$ are similar, written $\langle p, ctr, \sigma, n\rangle^b \simeq \langle p', ctr', \sigma', n'\rangle^{b'}$ iff $p = p'$, $ctr = ctr'$, $n = n'$, $b = b'$, $\sigma \sim_{\mathbf{pc}} \sigma'$ and $\sigma \sim_{next} \sigma'$.*

Definition 50 (SE V4 similar speculative instances). *Two speculative instances $\langle p, ctr, \sigma, h, n\rangle^b$ and $\langle p', ctr', \sigma', h', n'\rangle^{b'}$ are similar, written $\langle p, ctr, \sigma, h, n\rangle^b \simeq \langle p', ctr', \sigma', h, 'n'\rangle^{b'}$ iff $p = p'$, $ctr = ctr'$, $h = h'$, $n = n'$, $b = b'$, $\sigma \sim_{\mathbf{pc}} \sigma'$ and $\sigma \sim_{next} \sigma'$.*

Definition 51 (SE V4 similar speculative states). *Two speculative states $\overline{\Psi}_S \cdot \langle p, ctr, \sigma, h, n\rangle_{\overline{\rho}}$ $\overline{\Psi}'_S \cdot \langle p', ctr', \sigma', h', n'\rangle_{\overline{\rho}'}$ are similar, written $\overline{\Psi}_S \cdot \langle p, ctr, \sigma, h, n\rangle_{\overline{\rho}} \cong \overline{\Psi}'_S \cdot \langle p', ctr, \sigma', h', n'\rangle_{\overline{\rho}'}$ iff all the speculative instances in $\overline{\Psi}_S$ and $\overline{\Psi}'_S$ are similar speculative instances which is written $\overline{\Psi}_S \simeq \overline{\Psi}'_S$ and $ctr = ctr'$, $\sigma \sim_{\mathbf{pc}} \sigma'$, $n = n'$, $h = h'$, $\overline{\rho} = \overline{\rho}'$ and $b = b'$.*

Definition 52 (commit-free projection). *The commit-free projection of our speculative state X is defined as follows:*

$$\begin{aligned}
\varepsilon\restriction_{com} &= \varepsilon \\
\overline{\Psi}_S \cdot \langle p, ctr, \sigma, h, n\rangle^b\restriction_{com} &= \overline{\Psi}_S\restriction_{com} \cdot \langle p, ctr, \sigma, h, n\rangle^b \text{ with } b \neq false \\
\overline{\Psi}_S \cdot \langle p, ctr, \sigma, h, n\rangle\restriction_{com} &= \overline{\Psi}_S \cdot \langle p, ctr, \sigma, h, n\rangle \text{ where } |\overline{\Psi}| = 0 \\
\overline{\Psi}_S \cdot \langle p, ctr, \sigma, h, n\rangle^b \cdot \langle p, ctr', \sigma', h', n'\rangle^{false}\restriction_{com} &= \overline{\Psi}_S \cdot \langle p, ctr', \sigma', h', n\rangle^b\restriction_{com}
\end{aligned}$$

This executes the committed speculative instance and changes the speculative state.

Definition 53 (Invariants). *We write $INV(\Sigma_S, X_S)$ iff $INV_h(\Sigma_S, X_S\restriction_{com})$ holds. $INV_h(\Sigma_S, X_S)$ holds if $|X_S| = |\Sigma_S|$ and for all $1 \leq i \leq |\Sigma_S|$, $minWndw(X_S^i) \leq wndw(\Sigma_S^i)$, where Σ_S^i denotes the prefix of Σ_S of length i.*

Definition 54 (Invariants2). *We write $INV2(\Sigma_S, X_S)$ iff $INV2_h(\Sigma_S, X_S\restriction_{com})$ holds. $INV2_h(\Sigma, X_S)$ holds if $|X_S| = |\Sigma_S|$ and $minWndw(X_S) = wndw(\Sigma)$*

SPECTRE V4

Our main result for 🕵_S is the following:

Theorem 13 (🕵_S is *SSS*). $\vdash \text{🕵}_S$ *SSS*

Proof. Immediately follows from Theorem 17 (S SNI), Theorem 16 (S : Behaviour of AM and symbolic semantics), Theorem 15 (S AM: Behaviour of non-speculative semantics and AM semantics) and Theorem 14 (S SE: Behaviour of non-speculative and oracle semantics). □

I.1 Relating Non-speculative and Oracle Semantics

Theorem 14 (S SE: Behaviour of non-speculative and oracle semantics). *Let p be a program and O be a prediction oracle. Then* $Beh_{NS}(p) = Beh_S^O(p)\restriction_{ns}$

Proof. We prove the two directions separately:

⇐ Assume that $\overline{\tau} \in Beh_S^O(p)$.

By the definition of $Beh_S^O(p)$ we have an initial configuration σ such that $(p,\sigma)\ \text{🕵}_S^O\ \overline{\tau}$.

By definition of $p, \sigma\ \text{🕵}_S^O\ \overline{\tau}$, we know there exists a state X_S' such that $\vdash X_S' : \mathit{fin}$ and an initial state $\Sigma_S^{init} p, \sigma$ such that $\Sigma_S^{init} p, \sigma \overset{O}{\Downarrow}_{\overline{\tau}}^{S} X_S'$.

We apply Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) with $\Sigma_S^{init} p, \sigma \overset{O}{\Downarrow}_{\overline{\tau}}^{S} X_S'$, because $\Sigma_S^{init} p, \sigma$ has no speculative transactions by definition.

We get

(1) exists σ' and σ' is the configuration for some instance in X_S' and
(2) if $\vdash_O X_S' : \mathit{noongoing}$ then $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}} \sigma'$ and
(3) if $\vdash_O^i X_S' : \mathit{biggestongoingtransactionirolledback}$ then by definition exists id i such that it is the smallest transaction id that will be rolled back and is still active then $\sigma \Downarrow_{helper(\overline{\tau},i)} \sigma'$

Since $\vdash X_S' : \mathit{fin}$, we have $\vdash_O X_S' : \mathit{noongoing}$ and as such $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}} \sigma'$ by 2).
Since X_S' has only one instance, we have $X_S'.\sigma = \sigma'$.
Furthermore, because of $\vdash X_S' : \mathit{fin}$, we know $X_S'.\sigma \in \mathit{FinalConf}$.
We can now conclude that $(p,\sigma)\ \text{🕵}_{NS}^O\ \overline{\tau}\restriction_{ns} \in Beh_{NS}(p)$ by Rule NS-Trace.

⇒ Assume that $(p,\sigma)\ \text{🕵}_S^O\ \overline{\tau} \in Beh_{NS}(p)$. We thus know there exists $\sigma' \in \mathit{FinalConf}$ such that $\sigma \Downarrow_{\overline{\tau}} \sigma'$.

Let $X_S = X_S^{init}(p,\sigma)$. We now apply Lemma 31 (S SE: Completeness of the speculative semantics) and get

(1) X_S' with $\vdash_O X_S : \mathit{noongoing}$
(2) $\sigma' = X_S'.\sigma$
(3) $X_S \overset{O}{\Downarrow}_{\overline{\tau}'}^{S} X_S'$ and
(4) $\overline{\tau} = \overline{\tau}'\restriction_{ns}$.

Since $\sigma' \in \mathit{FinalConf}$, we know that $X_S'.\sigma \in \mathit{FinalConf}$.
We now show how we can reach a final state X_S''. We apply Lemma 21 (V4: Reaching Final state from final configuration) on X_S' and get

(1) $X_S' \overset{O}{\Downarrow}_{\overline{\tau}''}^{S} X_S''$
(2) $\forall \tau \in \overline{\tau}''.\ \tau = \texttt{commit}\ id$ for some $id \in \mathbb{N}$
(3) $\vdash X_S'' : \mathit{fin}$
(4) $X_S'.\sigma = X_S''.\sigma$

We now have an execution $X_S \overset{O}{\Downarrow}_{\overline{\tau}'\cdot\overline{\tau}''}^{S} X_S''$, since the oracle semantics are deterministic.
Note that by 2) we have $\overline{\tau}''\restriction_{ns} = \varepsilon$ and thus $\overline{\tau}' \cdot \overline{\tau}''\restriction_{ns} = \overline{\tau}'\restriction_{ns}$.
By 3) we have that $\vdash X_S'' : \mathit{fin}$.
We thus have $(p,\sigma)\ \text{🕵}_S^O\ \overline{\tau}' \cdot \overline{\tau}'' \in Beh_S^O(p)$.

□

Note that doing the induction without the condition $\vdash_O : \mathit{noongoing}$ does not work. In the induction case for the step, our IH only tells us about the execution until that point. But if that execution is currently speculating, the non-speculative semantics should not do a step, but wait until the speculation is finished. Without the additional information from $\vdash_O : \mathit{noongoing}$ and $\vdash_O i : \mathit{biggestongoingtransactionirolledback}$ we would be stuck, because the IH is unusable.

I.1.1 Soundness.

Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics)**.** *If*

(1) $X_S.\sigma = \sigma$ *and*
(2) $\vdash_O X_S$: *noongoing and*
(3) $X_S \overset{O}{\Downarrow}_{\overline{\tau}}^{S} X'_S$

Then there exists σ' *such that*

I if $\vdash_O X'_S$: *noongoing then* $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}\sigma'}$ *and (if* `start` $id \in X'_S.\overline{\rho}$ *then* $X'_S = \overline{\Psi}_S \cdot \langle p, ctr, \sigma', h, n\rangle$ *and* $\overline{\Phi}_S.\sigma = \sigma'$ *else* $X'_S.\sigma = \sigma'$*) and*
II if $\vdash^i_O X'_S$: *biggestongoingtransactionirolledback then by definition exists id i such that it is the smallest transaction id that will be rolled back and is still active then* $\sigma \Downarrow_{helper(\overline{\tau},i)} \sigma'$ *and* σ' *is the configuration with the instance with* $ctr = i$*.*

Proof. We proceed by induction on $X_S \overset{O}{\Downarrow}_{\overline{\tau}}^{S} X'_S$

Rule S:Reflection Then we have $X_S \overset{O}{\Downarrow}_{\varepsilon}^{S} X_S$ with $X'_S = X_S$ and by Rule NS-Reflection we have
I $\sigma \Downarrow_{\varepsilon\restriction_{ns}} \sigma'$ with $\sigma = \sigma'$.
II $\sigma \Downarrow_{helper(\varepsilon,i)} \sigma'$ with $\sigma = \sigma'$.

Rule S:Single We have $X_S \overset{O}{\Downarrow}_{\overline{\tau}'\cdot\tau}^{S} X'_S$ and by Rule S:Single we get $X_S \overset{O}{\Downarrow}_{\overline{\tau}'}^{S} X''_S$ and $X''_S \overset{\tau}{\rightsquigarrow}_S^O X'_S$.
We need to prove
I if $\vdash_O X'_S$: *noongoing* then $\sigma \Downarrow_{\overline{\tau}'\cdot\tau\restriction_{ns}\sigma'}$ and $X'_S.\sigma = \sigma'$
II if $\vdash^i_O X'_S$: *biggestongoingtransactionirolledback* then by definition exists *id i* such that it is the smallest transaction *id* that will be rolled back and is still active then $\sigma \Downarrow_{helper(\overline{\tau}'\cdot\tau,i)} \sigma'$ and σ' is the configuration for the instance with $ctr = i$.
We apply the IH on $X_S \overset{O}{\Downarrow}_{\overline{\tau}'}^{S} X''_S$ and have a σ'' where σ'' is the configuration for some instance in X''_S such that.
I' if $\vdash_O X''_S$: *noongoing* then $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}\sigma''}$ and $X''_S.\sigma = \sigma''$
II' if $\vdash^j_O X''_S$: *biggestongoingtransactionirolledback* then by definition exists *id* j such that it is the smallest transaction *id* that will be rolled back and is still active then $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$ and σ'' is the configuration with the instance with $ctr = j$.
We proceed by case analysis on X''_S.
no ongoing transactions in X''_S Then X''_S has no ongoing transactions, meaning $\vdash_O X''_S$: *noongoing* and we have $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}} \sigma''$ and $X''_S.\sigma = \sigma''$ by IH.

I Then $\vdash_O X'_S$: *noongoing* and we need to proof $\sigma \Downarrow_{\overline{\tau}\cdot\tau\restriction_{ns}\sigma'}$ and $X'_S.\sigma = \sigma'$. We now proceed by inversion on $X''_S \overset{\tau}{\rightsquigarrow}_S^O X'_S$:
Rule S:Rollback Then $\tau =$ `rlb` *id*.
Contradiction. Since $\vdash_O X''_S$: *noongoing* there does not exists a `rlb` *id* observation that does not have a corresponding `start` *id* observation in the execution $X_S \overset{O}{\Downarrow}_{\overline{\tau}}^{S} X''_S$. So $\tau \neq$ `rlb` *id*.
Rule S:Store-Skip Then we know that $\overline{\rho} =$ `bypass` $X''_S.\sigma(\mathbf{pc}) \cdot$ `start` *id* for X'_S. Contradiction. Since $\vdash_O X'_S$: *noongoing*, there exists a `start` *id* for every `rlb` *id* in the execution $X'_{S\overline{\rho}} \overset{O}{\Downarrow}_{\overline{\tau}_{fin}}^{S} X_{Sfin}$ and $\nexists$`start` $id \in \overline{\rho}$. `rlb` $id \in \overline{\tau}$
But we have a `start` $id \in \overline{\rho}$ by definition and since that was created by Rule S:Store-Skip, we know it belongs to a transaction that will be rolled back.
Since all transactions are terminated, we know there exists `rlb` *id*.
Now we have a contradiction.
otherwise We know that $\sigma'' = X''_S.\sigma$.
Since $\vdash_O X''_S$: *noongoing*, there no ongoing transactions that need to be rolled back.
Furthermore, no transaction that will be rolled back is created in the step $X''_S \overset{\tau}{\rightsquigarrow}_S^O X'_S$, because $\vdash_O X'_S$: *noongoing*.
We can now apply Lemma 28 (S SE: Soundness single step No Speculation) with $X''_S \overset{\tau}{\rightsquigarrow}_S^O X'_S$ and get

$$\sigma'' \Downarrow_{\tau\restriction_{ns}} \sigma'$$
$$X'_S.\sigma = \sigma'$$

Since $\overline{\tau}\restriction_{ns} \cdot \tau\restriction_{ns} = \overline{\tau} \cdot \tau\restriction_{ns}$ (because $\tau \neq$ `rlb` *id*), we are finished.

II Then X'_S has ongoing transactions, meaning $\vdash^i_O X'_S$: *biggestongoingtransactionirolledback* and we need to prove $\sigma \Downarrow_{helper(\overline{\tau}\cdot\tau,i)} \sigma'$ and σ' is the configuration for the instance with $ctr = i$.
We now proceed by inversion on $X''_S \overset{\tau}{\rightsquigarrow}_S^O X'_S$:
Rule S:Store-Skip Then we know that $\overline{\rho} =$ `bypass` $X''_S.\sigma(\mathbf{pc}) \cdot$ `start` *id* for X'_S.
Since we know a new transaction was created that will be rolled back, we also know that $id = i$.
We know that, because $\vdash_O X''_S$: *noongoing*, so there was not another ongoing transaction.

We can now apply Lemma 30 (S SE: Store step) and get

$$\sigma'' \xrightarrow{\texttt{store}\ m\restriction_{ns}} \sigma'$$

σ' is the configuration for the instance with $ctr = i$ in X_S'

By IH we have $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}} \sigma''$ where $X_S''.\sigma = \sigma''$.

Using $\sigma'' \xrightarrow{\texttt{store}\ m\restriction_{ns}} \sigma'$ we get $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}\cdot\texttt{store}\ m\restriction_{ns}} \sigma'$.

Since $\vdash_O X_S''$: *noongoing* we have $\texttt{store}\ m\restriction_{ns} = \texttt{store}\ m$ and thus $\overline{\tau}\restriction_{ns} \cdot \texttt{store}\ m = \overline{\tau} \cdot \texttt{store}\ m\restriction_{ns}$.

We are now finished.

otherwise By definition of $\vdash^i_O X_S'$: *biggestongoingtransactionirolledback* we know that there exists a `rlb` i in the execution $X_S' \overset{O}{\Downarrow}_{\overline{\tau}_{fin}} X_{S\,fin}$ with no matching `start` i observation in that execution.

This means the `start` i has to happen before in the execution $X_S \overset{O}{\Downarrow}_{\overline{\tau}\cdot\tau} X_S'$.

By definition of $\vdash_O X_S''$: *noongoing*, we have that all `rlb` id' have a matching `start` id' in the execution $X_S'' \overset{O}{\Downarrow}_{\tau\cdot\overline{\tau}_{fin}} X_{S\,fin}$.

Now we have a contradiction, since `rlb` i does not have a matching `start` i.

ongoing transactions in X_S'' Then X_S'' has ongoing transactions, meaning $\vdash^j_O X_S''$: *biggestongoingtransactionirolledback* and we have $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$ and σ'' is the configuration for the instance with $ctr = j$.

I Then $\vdash_O X_S'$: *noongoing* and we need to prove $\sigma \Downarrow_{\overline{\tau}\cdot\tau\restriction_{ns}\sigma'}$ and $X_S'.\sigma = \sigma'$. We now proceed by inversion on $X_S'' \overset{\tau}{\rightsquigarrow}_S^O X_S'$:

Rule S:Rollback and $\tau =$ `rlb` j Choose $\sigma' = \sigma''$. Since $\overline{\tau} \cdot \tau\restriction_{ns} = helper(\overline{\tau}, j)$ we can use IH $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$ and Rule NS-Reflection.

The roll back deletes all states higher up the stack then the instance with $ctr = j$.

By definition, σ'' is the configuration for the instance with $ctr = j$ and by rule S:Rollback we know that we keep the configuration of this instance. which is now at the top after the roll back.

So $X_S'.\sigma = \sigma''$ and we are finished.

otherwise Then $\tau \neq$ `rlb` j.

Since $\vdash_O X_S'$: *noongoing*, there does not exists `rlb` *id* without matching `start` *id* in the execution $X_S' \overset{O}{\Downarrow}_{\overline{\tau}_{fin}} X_{S\,fin}$.

Because $\vdash^j_O X_S''$: *biggestongoingtransactionirolledback*, there exists a a smallest `rlb` j that does not have a `start` j in the execution $X_S'' \overset{O}{\Downarrow}_{\tau\cdot\overline{\tau}_{fin}} X_{S\,fin}$.

Since $\tau \neq$ `rlb` j, `rlb` j would need to exist in $\overline{\tau}_{fin}$.

Contradiction, because it would not have a matching `start` j in the execution $X_S' \overset{O}{\Downarrow}_{\overline{\tau}_{fin}} X_{S\,fin}$.

II Then $\vdash^i_O X_S'$: *biggestongoingtransactionirolledback* and we need to prove $\sigma \Downarrow_{helper(\overline{\tau}\cdot\tau,i)} \sigma'$ and σ' is the configuration for the instance below the instance with $ctr = i$.

We now proceed by inversion on $X_S'' \overset{\tau}{\rightsquigarrow}_S^O X_S'$:

Rule S:Rollback Then $\tau =$ `rlb` *id*. We do a case analysis if $id = j$ or not.

$id = j$ Contradiction. Then there is no ongoing transactions in X_S', because j is the oldest ongoing transaction in X_S''.

$id \neq j$ Then $i = j$. Since no transaction was started and j is still ongoing.

We choose $\sigma' = \sigma''$ and derive a step by Rule NS-Reflection.

We have $helper(\overline{\tau} \cdot \tau, i) = helper(\overline{\tau}, i) = helper(\overline{\tau}, j)$.

By IH $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$.

Because the transaction j is still ongoing, we know that the configuration σ'' is still below the instance with $ctr = j$ in X_S'.

otherwise Then $\tau \neq$ `rlb` *id*.

Then $helper(\overline{\tau} \cdot \tau, i) = helper(\overline{\tau}, i)$

We choose $\sigma' = \sigma''$ and derive a step by Rule NS-Reflection.

Note that $i = j$, since $\tau \neq$ `rlb` *id*.

This means the transaction j is still not finished and active in X_S' as well.

Thus it is the smallest transaction in X_S' as well.

Then $helper(\overline{\tau} \cdot \tau, i) = helper(\overline{\tau}, i) = helper(\overline{\tau}, j)$ and by IH we have $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma'$.

Since the observation was not a rollback, we know that the instance with $ctr = j$ still exists in X_S'.

Because σ'' is the configuration for the instance with $ctr = j$, it is the configuration for the instance with $ctr = j$ in X_S' as well.

□

Lemma 28 (S SE: Soundness single step No Speculation). *If*

(1) $\vdash_O X_S$: *noongoing and*

(2) $X_S \overset{\tau}{\rightsquigarrow}{}^{O}_{S} X'_S$ *and*
(3) $\vdash_O X'_S$: *noongoing and*
(4) $\sigma = X_S.\sigma$

Then there exists σ' *such that*

I $\sigma \Downarrow_{\tau\restriction_{ns}} \sigma'$ *and*
II $X'_S.\sigma = \sigma'$

and σ' *is the configuration for some instance in* X'_S*. (Case where we do a store step then its not the topmost one).*

Proof. We proceed by inversion on $X_S \overset{\tau}{\rightsquigarrow}{}^{O}_{S} X'_S$:

Rule S:General Thus we have $X_S = \overline{\Psi}_S \cdot \Psi_{S\overline{\rho}\cdot\tau}$ and $X'_S = \overline{\Psi}_S \cdot \Psi_{S\overline{\rho}}$ with $\Psi_S.\sigma = \sigma$.
By the definition of $\Psi_S \overset{\tau}{\rightsquigarrow}{}^{O}_{S} X_S$ only Rule S:Store-Skip and Rule S:Store-Exe add observations to $\overline{\rho}$.
These observations are either $\texttt{start}_S$ *id* or bypass *n*.
By the definition of $\restriction_{ns}$ we have $\tau\restriction_{ns} = \varepsilon$ and we have $\sigma \Downarrow_{\varepsilon\restriction_{ns}} \sigma$ by Rule NS-Reflection.
Rule S:Commit Then the generated observation is $\tau = \texttt{commit}\ id$. Furthermore, $\texttt{commit}\ id\restriction_{ns} = \varepsilon$
By the definition of the rule, we have $X_S.\sigma = X'_S.\sigma$ and with this we get $X'_S.\sigma = \sigma$.
Thus, we can derive $\sigma \Downarrow_{\texttt{commit}\ id\restriction_{ns}} \sigma$.
Rule S:Rollback Contradiction, since $\vdash_O X_S$: *noongoing* and Definition 44 (Well orderedness of rollback and start).
Rule S:SE-Context Thus we have $X_S = \overline{\Psi}_S \cdot \Psi_S$ and $X'_S = \overline{\Psi}_S \cdot \overline{\Psi}'_S$ with $\Psi_S \overset{\tau}{\rightsquigarrow}{}^{O}_{S} \overline{\Psi}'_S$. By Lemma 29 (S SE: Single Step Instance Non Speculative) we have $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma$ with $\sigma = \Psi_S.\sigma$ and $\overline{\Psi}'_S.\sigma = \sigma$.

□

Lemma 29 (S SE: Single Step Instance Non Speculative)**.** *If*

(1) $X_S = \overline{\Psi}_S \cdot \Psi_S$ *and*
(2) $X'_S = \overline{\Psi}_S \cdot \overline{\Psi}'_S$ *and* $\vdash_O X'_S$: *noongoing and*
(3) $\Psi_S \overset{\tau}{\rightsquigarrow}{}^{O}_{S} \overline{\Psi}'_S$ *and*
(4) $\sigma = \Psi_S.\sigma$

Then there is a σ' *such that*

I $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ *and*
II $\overline{\Psi}'_S.\sigma = \sigma$

Proof. We proceed by case analysis on the rule used to derive $\Psi''_S \overset{\tau}{\rightsquigarrow}{}^{O}_{S} \Psi'_S$.

Rule S:barr-spec, Rule S:barr We show the proof for Rule S:barr, the proof for Rule S:barr-spec is analogous.
By Rule S:barr we know $\sigma \xrightarrow{\tau} \sigma'$ and $\overline{\Psi}'_S = \langle p, ctr, \sigma', h, n-1\rangle$.
Thus $\sigma' = \overline{\Psi}'_S.\sigma$ and $\tau = \varepsilon = \varepsilon\restriction_{ns}$.
Rule S:NoBranch We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule and $\overline{\Psi}'_S = \langle p, ctr, \sigma', h, n-1\rangle$.
Thus, $\sigma' = \overline{\Psi}'_S.\sigma$.
Because the rule used the observation received from the step $\sigma \xrightarrow{\tau} \sigma'$, we have $\tau\restriction_{ns} = \tau$ and are finished.
Rule S:Store-Skip Contradiction, because there are no ongoing transactions in X'_S by the fact $\vdash_O X'_S$: *noongoing*.
Rule S:Store-Exe By definition $\overline{\Psi}'_S = \langle p, ctr, \sigma', h, n\rangle \cdot \langle p, ctr', \sigma', h', n'\rangle_{\overline{\rho}}$. By premise of the rule we do the step $\sigma \xrightarrow{\tau'} \sigma'$. The generated trace is $\tau = \tau'$ and $\tau\restriction_{ns} = \tau'$. Thus the step $\sigma \xrightarrow{\tau'} \sigma'$ is what we look for and by construction $\overline{\Psi}'_S.\sigma = \sigma'$.

□

Lemma 30 (S SE: Store step)**.** *If*

(1) $X_S = \overline{\Psi}_S \cdot \Psi_S$ *and* $\vdash_O X_S$: *noongoing*
(2) $X'_S = \overline{\Psi}_S \cdot \overline{\Psi}'_S$ *and* $\vdash^{i}_{O} X'_S$: *biggestongoingtransactionirolledback and*
(3) $\Psi_S \overset{\tau}{\rightsquigarrow}{}^{O}_{S} \overline{\Psi}'_S$ *and*
(4) $\sigma = \Psi_S.\sigma$

Then

I $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ *and*
II σ' *is the configuration for the instance with* $ctr = i$ *in* X'_S

Proof. We proceed by inversion on $\Psi_S \overset{\tau}{\rightsquigarrow}_S^O \overline{\Psi}'_S$:

Rule S:Store-Skip By definition $\overline{\Psi}'_S = \langle p, ctr, \sigma_1, h, n\rangle \cdot \langle p, ctr+1, \sigma_2, h', n'\rangle_{\texttt{start}\ ctr \cdot \texttt{bypass}\ \sigma_1(\mathbf{pc})} \cdot$

By premise of the rule we do the step $\sigma \xrightarrow{\texttt{store}\ m} \sigma_1$ for some $m \in \mathbb{N}$. Since $\vdash_O X_S$: *noongoing* we know that $\texttt{store}\ m\restriction_{ns} = \texttt{store}\ m$.
Choose $\sigma' = \sigma_1$ and thus the step $\sigma \xrightarrow{\texttt{store}\ m} \sigma'$ is what we look for.
Furthermore, notice that the transaction created has *id ctr*.
Since $\vdash_O X_S$: *noongoing*, we know that this is the oldest transaction that is still ongoing in X'_S.
We thus have $i = ctr$.
By construction, σ' is the configuration of the instance with $ctr = i$ and we are finished.

otherwise Contradiction, because $\vdash_O X_S$: *noongoing* and $\vdash_O^i X'_S$: *biggestongoingtransactionirolledback*, we know that a transaction has to be started that will be rolled back.

□

I.1.2 Completeness.

Lemma 31 (S SE: Completeness of the speculative semantics)**.** *If*

(1) $\sigma \in InitConf$ *and*
(2) $\sigma \Downarrow_{\overline{\tau}} \sigma'$ *and*
(3) $X_S = X_S^{init}(p, \sigma)$

Then

I $X_S \overset{O}{\downarrow}_{\overline{\tau}'}^S X'_{S_\rho}$ *and*
II $\vdash_O X'_S$: *noongoing and*
III $\sigma' = X'_S.\sigma$ *and*
IV $\overline{\tau} = \overline{\tau}'\restriction_{ns}$ *and*
V $\rho = \varepsilon$

Proof. We proceed by induction on $\sigma \Downarrow_{\overline{\tau}} \sigma'$

Rule NS-Reflection Then we have $\sigma \Downarrow_{\varepsilon} \sigma'$ with $\sigma = \sigma'$.

I - IV By Rule S:Reflection we have $X_S \overset{O}{\downarrow}_{\varepsilon}^S X_S$. By construction $\vdash_O X_S$: *noongoing* and $X_S.\sigma = \sigma$. Since $\varepsilon\restriction_{ns} = \varepsilon$ we are finished.

Rule NS-Single Then we have $\sigma \Downarrow_{\overline{\tau}} \sigma''$ and $\sigma'' \xrightarrow{\tau} \sigma'$.

We need to show
I $X_S \overset{O}{\downarrow}_{\overline{\tau}'\cdot\tau'}^S X'_S$ and
II $\vdash_O X'_S$: *noongoing* and
III $\sigma' = X'_S.\sigma$ and
IV $\overline{\tau}\cdot\tau = \overline{\tau}'\cdot\tau'\restriction_{ns}$

We apply the IH on $\sigma \Downarrow_{\overline{\tau}} \sigma''$ we get
I' $X_S \overset{O}{\downarrow}_{\overline{\tau}'}^S X''_{S_\rho}$ and
II' $\vdash_O X''_{S_\rho}$: *noongoing* and
III' $\sigma'' = X''_S.\sigma$ and
IV' $\overline{\tau} = \overline{\tau}'\restriction_{ns}$
V' $\rho = \varepsilon$

To account for possible outstanding commits, we use Lemma 22 (V4: Executing a chain of commits) on X''_S and get
a) $X''_S \overset{O}{\downarrow}_{\overline{\tau}'''}^S X'''_S$
b) $minWndw(X'''_S) > 0$
c) $\forall \tau \in \overline{\tau}'''.\ \tau = \texttt{commit}\ id$ for some $id \in \mathbb{N}$
d) $X''_S.\sigma = X'''_S.\sigma$

By c) and the definition of $\restriction_{ns}$ we have $\overline{\tau}'''\restriction_{ns} = \varepsilon$.
Because only Rule S:Commit was used we have $X'''_S \cdot \overline{\rho} = X''_S \cdot \overline{\rho}$.
We now do a case analysis on the instruction $p(\sigma''(\mathbf{pc}))$:
$p(\sigma''(\mathbf{pc})) \neq \mathbf{store}\ x, e$ **I** Then either Rule S:barr, Rule S:barr-spec or Rule S:NoBranch in conjunction with Rule S:SE-Context was used to derive the step $X'''_S \overset{\tau'}{\rightsquigarrow}_S^O X^n_S$.

Here, τ' is generated from $X'''_S.\sigma \xrightarrow{\tau'} \sigma'$ and $X^n_S.\sigma = \sigma'$
Since $\rightarrow$ is deterministic, we know that $\tau' = \tau$.

II Since no speculative transaction is started and we have $\vdash_O X''_S$: *noongoing* by IH, we have $\vdash_O X^n_S$: *noongoing*.

III By definition and determinism of $\longrightarrow$.

IV Now we have $X_S'' \overset{O}{\Downarrow}_{\overline{\tau}'\cdot\overline{\tau}'''\cdot\tau'} X_S^n$. Looking at the trace that is generated we have

$$\begin{aligned}
&\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau' \restriction_{ns} \tau' = \tau \\
=\ &\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau' \restriction_{ns} \tau \text{ generated by} \longrightarrow \\
=\ &\overline{\tau}' \cdot \overline{\tau}''' \restriction_{ns} \cdot \tau\ \overline{\tau}''' \restriction_{ns} = \varepsilon \\
=\ &\overline{\tau}' \restriction_{ns} \cdot \tau \text{ by IH} \\
=\ &\overline{\tau} \cdot \tau
\end{aligned}$$

and thus, are finished.

$p(\sigma''(\mathbf{pc})) = \mathbf{store}\ x, e$ There are two cases depending on the decision of the oracle O.

$O(p, n, h) = (false, \omega)$ Then we do not skip the **store** instruction.

I We derive $X_S'' \overset{O}{\Downarrow}_{\tau\cdot\texttt{start}\ id} X_S^n$ by using Rule S:Store-Exe in conjunction with Rule S:SE-Context and produce the observation $\tau' = \tau$, where $\tau = \texttt{store}\ m \in Obs$.
Afterwards, we need to discharge the observation in $\overline{\rho}$ that was generated by Rule S:Store-Exe (which is always a $\texttt{start}\ id$). The only rule that can be used when $\overline{\rho}$ is non-empty is Rule S:General, which produces $\texttt{start}\ id$.
By Rule S:Store-Exe, we know that the step $X_S'''.\sigma \xrightarrow{\tau} \sigma'$ is made.

II No speculative transaction was started that needs to be rolled back. By $\vdash_O X_S'' : noongoing$ and $\vdash_O X_S''' : noongoing$ we get $\vdash_O X_S^n : noongoing$.

III By definition and determinism of $\longrightarrow$.

IV We now have:

$$\begin{aligned}
&\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau' \cdot \texttt{start}\ id \restriction_{ns} \text{ Def. and } \overline{\tau}''' \restriction_{ns} = \varepsilon \\
=\ &\overline{\tau}' \cdot \tau' \restriction_{ns} \tau' = \tau \\
=\ &\overline{\tau}' \cdot \tau \restriction_{ns} \tau \text{ generated by} \longrightarrow \\
=\ &\overline{\tau}' \restriction_{ns} \cdot \tau \text{ by IH} \\
=\ &\overline{\tau} \cdot \tau
\end{aligned}$$

and are finished.

$O(p, n, h) = (true, \omega)$ Then we skip the **store** instruction.

I We derive a step by using Rule S:Store-Skip in conjunction with Rule S:SE-Context This produces the observation τ'', where $\tau'' = \texttt{store}\ m$ and the step $X_S'''.\sigma \xrightarrow{\tau''} \sigma'''$ is made.
Since $\longrightarrow$ is deterministic and the fact that $\sigma'' \xrightarrow{\tau''} \sigma'''$, $\sigma'' \xrightarrow{\tau} \sigma'$ and $X_S'''.\sigma = \sigma''$, we have $\sigma''' = \sigma'$ and $\tau'' = \tau$.
Since Rule S:Store-Skip pushes two observations into $\overline{\rho}$, Rule S:General applies twice and produces $\texttt{bypass}\ id$ and $\texttt{start}\ id$.
We thus have $X_S''' \overset{O}{\Downarrow}_{\tau'\cdot\texttt{start}\ id\cdot\texttt{bypass}\ n} X_{S3}$.
Since all transactions are eventually closed, we know there exists X_S^n such that $X_S^3 \overset{O}{\Downarrow}_{\overline{\tau}^n\cdot\texttt{rlb}\ id} X_S^n$.
We now apply Lemma 32 (S SE: Non-speculative execution for rolled back transactions) on the execution $X_S''' \overset{O}{\Downarrow}_{\tau'\cdot\texttt{start}\ id\cdot\texttt{bypass}\ n\cdot\overline{\tau}^n\cdot\texttt{rlb}\ id} X_S^n$ and get $\sigma'' \xrightarrow{\tau''} \sigma'''$ and $X_S^n.\sigma = \sigma''$.

II Since the speculative transaction that was started was also rolled back and the fact that $\vdash_O X_S'' : noongoing$ by IH and $\vdash_O X_S''' : noongoing$, we have $\vdash_O X_S^n : noongoing$.

III Follows by definition and I).

IV By definition $\tau'' \cdot \texttt{start}\ id \cdots \texttt{rlb}\ id \restriction_{ns} = \tau'' \restriction_{ns} = \tau''$.

$$\begin{aligned}
&\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau'' \cdot \texttt{start}\ id \cdot \overline{\tau}^n \cdot \texttt{rlb}\ id \restriction_{ns} \text{ Def. and } \overline{\tau}''' \restriction_{ns} = \varepsilon \\
=&\overline{\tau}' \cdot \tau' \restriction_{ns} \tau'' = \tau \\
=\ &\overline{\tau}' \cdot \tau \restriction_{ns} \tau \text{ generated by} \longrightarrow \\
=\ &\overline{\tau}' \restriction_{ns} \cdot \tau \text{ by IH} \\
=\ &\overline{\tau} \cdot \tau
\end{aligned}$$

Note that $\overline{\rho}$ is empty for all the cases, because we discharge all the observations immediately using Rule S:General.

□

Lemma 32 (S SE: Non-speculative execution for rolled back transactions.). *If*

(1) $X_S \overset{O}{\downarrow}_{\overline{\tau}}^{S} X'_S$ *and*
(2) $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$ *and*
(3) $\sigma = X_S.\sigma$

Then

I *there is a configurations* σ' *with* $X'_S.\sigma = \sigma'$ *and*
II $\sigma \xrightarrow{\overline{\tau}\restriction_{ns}} \sigma'$ *and*
III $\overline{\tau}\restriction_{ns} = \tau$

Proof. Let $X_S \overset{O}{\downarrow}_{\overline{\tau}}^{S} X'_S$ be an execution with trace $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$. Let $\sigma = X_S.\sigma$

We know Rule S:Store-Skip was used to start the speculative transaction.

By this rule we know, there is a configuration σ' with $\sigma \xrightarrow{\tau} \sigma'$.

By definition of $\restriction_{ns}$ we have $\overline{\tau}\restriction_{ns} = \tau\restriction_{ns} = \tau$, where the last steps is because of the fact that τ was generated by $\longrightarrow$.

Thus, we have $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}} \sigma'$ by Rule NS-Reflection and $\sigma \xrightarrow{\tau} \sigma'$.

Now we need to show that $\sigma' = X'_S.\sigma$. We know that Rule S:Store-Skip created a new speculative instance Ψ'_S used for speculation that is at the top.

Thus the state after Rule S:Store-Skip has this form $X_S.\overline{\Psi}_S \cdot \Psi_S \cdot \Psi'_S$ and since Rule S:Rollback deletes the instance Ψ'_S and every other instance higher in the stack, we have the old Ψ_S at the top of the stack.

Now $X'_S.\sigma = \Psi_S.\sigma = \sigma'$ and we are finished. □

I.2 S: Relating Non-speculative and AM Semantics

These proofs are very similar to the corresponding proofs for the oracle semantics. They are a bit easier because we do not need to handle commits. This means we can reuse a lot of the reasoning.

Theorem 15 (S AM: Behaviour of non-speculative semantics and AM semantics). *Let p be a program. Then $Beh_{NS}(p) = Beh_{\mathsf{S}}^{\mathcal{A}}(p)\restriction_{ns}$*

Proof. The proposition can be proven in similar fashion to Theorem 14 (S SE: Behaviour of non-speculative and oracle semantics). We prove the two directions separately:

$\Leftarrow$ Assume that $\overline{\tau} \in Beh_{\mathsf{S}}^{\mathcal{A}}(p)$.

By the definition of $Beh_{\mathsf{S}}^{\mathcal{A}}(p)$ we have an initial configuration σ such that $(p,\sigma) \,\text{🕮}_{\mathsf{S}}^{\omega}\, \overline{\tau}$.
The proof proceeds in similar fashion to the analogous case in Theorem 14 (S SE: Behaviour of non-speculative and oracle semantics) by using Lemma 33 (S AM : Soundness of the AM semantics w.r.t. non-speculative semantics).
We can now conclude that $(p,\sigma) \,\text{🕮}_{NS}^{O}\, \overline{\tau}\restriction_{ns} \in Beh_{NS}(p)$ by Rule NS-Trace.

$\Rightarrow$ Assume that $(p,\sigma) \,\text{🕮}_{NS}^{O}\, \overline{\tau} \in Beh_{NS}(p)$.

We thus know there exists $\sigma' \in FinalConf$ such that $\sigma \Downarrow_{\overline{\tau}} \sigma'$.
We apply Lemma 37 (S AM: Completeness of the speculative semantics) with $\Sigma_{\mathsf{S}} = \Sigma_{\mathsf{S}}^{init} p, \sigma$ and get $\Sigma_{\mathsf{S}}^{init} p, \sigma \Downarrow_{\mathsf{S}}^{\overline{\tau}'} \Sigma'_{\mathsf{S}}$ with $\vdash_O \Sigma'_{\mathsf{S}} : noongoing$, $\sigma' = \Sigma'_{\mathsf{S}}.\sigma$ and $\overline{\tau} = \overline{\tau}'\restriction_{ns}$.
Because of $\vdash_O \Sigma'_{\mathsf{S}} : noongoing$ and $\sigma' = \Sigma'_{\mathsf{S}}.\sigma$ we know that $\vdash \Sigma'_{\mathsf{S}} : fin$.
We thus have $(p,\sigma) \,\text{🕮}_{\mathsf{S}}^{\omega}\, \overline{\tau}' \in Beh_{\mathsf{S}}^{\mathcal{A}}(p)$.

□

I.2.1 Soundness.

Lemma 33 (S AM : Soundness of the AM semantics w.r.t. non-speculative semantics). *If*

(1) $\Sigma_{\mathsf{S}}.\sigma = \sigma$ *and*
(2) $\vdash_O \Sigma_{\mathsf{S}} : noongoing$ *and*
(3) $\Sigma_{\mathsf{S}} \Downarrow_{\mathsf{S}}^{\overline{\tau}} \Sigma'_{\mathsf{S}}$

Then there exists σ' such that

I if $\vdash_O \Sigma'_{\mathsf{S}} : noongoing$ *then* $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}\sigma'}$ *and* $\Sigma'_{\mathsf{S}}.\sigma = \sigma'$ *and*
II if $\vdash_O^i \Sigma'_{\mathsf{S}} : biggestongoingtransactionirolledback$ *then by definition exists id i such that it is the smallest transaction id that will be rolled back and is still active then* $\sigma \Downarrow_{helper(\overline{\tau},i)} \sigma'$ *and* σ' *is the configuration for the instance with* $ctr = i$.

Proof. We proceed by induction on $\Sigma_{\mathsf{S}} \Downarrow_{\mathsf{S}}^{\overline{\tau}} \Sigma'_{\mathsf{S}}$

Rule S:AM-Reflection Then we have $\Sigma_{\mathsf{S}} \Downarrow_{\mathsf{S}}^{\varepsilon} \Sigma_{\mathsf{S}}$ with $\Sigma'_{\mathsf{S}} = \Sigma_{\mathsf{S}}$ and by Rule NS-Reflection we have
I $\sigma \Downarrow_{\varepsilon\restriction_{ns}} \sigma'$ with $\sigma = \sigma'$.
II $\sigma \Downarrow_{helper(\varepsilon,i)} \sigma'$ with $\sigma = \sigma'$.

Rule S:AM-Single We have $\Sigma_{\mathsf{S}} \Downarrow_{\mathsf{S}}^{\overline{\tau}'\cdot\tau} \Sigma'_{\mathsf{S}}$ and by Rule S:AM-Single we get $\Sigma_{\mathsf{S}} \Downarrow_{\mathsf{S}}^{\overline{\tau}'} \Sigma''_{\mathsf{S}}$ and $\Sigma''_{\mathsf{S}} \overset{\tau}{\text{🕮}}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$.
We need to prove
I if $\vdash_O \Sigma'_{\mathsf{S}} : noongoing$ then $\sigma \Downarrow_{\overline{\tau}\cdot\tau\restriction_{ns}\sigma'}$ and $\Sigma'_{\mathsf{S}}.\sigma = \sigma'$
II if $\vdash_O^i \Sigma'_{\mathsf{S}} : biggestongoingtransactionirolledback$ then by definition exists *id i* such that it is the smallest transaction *id* that will be rolled back and is still active then $\sigma \Downarrow_{helper(\overline{\tau}\cdot\tau,i)} \sigma'$ and σ' is the configuration for the instance with $ctr = i$.
We apply the IH on $\Sigma_{\mathsf{S}} \Downarrow_{\mathsf{S}}^{\overline{\tau}'} \Sigma''_{\mathsf{S}}$ and have a σ'' where σ'' is the configuration for some instance in Σ''_{S} such that.
I' if $\vdash_O \Sigma''_{\mathsf{S}} : noongoing$ then $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}\sigma''}$ and $\Sigma''_{\mathsf{S}}.\sigma = \sigma''$
II' if $\vdash_O^j \Sigma''_{\mathsf{S}} : biggestongoingtransactionirolledback$ then by definition exists *id* j such that it is the smallest transaction *id* that will be rolled back and is still active then $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$ and σ'' is the configuration with the instance with $ctr = j$.
We proceed by case analysis on Σ''_{S}.
no ongoing transactions in Σ''_{S} Then Σ''_{S} has no ongoing transactions, meaning $\vdash_O \Sigma''_{\mathsf{S}} : noongoing$ and we have $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}} \sigma''$ and $\Sigma''_{\mathsf{S}}.\sigma = \sigma''$ by IH.

I Then $\vdash_O \Sigma'_{\mathsf{S}} : noongoing$ and we need to proof $\sigma \Downarrow_{\overline{\tau}\cdot\tau\restriction_{ns}\sigma'}$ and $\Sigma'_{\mathsf{S}}.\sigma = \sigma'$. We now proceed by inversion on $\Sigma''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}}^{O} \Sigma'_{\mathsf{S}}$:
Rule S:AM-Rollback Then $\tau = \texttt{rlb}\ id$.
Analogous to the corresponding case in Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

Rule S:AM-Store-Spec Then we know that $\overline{\rho} = \texttt{start}\ id \cdot \texttt{bypass}\ \Sigma''_S.\sigma(\mathbf{pc})$ for Σ'_S.
Analogous to the corresponding case in Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise We know that $\sigma'' = \Sigma''_S.\sigma$.
Analogous to the corresponding case in Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) together with Lemma 34 (S AM: Soundness single step No Speculation) with $\Sigma''_S \overset{\tau}{\rightsquigarrow}^{O}_S \Sigma'_S$.

II Then Σ'_S has ongoing transactions, meaning $\vdash^{i}_{O} \Sigma'_S$: *biggestongoingtransactionirolledback* and we need to proof $\sigma \Downarrow_{helper(\overline{\tau}\cdot\tau,i)} \sigma'$ and σ' is the configuration for the instance with $ctr = i$.
We now proceed by inversion on $\Sigma''_S \overset{\tau}{\rightarrow\!\!\!\!\!\!\diagup}_S \Sigma'_S$:

Rule S:AM-Store-Spec Then we know that $\overline{\rho} = \texttt{start}\ id \cdot \texttt{bypass}\ \Sigma''_S.\sigma(\mathbf{pc})$ for Σ'_S.
Analogous to the corresponding case in Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) together with Lemma 36 (S AM: Store step).

otherwise By definition of $\vdash^{i}_{O} \Sigma'_S$: *biggestongoingtransactionirolledback* we know that there exists a rlb i in the execution $\Sigma'_S \Downarrow^{\overline{\tau}_{fin}}_S \Sigma_{S\,fin}$ with no matching start i observation in that execution.
Analogous to the corresponding case in Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

ongoing transactions in Σ''_S Then Σ''_S has ongoing transactions, meaning $\vdash^{j}_{O} \Sigma''_S$: *biggestongoingtransactionirolledback* and we have $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$ and σ'' is the configuration for the instance with $ctr = j$.

I Then $\vdash_O \Sigma'_S$: *noongoing* and we need to proof $\sigma \Downarrow_{\overline{\tau}\cdot\tau\restriction_{ns}} \sigma'$ and $\Sigma'_S.\sigma = \sigma'$. We now proceed by inversion on $\Sigma''_S \overset{\tau}{\rightsquigarrow}^{O}_S \Sigma'_S$:

Rule S:AM-Rollback and τ = rlb j Analogous to the corresponding case in Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Then $\tau \neq \texttt{rlb}\ j$.
Analogous to the corresponding case in Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

II Then $\vdash^{i}_{O} \Sigma'_S$: *biggestongoingtransactionirolledback* and we need to proof $\sigma \Downarrow_{helper(\overline{\tau}\cdot\tau,i)} \sigma'$ and σ' is the configuration for the instance below the instance with $ctr = i$.
We now proceed by inversion on $\Sigma''_S \overset{\tau}{\rightarrow\!\!\!\!\!\!\diagup}_S \Sigma'_S$:

Rule S:AM-Rollback Then $\tau = \texttt{rlb}\ id$. We do a case analysis if $id = j$ or not.

$id = j$ Analogous to the corresponding case in Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

$id \neq j$ Analogous to the corresponding case in Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Then $\tau \neq \texttt{rlb}\ id$.
Analogous to the corresponding case in Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics)

□

Lemma 34 (S AM: Soundness single step No Speculation)**.** *If*

(1) $\vdash_O \Sigma_S$: *noongoing and*
(2) $\Sigma_S \overset{\tau}{\rightarrow\!\!\!\!\!\!\diagup}_S \Sigma'_S$ *and*
(3) $\vdash_O \Sigma'_S$: *noongoing and*
(4) $\sigma = \Sigma_S.\sigma$

Then there exists σ' such that

I $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ *and*
II $\Sigma'_S.\sigma = \sigma'$

and σ' is the configuration for some instance in Σ'_S.

Proof. We proceed by inversion on $\Sigma_S \overset{\tau}{\rightarrow\!\!\!\!\!\!\diagup}_S \Sigma'_S$:

Rule S:AM-General Thus, we have $\Sigma_S = \overline{\Phi}_S \cdot \Phi_{S\overline{\rho}'\cdot\tau}$. Contradiction. By the definition of $\overset{\tau}{\rightarrow\!\!\!\!\!\!\diagup}_S$ only Rule S:AM-Store-Spec adds observations to $\overline{\rho}$.
Since $\overline{\rho} = \overline{\rho}' \cdot \tau$ is non-empty, there is a speculative transaction currently ongoing.
However, this contradicts the assumption $\vdash_O \Sigma_S$: *noongoing*.

Rule S:AM-Rollback Contradiction, since $\vdash_O \Sigma_S$: *noongoing* and Definition 44 (Well orderedness of rollback and start).

Rule S:AM-Context We have $\Sigma_S = \overline{\Phi}_S \cdot \Phi_S$ and $\Sigma'_S = \overline{\Phi}''_S \cdot \overline{\Phi}'_S$ with $\Phi_S \overset{\tau}{\twoheadrightarrow}_S \overline{\Phi}'_S$. By Lemma 35 (S AM: Single Step Instance Non Speculative) we have $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma$ with $\sigma = \Phi_S.\sigma$ and $\overline{\Phi}'_S.\sigma = \sigma$.

□

Lemma 35 (S AM: Single Step Instance Non Speculative)**.** *If*

(1) $\Sigma_S = \overline{\Phi}_S \cdot \Phi_S$ *and*
(2) $\Sigma'_S = \overline{\Phi}_S \cdot \overline{\Phi}'_S$ *and* $\vdash_O \Sigma'_S$ *: noongoing and*
(3) $\Phi_S \overset{\tau}{\twoheadrightarrow}_S \overline{\Phi}'_S$ *and*
(4) $\sigma = \Phi_S.\sigma$

Then there is a σ' *such that*

I $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ *and*
II $\overline{\Phi}'_S.\sigma = \sigma$

Proof. We proceed by case analysis on the rule used to derive $\Phi''_S \overset{\tau}{\twoheadrightarrow}_S \Phi'_S$.

Rule S:AM-NoBranch, Rule S:AM-barr-spec, Rule S:AM-barr We have $p(\sigma(\mathbf{pc})) \neq \mathbf{store}\ x, e$ and $n \neq 0$. The case is analogous to the corresponding case in Lemma 29 (S SE: Single Step Instance Non Speculative).

Rule S:AM-Store-Spec Contradiction, because there are no ongoing transactions in Σ'_S by the fact $\vdash_O \Sigma'_S$ *: noongoing*.

□

Lemma 36 (S AM: Store step)**.** *If*

(1) $\Sigma_S = \overline{\Phi}_S \cdot \Phi_S$ *and* $\vdash_O \Sigma_S$ *: noongoing*
(2) $\Sigma'_S = \overline{\Phi}_S \cdot \overline{\Phi}'_S$ *and* $\vdash^i_O \Sigma'_S$ *: biggestongoingtransactionirolledback and*
(3) $\Phi_S \overset{\tau}{\twoheadrightarrow}_S \overline{\Phi}'_S$ *and*
(4) $\sigma = \Phi_S.\sigma$

Then

I $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ *and*
II σ' *is the configuration for the instance with* $ctr = i$ *in* Σ'_S

Proof. We proceed by inversion on $\Phi_S \overset{\tau}{\twoheadrightarrow}_S \overline{\Phi}'_S$:

Rule S:AM-Store-Spec By definition $\overline{\Phi}'_S = \langle p, ctr, \sigma_1, n\rangle \cdot \langle p, ctr+1, \sigma_2, n'\rangle_{\texttt{start}\ ctr \cdot \texttt{bypass}\ \sigma_1(\mathbf{pc}) \cdot}$.
Analogous to the corresponding case in Lemma 30 (S SE: Store step).

otherwise Contradiction, because $\vdash_O \Sigma_S$ *: noongoing* and $\vdash^i_O \Sigma'_S$ *: biggestongoingtransactionirolledback*, we know that a speculative transaction has to be started that will be rolled back.

□

I.2.2 Completeness.

Lemma 37 (S AM: Completeness of the speculative semantics)**.** *If*

(1) $\sigma \in InitConf$ *and*
(2) $\sigma \Downarrow_{\overline{\tau}} \sigma'$ *and*
(3) $\Sigma_S = \Sigma^{init}_S p, \sigma$

Then

I $\Sigma_S \Downarrow^{\overline{\tau}'}_S \Sigma'_{S_\rho}$ *and*
II $\vdash_O \Sigma'_S$ *: noongoing and*
III $\sigma' = \Sigma'_S.\sigma$ *and*
IV $\overline{\tau} = \overline{\tau}'\restriction_{ns}$ *and*
V $\rho = \varepsilon$

Proof. We proceed by induction on $\sigma \Downarrow_{\overline{\tau}} \sigma'$

Rule NS-Reflection Then we have $\sigma \Downarrow_\varepsilon \sigma'$ with $\sigma = \sigma'$.
I - IV By Rule S:Reflection we have $\Sigma_S \Downarrow^\varepsilon_S \Sigma_S$. By construction $\vdash_O \Sigma_S$ *: noongoing* and $\Sigma_S.\sigma = \sigma$. Since $\varepsilon\restriction_{ns} = \varepsilon$ we are finished.

Rule NS-Single Then we have $\sigma \Downarrow_{\overline{\tau}} \sigma''$ and $\sigma'' \xrightarrow{\tau} \sigma'$.
We need to show

I $\Sigma_S \Downarrow_S^{\overline{\tau}'\cdot\tau'} \Sigma'_S$ and
II $\vdash_O \Sigma'_S$: *noongoing* and
III $\sigma' = \Sigma'_S.\sigma$ and
IV $\overline{\tau}\cdot\tau = \overline{\tau}'\cdot\tau'\restriction_{ns}$
V $\rho = \varepsilon$
We apply the IH on $\sigma \Downarrow_{\overline{\tau}} \sigma''$ we get
I' $\Sigma_S \Downarrow_S^{\overline{\tau}'} \Sigma''_{S\,\rho}$ and
II' $\vdash_O \Sigma''_{S\,\rho}$: *noongoing* and
III' $\sigma'' = \Sigma''_S.\sigma$ and
IV' $\overline{\tau} = \overline{\tau}'\restriction_{ns}$
V' $\rho = \varepsilon$
We now do a case analysis on the instruction $p(\sigma(\mathbf{pc}))$:
$p(\sigma(\mathbf{pc})) \neq \mathbf{store}\ x, e$ Analogous to the corresponding case in Lemma 31 (S SE: Completeness of the speculative semantics).
$p(\sigma(\mathbf{pc})) = \mathbf{store}\ x, e$ Analogous to the corresponding case Lemma 31 (S SE: Completeness of the speculative semantics), which is when the oracle mispredicted in the proof, together with Lemma 38 (S AM : Non-speculative execution for rolled back transactions).
Notice that ρ is empty for all the cases, because we discharge all the observations immediately using Rule S:AM-General.

□

Lemma 38 (S AM : Non-speculative execution for rolled back transactions.)**.** *If*

(1) $\Sigma_S \Downarrow_S^{\overline{\tau}} \Sigma'_S$ *and*
(2) $\overline{\tau} = \tau\cdot$ `start` $id\cdot\overline{\tau}'\cdot$ `rlb` id *and*
(3) $\sigma = \Sigma_S.\sigma$

Then

I there is a configurations σ' *with* $\Sigma'_S.\sigma = \sigma'$ *and*
II $\sigma \xrightarrow{\overline{\tau}\restriction_{ns}} \sigma'$ *and*
III $\overline{\tau}\restriction_{ns} = \tau$

Proof. Let $\Sigma_S \Downarrow_S^{\overline{\tau}} \Sigma'_S$ be an execution with trace $\overline{\tau} = \tau\cdot$ `start` $id\cdot\overline{\tau}'\cdot$ `rlb` id. Let $\sigma = \Sigma_S.\sigma$
The proof proceeds analogously to Lemma 32 (S SE: Non-speculative execution for rolled back transactions). □

I.3 S: Relating Symbolic and AM semantics

Theorem 16 (S : Behaviour of AM and symbolic semantics). $Beh^{\mathcal{A}}_{\mathsf{S}}(p) = \mu(Beh^{\mathcal{S}}_{\mathsf{S}}(p))$

Proof. The proposition can be proven in similar fashion to Theorem 14 (S SE: Behaviour of non-speculative and oracle semantics). We prove the two directions separately:

$\Leftarrow$ Assume that $(p, \sigma)\ {}_{\alpha}\!\!\oslash^{\omega}_{\mathsf{S}}\ \overline{\tau} \in Beh^{\mathcal{S}}_{\mathsf{S}}(p)$.

We thus know there exists $\vdash \Sigma^{\mathcal{S}'}_{\mathsf{S}} : \mathit{fin}$ such that $\Sigma^{\mathit{init}}_{\mathsf{S}}(p, \sigma_{\mathcal{S}})\ {}_{\alpha}\Downarrow^{\overline{\tau}}_{\mathsf{S}}\ \Sigma^{\mathcal{S}'}_{\mathsf{S}}$ and $\mu \vDash \mathit{pthCnd}(\overline{\tau_\alpha})$. We now apply Lemma 39 (S: Soundness of the AM semantics w.r.t. symbolic semantics) on $\Sigma^{\mathit{init}}_{\mathsf{S}}(p, \sigma_{\mathcal{S}})\ {}_{\alpha}\Downarrow^{\overline{\tau}}_{\mathsf{S}}\ \Sigma^{\mathcal{S}'}_{\mathsf{S}}$ and get $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$, $\mu(\Sigma^{\mathcal{S}'}_{\mathsf{S}}) = \Sigma'_{\mathsf{S}}$ and $\mu(\overline{\tau_\alpha}) = \overline{\tau}$

Since $\vdash \Sigma^{\mathcal{S}'}_{\mathsf{S}} : \mathit{fin}$ and $\mu(\Sigma^{\mathcal{S}'}_{\mathsf{S}}) = \Sigma'_{\mathsf{S}}$ we have $\vdash \Sigma'_{\mathsf{S}} : \mathit{fin}$ as well.

Thus, $(p, \mu(\sigma_{\mathcal{S}}))\ \oslash^{\omega}_{\mathsf{S}}\ \mu(\overline{\tau_\alpha}) \in Beh^{\mathcal{A}}_{\mathsf{S}}(p)$.

$\Rightarrow$ Assume that $(p, \sigma)\ \oslash^{\omega}_{\mathsf{S}}\ \overline{\tau} \in Beh^{\mathcal{A}}_{\mathsf{S}}(p)$. We thus know there exists $\vdash \Sigma'_{\mathsf{S}} : \mathit{fin}$ such that $\Sigma^{\mathit{init}}_{\mathsf{S}}(p, \sigma) \Downarrow^{\overline{\tau}}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$.

We now apply Lemma 41 (S: Completeness of the symbolic semantics) on $\Sigma^{\mathit{init}}_{\mathsf{S}}(p, \sigma) \Downarrow^{\overline{\tau}}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ and get

$$\begin{aligned} \Sigma^{\mathit{init}}_{\mathsf{S}}(p, \sigma) &= \mu(\Sigma^{\mathcal{S}}_{\mathsf{S}}) \\ \Sigma^{\mathcal{S}}_{\mathsf{S}}\ {}_{\alpha}\Downarrow^{\overline{\tau_\alpha}}_{\mathsf{S}}\ \Sigma^{\mathcal{S}'}_{\mathsf{S}} & \\ \Sigma'_{\mathsf{S}} &= \mu(\Sigma^{\mathcal{S}'}_{\mathsf{S}}) \\ \overline{\tau} &= \mu(\overline{\tau_\alpha}) \\ \mu \vDash \mathit{pthCnd}(\overline{\tau}') & \end{aligned}$$

Since $\vdash \Sigma'_{\mathsf{S}} : \mathit{fin}$ and $\mu(\Sigma^{\mathcal{S}'}_{\mathsf{S}}) = \Sigma'_{\mathsf{S}}$ we have $\vdash \Sigma^{\mathcal{S}'}_{\mathsf{S}} : \mathit{fin}$ as well.

Thus, $(p, \sigma_{\mathcal{S}})\ {}_{\alpha}\!\!\oslash^{\omega}_{\mathsf{S}}\ \overline{\tau_\alpha} \in Beh^{\mathcal{S}}_{\mathsf{S}}(p)$ and we are done, since $(p, \mu(\sigma_{\mathcal{S}}))\ {}_{\alpha}\!\!\oslash^{\omega}_{\mathsf{S}}\ \mu(\overline{\tau_\alpha}) = (p, \sigma)\ \oslash^{\omega}_{\mathsf{S}}\ \overline{\tau}$.

□

Now onto theorems for the new speculative semantics. We want to show Soundness and Completeness.
We lift $\mu()$ to speculative states $\Sigma^{\mathcal{S}}_{\mathsf{S}}$ in the following way by applying $\mu()$ pointwise for each instance in the state $\Sigma^{\mathcal{S}}_{\mathsf{S}}$.

I.4 Soundness

Lemma 39 (S: Soundness of the AM semantics w.r.t. symbolic semantics)**.** *If*

(1) $\Sigma^{\mathcal{S}}_{\mathsf{S}}\ {}_{\alpha}\Downarrow^{\overline{\tau_\alpha}}_{\mathsf{S}}\ \Sigma^{\mathcal{S}'}_{\mathsf{S}}$ *and*

(2) $\mu \vDash \mathit{pthCnd}(\Sigma^{\mathcal{S}'}_{\mathsf{S}})$

Then

I $\mu(\Sigma^{\mathcal{S}}_{\mathsf{S}}) \Downarrow^{\mu(\overline{\tau_\alpha})}_{\mathsf{S}} \mu(\Sigma^{\mathcal{S}'}_{\mathsf{S}})$ *and*

Proof. We proceed by induction on $\Sigma^{\mathcal{S}}_{\mathsf{S}}\ {}_{\alpha}\Downarrow^{\overline{\tau_\alpha}}_{\mathsf{S}}\ \Sigma^{\mathcal{S}'}_{\mathsf{S}}$

Rule S:Sym-Reflection Then we have $\Sigma^{\mathcal{S}}_{\mathsf{S}}\ {}_{\alpha}\Downarrow^{\varepsilon}_{\mathsf{S}}\ \Sigma^{\mathcal{S}'}_{\mathsf{S}}$ with $\Sigma^{\mathcal{S}'}_{\mathsf{S}} = \Sigma^{\mathcal{S}}_{\mathsf{S}}$. Using Rule S:AM-Reflection we get $\mu(\Sigma^{\mathcal{S}}_{\mathsf{S}})\ {}_{\alpha}\Downarrow^{\mu(\varepsilon)}_{\mathsf{S}}\ \mu(\Sigma^{\mathcal{S}'}_{\mathsf{S}})$ and are finished.

Rule S:Sym-Single We have $\Sigma^{\mathcal{S}}_{\mathsf{S}}\ {}_{\alpha}\Downarrow^{\overline{\tau_\alpha}' \cdot \tau_{\mathcal{S}}}_{\mathsf{S}}\ \Sigma^{\mathcal{S}'}_{\mathsf{S}}$ and by Rule S:Sym-Single we get $\Sigma^{\mathcal{S}}_{\mathsf{S}}\ {}_{\alpha}\Downarrow^{\overline{\tau_\alpha}'}_{\mathsf{S}}\ \Sigma^{\mathcal{S}''}_{\mathsf{S}}$ and $\Sigma^{\mathcal{S}''}_{\mathsf{S}}\ \overset{\tau}{=\!\!\oslash}_{\mathsf{S}}\ \Sigma^{\mathcal{S}'}_{\mathsf{S}}$.

We need to prove

(1) $\mu(\Sigma^{\mathcal{S}}_{\mathsf{S}}) \Downarrow^{\mu(\overline{\tau} \cdot \tau_{\mathcal{S}})}_{\mathsf{S}} \mu(\Sigma^{\mathcal{S}'}_{\mathsf{S}})$

We apply the IH on $\Sigma^{\mathcal{S}}_{\mathsf{S}}\ {}_{\alpha}\Downarrow^{\overline{\tau_\alpha}}_{\mathsf{S}}\ \Sigma^{\mathcal{S}''}_{\mathsf{S}}$ and have a $\Sigma''_{\mathsf{S}} = \mu(\Sigma^{\mathcal{S}''}_{\mathsf{S}})$ such that:

(1) $\mu(\Sigma^{\mathcal{S}}_{\mathsf{S}}) \Downarrow^{\mu(\overline{\tau_\alpha})}_{\mathsf{S}} \Sigma''_{\mathsf{S}}$ and

The result follows by applying Lemma 40 (S: Soundness single step) on $\Sigma^{\mathcal{S}''}_{\mathsf{S}}\ \overset{\tau_{\mathcal{S}}}{=\!\!\oslash}_{\mathsf{S}}\ \Sigma^{\mathcal{S}'}_{\mathsf{S}}$ and get a step $\Sigma''_{\mathsf{S}}\ \overset{\mu(\tau_{\mathcal{S}})}{=\!\!=\!\!\oslash}_{\mathsf{S}}\ \mu(\Sigma^{\mathcal{S}'}_{\mathsf{S}})$. We now use Rule S:AM-Single and get an execution $\mu(\Sigma^{\mathcal{S}}_{\mathsf{S}}) \Downarrow^{\mu(\overline{\tau_\alpha}) \cdot \mu(\tau_{\mathcal{S}})}_{\mathsf{S}} \mu(\Sigma^{\mathcal{S}'}_{\mathsf{S}})$ as required.

□

Lemma 40 (S: Soundness single step)**.** *If*

(1) $\Sigma^{\mathcal{S}}_{\mathsf{S}}\ \overset{\tau}{=\!\!\oslash}_{\mathsf{S}}\ \Sigma^{\mathcal{S}}_{\mathsf{S}}$ *and*

(2) $\mu \vDash \mathit{pthCnd}(\Sigma^{\mathcal{S}'}_{\mathsf{S}})$

Then

I $\mu(\Sigma_S^{\mathcal{S}}) \xrightarrow{\mu(\tau)}_S \mu(\Sigma_S^{\mathcal{S}\prime})$

Proof. We proceed by inversion on $\Sigma_S^{\mathcal{S}} \xrightarrow{\tau}_S^{\mathcal{S}} \Sigma_S^{\mathcal{S}\prime}$:

Rule S:Sym-Rollback Since $\mu()$ does not change the speculation window and *ctr* and $\mu(\Sigma_S^{\mathcal{S}}) = \Sigma_S$, we have $\Sigma_S.n = \Sigma_S^{\mathcal{S}}.n = 0$ and $\Sigma_S.ctr = \Sigma_S^{\mathcal{S}}.ctr$.

$\Sigma_S \xrightarrow{\tau'}_S \Sigma_S^{\mathcal{S}\prime}$ We can use Rule S:AM-Rollback to derive $\Sigma_S \xrightarrow{\tau'}_S \Sigma_S'$.

$\mu(\Sigma_S^{\mathcal{S}\prime}) = \Sigma_S'$ The rule only deletes the topmost instance and changes the *ctr* of the instance below. Since $\Sigma_S.ctr = \Sigma_S^{\mathcal{S}}.ctr$, we have $\mu(\Sigma_S^{\mathcal{S}\prime}) = \Sigma_S'$

$\mu \vDash pthCnd(\Sigma_S^{\mathcal{S}\prime})$ **and** $\mu(\tau') = \tau$ Since the $\Sigma_S.ctr = \Sigma_S^{\mathcal{S}}.ctr$ we already have $\mu(\tau') = \tau$. For $\mu \vDash pthCnd(\Sigma_S^{\mathcal{S}\prime})$, notice that $\mu \vDash pthCnd(\Sigma_S^{\mathcal{S}\prime}) = \mu \vDash pthCnd(\Sigma_S^{\mathcal{S}})$ because the rule only deletes a speculative instance. Thus, we are finished.

Rule S:Sym-Context We then have $\Phi_S^{\mathcal{S}} \xrightarrow{\tau}_S^{\mathcal{S}} \overline{\Phi}'_{S_{\mathcal{S}}}$. Thus, we know $\Phi_S^{\mathcal{S}} > 0$ and $\mu(\Phi_S^{\mathcal{S}}) > 0$ as well. We proceed by inversion on $\Phi_S^{\mathcal{S}} \xrightarrow{\tau_S}_S^{\mathcal{S}} \overline{\Phi}'_{S_{\mathcal{S}}}$:

Rule S:Sym-General Then $\Phi_S^{\mathcal{S}} \xrightarrow{\tau_S}_S^{\mathcal{S}} \Phi_{S\overline{\rho_{\mathcal{S}}}\backslash\tau_S}$. By $\mu(\Phi_S^{\mathcal{S}}) = \Phi_S$ we know that $\mu(\overline{\rho_{\mathcal{S}}}) = \overline{\rho}$. Furthermore, $\overline{\rho_{\mathcal{S}}}$ is non-empty because the rule was used. This means $\overline{\rho}$ is non-empty as well. This means Rule S:AM-General applies. Since that rule does not change the state Φ_S except for $\overline{\rho}$ we have $\Phi_S \xrightarrow{\tau}_S \Phi_{S\overline{\rho}\backslash\tau}$.
Now we have $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu(\Phi_S^{\mathcal{S}}{}_{\overline{\rho_{\mathcal{S}}}\backslash\tau_{\mathcal{S}}}) = \Phi_{S\overline{\rho}\backslash\tau}$ by construction.

Rule S:Sym-NoBranch Then we have $\Phi_S^{\mathcal{S}} \xrightarrow{\tau_S}_S^{\mathcal{S}} \Phi_S^{\mathcal{S}\prime}$ where $\Phi_S^{\mathcal{S}\prime} = \langle p, \Phi_S^{\mathcal{S}}.ctr, \Phi_S^{\mathcal{S}}.\sigma'_{\mathcal{S}}, \Phi_S^{\mathcal{S}}.n - 1\rangle$ with $\Phi_S^{\mathcal{S}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_S}^{\mathcal{S}} \sigma'_{\mathcal{S}}$.
Since we have $\mu \vDash pthCnd(\overline{\Phi}_{S_{\mathcal{S}}}.\sigma_{\mathcal{S}})$ (by assumption) we can use Lemma 17 (Non-spec: Soundness to symbolic) on $\Phi_S^{\mathcal{S}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_S}^{\mathcal{S}} \sigma'_{\mathcal{S}}$ and get $\mu(\Phi_S^{\mathcal{S}}\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_S)} \mu(\sigma'_{\mathcal{S}})$, where $\mu(\Phi_S.\sigma_{\mathcal{S}}) = \Phi_S.\sigma$ as per assumption.
We can now use Rule S:AM-NoBranch to derive the step $\mu(\Phi_S^{\mathcal{S}}) \xrightarrow{\mu(\tau_S)}_S \mu(\Phi_S^{\mathcal{S}\prime})$ using the derived $\xrightarrow{\mu(\tau_S)}$ step.

Rule S:Sym-barr Then we have $\Phi_S^{\mathcal{S}} \xrightarrow{\tau_S}_S^{\mathcal{S}} \Phi_S^{\mathcal{S}\prime}$ where $\Phi_S^{\mathcal{S}\prime} = \langle p, \Phi_S^{\mathcal{S}}.ctr, \Phi_S^{\mathcal{S}}.\sigma'_{\mathcal{S}}, \Phi_S^{\mathcal{S}}.n - 1\rangle$ with $\Phi_S^{\mathcal{S}}.\sigma \xrightarrow{\tau_S}^{\mathcal{S}} \sigma'_{\mathcal{S}}$. Analogous to Rule S:Sym-NoBranch using Rule S:AM-barr.

Rule S:Sym-barr-spec Then we have $\Phi_S^{\mathcal{S}} \xrightarrow{\tau_S}_S^{\mathcal{S}} \Phi_S^{\mathcal{S}\prime}$ where $\Phi_S^{\mathcal{S}\prime} = \langle p, \Phi_S^{\mathcal{S}}.ctr, \Phi_S^{\mathcal{S}}.\sigma'_{\mathcal{S}}, \Phi_S^{\mathcal{S}}.n - 1\rangle$ with $\Phi_S^{\mathcal{S}}.\sigma \xrightarrow{\tau_S}^{\mathcal{S}} \sigma'_{\mathcal{S}}$. Analogous to case Rule S:Sym-NoBranch using Rule S:AM-barr-spec.

Rule S:Sym-Store-Spec We have $\Phi_S^{\mathcal{S}} \xrightarrow{\tau_S}_S^{\mathcal{S}} \overline{\Phi}_{S_{\mathcal{S}}\overline{\rho_{\mathcal{S}}}\cdot\texttt{bypass}\ \Phi_S^{\mathcal{S}}.\mathbf{pc}\cdot\texttt{start}\ \Phi_S^{\mathcal{S}}.ctr}$ where $\overline{\Phi}_{S_{\mathcal{S}}} = \langle p, \Phi_S^{\mathcal{S}}.ctr, \sigma'_{\mathcal{S}}, \Phi_S^{\mathcal{S}}.n - 1\rangle \cdot \langle p, \Phi_S^{\mathcal{S}}.ctr + 1, \sigma''_{\mathcal{S}}, \min \Phi_S^{\mathcal{S}}.n, \omega\rangle$. Furthermore, we have $\Phi_S^{\mathcal{S}}.\sigma \xrightarrow{\tau_S} \sigma'_{\mathcal{S}}$ and $\sigma''_{\mathcal{S}} = \sigma_{\mathcal{S}}[\mathbf{pc} \mapsto \Phi_S^{\mathcal{S}}.\sigma_{\mathcal{S}}(\mathbf{pc}) + 1]$ (note that **pc** is always concrete).
We use Lemma 17 (Non-spec: Soundness to symbolic) on $\Phi_S^{\mathcal{S}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_S}^{\mathcal{S}} \sigma'_{\mathcal{S}}$ and get $\mu(\Phi_S^{\mathcal{S}}.\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_S)}^{\mathcal{S}} \mu(\sigma'_{\mathcal{S}})$.
Choose $\Phi_S = \mu(\Phi_S^{\mathcal{S}})$ and note that a **store**instruction is executed. We now derive a step using Rule S:AM-Store-Spec together with the non-speculative step $\mu(\Phi_S^{\mathcal{S}}.\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_S)}^{\mathcal{S}} \mu(\sigma'_{\mathcal{S}})$ above and define $\sigma'' = \sigma[\mathbf{pc} \mapsto \sigma(\mathbf{pc}) + 1]$: $\Phi_S \xrightarrow{\mu(\tau_S)}_S \overline{\Phi}_S$ with $\overline{\Phi}_S = \langle p, \Phi_S.ctr, \sigma', \Phi_S.n - 1\rangle \cdot \langle p, \Phi_S.ctr + 1, \sigma'', \min \Phi_S.n, \omega\rangle$.
We now show that $\mu(\overline{\Phi}_{S_{\mathcal{S}}}) = \overline{\Phi}_S$. Since **pc** is concrete and $\mu(\Phi_S^{\mathcal{S}}.\sigma) = \sigma$, it follow that $\mu(\sigma''_{\mathcal{S}}) = \sigma''$.
By $\mu(\Phi_S^{\mathcal{S}}) = \Phi_S$ we have $\Phi_S^{\mathcal{S}}.ctr = \Phi_S.ctr$ and $\Phi_S^{\mathcal{S}}.n = \Phi_S.n$.
Now, we have $\mu(\overline{\Phi}_{S_{\mathcal{S}}}) = \overline{\Phi}_S$ and thus $\mu(\Phi_S^{\mathcal{S}}) \xrightarrow{\mu(\tau_S)}_S \mu(\overline{\Phi}_{S_{\mathcal{S}}})$ as needed.

□

I.4.1 *Completeness.*

Lemma 41 (S: Completeness of the symbolic semantics)**.** *If*

(1) $\Sigma_S \Downarrow_S^{\overline{\tau}} \Sigma_S'$ *and*
(2) $\Sigma_S = \mu(\Sigma_S^{\mathcal{S}})$

Then there is a valuation $\mu()$*, a symbolic trace* $\overline{\tau}'$ *and a final state* $\Sigma_S^{\mathcal{S}\prime}$ *such that*

I $\Sigma_S^{\mathcal{S}} {}_{\alpha}\Downarrow_S^{\overline{\tau}'} \Sigma_S^{\mathcal{S}\prime}$ *and*
II $\Sigma_S' = \mu(\Sigma_S^{\mathcal{S}\prime})$ *and* $\overline{\tau} = \mu(\overline{\tau}')$ *and*

III $\mu \vDash pthCnd(\Sigma_S^{\mathcal{S}'})$

Proof. We proceed by induction on $\Sigma_S \Downarrow_S^{\overline{\tau}} \Sigma'_S$

Rule S:AM-Reflection Then we have $\Sigma_S \Downarrow_S^{\varepsilon} \Sigma'_S$ with $\Sigma_S = \Sigma'_S$.

I - III By Rule S:Sym-Reflection we have $\Sigma_S^{\mathcal{S}} {}_{\alpha}\Downarrow_S^{\varepsilon} \Sigma_S^{\mathcal{S}'}$. By construction $\Sigma_S^{\mathcal{S}'} = \Sigma_S^{\mathcal{S}'}$. We now trivially satisfy all conditions.

Rule S:AM-Single We have $\Sigma_S \Downarrow_S^{\overline{\tau}'\cdot\tau} \Sigma'_S$ and by Rule S:AM-Single we get $\Sigma_S \Downarrow_S^{\overline{\tau_\alpha}'} \Sigma''_S$ and $\Sigma''_S \overset{\tau}{\dashrightarrow}_S^{\mathcal{S}} \Sigma'_S$.

We need to prove

(1) $\Sigma_S^{\mathcal{S}} {}_{\alpha}\Downarrow_S^{\overline{\tau_\alpha}'\cdot\tau_S} \Sigma_S^{\mathcal{S}'}$ and
(2) $\Sigma'_S = \mu(\Sigma_S^{\mathcal{S}'})$ and $\overline{\tau}' \cdot \tau = \mu(\overline{\tau_\alpha}' \cdot \tau_{\mathcal{S}})$ and
(3) $\mu \vDash pthCnd(\Sigma_S^{\mathcal{S}'})$

We apply the IH on $\Sigma_S \Downarrow_S^{\overline{\tau_\alpha}'} \Sigma''_S$ and have a $\Sigma_S^{\mathcal{S}''}$ such that:

(1) $\Sigma_S^{\mathcal{S}} {}_{\alpha}\Downarrow_S^{\overline{\tau_\alpha}'} \Sigma_S^{\mathcal{S}''}$ and
(2) $\Sigma''_S = \mu(\Sigma_S^{\mathcal{S}''})$ and $\overline{\tau}' = \mu(\overline{\tau_\alpha}')$ and
(3) $\mu \vDash pthCnd(\Sigma_S^{\mathcal{S}''})$

The result follows from applying Lemma 42 (S: Completeness single step) on $\Sigma''_S \overset{\tau}{\dashrightarrow}_S \Sigma'_S$:

□

Lemma 42 (S: Completeness single step)**.** *If*

(1) $\Sigma_S \overset{\tau}{\dashrightarrow}_S \Sigma'_S$ *and*
(2) $\mu(\Sigma_S^{\mathcal{S}}) = \Sigma_S$ *and*
(3) $\mu \vDash pthCnd(\Sigma_S^{\mathcal{S}})$

Then

I $\Sigma_S^{\mathcal{S}} \overset{\tau'}{\dashrightarrow}_S^{\mathcal{S}} \Sigma_S^{\mathcal{S}'}$ *and*
II $\mu(\Sigma_S^{\mathcal{S}'}) = \Sigma'_S$ *and*
III $\mu \vDash pthCnd(\Sigma_S^{\mathcal{S}'})$ *and* $\mu(\tau') = \tau$

Proof. We proceed by inversion on $\Sigma_S \overset{\tau}{\dashrightarrow}_S \Sigma'_S$:

Rule S:AM-Rollback Since $\mu()$ does not change the speculation window and *ctr* and $\mu(\Sigma_S^{\mathcal{S}}) = \Sigma_S$, we have $\Sigma_S.n = \Sigma_S^{\mathcal{S}}.n = 0$ and $\Sigma_S.ctr = \Sigma_S^{\mathcal{S}}.ctr$.

$\Sigma_S^{\mathcal{S}} \overset{\tau'}{\dashrightarrow}_S^{\mathcal{S}} \Sigma_S^{\mathcal{S}'}$ We can use the rule Rule S:Sym-Rollback in the symbolic semantics to derive $\Sigma_S^{\mathcal{S}} \overset{\tau'}{\dashrightarrow}_S^{\mathcal{S}} \Sigma_S^{\mathcal{S}'}$.

$\mu(\Sigma_S^{\mathcal{S}'}) = \Sigma'_S$ The rule Rule S:Sym-Rollback only deletes the topmost instance and changes the *ctr* of the instance below. Since $\Sigma_S.ctr = \Sigma_S^{\mathcal{S}}.ctr$, we have $\mu(\Sigma_S^{\mathcal{S}'}) = \Sigma'_S$

$\mu \vDash pthCnd(\tau')$ **and** $\mu(\tau') = \tau$ Since the $\Sigma_S.ctr = \Sigma_S^{\mathcal{S}}.ctr$ we already have $\mu(\tau') = \tau$. For $\mu \vDash pthCnd(\Sigma_S^{\mathcal{S}'})$, notice that $\mu \vDash pthCnd(\Sigma_S^{\mathcal{S}'}) = \mu \vDash pthCnd(\Sigma_S^{\mathcal{S}})$ because the rule only deletes a speculative instance. Thus, we are finished.

Rule S:AM-Context We then have $\Phi_S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_S$. Note that $\Phi_S.n > 0$ and as such for all symbolic states where $\mu(\Phi_S^{\mathcal{S}}) = \Phi_S$ as well. We proceed by inversion on $\Phi_S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_S$:

Rule S:AM-General Then $\Phi_S \overset{\tau}{\dashrightarrow}_S \Phi_{S\overline{\rho}\setminus\tau}$. By $\mu(\Phi_S^{\mathcal{S}}) = \Phi_S$ we know that $\mu(\overline{\rho_{\mathcal{S}}}) = \overline{\rho}$. Furthermore, $\overline{\rho}$ is non-empty because the rule was used. This means $\overline{\rho_{\mathcal{S}}}$ is non-empty as well. This means Rule S:Sym-General applies. Since that rule does not change the state $\Phi_S^{\mathcal{S}}$ except for $\overline{\rho}$ we have $\Phi_S^{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\dashrightarrow}_S^{\mathcal{S}} \Phi_{S\overline{\rho_{\mathcal{S}}}\setminus\tau_{\mathcal{S}}}^{\mathcal{S}}$.

Now we have $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu(\Phi_{S\overline{\rho}\setminus\tau_{\mathcal{S}}}^{\mathcal{S}}) = \Phi_{S\overline{\rho}\setminus\tau}$ by construction.

Rule S:AM-barr Then we have $\Phi_S \overset{\tau}{\dashrightarrow}_S \Phi'_S$ where $\Phi'_S = \langle p, \Phi_S.ctr, \Phi_S.\sigma', \Phi_S.n-1\rangle$ with $\Phi_S.\sigma \xrightarrow{\tau} \sigma'$. We use Lemma 18 (Non-spec : Completeness to symbolic) on $\Phi_S.\sigma \rightarrow \sigma'$ and get $\Phi_S^{\mathcal{S}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}^{\mathcal{S}} \sigma'_{\mathcal{S}}$, where $\mu(\Phi_S) = \Phi_S$ as per assumption, $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu(\sigma'_{\mathcal{S}}) = \sigma'$. Now choose $\Phi_S^{\mathcal{S}'}.\sigma = \sigma'_{\mathcal{S}}$ and let it otherwise be equal to Φ'_S. We can now use Rule S:Sym-barr to derive the step $\Phi_S^{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\dashrightarrow}_S^{\mathcal{S}} \Phi_S^{\mathcal{S}'}$ using the derived $\rightarrow^{\mathcal{S}}$ step and trivially satisfy $\mu(\Phi_S^{\mathcal{S}'}) = \Phi'_S$.

Rule S:AM-barr-spec Analogous to the barrier case above.

Rule S:AM-NoBranch The case is analogous to Rule S:AM-barr above using Rule S:Sym-NoBranch.

Rule S:AM-Store-Spec We have $\Phi_S \overset{\tau}{\leadsto}_S \overline{\Phi}_{S\overline{\rho}\cdot\texttt{bypass}\ \Phi_S.\mathbf{pc}\cdot\texttt{start}\ \Phi_S.ctr}$ where $\overline{\Phi}_S = \langle p, \Phi_S.ctr, \sigma', \Phi_S.n-1\rangle \cdot \langle p, \Phi_S.ctr+1, \sigma'', \min \Phi_S.n, \omega\rangle$. Furthermore, we have $\Phi_S.\sigma \rightarrow \sigma'$ and $\sigma'' = \sigma[\mathbf{pc} \mapsto \Phi_S.\sigma(\mathbf{pc})+1]$

We use Lemma 18 (Non-spec : Completeness to symbolic) on $\Phi_S.\sigma \xrightarrow{\tau} \sigma'$ and get $\Phi_S^{\mathcal{S}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}{}^{\mathcal{S}} \sigma'_{\mathcal{S}}$, where $\mu(\Phi_S^{\mathcal{S}}) = \Phi_S$ as per assumption, $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu(\sigma'_{\mathcal{S}}) = \sigma'$.
Next, we define $\sigma''_{\mathcal{S}} = \Phi_S^{\mathcal{S}}.\sigma_{\mathcal{S}}[\mathbf{pc} \mapsto \Phi_S.\sigma(\mathbf{pc})+1]$ (per assumption **pc** is concrete).
It follows that $\mu(\sigma''_{\mathcal{S}}) = \sigma''$ by $\mu(\Phi_S^{\mathcal{S}}.\sigma) = \sigma$.

Since a **store** is executed, we can use Rule S:Sym-Store-Spec to derive a step and get $\Phi_S^{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\leadsto}{}_S^{\mathcal{S}} \langle p, \Phi_S^{\mathcal{S}}.ctr+1, \Phi_S^{\mathcal{S}}.\sigma_{\mathcal{S}}, \Phi_S^{\mathcal{S}}.n-1\rangle \cdot \langle p, \Phi_S^{\mathcal{S}}.ctr+1, \sigma''_{\mathcal{S}}, \min \Phi_S^{\mathcal{S}}.n, \omega\rangle_{\overline{\rho}\cdot\texttt{bypass}\ \Phi_S^{\mathcal{S}}.\mathbf{pc}\cdot\texttt{start}\ \Phi_S^{\mathcal{S}}.ctr}$.
By $\mu(\Phi_S^{\mathcal{S}}) = \Phi_S$ we have $\Phi_S^{\mathcal{S}}.ctr = \Phi_S.ctr$ and $\Phi_S^{\mathcal{S}}.n = \Phi_S.n$.
Now, we have $\mu(\overline{\Phi}_{S_{\mathcal{S}}}) = \overline{\Phi}_S$ and $\mu(\tau_{\mathcal{S}}) = \tau$.
It remains to show that $\mu \models pthCnd(\overline{\Phi}_{S_{\mathcal{S}}})$. Since $\overline{\Phi}_{S_{\mathcal{S}}}.\sigma_{\mathcal{S}} = \sigma''_{\mathcal{S}}$, $\sigma''_{\mathcal{S}}.\delta^{\mathcal{S}} = \sigma'_{\mathcal{S}}.\delta^{\mathcal{S}}$ and we have $\mu \models pthCnd(\sigma'_{\mathcal{S}})$ from above we have $\mu \models pthCnd(\overline{\Phi}_{S_{\mathcal{S}}})$.

□

I.5 S: Relating Oracle Semantics and AM Semantics

We define a few Lemmas

Lemma 43 (S AM: Single step preserves ≅). *If*

(1) $\Sigma_{S1} \cong \Sigma_{S2}$ *and*
(2) $\Sigma_{S1} \overset{\tau}{\leadsto}_S \Sigma'_S$ *and* $\Sigma_{S2} \overset{\tau}{\leadsto}_S \Sigma''_S$

Then

(1) $\Sigma'_S \cong \Sigma''_S$

Proof. We have

(1) $\Sigma_{S1} \cong \Sigma_{S2}$ and
(2) $\Sigma_{S1} \overset{\tau}{\leadsto}_S \Sigma'_S$ and $\Sigma_{S2} \overset{\tau'}{\leadsto}_S \Sigma''_S$

Because of (1), we know that the same rule was used to derive the steps $\Sigma_{S1} \overset{\tau}{\leadsto}_S \Sigma'_S$ and $\Sigma_{S2} \overset{\tau}{\leadsto}_S \Sigma''_S$.
We know that $\Sigma'_S.ctr = \Sigma''_S.ctr$, $\Sigma'_S.n = \Sigma''_S.n$, $\Sigma'_S.b = \Sigma''_S.b$, because of (1) and the fact that the same rule was used to derive the step.
For $\Sigma'_S.\sigma \sim_{\mathbf{pc}} \Sigma''_S.\sigma$, notice that the same instruction was executed and every change to the **pc** is reflected in the trace τ, which is equal between the two executions i.e., for branches we know the same branch was taken because their traces are equal.
We now can conclude that $\Sigma'_S \cong \Sigma''_S$. □

Lemma 44 (S SE: Single step preserves ≅). *If*

(1) $X_{S1} \cong X_{S2}$ *and*
(2) $X_{S1} \xrightarrow{\tau}{}_S^O X'_S$ *and* $X_{S2} \xrightarrow{\tau}{}_S^O X''_S$

Then

(1) $X'_S \cong X''_S$ *and*

Proof. We have

(1) $X_{S1} \cong X_{S2}$ and
(2) $X_{S1} \xrightarrow{\tau}{}_S^O X'_S$ and $X_{S2} \xrightarrow{\tau}{}_S^O X''_S$

Because of (1), we know that the same rule was used to derive the steps $X_{S1} \overset{\tau}{\leadsto}_S X'_S$ and $X_{S2} \overset{\tau}{\leadsto}_S X''_S$.
We know that $X'_S.ctr = X''_S.ctr$, $X'_S.n = X''_S.n$, $X'_S.b = X''_S.b$, because of (1) and the fact that the same rule was used to derive the step.
For $X'_S.\sigma \sim_{\mathbf{pc}} X''_S.\sigma$, notice that the same instruction was executed and every change to the **pc** is reflected in the trace τ, which is equal between the two executions i.e., for branches we know the same branch was taken because their traces are equal.
We now can conclude that $X'_S \cong X''_S$. □

Theorem 17 (S SNI). *A program p satisfies SNI for a security policy P and all prediction oracles O with speculative window at most ω iff for all initial configurations $\sigma, \sigma' \in InitConf$, if $\sigma \sim_P \sigma'$ and $(p, \sigma) \Downarrow_{NS}^{O} \overline{\tau}$, $(p, \sigma') \Downarrow_{NS}^{O} \overline{\tau}$, then $(p, \sigma) \Downarrow_S^{\omega} \overline{\tau}''$, $(p, \sigma') \Downarrow_S^{\omega} \overline{\tau}''$*

Proof. Let p be a program, P be a policy and $\omega \in \mathbb{N}$ be a speculative window. We prove the two directions separately.

($\Rightarrow$) We have
(1) $\sigma \sim_P \sigma'$ and
(2) (p,σ) 🕮^{O}_{NS} $\overline{\tau}'$, (p,σ') 🕮^{O}_{NS} $\overline{\tau}'$ and
(3) p satisfies SNI for policy P and all prediction oracles O with speculative window at most ω
and we need to show that (p,σ) 🕮^{ω}_{S} $\overline{\tau}''$, (p,σ') 🕮^{ω}_{S} $\overline{\tau}''$ holds.
We unfold the definition of SNI we have for all O with speculation window at most ω, for all initial configurations σ,σ', if $\sigma \sim_P \sigma'$ and (p,σ) 🕮^{O}_{NS} $\overline{\tau}$, (p,σ') 🕮^{O}_{NS} $\overline{\tau}$, then (p,σ) 🕮^{O}_{S} $\overline{\tau}'$ and (p,σ') 🕮^{O}_{S} $\overline{\tau}'$.
We fulfill all premises of SNI by a) and b) for p and get (p,σ) 🕮^{O}_{S} $\overline{\tau}'$ and (p,σ') 🕮^{O}_{S} $\overline{\tau}'$.
We use Proposition 1 (S: Sound and Completeness between Spec and AM semantics) with (p,σ) 🕮^{O}_{S} $\overline{\tau}'$ and (p,σ') 🕮^{O}_{S} $\overline{\tau}'$ to get (p,σ) 🕮^{ω}_{S} $\overline{\tau}''$, (p,σ') 🕮^{ω}_{S} $\overline{\tau}''$. This completes the proof.
($\Leftarrow$) We have
(1) $\sigma \sim_P \sigma'$ and
(2) (p,σ) 🕮^{O}_{NS} $\overline{\tau}'$, (p,σ') 🕮^{O}_{NS} $\overline{\tau}'$ and
(3) if $\sigma \sim_P \sigma'$ and (p,σ) 🕮^{O}_{NS} $\overline{\tau}$, (p,σ') 🕮^{O}_{NS} $\overline{\tau}$, then (p,σ) 🕮^{ω}_{S} $\overline{\tau}''$, (p,σ') 🕮^{ω}_{S} $\overline{\tau}''$
Note that we got assumptions a) and b) by the unfolding of the definition of SNI. We need to show that (p,σ) 🕮^{O}_{S} $\overline{\tau}'$ and (p,σ') 🕮^{O}_{S} $\overline{\tau}'$ holds.
By using assumption a) and b) for assumption c), we get (p,σ) 🕮^{ω}_{S} $\overline{\tau}''$, (p,σ') 🕮^{ω}_{S} $\overline{\tau}''$.
Let O be an arbitrary prediction oracle with speculative window at most ω.
From Proposition 1 (S: Sound and Completeness between Spec and AM semantics) with (p,σ) 🕮^{ω}_{S} $\overline{\tau}''$, (p,σ') 🕮^{ω}_{S} $\overline{\tau}''$ we get back (p,σ) 🕮^{O}_{S} $\overline{\tau}$, (p,σ') 🕮^{O}_{S} $\overline{\tau}$. Consequently, p satisfies SNI w.r.t. P and O.
Since O was an arbitrary prediction oracle with speculation window at most ω, then p satisfies SNI for P and all prediction oracles with speculation window at most ω.

□

Proposition 1 (S: Sound and Completeness between Spec and AM semantics)**.** *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, $\sigma,\sigma' \in InitConf$ be two initial configurations. We have (p,σ) 🕮^{ω}_{S} $\overline{\tau}$ and (p,σ') 🕮^{ω}_{S} $\overline{\tau}$ iff (p,σ) 🕮^{O}_{S} $\overline{\tau}'$, (p,σ) 🕮^{O}_{S} $\overline{\tau}'$ for all prediction oracles O with speculative window at most ω.*

Proof. The proposition immediately follows from Lemma 46 (S: Soundness Am semantics w.r.t. speculative semantics) and Lemma 49 (Completeness Am semantics w.r.t. speculative semantics) □

Definition 55 (S: Relation between AM and spec for all oracles)**.** *We define two relations between AM and oracle semantics. $\approx$ $\sim$*

$\boxed{\Sigma_S \approx X_S}$

$$\frac{}{\varnothing \approx \varnothing}\ (Base) \qquad \frac{\Sigma_S \sim X_S\restriction_{com} \quad INV(\Sigma_S, X_S)}{\Sigma_S \approx X_S}\ (Single\text{-}Base)$$

$$\frac{\begin{array}{c}\Sigma_S \sim X_S\restriction_{com} \quad \Sigma''_S \Downarrow^{\overline{\tau}}_S \Sigma'''_S \text{ where transaction with id ctr is rolled back} \\ X_S = X'_S \cdot \langle p, ctr, \sigma, h, n''\rangle \quad \Sigma_S = \Sigma'_S \cdot \langle p, ctr, \sigma, n\rangle \quad INV(\Sigma_S, X_S)\end{array}}{\Sigma'_S \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle \cdot \Sigma_{S1} \approx X'_S \cdot \langle p, ctr, \sigma, h, n''\rangle \cdot \langle p, ctr', \sigma, h, n'''\rangle^{true}}\ (Single\text{-}OracleTrue)$$

$$\frac{\begin{array}{c}\Sigma''_S \sim X''_S\restriction_{com} \quad n' \geq 0 \quad \Sigma''_S \Downarrow^{\overline{\tau}}_S \Sigma'''_S \text{ where transaction with id ctr is rolled back} \\ X_S = X'_S \cdot \langle p, ctr, \sigma, h, n''\rangle \quad \Sigma_S = \Sigma'_S \cdot \langle p, ctr, \sigma, n\rangle \quad INV(\Sigma_S, X_S)\end{array}}{\Sigma'_S \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle^{false} \cdot \Sigma_{S1} \approx X'_S \cdot \langle p, ctr, \sigma, h, n''\rangle \cdot \langle p, ctr', \sigma'', h', 0\rangle^{false} \cdot X_{S1}}\ (Single\text{-}Transaction\text{-}Rollback)$$

$\boxed{\Sigma_S \sim X_S}$

$$\frac{}{\varnothing \sim \varnothing}\ (Base) \qquad \frac{|\Sigma'_S| = |X'_S| \quad \Sigma'_S \sim X'_S}{\Sigma'_S \cdot \langle p, ctr, \sigma, n\rangle^b \sim X'_S \cdot \langle p, ctr', \sigma, h, n'\rangle^b}\ (Single)$$

Lemma 45 (S: Initial states fulfill properties)**.** *Let p be a program, ω be a speculation window and O be an oracle with speculation window at most ω. If*

(1) $\sigma,\sigma' \in InitConf$ and
(2) $\Sigma^{init}_S p,\sigma$ and $\Sigma^{init}_S p,\sigma'$ and

(3) $X_S^{init}(p,\sigma)$ *and* $X_S^{init}(p,\sigma')$

Then

(1) $X_S^{init}(p,\sigma) \cong X_S^{init}(p,\sigma')$ *and*
(2) $\Sigma_S^{init}p,\sigma \cong \Sigma_S^{init}p,\sigma'$ *and*
(3) $\Sigma_S^{init}p,\sigma \approx X_S^{init}(p,\sigma)$ *and* $\Sigma_S^{init}p,\sigma' \approx X_S^{init}(p,\sigma')$ *by Rule Single-Base and*

Proof. We have

(1) $\sigma,\sigma' \in InitConf$ and
(2) $\Sigma_S^{init}p,\sigma$ and $\Sigma_S^{init}p,\sigma'$ and
(3) $X_S^{init}(p,\sigma)$ and $X_S^{init}(p,\sigma')$

Notice that by definition of $X_S^{init}()$ and Σ_S^{init} we have:

$$X_S^{init}(p,\sigma) = \langle p,0,\sigma,\varnothing,\bot\rangle$$
$$X_S^{init}(p,\sigma') = \langle p,0,\sigma,\varnothing,\bot\rangle$$
$$\Sigma_S^{init}p,\sigma = \langle p,0,\sigma,\bot\rangle$$
$$\Sigma_S^{init}p,\sigma' = \langle p,0,\sigma,\bot\rangle$$

I Immediate
II Immediate
III Immediate using Rule Single-Base

□

Lemma 46 (S: Soundness Am semantics w.r.t. speculative semantics)**.** *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*
If

(1) $\sigma,\sigma' \in InitConf$ *and*
(2) $(p,\sigma) \,\text{👻}_S^{\omega}\, \overline{\tau}$, $(p,\sigma') \,\text{👻}_S^{\omega}\, \overline{\tau}$

Then for all prediction oracles O with speculation window at most ω.

I $(p,\sigma) \,\text{👻}_S^{O}\, \overline{\tau}'$, $(p,\sigma) \,\text{👻}_S^{O}\, \overline{\tau}'$

Proof. Let $\omega \in \mathbb{N}$ be a speculation window and $\sigma,\sigma' \in InitConf$ be two initial configurations. We have:

(1) $(p,\sigma) \,\text{👻}_S^{\omega}\, \overline{\tau}$, $(p,\sigma') \,\text{👻}_S^{\omega}\, \overline{\tau}$

Furthermore, let O be an arbitrary prediction oracle with speculative window at most ω. Then we know there are executions $\Sigma_S^{init}(p,\sigma \Downarrow_S^{\overline{\tau}} \Sigma'_S$ and $\Sigma_S^{init}p,\sigma' \overset{O}{\downarrow}{}^{S}_{\overline{\tau}} \Sigma''_S$ where $\vdash \Sigma'_S : fin$ and $\vdash \Sigma''_S : fin$.

We unfold the definition of $\,\text{👻}_S^{O}$ and get $X_S^{init}(p,\sigma)$ and $X_S^{init}(p,\sigma')$ as initial states.

We need to find $\vdash X'_S : fin, \vdash X''_S : fin$ such that $X_S^{init}(p,\sigma) \Downarrow_S^{\overline{\tau}} X'_S$ and $X_S^{init}(p,\sigma') \overset{O}{\downarrow}{}^{S}_{\overline{\tau}} X''_S$.

Since we know by Lemma 45 (S: Initial states fulfill properties) that our initial states fulfill all the premises for Lemma 47 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states) we get:

(1) $X_S^{init}(p,\sigma) \overset{O}{\downarrow}{}^{S}_{\overline{\tau}'} X'_{S_1}, X_S^{init}(p,\sigma') \overset{O}{\downarrow}{}^{S}_{\overline{\tau}''} X'_{S_2}$
(2) $\Sigma'_S \cong \Sigma''_S$
(3) $X'_{S_1} \cong X'_{S_2}$ and $\overline{\rho} = \varnothing$
(4) $\Sigma'_S \approx X'_{S_1}$ and $\Sigma'_S \approx X'_{S_2}$
(5) $\overline{\tau}' = \overline{\tau}''$

We now argue, how we obtain final states from the oracle states X'_{S_1} and X'_{S_2}.

Notice that because of $\vdash \Sigma'_S : fin$ and $\vdash \Sigma''_S : fin$ that $\Sigma'_S \approx X'_{S_1}$ and $\Sigma'_S \approx X'_{S_2}$ can only be related by Rule Single-Base, because there are no ongoing transactions in Σ'_S and Σ''_S.

We now do a case analysis on the length of X'_{S_1} and X'_{S_2}. Since $X'_{S_1} \cong X'_{S_2}$, we know that $|X'_{S_1}| = |X'_{S_2}|$.

$|X'_{S_1}| = 1$ We know that $\Sigma'_S \approx X'_{S_1}$ and $\vdash \Sigma'_S : fin$.
Because of $\vdash \Sigma'_S : fin$, we know that $\Sigma'_S.\sigma \in FinalConf$.
Thus, by $\Sigma'_S \approx X'_{S_1}$ we have $X'_{S_1}.\sigma \in FinalConf$ since $X'_{S_1}.\sigma = \Sigma'_S.\sigma$.
Because $|X'_{S_1}| = 1$, we also have $X'_{S_1}.n = \bot$.
We can now conclude that $\vdash X'_{S_1} : fin$.

$|X'_{S_1}| > 1$ We know that $\Sigma'_S \approx X'_{S_1}$ and $\vdash \Sigma'_S : \mathit{fin}$.
Because of $\vdash \Sigma'_S : \mathit{fin}$, we know that $\Sigma'_S.\sigma \in \mathit{FinalConf}$ and $\vdash_O \Sigma'_S : \mathit{noongoing}$
Thus, by $\Sigma'_S \approx X'_{S_1}$ we have $X'_{S_1}.\sigma \in \mathit{FinalConf}$ since $X'_{S_1}.\sigma = \Sigma'_S.\sigma$ and $\vdash_O X'_{S_1} : \mathit{noongoing}$,
Since $X'_{S_1}.\sigma \in \mathit{FinalConf}$ and $|X'_{S_1}| > 1$, we know there are speculative instances that need to be committed.
We can now apply Lemma 21 (V4: Reaching Final state from final configuration):

(1) $X'_{S_1} \overset{O}{\Downarrow}{}^{S}_{\overline{\tau}''} X'_S$
(2) $\forall \tau \in \overline{\tau}^{\dagger}.\, \tau = \texttt{commit}\ id$ for some $id \in \mathbb{N}$
(3) $\vdash X'_S : \mathit{fin}$
(4) $X'_S.\sigma = X'_{S_1}.\sigma$
Because of $X'_{S_1} \cong X'_{S_2}$, we know that X'_{S_2} generates the same trace with the same *ids* for the commits. Thus, $\vdash X'_S : \mathit{fin}$.

The case for X'_{S_2} are analogous and not shown here.
Thus, $(p, \sigma) \overset{O}{\frown}_S \overline{\tau}' \cdot \overline{\tau}^{\dagger}$, $(p, \sigma') \overset{O}{\frown}_S \overline{\tau}' \cdot \overline{\tau}^{\dagger}$. □

Lemma 47 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states)**.** *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*

If

(1) $\Sigma_{S_1} \cong \Sigma_{S_2}$
(2) $X_{S_1} \cong X_{S_2}$ *and* $\overline{\rho} = \emptyset$
(3) $\Sigma_{S_1} \approx X_{S_1}$ *and* $\Sigma_{S_2} \approx X_{S_2}$
(4) $\Sigma_{S_1} \Downarrow^{\overline{\tau}}_S \Sigma'_{S_1}$ *and* $\Sigma_{S_2} \Downarrow^{\overline{\tau}}_S \Sigma'_{S_2}$

Then for all prediction oracles O with speculation window at most ω.

I $X_{S_1} \overset{O}{\Downarrow}{}^{S}_{\overline{\tau}'} X'_{S_1}, X_{S_2} \overset{O}{\Downarrow}{}^{S}_{\overline{\tau}''} X'_{S_2}$
II $\Sigma'_{S_1} \cong \Sigma'_{S_2}$
III $X'_{S_1} \cong X'_{S_2}$ *and* $\overline{\rho} = \emptyset$
IV $\Sigma'_{S_1} \approx X'_{S_1}$ *and* $\Sigma'_{S_2} \approx X'_{S_2}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. By Induction on $\Sigma_{S_1} \Downarrow^{\overline{\tau}}_S \Sigma'_{S_1}$ and $\Sigma_{S_2} \Downarrow^{\overline{\tau}}_S \Sigma'_{S_2}$.

Rule S:AM-Reflection We have $\Sigma_{S_1} \Downarrow^{\varepsilon}_S \Sigma'_{S_1}$ and $\Sigma_{S_2} \Downarrow^{\varepsilon}_S \Sigma'_{S_2}$, where $\Sigma'_{S_1} = \Sigma_{S_1}$ and $\Sigma'_{S_2} = \Sigma_{S_2}$.
Furthermore, we use Rule S:Reflection to derive $X_{S_1} \overset{O}{\Downarrow}{}^{S}_{\varepsilon} X'_{S_1}, X_{S_2} \overset{O}{\Downarrow}{}^{S}_{\varepsilon} X'_{S_2}$ with $X'_{S_1} = X_{S_1}$ and $X'_{S_2} = X_{S_2}$.
We now trivially satisfy all conclusions.

Rule S:AM-Single We have $\Sigma_{S_1} \Downarrow^{\overline{\tau}''}_S \Sigma'_S$ with $\Sigma'_S \overset{\tau}{\dashrightarrow}_S \Sigma'_{S_1}$ and $\Sigma_{S_2} \Downarrow^{\overline{\tau}''}_S \Sigma''_S$ and $\Sigma''_S \overset{\tau}{\dashrightarrow}_S \Sigma'_{S_2}$.
We now apply IH on $\Sigma_{S_1} \Downarrow^{\overline{\tau}''}_S \Sigma'_S$ and $\Sigma_{S_2} \Downarrow^{\overline{\tau}''}_S \Sigma''_S$ and get

(a) $X_{S_1} \overset{O}{\Downarrow}{}^{S}_{\overline{\tau}'} X'_S, X_{S_2} \overset{O}{\Downarrow}{}^{S}_{\overline{\tau}''} X''_S$
(b) $\Sigma'_S \cong \Sigma''_S$
(c) $X'_S \cong X''_S$ and $\overline{\rho}' = \emptyset$
(d) $\Sigma'_S \approx X'_S$ and $\Sigma''_S \approx X''_S$
(e) $\overline{\tau}' = \overline{\tau}''$

We proceed by inversion on $\approx$ in $\Sigma'_S \approx X'_S$ and $\Sigma''_S \approx X''_S$:
v4-com-single-base We thus have $\Sigma'_S \sim X'_S \restriction_{com}$ and $\mathit{INV}(\Sigma'_S, X'_S)$ (Similar for Σ''_S and X''_S).
We only show the proof for X'_S here. The proof for X''_S is analogous, because of $X'_S \cong X''_S$.
Notice that if $\mathit{minWndw}(X'_S) = 0$ then the transaction with $n = 0$ has to be one that will be committed. Otherwise they would be related by Rule Single-Transaction-Rollback.
To account for possible outstanding commits, we can use Lemma 22 (V4: Executing a chain of commits) on X''_S and get

f) $X'_S \overset{O}{\Downarrow}{}^{S}_{\overline{\tau}'''} X'''_S$
g) $\mathit{minWndw}(X'''_S) > 0$
h) $\forall \tau \in \overline{\tau}'''.\, \tau = \texttt{commit}\ id$ for some $id \in \mathbb{N}$
i) $X'_S.\sigma = X'''_S.\sigma$
By h) and the definition of $\restriction_{ns}$ we have $\overline{\tau}''' \restriction_{ns} = \varepsilon$.
Furthermore, $X'_S \restriction_{com} = X'''_S \restriction_{com}$ by definition of $\restriction_{com}$ (we only executed commits) and $|X'_S \restriction_{com}| = |X'''_S \restriction_{com}|$.
Thus, $\Sigma'_S \sim X'''_S \restriction_{com}$, $\mathit{INV}(\Sigma'_S, X'''_S)$ and we have $\Sigma'_S \approx X'''_S$ by Rule Single-Base.
We now proceed by inversion on the derivations $\Sigma'_S \overset{\tau}{\dashrightarrow}_S \Sigma'_{S_1}$ and $\Sigma''_S \overset{\tau}{\dashrightarrow}_S \Sigma'_{S_2}$.

Note that by $\Sigma'_S \cong \Sigma''_S$ and the fact the same traces are generated, we know that the same rule was used to derive the step.

Rule S:AM-Context We have $\Psi'_S \overset{\tau}{\rightarrow}_S \overline{\Psi}'_S$ and $\Psi''_S \overset{\tau}{\rightarrow} \overline{\Psi}'''_S$ where $\Sigma'_S = \overline{\Psi}_S \cdot \Psi'_S$ and $\Sigma''_S = \overline{\Psi}''_S \cdot \Psi''_S$. Furthermore, note that all states point to the same instruction by b)-d).

Using Lemma 48 (S: Soundness Single Step AM) on $\Psi'_S \overset{\tau}{\rightarrow}_S \overline{\Psi}'_S$ and $\Psi''_S \overset{\tau}{\rightarrow} \overline{\Psi}'''_S$ we get the desired result.

Rule S:AM-Rollback Contradiction, because $minWndw(X'''_S) > 0$ and $INV(\Sigma'_S, X'''_S)$.

v4-com-single-oracle We thus have

$$\begin{aligned}
X'_S =& X_{S3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma, h, n''' \rangle^{true} \\
\Sigma'_S =& \Sigma_{S3} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle \cdot \Sigma_{S4} \\
X_S =& X_{S3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \\
\Sigma_S =& \Sigma_{S3} \cdot \langle p, ctr, \sigma, n \rangle \\
\Sigma_S \sim& X_S \restriction_{com} \\
& INV(\Sigma_S, X_S)
\end{aligned}$$

The form of X''_S and Σ''_S is analogous. We now apply inversion on $\Sigma'_S \overset{\tau}{\rightarrow}_S \Sigma'_{S1}$.

Rule S:AM-Context We choose $X'_{S1} = X'_S$ and $X'_{S2} = X''_S$.

I By IH a)

II By Lemma 43 (S AM: Single step preserves $\cong$).

III Since $X'_{S1} = X'_S$ and $X'_{S2} = X''_S$, we are finished using IH c).

IV We show that $X'_{S1} \approx \Sigma'_{S1}$ by Rule Single-OracleTrue. The proof for $X'_{S2} \approx \Sigma'_{S2}$ is analogous.
Since we did not roll back the transaction with id ctr', we have that Σ_S does not change.
Since X_S remains the same as well, we have $\Sigma_S \sim X_S \restriction_{com}$ and $INV(\Sigma_S, X_S) X_S \restriction_{com}$ by assumption.
Thus, we fulfill all premises for Rule Single-OracleTrue.

V By IH e).

Rule S:AM-Rollback There are two cases depending on the transaction id of the rolled back transaction:

$id > ctr$ Then an inner transaction w.r.t our ctr transaction was finished.
We choose $X'_{S1} = X'_S$ and $X'_{S2} = X''_S$.
The rest of the proof is analogous to the context case above.

$id = ctr$ Most cases are similar to the context case above. Only the relation changes. We choose $X'_{S1} = X'_S$ and $X'_{S2} = X''_S$

I By IH a)

IV Here, we only show $\Sigma'_{S1} \approx X'_{S1}$ by Rule Single-Base. The proof for $\Sigma'_{S2} \approx X'_{S2}$ is analogous. Notice that $\Sigma'_{S1} = \Sigma_{S3} \cdot \langle p, ctr'', \sigma, n \rangle$ (updated ctr) after the rollback.
Combined with the constructed X'_{S1}, we have $\Sigma'_{S1} \sim X'_{S1} \restriction_{com}$ and $INV(\Sigma'_{S1}, X'_{S1})$ by our assumptions.
So we can use Rule Single-Base and have $\Sigma'_{S1} \approx X'_{S1}$.

V By IH e)

v4-com-single-rollback We have

$$\begin{aligned}
X'_S =& X_{S3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma'', h', 0 \rangle^{false} \cdot X_{S4} \\
\Sigma'_S =& \Sigma_{S3} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle^{false} \cdot \Sigma_{S4} \\
X_S =& X_{S3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \\
\Sigma_S =& \Sigma_{S3} \cdot \langle p, ctr, \sigma, n \rangle \\
\Sigma_S \sim& X_S \restriction_{com} \\
& INV(\Sigma_S, X_S) \\
n' \geq& 0
\end{aligned}$$

The form of X''_S and Σ''_S is analogous.

Additionally we know that the transaction terminates in some state $\Sigma_S \Downarrow^{\overline{\tau}}_S \Sigma'''_S$. There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma'_S \overset{\tau}{\rightarrow}_S \Sigma'_{S1}$ is not a rollback for ctr and Rule S:AM-Context or Rule S:AM-Rollback for a different transaction with a different ctr was used.
Because of IH b), we know that the same rule was used for $\Sigma''_S \overset{\tau}{\rightarrow}_S \Sigma'_{S2}$ as well.
We choose $X'_{S1} = X'_S$ and $X'_{S2} = X''_S$.
The resulting proof obligations are exactly the same to the context case of the v4-com-single-oracle case above.

$n' = 0$ Then we know that $\Sigma'_S \overset{\tau}{\rightarrow}_S \Sigma'_{S1}$ was created by Rule S:AM-Rollback and is a rollback for ctr.

I Here we prove that $X'_S \overset{\tau_0}{\rightsquigarrow}{}^{O}_{S} X'_{S_1}$ and $X''_S \overset{\tau_1}{\rightsquigarrow}{}^{O}_{S} X'_{S_2}$.
Since in X'_S and X''_S we have a state with $n = 0$ and $b = true$, we know that Rule S:Rollback applies.
So $X'_S \overset{\tau_0}{\rightsquigarrow}{}^{O}_{S} X'_{S_1}$ and $X''_S \overset{\tau_1}{\rightsquigarrow}{}^{O}_{S} X'_{S_2}$ are derived by Rule S:Rollback.
II By Lemma 43 (S AM: Single step preserves $\cong$)
III By Lemma 44 (S SE: Single step preserves $\cong$) with fact V).
IV Here, we only show $\Sigma'_{S_1} \approx X'_{S_1}$ by Rule Single-Base. The proof for $\Sigma'_{S_2} \approx X'_{S_2}$ is analogous.
We know that the states after rollback are

$$X'_{S_1} = X_{S_3} \cdot \langle p, ctr', \sigma, h', n'' \rangle$$
$$\Sigma'_{S_1} = \Sigma_{S_3} \cdot \langle p, ctr', \sigma, n \rangle$$

Notice, that the only difference to X_S and Σ_S is the updated *ctr*. We also know by assumption that $\Sigma_S \sim X_S \restriction_{com}$ and $INV(\Sigma_S, X_S)$.
By construction of X'_{S_1} and Σ'_{S_1}, we can conclude that $\Sigma'_S \sim X'_{S_1} \restriction_{com}$ and $INV(\Sigma'_{S_1}, X'_{S_1})$.
This allows us to use Rule Single-Base to derive $\Sigma'_{S_1} \approx X'_{S_1}$.
V Here $\tau_0 = \texttt{rlb}\ ctr'$ and $\tau_1 = \texttt{rlb}\ ctr''$. Because of IH b) we know that $ctr' = ctr''$ and thus $\tau_0 = \tau_1$.

□

Lemma 48 (S: Soundness Single Step AM). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, O be a prediction oracle with speculative window at most ω, $\Sigma_{S_1} = \Sigma'_S \cdot \Phi'_S$, $\Sigma_{S_2} = \Sigma''_S \cdot \Phi''_S$ be two speculative states for the always mispredict semantics and X_{S_1}, X_{S_2}, be two speculative states for the speculative semantics.*
If the following conditions hold:

(1) $\Sigma_{S_1} \cong \Sigma_{S_2}$
(2) $X_{S_1} \cong X_{S_2}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma_{S_1} \approx X_{S_1}$ *and* $\Sigma_{S_2} \approx X_{S_2}$
(4) $\Phi'_S \overset{\tau''}{\dashrightarrow}_S \Sigma'_{S_1}$ *and* $\Phi''_S \overset{\tau''}{\dashrightarrow}_S \Sigma'_{S_2}$

then there are instances X'_{S_1}, X'_{S_2} for the speculative semantics such that:

I $X_{S_1} \overset{O}{\Downarrow}{}^{S}_{\tau} X'_{S_1}$ *and* $X_{S_2} \overset{O}{\Downarrow}{}^{S}_{\tau'} X'_{S_2}$
II $\Sigma'_{S_1} \cong \Sigma'_{S_2}$
III $X'_{S_1} \cong X'_{S_2}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{S_1} \approx X'_{S_1}$ *and* $\Sigma'_{S_2} \approx X'_{S_2}$
V $\tau = \tau'$

Proof. We proceed by inversion on $\Phi'_S \overset{\tau''}{\dashrightarrow}_S \Sigma'_{S_1}$ and $\Phi''_S \overset{\tau''}{\dashrightarrow}_S \Sigma'_{S_2}$:

Rule S:AM-General We choose $X'_{S_1} = X'_S$ and $X'_{S_2} = X''_S$.
I By Rule S:Reflection.
II Notice that by Rule S:AM-General we have $\Sigma'_{S_1} = \Sigma_{S_1}$ and $\Sigma'_{S_2} = \Sigma_{S_2}$, because the rule only emits the observations in $\overline{\rho}$. We are finished by using assumption 1).
III Since $X'_{S_1} = X'_S$ and $X'_{S_2} = X''_S$, we are finished using assumption 3).
IV Here, we only show $\Sigma'_{S_1} \approx X'_{S_1}$ by Rule Single-Base. The proof for $\Sigma'_{S_2} \approx X'_{S_2}$ is analogous.
The use of Rule S:AM-General does not change the state. That is why $\Sigma'_{S_1} = \Sigma_{S_1 \rho \setminus \tau}$.
By our assumptions we have $\Sigma_{S_1} \sim X_{S_1} \restriction_{com}$ and $INV(\Sigma_{S_1}, X_{S_1})$.
After substitution we have $\Sigma'_{S_1} \sim X'_{S_1} \restriction_{com}$ and $INV(\Sigma'_{S_1}, X'_{S_1})$. Thus, we fulfill all premises for Rule Single-Base and $\Sigma'_{S_1} \approx X'_{S_1}$.
V Since Rule S:Reflection only emits the empty trace, they are trivially equal.

Rule S:AM-Store-Spec There are two cases depending on the output of the oracle O.
($false, \omega$) **correct prediction w.r.t** X'_S The store instruction is not skipped and executed normally.

I We use Rule S:Store-Exe to derive the steps $X_{S_1} \overset{\tau_0}{\rightsquigarrow}{}^{O}_{S} X'_S$ and $X_{S_2} \overset{\tau_1}{\rightsquigarrow}{}^{O}_{S} X''_S$.
Furthermore, we execute Rule S:General once, because Rule S:Store-Exe created one observation in $\overline{\rho}$. We now have $X'_{S_1} = X'_S$ with an empty $\overline{\rho}$.
The rule only emits the observation but does not change the state apart from $\overline{\rho}$. As a result we have $X_{S_1} \overset{O}{\Downarrow}{}^{S}_{\overline{\tau}} X'_{S_1}$ and $X_{S_2} \overset{O}{\Downarrow}{}^{S}_{\overline{\tau}'} X'_{S_2}$.
II By Lemma 43 (S AM: Single step preserves $\cong$)
III By Lemma 44 (S SE: Single step preserves $\cong$) for $X_{S_1} \overset{\tau_0}{\rightsquigarrow}{}^{O}_{S} X'_S$ and $X_{S_2} \overset{\tau_1}{\rightsquigarrow}{}^{O}_{S} X''_S$ and the fact that the use of Rule S:General does not change the states and the $\overline{\rho}$ of both oracle states are equal. Notice that $\overline{\rho}$ is empty after applying Rule S:General once.

IV We have

$$\begin{aligned}
X'_{S_1} &= X_{S_3}' \cdot \langle p, ctr, \sigma', h, n\rangle \cdot \langle p, ctr', \sigma', h', n_0\rangle^{false}\\
\Sigma'_{S_1} &= \Sigma_{S_3} \cdot \langle p, ctr, \sigma', n_1\rangle \cdot \langle p, ctr', \sigma'', n_2\rangle\\
X'_{S_4} &= X_{S_3}' \cdot \langle p, ctr, \sigma', h, n\rangle\\
\Sigma'_{S_4} &= \Sigma_{S_3} \cdot \langle p, ctr, \sigma'', n_1\rangle
\end{aligned}$$

We now show that $\Sigma'_{S_4} \sim X'_{S_4}$.
$|\Sigma'_{S_4}| = |X'_{S_4}\restriction_{com}|$ First, notice that $|X_{S_1}\restriction_{com}| = |X'_{S_4}\restriction_{com}|$, because the rule does not change b.
Similarly, $|\Sigma_{S_1}| = |\Sigma'_{S_4}|$ and by our assumption $|\Sigma_{S_1}| = |X_{S_1}\restriction_{com}|$ we get after substitution: $|\Sigma'_{S_4}| = |X'_{S_4}\restriction_{com}|$.
$\sigma' = \sigma''$ We know that $X_{S_1}.\sigma \xrightarrow{\tau_0} X'_{S_4}.\sigma$ and $\Sigma'_{S}.\sigma \xrightarrow{\tau} \Sigma'_{S_4}.\sigma$.
Because of $\Sigma_{S_1} \approx X_{S_1}$ and the fact that $\rightarrow$ is deterministic, we know that $\Sigma'_{S_4}.\sigma = X'_{S_4}.\sigma$. Thus, $\sigma' = \sigma''$
We can now conclude that $\Sigma'_{S_4} \sim X'_{S_4}\restriction_{com}$.
We now show that $INV(\Sigma'_{S_4}, X'_{S_4})$ holds.
$|\Sigma'_{S_4}| = |X'_{S_4}\restriction_{com}|$ Already shown above.
$1 \leq i \leq |\Sigma'_{S_4}|$, $minWndw(X'_{S_4}\restriction_{com}{}^i) \leq \Sigma'_{S_4}{}^i.n$ There are two cases:
Either $\Sigma'_{S_4}{}^i.n = \Sigma_{S_1}.n - 1$ (if $i = |\Sigma'_{S_4}|$) or $\Sigma'_{S_4}{}^i.n = \Sigma_{S_1}.n$.
We will prove it for $\Sigma'_{S_4}{}^i.n = \Sigma_{S_1}.n - 1$, because that automatically yields us the the result for $\Sigma'_{S_4}{}^i.n = \Sigma_{S_1}.n$.
From Rule S:Store-Exe (which does not change older labels b) and the fact that we have a correct prediction we have $minWndw(X'_{S_4}\restriction_{com}{}^i) = minWndw(decr(X_{S_1})\restriction_{com}{}^i)$.
From the definition of $decr()$ we get $minWndw(decr(X_{S_1})\restriction_{com}{}^i) \leq minWndw(X_{S_1}\restriction_{com}{}^i)$.
Also, $minWndw(decr(X_{S_1})\restriction_{com}{}^i) \leq \Sigma_{S_1}.n - 1$, because $n > 0$ and $INV(\Sigma_{S_1}, X_{S_1})$. If n was 0, we would have executed Rule S:AM-Rollback instead of the store. Now we get:

$$\begin{aligned}
minWndw(X_{S_1}\restriction_{com}{}^i) &\leq \Sigma_{S_1}{}^i.n\\
minWndw(decr(X_{S_1})\restriction_{com}{}^i) &\leq \Sigma_{S_1}{}^i.n - 1\\
minWndw(decr(X_{S_1})\restriction_{com}{}^i) &\leq \Sigma'_{S_4}{}^i.n\\
minWndw(X'_{S_4}\restriction_{com}{}^i) &\leq \Sigma'_{S_4}{}^i.n
\end{aligned}$$

which proves our claim.
We now show by which rule $\Sigma'_{S_1} \approx X'_{S_1}$ are related.
For that, we do a case distinction if there are transactions that need to be rolled back or not in X'_{S_1}.
We have to do this, because we only know that $minWndw(X_{S_1}) > 0$ *before* we did the step. So it could happen that $minWndw(X'_{S_1}) = 0$ for some transaction that needs to be rolled back (we can ignore transactions that will be committed).
No Transaction that needs to be rolled back in X'_{S_1} with window 0 Then we can relate by Rule Single-OracleTrue because we showed that we fulfill the premises.
Transaction that needs to be rolled back in X'_{S_1} with window 0 Then we relate by Rule Single-Transaction-Rollback, because there is an instance in X'_{S_1} with speculation window 0 that needs to be rolled back.
Notice that the topmost state in X'_{S} cannot be the transaction that will be rolled back, because we know that it will be committed.
We showed that we fulfill all premises above.

V The observations are $\overline{\tau} = \texttt{store}\ m \cdot \texttt{start}\ ctr_1$ and $\overline{\tau}' = \texttt{store}\ m' \cdot \texttt{start}\ ctr_2$ for some $m, m' \in Vals$.
From $X_{S_1} \cong X_{S_2}$ we know that $X_{S_1}.\sigma(\mathbf{pc}) = X_{S_2}.\sigma(\mathbf{pc})$ and $X_{S_1}.ctr = X_{S_2}.ctr$.
As a result, by $X_{S_1}.ctr = ctr_1$ and $X_{S_2}.ctr = ctr_2$ we have $ctr_1 = ctr_2$.
Since $\Sigma_{S_1} \approx X_{S_1}$, we have $\Sigma_{S_1}.\sigma = X_{S_1}.\sigma$ (similar for Σ_{S_2} and X_{S_2}).
We know that the observation $\tau'' = \texttt{store}\ m$ is generated by $\Sigma_{S_1}.\sigma \xrightarrow{\tau''} \Sigma'_{S_1}.\sigma$ and $\Sigma_{S_2}.\sigma \xrightarrow{\tau''} \Sigma'_{S_2}.\sigma$ in the step Rule S:AM-Store-Spec and similarly $X_{S_1}.\sigma \xrightarrow{\texttt{store}\ m} X'_{S_1}.\sigma$ and $X_{S_2}.\sigma \xrightarrow{\texttt{store}\ m'} X'_{S_2}.\sigma$
Since $\rightarrow$ is deterministic, we have $\tau'' = \texttt{store}\ m$ and $\tau'' = \texttt{store}\ m'$.
Now everything combined results in $\overline{\tau} = \overline{\tau}'$ and we are finished.

$(true, \omega)$ **wrong prediction w.r.t X'_{S}** The store instruction is skipped.

I We use Rule S:Store-Skip to derive the steps $X'_{S} \overset{\tau_0}{\rightsquigarrow}{}^{O}_{S} X'_{S_1}$ and $X''_{S} \overset{\tau_1}{\rightsquigarrow}{}^{O}_{S} X'_{S_2}$.
Furthermore, we execute Rule S:General twice, because Rule S:Store-Exe created two observations in $\overline{\rho}$. We now have $X'_{S_1} = X'_{S}$ with an empty $\overline{\rho}$.
The rule only emits the observations but does not change the state apart from $\overline{\rho}$. As a result we have $X_{S_1} \overset{O}{\Downarrow}{}^{S}_{\overline{\tau}} X'_{S_1}$ and $X_{S_2} \overset{O}{\Downarrow}{}^{S}_{\overline{\tau}'} X'_{S_2}$.

Notice that the observations in $\overline{\rho}$ are equal between X_{S_1} and X_{S_2}, because of (2). We have $X_{S_1}.ctr = X_{S_2}.ctr$ and $X_{S_1}.\sigma \sim_{\mathbf{pc}} X_{S_2}.\sigma$ from our relation.

II By Lemma 43 (S AM: Single step preserves $\cong$)

III By Lemma 44 (S SE: Single step preserves $\cong$) for Rule S:Store-Skip and Rule S:General twice. Notice that $\overline{\rho}$ is empty now.

IV We have:

$$\begin{aligned}
X'_{S_1} =& X'_{S_3} \cdot \langle p, ctr, \sigma', h, n\rangle \cdot \langle p, ctr', \sigma''', h', n_0\rangle^{true}\\
\Sigma'_{S_1} =& \Sigma_{S_3} \cdot \langle p, ctr, \sigma', n_1\rangle \cdot \langle p, ctr', \sigma'', n_2\rangle\\
X'_{S_4} =& X'_{S_3} \cdot \langle p, ctr, \sigma', h, n\rangle\\
\Sigma'_{S_4} =& \Sigma_{S_3} \cdot \langle p, ctr, \sigma', n_1\rangle
\end{aligned}$$

We now show that $\Sigma'_{S_1} \sim X'_{S_1}$ and $INV(\Sigma'_{S_1}, X'_{S_1})$ hold.
Notice that we assume $\Sigma'_{S_4} \sim X'_{S_4}\restriction_{com}$ and $INV(\Sigma'_{S_4}, X'_{S_4})$, because the proofs are exactly the same as above.
We start by showing $\Sigma'_{S_1} \sim X'_{S_1}$:
$|\Sigma'_{S_1}| = |X'_{S_1}\restriction_{com}|$ We have $|X'_{S_1}\restriction_{com}| = |X'_{S_4}\restriction_{com}| + 1$ and $|\Sigma'_{S_1}| = |\Sigma'_{S_4}| + 1$, because we mispredict.
By assumption $\Sigma'_{S_4} \sim X'_{S_4}$ we have $|\Sigma'_{S_4}| = |X'_{S_4}\restriction_{com}|$ and are thus finished.
$\sigma''' = \sigma''$ Since the rules applied, changed $X_{S_1}.\sigma$ and $\Sigma_{S_1}.\sigma$ in the same way and the fact that $X_{S_1}.\sigma = \Sigma_{S_1}.\sigma$ we get $\sigma''' = \sigma''$.
We can now conclude that $\Sigma'_{S_1} \sim X'_{S_1}\restriction_{com}$.
Now for $INV(\Sigma'_{S_1}, X'_{S_1})$:
$|\Sigma'_{S_1}| = |X'_{S_1}\restriction_{com}|$ Already shown above.
$1 \leq i \leq |\Sigma'_{S_1}|$, $minWndw(X'_{S_1}\restriction_{com}{}^i) \leq \Sigma'_{S_1}{}^i.n$ There are two cases:
Either $\Sigma'_{S_1}{}^i.n = \min(\Sigma'_{S_4}.n + 1, \omega)$ (if $i = |\Sigma'_{S_1}|$) or $\Sigma'_{S_1}{}^i.n = \Sigma_{S_1}.n$.
We will prove it for $\Sigma'_{S_1}{}^i.n = \min(\Sigma'_{S_4}.n + 1, \omega)$, because we have the result for $i \leq |\Sigma'_{S_1}|$ by assumption $INV(\Sigma'_{S_4}, X'_{S_4})$.
By $INV(\Sigma'_{S_4}, X'_{S_4})$ we know this holds for Σ'_{S_4} and X'_{S_4}.
Notice that $minWndw(X'_{S_1}\restriction_{com}) \leq minWndw(X'_{S_4}\restriction_{com})$.
Furthermore, $\Sigma'_{S_4}.n \leq \Sigma'_{S_1}.n$ (the 1 comes from the fact that the window is reduced when executing the store normally), because $\Sigma'_{S_1} = \min(\Sigma'_{S_4}.n + 1, \omega)$ and the fact that all possible values for n are bound by ω.
Now we have:

$$\begin{aligned}
minWndw(X_{S_1}\restriction_{com}{}^i) &\leq \Sigma_{S_1}{}^i.n\\
minWndw(decr(X_{S_1})\restriction_{com}{}^i) &\leq \Sigma_{S_1}{}^i.n - 1\\
minWndw(decr(X_{S_1})\restriction_{com}{}^i) &\leq \Sigma'_{S_4}{}^i.n\\
minWndw(X'_{S_4}\restriction_{com}{}^i) \leq \Sigma'_{S_4}{}^i.n\ & minWndw(X'_{S_1}\restriction_{com}) \leq minWndw(X'_{S_4}\restriction_{com})\\
minWndw(X'_{S_1}\restriction_{com}{}^i) \leq \Sigma'_{S_4}{}^i.n\ & \Sigma'_{S_4}.n \leq \Sigma'_{S_1}.n\\
minWndw(X'_{S_1}\restriction_{com}{}^i) &\leq \Sigma'_{S_1}{}^i.n
\end{aligned}$$

and we are finished.
Similar to above, we need to check if there are transactions that need to be rolled back after taking a step in X'_{S_1}.
No Transaction that needs to be rolled back in X'_{S_1} with window 0 Then we can relate by Rule Single-Base because we showed above, that we fulfill the premises.
Transaction that needs to be rolled back in X'_{S_1} with window 0 Then we can relate by Rule Single-Transaction-Rollback for the same reasons above in the case of a correct prediction, since we fulfil all the premises.

V The observations are

$$\begin{aligned}
\overline{\tau} =& \texttt{store}\ m \cdot \texttt{start}\ X_{S_1}.ctr \cdot \texttt{bypass}\ X_{S_1}.\sigma(\mathbf{pc})\\
\overline{\tau}' =& \texttt{store}\ m' \cdot \texttt{start}\ X_{S_2}.ctr \cdot \texttt{bypass}\ X_{S_2}.\sigma(\mathbf{pc})
\end{aligned}$$

for some $m, m' \in Vals$.
From (2) we have $X_{S_1}.ctr = X_{S_2}.ctr$ and $X_{S_1}.\sigma \sim_{\mathbf{pc}} X_{S_2}.\sigma$.
We know that the observation $\tau'' = \texttt{store}\ m$ is generated by $\Sigma_{S_1}.\sigma \xrightarrow{\tau''} \Sigma'_{S_1}.\sigma$ and $\Sigma_{S_2}.\sigma \xrightarrow{\tau''} \Sigma'_{S_2}.\sigma$ in the step Rule S:AM-Store-Spec and similarly $X_{S_1}.\sigma \xrightarrow{\texttt{store}\ m'} X'_{S_1}.\sigma$ and $X_{S_2}.\sigma \xrightarrow{\texttt{store}\ m'} X'_{S_2}.\sigma$.
Since $\rightarrow$ is deterministic, we have $\tau'' = \texttt{store}\ m$ and $\tau'' = \texttt{store}\ m'$.
Thus, by the determinism of $\xrightarrow{\tau}$ we have $\overline{\tau} = \overline{\tau}'$.

Rule S:AM-barr and Rule S:AM-barr-spec We prove this for Rule S:AM-barr-spec. The proof for Rule S:AM-barr is analogous.

I Because of 3) and 1), we can apply Rule S:barr-spec once for X_{S_1} and X_{S_2}.
We get $X'_S \overset{\tau_0}{\overset{O}{\rightsquigarrow}}_S X'_{S_1}$ and $X''_S \overset{\tau_0}{\overset{O}{\rightsquigarrow}}_S X'_{S_2}$.
II By Lemma 43 (S AM: Single step preserves $\cong$).
III By Lemma 44 (S SE: Single step preserves $\cong$).
IV After the **spbarr** instruction, we know that there could be speculative transactions in X'_{S_1} that has a speculation window of 0.
We prove that $\Sigma'_{S_1} \sim X'_{S_1}\restriction_{com}$. The proof for $\Sigma'_{S_2} \sim X'_{S_2}\restriction_{com}$ is analogous.
$\Sigma'_{\mathbf{S}_1}.\sigma = X'_{\mathbf{S}_1}.\sigma$ We know by 3) that $\Sigma_{S_1}.\sigma = X_{S_1}.\sigma$.
Since the rules applied change the configuration σ in the same way by using $\rightarrow$, and $\rightarrow$ is deterministic, we know that they remain equal.
$|X'_{\mathbf{S}_1}\restriction_{com}| = |\Sigma'_{\mathbf{S}_1}|$ Since the executed rule does not add or remove speculative instances, we know that this holds by assumption.
We prove $INV(\Sigma'_{S_1}, X'_{S_1})$ still holds. The proof for $INV(\Sigma'_{S_2}, X'_{S_2})$ is analogous.
We need to show that $|\Sigma'_{S_1}| = |X'_{S_1}\restriction_{com}|$ and for all $1 \leq i \leq |\Sigma'_{S_1}|$, $minWndw(X'_{S_1}\restriction_{com}{}^i) \leq \Sigma'_{S_1}{}^i.n$.
$|\Sigma'_{\mathbf{S}_1}| = |X'_{\mathbf{S}_1}\restriction_{com}|$ Follows from above.
$1 \leq i \leq |\Sigma'_{\mathbf{S}}|$, $minWndw(X'_{\mathbf{S}}\restriction_{com}{}^i) \leq \Sigma'_{\mathbf{S}_1}{}^i.n$ Since the executed instruction was a barrier instruction, we know that $minWndw(X'_{\mathbf{S}}\restriction_{com}{}^i) = 0$.
There are two cases dependent on the chosen i:
$i = |\Sigma'_{\mathbf{S}_1}|$ Then $\Sigma'_{S_1}{}^i.n = 0$, because of the **spbarr** instruction and therefore $minWndw(X'_{S_1}\restriction_{com}{}^i) \leq \Sigma'_{S_1}{}^i.n$.
$i < |\Sigma'_{\mathbf{S}_1}|$ Then $\Sigma'_{S_1}.n = \Sigma'_S.n$ and we have $minWndw(X'_{S_1}\restriction_{com}{}^i) \leq \Sigma'_{S_1}{}^i.n$, since $minWndw(X'_{S_1}\restriction_{com}{}^i) = 0$.
Now, we do a case distinction if there is a speculative transaction with speculation window 0 and that needs to be rolled back in X'_{S_1}. Note that by assumption 1) that a similar transaction exists then in X'_{S_2} as well.
no transaction with speculation window 0 Then we have $\Sigma'_{S_1} \approx X'_{S_1}$ by Rule Single-Base using the facts $\Sigma'_{S_1} \sim X'_{S_1}\restriction_{com}$ and $INV(\Sigma'_{S_1}, X'_{S_1})$.
transaction with speculation window 0 We know by construction, that there exists a speculative transaction in Σ'_{S_1} with the same transaction id. We showed that $\Sigma'_{S_1} \sim X'_{S_1}\restriction_{com}$ and $INV(\Sigma'_{S_1}, X'_{S_1})$ hold. Thus we fulfill all conditions for Rule Single-Transaction-Rollback.
V From our relation, we have that $\Sigma'_S.\sigma = X'_S.\sigma$.
From the applied rules, we have $\Sigma_{S_1}.\sigma \xrightarrow{\tau''} \Sigma'_{S_1}$ and $X_{S_1}.\sigma \xrightarrow{\tau_0} X'_{S_1}$. Similarly, $\Sigma_{S_2}.\sigma \xrightarrow{\tau''} \Sigma'_{S_2}$ and $X_{S_2}.\sigma \xrightarrow{\tau_1} X'_{S_2}.\sigma$.
Since the non-speculative execution is deterministic we have $\tau'' = \tau_0$ and $\tau'' = \tau_1$ and thus $\tau_0 = \tau_1$.

Rule S:AM-NoBranch Most cases are analogous to the barrier case.
d) The proof proceeds in the same way as in the barrier case above. The argument for $INV(\Sigma'_{S_1}, X'_{S_1})$ is the same as for the store instructions above.

□

Definition 56 (Constructing the Oracle). *Constructing the prediction oracle O_{am_S}. We build our oracle based on the executions $\Sigma_S^{init}p, \sigma \Downarrow_S^{\overline{\tau}} \Sigma_{S_1} \overset{\tau_{am}}{\dashrightarrow}_S \Sigma_{S_2}, \Sigma_S^{init}p, \sigma' \Downarrow_S^{\overline{\tau}} \Sigma'_{S_1} \overset{\tau'_{am}}{\dashrightarrow}_S \Sigma'_{S_2}$ where $\tau_{am} \neq \tau'_{am}$.*
Let us denote by the set RB the ids of all ongoing transaction ids in Σ_{S_1}. Since $\Sigma_{S_1} \cong \Sigma'_{S_1}$ we know that the same transaction ids are still ongoing in Σ'_{S_1} as well. The set RB describes the store instructions that we need to mispredict to reach the difference in the trace.
Our oracle is now defined as follows:

$$O_{am_S}(p,n,h) = \begin{cases} (true, \omega) \text{ if } |h| \in RB \wedge p(\sigma(\mathbf{pc})) = \mathbf{store}\ x, e \\ (true, 0) \text{ otherwise (where } p(\sigma(\mathbf{pc})) = \mathbf{store}\ x, e) \end{cases}$$

Note that we use the length of h to reconstruct the ctr. Both start at 0 and are increased when a speculation starts. Since this oracle only mispredicts, we know that the ctr of the always mispredict run and the ctr of the oracle runs are equal.

> *Why we need the $(true, 0)$ case in our AM Oracle (This is fairly technical and not important at first read) Consider a program that has a store at location 1 and a store at location 1000 and the stroe at line 1000 is vulnerable to a V4 Spectre attack. The misprediction of the store at line 1 has no influence on the vulnerability (assuming a spec. window of 200) in the AM semantics. Only the topmost speculative instance speculation window is reduced and is then deleted. However, in the oracle semantics all speculative instances are reduced. If the first store is mispredicted and execution continues then we would not cover the same amount of instructions during the speculation as the AM semantics and the executions would get out of sync. That is why we instantly roll back this misprediction.*
> *It works in all other cases because the speculation window in AM is also reduced with each newly created speculative instance because of $min(\omega, i)$ where i is the current speculation window.*

Definition 57 (S: Relation between AM and Spec for oracles that only mispredict). *We define two relations, $\approx^{O_{am}}$ and $\sim$, between AM and oracle semantics. Note that $\approx^{O_{am}}$ is indexed by an oracle. This oracle has to always mispredict.*

$$\boxed{\Sigma_S \approx^{O_{am}} X_S}$$

$$\frac{}{\emptyset \approx^{O_{am}} \emptyset}\ (\textit{Base-Oracle}) \qquad \frac{\Sigma_S \sim X_S\restriction_{com} \quad \mathit{INV2}(\Sigma_S, X_S) \quad \mathit{minWndw}(X_S) > 0}{\Sigma_S \approx^{O_{am}} X_S}\ (\textit{Single-Base-Oracle})$$

$$\frac{\begin{array}{c}\Sigma''_S \sim X''_S\restriction_{com} \quad n' \geq 0 \quad \Sigma''_S \Downarrow^{\overline{\tau}}_S \Sigma'''_S \text{ where transaction with id ctr is rolled back} \\ X_S = X'_S \cdot \langle p, ctr, \sigma, h, n''\rangle \qquad \Sigma_S = \Sigma'_S \cdot \langle p, ctr, \sigma, n\rangle \qquad \mathit{INV2}(\Sigma_S, X_S)\end{array}}{\Sigma'_S \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle^{false} \cdot \Sigma_{S1} \approx^{O_{am}} X'_S \cdot \langle p, ctr, \sigma, h, n''\rangle \cdot \langle p, ctr', \sigma'', h', 0\rangle^{false}}\ (\textit{Single-Transaction-Rollback-Oracle})$$

Lemma 49 (Completeness Am semantics w.r.t. speculative semantics). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, $\sigma, \sigma' \in InitConf$ be two initial configurations. If*

(1) $p, \sigma \Subset^{\omega}_S \overline{\tau}$ and $p, \sigma' \Subset^{\omega}_S \overline{\tau}'$ and
(2) $\overline{\tau} \neq \overline{\tau}'$

Then there exists an oracle O such that

I $p, \sigma \Subset^{O}_S \overline{\tau}_1$ and $p, \sigma' \Subset^{O}_S \overline{\tau}'_1$ and
II $\overline{\tau}_1 \neq \overline{\tau}'_1$

Proof. Let $\omega \in \mathbb{N}$ be a speculative window, $\sigma, \sigma' \in InitConf$ be two initial configurations. We have If

(1) $p, \sigma \Subset^{\omega}_S \overline{\tau}$ and $p, \sigma' \Subset^{\omega}_S \overline{\tau}'$ and
(2) $\overline{\tau} \neq \overline{\tau}'$

By definition of $\Subset^{\omega}_S$ we have two final states Σ_{S_F} and Σ'_{S_F} such that $\Sigma^{init}_S p, \sigma \Downarrow^{\overline{\tau}}_S \Sigma_{S_F}$ $\Sigma^{init}_S p, \sigma' \Downarrow^{\overline{\tau}'}_S \Sigma'_{S_F}$. Combined with the fact that $\overline{\tau} \neq \overline{\tau}'$, it follows that there are speculative states $\Sigma_{S_1}, \Sigma_S, \Sigma'_{S_1}, \Sigma'_{S_2}$ and sequences of observations $\overline{\tau}, \overline{\tau}_{end}, \overline{\tau}'_{end}, \tau_{am}, \tau'_{am}$ such that $\tau_{am} \neq \tau'_{am}$, $\Sigma_{S_1} \cong \Sigma'_{S_1}$ and:

$$\Sigma^{init}_S p, \sigma \Downarrow^{\overline{\tau}}_S \Sigma_{S_1} \xrightarrow{\tau_{am}}_S \Sigma_{S_2} \Downarrow^{\overline{\tau}_{end}}_S \Sigma_{S_F}$$

$$\Sigma^{init}_S p, \sigma' \Downarrow^{\overline{\tau}}_S \Sigma'_{S_1} \xrightarrow{\tau'_{am}}_S \Sigma'_{S_2} \Downarrow^{\overline{\tau}'_{end}}_S \Sigma'_{S_F}$$

We claim that there is a prediction oracle O with speculative window at most ω such that

a $X^{init}_S(p, \sigma) \overset{O}{\rightsquigarrow}{}^{S}_{v} X_{S_1}$ and $X_{S_1}.\sigma = \Sigma_{S_1}.\sigma$ and $\mathit{INV2}(X_{S_1}, \Sigma_{S_1})$ and
b $X^{init}_S(p, \sigma') \overset{O}{\rightsquigarrow}{}^{S}_{v} X'_{S_1}$ and $X'_{S_1}.\sigma = \Sigma'_{S_1}.\sigma$ and $\mathit{INV2}(X'_{S_1}, \Sigma'_{S_1})$
c $X_{S_1} \cong X'_{S_1}$

We get this by applying Lemma 50 (Stronger Soundness for a specific oracle and for specific executions) on the Am execution up to the point of the difference i.e., $\Sigma^{init}_S p, \sigma \Downarrow^{\overline{\tau}}_S \Sigma_{S_1}$.

We now show that $\Sigma_{S_1} \approx^{O_{am}} X_{S_1}$ is derived by Rule Single-Base-Oracle.

We do a case distinction if there are ongoing transactions in X_{S_1} or not

no ongoing transactions in X_{S_1} Then $\Sigma_{S_1} \approx^{O_{am}} X_{S_1}$ can only be derived Rule Single-Base-Oracle and Σ_{S_1} has no ongoing transactions as well. Then we have by $\mathit{INV2}(\Sigma_{S_1}, X_{S_1})$ and $\Sigma_{S_1}.n = \bot$ that $X_{S_1}.n = \bot$.

ongoing transactions in X_S By the definition of the oracle O, we know that the for the transaction *id* where the difference $\tau_{am} \neq \tau_{am'}$ happens, the oracle mispredicted with a speculation window of ω. This is also the topmost transaction in X_S.
Furthermore, we know that $X_{S_1}.n \geq \mathit{minWndw}(X_{S_1})$ by definition of the oracle O_{amS} and $\mathit{minWndw}()$.
Since the next rule cannot be Rule S:AM-Rollback, we know that $\Sigma_{S_1}.n > 0$ and by $\mathit{INV2}(\Sigma_{S_1}, X_{S_1})$ we get $\mathit{minWndw}(X_{S_1}) > 0$ (Similar for X'_{S_1} because of $\Sigma_{S_1} \cong \Sigma'_{S_1}$).
If $\Sigma_{S_1} \approx^{O_{am}} X_{S_1}$ by rollback rule, we would have a contradiction because we would need the topmost speculation window of $X_{S_1}.n = 0$. But we know that $\mathit{minWndw}(X_{S_1}) > 0$, because the speculation window of the topmost instance was created with a speculation window of ω.
we know that $X_{S_1} \approx^{O_{am}} \Sigma_{S_1}$ by Rule Single-Base-Oracle.

We now proceed by case analysis on the rule in $\xrightarrow{}_S$ used to derive $\Sigma_{S_1} \xrightarrow{\tau_{am}}_S \Sigma_{S_2}$. Because $\Sigma_{S_1} \cong \Sigma'_{S_1}$ and $\overline{\tau}_1 = \overline{\tau}'_1$, we know that the same rule was used in $\Sigma'_{S_1} \xrightarrow{\tau'_{am}}_S \Sigma'_{S_2}$ as well.

Rule S:AM-Rollback Contradiction. Because $\Sigma_{S1} \cong \Sigma'_{S1}$ we have for all instances $\Phi_1.ctr = \Phi'_1.ctr$.
Since the same instance would be rolled back, we have $\tau_{am} = \tau'_{am}$.

Rule S:AM-Context By inversion on Rule S:AM-Context for the step $\Sigma_{S1} \xrightarrow{\tau_{am}}_S \Sigma_{S2}$ we have $\Sigma_{S1} = \overline{\Phi}_S \cdot \Phi_S$ and $\Sigma_{S2} = \overline{\Phi}_S \cdot \overline{\Phi}'_S$ with $\Phi_S \xrightarrow{\tau_{am}}_S \overline{\Phi}'_S$.

We now do inversion on $\Sigma_{S1} \xrightarrow{\tau_{am}}_S \Sigma_{S2}$ and $\Phi_S \xrightarrow{\tau_{am}}_S \overline{\Phi}'_S$:

Rule S:AM-General Contradiction. By $\Sigma_{S1} \cong \Sigma'_{S1}$ we know that $\Sigma_{S1}.\overline{\rho} = \Sigma'_{S1}.\overline{\rho}$.
This immediately implies that $\tau_{am} = \tau_{am'}$, which is not true by assumption.

Rule S:AM-barr-spec, Rule S:AM-barr Contradiction. Since these rules do not generate any observation by definition.
This leads to $\tau_{am} = \tau_{am'}$.

Rule S:AM-NoBranch From the rule we have that $\Sigma_{S1}.\sigma \xrightarrow{\tau_{am}} \Sigma_{S2}.\sigma$ and $\Sigma'_{S1}.\sigma \xrightarrow{\tau'_{am}} \Sigma'_{S1}.\sigma$.
From $X_{S1}.\sigma = \Sigma_{S1}.\sigma$, $X'_{S1}.\sigma = \Sigma'_{S1}.\sigma$ and $\Sigma_{S1} \cong \Sigma'_{S1}$ together with $INV2(X_{S1}, \Sigma_{S1})$ (so $X_{S1}.n = \Sigma_{S1}.n$) and $INV2(X''_{S1}, \Sigma'_{S1})$ we have that Rule S:NoBranch was used to derive $X_{S1} \overset{\tau_{sp}}{\rightsquigarrow}_S^O X_{S2}$ and $X'_{S1} \overset{\tau'_{sp}}{\rightsquigarrow}_S^O X'_{S2}$. From Rule S:NoBranch we have that τ_{sp}, τ'_{sp} come from $X_{S1} \xrightarrow{\tau_{sp}} X_{S2}$ and $X'_{S1} \xrightarrow{\tau'_{sp}} X'_{S2}$. Combined with $X_{S1}.\sigma = \Sigma_{S1}.\sigma$, $X'_{S1}.\sigma = \Sigma'_{S1}.\sigma$ and the determinism of the non-speculative semantics we have $\tau_{am} = \tau'_{sp}$ and $\tau'_{am} = \tau'_{sp}$ and by our assumption $\tau_{am} \neq \tau'_{am}$ we get $\tau_{sp} \neq \tau'_{sp}$.

Rule S:AM-Store-Spec Then, $\tau_{am}, \tau_{am'}$ are generated by the step $\Sigma_{S1}.\sigma \xrightarrow{\tau_{am}} \Sigma_{S2}.\sigma$ and $\Sigma'_{S1}.\sigma \xrightarrow{\tau_{am'}} \Sigma'_{S2}.\sigma$ generated by Rule S:AM-Store-Spec.
From the fact that $X_{S1} \cong X'_{S1}$, $X_{S1}.\sigma = \Sigma_{S1}.\sigma$, $X'_{S1}.\sigma = \Sigma'_{S1}.\sigma$, $INV2(X_{S1}, \Sigma_{S1})$, $INV2(X'_{S1}, \Sigma'_{S1})$ and from the way we construct the oracle (see above), we have that $O(p, X_{S1}.\sigma(pc), X_{S1}.h) = O(p, X'_{S1}.\sigma(\mathbf{pc}), X'_{S1}.h) = (true, \omega)$ it follows that Rule S:Store-Skip applies to both X_{S1} and X'_{S1}.

From Rule S:Store-Skip, we have $X_{S1} \overset{\tau_{sp}}{\rightsquigarrow}_S^O X_{S2}$ and $X'_{S1} \overset{\tau'_{sp}}{\rightsquigarrow}_S^O X'_{S2}$ and we know that $X_{S1}.\sigma \xrightarrow{\tau_{sp}} X_{S2}.\sigma$ and $X'_{S1}.\sigma \xrightarrow{\tau_{sp'}} X'_{S2}.\sigma$. Because the non-speculative semantics $\rightarrow$ is deterministic, we have $\tau_{am} = \tau_{sp}$ and $\tau_{am'} = \tau_{sp'}$ and by our assumption $\tau_{am} \neq \tau_{am'}$. This results in $\tau_{sp} \neq \tau'_{sp}$ which proves our claim.

This completes the proof of our claim.

□

Lemma 50 (Stronger Soundness for a specific oracle and for specific executions). *Specific executions means that there is a difference in the trace but before there is none. We use the oracle O_{am_S} as it is defined by Definition 56 (Constructing the Oracle) for the given execution. If*

(1) $\Sigma_{S1} \cong \Sigma_{S2}$
(2) $X_{S1} \cong X_{S2}$ *and* $\overline{\rho} = \emptyset$
(3) $\Sigma_{S1} \approx^{O_{am}} X_{S1}$ *and* $\Sigma_{S2} \approx^{O_{am}} X_{S2}$
(4) $\Sigma_{S1} \Downarrow_S^{\overline{\tau}} \Sigma'_{S1}$ *and* $\Sigma_{S2} \Downarrow_S^{\overline{\tau}} \Sigma'_{S2}$

and our oracle is constructed in the way described above Then

I $X_{S1} \overset{O}{\downarrow}_{\overline{\tau}'}^S X'_{S1}, X_{S2} \overset{O}{\downarrow}_{\overline{\tau}''}^S X'_{S2}$
II $\Sigma'_{S1} \cong \Sigma'_{S2}$
III $X'_{S1} \cong X'_{S2}$ *and* $\overline{\rho} = \emptyset$
IV $\Sigma'_{S1} \approx^{O_{am}} X'_{S1}$ *and* $\Sigma'_{S2} \approx^{O_{am}} X'_{S2}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. Notice that the proof is very similar to Lemma 47 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states). The only thing that is different is that (1) the specific oracle only mispredicts so there is one less case in the relation and (2) we have a different invariant for that specific oracle i.e., $INV2(\Sigma_S, X_S)$

For these reasons we will only argue why $INV2(\Sigma'_{S1}, X'_{S1})$ holds in the different cases and leave the rest to the old soundness proof.

By Induction on $\Sigma_{S1} \Downarrow_S^{\overline{\tau}} \Sigma'_{S1}$ and $\Sigma_{S2} \Downarrow_S^{\overline{\tau}} \Sigma'_{S2}$.

Rule S:AM-Reflection We have $\Sigma_{S1} \Downarrow_S^{\varepsilon} \Sigma'_S$ and $\Sigma_{S2} \Downarrow_S^{\varepsilon} \Sigma''_S$, where $\Sigma'_S = \Sigma_{S1}$ and $\Sigma''_S = \Sigma_{S2}$. We choose $\Sigma'_{S1} = \Sigma'_S$ and $\Sigma'_{S2} = \Sigma''_S$.
We further use Rule S:Reflection to derive $X_{S1} \overset{O}{\downarrow}_{\varepsilon}^S X'_{S1}, X_{S2} \overset{O}{\downarrow}_{\varepsilon}^S X'_{S2}$ with $X'_{S1} = X_{S1}$ and $X'_{S2} = X_{S2}$. We now trivially satisfy all conclusions.

Rule S:AM-Single We have $\Sigma_{S1} \Downarrow_S^{\overline{\tau}''} \Sigma'_S$ with $\Sigma'_S \xrightarrow{\tau}_S \Sigma'_{S1}$ and $\Sigma_{S2} \Downarrow_S^{\overline{\tau}''} \Sigma''_S$ and $\Sigma''_S \xrightarrow{\tau}_S \Sigma'_{S2}$.
We now apply IH on $\Sigma_{S1} \Downarrow_S^{\overline{\tau}''} \Sigma'_S$ and $\Sigma_{S2} \Downarrow_S^{\overline{\tau}''} \Sigma''_S$ and get

(a) $X_{S1} \overset{O}{\downarrow}_{\overline{\tau}'}^S X'_S, X_{S2} \overset{O}{\downarrow}_{\overline{\tau}''}^S X''_S$

(b) $\Sigma'_S \cong \Sigma''_S$
(c) $X'_S \cong X''_S$ and $\overline{\rho}' = \varnothing$
(d) $\Sigma'_S \approx^{O_{am}} X'_S$ and $\Sigma''_S \approx^{O_{am}} X''_S$
(e) $\overline{\tau}' = \overline{\tau}''$

We do a case distinction on $\approx^{O_{am}}$ in $\Sigma'_S \approx^{O_{am}} X'_S$ and $\Sigma''_S \approx^{O_{am}} X''_S$ by inversion:

Rule Single-Base-Oracle We thus have $\Sigma'_S \sim X'_S\restriction_{com}$, $minWndw(X'_S) > 0$ and $INV2(\Sigma'_S, X'_S)$ (Similar for Σ''_S and X''_S).

We now proceed by inversion on the derivation $\Sigma'_S \overset{\tau}{\Longrightarrow}_S \Sigma'_{S_1}$ and $\Sigma''_S \overset{\tau}{\Longrightarrow}_S \Sigma'_{S_2}$.

Rule S:AM-Rollback Contradiction, because of $minWndw(X'_S) > 0$ and $INV2(\Sigma'_S, X'_S)$.

Rule S:AM-General $INV2()$ trivially holds, because it does not change the speculation window of the states.

Rule S:AM-Context: We have $\Phi_S \overset{\tau}{\Longrightarrow}_S \overline{\Phi}_S$ and $\Phi'_S \overset{\tau}{\Longrightarrow}_S \overline{\Phi}'_S$. We fulfill all conditions for Lemma 51 (V4AM: Strong Soundness Single Step) which gives us the desired result.

Rule Single-Transaction-Rollback-Oracle We have

$$\begin{aligned}
X'_S &= X_{S3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma'', h', 0 \rangle^{false} \cdot X_{S4} \\
\Sigma'_S &= \Sigma_{S3} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle^{false} \cdot \Sigma_{S4} \\
X_S &= X_{S3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \\
\Sigma_S &= \Sigma_{S3} \cdot \langle p, ctr, \sigma, n \rangle \\
\Sigma_S &\sim X_S\restriction_{com} \\
&\quad INV2(\Sigma_S, X_S) \\
n' &\geq 0
\end{aligned}$$

The form of X''_S and Σ''_S is analogous.

Additionally we know that the transaction terminates in some state $\Sigma_S \Downarrow^{\overline{\tau}}_S \Sigma'''_S$. There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma'_S \overset{\tau}{\Longrightarrow}_S \Sigma'_{S_1}$ is not a roll back. Because Σ_S and X_S do not change, $INV2(\Sigma_S, X_S)$ does not change as well. The states are still related by Rule Single-Transaction-Rollback after the step.

$n' = 0$ Then we know that $\Sigma'_S \overset{\tau}{\Longrightarrow}_S \Sigma'_{S_1}$ was created by Rule S:AM-Rollback and is a rollback for ctr.
Notice, that the only difference to X_S and Σ_S is the updated ctr, because of the roll back. Updating the counter does not change the invariant $INV2()$. This means $INV2(\Sigma_S, X_S)$ (with updated ctr) still holds.

□

Lemma 51 (V4AM: Strong Soundness Single Step)**.** *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, O be a prediction oracle with speculative window at most ω, $\Sigma_{S1} = \Sigma'_S \cdot \Phi'_S$, $\Sigma_{S2} = \Sigma''_S \cdot \Phi''_S$ be two speculative states for the always mispredict semantics and X_{S1}, X_{S2}, be two speculative states for the speculative semantics.*

If the following conditions hold:

(1) $\Sigma_{S1} \cong \Sigma_{S2}$
(2) $X_{S1} \cong X_{S2}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma_{S1} \approx^{O_{am}} X_{S1}$ *and* $\Sigma_{S2} \approx^{O_{am}} X_{S2}$
(4) $\Phi'_S \overset{\tau''}{\Longrightarrow}_S \Sigma'_{S_1}$ *and* $\Phi''_S \overset{\tau''}{\Longrightarrow}_S \Sigma'_{S_2}$

then there are instances X'_{S_1}, X'_{S_2} for the speculative semantics such that:

I $X_{S_1} \overset{O_{\downarrow S}}{\Longrightarrow}_\tau X'_{S_1}$ *and* $X_{S_2} \overset{O_{\downarrow S}}{\Longrightarrow}_{\tau'} X'_{S_2}$
II $\Sigma'_{S_1} \cong \Sigma'_{S_2}$
III $X'_{S_1} \cong X'_{S_2}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{S_1} \approx^{O_{am}} X'_{S_1}$ *and* $\Sigma'_{S_2} \approx^{O_{am}} X'_{S_2}$
V $\tau = \tau'$

Proof. The proof is very similar to Lemma 48 (S: Soundness Single Step AM). The only thing that is different is that (1) the specific oracle only mispredicts so there is one less case in the relation and (2) we have a different invariant for that specific oracle i.e., $INV2(\Sigma_S, X_S)$

For these reasons we will only argue why $INV2(\Sigma'_{S_1}, X'_{S_1})$ holds in the different cases and leave the rest to the old soundness proof.

Now we do case distinction on the instruction executed:

not store instruction We prove that $INV2(\Sigma'_{S_1}, X'_{S_1})$ still holds. The proof for $INV2(\Sigma'_{S_2}, X'_{S_2})$ is analogous.

Note that $|X_S\restriction_{com}| = |X_S|$ for all states X_S, because our oracle only mispredicts. We need to show that $|\Sigma'_{S_1}| = |X'_{S_1}|$ and $minWndw(X'_{S_1}) = \Sigma'_{S_1}.n$.

$|\Sigma'_{S_1}| = |X'_{S_1}|$ Sine the rules that apply here do not create or remove a speculative instance we have

$$|\Sigma'_{S_1}| = |X'_{S_1}|$$
$$|\Sigma'_{S}| = |X'_{S}|$$

which we know by the assumption $INV2(\Sigma'_S, X'_S)$.

$minWndw(X'_S) = \Sigma'_{S_1}.n$ Since the executed instruction was not a store instruction instruction, we have two cases

barrier instruction Then $minWndw(X'_{S_1}) = minWndw(zeroes(X'_S)) = 0$ and $\Sigma'_{S_1}.n = 0$ and we satisfy $INV2(\Sigma'_{S_1}, X'_{S_1})$.

not barrier Then $minWndw(X'_{S_1}) = minWndw(decr(X'_S))$ and $\Sigma'_{S_1}.n = \Sigma'_S.n - 1$.

By definition of $INV2(\Sigma'_S, X'_S)$ we have $minWndw(X'_S) = \Sigma'_S.n$ and by $\approx^{O_{am}}$ in the base case, we know that $n > 0$. Note that this means that there is no instance in X'_S with a speculation window of 0. We can now conclude that $minWndw(decr(X'_S)) = minWndw(X'_S) - 1$.

$$\begin{aligned} minWndw(X'_S) &= \Sigma'_S.n \\ minWndw(X'_S) - 1 &= \Sigma'_S.n - 1 \\ minWndw(decr(X'_S)) &= \Sigma'_{S_1}.n \\ minWndw(X'_{S_1}) &= \Sigma'_{S_1}.n \end{aligned}$$

Rule S:AM-Store-Spec We know that our oracle only mispredicts. That is why only rule S:Store-Skip will be used for oracle states.

$$\begin{aligned} X'_{S_1} &= X'''_S \cdot \Psi_S \\ minWndw(X'''_S) &= minWndw(decr(X'_S)) = minWndw(X'_S) - 1 \\ X'_S.\sigma &\xrightarrow{\tau} X'''_S.\sigma \\ \Sigma'_{S_1} &= \Sigma'''_S \cdot \Phi_S \\ \Sigma'''_S.n &= \Sigma'_S.n - 1 \\ \Sigma'_S.\sigma &\xrightarrow{\tau} \Sigma'''_S.\sigma \end{aligned}$$

Note that the step $minWndw(decr(X'_S)) = minWndw(X'_S) - 1$ comes from the fact that $minWndw(X'_S) = \Sigma'_S.n$ and $\Sigma_S.n > 0$ by assumption.

Depending on the output of the oracle we switch the relation

$O(p, \sigma, h) = (true, 0)$ We need to show that $INV2(\Sigma'''_S, X'''_S)$ holds. The argument is the same as above for not store instruction. We now fulfill all premises to relate by Rule Single-Transaction-Rollback-Oracle.

$O(p, \sigma, h) = (true, \omega)$ We need to show that $INV2(\Sigma'''_S \cdot \Phi_S, X'''_S \cdot \Phi_S)$ holds. The argument for $INV2(\Sigma'''_S, X'''_S)$ is the same as above. Furthermore, we know that $\Psi_S.n = \omega$ by the output of the oracle and $\Phi_S.n = \min(\omega, \Sigma'_S.n - 1)$.

There are two cases depending on $\min(\omega, \Sigma_S.n - 1)$.

$\Phi_S.n = \omega$ Then by definition $\Sigma'_S.n = \bot$ and from $\Sigma'_S \sim X'_S$ we get $|\Sigma'_S| = |X'_S| = 1$ and $X'_S.n = \bot$. Otherwise they would not be related.

Since $\bot > \omega$ and $\bot - 1 = \bot$, we have $minWndw(X'_{S_1}) = \omega$ and $\Sigma'_{S_1}.n = \omega$ and are finished.

$\Phi_S.n = \Sigma'_S.n - 1$ Then $n \neq \bot$ and we now that $\Sigma'''_S.n = \Sigma'_S.n - 1$.

Furthermore we know that $INV2(\Sigma'''_S, X'''_S)$ holds.

So $minWndw(X'''_S) = \Sigma'''_S.n$. Since $\Sigma'''_S.n < \omega$ we know that $minWndw(X'''_S) < \omega$.

From this we can follow that $minWndw(X'_{S_1}) < \omega$ (because $\Psi_S.n = \omega$).

Now we have $minWndw(X'_{S_1}) = minWndw(X'''_S \cdot \Psi_S) = minWndw(X'''_S)$ and $\Sigma'_{S_1}.n = \Sigma'_S.n - 1 = \Sigma'''_S.n$.

Thus, by $INV2(\Sigma'''_S, X'''_S)$ we have $INV2(\Sigma'_{S_1}, X'_{S_1})$

We can relate by Rule Single-Base-Oracle.

□

J REDEFINITIONS B

Here, we write down all the lemmas that were proven for Spectre v1 by Spectector.

Definition 58 (Constructing the AM Oracle). *Constructing the prediction oracle O_{am_B}. Analogous to [21].*

Lemma 52 (B: Soundness Single Step AM). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, O be a prediction oracle with speculative window at most ω, $\Sigma_{B1} = \Sigma'_B \cdot \Phi'_S$, $\Sigma_{B2} = \Sigma''_B \cdot \Phi''_S$ be two speculative states for the always mispredict semantics and X_{B1}, X_{B2}, be two speculative states for the speculative semantics.*

If the following conditions hold:

(1) $\Sigma_{B1} \cong \Sigma_{B2}$
(2) $X_{B1} \cong X_{B2}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma_{B1} \approx X_{B1}$ *and* $\Sigma_{B2} \approx X_{B2}$
(4) $\Phi'_B \overset{\tau''}{\dashrightarrow}_B \Sigma'_{B1}$ *and* $\Phi''_B \overset{\tau''}{\dashrightarrow}_B \Sigma'_{B2}$

then there are instances X'_{B1}, X'_{B2} for the speculative semantics such that:

I $X_{B1} \overset{O_B}{\Downarrow}{}^B_{\tau} X'_{B1}$ *and* $X_{B2} \overset{O_B}{\Downarrow}{}^B_{\tau'} X'_{B2}$
II $\Sigma'_{B1} \cong \Sigma'_{B2}$
III $X'_{B1} \cong X'_{B2}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{B1} \approx X'_{B1}$ *and* $\Sigma'_{B2} \approx X'_{B2}$
V $\tau = \tau'$

Lemma 53 (B: Stronger Soundness for a specific oracle and for specific executions). *Specific executions means that there is a difference in the trace but before there is none. We use the oracle O_{am_S} as it is defined by Definition 56 (Constructing the Oracle) for the given execution. If*

(1) $\Sigma_{B1} \cong \Sigma_{B2}$
(2) $X_{B1} \cong X_{B2}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma_{B1} \approx^{O_{am}} X_{B1}$ *and* $\Sigma_{B2} \approx^{O_{am}} X_{B2}$
(4) $\Sigma_{B1} \overset{O_B}{\Downarrow}{}^B_{\overline{\tau}} \Sigma'_{B1}$ *and* $\Sigma_{B2} \Downarrow^{\overline{\tau}}_S \Sigma'_{B2}$

and our oracle is constructed in the way described above Then

I $X_{B1} \overset{O_B}{\Downarrow}{}^B_{\overline{\tau}'} X'_{B1}, X_{B2} \overset{O_B}{\Downarrow}{}^B_{\overline{\tau}''} X'_{B2}$
II $\Sigma'_{B1} \cong \Sigma'_{B2}$
III $X'_{B1} \cong X'_{B2}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{B1} \approx^{O_{am}} X'_{B1}$ *and* $\Sigma'_{B2} \approx^{O_{am}} X'_{B2}$
V $\overline{\tau}' = \overline{\tau}''$

Definition 59 (B: Relation between AM and spec for all oracles). *We define two relations between AM and oracle semantics. $\approx$ $\sim$*

$\boxed{\Sigma_B \approx_B X_B}$

$$\frac{}{\varnothing \approx_B \varnothing}\ (Base) \qquad \frac{\Sigma_B \sim X_B \restriction_{com} \quad INV(\Sigma_B, X_B)}{\Sigma_B \approx_B X_B}\ (V1{:}Single\text{-}Base)$$

$$\frac{\begin{array}{c}\Sigma_B \sim X_B \restriction_{com} \qquad \Sigma''_B \Downarrow^{\overline{\tau}}_B \Sigma'''_B \text{ where transaction with id ctr is rolled back} \\ X_B = X'_B \cdot \langle p, ctr, \sigma, h, n'' \rangle \quad \Sigma_B = \Sigma'_B \cdot \langle p, ctr, \sigma, n \rangle \quad INV(\Sigma_B, X_B) \quad \sigma(\mathbf{pc}) = m\end{array}}{\Sigma'_B \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle \cdot \Sigma_{B1} \approx_B X'_B \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma, h, n''' \rangle^m}\ (V1{:}Single\text{-}OracleTrue)$$

$$\frac{\begin{array}{c}\Sigma''_B \sim X''_B \restriction_{com} \quad n' \geq 0 \quad \Sigma''_B \Downarrow^{\overline{\tau}}_B \Sigma'''_B \text{ where transaction with id ctr is rolled back} \\ X_B = X'_B \cdot \langle p, ctr, \sigma, h, n'' \rangle \qquad \Sigma_B = \Sigma'_B \cdot \langle p, ctr, \sigma, n \rangle \qquad INV(\Sigma_B, X_B)\end{array}}{\Sigma'_B \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle^m \cdot \Sigma_{B1} \approx_B X'_B \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma'', h', 0 \rangle^m \cdot X_{B1}}\ (V1{:}Single\text{-}Transaction\text{-}Rollback)$$

$\boxed{\Sigma_B \sim X_B}$

$$\frac{}{\varnothing \sim \varnothing}\ (Base) \qquad \frac{|\Sigma'_B| = |X'_B| \quad \Sigma'_B \sim X'_B}{\Sigma'_B \cdot \langle p, ctr, \sigma, n \rangle^b \sim X'_B \cdot \langle p, ctr', \sigma, h, n' \rangle^b}\ (V1{:}Single)$$

Definition 60 (B: Relation between AM and Spec for oracles that only mispredict). *We define two relations, $\approx^{O_{am}}$ and $\sim$, between AM and oracle semantics. Note that $\approx^{O_{am}}$ is indexed by an oracle. This oracle has to always mispredict.*

$$\boxed{\Sigma_B \approx^{O_{am}} X_B}$$

$$\frac{}{\varnothing \approx^{O_{am}} \varnothing}\ \textit{(Base-Oracle)} \qquad \frac{\Sigma_B \sim X_B\restriction_{com} \quad INV2(\Sigma_B, X_B) \quad minWndw(X_B) > 0}{\Sigma_B \approx^{O_{am}} X_B}\ \textit{(Single-Base-Oracle)}$$

$$\frac{\begin{array}{c}\Sigma''_B \sim X''_B\restriction_{com} \quad n' \geq 0 \quad \Sigma''_B \overset{O_B}{\Rightarrow}_{\overline{\tau}} \Sigma'''_B \text{ where transaction with id ctr is rolled back} \\ X_B = X'_B \cdot \langle p, ctr, \sigma, h, n''\rangle \qquad \Sigma_B = \Sigma'_B \cdot \langle p, ctr, \sigma, n\rangle \qquad INV2(\Sigma_B, X_B)\end{array}}{\Sigma'_B \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle^m \cdot \Sigma_{B1} \approx^{O_{am}} X'_B \cdot \langle p, ctr, \sigma, h, n''\rangle \cdot \langle p, ctr', \sigma'', h', 0\rangle^m}\ \textit{(Single-Transaction-Rollback-Oracle)}$$

Lemma 54 (B: Completeness Am semantics w.r.t. speculative semantics). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, $\sigma, \sigma' \in InitConf$ be two initial configurations. If*

(1) $p, \sigma \text{🕱}^{\omega}_{B} \overline{\tau}$ and $p, \sigma' \text{🕱}^{\omega}_{B} \overline{\tau}'$ and
(2) $\overline{\tau} \neq \overline{\tau}'$

Then there exists an oracle O such that

I $p, \sigma \text{🕱}^{O}_{B} \overline{\tau}_1$ and $p, \sigma' \text{🕱}^{O}_{B} \overline{\tau}'_1$ and
II $\overline{\tau}_1 \neq \overline{\tau}'_1$

SPECTRE V5

Our main result for R is the following

Theorem 18 (R is *SSS*). $\vdash \text{R}\ SSS$

Proof. Immediately follows from Theorem 22 (R: SNI), Theorem 21 (R: Behaviour of AM and symbolic semantics), Theorem 20 (V5AM: Behaviour of non-speculative semantics and AM semantics) and Theorem 19 (R SE: Behaviour of non-speculative and oracle semantics). □

J.1 R: Relating Non-speculative and Oracle Semantics

Conceptually, these proofs are very similar to the ones from V4.

Theorem 19 (R SE: Behaviour of non-speculative and oracle semantics). *Let p be a program and O be a prediction oracle. Then* $Beh_{NS}(p) = Beh_{\text{R}}^{O}(p)\restriction_{ns}$

Proof. We prove the two directions separately:

⇐ By the definition of $Beh_{\text{R}}^{O}(p)$ we have an initial configuration σ such that $(p,\sigma)\ \text{R}_{\text{R}}^{O}\ \overline{\tau}$.

By definition of $(p,\sigma)\ \text{R}_{\text{R}}^{O}\ \overline{\tau}$, we know there exists a state X'_{R} such that $\vdash X'_{\text{R}}$: *fin* and an initial state $\Sigma_{\text{R}}^{init}p,\sigma$ such that $\Sigma_{\text{R}}^{init}p,\sigma\ {}^{O}\!\downarrow_{\overline{\tau}}^{\text{R}} X'_{\text{R}}$.
Analogous to the corresponding case in Theorem 14 (S SE: Behaviour of non-speculative and oracle semantics) by using Lemma 55 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).
We thus have $(p,\sigma)\ \text{R}_{NS}^{O}\ \overline{\tau}\restriction_{ns} \in Beh_{NS}(p)$ by Rule NS-Trace.

⇒ Assume that $(p,\sigma)\ \text{R}_{NS}^{O}\ \overline{\tau} \in Beh_{NS}(p)$. We thus know there exists $\sigma' \in FinalConf$ such that $\sigma \Downarrow_{\overline{\tau}} \sigma'$.

Analogous to the corresponding case in Theorem 14 (S SE: Behaviour of non-speculative and oracle semantics) by using Lemma 60 (R SE: Completeness of the speculative semantics).
We thus have $(p,\sigma)\ \text{R}_{\text{R}}^{O}\ \overline{\tau}\cdot\overline{\tau}'' \in Beh_{\text{R}}^{O}(p)$.

□

Lemma 55 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics)**.** *If*

(1) $X_{\text{R}}.\sigma = \sigma$ *and*
(2) $\vdash_O X_{\text{R}}$: *noongoing and*
(3) $X_{\text{R}}\ {}^{O}\!\downarrow_{\overline{\tau}}^{\text{R}} X'_{\text{R}}$

Then there exists σ' such that

I if $\vdash_O X'_{\text{R}}$: *noongoing then* $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}} \sigma'$ *and* $X'_{\text{R}}.\sigma = \sigma'$ *and*
II if $\vdash_O^i X'_{\text{R}}$: *biggestongoingtransactionirolledback then by definition exists id i such that it is the smallest transaction id that will be rolled back and is still active then* $\sigma \Downarrow_{helper(\overline{\tau},i)} \sigma'$ *and σ' is the configuration with the instance with ctr = i.*

Proof. We proceed by induction on $X_{\text{R}}\ {}^{O}\!\downarrow_{\overline{\tau}}^{\text{R}} X'_{\text{R}}$

Rule R:SE-Reflection Then we have $X_{\text{R}}\ {}^{O}\!\downarrow_{\varepsilon}^{\text{R}} X_{\text{R}}$ with $X'_{\text{R}} = X_{\text{R}}$ and by Rule NS-Reflection we have
I $\sigma \Downarrow_{\varepsilon\restriction_{ns}} \sigma'$ with $\sigma = \sigma'$.
II $\sigma \Downarrow_{helper(\varepsilon,i)} \sigma'$ with $\sigma = \sigma'$.

Rule R:SE-Single We have $X_{\text{R}}\ {}^{O}\!\downarrow_{\overline{\tau}'\cdot\tau}^{\text{R}} X'_{\text{R}}$ and by Rule R:SE-Single we get $X_{\text{R}}\ {}^{O}\!\downarrow_{\overline{\tau}'}^{\text{R}} X''_{\text{R}}$ and $X''_{\text{R}}\ \overset{\tau}{\rightsquigarrow}_{\text{R}}^{O}\ X'_{\text{R}}$.
We need to proof
I if $\vdash_O X'_{\text{R}}$: *noongoing* then $\sigma \Downarrow_{\overline{\tau}\cdot\tau\restriction_{ns}\sigma'}$ and $X'_{\text{R}}.\sigma = \sigma'$
II if $\vdash_O^i X'_{\text{R}}$: *biggestongoingtransactionirolledback* then by definition exists *id i* such that it is the smallest transaction *id* that will be rolled back and is still active then $\sigma \Downarrow_{helper(\overline{\tau}\cdot\tau,i)} \sigma'$ and σ' is the configuration for the instance with *ctr* = *i*.
We apply the IH on $X_{\text{R}}\ {}^{O}\!\downarrow_{\overline{\tau}'}^{\text{R}} X''_{\text{R}}$ and have a σ'' where σ'' is the configuration for some instance in X''_{R} such that.
I' if $\vdash_O X''_{\text{R}}$: *noongoing* then $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}\sigma''}$ and $X''_{\text{R}}.\sigma = \sigma''$
II' if $\vdash_O^j X''_{\text{R}}$: *biggestongoingtransactionirolledback* then by definition exists *id* j such that it is the smallest transaction *id* that will be rolled back and is still active then $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$ and σ'' is the configuration with the instance with *ctr* = *j*.
We proceed by case analysis on X''_{R}.
no ongoing transactions in X''_{R} Then X''_{R} has no ongoing transactions, meaning $\vdash_O X''_{\text{R}}$: *noongoing* and we have $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}} \sigma''$ and $X''_{\text{R}}.\sigma = \sigma''$ by IH.

I Then $\vdash_O X'_R$: *noongoing* and we need to prove $\sigma \Downarrow_{\overline{\tau}\cdot\tau\restriction_{ns}\sigma'}$ and $X'_R.\sigma = \sigma'$. We now proceed by inversion on $X''_R \overset{\tau}{\rightsquigarrow}{}^{O}_{R} X'_R$:

Rule R**:SE-Rollback** Analogous to the corresponding case in Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

Rule R**:SE-Ret and the top value of** $\mathbb{R}$ **is different to the saved return address in** $m(a(\mathbf{sp}))$ Then we know that $\overline{\rho} = \texttt{ret}\ l \cdot \texttt{start}\ id$ for X'_R, where l is the value at the top of the $\mathbb{R}$. The contradiction is analogous to the case of Rule S:Store-Skip in Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) and the fact that the created transaction will be rolled back.

otherwise We know that $\sigma'' = X''_R.\sigma$. Since $\vdash_O X''_R$: *noongoing*, there no ongoing transactions that need to be rolled back.

Furthermore, no transaction that will be rolled back is created in the step $X''_R \overset{\tau}{\rightsquigarrow}{}^{O}_{R} X'_R$, because $\vdash_O X'_R$: *noongoing*.
The case is analogous to Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) by using Lemma 56 (R SE: Soundness single step No Speculation).

II Then X'_R has ongoing transactions, meaning $\vdash^{i}_{O} X'_R$: *biggestongoingtransactionirolledback* and we need to prove $\sigma \Downarrow_{helper(\overline{\tau}\cdot\tau,i)} \sigma'$ and σ' is the configuration for the instance with $ctr = i$.

We now proceed by inversion on $X''_R \overset{\tau}{\rightsquigarrow}{}^{O}_{R} X'_R$:

Rule R**:SE-Ret and the top value of** $\mathbb{R}$ **is different to the saved return address in** $m(a(\mathbf{sp}))$ Then we know that $\overline{\rho} = \texttt{ret}\ l \cdot \texttt{start}\ id$ for X'_R.
Since we know a new transaction was created that will be rolled back, we also know that $id = i$.
We know that, because $\vdash_O X''_R$: *noongoing*, so there was not another ongoing transaction.
The case is analogous to Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) together with Lemma 59 (R SE: Return step Speculation).

otherwise By definition of $\vdash^{i}_{O} X'_R$: *biggestongoingtransactionirolledback* we know that there exists a $\texttt{rlb}\ i$ in the execution $X'_R \overset{O}{\Downarrow}{}^{R}_{\overline{\tau}_{fin}} X_{R_{fin}}$ with no matching $\texttt{start}\ i$ observation in that execution.
The contradiction can be derived in the same way as in the analogous case in Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

ongoing transactions in X''_R Then X''_R has ongoing transactions, meaning $\vdash^{j}_{O} X''_R$: *biggestongoingtransactionirolledback* and we have $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$ and σ'' is the configuration for the instance with $ctr = j$.

I Then $\vdash_O X'_R$: *noongoing* and we need to prove $\sigma \Downarrow_{\overline{\tau}\cdot\tau\restriction_{ns}\sigma'}$ and $X'_R.\sigma = \sigma'$. We now proceed by inversion on $X''_R \overset{\tau}{\rightsquigarrow}{}^{O}_{R} X'_R$:

Rule R**:SE-Rollback and** $\tau = \texttt{rlb}\ j$ Choose $\sigma' = \sigma''$. Since $\overline{\tau} \cdot \tau\restriction_{ns} = helper(\overline{\tau}, j)$ we can use IH $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$.
Analogous to the corresponding case in Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Then $\tau \neq \texttt{rlb}\ j$.
Deriving the contradiction is analogous to the corresponding case in Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

II Then $\vdash^{i}_{O} X'_R$: *biggestongoingtransactionirolledback* and we need to prove $\sigma \Downarrow_{helper(\overline{\tau}\cdot\tau,i)} \sigma'$ and σ' is the configuration for the instance below the instance with $ctr = i$.
We now proceed by inversion on $X''_R \overset{\tau}{\rightsquigarrow}{}^{O}_{R} X'_R$:

Rule R**:SE-Rollback** Then $\tau = \texttt{rlb}\ id$. We do a case analysis if $id = j$ or not.

$id = j$ Analogous to Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

$id \neq j$ Analogous to Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Analogous to Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

□

Lemma 56 (R SE: Soundness single step No Speculation)**.** *If*

(1) $\vdash_O X_R$: *noongoing and*
(2) $X_R \overset{\tau}{\rightsquigarrow}{}^{O}_{R} X'_R$ *and*
(3) $\vdash_O X'_R$: *noongoing and*
(4) $\sigma = X_R.\sigma$

Then there exists σ' *such that*

I $\sigma \Downarrow_{\tau\restriction_{ns}} \sigma'$ *and*
II $X'_R.\sigma = \sigma'$

Proof. We proceed by inversion on $X_R \overset{\tau}{\rightsquigarrow}{}^{O}_{R} X'_R$:

Rule R**:SE-General** Thus we have $X_R = \overline{\Psi}_R \cdot \Psi_{R\overline{\rho}\cdot\tau}$ and $X'_R = \overline{\Psi}_R \cdot \Psi_{R\overline{\rho}}$ with $\Psi_R.\sigma = \sigma$.

By the definition of $\Psi_R \overset{\tau}{\rightsquigarrow}{}^{O}_{R} X_R$ only Rule R:SE-Ret adds observations to $\overline{\rho}$.
These observations are only `start` n and `ret` l.
By the definition of $\restriction_{ns}$ we have $\tau\restriction_{ns} = \varepsilon$ and we have $\sigma \Downarrow_{\varepsilon\restriction_{ns}} \sigma$ by Rule NS-Reflection.

Rule R:SE-Commit Then the generated observation is $\tau =$ `commit` id. Furthermore, `commit` $id\restriction_{ns} = \varepsilon$.
By the definition of the rule, we have $X_R.\sigma = X'_R.\sigma$ and with this we get $X'_R.\sigma = \sigma$.
Thus, we can derive $\sigma \Downarrow_{\texttt{commit } id\restriction_{ns}} \sigma$.

Rule R:SE-Rollback Contradiction, since $\vdash_O X_R$: *noongoing* and Definition 44 (Well orderedness of rollback and start).

Rule R:SE-Context We have $X_R = \overline{\Psi}_R \cdot \Psi_R$ and $X'_R = \overline{\Psi}''_R \cdot \overline{\Psi}'_R$ with $\Psi_R \overset{\tau}{\rightsquigarrow}{}^{O}_{R} \overline{\Psi}'_R$. By Lemma 57 (R SE: Single Step Instance Non Speculative) we have $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ with $\sigma = \Psi_R.\sigma$ and $\overline{\Psi}'_R.\sigma = \sigma'$.

□

Lemma 57 (R SE: Single Step Instance Non Speculative)**.** *If*

(1) $X_R = \overline{\Psi}_R \cdot \Psi_R$ *and*
(2) $X'_R = \overline{\Psi}_R \cdot \overline{\Psi}'_R$ *and* $\vdash_O X'_R$: *noongoing and*
(3) $\Psi_S \overset{\tau}{\rightsquigarrow}{}^{O}_{R} \overline{\Psi}'_R$ *and*
(4) $\sigma = \Psi_R.\sigma$

Then there is a σ' *such that*

I $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ *and*
II $\overline{\Psi}'_R.\sigma = \sigma$

Proof. We proceed by case analysis on the rule used to derive $\Psi_R \overset{\tau}{\rightsquigarrow}{}^{O}_{R} \Psi'_R$.

Rule R:SE-Ret Then we have:

$$\begin{aligned}
\sigma \xrightarrow{\tau} &\sigma' \\
\mathbb{R} =&\mathbb{R}' \cdot l \\
\sigma'' =&\sigma[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto a(\mathbf{sp}) + 8] \\
\overline{\Psi}_R =&\langle p, ctr, \sigma', \mathbb{R}', h', n\rangle \cdot \langle p, ctr+1, \sigma'', \mathbb{R}', h', \omega\rangle^{l}_{\texttt{ret } l\cdot\texttt{start } ctr}
\end{aligned}$$

Then we have $\sigma \xrightarrow{\tau} \sigma', \mathbb{R} = \mathbb{R}'\cdot l$ and $\sigma'' = \sigma[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto a(\mathbf{sp})+8]$ and $\overline{\Psi}_R = \langle p, ctr, \sigma', \mathbb{R}', h', n\rangle \cdot \langle p, ctr+1, \sigma'', \mathbb{R}', h', \omega\rangle^{l}_{\texttt{ret } l\cdot\texttt{st } (ctr)}$.
There are two cases depending if the return address on top of the $\mathbb{R}$ and on the stack match:
$m(a(\mathbf{sp})) = l$ This is a commit. We know show that $\sigma' = \sigma''$.
Since $p(\sigma(\mathbf{pc})) =$ **ret** we know that Rule Retwas used in $\rightarrow$. Thus $\sigma' = \sigma[\mathbf{pc} \mapsto m(a(\mathbf{sp})), \mathbf{sp} \mapsto a(\mathbf{sp}) + 8]$.
Because $m(a(\mathbf{sp})) = l$ we have $\sigma'' = \sigma' = \sigma[\mathbf{pc} \mapsto m(a(\mathbf{sp})), \mathbf{sp} \mapsto a(\mathbf{sp}) + 8]$.
Thus, $\sigma' = \overline{\Psi}'_R.\sigma$.
Because the rule used the observation received from the the step $\sigma \xrightarrow{\tau} \sigma'$, we have $\tau\restriction_{ns} = \tau$ and are finished.
$m(a(\mathbf{sp})) \neq l$ Contradiction, because this starts a speculative transaction that needs to be rolled back.
This cannot happen because of $\vdash_O X'_R$: *noongoing*.

Rule R:SE-Ret-Empty We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule and $\overline{\Psi}'_R = \langle p, ctr, \sigma', \mathbb{R}, h, n-1\rangle$.
Thus, $\sigma' = \overline{\Psi}'_R.\sigma$.
Because the rule used the observation received from the the step $\sigma \xrightarrow{\tau} \sigma'$, we have $\tau\restriction_{ns} = \tau$ and are finished.

otherwise Thus, we have $p(\sigma(\mathbf{pc})) \neq$ **ret** and $n \neq 0$ and can apply Lemma 58 (R SE: no Ret speculation). We get get an execution $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ and $\sigma' = X'_R.\sigma$.

□

Lemma 58 (R SE: no Ret speculation)**.** *Let* p *be a program,* O *be a prediction oracle. If*

(1) $\Psi_R = \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle$ *and*
(2) $\Psi_R \overset{\tau}{\rightsquigarrow}{}^{O}_{R} \overline{\Psi}'_R$, *and*
(3) $p(\sigma(\mathbf{pc})) \neq$ **ret** *and*
(4) $n \neq 0$

Then there is a σ' *such that*

I $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ *and*
II $\sigma' = \overline{\Phi}'.\sigma$.

Proof. Let p be a program, O be a prediction oracle.
We have

(1) $\Psi_R = \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle$ and
(2) $\Psi_R \overset{\tau}{\rightsquigarrow}^{O}_{R} \overline{\Psi}'_R$ and
(3) $p(\sigma(\mathbf{pc})) \neq \mathbf{ret}$ and
(4) $n \neq 0$

By inversion on $\Psi_R \overset{\tau}{\rightsquigarrow}^{O}_{R} X'_R$ and the fact that $p(\sigma(\mathbf{pc})) \neq \mathbf{ret}$ and and $n \neq 0$ we have three cases.

Rule R:SE-barr or Rule R:SE-barr-spec We show the proof for Rule R:SE-barr, the proof for Rule R:SE-barr-spec is analogous.
By Rule R:SE-barr we know $\sigma \xrightarrow{\tau} \sigma'$ and $\overline{\Psi}'_R = \langle p, ctr, \sigma', \mathbb{R}, h, n-1\rangle$.
Thus $\sigma' = \overline{\Psi}'_R.\sigma$ and $\tau = \varepsilon = \varepsilon\restriction_{ns}$.

Rule R:SE-NoBranch We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule and $\overline{\Psi}'_R = \langle p, ctr, \sigma', \mathbb{R}, h, n-1\rangle$.
Thus, $\sigma' = \overline{\Psi}'_R.\sigma$.
Because the rule used the observation received from the the step $\sigma \xrightarrow{\tau} \sigma'$, we have $\tau\restriction_{ns} = \tau$ and are finished.

Rule R:SE-Call-Full or Rule R:SE-Call We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule and $\overline{\Psi}'_R = \langle p, ctr, \sigma', \mathbb{R}, h, n-1\rangle$.
The case is analogous to case Rule R:SE-NoBranch.

□

Lemma 59 (R SE: Return step Speculation)**.** *If*

(1) $X_R = \overline{\Psi}_R \cdot \Psi_R$ *and* $\vdash_O X_R$: *noongoing*
(2) $X'_R = \overline{\Psi}_R \cdot \overline{\Psi}'_R$ *and* $\vdash^{i}_{O} X'_R$: *biggestongoingtransactionirolledback and*
(3) $\Psi_R \overset{\tau}{\rightsquigarrow}^{O}_{R} \overline{\Psi}'_R$ *and*
(4) $\sigma = \Psi_R.\sigma$

Then

I $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ *and*
II σ' *is the configuration for the instance with* $ctr = i$ *in* X'_R

Proof. We proceed by inversion on $\Psi_R \overset{\tau}{\rightsquigarrow}^{O}_{R} \overline{\Psi}'_R$:

Rule R:SE-Ret Then we have

$$\begin{aligned}\sigma &\xrightarrow{\tau} \sigma'\\ \mathbb{R} &= \mathbb{R}' \cdot l\\ \sigma'' &= \sigma[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto a(\mathbf{sp}) + 8]\\ \overline{\Psi}_R &= \langle p, ctr, \sigma', \mathbb{R}', h', n\rangle \cdot \langle p, ctr+1, \sigma'', \mathbb{R}', h', \omega\rangle^{l}_{\texttt{ret}\ l\cdot\texttt{start}\ ctr}\end{aligned}$$

There are two cases depending if the return address on top of the $\mathbb{R}$ and on the stack match:
$m(a(\mathbf{sp})) = l$ Contradiction, because then no speculative transactions will be started that will be rolled back.
This cannot happen, because of $\vdash^{i}_{O} X'_R$: *biggestongoingtransactionirolledback*.
$m(a(\mathbf{sp})) \neq l$ We have $\sigma \xrightarrow{\tau} \sigma'$.
Since $\vdash_O X_R$: *noongoing* we know that $\tau\restriction_{ns} = \tau = \texttt{ret}\ l$.
Since a transaction with $id = ctr$ was started and we have $\vdash_O X_R$: *noongoing*, we know that $i = ctr$.
Notice that σ' is the configuration for the instance $ctr = i$ by definition.
This completes the case.

otherwise Contradiction, because $\vdash_O X_R$: *noongoing* and $\vdash^{i}_{O} X'_R$: *biggestongoingtransactionirolledback*, we know that a transaction has to be started that will be rolled back.

□

J.1.1 Completeness. We proceed with the Completeness direction

Lemma 60 (R SE: Completeness of the speculative semantics)**.** *If*

(1) $\sigma \in InitConf$ *and*
(2) $\sigma \Downarrow_{\overline{\tau}} \sigma'$ *and*
(3) $X_R = X^{init}_R(\sigma)$

Then

I $X_R \overset{O}{\downarrow}{}^R_{\overline{\tau}'} X'_{R\rho}$ *and*
II $\vdash_O X'_R$: *noongoing and*
III $\sigma' = X'_R.\sigma$ *and*
IV $\overline{\tau} = \overline{\tau}' \restriction_{ns}$ *and*
V $\rho = \varepsilon$

Proof. We proceed by induction on $\sigma \Downarrow_{\overline{\tau}} \sigma'$

Rule NS-Reflection Then we have $\sigma \Downarrow_{\varepsilon} \sigma'$ with $\sigma = \sigma'$.

I - IV By Rule R:SE-Reflection we have $X_R \overset{O}{\downarrow}{}^R_{\varepsilon} X_R$. By construction $\vdash_O X_R$: *noongoing* and $X_R.\sigma = \sigma$. Since $\varepsilon \restriction_{ns} = \varepsilon$ we are finished.

Rule NS-Single Then we have $\sigma \Downarrow_{\overline{\tau}} \sigma''$ and $\sigma'' \xrightarrow{\tau} \sigma'$.

We need to show
I $X_R \overset{O}{\downarrow}{}^R_{\overline{\tau}'\cdot\tau'} X'_R$ and
II $\vdash_O X'_R$: *noongoing* and
III $\sigma' = X'_R.\sigma$ and
IV $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \restriction_{ns}$

We apply the IH on $\sigma \xrightarrow{\overline{\tau}} \sigma''$ we get
I' $X_R \overset{O}{\downarrow}{}^R_{\overline{\tau}'} X''_{R\rho}$ and
II' $\vdash_O X''_{R\rho}$: *noongoing* and
III' $\sigma'' = X''_R.\sigma$ and
IV' $\overline{\tau} = \overline{\tau}' \restriction_{ns}$
V' $\rho = \varepsilon$

To account for possible outstanding commits, we use Lemma 22 (V4: Executing a chain of commits) on X''_R and get
a) $X''_R \overset{O}{\downarrow}{}^R_{\overline{\tau}'''} X'''_R$
b) $minWndw(X'''_R) > 0$
c) $\forall \tau \in \overline{\tau}'''.\, \tau =$ `commit` *id* for some $id \in \mathbb{N}$
d) $X''_R.\sigma = X'''_R.\sigma$

By c) and the definition of $\restriction_{ns}$ we have $\overline{\tau}''' \restriction_{ns} = \varepsilon$.
Because only Rule R:SE-Commit was used we have $X'''_{R\rho} = X''_{R\rho}$. We now do a case analysis on the instruction $p(\sigma(\mathbf{pc}))$:

$p(\sigma(\mathbf{pc})) \neq$ **ret** **I** Then either Rule R:SE-barr, Rule R:SE-barr-spec, Rule R:SE-Call-Full, Rule R:SE-Call or Rule R:SE-NoBranch in conjunction with Rule R:SE-Context was used to derive the step $X'''_R \overset{\tau'}{\rightsquigarrow}{}^O_R X^n_R$.

Here, τ' is generated from $X'''_R.\sigma \xrightarrow{\tau'} \sigma'$.
Since $\longrightarrow$ is deterministic, we know that $\tau' = \tau$.

II Since no speculative transaction is started and we have $\vdash_O X''_R$: *noongoing* by IH, we have $\vdash_O X^n_R$: *noongoing*.

III By definition and determinism of $\longrightarrow$.

IV Now we have $X''_R \overset{O}{\downarrow}{}^R_{\overline{\tau}'\cdot\overline{\tau}'''\cdot\tau'} X^n_R$. Looking at the trace that is generated we have

$$\begin{aligned}
&\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau' \restriction_{ns} \overline{\tau}''' \restriction_{ns} = \varepsilon \\
&= \overline{\tau}' \cdot \tau' \restriction_{ns} \tau' = \tau \\
&= \overline{\tau}' \cdot \tau \restriction_{ns} \tau \text{ generated by} \longrightarrow \\
&= \overline{\tau}' \restriction_{ns} \cdot \tau \text{ by IH} \\
&= \overline{\tau} \cdot \tau
\end{aligned}$$

and thus, are finished.

$p(\sigma(\mathbf{pc})) =$ **ret** Then either Rule R:SE-Ret or Rule R:SE-Ret-Empty is used in conjunction with Rule R:SE-Context:

Rule R:SE-Ret-Empty The case is analogous to the case above.

Rule R:SE-Ret There are two cases depending if $m(a(\mathbf{sp})) = l$.

$m(a(\mathbf{sp})) = l$ Commit step

I We derive $X''_R \overset{O}{\downarrow}{}^R_{\tau\cdot\texttt{start}\ id} X^n_R$ by using Rule R:SE-Ret in conjunction with Rule R:SE-Context and produce the observation $\tau' = \tau$, where $\tau =$ `ret` l.
Afterwards, we need to discharge the observation in $\overline{\rho}$ that was generated by Rule R:SE-Ret (which is always a `start` *id*).
The only rule that can be used when $\overline{\rho}$ is non-empty is Rule R:SE-General, which produces `start` *id*.
By Rule R:SE-Ret, we know that the step $X'''_R.\sigma \xrightarrow{\tau} \sigma'$ is made.

II No speculative transaction was started that needs to be rolled back. By $\vdash_O X''_R$: *noongoing* and $\vdash_O X'''_R$: *noongoing* we get $\vdash_O X^n_R$: *noongoing*.
III By definition and determinism of $\rightarrow$.
IV We now have:

$$\begin{aligned}
&\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau' \cdot \texttt{start}\ id\restriction_{ns} \text{ Def. and } \overline{\tau}'''\restriction_{ns} = \varepsilon \\
&= \overline{\tau}' \cdot \tau'\restriction_{ns} \tau' = \tau \\
&= \overline{\tau}' \cdot \tau\restriction_{ns} \tau \text{ generated by} \rightarrow \\
&= \overline{\tau}'\restriction_{ns} \cdot \tau \text{ by IH} \\
&= \overline{\tau} \cdot \tau
\end{aligned}$$

and are finished.

$m(a(\mathbf{sp})) \neq l$ A speculative transaction is started that will be rolled back
I We derive a step by using Rule R:SE-Ret in conjunction with Rule R:SE-Context This produces the observation τ'', where $\tau'' = \texttt{store}\ m$ and the step $X'''_R.\sigma \xrightarrow{\tau''} \sigma'''$ is made.

Since $\rightarrow$ is deterministic and the fact that $\sigma'' \xrightarrow{\tau''} \sigma'''$, $\sigma'' \xrightarrow{\tau} \sigma'$ and $X'''_R.\sigma = \sigma''$, we have $\sigma''' = \sigma'$ and $\tau'' = \tau$.
Since Rule R:SE-Ret pushes two observations into $\overline{\rho}$, Rule R:SE-General applies twice and produces $\texttt{ret}\ l$ and $\texttt{start}\ id$.
We thus have $X'''_R \overset{O}{\Downarrow}{}^{R}_{\tau'\cdot\texttt{start}\ id\cdot\texttt{ret}\ l} X_R 3$.

Since all transactions are eventually closed, we know there exists X^n_R such that $X^3_R \overset{O}{\Downarrow}{}^{R}_{\overline{\tau}^n\cdot\texttt{rlb}\ id} X^n_R$.

We now apply Lemma 61 (R SE: Non-speculative execution for rolled back transactions) on the execution $X'''_R \overset{O}{\Downarrow}{}^{R}_{\tau'\cdot\texttt{start}\ id\cdot\texttt{bypass}\ n\cdot\overline{\tau}^n\cdot\texttt{rlb}\ id} X^n_R$
and get $\sigma'' \xrightarrow{\tau''} \sigma'''$ and $X^n_R.\sigma = \sigma''$.
II Since the speculative transaction that was started was also rolled back and the fact that $\vdash_O X''_R$: *noongoing* by IH and $\vdash_O X'''_R$: *noongoing*, we have $\vdash_O X^n_R$: *noongoing*.
III Follows by definition and I).
IV By definition $\tau'' \cdot \texttt{start}\ id \cdots \texttt{rlb}\ id\restriction_{ns} = \tau''\restriction_{ns} = \tau''$.

$$\begin{aligned}
&\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau'' \cdot \texttt{start}\ id \cdot \overline{\tau}^n \cdot \texttt{rlb}\ id\restriction_{ns} \text{ Def. and } \overline{\tau}'''\restriction_{ns} = \varepsilon \\
&= \overline{\tau}' \cdot \tau'\restriction_{ns} \tau'' = \tau \\
&= \overline{\tau}' \cdot \tau\restriction_{ns} \tau \text{ generated by} \rightarrow \\
&= \overline{\tau}'\restriction_{ns} \cdot \tau \text{ by IH} \\
&= \overline{\tau} \cdot \tau
\end{aligned}$$

Notice that ρ is empty for all the cases, because we discharge all the observations immediately using Rule R:SE-General.

□

Lemma 61 (R SE: Non-speculative execution for rolled back transactions.)**.** *If*

(1) $X_R \overset{O}{\Downarrow}{}^{R}_{\overline{\tau}} X'_R$ *and*
(2) $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$ *and*
(3) $\sigma = X_R.\sigma$

Then

I there is a configurations σ' *with* $X'_R.\sigma = \sigma'$ *and*
II $\sigma \xrightarrow{\overline{\tau}\restriction_{ns}} \sigma'$ *and*
III $\overline{\tau}\restriction_{ns} = \tau$

Proof. Let $X_R \overset{O}{\Downarrow}{}^{R}_{\overline{\tau}} X'_R$ be an execution with trace $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$. Let $\sigma = X_R.\sigma$
We know Rule R:SE-Ret was used to start the speculative transaction.
By this rule we know, there is a configuration σ' with $\sigma \xrightarrow{\tau} \sigma'$.
By definition of $\restriction_{ns}$ we have $\overline{\tau}\restriction_{ns} = \tau\restriction_{ns} = \tau$, where the last steps is because of the fact $\tau \in Obs$.
Thus, we have $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}} \sigma'$ by Rule NS-Reflection and $\sigma \xrightarrow{\tau} \sigma'$.
Now we need to show that $\sigma' = X'_R.\sigma$, which is analogous to Lemma 32 (S SE: Non-speculative execution for rolled back transactions). □

J.2 R: Relating Non-speculative and AM Semantics

Theorem 20 (V5AM: Behaviour of non-speculative semantics and AM semantics). *Let p be a program. Then $Beh_{NS}(p) = Beh^{\mathcal{A}}_{R}(p)\restriction_{ns}$*

Proof. The lemma can be proven in a similar fashion to Theorem 15 (S AM: Behaviour of non-speculative semantics and AM semantics). We prove the two directions separately:

⇐ Assume that $\overline{\tau} \in Beh^{\mathcal{A}}_{R}(p)$.

By the definition of $Beh^{\mathcal{A}}_{S}(p)$ we have an initial configuration σ such that $(p,\sigma) \Mighty^{\omega}_{S} \overline{\tau}$.
The proof proceeds in similar fashion to the analogous case in Theorem 15 (S AM: Behaviour of non-speculative semantics and AM semantics) by using Lemma 62 (R AM : Soundness of the AM semantics w.r.t. non-speculative semantics).
We can now conclude that $(p,\sigma \Mighty^{O}_{NS} \overline{\tau}\restriction_{ns} \in Beh_{NS}(p)$ by Rule NS-Trace.

⇒ Assume that $(p,\sigma \Mighty^{O}_{NS} \overline{\tau} \in Beh_{NS}(p)$. We thus know there exists $\sigma' \in FinalConf$ such that $\sigma \Downarrow_{\overline{\tau}} \sigma'$.

We can now apply Lemma 68 (R AM: Completeness of the speculative AM semantics) and get $\Sigma^{init}_{R} p, \sigma \Downarrow^{\overline{\tau}'}_{R} \Sigma'_{R}$ with $\vdash_{O} \Sigma'_{R}$: *noongoing*, $\sigma' = \Sigma'_{R}.\sigma$ and $\overline{\tau} = \overline{\tau}'\restriction_{ns}$.
Because of $\vdash_{O} \Sigma'_{R}$: *noongoing* and $\sigma' = \Sigma'_{R}.\sigma$ we know that $\vdash \Sigma'_{R}$: *fin*.
We thus have $(p,\sigma) \Mighty^{\omega}_{R} \overline{\tau}' \in Beh^{\mathcal{A}}_{R}(p)$.

□

Lemma 62 (R AM : Soundness of the AM semantics w.r.t. non-speculative semantics)**.** *If*

(1) $\Sigma_{R}.\sigma = \sigma$ *and*
(2) $\vdash_{O} \Sigma_{R}$: *noongoing and*
(3) $\Sigma_{R} \Downarrow^{\overline{\tau}}_{R} \Sigma'_{R}$

Then there exists σ' such that

I if $\vdash_{O} \Sigma'_{R}$: *noongoing then* $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}\sigma'}$ *and* $\Sigma'_{R}.\sigma = \sigma'$ *and*
II if $\vdash^{i}_{O} \Sigma'_{R}$: *biggestongoingtransactionirolledback then by definition exists id i such that it is the smallest transaction id that will be rolled back and is still active then* $\sigma \Downarrow_{helper(\overline{\tau},i)} \sigma'$ *and* σ' *is the configuration for the instance with ctr = i.*

Proof. We proceed by induction on $\Sigma_{R} \Downarrow^{\overline{\tau}}_{R} \Sigma'_{R}$

Rule R:AM-Reflection Then we have $\Sigma_{R} \Downarrow^{\varepsilon}_{R} \Sigma_{R}$ with $\Sigma'_{R} = \Sigma_{R}$ and by Rule NS-Reflection we have
I $\sigma \Downarrow_{\varepsilon\restriction_{ns}} \sigma'$ with $\sigma = \sigma'$.
II $\sigma \Downarrow_{helper(\varepsilon,i)} \sigma'$ with $\sigma = \sigma'$.

Rule R:AM-Single We have $\Sigma_{R} \Downarrow^{\overline{\tau}'\cdot\tau}_{R} \Sigma'_{R}$ and by Rule R:AM-Single we get $\Sigma_{R} \Downarrow^{\overline{\tau}'}_{R} \Sigma''_{R}$ and $\Sigma''_{R} \overset{\tau}{\Mighty}_{R} \Sigma'_{R}$.
We need to prove
I if $\vdash_{O} \Sigma'_{R}$: *noongoing* then $\sigma \Downarrow_{\overline{\tau}\cdot\tau\restriction_{ns}\sigma'}$ and $\Sigma'_{R}.\sigma = \sigma'$
II if $\vdash^{i}_{O} \Sigma'_{R}$: *biggestongoingtransactionirolledback* then by definition exists *id i* such that it is the smallest transaction *id* that will be rolled back and is still active then $\sigma \Downarrow_{helper(\overline{\tau}\cdot\tau,i)} \sigma'$ and σ' is the configuration for the instance with *ctr* = *i*.
We apply the IH on $\Sigma_{R} \Downarrow^{\overline{\tau}'}_{R} \Sigma''_{R}$ and have a σ'' where σ'' is the configuration for some instance in Σ''_{R} such that.
I' if $\vdash_{O} \Sigma''_{R}$: *noongoing* then $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}\sigma''}$ and $\Sigma''_{R}.\sigma = \sigma''$
II' if $\vdash^{j}_{O} \Sigma''_{R}$: *biggestongoingtransactionirolledback* then by definition exists *id* j such that it is the smallest transaction *id* that will be rolled back and is still active then $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$ and σ'' is the configuration with the instance with *ctr* = *j*.
We proceed by case analysis on Σ''_{R}.
no ongoing transactions in Σ''_{R} Then Σ''_{R} has no ongoing transactions, meaning $\vdash_{O} \Sigma''_{R}$: *noongoing* and we have $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}} \sigma''$ and $\Sigma''_{R}.\sigma = \sigma''$ by IH.

I Then $\vdash_{O} \Sigma'_{R}$: *noongoing* and we need to proof $\sigma \Downarrow_{\overline{\tau}\cdot\tau\restriction_{ns}\sigma'}$ and $\Sigma'_{R}.\sigma = \sigma'$. We now proceed by inversion on $\Sigma''_{R} \overset{\tau}{\Mighty}_{R} \Sigma'_{R}$:
Rule R:AM-Rollback Then τ = `rlb` *id*.
Analogous to the corresponding case in Lemma 55 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).
Rule R:AM-Ret-Spec Then we know that $\overline{\rho}$ = `ret` $l \cdot$ `start` *id* for Σ'_{R}.
Analogous to the corresponding case in Lemma 55 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).
otherwise We know that $\sigma'' = \Sigma''_{R}.\sigma$.
Analogous to the corresponding case in Lemma 55 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) together with Lemma 63 (R AM: Soundness single step No Speculation) with $\Sigma''_{R} \overset{\tau}{\Mighty}_{R} \Sigma'_{R}$.

II Then Σ'_R has ongoing transactions, meaning $\vdash^{i}_{O} \Sigma'_R$: *biggestongoingtransactionirolledback* and we need to proof $\sigma \Downarrow_{helper(\overline{\tau}\cdot\tau,i)} \sigma'$ and σ' is the configuration for the instance with $ctr = i$.

We now proceed by inversion on $\Sigma''_R \overset{\tau}{\rightarrow\!\!\!\!\!\!\diamond}_R \Sigma'_R$:

Rule R**:AM-Ret-Spec** Then we know that $\overline{\rho} = \texttt{ret}\ l \cdot \texttt{start}\ id$ for Σ'_R.

Analogous to the corresponding case in Lemma 55 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) together with Lemma 66 (R AM: Return step Speculation).

otherwise By definition of $\vdash^{i}_{O} \Sigma'_R$: *biggestongoingtransactionirolledback* we know that there exists a $\texttt{rlb}\ i$ in the execution $\Sigma'_R \Downarrow^{\overline{\tau}_{fin}}_{R} \Sigma_{Rfin}$ with no matching $\texttt{start}\ i$ observation in that execution.

Analogous to the corresponding case in Lemma 55 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

ongoing transactions in Σ''_R Then Σ''_R has ongoing transactions, meaning $\vdash^{j}_{O} \Sigma''_R$: *biggestongoingtransactionirolledback* and we have $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$ and σ'' is the configuration for the instance with $ctr = j$.

I Then $\vdash_O \Sigma'_R$: *noongoing* and we need to proof $\sigma \Downarrow_{\overline{\tau}\cdot\tau\restriction_{ns}\sigma'}$ and $\Sigma'_R.\sigma = \sigma'$. We now proceed by inversion on $\Sigma''_R \overset{\tau}{\rightsquigarrow}^{O}_{S} \Sigma'_R$:

Rule R**:AM-Rollback and** $\tau = \texttt{rlb}\ j$ Analogous to the corresponding case in Lemma 55 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Then $\tau \neq \texttt{rlb}\ j$.

Analogous to the corresponding case in Lemma 55 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

II Then $\vdash^{i}_{O} \Sigma'_R$: *biggestongoingtransactionirolledback* and we need to proof $\sigma \Downarrow_{helper(\overline{\tau}\cdot\tau,i)} \sigma'$ and σ' is the configuration for the instance below the instance with $ctr = i$.

We now proceed by inversion on $\Sigma''_R \overset{\tau}{\rightarrow\!\!\!\!\!\!\diamond}_R \Sigma'_R$:

Rule R**:AM-Rollback** Then $\tau = \texttt{rlb}\ id$. We do a case analysis if $id = j$ or not.

$id = j$ Analogous to the corresponding case in Lemma 55 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

$id \neq j$ Analogous to the corresponding case in Lemma 55 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Then $\tau \neq \texttt{rlb}\ id$.

Analogous to the corresponding case in Lemma 55 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics)

□

Lemma 63 (R AM: Soundness single step No Speculation)**.** *If*

(1) $\vdash_O \Sigma_R$: *noongoing and*
(2) $\Sigma_R \overset{\tau}{\rightarrow\!\!\!\!\!\!\diamond}_R \Sigma'_R$ *and*
(3) $\vdash_O \Sigma'_R$: *noongoing and*
(4) $\sigma = \Sigma_R.\sigma$

Then there exists σ' *such that*

I $\sigma \Downarrow_{\tau\restriction_{ns}} \sigma'$ *and*
II $\Sigma'_R.\sigma = \sigma'$

Proof. We proceed by inversion on $\Sigma_R \overset{\tau}{\rightarrow\!\!\!\!\!\!\diamond}_R \Sigma'_R$:

Rule R**:AM-General** Thus we have $\Sigma_R = \overline{\Phi}_R \cdot \Phi_R \overline{\rho\cdot\tau}$ and $\Sigma'_R = \overline{\Phi}_R \cdot \Phi_R \overline{\rho}$ with $\Phi_R.\sigma = \sigma$. This means we can apply Lemma 67 (R AM: General Step) and get $\sigma \Downarrow_{\varepsilon\restriction_{ns}} \sigma$.

Rule R**:AM-Rollback** Contradiction, since $\vdash_O \Sigma_R$: *noongoing* and Definition 44 (Well orderedness of rollback and start).

Rule R**:AM-Context** We have $\Sigma_R = \overline{\Phi}_R \cdot \Phi_R$ and $\Sigma'_R = \overline{\Phi}'_R \cdot \overline{\Phi}'_R$ with $\Phi_R \overset{\tau}{\rightarrow\!\!\!\!\!\!\diamond}_R \overline{\Phi}'_R$. By Lemma 64 (R AM: Single Step Instance Non Speculative) we have $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ with $\sigma = \Phi_R.\sigma$ and $\overline{\Phi}'_R.\sigma = \sigma'$.

□

Lemma 64 (R AM: Single Step Instance Non Speculative)**.** *If*

(1) $\Sigma_R = \overline{\Psi}_R \cdot \Psi_R$ *and*
(2) $\Sigma'_R = \overline{\Psi}_R \cdot \overline{\Phi}'_R$ *and* $\vdash_O \Sigma'_R$: *noongoing and*
(3) $\Phi_R \overset{\tau}{\rightarrow\!\!\!\!\!\!\diamond}_R \overline{\Phi}'_R$ *and*

(4) $\sigma = \Psi_S.\sigma$

Then there is a σ' *such that*

I $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ *and*

II $\overline{\Phi}'_R.\sigma = \sigma$

Proof. We proceed by case analysis on the rule used to derive $\Phi_R \overset{\tau}{\eqslantless}_R \Phi'_R$.

Rule R:AM-Ret-Spec Then we have $\sigma \xrightarrow{\tau} \sigma'$, $\mathbb{R} = \mathbb{R}' \cdot l$ and $\sigma'' = \sigma[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto a(\mathbf{sp}) + 8]$, $m(a(\mathbf{sp})) \neq l$ and $\overline{\Phi}_R = \langle p, ctr, \sigma', \mathbb{R}', h', n\rangle \cdot \langle p, ctr+1, \sigma'', \mathbb{R}', h', \omega\rangle^{l}_{\texttt{st}\ (ctr)}$.
Contradiction, because this starts a speculative transaction that needs to be rolled back.
This cannot happen because of $\vdash_O \Sigma'_R$: *noongoing*.

Rule R:AM-Ret-Empty We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule and $\overline{\Phi}'_R = \langle p, ctr, \sigma', \mathbb{R}, h, n-1\rangle$.
Thus, $\sigma' = \overline{\Phi}'_R.\sigma$.
Because the rule used the observation received from the the step $\sigma \xrightarrow{\tau} \sigma'$, we have $\tau\restriction_{ns} = \tau$ and are finished.

Rule R:AM-Ret-Same We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule and $\overline{\Phi}'_R = \langle p, ctr, \sigma', \mathbb{R}, h, n-1\rangle$.
The rest is analogous to the case for Rule R:AM-Ret-Empty.

otherwise Thus, we have $p(\sigma(\mathbf{pc})) \neq \mathbf{ret}$ and $n \neq 0$ and can apply Lemma 65 (R AM: no Ret speculation). We get an execution $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ and $\sigma' = \Sigma'_R.\sigma$.

□

Lemma 65 (R AM: no Ret speculation)**.** *If*

(1) $\Phi_R = \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle$ *and*

(2) $\Phi_R \overset{\tau}{\eqslantless}_R \overline{\Phi}'_R$, *and*

(3) $p(\sigma(\mathbf{pc})) \neq \mathbf{ret}$ *and*

(4) $n \neq 0$

Then there is a σ' *such that*

I $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ *and*

II $\sigma' = \overline{\Phi}'.\sigma$.

Proof. Let p be a program, O be a prediction oracle.
We have

(1) $\Phi_R = \langle p, ctr, \sigma, \mathbb{R}, n\rangle$ and

(2) $\Phi_R \overset{\tau}{\eqslantless}_R \overline{\Phi}'_R$ and

(3) $p(\sigma(\mathbf{pc})) \neq \mathbf{ret}$ and

(4) $n \neq 0$

By inversion on $\Psi_R \overset{\tau}{\eqslantless}_R \Sigma'_R$ and the fact that $p(\sigma(\mathbf{pc})) \neq \mathbf{ret}$ and $n \neq 0$ we have four cases.

Rule R:AM-barr or Rule R:AM-barr-spec We show the proof for Rule R:AM-barr, the proof for Rule R:AM-barr-spec is analogous.
By Rule R:AM-barr we know $\sigma \xrightarrow{\tau} \sigma'$ and $\overline{\Phi}'_R = \langle p, ctr, \sigma', \mathbb{R}, n-1\rangle$.
Thus $\sigma' = \overline{\Psi}'_R.\sigma$ and $\tau = \varepsilon = \varepsilon\restriction_{ns}$.

Rule R:AM-NoBranch We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule and $\overline{\Psi}'_R = \langle p, ctr, \sigma', \mathbb{R}, h, n-1\rangle$.
Thus, $\sigma' = \overline{\Phi}'_R.\sigma$.
Because the rule used the observation received from the the step $\sigma \xrightarrow{\tau} \sigma'$, we have $\tau\restriction_{ns} = \tau$ and are finished.

Rule R:AM-Call We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule and $\overline{\Phi}'_R = \langle p, ctr, \sigma', \mathbb{R}, n-1\rangle$.
The case is analogous to case Rule R:AM-NoBranch.

Rule R:AM-Call-Full We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule and $\overline{\Phi}'_R = \langle p, ctr, \sigma', \mathbb{R}, n-1\rangle$.
The case is analogous to case Rule R:AM-NoBranch.

□

Lemma 66 (R AM: Return step Speculation)**.** *If*

(1) $\Sigma_R = \overline{\Phi}_R \cdot \Phi_R$ *and* $\vdash_O \Sigma_R$: *noongoing*

(2) $\Sigma'_R = \overline{\Phi}_R \cdot \overline{\Phi}'_R$ *and* $\vdash^{i}_{O} \Sigma'_R$: *biggestongoingtransactionirolledback and*

(3) $\Phi_R \overset{\tau}{\eqslantless}_R \overline{\Phi}'_R$ *and*

(4) $\sigma = \Phi_R.\sigma$

Then

I $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ *and*
II σ' *is the configuration for the instance with ctr* $= i$ *in* Σ'_R

Proof. We proceed by inversion on $\Phi_R \overset{\tau}{\doteq\!\!\not\frown}_R \overline{\Phi}'_R$:

Rule R**:AM-Ret-Spec** Then we have

$$\begin{aligned}
\sigma &\xrightarrow{\tau} \sigma' \\
\mathbb{R} &= \mathbb{R}' \cdot l \\
m(a(\mathbf{sp})) &\neq l \\
\sigma'' &= \sigma[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto a(\mathbf{sp}) + 8] \\
\overline{\Phi}_R &= \langle p, ctr, \sigma', \mathbb{R}', h', n\rangle \cdot \langle p, ctr+1, \sigma'', \mathbb{R}', h', \omega\rangle^{l}_{\texttt{ret}\ l \cdot \texttt{st}\ (ctr)}
\end{aligned}$$

We have $\sigma \xrightarrow{\tau} \sigma'$.
Since $\vdash_O \Sigma_R$: *noongoing* we know that $\tau\restriction_{ns} = \tau = \texttt{ret}\ l$.
Since a transaction with $id = ctr$ was started and we have $\vdash_O \Sigma_R$: *noongoing*, we know that $i = ctr$.
Notice that σ' is the configuration for the instance $ctr = i$ by definition.
This completes the case.

otherwise Contradiction, because $\vdash_O \Sigma_R$: *noongoing* and $\vdash^i_O \Sigma'_R$: *biggestongoingtransactionirolledback*, we know that a transaction has to be started that will be rolled back.

□

Lemma 67 (R AM: General Step)**.** *If*

(1) $\Sigma_R = \overline{\Phi}_R \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle_{\overline{\rho}\cdot\tau}$ *and*
(2) $\overline{\Phi}_R \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle_{\overline{\rho}\cdot\tau} \overset{\tau}{\doteq\!\!\not\frown}_R \overline{\Phi}_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle_{\overline{\rho}}$

Then

I $\sigma \Downarrow_{\varepsilon\restriction_{ns}} \sigma$.

Proof. Let p be a program, O be a prediction oracle. We have

(1) $\Sigma_R = \overline{\Phi}_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle_{\overline{\rho}\cdot\tau}$ and
(2) $\overline{\Phi}_R \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle_{\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow} \overline{\Psi} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle_{\overline{\rho}}$.

By the definition of $\Phi_R \overset{\tau}{\doteq\!\!\not\frown}_R \Sigma_R$ only Rule R:AM-Ret-Spec adds observations to $\overline{\rho}$.
These observations are only `start` n and `ret` l.
By the definition of $\restriction_{ns}$ we have $\tau\restriction_{ns} = \varepsilon$ and we have $\sigma \Downarrow_{\varepsilon\restriction_{ns}} \sigma$ by Rule NS-Reflection. □

J.2.1 Completeness.

Lemma 68 (R AM: Completeness of the speculative AM semantics)**.** *If*

(1) $\sigma \in InitConf$ *and*
(2) $\sigma \Downarrow_{\overline{\tau}} \sigma'$ *and*
(3) $\Sigma_R = \Sigma^{init}_R \sigma$

Then

I $\Sigma_R \Downarrow^{\overline{\tau}'}_R \Sigma'_{R_\rho}$ *and*
II $\vdash_O \Sigma'_R$: *noongoing and*
III $\sigma' = \Sigma'_R.\sigma$ *and*
IV $\overline{\tau} = \overline{\tau}'\restriction_{ns}$ *and*
V $\rho = \varepsilon$

Proof. We proceed by induction on $\sigma \Downarrow_{\overline{\tau}} \sigma'$

Rule NS-Reflection Then we have $\sigma \Downarrow_\varepsilon \sigma'$ with $\sigma = \sigma'$.

I - V By Rule R:AM-Reflection we have $\Sigma_R \Downarrow^{\varepsilon}_R \Sigma_R$. By construction $\vdash_O \Sigma_R$: *noongoing* and $\Sigma_R.\sigma = \sigma$. Since $\varepsilon\restriction_{ns} = \varepsilon$ we are finished.

Rule NS-Single Then we have $\sigma \xrightarrow{\overline{\tau}} \sigma''$ and $\sigma'' \xrightarrow{\tau} \sigma'$.

We need to show

I $\Sigma_R \Downarrow_R^{\overline{\tau}\cdot\tau'} \Sigma'_R$ and

II $\vdash_O \Sigma'_R$: *noongoing* and

III $\sigma' = \Sigma'_R.\sigma$ and

IV $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \restriction_{ns}$

We apply the IH on $\sigma \xrightarrow{\overline{\tau}} \sigma''$ we get

I' $\Sigma_R \Downarrow_R^{\overline{\tau}'} \Sigma''_{R\,\rho}$ and

II' $\vdash_O \Sigma''_{R\,\rho}$: *noongoing* and

III' $\sigma'' = \Sigma''_R.\sigma$ and

IV' $\overline{\tau} = \overline{\tau}' \restriction_{ns}$

V' $\rho = \varepsilon$

We now do a case analysis on the instruction $p(\sigma(\mathbf{pc}))$:

$p(\sigma(\mathbf{pc})) \neq \mathbf{ret}$ Analogous to the corresponding case in Lemma 60 (R SE: Completeness of the speculative semantics).

$p(\sigma(\mathbf{pc})) = \mathbf{ret}$ Analogous to the corresponding case Lemma 60 (R SE: Completeness of the speculative semantics), which is when the oracle mispredicted in the proof, together with Lemma 69 (R AM: Non-speculative execution for rolled back transactions)

Notice that ρ is empty for all the cases, because we discharge all the observations immediately using Rule R:AM-General.

□

Lemma 69 (R AM: Non-speculative execution for rolled back transactions.)**.** *If*

(1) $\Sigma_R \Downarrow_R^{\overline{\tau}} \Sigma'_R$ *and*

(2) $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$ *and*

(3) $\sigma = \Sigma.\sigma$

Then there exists a configuration σ' *such that*

I $\Sigma'_R.\sigma = \sigma'$ *and*

II $\sigma \xrightarrow{\overline{\tau}\restriction_{ns}} \sigma'$ *and*

III $\overline{\tau}\restriction_{ns} = \tau$

Proof. Let $\Sigma_R \Downarrow_R^{\overline{\tau}} \Sigma'_R$ be an execution with trace $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$. Let $\sigma = \Sigma_R.\sigma$

The proof proceeds analogously to Lemma 61 (R SE: Non-speculative execution for rolled back transactions). □

J.3 R: Relating Symbolic and AM semantics

These proofs are conceptually very similar to the proofs of S.

Theorem 21 ($\curvearrowright_R$: Behaviour of AM and symbolic semantics). $Beh^{\mathcal{A}}_R(p) = \mu(Beh^{\mathcal{S}}_R(p))$

Proof. The proposition can be proven in similar fashion to Theorem 14 (S SE: Behaviour of non-speculative and oracle semantics). We prove the two directions separately:

⇐ Assume that $(p,\sigma)\ {}_\alpha\curvearrowright^\omega_R\ \overline{\tau} \in Beh^{\mathcal{S}}_R(p)$.

We thus know there exists $\vdash \Sigma^{\mathcal{S}'}_R : fin$ such that $\Sigma^{init}_R(p,\sigma_{\mathcal{S}})\ {}_\alpha\Downarrow^{\overline{\tau}}_R\ \Sigma^{\mathcal{S}'}_R$ and $\mu \vDash pthCnd(\overline{\tau_\alpha})$. We now apply Lemma 70 (R: Soundness of the AM semantics w.r.t. symbolic semantics) on $\Sigma^{init}_R(p,\sigma_{\mathcal{S}})\ {}_\alpha\Downarrow^{\overline{\tau}}_R\ \Sigma^{\mathcal{S}'}_R$ and get $\Sigma_R \Downarrow^{\overline{\tau}}_R \Sigma'_R$, $\mu(\Sigma^{\mathcal{S}'}_R) = \Sigma'_R$ and $\mu(\overline{\tau_\alpha}) = \overline{\tau}$

Since $\vdash \Sigma^{\mathcal{S}'}_R : fin$ and $\mu(\Sigma^{\mathcal{S}'}_R) = \Sigma'_R$ we have $\vdash \Sigma'_R : fin$ as well.

Thus, $(p, \mu(\sigma_{\mathcal{S}}))\ \curvearrowright^\omega_R\ \mu(\overline{\tau_\alpha}) \in Beh^{\mathcal{A}}_R(p)$.

⇒ Assume that $(p,\sigma)\ \curvearrowright^\omega_R\ \overline{\tau} \in Beh^{\mathcal{A}}_R(p)$. We thus know there exists $\vdash \Sigma'_R : fin$ such that $\Sigma^{init}_R(p,\sigma) \Downarrow^{\overline{\tau}}_R \Sigma'_R$.

We now apply Lemma 72 (R: Completeness of the symbolic semantics) on $\Sigma^{init}_R(p,\sigma) \Downarrow^{\overline{\tau}}_R \Sigma'_R$ and get

$$\begin{aligned} \Sigma^{init}_R(p,\sigma) &= \mu(\Sigma^{\alpha}_R) \\ \Sigma^{\alpha}_R\ {}_\alpha\Downarrow^{\overline{\tau_\alpha}}_R\ \Sigma^{\mathcal{S}'}_R & \\ \Sigma'_R &= \mu(\Sigma^{\mathcal{S}'}_R) \\ \overline{\tau} &= \mu(\overline{\tau_\alpha}) \\ \mu \vDash pthCnd(\overline{\tau}') & \end{aligned}$$

Since $\vdash \Sigma'_R : fin$ and $\mu(\Sigma^{\mathcal{S}'}_R) = \Sigma'_R$ we have $\vdash \Sigma^{\mathcal{S}'}_R : fin$ as well.

Thus, $(p,\sigma_{\mathcal{S}})\ {}_\alpha\curvearrowright^\omega_R\ \overline{\tau_\alpha} \in Beh^{\mathcal{S}}_R(p)$ and we are done, since $(p,\mu(\sigma_{\mathcal{S}}))\ {}_\alpha\curvearrowright^\omega_R\ \mu(\overline{\tau_\alpha}) = (p,\sigma)\ \curvearrowright^\omega_R\ \overline{\tau}$.

□

Now onto theorems for the new speculative semantics. We want to show Soundness and Completeness.

J.3.1 *Soundness.*

Lemma 70 (R: Soundness of the AM semantics w.r.t. symbolic semantics)**.** *If*

(1) $\Sigma^{\alpha}_R\ {}_\alpha\Downarrow^{\overline{\tau}}_R\ \Sigma^{\alpha\prime}_R$ *and*

(2) $\mu \vDash pthCnd(\Sigma^{\alpha\prime}_R)$

Then

I $\mu(\Sigma^{\alpha}_R) \Downarrow^{\mu(\overline{\tau})}_R \mu(\Sigma^{\alpha\prime}_R)$ *and*

Proof. We proceed by induction on $\Sigma^{\alpha}_R\ {}_\alpha\Downarrow^{\overline{\tau_\alpha}}_R\ \Sigma^{\alpha\prime}_R$

Rule R:Sym-Reflection Then we have $\Sigma^{\alpha}_R\ {}_\alpha\Downarrow^{\varepsilon}_R\ \Sigma^{\alpha\prime}_R$ with $\Sigma^{\alpha\prime}_R = \Sigma^{\alpha}_R$. Using Rule R:AM-Reflection we get $\mu(\Sigma^{\alpha}_R)\ {}_\alpha\Downarrow^{\mu(\varepsilon)}_R\ \mu(\Sigma^{\alpha\prime}_R)$ and are finished.

Rule R:Sym-Single We have $\Sigma^{\alpha}_R\ {}_\alpha\Downarrow^{\overline{\tau_\alpha}'\cdot\tau_{\mathcal{S}}}_R\ \Sigma^{\alpha\prime}_R$ and by Rule R:Sym-Single we get $\Sigma^{\alpha}_R\ {}_\alpha\Downarrow^{\overline{\tau_\alpha}'}_R\ \Sigma^{\alpha\prime\prime}_R$ and $\Sigma^{\alpha\prime\prime}_R \overset{\tau}{=}\!\curvearrowright^{\alpha}_R\ \Sigma^{\alpha\prime}_R$.

We need to prove

(1) $\mu(\Sigma^{\alpha}_R) \Downarrow^{\mu(\overline{\tau}\cdot\tau_{\mathcal{S}})}_R \mu(\Sigma^{\alpha\prime}_R)$

We apply the IH on $\Sigma^{\alpha}_R\ {}_\alpha\Downarrow^{\overline{\tau_\alpha}}_R\ \Sigma^{\alpha\prime\prime}_R$ and have a $\Sigma''_R = \mu(\Sigma^{\alpha\prime\prime}_R)$ such that:

(1) $\mu(\Sigma^{\alpha}_R) \Downarrow^{\mu(\overline{\tau_\alpha})}_R \Sigma''_R$ and

(2) $\mu \vDash pthCnd(\Sigma^{\alpha\prime\prime}_R)$

The result follows by applying Lemma 71 (R: Soundness single step) on $\Sigma^{\alpha\prime\prime}_R \overset{\tau_{\mathcal{S}}}{=}\!\curvearrowright^{\alpha}_R\ \Sigma^{\alpha\prime}_R$ and get a step $\Sigma''_R \overset{\mu(\tau_{\mathcal{S}})}{=\!=}\!\curvearrowright_R\ \mu(\Sigma^{\alpha}_R)$. We now use Rule R:AM-Single and get an execution $\mu(\Sigma^{\alpha}_R) \Downarrow^{\mu(\overline{\tau_\alpha})\cdot\mu(\tau_{\mathcal{S}})}_R \mu(\Sigma^{\alpha\prime}_R)$ as required.

□

Lemma 71 (R: Soundness single step)**.** *If*

(1) $\Sigma^{\alpha}_R \overset{\tau_{\mathcal{S}}}{=}\!\curvearrowright^{\alpha}_R\ \Sigma^{\alpha}_R$ *and*

(2) $\mu \vDash pthCnd(\Sigma_R^{\alpha\prime})$

Then

I $\mu(\Sigma_R^{\alpha}) \xrightarrow{\mu(\tau_S)}_R \mu(\Sigma_R^{\alpha\prime})$

Proof. We proceed by inversion on $\Sigma_R^{\alpha} \xrightarrow{\tau}_R^{\alpha} \Sigma_R^{\alpha\prime}$:

Rule R:Sym-Rollback Since $\mu()$ does not change the speculation window and ctr and $\mu(\Sigma_R^{\alpha}) = \Sigma_R$, we have $\Sigma_R.n = \Sigma_R^{\alpha}.n = 0$ and $\Sigma_R.ctr = \Sigma_R^{\alpha}.ctr$.
Analogous to Lemma 40 using Rule R:AM-Rollback.

Rule R:Sym-Context We then have $\Phi_R^{\alpha} \xrightarrow{\tau}_R^{\alpha} \overline{\Phi^{\mathcal{S}\prime}}_R$. Thus, we know $\Phi_R^{\alpha} > 0$ and $\mu(\Phi_R^{\alpha}) > 0$ as well. We proceed by inversion on $\Phi_R^{\alpha} \xrightarrow{\tau_S}_R^{\alpha} \overline{\Phi^{\mathcal{S}\prime}}_R$:

Rule R:Sym-General Then $\Phi_R^{\alpha} \xrightarrow{\tau_S}_R^{\alpha} \Phi_{R\overline{\rho_S}\setminus\tau_S}^{\alpha}$. Analogous to Lemma 40 using Rule R:AM-General.

Rule R:Sym-NoBranch, Rule R:Sym:AM-barr, Rule R:Sym-barr-spec, Rule R:Sym-Call-Full, Rule R:Sym-Ret-Empty, Rule R:Sym-Ret-S

Then we have $\Phi_R^{\alpha} \xrightarrow{\tau_S}_R^{\alpha} \Phi_R^{\alpha\prime}$ where $\Phi_R^{\alpha\prime} = \langle p, \Phi_R^{\alpha}.ctr, \Phi_R^{\alpha}.\sigma'_{\mathcal{S}}, \mathbb{R}, \Phi_R^{\alpha}.n - 1\rangle$ with $\Phi_R^{\alpha}.\sigma_{\mathcal{S}} \xrightarrow{\tau_S}^{\mathcal{S}} \sigma'_{\mathcal{S}}$.

Since we have $\mu \vDash pthCnd(\overline{\Phi^{\mathcal{S}}}_R.\sigma_{\mathcal{S}})$ (by assumption) we can use Lemma 17 (Non-spec: Soundness to symbolic) on $\Phi_R^{\alpha}.\sigma_{\mathcal{S}} \xrightarrow{\tau_S}^{\mathcal{S}} \sigma'_{\mathcal{S}}$ and get $\mu(\Phi_R^{\alpha}\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_S)} \mu(\sigma'_{\mathcal{S}})$, where $\mu(\Phi_R^{\alpha}.\sigma_{\mathcal{S}}) = \Phi_R.\sigma$ as per assumption.

We can now use Rule R:AM-NoBranch to derive the step $\mu(\Phi_R^{\alpha}) \xrightarrow{\mu(\tau_S)}_R \mu(\Phi_R^{\alpha\prime})$ using the derived $\xrightarrow{\mu(\tau_S)}$ step.

Rule R:AM-Call Then we have $\Phi_R^{\alpha} \xrightarrow{\tau_S}_R^{\alpha} \Phi_R^{\alpha\prime}$ where $\Phi_R^{\alpha\prime} = \langle p, \Phi_R^{\alpha}.ctr, \Phi_R^{\alpha}.\sigma', \mathbb{R}', \Phi_R^{\alpha}.n - 1\rangle$ with $\Phi_R^{\alpha}.\sigma_{\mathcal{S}} \xrightarrow{\tau_S}^{\mathcal{S}} \sigma'_{\mathcal{S}}$ and $\mathbb{R}' = \Phi_R^{\alpha}.\mathbb{R}.\Phi_R^{\alpha}.\sigma_{\mathcal{S}}(\mathbf{pc}) + 1$. Since the symbolic $\mathbb{R}$ only contains entries created with the **pc** register, all entries in the symbolic $\mathbb{R}$ are always concrete. The rest of the case is analogous to case Rule S:AM-barr in Lemma 40 (S: Soundness single step).

Rule R:Sym-Ret-Spec We have $\Phi_R^{\alpha}.\mathbb{R} = \mathbb{R}' \cdot l$ and $\Phi_R^{\alpha} \xrightarrow{\tau_S}_R^{\alpha} \overline{\Phi^{\mathcal{S}}}_{R\overline{\rho_S}\cdot \texttt{ret}\ l \cdot \texttt{start}_R\ \Phi_R^{\alpha}.ctr}$ where $\overline{\Phi^{\mathcal{S}}}_R = \langle p, \Phi_R^{\alpha}.ctr, \sigma'_{\mathcal{S}}, \Phi_R^{\alpha}.\mathbb{R}, \Phi_R^{\alpha}.n{-}1\rangle \cdot \langle p, \Phi_R^{\alpha}.ctr + 1, \sigma''_{\mathcal{S}}, \mathbb{R}', \min \Phi_S^{\mathcal{S}}.n, \omega\rangle$.

Furthermore, we have $\Phi_R^{\alpha}.\sigma \xrightarrow{\tau_S} \sigma'_{\mathcal{S}}$ and $\sigma''_{\mathcal{S}} = \sigma_{\mathcal{S}}[\mathbf{pc} \mapsto l, ^{\iota} \rightarrow sa(\mathbf{sp}) + 8]$.

We use Lemma 17 (Non-spec: Soundness to symbolic) on $\Phi_R^{\alpha}.\sigma_{\mathcal{S}} \xrightarrow{\tau_S}^{\mathcal{S}} \sigma'_{\mathcal{S}}$ and get $\mu(\Phi_R^{\alpha}.\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_S)}^{\mathcal{S}} \mu(\sigma'_{\mathcal{S}})$.
Choose $\Phi_R = \mu(\Phi_R^{\alpha})$ and note that a **ret** instruction is executed. We now derive a step using Rule R:AM-Ret-Spec together with the non-speculative step $\mu(\Phi_R^{\alpha}.\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_S)}^{\mathcal{S}} \mu(\sigma'_{\mathcal{S}})$ above and $\sigma'' = \sigma[\mathbf{pc} \mapsto l, ^{\iota} \rightarrow a(\mathbf{sp}) + 8]$: $\Phi_R \xrightarrow{\mu(\tau_S)}_R \overline{\Phi}_R$ with $\overline{\Phi}_R = \langle p, \Phi_R.ctr, \mu(\sigma'_{\mathcal{S}}), \Phi_R.n - 1\rangle \cdot \langle p, \Phi_R.ctr + 1, \sigma'', \min \Phi_R.n, \omega\rangle$.

By definition we have $\mu(\sigma''_{\mathcal{S}}) = \sigma''$, because **pc** and **sp** are always concrete. We now show that $\mu(\overline{\Phi^{\mathcal{S}}}_R) = \overline{\Phi}_R$.

By $\mu(\Phi_R^{\alpha}) = \Phi_R$ we have $\Phi_R^{\alpha}.ctr = \Phi_R.ctr$ and $\Phi_R^{\alpha}.n = \Phi_R.n$ and by construction $\mu(\overline{\Phi^{\mathcal{S}}}_R) = \overline{\Phi}_R$ and thus $\mu(\Phi_R^{\alpha}) \xrightarrow{\mu(\tau_S)}_R \mu(\overline{\Phi^{\mathcal{S}}}_R)$ as needed.

□

J.3.2 Completeness.

Lemma 72 (R: Completeness of the symbolic semantics)**.** *If*

(1) $\Sigma_R \Downarrow_R^{\overline{\tau}} \Sigma'_R$ *and*
(2) $\Sigma_R = \mu(\Sigma_R^{\alpha})$

Then there is a valuation $\mu()$*, a symbolic trace* $\overline{\tau}'$ *and a final state* $\Sigma_R^{\alpha\prime}$ *such that*

I $\Sigma_R^{\alpha}\ {}_{\alpha}\Downarrow_R^{\overline{\tau}'} \Sigma_R^{\alpha\prime}$ *and*
II $\Sigma'_R = \mu(\Sigma_R^{\alpha\prime})$ *and* $\overline{\tau} = \mu(\overline{\tau}')$ *and*
III $\mu \vDash pthCnd(\Sigma_R^{\alpha\prime})$

Proof. We proceed by induction on $\Sigma_R \Downarrow_R^{\overline{\tau}} \Sigma'_R$

Rule R:AM-Reflection Then we have $\Sigma_R \Downarrow_R^{\varepsilon} \Sigma'_R$ with $\Sigma_R = \Sigma'_R$.
I - III By Rule R:Sym-Reflection we have $\Sigma_R^{\alpha}\ {}_{\alpha}\Downarrow_R^{\varepsilon} \Sigma_R^{\alpha\prime}$. By construction $\Sigma_R^{\alpha\prime} = \Sigma_R^{\alpha\prime}$. We now trivially satisfy all conditions.

Rule R:AM-Single We have $\Sigma_R \Downarrow_R^{\overline{\tau}'\cdot\tau} \Sigma'_R$ and by Rule R:AM-Single we get $\Sigma_R \Downarrow_R^{\overline{\tau_\alpha}'} \Sigma_R''$ and $\Sigma_R'' \xrightarrow{\tau}_R^{\alpha} \Sigma'_R$.
We need to prove

(1) $\Sigma_R^\alpha \; \alpha \Downarrow_R^{\overline{\tau_\alpha}' \cdot \tau_S} \; \Sigma_R^{\alpha\prime}$ and
(2) $\Sigma_R' = \mu(\Sigma_R^{\alpha\prime})$ and $\overline{\tau}' \cdot \tau = \mu(\overline{\tau_\alpha}' \cdot \tau_S)$ and
(3) $\mu \vDash pthCnd(\Sigma_R^{\alpha\prime})$

We apply the IH on $\Sigma_R \Downarrow_R^{\overline{\tau_\alpha}'} \Sigma_R''$ and have a $\Sigma_R^{\alpha\prime\prime}$ such that:

(1) $\Sigma_R^\alpha \; \alpha \Downarrow_R^{\overline{\tau_\alpha}'} \; \Sigma_R^{\alpha\prime\prime}$ and
(2) $\Sigma_R'' = \mu(\Sigma_R^{\alpha\prime\prime})$ and $\overline{\tau}' = \mu(\overline{\tau_\alpha}')$ and
(3) $\mu \vDash pthCnd(\Sigma_R^{\alpha\prime\prime})$

The result follows from applying Lemma 73 (R: Completeness single step) on $\Sigma_R'' \overset{\tau}{\dashrightarrow}_R \Sigma_R'$ and get a step $\Sigma_R^{\alpha\prime\prime} \overset{\tau_S}{\dashrightarrow}_R^\alpha \Sigma_R^\alpha$. We now use Rule R:Sym-Single and get an execution $\Sigma_R^\alpha \; \alpha \Downarrow_R^{\overline{\tau_\alpha} \cdot \tau_S} \mu(\Sigma_R^{\alpha\prime})$ as required.

□

Lemma 73 (R: Completeness single step)**.** *If*

(1) $\Sigma_R \overset{\tau}{\dashrightarrow}_R \Sigma_R'$ *and* $\mu(\Sigma_R^\alpha) = \Sigma_R$ *and*
(2) $\mu \vDash pthCnd(\Sigma_R^\alpha)$

Then

I $\Sigma_R^\alpha \overset{\tau_S}{\dashrightarrow}_R^\alpha \Sigma_R^{\alpha\prime}$ *and*
II $\mu(\Sigma_R^{\alpha\prime}) = \Sigma_R'$ *and*
III $\mu \vDash pthCnd(\Sigma_R^{\alpha\prime})$ *and* $\mu(\tau_S) = \tau$

Proof. We proceed by inversion on $\Sigma_R \overset{\tau}{\dashrightarrow}_R \Sigma_R'$:

Rule R:AM-Rollback Since $\mu()$ does not change the speculation window and *ctr* and $\mu(\Sigma_R^\alpha) = \Sigma_R$, we have $\Sigma_R.n = \Sigma_R^\alpha.n = 0$ and $\Sigma_R.ctr = \Sigma_R^\alpha.ctr$. The rest of the proof is analogous to the corresponding case in Lemma 42 (S: Completeness single step)

Rule R:AM-Context We then have $\Phi_R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}_R'$. Note that $\Phi_R.n > 0$ and as such for all symbolic states where $\mu(\Phi_R^\alpha) = \Phi_R$ as well. We proceed by inversion on $\Phi_R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}_R'$:

Rule R:AM-General Analogous to the corresponding case in Lemma 42 (S: Completeness single step).

Rule R:AM-NoBranch, Rule R:AM-barr-spec, Rule R:AM-barr, Rule R:AM-Call-Full, Rule R:AM-Ret-Empty, Rule R:AM-Ret-Same Then we have $\Phi_R \overset{\tau}{\dashrightarrow}_R \Phi_R'$ where $\Phi_R' = \langle p, \Phi_R.ctr, \Phi_R.\sigma', \Phi_R.\mathbb{R}, \Phi_R.n - 1\rangle$ with $\Phi_R.\sigma \xrightarrow{\tau} \sigma'$. Analogous to the corresponding case in Lemma 42 (S: Completeness single step).

Rule R:AM-Call Then we have $\Phi_R \overset{\tau}{\dashrightarrow}_R \Phi_R'$ where $\Phi_R' = \langle p, \Phi_R.ctr, \Phi_R.\sigma', \mathbb{R}', \Phi_R.n - 1\rangle$ with $\Phi_R.\sigma \xrightarrow{\tau} \sigma'$ and $\mathbb{R}' = \Phi_R.\mathbb{R}.\Phi_R.\sigma(\mathbf{pc}) + 1$. Since the symbolic $\mathbb{R}$ only contains entries created with the **pc** register, all entries in the symbolic $\mathbb{R}$ are concrete. The rest of the case is analogous to case Rule S:AM-barr in Lemma 42 (S: Completeness single step).

Rule R:AM-Ret-Spec We have $\Phi_R.\mathbb{R} = \mathbb{R}' \cdot l$ and $\Phi_R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}_{R\,\overline{\rho}\cdot \texttt{ret}\; l \cdot \texttt{start}_R\; \Phi_R.ctr}$ where $\overline{\Phi}_R = \langle p, \Phi_R.ctr, \sigma', \Phi_R.\mathbb{R}, \Phi_R.n - 1\rangle \cdot \langle p, \Phi_R.ctr + 1, \sigma'', \mathbb{R}', \min \Phi_R^\alpha.n, \omega\rangle$.

Furthermore, we have $\Phi_R.\sigma \xrightarrow{\tau} \sigma'$ and $\sigma'' = \sigma[\mathbf{pc} \mapsto l, {}^\iota \to a(\mathbf{sp}) + 8]$.

We use Lemma 18 (Non-spec : Completeness to symbolic) on $\Phi_R.\sigma \xrightarrow{\tau} \sigma'$ and get $\sigma_S \xrightarrow{\tau_S}{}^{S} \sigma'_S$ with $\mu(\sigma_S) = \sigma$, $\mu(\tau_S) = \tau$ and $\mu(\sigma'_S) = \sigma'$ and $\mu \vDash pthCnd(\sigma'_S)$.

Choose $\Phi_R = \mu(\Phi_R^\alpha)$ and note that a **ret** instruction is executed. We now derive a step using Rule R:Sym-Ret-Spec together with the non-speculative step $\mu(\Phi_R^\alpha.\sigma_S) \xrightarrow{\mu(\tau_S)}{}^{S} \mu(\sigma'_S)$ above and $\sigma'' = \sigma[\mathbf{pc} \mapsto \sigma(\mathbf{pc}) + 1]$: $\Phi_R^\alpha \overset{\tau_S}{\dashrightarrow}_R^\alpha \overline{\Phi^S}_R$ with $\overline{\Phi^S}_R = \langle p, \Phi_R^\alpha.ctr, \sigma'_S, \Phi_R^\alpha.\mathbb{R}, \Phi_R.n - 1\rangle \cdot \langle p, \Phi_R^\alpha.ctr + 1, \sigma'', \Phi_R^\alpha.\mathbb{R}', \min \Phi_R^\alpha.n, \omega\rangle$.

By definition we have $\mu(\sigma''_S) = \sigma''$, because **pc** and **sp** are always concrete. We now show that $\mu(\overline{\Phi^S}_R) = \overline{\Phi}_R$.

By $\mu(\Phi_R^\alpha) = \Phi_R$ we have $\Phi_R^\alpha.ctr = \Phi_R.ctr$ and $\Phi_R^\alpha.n = \Phi_R.n$ and by construction $\mu(\overline{\Phi^S}_R) = \overline{\Phi}_R$ and thus $\mu(\Phi_R^\alpha) \overset{\mu(\tau_S)}{\dashrightarrow}_R \mu(\overline{\Phi^S}_R)$ as needed.

Since $\overline{\Phi^S}_R.\sigma = \sigma''$ and $\sigma''.\delta^S = \sigma'.\delta^S$ we have $\mu \vDash pthCnd(\sigma'')$ by $\mu \vDash pthCnd(\sigma')$ from above.

□

J.4 Relating Speculative Oracle Semantics and Always-Mispredict Semantics

We define a few Lemmas

Lemma 74 (AM R: Single step preserves ≅). *If*

(1) $\Sigma_{R1} \cong \Sigma_{R2}$ *and*

(2) $\Sigma_{R1} \overset{\tau}{\dashrightarrow}_R \Sigma'_R$ *and* $\Sigma_{R2} \overset{\tau}{\dashrightarrow}_R \Sigma''_R$

Then

(1) $\Sigma'_R \cong \Sigma''_R$

Proof. We have

(1) $\Sigma_{R1} \cong \Sigma_{R2}$ and

(2) $\Sigma_{R1} \overset{\tau}{\dashrightarrow}_R \Sigma'_R$ and $\Sigma_{R2} \overset{\tau'}{\dashrightarrow}_R \Sigma''_R$

Because of (1), we know that the same rule was used to derive the steps $\Sigma_{R1} \overset{\tau}{\dashrightarrow}_R \Sigma'_R$ and $\Sigma_{R2} \overset{\tau}{\dashrightarrow}_R \Sigma''_R$.

We know that $\Sigma'_R.ctr = \Sigma''_R.ctr$, $\Sigma'_R.n = \Sigma''_R.n$, $\Sigma'_R.l = \Sigma''_R.l$, because of (1) and the fact that the same rule was used to derive the step.

The proof is analogous to Lemma 43 (S AM: Single step preserves ≅).

□

Lemma 75 (R SE: Single step preserves ≅). *If*

(1) $X_{R1} \cong X_{R2}$ *and*

(2) $X_{R1} \overset{\tau}{\rightsquigarrow}^O_R X'_R$ *and* $X_{R2} \overset{\tau}{\rightsquigarrow}^O_R X''_R$

Then

(1) $X'_R \cong X''_R$ *and*

Proof. We have

(1) $X_{R1} \cong X_{R2}$ and

(2) $X_{R1} \overset{\tau}{\rightsquigarrow}^O_R X'_R$ and $X_{R2} \overset{\tau}{\rightsquigarrow}^O_R X''_R$

Because of (1), we know that the same rule was used to derive the steps $X_{R1} \overset{\tau}{\dashrightarrow}_R X'_R$ and $X_{R2} \overset{\tau}{\dashrightarrow}_R X''_R$.

We know that $X'_R.ctr = X''_R.ctr$, $X'_R.n = X''_R.n$, $X'_R.l = X''_R.l$, because of (1) and the fact that the same rule was used to derive the step.

The proof is analogous to Lemma 44 (S SE: Single step preserves ≅). □

Theorem 22 (R: SNI). *A program p satisfies SNI for a security policy P and all prediction oracles O with speculative window at most ω iff for all initial configurations $\sigma, \sigma' \in InitConf$, if $\sigma \sim_P \sigma'$ and (p,σ) $\mathbb{A}^O_{NS}$ $\overline{\tau}$, (p,σ') $\mathbb{A}^O_{NS}$ $\overline{\tau}$, then (p,σ) $\mathbb{A}^\omega_R$ $\overline{\tau}''$, (p,σ') $\mathbb{A}^\omega_R$ $\overline{\tau}''$*

Proof. Let p be a program, P be a policy and $\omega \in \mathbb{N}$ be a speculative window. We prove the two directions separately.

(⇒) We have

(1) $\sigma \sim_P \sigma'$ and

(2) (p,σ) $\mathbb{A}^O_{NS}$ $\overline{\tau}'$, (p,σ') $\mathbb{A}^O_{NS}$ $\overline{\tau}'$ and

(3) p satisfies SNI for policy P and all prediction oracles O with speculative window at most ω

and we need to show that (p,σ) $\mathbb{A}^\omega_R$ $\overline{\tau}''$, (p,σ') $\mathbb{A}^\omega_R$ $\overline{\tau}''$ holds.

We unfold the definition of SNI we have for all O with speculation window at most ω, for all initial configurations σ, σ', if $\sigma \sim_P \sigma'$ and (p,σ) $\mathbb{A}^O_{NS}$ $\overline{\tau}$, (p,σ') $\mathbb{A}^O_{NS}$ $\overline{\tau}$, then (p,σ) $\mathbb{A}^O_R$ $\overline{\tau}'$ and (p,σ') $\mathbb{A}^O_R$ $\overline{\tau}'$.

We fulfill all premises of SNI by 1) and 2) for p and get (p,σ) $\mathbb{A}^O_R$ $\overline{\tau}'$ and (p,σ') $\mathbb{A}^O_R$ $\overline{\tau}'$.

We use Proposition 2 (R: Sound and Completeness between Spec and AM semantics) with (p,σ) $\mathbb{A}^O_R$ $\overline{\tau}'$ and (p,σ') $\mathbb{A}^O_R$ $\overline{\tau}'$ to get (p,σ) $\mathbb{A}^\omega_R$ $\overline{\tau}''$, (p,σ') $\mathbb{A}^\omega_R$ $\overline{\tau}''$. This completes the proof.

(⇐) We have

(1) $\sigma \sim_P \sigma'$ and

(2) (p,σ) $\mathbb{A}^O_{NS}$ $\overline{\tau}'$, (p,σ') $\mathbb{A}^O_{NS}$ $\overline{\tau}'$ and

(3) if $\sigma \sim_P \sigma'$ and (p,σ) $\mathbb{A}^O_{NS}$ $\overline{\tau}$, (p,σ') $\mathbb{A}^O_{NS}$ $\overline{\tau}$, then (p,σ) $\mathbb{A}^\omega_R$ $\overline{\tau}''$, (p,σ') $\mathbb{A}^\omega_R$ $\overline{\tau}''$

Note that we got assumptions 1) and 2) by the unfolding of the definition of SNI. We need to show that (p,σ) $\mathbb{A}^O_R$ $\overline{\tau}'$ and (p,σ') $\mathbb{A}^O_R$ $\overline{\tau}'$ holds.

By using assumption 1) and 2) for assumption 3), we get (p,σ) $\mathbb{A}^\omega_R$ $\overline{\tau}''$, (p,σ') $\mathbb{A}^\omega_R$ $\overline{\tau}''$.

Let O be an arbitrary prediction oracle with speculative window at most ω.

From Proposition 2 (R: Sound and Completeness between Spec and AM semantics) with (p,σ) $\mathbb{A}^\omega_R$ $\overline{\tau}''$, (p,σ') $\mathbb{A}^\omega_R$ $\overline{\tau}''$ we get back (p,σ) $\mathbb{A}^O_R$ $\overline{\tau}$, (p,σ') $\mathbb{A}^O_R$ $\overline{\tau}$. Consequently, p satisfies SNI w.r.t. P and O.

Since O was an arbitrary prediction oracle with speculation window at most ω, then p satisfies SNI for P and all prediction oracles with speculation window at most ω.

□

Proposition 2 (R: Sound and Completeness between Spec and AM semantics). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, $\sigma, \sigma' \in InitConf$ be two initial configurations. We have (p,σ) ᗣ^{ω}_{R} $\overline{\tau}$ and (p,σ') ᗣ^{ω}_{R} $\overline{\tau}$ iff (p,σ) ᗣ^{O}_{R} $\overline{\tau}'$, (p,σ) ᗣ^{O}_{R} $\overline{\tau}'$ for all prediction oracles O with speculative window at most ω.*

Proof. The proposition immediately follows from Lemma 77 (R: Soundness Am semantics w.r.t. speculative semantics) and Lemma 80 (R: Completeness AM semantics w.r.t. speculative semantics) □

Definition 61 (R: Relation between AM and spec for all oracles). *We define two relations between AM and oracle semantics. $\approx$ $\sim$*

$$\boxed{\Sigma_R \approx X_R}$$

$$\frac{}{\varnothing \approx \varnothing}\ (Base) \qquad \frac{\Sigma_R \sim X_R\restriction_{com} \quad INV(\Sigma_R, X_R)}{\Sigma_R \approx X_R}\ (Single\text{-}Base)$$

$$\frac{\begin{array}{c}\Sigma_R \sim X_R\restriction_{com} \quad \Sigma''_R \Downarrow^{\overline{\tau}}_R \Sigma'''_R \text{ where transaction with id ctr is rolled back} \\ X_R = X'_R \cdot \langle p, ctr, \sigma, h, n''\rangle \quad \Sigma_R = \Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \quad INV(\Sigma_R, X_R)\end{array}}{\Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n'\rangle \cdot \Sigma_{R_1} \approx X'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n''\rangle \cdot \langle p, ctr', \sigma, \mathbb{R}', h, n'''\rangle^{true}}\ (Single\text{-}OracleTrue)$$

$$\frac{\begin{array}{c}\Sigma''_R \sim X''_R\restriction_{com} \quad n' \geq 0 \quad \Sigma''_R \Downarrow^{\overline{\tau}}_R \Sigma'''_R \text{ where transaction with id ctr is rolled back} \\ X_R = X'_R \cdot \langle p, ctr, \sigma, h, n''\rangle \quad \Sigma_R = \Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \quad INV(\Sigma_R, X_R)\end{array}}{\Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}' n'\rangle^{false} \cdot \Sigma_{R_1} \approx X'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n''\rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0\rangle^{false} \cdot X_{R_1}}\ (Single\text{-}Transaction\text{-}Rollback)$$

$$\boxed{\Sigma_R \sim X_R}$$

$$\frac{}{\varnothing \sim \varnothing}\ (Base) \qquad \frac{|\Sigma'_R| = |X'_R| \quad \Sigma'_R \sim X'_R}{\Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle^b \sim X'_R \cdot \langle p, ctr', \sigma, \mathbb{R}, h, n'\rangle^b}\ (Single)$$

Lemma 76 (Initial states fulfill properties). *Let p be a program, ω be a speculation window and O be an oracle with speculation window at most ω. If*

(1) $\sigma, \sigma' \in InitConf$ and
(2) $\Sigma^{init}_R p, \sigma$ and $\Sigma^{init}_R p, \sigma'$ and
(3) $X^{init}_R(p,\sigma)$ and $X^{init}_R(p,\sigma')$

Then

(1) $X^{init}_R(p,\sigma) \cong X^{init}_R(p,\sigma')$ and
(2) $\Sigma^{init}_R p, \sigma \cong \Sigma^{init}_R p, \sigma'$ and
(3) $\Sigma^{init}_R p, \sigma \approx X^{init}_R(p,\sigma)$ and $\Sigma^{init}_R p, \sigma' \approx X^{init}_R(p,\sigma')$ by Rule Single-Base and

Proof. We have

(1) $\sigma, \sigma' \in InitConf$ and
(2) $\Sigma^{init}_R p, \sigma$ and $\Sigma^{init}_R p, \sigma'$ and
(3) $X^{init}_R(p,\sigma)$ and $X^{init}_R(p,\sigma')$

Notice that by definition of $X^{init}_R()$ and Σ^{init}_R we have:

$$X^{init}_R(p,\sigma) = \langle p, 0, \sigma, \varnothing, \bot\rangle$$
$$X^{init}_R(p,\sigma') = \langle p, 0, \sigma, \varnothing, \bot\rangle$$
$$\Sigma^{init}_R p, \sigma = \langle p, 0, \sigma, \bot\rangle$$
$$\Sigma^{init}_R p, \sigma' = \langle p, 0, \sigma, \bot\rangle$$

I Immediate
II Immediate
III Immediate using Rule Single-Base

□

Lemma 77 (R: Soundness Am semantics w.r.t. speculative semantics)**.** *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*
If

(1) $\sigma, \sigma' \in InitConf$ *and*
(2) $(p, \sigma) \; \text{ghost}^{\omega}_{R} \; \overline{\tau}$, $(p, \sigma') \; \text{ghost}^{\omega}_{R} \; \overline{\tau}$

Then for all prediction oracles O with speculation window at most ω.

I $(p, \sigma) \; \text{ghost}^{O}_{R} \; \overline{\tau}'$, $(p, \sigma) \; \text{ghost}^{O}_{R} \; \overline{\tau}'$

Proof. Let $\omega \in \mathbb{N}$ be a speculation window and $\sigma, \sigma' \in InitConf$ be two initial configurations. We have:

(1) $(p, \sigma) \; \text{ghost}^{\omega}_{R} \; \overline{\tau}$, $(p, \sigma') \; \text{ghost}^{\omega}_{R} \; \overline{\tau}$

Furthermore, let O be an arbitrary prediction oracle with speculative window at most ω.

The reasoning ins analogous to Lemma 46 (S: Soundness Am semantics w.r.t. speculative semantics) using Lemma 78 (R: Soundness Am semantics w.r.t. speculative semantics with new relation between states) together with Lemma 76 (Initial states fulfill properties).

□

Lemma 78 (R: Soundness Am semantics w.r.t. speculative semantics with new relation between states)**.** *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*
If

(1) $\Sigma_{R1} \cong \Sigma_{R2}$
(2) $X_{R1} \cong X_{R2}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma_{R1} \approx X_{R1}$ *and* $\Sigma_{R2} \approx X_{R2}$
(4) $\Sigma_{R1} \Downarrow^{\overline{\tau}}_{R} \Sigma'_{R1}$ *and* $\Sigma_{R2} \Downarrow^{\overline{\tau}}_{R} \Sigma'_{R2}$

Then for all prediction oracles O with speculation window at most ω.

I $X_{R1} \; {}^{O}\!\downarrow^{R}_{\overline{\tau}'} X'_{R1}$, $X_{R2} \; {}^{O}\!\downarrow^{R}_{\overline{\tau}''} X'_{R2}$
II $\Sigma'_{R1} \cong \Sigma'_{R2}$
III $X'_{R1} \cong X'_{R2}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{R1} \approx X'_{R1}$ *and* $\Sigma'_{R2} \approx X'_{R2}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. By Induction on $\Sigma_{R1} \Downarrow^{\overline{\tau}}_{R} \Sigma'_{R1}$ and $\Sigma_{R2} \Downarrow^{\overline{\tau}}_{R} \Sigma'_{R2}$.

Rule R:AM-Reflection We have $\Sigma_{R1} \Downarrow^{\varepsilon}_{R} \Sigma'_{R1}$ and $\Sigma_{R2} \Downarrow^{\varepsilon}_{R} \Sigma'_{R2}$, where $\Sigma'_{R1} = \Sigma_{R1}$ and $\Sigma'_{R2} = \Sigma_{R2}$.

Furthermore, we use Rule R:SE-Reflection to derive $X_{R1} \; {}^{O}\!\downarrow^{R}_{\varepsilon} X'_{R1}$, $X_{R2} \; {}^{O}\!\downarrow^{R}_{\varepsilon} X'_{R2}$ with $X'_{R1} = X_{R1}$ and $X'_{R2} = X_{R2}$.
We now trivially satisfy all conclusions.

Rule R:AM-Single We have $\Sigma_{R1} \Downarrow^{\overline{\tau}''}_{R} \Sigma'_{R}$ with $\Sigma'_{R} \; \overset{\tau}{\div}\!\!\text{ghost}_{R} \; \Sigma'_{R1}$ and $\Sigma_{R2} \Downarrow^{\overline{\tau}''}_{R} \Sigma''_{R}$ and $\Sigma''_{R} \; \overset{\tau}{\div}\!\!\text{ghost}_{R} \; \Sigma'_{R2}$.

We now apply IH on $\Sigma_{R1} \Downarrow^{\overline{\tau}''}_{R} \Sigma'_{R}$ and $\Sigma_{R2} \Downarrow^{\overline{\tau}''}_{R} \Sigma''_{R}$ and get

(a) $X_{R1} \; {}^{O}\!\downarrow^{R}_{\overline{\tau}'} X'_{R}$, $X_{R2} \; {}^{O}\!\downarrow^{R}_{\overline{\tau}''} X''_{R}$
(b) $\Sigma'_{R} \cong \Sigma''_{R}$
(c) $X'_{R} \cong X''_{R}$ and $\overline{\rho}' = \varnothing$
(d) $\Sigma'_{R} \approx X'_{R}$ and $\Sigma''_{R} \approx X''_{R}$
(e) $\overline{\tau}' = \overline{\tau}''$

We proceed by inversion on $\approx$ in $\Sigma'_{R} \approx X'_{R}$ and $\Sigma''_{R} \approx X''_{R}$:

v5-com-single-base We thus have $\Sigma'_{R} \sim X'_{R} \upharpoonright_{com}$ and $INV(\Sigma'_{R}, X'_{R})$ (Similar for Σ''_{R} and X''_{R}).
We only show the proof for X'_{R} here. The proof for X''_{R} is analogous, because of $X'_{R} \cong X''_{R}$.
Notice that if $minWndw(X'_{R}) = 0$ then the transaction with $n = 0$ has to be one that will be committed. Otherwise they would be related by Rule Single-Transaction-Rollback.
The case is analogous to the corresponding case in Lemma 47 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states) using Lemma 79 (R: Soundness Single Step AM).

v5-com-single-oracle We thus have

$$\begin{aligned}
X'_{\mathrm{R}} =& X_{\mathrm{R}3} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \cdot \langle p, ctr', \sigma, \mathbb{R}', h, n''' \rangle^{l} \\
\Sigma'_{\mathrm{R}} =& \Sigma_{\mathrm{R}3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle \cdot \Sigma_{\mathrm{R}4} \\
X_{\mathrm{R}} =& X_{\mathrm{R}3} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \\
\Sigma_{\mathrm{R}} =& \Sigma_{\mathrm{R}3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \\
\Sigma_{\mathrm{R}} \sim& X_{\mathrm{R}} \restriction_{com}
\end{aligned}$$

The form of X''_{R} and Σ''_{R} is analogous.
The case is analogous to the corresponding case in Lemma 47 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

v5-com-single-rollback We have

$$\begin{aligned}
X'_{\mathrm{R}} =& X_{\mathrm{R}3} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0 \rangle^{l} \cdot X_{\mathrm{R}4} \\
\Sigma'_{\mathrm{R}} =& \Sigma_{\mathrm{R}3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle^{l} \cdot \Sigma_{\mathrm{R}4} \\
X_{\mathrm{R}} =& X_{\mathrm{R}3} \cdot \langle p, ctr, \sigma, h, \mathbb{R}, n'' \rangle \\
\Sigma_{\mathrm{R}} =& \Sigma_{\mathrm{R}3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \\
\Sigma_{\mathrm{R}} \sim& X_{\mathrm{R}} \restriction_{com} \\
n' \geq& 0
\end{aligned}$$

The form of X''_{R} and Σ''_{R} is analogous.
Additionally we know that the transaction terminates in some state $\Sigma_{\mathrm{R}} \Downarrow^{\overline{\tau}}_{\mathrm{R}} \Sigma'''_{\mathrm{R}}$. There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma'_{\mathrm{R}} \overset{\tau}{\dashrightarrow}_{\mathrm{R}} \Sigma'_{\mathrm{R}1}$ is not a rollback for *ctr* and Rule R:AM-Context or Rule R:AM-Rollback for a different transaction with a different *ctr* was used.
The case is analogous to the corresponding case in Lemma 47 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

$n' = 0$ Then we know that $\Sigma'_{\mathrm{R}} \overset{\tau}{\dashrightarrow}_{\mathrm{R}} \Sigma'_{\mathrm{R}1}$ was created by Rule R:AM-Rollback and is a rollback for *ctr*.

I Here we prove that $X'_{\mathrm{R}} \overset{\tau_0}{\rightsquigarrow}^{O}_{\mathrm{R}} X'_{\mathrm{R}1}$ and $X''_{\mathrm{R}} \overset{\tau_1}{\rightsquigarrow}^{O}_{\mathrm{R}} X'_{\mathrm{R}2}$.
Since in X'_{R} and X''_{R} we have a state with $n = 0$ and we mispredicted, we know that Rule R:SE-Rollback applies.
So $X'_{\mathrm{R}} \overset{\tau_0}{\rightsquigarrow}^{O}_{\mathrm{R}} X'_{\mathrm{R}1}$ and $X''_{\mathrm{R}} \overset{\tau_1}{\rightsquigarrow}^{O}_{\mathrm{R}} X'_{\mathrm{R}2}$ are derived by Rule R:SE-Rollback.
The rest of the case is analogous to the corresponding case Lemma 47 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

□

Lemma 79 (R: Soundness Single Step AM). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, O be a prediction oracle with speculative window at most ω, $\Sigma_{\mathrm{R}1} = \Sigma'_{\mathrm{R}} \cdot \Phi'_{\mathrm{R}}$, $\Sigma_{\mathrm{R}2} = \Sigma''_{\mathrm{R}} \cdot \Phi''_{\mathrm{R}}$ be two speculative states for the always mispredict semantics and $X_{\mathrm{R}1}, X_{\mathrm{R}2}$, be two speculative states for the speculative semantics.*
If the following conditions hold:

(1) $\Sigma_{\mathrm{R}1} \cong \Sigma_{\mathrm{R}2}$
(2) $X_{\mathrm{R}1} \cong X_{\mathrm{R}2}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma_{\mathrm{R}1} \approx X_{\mathrm{R}1}$ *and* $\Sigma_{\mathrm{R}2} \approx X_{\mathrm{R}2}$
(4) $\Phi'_{\mathrm{R}} \overset{\tau''}{\dashrightarrow}_{\mathrm{R}} \Sigma'_{\mathrm{R}1}$ *and* $\Phi''_{\mathrm{R}} \overset{\tau''}{\dashrightarrow}_{\mathrm{R}} \Sigma'_{\mathrm{R}2}$

then there are instances $X'_{\mathrm{R}1}, X'_{\mathrm{R}2}$ for the speculative semantics such that:

I $X_{\mathrm{R}1} \overset{O}{\downarrow}^{\mathrm{R}}_{\tau} X'_{\mathrm{R}1}$ *and* $X_{\mathrm{R}2} \overset{O}{\downarrow}^{\mathrm{R}}_{\tau'} X'_{\mathrm{R}2}$
II $\Sigma'_{\mathrm{R}1} \cong \Sigma'_{\mathrm{R}2}$
III $X'_{\mathrm{R}1} \cong X'_{\mathrm{R}2}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{\mathrm{R}1} \approx X'_{\mathrm{R}1}$ *and* $\Sigma'_{\mathrm{R}2} \approx X'_{\mathrm{R}2}$
V $\tau = \tau'$

Proof. We proceed by inversion on $\Phi'_{\mathrm{R}} \overset{\tau''}{\dashrightarrow}_{\mathrm{R}} \Sigma'_{\mathrm{R}1}$ and $\Phi''_{\mathrm{R}} \overset{\tau''}{\dashrightarrow}_{\mathrm{R}} \Sigma'_{\mathrm{R}2}$:

Rule R:AM-General We choose $X'_{\mathrm{R}1} = X'_{\mathrm{R}}$ and $X'_{\mathrm{R}2} = X''_{\mathrm{R}}$. The case is analogous to the corresponding case in Lemma 48 (S: Soundness Single Step AM).

Rule R:AM-Ret-Spec There are two cases depending on the output of the oracle O and the top of the $\mathbb{R}$ which we denote as l:

(ω) **and $m(a(\mathbf{sp})) = l$, correct prediction w.r.t X'_R** The execution jumps to the correct return address.

I We use Rule R:SE-Ret to derive the steps $X_{R1} \overset{\tau_0}{\rightsquigarrow}{}^{O}_{R} X'_R$ and $X_{R2} \overset{\tau_1}{\rightsquigarrow}{}^{O}_{R} X''_R$.
Furthermore, we execute Rule R:SE-General twice, because Rule R:SE-Ret created two observations in $\overline{\rho}$. We now have $X'_{R1} = X'_R$ with an empty $\overline{\rho}$.
The rule only emits the observation but does not change the state apart from $\overline{\rho}$. As a result we have $X_{R1} \overset{O}{\downarrow}{}^{S}_{\overline{\tau}} X'_{R1}$ and $X_{R2} \overset{O}{\downarrow}{}^{S}_{\overline{\tau}'} X'_{R2}$.

II By Lemma 74 (AM R: Single step preserves $\cong$).

III By Lemma 75 (R SE: Single step preserves $\cong$) for $X_{R1} \overset{\tau_0}{\rightsquigarrow}{}^{O}_{R} X'_R$ and $X_{R2} \overset{\tau_1}{\rightsquigarrow}{}^{O}_{R} X''_R$ and the fact that the use of Rule R:SE-General does not change the states and the $\overline{\rho}$ of both oracle states are equal. Notice that $\overline{\rho}$ is empty after applying Rule R:SE-General twice.

IV We have

$$\begin{aligned}
X'_{R1} &= X'_{R3} \cdot \langle p, ctr, \sigma', \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n_0\rangle \\
\Sigma'_{R1} &= \Sigma_{R3} \cdot \langle p, ctr, \sigma', \mathbb{R}, n_1\rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', n_2\rangle \\
X'_{R4} &= X'_{R3} \cdot \langle p, ctr, \sigma', \mathbb{R}, h, n\rangle \\
\Sigma'_{R4} &= \Sigma_{R3} \cdot \langle p, ctr, \sigma', \mathbb{R}, n_1\rangle
\end{aligned}$$

The case is analogous to the Rule S:AM-Store-Spec correct prediction case in Lemma 48 (S: Soundness Single Step AM) replacing Rule Single-OracleTrue and Rule Single-Transaction-Rollback with Rule Single-OracleTrue and Rule Single-Transaction-Rollback.

V The observations are $\overline{\tau} = \texttt{ret}\ m \cdot \texttt{start}\ ctr_1$ and $\overline{\tau}' = \texttt{ret}\ m' \cdot \texttt{start}\ ctr_2$ for some $m, m' \in Vals$.
The case is analogous to the Rule S:AM-Store-Spec correct prediction case in Lemma 48 (S: Soundness Single Step AM).

(ω) $m(a(\mathbf{sp})) \neq l$, **wrong prediction w.r.t X'_R** The execution jumps to the wrong return address.

a) We use Rule R:SE-Ret to derive the steps $X'_R \overset{\tau_0}{\rightsquigarrow}{}^{O}_{R} X'_{R1}$ and $X''_R \overset{\tau_1}{\rightsquigarrow}{}^{O}_{R} X'_{R2}$.
Furthermore, we execute Rule R:SE-General twice, because Rule R:SE-Ret created two observations in $\overline{\rho}$. We now have $X'_{R1} = X'_R$ with an empty $\overline{\rho}$.
The rule only emits the observations but does not change the state apart from $\overline{\rho}$. As a result we have $X_{R1} \overset{O}{\downarrow}{}^{R}_{\overline{\tau}} X'_{R1}$ and $X_{R2} \overset{O}{\downarrow}{}^{R}_{\overline{\tau}'} X'_{R2}$. Notice that the observations in $\overline{\rho}$ are equal between X_{R1} and X_{R2}, because of (2). We have $X_{R1}.ctr = X_{R2}.ctr$ and $X_{R1}.\sigma \sim_{\mathbf{pc}} X_{R2}.\sigma$ from our relation.

b) By Lemma 74 (AM R: Single step preserves $\cong$).

c) By Lemma 75 (R SE: Single step preserves $\cong$) for Rule R:SE-Ret and Rule R:SE-General twice. Notice that $\overline{\rho}$ is empty now.

d) We have:

$$\begin{aligned}
X'_{R1} &= X'_{R3} \cdot \langle p, ctr, \sigma', \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma''', \mathbb{R}', h', n_0\rangle \\
\Sigma'_{R1} &= \Sigma_{R3} \cdot \langle p, ctr, \sigma', \mathbb{R}, n_1\rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', n_2\rangle \\
X'_{R4} &= X'_{R3} \cdot \langle p, ctr, \sigma', \mathbb{R}, h, n\rangle \\
\Sigma'_{R4} &= \Sigma_{R3} \cdot \langle p, ctr, \sigma', \mathbb{R}, n_1\rangle
\end{aligned}$$

The case is analogous to the Rule S:AM-Store-Spec correct prediction case in Lemma 48 (S: Soundness Single Step AM) replacing Rule Single-OracleTrue and Rule Single-Transaction-Rollback with Rule Single-OracleTrue and Rule Single-Transaction-Rollback.

e) The observations are

$$\begin{aligned}
\overline{\tau} &= \texttt{ret}\ m \cdot \texttt{start}\ X_{R1}.ctr \cdot \texttt{ret}\ X_{R1}.\sigma(\mathbf{pc}) \\
\overline{\tau}' &= \texttt{ret}\ m' \cdot \texttt{start}\ X_{R2}.ctr \cdot \texttt{ret}\ X_{R2}.\sigma(\mathbf{pc})
\end{aligned}$$

for some $m, m' \in Vals$.
The case is analogous to the misprediction case in Lemma 48 (S: Soundness Single Step AM).

Rule R:AM-barr and Rule R:AM-barr-spec We prove this for Rule R:AM-barr-spec. The proof for Rule R:AM-barr is analogous.
The proof is analogous to the corresponding case in Lemma 48 (S: Soundness Single Step AM) using Lemma 74 (AM R: Single step preserves $\cong$) and Lemma 75 (R SE: Single step preserves $\cong$),

not a barrier instruction The rules that are included here are: Rule R:SE-NoBranch, Rule R:SE-Ret-Empty, Rule R:SE-Call-Full and Rule R:SE-Call. Most cases are analogous to the barrier case.

d) The proof proceeds in the same way as in the barrier case above. The argument for $INV(\Sigma'_{R1}, X'_{R1})$ is the same as for the store instructions above.

□

Definition 62 (R: Constructing the Oracle). *Constructing the prediction oracle O_{am_R}. We build our oracle based on the executions $\Sigma_R^{init} p, \sigma \Downarrow_R^{\overline{\tau}} \Sigma_{R1} \overset{\tau_{am}}{\dashrightarrow}_R \Sigma_{R2}, \Sigma_R^{init} p, \sigma' \Downarrow_R^{\overline{\tau}} \Sigma'_{R1} \overset{\tau'_{am}}{\dashrightarrow}_R \Sigma'_{R2}$ where $\tau_{am} \neq \tau'_{am}$.*

Let us denote by the set RB the ids of all ongoing transaction ids in Σ_{R1}. Since $\Sigma_{R1} \cong \Sigma'_{R1}$ we know that the same transaction ids are still ongoing in Σ'_{R1} as well. The set RB describes the return instructions that we need to mispredict to reach the difference in the trace.

Our oracle is now defined as follows:

$$O_{am_R}(p, n, h) = \begin{cases} (\omega) \text{ if } |h| \in RB \wedge p(\sigma(\mathbf{pc})) = \mathbf{ret} \\ (0) \text{ otherwise (where } p(\sigma(\mathbf{pc})) = \mathbf{ret}) \end{cases}$$

Note that we use the length of h to reconstruct the ctr. Both start at 0 and are increased when a speculation starts. Since this oracle only mispredicts, we know that the ctr of the always mispredict run and the ctr of the oracle runs are equal.

Definition 63 (R: Relation between AM and Spec for oracles that only mispredict). *We define two relations, $\approx^{O_{am}}$ and $\sim$, between AM and oracle semantics. Note that $\approx^{O_{am}}$ is indexed by an oracle. This oracle has to always mispredict.*

$$\boxed{\Sigma_R \approx^{O_{am}} X_R}$$

$$\frac{}{\varnothing \approx^{O_{am}} \varnothing}\ \textit{(Base-Oracle)} \qquad \frac{\Sigma_R \sim X_R\restriction_{com} \quad \mathit{INV2}(\Sigma_R, X_R) \quad \mathit{minWndw}(X_R) > 0}{\Sigma_R \approx^{O_{am}} X_R}\ \textit{(Single-Base-Oracle)}$$

$$\frac{\begin{array}{c}\Sigma''_R \sim X''_R\restriction_{com} \quad n' \geq 0 \quad \Sigma''_R \Downarrow_R^{\overline{\tau}} \Sigma'''_R \text{ where transaction with id ctr is rolled back} \\ X_R = X'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \qquad \Sigma_R = \Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \qquad \mathit{INV2}(\Sigma_R, X_R)\end{array}}{\Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle^{false} \cdot \Sigma_{R1} \approx^{O_{am}} X'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0 \rangle^{false}}\ \textit{(Single-Transaction-Rollback-Oracle)}$$

Lemma 80 (R: Completeness AM semantics w.r.t. speculative semantics). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, $\sigma, \sigma' \in InitConf$ be two initial configurations. If*

(1) $p, \sigma \,\text{🕱}_R^{\omega}\, \overline{\tau}$ and $p, \sigma' \,\text{🕱}_R^{\omega}\, \overline{\tau}'$ and
(2) $\overline{\tau} \neq \overline{\tau}'$

Then there exists an oracle O such that

I $p, \sigma \,\text{🕱}_R^{O}\, \overline{\tau}_1$ and $p, \sigma' \,\text{🕱}_R^{O}\, \overline{\tau}'_1$ and
II $\overline{\tau}_1 \neq \overline{\tau}'_1$

Proof. Let $\omega \in \mathbb{N}$ be a speculative window, $\sigma, \sigma' \in InitConf$ be two initial configurations. We have If

(1) $p, \sigma \,\text{🕱}_R^{\omega}\, \overline{\tau}$ and $p, \sigma' \,\text{🕱}_R^{\omega}\, \overline{\tau}'$ and
(2) $\overline{\tau} \neq \overline{\tau}'$

By definition of 🕱_R^{ω} we have two final states Σ_{RF} and Σ'_{RF} such that $\Sigma_R^{init} p, \sigma \Downarrow_R^{\overline{\tau}} \Sigma_{RF}$ $\Sigma_R^{init} p, \sigma' \Downarrow_R^{\overline{\tau}'} \Sigma'_{RF}$. Combined with the fact that $\overline{\tau} \neq \overline{\tau}'$, it follows that there are speculative states $\Sigma_{R1}, \Sigma_R, \Sigma'_{R1}, \Sigma'_{R2}$ and sequences of observations $\overline{\tau}, \overline{\tau}_{end}, \overline{\tau}'_{end}, \tau_{am}, \tau'_{am}$ such that $\tau_{am} \neq \tau'_{am}$, $\Sigma_{R1} \cong \Sigma'_{R1}$ and:

$$\Sigma_R^{init} p, \sigma \Downarrow_R^{\overline{\tau}} \Sigma_{R1} \overset{\tau_{am}}{\dashrightarrow}_R \Sigma_{R2} \Downarrow_R^{\overline{\tau}_{end}} \Sigma_{RF}$$

$$\Sigma_R^{init} p, \sigma' \Downarrow_R^{\overline{\tau}} \Sigma'_{R1} \overset{\tau'_{am}}{\dashrightarrow}_R \Sigma'_{R2} \Downarrow_R^{\overline{\tau}'_{end}} \Sigma'_{RF}$$

We claim that there is a prediction oracle O with speculative window at most ω such that

a $X_R^{init}(p, \sigma) \overset{O}{\rightsquigarrow}_v^R X_{R1}$ and $X_{R1}.\sigma = \Sigma_{R1}.\sigma$ and $\mathit{INV2}(X_{R1}, \Sigma_{R1})$ and
b $X_R^{init}(p, \sigma') \overset{O}{\rightsquigarrow}_v^R X'_{R1}$ and $X'_{R1}.\sigma = \Sigma'_{R1}.\sigma$ and $\mathit{INV2}(X'_{R1}, \Sigma'_{R1})$
c $X_{R1} \cong X'_{R1}$

We get this by applying Lemma 81 (Stronger Soundness for a specific oracle and for specific executions) on the Am execution up to the point of the difference i.e., $\Sigma_R^{init} p, \sigma \Downarrow_R^{\overline{\tau}} \Sigma_{R1}$.

We now show that $\Sigma_{R1} \approx^{O_{am}} X_{R1}$ is derived by Rule Single-Base-Oracle.

We do a case distinction if there are ongoing transactions in X_{R1} or not

no ongoing transactions in X_{R1} Then $\Sigma_{R1} \approx^{O_{am}} X_{R1}$ can only be derived Rule Single-Base-Oracle and Σ_{R1} has no ongoing transactions as well. Then we have by $\mathit{INV2}(\Sigma_{R1}, X_{R1})$ and $\Sigma_{R1}.n = \bot$ that $X_{R1}.n = \bot$.

ongoing transactions in X_R By the definition of the oracle O, we know that the for the transaction id where the difference $\tau_{am} \neq \tau_{am'}$ happens, the oracle mispredicted with a speculation window of ω. This is also the topmost transaction in X_R.
Furthermore, we know that $X_{R1}.n \geq minWndw(X_{R1})$ by definition of the oracle O_{amR} and $minWndw()$.
Since the next rule cannot be Rule R:AM-Rollback, we know that $\Sigma_{R1}.n > 0$ and by $INV2(\Sigma_{R1}, X_{R1})$ we get $minWndw(X_{R1}) > 0$ (Similar for X'_{R1} because of $\Sigma_{R1} \cong \Sigma'_{R1}$).
If $\Sigma_{R1} \approx^{O_{am}} X_{R1}$ by rollback rule, we would have a contradiction because we would need the topmost speculation window of $X_{R1}.n = 0$. But we know that $minWndw(X_{R1}) > 0$, because the speculation window of the topmost instance was created with a speculation window of ω.
we know that $X_{R1} \approx^{O_{am}} \Sigma_{R1}$ by Rule Single-Base-Oracle.

We now proceed by case analysis on the rule in $\overset{}{\dashrightarrow}_R$ used to derive $\Sigma_{R1} \overset{\tau_{am}}{\dashrightarrow}_R \Sigma_{R2}$. Because $\Sigma_{R1} \cong \Sigma'_{R1}$ and $\overline{\tau}_1 = \overline{\tau}'_1$, we know that the same rule was used in $\Sigma'_{R1} \overset{\tau'_{am}}{\dashrightarrow}_R \Sigma'_{R2}$ as well.

Rule R:AM-Rollback Contradiction. Because $\Sigma_{R1} \cong \Sigma'_{R1}$ we have for all instances $\Phi_1.ctr = \Phi'_1.ctr$.
Since the same instance would be rolled back, we have $\tau_{am} = \tau'_{am}$.

Rule R:AM-Context By inversion on Rule R:AM-Context for the step $\Sigma_{R1} \overset{\tau_{am}}{\dashrightarrow}_R \Sigma_{R2}$ we have $\Sigma_{R1} = \overline{\Phi}_R \cdot \Phi_R$ and $\Sigma_{R2} = \overline{\Phi}_R \cdot \overline{\Phi}'_R$ with $\Phi_R \overset{\tau_{am}}{\dashrightarrow}_R \overline{\Phi}'_R$.
We now do inversion on $\Sigma_{R1} \overset{\tau_{am}}{\dashrightarrow}_R \Sigma_{R2}$ and $\Phi_R \overset{\tau_{am}}{\dashrightarrow}_R \overline{\Phi}'_S$:

Rule R:AM-General Contradiction. By $\Sigma_{R1} \cong \Sigma'_{R1}$ we know that $\Sigma_{R1}.\overline{\rho} = \Sigma'_{R1}.\overline{\rho}$.
This immediately implies that $\tau_{am} = \tau_{am'}$, which is not true by assumption.

Rule R:AM-barr-spec, Rule R:AM-barr Contradiction. Since these rules do not generate any observation by definition.
This leads to $\tau_{am} = \tau_{am'}$.

Rule R:AM-NoBranch From the rule we have that $\Sigma_{R1}.\sigma \xrightarrow{\tau_{am}} \Sigma_{R2}.\sigma$ and $\Sigma'_{R1}.\sigma \xrightarrow{\tau'_{am}} \Sigma'_{R1}.\sigma$.
The case is analogous to the corresponding case in Lemma 49 (Completeness Am semantics w.r.t. speculative semantics).

Rule R:AM-Ret-Spec Then, $\tau_{am}, \tau_{am'}$ are generated by the step $\Sigma_{R1}.\sigma \xrightarrow{\tau_{am}} \Sigma_{R2}.\sigma$ and $\Sigma'_{R1}.\sigma \xrightarrow{\tau_{am'}} \Sigma'_{R2}.\sigma$ generated by Rule R:AM-Ret-Spec.
From the fact that $X_{R1} \cong X'_{R1}$, $X_{R1}.\sigma = \Sigma_{R1}.\sigma$, $X'_{R1}.\sigma = \Sigma'_{R1}.\sigma$, $INV2(X_{R1}, \Sigma_{R1})$, $INV2(X'_{R1}, \Sigma'_{R1})$ and from the way we construct the oracle (see above), we have that $O(p, X_{R1}.\sigma(pc), X_{R1}.h) = O(p, X'_{R1}.\sigma(\mathbf{pc}), X'_{R1}.h) = \omega$ it follows that Rule R:SE-Ret applies to both X_{R1} and X'_{R1}.
From Rule R:SE-Ret, we have $X_{R1} \overset{\tau_{sp}}{\rightsquigarrow}{}^{O}_{R} X_{R2}$ and $X'_{R1} \overset{\tau'_{sp}}{\rightsquigarrow}{}^{O}_{R} X'_{R2}$ and we know that $X_{R1}.\sigma \xrightarrow{\tau_{sp}} X_{R2}.\sigma$ and $X'_{R1}.\sigma \xrightarrow{\tau_{sp'}} X'_{R2}.\sigma$.
Because the non-speculative semantics $\rightarrow$ is deterministic, we have $\tau_{am} = \tau_{sp}$ and $\tau_{am'} = \tau_{sp'}$ and by our assumption $\tau_{am} \neq \tau_{am'}$.
This results in $\tau_{sp} \neq \tau'_{sp}$ which proves our claim.

This completes the proof of our claim.

□

Lemma 81 (Stronger Soundness for a specific oracle and for specific executions)**.** *Specific executions means that there is a difference in the trace but before there is none. We use the oracle O_{amR} as it is defined by Definition 56 (Constructing the Oracle) for the given execution. If*

(1) $\Sigma_{R1} \cong \Sigma_{R2}$
(2) $X_{R1} \cong X_{R2}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma_{R1} \approx^{O_{am}} X_{R1}$ *and* $\Sigma_{R2} \approx^{O_{am}} X_{R2}$
(4) $\Sigma_{R1} \Downarrow^{\overline{\tau}}_{R} \Sigma'_{R1}$ *and* $\Sigma_{R2} \Downarrow^{\overline{\tau}}_{R} \Sigma'_{R2}$

and our oracle is constructed in the way described above Then

I $X_{R1} \overset{O}{\downarrow}{}^{R}_{\overline{\tau}'} X'_{R1}, X_{R2} \overset{O}{\downarrow}{}^{R}_{\overline{\tau}''} X'_{R2}$
II $\Sigma'_{R1} \cong \Sigma'_{R2}$
III $X'_{R1} \cong X'_{R2}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{R1} \approx^{O_{am}} X'_{R1}$ *and* $\Sigma'_{R2} \approx^{O_{am}} X'_{R2}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. Notice that the proof is very similar to Lemma 27 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics). The only thing that is different is that (1) the specific oracle only mispredicts so there is one less case in the relation and (2) we have a stronger invariant for that specific oracle.

For these reasons we will only argue why $INV2(\Sigma'_{R1}, X'_{R1})$ holds in the different cases and leave the rest to the old soundness proof.

By Induction on $\Sigma_{R1} \Downarrow^{\overline{\tau}}_{R} \Sigma'_{R1}$ and $\Sigma_{R2} \Downarrow^{\overline{\tau}}_{R} \Sigma'_{R2}$.

Rule R:AM-Reflection We have $\Sigma_{R1} \Downarrow_R^{\varepsilon} \Sigma'_R$ and $\Sigma_{R2} \Downarrow_R^{\varepsilon} \Sigma''_R$, where $\Sigma'_R = \Sigma_{R1}$ and $\Sigma''_R = \Sigma_{R2}$. We choose $\Sigma'_{R1} = \Sigma'_R$ and $\Sigma'_{R2} = \Sigma''_R$.

We further use Rule R:SE-Reflection to derive $X_{R1} \overset{O}{\downarrow}{}^{R}_{\varepsilon} X'_{R1}, X_{R2} \overset{O}{\downarrow}{}^{R}_{\varepsilon} X'_{R2}$ with $X'_{R1} = X_{R1}$ and $X'_{R2} = X_{R2}$. We now trivially satisfy all conclusions.

Rule R:AM-Single We have $\Sigma_{R1} \Downarrow_R^{\overline{\tau}''} \Sigma'_R$ with $\Sigma'_R \overset{\tau}{\rightarrow}_R \Sigma'_{R1}$ and $\Sigma_{R2} \Downarrow_R^{\overline{\tau}''} \Sigma''_R$ and $\Sigma''_R \overset{\tau}{\rightarrow}_R \Sigma'_{R2}$.

We now apply IH on $\Sigma_{R1} \Downarrow_R^{\overline{\tau}''} \Sigma'_R$ and $\Sigma_{R2} \Downarrow_R^{\overline{\tau}''} \Sigma''_R$ and get

(a) $X_{R1} \overset{O}{\downarrow}{}^{R}_{\overline{\tau}'} X'_R, X_{R2} \overset{O}{\downarrow}{}^{R}_{\overline{\tau}''} X''_R$
(b) $\Sigma'_R \cong \Sigma''_R$
(c) $X'_R \cong X''_R$ and $\overline{\rho}' = \varnothing$
(d) $\Sigma'_R \approx^{O_{am}} X'_R$ and $\Sigma''_R \approx^{O_{am}} X''_R$
(e) $\overline{\tau}' = \overline{\tau}''$

We do a case distinction on $\approx^{O_{am}}$ in $\Sigma'_R \approx^{O_{am}} X'_R$ and $\Sigma''_R \approx^{O_{am}} X''_R$ by inversion:

v5-com-single-base We thus have $\Sigma'_R \sim X'_R\restriction_{com}$, $minWndw(X'_R) > 0$ and $INV2(\Sigma'_R, X'_R)$ (Similar for Σ''_R and X''_R).

We now proceed by inversion on the derivation $\Sigma'_R \overset{\tau}{\rightarrow}_S \Sigma'_{R1}$.

Rule R:AM-Rollback Contradiction, because of $minWndw(X'_R) > 0$ and $INV2(\Sigma'_R, X'_R)$.

Rule R:AM-General $INV2()$ trivially holds, because it does not change the speculation window of the states.

Rule R:AM-Context We have $\Phi_R \overset{\tau}{\rightarrow}_R \overline{\Phi}_R$ and $\Phi'_R \overset{\tau}{\rightarrow}_R \overline{\Phi}'_R$. We fulfill all conditions for Lemma 82 (V5AM: Strong Soundness Single Step) which gives us the desired result.

v5-com-single-rollback We have

$$\begin{aligned}
X'_R &= X_{R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0 \rangle \cdot X_{R4} \\
\Sigma'_R &= \Sigma_{R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle \cdot \Sigma_{R4} \\
X_R &= X_{R3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \\
\Sigma_R &= \Sigma_{R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \\
\Sigma_R &\sim X_R\restriction_{com} \\
&\quad INV2(\Sigma_R, X_R) \\
n' &\geq 0
\end{aligned}$$

The form of X''_R and Σ''_R is analogous.

The case is analogous to the corresponding case in Lemma 50 (Stronger Soundness for a specific oracle and for specific executions).

□

Lemma 82 (V5AM: Strong Soundness Single Step)**.** *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, O be a prediction oracle with speculative window at most ω, $\Sigma_{R1} = \Sigma'_R \cdot \Phi'_R$, $\Sigma_{R2} = \Sigma''_R \cdot \Phi''_R$ be two speculative states for the always mispredict semantics and X_{R1}, X_{R2}, be two speculative states for the speculative semantics.*

If the following conditions hold:

(1) $\Sigma_{R1} \cong \Sigma_{R2}$
(2) $X_{R1} \cong X_{R2}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma_{R1} \approx^{O_{am}} X_{R1}$ *and* $\Sigma_{R2} \approx^{O_{am}} X_{R2}$
(4) $\Phi'_R \overset{\tau''}{\rightarrow}_R \Sigma'_{R1}$ *and* $\Phi''_R \overset{\tau''}{\rightarrow}_R \Sigma'_{R2}$

then there are instances X'_{R1}, X'_{R2} for the speculative semantics such that:

I $X_{R1} \overset{O}{\downarrow}{}^{R}_{\tau} X'_{R1}$ *and* $X_{R2} \overset{O}{\downarrow}{}^{R}_{\tau'} X'_{R2}$
II $\Sigma'_{R1} \cong \Sigma'_{R2}$
III $X'_{R1} \cong X'_{R2}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{R1} \approx^{O_{am}} X'_{R1}$ *and* $\Sigma'_{R2} \approx^{O_{am}} X'_{R2}$
V $\tau = \tau'$

Proof. The proof is very similar to Lemma 48 (S: Soundness Single Step AM). The only thing that is different is that (1) the specific oracle only mispredicts so there is one less case in the relation and (2) we have a different invariant for that specific oracle i.e., $INV2(\Sigma_R, X_R)$

For these reasons we will only argue why $INV2(\Sigma'_{R1}, X'_{R1})$ holds in the different cases and leave the rest to the old soundness proof.

Now we do case distinction on the instruction executed:

not ret instruction or ret instruction and $\mathbb{R}$ is empty This includes the rules Rule R:SE-NoBranch, Rule R:SE-Ret-Empty, Rule R:SE-Call-Full and Rule R:SE-Call. We prove that $INV2(\Sigma'_{R1}, X'_{R1})$ still holds. The proof for $INV2(\Sigma'_{R2}, X'_{R2})$ is analogous.

The proof is analogous to the corresponding case 'not store instruction' in Lemma 50 (Stronger Soundness for a specific oracle and for specific executions).

Rule R:AM-Ret-Spec We know that rule R:SE-Ret applies since it is a **ret** instruction. We have:

$$\begin{aligned} X'_{R1} =& X'''_R \cdot \Psi_R \\ minWndw(X'''_R) =& minWndw(decr(X'_R)) = minWndw(X'_R) - 1 \\ X'_R.\sigma \xrightarrow{\tau}& X'''_R.\sigma \\ \Sigma'_{R1} =& \Sigma'''_R \cdot \Phi_R \\ \Sigma'''_R.n =& \Sigma'_R.n - 1 \\ \Sigma'_R.\sigma \xrightarrow{\tau}& \Sigma'''_R.\sigma \end{aligned}$$

Note that the step $minWndw(decr(X'_R)) = minWndw(X'_R) - 1$ comes from the fact that $minWndw(X'_R) = \Sigma'_R.n$ and $\Sigma_R.n > 0$ by assumption.

Depending on the output of the oracle we switch the relation

$O(p, \sigma, h) = 0$ We need to show that $INV2(\Sigma'''_R, X'''_R)$ holds. The argument is the same as above for not **ret** instructions.

$O(p, \sigma, h) = \omega$ We need to show that $INV2(\Sigma'''_R \cdot \Phi_R, X'''_R \cdot \Phi_R)$ holds.

The case is analogous to the corresponding case (store misprediction) in Lemma 50 (Stronger Soundness for a specific oracle and for specific executions).

□

K PROOFS FOR COMBINED SEMANTICS

Note that for all the following combinations, we left the Oracle overapproximations proofs in these sections for the sake of completeness. These proofs are needed to show that the combination is SSS. Furthermore, for Symbolic Preservation of WFC directly follows from the fact that the source semantics we have fulfill the assumptions made in Appendix E.10 and thus we can reuse that proof generally for all combinations. A similar thing holds for Relation Preservation for all the source semantics.

First, let us state one of the main results.

Theorem 23 (Well-formed Composition $\lightning_{S+R}$). $\vdash \lightning_{S+R} : WFC$

Proof. Immediately follows from Lemma 83 (V45 AM: Confluence), Theorem 24 (V45: Relating V4 with projection of combined), Theorem 25 (V45: Relating V5 with projection of combined) and Lemma 98 (V45: Soundness Am semantics w.r.t. speculative semantics with new relation between states). □

Note that we need to require a form of alpha renaming for the speculative projection to the base parts. Since the combination speculates more than one of its parts, the *ctr* value is increased more and is out-of-sync with the base. So we cannot require that the traces are equivalent. But they are alpha equivalent up to renaming of the *ctr* values.
Consider the example trace (elliding some details):
See that the counters are now out of sync. But note that this is not problematic. It is only the renaming of the counters that is effected. If we would define an erase function on the traces that deletes the occurrences of the counter from start and rollback observations, then the traces would be equal again under the speculative projection (See the traces below for an example)
The important thing is, that the speculation happens in both semantics and the same steps were made.
Additionally, these *ctr* values are only used for us humans to make it more clear what happens. For the AM semantics we could leave them out, because we know that always the topmost speculation is finished first.

$$t_{v45} := \cdots \mathtt{start}_S\ i \ldots \mathtt{start}_R\ i+1 \mathtt{start}_R\ i+2 \cdots \mathtt{rlb}_R\ i+1 \cdot \mathtt{rlb}_S\ i \cdots \mathtt{start}_S\ i+3$$
$$t_{v4} := \ldots \mathtt{start}_S\ i \cdots \mathtt{rlb}_S\ i \cdots \mathtt{start}_S\ i+1$$
$$t_{v45}\restriction^S := \cdots \mathtt{start}_S\ i \cdot \mathtt{rlb}_S\ i \cdots \mathtt{start}_S\ i+3$$

If I take a step in the corresponding semantics and they were related before then You relate them on the speculative projection like you did for the non speculative semantics

We now describe a very important fact about our semantics, Namely that it is confluent.

Lemma 83 (V45 AM: Confluence)**.** *If*

(1) $\Sigma_{S+R} \overset{\tau}{\dashrightarrow}_{\lightning_{S+R}} \Sigma'_{S+R}$ *and*

(2) $\Sigma_{S+R} \overset{\tau}{\dashrightarrow}_{\lightning_{S+R}} \Sigma''_{S+R}$ *derived by a different rule*

Then

(1) $\Sigma'_{S+R} = \Sigma_{S+R}$

Proof. Note that a difference can only come from using Rule AM-v4-step-V45 for one derivation and Rule AM-v5-step-V45 for the other. Since these two rules delegate back to the semantics of V4 and V5, we look which two rules are applicable there.

Let us first look at the instructions and rule that could lead to two different rules to be applied:

store x, e, **call** f, **ret** Contradiction. There are no two different rules to derive the steps. This is because of the metaparameter Z introduced into the semantics.

spbarr Then either Rule S:AM-barr and Rule R:AM-barr or Rule S:AM-barr-spec and Rule R:AM-barr-spec are used to derive the steps (dependent on the value of n).

Here we talk about the case of Rule S:AM-barr and Rule R:AM-barr. The case for Rule S:AM-barr-spec and Rule R:AM-barr-spec is analogous.

Note that both Rule S:AM-barr and Rule R:AM-barr delegate back to the non-speculative semantics by $\sigma \xrightarrow{\tau} \sigma'$.

Since the starting state in both derivations is Σ_{S+R} and the non-speculative semantics is deterministic, we have that $\Sigma'_{S+R} = \Sigma''_{S+R}$.

otherwise Then Rule S:AM-NoBranch and Rule R:AM-NoBranch were used for different derivations.

But both of these rules delegate back to the non-speculative semantics with $\sigma \xrightarrow{\tau} \sigma'$.

By determinism of $\xrightarrow{\tau}$ and the fact that the starting state Σ_{S+R} is the same for both derivations, we have $\Sigma'_{S+R} = \Sigma''_{S+R}$.

□

K.1 Relating the semantics on their projections with combined.

Lemma 84 (V45: V4 Initial states are in Relation). *If*

(1) $\Sigma_S = \Sigma_S^{init} p, \sigma$ *and*

(2) $\Sigma_{S+R} = \Sigma_{S+R}^{init}(p, \sigma)$

Then

(1) $\Sigma_S \approx \Sigma_{S+R}$ *by Rule V45-V4:Single-Base.*

Proof. Follows from the definition of Σ_S^{init}, $\Sigma_{S+R}^{init}()$ and Rule V45-V4:Single-Base. □

Theorem 24 (V45: Relating V4 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh_S^{\mathcal{A}}(p) = Beh_{\mathcal{A}}^{S+R}(p)\restriction^S$.*

Proof. The proposition can be proven in similar fashion to Theorem 15 (S AM: Behaviour of non-speculative semantics and AM semantics). We prove the two directions separately:

⇐ Assume that $(p, \sigma) \Lightarrow_{S+R}^{\omega} \overline{\tau} \in Beh_{\mathcal{A}}^{S+R}(p)$.

By the definition of $Beh_{\mathcal{A}}^{S+R}(p)$ we have an initial configuration σ such that $(p, \sigma) \Lightarrow_{S+R}^{\omega} \overline{\tau}$.
The proof proceeds in similar fashion to the analogous case in Theorem 15 (S AM: Behaviour of non-speculative semantics and AM semantics) by using Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).
We can now conclude that $p, \sigma \Lightarrow_S^{\omega} \overline{\tau}\restriction^S \in Beh_S^{\mathcal{A}}(p)$ by Rule S:AM-Trace.

⇒ Assume that $(p, \sigma) \Lightarrow_S^{\omega} \overline{\tau} \in Beh_S^{\mathcal{A}}(p)$. We thus know there exists $\vdash \Sigma_S' : fin$ such that $\Sigma_S^{init} p, \sigma \Downarrow_S^{\overline{\tau}} \Sigma_S'$.

Let $\Sigma_S = \Sigma_S^{init} p, \sigma$ and $\Sigma_{S+R} = \Sigma_{S+R}^{init}(p, \sigma)$. By Lemma 84 we have $\Sigma_S \approx \Sigma_{S+R}$.
We can now We apply Lemma 88 (V45 AM: Completeness w.r.t V4 and projection) and get $\Sigma_{S+R} \Downarrow_{S+R}^{\overline{\tau}'} \Sigma_{S+R}'$ with
$\Sigma_S' \approx \Sigma_{S+R}'$ by Rule V45-V4:Single-Base and $\overline{\tau} = \overline{\tau}'\restriction^S$.
Because of $\vdash \Sigma_S' : fin$ and $\Sigma_S' \approx \Sigma_{S+R}'$, we know that $\vdash \Sigma_{S+R}' : fin$.
We thus have $(p, \sigma) \Lightarrow_{S+R}^{\omega} \overline{\tau}'\restriction^S \in Beh_{\mathcal{A}}^{S+R}(p)$.

□

> Note that Rule V45-V4:Single-Speculation-Start is used as a bridge between speculation and non-speculation. This is necessary because we delay the putput of a $\texttt{start}_R$ *id* observation using the genreal rule. So starting a speculation actually takes two turns, until it is visible in the trace. This is exactly what this state in the relatin is for.

$\boxed{\Sigma_S \approx \Sigma_{S+R}}$

$$\frac{}{\emptyset \approx \emptyset}\ (\text{V45-V4:Base}) \qquad \frac{\Sigma_S' \sim \Sigma_{S+R}'}{\Sigma_S' \cdot \langle p, ctr, \sigma, n\rangle \approx \Sigma_{S+R}' \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}\ (\text{V45-V4:Single-Base})$$

$$\frac{\Sigma_S \sim \Sigma_{S+R} \quad \Sigma_{S+R}'' \Downarrow_{S+R}^{\overline{\tau}} \Sigma_{S+R}''' \text{where transaction with id } ctr \text{ is rolled back} \quad \Sigma_S = \Sigma_S' \cdot \langle p, ctr', \sigma, n\rangle \quad \Sigma_{S+R} = \Sigma_{S+R}' \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle}{\Sigma_S' \cdot \langle p, ctr', \sigma, n\rangle \approx \Sigma_{S+R}' \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^{v5}_{\texttt{ret}\ l \cdot \texttt{start}\ ctr}}\ (\text{V45-V4:Single-Speculation-Start})$$

$$\frac{\Sigma_S \sim \Sigma_{S+R} \quad \Sigma_{S+R}'' \Downarrow_{S+R}^{\overline{\tau}} \Sigma_{S+R}''' \text{where transaction with id } ctr \text{ is rolled back} \quad \Sigma_S = \Sigma_S' \cdot \langle p, ctr', \sigma, n\rangle \quad \Sigma_{S+R} = \Sigma_{S+R}' \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle}{\Sigma_S' \cdot \langle p, ctr', \sigma, n\rangle \approx \Sigma_{S+R}' \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^{v5} \cdot \Sigma_{S+R1}}\ (\text{V45-V4:Single-Speculation-Diff})$$

$\boxed{\Sigma_S \sim \Sigma_{S+R}}$

$$\frac{}{\emptyset \sim \emptyset}\ (\text{V45-V4:Base}) \qquad \frac{|\Sigma_S'| = |\Sigma_{S+R}'| \quad \Sigma_S' \sim \Sigma_{S+R}'}{\Sigma_S' \cdot \langle p, ctr, \sigma, n\rangle \sim \Sigma_{S+R}' \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}\ (\text{V45-V4:Single})$$

Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics). *If*

(1) $\Sigma_S \approx \Sigma_{S+R}$ *and*

(2) $\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma'_{S+R}$

Then exists Σ_S *such that*

I $\Sigma'_S \approx \Sigma'_{S+R}$ *and*

II if $\Sigma'_S \approx \Sigma'_{S+R}$ *by Rule V45-V4:Single-Base then* $\Sigma_S \Downarrow^{\overline{\tau}\restriction^S}_S \Sigma'_S$ *and*

III if $\Sigma'_S \approx \Sigma'_{S+R}$ *by Rule V45-V4:Single-Speculation-Start then* $\Sigma_S \Downarrow^{\overline{\tau}\restriction^S}_S \Sigma'_S$ *and*

IV if $\Sigma'_S \approx \Sigma'_{S+R}$ *by Rule V45-V4:Single-Speculation-Diff* $\Sigma_S \Downarrow^{helpers_S(\overline{\tau},i)}_S \Sigma'_S$, *where* $i = ctr'$ *by unpacking* Σ'_{S+R} *according to Rule V45-V4:Single-Speculation-Diff*

Proof. By Induction on $\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma'_{S+R}$.

Rule AM-Reflection-V45 Then we have $\Sigma_{S+R} \Downarrow^{\varepsilon}_S \Sigma_{S+R}$ with $\Sigma'_{S+R} = \Sigma_{S+R}$ and by Rule AM-Reflection-V45 we have

I $\Sigma_S \Downarrow^{\varepsilon\restriction^S}_S \Sigma'_S$ with $\Sigma_S = \Sigma'_S$.

II $\Sigma_S \Downarrow^{helpers_S(\varepsilon,i)}_S \Sigma'_S$ with $\Sigma_S = \Sigma'_S$.

III $\Sigma'_S \approx \Sigma'_{S+R}$

Rule AM-Single-V45 We have $\Sigma_{S+R} \Downarrow^{\overline{\tau}''}_{S+R} \Sigma''_{S+R}$ with $\Sigma''_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Sigma'_{S+R}$.

We now apply IH on $\Sigma''_{S+R} \Downarrow^{\overline{\tau}''}_{S+R} \Sigma''_{S+R}$ and get

(a) $\Sigma''_S \approx \Sigma''_{S+R}$

(b) if $\Sigma''_S \approx \Sigma''_{S+R}$ by Rule V45-V4:Single-Base then $\Sigma_S \Downarrow^{\overline{\tau}\restriction^S}_S \Sigma''_S$ and

(c) if $\Sigma''_S \approx \Sigma''_{S+R}$ by Rule V45-V4:Single-Speculation-Start then $\Sigma_S \Downarrow^{\overline{\tau}\restriction^S}_S \Sigma''_S$ and

(d) if $\Sigma''_S \approx \Sigma''_{S+R}$ by Rule V45-V4:Single-Speculation-Diff then $\Sigma_S \Downarrow^{helpers_S(\overline{\tau},i)}_S \Sigma''_S$, where $j = ctr'$ by unpacking Σ''_{S+R} according to Rule V45-V4:Single-Speculation-Diff

We do a case distinction on $\approx$ in $\Sigma''_S \approx \Sigma''_{S+R}$:

Rule V45-V4:Single-Base We have

$$\begin{aligned}\Sigma_S \Downarrow^{\overline{\tau}\restriction^S}_S \Sigma''_S\\ \Sigma''_S = \Sigma'''_S \cdot \langle p, ctr, \sigma, n\rangle_{\overline{\rho}}\\ \Sigma''_{S+R} = \Sigma'''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle_{\overline{\rho}}\\ \Sigma'''_S \sim \Sigma'''_{S+R}\end{aligned}$$

We proceed by inversion on the derivation $\Sigma''_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Sigma'_{S+R}$.

Rule AM-v5-Rollback-V45 Since $\Sigma''_S \approx \Sigma''_{S+R}$ by Rule V45-V4:Single-Base, there cannot be a roll back of V5.

Rule AM-v4-Rollback-V45 By (b), it can only be roll back of V4 and only be the topmost state.

Furthermore, this means that $n = 0$.

Then $\Sigma''_S \overset{\mathtt{rlb}_S\ ctr}{\dashrightarrow}_S \Sigma'_S$ by Rule S:AM-Rollback, since n is equal between the two states.

Since $\Sigma'''_S \sim \Sigma'''_{S+R}$ and the fact that the rollback only changed the counter of Σ'''_S and Σ'''_{S+R} (and deleting the topmost state), we have $\Sigma'_S \approx \Sigma'_{S+R}$ by Rule V45-V4:Single-Base.

This means we need to show that $\overline{\tau} \cdot \tau'\restriction^S = \overline{\tau}\restriction^S \cdot \tau$.

Because the rollback observations is from V4, we have $\overline{\tau} \cdot \tau\restriction^S = \overline{\tau}\restriction^S \cdot \tau$ by definition of $\restriction^S$ and thus have $\Sigma_S \Downarrow^{\overline{\tau}\cdot\tau\restriction^S}_S \Sigma'_S$.

Rule AM-Context-V45 We have $\Phi_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}'_{S+R}$ and $n > 0$.

We now use inversion on $\Phi_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}_{S+R}$:

Rule AM-v4-step-V45 Then we have $\Phi_{S+R}\restriction^S = (\Phi_S, \mathbb{R})$ and $\Phi_S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_S$.

By relation $\approx$ we have that $\Sigma''_S = \overline{\Phi}_S \cdot \langle p, ctr', \sigma, n\rangle$ and $\Phi_S = \langle p, ctr', \sigma, n\rangle$.

Thus, Σ''_S can take the same step (in conjunction with Rule S:AM-Context) using $\overset{\tau'}{\dashrightarrow}_S$: $\Sigma''_S \overset{\tau'}{\dashrightarrow}_S \Sigma'_S$.

Since the same rule was used to derive the step and $\Sigma''_S \approx \Sigma''_{S+R}$ by Rule V45-V4:Single-Base, we have $\Sigma'_S \approx \Sigma'_{S+R}$ by Rule V45-V4:Single-Base.

This means we need to show that $\overline{\tau} \cdot \tau'\restriction^S = \overline{\tau}\restriction^S \cdot \tau$.

Since the same rule was used and the fact that $\Sigma''_S \approx \Sigma''_{S+R}$, we know that $\tau' = \tau$.

Since the rules of V4 cannot generate a $\mathtt{start}_R\ id$ or $\mathtt{rlb}_R\ id$ observation, we have $\overline{\tau} \cdot \tau\restriction^S = \overline{\tau}\restriction^S \cdot \tau$ by definition of $\restriction^S$.

This means we have $\Sigma_S \Downarrow^{\overline{\tau}\cdot\tau\restriction^S}_S \Sigma'_S$ as needed to show.

Rule AM-v5-step-V45 Then we have $\Phi_{S+R}\restriction^R \xRightarrow{\tau}_R \overline{\Phi}'_R$.

By inversion on $\Phi_{S+R}\restriction^R \xRightarrow{\tau}_R \overline{\Phi}'_R$ we get:

Rule R:AM-Ret-Spec We use Lemma 86 (V45: V4 step) and get $\Sigma''_S \xRightarrow{\tau\restriction^S}_S \Sigma'_S$ and $\Sigma'_S \approx \Sigma'_{S+R}$ by Rule V45-V4:Single-Speculation-Start, since Rule R:AM-Ret-Spec was used.
This means we need to show that $\overline{\tau}\cdot\tau\restriction^S = \overline{\tau}\restriction^S\cdot\tau$.
We know that $\tau\restriction^S = \tau$ and since τ is not a `start` *id* or `rlb` *id* observation, we have $\overline{\tau}\cdot\tau\restriction^S = \overline{\tau}\restriction^S\cdot\tau$.
This means we have $\Sigma_S \Downarrow_S^{\overline{\tau}\cdot\tau\restriction^S} \Sigma'_S$ as needed to show.

otherwise We use Lemma 86 (V45: V4 step) and get $\Sigma''_S \xRightarrow{\tau\restriction^S}_S \Sigma'_S$, $\tau\restriction^S = \tau$ and $\Sigma'_S \approx \Sigma'_{S+R}$ by Rule V45-V4:Single-Base, since Rule R:AM-Ret-Spec was not used.
This means we need to show that $\overline{\tau}\cdot\tau\restriction^S = \overline{\tau}\restriction^S\cdot\tau$.
We know that $\tau\restriction^S = \tau$ and have $\overline{\tau}\cdot\tau\restriction^S = \overline{\tau}\restriction^S\cdot\tau$ by definition of $\restriction^S$.
This means we have $\Sigma_S \Downarrow_S^{\overline{\tau}\cdot\tau\restriction^S} \Sigma'_S$ as needed to show.

Rule V45-V4:Single-Speculation-Start We have:

$$\begin{aligned}\Sigma_S \Downarrow_S^{\overline{\tau}\restriction^S} \Sigma''_S\\ \Sigma''_S = \Sigma'''_S \cdot \langle p, ctr, \sigma, n\rangle\\ \Sigma''_{S+R} = \Sigma'''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle_{\texttt{ret}\ l\cdot \texttt{start}_R\ ctr'}\\ \Sigma'''_S \cdot \langle p, ctr, \sigma, n\rangle \sim \Sigma'''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\end{aligned}$$

We now proceed by inversion on the derivation $\Sigma''_{S+R} \xRightarrow{\tau}_{S+R} \Sigma'_{S+R}$.
Rule AM-v4-Rollback-V45 Contradiction, because $\overline{\rho}$ is non-empty.
Rule AM-v5-Rollback-V45 Contradiction, because $\overline{\rho}$ is non-empty.
Rule AM-Context-V45 We have $\Phi_{S+R} \xRightarrow{\tau}_{S+R} \overline{\Phi}'_{S+R}$.

We now use inversion on $\Phi_{S+R} \xRightarrow{\tau}_{S+R} \overline{\Phi}_{S+R}$:
Rule AM-v4-step-V45 Contradiction, because $\overline{\rho}$ is non-empty and Rule S:AM-General does not work on $\texttt{start}_R$ *id* observations.
Rule AM-v5-step-V45 Then we have $\Phi_{S+R}\restriction^R \xRightarrow{\tau}_R \overline{\Phi}'_R$.

By inversion on $\Phi_{S+R}\restriction^R \xRightarrow{\tau}_R \overline{\Phi}'_R$ we get:
Rule R:AM-General By definition we have $\tau = \texttt{start}_R\ ctr$. Since Rule R:AM-General does not modify the state, we have $\Sigma'_{S+R} = \Sigma''_{S+R\texttt{ret}\ l}$.
Then we choose $\Sigma'_S = \Sigma''_S$ and derive the step $\Sigma''_S \Downarrow_S^{\varepsilon} \Sigma'_S$ by Rule S:AM-Reflection.
We now fulfill all premises for Rule V45-V4:Single-Speculation-Diff and have $\Sigma'_S \approx \Sigma'_{S+R}$.
We need to show that $\Sigma_S \Downarrow_S^{helpers_S(\overline{\tau}\cdot\tau, i)} \Sigma'_S$ holds.
We have:

$$\begin{aligned}&\overline{\tau}\restriction^S && \text{Definition } helpers_S()\\ &= helpers_S(\overline{\tau}\cdot \texttt{start}_R\ ctr', ctr') && \tau = \texttt{start}_R\ ctr'\\ &= helpers_S(\overline{\tau}\cdot\tau, i)\end{aligned}$$

and we have $\overline{\tau}\restriction^S$ by IH.
Since $\Sigma'_S = \Sigma''_S$ and IH $\Sigma_S \Downarrow_S^{\overline{\tau}\restriction^S} \Sigma''_S$, we have $\Sigma_S \Downarrow_S^{helpers_S(\overline{\tau}\cdot\tau)} \Sigma'_S$ as needed to show.

otherwise Contradiction, because $\overline{\rho}$ is non-empty.

Rule V45-V4:Single-Speculation-Diff We have

$$\begin{aligned}\Sigma_S \Downarrow_S^{helpers_S(\overline{\tau}, j)} \Sigma''_S\\ \Sigma''_S = \Sigma'''_S \cdot \langle p, ctr, \sigma, n\rangle\\ \Sigma''_{S+R} = \Sigma'''_{S+R} \cdot \langle p, ctr'', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr''', \sigma'', \mathbb{R}'', n''\rangle \cdot \Sigma^{\dagger}_{S+R}\\ \Sigma'''_S \cdot \langle p, ctr, \sigma, n\rangle \sim \Sigma'''_{S+R} \cdot \langle p, ctr'', \sigma, \mathbb{R}, n\rangle\\ j = ctr''\end{aligned}$$

Rule AM-v4-Rollback-V45 This means a transaction is rolled back that was created later than the transaction with $id = j$.
Then we choose $\Sigma'_S = \Sigma''_S$ and derive the step $\Sigma''_S \Downarrow^{\varepsilon}_S \Sigma'_S$ by Rule S:AM-Reflection.
Since the transaction with $id = j$ was not rolled back, it is still ongoing. Furthermore, only the topmost instance of Σ''_{S+R} did change.
Thus, $\Sigma'''_S \cdot \langle p, ctr, \sigma, n\rangle \sim \Sigma'''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle$ still holds and we fulfill all preconditions.
That is why $\Sigma'_S \approx \Sigma'_{S+R}$ by Rule V45-V4:Single-Speculation-Diff still holds.
Since the transactions of v5 is still ongoing, we have $helper_S(\overline{\tau} \cdot \texttt{rlb}_R\ id, j) = helper_S(\overline{\tau}, j)$.
By IH we have $\Sigma_S \Downarrow_S^{helper_S(\overline{\tau},j)} \Sigma''_S$.
Combined with $\Sigma''_S = \Sigma'_S$ we get $\Sigma_S \Downarrow_S^{helper_S(\overline{\tau},j)} \Sigma'_S$ and are finished.

Rule AM-v5-Rollback-V45 There are two cases depending on the id of the rolled back transaction:

$id \neq j$ This means a transaction is rolled back that was created later than the transaction with $id = j$.
The case is analogous to the case of Rule AM-v4-Rollback-V45 in Rule V45-V4:Single-Speculation-Diff.

$id = j$ Then we choose $\Sigma'_S = \Sigma''_S$ and derive the step $\Sigma''_S \Downarrow^{\varepsilon}_S \Sigma'_S$ by Rule S:AM-Reflection.
Since the transaction with $id = j$ was rolled back, we know that $\Sigma'_{S+R} = \Sigma'''_{S+R} \cdot \langle p, ctr''', \sigma, \mathbb{R}, n\rangle$.
Because only the ctr did change in the now topmost state of Σ'_{S+R}, we have $\Sigma'''_S \cdot \langle p, ctr, \sigma, n\rangle \sim \Sigma'''_{S+R} \cdot \langle p, ctr''', \sigma, \mathbb{R}, n\rangle$.
We thus have $\Sigma'_S \sim \Sigma'_{S+R}$ and can derive $\Sigma'_S \approx \Sigma'_{S+R}$ by Rule V45-V4:Single-Base.
For the trace, we get $\overline{\tau} \cdot \texttt{rlb}_R\ j \restriction^S = helper_S(\overline{\tau}, j)$ by definition of $\restriction^S$ and $id = j$.
Since by IH we know $\Sigma_S \Downarrow_S^{helper_S(\overline{\tau},j)} \Sigma''_S$ and by the fact that $\Sigma''_S = \Sigma'_S$ we are finished.

otherwise Then we choose $\Sigma'_S = \Sigma''_S$ and derive the step $\Sigma''_S \Downarrow^{\varepsilon}_S \Sigma'_S$ by Rule S:AM-Reflection since the transaction with $id = j$ is still ongoing.
The case is analogous to the case of Rule AM-v4-Rollback-V45 in Rule V45-V4:Single-Speculation-Diff.

□

Notice here, that there is a difference in the semantics of its parts of the combined, because of the meta parameter Z that influences the no Branching rule.
This is where the difference comes from.
Furthermore, these proofs are repeatable for each version, because the uderlzing semantics just uses the no Branching rule, which is always there.

Lemma 86 (V45: V4 step)**.** *If*

(1) $\Sigma_S \approx \Sigma_{S+R}$ *by Rule V45-V4:Single-Base and*
(2) $\Sigma_{S+R} = \overline{\Phi}_{S+R} \cdot \Phi_{S+R}$ *and* $\Sigma'_{S+R} = \overline{\Phi}_{S+R} \cdot \overline{\Phi}'_{S+R}$ *and*
(3) $\Phi_{S+R} \restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_R$ *and*

Then

(1) $\Sigma_S \overset{\tau\restriction^S}{\dashrightarrow}_S \Sigma'_S$ *and*
(2) if the step was not derived by Rule R:AM-Ret-Spec then $\Sigma'_S \approx \Sigma'_{S+R}$ *by Rule V45-V4:Single-Base and*
(3) if the step was derived by Rule R:AM-Ret-Spec then $\Sigma'_S \approx \Sigma'_{S+R}$ *by Rule V45-V4:Single-Speculation-Start*

Proof. We have by $\approx$:

$$\begin{aligned}\Sigma_S &= \Sigma''_S \cdot \langle p, ctr, \sigma, n\rangle\\ \Sigma_{S+R} &= \Sigma''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\\ \Sigma''_S &\sim \Sigma''_{S+R}\end{aligned}$$

We proceed by inversion on $\Phi_{S+R} \restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_R$:

Rule R:AM-Ret-Spec Then we use Rule S:AM-NoBranch to derive a step $\Sigma_S \overset{\tau}{\dashrightarrow}_S \Sigma'_S$.
Since Rule R:AM-Ret-Spec creates a new instance that is used for speculation but updates the state below correctly using the non-speculative semantics $\Sigma_{S+R}.\sigma \xrightarrow{\tau} \sigma'$, we have $\Sigma'_{S+R} = \overline{\Phi}_{S+R} \cdot \langle p, ctr, \sigma', \mathbb{R}', n\rangle \cdot \langle p, ctr+1, \sigma'', \mathbb{R}', n'\rangle_{\texttt{ret}\ l \cdot \texttt{start}_R\ ctr \cdot}$
Since Rule S:AM-NoBranch was used, we have $\Sigma'_S.\sigma \xrightarrow{\tau'} \sigma''$.

By Rule V45-V4:Single-Base we know that $\Sigma_S.\sigma = \Sigma_{S+R}.\sigma$ and thus $\tau = \tau'$ and $\sigma' = \sigma''$ by determinism of the non-speculative semantics.
We thus have that $\overline{\Phi}_{S+R} \cdot \langle p, ctr, \sigma', \mathbb{R}', n\rangle \sim \Sigma'_S$ (the speculation window n was changed in the same way) and can relate $\Sigma'_S \approx \Sigma'_{S+R}$ by Rule V45-V4:Single-Speculation-Start.
Furthermore, $\tau\restriction^S = \tau$ by definition of $\restriction^S$.

Rule R:AM-barr or Rule R:AM-barr-spec or Rule R:AM-NoBranch We do the case for Rule R:AM-barr. The case for Rule R:AM-barr-spec and Rule R:AM-NoBranch is analogous.
By Lemma 83 (V45 AM: Confluence) we know that Rule S:AM-barr could have been used as well.
Since $\Sigma_S \approx \Sigma_{S+R}$ by Rule V45-V4:Single-Base, we know that Rule S:AM-barr applies.
We thus derive $\Sigma_S \overset{\tau}{\Rightarrow}_S \Sigma'_S$ by Rule S:AM-barr.
Because of confluence, we know that Rule S:AM-barr and Rule R:AM-barr change the state in the same way.
Thus, $\Sigma'_S \approx \Sigma'_{S+R}$ holds by Rule V45-V4:Single-Base and the same observation was generated.
Furthermore $\tau\restriction^S = \tau$ by definition of $\restriction^S$.

Rule R:AM-General Contradiction. This means that $\Sigma_{S+R}.\overline{\rho}$ either contains a $\texttt{start}_R$ *id* or a $\texttt{ret}$ *l* observation.
But then by $\Sigma_S \approx \Sigma_{S+R}$ we have that $\Sigma_S.\overline{\rho}$ contains one of these observations as well.
This is impossible, because they cannot be generated according to $\Rightarrow_S$, contradicting the assumption that $\Sigma_S \approx \Sigma_{S+R}$.

otherwise This includes the rules: Rule R:AM-Call-Full, Rule R:AM-Ret-Empty, Rule R:AM-Ret-Same and Rule R:AM-Call.
We do the proof for Rule R:AM-Call-Full. The proof for the other rules is analogous.
Then we use Rule S:AM-NoBranch to derive a step $\Sigma_S \overset{\tau}{\Rightarrow}_S \Sigma'_S$.
Because both Rule S:AM-NoBranch and Rule R:AM-Call-Full delegate back to the non-speculative semantics and we know that $\Sigma_S.\sigma = \Sigma_{S+R}.\sigma$, we know that the same rule in the non-speculative semantics was used.
Since the non-speculative semantics is deterministic, we know that the same configuration σ' is reached for both derivations. and the same observation τ is generated in both as well.
We thus have $\Sigma'_S \approx \Sigma'_{S+R}$ by Rule V45-V4:Single-Base.
Furthermore $\tau\restriction^S = \tau$ by definition of $\restriction^S$.

□

Lemma 87 (V45: V5 step)**.** *If*

(1) $\Sigma_R \approx \Sigma_{S+R}$ *by Rule V45-V5:Single-Base and*
(2) $\Sigma_{S+R} = \overline{\Phi}_{S+R} \cdot \Phi_{S+R}$ *and* $\Sigma'_{S+R} = \overline{\Phi}_{S+R} \cdot \overline{\Phi}'_{S+R}$ *and*
(3) $\Phi_{S+R}\restriction^S \overset{\tau}{\Rightarrow}_S \overline{\Phi}'_S$ *and*

Then

(1) $\Sigma_R \overset{\tau\restriction^R}{\Rightarrow}_R \Sigma'_R$ *and*
(2) if the step was not derived by Rule S:AM-Store-Spec then $\Sigma'_R \approx \Sigma'_{S+R}$ *by Rule V45-V5:Single-Base and*
(3) if the step was derived by Rule S:AM-Store-Spec then $\Sigma'_R \approx \Sigma'_{S+R}$ *by Rule V45-V5:Single-Transaction-Start*

Proof. We have by $\approx$:

$$\begin{aligned}\Sigma_R &= \Sigma''_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle\\ \Sigma_{S+R} &= \Sigma''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\\ \Sigma''_R &\sim \Sigma''_{S+R}\end{aligned}$$

We proceed by inversion on $\Phi_{S+R}\restriction^S \overset{\tau}{\Rightarrow}_S \overline{\Phi}'_R$:

Rule S:AM-Store-Spec Then we use Rule R:AM-NoBranch to derive a step $\Sigma_R \overset{\tau}{\Rightarrow}_R \Sigma'_R$.
The case is analogous to the corresponding case of Rule R:AM-Ret-Spec in Lemma 86 (V45: V4 step).

otherwise This includes Rule S:AM-barr or Rule S:AM-barr-spec or Rule S:AM-NoBranch.
We do the case for Rule S:AM-barr. The case for Rule S:AM-barr-spec and Rule S:AM-NoBranch is analogous.
The case is analogous to the corresponding case in Lemma 86 (V45: V4 step).

□

Completeness

Lemma 88 (V45 AM: Completeness w.r.t V4 and projection)**.** *If*

(1) $\Sigma_S \approx \Sigma_{S+R}$ *by Rule V45-V4:Single-Base and*
(2) $\Sigma_S \Downarrow^{\overline{\tau}}_S \Sigma'_S$

Then exists Σ'_{S+R} *such that*

I $\Sigma'_S \approx \Sigma'_{S+R}$ *by Rule V45-V4:Single-Base and*
II $\Sigma_{S+R} \Downarrow^{\overline{\tau}'}_{S+R} \Sigma'_{S+R}$ *and*
III $\overline{\tau} = \overline{\tau}' \restriction^S$

Proof. We proceed by induction on $\Sigma_S \Downarrow^{\overline{\tau}}_S \Sigma'_S$:

Rule S:AM-Reflection By Rule S:AM-Reflection we have $\Sigma_S \Downarrow^{\varepsilon}_S \Sigma_S$. with $\Sigma_S = \Sigma'_S$.

I - III We derive $\Sigma_{S+R} \Downarrow^{\overline{\tau}'}_{S+R} \Sigma'_{S+R}$ by Rule AM-Reflection-V45 and thus $\Sigma_{S+R} = \Sigma'_{S+R}$.
By construction and 1) we have $\Sigma'_S \approx \Sigma'_{S+R}$ by Rule V45-V4:Single-Base.
Since $\varepsilon \restriction^S = \varepsilon$ we are finished.

Rule S:AM-Single Then we have $\Sigma_S \Downarrow^{\overline{\tau}}_S \Sigma''_S$ and $\Sigma''_S \overset{\tau}{\rightsquigarrow}_S \Sigma'_S$.
We need to show
I $\Sigma_{S+R} \Downarrow^{\overline{\tau}' \cdot \tau'}_S \Sigma'_{S+R}$ and
II $\Sigma'_S \approx \Sigma'_{S+R}$ by Rule V45-V4:Single-Base and
III $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \restriction^S$
We apply the IH on $\Sigma_S \Downarrow^{\overline{\tau}}_S \Sigma''_S$ we get
I' $\Sigma_{S+R} \Downarrow^{\overline{\tau}'}_S \Sigma''_{S+R\rho}$ and
II' $\Sigma''_S \approx \Sigma''_{S+R}$ by Rule V45-V4:Single-Base and
IV' $\overline{\tau} = \overline{\tau}' \restriction^S$
By Rule V45-V4:Single-Base we have:

$$\begin{aligned}\Sigma''_S &= \Sigma'''_S \cdot \langle p, ctr, \sigma, n\rangle\\ \Sigma''_{S+R} &= \Sigma'''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\\ \Sigma'''_S &\sim \Sigma'''_{S+R}\end{aligned}$$

We continue by inversion on $\Sigma''_S \overset{\tau}{\rightsquigarrow}_S \Sigma'_S$:
Rule S:AM-Rollback Then $n = 0$ and $\Sigma'_S = \Sigma'''_S$ except that the *ctr* was updated: $\Sigma'_S.ctr = ctr$.

Since n = 0 and $\Sigma''_S \approx \Sigma''_{S+R}$ we can apply Rule AM-v4-Rollback-V45 and get $\Sigma''_{S+R} \overset{\tau'}{\rightsquigarrow}_{S+R} \Sigma'_{S+R}$ with $\Sigma'_{S+R} = \Sigma'''_{S+R}$, where $\Sigma'_{S+R}.ctr = ctr'$.
Since the *ctr* value does not influence $\sim$, we have $\Sigma'_S \sim \Sigma'_{S+R}$ and can conclude $\Sigma'_S \approx \Sigma'_{S+R}$ by Rule V45-V4:Single-Base.
Next, we need to show that $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \restriction^S$.
We have $\tau \restriction^S = \tau$ by definition of $\restriction^S$ and the fact that $\tau' = \texttt{rlb}_S\ ctr$.
This means we have:

$$\begin{aligned}&\overline{\tau}' \cdot \tau \restriction^S \text{ Definition } \restriction^S\\ &= \overline{\tau}' \restriction^S \cdot \tau' \text{ by IH}\\ &= \overline{\tau} \cdot \tau' \ \tau = \tau'\\ &= \overline{\tau} \cdot \tau\end{aligned}$$

and we are finished.

Rule S:AM-Context We then have $\langle p, ctr, \sigma, n\rangle \overset{\tau}{\rightsquigarrow}_S \overline{\Phi}'_S$ and $n > 0$.

By $\Sigma''_S \approx \Sigma''_{S+R}$ we know that Rule AM-Context-V45 applies for the step $\Sigma''_{S+R} \overset{\tau'}{\rightsquigarrow}_{S+R} \Sigma'_{S+R}$ as well.

We now need to find a derivation for the step $\langle p, ctr', \sigma, \mathbb{R}, n\rangle \overset{\tau'}{\rightsquigarrow}_{S+R} \overline{\Phi}'_{S+R}$ according to Rule AM-Context-V45.

We proceed by inversion on $\langle p, ctr, \sigma, n\rangle \overset{\tau}{\rightsquigarrow}_S \overline{\Phi}'_S$:

Rule S:AM-NoBranch We get $\langle p, ctr, \sigma, n\rangle \overset{\tau}{\rightsquigarrow}_S \overline{\Phi}'_S$ by $\sigma \xrightarrow{\tau} \sigma'$.
Furthermore, $\Sigma'_S.n = n - 1$.
We now do a case analysis on the instruction $p(\sigma(\mathbf{pc}))$:
$p(\sigma(\mathbf{pc})) =$ **ret and** $\mathbb{R}$ **is non-empty and** $\mathbb{R}$ **value is different to return address** Then, a speculative transaction of V5 with *id* is started using Rule R:AM-Ret-Spec through Rule AM-v5-step-V45 and a new instance Φ'_{S+R} was pushed on top of the stack of Σ''_{S+R}.

Furthermore, the instance below the newly created state was updated correctly using $\sigma \xrightarrow{\tau'} \sigma'$ and reduced their speculation window by 1.
The state now consists of $\Sigma'''_{S+R} \cdot \langle p, ctr', \sigma', \mathbb{R}', n-1\rangle \cdot \Phi'_{S+R}$.
Since every transaction is rolled back at some point, we know that there exists Σ'_{S+R} such that $\Sigma''_{S+R} \Downarrow^{\tau \cdot \texttt{start}\ id \cdot \overline{\tau}'' \cdot \texttt{rlb}\ id}_{S+R} \Sigma'_{S+R}$ and the last rule that was used was Rule AM-v5-Rollback-V45.
Because during the execution of the speculative transaction with id id, only the topmost state is changed, we know that the correctly updated state was not changed.
Since the roll back deleted the topmost state, the correctly updated one is now at the top again.
This means that $\Sigma'_S \approx \Sigma'_{S+R}$ by Rule V45-V4:Single-Base by determinism of the non-speculative semantics.
Next, we need to show that $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \cdot \texttt{start}_R\ id \cdot \overline{\tau}'' \cdot \texttt{rlb}_R\ id \restriction^S$.
Notice that $\tau' \cdot \texttt{start}_R\ id \cdot \overline{\tau}'' \cdot \texttt{rlb}_R\ id \restriction^S = \tau' \restriction^S = \tau'$ by definition of $\restriction^S$ and the fact that $\Sigma''_{S+R} \approx \Sigma''_S$.
This means we have:

$$\begin{aligned}
&\overline{\tau}' \cdot \tau' \cdot \texttt{start}_R\ id \cdot \overline{\tau}'' \cdot \texttt{rlb}_R\ id \restriction^S \\
&= \overline{\tau}' \cdot \tau' \restriction^S \text{ Definition } \restriction^S \\
&= \overline{\tau}' \restriction^S \cdot \tau'\ \tau = \tau' \text{ and IH} \\
&= \overline{\tau} \cdot \tau
\end{aligned}$$

and we are finished.

$p(\sigma(\mathbf{pc}))$ = **ret and $\mathbb{R}$ is empty or $\mathbb{R}$ is not different to return address** Since $n > 0$, the state can do a step using either Rule R:AM-Ret-Empty or Rule R:AM-Ret-Same through Rule AM-v5-step-V45 (Note that the meta parameter Z restricts the V4 semantics in the combined part).
The rules delegate back to the non-speculative semantics to do the step: $\sigma \xrightarrow{\tau'} \sigma'$. and reduces n by 1.
This gives us $\Sigma''_{S+R} \overset{\tau'}{=\!\!\not\Rightarrow}_{S+R} \Sigma'_{S+R}$.
From the determinism of the non-speculative semantics and $\Sigma''_S \approx \Sigma''_{S+R}$ we can conclude that $\Sigma'_S \approx \Sigma'_{S+R}$ by Rule V45-V4:Single-Base.
Next, we need to show that $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \restriction^S$.
Since the observation τ' was generated by the non-speculative semantics and there is no ongoing transaction of V5 (because $\Sigma'_S \approx \Sigma'_{S+R}$) we have $\tau' \restriction^S = \tau$.
Furthermore, by determinism of $\rightarrow$ we have $\tau' = \tau$. This means we have:

$$\begin{aligned}
&\overline{\tau}' \cdot \tau \restriction^S \text{ Definition } \restriction^S \\
&= \overline{\tau}' \restriction^S \cdot \tau' \text{ by IH} \\
&= \overline{\tau} \cdot \tau'\ \tau = \tau' \\
&= \overline{\tau} \cdot \tau
\end{aligned}$$

and we are finished.

$p(\sigma(\mathbf{pc}))$ = **call** f Since $n > 0$, the state can do a step using either Rule R:AM-Call or Rule R:AM-Call-Full through Rule AM-v5-step-V45. (Note that the meta parameter Z restricts the V4 semantics in the combined part).
Both of these rules delegate back to the non-speculative semantics to do the step: $\sigma \xrightarrow{\tau'} \sigma'$ and reduces n by 1.
The rest is analogous to the case above.

otherwise Then we can either use Rule R:AM-NoBranch through Rule AM-v5-step-V45 or Rule S:AM-NoBranch through Rule AM-v4-step-V45.
Because of Lemma 83 (V45 AM: Confluence), we know that it does not matter which rule we use, which means we can use the same rule as for v4 do derive the step.
This gives us $\Sigma''_{S+R} \overset{\tau'}{=\!\!\not\Rightarrow}_{S+R} \Sigma'_{S+R}$.
Since the same rule was used, we have $\tau = \tau'$ and $\Sigma'_S \approx \Sigma'_{S+R}$ by Rule V45-V4:Single-Base.
Furthermore, since the observation τ was generated by the non-speculative semantics and there is no ongoing transaction of V5 (because $\Sigma'_S \approx \Sigma'_{S+R}$) we have $\tau' \restriction^S = \tau'$.

This means we have

$$\begin{aligned} &\overline{\tau}' \cdot \tau \restriction^S && \text{Definition } \restriction^S \\ &= \overline{\tau}' \restriction^S \cdot \tau' && \text{by IH} \\ &= \overline{\tau} \cdot \tau' && \tau = \tau' \\ &= \overline{\tau} \cdot \tau \end{aligned}$$

and we are finished.

otherwise These rules include Rule S:AM-barr, Rule S:AM-barr-spec, Rule S:AM-General and Rule S:AM-Store-Spec. Since the rules of V4 are included in the combined semantics and $\Sigma_S \approx \Sigma_{S+R}$, we can use the corresponding rule in the combined semantics by Confluence or delegate back to V4 by Rule AM-v4-step-V45.
This means we can always do the same step in the combined as in the V4 semantics.

□

K.2 Combination V45 and projection to V5

Theorem 25 (V45: Relating V5 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\mathcal{A}}_{R}(p) = Beh^{S+R}_{\mathcal{A}}(p)\restriction^R$.*

Proof. The proposition can be proven in similar fashion to Theorem 24 (V45: Relating V4 with projection of combined). We prove the two directions separately:

⇐ Assume that $(p,\sigma) \overset{\omega}{\underset{S+R}{\frown}} \overline{\tau} \in Beh^{S+R}_{\mathcal{A}}(p)$.

By the definition of $Beh^{S+R}_{\mathcal{A}}(p)$ we have an initial state $\Sigma_{S+R} = \Sigma^{init}_{S+R}(p,\sigma)$ such that $(p,\sigma) \overset{\omega}{\underset{S+R}{\frown}} \overline{\tau}$.
The proof proceeds in similar fashion to the analogous case in Theorem 24 (V45: Relating V4 with projection of combined) by using Lemma 89 (V45: Soundness of the AM speculative semantics w.r.t. AM v5 semantics).
We can now conclude that $(p,\sigma) \overset{\omega}{\underset{R}{\frown}} \overline{\tau}\restriction^R \in Beh^{\mathcal{A}}_{R}(p)$ by Rule R:AM-Trace.

⇒ Assume that $(p,\sigma) \overset{\omega}{\underset{R}{\frown}} \overline{\tau} \in Beh^{\mathcal{A}}_{R}(p)$. We thus know there exists $\vdash \Sigma'_R : fin$ such that $\Sigma^{init}_R p, \sigma \Downarrow^{\overline{\tau}}_R \Sigma'_R$.

The proof proceeds in the same way as the corresponding case in Theorem 24 (V45: Relating V4 with projection of combined) by using Lemma 90 (V45 AM: Completeness w.r.t V5 and projection).
We thus have $(p,\sigma) \overset{\omega}{\underset{S+R}{\frown}} \overline{\tau}' \in Beh^{S+R}_{\mathcal{A}}(p)$ with $\overline{\tau}'\restriction^R = \overline{\tau}$.

□

$\boxed{\Sigma_R \approx \Sigma_{S+R}}$

$$\frac{}{\varnothing \approx \varnothing}\ \text{(V45-V5:Base)} \qquad \frac{|\Sigma'_S| = |X'_S| \quad \Sigma'_R \sim \Sigma'_{S+R}}{\Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle^b \approx \Sigma'_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle^b}\ \text{(V45-V5:Single-Base)}$$

$$\frac{\Sigma_R \sim \Sigma_{S+R} \quad n' \geq 0 \quad \Sigma''_S \Downarrow^{\overline{\tau}}_S \Sigma'''_S \text{where transaction with id } ctr \text{ is rolled back} \quad \Sigma_R = \Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \quad \Sigma_{S+R} = \Sigma'_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}{\Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \approx \Sigma'_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^{false}_{\texttt{bypass}\ n \cdot \texttt{start}_S\ ctr}}\ \text{(V45-V5:Single-Transaction-Start)}$$

$$\frac{\Sigma_R \sim \Sigma_{S+R} \quad n' \geq 0 \quad \Sigma''_S \Downarrow^{\overline{\tau}}_S \Sigma'''_S \text{where transaction with id } ctr \text{ is rolled back} \quad \Sigma_R = \Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \quad \Sigma_{S+R} = \Sigma'_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}{\Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \approx \Sigma'_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^{false} \cdot \Sigma_{S+R1}}\ \text{(V45-V5:Single-Transaction-Rollback)}$$

$\boxed{\Sigma_R \sim \Sigma_{S+R}}$

$$\frac{}{\varnothing \sim \varnothing}\ \text{(V45-V5:Base)} \qquad \frac{|\Sigma'_R| = |\Sigma'_{S+R}| \quad \Sigma'_R \sim \Sigma'_{S+R}}{\Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \sim \Sigma'_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}\ \text{(V45-V5:Single)}$$

Lemma 89 (V45: Soundness of the AM speculative semantics w.r.t. AM v5 semantics)**.** *If*

(1) $\Sigma_R \approx \Sigma_{S+R}$ *and*
(2) $\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma'_{S+R}$

Then exists Σ'_R *such that*

I $\Sigma'_R \approx \Sigma'_{S+R}$ *and*

II if $\Sigma'_R \approx \Sigma'_{S+R}$ *by Rule V45-V5:Single-Base then* $\Sigma_R \Downarrow_R^{\overline{\tau}\restriction^R} \Sigma'_R$ *and*

III if $\Sigma'_R \approx \Sigma'_{S+R}$ *by Rule V45-V5:Single-Transaction-Start then* $\Sigma_R \Downarrow_R^{\overline{\tau}\restriction^R} \Sigma'_R$ *and*

IV if $\Sigma'_R \approx \Sigma'_{S+R}$ *by Rule V45-V5:Single-Transaction-Rollback* $\Sigma_R \Downarrow_R^{helper_R(\overline{\tau},i)} \Sigma'_R$*, where* $i = ctr'$ *by unpacking* Σ'_{S+R} *according to Rule V45-V5:Single-Transaction-Rollback.*

Proof. By Induction on $\Sigma_{S+R} \Downarrow_{S+R}^{\overline{\tau}} \Sigma'_{S+R}$.

Rule AM-Reflection-V45 Then we have $\Sigma_{S+R} \Downarrow_{S+R}^{\varepsilon} \Sigma_{S+R}$ with $\Sigma'_{S+R} = \Sigma_{S+R}$ and by Rule AM-Reflection-V45 we have

I $\Sigma'_R \approx \Sigma'_{S+R}$

II $\Sigma_R \Downarrow_R^{\varepsilon\restriction^R} \Sigma'_R$ with $\Sigma_R = \Sigma'_R$.

III $\Sigma_R \Downarrow_R^{helper_R(\varepsilon,i)} \Sigma'_R$ with $\Sigma_S = \Sigma'_R$.

Note, that the initial relation $\Sigma_R \approx \Sigma_{S+R}$ does not change.

Rule AM-Single-V45 We have $\Sigma_{S+R} \Downarrow_{S+R}^{\overline{\tau}''} \Sigma''_{S+R}$ with $\Sigma''_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Sigma'_{S+R}$.

We now apply IH on $\Sigma''_{S+R} \Downarrow_{S+R}^{\overline{\tau}''} \Sigma''_{S+R}$ and get

(a) $\Sigma''_S \approx \Sigma''_{S+R}$

(b) if $\Sigma''_R \approx \Sigma''_{S+R}$ by Rule V45-V5:Single-Base then $\Sigma_R \Downarrow_S^{\overline{\tau}\restriction^R} \Sigma''_R$ and

(c) if $\Sigma''_R \approx \Sigma''_{S+R}$ by Rule V45-V5:Single-Transaction-Start then $\Sigma_R \Downarrow_R^{\overline{\tau}\restriction^R} \Sigma''_R$ and

(d) if $\Sigma''_R \approx \Sigma''_{S+R}$ by Rule V45-V5:Single-Transaction-Rollback $\Sigma_R \Downarrow_S^{helper_R(\overline{\tau},j)} \Sigma''_R$, where $j = ctr'$ by unpacking Σ''_{S+R} according to Rule V45-V5:Single-Transaction-Rollback

We do a case distinction on $\approx$ in $\Sigma''_R \approx \Sigma''_{S+R}$:

Rule V45-V5:Single-Base We have

$$\begin{gathered}\Sigma_R \Downarrow_S^{\overline{\tau}\restriction^R} \Sigma''_R \\ \Sigma''_R = \Sigma'''_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle_{\overline{\rho}} \\ \Sigma''_{S+R} = \Sigma'''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle_{\overline{\rho}} \\ \Sigma'''_R \sim \Sigma'''_{S+R}\end{gathered}$$

We now proceed by inversion on the derivation $\Sigma''_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Sigma'_{S+R}$:

Rule AM-v5-Rollback-V45 By (b), it can only be roll back of V5 and only be the topmost state.

Furthermore, this means that $n = 0$.

Then $\Sigma''_R \overset{\mathtt{rlb}_R\ ctr}{\dashrightarrow}_R \Sigma'_R$ by Rule R:AM-Rollback, since n is equal between the two states. The rest of the case is analogous to Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

Rule AM-v4-Rollback-V45 Since $\Sigma''_R \approx \Sigma''_{S+R}$ by Rule V45-V5:Single-Base, there cannot be a roll back of V4.

Rule AM-Context-V45 We have $\Phi_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}'_{S+R}$.

We now use inversion on $\Phi_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}_{S+R}$:

Rule AM-v4-step-V45 Then we have $\Phi_{S+R}\restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_S$.

By inversion on $\Phi_{S+R}\restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_S$ we get:

Rule S:AM-Store-Spec The case is analogous to the corresponding case Rule AM-v5-step-V45 Rule R:AM-Ret-Spec in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) using Lemma 87 (V45: V5 step) and the fact that Rule S:AM-Store-Spec was used.

otherwise The case is analogous to the corresponding case Rule AM-v5-step-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) using Lemma 87 (V45: V5 step) and the fact that Rule S:AM-Store-Spec was not used.

Rule AM-v5-step-V45 Then we have $\Phi_{S+R}\restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_R$.

The case is analogous to the corresponding case Rule AM-v4-step-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) combined with the fact that the rules of V4 cannot generate a $\mathtt{start}_R$ *id* or $\mathtt{rlb}_R$ *id* observation.

Rule V45-V5:Single-Transaction-Start We have:

$$\begin{aligned}\Sigma_R \Downarrow_R^{\overline{\tau}\restriction^R} \Sigma_R''\\ \Sigma_R'' =& \Sigma_R''' \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle\\ \Sigma_{S+R}'' =& \Sigma_{S+R}''' \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle_{\texttt{bypass}\ n\cdot \texttt{start}_S\ ctr'}\\ \Sigma_R''' \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \sim& \Sigma_{S+R}''' \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\end{aligned}$$

We now proceed by inversion on the derivation $\Sigma_{S+R}'' \overset{\tau}{\rightsquigarrow}_{S+R} \Sigma_{S+R}'$.

Rule AM-v4-Rollback-V45 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v5-Rollback-V45 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-Context-V45 We have $\Phi_{S+R} \overset{\tau}{\rightsquigarrow}_{S+R} \overline{\Phi}_{S+R}'$.

We now use inversion on $\Phi_{S+R} \overset{\tau}{\rightsquigarrow}_{S+R} \overline{\Phi}_{S+R}$:

Rule AM-v4-step-V45 Then we have $\Phi_{S+R}\restriction^S \overset{\tau}{\rightsquigarrow}_S \overline{\Phi}_R'$.

By inversion on $\Phi_{S+R}\restriction^S \overset{\tau}{\rightsquigarrow}_S \overline{\Phi}_S'$ we get:

Rule S:AM-General By definition we have $\tau = \texttt{start}_S\ ctr'$. Since Rule S:AM-General does not modify the state, we have $\Sigma_{S+R}' = \Sigma_{S+R\texttt{bypass}\ n}''$.

Then we choose $\Sigma_R' = \Sigma_R''$ and derive the step $\Sigma_R'' \Downarrow_R^{\varepsilon} \Sigma_R'$ by Rule R:AM-Reflection.

We now fulfill all premises for Rule V45-V5:Single-Transaction-Rollback and have $\Sigma_R' \approx \Sigma_{S+R}'$.

We need to show that $\Sigma_R \Downarrow_R^{helper_R(\overline{\tau}\cdot\tau, ctr')} \Sigma_R'$ holds.

We have:

$$\begin{aligned}&\overline{\tau}\restriction^R && \text{Definition } helper_R()\\ =&helper_R(\overline{\tau}\cdot \texttt{start}_S\ ctr', ctr') && \tau = \texttt{start}_S\ ctr'\\ =&helper_R(\overline{\tau}\cdot\tau, ctr')\end{aligned}$$

and we have $\overline{\tau}\restriction^R$ by IH.

Since $\Sigma_R' = \Sigma_R''$ and IH $\Sigma_R \Downarrow_R^{\overline{\tau}\restriction^R} \Sigma_R''$, we have $\Sigma_R \Downarrow_R^{helper_R(\overline{\tau}\cdot\tau, ctr')} \Sigma_R'$ as needed to show.

otherwise Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v5-step-V45 Contradiction, because $\overline{\rho}$ is non-empty and Rule R:AM-General does not work on $\texttt{start}_S\ id$ observations.

Rule V45-V5:Single-Transaction-Rollback We have:

$$\begin{aligned}\Sigma_R \Downarrow_S^{helper_R(\overline{\tau}, j)} \Sigma_R''\\ \Sigma_R'' =& \Sigma_R''' \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle\\ \Sigma_{S+R}'' =& \Sigma_{S+R}''' \cdot \langle p, ctr'', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr''', \sigma'', \mathbb{R}'', n''\rangle \cdot \Sigma_{S+R}^{\dagger}\\ \Sigma_R''' \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \sim& \Sigma_{S+R}''' \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\\ j =& ctr'\end{aligned}$$

We now proceed by inversion on the derivation $\Sigma_{S+R}'' \overset{\tau}{\rightsquigarrow}_{S+R} \Sigma_{S+R}'$:

Rule AM-v5-Rollback-V45 This means a transaction is rolled back that was created later than the transaction with $id = j$.

Then we choose $\Sigma_R' = \Sigma_R''$ and derive the step $\Sigma_R'' \Downarrow_R^{\varepsilon} \Sigma_R'$ by Rule R:AM-Reflection.

The case is analogous to the corresponding case in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

Rule AM-v4-Rollback-V45 There are two cases depending on the id of the rolled back transaction:

$id \neq j$ This means a transaction is rolled back that was created later than the transaction with $id = j$.

The case is analogous to the case of Rule AM-v5-Rollback-V45 in Rule V45-V5:Single-Transaction-Rollback.

$id = j$ Then we choose $\Sigma_R' = \Sigma_R''$ and derive the step $\Sigma_R'' \Downarrow_R^{\varepsilon} \Sigma_R'$ by Rule R:AM-Reflection.

Since the transaction with $id = j$ was rolled back, we know that $\Sigma_{S+R}' = \Sigma_{S+R}''' \cdot \langle p, ctr''', \sigma, \mathbb{R}, n\rangle$.

For the trace, we get $\overline{\tau} \cdot \texttt{rlb}_S\ j\restriction^R = helper_R(\overline{\tau}, j)$ by definition of $\restriction^R$ and $id = j$.

The rest of the case is analogous to the corresponding case Rule AM-v5-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

otherwise Then we choose $\Sigma'_R = \Sigma''_R$ and derive the step $\Sigma''_R \Downarrow^{\varepsilon}_R \Sigma'_R$ by Rule R:AM-Reflection. Analogous to the corresponding case in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

□

Lemma 90 (V45 AM: Completeness w.r.t V5 and projection)**.** *If*

(1) $\Sigma_R \approx \Sigma_{S+R}$ *by Rule V45-V5:Single-Base and*
(2) $\Sigma_R \Downarrow^{\overline{\tau}}_R \Sigma'_R$

Then exists Σ'_{S+R} *such that*

I $\Sigma'_R \approx \Sigma'_{S+R}$ *by Rule V45-V5:Single-Base and*
II $\Sigma_{S+R} \Downarrow^{\overline{\tau}'}_{S+R} \Sigma'_{S+R}$ *and*
III $\overline{\tau} = \overline{\tau}' \restriction^R$

Proof. We proceed by induction on $\Sigma_R \Downarrow^{\overline{\tau}}_R \Sigma'_R$:

Rule R:AM-Reflection By Rule R:AM-Reflection we have $\Sigma_R \Downarrow^{\varepsilon}_R \Sigma_R$. with $\Sigma_R = \Sigma'_R$.

I - III We derive $\Sigma_{S+R} \Downarrow^{\overline{\tau}'}_{S+R} \Sigma'_{S+R}$ by Rule AM-Reflection-V45 and thus $\Sigma_{S+R} = \Sigma'_{S+R}$.
By construction and 2) we have $\Sigma'_R \approx \Sigma'_{S+R}$ by Rule V45-V5:Single-Base.
Since $\varepsilon \restriction^S = \varepsilon$ we are finished.

Rule AM-Single-V45 Then we have $\Sigma_R \Downarrow^{\overline{\tau}}_S \Sigma''_R$ and $\Sigma''_R \overset{\tau}{\dashrightarrow}_R \Sigma'_R$.

We need to show
I $\Sigma_{S+R} \Downarrow^{\overline{\tau}' \cdot \tau'}_S \Sigma'_{S+R}$ and
II $\Sigma'_R \approx \Sigma'_{S+R}$ by Rule V45-V5:Single-Base and
III $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \restriction^R$

We apply the IH on $\Sigma_R \Downarrow^{\overline{\tau}}_R \Sigma''_R$ we get
I' $\Sigma_{S+R} \Downarrow^{\overline{\tau}'}_{S+R} \Sigma''_{S+R}$ and
II' $\Sigma''_R \approx \Sigma''_{S+R}$ by Rule V45-V5:Single-Base and
IV' $\overline{\tau} = \overline{\tau}' \restriction^R$

By Rule V45-V5:Single-Base we have:

$$\begin{aligned} \Sigma''_R &= \Sigma'''_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \\ \Sigma''_{S+R} &= \Sigma'''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n \rangle \\ \Sigma'''_R &\sim \Sigma'''_{S+R} \end{aligned}$$

We continue by inversion on $\Sigma''_R \overset{\tau}{\dashrightarrow}_R \Sigma'_R$:

Rule R:AM-Rollback The case is analogous to the corresponding case in Lemma 88 (V45 AM: Completeness w.r.t V4 and projection) using Rule AM-v5-Rollback-V45.

Rule R:AM-Context We then have $\langle p, ctr, \sigma, \mathbb{R}, n \rangle \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_R$ and $n > 0$.

By $\Sigma''_R \approx \Sigma''_{S+R}$ we know that Rule AM-Context-V45 applies for the step $\Sigma''_{S+R} \overset{\tau'}{\dashrightarrow}_{S+R} \Sigma'_{S+R}$ as well.

We now need to find a derivation for the step $\langle p, ctr', \sigma, \mathbb{R}, n \rangle \overset{\tau'}{\dashrightarrow}_{S+R} \overline{\Phi}'_{S+R}$ according to Rule AM-Context-V45.

We proceed by inversion on $\langle p, ctr, \sigma, \mathbb{R}, n \rangle \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_R$:

Rule R:AM-NoBranch Then $n > 0$ and $\langle p, ctr, \sigma, \mathbb{R}, n \rangle \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_R$ by $\sigma \xrightarrow{\tau} \sigma'$.
Furthermore, $\Sigma'_R.n = n - 1$.
We now do a case analysis on the instruction $p(\sigma(\mathbf{pc}))$:
$p(\sigma(\mathbf{pc})) = \mathbf{store}\ x, e$ Then, a speculative transaction of V4 with *id* is started using Rule S:AM-Store-Spec through Rule AM-v4-step-V45 and a new instance $\overline{\Phi}'_{S+R}$ was pushed on top of the stack.
Furthermore, the instance below the newly created state was updated correctly using $\sigma \xrightarrow{\tau} \sigma'$ and reduced their speculation window by 1.
The rest of the case is analogous to the corresponding case ($p(\sigma(\mathbf{pc})) = \mathbf{ret}$ and $\mathbb{R}$ is non-empty and $\mathbb{R}$ value is different to return address) in Lemma 88 (V45 AM: Completeness w.r.t V4 and projection).
otherwise Then we can either use Rule R:AM-NoBranch through Rule AM-v5-step-V45 or Rule S:AM-NoBranch through Rule AM-v4-step-V45.

Because of Lemma 83 (V45 AM: Confluence), we know that it does not matter which rule we use, which means we can use the same rule as for v5 do derive the step.
This gives us $\Sigma''_{S+R} \overset{\tau'}{\Rightarrow}_{S+R} \Sigma'_{S+R}$.
Since the same rule was used, we have $\tau = \tau'$ and $\Sigma'_S \approx \Sigma'_{S+R}$.
Furthermore, since the observation τ was generated by the non-speculative semantics and there is no ongoing transaction of V4 (because $\Sigma'_S \approx \Sigma'_{S+R}$) we have $\tau' \restriction^R = \tau$.
This means we have

$$\begin{aligned}
&\overline{\tau}' \cdot \tau \restriction^R \text{ Definition } \restriction^R \\
&= \overline{\tau}' \restriction^R \cdot \tau' \text{ by IH} \\
&= \overline{\tau} \cdot \tau' \ \tau = \tau' \\
&= \overline{\tau} \cdot \tau
\end{aligned}$$

and we are finished.

otherwise These rules include Rule R:AM-barr, Rule R:AM-barr-spec, Rule R:AM-General, Rule R:AM-Ret-Spec, Rule R:AM-Ret-Same, Rule R:AM-Ret-Empty, Rule R:AM-Call and Rule R:AM-Call-Full. Since the rules of V5 are included in the combined semantics and $\Sigma_S \approx \Sigma_{S+R}$, we can use the corresponding rule in the combined semantics by Confluence or delegate back to V5 by Rule AM-v5-step-V45.
This means we can always do the same step in the combined as in the V5 semantics.

□

Corollary 2 (V45: Relating Combined to non-speculative)**.** *Let p be a program and ω be a speculation window. Then $Beh_{NS}(p) = Beh^{S+R}_{\mathcal{A}}(p) \restriction_{ns}$.*

Proof. By Lemma 10 (V45: Relating speculative projections to non-speculative projection), we have $Beh^{S+R}_{\mathcal{A}}(p) \restriction_{ns} = Beh^{S+R}_{\mathcal{A}}(p) \restriction^S \restriction^R$.
By Theorem 24 (V45: Relating V4 with projection of combined), we have that $Beh^{S+R}_{\mathcal{A}}(p) \restriction^S = Beh^{\mathcal{A}}_S(p)$.
By Lemma 16 (V5: speculative-projections equal to non-speculative Projections), we get $Beh^{\mathcal{A}}_S(p) \restriction^R = Beh^{\mathcal{A}}_S(p) \restriction_{ns}$.
By Theorem 14 (S SE: Behaviour of non-speculative and oracle semantics), we know that $Beh^{\mathcal{A}}_S(p) \restriction_{ns} = Beh_{NS}(p)$.
Combining these facts we get:

$$\begin{aligned}
&Beh^{S+R}_{\mathcal{A}}(p) \restriction_{ns} \\
&= Beh^{S+R}_{\mathcal{A}}(p) \restriction^S \restriction^R \\
&= Beh^{\mathcal{A}}_S(p) \restriction^R \\
&= Beh^{\mathcal{A}}_S(p) \restriction_{ns} \\
&= Beh_{NS}(p)
\end{aligned}$$

and are finished. □

Corollary 3 (V45: SNI of combined)**.** *Let p be a program. If p satisfies SNI under the combined semantics, then it also satisfies SNI for the semantics of v4 and v5.*

Proof. Let p be a program that satisfies SNI under the combined semantics. Assume there are $\sigma, \sigma' \in InitConf$ with $\sigma \sim_P \sigma'$ for some policy P and $(p, \sigma) \overset{O}{\multimap}_{NS} \overline{\tau}', (p, \sigma') \overset{O}{\multimap}_{NS} \overline{\tau}'$.
We need to show that
(1) $(p, \sigma) \overset{\omega}{\multimap}_S \overline{\tau}_s, (p, \sigma') \overset{\omega}{\multimap}_S \overline{\tau}_s$
(2) $(p, \sigma) \overset{\omega}{\multimap}_R \overline{\tau}_r, (p, \sigma') \overset{\omega}{\multimap}_R \overline{\tau}_r$
We show the proof for 1). The proof for 2) is analogous using Theorem 25 (V45: Relating V5 with projection of combined).
Unfolding the definition of SNI for the combination we get:
(1) if $\sigma \sim_P \sigma'$ and $(p, \sigma) \overset{O}{\multimap}_{NS} \overline{\tau}, (p, \sigma') \overset{O}{\multimap}_{NS} \overline{\tau}$, then $(p, \sigma) \overset{\omega}{\multimap}_{S+R} \overline{\tau}_{sr}, (p, \sigma') \overset{\omega}{\multimap}_{S+R} \overline{\tau}_{sr}$
After initialization we have $(p, \sigma) \overset{\omega}{\multimap}_{S+R} \overline{\tau}_{sr}, (p, \sigma') \overset{\omega}{\multimap}_{S+R} \overline{\tau}_{sr}$.
By Theorem 24 (V45: Relating V4 with projection of combined) we have $(p, \sigma) \overset{\omega}{\multimap}_S (\overline{\tau}_{sr} \restriction^S) \in Beh^{\mathcal{A}}_S(p)$ and $p, \sigma' \overset{\omega}{\multimap}_S (\overline{\tau}_{sr} \restriction^S) \in Beh^{\mathcal{A}}_S(p)$, which is what we needed to show.

□

K.3 Relating Speculative and AM semantics

The oracle semantics is Confluent as well:

Lemma 91 (V45SE: Confluence)**.** *If*

(1) $X_{S+R} \xrightarrow{\tau}{}^{O_{S+R}}_{S+R} X'_{S+R}$ *and*

(2) $X_{S+R} \xrightarrow{\tau}{}^{O_{S+R}}_{S+R} X''_{S+R}$ *derived by a different rule*

Then

(1) $X'_{S+R} = X_{S+R}$

Proof. Analogous to Lemma 83 (V45 AM: Confluence) □

Theorem 26 (V45: SNI). *For a program p, all oracles O with speculative window at most ω and for a security Policy P,* $p \vdash^{O}_{S+R}$ *SNI iff* $p \vdash_{S+R}$ *SNI.*

Proof. We prove the two directions separately:

(⇒) The proof proceeds analogous to Theorem 17 (S SNI) using (Lemma 102 (V45: Completeness Am semantics w.r.t. speculative semantics))

(⇐) The proof proceeds analogously to Theorem 17 (S SNI) using the Soundness (Lemma 97 (V45: Soundness Big-step))

and Completeness () results. □

> The relation is very similar to the one of V4 and V5. We just have to account for both speculation sources. This is done by adding the condition $x = \mathit{false} \vee (x \in \mathbb{N} \wedge x = m(a(\mathbf{sp})))$ to the cases to show that speculation can come from either side

Definition 64 (V45: Relation between AM and spec for all oracles)**.** *We define two relations between AM and oracle semantics.* $\approx \sim$

$$\boxed{\Sigma_{S+R} \approx_{S+R} X_{S+R}}$$

$$\frac{}{\varnothing \approx_{S+R} \varnothing}\ \textit{(V45:Base)} \qquad \frac{\Sigma_{S+R} \sim X_{S+R}\restriction_{com} \quad INV(\Sigma_{S+R}, X_{S+R})}{\Sigma_{S+R} \approx_{S+R} X_{S+R}}\ \textit{(V45:Single-Base)}$$

$$\frac{\begin{array}{c}\Sigma_{S+R} \sim X_{S+R}\restriction_{com} \quad \Sigma''_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma'''_{S+R} \textit{ where transaction with id ctr is rolled back} \\ X_{S+R} = X'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n''\rangle \qquad x = (S, \mathit{false}) \vee (R, m \wedge m = m(a(\mathbf{sp}))) \\ \Sigma_{S+R} = \Sigma'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \qquad INV(\Sigma_{S+R}, X_{S+R})\end{array}}{\Sigma'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n'\rangle \cdot \Sigma_{S+R1} \approx_{S+R} X'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n''\rangle \cdot \langle p, ctr', \sigma, \mathbb{R}, h, n'''\rangle^{x}}\ \textit{(V45:Single-OracleTrue)}$$

$$\frac{\begin{array}{ccc}\Sigma''_{S+R} \sim X''_{S+R}\restriction_{com} & n' \geq 0 & \Sigma''_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma'''_{S+R} \textit{ where transaction with id ctr is rolled back} \qquad x = (S, \mathit{true}) \vee (R, m) \\ X_{S+R} = X'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n''\rangle & & \Sigma_{S+R} = \Sigma'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \qquad INV(\Sigma_{S+R}, X_{S+R})\end{array}}{\Sigma'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n'\rangle^{x} \cdot \Sigma_{S+R1} \approx_{S+R} X'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n''\rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0\rangle^{x} \cdot X_{S+R1}}\ \textit{(V45:Single-Transaction-Rollback)}$$

$$\boxed{\Sigma_{S+R} \sim X_{S+R}}$$

$$\frac{}{\varnothing \sim \varnothing}\ \textit{(V45:Base)} \qquad \frac{|\Sigma'_{S+R}| = |X'_{S+R}| \quad \Sigma'_{S+R} \sim X'_{S+R}}{\Sigma'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle^{b} \sim X'_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, h, n'\rangle^{b}}\ \textit{(V45:Single)}$$

Lemma 92 (V45: Coincide on $\approx_{S+R}$ for projections)**.** *If*

(1) $\Sigma_{S+R} \approx_{S+R} X_{S+R}$ *by Rule V45:Single-Base*

Then

(1) $\Sigma_{S+R}\restriction^{S} \approx_{S} X_{S+R}\restriction^{S}$ *by Rule Single-Base and*

(2) $\Sigma_{S+R}\restriction^{R} \approx_{R} X_{S+R}\restriction^{R}$ *by Rule Single-Base*

Proof. We show the proof for $\Sigma_{S+R}\restriction^{S} \approx_{S} X_{S+R}\restriction^{S}$. The proof for $\Sigma_{S+R}\restriction^{R} \approx_{R} X_{S+R}\restriction^{R}$ is analogous.
We have:

$$\Sigma_{S+R} \sim X_{S+R}\restriction_{com}$$
$$INV(\Sigma_{S+R}, X_{S+R})$$

By ∼ we know that all instances in the states are equivalent. This means the instances in $\Sigma_{S+R}\restriction^S$ and $X_{S+R}\restriction^S$ are equivalent as well, because they only project out of the states but do not change them.

Thus, we can derive $\Sigma_{S+R}\restriction^S \approx_S X_{S+R}\restriction^S$ using Rule Single-Base. □

Lemma 93 (V45: Coincide on ≅ for projections). *If*

(1) $\Sigma_{S+R} \cong X_{S+R}$

Then

(1) $\Sigma_{S+R}\restriction^S \cong X_{S+R}\restriction^S$ *and*
(2) $\Sigma_{S+R}\restriction^R \cong X_{S+R}\restriction^R$

Proof. The projection function does not change the values of the instances in the state. Thus, $\Sigma_{S+R}\restriction^S \cong X_{S+R}\restriction^S$ and $\Sigma_{S+R}\restriction^R \cong X_{S+R}\restriction^R$ trivially holds. □

Lemma 94 (V45: Initial states fulfill properties). *Let p be a program, ω be a speculation window and O be an oracle with speculation window at most ω. If*

(1) $\sigma, \sigma' \in InitConf$ *and*
(2) $\Sigma^{init}_{S+R}(p,\sigma)$ *and* $\Sigma^{init}_{S+R}(p,\sigma')$ *and*
(3) $X^{init}_{S+R}(p,\sigma)$ *and* $X^{init}_{S+R}(p,\sigma')$

Then

(1) $X^{init}_{S+R}(p,\sigma) \cong X^{init}_{S+R}(p,\sigma')$ *and*
(2) $\Sigma^{init}_{S+R}(p,\sigma) \cong \Sigma^{init}_{S+R}(p,\sigma')$ *and*
(3) $\Sigma^{init}_{S+R}(p,\sigma) \approx_{S+R} X^{init}_{S+R}(p,\sigma)$ *and* $\Sigma^{init}_{S+R}(p,\sigma') \approx_{S+R} X^{init}_{S+R}(p,\sigma')$ *by Rule V45:Single-Base and*

Proof. The proof is analogous to Lemma 45 (S: Initial states fulfill properties). □

Lemma 95 (V45AM: Single step preserves ≅). *If*

(1) $\Sigma_{S+R} \cong \Sigma^{\dagger}_{S+R}$ *and*
(2) $\Sigma_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Sigma'_S$ *and* $\Sigma^{\dagger}_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Sigma^{\dagger\dagger}_{S+R}$

Then

(1) $\Sigma'_{S+R} \cong \Sigma^{\dagger\dagger}_{S+R}$

Proof. The proof is analogous to Lemma 43 (S AM: Single step preserves ≅). □

Lemma 96 (V45SE: Single step preserves ≅). *If*

(1) $X_{S+R} \cong X^{\dagger}_{S+R}$ *and*
(2) $X_{S+R} \overset{\tau}{\rightsquigarrow}^{O_{S+R}}_{S+R} X'_{S+R}$ *and* $X^{\dagger}_{S+R} \overset{\tau}{\rightsquigarrow}^{O_{S+R}}_{S+R} X^{\dagger\dagger}_{S+R}$

Then

(1) $X'_{S+R} \cong X^{\dagger\dagger}_{S+R}$ *and*

Proof. The proof is analogous to Lemma 44 (S SE: Single step preserves ≅). □

K.4 Soundness

Lemma 97 (V45: Soundness Big-step). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*

If

(1) $\sigma, \sigma' \in InitConf$ *and*
(2) $(p,\sigma) \Downarrow^{\omega}_{S+R} \overline{\tau}$, $(p,\sigma') \Downarrow^{\omega}_{S+R} \overline{\tau}$

Then for all prediction oracles O with speculation window at most ω.

I $(p,\sigma) \Downarrow^{O}_{S+R} \overline{\tau}'$, $(p,\sigma) \Downarrow^{O}_{S+R} \overline{\tau}'$

Proof. The proof is analogous to Lemma 46 (S: Soundness Am semantics w.r.t. speculative semantics) using Lemma 94 (V45: Initial states fulfill properties) to show that our initial states fulfill all the premises for Lemma 98 (V45: Soundness Am semantics w.r.t. speculative semantics with new relation between states). □

Lemma 98 (V45: Soundness Am semantics w.r.t. speculative semantics with new relation between states). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*

If

(1) $\Sigma_{S+R} \cong \Sigma^{\dagger}_{S+R}$
(2) $X_{S+R} \cong X^{\dagger}_{S+R}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma^{\dagger}_{S+R} \approx_{S+R} X_{S+R}$ *and* $\Sigma^{\dagger}_{S+R} \approx_{S+R} X^{\dagger}_{S+R}$
(4) $\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma'_{S+R}$ *and* $\Sigma^{\dagger}_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma^{\dagger\dagger}_{S+R}$

Then for all prediction oracles O *with speculation window at most* ω.

I $X_{S+R} \overset{O}{\Downarrow}^{S}_{\overline{\tau}'} X'_{S+R}, X^{\dagger}_{S+R} \overset{O}{\Downarrow}^{S}_{\overline{\tau}''} X^{\dagger\dagger}_{S+R}$
II $\Sigma'_{S+R} \cong \Sigma^{\dagger\dagger}_{S+R}$
III $X'_{S+R} \cong X^{\dagger\dagger}_{S+R}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$ *and* $\Sigma^{\dagger\dagger}_{S+R} \approx_{S+R} X^{\dagger\dagger}_{S+R}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. By Induction on $\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma'_{S+R}$ and $\Sigma^{\dagger}_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma^{\dagger\dagger}_{S+R}$.

Rule AM-Reflection-V45 We have $\Sigma_{S+R} \Downarrow^{\varepsilon}_{S+R} \Sigma'_{S+R}$ and $\Sigma^{\dagger}_{S+R} \Downarrow^{\varepsilon}_{S+R} \Sigma''_{S+R}$, where $\Sigma'_{S+R} = \Sigma_{S+R}$ and $\Sigma''_{S+R} = \Sigma^{\dagger}_{S+R}$. We choose $\Sigma'_{S+R} = \Sigma'_{S+R}$ and $\Sigma^{\dagger\dagger}_{S+R} = \Sigma''_{S+R}$.

We further use Rule SE-Reflection-V45 to derive $X_{S+R} \overset{O}{\Downarrow}^{S}_{\varepsilon} X'_{S+R}, X^{\dagger}_{S+R} \overset{O}{\Downarrow}^{S}_{\varepsilon} X^{\dagger\dagger}_{S+R}$ with $X'_{S+R} = X_{S+R}$ and $X^{\dagger\dagger}_{S+R} = X^{\dagger}_{S+R}$. We now trivially satisfy all conclusions.

Rule AM-Single-V45 We have $\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma''_{S+R}$ with $\Sigma''_{S+R} \overset{\tau}{\rightarrow\!\!\!\!\!\!\rightarrow}_{S+R} \Sigma'_{S+R}$ and $\Sigma^{\dagger}_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma'''_{S+R}$ and $\Sigma'''_{S+R} \overset{\tau}{\rightarrow\!\!\!\!\!\!\rightarrow}_{S+R} \Sigma^{\dagger\dagger}_{S+R}$.

We now apply IH on $\Sigma_{S+R} \Downarrow^{\overline{\tau}''}_{S+R} \Sigma''_{S+R}$ and $\Sigma^{\dagger}_{S+R} \Downarrow^{\overline{\tau}'''}_{S+R} \Sigma^{*}_{S+R}$ and get

(a) $X_{S+R} \overset{O}{\Downarrow}^{S}_{\overline{\tau}'} X''_{S+R}, X^{\dagger}_{S+R} \overset{O}{\Downarrow}^{S}_{\overline{\tau}''} X^{*}_{S+R}$
(b) $\Sigma''_{S+R} \cong \Sigma^{*}_{S+R}$
(c) $X''_{S+R} \cong X^{*}_{S+R}$ and $\overline{\rho}' = \varnothing$
(d) $\Sigma''_{S+R} \approx_{S+R} X''_{S+R}$ and $\Sigma^{*}_{S+R} \approx_{S+R} X^{*}_{S+R}$
(e) $\overline{\tau}' = \overline{\tau}''$

We do a case distinction on $\approx_{S+R}$ in $\Sigma''_{S+R} \approx_{S+R} X''_{S+R}$ and $\Sigma^{*}_{S+R} \approx_{S+R} X^{*}_{S+R}$:

Rule V45:Single-Base We thus have $\Sigma''_{S+R} \sim X''_{S+R}\restriction_{com}$ and $INV(\Sigma''_{S+R}, X''_{S+R})$ (Similar for Σ^{*}_{S+R} and X^{*}_{S+R}).

We only show the proof for X''_{S+R} here. The proof for X^{*}_{S+R} is analogous, because of $X''_{S+R} \cong X^{*}_{S+R}$.

Notice that if $minWndw(X''_{S+R}) = 0$ then the transaction with $n = 0$ has to be one that will be committed. Otherwise they would be related by Rule V45:Single-Transaction-Rollback.

To account for possible outstanding commits, we can use Lemma 23 (V45: Executing a chain of commits) on X''_{S+R} and get

f) $X''_{S+R} \overset{O}{\Downarrow}^{S}_{\overline{\tau}'''} X^{**}_{S+R}$
g) $minWndw(X^{**}_{S+R}) > 0$
h) $\forall \tau \in \overline{\tau}'''.\ \tau = \texttt{commit}\ id$ for some $id \in \mathbb{N}$
i) $X''_{S+R}.\sigma = X^{**}_{S+R}.\sigma$

By h) and the definition of $\restriction_{ns}$ we have $\overline{\tau}'''\restriction_{ns} = \varepsilon$.

Furthermore, $X''_{S+R}\restriction_{com} = X^{**}_{S+R}\restriction_{com}$ by definition of $\restriction_{com}$ (we only executed commits) and we have $|X''_{S+R}\restriction_{com}| = |X^{**}_{S+R}\restriction_{com}|$.

Thus, $\Sigma''_{S+R} \sim X^{**}_{S+R}\restriction_{com}$ and $INV(\Sigma''_{S+R}, X^{**}_{S+R})$ and we have $\Sigma''_{S+R} \approx_{S+R} X^{**}_{S+R}$ by Rule V45:Single-Base.

We now proceed by inversion on the derivations $\Sigma''_{S+R} \overset{\tau}{\rightarrow\!\!\!\!\!\!\rightarrow}_{S+R} \Sigma'_{S+R}$ and $\Sigma^{*}_{S+R} \overset{\tau}{\rightarrow\!\!\!\!\!\!\rightarrow}_{S+R} \Sigma^{\dagger\dagger}_{S+R}$.

Note that by $\Sigma''_{S+R} \cong \Sigma^{*}_{S+R}$ and the fact the same traces are generated, we know that the same rule was used to derive the step.

Rule AM-Context-V45 We now have $\Phi'_{S+R} \overset{\tau}{\rightarrow\!\!\!\!\!\!\rightarrow}_{S+R} \overline{\Phi}'_{S+R}$ and $\Phi''_{S+R} \overset{\tau}{\rightarrow\!\!\!\!\!\!\rightarrow}_{S+R} \overline{\Phi}'''_{S+R}$ where $\Sigma''_{S+R} = \overline{\Phi}_{S+R} \cdot \Phi'_{S+R}$ and $\Sigma^{*}_{S+R} = \overline{\Phi}''_{S+R} \cdot \Phi''_{S+R}$.

Furthermore, $n > 0$ and note that all states point to the same instruction by b-d.

Rule AM-v4-step-V45 Then, we have $\Phi_S\restriction^{S} \overset{\tau}{\rightarrow\!\!\!\!\!\!\rightarrow}_{S} \overline{\Phi}'_{S+R}\restriction^{S}$

We use Lemma 99 (V45: V4 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule AM-v5-step-V45 Then we have $\Phi_{S+R}\restriction^{R} \overset{\tau}{\rightarrow\!\!\!\!\!\!\rightarrow}_{R} \overline{\Phi}'_{S+R}\restriction^{R}$.

We use Lemma 100 (V45: V5 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule AM-v5-Rollback-V45 Contradiction, because $minWndw(X'''_{S+R}) > 0$ and $INV(\Sigma'_{S+R}, X'''_{S+R})$.

Rule AM-v4-Rollback-V45 Contradiction, because $minWndw(X'''_{S+R}) > 0$ and $INV(\Sigma'_{S+R}, X'''_{S+R})$.

Rule V45:Single-OracleTrue We thus have

$$
\begin{aligned}
X''_{S+R} &= X_{S+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \cdot \langle p, ctr', \sigma, \mathbb{R}', h, n''' \rangle^{false} \\
\Sigma''_{S+R} &= \Sigma_{S+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}'', n' \rangle \cdot \Sigma_{S+R4} \\
X_{S+R} &= X_{S+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \\
\Sigma_{S+R} &= \Sigma_{S+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \\
\Sigma_{S+R} &\sim X_{S+R} \restriction_{com}
\end{aligned}
$$

The form of X^*_{S+R} and Σ^*_{S+R} is analogous. We now apply inversion on $\Sigma''_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Sigma'_{S+R}$.

Rule AM-Context-V45 We choose $X'_{S+R} = X''_{S+R}$ and $X^{\dagger\dagger}_{S+R} = X^*_{S+R}$.

I By IH a) and Rule SE-Reflection-V45

II By Lemma 95 (V45AM: Single step preserves $\cong$).

III Since $X'_{S+R} = X''_{S+R}$ and $X^{\dagger\dagger}_{S+R} = X^*_{S+R}$, we are finished using IH c).

IV We show that $X'_{S+R} \approx_{S+R} \Sigma'_{S+R}$ by Rule V45:Single-OracleTrue. The proof for $X^{\dagger\dagger}_{S+R} \approx \Sigma^{\dagger\dagger}_{S+R}$ is analogous.
Since we did not roll back the transaction with *id ctr'* we have that Σ_{S+R} does not change.
Since X_{S+R} remains the same as well, we have $\Sigma_{S+R} \sim X_{S+R} \restriction_{com}$ and $INV(\Sigma_{S+R}, X_{S+R})X_{S+R} \restriction_{com}$.
Thus, we fulfill all premises for Rule V45:Single-OracleTrue.

V By IH e).

Rule AM-v4-Rollback-V45 There are two cases depending on the transaction *id* of the rolled back transaction:

id > *ctr* Then an inner transaction w.r.t our *ctr* transaction was finished. Similar to before, only Σ''_{S+R} and Σ^*_{S+R} do a step. We choose $X'_{S+R} = X''_{S+R}$ and $X^{\dagger\dagger}_{S+R} = X^*_{S+R}$. The rest of the proof proceeds analogous to the context case above.

id = *ctr* Most cases are similar to the context case above. Only the relation changes. We choose $X'_{S+R} = X''_{S+R}$ and $X^{\dagger\dagger}_{S+R} = X^*_{S+R}$

I By IH a) and Rule SE-Reflection-V45

IV Here, we only show $\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$ by Rule V45:Single-Base. The proof for $\Sigma^{\dagger\dagger}_{S+R} \approx X^{\dagger\dagger}_{S+R}$ is analogous.
Notice that $\Sigma'_{S+R} = \Sigma_{S+R3} \cdot \langle p, ctr', \sigma, n \rangle$ (updated *ctr*) after the rollback.
Combined with the constructed X'_{S+R} we have $\Sigma'_{S+R} \sim X'_{S+R} \restriction_{com}$ and $INV(\Sigma'_{S+R}, X'_{S+R})$ by our assumptions.
So we can use Rule V45:Single-Base and have $\Sigma'_{S+R} \approx X'_{S+R}$.

V By IH e)

Rule AM-v5-Rollback-V45 The case is analogous to the case Rule AM-v4-Rollback-V45 above.

Rule V45:Single-Transaction-Rollback We have

$$
\begin{aligned}
X''_{S+R} &= X_{S+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0 \rangle^{true} \cdot X_{S+R4} \\
\Sigma''_{S+R} &= \Sigma_{S+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle^{true} \cdot \Sigma_{S+R4} \\
X_{S+R} &= X_{S+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \\
\Sigma_{S+R} &= \Sigma_{S+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \\
\Sigma_{S+R} &\sim X_{S+R} \restriction_{com} \\
n' &\geq 0
\end{aligned}
$$

The form of X^*_{S+R} and Σ^*_{S+R} is analogous.

Additionally we know that the transaction terminates in some state $\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma'''_{S+R}$. There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma''_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Sigma'_{S+R}$ is not a rollback for *ctr* and Rule AM-Context-V45 or Rule AM-v4-Rollback-V45 or Rule AM-v5-Rollback-V45 for a different transaction with a different *ctr* was used.
Because of IH b), we know that the same rule was used for $\Sigma^{\dagger}_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Sigma^{\dagger\dagger}_{S+R}$ as well. We choose $X'_{S+R} = X''_{S+R}$ and $X^{\dagger\dagger}_{S+R} = X^*_{S+R}$.
The resulting proof obligations are exactly the same to the context case of the oracle above.

$n' = 0$ Then we know that $\Sigma''_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Sigma'_{S+R}$ was created by either Rule AM-v4-Rollback-V45 or Rule AM-v5-Rollback-V45 and is a rollback for *ctr*.
We do the proof for Rule AM-v4-Rollback-V45, since the case for Rule AM-v5-Rollback-V45 is analogous.

I Here we prove that $X''_{S+R} \overset{\tau_0}{\rightsquigarrow}^{O_{S+R}}_{S+R} X'_{S+R}$ and $X^*_{S+R} \overset{\tau_1}{\rightsquigarrow}^{O_{S+R}}_{S+R} X^{\dagger\dagger}_{S+R}$.
Since in X''_{S+R} and X^*_{S+R} we have a state that needs to be rolled back for the same *ctr*, we know that Rule V45-SE:v4-Rollback applies.
So $X''_{S+R} \overset{\tau_0}{\rightsquigarrow}^{O_{S+R}}_{S+R} X'_{S+R}$ and $X^*_{S+R} \overset{\tau_1}{\rightsquigarrow}^{O_{S+R}}_{S+R} X^{\dagger\dagger}_{S+R}$ are derived by Rule V45-SE:v4-Rollback.

II By Lemma 95 (V45AM: Single step preserves $\cong$)

III By Lemma 96 (V45SE: Single step preserves $\cong$) with fact V).

IV Here, we only show $\Sigma'_{S+R} \approx X'_{S+R}$ by Rule V45:Single-Base. The proof for $\Sigma^{\dagger\dagger}_{S+R} \approx X^{\dagger\dagger}_{S+R}$ is analogous.
We know that the states after rollback are

$$X'_{S+R} = X_{S+R3} \cdot \langle p, ctr', \sigma, h', n'' \rangle$$
$$\Sigma'_{S+R} = \Sigma_{S+R3} \cdot \langle p, ctr', \sigma, n \rangle$$

Notice, that the only difference to X''_{S+R} and Σ''_{S+R} is the updated *ctr*. We also know by assumption that $\Sigma''_{S+R} \sim X''_{S+R}\restriction_{com}$ and $INV(\Sigma''_{S+R}, X''_{S+R})$.
By construction of X'_{S+R} and Σ'_{S+R}, we can conclude that $\Sigma'_{S+R} \sim X'_{S+R}\restriction_{com}$ and $INV(\Sigma'_{S+R}, X'_{S+R})$.
This allows us to use Rule V45:Single-Base to derive $\Sigma'_{S+R} \approx X'_{S+R}$.

V Here $\tau_0 = \texttt{rlb}\ ctr'$ and $\tau_1 = \texttt{rlb}\ ctr''$. Because of IH b) we know that $ctr' = ctr''$ and thus $\tau_0 = \tau_1$.

□

Lemma 99 (V45: V4 Soundness Single step)**.** *If*

(1) $\Sigma_{S+R} \approx_{S+R} X_{S+R}$ *and* $\Sigma^{\dagger}_{S+R} \approx_{S+R} X^{\dagger}_{S+R}$ *by Rule V45:Single-Base and*
(2) $\Sigma_{S+R} \cong \Sigma^{\dagger}_{S+R}$ *and* $X_{S+R} \cong X^{\dagger}_{S+R}$ *and*
(3) $\Phi_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}'_{S+R}$ *and* $\Phi^{\dagger}_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}^{\dagger\dagger}_{S+R}$ *by*
(4) $\Phi_{S+R}\restriction^S \overset{\tau}{\dashrightarrow}_{S} \overline{\Phi}'_{S+R}\restriction^S$ *and* $\Phi^{\dagger}_{S+R}\restriction^S \overset{\tau}{\dashrightarrow}_{S} \overline{\Phi}^{\dagger\dagger}_{S+R}\restriction^S$

Then

(1) $\Psi_{S+R} \overset{\tau', O_{S+R}}{\rightsquigarrow}_{S+R} \overline{\Psi}'_{S+R}$ *and* $\Psi^{\dagger}_{S+R} \overset{\tau', O_{S+R}}{\rightsquigarrow}_{S+R} \overline{\Psi}^{\dagger\dagger}_{S+R}$ *in combination with Context rule*
(2) $\Psi_{S+R}\restriction^S \overset{\tau, O}{\rightsquigarrow}_{S} \overline{\Psi}'_{S+R}\restriction^S$ *and* $\Psi^{\dagger}_{S+R}\restriction^S \overset{\tau, O}{\rightsquigarrow}_{S} \overline{\Psi}^{\dagger\dagger}_{S+R}\restriction^S$
(3) $\Sigma'_{S+R} \cong \Sigma^{\dagger\dagger}_{S+R}$ *and* $X'_{S+R} \cong X^{\dagger\dagger}_{S+R}$ *and*
(4) $\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$ *and* $\Sigma^{\dagger\dagger}_{S+R} \approx_{S+R} X^{\dagger\dagger}_{S+R}$

Proof. By Rule V45:Single-Base and $X_{S+R} \cong X^{\dagger}_{S+R}$ we know that $minWndw(X_{S+R}) > 0$ (similar for $X^{\dagger}_{S+R}$). This means Rule V45-SE-Context applies. We now need to find a step $\Psi_{S+R} \overset{\tau'}{\dashrightarrow}_{S+R} \overline{\Psi}'_{S+R}$ and $\Psi^{\dagger}_{S+R} \overset{\tau'}{\dashrightarrow}_{S+R} \overline{\Psi}^{\dagger\dagger}_{S+R}$. Note that Rule V45-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 93 and Lemma 92 we get $\Sigma_{S+R}\restriction^S \approx_S X_{S+R}\restriction^S$ and $\Sigma_{S+R}\restriction^S \cong \Sigma^{\dagger}_{S+R}\restriction^S$.

Because of $\Phi_{S+R}\restriction^S \overset{\tau}{\dashrightarrow}_{S} \overline{\Phi}'_{S+R}\restriction^S$ and $\Phi^{\dagger}_{S+R}\restriction^S \overset{\tau}{\dashrightarrow}_{S} \overline{\Phi}^{\dagger\dagger}_{S+R}\restriction^S$ and Rule V45:Single-Base, we fulfill all premises for Lemma 48 (S: Soundness Single Step AM) and derive a step in the oracle semantics:

a) $\Sigma'_{S+R}\restriction^S \cong \Sigma^{\dagger\dagger}_{S+R}\restriction^S$ and $X'_{S+R}\restriction^S \cong X^{\dagger\dagger}_{S+R}\restriction^S$
b) $\Sigma'_{S+R}\restriction^S \approx_S X'_{S+R}\restriction^S$ and $\Sigma^{\dagger\dagger}_{S+R}\restriction^S \approx_S X^{\dagger\dagger}_{S+R}\restriction^S$
c) $\Psi_{S+R}\restriction^S \overset{\tau}{\dashrightarrow}_{S} \overline{\Psi}'_{S+R}\restriction^{S'}$ and $\Psi^{\dagger}_{S+R}\restriction^S \overset{\tau}{\dashrightarrow}_{S} \overline{\Psi}^{\dagger}_{S+R}\restriction^S$ the step of the oracle

Since we have $\Psi_{S+R}\restriction^S \overset{\tau}{\dashrightarrow}_{S} \overline{\Psi}'_{S+R}\restriction^{S'}$ we can derive a step $\Psi_{S+R} \overset{\tau'}{\dashrightarrow}_{S+R} \overline{\Psi}'_{S+R}$ using Rule V45-SE:v4-step (or another applicable rule by Lemma 83 (V45 AM: Confluence)).

Let us collect what we already have:

$$X'_{S+R} = X''_{S+R} \cdot \overline{\Psi}'_{S+R}$$
$$\Sigma'_{S+R} = \Sigma''_{S+R} \cdot \overline{\Phi}'_{S+R}$$
$$X^{\dagger\dagger}_{S+R} = X^{*}_{S+R} \cdot \overline{\Psi}^{\dagger\dagger}_{S+R}$$
$$\Sigma^{\dagger\dagger}_{S+R} = \Sigma^{*}_{S+R} \cdot \overline{\Phi}^{\dagger\dagger}_{S+R}$$

We now need to show that $\Sigma'_{S+R} \cong \Sigma^{\dagger\dagger}_{S+R}$ and $X'_{S+R} \cong X^{\dagger\dagger}_{S+R}$ and $\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$ and $\Sigma^{\dagger\dagger}_{S+R} \approx_{S+R} X^{\dagger\dagger}_{S+R}$ hold.

$\Sigma'_{S+R} \cong \Sigma^{\dagger\dagger}_{S+R}$ and $X'_{S+R} \cong X^{\dagger\dagger}_{S+R}$ Since only the topmost state (and the speculation window for the oracles which does not matter for $\cong$) was changed during the step we can conclude $X''_{S+R} \cong X^{*}_{S+R}$ and $\Sigma''_{S+R} \cong \Sigma^{*}_{S+R}$
We need to prove that $\overline{\Phi}'_{S+R} \cong \overline{\Phi}^{\dagger\dagger}_{S+R}$. The proof for $\overline{\Psi}'_{S+R} \cong \overline{\Psi}^{\dagger\dagger}_{S+R}$ is analogous.
Because the step can only change the parts of the state that is in the projection $\restriction^S$ and the states were related by $\cong$ before, it is sufficient to show $\overline{\Phi}'_{S+R}\restriction^S \cong \overline{\Phi}^{\dagger\dagger}_{S+R}\restriction^S$.
We get this fact from a) above and are finished.

$\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$ **and** $\Sigma^{\dagger\dagger}_{S+R} \approx_{S+R} X^{\dagger\dagger}_{S+R}$ We want to show that $\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$. The case for $\Sigma^{\dagger\dagger}_{S+R} \approx_{S+R} X^{\dagger\dagger}_{S+R}$ is analogous.

We first check if there is a transaction of V5 that needs to be rolled back in X'_{S+R}, since the speculation window of each instance was reduced.

This has to be done, because we only know that $minWndw(X'_{S+R}) > 0$ *before* we did the step. So it could happen that $minWndw(X'_{S+R}) = 0$ for some transaction of V5 that needs to be rolled back (we can ignore transactions that will be committed).

Transaction of V5 that needs to be rolled back in X'_{S+R} with window 0 The step made cannot create a new speculative instance of V5 that would be on top. This means we can derive all premises of Rule V45:Single-Transaction-Rollback just from $\Sigma_{S+R} \approx_{S+R} X_{S+R}$. Thus, we have $\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$ by Rule V45:Single-Transaction-Rollback.

No V5 Transaction that needs to be rolled back in X'_{S+R} with window 0 Since the speculation window was reduced for all entries in X'_{S+R} and only for the topmost entry in Σ_{S+R} and we had $INV(\Sigma_{S+R}, X_{S+R})$ from $\Sigma_{S+R} \approx_{S+R} X_{S+R}$, we have $INV(\Sigma'_{S+R}, X'_{S+R})$ again. This reasoning extends to newly created instances by speculation as well.

We do a case distinction on $\approx_S$:

Rule Single-Base Only the topmost state did change during the step (apart from the reduction of the speculation window for X_{S+R}).

We can then conclude from $\Sigma_{S+R} \approx_{S+R} X_{S+R}$ that $\Sigma''_{S+R} \sim X''_{S+R}\restriction_{com}$.

From $\approx_S$ we get $\overline{\Phi}'_{S+R}\restriction^S \sim \overline{\Psi}'_{S+R}\restriction^S\restriction_{com}$.

And combined with $\Sigma'_{S+R} \cong X'_{S+R}$, we get $\overline{\Phi}'_{S+R} \sim \overline{\Psi}'_{S+R}\restriction_{com}$.

Because $INV(\Sigma'_{S+R}, X'_{S+R})$ holds from above, we can conclude that $\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$ are related by Rule V45:Single-Base.

Rule Single-OracleTrue Then, the oracle predicted correctly

Thus, we have

$$\overline{\Psi}'_{S+R} = \Psi_{S+R} \cdot \langle p, ctr, \sigma, h, \mathbb{R}, n\rangle^{false}$$
$$\overline{\Phi}'_{S+R} = \Phi_{S+R} \cdot \langle p, ctr, \sigma', \mathbb{R}, n'\rangle^{true}$$

Similarly, we had $\Sigma_{S+R} \sim_{S+R} X_{S+R}\restriction_{com}$ and since only the speculation window was reduced, we have $\Sigma''_{S+R} \sim X''_{S+R}\restriction_{com}$ as well. Combined with $INV(\Sigma'_{S+R}, X'_{S+R})$ from above, we fulfill all premises for Rule V45:Single-OracleTrue and have $\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$.

Rule Single-Transaction-Rollback Then one of the instances in $X'_{S+R}\restriction^S$ needs to be rolled back.

This means the same instance in X'_{S+R} needs to be rolled back as well.

We do a case distinction if the instance is part of $\overline{\Psi}'_{S+R}$ or not:

instance is not part of $\overline{\Psi}'_{S+R}$ Since the instance is not part of $\overline{\Psi}'_{S+R}$, it is part of X''_{S+R}. This means from $\Sigma_{S+R} \approx_{S+R} X_{S+R}$ related by Rule V45:Single-Base, we get all the necessary facts to conclude that $\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$ by Rule V45:Single-Transaction-Rollback.

instance is part of $\overline{\Psi}_{S+R}$ We do a case distinction if a new state was created or not:

$|\overline{\Psi}_{S+R}| = 1$ Because we only need to relate below $\overline{\Psi}_{S+R}$ to relate by Rule V45:Single-Transaction-Rollback, we can reuse our reasoning in the case above to conclude $\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$ by Rule V45:Single-Transaction-Rollback.

$|\overline{\Psi}_{S+R}| = 2$ Then we have

$$\overline{\Psi}'_{S+R} = \Psi_{S+R} \cdot \langle p, ctr, \sigma, h, \mathbb{R}, n\rangle^{true}$$
$$\overline{\Phi}'_{S+R} = \Phi_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n'\rangle^{true}$$

From $\approx_S$ we get $\Phi_{S+R}\restriction^S \sim \Psi_{S+R}\restriction^S$ and since only the projection changed during the step we have $\Phi_{S+R} \sim \Psi_{S+R}$.

For all instances below $\overline{\Phi}_{S+R}$, we can use the fact that $\Sigma_{S+R} \approx_{S+R} X_{S+R}$ related by Rule V45:Single-Base to conclude that $\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$ Rule V45:Single-Transaction-Rollback

□

Lemma 100 (V45: V5 Soundness Single step). *If*

(1) $\Sigma_{S+R} \approx_{S+R} X_{S+R}$ *and* $\Sigma^{\dagger}_{S+R} \approx_{S+R} X^{\dagger}_{S+R}$ *by Rule V45:Single-Base and*

(2) $\Sigma_{S+R} \cong \Sigma^{\dagger}_{S+R}$ *and* $X_{S+R} \cong X^{\dagger}_{S+R}$ *and*

(3) $\Phi_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}'_{S+R}$ *and* $\Phi^{\dagger}_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}^{\dagger\dagger}_{S+R}$ *by*

(4) $\Phi_{S+R}\restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_{S+R}\restriction^R$ *and* $\Phi^{\dagger}_{S+R}\restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}^{\dagger\dagger}_{S+R}\restriction^R$

Then

(1) $\Psi_{S+R} \overset{\tau', O_{S+R}}{\rightsquigarrow}_{S+R} \overline{\Psi}'_{S+R}$ *and* $\Psi^{\dagger}_{S+R} \overset{\tau', O_{S+R}}{\rightsquigarrow}_{S+R} \overline{\Psi}^{\dagger\dagger}_{S+R}$ *in combination with Context rule*

(2) $\Psi_{S+R}\restriction^R \overset{\tau, O}{\rightsquigarrow}_R \overline{\Psi}'_{S+R}\restriction^R$ *and* $\Psi^{\dagger}_{S+R}\restriction^R \overset{\tau, O}{\rightsquigarrow}_R \overline{\Psi}^{\dagger\dagger}_{S+R}\restriction^R$

(3) $\Sigma'_{S+R} \cong \Sigma^{\dagger\dagger}_{S+R}$ *and* $X'_{S+R} \cong X^{\dagger\dagger}_{S+R}$ *and*

(4) $\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$ *and* $\Sigma^{\dagger\dagger}_{S+R} \approx_{S+R} X^{\dagger\dagger}_{S+R}$

Proof. The proof is very similar to Lemma 99 (V45: V4 Soundness Single step). We only discuss the key aspects.

By Rule V45:Single-Base and $X_{S+R} \cong X^{\dagger}_{S+R}$ we know that $minWndw(X_{S+R}) > 0$ (similar for $X^{\dagger}_{S+R}$). This means Rule V45-SE-Context applies. We now need to find a step $\Psi_{S+R} \xrightarrow{\tau'}_{S+R} \overline{\Psi}'_{S+R}$ and $\Psi^{\dagger}_{S+R} \xrightarrow{\tau'}_{S+R} \overline{\Psi}^{\dagger\dagger}_{S+R}$. Note that Rule V45-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 93 and Lemma 92 we get $\Sigma_{S+R}\restriction^R \approx_R X_{S+R}\restriction^R$ and $\Sigma_{S+R}\restriction^R \cong \Sigma^{\dagger}_{S+R}\restriction^R$.

Because of $\Phi_{S+R}\restriction^R \xrightarrow{\tau}_R \overline{\Phi}'_{S+R}\restriction^R$ and $\Phi^{\dagger}_{S+R}\restriction^R \xrightarrow{\tau}_R \overline{\Phi}^{\dagger\dagger}_{S+R}\restriction^R$ and Rule V45:Single-Base, we fulfill all premises for Lemma 79 (R: Soundness Single Step AM) and derive a step in the oracle semantics:

a) $\Sigma'_{S+R}\restriction^R \cong \Sigma^{\dagger\dagger}_{S+R}\restriction^R$ and $X'_{S+R}\restriction^R \cong X^{\dagger\dagger}_{S+R}\restriction^R$
b) $\Sigma'_{S+R}\restriction^R \approx_R X'_{S+R}\restriction^R$ and $\Sigma^{\dagger\dagger}_{S+R}\restriction^R \approx_R X^{\dagger\dagger}_{S+R}\restriction^R$
c) $\Psi_{S+R}\restriction^R \xrightarrow{\tau}_R \overline{\Psi}'_{S+R}\restriction^{R'}$ and $\Psi^{\dagger}_{S+R}\restriction^R \xrightarrow{\tau}_R \overline{\Psi}^{\dagger}_{S+R}\restriction^R$ the step of the oracle

Since we have $\Psi_{S+R}\restriction^S \xrightarrow{\tau}_S \overline{\Psi}'_{S+R}\restriction^{S'}$ we can derive a step $\Psi_{S+R} \xrightarrow{\tau'}_{S+R} \overline{\Psi}'_{S+R}$ using Rule V45-SE:v5-step (or another applicable rule by Lemma 83 (V45 AM: Confluence)).

Let us collect what we already have:

$$\begin{aligned} X'_{S+R} &= X''_{S+R} \cdot \overline{\Psi}'_{S+R} \\ \Sigma'_{S+R} &= \Sigma''_{S+R} \cdot \overline{\Phi}'_{S+R} \\ X^{\dagger\dagger}_{S+R} &= X^{*}_{S+R} \cdot \overline{\Psi}^{\dagger\dagger}_{S+R} \\ \Sigma^{\dagger\dagger}_{S+R} &= \Sigma^{*}_{S+R} \cdot \overline{\Phi}^{\dagger\dagger}_{S+R} \end{aligned}$$

We now need to show that $\Sigma'_{S+R} \cong \Sigma^{\dagger\dagger}_{S+R}$ and $X'_{S+R} \cong X^{\dagger\dagger}_{S+R}$ and $\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$ and $\Sigma^{\dagger\dagger}_{S+R} \approx_{S+R} X^{\dagger\dagger}_{S+R}$ hold.

The proof for $\Sigma'_{S+R} \cong \Sigma^{\dagger\dagger}_{S+R}$ and $X'_{S+R} \cong X^{\dagger\dagger}_{S+R}$ is anlaogous to the corresponding case in Lemma 99 (V45: V4 Soundness Single step).

We first check if there is a transaction of V4 that needs to be rolled back in X'_{S+R}, since the speculation window of each instance was reduced.

This has to be done, because we only know that $minWndw(X'_{S+R}) > 0$ *before* we did the step. So it could happen that $minWndw(X'_{S+R}) = 0$ for some transaction of V4 that needs to be rolled back.

Transaction of V4 that needs to be rolled back in X'_{S+R} with window 0 The step made cannot create a new speculative instance of V4. This means we can derive all premises of Rule V45:Single-Transaction-Rollback just from $\Sigma_{S+R} \approx_{S+R} X_{S+R}$. Thus, we have $\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$ by Rule V45:Single-Transaction-Rollback.

No V4 Transaction that needs to be rolled back in X'_{S+R} with window 0 Since the speculation window was reduced for all entries in X'_{S+R} and only for the topmost entry in Σ_{S+R} and we had $INV(\Sigma_{S+R}, X_{S+R})$ from $\Sigma_{S+R} \approx_{S+R} X_{S+R}$, we have $INV(\Sigma'_{S+R}, X'_{S+R})$ again. This reasoning extends to newly created instances by speculation as well.

We do a case distinction on $\approx_R$:

Rule Single-Base Analogous to the corresponding case in Lemma 99 (V45: V4 Soundness Single step).

Rule Single-OracleTrue Analogous to the corresponding case in Lemma 99 (V45: V4 Soundness Single step).

Rule Single-Transaction-Rollback Then one of the instances in $X'_{S+R}\restriction^R$ needs to be rolled back.

This means the same instance in X'_{S+R} needs to be rolled back as well.

We do a case distinction if the instance is part of $\overline{\Psi}'_{S+R}$ or not.

These cases are analogous to the corresponding cases in Lemma 99 (V45: V4 Soundness Single step).

□

K.5 Completeness Proof

Definition 65 (V45: Relation between AM and Spec for oracles that only mispredict)**.** *We define two relations,* $\approx^{O_{am}}$ *and* $\sim$*, between AM and oracle semantics. Note that* $\approx^{O_{am}}$ *is indexed by an oracle. This oracle has to always mispredict.*

Note that the condition $x = false \vee (x \in \mathbb{N} \wedge x \neq m(a(\mathbf{sp})))$ *just encapsulates the speculation of both V4 and V5.* $x = false$ *is the condition for V4, whereas* $x \neq m(a(\mathbf{sp}))$ *is the condition for V5 for misprediction.*

$$\boxed{\Sigma_{S+R} \approx^{O_{am}}_{S+R} X_{S+R}}$$

$$\frac{\text{(V45:Base-Oracle)}}{\varnothing \approx^{O_{am}}_{S+R} \varnothing} \qquad \frac{\Sigma_{S+R} \sim X_{S+R}\restriction_{com} \quad \text{(V45:Single-Base-Oracle)}\ INV2(\Sigma_{S+R}, X_{S+R}) \quad minWndw(X_{S+R}) > 0}{\Sigma_{S+R} \approx^{O_{am}}_{S+R} X_{S+R}}$$

$$\frac{\begin{array}{ccc}\Sigma''_{S+R} \sim X''_{S+R}\restriction_{com} & n' \geq 0 & \Sigma''_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma'''_{S+R} \text{ where transaction with id ctr is rolled back} \quad x = (S, true) \vee (R, m) \\ X_{S+R} = X'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle & & \Sigma_{S+R} = \Sigma'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \quad INV2(\Sigma_{S+R}, X_{S+R})\end{array}}{\Sigma'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle^x \cdot \Sigma_{S_1} \approx^{O_{am}}_{S+R} X'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0 \rangle^x}$$

Lemma 101 (V45: Coincide on $\approx^{O_{am}}_{S+R}$ for projections)**.** *If*

(1) $\Sigma_{S+R} \approx^{O_{am}}_{S+R} X_{S+R}$ *by Rule V45:Single-Base*

Then

(1) $\Sigma_{S+R}\restriction^S \approx^{O_{am}}_{S} X_{S+R}\restriction^S$ *by Rule Single-Base-Oracle and*

(2) $\Sigma_{S+R}\restriction^R \approx^{O_{am}}_{R} X_{S+R}\restriction^R$ *by Rule Single-Base-Oracle*

Proof. The proof is analogous to Lemma 92 (V45: Coincide on $\approx_{S+R}$ for projections). □

Definition 66 (V45: Constructing the AM Oracle)**.** *We rely for the construction of the oracle $O_{am_{S+R}}$ on the construction of its parts. Here Definition 56 (Constructing the Oracle) and Definition 62 (R: Constructing the Oracle).*

Thus, we have: $O_{am_{S+R}} = (O_{am_S}, O_{am_R})$ for the speculative oracle combined semantics.

Lemma 102 (V45: Completeness Am semantics w.r.t. speculative semantics)**.** *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, σ, $\sigma' \in InitConf$ be two initial configurations. If*

(1) $(p, \sigma) \text{👻}^{\omega}_{S+R} \overline{\tau}$ *and* $(p, \sigma') \text{👻}^{\omega}_{S+R} \overline{\tau}'$ *and*

(2) $\overline{\tau} \neq \overline{\tau}'$

Then there exists an oracle O such that

I $(p, \sigma) \text{👻}^{O}_{S+R} \overline{\tau}_1$ *and* $(p, \sigma') \text{👻}^{O}_{S+R} \overline{\tau}'_1$ *and*

II $\overline{\tau}_1 \neq \overline{\tau}'_1$

Proof. Let $\omega \in \mathbb{N}$ be a speculative window, $\sigma, \sigma' \in InitConf$ be two initial configurations. We have If

(1) $(p, \sigma) \text{👻}^{\omega}_{S+R} \overline{\tau}$ and $(p, \sigma') \text{👻}^{\omega}_{S+R} \overline{\tau}'$ and

(2) $\overline{\tau} \neq \overline{\tau}'$

By definition of 👻^{ω}_{S+R} we have two final states Σ_{S+R_F} and Σ'_{S+R_F} such that $\Sigma^{init}_{S+R}(p, \sigma) \Downarrow^{\overline{\tau}}_{S+R} \Sigma_{S+R_F}$ $\Sigma^{init}_{S} p, \sigma' \Downarrow^{\overline{\tau}'}_{S+R} \Sigma'_{S+R_F}$. Combined with the fact that $\overline{\tau} \neq \overline{\tau}'$, it follows that there are speculative states $\Sigma^{*}_{S+R}, \Sigma^{**}_{S+R}, \Sigma^{\dagger}_{S+R}, \Sigma^{\dagger\dagger}_{S+R}$ and sequences of observations $\overline{\tau}, \overline{\tau}_{end}, \overline{\tau}'_{end}, \tau_{am}, \tau'_{am}$ such that $\tau_{am} \neq \tau'_{am}$, $\Sigma^{*}_{S+R} \cong \Sigma^{\dagger}_{S+R}$ and:

$$\Sigma^{init}_{S+R}(p, \sigma) \Downarrow^{\overline{\tau}}_{S+R} \Sigma^{*}_{S+R} \xrightarrow{\tau_{am}}_{S+R} \Sigma^{**}_{S+R} \Downarrow^{\overline{\tau}_{end}}_{S+R} \Sigma_{S+R_F}$$

$$\Sigma^{init}_{S+R}(p, \sigma') \Downarrow^{\overline{\tau}}_{S+R} \Sigma^{\dagger}_{S+R} \xrightarrow{\tau'_{am}}_{S+R} \Sigma^{\dagger\dagger}_{S+R} \Downarrow^{\overline{\tau}'_{end}}_{S+R} \Sigma'_{S+R_F}$$

We claim that there is a prediction oracle O with speculative window at most ω such that

a) $X^{init}_{S+R}(p, \sigma) \overset{O_{S+R}}{\wr}{}^{S+R}_{v} X^{*}_{S+R}$ and $X^{*}_{S+R}.\sigma = \Sigma^{*}_{S+R}.\sigma$ and $INV2(X^{*}_{S+R}, \Sigma^{*}_{S+R})$ and

b) $X^{init}_{S+R}(p, \sigma') \overset{O_{S+R}}{\wr}{}^{S+R}_{v} X^{\dagger}_{S+R}$ and $X^{\dagger}_{S+R}.\sigma = \Sigma^{\dagger}_{S+R}.\sigma$ and $INV2(X^{\dagger}_{S+R}, \Sigma^{\dagger}_{S+R})$

c) $X^{*}_{S+R} \cong X^{\dagger}_{S+R}$

We achieve this by applying Lemma 103 (V45: Stronger Soundness for a specific oracle and for specific executions) on the AM execution up to the point of the difference i.e., $\Sigma^{init}_{S+R}(p, \sigma) \Downarrow^{\overline{\tau}}_{S+R} \Sigma^{*}_{S+R}$ and $\Sigma^{init}_{S+R}(p, \sigma') \Downarrow^{\overline{\tau}}_{S+R} \Sigma^{\dagger}_{S+R}$.

We now show that $\Sigma^{*}_{S+R} \approx^{O_{am}} X^{*}_{S+R}$ is derived by Rule V45:Single-Base-Oracle.

We do a case distinction if there are ongoing speculative transactions in X^{*}_{S+R} or not:

no ongoing transactions in X^{*}_{S+R} Then, Σ^{*}_{S+R} has no ongoing transactions as well and we have by $INV2(\Sigma^{*}_{S+R}, X^{*}_{S+R})$ and $\Sigma^{*}_{S+R}.n = \bot$ that $X^{*}_{S+R}.n = \bot$ that $\Sigma^{*}_{S+R} \approx^{O_{am}} X^{*}_{S+R}$ can only be derived Rule V45:Single-Base-Oracle .

ongoing transactions in X^{*}_{S+R} By the definition of the oracle O, we know that the for the transaction id where the difference $\tau_{am} \neq \tau_{am'}$ happens, the oracle mispredicted with a speculation window of ω. This is also the topmost transaction in X_{S+R}. Furthermore, we know that $X^{*}_{S+R}.n \geq minWndw(X^{*}_{S+R})$ by definition of the oracle $O_{am_{S+R}}$ and $minWndw()$.

Since the next rule cannot be Rule AM-v4-Rollback-V45 or Rule AM-v5-Rollback-V45, we know that $\Sigma^*_{S+R}.n > 0$ and by $INV2(\Sigma^*_{S+R}, X^*_{S+R})$ we get $minWndw(X^*_{S+R}) > 0$ (Similar for $X^\dagger_{S+R}$ because of $\Sigma^*_{S+R} \cong \Sigma^\dagger_{S+R}$).
If $\Sigma^*_{S+R} \approx^{O_{am}} X^*_{S+R}$ by rollback rule, we would have a contradiction because we would need the topmost speculation window of $X^*_{S+R}.n = 0$. But we know that $minWndw(X^*_{S+R}) > 0$, because the speculation window of the topmost instance was created with a speculation window of ω.
Now we know that $X^*_{S+R} \approx^{O_{am}} \Sigma^*_{S+R}$ by Rule V45:Single-Base-Oracle.

We proceed by case analysis on the rule in $\not\Longrightarrow_{S+R}$ used to derive $\Sigma^*_{S+R} \overset{\tau_{am}}{\not\Longrightarrow}_{S+R} \Sigma^{**}_{S+R}$. Because $\Sigma^*_{S+R} \cong \Sigma^\dagger_{S+R}$ and $\overline{\tau}_1 = \overline{\tau}'_1$, we know that the same rule was used in $\Sigma^\dagger_{S+R} \overset{\tau'_{am}}{\not\Longrightarrow}_S \Sigma^{\dagger\dagger}_{S+R}$ as well.

Rule AM-v4-Rollback-V45 Contradiction. Because $\Sigma^*_{S+R} \cong \Sigma^\dagger_{S+R}$ we have for all instances $\Phi_1.ctr = \Phi'_1.ctr$.
Since the same instance would be rolled back, we have $\tau_{am} = \tau'_{am}$.

Rule AM-v5-Rollback-V45 Analogous to the case above.

Rule AM-Context-V45 By inversion on Rule AM-Context-V45 for the step $\Sigma^*_{S+R} \overset{\tau_{am}}{\not\Longrightarrow}_{S+R} \Sigma^{**}_{S+R}$ we have $\Sigma^*_{S+R} = \overline{\Phi}_{S+R} \cdot \Phi_{S+R}$ and $\Sigma^{**}_{S+R} = \overline{\Phi}_{S+R} \cdot \overline{\Phi}'_{S+R}$ with $\Phi_{S+R} \overset{\tau_{am}}{\not\Longrightarrow}_{S+R} \overline{\Phi}'_{S+R}$.
We now do inversion on $\Phi_{S+R} \overset{\tau_{am}}{\not\Longrightarrow}_{S+R} \overline{\Phi}'_{S+R}$:

Rule AM-v4-step-V45 Then we have $\Phi_{B+S} \restriction^S \overset{\tau}{\not\Longrightarrow}_S \overline{\Phi}'_S \restriction^S$.
The case is analogous to Lemma 49 (Completeness Am semantics w.r.t. speculative semantics) in the Rule S:AM-Context case.

Rule AM-v5-step-V45 Then we have $\Phi_{S+R} \restriction^R \overset{\tau}{\not\Longrightarrow}_R \overline{\Phi}'_R$.
The case is analogous to Lemma 80 (R: Completeness AM semantics w.r.t. speculative semantics) in the Rule R:AM-Context case.

This completes the proof of our claim.

□

Lemma 103 (V45: Stronger Soundness for a specific oracle and for specific executions)**.** *Specific executions means that there is a difference in the trace but before there is none. We use the oracle O_{am} as it is defined by Definition 66 (V45: Constructing the AM Oracle) for the given execution. If*

(1) $\Sigma_{S+R} \cong \Sigma^\dagger_{S+R}$
(2) $X_{S+R} \cong X^\dagger_{S+R}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma_{S+R} \approx^{O_{am}}_{S+R} X_{S+R}$ *and* $\Sigma^\dagger_{S+R} \approx^{O_{am}}_{S+R} X^\dagger_{S+R}$
(4) $\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma'_{S+R}$ *and* $\Sigma^\dagger_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma^{\dagger\dagger}_{S+R}$

and our oracle is constructed in the way described above Then

I $X_{S+R} \overset{O_{S+R}}{\downarrow}{}^{S+R}_{\overline{\tau}'} X'_{S+R}, X^\dagger_{S+R} \overset{O_S}{\downarrow}{}^{S}_{\overline{\tau}''} X^{\dagger\dagger}_{S+R}$
II $\Sigma'_{S+R} \cong \Sigma^{\dagger\dagger}_{S+R}$
III $X'_{S+R} \cong X^{\dagger\dagger}_{S+R}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{S+R} \approx^{O_{am}} X'_{S+R}$ *and* $\Sigma^{\dagger\dagger}_{S+R} \approx^{O_{am}} X^{\dagger\dagger}_{S+R}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. Notice that the proof is very similar to Lemma 98 (V45: Soundness Am semantics w.r.t. speculative semantics with new relation between states). The only thing that is different is that (1) the specific oracle only mispredicts so there is one less case in the relation and (2) we have a different invariant for that specific oracle i.e., $INV2(\Sigma_{S+R}, X_{S+R})$

For these reasons we will only argue why $INV2(\Sigma^\dagger_{S+R}, X'_{S+R})$ holds in the different cases and leave the rest to the old soundness proof.

By Induction on $\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma'_{S+R}$ and $\Sigma^\dagger_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma^{\dagger\dagger}_{S+R}$.

Rule AM-Reflection-V45 We have $\Sigma_{S+R} \Downarrow^{\varepsilon}_{S+R} \Sigma'_{S+R}$ and $\Sigma^\dagger_{S+R} \Downarrow^{\varepsilon}_{S+R} \Sigma''_{S+R}$, where $\Sigma'_{S+R} = \Sigma_{S+R}$ and $\Sigma''_{S+R} = \Sigma^\dagger_{S+R}$. We choose $\Sigma'_{S+R} = \Sigma'_{S+R}$ and $\Sigma^{\dagger\dagger}_{S+R} = \Sigma''_{S+R}$.
We further use Rule S:Reflection to derive $X_{S+R} \overset{O_{S+R}}{\downarrow}{}^{S+R}_{\varepsilon} X'_{S+R}, X^\dagger_{S+R} \overset{O_{S+R}}{\downarrow}{}^{S+R}_{\varepsilon} X^{\dagger\dagger}_{S+R}$ with $X'_{S+R} = X_{S+R}$ and $X^{\dagger\dagger}_{S+R} = X^\dagger_{S+R}$. We now trivially satisfy all conclusions.

Rule AM-Single-V45 We have $\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma''_{S+R}$ with $\Sigma''_{S+R} \overset{\tau}{\not\Longrightarrow}_{S+R} \Sigma'_{S+R}$ and $\Sigma^\dagger_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma^*_{S+R}$ and $\Sigma^*_{S+R} \overset{\tau}{\not\Longrightarrow}_{S+R} \Sigma^{\dagger\dagger}_{S+R}$.
We now apply IH on $\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma''_{S+R}$ and $\Sigma^\dagger_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma^*_{S+R}$ and get
(a) $X_{S+R} \overset{O_{S+R}}{\downarrow}{}^{S+R}_{\overline{\tau}'} X''_{S+R}, X^\dagger_{S+R} \overset{O_{S+R}}{\downarrow}{}^{S+R}_{\overline{\tau}''} X^*_{S+R}$

(b) $\Sigma''_{S+R} \cong \Sigma^*_{S+R}$
(c) $X''_{S+R} \cong X^*_{S+R}$ and $\overline{\rho}' = \varnothing$
(d) $\Sigma''_{S+R} \approx^{O_{am}}_{S+R} X''_{S+R}$ and $\Sigma^*_{S+R} \approx^{O_{am}}_{S+R} X^*_{S+R}$
(e) $\overline{\tau}' = \overline{\tau}''$

We do a case distinction on $\approx^{O_{am}}_{S+R}$ in $\Sigma''_{S+R} \approx^{O_{am}}_{S+R} X''_{S+R}$ and $\Sigma^*_{S+R} \approx^{O_{am}} X^*_{S+R}$:

Rule V45:Single-Base-Oracle We thus have $\Sigma''_{S+R} \sim X''_{S+R}\restriction_{com}$, $minWndw(X''_{S+R}) > 0$ and $INV2(\Sigma''_{S+R}, X''_{S+R})$ (Similar for Σ^*_{S+R} and X^*_{S+R}).

We now proceed by inversion on the derivation $\Sigma''_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Sigma'_{S+R}$:

Rule AM-v4-Rollback-V45 Contradiction, since $minWndw(X''_{S+R}) > 0$ and $INV2(\Sigma''_{S+R}, X''_{S+R})$.

Rule AM-v5-Rollback-V45 Analogous to above.

Rule AM-Context-V45 We have $\Phi_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}'_{S+R}$ and $n > 0$.

We now use inversion on $\Phi_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}_{S+R}$:

Rule AM-v4-step-V45 Then, we have $\Phi_{S+R}\restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_{S+R}\restriction^S$
We use Lemma 99 (V45: V4 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule AM-v5-step-V45 Then, we have $\Phi_{S+R}\restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_{S+R}\restriction^R$
We use Lemma 100 (V45: V5 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule V45:Single-Transaction-Rollback-Oracle We have

$$\begin{aligned}
X''_{S+R} &= X_{S+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0 \rangle^x \cdot X_{S+R4} \\
\Sigma''_{S+R} &= \Sigma_{S+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle^x \cdot \Sigma_{S+R4} \\
X_{S+R} &= X_{S+R3} \cdot \langle p, ctr, \sigma, h, \mathbb{R}, n'' \rangle \\
\Sigma_{S+R} &= \Sigma_{S+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \\
\Sigma_{S+R} &\sim X_{S+R}\restriction_{com} \\
INV2(\Sigma_{S+R}, X_{S+R}) & \\
n' &\geq 0
\end{aligned}$$

The form of X^*_{S+R} and Σ^*_{S+R} is analogous.
Additionally we know that the transaction terminates in some state $\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{S+R} \Sigma'''_{S+R}$. There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma''_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Sigma'_{S+R}$ is not a roll back. Because Σ_{S+R} and X_{S+R} do not change, $INV2(\Sigma_{S+R}, X_{S+R})$ does not change as well.

$n' = 0$ Then we know that $\Sigma''_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \Sigma'_{S+R}$ was created by Rule AM-v4-Rollback-V45 or Rule AM-v5-Rollback-V45 and is a rollback for *ctr*.
Notice, that the only difference to X_{S+R} and Σ_{S+R} is the updated *ctr*, because of the roll back. Updating the counter does not change the invariant *INV2*(). This means $INV2(\Sigma_{S+R}, X_{S+R})$ (with updated *ctr*) still holds.

□

Lemma 104 (V45: Stronger V4 Soundness Single step)**.** *If*

(1) $\Sigma_{S+R} \approx^{O_{am}}_{S+R} X_{S+R}$ *and* $\Sigma^\dagger_{S+R} \approx^{O_{am}}_{S+R} X^\dagger_{S+R}$ *by Rule V45:Single-Base-Oracle and*
(2) $\Sigma_{S+R} \cong \Sigma^\dagger_{S+R}$ *and* $X_{S+R} \cong X^\dagger_{S+R}$ *and*
(3) $\Phi_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}'_{S+R}$ *and* $\Phi^\dagger_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}^{\dagger\dagger}_{S+R}$ *by*
(4) $\Phi_{S+R}\restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_{S+R}\restriction^S$ *and* $\Phi^\dagger_{S+R}\restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}^{\dagger\dagger}_{S+R}\restriction^S$

Then

(1) $\Psi_{S+R} \overset{\tau', O_{S+R}}{\rightsquigarrow}_{S+R} \overline{\Psi}'_{S+R}$ *and* $\Psi^\dagger_{S+R} \overset{\tau', O_{S+R}}{\rightsquigarrow}_{S+R} \overline{\Psi}^{\dagger\dagger}_{S+R}$ *in combination with Context rule*
(2) $\Psi_{S+R} \overset{\tau, O_{S+R}}{\rightsquigarrow}_{S+R} \overline{\Psi}'_{S+R}$ *and* $\Psi^\dagger_{S+R} \overset{\tau, O_{S+R}}{\rightsquigarrow}_{S+R} \overline{\Psi}^{\dagger\dagger}_{S+R}$
(3) $\Sigma'_{S+R} \cong \Sigma^{\dagger\dagger}_{S+R}$ *and* $X'_{S+R} \cong X^{\dagger\dagger}_{S+R}$ *and*
(4) $\Sigma'_{S+R} \approx^{O_{am}}_{S+R} X'_{S+R}$ *and* $\Sigma^{\dagger\dagger}_{S+R} \approx^{O_{am}}_{S+R} X^{\dagger\dagger}_{S+R}$

Proof. By Rule V45:Single-Base-Oracle and $X_{S+R} \cong X^{\dagger}_{S+R}$ we know that $minWndw(X_{S+R}) > 0$ (similar for $X^{\dagger}_{S+R}$). This means Rule V45-SE-Context applies. We now need to find a step $\Psi_{S+R} \xrightarrow{\tau'}_{S+R} \overline{\Psi}'_{S+R}$ and $\Psi^{\dagger}_{S+R} \xrightarrow{\tau'}_{S+R} \overline{\Psi}^{\dagger\dagger}_{S+R}$. Note that Rule V45-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 93 and Lemma 101 we get $\Sigma_{S+R}\restriction^S \approx_S X_{S+R}\restriction^S$ and $\Sigma_{S+R}\restriction^S \cong \Sigma^{\dagger}_{S+R}\restriction^S$.

Because of $\Phi_{S+R}\restriction^S \xrightarrow{\tau}_S \overline{\Phi}'_{S+R}\restriction^S$ and $\Phi^{\dagger}_{S+R}\restriction^S \xrightarrow{\tau}_S \overline{\Phi}^{\dagger\dagger}_{S+R}\restriction^S$ and Rule V45:Single-Base-Oracle, we fulfill all premises for Lemma 50 (Stronger Soundness for a specific oracle and for specific executions) and derive a step in the oracle semantics:

a) $\Sigma'_{S+R}\restriction^S \cong \Sigma^{\dagger\dagger}_{S+R}\restriction^S$ and $X'_{S+R}\restriction^S \cong X^{\dagger\dagger}_{S+R}\restriction^S$
b) $\Sigma'_{S+R}\restriction^S \approx^{O_{am}}_S X'_{S+R}\restriction^S$ and $\Sigma^{\dagger\dagger}_{S+R}\restriction^S \approx^{O_{am}}_S X^{\dagger\dagger}_{S+R}\restriction^S$
c) $\Psi_{S+R}\restriction^S \xrightarrow{\tau}_S \overline{\Psi}'_{S+R}\restriction^{S'}$ and $\Psi^{\dagger}_{S+R}\restriction^S \xrightarrow{\tau}_S \overline{\Psi}^{\dagger}_{S+R}\restriction^S$ the step of the oracle

Since we have $\Psi_{S+R}\restriction^S \xrightarrow{\tau}_S \overline{\Psi}'_{S+R}\restriction^{S'}$ we can derive a step $\Psi_{S+R} \xrightarrow{\tau'}_{S+R} \overline{\Psi}'_{S+R}$ using Rule V45-SE:v4-step (or another applicable rule by Lemma 91 (V45SE: Confluence)).

Let us collect what we already have:

$$
\begin{aligned}
X'_{S+R} &= X''_{S+R} \cdot \overline{\Psi}'_{S+R} \\
\Sigma'_{S+R} &= \Sigma''_{S+R} \cdot \overline{\Phi}'_{S+R} \\
X^{\dagger\dagger}_{S+R} &= X^{*}_{S+R} \cdot \overline{\Psi}^{\dagger\dagger}_{S+R} \\
\Sigma^{\dagger\dagger}_{S+R} &= \Sigma^{*}_{S+R} \cdot \overline{\Phi}^{\dagger\dagger}_{S+R}
\end{aligned}
$$

We now need to show that $\Sigma'_{S+R} \cong \Sigma^{\dagger\dagger}_{S+R}$ and $X'_{S+R} \cong X^{\dagger\dagger}_{S+R}$ and $\Sigma'_{S+R} \approx^{O_{am}}_{S+R} X'_{S+R}$ and $\Sigma^{\dagger\dagger}_{S+R} \approx^{O_{am}}_{S+R} X^{\dagger\dagger}_{S+R}$ hold.

$\Sigma'_{S+R} \cong \Sigma^{\dagger\dagger}_{S+R}$ and $X'_{S+R} \cong X^{\dagger\dagger}_{S+R}$ Analogous to the corresponding case in Lemma 99 (V45: V4 Soundness Single step)

$\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$ and $\Sigma^{\dagger\dagger}_{S+R} \approx_{S+R} X^{\dagger\dagger}_{S+R}$ We want to show that $\Sigma'_{S+R} \approx^{O_{am}}_{S+R} X'_{S+R}$. The case for $\Sigma^{\dagger\dagger}_{S+R} \approx^{O_{am}}_{S+R} X^{\dagger\dagger}_{S+R}$ is analogous.

We first check if there is a transaction of V5 that needs to be rolled back in X'_{S+R}, since the speculation window of each instance was reduced.

This has to be done, because we only know that $minWndw(X'_{S+R}) > 0$ *before* we did the step. So it could happen that $minWndw(X'_{S+R}) = 0$ for some transaction of V5 that needs to be rolled back (we can ignore transactions that will be committed).

Transaction of V5 that needs to be rolled back in X'_{S+R} with window 0 The step made cannot create a new speculative instance of V5 that would be on top. This means we can derive all premises of Rule V45:Single-Transaction-Rollback-Oracle just from $\Sigma_{S+R} \approx^{O_{am}}_{S+R} X_{S+R}$. Thus, we have $\Sigma'_{S+R} \approx^{O_{am}}_{S+R} X'_{S+R}$ by Rule V45:Single-Transaction-Rollback-Oracle.

No V5 Transaction that needs to be rolled back in X'_{S+R} with window 0 We do a case distinction on $\approx^{O_{am}}_S$:

Rule Single-Base-Oracle Since the speculation window was reduced for all entries in X'_{S+R} and only for the topmost entry in Σ_{S+R} and we had $INV2(\Sigma_{S+R}, X_{S+R})$ from $\Sigma_{S+R} \approx^{O_{am}}_{S+R} X_{S+R}$, we have $INV2(\Sigma'_{S+R}, X'_{S+R})$ again. If a new speculative state was created, we know from the oracle that the speculation window is either 0 or ω.

It cannot be 0 because then the states would be related by Rule Single-Transaction-Rollback-Oracle.

If it is ω we have $minWndw(X_{S+R}) \leq \omega$ and combined with $INV2(\Sigma_{S+R}, X_{S+R})$ we have $INV2(\Sigma'_{S+R}, X'_{S+R})$

We can then conclude from $\Sigma_{S+R} \approx_{S+R} X_{S+R}$ that $\Sigma''_{S+R} \sim X''_{S+R}\restriction_{com}$.

From $\approx^{O_{am}}_S$ we get $\overline{\Phi}'_{S+R}\restriction^S \sim \overline{\Psi}'_{S+R}\restriction^S\restriction_{com}$.

And combined with $\Sigma'_{S+R} \cong X'_{S+R}$, we get $\overline{\Phi}'_{S+R} \sim \overline{\Psi}'_{S+R}\restriction_{com}$.

Because $INV2(\Sigma'_{S+R}, X'_{S+R})$ holds from above, we can conclude that $\Sigma'_{S+R} \approx^{O_{am}}_{S+R} X'_{S+R}$ are related by Rule V45:Single-Base-Oracle.

Rule Single-Transaction-Rollback-Oracle Then one of the instances in $X'_{S+R}\restriction^S$ needs to be rolled back.

This means the same instance in X'_{S+R} needs to be rolled back as well.

We do a case distinction if the instance is part of $\overline{\Psi}'_{S+R}$ or not:

instance is not part of $\overline{\Psi}'_{S+R}$ Since the instance is not part of $\overline{\Psi}'_{S+R}$, it is part of X''_{S+R}. This means from $\Sigma_{S+R} \approx^{O_{am}}_{S+R} X_{S+R}$ related by Rule V45:Single-Base-Oracle, we get all the necessary facts to conclude that $\Sigma'_{S+R} \approx^{O_{am}}_{S+R} X'_{S+R}$ by Rule V45:Single-Transaction-Rollback-Oracle.

instance is part of $\overline{\Psi}_{S+R}$ We do a case distinction if a new state was created or not:

$|\overline{\Psi}_{S+R}| = 1$ Because we only need to relate below $\overline{\Psi}_{S+R}$ to relate by Rule V45:Single-Transaction-Rollback-Oracle, we can reuse our reasoning in the case above to conclude $\Sigma'_{S+R} \approx^{O_{am}}_{S+R} X'_{S+R}$ by Rule V45:Single-Transaction-Rollback-Oracle.

$|\overline{\Psi}_{S+R}| = 2$ Then we have

$$\overline{\Psi}'_{S+R} = \Psi_{S+R} \cdot \langle p, ctr, \sigma, h, \mathbb{R}, n\rangle^{true}$$
$$\overline{\Phi}'_{S+R} = \Phi_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n'\rangle^{true}$$

From $\approx_S$ we get $\Phi_{S+R}\restriction^S \sim \Psi_{S+R}\restriction^S$ and since only the projection changed during the step we have $\Phi_{S+R} \sim \Psi_{S+R}$. The reason for$INV2(\Phi_{S+R}, \Psi_{S+R})$ is the same as in case Rule Single-Base-Oracle above.

For all instances below $\overline{\Phi}_{S+R}$, we can use the fact that $\Sigma_{S+R} \approx^{O_{am}}_{S+R} X_{S+R}$ related by Rule V45:Single-Base-Oracle to conclude that $\Sigma'_{S+R} \approx_{S+R} X'_{S+R}$ Rule V45:Single-Transaction-Rollback-Oracle

□

Lemma 105 (V45: Stronger V5 Soundness Single step)**.** *If*

(1) $\Sigma_{S+R} \approx^{O_{am}}_{S+R} X_{S+R}$ *and* $\Sigma^{\dagger}_{S+R} \approx^{O_{am}}_{S+R} X^{\dagger}_{S+R}$ *by Rule V45:Single-Base-Oracle and*
(2) $\Sigma_{S+R} \cong \Sigma^{\dagger}_{S+R}$ *and* $X_{S+R} \cong X^{\dagger}_{S+R}$ *and*
(3) $\Phi_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}'_{S+R}$ *and* $\Phi^{\dagger}_{S+R} \overset{\tau}{\dashrightarrow}_{S+R} \overline{\Phi}^{\dagger\dagger}_{S+R}$ *by*
(4) $\Phi_{S+R}\restriction^S \overset{\tau}{\dashrightarrow}_{S} \overline{\Phi}'_{S+R}\restriction^S$ *and* $\Phi^{\dagger}_{S+R}\restriction^S \overset{\tau}{\dashrightarrow}_{S} \overline{\Phi}^{\dagger\dagger}_{S+R}\restriction^S$

Then

(1) $\Psi_{S+R} \overset{\tau', O_{S+R}}{\rightsquigarrow}_{S+R} \overline{\Psi}'_{S+R}$ *and* $\Psi^{\dagger}_{S+R} \overset{\tau', O_{S+R}}{\rightsquigarrow}_{S+R} \overline{\Psi}^{\dagger\dagger}_{S+R}$ *in combination with Context rule*
(2) $\Psi_{S+R} \overset{\tau, O_{S+R}}{\rightsquigarrow}_{S+R} \overline{\Psi}'_{S+R}$ *and* $\Psi^{\dagger}_{S+R} \overset{\tau, O_{S+R}}{\rightsquigarrow}_{S+R} \overline{\Psi}^{\dagger\dagger}_{S+R}$
(3) $\Sigma'_{S+R} \cong \Sigma^{\dagger\dagger}_{S+R}$ *and* $X'_{S+R} \cong X^{\dagger\dagger}_{S+R}$ *and*
(4) $\Sigma'_{S+R} \approx^{O_{am}}_{S+R} X'_{S+R}$ *and* $\Sigma^{\dagger\dagger}_{S+R} \approx^{O_{am}}_{S+R} X^{\dagger\dagger}_{S+R}$

Proof. By Rule V45:Single-Base-Oracle and $X_{S+R} \cong X^{\dagger}_{S+R}$ we know that $minWndw(X_{S+R}) > 0$ (similar for $X^{\dagger}_{S+R}$). This means Rule V45-SE-Context applies. We now need to find a step $\Psi_{S+R} \overset{\tau'}{\dashrightarrow}_{S+R} \overline{\Psi}'_{S+R}$ and $\Psi^{\dagger}_{S+R} \overset{\tau'}{\dashrightarrow}_{S+R} \overline{\Psi}^{\dagger\dagger}_{S+R}$. Note that Rule V45-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 93 and Lemma 101 we get $\Sigma_{S+R}\restriction^R \approx^{O_{am}}_{R} X_{S+R}\restriction^R$ and $\Sigma_{S+R}\restriction^R \cong \Sigma^{\dagger}_{S+R}\restriction^R$.

Because of $\Phi_{S+R}\restriction^R \overset{\tau}{\dashrightarrow}_{R} \overline{\Phi}'_{S+R}\restriction^R$ and $\Phi^{\dagger}_{S+R}\restriction^R \overset{\tau}{\dashrightarrow}_{R} \overline{\Phi}^{\dagger\dagger}_{S+R}\restriction^R$ and Rule V45:Single-Base-Oracle, we fulfill all premises for Lemma 81 (Stronger Soundness for a specific oracle and for specific executions) and derive a step in the oracle semantics:

a) $\Sigma'_{S+R}\restriction^R \cong \Sigma^{\dagger\dagger}_{S+R}\restriction^R$ and $X'_{S+R}\restriction^R \cong X^{\dagger\dagger}_{S+R}\restriction^R$
b) $\Sigma'_{S+R}\restriction^R \approx^{O_{am}}_{R} X'_{S+R}\restriction^R$ and $\Sigma^{\dagger\dagger}_{S+R}\restriction^R \approx^{O_{am}}_{R} X^{\dagger\dagger}_{S+R}\restriction^R$
c) $\Psi_{S+R}\restriction^R \overset{\tau}{\dashrightarrow}_{R} \overline{\Psi}'_{S+R}\restriction^{R'}$ and $\Psi^{\dagger}_{S+R}\restriction^R \overset{\tau}{\dashrightarrow}_{R} \overline{\Psi}^{\dagger}_{S+R}\restriction^R$ the step of the oracle

Since we have $\Psi_{S+R}\restriction^R \overset{\tau}{\dashrightarrow}_{R} \overline{\Psi}'_{S+R}\restriction^{R'}$ we can derive a step $\Psi_{S+R} \overset{\tau'}{\dashrightarrow}_{S+R} \overline{\Psi}'_{S+R}$ using Rule V45-SE:v4-step (or another applicable rule by Lemma 91 (V45SE: Confluence)).

Let us collect what we already have:

$$X'_{S+R} = X''_{S+R} \cdot \overline{\Psi}'_{S+R}$$
$$\Sigma'_{S+R} = \Sigma''_{S+R} \cdot \overline{\Phi}'_{S+R}$$
$$X^{\dagger\dagger}_{S+R} = X^{*}_{S+R} \cdot \overline{\Psi}^{\dagger\dagger}_{S+R}$$
$$\Sigma^{\dagger\dagger}_{S+R} = \Sigma^{*}_{S+R} \cdot \overline{\Phi}^{\dagger\dagger}_{S+R}$$

We now need to show that $\Sigma'_{S+R} \cong \Sigma^{\dagger\dagger}_{S+R}$ and $X'_{S+R} \cong X^{\dagger\dagger}_{S+R}$ and $\Sigma'_{S+R} \approx^{O_{am}}_{S+R} X'_{S+R}$ and $\Sigma^{\dagger\dagger}_{S+R} \approx^{O_{am}}_{S+R} X^{\dagger\dagger}_{S+R}$ hold.

The rest of the proof is analogous to Lemma 104 (V45: Stronger V4 Soundness Single step).

□

L PROOFS V14

Theorem 27 (Well-formed Composition $\lightning_{B+S}$). $\vdash \lightning_{B+S} : WFC$

Proof. Immediately follows from Lemma 106 (V14 AM: Confluence), Theorem 29 (V14: Relating V1 with projection of combined), Theorem 28 (V14: Relating V4 with projection of combined) and Lemma 120 (V14: Soundness Am semantics w.r.t. speculative semantics with new relation between states). □

Lemma 106 (V14 AM: Confluence)**.** *If*

(1) $\Sigma_{B+S} \xrightarrow{\tau} \lightning_{B+S} \Sigma'_{B+S}$ *and*

(2) $\Sigma_{B+S} \xrightarrow{\tau} \lightning_{B+S} \Sigma''_{B+S}$ *derived by a different rule*

Then

(1) $\Sigma'_{B+S} = \Sigma_{B+S}$

Proof. Note that a difference can only come from using Rule AM-v1-step-V14 for one derivation and Rule AM-v4-step-V14 for the other. Since these two rules delegate back to the semantics of V1 and V4, we look which two rules are applicable there.
Let us first look at the instructions and rule that could lead to two different rules to be applied:

beqz x, ℓ, **store** x, e Contradiction. There are no two different rules to derive the steps. This is because of the metaparameter Z introduced into the semantics.

spbarr Then either Rule B:AM-barr and Rule S:AM-barr or Rule B:AM-barr-spec and Rule S:AM-barr-spec are used to derive the steps (dependent on the value of n).
The case is analogous to the corresponding case in Lemma 83 (V45 AM: Confluence).

otherwise Then Rule AM-NoBranch and Rule S:AM-NoBranch were used for different derivations.
The case is analogous to the corresponding case in Lemma 83 (V45 AM: Confluence).

□

We first define two relations for states of V1 and V4: These relations are virtually the same as the ones in V45.

$\boxed{\Sigma_B \approx \Sigma_{B+S}}$

$$\frac{}{\varnothing \approx \varnothing}\ \text{(V14-V1:Base)} \qquad \frac{\Sigma'_B \sim \Sigma'_{B+S}}{\Sigma'_B \cdot \langle p, ctr, \sigma, n\rangle \approx \Sigma'_{B+S} \cdot \langle p, ctr', \sigma, n\rangle}\ \text{(V14-V1:Single-Base)}$$

$$\frac{\Sigma_B \sim \Sigma_{B+S} \quad \Sigma''_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma'''_{B+S} \text{ where transaction with id } ctr \text{ is rolled back} \quad \Sigma_B = \Sigma'_B \cdot \langle p, ctr', \sigma, n\rangle \quad \Sigma_{B+S} = \Sigma'_{B+S} \cdot \langle p, ctr, \sigma, n\rangle}{\Sigma'_B \cdot \langle p, ctr', \sigma, n\rangle \approx \Sigma'_{B+S} \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr'', \sigma', n'\rangle^{v4}_{\texttt{bypass}\ n \cdot \texttt{start}_S\ ctr}}\ \text{(V14-V1:Single-Speculation-Start)}$$

$$\frac{\Sigma_B \sim \Sigma_{B+S} \quad \Sigma''_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma'''_{B+S} \text{ where transaction with id } ctr \text{ is rolled back} \quad \Sigma_B = \Sigma'_B \cdot \langle p, ctr', \sigma, n\rangle \quad \Sigma_{B+S} = \Sigma'_{B+S} \cdot \langle p, ctr, \sigma, n\rangle}{\Sigma'_B \cdot \langle p, ctr', \sigma, n\rangle \approx \Sigma'_{B+S} \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^{v4} \cdot \Sigma_{B+S1}}\ \text{(V14-V1:Single-Speculation-Diff)}$$

$\boxed{\Sigma_B \sim \Sigma_{B+S}}$

$$\frac{}{\varnothing \sim \varnothing}\ \text{(V14-V1:Base)} \qquad \frac{|\Sigma'_B| = |\Sigma'_{B+S}| \quad \Sigma'_B \sim \Sigma'_{B+S}}{\Sigma'_B \cdot \langle p, ctr, \sigma, n\rangle \sim \Sigma'_{B+S} \cdot \langle p, ctr', \sigma, n\rangle}\ \text{(V14-V1:Single)}$$

$\boxed{\Sigma_S \approx \Sigma_{B+S}}$

$$\frac{}{\varnothing \approx \varnothing}\ \text{(V14-V4:Base)} \qquad \frac{\Sigma'_S \sim \Sigma'_{B+S}}{\Sigma'_S \cdot \langle p, ctr, \sigma, n\rangle \approx \Sigma'_{B+S} \cdot \langle p, ctr', \sigma, n\rangle}\ \text{(V14-V4:Single-Base)}$$

$$\frac{\Sigma_S \sim \Sigma_{B+S} \quad \Sigma''_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma'''_{B+S} \text{ where transaction with id } ctr \text{ is rolled back} \quad \Sigma_S = \Sigma'_S \cdot \langle p, ctr', \sigma, n\rangle \quad \Sigma_{B+S} = \Sigma'_{B+S} \cdot \langle p, ctr, \sigma, n\rangle}{\Sigma'_S \cdot \langle p, ctr', \sigma, n\rangle \approx \Sigma'_{B+S} \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^{v1}_{\texttt{pc}\ n \cdot \texttt{start}_B\ ctr}}\ \text{(V14-V4:Single-Speculation-Start)}$$

$$\frac{\Sigma_S \sim \Sigma_{B+S} \quad \Sigma''_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma'''_{B+S} \text{where transaction with id } ctr \text{ is rolled back} \quad \Sigma_S = \Sigma'_S \cdot \langle p, ctr', \sigma, n\rangle \quad \Sigma_{B+S} = \Sigma'_{B+S} \cdot \langle p, ctr, \sigma, n\rangle}{\Sigma'_S \cdot \langle p, ctr', \sigma, n\rangle \approx \Sigma'_{B+S} \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr'', \sigma', n'\rangle^{v1} \cdot \Sigma_{B+S1}} \text{(V14-V4:Single-Speculation-Diff)}$$

$\boxed{\Sigma_S \sim \Sigma_{B+S}}$

$$\frac{}{\varnothing \sim \varnothing} \text{(V14-V4:Base)} \qquad \frac{|\Sigma'_S| = |\Sigma'_{B+S}| \quad \Sigma'_S \sim \Sigma'_{B+S}}{\Sigma'_S \cdot \langle p, ctr, \sigma, n\rangle \sim \Sigma'_{B+S} \cdot \langle p, ctr', \sigma, n\rangle} \text{(V14-V4:Single)}$$

Lemma 107 (V14: V1 step)**.** *If*

(1) $\Sigma_B \approx \Sigma_{B+S}$ *by Rule V14-V1:Single-Base and*
(2) $\Sigma_{B+S} = \overline{\Phi}_{B+S} \cdot \Phi_{B+S}$ *and* $\Sigma'_{B+S} = \overline{\Phi}_{B+S} \cdot \overline{\Phi}'_{B+S}$ *and*
(3) $\Phi_{B+S} \restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_S$ *and*

Then

(1) $\Sigma_B \overset{\tau \restriction^B}{\dashrightarrow}_B \Sigma'_B$ *and*
(2) if the step was not derived by Rule S*:AM-Store-Spec then* $\Sigma'_B \approx \Sigma'_{B+S}$ *by Rule V14-V1:Single-Base and*
(3) if the step was derived by Rule S*:AM-Store-Spec then* $\Sigma'_B \approx \Sigma'_{B+S}$ *by Rule V14-V1:Single-Speculation-Start*

Proof. We have by $\approx$:

$$\begin{aligned}\Sigma_B &= \Sigma''_B \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle\\ \Sigma_{B+S} &= \Sigma''_{B+S} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\\ \Sigma''_B &\sim \Sigma''_{B+S}\end{aligned}$$

We proceed by inversion on $\Phi_{B+S} \restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_S$:

Rule S:AM-Store-Spec Then we use Rule AM-NoBranch to derive a step $\Sigma_B \overset{\tau}{\dashrightarrow}_B \Sigma'_B$.
The case is analogous to the corresponding case of Rule R:AM-Ret-Spec in Lemma 87 (V45: V5 step).

otherwise This includes Rule S:AM-barr or Rule S:AM-barr-spec or Rule S:AM-NoBranch.
We do the case for Rule S:AM-barr. The case for Rule S:AM-barr-spec and Rule S:AM-NoBranch is analogous.
The case is analogous to the corresponding case in Lemma 87 (V45: V5 step).

□

Lemma 108 (V14: V4 step)**.** *If*

(1) $\Sigma_S \approx \Sigma_{B+S}$ *by Rule V14-V4:Single-Base and*
(2) $\Sigma_{B+S} = \overline{\Phi}_{B+S} \cdot \Phi_{B+S}$ *and* $\Sigma'_{B+S} = \overline{\Phi}_{B+S} \cdot \overline{\Phi}'_{B+S}$ *and*
(3) $\Phi_{B+S} \restriction^B \overset{\tau}{\dashrightarrow}_B \overline{\Phi}'_B$ *and*

Then

(1) $\Sigma_S \overset{\tau \restriction^S}{\dashrightarrow}_S \Sigma'_S$ *and*
(2) if the step was not derived by Rule B*:AM-Spec then* $\Sigma'_S \approx \Sigma'_{B+S}$ *by Rule V14-V4:Single-Base and*
(3) if the step was derived by Rule B*:AM-Spec then* $\Sigma'_S \approx \Sigma'_{B+S}$ *by Rule V14-V4:Single-Speculation-Start*

Proof. We have by $\approx$:

$$\begin{aligned}\Sigma_S &= \Sigma''_S \cdot \langle p, ctr, \sigma, n\rangle\\ \Sigma_{B+S} &= \Sigma''_{B+S} \cdot \langle p, ctr', \sigma, n\rangle\\ \Sigma''_S &\sim \Sigma''_{B+S}\end{aligned}$$

We proceed by inversion on $\Phi_{B+S} \restriction^B \overset{\tau}{\dashrightarrow}_B \overline{\Phi}'_B$:

Rule B:AM-Spec Then we use Rule S:AM-NoBranch to derive a step $\Sigma_S \overset{\tau}{\dashrightarrow}_S \Sigma'_S$.
The case is analogous to the corresponding case of Rule R:AM-Ret-Spec in Lemma 86 (V45: V4 step).

otherwise This includes Rule B:AM-barr or Rule B:AM-barr-spec or Rule AM-NoBranch.
We do the case for Rule B:AM-barr. The case for Rule B:AM-barr-spec and Rule AM-NoBranch is analogous.
The case is analogous to the corresponding case in Lemma 86 (V45: V4 step).

□

L.1 Projection to V4: Soundness and Completeness

Theorem 28 (V14: Relating V4 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh_{\mathsf{S}}^{\mathcal{A}}(p) = Beh_{\mathcal{A}}^{\mathsf{B+S}}(p)\restriction^{S}$.*

Proof. We prove the two directions separately:

⇐ Assume that $(p,\sigma)\ \text{🕮}^{\omega}_{\mathsf{B+S}}\ \overline{\tau} \in Beh_{\mathcal{A}}^{\mathsf{B+S}}(p)$.
The case is analogous to Theorem 24 (V45: Relating V4 with projection of combined) using Lemma 109 (V14: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).
We can now conclude that $p,\sigma\ \text{🕮}^{\omega}_{\mathsf{S}}\ \overline{\tau}\restriction^{S} \in Beh_{\mathsf{S}}^{\mathcal{A}}(p)$ by Rule S:AM-Trace.

⇒ Assume that $(p,\sigma)\ \text{🕮}^{\omega}_{\mathsf{S}}\ \overline{\tau} \in Beh_{\mathsf{S}}^{\mathcal{A}}(p)$.
The case is analogous to Theorem 24 (V45: Relating V4 with projection of combined) using Lemma 110 (V14 AM: Completeness w.r.t V4 and projection).
We thus have $(p,\sigma)\ \text{🕮}^{\omega}_{\mathsf{B+S}}\ \overline{\tau}' \in Beh_{\mathcal{A}}^{\mathsf{B+S}}(p)$ with $\overline{\tau}'\restriction^{S} = \overline{\tau}$.

□

Lemma 109 (V14: Soundness of the AM speculative semantics w.r.t. AM v4 semantics)**.** *If*

(1) $\Sigma_{\mathsf{S}} \approx \Sigma_{\mathsf{B+S}}$ *and*
(2) $\Sigma_{\mathsf{B+S}} \Downarrow^{\overline{\tau}}_{\mathsf{B+S}} \Sigma'_{\mathsf{B+S}}$

Then exists Σ'_{S} *such that*

I $\Sigma'_{\mathsf{S}} \approx \Sigma'_{\mathsf{B+S}}$ *and*
II if $\Sigma'_{\mathsf{S}} \approx \Sigma'_{\mathsf{B+S}}$ *by Rule V14-V4:Single-Base then* $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}\restriction^{S}}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ *and*
III if $\Sigma'_{\mathsf{S}} \approx \Sigma'_{\mathsf{B+S}}$ *by Rule V14-V4:Single-Speculation-Start then* $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}\restriction^{S}}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ *and*
IV if $\Sigma'_{\mathsf{S}} \approx \Sigma'_{\mathsf{B+S}}$ *by Rule V14-V4:Single-Speculation-Diff* $\Sigma_{\mathsf{S}} \Downarrow^{helpers_S(\overline{\tau},i)}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$*, where* $i = ctr'$ *by unpacking* $\Sigma'_{\mathsf{B+S}}$ *according to Rule V14-V4:Single-Speculation-Diff.*

Proof. By Induction on $\Sigma_{\mathsf{B+S}} \Downarrow^{\overline{\tau}}_{\mathsf{B+S}} \Sigma'_{\mathsf{B+S}}$.

Rule AM-Reflection-V14 Then we have $\Sigma_{\mathsf{B+S}} \Downarrow^{\varepsilon}_{\mathsf{S}} \Sigma_{\mathsf{B+S}}$ with $\Sigma'_{\mathsf{B+S}} = \Sigma_{\mathsf{B+S}}$ and by Rule AM-Reflection-V15 we have
I $\Sigma'_{\mathsf{S}} \approx \Sigma'_{\mathsf{B+S}}$
II $\Sigma_{\mathsf{S}} \Downarrow^{\varepsilon\restriction^{S}}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ with $\Sigma_{\mathsf{S}} = \Sigma'_{\mathsf{S}}$.
III $\Sigma_{\mathsf{S}} \Downarrow^{helpers_S(\varepsilon,i)}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ with $\Sigma_{\mathsf{S}} = \Sigma'_{\mathsf{S}}$.
Note, that the initial relation $\Sigma_{\mathsf{S}} \approx \Sigma_{\mathsf{B+S}}$ does not change.

Rule AM-Single-V14 We have $\Sigma_{\mathsf{B+S}} \Downarrow^{\overline{\tau}''}_{\mathsf{B+S}} \Sigma''_{\mathsf{B+S}}$ with $\Sigma''_{\mathsf{B+S}} \overset{\tau}{\text{-}\!\!\overline{\text{-}}\!\!\text{🕮}}_{\mathsf{B+S}} \Sigma'_{\mathsf{B+S}}$.
We now apply IH on $\Sigma''_{\mathsf{B+S}} \Downarrow^{\overline{\tau}''}_{\mathsf{B+S}} \Sigma''_{\mathsf{B+S}}$ and get
(a) $\Sigma''_{\mathsf{S}} \approx \Sigma''_{\mathsf{B+S}}$
(b) if $\Sigma''_{\mathsf{S}} \approx \Sigma''_{\mathsf{B+S}}$ by Rule V14-V4:Single-Base then $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}\restriction^{S}}_{\mathsf{S}} \Sigma''_{\mathsf{S}}$ and
(c) if $\Sigma''_{\mathsf{S}} \approx \Sigma''_{\mathsf{B+S}}$ by Rule V14-V4:Single-Speculation-Start then $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}\restriction^{S}}_{\mathsf{S}} \Sigma''_{\mathsf{S}}$ and
(d) if $\Sigma''_{\mathsf{S}} \approx \Sigma''_{\mathsf{B+S}}$ by Rule V14-V4:Single-Speculation-Diff $\Sigma_{\mathsf{S}} \Downarrow^{helpers_S(\overline{\tau},j)}_{\mathsf{S}} \Sigma''_{\mathsf{S}}$, where $j = ctr'$ by unpacking $\Sigma''_{\mathsf{B+S}}$ according to Rule V14-V4:Single-Speculation-Diff
We do a case distinction on $\approx$ in $\Sigma''_{\mathsf{S}} \approx \Sigma''_{\mathsf{B+S}}$:
Rule V14-V4:Single-Base We have

$$\begin{aligned}
\Sigma_{\mathsf{S}} &\Downarrow^{\overline{\tau}\restriction^{S}}_{\mathsf{S}} \Sigma''_{\mathsf{S}} \\
\Sigma''_{\mathsf{S}} &= \Sigma'''_{\mathsf{S}} \cdot \langle p, ctr, \sigma, n\rangle_{\overline{\rho}} \\
\Sigma''_{\mathsf{B+S}} &= \Sigma'''_{\mathsf{B+S}} \cdot \langle p, ctr', \sigma, n\rangle_{\overline{\rho}} \\
\Sigma'''_{\mathsf{S}} &\sim \Sigma'''_{\mathsf{B+S}}
\end{aligned}$$

We now proceed by inversion on the derivation $\Sigma''_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \Sigma'_{B+S}$:

Rule AM-v4-Rollback-V14 By (b), it can only be roll back of V4 and only be the topmost state.

Furthermore, this means that $n = 0$.

Then $\Sigma''_S \overset{\mathtt{rlb}_S\ ctr}{\dashrightarrow}_S \Sigma'_S$ by Rule S:AM-Rollback, since n is equal between the two states. The rest of the case is analogous to Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

Rule AM-v1-Rollback-V14 Since $\Sigma''_S \approx \Sigma''_{B+S}$ by Rule V14-V4:Single-Base, there cannot be a roll back of V1.

Rule AM-Context-V14 We have $\Phi_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \overline{\Phi}'_{B+S}$.

We now use inversion on $\Phi_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \overline{\Phi}_{B+S}$:

Rule AM-v1-step-V14 Then we have $\Phi_{B+S} \restriction^B \overset{\tau}{\dashrightarrow}_B \overline{\Phi}'_B$.

By inversion on $\Phi_{B+S} \restriction^B \overset{\tau}{\dashrightarrow}_B \overline{\Phi}'_B$ we get:

Rule B:AM-Spec The case is analogous to the corresponding case Rule AM-v5-step-V45 Rule R:AM-Ret-Spec in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) using Lemma 108 (V14: V4 step) and the fact that Rule B:AM-Spec was used.

otherwise The case is analogous to the corresponding case Rule AM-v5-step-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) using Lemma 108 (V14: V4 step) and the fact that Rule B:AM-Spec was not used.

Rule AM-v4-step-V14 Then we have $\Phi_{B+S} \restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_S$.

The case is analogous to the corresponding case Rule AM-v4-step-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) combined with the fact that the rules of V4 cannot generate a $\mathtt{start}_B\ id$ or $\mathtt{rlb}_B\ id$ observation.

Rule V14-V4:Single-Speculation-Start We have:

$$\begin{aligned}
\Sigma_S \Downarrow_S^{\overline{\tau}\restriction^S} \Sigma''_S \\
\Sigma''_S =& \Sigma'''_S \cdot \langle p, ctr, \sigma, n\rangle \\
\Sigma''_{B+S} =& \Sigma'''_{B+S} \cdot \langle p, ctr', \sigma, n\rangle \cdot \langle p, ctr'', \sigma', n'\rangle_{\mathtt{pc}\ n \cdot \mathtt{start}_B\ ctr'} \\
\Sigma'''_S \cdot \langle p, ctr, \sigma, n\rangle \sim& \Sigma'''_{B+S} \cdot \langle p, ctr', \sigma, n\rangle
\end{aligned}$$

We now proceed by inversion on the derivation $\Sigma''_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \Sigma'_{B+S}$.

Rule AM-v1-Rollback-V14 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v4-Rollback-V14 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-Context-V14 We have $\Phi_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \overline{\Phi}'_{B+S}$.

We now use inversion on $\Phi_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \overline{\Phi}_{B+S}$:

Rule AM-v1-step-V14 Then we have $\Phi_{B+S} \restriction^B \overset{\tau}{\dashrightarrow}_B \overline{\Phi}'_B$.

By inversion on $\Phi_{B+S} \restriction^B \overset{\tau}{\dashrightarrow}_B \overline{\Phi}'_B$ we get:

Rule B:AM-General By definition we have $\tau = \mathtt{start}_B\ ctr'$.

Since Rule B:AM-General does not modify the state, we have $\Sigma'_{B+S} = \Sigma''_{B+\mathtt{Spc}\ n}$.

Then we choose $\Sigma'_S = \Sigma''_S$ and derive the step $\Sigma''_S \Downarrow_S^{\varepsilon} \Sigma'_S$ by Rule S:AM-Reflection.

The case is analogous to the corresponding case Rule R:AM-General in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) and the fact that $helper_S()$ behaves the same for $\mathtt{start}_B$ observations.

otherwise Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v4-step-V45 Contradiction, because $\overline{\rho}$ is non-empty and Rule S:AM-General does not work on $\mathtt{start}_B\ id$ observations.

Rule V14-V4:Single-Speculation-Diff We have:

$$\begin{aligned}
\Sigma_S \Downarrow_S^{helper_S(\overline{\tau}, j)} \Sigma''_S \\
\Sigma''_S =& \Sigma'''_R \cdot \langle p, ctr, \sigma, n\rangle \\
\Sigma''_{B+S} =& \Sigma'''_{B+S} \cdot \langle p, ctr'', \sigma, n\rangle \cdot \langle p, ctr''', \sigma'', n''\rangle \cdot \Sigma^{\dagger}_{B+S} \\
\Sigma'''_S \cdot \langle p, ctr, \sigma, n\rangle \sim& \Sigma'''_{B+S} \cdot \langle p, ctr', \sigma, n\rangle \\
j =& ctr'
\end{aligned}$$

We now proceed by inversion on the derivation $\Sigma''_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \Sigma'_{B+S}$:

Rule AM-v4-Rollback-V14 This means a transaction is rolled back that was created later than the transaction with $id = j$.
Then we choose $\Sigma'_S = \Sigma''_S$ and derive the step $\Sigma''_S \Downarrow^{\varepsilon}_S \Sigma'_S$ by Rule S:AM-Reflection.
The case is analogous to the corresponding case in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

Rule AM-v1-Rollback-V14 There are two cases depending on the id of the rolled back transaction:

$id \neq j$ This means a transaction is rolled back that was created later than the transaction with $id = j$.
The case is analogous to the case of Rule AM-v5-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

$id = j$ Then we choose $\Sigma'_S = \Sigma''_S$ and derive the step $\Sigma''_S \Downarrow^{\varepsilon}_S \Sigma'_S$ by Rule S:AM-Reflection.
Since the transaction with $id = j$ was rolled back, we know that $\Sigma'_{B+S} = \Sigma'''_{B+S} \cdot \langle p, ctr''', \sigma, n\rangle$.
For the trace, we get $\overline{\tau} \cdot \texttt{rlb}_B\ j \restriction^S = helper_S(\overline{\tau}, j)$ by definition of $\restriction^S$ and $id = j$.
The rest of the case is analogous to the corresponding case Rule AM-v5-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

otherwise Then we choose $\Sigma'_S = \Sigma''_S$ and derive the step $\Sigma''_S \Downarrow^{\varepsilon}_S \Sigma'_S$ by Rule S:AM-Reflection. Analogous to the corresponding case in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

□

Lemma 110 (V14 AM: Completeness w.r.t V4 and projection)**.** *If*

(1) $\Sigma_S \approx \Sigma_{B+S}$ *by Rule V14-V4:Single-Base and*
(2) $\Sigma_S \Downarrow^{\overline{\tau}}_S \Sigma'_S$

Then exists Σ'_{B+S} *such that*

I $\Sigma'_S \approx \Sigma'_{B+S}$ *by Rule V14-V4:Single-Base and*
II $\Sigma_{B+S} \Downarrow^{\overline{\tau}'}_{B+S} \Sigma'_{B+S}$ *and*
III $\overline{\tau} = \overline{\tau}' \restriction^S$

Proof. We proceed by induction on $\Sigma_S \Downarrow^{\overline{\tau}}_S \Sigma'_S$:

Rule S:AM-Reflection By Rule S:AM-Reflection we have $\Sigma_S \Downarrow^{\epsilon}_S \Sigma_S$ with $\Sigma_S = \Sigma'_S$.

I - III We derive $\Sigma_{B+S} \Downarrow^{\overline{\tau}'}_{B+S} \Sigma'_{B+S}$ by Rule AM-Reflection-V14 and thus $\Sigma_{B+S} = \Sigma'_{B+S}$.
By construction and 2) we have $\Sigma'_S \approx \Sigma'_{B+S}$ by Rule V14-V4:Single-Base.
Since $\varepsilon \restriction^S = \varepsilon$ we are finished.

Rule S:AM-Single Then we have $\Sigma_S \Downarrow^{\overline{\tau}}_S \Sigma''_S$ and $\Sigma''_S \xrightarrow{\tau}_S \Sigma'_S$.
We need to show
I $\Sigma_{B+S} \Downarrow^{\overline{\tau}' \cdot \tau'}_S \Sigma'_{B+S}$ and
II $\Sigma'_S \approx \Sigma'_{B+S}$ by Rule V14-V4:Single-Base and
III $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \restriction^S$
We apply the IH on $\Sigma_S \Downarrow^{\overline{\tau}}_S \Sigma''_S$ we get
I' $\Sigma_{B+S} \Downarrow^{\overline{\tau}'}_{B+S} \Sigma''_{B+S}$ and
II' $\Sigma''_S \approx \Sigma''_{B+S}$ by Rule V14-V4:Single-Base and
IV' $\overline{\tau} = \overline{\tau}' \restriction^S$
By Rule V14-V4:Single-Base we have:

$$\begin{aligned}\Sigma''_S &= \Sigma'''_S \cdot \langle p, ctr, \sigma, n\rangle\\ \Sigma''_{B+S} &= \Sigma'''_{B+S} \cdot \langle p, ctr', \sigma, n\rangle\\ \Sigma'''_S &\sim \Sigma'''_{B+S}\end{aligned}$$

We continue by inversion on $\Sigma''_S \xrightarrow{\tau}_S \Sigma'_S$:

Rule S:AM-Rollback The case is analogous to the corresponding case in Lemma 88 (V45 AM: Completeness w.r.t V4 and projection) using Rule AM-v4-Rollback-V14.

Rule S:AM-Context We then have $\langle p, ctr, \sigma, n\rangle \xrightarrow{\tau}_S \overline{\Phi}'_S$ and $n > 0$.

By $\Sigma''_S \approx \Sigma''_{B+S}$ we know that Rule AM-Context-V14 applies for the step $\Sigma''_{B+S} \xrightarrow{\tau'}_{B+S} \Sigma'_{B+S}$.

We now need to find a derivation for the step $\langle p, ctr', \sigma, n\rangle \xrightarrow{\tau'}_{B+S} \overline{\Phi}'_{B+S}$ according to Rule AM-Context-V14.

We proceed by inversion on $\langle p, ctr, \sigma, n\rangle \xrightarrow{\tau}_S \overline{\Phi}'_S$:

Rule S:AM-NoBranch Then $n > 0$ and $\langle p, ctr, \sigma, n\rangle \overset{\tau}{\rightsquigarrow}_{S} \overline{\Phi}'_{S}$ by $\sigma \xrightarrow{\tau} \sigma'$.
Furthermore, $\Sigma'_{S}.n = n - 1$.
We now do a case analysis on the instruction $p(\sigma(\mathbf{pc}))$:
$p(\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, l$ Then, a speculative transaction of V1 with *id* is started using Rule B:AM-Spec through Rule AM-v1-step-V14 and a new instance $\overline{\Phi}'_{B+S}$ was pushed on top of the stack.
The rest of the case is analogous to the corresponding case $p(\sigma(\mathbf{pc})) = \mathbf{ret}$ in Lemma 88 (V45 AM: Completeness w.r.t V4 and projection).
otherwise Then we can either use Rule AM-NoBranch through Rule AM-v1-step-V14 or Rule S:AM-NoBranch through Rule AM-v4-step-V14.
Because of Lemma 106 (V14 AM: Confluence), we know that it does not matter which rule we use, which means we can use the same rule as for v5 do derive the step.
The rest of the proof is analogous to the corresponding case in Lemma 90 (V45 AM: Completeness w.r.t V5 and projection).
otherwise These rules include Rule S:AM-barr, Rule S:AM-barr-spec, Rule S:AM-General and Rule S:AM-Store-Spec. Since the rules of V4 are included unchanged in the combined semantics and $\Sigma_{S} \approx \Sigma_{B+S}$, we can use the corresponding rule in the combined semantics by Confluence or delegate back to V4 by Rule AM-v4-step-V14.
This means we can always do the same step in the combined as in the V4 semantics.

□

L.2 Projection to V1: Soundness and Completeness

Theorem 29 (V14: Relating V1 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\mathcal{A}}_{B}(p) = Beh^{B+S}_{\mathcal{A}}(p)\upharpoonright^{B}$.*

Proof. We prove the two directions separately:

$\Leftarrow$ Assume that $(p, \sigma) \Downarrow^{\omega}_{B+S} \overline{\tau} \in Beh^{B+S}_{\mathcal{A}}(p)$.
The case is analogous to Theorem 24 (V45: Relating V4 with projection of combined) using Lemma 111 (V14: Soundness of the AM speculative semantics w.r.t. AM v1 semantics).
We can now conclude that $p, \sigma \Downarrow^{\omega}_{S} \overline{\tau}\upharpoonright^{S} \in Beh^{\mathcal{A}}_{S}(p)$ by Rule S:AM-Trace.

$\Rightarrow$ Assume that $(p, \sigma) \Downarrow^{\omega}_{B} \overline{\tau} \in Beh^{\mathcal{A}}_{B}(p)$.
The case is analogous to Theorem 24 (V45: Relating V4 with projection of combined) using Lemma 112 (V14 AM: Completeness w.r.t V1 and projection)
We thus have $(p, \sigma) \Downarrow^{\omega}_{B+S} \overline{\tau}' \in Beh^{B+S}_{\mathcal{A}}(p)$ with $\overline{\tau}'\upharpoonright^{B} = \overline{\tau}$.

□

Lemma 111 (V14: Soundness of the AM speculative semantics w.r.t. AM v1 semantics)**.** *If*

(1) $\Sigma_{B} \approx \Sigma_{B+S}$ *and*
(2) $\Sigma_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma'_{B+S}$

Then exists Σ'_{B} such that

I $\Sigma'_{B} \approx \Sigma'_{B+S}$ *and*
II if $\Sigma'_{B} \approx \Sigma'_{B+S}$ by Rule V14-V1:Single-Base then $\Sigma_{B} \Downarrow^{\overline{\tau}\upharpoonright^{B}}_{B} \Sigma'_{B}$ and
III if $\Sigma'_{B} \approx \Sigma'_{B+S}$ by Rule V14-V1:Single-Speculation-Start then $\Sigma_{B} \Downarrow^{\overline{\tau}\upharpoonright^{B}}_{B} \Sigma'_{B}$ and
IV if $\Sigma'_{B} \approx \Sigma'_{B+S}$ by Rule V14-V1:Single-Speculation-Diff then $\Sigma_{B} \Downarrow^{helper_{B}(\overline{\tau},i)}_{B} \Sigma'_{B}$, where $i = ctr'$ by unpacking Σ'_{B+S} according to Rule V14-V1:Single-Speculation-Diff.

Proof. By Induction on $\Sigma_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma'_{B+S}$.

Rule AM-Reflection-V14 Then we have $\Sigma_{B+S} \Downarrow^{\varepsilon}_{S} \Sigma_{B+S}$ with $\Sigma'_{B+S} = \Sigma_{B+S}$ and by Rule AM-Reflection-V14 we have
I $\Sigma'_{B} \approx \Sigma'_{B+S}$
II $\Sigma_{B} \Downarrow^{\varepsilon\upharpoonright^{B}}_{B} \Sigma'_{B}$ with $\Sigma_{B} = \Sigma'_{B}$.
III $\Sigma_{B} \Downarrow^{helper_{B}(\varepsilon,i)}_{B} \Sigma'_{B}$ with $\Sigma_{B} = \Sigma'_{B}$.
Note, that the initial relation $\Sigma_{B} \approx \Sigma_{B+S}$ does not change.

Rule AM-Single-V14 We have $\Sigma_{B+S} \Downarrow^{\overline{\tau}''}_{B+S} \Sigma''_{B+S}$ with $\Sigma''_{B+S} \overset{\tau}{\rightsquigarrow}_{B+S} \Sigma'_{B+S}$.
We now apply IH on $\Sigma''_{B+S} \Downarrow^{\overline{\tau}''}_{B+S} \Sigma''_{B+S}$ and get
(a) $\Sigma''_{B} \approx \Sigma''_{B+S}$

(b) if $\Sigma''_{\mathtt{B}} \approx \Sigma''_{\mathtt{B+S}}$ by Rule V14-V1:Single-Base then $\Sigma_{\mathtt{B}} \Downarrow_{\mathtt{B}}^{\overline{\tau}\restriction^{B}} \Sigma''_{\mathtt{B}}$ and

(c) if $\Sigma''_{\mathtt{B}} \approx \Sigma''_{\mathtt{B+S}}$ by Rule V14-V1:Single-Speculation-Start then $\Sigma_{\mathtt{B}} \Downarrow_{\mathtt{B}}^{\overline{\tau}\restriction^{B}} \Sigma''_{\mathtt{B}}$ and

(d) if $\Sigma''_{\mathtt{B}} \approx \Sigma''_{\mathtt{B+S}}$ by Rule V14-V1:Single-Speculation-Diff $\Sigma_{\mathtt{B}} \Downarrow_{\mathtt{B}}^{helper_B(\overline{\tau},j)} \Sigma''_{\mathtt{B}}$, where $j = ctr'$ by unpacking $\Sigma''_{\mathtt{B+S}}$ according to Rule V14-V1:Single-Speculation-Diff

We do a case distinction on $\approx$ in $\Sigma''_{\mathtt{B}} \approx \Sigma''_{\mathtt{B+S}}$:

Rule V14-V4:Single-Base We have

$$\begin{aligned}\Sigma_{\mathtt{B}} &\Downarrow_{\mathtt{B}}^{\overline{\tau}\restriction^{B}} \Sigma''_{\mathtt{B}}\\ \Sigma''_{\mathtt{B}} &= \Sigma'''_{\mathtt{B}} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle_{\overline{\rho}}\\ \Sigma''_{\mathtt{B+S}} &= \Sigma'''_{\mathtt{B+S}} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle_{\overline{\rho}}\\ \Sigma'''_{\mathtt{B}} &\sim \Sigma'''_{\mathtt{B+S}}\end{aligned}$$

We now proceed by inversion on the derivation $\Sigma''_{\mathtt{B+S}} \xrightarrow{\tau}_{\mathtt{B+S}} \Sigma'_{\mathtt{B+S}}$:

Rule AM-v1-Rollback-V14 By (b), it can only be roll back of V1 and only be the topmost state.

Furthermore, this means that $n = 0$.

Then $\Sigma''_{\mathtt{B}} \xrightarrow{\mathtt{rlb}_{\mathtt{S}}\ ctr}_{\mathtt{S}} \Sigma'_{\mathtt{B}}$ by Rule B:AM-Rollback, since n is equal between the two states. The rest of the case is analogous to Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

Rule AM-v4-Rollback-V14 Since $\Sigma''_{\mathtt{B}} \approx \Sigma''_{\mathtt{B+S}}$ by Rule V14-V1:Single-Base, there cannot be a roll back of V4.

Rule AM-Context-V14 We have $\Phi_{\mathtt{B+S}} \xrightarrow{\tau}_{\mathtt{B+S}} \overline{\Phi}'_{\mathtt{B+S}}$.

We now use inversion on $\Phi_{\mathtt{B+S}} \xrightarrow{\tau}_{\mathtt{B+S}} \overline{\Phi}_{\mathtt{B+S}}$:

Rule AM-v4-step-V14 Then we have $\Phi_{\mathtt{B+S}}\restriction^{S} \xrightarrow{\tau}_{\mathtt{S}} \overline{\Phi}'_{\mathtt{S}}$.

By inversion on $\Phi_{\mathtt{B+S}}\restriction^{S} \xrightarrow{\tau}_{\mathtt{S}} \overline{\Phi}'_{\mathtt{S}}$ we get:

Rule S:AM-Store-Spec The case is analogous to the corresponding case Rule S:AM-Store-Spec in Lemma 89 (V45: Soundness of the AM speculative semantics w.r.t. AM v5 semantics) using Lemma 108 (V14: V4 step) and the fact that Rule S:AM-Store-Spec was used.

otherwise The case is analogous to the corresponding case Rule AM-v4-step-V45 in Lemma 89 (V45: Soundness of the AM speculative semantics w.r.t. AM v5 semantics) using Lemma 108 (V14: V4 step) and the fact that Rule S:AM-Store-Spec was not used.

Rule AM-v1-step-V14 Then we have $\Phi_{\mathtt{B+S}}\restriction^{B} \xrightarrow{\tau}_{\mathtt{B}} \overline{\Phi}'_{\mathtt{B}}$.

The case is analogous to the corresponding case Rule AM-v4-step-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) combined with the fact that the rules of V1 cannot generate a $\mathtt{start}_{\mathtt{S}}$ *id* or $\mathtt{rlb}_{\mathtt{S}}$ *id* observation.

Rule V14-V4:Single-Speculation-Start We have:

$$\begin{aligned}\Sigma_{\mathtt{B}} &\Downarrow_{\mathtt{B}}^{\overline{\tau}\restriction^{B}} \Sigma''_{\mathtt{B}}\\ \Sigma''_{\mathtt{B}} &= \Sigma'''_{\mathtt{B}} \cdot \langle p, ctr, \sigma, n\rangle\\ \Sigma''_{\mathtt{B+S}} &= \Sigma'''_{\mathtt{B+S}} \cdot \langle p, ctr', \sigma, n\rangle \cdot \langle p, ctr'', \sigma', n'\rangle_{\mathtt{bypass}\ n \cdot \mathtt{start}_{\mathtt{S}}\ ctr'}\\ \Sigma'''_{\mathtt{B}} \cdot \langle p, ctr, \sigma, n\rangle &\sim \Sigma'''_{\mathtt{B+S}} \cdot \langle p, ctr', \sigma, n\rangle\end{aligned}$$

We now proceed by inversion on the derivation $\Sigma''_{\mathtt{B+S}} \xrightarrow{\tau}_{\mathtt{B+S}} \Sigma'_{\mathtt{B+S}}$.

Rule AM-v1-Rollback-V14 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v4-Rollback-V14 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-Context-V14 We have $\Phi_{\mathtt{B+S}} \xrightarrow{\tau}_{\mathtt{B+S}} \overline{\Phi}'_{\mathtt{B+S}}$.

We now use inversion on $\Phi_{\mathtt{B+S}} \xrightarrow{\tau}_{\mathtt{B+S}} \overline{\Phi}_{\mathtt{B+S}}$:

Rule AM-v4-step-V14 Then we have $\Phi_{\mathtt{B+S}}\restriction^{S} \xrightarrow{\tau}_{\mathtt{S}} \overline{\Phi}'_{\mathtt{S}}$.

By inversion on $\Phi_{\mathtt{B+S}}\restriction^{S} \xrightarrow{\tau}_{\mathtt{S}} \overline{\Phi}'_{\mathtt{S}}$ we get:

Rule S:AM-General By definition we have $\tau = \mathtt{start}_{\mathtt{S}}\ ctr'$. Since Rule S:AM-General does not modify the state, we have $\Sigma'_{\mathtt{B+S}} = \Sigma''_{\mathtt{B+S}\mathtt{bypass}\ n}$.

Then we choose $\Sigma'_B = \Sigma''_B$ and derive the step $\Sigma''_B \Downarrow^{\varepsilon}_B \Sigma'_B$ by Rule B:AM-Reflection.
We now fulfill all premises for Rule V14-V1:Single-Speculation-Diff and have $\Sigma'_B \approx \Sigma'_{B+S}$.
We need to show that $\Sigma_B \Downarrow^{helper_B(\overline{\tau}\cdot\tau,ctr')}_B \Sigma'_B$ holds.
We have:

$$\begin{aligned} &\overline{\tau}\restriction^B && \text{Definition } helper_B() \\ =&helper_B(\overline{\tau}\cdot \texttt{start}_S\ ctr', ctr') && \tau = \texttt{start}_S\ ctr' \\ =&helper_B(\overline{\tau}\cdot\tau, ctr') \end{aligned}$$

and we have $\overline{\tau}\restriction^B$ by IH.
Since $\Sigma'_B = \Sigma''_B$ and IH $\Sigma_B \Downarrow^{\overline{\tau}\restriction^B}_B \Sigma''_B$, we have $\Sigma_B \Downarrow^{helper_B(\overline{\tau}\cdot\tau,ctr')}_B \Sigma'_B$ as needed to show.

otherwise Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v1-step-V14 Contradiction, because $\overline{\rho}$ is non-empty and Rule B:AM-General does not work on $\texttt{start}_S$ *id* observations.

Rule V14-V1:Single-Speculation-Diff We have:

$$\begin{aligned} \Sigma_B \Downarrow^{helper_B(\overline{\tau},j)}_B \Sigma''_B \\ \Sigma''_B =& \Sigma'''_R \cdot \langle p, ctr, \sigma, n\rangle \\ \Sigma''_{B+S} =& \Sigma'''_{B+S} \cdot \langle p, ctr'', \sigma, n\rangle \cdot \langle p, ctr''', \sigma'', n''\rangle \cdot \Sigma^{\dagger}_{B+S} \\ \Sigma'''_B \cdot \langle p, ctr, \sigma, n\rangle \sim& \Sigma'''_{B+S} \cdot \langle p, ctr', \sigma, n\rangle \\ j =& ctr' \end{aligned}$$

We now proceed by inversion on the derivation $\Sigma''_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \Sigma'_{B+S}$:

Rule AM-v1-Rollback-V14 This means a transaction is rolled back that was created later than the transaction with $id = j$.
Then we choose $\Sigma'_B = \Sigma''_B$ and derive the step $\Sigma''_B \Downarrow^{\varepsilon}_B \Sigma'_B$ by Rule B:AM-Reflection.
The case is analogous to the corresponding case Rule AM-v4-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

Rule AM-v4-Rollback-V14 There are two cases depending on the *id* of the rolled back transaction:

$id \neq j$ This means a transaction is rolled back that was created later than the transaction with $id = j$.
The case is analogous to the case of Rule AM-v5-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

$id = j$ Then we choose $\Sigma'_B = \Sigma''_B$ and derive the step $\Sigma''_B \Downarrow^{\varepsilon}_B \Sigma'_B$ by Rule B:AM-Reflection.
Since the transaction with $id = j$ was rolled back, we know that $\Sigma'_{B+S} = \Sigma'''_{B+S} \cdot \langle p, ctr''', \sigma, n\rangle$.
For the trace, we get $\overline{\tau}\cdot \texttt{rlb}_S\ j\restriction^B = helper_B(\overline{\tau}, j)$ by definition of $\restriction^B$ and $id = j$.
The rest of the case is analogous to the corresponding case Rule AM-v5-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

otherwise Then we choose $\Sigma'_B = \Sigma''_B$ and derive the step $\Sigma''_B \Downarrow^{\varepsilon}_B \Sigma'_B$ by Rule B:AM-Reflection. Analogous to the corresponding case Rule AM-v4-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

□

Lemma 112 (V14 AM: Completeness w.r.t V1 and projection)**.** *If*

(1) $\Sigma_B \approx \Sigma_{B+S}$ *by Rule V14-V1:Single-Base and*
(2) $\Sigma_B \Downarrow^{\overline{\tau}}_B \Sigma'_B$

Then exists Σ'_{B+S} *such that*

I $\Sigma'_B \approx \Sigma'_{B+S}$ *by Rule V14-V1:Single-Base and*
II $\Sigma_{B+S} \Downarrow^{\overline{\tau}'}_{B+S} \Sigma'_{B+S}$ *and*
III $\overline{\tau} = \overline{\tau}'\restriction^B$

Proof. We proceed by induction on $\Sigma_B \Downarrow^{\overline{\tau}}_B \Sigma'_B$:

Rule B:AM-Reflection By Rule B:AM-Reflection we have $\Sigma_B \Downarrow^{\varepsilon}_R \Sigma_B$ with $\Sigma_B = \Sigma'_B$.

I - III We derive $\Sigma_{B+S} \Downarrow^{\overline{\tau}'}_{B+S} \Sigma'_{B+S}$ by Rule AM-Reflection-V14 and thus $\Sigma_{B+S} = \Sigma'_{B+S}$.
By construction and 2) we have $\Sigma'_B \approx \Sigma'_{B+S}$ by Rule V14-V1:Single-Base.
Since $\varepsilon\restriction^B = \varepsilon$ we are finished.

Rule B:AM-Single Then we have $\Sigma_B \Downarrow_B^{\overline{\tau}} \Sigma''_B$ and $\Sigma''_B \overset{\tau}{\dashrightarrow}_R \Sigma'_R$.

We need to show

I $\Sigma_{B+S} \Downarrow_S^{\overline{\tau}'\cdot\tau'} \Sigma'_{B+S}$ and

II $\Sigma'_B \approx \Sigma'_{B+S}$ by Rule V14-V1:Single-Base and

III $\overline{\tau}\cdot\tau = \overline{\tau}'\cdot\tau'\restriction^B$

We apply the IH on $\Sigma_B \Downarrow_B^{\overline{\tau}} \Sigma''_B$ we get

I' $\Sigma_{B+S} \Downarrow_{B+S}^{\overline{\tau}'} \Sigma''_{B+S}$ and

II' $\Sigma''_B \approx \Sigma''_{B+S}$ by Rule V14-V1:Single-Base and

IV' $\overline{\tau} = \overline{\tau}'\restriction^B$

By Rule V14-V1:Single-Base we have:

$$\begin{aligned}\Sigma''_B &= \Sigma'''_B \cdot \langle p, ctr, \sigma, n\rangle\\ \Sigma''_{B+S} &= \Sigma'''_{B+S} \cdot \langle p, ctr', \sigma, n\rangle\\ \Sigma'''_B &\sim \Sigma'''_{B+S}\end{aligned}$$

We continue by inversion on $\Sigma''_B \overset{\tau}{\dashrightarrow}_B \Sigma'_B$:

Rule B:AM-Rollback The case is analogous to the corresponding case in Lemma 90 (V45 AM: Completeness w.r.t V5 and projection) using Rule AM-v1-Rollback-V14.

Rule B:AM-Context We then have $\langle p, ctr, \sigma, n\rangle \overset{\tau}{\dashrightarrow}_B \overline{\Phi}'_B$ and $n > 0$.

By $\Sigma''_B \approx \Sigma''_{B+S}$ we know that Rule AM-Context-V14 applies for the step $\Sigma''_{B+S} \overset{\tau'}{\dashrightarrow}_{B+S} \Sigma'_{B+S}$.

We now need to find a derivation for the step $\langle p, ctr', \sigma, n\rangle \overset{\tau'}{\dashrightarrow}_{B+S} \overline{\Phi}'_{B+S}$ according to Rule AM-Context-V14.

We proceed by inversion on $\langle p, ctr, \sigma, n\rangle \overset{\tau}{\dashrightarrow}_B \overline{\Phi}'_B$:

Rule AM-NoBranch Then $n > 0$ and $\langle p, ctr, \sigma, \mathbb{R}, n\rangle \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_R$ by $\sigma \xrightarrow{\tau} \sigma'$.

Furthermore, $\Sigma'_R.n = n - 1$.

We now do a case analysis on the instruction $p(\sigma(\mathbf{pc}))$:

$p(\sigma(\mathbf{pc})) = \mathbf{store}\ x, e$ Then, a speculative transaction of V4 with *id* is started using Rule S:AM-Store-Spec through Rule AM-v4-step-V45 and a new instance $\overline{\Phi}'_{B+S}$ was pushed on top of the stack.

The rest of the case is analogous to the corresponding case in Lemma 90 (V45 AM: Completeness w.r.t V5 and projection).

otherwise Then we can either use Rule AM-NoBranch through Rule AM-v1-step-V14 or Rule S:AM-NoBranch through Rule AM-v4-step-V14.

Because of Lemma 106 (V14 AM: Confluence), we know that it does not matter which rule we use, which means we can use the same rule as for v5 do derive the step.

The rest of the proof is analogous to the corresponding case in Lemma 90 (V45 AM: Completeness w.r.t V5 and projection).

otherwise These rules include Rule B:AM-barr, Rule B:AM-barr-spec, Rule B:AM-General and Rule B:AM-Spec. Since the rules of V1 are included in the combined semantics and $\Sigma_S \approx \Sigma_{B+S}$, we can use the corresponding rule in the combined semantics by Confluence or delegate back to V1 by Rule AM-v1-step-V14.

This means we can always do the same step in the combined as in the V1 semantics.

□

Theorem 30 (V14: Relating Combined to non-speculative). *Let p be a program and ω be a speculation window. Then $Beh_{NS}(p) = Beh^{B+S}_{\mathcal{A}}(p)\restriction_{ns}$.*

Proof. By Lemma 11 (V14: Relating speculative projections to non-speculative projection), we have $Beh^{B+S}_{\mathcal{A}}(p)\restriction_{ns} = Beh^{B+S}_{\mathcal{A}}(p)\restriction^S\restriction^B$.

By Theorem 28 (V14: Relating V4 with projection of combined), we have that $Beh^{B+S}_{\mathcal{A}}(p)\restriction^S = Beh^{\mathcal{A}}_S(p)$.

By Lemma 15 (V4: speculative-projections equal to non-speculative Projections), we get $Beh^{\mathcal{A}}_S(p)\restriction^B = Beh^{\mathcal{A}}_S(p)\restriction_{ns}$.

By Theorem 15 (S AM: Behaviour of non-speculative semantics and AM semantics), we know that $Beh^{\mathcal{A}}_S(p)\restriction_{ns} = Beh_{NS}(p)$.

Combining these facts we get:

$$\begin{aligned} & Beh^{\mathsf{B+S}}_{\mathcal{A}}(p)\restriction_{ns} \\ &= Beh^{\mathsf{B+S}}_{\mathcal{A}}(p)\restriction^{S}\restriction^{B} \\ &= Beh^{\mathcal{A}}_{\mathsf{S}}(p)\restriction^{B} \\ &= Beh^{\mathcal{A}}_{\mathsf{S}}(p)\restriction_{ns} \\ &= Beh_{NS}(p) \end{aligned}$$

and are finished. □

Corollary 4 (V14: SNI of combined preserves SNI of parts)**.** *Let p be a program and ω be a speculation window. If $p \vdash_{\mathsf{B+S}}$ SNI then $p \vdash_{\mathsf{B}}$ SNI and $p \vdash_{\mathsf{S}}$ SNI.*

Proof. Assume $p \vdash_{\mathsf{B+S}}$ SNI and that there are $\sigma, \sigma' \in InitConf$ with $\sigma \sim_P \sigma'$ for some policy P and $(p,\sigma) \,\text{🕮}^{O}_{NS}\, \overline{\tau}'$, $(p,\sigma') \,\text{🕮}^{O}_{NS}\, \overline{\tau}'$.
We need to show that

(1) $(p,\sigma) \,\text{🕮}^{\omega}_{\mathsf{S}}\, \overline{\tau}_s$, $(p,\sigma') \,\text{🕮}^{\omega}_{\mathsf{S}}\, \overline{\tau}_s$
(2) $(p,\sigma) \,\text{🕮}^{\omega}_{\mathsf{B}}\, \overline{\tau}_b$, $(p,\sigma') \,\text{🕮}^{\omega}_{\mathsf{B}}\, \overline{\tau}_b$

We show the proof for 1). The proof for 2) is analogous using Theorem 29 (V14: Relating V1 with projection of combined).
Unfolding the definition of $p \vdash_{\mathsf{B+S}}$ SNI we get:

(1) if $\sigma \sim_P \sigma'$ and $(p,\sigma) \,\text{🕮}^{O}_{NS}\, \overline{\tau}$, $(p,\sigma') \,\text{🕮}^{O}_{NS}\, \overline{\tau}$, then $(p,\sigma) \,\text{🕮}^{\omega}_{\mathsf{B+S}}\, \overline{\tau}_{bs}$, $(p,\sigma') \,\text{🕮}^{\omega}_{\mathsf{B+S}}\, \overline{\tau}_{bs}$

After initialization we have $(p,\sigma) \,\text{🕮}^{\omega}_{\mathsf{B+S}}\, \overline{\tau}_{bs}$, $(p,\sigma') \,\text{🕮}^{\omega}_{\mathsf{B+S}}\, \overline{\tau}_{bs}$.

By Theorem 28 (V14: Relating V4 with projection of combined) we have $(p,\sigma) \,\text{🕮}^{\omega}_{\mathsf{S}}\, \overline{\tau}_{bs}\restriction^{S} \in Beh^{\mathcal{A}}_{\mathsf{S}}(p)$ and $(p,\sigma') \,\text{🕮}^{\omega}_{\mathsf{S}}\, \overline{\tau}_{bs}\restriction^{S} \in Beh^{\mathcal{A}}_{\mathsf{S}}(p)$, which is what we needed to show.

□

L.3 Relating Speculative and AM semantics

Lemma 113 (V14SE: Confluence). *If*

(1) $X_{B+S} \overset{\tau}{\rightsquigarrow}^{O_{B+S}}_{B+S} X'_{B+S}$ *and*

(2) $X_{B+S} \overset{\tau}{\rightsquigarrow}^{O_{B+S}}_{B+S} X''_{B+S}$ *derived by a different rule*

Then

(1) $X'_{B+S} = X_{B+S}$

Proof. Analogous to Lemma 91 (V45SE: Confluence) □

Theorem 31 (V14: SNI). *For a program p, all oracles O with speculative window at most ω and for a security Policy P,* $p \vdash^{O}_{B+S}$ *SNIp iff* $p \vdash_{B+S}$ *SNIp.*

Proof. We prove the two directions separately:

(⇒) The proof proceeds analogous to Theorem 17 (S SNI) using (Lemma 124 (V14: Completeness Am semantics w.r.t. speculative semantics))

(⇐) The proof proceeds analogously to Theorem 17 (S SNI) using the Soundness (Lemma 119 (V14: Soundness Big-step))

□

Definition 67 (V14: Relation between AM and spec for all oracles). *We define two relations between AM and oracle semantics.* $\approx_{B+S}$ $\sim$

$\boxed{\Sigma_{B+S} \approx_{B+S} X_{B+S}}$

$$\frac{}{\varnothing \approx_{B+S} \varnothing}\ (V14{:}Base) \qquad \frac{\Sigma_{B+S} \sim X_{B+S}\restriction_{com} \quad INV(\Sigma_{B+S}, X_{B+S})}{\Sigma_{B+S} \approx_{B+S} X_{B+S}}\ (V14{:}Single\text{-}Base)$$

$$\frac{\begin{array}{c}\Sigma_{B+S} \sim X_{B+S}\restriction_{com} \quad \Sigma''_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma'''_{B+S} \text{ where transaction with id ctr is rolled back} \\ X_{B+S} = X'_{B+S} \cdot \langle p, ctr, \sigma, h, n''\rangle \qquad x = (S, true) \vee (B, m \wedge m = \sigma(\mathbf{pc}) \\ \Sigma_{B+S} = \Sigma'_{B+S} \cdot \langle p, ctr, \sigma, n\rangle \qquad INV(\Sigma_{B+S}, X_{B+S})\end{array}}{\Sigma'_{B+S} \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma'', n'\rangle \cdot \Sigma_{B+S1} \approx_{B+S} X'_{B+S} \cdot \langle p, ctr, \sigma, h, n''\rangle \cdot \langle p, ctr', \sigma, h, n'''\rangle^{x}}\ (V14{:}Single\text{-}OracleTrue)$$

$$\frac{\begin{array}{c}\Sigma''_{B+S} \sim X''_{B+S}\restriction_{com} \quad n' \geq 0 \quad \Sigma''_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma'''_{B+S} \text{ where transaction with id ctr is rolled back} \quad x = (S, true) \vee (B, m) \\ X_{B+S} = X'_{B+S} \cdot \langle p, ctr, \sigma, h, n''\rangle \qquad \Sigma_{B+S} = \Sigma'_{B+S} \cdot \langle p, ctr, \sigma, n\rangle \qquad INV(\Sigma_{B+S}, X_{B+S})\end{array}}{\Sigma'_{B+S} \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma'', n'\rangle^{x} \cdot \Sigma_{B+S1} \approx_{B+S} X'_{B+S} \cdot \langle p, ctr, \sigma, h, n''\rangle \cdot \langle p, ctr', \sigma'', h', 0\rangle^{x} \cdot X_{B+S1}}\ (V14{:}Single\text{-}Transaction\text{-}Rollback)$$

$\boxed{\Sigma_{B+S} \sim X_{B+S}}$

$$\frac{}{\varnothing \sim \varnothing}\ (V14{:}Base) \qquad \frac{|\Sigma'_{B+S}| = |X'_{B+S}| \quad \Sigma'_{B+S} \sim X'_{B+S}}{\Sigma'_{B+S} \cdot \langle p, ctr, \sigma, n\rangle^{b} \sim X'_{B+S} \cdot \langle p, ctr', \sigma, h, n'\rangle^{b}}\ (V14{:}Single)$$

Lemma 114 (V14: Coincide on $\approx_{B+S}$ for projections). *If*

(1) $\Sigma_{B+S} \approx_{B+S} X_{B+S}$ *by Rule V14:Single-Base*

Then

(1) $\Sigma_{B+S}\restriction^{S} \approx_{S} X_{B+S}\restriction^{S}$ *by Rule Single-Base and*

(2) $\Sigma_{B+S}\restriction^{B} \approx_{B} X_{B+S}\restriction^{B}$ *by Rule V1:Single-Base*

Proof. The proof is analogous to Lemma 92 (V45: Coincide on $\approx_{S+R}$ for projections). □

Lemma 115 (V14: Coincide on $\cong$ for projections). *If*

(1) $\Sigma_{B+S} \cong X_{B+S}$

Then

(1) $\Sigma_{B+S}\restriction^{S} \cong X_{B+S}\restriction^{S}$ *and*

(2) $\Sigma_{B+S}\restriction^{B} \cong X_{B+S}\restriction^{B}$

Proof. The projection function does not change the values of the instances in the state. Thus, $\Sigma_{B+S}\restriction^{S} \cong X_{B+S}\restriction^{S}$ and $\Sigma_{B+S}\restriction^{B} \cong X_{B+S}\restriction^{B}$ trivially holds. □

Lemma 116 (V14: Initial states fulfill properties). *Let p be a program, ω be a speculation window and O be an oracle with speculation window at most ω. If*

(1) $\sigma, \sigma' \in InitConf$ *and*
(2) $\Sigma^{init}_{B+S}(p,\sigma)$ *and* $\Sigma^{init}_{B+S}(p,\sigma')$ *and*
(3) $X^{init}_{B+S}(p,\sigma)$ *and* $X^{init}_{B+S}(p,\sigma')$

Then

(1) $X^{init}_{B+S}(p,\sigma) \cong X^{init}_{B+S}(p,\sigma')$ *and*
(2) $\Sigma^{init}_{B+S}(p,\sigma) \cong \Sigma^{init}_{B+S}(p,\sigma')$ *and*
(3) $\Sigma^{init}_{B+S}(p,\sigma) \approx_{B+S} X^{init}_{B+S}(p,\sigma)$ *and* $\Sigma^{init}_{B+S}(p,\sigma') \approx_{B+S} X^{init}_{B+S}(p,\sigma')$ *by Rule V14:Single-Base and*

Proof. The proof is analogous to Lemma 45 (S: Initial states fulfill properties). □

Lemma 117 (V14AM: Single step preserves $\cong$). *If*

(1) $\Sigma_{B+S} \cong \Sigma^{\dagger}_{B+S}$ *and*
(2) $\Sigma_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \Sigma'_S$ *and* $\Sigma^{\dagger}_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \Sigma^{\dagger\dagger}_{B+S}$

Then

(1) $\Sigma'_{B+S} \cong \Sigma^{\dagger\dagger}_{B+S}$

Proof. The proof is analogous to Lemma 43 (S AM: Single step preserves $\cong$). □

Lemma 118 (V14SE: Single step preserves $\cong$). *If*

(1) $X_{B+S} \cong X^{\dagger}_{B+S}$ *and*
(2) $X_{B+S} \overset{\tau, O_{B+S}}{\rightsquigarrow}_{B+S} X'_{B+S}$ *and* $X^{\dagger}_{B+S} \overset{\tau, O_{B+S}}{\rightsquigarrow}_{B+S} X^{\dagger\dagger}_{B+S}$

Then

(1) $X'_{B+S} \cong X^{\dagger\dagger}_{B+S}$ *and*

Proof. The proof is analogous to Lemma 44 (S SE: Single step preserves $\cong$). □

L.4 Soundness

Lemma 119 (V14: Soundness Big-step). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*
If

(1) $\sigma, \sigma' \in InitConf$ *and*
(2) $(p,\sigma) \overset{\omega}{\Subset}_{B+S} \overline{\tau}$, $(p,\sigma') \overset{\omega}{\Subset}_{B+S} \overline{\tau}$

Then for all prediction oracles O with speculation window at most ω.

I $(p,\sigma) \overset{O}{\Subset}_{B+S} \overline{\tau}'$, $(p,\sigma) \overset{O}{\Subset}_{B+S} \overline{\tau}'$

Proof. The proof is analogous to Lemma 46 (S: Soundness Am semantics w.r.t. speculative semantics) using Lemma 116 (V14: Initial states fulfill properties) to show that our initial states fulfill all the premises for Lemma 120 (V14: Soundness Am semantics w.r.t. speculative semantics with new relation between states). □

Lemma 120 (V14: Soundness Am semantics w.r.t. speculative semantics with new relation between states). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*
If

(1) $\Sigma_{B+S} \cong \Sigma^{\dagger}_{B+S}$
(2) $X_{B+S} \cong X^{\dagger}_{B+S}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma^{*}_{B+S} \approx_{B+S} X_{B+S}$ *and* $\Sigma^{\dagger}_{B+S} \approx_{B+S} X^{\dagger}_{B+S}$
(4) $\Sigma_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma'_{B+S}$ *and* $\Sigma^{\dagger}_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma^{\dagger\dagger}_{B+S}$

Then for all prediction oracles O with speculation window at most ω.

I $X_{B+S} \overset{O}{\downarrow}^{S}_{\overline{\tau}'} X'_{B+S}$, $X^{\dagger}_{B+S} \overset{O}{\downarrow}^{S}_{\overline{\tau}''} X^{\dagger\dagger}_{B+S}$
II $\Sigma'_{B+S} \cong \Sigma^{\dagger\dagger}_{B+S}$
III $X'_{B+S} \cong X^{\dagger\dagger}_{B+S}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{B+S} \approx_{B+S} X'_{B+S}$ *and* $\Sigma^{\dagger\dagger}_{B+S} \approx_{B+S} X^{\dagger\dagger}_{B+S}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. By Induction on $\Sigma_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma'_{B+S}$ and $\Sigma^{\dagger}_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma^{\dagger\dagger}_{B+S}$.

Rule AM-Reflection-V14 We have $\Sigma_{B+S} \Downarrow^{\varepsilon}_{B+S} \Sigma'_{B+S}$ and $\Sigma^{\dagger}_{B+S} \Downarrow^{\varepsilon}_{B+S} \Sigma''_{B+S}$, where $\Sigma'_{B+S} = \Sigma_{B+S}$ and $\Sigma''_{B+S} = \Sigma^{\dagger}_{B+S}$. We choose $\Sigma'_{B+S} = \Sigma'_{B+S}$ and $\Sigma^{\dagger\dagger}_{B+S} = \Sigma''_{B+S}$.

We further use Rule V14-SE:Reflection to derive $X_{B+S} \overset{O}{\downarrow}^{S}_{\varepsilon} X'_{B+S}$, $X^{\dagger}_{B+S} \overset{O}{\downarrow}^{S}_{\varepsilon} X^{\dagger\dagger}_{B+S}$ with $X'_{B+S} = X_{B+S}$ and $X^{\dagger\dagger}_{B+S} = X^{\dagger}_{B+S}$. We now trivially satisfy all conclusions.

Rule AM-Single-V14 We have $\Sigma_{B+S} \Downarrow^{\overline{\tau}''}_{B+S} \Sigma''_{B+S}$ with $\Sigma''_{B+S} \overset{\tau}{\twoheadrightarrow}_{B+S} \Sigma'_{B+S}$ and $\Sigma^{\dagger}_{B+S} \Downarrow^{\overline{\tau}''}_{B+S} \Sigma^{*}_{B+S}$ and $\Sigma''_{B+S} \overset{\tau}{\twoheadrightarrow}_{B+S} \Sigma^{\dagger\dagger}_{B+S}$.

We now apply IH on $\Sigma_{B+S} \Downarrow^{\overline{\tau}''}_{B+S} \Sigma''_{B+S}$ and $\Sigma^{\dagger}_{B+S} \Downarrow^{\overline{\tau}''}_{B+S} \Sigma^{*}_{B+S}$ and get

(a) $X_{B+S} \overset{O}{\downarrow}^{S}_{\overline{\tau}'} X''_{B+S}$, $X^{\dagger}_{B+S} \overset{O}{\downarrow}^{S}_{\overline{\tau}''} X^{*}_{B+S}$
(b) $\Sigma''_{B+S} \cong \Sigma^{*}_{B+S}$
(c) $X''_{B+S} \cong X^{*}_{B+S}$ and $\overline{\rho}' = \emptyset$
(d) $\Sigma''_{B+S} \approx_{B+S} X''_{B+S}$ and $\Sigma^{*}_{B+S} \approx_{B+S} X^{*}_{B+S}$
(e) $\overline{\tau}' = \overline{\tau}''$

We do a case distinction on $\approx_{B+S}$ in $\Sigma''_{B+S} \approx_{B+S} X''_{B+S}$ and $\Sigma^{*}_{B+S} \approx_{B+S} X^{*}_{B+S}$ by inversion

Rule V14:Single-Base We thus have $\Sigma''_{B+S} \sim X''_{B+S}\restriction_{com}$ and $INV(\Sigma''_{B+S}, X''_{B+S})$ (Similar for Σ^{*}_{B+S} and X^{*}_{B+S}).

Similarly to Lemma 98 (V45: Soundness Am semantics w.r.t. speculative semantics with new relation between states) we can account for possible commits and get a state X^{**}_{B+S} such that $\Sigma''_{B+S} \approx_{B+S} X^{**}_{B+S}$ by Rule V14:Single-Base

We now proceed by inversion on the derivations $\Sigma''_{B+S} \overset{\tau}{\twoheadrightarrow}_{B+S} \Sigma'_{B+S}$ and $\Sigma^{*}_{B+S} \overset{\tau}{\twoheadrightarrow}_{B+S} \Sigma^{\dagger\dagger}_{B+S}$.

Note that by $\Sigma''_{B+S} \cong \Sigma^{*}_{B+S}$ and the fact the same traces are generated, we know that the same rule was used to derive the step.

Rule AM-Context-V14 We now have $\Phi'_{B+S} \overset{\tau}{\twoheadrightarrow}_{B+S} \overline{\Phi}'_{B+S}$ and $\Phi''_{B+S} \overset{\tau}{\twoheadrightarrow}_{B+S} \overline{\Phi}'''_{B+S}$ where $\Sigma''_{B+S} = \overline{\Phi}_{B+S} \cdot \Phi'_{B+S}$ and $\Sigma^{*}_{B+S} = \overline{\Phi}''_{B+S} \cdot \Phi''_{B+S}$.

Furthermore, $n > 0$ and note that all states point to the same instruction by b-d.

Rule AM-v4-step-V14 Then, we have $\Phi_S\restriction^{S} \overset{\tau}{\twoheadrightarrow}_{S} \overline{\Phi}'_{B+S}\restriction^{S}$

We use Lemma 121 (V14: V4 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule AM-v1-step-V14 Then we have $\Phi_{B+S}\restriction^{B} \overset{\tau}{\twoheadrightarrow}_{B} \overline{\Phi}'_{B+S}\restriction^{B}$.

We use Lemma 122 (V14: V1 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule AM-v1-Rollback-V14 Contradiction, because $minWndw(X^{**}_{B+S}) > 0$ and $INV(\Sigma''_{B+S}, X^{**}_{B+S})$.

Rule AM-v4-Rollback-V14 Contradiction, because $minWndw(X^{**}_{B+S}) > 0$ and $INV(\Sigma''_{B+S}, X^{**}_{B+S})$.

Rule V14:Single-OracleTrue We thus have

$$
\begin{aligned}
X''_{B+S} &= X_{B+S3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma, h, n''' \rangle^{false} \\
\Sigma''_{B+S} &= \Sigma_{B+S3} \cdot \langle p, ctr, \sigma, h, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle \cdot \Sigma_{B+S4} \\
X_{B+S} &= X_{B+S3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \\
\Sigma_{B+S} &= \Sigma_{B+S3} \cdot \langle p, ctr, \sigma, n \rangle \\
\Sigma_{B+S} &\sim X_{B+S}\restriction_{com}
\end{aligned}
$$

The form of X^{*}_{B+S} and Σ^{*}_{B+S} is analogous. We now apply inversion on $\Sigma''_{B+S} \overset{\tau}{\twoheadrightarrow}_{B+S} \Sigma'_{B+S}$.

Rule AM-Context-V14 We choose $X'_{B+S} = X''_{B+S}$ and $X^{\dagger\dagger}_{B+S} = X^{*}_{B+S}$.

I By IH a) and Rule V14-SE:Reflection

II By Lemma 117 (V14AM: Single step preserves $\cong$).

III Since $X'_{B+S} = X''_{B+S}$ and $X^{\dagger\dagger}_{B+S} = X^{*}_{B+S}$, we are finished using IH c).

IV We show that $X'_{B+S} \approx_{B+S} \Sigma'_{B+S}$ by Rule V14:Single-OracleTrue. The proof for $X^{\dagger\dagger}_{B+S} \approx \Sigma^{\dagger\dagger}_{B+S}$ is analogous.

Since we did not roll back the transaction with *id ctr'* we have that Σ_{B+S} does not change.

Since X_{B+S} remains the same as well, we have $\Sigma_{B+S} \sim X_{B+S}\restriction_{com}$ and $INV(\Sigma_{B+S}, X_{B+S})X_{B+S}\restriction_{com}$.

Thus, we fulfill all premises for Rule V14:Single-OracleTrue.

V By IH e).

Rule AM-v4-Rollback-V14 There are two cases depending on the transaction *id* of the rolled back transaction:

id > *ctr* Then an inner transaction w.r.t our *ctr* transaction was finished. We choose $X'_{B+S} = X_{B+S}$ and $X^{\dagger\dagger}_{B+S} = X^{\dagger}_{B+S}$. The rest of the proof proceeds similar to the context case above.

id = *ctr* Most cases are similar to the context case above. Only the relation changes. We choose $X'_{B+S} = X_{B+S}$ and $X^{\dagger\dagger}_{B+S} = X^{\dagger}_{B+S}$. The case is analogous to the corresponding case in Lemma 120 (V14: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

Rule AM-v1-Rollback-V14 The case is analogous to the case Rule AM-v4-Rollback-V14 above.

Rule V14:Single-Transaction-Rollback We have

$$
\begin{aligned}
X''_{B+S} &= X_{B+S3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma'', h', 0 \rangle^{true} \cdot X_{B+S4} \\
\Sigma''_{B+S} &= \Sigma_{B+S3} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle^{true} \cdot \Sigma_{B+S4} \\
X_{B+S} &= X_{B+S3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \\
\Sigma_{B+S} &= \Sigma_{B+S3} \cdot \langle p, ctr, \sigma, n \rangle \\
\Sigma_{B+S} &\sim X_{B+S} \restriction_{com} \\
n' &\geq 0
\end{aligned}
$$

The form of X^*_{B+S} and Σ^*_{B+S} is analogous.
There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma''_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \Sigma'_{B+S}$ is not a rollback for *ctr*. The case is analogous to the corresponding case in Lemma 98 (V45: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

$n' = 0$ Then we know that $\Sigma''_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \Sigma'_{B+S}$ was created by either Rule AM-v1-Rollback-V14 or Rule AM-v4-Rollback-V14 and is a rollback for *ctr*.
We do the proof for Rule AM-v4-Rollback-V14, since the case for Rule AM-v1-Rollback-V14 is analogous.
The proof obligations are analogous to the corresponding case in Lemma 98 (V45: Soundness Am semantics w.r.t. speculative semantics with new relation between states) using Lemma 117 (V14AM: Single step preserves ≅) for II and Lemma 118 (V14SE: Single step preserves ≅) for III.

□

Lemma 121 (V14: V4 Soundness Single step). *If*

(1) $\Sigma_{B+S} \approx_{B+S} X_{B+S}$ *and* $\Sigma^{\dagger}_{B+S} \approx_{B+S} X^{\dagger}_{B+S}$ *by Rule V14:Single-Base and*
(2) $\Sigma_{B+S} \cong \Sigma^{\dagger}_{B+S}$ *and* $X_{B+S} \cong X^{\dagger}_{B+S}$ *and*
(3) $\Phi_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \overline{\Phi}'_{B+S}$ *and* $\Phi^{\dagger}_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \overline{\Phi}^{\dagger\dagger}_{B+S}$ *by*
(4) $\Phi_{B+S}\restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_{B+S}\restriction^S$ *and* $\Phi^{\dagger}_{B+S}\restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}^{\dagger\dagger}_{B+S}\restriction^S$

Then

(1) $\Psi_{B+S} \overset{\tau', O_{B+S}}{\rightsquigarrow}_{B+S} \overline{\Psi}'_{B+S}$ *and* $\Psi^{\dagger}_{B+S} \overset{\tau', O_{B+S}}{\rightsquigarrow}_{B+S} \overline{\Psi}^{\dagger\dagger}_{B+S}$ *in combination with Context rule*
(2) $\Psi_{B+S}\restriction^S \overset{\tau, O}{\rightsquigarrow}_S \overline{\Psi}'_{B+S}\restriction^S$ *and* $\Psi^{\dagger}_{B+S}\restriction^S \overset{\tau, O}{\rightsquigarrow}_S \overline{\Psi}^{\dagger\dagger}_{B+S}\restriction^S$
(3) $\Sigma'_{B+S} \cong \Sigma^{\dagger\dagger}_{B+S}$ *and* $X'_{B+S} \cong X^{\dagger\dagger}_{B+S}$ *and*
(4) $\Sigma'_{B+S} \approx_{B+S} X'_{B+S}$ *and* $\Sigma^{\dagger\dagger}_{B+S} \approx_{B+S} X^{\dagger\dagger}_{B+S}$

Proof. By Rule V14:Single-Base and $X_{B+S} \cong X^{\dagger}_{B+S}$ we know that $minWndw(X_{B+S}) > 0$ (similar for $X^{\dagger}_{B+S}$). This means Rule V14-SE-Context applies. We now need to find a step $\Psi_{B+S} \overset{\tau'}{\dashrightarrow}_{B+S} \overline{\Psi}'_{B+S}$ and $\Psi^{\dagger}_{B+S} \overset{\tau'}{\dashrightarrow}_{B+S} \overline{\Psi}^{\dagger\dagger}_{B+S}$. Note that Rule V14-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 115 and Lemma 114 we get $\Sigma_{B+S}\restriction^S \approx_S X_{B+S}\restriction^S$ and $\Sigma_{B+S}\restriction^S \cong \Sigma^{\dagger}_{B+S}\restriction^S$.

Because of $\Phi_{B+S}\restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_{B+S}\restriction^S$ and $\Phi^{\dagger}_{B+S}\restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}^{\dagger\dagger}_{B+S}\restriction^S$ and Rule V14:Single-Base, we fulfill all premises for Lemma 48 (S: Soundness Single Step AM) and derive a step in the oracle semantics:

a) $\Sigma'_{B+S}\restriction^S \cong \Sigma^{\dagger\dagger}_{B+S}\restriction^S$ and $X'_{B+S}\restriction^S \cong X^{\dagger\dagger}_{B+S}\restriction^S$
b) $\Sigma'_{B+S}\restriction^S \approx_S X'_{B+S}\restriction^S$ and $\Sigma^{\dagger\dagger}_{B+S}\restriction^S \approx_S X^{\dagger\dagger}_{B+S}\restriction^S$
c) $\Psi_{B+S}\restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Psi}'_{B+S}\restriction^{S'}$ and $\Psi^{\dagger}_{B+S}\restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Psi}^{\dagger}_{B+S}\restriction^S$ the step of the oracle

Since we have $\Psi_{B+S}\restriction^S \overset{\tau, O}{\rightsquigarrow}_S \overline{\Psi}'_{B+S}\restriction^{S'}$ we can derive a step $\Psi_{B+S} \overset{\tau', O_{B+S}}{\rightsquigarrow}_{B+S} \overline{\Psi}'_{B+S}$ using Rule V14-SE:v4-step (or another applicable rule by Lemma 113 (V14SE: Confluence)).

Let us collect what we already have:

$$X'_{B+S} = X''_{B+S} \cdot \overline{\Psi}'_{B+S}$$
$$\Sigma'_{B+S} = \Sigma''_{B+S} \cdot \overline{\Phi}'_{B+S}$$
$$X^{\dagger\dagger}_{B+S} = X^{*}_{B+S} \cdot \overline{\Psi}^{\dagger\dagger}_{B+S}$$
$$\Sigma^{\dagger\dagger}_{B+S} = \Sigma^{*}_{B+S} \cdot \overline{\Phi}^{\dagger\dagger}_{B+S}$$

We now need to show that $\Sigma'_{B+S} \cong \Sigma^{\dagger\dagger}_{B+S}$ and $X'_{B+S} \cong X^{\dagger\dagger}_{B+S}$ and $\Sigma'_{B+S} \approx_{B+S} X'_{B+S}$ and $\Sigma^{\dagger\dagger}_{B+S} \approx_{B+S} X^{\dagger\dagger}_{B+S}$ hold.

$\Sigma'_{B+S} \cong \Sigma^{\dagger\dagger}_{B+S}$ and $X'_{B+S} \cong X^{\dagger\dagger}_{B+S}$ The proof for $\Sigma'_{B+S} \cong \Sigma^{\dagger\dagger}_{B+S}$ and $X'_{B+S} \cong X^{\dagger\dagger}_{B+S}$ is analogous to the corresponding case in Lemma 99 (V45: V4 Soundness Single step).

$\Sigma'_{B+S} \approx_{B+S} X'_{B+S}$ and $\Sigma^{\dagger\dagger}_{B+S} \approx_{B+S} X^{\dagger\dagger}_{B+S}$ We want to show that $\Sigma'_{B+S} \approx_{B+S} X'_{B+S}$. The case for $\Sigma^{\dagger\dagger}_{B+S} \approx_{B+S} X^{\dagger\dagger}_{B+S}$ is analogous.

We first check if there is a transaction of V5 that needs to be rolled back in X'_{B+S}, since the speculation window of each instance was reduced.

This has to be done, because we only know that $minWndw(X'_{B+S}) > 0$ *before* we did the step. So it could happen that $minWndw(X'_{B+S}) = 0$ for some transaction of V1 that needs to be rolled back.

Transaction of V1 that needs to be rolled back in X'_{B+S} with window 0 The step made cannot create a new speculative instance of V5 that would be on top. This means we can derive all premises of Rule V14:Single-Transaction-Rollback just from $\Sigma_{B+S} \approx_{B+S} X_{B+S}$. Thus, we have $\Sigma'_{B+S} \approx_{B+S} X'_{B+S}$ by Rule V14:Single-Transaction-Rollback.

No V1 Transaction that needs to be rolled back in X'_{B+S} with window 0 Since the speculation window was reduced for all entries in X'_{B+S} and only for the topmost entry in Σ_{B+S} and we had $INV(\Sigma_{B+S}, X_{B+S})$ from $\Sigma_{B+S} \approx_{B+S} X_{B+S}$, we have $INV(\Sigma'_{B+S}, X'_{B+S})$ again. This reasoning extends to newly created instances by speculation as well.

We do a case distinction on $\approx_S$:

Rule Single-Base Analogous to the corresponding cases in Lemma 99 (V45: V4 Soundness Single step).

Rule Single-OracleTrue Then, the oracle predicted correctly. Analogous to the corresponding cases in Lemma 99 (V45: V4 Soundness Single step). Rule V14:Single-OracleTrue and have $\Sigma'_{B+S} \approx_{B+S} X'_{B+S}$.

Rule Single-Transaction-Rollback Then one of the instances in $X'_{B+S}\restriction^{S}$ needs to be rolled back.

This means the same instance in X'_{B+S} needs to be rolled back as well.

We do a case distinction if the instance is part of $\overline{\Psi}'_{B+S}$ or not. These cases are analogous to the corresponding cases in Lemma 99 (V45: V4 Soundness Single step).

□

Lemma 122 (V14: V1 Soundness Single step). *If*

(1) $\Sigma_{B+S} \approx_{B+S} X_{B+S}$ *and* $\Sigma^{\dagger}_{B+S} \approx_{B+S} X^{\dagger}_{B+S}$ *by Rule V14:Single-Base and*

(2) $\Sigma_{B+S} \cong \Sigma^{\dagger}_{B+S}$ *and* $X_{B+S} \cong X^{\dagger}_{B+S}$ *and*

(3) $\Phi_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \overline{\Phi}'_{B+S}$ *and* $\Phi^{\dagger}_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \overline{\Phi}^{\dagger\dagger}_{B+S}$ *by*

(4) $\Phi_{B+S}\restriction^{B} \overset{\tau}{\dashrightarrow}_{B} \overline{\Phi}'_{B+S}\restriction^{B}$ *and* $\Phi^{\dagger}_{B+S}\restriction^{B} \overset{\tau}{\dashrightarrow}_{B} \overline{\Phi}^{\dagger\dagger}_{B+S}\restriction^{B}$

Then

(1) $\Psi_{B+S} \overset{\tau', O_{B+S}}{\rightsquigarrow}_{B+S} \overline{\Psi}'_{B+S}$ *and* $\Psi^{\dagger}_{B+S} \overset{\tau', O_{B+S}}{\rightsquigarrow}_{B+S} \overline{\Psi}^{\dagger\dagger}_{B+S}$ *in combination with Context rule*

(2) $\Psi_{B+S}\restriction^{B} \overset{\tau, O}{\rightsquigarrow}_{B} \overline{\Psi}'_{B+S}\restriction^{B}$ *and* $\Psi^{\dagger}_{B+S}\restriction^{B} \overset{\tau, O}{\rightsquigarrow}_{B} \overline{\Psi}^{\dagger\dagger}_{B+S}\restriction^{B}$

(3) $\Sigma'_{B+S} \cong \Sigma^{\dagger\dagger}_{B+S}$ *and* $X'_{B+S} \cong X^{\dagger\dagger}_{B+S}$ *and*

(4) $\Sigma'_{B+S} \approx_{B+S} X'_{B+S}$ *and* $\Sigma^{\dagger\dagger}_{B+S} \approx_{B+S} X^{\dagger\dagger}_{B+S}$

Proof. The proof is very similar to Lemma 121 (V14: V4 Soundness Single step). We only discuss the key aspects.

By Rule V14:Single-Base and $X_{B+S} \cong X^{\dagger}_{B+S}$ we know that $minWndw(X_{B+S}) > 0$ (similar for $X^{\dagger}_{B+S}$). This means Rule V14-SE-Context applies. We now need to find a step $\Psi_{B+S} \overset{\tau'}{\dashrightarrow}_{B+S} \overline{\Psi}'_{B+S}$ and $\Psi^{\dagger}_{B+S} \overset{\tau'}{\dashrightarrow}_{B+S} \overline{\Psi}^{\dagger\dagger}_{B+S}$. Note that Rule V14-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 115 and Lemma 114 we get $\Sigma_{B+S}\restriction^{B} \approx_{B} X_{B+S}\restriction^{B}$ and $\Sigma_{B+S}\restriction^{B} \cong \Sigma^{\dagger}_{B+S}\restriction^{B}$.

Combined with Rule V14:Single-Base, we fulfill all premises for Lemma 52 (B: Soundness Single Step AM) and derive a step in the oracle semantics:

a) $\Sigma'_{B+S}\restriction^{B} \cong \Sigma^{\dagger\dagger}_{B+S}\restriction^{B}$ and $X'_{B+S}\restriction^{B} \cong X^{\dagger\dagger}_{B+S}\restriction^{B}$

b) $\Sigma'_{B+S}\restriction^{B} \approx_{B} X'_{B+S}\restriction^{B}$ and $\Sigma^{\dagger\dagger}_{B+S}\restriction^{B} \approx_{B} X^{\dagger\dagger}_{B+S}\restriction^{B}$

c) $\Psi_{B+S}\restriction^B \xrightarrow{\tau}_B \overline{\Psi}'_{B+S}\restriction^{B'}$ and $\Psi^{\dagger}_{B+S}\restriction^B \xrightarrow{\tau}_B \overline{\Psi}^{\dagger}_{B+S}\restriction^B$ the step of the oracle

Since we have $\Psi_{B+S}\restriction^S \xrightarrow{\tau}_S \overline{\Psi}'_{B+S}\restriction^{S'}$ we can derive a step $\Psi_{B+S} \xrightarrow{\tau'}_{B+S} \overline{\Psi}'_{B+S}$ using Rule V14-SE:v1-step (or another applicable rule by Lemma 113 (V14SE: Confluence)).

Let us collect what we already have:

$$\begin{aligned} X'_{B+S} &= X''_{B+S} \cdot \overline{\Psi}'_{B+S} \\ \Sigma'_{B+S} &= \Sigma''_{B+S} \cdot \overline{\Phi}'_{B+S} \\ X^{\dagger\dagger}_{B+S} &= X^{*}_{B+S} \cdot \overline{\Psi}^{\dagger\dagger}_{B+S} \\ \Sigma^{\dagger\dagger}_{B+S} &= \Sigma^{*}_{B+S} \cdot \overline{\Phi}^{\dagger\dagger}_{B+S} \end{aligned}$$

We now need to show that $\Sigma'_{B+S} \cong \Sigma^{\dagger\dagger}_{B+S}$ and $X'_{B+S} \cong X^{\dagger\dagger}_{B+S}$ and $\Sigma'_{B+S} \approx_{B+S} X'_{B+S}$ and $\Sigma^{\dagger\dagger}_{B+S} \approx_{B+S} X^{\dagger\dagger}_{B+S}$ hold.

$\Sigma'_{B+S} \cong \Sigma^{\dagger\dagger}_{B+S}$ **and** $X'_{B+S} \cong X^{\dagger\dagger}_{B+S}$ The proof for $\Sigma'_{B+S} \cong \Sigma^{\dagger\dagger}_{B+S}$ and $X'_{B+S} \cong X^{\dagger\dagger}_{B+S}$ is analogous to the corresponding case in Lemma 99 (V45: V4 Soundness Single step).

$\Sigma'_{B+S} \approx_{B+S} X'_{B+S}$ **and** $\Sigma^{\dagger\dagger}_{B+S} \approx_{B+S} X^{\dagger\dagger}_{B+S}$ We first check if there is a transaction of V4 that needs to be rolled back in X'_{B+S}, since the speculation window of each instance was reduced.

This has to be done, because we only know that $minWndw(X'_{B+S}) > 0$ *before* we did the step. So it could happen that $minWndw(X'_{B+S}) = 0$ for some transaction of V4 that needs to be rolled back.

Transaction of V4 that needs to be rolled back in X'_{B+S} with window 0 The step made cannot create a new speculative instance of V4. This means we can derive all premises of Rule V14:Single-Transaction-Rollback just from $\Sigma_{B+S} \approx_{B+S} X_{B+S}$. Thus, we have $\Sigma'_{B+S} \approx_{B+S} X'_{B+S}$ by Rule V14:Single-Transaction-Rollback.

No V4 Transaction that needs to be rolled back in X'_{B+S} with window 0 Since the speculation window was reduced for all entries in X'_{B+S} and only for the topmost entry in Σ_{B+S} and we had $INV(\Sigma_{B+S}, X_{B+S})$ from $\Sigma_{B+S} \approx_{B+S} X_{B+S}$, we have $INV(\Sigma'_{B+S}, X'_{B+S})$ again. This reasoning extends to newly created instances by speculation as well.

We do a case distinction on $\approx_B$:

Rule V1:Single-Base Analogous to the corresponding case in Lemma 121 (V14: V4 Soundness Single step).

Rule V1:Single-OracleTrue Analogous to the corresponding case in Lemma 121 (V14: V4 Soundness Single step).

Rule V1:Single-Transaction-Rollback Then one of the instances in $X'_{B+S}\restriction^B$ needs to be rolled back.

This means the same instance in X'_{B+S} needs to be rolled back as well.

We do a case distinction if the instance is part of $\overline{\Psi}'_{B+S}$ or not.

These cases are analogous to the corresponding cases in Lemma 99 (V45: V4 Soundness Single step).

□

L.5 Completeness

Definition 68 (V14: Relation between AM and Spec for oracles that only mispredict). $\boxed{\Sigma_{B+S} \approx^{O_{am}}_{B+S} X_{B+S}}$

$$\frac{}{\varnothing \approx^{O_{am}}_{B+S} \varnothing}\ \textit{(V14:Base-Oracle)} \qquad \frac{\Sigma_{B+S} \sim X_{B+S}\restriction_{com} \quad INV2(\Sigma_{B+S}, X_{B+S}) \quad minWndw(X_{B+S}) > 0}{\Sigma_{B+S} \approx^{O_{am}}_{B+S} X_{B+S}}\ \textit{(V14:Single-Base-Oracle)}$$

$$\frac{\begin{array}{ccc} \Sigma''_{B+S} \sim X''_{B+S}\restriction_{com} & n' \geq 0 & \Sigma''_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma'''_{B+S} \textit{ where transaction with id ctr is rolled back} \quad x = (S, true) \vee (B, m) \\ X_{B+S} = X'_{B+S} \cdot \langle p, ctr, \sigma, h, n'' \rangle & \Sigma_{B+S} = \Sigma'_{B+S} \cdot \langle p, ctr, \sigma, n \rangle & INV2(\Sigma_{B+S}, X_{B+S}) \end{array}}{\Sigma'_{B+S} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle^x \cdot \Sigma_{S1} \approx^{O_{am}}_{B+S} X'_{B+S} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0 \rangle^x}\ \textit{(V14:Single-Transaction-Rollback-Oracle)}$$

Lemma 123 (V14: Coincide on $\approx^{O_{am}}_{B+S}$ for projections). *If*

(1) $\Sigma_{B+S} \approx^{O_{am}}_{B+S} X_{B+S}$ *by Rule V14:Single-Base*

Then

(1) $\Sigma_{B+S}\restriction^S \approx^{O_{am}}_{S} X_{B+S}\restriction^S$ *by Rule Single-Base-Oracle and*

(2) $\Sigma_{B+S}\restriction^B \approx^{O_{am}}_{B} X_{B+S}\restriction^B$ *by Rule Single-Base-Oracle*

Proof. The proof is analogous to Lemma 101 (V45: Coincide on $\approx^{O_{am}}_{S+R}$ for projections). □

Definition 69 (V14: Constructing the AM Oracle). *We rely for the construction of the oracle O_{am}^{B+S} on the construction of its parts. Here Definition 58 (Constructing the AM Oracle) and Definition 56 (Constructing the Oracle).*

Thus, we have: $O_{am}^{B+S} = (O_{amB}, O_{amS})$ for the speculative oracle combined semantics.

Lemma 124 (V14: Completeness Am semantics w.r.t. speculative semantics). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, σ, $\sigma' \in InitConf$ be two initial configurations. If*

(1) $(p,\sigma) \Uparrow^{\omega}_{B+S} \overline{\tau}$ and $(p,\sigma') \Uparrow^{\omega}_{B+S} \overline{\tau}'$ and
(2) $\overline{\tau} \neq \overline{\tau}'$

Then there exists an oracle O such that

I $(p,\sigma) \Uparrow^{O}_{B+S} \overline{\tau}_1$ and $(p,\sigma') \Uparrow^{O}_{B+S} \overline{\tau}'_1$ and
II $\overline{\tau}_1 \neq \overline{\tau}'_1$

Proof. Let $\omega \in \mathbb{N}$ be a speculative window, $\sigma, \sigma' \in InitConf$ be two initial configurations. If
(1) $(p,\sigma) \Uparrow^{\omega}_{B+S} \overline{\tau}$ and $(p,\sigma') \Uparrow^{\omega}_{B+S} \overline{\tau}'$ and
(2) $\overline{\tau} \neq \overline{\tau}'$

By definition of $\Uparrow^{\omega}_{B+S}$ we have two final states Σ_{B+S_F} and Σ'_{B+S_F} such that $\Sigma^{init}_{B+S}(p,\sigma) \Downarrow^{\overline{\tau}}_{B+S} \Sigma_{B+S_F}$ $\Sigma^{init}_{S} p,\sigma' \Downarrow^{\overline{\tau}'}_{B+S} \Sigma'_{B+S_F}$. Combined with the fact that $\overline{\tau} \neq \overline{\tau}'$, it follows that there are speculative states $\Sigma^{*}_{B+S}, \Sigma^{**}_{B+S}, \Sigma^{\dagger}_{B+S}, \Sigma^{\dagger\dagger}_{B+S}$ and sequences of observations $\overline{\tau}, \overline{\tau}_{end}, \overline{\tau}'_{end}, \tau_{am}, \tau'_{am}$ such that $\tau_{am} \neq \tau'_{am}$, $\Sigma^{*}_{B+S} \cong \Sigma^{\dagger}_{B+S}$ and:

$$\Sigma^{init}_{B+S}(p,\sigma) \Downarrow^{\overline{\tau}}_{B+S} \Sigma^{*}_{B+S} \xrightarrow{\tau_{am}}_{B+S} \Sigma^{**}_{B+S} \Downarrow^{\overline{\tau}_{end}}_{B+S} \Sigma_{B+S_F}$$

$$\Sigma^{init}_{B+S}(p,\sigma') \Downarrow^{\overline{\tau}}_{B+S} \Sigma^{\dagger}_{B+S} \xrightarrow{\tau'_{am}}_{B+S} \Sigma^{\dagger\dagger}_{B+S} \Downarrow^{\overline{\tau}'_{end}}_{B+S} \Sigma'_{B+S_F}$$

We claim that there is a prediction oracle O with speculative window at most ω such that

a) $X^{init}_{B+S}(p,\sigma) \overset{O_{B+S}}{\underset{v}{\wr}}{}^{B+S} X^{*}_{B+S}$ and $X^{*}_{B+S}.\sigma = \Sigma^{*}_{B+S}.\sigma$ and $INV2(X^{*}_{B+S}, \Sigma^{*}_{B+S})$ and
b) $X^{init}_{B+S}(p,\sigma') \overset{O_{B+S}}{\underset{v}{\wr}}{}^{B+S} X^{\dagger}_{B+S}$ and $X^{\dagger}_{B+S}.\sigma = \Sigma^{\dagger}_{B+S}.\sigma$ and $INV2(X^{\dagger}_{B+S}, \Sigma^{\dagger}_{B+S})$
c) $X^{*}_{B+S} \cong X^{\dagger}_{B+S}$

We achieve this by applying Lemma 125 (V14: Stronger Soundness for a specific oracle and for specific executions) on the AM execution up to the point of the difference i.e., $\Sigma^{init}_{B+S}(p,\sigma) \Downarrow^{\overline{\tau}}_{B+S} \Sigma^{*}_{B+S}$ and $\Sigma^{init}_{B+S}(p,\sigma') \Downarrow^{\overline{\tau}}_{B+S} \Sigma^{\dagger}_{B+S}$.

The argument why $\Sigma^{*}_{B+S} \approx^{O_{am}} X^{*}_{B+S}$ is derived by Rule V14:Single-Base-Oracle is analogous to Lemma 102 (V45: Completeness Am semantics w.r.t. speculative semantics).

We proceed by case analysis on the rule in $\xrightarrow{}_{B+S}$ used to derive $\Sigma^{*}_{B+S} \xrightarrow{\tau_{am}}_{B+S} \Sigma^{**}_{B+S}$. Because $\Sigma^{*}_{B+S} \cong \Sigma^{\dagger}_{B+S}$ and $\overline{\tau}_1 = \overline{\tau}'_1$, we know that the same rule was used in $\Sigma^{\dagger}_{B+S} \xrightarrow{\tau'_{am}}_{S} \Sigma^{\dagger\dagger}_{B+S}$ as well.

Rule AM-v4-Rollback-V14 Contradiction. Because $\Sigma^{*}_{B+S} \cong \Sigma^{\dagger}_{B+S}$ we have for all instances $\Phi_1.ctr = \Phi'_1.ctr$.
Since the same instance would be rolled back, we have $\tau_{am} = \tau'_{am}$.

Rule AM-v1-Rollback-V14 Analogous to the case above.

Rule AM-Context-V14 By inversion on Rule AM-Context-V14 for the step $\Sigma^{*}_{B+S} \xrightarrow{\tau_{am}}_{B+S} \Sigma^{**}_{B+S}$ we have $\Sigma^{*}_{B+S} = \overline{\Phi}_{B+S} \cdot \Phi_{B+S}$ and $\Sigma^{**}_{B+S} = \overline{\Phi}_{B+S} \cdot \overline{\Phi}'_{B+S}$ with $\Phi_{B+S} \xrightarrow{\tau_{am}}_{B+S} \overline{\Phi}'_{B+S}$.

We now do inversion on $\Phi_{B+S} \xrightarrow{\tau_{am}}_{B+S} \overline{\Phi}'_{B+S}$:

Rule AM-v4-step-V14 Then we have $\Phi_{B+S} \restriction^{S} \xrightarrow{\tau}_{S} \overline{\Phi}'_{S} \restriction^{S}$.
The case is analogous to Lemma 49 (Completeness Am semantics w.r.t. speculative semantics) in the Rule S:AM-Context case.

Rule AM-v1-step-V14 Then we have $\Phi_{B+S} \restriction^{B} \xrightarrow{\tau}_{B} \overline{\Phi}'_{B+S} \restriction^{B}$.
The case is analogous to Lemma 54 (B: Completeness Am semantics w.r.t. speculative semantics) in the Rule B:AM-Context case.

This completes the proof of our claim.

□

Lemma 125 (V14: Stronger Soundness for a specific oracle and for specific executions). *Specific executions means that there is a difference in the trace but before there is none. We use the oracle O_{am} as it is defined by Definition 69 (V14: Constructing the AM Oracle) for the given execution. If*

(1) $\Sigma_{B+S} \cong \Sigma^{\dagger}_{B+S}$
(2) $X_{B+S} \cong X^{\dagger}_{B+S}$ and $\overline{\rho} = \varnothing$

(3) $\Sigma_{B+S} \approx^{O_{am}} X_{B+S}$ *and* $\Sigma^{\dagger}_{B+S} \approx^{O_{am}} X^{\dagger}_{B+S}$
(4) $\Sigma_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma'_{B+S}$ *and* $\Sigma^{\dagger}_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma^{\dagger\dagger}_{B+S}$

and our oracle is constructed in the way described above Then

I $X_{B+S} \overset{O_{B+S}}{\underset{\overline{\tau}'}{\wr\!\downarrow}}{}^{B+S} X'_{B+S}, X^{\dagger}_{B+S} \overset{O_S}{\underset{\overline{\tau}''}{\wr\!\downarrow}}{}^{S} X^{\dagger\dagger}_{B+S}$
II $\Sigma'_{B+S} \cong \Sigma^{\dagger\dagger}_{B+S}$
III $X'_{B+S} \cong X^{\dagger\dagger}_{B+S}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{B+S} \approx^{O_{am}} X'_{B+S}$ *and* $\Sigma^{\dagger\dagger}_{B+S} \approx^{O_{am}} X^{\dagger\dagger}_{B+S}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. Notice that the proof is very similar to Lemma 98 (V45: Soundness Am semantics w.r.t. speculative semantics with new relation between states). The only thing that is different is that (1) the specific oracle only mispredicts so there is one less case in the relation and (2) we have a different invariant for that specific oracle i.e., $INV2(\Sigma_{B+S}, X_{B+S})$

For these reasons we will only argue why $INV2(\Sigma^{\dagger}_{B+S}, X'_{B+S})$ holds in the different cases and leave the rest to the old soundness proof.

By Induction on $\Sigma_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma'_{B+S}$ and $\Sigma^{\dagger}_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma^{\dagger\dagger}_{B+S}$.

Rule AM-Reflection-V14 We have $\Sigma_{B+S} \Downarrow^{\varepsilon}_{B+S} \Sigma'_{B+S}$ and $\Sigma^{\dagger}_{B+S} \Downarrow^{\varepsilon}_{B+S} \Sigma''_{B+S}$, where $\Sigma'_{B+S} = \Sigma_{B+S}$ and $\Sigma''_{B+S} = \Sigma^{\dagger}_{B+S}$. We choose $\Sigma'_{B+S} = \Sigma'_{B+S}$ and $\Sigma^{\dagger\dagger}_{B+S} = \Sigma''_{B+S}$.

We further use Rule V14-SE:Reflection to derive $X_{B+S} \overset{O_{B+S}}{\underset{\varepsilon}{\wr\!\downarrow}}{}^{B+S} X'_{B+S}, X^{\dagger}_{B+S} \overset{O_{B+S}}{\underset{\varepsilon}{\wr\!\downarrow}}{}^{B+S} X^{\dagger\dagger}_{B+S}$ with $X'_{B+S} = X_{B+S}$ and $X^{\dagger\dagger}_{B+S} = X^{\dagger}_{B+S}$. We now trivially satisfy all conclusions.

Rule AM-Single-V14 We have $\Sigma_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma''_{B+S}$ with $\Sigma''_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \Sigma'_{B+S}$ and $\Sigma^{\dagger}_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma^{*}_{B+S}$ and $\Sigma^{*}_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \Sigma^{\dagger\dagger}_{B+S}$.

We now apply IH on $\Sigma_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma''_{B+S}$ and $\Sigma^{\dagger}_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma^{*}_{B+S}$ and get

(a) $X_{B+S} \overset{O_{B+S}}{\underset{\overline{\tau}'}{\wr\!\downarrow}}{}^{B+S} X''_{B+S}, X^{\dagger}_{B+S} \overset{O_{B+S}}{\underset{\overline{\tau}''}{\wr\!\downarrow}}{}^{B+S} X^{*}_{B+S}$
(b) $\Sigma''_{B+S} \cong \Sigma^{*}_{B+S}$
(c) $X''_{B+S} \cong X^{*}_{B+S}$ and $\overline{\rho}' = \varnothing$
(d) $\Sigma''_{B+S} \approx^{O_{am}}_{B+S} X''_{B+S}$ and $\Sigma^{*}_{B+S} \approx^{O_{am}}_{B+S} X^{*}_{B+S}$
(e) $\overline{\tau}' = \overline{\tau}''$

We do a case distinction on $\approx^{O_{am}}_{B+S}$ in $\Sigma''_{B+S} \approx^{O_{am}}_{B+S} X''_{B+S}$ and $\Sigma^{*}_{B+S} \approx^{O_{am}} X^{*}_{B+S}$:

Rule V14:Single-Base-Oracle We thus have $\Sigma''_{B+S} \sim X''_{B+S}\restriction_{com}$, $minWndw(X''_{B+S}) > 0$ and $INV2(\Sigma''_{B+S}, X''_{B+S})$ (Similar for Σ^{*}_{B+S} and X^{*}_{B+S}).

We now proceed by inversion on the derivation $\Sigma''_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \Sigma'_{B+S}$:

Rule AM-v4-Rollback-V14 Contradiction, since $minWndw(X''_{B+S}) > 0$ and $INV2(\Sigma''_{B+S}, X''_{B+S})$.

Rule AM-v1-Rollback-V14 Analogous to above.

Rule AM-Context-V14 We have $\Phi_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \overline{\Phi}'_{B+S}$ and $n > 0$.

We now use inversion on $\Phi_{B+S} \overset{\tau}{\dashrightarrow}_{B+S} \overline{\Phi}_{B+S}$:

Rule AM-v4-step-V14 Then, we have $\Phi_{B+S}\restriction^{S} \overset{\tau}{\dashrightarrow}_{S} \overline{\Phi}'_{B+S}\restriction^{S}$
We use Lemma 121 (V14: V4 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule AM-v1-step-V14 Then, we have $\Phi_{B+S}\restriction^{B} \overset{\tau}{\dashrightarrow}_{B} \overline{\Phi}'_{B+S}\restriction^{B}$
We use Lemma 122 (V14: V1 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule V14:Single-Transaction-Rollback-Oracle We have

$$
\begin{aligned}
X''_{B+S} =& X_{B+S3} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0 \rangle^{x} \cdot X_{B+S4} \\
\Sigma''_{B+S} =& \Sigma_{B+S3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle^{x} \cdot \Sigma_{B+S4} \\
X_{B+S} =& X_{B+S3} \cdot \langle p, ctr, \sigma, h, \mathbb{R}, n'' \rangle \\
\Sigma_{B+S} =& \Sigma_{B+S3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \\
\Sigma_{B+S} \sim& X_{B+S}\restriction_{com} \\
INV2(\Sigma_{B+S}, X_{B+S}) & \\
n' \geq& 0
\end{aligned}
$$

The form of X^{*}_{B+S} and Σ^{*}_{B+S} is analogous.

Additionally we know that the transaction terminates in some state $\Sigma_{B+S} \Downarrow^{\overline{\tau}}_{B+S} \Sigma'''_{B+S}$. There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma''_{B+S} \xrightarrow{\tau}_{B+S} \Sigma'_{B+S}$ is not a roll back. Because Σ_{B+S} and X_{B+S} do not change, $INV2(\Sigma_{B+S}, X_{B+S})$ does not change as well.

$n' = 0$ Then we know that $\Sigma''_{B+S} \xrightarrow{\tau}_{B+S} \Sigma'_{B+S}$ was created by Rule AM-v4-Rollback-V14 or Rule AM-v1-Rollback-V14 and is a rollback for *ctr*.
Notice, that the only difference to X_{B+S} and Σ_{B+S} is the updated *ctr*, because of the roll back. Updating the counter does not change the invariant $INV2()$. This means $INV2(\Sigma_{B+S}, X_{B+S})$ (with updated *ctr*) still holds.

□

Lemma 126 (V14: Stronger V4 Soundness Single step)**.** *If*

(1) $\Sigma_{B+S} \approx^{O_{am}}_{B+S} X_{B+S}$ *and* $\Sigma^{\dagger}_{B+S} \approx^{O_{am}}_{B+S} X^{\dagger}_{B+S}$ *by Rule V14:Single-Base-Oracle and*
(2) $\Sigma_{B+S} \cong \Sigma^{\dagger}_{B+S}$ *and* $X_{B+S} \cong X^{\dagger}_{B+S}$ *and*
(3) $\Phi_{B+S} \xrightarrow{\tau}_{B+S} \overline{\Phi}'_{B+S}$ *and* $\Phi^{\dagger}_{B+S} \xrightarrow{\tau}_{B+S} \overline{\Phi}^{\dagger\dagger}_{B+S}$ *by*
(4) $\Phi_{B+S}\restriction^S \xrightarrow{\tau}_{S} \overline{\Phi}'_{B+S}\restriction^S$ *and* $\Phi^{\dagger}_{B+S}\restriction^S \xrightarrow{\tau}_{S} \overline{\Phi}^{\dagger\dagger}_{B+S}\restriction^S$

Then

(1) $\Psi_{B+S} \overset{\tau', O_{B+S}}{\rightsquigarrow}_{B+S} \overline{\Psi}'_{B+S}$ *and* $\Psi^{\dagger}_{B+S} \overset{\tau', O_{B+S}}{\rightsquigarrow}_{B+S} \overline{\Psi}^{\dagger\dagger}_{B+S}$ *in combination with Context rule*
(2) $\Psi_{B+S} \overset{\tau, O_{B+S}}{\rightsquigarrow}_{B+S} \overline{\Psi}'_{B+S}$ *and* $\Psi^{\dagger}_{B+S} \overset{\tau, O_{B+S}}{\rightsquigarrow}_{B+S} \overline{\Psi}^{\dagger\dagger}_{B+S}$
(3) $\Sigma'_{B+S} \cong \Sigma^{\dagger\dagger}_{B+S}$ *and* $X'_{B+S} \cong X^{\dagger\dagger}_{B+S}$ *and*
(4) $\Sigma'_{B+S} \approx^{O_{am}}_{B+S} X'_{B+S}$ *and* $\Sigma^{\dagger\dagger}_{B+S} \approx^{O_{am}}_{B+S} X^{\dagger\dagger}_{B+S}$

Proof. By Rule V14:Single-Base-Oracle and $X_{B+S} \cong X^{\dagger}_{B+S}$ we know that $minWndw(X_{B+S}) > 0$ (similar for $X^{\dagger}_{B+S}$). This means Rule V14-SE-Context applies. We now need to find a step $\Psi_{B+S} \xrightarrow{\tau'}_{B+S} \overline{\Psi}'_{B+S}$ and $\Psi^{\dagger}_{B+S} \xrightarrow{\tau'}_{B+S} \overline{\Psi}^{\dagger\dagger}_{B+S}$. Note that Rule V14-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 115 and Lemma 123 we get $\Sigma_{B+S}\restriction^S \approx_S X_{B+S}\restriction^S$ and $\Sigma_{B+S}\restriction^S \cong \Sigma^{\dagger}_{B+S}\restriction^S$.

Because of $\Phi_{B+S}\restriction^S \xrightarrow{\tau}_{S} \overline{\Phi}'_{B+S}\restriction^S$ and $\Phi^{\dagger}_{B+S}\restriction^S \xrightarrow{\tau}_{S} \overline{\Phi}^{\dagger\dagger}_{B+S}\restriction^S$ and Rule V14:Single-Base-Oracle, we fulfill all premises for Lemma 50 (Stronger Soundness for a specific oracle and for specific executions) and derive a step in the oracle semantics:

a) $\Sigma'_{B+S}\restriction^S \cong \Sigma^{\dagger\dagger}_{B+S}\restriction^S$ and $X'_{B+S}\restriction^S \cong X^{\dagger\dagger}_{B+S}\restriction^S$
b) $\Sigma'_{B+S}\restriction^S \approx^{O_{am}}_{S} X'_{B+S}\restriction^S$ and $\Sigma^{\dagger\dagger}_{B+S}\restriction^S \approx^{O_{am}}_{S} X^{\dagger\dagger}_{B+S}\restriction^S$
c) $\Psi_{B+S}\restriction^S \xrightarrow{\tau}_{S} \overline{\Psi}'_{B+S}\restriction^{S'}$ and $\Psi^{\dagger}_{B+S}\restriction^S \xrightarrow{\tau}_{S} \overline{\Psi}^{\dagger}_{B+S}\restriction^S$ the step of the oracle

Since we have $\Psi_{B+S}\restriction^S \xrightarrow{\tau}_{S} \overline{\Psi}'_{B+S}\restriction^{S'}$ we can derive a step $\Psi_{B+S} \xrightarrow{\tau'}_{B+S} \overline{\Psi}'_{B+S}$ using Rule V14-SE:v4-step (or another applicable rule by Lemma 113 (V14SE: Confluence)).

Let us collect what we already have:

$$X'_{B+S} = X''_{B+S} \cdot \overline{\Psi}'_{B+S}$$
$$\Sigma'_{B+S} = \Sigma''_{B+S} \cdot \overline{\Phi}'_{B+S}$$
$$X^{\dagger\dagger}_{B+S} = X^{*}_{B+S} \cdot \overline{\Psi}^{\dagger\dagger}_{B+S}$$
$$\Sigma^{\dagger\dagger}_{B+S} = \Sigma^{*}_{B+S} \cdot \overline{\Phi}^{\dagger\dagger}_{B+S}$$

We now need to show that $\Sigma'_{B+S} \cong \Sigma^{\dagger\dagger}_{B+S}$ and $X'_{B+S} \cong X^{\dagger\dagger}_{B+S}$ and $\Sigma'_{B+S} \approx^{O_{am}}_{B+S} X'_{B+S}$ and $\Sigma^{\dagger\dagger}_{B+S} \approx^{O_{am}}_{B+S} X^{\dagger\dagger}_{B+S}$ hold.

The rest of the proof is analogous to Lemma 104 (V45: Stronger V4 Soundness Single step).

□

Lemma 127 (V14: Stronger V1 Soundness Single step)**.** *If*

(1) $\Sigma_{B+S} \approx^{O_{am}}_{B+S} X_{B+S}$ *and* $\Sigma^{\dagger}_{B+S} \approx^{O_{am}}_{B+S} X^{\dagger}_{B+S}$ *by Rule V14:Single-Base-Oracle and*
(2) $\Sigma_{B+S} \cong \Sigma^{\dagger}_{B+S}$ *and* $X_{B+S} \cong X^{\dagger}_{B+S}$ *and*
(3) $\Phi_{B+S} \xrightarrow{\tau}_{B+S} \overline{\Phi}'_{B+S}$ *and* $\Phi^{\dagger}_{B+S} \xrightarrow{\tau}_{B+S} \overline{\Phi}^{\dagger\dagger}_{B+S}$ *by*
(4) $\Phi_{B+S}\restriction^B \xrightarrow{\tau}_{B} \overline{\Phi}'_{B+S}\restriction^B$ *and* $\Phi^{\dagger}_{B+S}\restriction^B \xrightarrow{\tau}_{B} \overline{\Phi}^{\dagger\dagger}_{B+S}\restriction^B$

Then

(1) $\Psi_{B+S} \overset{\tau', O_{B+S}}{\rightsquigarrow}_{B+S} \overline{\Psi}'_{B+S}$ *and* $\Psi^{\dagger}_{B+S} \overset{\tau', O_{B+S}}{\rightsquigarrow}_{B+S} \overline{\Psi}^{\dagger\dagger}_{B+S}$ *in combination with Context rule*

(2) $\Psi_{B+S} \overset{\tau}{\rightsquigarrow}^{O_{B+S}}_{B+S} \overline{\Psi}'_{B+S}$ *and* $\Psi^{\dagger}_{B+S} \overset{\tau}{\rightsquigarrow}^{O_{B+S}}_{B+S} \overline{\Psi}^{\dagger\dagger}_{B+S}$
(3) $\Sigma'_{B+S} \cong \Sigma^{\dagger\dagger}_{B+S}$ *and* $X'_{B+S} \cong X^{\dagger\dagger}_{B+S}$ *and*
(4) $\Sigma'_{B+S} \approx^{O_{am}}_{B+S} X'_{B+S}$ *and* $\Sigma^{\dagger\dagger}_{B+S} \approx^{O_{am}}_{B+S} X^{\dagger\dagger}_{B+S}$

Proof. By Rule V14:Single-Base-Oracle and $X_{B+S} \cong X^{\dagger}_{B+S}$ we know that $minWndw(X_{B+S}) > 0$ (similar for $X^{\dagger}_{B+S}$). This means Rule V14-SE-Context applies. We now need to find a step $\Psi_{B+S} \overset{\tau'}{\dashrightarrow}_{B+S} \overline{\Psi}'_{B+S}$ and $\Psi^{\dagger}_{B+S} \overset{\tau'}{\dashrightarrow}_{B+S} \overline{\Psi}^{\dagger\dagger}_{B+S}$. Note that Rule V14-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 115 (V14: Coincide on $\cong$ for projections) and Lemma 123 (V14: Coincide on $\approx^{O_{am}}_{B+S}$ for projections) we get $\Sigma_{B+S}\restriction^{B} \approx^{O_{am}}_{B} X_{B+S}\restriction^{B}$ and $\Sigma_{B+S}\restriction^{B} \cong \Sigma^{\dagger}_{B+S}\restriction^{B}$.

Because of $\Phi_{B+S}\restriction^{B} \overset{\tau}{\dashrightarrow}_{B} \overline{\Phi}'_{B+S}\restriction^{B}$ and $\Phi^{\dagger}_{B+S}\restriction^{B} \overset{\tau}{\dashrightarrow}_{B} \overline{\Phi}^{\dagger\dagger}_{B+S}\restriction^{B}$ and Rule V14:Single-Base-Oracle, we fulfill all premises for Lemma 53 (B: Stronger Soundness for a specific oracle and for specific executions) and derive a step in the oracle semantics:

a) $\Sigma'_{B+S}\restriction^{B} \cong \Sigma^{\dagger\dagger}_{B+S}\restriction^{B}$ and $X'_{B+S}\restriction^{B} \cong X^{\dagger\dagger}_{B+S}\restriction^{B}$
b) $\Sigma'_{B+S}\restriction^{B} \approx^{O_{am}}_{B} X'_{B+S}\restriction^{B}$ and $\Sigma^{\dagger\dagger}_{B+S}\restriction^{B} \approx^{O_{am}}_{B} X^{\dagger\dagger}_{B+S}\restriction^{B}$
c) $\Psi_{B+S}\restriction^{B} \overset{\tau}{\dashrightarrow}_{B} \overline{\Psi}'_{B+S}\restriction^{B'}$ and $\Psi^{\dagger}_{B+S}\restriction^{B} \overset{\tau}{\dashrightarrow}_{B} \overline{\Psi}^{\dagger}_{B+S}\restriction^{B}$ the step of the oracle

Since we have $\Psi_{B+S}\restriction^{B} \overset{\tau}{\dashrightarrow}_{B} \overline{\Psi}'_{B+S}\restriction^{B'}$ we can derive a step $\Psi_{B+S} \overset{\tau'}{\dashrightarrow}_{B+S} \overline{\Psi}'_{B+S}$ using Rule V14-SE:v4-step (or another applicable rule by Lemma 113 (V14SE: Confluence)).

Let us collect what we already have:

$$X'_{B+S} = X''_{B+S} \cdot \overline{\Psi}'_{B+S}$$
$$\Sigma'_{B+S} = \Sigma''_{B+S} \cdot \overline{\Phi}'_{B+S}$$
$$X^{\dagger\dagger}_{B+S} = X^{*}_{B+S} \cdot \overline{\Psi}^{\dagger\dagger}_{B+S}$$
$$\Sigma^{\dagger\dagger}_{B+S} = \Sigma^{*}_{B+S} \cdot \overline{\Phi}^{\dagger\dagger}_{B+S}$$

We now need to show that $\Sigma'_{B+S} \cong \Sigma^{\dagger\dagger}_{B+S}$ and $X'_{B+S} \cong X^{\dagger\dagger}_{B+S}$ and $\Sigma'_{B+S} \approx^{O_{am}}_{B+S} X'_{B+S}$ and $\Sigma^{\dagger\dagger}_{B+S} \approx^{O_{am}}_{B+S} X^{\dagger\dagger}_{B+S}$ hold.

The rest of the proof is analogous to Lemma 104 (V45: Stronger V4 Soundness Single step).

□

M PROOFS V15

Theorem 32 (Well-formed Composition $\lightning_{B+R}$). $\vdash \lightning_{B+R} : WFC$

Proof. Immediately follows from Lemma 128 (V15 AM: Confluence), Theorem 34 (V15: Relating V1 with projection of combined), Theorem 33 (V15: Relating V5 with projection of combined) and Lemma 142 (V15: Soundness Am semantics w.r.t. speculative semantics with new relation between states). □

Lemma 128 (V15 AM: Confluence). *If*

(1) $\Sigma_{B+R} \xrightarrow{\tau} \lightning_{B+R} \Sigma'_{B+R}$ *and*

(2) $\Sigma_{B+R} \xrightarrow{\tau} \lightning_{B+R} \Sigma''_{B+R}$ *derived by a different rule*

Then

(1) $\Sigma'_{B+R} = \Sigma_{B+R}$

Proof. Note that a difference can only come from using Rule AM-v1-step-V15 for one derivation and Rule AM-v5-step-V15 for the other. Since these two rules delegate back to the semantics of V1 and V5, we look which two rules are applicable there.

Let us first look at the instructions and rule that could lead to two different rules to be applied:

beqz x, ℓ, **call** f, **ret** Contradiction. There are no two different rules to derive the steps. This is because of the metaparameter Z introduced into the semantics.

spbarr Then either Rule B:AM-barr and Rule R:AM-barr or Rule B:AM-barr-spec and Rule R:AM-barr-spec are used to derive the steps (dependent on the value of n).

The case is analogous to the corresponding case in Lemma 83 (V45 AM: Confluence).

otherwise Then Rule AM-NoBranch and Rule R:AM-NoBranch were used for different derivations.

The case is analogous to the corresponding case in Lemma 83 (V45 AM: Confluence).

□

We first define two relations for states of V1 and V5: These relations are virtually the same as the ones in V45.

$\boxed{\Sigma_B \approx \Sigma_{B+R}}$

$$\frac{}{\varnothing \approx \varnothing}\ (\text{V15-V1:Base}) \qquad \frac{\Sigma'_B \sim \Sigma'_{B+R}}{\Sigma'_B \cdot \langle p, ctr, \sigma, n\rangle \approx \Sigma'_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}\ (\text{V15-V1:Single-Base})$$

$$\frac{\Sigma_B \sim \Sigma_{B+R} \quad \Sigma''_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma'''_{B+R} \text{ where transaction with id } ctr \text{ is rolled back} \quad \Sigma_B = \Sigma'_B \cdot \langle p, ctr', \sigma, n\rangle \quad \Sigma_{B+R} = \Sigma'_{B+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle}{\Sigma'_B \cdot \langle p, ctr', \sigma, n\rangle \approx \Sigma'_{B+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^{v5}_{\texttt{ret}\ l \cdot \texttt{start}_R\ ctr}}\ (\text{V15-V1:Single-Speculation-Start})$$

$$\frac{\Sigma_B \sim \Sigma_{B+R} \quad \Sigma''_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma'''_{B+R} \text{ where transaction with id } ctr \text{ is rolled back} \quad \Sigma_B = \Sigma'_B \cdot \langle p, ctr', \sigma, n\rangle \quad \Sigma_{B+R} = \Sigma'_{B+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle}{\Sigma'_B \cdot \langle p, ctr', \sigma, n\rangle \approx \Sigma'_{B+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^{v5} \cdot \Sigma_{B+R1}}\ (\text{V15-V1:Single-Speculation-Diff})$$

$\boxed{\Sigma_B \sim \Sigma_{B+R}}$

$$\frac{}{\varnothing \sim \varnothing}\ (\text{V15-V1:Base}) \qquad \frac{|\Sigma'_B| = |\Sigma'_{B+R}| \quad \Sigma'_B \sim \Sigma'_{B+R}}{\Sigma'_B \cdot \langle p, ctr, \sigma, n\rangle \sim \Sigma'_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}\ (\text{V15-V1:Single})$$

$\boxed{\Sigma_R \approx \Sigma_{B+R}}$

$$\frac{}{\varnothing \approx \varnothing}\ (\text{V15-V5:Base}) \qquad \frac{\Sigma'_R \sim \Sigma'_{B+R}}{\Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \approx \Sigma'_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}\ (\text{V15-V5:Single-Base})$$

$$\frac{\Sigma_R \sim \Sigma_{B+R} \quad \Sigma''_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma'''_{B+R} \text{ where transaction with id } ctr \text{ is rolled back} \quad \Sigma_R = \Sigma'_R \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \quad \Sigma_{B+R} = \Sigma'_{B+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle}{\Sigma'_R \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \approx \Sigma'_{B+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^{v1}_{\texttt{pc}\ n \cdot \texttt{start}_B\ ctr}}\ (\text{V15-V5:Single-Speculation-Start})$$

$$\frac{\Sigma_R \sim \Sigma_{B+R} \quad \Sigma''_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma'''_{B+R} \text{ where transaction with id } ctr \text{ is rolled back} \quad \Sigma_R = \Sigma'_R \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \quad \Sigma_{B+R} = \Sigma'_{B+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle}{\Sigma'_R \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \approx \Sigma'_{B+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^{v1} \cdot \Sigma_{B+R1}} \text{(V15-V5:Single-Speculation-Diff)}$$

$\boxed{\Sigma_R \sim \Sigma_{B+R}}$

$$\frac{}{\varnothing \sim \varnothing} \text{(V15-V5:Base)} \qquad \frac{|\Sigma'_R| = |\Sigma'_{B+R}| \quad \Sigma'_R \sim \Sigma'_{B+R}}{\Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \sim \Sigma'_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle} \text{(V15-V5:Single)}$$

Lemma 129 (V15: V5 step)**.** *If*

(1) $\Sigma_R \approx \Sigma_{B+R}$ *by Rule V15-V5:Single-Base and*
(2) $\Sigma_{B+R} = \overline{\Phi}_{B+R} \cdot \Phi_{B+R}$ *and* $\Sigma'_{B+R} = \overline{\Phi}_{B+R} \cdot \overline{\Phi}'_{B+R}$ *and*
(3) $\Phi_{B+R} \upharpoonright^B \xrightarrow{\tau}_B \overline{\Phi}'_B$ *and*

Then

(1) $\Sigma_R \xrightarrow{\tau \upharpoonright^R}_R \Sigma'_R$ *and*
(2) if the step was not derived by Rule B*:AM-Spec then* $\Sigma'_R \approx \Sigma'_{B+R}$ *by Rule V15-V5:Single-Base and*
(3) if the step was derived by Rule B*:AM-Spec then* $\Sigma'_R \approx \Sigma'_{B+R}$ *by Rule V15-V5:Single-Speculation-Start*

Proof. We have by $\approx$:

$$\begin{aligned}\Sigma_R &= \Sigma''_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle\\ \Sigma_{B+R} &= \Sigma''_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\\ \Sigma''_R &\sim \Sigma''_{B+R}\end{aligned}$$

We proceed by inversion on $\Phi_{B+R} \upharpoonright^B \xrightarrow{\tau}_B \overline{\Phi}'_B$:

Rule B**:AM-Spec** Then we use Rule R:AM-NoBranch to derive a step $\Sigma_R \xrightarrow{\tau}_R \Sigma'_R$.
The case is analogous to the corresponding case of Rule R:AM-Ret-Spec in Lemma 86 (V45: V4 step).
otherwise This includes Rule B:AM-barr or Rule B:AM-barr-spec or Rule AM-NoBranch.
We do the case for Rule B:AM-barr. The case for Rule B:AM-barr-spec and Rule AM-NoBranch is analogous.
The case is analogous to the corresponding case in Lemma 86 (V45: V4 step).

□

Lemma 130 (V15: V1 step)**.** *If*

(1) $\Sigma_B \approx \Sigma_{B+R}$ *by Rule V45-V4:Single-Base and*
(2) $\Sigma_{B+R} = \overline{\Phi}_{B+R} \cdot \Phi_{B+R}$ *and* $\Sigma'_{B+R} = \overline{\Phi}_{B+R} \cdot \overline{\Phi}'_{B+R}$ *and*
(3) $\Phi_{B+R} \upharpoonright^R \xrightarrow{\tau}_R \overline{\Phi}'_R$ *and*

Then

(1) $\Sigma_B \xrightarrow{\tau \upharpoonright^S}_S \Sigma'_B$ *and*
(2) if the step was not derived by Rule R*:AM-Ret-Spec then* $\Sigma'_B \approx \Sigma'_{B+R}$ *by Rule V15-V1:Single-Base and*
(3) if the step was derived by Rule R*:AM-Ret-Spec then* $\Sigma'_B \approx \Sigma'_{B+R}$ *by Rule V15-V1:Single-Speculation-Start*

Proof. We have by $\approx$:

$$\begin{aligned}\Sigma_B &= \Sigma''_B \cdot \langle p, ctr, \sigma, n\rangle\\ \Sigma_{B+R} &= \Sigma''_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\\ \Sigma''_B &\sim \Sigma''_{B+R}\end{aligned}$$

We proceed by inversion on $\Phi_{B+R} \upharpoonright^R \xrightarrow{\tau}_R \overline{\Phi}'_R$:

Rule R**:AM-Ret-Spec** Then we use Rule AM-NoBranch to derive a step $\Sigma_B \xrightarrow{\tau}_S \Sigma'_B$.
The case is analogous to the corresponding case in Lemma 86 (V45: V4 step).

Rule R:AM-barr or Rule R:AM-barr-spec or Rule R:AM-NoBranch We do the case for Rule R:AM-barr. The case for Rule R:AM-barr-spec and Rule R:AM-NoBranch is analogous.
The case is analogous to the corresponding case in Lemma 86 (V45: V4 step) using Lemma 128 (V15 AM: Confluence).

otherwise This includes Rule R:AM-Call-Full, Rule R:AM-Ret-Empty, Rule R:AM-Ret-Same and Rule R:AM-Call.
Then we use Rule AM-NoBranch to derive a step $\Sigma_B \overset{\tau}{\dashrightarrow}_B \Sigma'_B$.
The case is analogous to Lemma 86 (V45: V4 step) using Lemma 128 (V15 AM: Confluence).

□

M.1 Projection V5 : Soundness and Completeness

Theorem 33 (V15: Relating V5 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\mathcal{A}}_{R}(p) = Beh^{B+R}_{\mathcal{A}}(p)\restriction^{R}$.*

Proof. We prove the two directions separately:

⇐ Assume that $(p,\sigma)\ \text{🕮}^{\omega}_{B+R}\ \overline{\tau} \in Beh^{B+R}_{\mathcal{A}}(p)$.
The case is analogous to Theorem 24 (V45: Relating V4 with projection of combined) using Lemma 131 (V15: Soundness of the AM speculative semantics w.r.t. AM v5 semantics)
We can now conclude that $p,\sigma\ \text{🕮}^{\omega}_{R}\ \overline{\tau}\restriction^{S} \in Beh^{\mathcal{A}}_{R}(p)$ by Rule S:AM-Trace.

⇒ Assume that $(p,\sigma)\ \text{🕮}^{\omega}_{R}\ \overline{\tau} \in Beh^{\mathcal{A}}_{R}(p)$.
The case is analogous to Theorem 24 (V45: Relating V4 with projection of combined) using Lemma 132 (V15 AM: Completeness w.r.t V5 and projection).
We thus have $(p,\sigma)\ \text{🕮}^{\omega}_{B+R}\ \overline{\tau}' \in Beh^{B+R}_{\mathcal{A}}(p)$ with $\overline{\tau}'\restriction^{R} = \overline{\tau}$.

□

Lemma 131 (V15: Soundness of the AM speculative semantics w.r.t. AM v5 semantics)**.** *If*

(1) $\Sigma_R \approx \Sigma_{B+R}$ *and*
(2) $\Sigma_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma'_{B+R}$

Then exists Σ'_R *such that*

I $\Sigma'_R \approx \Sigma'_{B+R}$ *and*
II if $\Sigma'_R \approx \Sigma'_{B+R}$ *by Rule V15-V5:Single-Base then* $\Sigma_R \Downarrow^{\overline{\tau}\restriction^{R}}_{R} \Sigma'_R$ *and*
III if $\Sigma'_R \approx \Sigma'_{B+R}$ *by Rule V15-V5:Single-Speculation-Start then* $\Sigma_R \Downarrow^{\overline{\tau}\restriction^{R}}_{R} \Sigma'_R$ *and*
IV if $\Sigma'_R \approx \Sigma'_{B+R}$ *by Rule V15-V5:Single-Speculation-Diff* $\Sigma_R \Downarrow^{helper_R(\overline{\tau},i)}_{S} \Sigma'_R$*, where* $i = ctr'$ *by unpacking* Σ'_{B+R} *according to Rule V15-V5:Single-Speculation-Diff.*

Proof. By Induction on $\Sigma_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma'_{B+R}$.

Rule AM-Reflection-V15 Then we have $\Sigma_{B+R} \Downarrow^{\varepsilon}_{S} \Sigma_{B+R}$ with $\Sigma'_{B+R} = \Sigma_{B+R}$ and by Rule AM-Reflection-V15 we have
I $\Sigma'_R \approx \Sigma'_{B+R}$
II $\Sigma_R \Downarrow^{\varepsilon\restriction^{R}}_{R} \Sigma'_R$ with $\Sigma_R = \Sigma'_R$.
III $\Sigma_R \Downarrow^{helper_R(\varepsilon,i)}_{R} \Sigma'_R$ with $\Sigma_R = \Sigma'_R$.
Note, that the initial relation $\Sigma_R \approx \Sigma_{B+R}$ does not change.

Rule AM-Single-V15 We have $\Sigma_{B+R} \Downarrow^{\overline{\tau}''}_{B+R} \Sigma''_{B+R}$ with $\Sigma''_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \Sigma'_{B+R}$.
We now apply IH on $\Sigma''_{B+R} \Downarrow^{\overline{\tau}''}_{B+R} \Sigma''_{B+R}$ and get
(a) $\Sigma''_R \approx \Sigma''_{B+R}$
(b) if $\Sigma''_R \approx \Sigma''_{B+R}$ by Rule V15-V5:Single-Base then $\Sigma_R \Downarrow^{\overline{\tau}\restriction^{R}}_{R} \Sigma''_R$ and
(c) if $\Sigma''_R \approx \Sigma''_{B+R}$ by Rule V15-V5:Single-Speculation-Start then $\Sigma_R \Downarrow^{\overline{\tau}\restriction^{R}}_{R} \Sigma''_R$ and
(d) if $\Sigma''_R \approx \Sigma''_{B+R}$ by Rule V15-V5:Single-Speculation-Diff $\Sigma_R \Downarrow^{helper_R(\overline{\tau},j)}_{R} \Sigma''_R$, where $j = ctr'$ by unpacking Σ''_{B+R} according to Rule V15-V5:Single-Speculation-Diff
We do a case distinction on $\approx$ in $\Sigma''_R \approx \Sigma''_{B+R}$:

Rule V15-V5:Single-Base We have

$$\begin{aligned}\Sigma_R \Downarrow_R^{\overline{\tau}\restriction^R} \Sigma''_R\\ \Sigma''_R = \Sigma'''_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle_{\overline{\rho}}\\ \Sigma''_{B+R} = \Sigma'''_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle_{\overline{\rho}}\\ \Sigma'''_R \sim \Sigma'''_{B+R}\end{aligned}$$

We now proceed by inversion on the derivation $\Sigma''_{B+R} \overset{\tau}{\Longrightarrow}_{B+R} \Sigma'_{B+R}$:

Rule AM-v5-Rollback-V15 By (b), it can only be roll back of V5 and only be the topmost state.
Furthermore, this means that $n = 0$.
Then $\Sigma''_R \overset{\texttt{rlb}_R\ ctr}{\Longrightarrow}_R \Sigma'_R$ by Rule R:AM-Rollback, since n is equal between the two states. The rest of the case is analogous to Lemma 89 (V45: Soundness of the AM speculative semantics w.r.t. AM v5 semantics).

Rule AM-v1-Rollback-V15 Since $\Sigma''_R \approx \Sigma''_{B+R}$ by Rule V15-V5:Single-Base, there cannot be a roll back of V1.

Rule AM-Context-V15 We have $\Phi_{B+R} \overset{\tau}{\Longrightarrow}_{B+R} \overline{\Phi}'_{B+R}$.
We now use inversion on $\Phi_{B+R} \overset{\tau}{\Longrightarrow}_{B+R} \overline{\Phi}_{B+R}$:

Rule AM-v1-step-V15 Then we have $\Phi_{B+R}\restriction^B \overset{\tau}{\Longrightarrow}_B \overline{\Phi}'_B$.
By inversion on $\Phi_{B+R}\restriction^B \overset{\tau}{\Longrightarrow}_B \overline{\Phi}'_B$ we get:

Rule B:AM-Spec The case is analogous to the corresponding case Rule AM-v5-step-V45 Rule R:AM-Ret-Spec in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) using Lemma 129 (V15: V5 step) and the fact that Rule B:AM-Spec was used.

otherwise The case is analogous to the corresponding case Rule AM-v5-step-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) using Lemma 129 (V15: V5 step) and the fact that Rule B:AM-Spec was not used.

Rule AM-v5-step-V15 Then we have $\Phi_{B+R}\restriction^R \overset{\tau}{\Longrightarrow}_R \overline{\Phi}'_R$.
The case is analogous to the corresponding case Rule AM-v4-step-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) combined with the fact that the rules of V5 cannot generate a $\texttt{start}_B\ id$ or $\texttt{rlb}_B\ id$ observation.

Rule V15-V5:Single-Speculation-Start We have:

$$\begin{aligned}\Sigma_R \Downarrow_R^{\overline{\tau}\restriction^R} \Sigma''_R\\ \Sigma''_R = \Sigma'''_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle\\ \Sigma''_{B+R} = \Sigma'''_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle_{\texttt{pc}\ n \cdot \texttt{start}_B\ ctr'}\\ \Sigma'''_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \sim \Sigma'''_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\end{aligned}$$

We now proceed by inversion on the derivation $\Sigma''_{B+R} \overset{\tau}{\Longrightarrow}_{B+R} \Sigma'_{B+R}$.

Rule AM-v1-Rollback-V15 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v5-Rollback-V15 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-Context-V15 We have $\Phi_{B+R} \overset{\tau}{\Longrightarrow}_{B+R} \overline{\Phi}'_{B+R}$.
We now use inversion on $\Phi_{B+R} \overset{\tau}{\Longrightarrow}_{B+R} \overline{\Phi}_{B+R}$:

Rule AM-v1-step-V15 Then we have $\Phi_{B+R}\restriction^B \overset{\tau}{\Longrightarrow}_B \overline{\Phi}'_B$.
By inversion on $\Phi_{B+R}\restriction^B \overset{\tau}{\Longrightarrow}_B \overline{\Phi}'_B$ we get:

Rule B:AM-General By definition we have $\tau = \texttt{start}_B\ ctr'$.
Since Rule B:AM-General does not modify the state, we have $\Sigma'_{B+R} = \Sigma''_{B+R\,\texttt{pc}\ n}$.
Then we choose $\Sigma'_R = \Sigma''_R$ and derive the step $\Sigma''_R \Downarrow_R^{\varepsilon} \Sigma'_R$ by Rule R:AM-Reflection.
The case is analogous to the corresponding case Rule R:AM-General in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) and the fact that $helper_R()$ behaves the same for $\texttt{start}_B$ and $\texttt{start}_R$ observations.

otherwise Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v5-step-V45 Contradiction, because $\overline{\rho}$ is non-empty and Rule R:AM-General does not work on $\texttt{start}_B\ id$ observations.

Rule V15-V5:Single-Speculation-Diff We have:

$$\begin{aligned}
\Sigma_R \Downarrow_R^{helper_R(\overline{\tau},j)} \Sigma''_R \\
\Sigma''_R = \Sigma'''_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \\
\Sigma''_{B+R} = \Sigma'''_{B+R} \cdot \langle p, ctr'', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr''', \sigma'', \mathbb{R}', n''\rangle \cdot \Sigma^{\dagger}_{B+R} \\
\Sigma'''_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \sim \Sigma'''_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \\
j = ctr'
\end{aligned}$$

We now proceed by inversion on the derivation $\Sigma''_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \Sigma'_{B+R}$:

Rule AM-v5-Rollback-V15 This means a transaction is rolled back that was created later than the transaction with $id = j$.
Then we choose $\Sigma'_R = \Sigma''_R$ and derive the step $\Sigma''_R \Downarrow_R^{\varepsilon} \Sigma'_R$ by Rule R:AM-Reflection.
The case is analogous to the corresponding case in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

Rule AM-v1-Rollback-V15 There are two cases depending on the id of the rolled back transaction:

$id \neq j$ This means a transaction is rolled back that was created later than the transaction with $id = j$.
The case is analogous to the case of Rule AM-v5-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

$id = j$ Then we choose $\Sigma'_R = \Sigma''_R$ and derive the step $\Sigma''_R \Downarrow_R^{\varepsilon} \Sigma'_R$ by Rule R:AM-Reflection.
Since the transaction with $id = j$ was rolled back, we know that $\Sigma'_{B+R} = \Sigma''''_{B+R} \cdot \langle p, ctr''', \sigma, \mathbb{R}, n\rangle$.
For the trace, we get $\overline{\tau} \cdot \texttt{rlb}_B\ j \restriction^R = helper_R(\overline{\tau}, j)$ by definition of $\restriction^R$ and $id = j$.
The rest of the case is analogous to the corresponding case Rule AM-v5-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

otherwise Then we choose $\Sigma'_R = \Sigma''_R$ and derive the step $\Sigma''_R \Downarrow_R^{\varepsilon} \Sigma'_R$ by Rule R:AM-Reflection. Analogous to the corresponding case in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

□

Lemma 132 (V15 AM: Completeness w.r.t V5 and projection)**.** *If*

(1) $\Sigma_R \approx \Sigma_{B+R}$ *by Rule V15-V5:Single-Base and*
(2) $\Sigma_R \Downarrow_R^{\overline{\tau}} \Sigma'_R$

Then exists Σ'_{B+R} *such that*

I $\Sigma'_R \approx \Sigma'_{B+R}$ *by Rule V15-V1:Single-Base and*
II $\Sigma_{B+R} \Downarrow_{B+R}^{\overline{\tau}'} \Sigma'_{B+R}$ *and*
III $\overline{\tau} = \overline{\tau}' \restriction^R$

Proof. We proceed by induction on $\Sigma_R \Downarrow_R^{\overline{\tau}} \Sigma'_R$:

Rule R:AM-Reflection By Rule R:AM-Reflection we have $\Sigma_R \Downarrow_R^{\varepsilon} \Sigma_R$. with $\Sigma_R = \Sigma'_R$.

I - III We derive $\Sigma_{B+R} \Downarrow_{B+R}^{\overline{\tau}'} \Sigma'_{B+R}$ by Rule AM-Reflection-V15 and thus $\Sigma_{B+R} = \Sigma'_{B+R}$.
By construction and 2) we have $\Sigma'_R \approx \Sigma'_{B+R}$ by Rule V15-V5:Single-Base.
Since $\varepsilon \restriction^R = \varepsilon$ we are finished.

Rule R:AM-Single Then we have $\Sigma_R \Downarrow_R^{\overline{\tau}} \Sigma''_R$ and $\Sigma''_R \overset{\tau}{\dashrightarrow}_R \Sigma'_R$.
We need to show
I $\Sigma_{B+R} \Downarrow_S^{\overline{\tau}' \cdot \tau'} \Sigma'_{B+R}$ and
II $\Sigma'_R \approx \Sigma'_{B+R}$ by Rule V15-V5:Single-Base and
III $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \restriction^R$
We apply the IH on $\Sigma_R \Downarrow_R^{\overline{\tau}} \Sigma''_R$ we get
I' $\Sigma_{B+R} \Downarrow_{B+R}^{\overline{\tau}'} \Sigma''_{B+R}$ and
II' $\Sigma''_R \approx \Sigma''_{B+R}$ by Rule V15-V5:Single-Base and
IV' $\overline{\tau} = \overline{\tau}' \restriction^R$

By Rule V15-V5:Single-Base we have:

$$\begin{aligned}\Sigma''_{\mathrm{R}} &= \Sigma'''_{\mathrm{R}} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle\\ \Sigma''_{\mathrm{B+R}} &= \Sigma'''_{\mathrm{B+R}} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\\ \Sigma'''_{\mathrm{R}} &\sim \Sigma'''_{\mathrm{B+R}}\end{aligned}$$

We continue by inversion on $\Sigma''_{\mathrm{R}} \overset{\tau}{\multimap}_{\mathrm{R}} \Sigma'_{\mathrm{R}}$:

Rule R:AM-Rollback The case is analogous to the corresponding case in Lemma 90 (V45 AM: Completeness w.r.t V5 and projection) using Rule AM-v5-Rollback-V15.

Rule R:AM-Context We then have $\langle p, ctr, \sigma, \mathbb{R}, n\rangle \overset{\tau}{\multimap}_{\mathrm{R}} \overline{\Phi}'_{\mathrm{R}}$ and $n > 0$.

By $\Sigma''_{\mathrm{R}} \approx \Sigma''_{\mathrm{B+R}}$ we know that Rule AM-Context-V15 applies for the step $\Sigma''_{\mathrm{B+R}} \overset{\tau'}{\multimap}_{\mathrm{B+R}} \Sigma'_{\mathrm{B+R}}$.

We now need to find a derivation for the step $\langle p, ctr', \sigma, \mathbb{R}, n\rangle \overset{\tau'}{\multimap}_{\mathrm{B+R}} \overline{\Phi}'_{\mathrm{B+R}}$ according to Rule AM-Context-V15.

We proceed by inversion on $\langle p, ctr, \sigma, \mathbb{R}, n\rangle \overset{\tau}{\multimap}_{\mathrm{R}} \overline{\Phi}'_{\mathrm{R}}$:

Rule R:AM-NoBranch Then $n > 0$ and $\langle p, ctr, \sigma, \mathbb{R}, n\rangle \overset{\tau}{\multimap}_{\mathrm{R}} \overline{\Phi}'_{\mathrm{R}}$ by $\sigma \xrightarrow{\tau} \sigma'$.

Furthermore, $\Sigma'_{\mathrm{R}}.n = n - 1$.

We now do a case analysis on the instruction $p(\sigma(\mathbf{pc}))$:

$p(\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, l$ Then, a speculative transaction of V1 with *id* is started using Rule B:AM-Spec through Rule AM-v1-step-V15 and a new instance $\overline{\Phi}'_{\mathrm{B+R}}$ was pushed on top of the stack.

The rest of the case is analogous to the corresponding case in Lemma 90 (V45 AM: Completeness w.r.t V5 and projection).

otherwise Then we can either use Rule AM-NoBranch through Rule AM-v1-step-V15 or Rule S:AM-NoBranch through Rule AM-v5-step-V15.

Because of Lemma 83 (V45 AM: Confluence), we know that it does not matter which rule we use, which means we can use the same rule as for v5 do derive the step.

The rest of the proof is analogous to the corresponding case in Lemma 90 (V45 AM: Completeness w.r.t V5 and projection).

otherwise These rules include Rule R:AM-barr, Rule R:AM-barr-spec, Rule R:AM-General, Rule R:AM-Ret-Spec, Rule R:AM-Ret-Same, Rule R:AM-Ret-Empty, Rule R:AM-Call and Rule R:AM-Call-Full. Since the rules of V5 are included in the combined semantics and $\Sigma_{\mathrm{B}} \approx \Sigma_{\mathrm{B+R}}$, we can use the corresponding rule in the combined semantics by Confluence or delegate back to V5 by Rule AM-v5-step-V15.

This means we can always do the same step in the combined as in the V5 semantics..

□

M.2 Projections V1 : Soundness and Completeness

Theorem 34 (V15: Relating V1 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\mathcal{A}}_{\mathrm{B}}(p) = Beh^{\mathrm{B+R}}_{\mathcal{A}}(p)\restriction^{B}$.*

Proof. We prove the two directions separately:

⇐ Assume that $(p, \sigma) \Subset^{\omega}_{\mathrm{B+R}} \overline{\tau} \in Beh^{\mathrm{B+R}}_{\mathcal{A}}(p)$.

The case is analogous to Theorem 24 (V45: Relating V4 with projection of combined) using Lemma 133 (V15: Soundness of the AM speculative semantics w.r.t. AM v1 semantics).

We can now conclude that $p, \sigma \Subset^{\omega}_{\mathrm{S}} \overline{\tau}\restriction^{S} \in Beh^{\mathcal{A}}_{\mathrm{S}}(p)$ by Rule S:AM-Trace.

⇒ Assume that $(p, \sigma) \Subset^{\omega}_{\mathrm{B}} \overline{\tau} \in Beh^{\mathcal{A}}_{\mathrm{B}}(p)$.

The case is analogous to Theorem 24 (V45: Relating V4 with projection of combined) using Lemma 134 (V15 AM: Completeness w.r.t V1 and projection).

We thus have $(p, \sigma) \Subset^{\omega}_{\mathrm{B+R}} \overline{\tau}' \in Beh^{\mathrm{B+R}}_{\mathcal{A}}(p)$ with $\overline{\tau}'\restriction^{B} = \overline{\tau}$.

□

Lemma 133 (V15: Soundness of the AM speculative semantics w.r.t. AM v1 semantics). *If*

(1) $\Sigma_{\mathrm{B}} \approx \Sigma_{\mathrm{B+R}}$ *and*

(2) $\Sigma_{\mathrm{B+R}} \Downarrow^{\overline{\tau}}_{\mathrm{B+R}} \Sigma'_{\mathrm{B+R}}$

Then exists Σ_{B} *such that*

I $\Sigma'_{\mathrm{B}} \approx \Sigma'_{\mathrm{B+R}}$ *and*

II if $\Sigma'_B \approx \Sigma'_{B+R}$ *by Rule V15-V1:Single-Base then* $\Sigma_B \Downarrow_B^{\overline{\tau}\restriction^B} \Sigma'_B$ *and*

III if $\Sigma'_B \approx \Sigma'_{B+R}$ *by Rule V15-V1:Single-Speculation-Start then* $\Sigma_B \Downarrow_B^{\overline{\tau}\restriction^B} \Sigma'_B$ *and*

IV if $\Sigma'_B \approx \Sigma'_{B+R}$ *by Rule V15-V1:Single-Speculation-Diff* $\Sigma_B \Downarrow_B^{helper_B(\overline{\tau},i)} \Sigma'_B$, *where* $i = ctr'$ *by unpacking* Σ'_{B+R} *according to Rule V15-V1:Single-Speculation-Diff*

Proof. By Induction on $\Sigma_{B+R} \Downarrow_{B+R}^{\overline{\tau}} \Sigma'_{B+R}$.

Rule AM-Reflection-V15 Then we have $\Sigma_{B+R} \Downarrow_{B+R}^{\varepsilon} \Sigma_{B+R}$ with $\Sigma'_{B+R} = \Sigma_{B+R}$ and by Rule AM-Reflection-V15 we have

I $\Sigma_B \Downarrow_B^{\varepsilon\restriction^B} \Sigma'_B$ with $\Sigma_B = \Sigma'_B$.

II $\Sigma_B \Downarrow_B^{helper_B(\varepsilon,i)} \Sigma'_B$ with $\Sigma_B = \Sigma'_B$.

III $\Sigma'_B \approx \Sigma'_{B+R}$

Rule AM-Single-V15 We have $\Sigma_{B+R} \Downarrow_{B+R}^{\overline{\tau}''} \Sigma''_{B+R}$ with $\Sigma''_{B+R} \overset{\tau}{\rightarrow\!\!\!\!\circ}_{B+R} \Sigma'_{B+R}$.

We now apply IH on $\Sigma''_{B+R} \Downarrow_{B+R}^{\overline{\tau}''} \Sigma''_{B+R}$ and get

(a) $\Sigma''_B \approx \Sigma''_{B+R}$

(b) if $\Sigma''_B \approx \Sigma''_{B+R}$ by Rule V15-V1:Single-Base then $\Sigma_B \Downarrow_B^{\overline{\tau}\restriction^B} \Sigma''_B$ and

(c) if $\Sigma''_B \approx \Sigma''_{B+R}$ by Rule V15-V1:Single-Speculation-Start then $\Sigma_B \Downarrow_B^{\overline{\tau}\restriction^B} \Sigma''_B$ and

(d) if $\Sigma''_B \approx \Sigma''_{B+R}$ by Rule V15-V1:Single-Speculation-Diff then $\Sigma_B \Downarrow_B^{helper_B(\overline{\tau},i)} \Sigma''_B$, where $j = ctr'$ by unpacking Σ''_{B+R} according to Rule V15-V1:Single-Speculation-Diff

We do a case distinction on $\approx$ in $\Sigma''_B \approx \Sigma''_{B+R}$:

Rule V15-V1:Single-Base We have

$$\begin{aligned}
&\Sigma_B \Downarrow_B^{\overline{\tau}\restriction^B} \Sigma''_B\\
&\Sigma''_B = \Sigma'''_B \cdot \langle p, ctr, \sigma, n\rangle_{\overline{\rho}}\\
&\Sigma''_{B+R} = \Sigma'''_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle_{\overline{\rho}}\\
&\Sigma'''_B \sim \Sigma'''_{B+R}
\end{aligned}$$

We proceed by inversion on the derivation $\Sigma''_{B+R} \overset{\tau}{\rightarrow\!\!\!\!\circ}_{B+R} \Sigma'_{B+R}$.

Rule AM-v5-Rollback-V15 Since $\Sigma''_B \approx \Sigma''_{B+R}$ by Rule V15-V1:Single-Base, there cannot be a roll back of V5.

Rule AM-v1-Rollback-V15 By (b), it can only be roll back of V4 and only be the topmost state.

Furthermore, this means that $n = 0$.

Then $\Sigma''_B \overset{\texttt{rlb}_B\ ctr}{\rightarrow\!\!\!\!\circ}_B \Sigma'_B$ by Rule B:AM-Rollback, since n is equal between the two states.

The rest of the case is analogous to the corresponding case in Lemma 111 (V14: Soundness of the AM speculative semantics w.r.t. AM v1 semantics).

Rule AM-Context-V15 We have $\Phi_{B+R} \overset{\tau}{\rightarrow\!\!\!\!\circ}_{B+R} \overline{\Phi}'_{B+R}$ and $n > 0$.

We now use inversion on $\Phi_{B+R} \overset{\tau}{\rightarrow\!\!\!\!\circ}_{B+R} \overline{\Phi}_{B+R}$:

Rule AM-v5-step-V15 Then we have $\Phi_{B+R}\restriction^R \overset{\tau}{\rightarrow\!\!\!\!\circ}_R \overline{\Phi}'_R$.

By inversion on $\Phi_{B+R}\restriction^R \overset{\tau}{\rightarrow\!\!\!\!\circ}_R \overline{\Phi}'_R$ we get:

Rule R:AM-Ret-Spec The case is analogous to the corresponding case in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) using Lemma 130 (V15: V1 step)

otherwise The case is analogous to the corresponding case in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) using Lemma 130 (V15: V1 step)

Rule AM-v1-step-V15 Then we have $\Phi_{B+R}\restriction^B = (\Phi_B, \mathbb{R})$ and $\Phi_B \overset{\tau}{\rightarrow\!\!\!\!\circ}_B \overline{\Phi}'_B$.

The case is analogous to the Rule AM-v1-step-V14 case in Lemma 111 (V14: Soundness of the AM speculative semantics w.r.t. AM v1 semantics) combined with the fact that the rules of V1 cannot generate a $\texttt{start}_R\ id$ or $\texttt{rlb}_R\ id$ observation.

Rule V15-V1:Single-Speculation-Start We have:

$$\begin{aligned}\Sigma_B \Downarrow_B^{\overline{\tau}\restriction^B} \Sigma''_B\\ \Sigma''_B =& \Sigma'''_B \cdot \langle p, ctr, \sigma, n\rangle\\ \Sigma''_{B+R} =& \Sigma'''_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle_{\texttt{ret}\ l\cdot \texttt{start}_R\ ctr'}\\ \Sigma'''_B \cdot \langle p, ctr, \sigma, n\rangle \sim& \Sigma'''_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\end{aligned}$$

We now proceed by inversion on the derivation $\Sigma''_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \Sigma'_{B+R}$.

Rule AM-v1-Rollback-V15 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v5-Rollback-V15 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-Context-V15 We have $\Phi_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \overline{\Phi}'_{B+R}$.

We now use inversion on $\Phi_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \overline{\Phi}_{B+R}$:

Rule AM-v1-step-V15 Contradiction, because $\overline{\rho}$ is non-empty and Rule B:AM-General does not work on $\texttt{start}_R$ *id* observations.

Rule AM-v5-step-V15 Then we have $\Phi_{B+R}\restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_R$.

By inversion on $\Phi_{B+R}\restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_R$ we get:

Rule R:AM-General By definition we have $\tau = \texttt{start}_R\ ctr$.

Since Rule R:AM-General does not modify the state, we have $\Sigma'_{B+R} = \Sigma''_{B+R}\texttt{ret}\ l$.

Then we choose $\Sigma'_B = \Sigma''_B$ and derive the step $\Sigma''_B \Downarrow_B^{\varepsilon} \Sigma'_B$ by Rule B:AM-Reflection.

The case is analogous to the corresponding case Rule R:AM-General in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) and the fact that $helper_B()$ behaves the same as $helper_S()$ for $\texttt{start}_R$ observations.

otherwise Contradiction, because $\overline{\rho}$ is non-empty.

Rule V15-V1:Single-Speculation-Diff We have

$$\begin{aligned}\Sigma_B \Downarrow_B^{helper_B(\overline{\tau},j)} \Sigma''_B\\ \Sigma''_B =& \Sigma'''_B \cdot \langle p, ctr, \sigma, n\rangle\\ \Sigma''_{B+R} =& \Sigma'''_{B+R} \cdot \langle p, ctr'', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr''', \sigma'', \mathbb{R}'', n''\rangle \cdot \Sigma^{\dagger}_{B+R}\\ \Sigma'''_B \cdot \langle p, ctr, \sigma, n\rangle \sim& \Sigma'''_{B+R} \cdot \langle p, ctr'', \sigma, \mathbb{R}, n\rangle\\ j =& ctr''\end{aligned}$$

Rule AM-v1-Rollback-V15 This means a transaction is rolled back that was created later than the transaction with $id = j$.

Then we choose $\Sigma'_B = \Sigma''_B$ and derive the step $\Sigma''_B \Downarrow_S^{\varepsilon} \Sigma'_B$ by Rule B:AM-Reflection.

The case is analogous to the corresponding case in Lemma 111 (V14: Soundness of the AM speculative semantics w.r.t. AM v1 semantics).

Rule AM-v5-Rollback-V15 There are two cases depending on the *id* of the rolled back transaction:

$id \neq j$ This means a transaction is rolled back that was created later than the transaction with $id = j$.

The case is analogous to the case of Rule AM-v5-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

$id = j$ Then we choose $\Sigma'_B = \Sigma''_B$ and derive the step $\Sigma''_B \Downarrow_B^{\varepsilon} \Sigma'_B$ by Rule B:AM-Reflection.

Since the transaction with $id = j$ was rolled back, we know that $\Sigma'_{B+R} = \Sigma'''_{B+R} \cdot \langle p, ctr''', \sigma, \mathbb{R}, n\rangle$.

For the trace, we get $\overline{\tau} \cdot \texttt{rlb}_R\ j\restriction^B = helper_B(\overline{\tau}, j)$ by definition of $\restriction^B$ and $id = j$.

The case is analogous to the case of Rule AM-v5-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) using the definitions of $\restriction^B$ and $helper_B()$.

otherwise Then we choose $\Sigma'_B = \Sigma''_B$ and derive the step $\Sigma''_B \Downarrow_B^{\varepsilon} \Sigma'_B$ by Rule B:AM-Reflection since the transaction with $id = j$ is still ongoing.

The case is analogous to the case Rule AM-v4-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

□

We abuse the fact that $\restriction^B$ and $\restriction^S$ behave similar with speculative transactions generated by V5. Also for all other combinations. That is why we sometimes elide details when we write analogous to. Even if another projection is used, it behaves in the same way.

Lemma 134 (V15 AM: Completeness w.r.t V1 and projection)**.** *If*

(1) $\Sigma_B \approx \Sigma_{B+R}$ *by Rule V15-V1:Single-Base and*

(2) $\Sigma_B \Downarrow_B^{\overline{\tau}} \Sigma'_B$

Then exists Σ'_{B+R} *such that*

I $\Sigma'_B \approx \Sigma'_{B+R}$ *by Rule V15-V1:Single-Base and*

II $\Sigma_{B+R} \Downarrow_{B+R}^{\overline{\tau}'} \Sigma'_{B+R}$ *and*

III $\overline{\tau} = \overline{\tau}' \restriction^B$

Proof. We proceed by induction on $\Sigma_B \Downarrow_R^{\overline{\tau}} \Sigma'_B$:

Rule B:AM-Reflection By Rule B:AM-Reflection we have $\Sigma_B \Downarrow_B^{\varepsilon} \Sigma_B$. with $\Sigma_B = \Sigma'_B$.

I - III We derive $\Sigma_{B+R} \Downarrow_{B+R}^{\overline{\tau}'} \Sigma'_{B+R}$ by Rule AM-Reflection-V15 and thus $\Sigma_{B+R} = \Sigma'_{B+R}$.
By construction and 2) we have $\Sigma'_B \approx \Sigma'_{B+R}$ by Rule V15-V1:Single-Base.
Since $\varepsilon \restriction^B = \varepsilon$ we are finished.

Rule R:AM-Single Then we have $\Sigma_B \Downarrow_B^{\overline{\tau}} \Sigma''_B$ and $\Sigma''_B \overset{\tau}{\Rightarrow}_R \Sigma'_B$.
We need to show
I $\Sigma_{B+R} \Downarrow_S^{\overline{\tau}' \cdot \tau'} \Sigma'_{B+R}$ and
II $\Sigma'_B \approx \Sigma'_{B+R}$ by Rule V15-V5:Single-Base and
III $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \restriction^B$
We apply the IH on $\Sigma_B \Downarrow_B^{\overline{\tau}} \Sigma''_B$ we get
I' $\Sigma_{B+R} \Downarrow_{B+R}^{\overline{\tau}'} \Sigma''_{B+R}$ and
II' $\Sigma''_B \approx \Sigma''_{B+R}$ by Rule V15-V5:Single-Base and
IV' $\overline{\tau} = \overline{\tau}' \restriction^B$
By Rule V15-V5:Single-Base we have:

$$\begin{aligned} \Sigma''_B &= \Sigma'''_B \cdot \langle p, ctr, \sigma, n \rangle \\ \Sigma''_{B+R} &= \Sigma'''_{B+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n \rangle \\ \Sigma'''_B &\sim \Sigma'''_{B+R} \end{aligned}$$

We continue by inversion on $\Sigma''_B \overset{\tau}{\Rightarrow}_B \Sigma'_B$:

Rule B:AM-Rollback The case is analogous to the corresponding case in Lemma 88 (V45 AM: Completeness w.r.t V4 and projection) using Rule AM-v1-Rollback-V15.

Rule B:AM-Context We then have $\langle p, ctr, \sigma, n \rangle \overset{\tau}{\Rightarrow}_B \overline{\Phi}'_B$ and $n > 0$.

By $\Sigma''_B \approx \Sigma''_{B+R}$ we know that Rule AM-Context-V15 applies for the step $\Sigma''_{B+R} \overset{\tau'}{\Rightarrow}_{B+R} \Sigma'_{B+R}$.

We now need to find a derivation for the step $\langle p, ctr', \sigma, \mathbb{R}, n \rangle \overset{\tau'}{\Rightarrow}_{B+R} \overline{\Phi}'_{B+R}$ according to Rule AM-Context-V15.

We proceed by inversion on $\langle p, ctr, \sigma, n \rangle \overset{\tau}{\Rightarrow}_B \overline{\Phi}'_B$:

Rule AM-NoBranch Then $n > 0$ and $\langle p, ctr, \sigma, n \rangle \overset{\tau}{\Rightarrow}_B \overline{\Phi}'_B$ by $\sigma \xrightarrow{\tau} \sigma'$.
Furthermore, $\Sigma'_B.n = n - 1$.
We now do a case analysis on the instruction $p(\sigma(\mathbf{pc}))$:

$p(\sigma(\mathbf{pc})) =$ **ret and** $\mathbb{R}$ **is non-empty and** $\mathbb{R}$ **value is different to return address** Then, a speculative transaction of V5 with *id* is started using Rule R:AM-Ret-Spec through Rule AM-v5-step-V15 and a new instance Φ'_{B+R} was pushed on top of the stack of Σ''_{B+R}.
The rest of the case is analogous to the corresponding case in Lemma 88 (V45 AM: Completeness w.r.t V4 and projection).

$p(\sigma(\mathbf{pc})) =$ **ret and** $\mathbb{R}$ **is empty or** $\mathbb{R}$ **is not different to return address** Since $n > 0$, the state can do a step using either Rule R:AM-Ret-Empty or Rule R:AM-Ret-Same through Rule AM-v5-step-V15 (Note that the meta parameter Z restricts the V4 semantics in the combined part).
The case is analogous to the corresponding case in Lemma 88 (V45 AM: Completeness w.r.t V4 and projection) together with the fact that $\restriction^B$ and $\restriction^S$ behave similar with speculative transactions generated by V5.

$p(\sigma(\mathbf{pc})) =$ **call** f Since $n > 0$, the state can do a step using either Rule R:AM-Call or Rule R:AM-Call-Full through Rule AM-v5-step-V15. The case is analogous to the corresponding case in Lemma 88 (V45 AM: Completeness w.r.t V4 and projection).

otherwise Then we can either use Rule AM-NoBranch through Rule AM-v1-step-V15 or Rule S:AM-NoBranch through Rule AM-v5-step-V15.

Because of Lemma 83 (V45 AM: Confluence), we know that it does not matter which rule we use, which means we can use the same rule as for v5 do derive the step.
The rest of the proof is analogous to the corresponding case in Lemma 90 (V45 AM: Completeness w.r.t V5 and projection).

otherwise These rules include Rule B:AM-barr, Rule B:AM-barr-spec, Rule B:AM-General. Since these rules of V1 are included unchanged in the combined semantics and $\Sigma_B \approx \Sigma_{B+R}$, we can use the corresponding rule in the combined semantics by Confluence or delegate back to V1 by Rule AM-v1-step-V15.
This means we can always do the same step in the combined as in the V1 semantics.

□

Theorem 35 (V15: Relating Combined to non-speculative). *Let p be a program and ω be a speculation window. Then $Beh_{NS}(p) = Beh^{B+R}_{\mathcal{A}}(p)\restriction_{ns}$.*

Proof. By Lemma 12 (V15: Relating speculative projections to non-speculative projection), we have $Beh^{B+R}_{\mathcal{A}}(p)\restriction_{ns} = Beh^{B+R}_{\mathcal{A}}(p)\restriction^{R}\restriction^{B}$.
By Theorem 33 (V15: Relating V5 with projection of combined), we have that $Beh^{B+R}_{\mathcal{A}}(p)\restriction^{R} = Beh^{\mathcal{A}}_{R}(p)$.
By Lemma 16 (V5: speculative-projections equal to non-speculative Projections), we get $Beh^{\mathcal{A}}_{R}(p)\restriction^{B} = Beh^{\mathcal{A}}_{R}(p)\restriction_{ns}$.
By Theorem 20 (V5AM: Behaviour of non-speculative semantics and AM semantics), we know that $Beh^{\mathcal{A}}_{R}(p)\restriction_{ns} = Beh_{NS}(p)$.
Combining these facts we get:

$$\begin{aligned}
&Beh^{B+R}_{\mathcal{A}}(p)\restriction_{ns}\\
&= Beh^{B+R}_{\mathcal{A}}(p)\restriction^{R}\restriction^{B}\\
&= Beh^{\mathcal{A}}_{R}(p)\restriction^{B}\\
&= Beh^{\mathcal{A}}_{R}(p)\restriction_{ns}\\
&= Beh_{NS}(p)
\end{aligned}$$

and are finished. □

Corollary 5 (V15: SNI of combined preserves SNI of parts)**.** *Let p be a program and ω be a speculation window. If $p \vdash_{B+R}$ SNI then $p \vdash_{B}$ SNI and $p \vdash_{R}$ SNI.*

Proof. Assume $p \vdash_{B+R}$ SNI and that there are $\sigma, \sigma' \in InitConf$ with $\sigma \sim_P \sigma'$ for some policy P and $(p,\sigma) \,\text{\faGhost}^{O}_{NS}\, \overline{\tau}$, $(p,\sigma') \,\text{\faGhost}^{O}_{NS}\, \overline{\tau}'$.
We need to show that
(1) $(p,\sigma) \,\text{\faGhost}^{\omega}_{R}\, \overline{\tau}_r$, $(p,\sigma') \,\text{\faGhost}^{\omega}_{R}\, \overline{\tau}_r$
(2) $(p,\sigma) \,\text{\faGhost}^{\omega}_{B}\, \overline{\tau}_b$, $(p,\sigma') \,\text{\faGhost}^{\omega}_{B}\, \overline{\tau}_b$
We show the proof for 1). The proof for 2) is analogous using Theorem 34 (V15: Relating V1 with projection of combined).
Unfolding the definition of $p \vdash_{B+R}$ SNI we get:
(1) if $\sigma \sim_P \sigma'$ and $(p,\sigma) \,\text{\faGhost}^{O}_{NS}\, \overline{\tau}$, $(p,\sigma') \,\text{\faGhost}^{O}_{NS}\, \overline{\tau}$, then $(p,\sigma) \,\text{\faGhost}^{\omega}_{B+R}\, \overline{\tau}_{br}$, $(p,\sigma') \,\text{\faGhost}^{\omega}_{B+R}\, \overline{\tau}_{br}$
After initialization we have $(p,\sigma) \,\text{\faGhost}^{\omega}_{B+R}\, \overline{\tau}_{br}$, $(p,\sigma') \,\text{\faGhost}^{\omega}_{B+R}\, \overline{\tau}_{br}$.
By Theorem 33 (V15: Relating V5 with projection of combined) we have $(p,\sigma) \,\text{\faGhost}^{\omega}_{R}\, \overline{\tau}_{br}\restriction^{R} \in Beh^{\mathcal{A}}_{R}(p)$ and $(p,\sigma') \,\text{\faGhost}^{\omega}_{R}\, \overline{\tau}_{br}\restriction^{R} \in Beh^{\mathcal{A}}_{R}(p)$, which is what we needed to show.

□

M.3 Relating Speculative and AM semantics

Lemma 135 (V15SE: Confluence). *If*

(1) $X_{B+R} \overset{\tau}{\rightsquigarrow}^{O_{B+R}}_{B+R} X'_{B+R}$ *and*

(2) $X_{B+R} \overset{\tau}{\rightsquigarrow}^{O_{B+R}}_{B+R} X''_{B+R}$ *derived by a different rule*

Then

(1) $X'_{B+R} = X_{B+R}$

Proof. Analogous to Lemma 91 (V45SE: Confluence) □

Theorem 36 (V15: SNI). *For a program p, all oracles O with speculative window at most ω and for a security Policy P,* $p \vdash^{O}_{B+R}$ *SNIp iff* $p \vdash_{B+R}$ *SNIp.*

Proof. We prove the two directions separately:

(⇒) The proof proceeds analogous to Theorem 17 (S SNI) using (Lemma 146 (V15: Completeness Am semantics w.r.t. speculative semantics))

(⇐) The proof proceeds analogously to Theorem 17 (S SNI) using the Soundness (Lemma 141 (V15: Soundness Big-step))

□

Definition 70 (V15: Relation between AM and spec for all oracles). *We define two relations between AM and oracle semantics.* $\approx_{B+R}$ $\sim$

$\boxed{\Sigma_{B+R} \approx_{B+R} X_{B+R}}$

$$\frac{}{\varnothing \approx_{B+R} \varnothing}\ (V15{:}Base) \qquad \frac{\Sigma_{B+R} \sim X_{B+R}\restriction_{com} \quad INV(\Sigma_{B+R}, X_{B+R})}{\Sigma_{B+R} \approx_{B+R} X_{B+R}}\ (V15{:}Single\text{-}Base)$$

$$\frac{\begin{array}{c}\Sigma_{B+R} \sim X_{B+R}\restriction_{com} \quad \Sigma''_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma'''_{B+R} \text{ where transaction with id ctr is rolled back} \\ X_{B+R} = X'_{B+R} \cdot \langle p, ctr, \sigma, h, n''\rangle \qquad x = (S, true) \vee (B, m \wedge m = \sigma(\mathbf{pc}) \\ \Sigma_{B+R} = \Sigma'_{B+R} \cdot \langle p, ctr, \sigma, n\rangle \qquad INV(\Sigma_{B+R}, X_{B+R})\end{array}}{\Sigma'_{B+R} \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma'', n'\rangle \cdot \Sigma_{B+R1} \approx_{B+R} X'_{B+R} \cdot \langle p, ctr, \sigma, h, n''\rangle \cdot \langle p, ctr', \sigma, h, n'''\rangle^{x}}\ (V15{:}Single\text{-}OracleTrue)$$

$$\frac{\begin{array}{c}\Sigma''_{B+R} \sim X''_{B+R}\restriction_{com} \quad n' \geq 0 \quad \Sigma''_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma'''_{B+R} \text{ where transaction with id ctr is rolled back} \quad x = (S, true) \vee (B, m) \\ X_{B+R} = X'_{B+R} \cdot \langle p, ctr, \sigma, h, n''\rangle \qquad \Sigma_{B+R} = \Sigma'_{B+R} \cdot \langle p, ctr, \sigma, n\rangle \qquad INV(\Sigma_{B+R}, X_{B+R})\end{array}}{\Sigma'_{B+R} \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma'', n'\rangle^{x} \cdot \Sigma_{B+R1} \approx_{B+R} X'_{B+R} \cdot \langle p, ctr, \sigma, h, n''\rangle \cdot \langle p, ctr', \sigma'', h', 0\rangle^{x} \cdot X_{B+R1}}\ (V15{:}Single\text{-}Transaction\text{-}Rollback)$$

$\boxed{\Sigma_{B+R} \sim X_{B+R}}$

$$\frac{}{\varnothing \sim \varnothing}\ (V15{:}Base) \qquad \frac{|\Sigma'_{B+R}| = |X'_{B+R}| \quad \Sigma'_{B+R} \sim X'_{B+R}}{\Sigma'_{B+R} \cdot \langle p, ctr, \sigma, n\rangle^{b} \sim X'_{B+R} \cdot \langle p, ctr', \sigma, h, n'\rangle^{b}}\ (V15{:}Single)$$

Lemma 136 (V15: Coincide on $\approx_{B+R}$ for projections). *If*

(1) $\Sigma_{B+R} \approx_{B+R} X_{B+R}$ *by Rule V15:Single-Base*

Then

(1) $\Sigma_{B+R}\restriction^{R} \approx_{R} X_{B+R}\restriction^{R}$ *by Rule Single-Base and*

(2) $\Sigma_{B+R}\restriction^{B} \approx_{B} X_{B+R}\restriction^{B}$ *by Rule V1:Single-Base*

Proof. The proof is analogous to Lemma 92 (V45: Coincide on $\approx_{S+R}$ for projections). □

Lemma 137 (V15: Coincide on ≅ for projections). *If*

(1) $\Sigma_{B+R} \cong X_{B+R}$

Then

(1) $\Sigma_{B+R}\restriction^{R} \cong X_{B+R}\restriction^{R}$ *and*

(2) $\Sigma_{B+R}\restriction^{B} \cong X_{B+R}\restriction^{B}$

Proof. The projection function does not change the values of the instances in the state. Thus, $\Sigma_{B+R}\restriction^{R} \cong X_{B+R}\restriction^{R}$ and $\Sigma_{B+R}\restriction^{B} \cong X_{B+R}\restriction^{B}$ trivially holds. □

Lemma 138 (V15: Initial states fulfill properties). *Let p be a program, ω be a speculation window and O be an oracle with speculation window at most ω. If*

(1) $\sigma, \sigma' \in InitConf$ *and*
(2) $\Sigma^{init}_{B+R}(p,\sigma)$ *and* $\Sigma^{init}_{B+R}(p,\sigma')$ *and*
(3) $X^{init}_{B+R}(p,\sigma)$ *and* $X^{init}_{B+R}(p,\sigma')$

Then

(1) $X^{init}_{B+R}(p,\sigma) \cong X^{init}_{B+R}(p,\sigma')$ *and*
(2) $\Sigma^{init}_{B+R}(p,\sigma) \cong \Sigma^{init}_{B+R}(p,\sigma')$ *and*
(3) $\Sigma^{init}_{B+R}(p,\sigma) \approx_{B+R} X^{init}_{B+R}(p,\sigma)$ *and* $\Sigma^{init}_{B+R}(p,\sigma') \approx_{B+R} X^{init}_{B+R}(p,\sigma')$ *by Rule V15:Single-Base and*

Proof. The proof is analogous to Lemma 45 (S: Initial states fulfill properties). □

Lemma 139 (V15AM: Single step preserves $\cong$). *If*

(1) $\Sigma_{B+R} \cong \Sigma^{\dagger}_{B+R}$ *and*
(2) $\Sigma_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \Sigma'_S$ *and* $\Sigma^{\dagger}_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \Sigma^{\dagger\dagger}_{B+R}$

Then

(1) $\Sigma'_{B+R} \cong \Sigma^{\dagger\dagger}_{B+R}$

Proof. The proof is analogous to Lemma 43 (S AM: Single step preserves $\cong$). □

Lemma 140 (V15SE: Single step preserves $\cong$). *If*

(1) $X_{B+R} \cong X^{\dagger}_{B+R}$ *and*
(2) $X_{B+R} \overset{\tau}{\rightsquigarrow}^{O_{B+R}}_{B+R} X'_{B+R}$ *and* $X^{\dagger}_{B+R} \overset{\tau}{\rightsquigarrow}^{O_{B+R}}_{B+R} X^{\dagger\dagger}_{B+R}$

Then

(1) $X'_{B+R} \cong X^{\dagger\dagger}_{B+R}$ *and*

Proof. The proof is analogous to Lemma 44 (S SE: Single step preserves $\cong$). □

M.4 Soundness

Lemma 141 (V15: Soundness Big-step). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*
If

(1) $\sigma, \sigma' \in InitConf$ *and*
(2) $(p,\sigma) \overset{\omega}{\Subset}_{B+R} \overline{\tau}, (p,\sigma') \overset{\omega}{\Subset}_{B+R} \overline{\tau}$

Then for all prediction oracles O with speculation window at most ω.

I $(p,\sigma) \overset{O}{\Subset}_{B+R} \overline{\tau}', (p,\sigma) \overset{O}{\Subset}_{B+R} \overline{\tau}'$

Proof. The proof is analogous to Lemma 46 (S: Soundness Am semantics w.r.t. speculative semantics) using Lemma 138 (V15: Initial states fulfill properties) to show that our initial states fulfill all the premises for Lemma 142 (V15: Soundness Am semantics w.r.t. speculative semantics with new relation between states). □

Lemma 142 (V15: Soundness Am semantics w.r.t. speculative semantics with new relation between states). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*
If

(1) $\Sigma_{B+R} \cong \Sigma^{\dagger}_{B+R}$
(2) $X_{B+R} \cong X^{\dagger}_{B+R}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma^{*}_{B+R} \approx_{B+R} X_{B+R}$ *and* $\Sigma^{\dagger}_{B+R} \approx_{B+R} X^{\dagger}_{B+R}$
(4) $\Sigma_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma'_{B+R}$ *and* $\Sigma^{\dagger}_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma^{\dagger\dagger}_{B+R}$

Then for all prediction oracles O with speculation window at most ω.

I $X_{B+R} \overset{O}{\downarrow}^{R}_{\overline{\tau}'} X'_{B+R}, X^{\dagger}_{B+R} \overset{O}{\downarrow}^{R}_{\overline{\tau}''} X^{\dagger\dagger}_{B+R}$
II $\Sigma'_{B+R} \cong \Sigma^{\dagger\dagger}_{B+R}$
III $X'_{B+R} \cong X^{\dagger\dagger}_{B+R}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{B+R} \approx_{B+R} X'_{B+R}$ *and* $\Sigma^{\dagger\dagger}_{B+R} \approx_{B+R} X^{\dagger\dagger}_{B+R}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. By Induction on $\Sigma_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma'_{B+R}$ and $\Sigma^{\dagger}_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma^{\dagger\dagger}_{B+R}$.

Rule AM-Reflection-V15 We have $\Sigma_{B+R} \Downarrow^{\varepsilon}_{B+R} \Sigma'_{B+R}$ and $\Sigma^{\dagger}_{B+R} \Downarrow^{\varepsilon}_{B+R} \Sigma''_{B+R}$, where $\Sigma'_{B+R} = \Sigma_{B+R}$ and $\Sigma''_{B+R} = \Sigma^{\dagger}_{B+R}$. We choose $\Sigma'_{B+R} = \Sigma'_{B+R}$ and $\Sigma^{\dagger\dagger}_{B+R} = \Sigma''_{B+R}$.

We further use Rule V15-SE:Reflection to derive $X_{B+R} \overset{O}{\Downarrow}{}^{R}_{\varepsilon} X'_{B+R}$, $X^{\dagger}_{B+R} \overset{O}{\Downarrow}{}^{R}_{\varepsilon} X^{\dagger\dagger}_{B+R}$ with $X'_{B+R} = X_{B+R}$ and $X^{\dagger\dagger}_{B+R} = X^{\dagger}_{B+R}$. We now trivially satisfy all conclusions.

Rule AM-Single-V15 We have $\Sigma_{B+R} \Downarrow^{\overline{\tau}''}_{B+R} \Sigma''_{B+R}$ with $\Sigma''_{B+R} \overset{\tau}{\twoheadrightarrow}_{B+R} \Sigma'_{B+R}$ and $\Sigma^{\dagger}_{B+R} \Downarrow^{\overline{\tau}''}_{B+R} \Sigma^{*}_{B+R}$ and $\Sigma''_{B+R} \overset{\tau}{\twoheadrightarrow}_{B+R} \Sigma^{\dagger\dagger}_{B+R}$.

We now apply IH on $\Sigma_{B+R} \Downarrow^{\overline{\tau}''}_{B+R} \Sigma''_{B+R}$ and $\Sigma^{\dagger}_{B+R} \Downarrow^{\overline{\tau}''}_{B+R} \Sigma^{*}_{B+R}$ and get

(a) $X_{B+R} \overset{O}{\Downarrow}{}^{R}_{\overline{\tau}'} X''_{B+R}$, $X^{\dagger}_{B+R} \overset{O}{\Downarrow}{}^{R}_{\overline{\tau}''} X^{*}_{B+R}$
(b) $\Sigma''_{B+R} \cong \Sigma^{*}_{B+R}$
(c) $X''_{B+R} \cong X^{*}_{B+R}$ and $\overline{\rho}' = \varnothing$
(d) $\Sigma''_{B+R} \approx_{B+R} X''_{B+R}$ and $\Sigma^{*}_{B+R} \approx_{B+R} X^{*}_{B+R}$
(e) $\overline{\tau}' = \overline{\tau}''$

We do a case distinction on $\approx_{B+R}$ in $\Sigma''_{B+R} \approx_{B+R} X''_{B+R}$ and $\Sigma^{*}_{B+R} \approx_{B+R} X^{*}_{B+R}$ by inversion

Rule V15:Single-Base We thus have $\Sigma''_{B+R} \sim X''_{B+R}\restriction_{com}$ and $INV(\Sigma''_{B+R}, X''_{B+R})$ (Similar for Σ^{*}_{B+R} and X^{*}_{B+R}).

Similarly to Lemma 98 (V45: Soundness Am semantics w.r.t. speculative semantics with new relation between states) we can account for possible commits and get a state X^{**}_{B+R} such that $\Sigma''_{B+R} \approx_{B+R} X^{**}_{B+R}$ by Rule V15:Single-Base

We now proceed by inversion on the derivations $\Sigma''_{B+R} \overset{\tau}{\twoheadrightarrow}_{B+R} \Sigma'_{B+R}$ and $\Sigma^{*}_{B+R} \overset{\tau}{\twoheadrightarrow}_{B+R} \Sigma^{\dagger\dagger}_{B+R}$.

Note that by $\Sigma''_{B+R} \cong \Sigma^{*}_{B+R}$ and the fact the same traces are generated, we know that the same rule was used to derive the step.

Rule AM-Context-V15 We now have $\Phi'_{B+R} \overset{\tau}{\twoheadrightarrow}_{B+R} \overline{\Phi}'_{B+R}$ and $\Phi''_{B+R} \overset{\tau}{\twoheadrightarrow}_{B+R} \overline{\Phi}'''_{B+R}$ where $\Sigma''_{B+R} = \overline{\Phi}_{B+R} \cdot \Phi'_{B+R}$ and $\Sigma^{*}_{B+R} = \overline{\Phi}''_{B+R} \cdot \Phi''_{B+R}$.

Furthermore, $n > 0$ and note that all states point to the same instruction by b-d.

Rule AM-v5-step-V15 Then, we have $\Phi_S\restriction^{R} \overset{\tau}{\twoheadrightarrow}_{R} \overline{\Phi}'_{B+R}\restriction^{R}$

We use Lemma 143 (V15: V5 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule AM-v1-step-V15 Then we have $\Phi_{B+R}\restriction^{B} \overset{\tau}{\twoheadrightarrow}_{B} \overline{\Phi}'_{B+R}\restriction^{B}$.

We use Lemma 144 (V15: V1 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule AM-v1-Rollback-V15 Contradiction, because $minWndw(X^{**}_{B+R}) > 0$ and $INV(\Sigma''_{B+R}, X^{**}_{B+R})$.

Rule AM-v5-Rollback-V15 Contradiction, because $minWndw(X^{**}_{B+R}) > 0$ and $INV(\Sigma''_{B+R}, X^{**}_{B+R})$.

Rule V15:Single-OracleTrue We thus have

$$
\begin{aligned}
X''_{B+R} &= X_{B+R3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma, h, n''' \rangle^{false} \\
\Sigma''_{B+R} &= \Sigma_{B+R3} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle \cdot \Sigma_{B+R4} \\
X_{B+R} &= X_{B+R3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \\
\Sigma_{B+R} &= \Sigma_{B+R3} \cdot \langle p, ctr, \sigma, n \rangle \\
\Sigma_{B+R} &\sim X_{B+R}\restriction_{com}
\end{aligned}
$$

The form of X^{*}_{B+R} and Σ^{*}_{B+R} is analogous. We now apply inversion on $\Sigma''_{B+R} \overset{\tau}{\twoheadrightarrow}_{B+R} \Sigma'_{B+R}$.

Rule AM-Context-V15 We choose $X'_{B+R} = X''_{B+R}$ and $X^{\dagger\dagger}_{B+R} = X^{*}_{B+R}$.

I By IH a) and Rule V15-SE:Reflection

II By Lemma 139 (V15AM: Single step preserves $\cong$).

III Since $X'_{B+R} = X''_{B+R}$ and $X^{\dagger\dagger}_{B+R} = X^{*}_{B+R}$, we are finished using IH c).

IV We show that $X'_{B+R} \approx_{B+R} \Sigma'_{B+R}$ by Rule V15:Single-OracleTrue. The proof for $X^{\dagger\dagger}_{B+R} \approx \Sigma^{\dagger\dagger}_{B+R}$ is analogous.

Since we did not roll back the transaction with *id ctr'* we have that Σ_{B+R} does not change.

Since X_{B+R} remains the same as well, we have $\Sigma_{B+R} \sim X_{B+R}\restriction_{com}$ and $INV(\Sigma_{B+R}, X_{B+R})X_{B+R}\restriction_{com}$.

Thus, we fulfill all premises for Rule V15:Single-OracleTrue.

V By IH e).

Rule AM-v5-Rollback-V15 There are two cases depending on the transaction *id* of the rolled back transaction:

id > *ctr* Then an inner transaction w.r.t our *ctr* transaction was finished. We choose $X'_{B+R} = X_{B+R}$ and $X^{\dagger\dagger}_{B+R} = X^{\dagger}_{B+R}$. The rest of the proof proceeds similar to the context case above.

id = *ctr* Most cases are similar to the context case above. Only the relation changes. We choose $X'_{B+R} = X_{B+R}$ and $X^{\dagger\dagger}_{B+R} = X^{\dagger}_{B+R}$. The case is analogous to the corresponding case in Lemma 142 (V15: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

Rule AM-v1-Rollback-V15 The case is analogous to the case Rule AM-v5-Rollback-V15 above.

Rule V15:Single-Transaction-Rollback We have

$$\begin{aligned}
X''_{B+R} &= X_{B+R3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma'', h', 0 \rangle^{true} \cdot X_{B+R4} \\
\Sigma''_{B+R} &= \Sigma_{B+R3} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle^{true} \cdot \Sigma_{B+R4} \\
X_{B+R} &= X_{B+R3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \\
\Sigma_{B+R} &= \Sigma_{B+R3} \cdot \langle p, ctr, \sigma, n \rangle \\
\Sigma_{B+R} &\sim X_{B+R} \restriction_{com} \\
n' &\geq 0
\end{aligned}$$

The form of X^*_{B+R} and Σ^*_{B+R} is analogous.
There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma''_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \Sigma'_{B+R}$ is not a rollback for ctr. The case is analogous to the corresponding case in Lemma 98 (V45: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

$n' = 0$ Then we know that $\Sigma''_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \Sigma'_{B+R}$ was created by either Rule AM-v1-Rollback-V15 or Rule AM-v5-Rollback-V15 and is a rollback for ctr.
We do the proof for Rule AM-v5-Rollback-V15, since the case for Rule AM-v1-Rollback-V15 is analogous.
The proof obligations are analogous to the corresponding case in Lemma 98 (V45: Soundness Am semantics w.r.t. speculative semantics with new relation between states) using Lemma 139 (V15AM: Single step preserves $\cong$) for II and Lemma 140 (V15SE: Single step preserves $\cong$) for III.

□

Lemma 143 (V15: V5 Soundness Single step). *If*

(1) $\Sigma_{B+R} \approx_{B+R} X_{B+R}$ *and* $\Sigma^{\dagger}_{B+R} \approx_{B+R} X^{\dagger}_{B+R}$ *by Rule V15:Single-Base and*
(2) $\Sigma_{B+R} \cong \Sigma^{\dagger}_{B+R}$ *and* $X_{B+R} \cong X^{\dagger}_{B+R}$ *and*
(3) $\Phi_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \overline{\Phi}'_{B+R}$ *and* $\Phi^{\dagger}_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \overline{\Phi}^{\dagger\dagger}_{B+R}$ *by*
(4) $\Phi_{B+R}\restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_{B+R}\restriction^R$ *and* $\Phi^{\dagger}_{B+R}\restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}^{\dagger\dagger}_{B+R}\restriction^R$

Then

(1) $\Psi_{B+R} \overset{\tau', O_{B+R}}{\rightsquigarrow}_{B+R} \overline{\Psi}'_{B+R}$ *and* $\Psi^{\dagger}_{B+R} \overset{\tau', O_{B+R}}{\rightsquigarrow}_{B+R} \overline{\Psi}^{\dagger\dagger}_{B+R}$ *in combination with Context rule*
(2) $\Psi_{B+R}\restriction^R \overset{\tau, O}{\rightsquigarrow}_R \overline{\Psi}'_{B+R}\restriction^R$ *and* $\Psi^{\dagger}_{B+R}\restriction^R \overset{\tau, O}{\rightsquigarrow}_R \overline{\Psi}^{\dagger\dagger}_{B+R}\restriction^R$
(3) $\Sigma'_{B+R} \cong \Sigma^{\dagger\dagger}_{B+R}$ *and* $X'_{B+R} \cong X^{\dagger\dagger}_{B+R}$ *and*
(4) $\Sigma'_{B+R} \approx_{B+R} X'_{B+R}$ *and* $\Sigma^{\dagger\dagger}_{B+R} \approx_{B+R} X^{\dagger\dagger}_{B+R}$

Proof. By Rule V15:Single-Base and $X_{B+R} \cong X^{\dagger}_{B+R}$ we know that $minWndw(X_{B+R}) > 0$ (similar for $X^{\dagger}_{B+R}$). This means Rule V15-SE-Context applies. We now need to find a step $\Psi_{B+R} \overset{\tau'}{\dashrightarrow}_{B+R} \overline{\Psi}'_{B+R}$ and $\Psi^{\dagger}_{B+R} \overset{\tau'}{\dashrightarrow}_{B+R} \overline{\Psi}^{\dagger\dagger}_{B+R}$. Note that Rule V15-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 137 and Lemma 136 we get $\Sigma_{B+R}\restriction^R \approx_R X_{B+R}\restriction^R$ and $\Sigma_{B+R}\restriction^R \cong \Sigma^{\dagger}_{B+R}\restriction^R$.

Because of $\Phi_{B+R}\restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_{B+R}\restriction^R$ and $\Phi^{\dagger}_{B+R}\restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}^{\dagger\dagger}_{B+R}\restriction^R$ and Rule V15:Single-Base, we fulfill all premises for Lemma 79 (R: Soundness Single Step AM) and derive a step in the oracle semantics:

a) $\Sigma'_{B+R}\restriction^R \cong \Sigma^{\dagger\dagger}_{B+R}\restriction^R$ and $X'_{B+R}\restriction^R \cong X^{\dagger\dagger}_{B+R}\restriction^R$
b) $\Sigma'_{B+R}\restriction^R \approx_R X'_{B+R}\restriction^R$ and $\Sigma^{\dagger\dagger}_{B+R}\restriction^R \approx_R X^{\dagger\dagger}_{B+R}\restriction^R$
c) $\Psi_{B+R}\restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Psi}'_{B+R}\restriction^{R'}$ and $\Psi^{\dagger}_{B+R}\restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Psi}^{\dagger}_{B+R}\restriction^R$ the step of the oracle

Since we have $\Psi_{B+R}\restriction^R \overset{\tau, O}{\rightsquigarrow}_R \overline{\Psi}'_{B+R}\restriction^{R'}$ we can derive a step $\Psi_{B+R} \overset{\tau', O_{B+R}}{\rightsquigarrow}_{B+R} \overline{\Psi}'_{B+R}$ using Rule V15-SE:v5-step (or another applicable rule by Lemma 135 (V15SE: Confluence)).

Let us collect what we already have:

$$X'_{B+R} = X''_{B+R} \cdot \overline{\Psi}'_{B+R}$$
$$\Sigma'_{B+R} = \Sigma''_{B+R} \cdot \overline{\Phi}'_{B+R}$$
$$X^{\dagger\dagger}_{B+R} = X^{*}_{B+R} \cdot \overline{\Psi}^{\dagger\dagger}_{B+R}$$
$$\Sigma^{\dagger\dagger}_{B+R} = \Sigma^{*}_{B+R} \cdot \overline{\Phi}^{\dagger\dagger}_{B+R}$$

We now need to show that $\Sigma'_{B+R} \cong \Sigma^{\dagger\dagger}_{B+R}$ and $X'_{B+R} \cong X^{\dagger\dagger}_{B+R}$ and $\Sigma'_{B+R} \approx_{B+R} X'_{B+R}$ and $\Sigma^{\dagger\dagger}_{B+R} \approx_{B+R} X^{\dagger\dagger}_{B+R}$ hold.

$\Sigma'_{B+R} \cong \Sigma^{\dagger\dagger}_{B+R}$ **and** $X'_{B+R} \cong X^{\dagger\dagger}_{B+R}$ The proof for $\Sigma'_{B+R} \cong \Sigma^{\dagger\dagger}_{B+R}$ and $X'_{B+R} \cong X^{\dagger\dagger}_{B+R}$ is analogous to the corresponding case in Lemma 99 (V45: V4 Soundness Single step).

$\Sigma'_{B+R} \approx_{B+R} X'_{B+R}$ **and** $\Sigma^{\dagger\dagger}_{B+R} \approx_{B+R} X^{\dagger\dagger}_{B+R}$ We want to show that $\Sigma'_{B+R} \approx_{B+R} X'_{B+R}$. The case for $\Sigma^{\dagger\dagger}_{B+R} \approx_{B+R} X^{\dagger\dagger}_{B+R}$ is analogous.

We first check if there is a transaction of V5 that needs to be rolled back in X'_{B+R}, since the speculation window of each instance was reduced.

This has to be done, because we only know that $minWndw(X'_{B+R}) > 0$ *before* we did the step. So it could happen that $minWndw(X'_{B+R}) = 0$ for some transaction of V1 that needs to be rolled back.

Transaction of V1 that needs to be rolled back in X'_{B+R} with window 0 The step made cannot create a new speculative instance of V5 that would be on top. This means we can derive all premises of Rule V15:Single-Transaction-Rollback just from $\Sigma_{B+R} \approx_{B+R} X_{B+R}$. Thus, we have $\Sigma'_{B+R} \approx_{B+R} X'_{B+R}$ by Rule V15:Single-Transaction-Rollback.

No V1 Transaction that needs to be rolled back in X'_{B+R} with window 0 Since the speculation window was reduced for all entries in X'_{B+R} and only for the topmost entry in Σ_{B+R} and we had $INV(\Sigma_{B+R}, X_{B+R})$ from $\Sigma_{B+R} \approx_{B+R} X_{B+R}$, we have $INV(\Sigma'_{B+R}, X'_{B+R})$ again. This reasoning extends to newly created instances by speculation as well.

We do a case distinction on $\approx_R$:

Rule Single-Base Analogous to the corresponding cases in Lemma 99 (V45: V4 Soundness Single step).

Rule Single-OracleTrue Then, the oracle predicted correctly. Analogous to the corresponding cases in Lemma 99 (V45: V4 Soundness Single step). Rule V15:Single-OracleTrue and have $\Sigma'_{B+R} \approx_{B+R} X'_{B+R}$.

Rule Single-Transaction-Rollback Then one of the instances in $X'_{B+R}\restriction^{R}$ needs to be rolled back.

This means the same instance in X'_{B+R} needs to be rolled back as well.

We do a case distinction if the instance is part of $\overline{\Psi}'_{B+R}$ or not. These cases are analogous to the corresponding cases in Lemma 99 (V45: V4 Soundness Single step).

□

Lemma 144 (V15: V1 Soundness Single step). *If*

(1) $\Sigma_{B+R} \approx_{B+R} X_{B+R}$ *and* $\Sigma^{\dagger}_{B+R} \approx_{B+R} X^{\dagger}_{B+R}$ *by Rule V15:Single-Base and*
(2) $\Sigma_{B+R} \cong \Sigma^{\dagger}_{B+R}$ *and* $X_{B+R} \cong X^{\dagger}_{B+R}$ *and*
(3) $\Phi_{B+R} \xrightarrow{\tau}_{B+R} \overline{\Phi}'_{B+R}$ *and* $\Phi^{\dagger}_{B+R} \xrightarrow{\tau}_{B+R} \overline{\Phi}^{\dagger\dagger}_{B+R}$ *by*
(4) $\Phi_{B+R}\restriction^{B} \xrightarrow{\tau}_{B} \overline{\Phi}'_{B+R}\restriction^{B}$ *and* $\Phi^{\dagger}_{B+R}\restriction^{B} \xrightarrow{\tau}_{B} \overline{\Phi}^{\dagger\dagger}_{B+R}\restriction^{B}$

Then

(1) $\Psi_{B+R} \xrightarrow{\tau', O_{B+R}}_{B+R} \overline{\Psi}'_{B+R}$ *and* $\Psi^{\dagger}_{B+R} \xrightarrow{\tau', O_{B+R}}_{B+R} \overline{\Psi}^{\dagger\dagger}_{B+R}$ *in combination with Context rule*
(2) $\Psi_{B+R}\restriction^{B} \xrightarrow{\tau, O}_{B} \overline{\Psi}'_{B+R}\restriction^{B}$ *and* $\Psi^{\dagger}_{B+R}\restriction^{B} \xrightarrow{\tau, O}_{B} \overline{\Psi}^{\dagger\dagger}_{B+R}\restriction^{B}$
(3) $\Sigma'_{B+R} \cong \Sigma^{\dagger\dagger}_{B+R}$ *and* $X'_{B+R} \cong X^{\dagger\dagger}_{B+R}$ *and*
(4) $\Sigma'_{B+R} \approx_{B+R} X'_{B+R}$ *and* $\Sigma^{\dagger\dagger}_{B+R} \approx_{B+R} X^{\dagger\dagger}_{B+R}$

Proof. The proof is very similar to Lemma 143 (V15: V5 Soundness Single step). We only discuss the key aspects.

By Rule V15:Single-Base and $X_{B+R} \cong X^{\dagger}_{B+R}$ we know that $minWndw(X_{B+R}) > 0$ (similar for $X^{\dagger}_{B+R}$). This means Rule V15-SE-Context applies. We now need to find a step $\Psi_{B+R} \xrightarrow{\tau'}_{B+R} \overline{\Psi}'_{B+R}$ and $\Psi^{\dagger}_{B+R} \xrightarrow{\tau'}_{B+R} \overline{\Psi}^{\dagger\dagger}_{B+R}$. Note that Rule V15-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 137 and Lemma 136 we get $\Sigma_{B+R}\restriction^{B} \approx_{B} X_{B+R}\restriction^{B}$ and $\Sigma_{B+R}\restriction^{B} \cong \Sigma^{\dagger}_{B+R}\restriction^{B}$.

Combined with Rule V15:Single-Base, we fulfill all premises for Lemma 52 (B: Soundness Single Step AM) and derive a step in the oracle semantics:

a) $\Sigma'_{B+R}\restriction^{B} \cong \Sigma^{\dagger\dagger}_{B+R}\restriction^{B}$ and $X'_{B+R}\restriction^{B} \cong X^{\dagger\dagger}_{B+R}\restriction^{B}$
b) $\Sigma'_{B+R}\restriction^{B} \approx_{B} X'_{B+R}\restriction^{B}$ and $\Sigma^{\dagger\dagger}_{B+R}\restriction^{B} \approx_{B} X^{\dagger\dagger}_{B+R}\restriction^{B}$

c) $\Psi_{B+R}\restriction^B \xrightarrow{\tau}_B \overline{\Psi}'_{B+R}\restriction^{B'}$ and $\Psi^{\dagger}_{B+R}\restriction^B \xrightarrow{\tau}_B \overline{\Psi}^{\dagger}_{B+R}\restriction^B$ the step of the oracle

Since we have $\Psi_{B+R}\restriction^R \xrightarrow{\tau}_R \overline{\Psi}'_{B+R}\restriction^{R'}$ we can derive a step $\Psi_{B+R} \xrightarrow{\tau'}_{B+R} \overline{\Psi}'_{B+R}$ using Rule V15-SE:v1-step (or another applicable rule by Lemma 135 (V15SE: Confluence)).

Let us collect what we already have:

$$\begin{aligned} X'_{B+R} &= X''_{B+R} \cdot \overline{\Psi}'_{B+R} \\ \Sigma'_{B+R} &= \Sigma''_{B+R} \cdot \overline{\Phi}'_{B+R} \\ X^{\dagger\dagger}_{B+R} &= X^{*}_{B+R} \cdot \overline{\Psi}^{\dagger\dagger}_{B+R} \\ \Sigma^{\dagger\dagger}_{B+R} &= \Sigma^{*}_{B+R} \cdot \overline{\Phi}^{\dagger\dagger}_{B+R} \end{aligned}$$

We now need to show that $\Sigma'_{B+R} \cong \Sigma^{\dagger\dagger}_{B+R}$ and $X'_{B+R} \cong X^{\dagger\dagger}_{B+R}$ and $\Sigma'_{B+R} \approx_{B+R} X'_{B+R}$ and $\Sigma^{\dagger\dagger}_{B+R} \approx_{B+R} X^{\dagger\dagger}_{B+R}$ hold.

$\Sigma'_{B+R} \cong \Sigma^{\dagger\dagger}_{B+R}$ **and** $X'_{B+R} \cong X^{\dagger\dagger}_{B+R}$ The proof for $\Sigma'_{B+R} \cong \Sigma^{\dagger\dagger}_{B+R}$ and $X'_{B+R} \cong X^{\dagger\dagger}_{B+R}$ is analogous to the corresponding case in Lemma 99 (V45: V4 Soundness Single step).

$\Sigma'_{B+R} \approx_{B+R} X'_{B+R}$ **and** $\Sigma^{\dagger\dagger}_{B+R} \approx_{B+R} X^{\dagger\dagger}_{B+R}$ We first check if there is a transaction of V4 that needs to be rolled back in X'_{B+R}, since the speculation window of each instance was reduced.

This has to be done, because we only know that $minWndw(X'_{B+R}) > 0$ *before* we did the step. So it could happen that $minWndw(X'_{B+R}) = 0$ for some transaction of V4 that needs to be rolled back.

Transaction of V4 that needs to be rolled back in X'_{B+R} with window 0 The step made cannot create a new speculative instance of V4. This means we can derive all premises of Rule V15:Single-Transaction-Rollback just from $\Sigma_{B+R} \approx_{B+R} X_{B+R}$. Thus, we have $\Sigma'_{B+R} \approx_{B+R} X'_{B+R}$ by Rule V15:Single-Transaction-Rollback.

No V4 Transaction that needs to be rolled back in X'_{B+R} with window 0 Since the speculation window was reduced for all entries in X'_{B+R} and only for the topmost entry in Σ_{B+R} and we had $INV(\Sigma_{B+R}, X_{B+R})$ from $\Sigma_{B+R} \approx_{B+R} X_{B+R}$, we have $INV(\Sigma'_{B+R}, X'_{B+R})$ again. This reasoning extends to newly created instances by speculation as well.

We do a case distinction on $\approx_B$:

Rule V1:Single-Base Analogous to the corresponding case in Lemma 143 (V15: V5 Soundness Single step).

Rule V1:Single-OracleTrue Analogous to the corresponding case in Lemma 143 (V15: V5 Soundness Single step).

Rule V1:Single-Transaction-Rollback Then one of the instances in $X'_{B+R}\restriction^B$ needs to be rolled back.

This means the same instance in X'_{B+R} needs to be rolled back as well.

We do a case distinction if the instance is part of $\overline{\Psi}'_{B+R}$ or not.

These cases are analogous to the corresponding cases in Lemma 99 (V45: V4 Soundness Single step).

□

M.5 Completeness

Definition 71 (V15: Relation between AM and Spec for oracles that only mispredict). $\boxed{\Sigma_{B+R} \approx^{O_{am}}_{B+R} X_{B+R}}$

$$\frac{}{\varnothing \approx^{O_{am}}_{B+R} \varnothing}\ \textit{(V15:Base-Oracle)} \qquad \frac{\Sigma_{B+R} \sim X_{B+R}\restriction_{com} \quad INV2(\Sigma_{B+R}, X_{B+R}) \quad minWndw(X_{B+R}) > 0}{\Sigma_{B+R} \approx^{O_{am}}_{B+R} X_{B+R}}\ \textit{(V15:Single-Base-Oracle)}$$

$$\frac{\begin{array}{ccc} \Sigma''_{B+R} \sim X''_{B+R}\restriction_{com} & n' \geq 0 & \Sigma''_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma'''_{B+R} \textit{ where transaction with id ctr is rolled back} \quad x = (S, true) \vee (B, m) \\ X_{B+R} = X'_{B+R} \cdot \langle p, ctr, \sigma, h, n'' \rangle & \Sigma_{B+R} = \Sigma'_{B+R} \cdot \langle p, ctr, \sigma, n \rangle & INV2(\Sigma_{B+R}, X_{B+R}) \end{array}}{\Sigma'_{B+R} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle^x \cdot \Sigma_{S1} \approx^{O_{am}}_{B+R} X'_{B+R} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0 \rangle^x}\ \textit{(V15:Single-Transaction-Rollback-Oracle)}$$

Lemma 145 (V15: Coincide on $\approx^{O_{am}}_{B+R}$ for projections). *If*

(1) $\Sigma_{B+R} \approx^{O_{am}}_{B+R} X_{B+R}$ *by Rule V15:Single-Base*

Then

(1) $\Sigma_{B+R}\restriction^R \approx^{O_{am}}_{R} X_{B+R}\restriction^R$ *by Rule Single-Base-Oracle and*

(2) $\Sigma_{B+R}\restriction^B \approx^{O_{am}}_{B} X_{B+R}\restriction^B$ *by Rule Single-Base-Oracle*

Proof. The proof is analogous to Lemma 101 (V45: Coincide on $\approx^{O_{am}}_{S+R}$ for projections). □

Definition 72 (V15: Constructing the AM Oracle). *We rely for the construction of the oracle O_{am}^{B+R} on the construction of its parts. Here Definition 58 (Constructing the AM Oracle) and Definition 62 (R: Constructing the Oracle).*

Thus, we have: $O_{am}^{B+R} = (O_{amB}, O_{amR})$ for the speculative oracle combined semantics.

Lemma 146 (V15: Completeness Am semantics w.r.t. speculative semantics). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, σ, $\sigma' \in InitConf$ be two initial configurations. If*

(1) $(p,\sigma) \Uparrow^{\omega}_{B+R} \overline{\tau}$ and $(p,\sigma') \Uparrow^{\omega}_{B+R} \overline{\tau}'$ and

(2) $\overline{\tau} \neq \overline{\tau}'$

Then there exists an oracle O such that

I $(p,\sigma) \Uparrow^{O}_{B+R} \overline{\tau}_1$ and $(p,\sigma') \Uparrow^{O}_{B+R} \overline{\tau}'_1$ and

II $\overline{\tau}_1 \neq \overline{\tau}'_1$

Proof. Let $\omega \in \mathbb{N}$ be a speculative window, $\sigma, \sigma' \in InitConf$ be two initial configurations. If

(1) $(p,\sigma) \Uparrow^{\omega}_{B+R} \overline{\tau}$ and $(p,\sigma') \Uparrow^{\omega}_{B+R} \overline{\tau}'$ and

(2) $\overline{\tau} \neq \overline{\tau}'$

By definition of $\Uparrow^{\omega}_{B+R}$ we have two final states Σ_{B+RF} and Σ'_{B+RF} such that $\Sigma^{init}_{B+R}(p,\sigma) \Downarrow^{\overline{\tau}}_{B+R} \Sigma_{B+RF}$ $\Sigma^{init}_{S} p,\sigma' \Downarrow^{\overline{\tau}'}_{B+R} \Sigma'_{B+RF}$. Combined with the fact that $\overline{\tau} \neq \overline{\tau}'$, it follows that there are speculative states $\Sigma^{*}_{B+R}, \Sigma^{**}_{B+R}, \Sigma^{\dagger}_{B+R}, \Sigma^{\dagger\dagger}_{B+R}$ and sequences of observations $\overline{\tau}, \overline{\tau}_{end}, \overline{\tau}'_{end}, \tau_{am}, \tau'_{am}$ such that $\tau_{am} \neq \tau'_{am}$, $\Sigma^{*}_{B+R} \cong \Sigma^{\dagger}_{B+R}$ and:

$$\Sigma^{init}_{B+R}(p,\sigma) \Downarrow^{\overline{\tau}}_{B+R} \Sigma^{*}_{B+R} \xrightarrow{\tau_{am}}_{B+R} \Sigma^{**}_{B+R} \Downarrow^{\overline{\tau}_{end}}_{B+R} \Sigma_{B+RF}$$

$$\Sigma^{init}_{B+R}(p,\sigma') \Downarrow^{\overline{\tau}}_{B+R} \Sigma^{\dagger}_{B+R} \xrightarrow{\tau'_{am}}_{B+R} \Sigma^{\dagger\dagger}_{B+R} \Downarrow^{\overline{\tau}'_{end}}_{B+R} \Sigma'_{B+RF}$$

We claim that there is a prediction oracle O with speculative window at most ω such that

a) $X^{init}_{B+R}(p,\sigma) \overset{O_{B+R}}{\wr}{}^{B+R}_{v} X^{*}_{B+R}$ and $X^{*}_{B+R}.\sigma = \Sigma^{*}_{B+R}.\sigma$ and $INV2(X^{*}_{B+R}, \Sigma^{*}_{B+R})$ and

b) $X^{init}_{B+R}(p,\sigma') \overset{O_{B+R}}{\wr}{}^{B+R}_{v} X^{\dagger}_{B+R}$ and $X^{\dagger}_{B+R}.\sigma = \Sigma^{\dagger}_{B+R}.\sigma$ and $INV2(X^{\dagger}_{B+R}, \Sigma^{\dagger}_{B+R})$

c) $X^{*}_{B+R} \cong X^{\dagger}_{B+R}$

We achieve this by applying Lemma 147 (V15: Stronger Soundness for a specific oracle and for specific executions) on the AM execution up to the point of the difference i.e., $\Sigma^{init}_{B+R}(p,\sigma) \Downarrow^{\overline{\tau}}_{B+R} \Sigma^{*}_{B+R}$ and $\Sigma^{init}_{B+R}(p,\sigma') \Downarrow^{\overline{\tau}}_{B+R} \Sigma^{\dagger}_{B+R}$.

The argument why $\Sigma^{*}_{B+R} \approx^{O_{am}}_{B+R} X^{*}_{B+R}$ is derived by Rule V15:Single-Base-Oracle is analogous to Lemma 102 (V45: Completeness Am semantics w.r.t. speculative semantics).

We proceed by case analysis on the rule in $\xrightarrow{}_{B+R}$ used to derive $\Sigma^{*}_{B+R} \xrightarrow{\tau_{am}}_{B+R} \Sigma^{**}_{B+R}$. Because $\Sigma^{*}_{B+R} \cong \Sigma^{\dagger}_{B+R}$ and $\overline{\tau}_1 = \overline{\tau}'_1$, we know that the same rule was used in $\Sigma^{\dagger}_{B+R} \xrightarrow{\tau'_{am}}_{R} \Sigma^{\dagger\dagger}_{B+R}$ as well.

Rule AM-v5-Rollback-V15 Contradiction. Because $\Sigma^{*}_{B+R} \cong \Sigma^{\dagger}_{B+R}$ we have for all instances $\Phi_1.ctr = \Phi'_1.ctr$.
Since the same instance would be rolled back, we have $\tau_{am} = \tau'_{am}$.

Rule AM-v1-Rollback-V15 Analogous to the case above.

Rule AM-Context-V15 By inversion on Rule AM-Context-V15 for the step $\Sigma^{*}_{B+R} \xrightarrow{\tau_{am}}_{B+R} \Sigma^{**}_{B+R}$ we have $\Sigma^{*}_{B+R} = \overline{\Phi}_{B+R} \cdot \Phi_{B+R}$ and $\Sigma^{**}_{B+R} = \overline{\Phi}_{B+R} \cdot \overline{\Phi}'_{B+R}$ with $\Phi_{B+R} \xrightarrow{\tau_{am}}_{B+R} \overline{\Phi}'_{B+R}$.

We now do inversion on $\Phi_{B+R} \xrightarrow{\tau_{am}}_{B+R} \overline{\Phi}'_{B+R}$:

Rule AM-v5-step-V15 Then we have $\Phi_{B+R}\restriction^{R} \xrightarrow{\tau}_{R} \overline{\Phi}'_{S}\restriction^{R}$.
The case is analogous to Lemma 80 (R: Completeness AM semantics w.r.t. speculative semantics) in the Rule R:AM-Context case.

Rule AM-v1-step-V15 Then we have $\Phi_{B+R}\restriction^{B} \xrightarrow{\tau}_{B} \overline{\Phi}'_{B+R}\restriction^{B}$.
The case is analogous to Lemma 54 (B: Completeness Am semantics w.r.t. speculative semantics) in the Rule B:AM-Context case.

This completes the proof of our claim.

□

Lemma 147 (V15: Stronger Soundness for a specific oracle and for specific executions). *Specific executions means that there is a difference in the trace but before there is none. We use the oracle O_{am} as it is defined by Definition 72 (V15: Constructing the AM Oracle) for the given execution. If*

(1) $\Sigma_{B+R} \cong \Sigma^{\dagger}_{B+R}$

(2) $X_{B+R} \cong X^{\dagger}_{B+R}$ and $\overline{\rho} = \emptyset$

(3) $\Sigma_{B+R} \approx^{O_{am}} X_{B+R}$ *and* $\Sigma^{\dagger}_{B+R} \approx^{O_{am}} X^{\dagger}_{B+R}$
(4) $\Sigma_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma'_{B+R}$ *and* $\Sigma^{\dagger}_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma^{\dagger\dagger}_{B+R}$

and our oracle is constructed in the way described above Then

I X_{B+R} $^{O_{B+R}}\!\!\wr^{B+R}_{\overline{\tau}'} X'_{B+R}, X^{\dagger}_{B+R}$ $^{O}\!\!\wr^{R}_{\overline{\tau}''} X^{\dagger\dagger}_{B+R}$
II $\Sigma'_{B+R} \cong \Sigma^{\dagger\dagger}_{B+R}$
III $X'_{B+R} \cong X^{\dagger\dagger}_{B+R}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{B+R} \approx^{O_{am}} X'_{B+R}$ *and* $\Sigma^{\dagger\dagger}_{B+R} \approx^{O_{am}} X^{\dagger\dagger}_{B+R}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. Notice that the proof is very similar to Lemma 98 (V45: Soundness Am semantics w.r.t. speculative semantics with new relation between states). The only thing that is different is that (1) the specific oracle only mispredicts so there is one less case in the relation and (2) we have a different invariant for that specific oracle i.e., $INV2(\Sigma_{B+R}, X_{B+R})$

For these reasons we will only argue why $INV2(\Sigma^{\dagger}_{B+R}, X'_{B+R})$ holds in the different cases and leave the rest to the old soundness proof.

By Induction on $\Sigma_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma'_{B+R}$ and $\Sigma^{\dagger}_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma^{\dagger\dagger}_{B+R}$.

Rule AM-Reflection-V15 We have $\Sigma_{B+R} \Downarrow^{\varepsilon}_{B+R} \Sigma'_{B+R}$ and $\Sigma^{\dagger}_{B+R} \Downarrow^{\varepsilon}_{B+R} \Sigma''_{B+R}$, where $\Sigma'_{B+R} = \Sigma_{B+R}$ and $\Sigma''_{B+R} = \Sigma^{\dagger}_{B+R}$. We choose $\Sigma'_{B+R} = \Sigma'_{B+R}$ and $\Sigma^{\dagger\dagger}_{B+R} = \Sigma''_{B+R}$.

We further use Rule V15-SE:Reflection to derive X_{B+R} $^{O_{B+R}}\!\!\wr^{B+R}_{\varepsilon} X'_{B+R}, X^{\dagger}_{B+R}$ $^{O_{B+R}}\!\!\wr^{B+R}_{\varepsilon} X^{\dagger\dagger}_{B+R}$ with $X'_{B+R} = X_{B+R}$ and $X^{\dagger\dagger}_{B+R} = X^{\dagger}_{B+R}$. We now trivially satisfy all conclusions.

Rule AM-Single-V15 We have $\Sigma_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma''_{B+R}$ with $\Sigma''_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \Sigma'_{B+R}$ and $\Sigma^{\dagger}_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma^{*}_{B+R}$ and $\Sigma^{*}_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \Sigma^{\dagger\dagger}_{B+R}$.

We now apply IH on $\Sigma_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma''_{B+R}$ and $\Sigma^{\dagger}_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma^{*}_{B+R}$ and get

(a) X_{B+R} $^{O_{B+R}}\!\!\wr^{B+R}_{\overline{\tau}'} X''_{B+R}, X^{\dagger}_{B+R}$ $^{O_{B+R}}\!\!\wr^{B+R}_{\overline{\tau}''} X^{*}_{B+R}$
(b) $\Sigma''_{B+R} \cong \Sigma^{*}_{B+R}$
(c) $X''_{B+R} \cong X^{*}_{B+R}$ and $\overline{\rho}' = \varnothing$
(d) $\Sigma''_{B+R} \approx^{O_{am}}_{B+R} X''_{B+R}$ and $\Sigma^{*}_{B+R} \approx^{O_{am}}_{B+R} X^{*}_{B+R}$
(e) $\overline{\tau}' = \overline{\tau}''$

We do a case distinction on $\approx^{O_{am}}_{B+R}$ in $\Sigma''_{B+R} \approx^{O_{am}}_{B+R} X''_{B+R}$ and $\Sigma^{*}_{B+R} \approx^{O_{am}} X^{*}_{B+R}$:

Rule V15:Single-Base-Oracle We thus have $\Sigma''_{B+R} \sim X''_{B+R}\restriction_{com}$, $minWndw(X''_{B+R}) > 0$ and $INV2(\Sigma''_{B+R}, X''_{B+R})$ (Similar for Σ^{*}_{B+R} and X^{*}_{B+R}).

We now proceed by inversion on the derivation $\Sigma''_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \Sigma'_{B+R}$:

Rule AM-v5-Rollback-V15 Contradiction, since $minWndw(X''_{S}) > 0$ and $INV2(\Sigma''_{B+R}, X''_{B+R})$.

Rule AM-v5-Rollback-V15 Analogous to above.

Rule AM-Context-V15 We have $\Phi_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \overline{\Phi}'_{B+R}$ and $n > 0$.

We now use inversion on $\Phi_{B+R} \overset{\tau}{\dashrightarrow}_{B+R} \overline{\Phi}_{B+R}$:

Rule AM-v5-step-V15 Then, we have $\Phi_{B+R}\restriction^{R} \overset{\tau}{\dashrightarrow}_{R} \overline{\Phi}'_{B+R}\restriction^{R}$
We use Lemma 143 (V15: V5 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule AM-v1-step-V15 Then, we have $\Phi_{B+R}\restriction^{B} \overset{\tau}{\dashrightarrow}_{B} \overline{\Phi}'_{B+R}\restriction^{B}$
We use Lemma 144 (V15: V1 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule V15:Single-Transaction-Rollback-Oracle We have

$$
\begin{aligned}
X''_{B+R} =& X_{B+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0 \rangle^{x} \cdot X_{B+R4} \\
\Sigma''_{B+R} =& \Sigma_{B+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle^{x} \cdot \Sigma_{B+R4} \\
X_{B+R} =& X_{B+R3} \cdot \langle p, ctr, \sigma, h, \mathbb{R}, n'' \rangle \\
\Sigma_{B+R} =& \Sigma_{B+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \\
\Sigma_{B+R} \sim& X_{B+R}\restriction_{com} \\
INV2(\Sigma_{B+R}, X_{B+R}) & \\
n' \geq& 0
\end{aligned}
$$

The form of X^{*}_{B+R} and Σ^{*}_{B+R} is analogous.

Additionally we know that the transaction terminates in some state $\Sigma_{B+R} \Downarrow^{\overline{\tau}}_{B+R} \Sigma'''_{B+R}$. There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma''_{B+R} \xrightarrow{\tau}_{B+R} \Sigma'_{B+R}$ is not a roll back. Because Σ_{B+R} and X_{B+R} do not change, $INV2(\Sigma_{B+R}, X_{B+R})$ does not change as well.

$n' = 0$ Then we know that $\Sigma''_{B+R} \xrightarrow{\tau}_{B+R} \Sigma'_{B+R}$ was created by Rule AM-v5-Rollback-V15 or Rule AM-v1-Rollback-V15 and is a rollback for *ctr*.
Notice, that the only difference to X_{B+R} and Σ_{B+R} is the updated *ctr*, because of the roll back. Updating the counter does not change the invariant $INV2()$. This means $INV2(\Sigma_{B+R}, X_{B+R})$ (with updated *ctr*) still holds.

□

Lemma 148 (V15: Stronger V5 Soundness Single step)**.** *If*

(1) $\Sigma_{B+R} \approx^{O_{am}}_{B+R} X_{B+R}$ *and* $\Sigma^{\dagger}_{B+R} \approx^{O_{am}}_{B+R} X^{\dagger}_{B+R}$ *by Rule V15:Single-Base-Oracle and*
(2) $\Sigma_{B+R} \cong \Sigma^{\dagger}_{B+R}$ *and* $X_{B+R} \cong X^{\dagger}_{B+R}$ *and*
(3) $\Phi_{B+R} \xrightarrow{\tau}_{B+R} \overline{\Phi}'_{B+R}$ *and* $\Phi^{\dagger}_{B+R} \xrightarrow{\tau}_{B+R} \overline{\Phi}^{\dagger\dagger}_{B+R}$ *by*
(4) $\Phi_{B+R}\restriction^{R} \xrightarrow{\tau}_{R} \overline{\Phi}'_{B+R}\restriction^{R}$ *and* $\Phi^{\dagger}_{B+R}\restriction^{R} \xrightarrow{\tau}_{R} \overline{\Phi}^{\dagger\dagger}_{B+R}\restriction^{R}$

Then

(1) $\Psi_{B+R} \xrightarrow{\tau', O_{B+R}}_{B+R} \overline{\Psi}'_{B+R}$ *and* $\Psi^{\dagger}_{B+R} \xrightarrow{\tau', O_{B+R}}_{B+R} \overline{\Psi}^{\dagger\dagger}_{B+R}$ *in combination with Context rule*
(2) $\Psi_{B+R} \xrightarrow{\tau, O_{B+R}}_{B+R} \overline{\Psi}'_{B+R}$ *and* $\Psi^{\dagger}_{B+R} \xrightarrow{\tau, O_{B+R}}_{B+R} \overline{\Psi}^{\dagger\dagger}_{B+R}$
(3) $\Sigma'_{B+R} \cong \Sigma^{\dagger\dagger}_{B+R}$ *and* $X'_{B+R} \cong X^{\dagger\dagger}_{B+R}$ *and*
(4) $\Sigma'_{B+R} \approx^{O_{am}}_{B+R} X'_{B+R}$ *and* $\Sigma^{\dagger\dagger}_{B+R} \approx^{O_{am}}_{B+R} X^{\dagger\dagger}_{B+R}$

Proof. By Rule V15:Single-Base-Oracle and $X_{B+R} \cong X^{\dagger}_{B+R}$ we know that $minWndw(X_{B+R}) > 0$ (similar for $X^{\dagger}_{B+R}$). This means Rule V15-SE-Context applies. We now need to find a step $\Psi_{B+R} \xrightarrow{\tau'}_{B+R} \overline{\Psi}'_{B+R}$ and $\Psi^{\dagger}_{B+R} \xrightarrow{\tau'}_{B+R} \overline{\Psi}^{\dagger\dagger}_{B+R}$. Note that Rule V15-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 137 and Lemma 145 we get $\Sigma_{B+R}\restriction^{R} \approx_{R} X_{B+R}\restriction^{R}$ and $\Sigma_{B+R}\restriction^{R} \cong \Sigma^{\dagger}_{B+R}\restriction^{R}$.

Because of $\Phi_{B+R}\restriction^{R} \xrightarrow{\tau}_{R} \overline{\Phi}'_{B+R}\restriction^{R}$ and $\Phi^{\dagger}_{B+R}\restriction^{R} \xrightarrow{\tau}_{R} \overline{\Phi}^{\dagger\dagger}_{B+R}\restriction^{R}$ and Rule V15:Single-Base-Oracle, we fulfill all premises for Lemma 81 (Stronger Soundness for a specific oracle and for specific executions) and derive a step in the oracle semantics:

a) $\Sigma'_{B+R}\restriction^{R} \cong \Sigma^{\dagger\dagger}_{B+R}\restriction^{R}$ and $X'_{B+R}\restriction^{R} \cong X^{\dagger\dagger}_{B+R}\restriction^{R}$
b) $\Sigma'_{B+R}\restriction^{R} \approx^{O_{am}}_{R} X'_{B+R}\restriction^{R}$ and $\Sigma^{\dagger\dagger}_{B+R}\restriction^{R} \approx^{O_{am}}_{R} X^{\dagger\dagger}_{B+R}\restriction^{R}$
c) $\Psi_{B+R}\restriction^{R} \xrightarrow{\tau}_{R} \overline{\Psi}'_{B+R}\restriction^{R'}$ and $\Psi^{\dagger}_{B+R}\restriction^{R} \xrightarrow{\tau}_{R} \overline{\Psi}^{\dagger}_{B+R}\restriction^{R}$ the step of the oracle

Since we have $\Psi_{B+R}\restriction^{R} \xrightarrow{\tau}_{R} \overline{\Psi}'_{B+R}\restriction^{R'}$ we can derive a step $\Psi_{B+R} \xrightarrow{\tau'}_{B+R} \overline{\Psi}'_{B+R}$ using Rule V15-SE:v5-step (or another applicable rule by Lemma 135 (V15SE: Confluence)).

Let us collect what we already have:

$$X'_{B+R} = X''_{B+R} \cdot \overline{\Psi}'_{B+R}$$
$$\Sigma'_{B+R} = \Sigma''_{B+R} \cdot \overline{\Phi}'_{B+R}$$
$$X^{\dagger\dagger}_{B+R} = X^{*}_{B+R} \cdot \overline{\Psi}^{\dagger\dagger}_{B+R}$$
$$\Sigma^{\dagger\dagger}_{B+R} = \Sigma^{*}_{B+R} \cdot \overline{\Phi}^{\dagger\dagger}_{B+R}$$

We now need to show that $\Sigma'_{B+R} \cong \Sigma^{\dagger\dagger}_{B+R}$ and $X'_{B+R} \cong X^{\dagger\dagger}_{B+R}$ and $\Sigma'_{B+R} \approx^{O_{am}}_{B+R} X'_{B+R}$ and $\Sigma^{\dagger\dagger}_{B+R} \approx^{O_{am}}_{B+R} X^{\dagger\dagger}_{B+R}$ hold.

The rest of the proof is analogous to Lemma 104 (V45: Stronger V4 Soundness Single step).

□

Lemma 149 (V15: Stronger V1 Soundness Single step)**.** *If*

(1) $\Sigma_{B+R} \approx^{O_{am}}_{B+R} X_{B+R}$ *and* $\Sigma^{\dagger}_{B+R} \approx^{O_{am}}_{B+R} X^{\dagger}_{B+R}$ *by Rule V15:Single-Base-Oracle and*
(2) $\Sigma_{B+R} \cong \Sigma^{\dagger}_{B+R}$ *and* $X_{B+R} \cong X^{\dagger}_{B+R}$ *and*
(3) $\Phi_{B+R} \xrightarrow{\tau}_{B+R} \overline{\Phi}'_{B+R}$ *and* $\Phi^{\dagger}_{B+R} \xrightarrow{\tau}_{B+R} \overline{\Phi}^{\dagger\dagger}_{B+R}$ *by*
(4) $\Phi_{B+R}\restriction^{B} \xrightarrow{\tau}_{B} \overline{\Phi}'_{B+R}\restriction^{B}$ *and* $\Phi^{\dagger}_{B+R}\restriction^{B} \xrightarrow{\tau}_{B} \overline{\Phi}^{\dagger\dagger}_{B+R}\restriction^{B}$

Then

(1) $\Psi_{B+R} \xrightarrow{\tau', O_{B+R}}_{B+R} \overline{\Psi}'_{B+R}$ *and* $\Psi^{\dagger}_{B+R} \xrightarrow{\tau', O_{B+R}}_{B+R} \overline{\Psi}^{\dagger\dagger}_{B+R}$ *in combination with Context rule*

(2) $\Psi_{B+R} \overset{\tau}{\rightsquigarrow}{}^{O_{B+R}}_{B+R} \overline{\Psi}'_{B+R}$ *and* $\Psi^{\dagger}_{B+R} \overset{\tau}{\rightsquigarrow}{}^{O_{B+R}}_{B+R} \overline{\Psi}^{\dagger\dagger}_{B+R}$
(3) $\Sigma'_{B+R} \cong \Sigma^{\dagger\dagger}_{B+R}$ *and* $X'_{B+R} \cong X^{\dagger\dagger}_{B+R}$ *and*
(4) $\Sigma'_{B+R} \approx^{O_{am}}_{B+R} X'_{B+R}$ *and* $\Sigma^{\dagger\dagger}_{B+R} \approx^{O_{am}}_{B+R} X^{\dagger\dagger}_{B+R}$

Proof. By Rule V15:Single-Base-Oracle and $X_{B+R} \cong X^{\dagger}_{B+R}$ we know that $minWndw(X_{B+R}) > 0$ (similar for $X^{\dagger}_{B+R}$). This means Rule V15-SE-Context applies. We now need to find a step $\Psi_{B+R} \overset{\tau'}{\dashrightarrow}_{B+R} \overline{\Psi}'_{B+R}$ and $\Psi^{\dagger}_{B+R} \overset{\tau'}{\dashrightarrow}_{B+R} \overline{\Psi}^{\dagger\dagger}_{B+R}$. Note that Rule V15-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 137 (V15: Coincide on $\cong$ for projections) and Lemma 145 (V15: Coincide on $\approx^{O_{am}}_{B+R}$ for projections) we get $\Sigma_{B+R}\restriction^{R} \approx^{O_{am}}_{R} X_{B+R}\restriction^{R}$ and $\Sigma_{B+R}\restriction^{R} \cong \Sigma^{\dagger}_{B+R}\restriction^{R}$.

Because of $\Phi_{B+R}\restriction^{B} \overset{\tau}{\dashrightarrow}_{B} \overline{\Phi}'_{B+R}\restriction^{B}$ and $\Phi^{\dagger}_{B+R}\restriction^{B} \overset{\tau}{\dashrightarrow}_{B} \overline{\Phi}^{\dagger\dagger}_{B+R}\restriction^{B}$ and Rule V15:Single-Base-Oracle, we fulfill all premises for Lemma 53 (B: Stronger Soundness for a specific oracle and for specific executions) and derive a step in the oracle semantics:

a) $\Sigma'_{B+R}\restriction^{B} \cong \Sigma^{\dagger\dagger}_{B+R}\restriction^{B}$ and $X'_{B+R}\restriction^{B} \cong X^{\dagger\dagger}_{B+R}\restriction^{B}$
b) $\Sigma'_{B+R}\restriction^{B} \approx^{O_{am}}_{B} X'_{B+R}\restriction^{B}$ and $\Sigma^{\dagger\dagger}_{B+R}\restriction^{B} \approx^{O_{am}}_{B} X^{\dagger\dagger}_{B+R}\restriction^{B}$
c) $\Psi_{B+R}\restriction^{B} \overset{\tau}{\dashrightarrow}_{B} \overline{\Psi}'_{B+R}\restriction^{B'}$ and $\Psi^{\dagger}_{B+R}\restriction^{B} \overset{\tau}{\dashrightarrow}_{B} \overline{\Psi}^{\dagger}_{B+R}\restriction^{B}$ the step of the oracle

Since we have $\Psi_{B+R}\restriction^{B} \overset{\tau}{\dashrightarrow}_{B} \overline{\Psi}'_{B+R}\restriction^{B'}$ we can derive a step $\Psi_{B+R} \overset{\tau'}{\dashrightarrow}_{B+R} \overline{\Psi}'_{B+R}$ using Rule V15-SE:v5-step (or another applicable rule by Lemma 135 (V15SE: Confluence)).

Let us collect what we already have:

$$X'_{B+R} = X''_{B+R} \cdot \overline{\Psi}'_{B+R}$$
$$\Sigma'_{B+R} = \Sigma''_{B+R} \cdot \overline{\Phi}'_{B+R}$$
$$X^{\dagger\dagger}_{B+R} = X^{*}_{B+R} \cdot \overline{\Psi}^{\dagger\dagger}_{B+R}$$
$$\Sigma^{\dagger\dagger}_{B+R} = \Sigma^{*}_{B+R} \cdot \overline{\Phi}^{\dagger\dagger}_{B+R}$$

We now need to show that $\Sigma'_{B+R} \cong \Sigma^{\dagger\dagger}_{B+R}$ and $X'_{B+R} \cong X^{\dagger\dagger}_{B+R}$ and $\Sigma'_{B+R} \approx^{O_{am}}_{B+R} X'_{B+R}$ and $\Sigma^{\dagger\dagger}_{B+R} \approx^{O_{am}}_{B+R} X^{\dagger\dagger}_{B+R}$ hold.

The rest of the proof is analogous to Lemma 104 (V45: Stronger V4 Soundness Single step).

□

N PROOFS V145

Theorem 37 (Well-formed Composition $\curvearrowright_{B+S+R}$). $\vdash \curvearrowright_{B+S+R} : WFC$

Proof. Immediately follows from Lemma 150 (V145 AM: Confluence), Theorem 38 (V145: Relating V1 with projection of combined), Theorem 39 (V145: Relating V1 with projection of combined), Theorem 40 (V145: Relating V5 with projection of combined) and Lemma 167 (V145: Soundness Am semantics w.r.t. speculative semantics with new relation between states). □

Lemma 150 (V145 AM: Confluence). *If*

(1) $\Sigma_{B+S+R} \overset{\tau}{\curvearrowright}_{B+S+R} \Sigma'_{B+S+R}$ *and*

(2) $\Sigma_{B+S+R} \overset{\tau}{\curvearrowright}_{B+S+R} \Sigma''_{B+S+R}$ *derived by a different rule*

Then

(1) $\Sigma'_{B+S+R} = \Sigma_{B+S+R}$

Proof. Note that a difference can only come from using a combination of Rule AM-v1-step-V145, Rule AM-v4-step-V145 and Rule AM-v5-step-V145.

Since these two rules delegate back to the semantics of V1, V4 and V5, we look which two rules are applicable there.

By Lemma 106 (V14 AM: Confluence), Lemma 128 (V15 AM: Confluence) and Lemma 83 (V45 AM: Confluence), we know that each combination of these delegation rules is confluent. Thus, we have confluence here as well. □

We first define two relations for states of V1 and V4: These relations are virtually the same as the ones in V45.

$\boxed{\Sigma_B \approx \Sigma_{B+S+R}}$

$$\frac{}{\varnothing \approx \varnothing}\ \text{(V145-V1:Base)} \qquad \frac{\Sigma'_B \sim \Sigma'_{B+S+R}}{\Sigma'_B \cdot \langle p, ctr, \sigma, n\rangle \approx \Sigma'_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}\ \text{(V145-V1:Single-Base)}$$

$$\frac{\Sigma_B \sim \Sigma_{B+S+R} \quad \Sigma''_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma'''_{B+S+R} \quad \text{where transaction with id } ctr \text{ is rolled back} \quad \Sigma_B = \Sigma'_B \cdot \langle p, ctr', \sigma, n\rangle \quad x = v4 \vee v5 \quad \Sigma_{B+S+R} = \Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \quad \overline{\rho} = \begin{cases} \texttt{bypass}\ n \cdot \texttt{start}_S\ ctr & \text{if x = v4} \\ \texttt{ret}\ m \cdot \texttt{start}_R\ ctr & \text{if x = v5} \end{cases}}{\Sigma'_B \cdot \langle p, ctr', \sigma, n\rangle \approx \Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}, n'\rangle^x_{\overline{\rho}}}\ \text{(V145-V1:Single-Speculation-Start)}$$

$$\frac{\Sigma_B \sim \Sigma_{B+S+R} \quad \Sigma''_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma'''_{B+S+R} \quad \text{where transaction with id } ctr \text{ is rolled back} \quad \Sigma_B = \Sigma'_B \cdot \langle p, ctr', \sigma, n\rangle \quad x = v4 \vee v5 \quad \Sigma_{B+S+R} = \Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle}{\Sigma'_B \cdot \langle p, ctr', \sigma, n\rangle \approx \Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^x \cdot \Sigma_{B+S+R_1}}\ \text{(V145-V1:Single-Speculation-Diff)}$$

$\boxed{\Sigma_B \sim \Sigma_{B+S+R}}$

$$\frac{}{\varnothing \sim \varnothing}\ \text{(V145-V1:Base)} \qquad \frac{|\Sigma'_B| = |\Sigma'_{B+S+R}| \quad \Sigma'_B \sim \Sigma'_{B+S+R}}{\Sigma'_B \cdot \langle p, ctr, \sigma, n\rangle \sim \Sigma'_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}\ \text{(V145-V1:Single)}$$

$\boxed{\Sigma_S \approx \Sigma_{B+S+R}}$

$$\frac{}{\varnothing \approx \varnothing}\ \text{(V145-V4:Base)} \qquad \frac{\Sigma'_S \sim \Sigma'_{B+S+R}}{\Sigma'_S \cdot \langle p, ctr, \sigma, n\rangle \approx \Sigma'_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}\ \text{(V145-V4:Single-Base)}$$

$$\frac{\Sigma_S \sim \Sigma_{B+S+R} \quad \Sigma''_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma'''_{B+S+R} \quad \text{where transaction with id } ctr \text{ is rolled back} \quad \Sigma_S = \Sigma'_S \cdot \langle p, ctr', \sigma, n\rangle \quad x = v1 \vee v5 \quad \Sigma_{B+S+R} = \Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \quad \overline{\rho} = \begin{cases} \texttt{ret}\ n \cdot \texttt{start}_R\ ctr & \text{if x = v5} \\ \texttt{pc}\ m \cdot \texttt{start}_B\ ctr & \text{if x = v1} \end{cases}}{\Sigma'_S \cdot \langle p, ctr', \sigma, n\rangle \approx \Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}, n'\rangle^x_{\overline{\rho}}}\ \text{(V145-V4:Single-Speculation-Start)}$$

$$\frac{\Sigma_S \sim \Sigma_{B+S+R} \quad \Sigma''_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma'''_{B+S+R} \text{ where transaction with id } ctr \text{ is rolled back} \quad \Sigma_S = \Sigma'_S \cdot \langle p, ctr', \sigma, n\rangle \quad x = v1 \vee v5 \quad \Sigma_{B+S+R} = \Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle}{\Sigma'_S \cdot \langle p, ctr', \sigma, n\rangle \approx \Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^x \cdot \Sigma_{B+S+R1}} \text{(V145-V4:Single-Speculation-Diff)}$$

$\boxed{\Sigma_S \sim \Sigma_{B+S+R}}$

$$\frac{}{\varnothing \sim \varnothing} \text{(V145-V4:Base)} \qquad \frac{|\Sigma'_S| = |\Sigma'_{B+S+R}| \quad \Sigma'_S \sim \Sigma'_{B+S+R}}{\Sigma'_S \cdot \langle p, ctr, \sigma, n\rangle \sim \Sigma'_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle} \text{(V145-V4:Single)}$$

$\boxed{\Sigma_R \approx \Sigma_{B+S+R}}$

$$\frac{}{\varnothing \approx \varnothing} \text{(V145-V5:Base)} \qquad \frac{\Sigma'_R \sim \Sigma'_{B+S+R}}{\Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \approx \Sigma'_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle} \text{(V145-V5:Single-Base)}$$

$$\frac{\Sigma_R \sim \Sigma_{B+S+R} \quad \Sigma''_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma'''_{B+S+R} \text{ where transaction with id } ctr \text{ is rolled back} \quad \Sigma_R = \Sigma'_R \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \quad x = v1 \vee v4 \quad \Sigma_{B+S+R} = \Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \quad \overline{\rho} = \begin{cases} \texttt{bypass}\ n \cdot \texttt{start}_S\ ctr & \text{if x = v4} \\ \texttt{pc}\ m \cdot \texttt{start}_B\ ctr & \text{if x = v1} \end{cases}}{\Sigma'_R \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \approx \Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^x_{\overline{\rho}}} \text{(V145-V5:Single-Speculation-Start)}$$

$$\frac{\Sigma_R \sim \Sigma_{B+S+R} \quad \Sigma''_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma'''_{B+S+R} \text{ where transaction with id } ctr \text{ is rolled back} \quad \Sigma_R = \Sigma'_R \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \quad x = v1 \vee v4 \quad \Sigma_{B+S+R} = \Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle}{\Sigma'_R \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \approx \Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^x \cdot \Sigma_{B+S+R1}} \text{(V145-V5:Single-Speculation-Diff)}$$

$\boxed{\Sigma_R \sim \Sigma_{B+S+R}}$

$$\frac{}{\varnothing \sim \varnothing} \text{(V145-V5:Base)} \qquad \frac{|\Sigma'_R| = |\Sigma'_{B+S+R}| \quad \Sigma'_R \sim \Sigma'_{B+S+R}}{\Sigma'_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \sim \Sigma'_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle} \text{(V145-V5:Single)}$$

Lemma 151 (V145: V1 step). *If*

(1) $\Sigma_B \approx \Sigma_{B+S+R}$ *by Rule V145-V1:Single-Base and*
(2) $\Sigma_{B+S+R} = \overline{\Phi}_{B+S+R} \cdot \Phi_{B+S}$ *and* $\Sigma'_{B+S+R} = \overline{\Phi}_{B+S+R} \cdot \overline{\Phi}'_{B+S+R}$ *and*
(3) $\Phi_{B+S+R} \restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_{B+S+R}$ *or* $\Phi_{B+S+R} \restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_{B+S+R}$ *and*

Then

(1) $\Sigma_B \overset{\tau \restriction^B}{\dashrightarrow}_B \Sigma'_B$ *and*
(2) if the step was not derived by Rule S*:AM-Store-Spec or Rule* R*:AM-Ret-Spec then* $\Sigma'_S \approx \Sigma'_{B+S}$ *by Rule V145-V1:Single-Base and*
(3) if the step was derived by Rule S*:AM-Store-Spec or Rule* R*:AM-Ret-Spec then* $\Sigma'_S \approx \Sigma'_{B+S}$ *by Rule V145-V1:Single-Speculation-Start*

Proof. We have by $\approx$:

$$\begin{aligned} \Sigma_B &= \Sigma''_B \cdot \langle p, ctr, \sigma, n\rangle \\ \Sigma_{B+S+R} &= \Sigma''_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \\ \Sigma''_B &\sim \Sigma''_{B+S+R} \end{aligned}$$

There are two cases:

$\Phi_{B+S+R} \restriction^S \overset{\tau}{\dashrightarrow}_S \overline{\Phi}'_{B+S+R}$ The case is analogous to Lemma 107 (V14: V1 step).

$\Phi_{B+S+R} \restriction^R \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_{B+S+R}$ The case is analogous to Lemma 130 (V15: V1 step).

□

Lemma 152 (V145: V4 step). *If*

(1) $\Sigma_S \approx \Sigma_{B+S+R}$ *by Rule V145-V1:Single-Base and*
(2) $\Sigma_{B+S+R} = \overline{\Phi}_{B+S+R} \cdot \Phi_{B+S}$ *and* $\Sigma'_{B+S+R} = \overline{\Phi}_{B+S+R} \cdot \overline{\Phi}'_{B+S+R}$ *and*
(3) $\Phi_{B+S+R}\restriction^B \xrightarrow{\tau} {}_B\ \overline{\Phi}'_{B+S+R}$ *or* $\Phi_{B+S+R}\restriction^R \xrightarrow{\tau}_R\ \overline{\Phi}'_{B+S+R}$ *and*

Then

(1) $\Sigma_S \xrightarrow{\tau\restriction^S}_S \Sigma'_S$ *and*
(2) if the step was not derived by Rule B*:AM-Spec or Rule* R*:AM-Ret-Spec then* $\Sigma'_S \approx \Sigma'_{B+S}$ *by Rule V145-V4:Single-Base and*
(3) if the step was derived by Rule B*:AM-Spec or Rule* R*:AM-Ret-Spec then* $\Sigma'_S \approx \Sigma'_{B+S}$ *by Rule V145-V4:Single-Speculation-Start*

Proof. We have by $\approx$:

$$\begin{aligned}\Sigma_S &= \Sigma''_S \cdot \langle p, ctr, \sigma, n\rangle\\ \Sigma_{B+S+R} &= \Sigma''_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\\ \Sigma''_S &\sim \Sigma''_{B+S+R}\end{aligned}$$

There are two cases:

$\Phi_{B+S+R}\restriction^B \xrightarrow{\tau} {}_B\ \overline{\Phi}'_{B+S+R}$ The case is analogous to Lemma 108 (V14: V4 step).
$\Phi_{B+S+R}\restriction^R \xrightarrow{\tau}_R\ \overline{\Phi}'_{B+S+R}$ The case is analogous to Lemma 86 (V45: V4 step).

□

Lemma 153 (V145: V5 step)**.** *If*

(1) $\Sigma_R \approx \Sigma_{B+S+R}$ *by Rule V145-V5:Single-Base and*
(2) $\Sigma_{B+S+R} = \overline{\Phi}_{B+S+R} \cdot \Phi_{B+S}$ *and* $\Sigma'_{B+S+R} = \overline{\Phi}_{B+S+R} \cdot \overline{\Phi}'_{B+S+R}$ *and*
(3) $\Phi_{B+S+R}\restriction^B \xrightarrow{\tau} {}_B\ \overline{\Phi}'_{B+S+R}$ *or* $\Phi_{B+S+R}\restriction^S \xrightarrow{\tau}_S\ \overline{\Phi}'_{B+S+R}$ *and*

Then

(1) $\Sigma_R \xrightarrow{\tau\restriction^S}_R \Sigma'_R$ *and*
(2) if the step was not derived by Rule B*:AM-Spec or Rule* S*:AM-Store-Spec then* $\Sigma'_R \approx \Sigma'_{B+S}$ *by Rule V145-V5:Single-Base and*
(3) if the step was derived by Rule B*:AM-Spec or Rule* S*:AM-Store-Spec then* $\Sigma'_R \approx \Sigma'_{B+S}$ *by Rule V145-V5:Single-Speculation-Start*

Proof. We have by $\approx$:

$$\begin{aligned}\Sigma_R &= \Sigma''_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle\\ \Sigma_{B+S+R} &= \Sigma''_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\\ \Sigma''_R &\sim \Sigma''_{B+S+R}\end{aligned}$$

There are two cases:

$\Phi_{B+S+R}\restriction^B \xrightarrow{\tau} {}_B\ \overline{\Phi}'_{B+S+R}$ The case is analogous to Lemma 129 (V15: V5 step).
$\Phi_{B+S+R}\restriction^S \xrightarrow{\tau}_S\ \overline{\Phi}'_{B+S+R}$ The case is analogous to Lemma 87 (V45: V5 step).

□

The Completeness proofs now need to do a bigger case distinction in the noBranching case, since speculation can come from multiple different instructions. But we have seen all of these cases already. Again the case distinction on the instruction is exactly on the metaparameter Z that is introduced for the combinations, because that is the difference in the semantics of its part to the original semantics

N.1 Projection to V1

Theorem 38 (V145: Relating V1 with projection of combined). *Let* p *be a program and* ω *be a speculation window. Then* $Beh^{\mathcal{A}}_{B}(p) = Beh^{B+S+R}_{\mathcal{A}}(p)\restriction^B$.

Proof. We prove the two directions separately:

$\Leftarrow$ Assume that (p,σ) $\text{👻}^{\omega}_{\mathrm{B+S+R}}$ $\overline{\tau} \in Beh^{\mathrm{B+S+R}}_{\mathcal{A}}(p)$.

The case is analogous to Theorem 24 (V45: Relating V4 with projection of combined) using Lemma 154 (V145: Soundness of the AM speculative semantics w.r.t. AM v1 semantics).

We can now conclude that p, σ $\text{👻}^{\omega}_{\mathrm{B}}$ $\overline{\tau}\restriction^{B} \in Beh^{\mathcal{A}}_{\mathrm{B}}(p)$ by Rule B:AM-Trace.

$\Rightarrow$ Assume that (p,σ) $\text{👻}^{\omega}_{\mathrm{B}}$ $\overline{\tau} \in Beh^{\mathcal{A}}_{\mathrm{B}}(p)$.

The case is analogous to Theorem 24 (V45: Relating V4 with projection of combined) using Lemma 155 (V145 AM: Completeness w.r.t V1 and projection).

We thus have (p,σ) $\text{👻}^{\omega}_{\mathrm{B+S+R}}$ $\overline{\tau}' \in Beh^{\mathrm{B+S+R}}_{\mathcal{A}}(p)$ with $\overline{\tau}'\restriction^{B} = \overline{\tau}$.

□

Lemma 154 (V145: Soundness of the AM speculative semantics w.r.t. AM v1 semantics)**.** *If*

(1) $\Sigma_{\mathrm{B}} \approx \Sigma_{\mathrm{B+S+R}}$ *and*

(2) $\Sigma_{\mathrm{B+S+R}} \Downarrow^{\overline{\tau}}_{\mathrm{B+S+R}} \Sigma'_{\mathrm{B+S+R}}$

Then exists Σ'_{B} *such that*

I $\Sigma'_{\mathrm{B}} \approx \Sigma'_{\mathrm{B+S+R}}$ *and*

II if $\Sigma'_{\mathrm{B}} \approx \Sigma'_{\mathrm{B+S+R}}$ *by Rule V145-V1:Single-Base then* $\Sigma_{\mathrm{B}} \Downarrow^{\overline{\tau}\restriction^{B}}_{\mathrm{B}} \Sigma'_{\mathrm{B}}$ *and*

III if $\Sigma'_{\mathrm{B}} \approx \Sigma'_{\mathrm{B+S+R}}$ *by Rule V145-V1:Single-Speculation-Start then* $\Sigma_{\mathrm{B}} \Downarrow^{\overline{\tau}\restriction^{B}}_{\mathrm{B}} \Sigma'_{\mathrm{B}}$ *and*

IV if $\Sigma'_{\mathrm{B}} \approx \Sigma'_{\mathrm{B+S+R}}$ *by Rule V145-V1:Single-Speculation-Diff then* $\Sigma_{\mathrm{B}} \Downarrow^{helper_B(\overline{\tau},i)}_{\mathrm{B}} \Sigma'_{\mathrm{B}}$*, where* $i = ctr'$ *by unpacking* $\Sigma'_{\mathrm{B+S+R}}$ *according to Rule V145-V1:Single-Speculation-Diff.*

Proof. By Induction on $\Sigma_{\mathrm{B+S+R}} \Downarrow^{\overline{\tau}}_{\mathrm{B+S+R}} \Sigma'_{\mathrm{B+S+R}}$.

Rule AM-Reflection-V145 Then we have $\Sigma_{\mathrm{B+S+R}} \Downarrow^{\varepsilon}_{\mathrm{S}} \Sigma_{\mathrm{B+S+R}}$ with $\Sigma'_{\mathrm{B+S+R}} = \Sigma_{\mathrm{B+S+R}}$ and by Rule AM-Reflection-V14 we have

I $\Sigma'_{\mathrm{B}} \approx \Sigma'_{\mathrm{B+S+R}}$

II $\Sigma_{\mathrm{B}} \Downarrow^{\varepsilon\restriction^{B}}_{\mathrm{B}} \Sigma'_{\mathrm{B}}$ with $\Sigma_{\mathrm{B}} = \Sigma'_{\mathrm{B}}$.

III $\Sigma_{\mathrm{B}} \Downarrow^{helper_B(\varepsilon,i)}_{\mathrm{B}} \Sigma'_{\mathrm{B}}$ with $\Sigma_{\mathrm{B}} = \Sigma'_{\mathrm{B}}$.

Note, that the initial relation $\Sigma_{\mathrm{B}} \approx \Sigma_{\mathrm{B+S+R}}$ does not change.

Rule AM-Single-V145 We have $\Sigma_{\mathrm{B+S+R}} \Downarrow^{\overline{\tau}''}_{\mathrm{B+S+R}} \Sigma''_{\mathrm{B+S+R}}$ with $\Sigma''_{\mathrm{B+S+R}} \overset{\tau}{\text{=}}\text{👻}_{\mathrm{B+S+R}} \Sigma'_{\mathrm{B+S+R}}$.

We now apply IH on $\Sigma''_{\mathrm{B+S+R}} \Downarrow^{\overline{\tau}''}_{\mathrm{B+S+R}} \Sigma''_{\mathrm{B+S+R}}$ and get

(a) $\Sigma''_{\mathrm{B}} \approx \Sigma''_{\mathrm{B+S+R}}$

(b) if $\Sigma''_{\mathrm{B}} \approx \Sigma''_{\mathrm{B+S+R}}$ by Rule V145-V1:Single-Base then $\Sigma_{\mathrm{B}} \Downarrow^{\overline{\tau}\restriction^{B}}_{\mathrm{B}} \Sigma''_{\mathrm{B}}$ and

(c) if $\Sigma''_{\mathrm{B}} \approx \Sigma''_{\mathrm{B+S+R}}$ by Rule V145-V1:Single-Speculation-Start then $\Sigma_{\mathrm{B}} \Downarrow^{\overline{\tau}\restriction^{B}}_{\mathrm{B}} \Sigma''_{\mathrm{B}}$ and

(d) if $\Sigma''_{\mathrm{B}} \approx \Sigma''_{\mathrm{B+S+R}}$ by Rule V145-V1:Single-Speculation-Diff $\Sigma_{\mathrm{B}} \Downarrow^{helper_B(\overline{\tau},j)}_{\mathrm{B}} \Sigma''_{\mathrm{B}}$, where $j = ctr'$ by unpacking $\Sigma''_{\mathrm{B+S+R}}$ according to Rule V145-V1:Single-Speculation-Diff

We do a case distinction on $\approx$ in $\Sigma''_{\mathrm{B}} \approx \Sigma''_{\mathrm{B+S+R}}$:

Rule V14-V4:Single-Base We have

$$\Sigma_{\mathrm{B}} \Downarrow^{\overline{\tau}\restriction^{B}}_{\mathrm{B}} \Sigma''_{\mathrm{B}}$$
$$\Sigma''_{\mathrm{B}} = \Sigma'''_{\mathrm{B}} \cdot \langle p, ctr, \sigma, n\rangle_{\overline{\rho}}$$
$$\Sigma''_{\mathrm{B+S+R}} = \Sigma'''_{\mathrm{B+S+R}} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle_{\overline{\rho}}$$
$$\Sigma'''_{\mathrm{B}} \sim \Sigma'''_{\mathrm{B+S+R}}$$

We now proceed by inversion on the derivation $\Sigma''_{\mathrm{B+S+R}} \overset{\tau}{\text{=}}\text{👻}_{\mathrm{B+S+R}} \Sigma'_{\mathrm{B+S+R}}$:

Rule AM-v1-Rollback-V145 By (b), it can only be roll back of V1 and only be the topmost state.

Furthermore, this means that $n = 0$.

Then $\Sigma''_{\mathrm{B}} \overset{\mathrm{rlb}_{\mathrm{B}}\ ctr}{\text{=}\!\text{=}}\text{👻}_{\mathrm{B}} \Sigma'_{\mathrm{B}}$ by Rule B:AM-Rollback, since n is equal between the two states. The rest of the case is analogous to Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

Rule AM-v4-Rollback-V145 Since $\Sigma''_{\mathrm{B}} \approx \Sigma''_{\mathrm{B+S+R}}$ by Rule V145-V1:Single-Base, there cannot be a roll back of V4.

Rule AM-v5-Rollback-V145 Since $\Sigma''_{\mathrm{B}} \approx \Sigma''_{\mathrm{B+S+R}}$ by Rule V145-V1:Single-Base, there cannot be a roll back of V4.

Rule AM-Context-V145 We have $\Phi_{\mathrm{B+S+R}} \overset{\tau}{\text{=}}\text{👻}_{\mathrm{B+S+R}} \Phi'_{\mathrm{B+S+R}}$.

We now use inversion on $\Phi_{B+S+R} \overset{\tau}{\Longrightarrow}_{B+S+R} \overline{\Phi}_{B+S+R}$:

Rule AM-v4-step-V145 Then we have $\Phi_{B+S+R} \restriction^{S} \overset{\tau}{\Longrightarrow}_{S} \overline{\Phi}'_{S}$.

By inversion on $\Phi_{B+S+R} \restriction^{S} \overset{\tau}{\Longrightarrow}_{S} \overline{\Phi}'_{S}$ we get:
The cases are analogous to the corresponding cases Rule AM-v4-step-V45 in Lemma 89 (V45: Soundness of the AM speculative semantics w.r.t. AM v5 semantics) using Lemma 151 (V145: V1 step)

Rule AM-v5-step-V145 Then we have $\Phi_{B+R} \restriction^{R} \overset{\tau}{\Longrightarrow}_{R} \overline{\Phi}'_{R}$. The cases are analogous to the corresponding cases Rule AM-v5-step-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) using Lemma 151 (V145: V1 step)

Rule AM-v1-step-V145 Then we have $\Phi_{B+S+R} \restriction^{B} \overset{\tau}{\Longrightarrow}_{B} \overline{\Phi}'_{B}$.
The case is analogous to the corresponding case Rule AM-v4-step-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) combined with the fact that the rules of V1 cannot generate a $\texttt{start}_S$ *id*, $\texttt{start}_R$ *id*, $\texttt{rlb}_R$ *id* or $\texttt{rlb}_S$ *id* observation.

Rule V145-V1:Single-Speculation-Start We have:

$$
\begin{aligned}
\Sigma_B \Downarrow_B^{\overline{\tau}\restriction^B} \Sigma''_B \\
\Sigma''_B =& \Sigma'''_B \cdot \langle p, ctr, \sigma, n\rangle \\
x =& v4 \vee v5 \\
\overline{\rho} =& \begin{cases} \texttt{bypass}\ n \cdot \texttt{start}_S\ ctr & \text{if x = v4} \\ \texttt{ret}\ l \cdot \texttt{start}_R\ ctr & \text{if x = v5} \end{cases} \\
\Sigma''_{B+S+R} =& \Sigma'''_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle_{\overline{\rho}} \\
\Sigma'''_B \cdot \langle p, ctr, \sigma, n\rangle \sim& \Sigma'''_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle
\end{aligned}
$$

We now proceed by inversion on the derivation $\Sigma''_{B+S+R} \overset{\tau}{\Longrightarrow}_{B+S+R} \Sigma'_{B+S+R}$.

Rule AM-v1-Rollback-V145 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v4-Rollback-V145 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v5-Rollback-V145 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-Context-V145 We have $\Phi_{B+S+R} \overset{\tau}{\Longrightarrow}_{B+S+R} \overline{\Phi}'_{B+S+R}$.

We now use inversion on $\Phi_{B+S+R} \overset{\tau}{\Longrightarrow}_{B+S+R} \overline{\Phi}_{B+S+R}$:

Rule AM-v4-step-V145 Then we have $\Phi_{B+S+R} \restriction^{S} \overset{\tau}{\Longrightarrow}_{S} \overline{\Phi}'_{S}$.

By inversion on $\Phi_{B+S+R} \restriction^{S} \overset{\tau}{\Longrightarrow}_{S} \overline{\Phi}'_{S}$ we get:
Rule S:AM-General By definition we have $\tau = \texttt{start}_S\ ctr'$. Since Rule S:AM-General does not modify the state, we have $\Sigma'_{B+S+R} = \Sigma''_{B+S+R\texttt{bypass}\ n}$.
Then we choose $\Sigma'_B = \Sigma''_B$ and derive the step $\Sigma''_B \Downarrow_B^{\epsilon} \Sigma'_B$ by Rule B:AM-Reflection.
We now fulfill all premises for Rule V14-V1:Single-Speculation-Diff and have $\Sigma'_B \approx \Sigma'_{B+S+R}$.
We need to show that $\Sigma_B \Downarrow_B^{helper_B(\overline{\tau}\cdot\tau, ctr')} \Sigma'_B$ holds.
We have:

$$
\begin{aligned}
& \overline{\tau}\restriction^B && \text{Definition } helper_B() \\
=& helper_B(\overline{\tau} \cdot \texttt{start}_S\ ctr', ctr') && \tau = \texttt{start}_S\ ctr' \\
=& helper_B(\overline{\tau} \cdot \tau, ctr')
\end{aligned}
$$

and we have $\overline{\tau}\restriction^B$ by IH.
Since $\Sigma'_B = \Sigma''_B$ and IH $\Sigma_B \Downarrow_B^{\overline{\tau}\restriction^B} \Sigma''_B$, we have $\Sigma_B \Downarrow_B^{helper_B(\overline{\tau}\cdot\tau, ctr')} \Sigma'_B$ as needed to show.

otherwise Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v5-step-V145 Then we have $\Phi_{B+S+R} \restriction^{R} \overset{\tau}{\Longrightarrow}_{R} \overline{\Phi}'_{R}$.

By inversion on $\Phi_{B+S+R} \restriction^{R} \overset{\tau}{\Longrightarrow}_{R} \overline{\Phi}'_{R}$ we get:
Rule R:AM-General By definition we have $\tau = \texttt{start}_R\ ctr$.
Since Rule R:AM-General does not modify the state, we have $\Sigma'_{B+R} = \Sigma''_{B+R\texttt{ret}\ l}$.

Then we choose $\Sigma'_B = \Sigma''_B$ and derive the step $\Sigma''_B \Downarrow^{\varepsilon}_B \Sigma'_B$ by Rule B:AM-Reflection.
The case is analogous to the corresponding case Rule R:AM-General in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) and the fact that $helper_B()$ behaves the same as $helper_S()$ for $\texttt{start}_R$ observations.

otherwise Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v1-step-V145 Contradiction, because $\overline{\rho}$ is non-empty and Rule B:AM-General does not work on $\texttt{start}_S$ *id* or $\texttt{start}_R$ observations.

Rule V145-V1:Single-Speculation-Diff We have:

$$\begin{aligned}
\Sigma_B \Downarrow^{helper_B(\overline{\tau},j)}_B \Sigma''_B \\
\Sigma''_B &= \Sigma'''_R \cdot \langle p, ctr, \sigma, n\rangle \\
x &= v4 \vee v5 \\
\Sigma''_{B+S+R} &= \Sigma'''_{B+S+R} \cdot \langle p, ctr'', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr''', \sigma'', \mathbb{R}', n''\rangle^x \cdot \Sigma^{\dagger}_{B+S+R} \\
\Sigma'''_B \cdot \langle p, ctr, \sigma, n\rangle &\sim \Sigma'''_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \\
j &= ctr'
\end{aligned}$$

We now proceed by inversion on the derivation $\Sigma''_{B+S+R} \overset{\overline{\tau}}{\rightsquigarrow}_{B+S+R} \Sigma'_{B+S+R}$:

Rule AM-v1-Rollback-V145 This means a transaction is rolled back that was created later than the transaction with $id = j$.
Then we choose $\Sigma'_B = \Sigma''_B$ and derive the step $\Sigma''_B \Downarrow^{\varepsilon}_B \Sigma'_B$ by Rule B:AM-Reflection.
The case is analogous to the corresponding case Rule AM-v4-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

Rule AM-v4-Rollback-V145 or Rule AM-v5-Rollback-V145 There are two cases depending on the *id* of the rolled back transaction:

$id \neq j$ This means a transaction is rolled back that was created later than the transaction with $id = j$.
The case is analogous to the case of Rule AM-v5-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

$id = j$ Then we choose $\Sigma'_B = \Sigma''_B$ and derive the step $\Sigma''_B \Downarrow^{\varepsilon}_B \Sigma'_B$ by Rule B:AM-Reflection.
Since the transaction with $id = j$ was rolled back, we know that $\Sigma'_{B+S+R} = \Sigma'''_{B+S+R} \cdot \langle p, ctr''', \sigma, n\rangle$.
For the trace, we get $\overline{\tau} \cdot \texttt{rlb}_S\ j\restriction^B = helper_B(\overline{\tau}, j)$ and $\overline{\tau} \cdot \texttt{rlb}_R\ j\restriction^B = helper_B(\overline{\tau}, j)$ by definition of $\restriction^B$ and $id = j$.
The rest of the case is analogous to the corresponding case Rule AM-v5-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

otherwise Then we choose $\Sigma'_B = \Sigma''_B$ and derive the step $\Sigma''_B \Downarrow^{\varepsilon}_B \Sigma'_B$ by Rule B:AM-Reflection. Analogous to the corresponding case Rule AM-v4-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

□

Lemma 155 (V145 AM: Completeness w.r.t V1 and projection)**.** *If*

(1) $\Sigma_B \approx \Sigma_{B+S+R}$ *by Rule V14-V1:Single-Base and*
(2) $\Sigma_B \Downarrow^{\overline{\tau}}_B \Sigma'_B$

Then exists Σ'_{B+S+R} *such that*

I $\Sigma'_B \approx \Sigma'_{B+S+R}$ *by Rule V14-V1:Single-Base and*
II $\Sigma_{B+S+R} \Downarrow^{\overline{\tau}'}_{B+S+R} \Sigma'_{B+S+R}$ *and*
III $\overline{\tau} = \overline{\tau}'\restriction^B$

Proof. We proceed by induction on $\Sigma_B \Downarrow^{\overline{\tau}}_B \Sigma'_B$:

Rule B:AM-Reflection By Rule B:AM-Reflection we have $\Sigma_B \Downarrow^{\varepsilon}_B \Sigma_B$ with $\Sigma_B = \Sigma'_B$.

I - III We derive $\Sigma_{B+S+R} \Downarrow^{\overline{\tau}'}_{B+S+R} \Sigma'_{B+S+R}$ by Rule AM-Reflection-V145 and thus $\Sigma_{B+S+R} = \Sigma'_{B+S+R}$.
By construction and 2) we have $\Sigma'_B \approx \Sigma'_{B+S+R}$ by Rule V145-V1:Single-Base.
Since $\varepsilon\restriction^B = \varepsilon$ we are finished.

Rule B:AM-Single Then we have $\Sigma_B \Downarrow^{\overline{\tau}}_B \Sigma''_B$ and $\Sigma''_B \overset{\tau}{\rightsquigarrow}_B \Sigma'_R$.
We need to show
I $\Sigma_{B+S+R} \Downarrow^{\overline{\tau}'\cdot\tau'}_{B+S+R} \Sigma'_{B+S+R}$ and
II $\Sigma'_B \approx \Sigma'_{B+S+R}$ by Rule V145-V1:Single-Base and
III $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau'\restriction^B$
We apply the IH on $\Sigma_B \Downarrow^{\overline{\tau}}_B \Sigma''_B$ we get
I' $\Sigma_{B+S+R} \Downarrow^{\overline{\tau}'}_{B+S+R} \Sigma''_{B+S+R}$ and

II' $\Sigma''_{\mathsf{B}} \approx \Sigma''_{\mathsf{B+S+R}}$ by Rule V145-V1:Single-Base and
IV' $\overline{\tau} = \overline{\tau}' \restriction^{B}$
By Rule V145-V1:Single-Base we have:

$$\begin{aligned} \Sigma''_{\mathsf{B}} &= \Sigma'''_{\mathsf{B}} \cdot \langle p, ctr, \sigma, n\rangle \\ \Sigma''_{\mathsf{B+S+R}} &= \Sigma'''_{\mathsf{B+S+R}} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \\ \Sigma'''_{\mathsf{B}} &\sim \Sigma'''_{\mathsf{B+S+R}} \end{aligned}$$

We continue by inversion on $\Sigma''_{\mathsf{B}} \overset{\tau}{\Rightarrow}_{\mathsf{B}} \Sigma'_{\mathsf{B}}$:

Rule B:AM-Rollback The case is analogous to the corresponding case in Lemma 90 (V45 AM: Completeness w.r.t V5 and projection) using Rule AM-v1-Rollback-V145.

Rule B:AM-Context We then have $\langle p, ctr, \sigma, n\rangle \overset{\tau}{\Rightarrow}_{\mathsf{B}} \overline{\Phi}'_{\mathsf{B}}$ and $n > 0$.

By $\Sigma''_{\mathsf{B}} \approx \Sigma''_{\mathsf{B+S+R}}$ we know that Rule AM-Context-V145 applies for the step $\Sigma''_{\mathsf{B+S+R}} \overset{\tau'}{\Rightarrow}_{\mathsf{B+S+R}} \Sigma'_{\mathsf{B+S+R}}$.

We now need to find a derivation for the step $\langle p, ctr', \sigma, \mathbb{R}, n\rangle \overset{\tau'}{\Rightarrow}_{\mathsf{B+S+R}} \overline{\Phi}'_{\mathsf{B+S+R}}$ according to Rule AM-Context-V145.

We proceed by inversion on $\langle p, ctr, \sigma, n\rangle \overset{\tau}{\Rightarrow}_{\mathsf{B}} \overline{\Phi}'_{\mathsf{B}}$:

Rule AM-NoBranch Then $n > 0$ and $\langle p, ctr, \sigma, n\rangle \overset{\tau}{\Rightarrow}_{\mathsf{B}} \overline{\Phi}'_{\mathsf{B}}$ by $\sigma \xrightarrow{\tau} \sigma'$.
Furthermore, $\Sigma'_{\mathsf{B}}.n = n - 1$.
We now do a case analysis on the instruction $p(\sigma(\mathbf{pc}))$:

$p(\sigma(\mathbf{pc})) = \mathbf{store}\ x, e$ Then, a speculative transaction of V4 with id is started using Rule S:AM-Store-Spec through Rule AM-v4-step-V145 and a new instance $\overline{\Phi}'_{\mathsf{B+S}}$ was pushed on top of the stack.
The rest of the case is analogous to the corresponding case in Lemma 90 (V45 AM: Completeness w.r.t V5 and projection).

$p(\sigma(\mathbf{pc})) = \mathbf{ret\ and}\ \mathbb{R}\ \mathbf{is\ non\text{-}empty\ and}\ \mathbb{R}\ \mathbf{value\ is\ different\ to\ return\ address}$ Then, a speculative transaction of V5 with id is started using Rule R:AM-Ret-Spec through Rule AM-v5-step-V145 and a new instance $\Phi'_{\mathsf{B+R}}$ was pushed on top of the stack of $\Sigma''_{\mathsf{B+R}}$.
The rest of the case is analogous to the corresponding case in Lemma 88 (V45 AM: Completeness w.r.t V4 and projection).

$p(\sigma(\mathbf{pc})) = \mathbf{ret\ and}\ \mathbb{R}\ \mathbf{is\ empty\ or}\ \mathbb{R}\ \mathbf{is\ not\ different\ to\ return\ address}$ Since $n > 0$, the state can do a step using either Rule R:AM-Ret-Empty or Rule R:AM-Ret-Same through Rule AM-v5-step-V145 (Note that the meta parameter Z restricts the V4 semantics in the combined part).
The case is analogous to the corresponding case in Lemma 88 (V45 AM: Completeness w.r.t V4 and projection) together with the fact that $\restriction^{B}$ and $\restriction^{S}$ behave similar with speculative transactions generated by V5.

$p(\sigma(\mathbf{pc})) = \mathbf{call}\ f$ Since $n > 0$, the state can do a step using either Rule R:AM-Call or Rule R:AM-Call-Full through Rule AM-v5-step-V15. The case is analogous to the corresponding case in Lemma 88 (V45 AM: Completeness w.r.t V4 and projection).

otherwise Then we can either use Rule AM-NoBranch through Rule AM-v1-step-V145, Rule S:AM-NoBranch through Rule AM-v4-step-V145 or Rule R:AM-NoBranch through Rule AM-v5-step-V145.
Because of Lemma 150 (V145 AM: Confluence), we know that it does not matter which rule we use, which means we can use the same rule as for v5 do derive the step.
The rest of the proof is analogous to the corresponding case in Lemma 90 (V45 AM: Completeness w.r.t V5 and projection).

otherwise These rules include Rule B:AM-barr, Rule B:AM-barr-spec, Rule B:AM-General and Rule B:AM-Spec. Since the rules of V1 are included in the combined semantics and $\Sigma_{\mathsf{S}} \approx \Sigma_{\mathsf{B+S+R}}$, we can use the corresponding rule in the combined semantics by Confluence or delegate back to V1 by Rule AM-v1-step-V145.
This means we can always do the same step in the combined as in the V1 semantics.

□

N.2 Projection to V4

Theorem 39 (V145: Relating V1 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\mathcal{A}}_{\mathsf{S}}(p) = Beh^{\mathsf{B+S+R}}_{\mathcal{A}}(p) \restriction^{B}$.*

Proof. We prove the two directions separately:

⇐ Assume that $(p, \sigma) \Subset^{\omega}_{\mathsf{B+S+R}} \overline{\tau} \in Beh^{\mathsf{B+S+R}}_{\mathcal{A}}(p)$.
The case is analogous to Theorem 24 (V45: Relating V4 with projection of combined) using Lemma 156 (V145: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).
We can now conclude that $p, \sigma \Subset^{\omega}_{\mathsf{S}} \overline{\tau}\restriction^{S} \in Beh^{\mathcal{A}}_{\mathsf{S}}(p)$ by Rule S:AM-Trace.

$\Rightarrow$ Assume that $(p,\sigma) \; \text{Ω}^{\omega}_{\mathsf{S}} \; \overline{\tau} \in Beh^{\mathcal{A}}_{\mathsf{S}}(p)$.

The case is analogous to Theorem 24 (V45: Relating V4 with projection of combined) using Lemma 157 (V145 AM: Completeness w.r.t V4 and projection).

We thus have $(p,\sigma) \; \text{Ω}^{\omega}_{\mathsf{B+S+R}} \; \overline{\tau}' \in Beh^{\mathsf{B+S+R}}_{\mathcal{A}}(p)$ with $\overline{\tau}' \restriction^{S} = \overline{\tau}$.

□

Lemma 156 (V145: Soundness of the AM speculative semantics w.r.t. AM v4 semantics)**.** *If*

(1) $\Sigma_{\mathsf{S}} \approx \Sigma_{\mathsf{B+S+R}}$ *and*

(2) $\Sigma_{\mathsf{B+S+R}} \Downarrow^{\overline{\tau}}_{\mathsf{B+S+R}} \Sigma'_{\mathsf{B+S+R}}$

Then exists Σ'_{S} *such that*

I $\Sigma'_{\mathsf{S}} \approx \Sigma'_{\mathsf{B+S+R}}$ *and*

II if $\Sigma'_{\mathsf{S}} \approx \Sigma'_{\mathsf{B+S+R}}$ *by Rule V145-V4:Single-Base then* $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}\restriction^{S}}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ *and*

III if $\Sigma'_{\mathsf{S}} \approx \Sigma'_{\mathsf{B+S+R}}$ *by Rule V145-V4:Single-Speculation-Start then* $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}\restriction^{S}}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ *and*

IV if $\Sigma'_{\mathsf{S}} \approx \Sigma'_{\mathsf{B+S+R}}$ *by Rule V145-V4:Single-Speculation-Diff then* $\Sigma_{\mathsf{S}} \Downarrow^{helpers_S(\overline{\tau},i)}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$*, where* $i = ctr'$ *by unpacking* $\Sigma'_{\mathsf{B+S+R}}$ *according to Rule V145-V4:Single-Speculation-Diff.*

Proof. By Induction on $\Sigma_{\mathsf{B+S+R}} \Downarrow^{\overline{\tau}}_{\mathsf{B+S+R}} \Sigma'_{\mathsf{B+S+R}}$.

Rule AM-Reflection-V145 Then we have $\Sigma_{\mathsf{B+S+R}} \Downarrow^{\varepsilon}_{\mathsf{S}} \Sigma_{\mathsf{B+S+R}}$ with $\Sigma'_{\mathsf{B+S+R}} = \Sigma_{\mathsf{B+S+R}}$ and by Rule AM-Reflection-V145 we have

I $\Sigma'_{\mathsf{S}} \approx \Sigma'_{\mathsf{B+S+R}}$

II $\Sigma_{\mathsf{S}} \Downarrow^{\varepsilon\restriction^{S}}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ with $\Sigma_{\mathsf{S}} = \Sigma'_{\mathsf{S}}$.

III $\Sigma_{\mathsf{S}} \Downarrow^{helpers_S(\varepsilon,i)}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ with $\Sigma_{\mathsf{S}} = \Sigma'_{\mathsf{S}}$.

Note, that the initial relation $\Sigma_{\mathsf{S}} \approx \Sigma_{\mathsf{B+S+R}}$ does not change.

Rule AM-Single-V145 We have $\Sigma_{\mathsf{B+S+R}} \Downarrow^{\overline{\tau}''}_{\mathsf{B+S+R}} \Sigma''_{\mathsf{B+S+R}}$ with $\Sigma''_{\mathsf{B+S+R}} \overset{\tau}{\text{Ω}}_{\mathsf{B+S+R}} \Sigma'_{\mathsf{B+S+R}}$.

We now apply IH on $\Sigma''_{\mathsf{B+S+R}} \Downarrow^{\overline{\tau}''}_{\mathsf{B+S+R}} \Sigma''_{\mathsf{B+S+R}}$ and get

(a) $\Sigma''_{\mathsf{S}} \approx \Sigma''_{\mathsf{B+S+R}}$

(b) if $\Sigma''_{\mathsf{S}} \approx \Sigma''_{\mathsf{B+S+R}}$ by Rule V145-V4:Single-Base then $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}\restriction^{S}}_{\mathsf{S}} \Sigma''_{\mathsf{S}}$ and

(c) if $\Sigma''_{\mathsf{S}} \approx \Sigma''_{\mathsf{B+S+R}}$ by Rule V145-V4:Single-Speculation-Start then $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}\restriction^{S}}_{\mathsf{S}} \Sigma''_{\mathsf{S}}$ and

(d) if $\Sigma''_{\mathsf{S}} \approx \Sigma''_{\mathsf{B+S+R}}$ by Rule V145-V4:Single-Speculation-Diff $\Sigma_{\mathsf{S}} \Downarrow^{helpers_S(\overline{\tau},j)}_{\mathsf{S}} \Sigma''_{\mathsf{S}}$, where $j = ctr'$ by unpacking $\Sigma''_{\mathsf{B+S+R}}$ according to Rule V145-V4:Single-Speculation-Diff

We do a case distinction on $\approx$ in $\Sigma''_{\mathsf{S}} \approx \Sigma''_{\mathsf{B+S+R}}$:

Rule V145-V4:Single-Base We have

$$\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}\restriction^{S}}_{\mathsf{S}} \Sigma''_{\mathsf{S}}$$
$$\Sigma''_{\mathsf{S}} = \Sigma'''_{\mathsf{S}} \cdot \langle p, ctr, \sigma, n\rangle_{\overline{\rho}}$$
$$\Sigma''_{\mathsf{B+S+R}} = \Sigma'''_{\mathsf{B+S+R}} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle_{\overline{\rho}}$$
$$\Sigma'''_{\mathsf{S}} \sim \Sigma'''_{\mathsf{B+S+R}}$$

We now proceed by inversion on the derivation $\Sigma''_{\mathsf{B+S+R}} \overset{\tau}{\text{Ω}}_{\mathsf{B+S+R}} \Sigma'_{\mathsf{B+S+R}}$:

Rule AM-v4-Rollback-V145 By (b), it can only be roll back of V1 and only be the topmost state.

Furthermore, this means that $n = 0$.

Then $\Sigma''_{\mathsf{S}} \overset{\mathtt{rlb}_{\mathsf{S}}\ ctr}{\text{Ω}}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ by Rule S:AM-Rollback, since n is equal between the two states. The rest of the case is analogous to Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

Rule AM-v1-Rollback-V145 Since $\Sigma''_{\mathsf{S}} \approx \Sigma''_{\mathsf{B+S+R}}$ by Rule V145-V1:Single-Base, there cannot be a roll back of V4.

Rule AM-v5-Rollback-V145 Since $\Sigma''_{\mathsf{S}} \approx \Sigma''_{\mathsf{B+S+R}}$ by Rule V145-V1:Single-Base, there cannot be a roll back of V4.

Rule AM-Context-V145 We have $\Phi_{\mathsf{B+S+R}} \overset{\tau}{\text{Ω}}_{\mathsf{B+S+R}} \overline{\Phi}'_{\mathsf{B+S+R}}$.

We now use inversion on $\Phi_{\mathsf{B+S+R}} \overset{\tau}{\text{Ω}}_{\mathsf{B+S+R}} \overline{\Phi}_{\mathsf{B+S+R}}$:

Rule AM-v1-step-V145 Then we have $\Phi_{\mathsf{B+S+R}}\restriction^{B} \overset{\tau}{\text{Ω}}_{\mathsf{B}} \overline{\Phi}'_{\mathsf{B}}$.

By inversion on $\Phi_{\mathsf{B+S+R}}\restriction^{B} \overset{\tau}{\text{Ω}}_{\mathsf{B}} \overline{\Phi}'_{\mathsf{B}}$ we get:

The cases are analogous to the corresponding cases Rule AM-v1-step-V14 in Lemma 109 (V14: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) using Lemma 152 (V145: V4 step)

Rule AM-v5-step-V145 Then we have $\Phi_{B+R} \upharpoonright^{R} \overset{\tau}{=\!\!\Rightarrow}_{R} \overline{\Phi}'_{R}$. The cases are analogous to the corresponding cases Rule AM-v5-step-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) using Lemma 152 (V145: V4 step)

Rule AM-v4-step-V145 Then we have $\Phi_{B+S+R} \upharpoonright^{S} \overset{\tau}{=\!\!\Rightarrow}_{S} \overline{\Phi}'_{S}$.
The case is analogous to the corresponding case Rule AM-v4-step-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) combined with the fact that the rules of V4 cannot generate a $\texttt{start}_B$ *id*, $\texttt{start}_R$ *id*, $\texttt{rlb}_R$ *id* or $\texttt{rlb}_B$ *id* observation.

Rule V145-V4:Single-Speculation-Start We have:

$$
\begin{aligned}
\Sigma_S \Downarrow_S^{\overline{\tau}} \upharpoonright^{S} \Sigma''_S \\
\Sigma''_S = \Sigma'''_S \cdot \langle p, ctr, \sigma, n \rangle \\
x = v1 \vee v5 \\
\overline{\rho} = \begin{cases} \texttt{pc}\ n \cdot \texttt{start}_B\ ctr & \text{if x = v1} \\ \texttt{ret}\ l \cdot \texttt{start}_R\ ctr & \text{if x = v5} \end{cases} \\
\Sigma''_{B+S+R} = \Sigma'''_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n' \rangle_{\overline{\rho}} \\
\Sigma'''_S \cdot \langle p, ctr, \sigma, n \rangle \sim \Sigma'''_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n \rangle
\end{aligned}
$$

We now proceed by inversion on the derivation $\Sigma''_{B+S+R} \overset{\tau}{=\!\!\Rightarrow}_{B+S+R} \Sigma'_{B+S+R}$.

Rule AM-v1-Rollback-V145 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v4-Rollback-V145 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v5-Rollback-V145 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-Context-V145 We have $\Phi_{B+S+R} \overset{\tau}{=\!\!\Rightarrow}_{B+S+R} \overline{\Phi}'_{B+S+R}$.

We now use inversion on $\Phi_{B+S+R} \overset{\tau}{=\!\!\Rightarrow}_{B+S+R} \overline{\Phi}_{B+S+R}$:

Rule AM-v1-step-V145 Then we have $\Phi_{B+S+R} \upharpoonright^{B} \overset{\tau}{=\!\!\Rightarrow}_{B} \overline{\Phi}'_{B}$.

By inversion on $\Phi_{B+S+R} \upharpoonright^{B} \overset{\tau}{=\!\!\Rightarrow}_{B} \overline{\Phi}'_{B}$ we get:

Rule B:AM-General By definition we have $\tau = \texttt{start}_B\ ctr'$. Since Rule B:AM-General does not modify the state, we have $\Sigma'_{B+S+R} = \Sigma''_{B+S+R\texttt{pc}\ n}$.
Then we choose $\Sigma'_S = \Sigma''_S$ and derive the step $\Sigma''_S \Downarrow_S^{\varepsilon} \Sigma'_S$ by Rule S:AM-Reflection.
The case is analogous to the corresponding case Rule B:AM-General in Lemma 109 (V14: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

otherwise Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v5-step-V145 Then we have $\Phi_{B+S+R} \upharpoonright^{R} \overset{\tau}{=\!\!\Rightarrow}_{R} \overline{\Phi}'_{R}$.

By inversion on $\Phi_{B+S+R} \upharpoonright^{R} \overset{\tau}{=\!\!\Rightarrow}_{R} \overline{\Phi}'_{R}$ we get:

Rule R:AM-General By definition we have $\tau = \texttt{start}_R\ ctr$.
Since Rule R:AM-General does not modify the state, we have $\Sigma'_{B+R} = \Sigma''_{B+R\texttt{ret}\ l}$.
Then we choose $\Sigma'_S = \Sigma''_S$ and derive the step $\Sigma''_S \Downarrow_B^{\varepsilon} \Sigma'_S$ by Rule S:AM-Reflection.
The case is analogous to the corresponding case Rule R:AM-General in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

otherwise Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v4-step-V145 Contradiction, because $\overline{\rho}$ is non-empty and Rule S:AM-General does not work on $\texttt{start}_B$ *id* or $\texttt{start}_R$ observations.

Rule V145-V1:Single-Speculation-Diff We have:

$$\begin{aligned}
\Sigma_S \Downarrow_S^{helpers_S(\overline{\tau},j)} \Sigma''_S \\
\Sigma''_S =& \Sigma'''_R \cdot \langle p, ctr, \sigma, n\rangle \\
x =& v4 \vee v5 \\
\Sigma''_{B+S+R} =& \Sigma'''_{B+S+R} \cdot \langle p, ctr'', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr''', \sigma'', \mathbb{R}', n''\rangle^x \cdot \Sigma^{\dagger}_{B+S+R} \\
\Sigma'''_S \cdot \langle p, ctr, \sigma, n\rangle \sim& \Sigma'''_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \\
j =& ctr'
\end{aligned}$$

We now proceed by inversion on the derivation $\Sigma''_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \Sigma'_{B+S+R}$:

Rule AM-v4-Rollback-V145 This means a transaction is rolled back that was created later than the transaction with $id = j$.
Then we choose $\Sigma'_S = \Sigma''_S$ and derive the step $\Sigma''_S \Downarrow_S^{\varepsilon} \Sigma'_S$ by Rule S:AM-Reflection.
The case is analogous to the corresponding case Rule AM-v4-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

Rule AM-v1-Rollback-V145 or Rule AM-v5-Rollback-V145 There are two cases depending on the id of the rolled back transaction:

$id \neq j$ This means a transaction is rolled back that was created later than the transaction with $id = j$.
The case is analogous to the case of Rule AM-v5-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

$id = j$ Then we choose $\Sigma'_S = \Sigma''_S$ and derive the step $\Sigma''_S \Downarrow_S^{\varepsilon} \Sigma'_S$ by Rule S:AM-Reflection.
Since the transaction with $id = j$ was rolled back, we know that $\Sigma'_{B+S+R} = \Sigma'''_{B+S+R} \cdot \langle p, ctr''', \sigma, n\rangle$.
For the trace, we get $\overline{\tau} \cdot \mathtt{rlb}_B\ j \restriction^S = helpers_S(\overline{\tau}, j)$ and $\overline{\tau} \cdot \mathtt{rlb}_R\ j \restriction^S = helpers_S(\overline{\tau}, j)$ by definition of $\restriction^S$ and $id = j$.
The rest of the case is analogous to the corresponding case Rule AM-v5-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

otherwise Then we choose $\Sigma'_B = \Sigma''_B$ and derive the step $\Sigma''_B \Downarrow_B^{\varepsilon} \Sigma'_B$ by Rule B:AM-Reflection. Analogous to the corresponding case Rule AM-v4-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

□

Lemma 157 (V145 AM: Completeness w.r.t V4 and projection)**.** *If*

(1) $\Sigma_S \approx \Sigma_{B+S+R}$ *by Rule V14-V4:Single-Base and*
(2) $\Sigma_S \Downarrow_S^{\overline{\tau}} \Sigma'_S$

Then exists Σ'_{B+S+R} *such that*

I $\Sigma'_S \approx \Sigma'_{B+S+R}$ *by Rule V14-V4:Single-Base and*
II $\Sigma_{B+S+R} \Downarrow_{B+S+R}^{\overline{\tau}'} \Sigma'_{B+S+R}$ *and*
III $\overline{\tau} = \overline{\tau}' \restriction^S$

Proof. We proceed by induction on $\Sigma_S \Downarrow_S^{\overline{\tau}} \Sigma'_S$:

Rule S:AM-Reflection By Rule S:AM-Reflection we have $\Sigma_S \Downarrow_S^{\varepsilon} \Sigma_S$ with $\Sigma_S = \Sigma'_S$.

I - III We derive $\Sigma_{B+S+R} \Downarrow_{B+S+R}^{\overline{\tau}'} \Sigma'_{B+S+R}$ by Rule AM-Reflection-V145 and thus $\Sigma_{B+S+R} = \Sigma'_{B+S+R}$.
By construction and 2) we have $\Sigma'_S \approx \Sigma'_{B+S+R}$ by Rule V145-V4:Single-Base.
Since $\varepsilon \restriction^S = \varepsilon$ we are finished.

Rule S:AM-Single Then we have $\Sigma_S \Downarrow_S^{\overline{\tau}} \Sigma''_S$ and $\Sigma''_S \overset{\tau}{\dashrightarrow}_S \Sigma'_R$.
We need to show
I $\Sigma_{B+S+R} \Downarrow_{B+S+R}^{\overline{\tau}'\cdot\tau'} \Sigma'_{B+S+R}$ and
II $\Sigma'_S \approx \Sigma'_{B+S+R}$ by Rule V145-V4:Single-Base and
III $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \restriction^S$
We apply the IH on $\Sigma_S \Downarrow_S^{\overline{\tau}} \Sigma''_S$ we get
I' $\Sigma_{B+S+R} \Downarrow_{B+S+R}^{\overline{\tau}'} \Sigma''_{B+S+R}$ and
II' $\Sigma''_S \approx \Sigma''_{B+S+R}$ by Rule V145-V4:Single-Base and
IV' $\overline{\tau} = \overline{\tau}' \restriction^S$

By Rule V145-V4:Single-Base we have:

$$\begin{aligned}\Sigma''_{\mathsf{S}} &= \Sigma'''_{\mathsf{S}} \cdot \langle p, ctr, \sigma, n\rangle\\ \Sigma''_{\mathsf{B+S+R}} &= \Sigma'''_{\mathsf{B+S+R}} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\\ \Sigma'''_{\mathsf{S}} &\sim \Sigma'''_{\mathsf{B+S+R}}\end{aligned}$$

We continue by inversion on $\Sigma''_{\mathsf{S}} \overset{\tau}{\leadsto}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$:

Rule S:AM-Rollback The case is analogous to the corresponding case in Lemma 88 (V45 AM: Completeness w.r.t V4 and projection) using Rule AM-v4-Rollback-V145.

Rule S:AM-Context We then have $\langle p, ctr, \sigma, n\rangle \overset{\tau}{\leadsto}_{\mathsf{S}} \overline{\Phi}'_{\mathsf{S}}$ and $n > 0$.

By $\Sigma''_{\mathsf{S}} \approx \Sigma''_{\mathsf{B+S+R}}$ we know that Rule AM-Context-V145 applies for the step $\Sigma''_{\mathsf{B+S+R}} \overset{\tau'}{\leadsto}_{\mathsf{B+S+R}} \Sigma'_{\mathsf{B+S+R}}$.

We now need to find a derivation for the step $\langle p, ctr', \sigma, \mathbb{R}, n\rangle \overset{\tau'}{\leadsto}_{\mathsf{B+S+R}} \overline{\Phi}'_{\mathsf{B+S+R}}$ according to Rule AM-Context-V145.

We proceed by inversion on $\langle p, ctr, \sigma, n\rangle \overset{\tau}{\leadsto}_{\mathsf{S}} \overline{\Phi}'_{\mathsf{S}}$:

Rule S:AM-NoBranch Then $n > 0$ and $\langle p, ctr, \sigma, n\rangle \overset{\tau}{\leadsto}_{\mathsf{S}} \overline{\Phi}'_{\mathsf{S}}$ by $\sigma \xrightarrow{\tau} \sigma'$.

Furthermore, $\Sigma'_{\mathsf{S}}.n = n - 1$.

We now do a case analysis on the instruction $p(\sigma(\mathbf{pc}))$:

$p(\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, l$ Then, a speculative transaction of V4 with *id* is started using Rule B:AM-Spec through Rule AM-v1-step-V145 and a new instance $\overline{\Phi}'_{\mathsf{B+S+R}}$ was pushed on top of the stack.

The rest of the case is analogous to the corresponding case in Lemma 108 (V14: V4 step).

$p(\sigma(\mathbf{pc})) = \mathbf{ret\ and}\ \mathbb{R}\ \mathbf{is\ non\text{-}empty\ and}\ \mathbb{R}\ \mathbf{value\ is\ different\ to\ return\ address}$ Then, a speculative transaction of V5 with *id* is started using Rule R:AM-Ret-Spec through Rule AM-v5-step-V145 and a new instance $\Phi'_{\mathsf{B+R}}$ was pushed on top of the stack of $\Sigma''_{\mathsf{B+R}}$.

The rest of the case is analogous to the corresponding case in Lemma 88 (V45 AM: Completeness w.r.t V4 and projection).

$p(\sigma(\mathbf{pc})) = \mathbf{ret\ and}\ \mathbb{R}\ \mathbf{is\ empty\ or}\ \mathbb{R}\ \mathbf{is\ not\ different\ to\ return\ address}$ Since $n > 0$, the state can do a step using either Rule R:AM-Ret-Empty or Rule R:AM-Ret-Same through Rule AM-v5-step-V145 (Note that the meta parameter Z restricts the V4 semantics in the combined part).

The case is analogous to the corresponding case in Lemma 88 (V45 AM: Completeness w.r.t V4 and projection) together with the fact that $\restriction^B$ and $\restriction^S$ behave similar with speculative transactions generated by V5.

$p(\sigma(\mathbf{pc})) = \mathbf{call}\ f$ Since $n > 0$, the state can do a step using either Rule R:AM-Call or Rule R:AM-Call-Full through Rule AM-v5-step-V15. The case is analogous to the corresponding case in Lemma 88 (V45 AM: Completeness w.r.t V4 and projection).

otherwise Then we can either use Rule AM-NoBranch through Rule AM-v1-step-V145, Rule S:AM-NoBranch through Rule AM-v4-step-V145 or Rule R:AM-NoBranch through Rule AM-v5-step-V145.

Because of Lemma 150 (V145 AM: Confluence), we know that it does not matter which rule we use, which means we can use the same rule as for v5 do derive the step.

The rest of the proof is analogous to the corresponding case in Lemma 88 (V45 AM: Completeness w.r.t V4 and projection).

otherwise These rules include Rule S:AM-barr, Rule S:AM-barr-spec, Rule S:AM-General and Rule S:AM-Store-Spec. Since the rules of V4 are included in the combined semantics and $\Sigma_{\mathsf{S}} \approx \Sigma_{\mathsf{B+S+R}}$, we can use the corresponding rule in the combined semantics by Confluence or delegate back to V4 by Rule AM-v4-step-V145.

This means we can always do the same step in the combined as in the V4 semantics.

□

N.3 Projection to V5

Theorem 40 (V145: Relating V5 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\mathcal{A}}_{\mathsf{R}}(p) = Beh^{\mathsf{B+S+R}}_{\mathcal{A}}(p)\restriction^R$.*

Proof. We prove the two directions separately:

⇐ Assume that $(p, \sigma) \Subset^{\omega}_{\mathsf{B+S+R}} \overline{\tau} \in Beh^{\mathsf{B+S+R}}_{\mathcal{A}}(p)$.

The case is analogous to Theorem 24 (V45: Relating V4 with projection of combined) using Lemma 158 (V145: Soundness of the AM speculative semantics w.r.t. AM v5 semantics).

We can now conclude that $p, \sigma \Subset^{\omega}_{\mathsf{R}} \overline{\tau}\restriction^R \in Beh^{\mathcal{A}}_{\mathsf{B}}(p)$ by Rule R:AM-Trace.

⇒ Assume that $(p, \sigma) \Subset^{\omega}_{\mathsf{R}} \overline{\tau} \in Beh^{\mathcal{A}}_{\mathsf{R}}(p)$.

The case is analogous to Theorem 24 (V45: Relating V4 with projection of combined) using Lemma 159 (V145 AM: Completeness w.r.t V4 and projection).
We thus have $(p,\sigma)\ \text{👻}^{\omega}_{\mathrm{B+S+R}}\ \overline{\tau}' \in Beh^{\mathrm{B+S+R}}_{\mathcal{A}}(p)$ with $\overline{\tau}'\restriction^{R} = \overline{\tau}$.

□

Lemma 158 (V145: Soundness of the AM speculative semantics w.r.t. AM v5 semantics)**.** *If*

(1) $\Sigma_{\mathrm{R}} \approx \Sigma_{\mathrm{B+S+R}}$ *and*
(2) $\Sigma_{\mathrm{B+S+R}} \Downarrow^{\overline{\tau}}_{\mathrm{B+S+R}} \Sigma'_{\mathrm{B+S+R}}$

Then exists Σ'_{R} *such that*

I $\Sigma'_{\mathrm{R}} \approx \Sigma'_{\mathrm{B+S+R}}$ *and*
II if $\Sigma'_{\mathrm{R}} \approx \Sigma'_{\mathrm{B+S+R}}$ *by Rule V145-V5:Single-Base then* $\Sigma_{\mathrm{R}} \Downarrow^{\overline{\tau}\restriction^{R}}_{\mathrm{R}} \Sigma'_{\mathrm{R}}$ *and*
III if $\Sigma'_{\mathrm{R}} \approx \Sigma'_{\mathrm{B+S+R}}$ *by Rule V145-V5:Single-Speculation-Start then* $\Sigma_{\mathrm{R}} \Downarrow^{\overline{\tau}\restriction^{R}}_{\mathrm{R}} \Sigma'_{\mathrm{R}}$ *and*
IV if $\Sigma'_{\mathrm{R}} \approx \Sigma'_{\mathrm{B+S+R}}$ *by Rule V145-V5:Single-Speculation-Diff then* $\Sigma_{\mathrm{R}} \Downarrow^{helper_R(\overline{\tau},i)}_{\mathrm{R}} \Sigma'_{\mathrm{R}}$*, where* $i = ctr'$ *by unpacking* $\Sigma'_{\mathrm{B+S+R}}$ *according to Rule V145-V5:Single-Speculation-Diff.*

Proof. By Induction on $\Sigma_{\mathrm{B+S+R}} \Downarrow^{\overline{\tau}}_{\mathrm{B+S+R}} \Sigma'_{\mathrm{B+S+R}}$.

Rule AM-Reflection-V145 Then we have $\Sigma_{\mathrm{B+S+R}} \Downarrow^{\varepsilon}_{\mathrm{B+S+R}} \Sigma_{\mathrm{B+S+R}}$ with $\Sigma'_{\mathrm{B+S+R}} = \Sigma_{\mathrm{B+S+R}}$ and by Rule AM-Reflection-V145 we have

I $\Sigma'_{\mathrm{R}} \approx \Sigma'_{\mathrm{B+S+R}}$
II $\Sigma_{\mathrm{R}} \Downarrow^{\varepsilon\restriction^{R}}_{\mathrm{R}} \Sigma'_{\mathrm{R}}$ with $\Sigma_{\mathrm{R}} = \Sigma'_{\mathrm{R}}$.
III $\Sigma_{\mathrm{R}} \Downarrow^{helper_R(\varepsilon,i)}_{\mathrm{R}} \Sigma'_{\mathrm{R}}$ with $\Sigma_{\mathrm{R}} = \Sigma'_{\mathrm{R}}$.
Note, that the initial relation $\Sigma_{\mathrm{R}} \approx \Sigma_{\mathrm{B+S+R}}$ does not change.

Rule AM-Single-V145 We have $\Sigma_{\mathrm{B+S+R}} \Downarrow^{\overline{\tau}''}_{\mathrm{B+S+R}} \Sigma''_{\mathrm{B+S+R}}$ with $\Sigma''_{\mathrm{B+S+R}} \overset{\tau}{\dashrightarrow}_{\mathrm{B+S+R}} \Sigma'_{\mathrm{B+S+R}}$.
We now apply IH on $\Sigma''_{\mathrm{B+S+R}} \Downarrow^{\overline{\tau}''}_{\mathrm{B+S+R}} \Sigma''_{\mathrm{B+S+R}}$ and get

(a) $\Sigma''_{\mathrm{R}} \approx \Sigma''_{\mathrm{B+S+R}}$
(b) if $\Sigma''_{\mathrm{R}} \approx \Sigma''_{\mathrm{B+S+R}}$ by Rule V145-V5:Single-Base then $\Sigma_{\mathrm{R}} \Downarrow^{\overline{\tau}\restriction^{R}}_{\mathrm{R}} \Sigma''_{\mathrm{R}}$ and
(c) if $\Sigma''_{\mathrm{R}} \approx \Sigma''_{\mathrm{B+S+R}}$ by Rule V145-V5:Single-Speculation-Start then $\Sigma_{\mathrm{R}} \Downarrow^{\overline{\tau}\restriction^{R}}_{\mathrm{R}} \Sigma''_{\mathrm{R}}$ and
(d) if $\Sigma''_{\mathrm{R}} \approx \Sigma''_{\mathrm{B+S+R}}$ by Rule V145-V5:Single-Speculation-Diff $\Sigma_{\mathrm{R}} \Downarrow^{helper_S(\overline{\tau},j)}_{\mathrm{S}} \Sigma''_{\mathrm{R}}$, where $j = ctr'$ by unpacking $\Sigma''_{\mathrm{B+S+R}}$ according to Rule V145-V5:Single-Speculation-Diff

We do a case distinction on $\approx$ in $\Sigma''_{\mathrm{R}} \approx \Sigma''_{\mathrm{B+S+R}}$:
Rule V145-V5:Single-Base We have

$$\Sigma_{\mathrm{R}} \Downarrow^{\overline{\tau}\restriction^{R}}_{\mathrm{R}} \Sigma''_{\mathrm{R}}$$
$$\Sigma''_{\mathrm{R}} = \Sigma'''_{\mathrm{R}} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle_{\overline{\rho}}$$
$$\Sigma''_{\mathrm{B+S+R}} = \Sigma'''_{\mathrm{B+S+R}} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle_{\overline{\rho}}$$
$$\Sigma'''_{\mathrm{R}} \sim \Sigma'''_{\mathrm{B+S+R}}$$

We now proceed by inversion on the derivation $\Sigma''_{\mathrm{B+S+R}} \overset{\tau}{\dashrightarrow}_{\mathrm{B+S+R}} \Sigma'_{\mathrm{B+S+R}}$:
Rule AM-v5-Rollback-V145 By (b), it can only be roll back of V1 and only be the topmost state.
Furthermore, this means that $n = 0$.
Then $\Sigma''_{\mathrm{R}} \overset{\mathtt{rlb}_{\mathrm{R}}\ ctr}{\dashrightarrow}_{\mathrm{R}} \Sigma'_{\mathrm{R}}$ by Rule R:AM-Rollback, since n is equal between the two states. The rest of the case is analogous to Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).
Rule AM-v1-Rollback-V145 Since $\Sigma''_{\mathrm{R}} \approx \Sigma''_{\mathrm{B+S+R}}$ by Rule V145-V5:Single-Base, there cannot be a roll back of V1.
Rule AM-v4-Rollback-V145 Since $\Sigma''_{\mathrm{R}} \approx \Sigma''_{\mathrm{B+S+R}}$ by Rule V145-V5:Single-Base, there cannot be a roll back of V4.
Rule AM-Context-V145 We have $\Phi_{\mathrm{B+S+R}} \overset{\tau}{\dashrightarrow}_{\mathrm{B+S+R}} \overline{\Phi}'_{\mathrm{B+S+R}}$.
We now use inversion on $\Phi_{\mathrm{B+S+R}} \overset{\tau}{\dashrightarrow}_{\mathrm{B+S+R}} \overline{\Phi}_{\mathrm{B+S+R}}$:
Rule AM-v1-step-V145 Then we have $\Phi_{\mathrm{B+S+R}}\restriction^{B} \overset{\tau}{\dashrightarrow}_{\mathrm{B}} \overline{\Phi}'_{\mathrm{B}}$.
By inversion on $\Phi_{\mathrm{B+S+R}}\restriction^{B} \overset{\tau}{\dashrightarrow}_{\mathrm{B}} \overline{\Phi}'_{\mathrm{B}}$ we get:
The cases are analogous to the corresponding cases Rule AM-v1-step-V14 in Lemma 131 (V15: Soundness of the AM speculative semantics w.r.t. AM v5 semantics) using Lemma 153 (V145: V5 step)

Rule AM-v4-step-V145 Then we have $\Phi_{B+S+R} \restriction^{S} \overset{\tau}{\Longrightarrow}_{S} \overline{\Phi}'_{S}$. The cases are analogous to the corresponding cases Rule AM-v4-step-V45 in Lemma 89 (V45: Soundness of the AM speculative semantics w.r.t. AM v5 semantics) using Lemma 153 (V145: V5 step)

Rule AM-v5-step-V145 Then we have $\Phi_{B+S+R} \restriction^{R} \overset{\tau}{\Longrightarrow}_{R} \overline{\Phi}'_{R}$.
The case is analogous to the corresponding case Rule AM-v5-step-V45 in Lemma 89 (V45: Soundness of the AM speculative semantics w.r.t. AM v5 semantics) combined with the fact that the rules of V5 cannot generate a $\texttt{start}_B$ *id*, $\texttt{start}_S$ *id*, $\texttt{rlb}_S$ *id* or $\texttt{rlb}_B$ *id* observation.

Rule V145-V4:Single-Speculation-Start We have:

$$
\begin{aligned}
\Sigma_R \Downarrow_R^{\overline{\tau}\restriction^R} \Sigma''_R \\
\Sigma''_R =& \Sigma'''_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \\
x =& v1 \vee v4 \\
\overline{\rho} =& \begin{cases} \texttt{pc}\ n \cdot \texttt{start}_B\ ctr & \text{if x = v1} \\ \texttt{bypass}\ n \cdot \texttt{start}_S\ ctr & \text{if x = v4} \end{cases} \\
\Sigma''_{B+S+R} =& \Sigma'''_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle_{\overline{\rho}} \\
\Sigma'''_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \sim& \Sigma'''_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle
\end{aligned}
$$

We now proceed by inversion on the derivation $\Sigma''_{B+S+R} \overset{\tau}{\Longrightarrow}_{B+S+R} \Sigma'_{B+S+R}$.

Rule AM-v1-Rollback-V145 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v4-Rollback-V145 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v5-Rollback-V145 Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-Context-V145 We have $\Phi_{B+S+R} \overset{\tau}{\Longrightarrow}_{B+S+R} \overline{\Phi}'_{B+S+R}$.

We now use inversion on $\Phi_{B+S+R} \overset{\tau}{\Longrightarrow}_{B+S+R} \overline{\Phi}_{B+S+R}$:

Rule AM-v1-step-V145 Then we have $\Phi_{B+S+R} \restriction^{B} \overset{\tau}{\Longrightarrow}_{B} \overline{\Phi}'_{B}$.

By inversion on $\Phi_{B+S+R} \restriction^{B} \overset{\tau}{\Longrightarrow}_{B} \overline{\Phi}'_{B}$ we get:

Rule B:AM-General By definition we have $\tau = \texttt{start}_B\ ctr'$. Since Rule B:AM-General does not modify the state, we have $\Sigma'_{B+S+R} = \Sigma''_{B+S+R\texttt{pc}\ n}$.
Then we choose $\Sigma'_R = \Sigma''_R$ and derive the step $\Sigma''_R \Downarrow_R^{\varepsilon} \Sigma'_R$ by Rule R:AM-Reflection.
The case is analogous to the corresponding case Rule B:AM-General in Lemma 131 (V15: Soundness of the AM speculative semantics w.r.t. AM v5 semantics).

otherwise Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v4-step-V145 Then we have $\Phi_{B+S+R} \restriction^{S} \overset{\tau}{\Longrightarrow}_{S} \overline{\Phi}'_{S}$.

By inversion on $\Phi_{B+S+R} \restriction^{S} \overset{\tau}{\Longrightarrow}_{S} \overline{\Phi}'_{S}$ we get:

Rule S:AM-General By definition we have $\tau = \texttt{start}_S\ ctr$.
Since Rule S:AM-General does not modify the state, we have $\Sigma'_{B+S+R} = \Sigma''_{B+S+R\texttt{bypass}\ n}$.
Then we choose $\Sigma'_R = \Sigma''_R$ and derive the step $\Sigma''_R \Downarrow_R^{\varepsilon} \Sigma'_R$ by Rule R:AM-Reflection.
The case is analogous to the corresponding case Rule S:AM-General in Lemma 89 (V45: Soundness of the AM speculative semantics w.r.t. AM v5 semantics).

otherwise Contradiction, because $\overline{\rho}$ is non-empty.

Rule AM-v5-step-V145 Contradiction, because $\overline{\rho}$ is non-empty and Rule R:AM-General does not work on $\texttt{start}_B$ *id* or $\texttt{start}_S$ observations.

Rule V145-V5:Single-Speculation-Diff We have:

$$
\begin{aligned}
\Sigma_R \Downarrow_R^{helper_R(\overline{\tau}, j)} \Sigma''_R \\
\Sigma''_R =& \Sigma'''_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \\
x =& v1 \vee v4 \\
\Sigma''_{B+S+R} =& \Sigma'''_{B+S+R} \cdot \langle p, ctr'', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr''', \sigma'', \mathbb{R}', n''\rangle^{x} \cdot \Sigma^{\dagger}_{B+S+R} \\
\Sigma'''_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \sim& \Sigma'''_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \\
j =& ctr'
\end{aligned}
$$

We now proceed by inversion on the derivation $\Sigma''_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \Sigma'_{B+S+R}$:

Rule AM-v5-Rollback-V145 This means a transaction is rolled back that was created later than the transaction with $id = j$.
Then we choose $\Sigma'_R = \Sigma''_R$ and derive the step $\Sigma''_R \Downarrow^{\varepsilon}_R \Sigma'_R$ by Rule R:AM-Reflection.
The case is analogous to the corresponding case Rule AM-v5-Rollback-V45 in Lemma 89 (V45: Soundness of the AM speculative semantics w.r.t. AM v5 semantics).

Rule AM-v1-Rollback-V145 or Rule AM-v4-Rollback-V145 There are two cases depending on the id of the rolled back transaction:

$id \neq j$ This means a transaction is rolled back that was created later than the transaction with $id = j$.
The case is analogous to the case of Rule AM-v5-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

$id = j$ Then we choose $\Sigma'_R = \Sigma''_R$ and derive the step $\Sigma''_R \Downarrow^{\varepsilon}_R \Sigma'_R$ by Rule R:AM-Reflection.
Since the transaction with $id = j$ was rolled back, we know that $\Sigma'_{B+S+R} = \Sigma'''_{B+S+R} \cdot \langle p, ctr''', \sigma, n\rangle$.
For the trace, we get $\overline{\tau} \cdot \texttt{rlb}_B\ j \restriction^S = helper_S(\overline{\tau}, j)$ and $\overline{\tau} \cdot \texttt{rlb}_R\ j \restriction^S = helper_S(\overline{\tau}, j)$ by definition of $\restriction^S$ and $id = j$.
The rest of the case is analogous to the corresponding case Rule AM-v5-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

otherwise Then we choose $\Sigma'_B = \Sigma''_B$ and derive the step $\Sigma''_B \Downarrow^{\varepsilon}_B \Sigma'_B$ by Rule B:AM-Reflection. Analogous to the corresponding case Rule AM-v4-Rollback-V45 in Lemma 85 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

□

Lemma 159 (V145 AM: Completeness w.r.t V4 and projection)**.** *If*

(1) $\Sigma_R \approx \Sigma_{B+S+R}$ *by Rule V145-V5:Single-Base and*
(2) $\Sigma_R \Downarrow^{\overline{\tau}}_R \Sigma'_R$

Then exists Σ'_{B+S+R} *such that*

I $\Sigma'_R \approx \Sigma'_{B+S+R}$ *by Rule V145-V5:Single-Base and*
II $\Sigma_{B+S+R} \Downarrow^{\overline{\tau}'}_{B+S+R} \Sigma'_{B+S+R}$ *and*
III $\overline{\tau} = \overline{\tau}' \restriction^R$

Proof. We proceed by induction on $\Sigma_R \Downarrow^{\overline{\tau}}_R \Sigma'_R$:

Rule R:AM-Reflection By Rule R:AM-Reflection we have $\Sigma_R \Downarrow^{\varepsilon}_R \Sigma_R$ with $\Sigma_R = \Sigma'_R$.

I - III We derive $\Sigma_{B+S+R} \Downarrow^{\overline{\tau}'}_{B+S+R} \Sigma'_{B+S+R}$ by Rule AM-Reflection-V145 and thus $\Sigma_{B+S+R} = \Sigma'_{B+S+R}$.
By construction and 2) we have $\Sigma'_R \approx \Sigma'_{B+S+R}$ by Rule V145-V5:Single-Base.
Since $\varepsilon \restriction^R = \varepsilon$ we are finished.

Rule R:AM-Single Then we have $\Sigma_R \Downarrow^{\overline{\tau}}_R \Sigma''_R$ and $\Sigma''_R \overset{\tau}{\dashrightarrow}_R \Sigma'_R$.
We need to show
I $\Sigma_{B+S+R} \Downarrow^{\overline{\tau}' \cdot \tau'}_{B+S+R} \Sigma'_{B+S+R}$ and
II $\Sigma'_R \approx \Sigma'_{B+S+R}$ by Rule V145-V5:Single-Base and
III $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \restriction^R$
We apply the IH on $\Sigma_R \Downarrow^{\overline{\tau}}_R \Sigma''_R$ we get
I' $\Sigma_{B+S+R} \Downarrow^{\overline{\tau}'}_{B+S+R} \Sigma''_{B+S+R}$ and
II' $\Sigma''_R \approx \Sigma''_{B+S+R}$ by Rule V145-V5:Single-Base and
IV' $\overline{\tau} = \overline{\tau}' \restriction^R$
By Rule V145-V5:Single-Base we have:

$$\begin{aligned} \Sigma''_R &= \Sigma'''_R \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \\ \Sigma''_{B+S+R} &= \Sigma'''_{B+S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \\ \Sigma'''_R &\sim \Sigma'''_{B+S+R} \end{aligned}$$

We continue by inversion on $\Sigma''_R \overset{\tau}{\dashrightarrow}_R \Sigma'_R$:

Rule R:AM-Rollback The case is analogous to the corresponding case in Lemma 90 (V45 AM: Completeness w.r.t V5 and projection) using Rule AM-v5-Rollback-V145.

Rule R:AM-Context We then have $\langle p, ctr, \sigma, \mathbb{R}, n\rangle \overset{\tau}{\dashrightarrow}_R \overline{\Phi}'_R$ and $n > 0$.

By $\Sigma''_R \approx \Sigma''_{B+S+R}$ we know that Rule AM-Context-V145 applies for the step $\Sigma''_{B+S+R} \overset{\tau'}{\dashrightarrow}_{B+S+R} \Sigma'_{B+S+R}$.

We now need to find a derivation for the step $\langle p, ctr', \sigma, \mathbb{R}, n\rangle \overset{\tau'}{\dashrightarrow}_{\mathsf{B+S+R}} \overline{\Phi}'_{\mathsf{B+S+R}}$ according to Rule AM-Context-V145.

We proceed by inversion on $\langle p, ctr, \sigma, \mathbb{R}, n\rangle \overset{\tau}{\dashrightarrow}_{\mathsf{R}} \overline{\Phi}'_{\mathsf{R}}$:

Rule R:AM-NoBranch Then $n > 0$ and $\langle p, ctr, \sigma, \mathbb{R}, n\rangle \overset{\tau}{\dashrightarrow}_{\mathsf{R}} \overline{\Phi}'_{\mathsf{R}}$ by $\sigma \xrightarrow{\tau} \sigma'$.

Furthermore, $\Sigma'_{\mathsf{R}}.n = n - 1$.

We now do a case analysis on the instruction $p(\sigma(\mathbf{pc}))$:

$p(\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, l$ Then, a speculative transaction of V4 with *id* is started using Rule B:AM-Spec through Rule AM-v1-step-V145 and a new instance $\overline{\Phi}'_{\mathsf{B+S+R}}$ was pushed on top of the stack.

The rest of the case is analogous to the corresponding case in Lemma 108 (V14: V4 step).

$p(\sigma(\mathbf{pc})) = \mathbf{store}\ x, e$ Then, a speculative transaction of V4 with *id* is started using Rule S:AM-Store-Spec through Rule AM-v4-step-V45 and a new instance $\overline{\Phi}'_{\mathsf{S+R}}$ was pushed on top of the stack.

The rest of the case is analogous to the corresponding case in Lemma 90 (V45 AM: Completeness w.r.t V5 and projection).

otherwise Then we can either use Rule AM-NoBranch through Rule AM-v1-step-V145, Rule S:AM-NoBranch through Rule AM-v4-step-V145 or Rule R:AM-NoBranch through Rule AM-v5-step-V145.

Because of Lemma 150 (V145 AM: Confluence), we know that it does not matter which rule we use, which means we can use the same rule as for v5 do derive the step.

The rest of the proof is analogous to the corresponding case in Lemma 90 (V45 AM: Completeness w.r.t V5 and projection).

otherwise These rules include Rule R:AM-barr, Rule R:AM-barr-spec, Rule R:AM-General, Rule R:AM-Ret-Spec, Rule R:AM-Ret-Same, Rule R:AM-Ret-Empty, Rule R:AM-Call and Rule R:AM-Call-Full.

Since the rules of V5 are included in the combined semantics and $\Sigma_{\mathsf{R}} \approx \Sigma_{\mathsf{B+S+R}}$, we can use the corresponding rule in the combined semantics by Confluence or delegate back to V5 by Rule AM-v5-step-V145.

This means we can always do the same step in the combined as in the V5 semantics.

□

Theorem 41 (V145: Relating Combined to non-speculative). *Let p be a program and ω be a speculation window. Then $Beh_{NS}(p) = Beh^{\mathsf{B+S+R}}_{\mathcal{A}}(p)\restriction_{ns}$.*

Proof. By Lemma 13 (V145 Relating speculative projections to non-speculative projection), we have $Beh^{\mathsf{B+S+R}}_{\mathcal{A}}(p)\restriction_{ns} = Beh^{\mathsf{B+S+R}}_{\mathcal{A}}(p)\restriction^{R}\restriction^{S}\restriction^{B}$.

By Theorem 40 (V145: Relating V5 with projection of combined), we have that $Beh^{\mathsf{B+S+R}}_{\mathcal{A}}(p)\restriction^{R} = Beh^{\mathcal{A}}_{\mathsf{R}}(p)$.

By Lemma 16 (V5: speculative-projections equal to non-speculative Projections), we get $Beh^{\mathcal{A}}_{\mathsf{R}}(p)\restriction^{S} = Beh^{\mathcal{A}}_{\mathsf{R}}(p)\restriction_{ns}$.

By Theorem 20 (V5AM: Behaviour of non-speculative semantics and AM semantics), we know that $Beh^{\mathcal{A}}_{\mathsf{R}}(p)\restriction_{ns} = Beh_{NS}(p)$.

Combining these facts we get:

$$
\begin{aligned}
&Beh^{\mathsf{B+S+R}}_{\mathcal{A}}(p)\restriction_{ns}\\
&= Beh^{\mathsf{B+S+R}}_{\mathcal{A}}(p)\restriction^{R}\restriction^{S}\restriction^{B}\\
&= Beh^{\mathcal{A}}_{\mathsf{R}}(p)\restriction^{S}\restriction^{B}\\
&= Beh^{\mathcal{A}}_{\mathsf{R}}(p)\restriction_{ns}\restriction^{B}\\
&= Beh_{NS}(p)\restriction^{B}\\
&= Beh_{NS}(p)
\end{aligned}
$$

and are finished. □

Corollary 6 (V145: SNI of combined preserves SNI of parts)**.** *Let p be a program and ω be a speculation window. If $p \vdash_{\mathsf{B+S+R}}$ SNI then $p \vdash_{\mathsf{S}}$ SNI, $p \vdash_{\mathsf{B}}$ SNI and $p \vdash_{\mathsf{R}}$ SNI.*

Proof. Assume $p \vdash_{\mathsf{B+S+R}}$ SNI and that there are $\sigma, \sigma' \in InitConf$ with $\sigma \sim_P \sigma'$ for some policy P and $(p, \sigma) \overset{O}{\multimap}_{NS} \overline{\tau}'$, $(p, \sigma') \overset{O}{\multimap}_{NS} \overline{\tau}'$.

We need to show that

(1) $(p, \sigma) \overset{\omega}{\multimap}_{\mathsf{S}} \overline{\tau}_s$, $(p, \sigma') \overset{\omega}{\multimap}_{\mathsf{S}} \overline{\tau}_s$
(2) $(p, \sigma) \overset{\omega}{\multimap}_{\mathsf{R}} \overline{\tau}_r$, $(p, \sigma') \overset{\omega}{\multimap}_{\mathsf{R}} \overline{\tau}_r$
(3) $(p, \sigma) \overset{\omega}{\multimap}_{\mathsf{B}} \overline{\tau}_b$, $(p, \sigma') \overset{\omega}{\multimap}_{\mathsf{B}} \overline{\tau}_b$

We show the proof for 1). The proof for 2) and 3) is analogous using Theorem 40 (V145: Relating V5 with projection of combined) and Theorem 38 (V145: Relating V1 with projection of combined).

Unfolding the definition of $p \vdash_{\mathsf{B+S+R}}$ SNI we get:

(1) if $\sigma \sim_P \sigma'$ and $(p, \sigma) \overset{O}{\multimap}_{NS} \overline{\tau}$, $(p, \sigma') \overset{O}{\multimap}_{NS} \overline{\tau}$, then $(p, \sigma) \overset{\omega}{\multimap}_{\mathsf{B+S+R}} \overline{\tau}_{bsr}$, $(p, \sigma') \overset{\omega}{\multimap}_{\mathsf{B+S+R}} \overline{\tau}_{bsr}$

After initialization we have $(p,\sigma)\ \text{👻}^{\omega}_{\mathsf{B+S+R}}\ \overline{\tau}_{bsr}$, $(p,\sigma')\ \text{👻}^{\omega}_{\mathsf{B+S+R}}\ \overline{\tau}_{bsr}$.

By Theorem 39 (V145: Relating V1 with projection of combined) we have $(p,\sigma)\ \text{👻}^{\omega}_{\mathsf{S}}\ \overline{\tau}_{bsr}\restriction^{S} \in Beh^{\mathcal{A}}_{\mathsf{S}}(p)$ and $(p,\sigma')\ \text{👻}^{\omega}_{\mathsf{S}}\ \overline{\tau}_{bsr}\restriction^{S} \in Beh^{\mathcal{A}}_{\mathsf{S}}(p)$, which is what we needed to show.

□

N.4 Relating Speculative and AM semantics

Lemma 160 (V145SE: Confluence). *If*

(1) $X_{B+S+R} \overset{\tau}{\rightsquigarrow}_{B+S+R}^{O_{B+S+R}} X'_{B+S+R}$ *and*

(2) $X_{B+S+R} \overset{\tau}{\rightsquigarrow}_{B+S+R}^{O_{B+S+R}} X''_{B+S+R}$ *derived by a different rule*

Then

(1) $X'_{B+S+R} = X_{B+S+R}$

Proof. Analogous to Lemma 150 (V145 AM: Confluence) □

Theorem 42 (V145: SNI). *For a program p, all oracles O with speculative window at most ω and for a security Policy P,* $p \vdash^{O}_{B+S+R}$ *SNIp iff* $p \vdash_{B+S+R}$ *SNIp.*

Proof. We prove the two directions separately:

(⇒) The proof proceeds analogous to Theorem 17 (S SNI) using (Lemma 172 (V145: Completeness Am semantics w.r.t. speculative semantics))

(⇐) The proof proceeds analogously to Theorem 17 (S SNI) using the Soundness (Lemma 166 (V145: Soundness Big-step))

□

Definition 73 (V145: Relation between AM and spec for all oracles). *We define two relations between AM and oracle semantics.* $\approx_{B+S+R}$ ∼

$$\boxed{\Sigma_{B+S+R} \approx_{B+S+R} X_{B+S+R}}$$

$$\frac{}{\emptyset \approx_{B+S+R} \emptyset}\ (V145{:}Base) \qquad \frac{\Sigma_{B+S+R} \sim X_{B+S+R}\restriction_{com} \quad INV(\Sigma_{B+S+R}, X_{B+S+R})}{\Sigma_{B+S+R} \approx_{B+S+R} X_{B+S+R}}\ (V145{:}Single\text{-}Base)$$

$$\frac{\begin{array}{cc}\Sigma_{B+S+R} \sim X_{B+S+R}\restriction_{com} & \Sigma''_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma'''_{B+S+R} \text{ where transaction with id ctr is rolled back} \\ X_{B+S+R} = X'_{B+S+R} \cdot \langle p, ctr, \sigma, h, n'' \rangle & x = (S, true) \vee (B, m \wedge m = \sigma(\mathbf{pc}) \\ \Sigma_{B+S+R} = \Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, n \rangle & INV(\Sigma_{B+S+R}, X_{B+S+R})\end{array}}{\Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma'', n' \rangle \cdot \Sigma_{B+S+R1} \approx_{B+S+R} X'_{B+S+R} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma, h, n''' \rangle^{x}}\ (V145{:}Single\text{-}OracleTrue)$$

$$\frac{\begin{array}{ccc}\Sigma''_{B+S+R} \sim X''_{B+S+R}\restriction_{com} & n' \geq 0 & \Sigma''_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma'''_{B+S+R} \text{ where transaction with id ctr is rolled back} \quad x = (S, true) \vee (B, m) \\ X_{B+S+R} = X'_{B+S+R} \cdot \langle p, ctr, \sigma, h, n'' \rangle & & \Sigma_{B+S+R} = \Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, n \rangle \quad INV(\Sigma_{B+S+R}, X_{B+S+R})\end{array}}{\Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma'', n' \rangle^{x} \cdot \Sigma_{B+S+R1} \approx_{B+S+R} X'_{B+S+R} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma'', h', 0 \rangle^{x} \cdot X_{B+S+R1}}\ (V145{:}Single\text{-}Transaction\text{-}Rollback)$$

$$\boxed{\Sigma_{B+S+R} \sim X_{B+S+R}}$$

$$\frac{}{\emptyset \sim \emptyset}\ (V145{:}Base) \qquad \frac{|\Sigma'_{B+S+R}| = |X'_{B+S+R}| \quad \Sigma'_{B+S+R} \sim X'_{B+S+R}}{\Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, n \rangle^{b} \sim X'_{B+S+R} \cdot \langle p, ctr', \sigma, h, n' \rangle^{b}}\ (V145{:}Single)$$

Lemma 161 (V145: Coincide on $\approx_{B+S+R}$ for projections). *If*

(1) $\Sigma_{B+S+R} \approx_{B+S+R} X_{B+S+R}$ *by Rule V145:Single-Base*

Then

(1) $\Sigma_{B+S+R}\restriction^{R} \approx_{R} X_{B+S+R}\restriction^{R}$ *by Rule Single-Base and*

(2) $\Sigma_{B+S+R}\restriction^{S} \approx_{S} X_{B+S+R}\restriction^{S}$ *by Rule Single-Base and*

(3) $\Sigma_{B+S+R}\restriction^{B} \approx_{B} X_{B+S+R}\restriction^{B}$ *by Rule V1:Single-Base*

Proof. The proof is analogous to Lemma 92 (V45: Coincide on $\approx_{S+R}$ for projections). □

Lemma 162 (V145: Coincide on ≅ for projections). *If*

(1) $\Sigma_{B+S+R} \cong X_{B+S+R}$

Then

(1) $\Sigma_{B+S+R}\restriction^{R} \cong X_{B+S+R}\restriction^{R}$ *and*

(2) $\Sigma_{B+S+R}\restriction^{S} \cong X_{B+S+R}\restriction^{S}$ *and*

(3) $\Sigma_{B+S+R}\restriction^{B} \cong X_{B+S+R}\restriction^{B}$

Proof. Analogous to Lemma 93 (V45: Coincide on ≅ for projections). □

Lemma 163 (V145: Initial states fulfill properties). *Let p be a program, ω be a speculation window and O be an oracle with speculation window at most ω. If*

(1) $\sigma, \sigma' \in InitConf$ *and*
(2) $\Sigma^{init}_{B+S+R}(p,\sigma)$ *and* $\Sigma^{init}_{B+S+R}(p,\sigma')$ *and*
(3) $X^{init}_{B+S+R}(p,\sigma)$ *and* $X^{init}_{B+S+R}(p,\sigma')$

Then

(1) $X^{init}_{B+S+R}(p,\sigma) \cong X^{init}_{B+S+R}(p,\sigma')$ *and*
(2) $\Sigma^{init}_{B+S+R}(p,\sigma) \cong \Sigma^{init}_{B+S+R}(p,\sigma')$ *and*
(3) $\Sigma^{init}_{B+S+R}(p,\sigma) \approx_{B+S+R} X^{init}_{B+S+R}(p,\sigma)$ *and* $\Sigma^{init}_{B+S+R}(p,\sigma') \approx_{B+S+R} X^{init}_{B+S+R}(p,\sigma')$ *by Rule V145:Single-Base and*

Proof. The proof is analogous to Lemma 45 (S: Initial states fulfill properties). □

Lemma 164 (V145AM: Single step preserves $\cong$). *If*

(1) $\Sigma_{B+S+R} \cong \Sigma^{\dagger}_{B+S+R}$ *and*
(2) $\Sigma_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \Sigma'_{S}$ *and* $\Sigma^{\dagger}_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \Sigma^{\dagger\dagger}_{B+S+R}$

Then

(1) $\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$

Proof. The proof is analogous to Lemma 43 (S AM: Single step preserves $\cong$). □

Lemma 165 (V145SE: Single step preserves $\cong$). *If*

(1) $X_{B+S+R} \cong X^{\dagger}_{B+S+R}$ *and*
(2) $X_{B+S+R} \overset{\tau}{\rightsquigarrow}^{O_{B+S+R}}_{B+S+R} X'_{B+S+R}$ *and* $X^{\dagger}_{B+S+R} \overset{\tau}{\rightsquigarrow}^{O_{B+S+R}}_{B+S+R} X^{\dagger\dagger}_{B+S+R}$

Then

(1) $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ *and*

Proof. The proof is analogous to Lemma 44 (S SE: Single step preserves $\cong$). □

N.5 Soundness

Lemma 166 (V145: Soundness Big-step). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*
If

(1) $\sigma, \sigma' \in InitConf$ *and*
(2) $(p,\sigma) \text{🕱}^{\omega}_{B+S+R} \overline{\tau}$, $(p,\sigma') \text{🕱}^{\omega}_{B+S+R} \overline{\tau}$

Then for all prediction oracles O with speculation window at most ω.

I $(p,\sigma) \text{🕱}^{O}_{B+S+R} \overline{\tau}'$, $(p,\sigma) \text{🕱}^{O}_{B+S+R} \overline{\tau}'$

Proof. The proof is analogous to Lemma 46 (S: Soundness Am semantics w.r.t. speculative semantics) using Lemma 163 (V145: Initial states fulfill properties) to show that our initial states fulfill all the premises for Lemma 167 (V145: Soundness Am semantics w.r.t. speculative semantics with new relation between states). □

Lemma 167 (V145: Soundness Am semantics w.r.t. speculative semantics with new relation between states). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*
If

(1) $\Sigma_{B+S+R} \cong \Sigma^{\dagger}_{B+S+R}$
(2) $X_{B+S+R} \cong X^{\dagger}_{B+S+R}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma^{*}_{B+S+R} \approx_{B+S+R} X_{B+S+R}$ *and* $\Sigma^{\dagger}_{B+S+R} \approx_{B+S+R} X^{\dagger}_{B+S+R}$
(4) $\Sigma_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma'_{B+S+R}$ *and* $\Sigma^{\dagger}_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma^{\dagger\dagger}_{B+S+R}$

Then for all prediction oracles O with speculation window at most ω.

I $X_{B+S+R} \overset{O}{\downarrow^{R}_{\overline{\tau}}} X'_{B+S+R}$, $X^{\dagger}_{B+S+R} \overset{O}{\downarrow^{R}_{\overline{\tau}''}} X^{\dagger\dagger}_{B+S+R}$
II $\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$
III $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{B+S+R} \approx_{B+S+R} X'_{B+S+R}$ *and* $\Sigma^{\dagger\dagger}_{B+S+R} \approx_{B+S+R} X^{\dagger\dagger}_{B+S+R}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. By Induction on $\Sigma_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma'_{B+S+R}$ and $\Sigma^{\dagger}_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma^{\dagger\dagger}_{B+S+R}$.

Rule AM-Reflection-V145 We have $\Sigma_{B+S+R} \Downarrow^{\varepsilon}_{B+S+R} \Sigma'_{B+S+R}$ and $\Sigma^{\dagger}_{B+S+R} \Downarrow^{\varepsilon}_{B+S+R} \Sigma''_{B+S+R}$, where $\Sigma'_{B+S+R} = \Sigma_{B+S+R}$ and $\Sigma''_{B+S+R} = \Sigma^{\dagger}_{B+S+R}$.
We choose $\Sigma'_{B+S+R} = \Sigma'_{B+S+R}$ and $\Sigma^{\dagger\dagger}_{B+S+R} = \Sigma''_{B+S+R}$.
We further use Rule V145-SE:Reflection to derive $X_{B+S+R} \overset{O}{\downarrow}{}^{R}_{\varepsilon} X'_{B+S+R}$, $X^{\dagger}_{B+S+R} \overset{O}{\downarrow}{}^{R}_{\varepsilon} X^{\dagger\dagger}_{B+S+R}$ with $X'_{B+S+R} = X_{B+S+R}$ and $X^{\dagger\dagger}_{B+S+R} = X^{\dagger}_{B+S+R}$. We now trivially satisfy all conclusions.

Rule AM-Single-V145 We have $\Sigma_{B+S+R} \Downarrow^{\overline{\tau}''}_{B+S+R} \Sigma''_{B+S+R}$ with $\Sigma''_{B+S+R} \overset{\tau}{\twoheadrightarrow}_{B+S+R} \Sigma'_{B+S+R}$ and $\Sigma^{\dagger}_{B+S+R} \Downarrow^{\overline{\tau}''}_{B+S+R} \Sigma^{*}_{B+S+R}$ and $\Sigma''_{B+S+R} \overset{\tau}{\twoheadrightarrow}_{B+S+R} \Sigma^{\dagger\dagger}_{B+S+R}$.
We now apply IH on $\Sigma_{B+S+R} \Downarrow^{\overline{\tau}''}_{B+S+R} \Sigma''_{B+S+R}$ and $\Sigma^{\dagger}_{B+S+R} \Downarrow^{\overline{\tau}''}_{B+S+R} \Sigma^{*}_{B+S+R}$ and get

(a) $X_{B+S+R} \overset{O}{\downarrow}{}^{R}_{\overline{\tau}'} X''_{B+S+R}$, $X^{\dagger}_{B+S+R} \overset{O}{\downarrow}{}^{R}_{\overline{\tau}''} X^{*}_{B+S+R}$
(b) $\Sigma''_{B+S+R} \cong \Sigma^{*}_{B+S+R}$
(c) $X''_{B+S+R} \cong X^{*}_{B+S+R}$ and $\overline{\rho}' = \varnothing$
(d) $\Sigma''_{B+S+R} \approx_{B+S+R} X''_{B+S+R}$ and $\Sigma^{*}_{B+S+R} \approx_{B+S+R} X^{*}_{B+S+R}$
(e) $\overline{\tau}' = \overline{\tau}''$

We do a case distinction on $\approx_{B+S+R}$ in $\Sigma''_{B+S+R} \approx_{B+S+R} X''_{B+S+R}$ and $\Sigma^{*}_{B+S+R} \approx_{B+S+R} X^{*}_{B+S+R}$ by inversion

Rule V145:Single-Base We thus have $\Sigma''_{B+S+R} \sim X''_{B+S+R}\restriction_{com}$ and $INV(\Sigma''_{B+S+R}, X''_{B+S+R})$ (Similar for Σ^{*}_{B+S+R} and X^{*}_{B+S+R}).
Similarly to Lemma 98 (V45: Soundness Am semantics w.r.t. speculative semantics with new relation between states) we can account for possible commits and get a state X^{**}_{B+S+R} such that $\Sigma''_{B+S+R} \approx_{B+S+R} X^{**}_{B+S+R}$ by Rule V145:Single-Base
We now proceed by inversion on the derivations $\Sigma''_{B+S+R} \overset{\tau}{\twoheadrightarrow}_{B+S+R} \Sigma'_{B+S+R}$ and $\Sigma^{*}_{B+S+R} \overset{\tau}{\twoheadrightarrow}_{B+S+R} \Sigma^{\dagger\dagger}_{B+S+R}$.
Note that by $\Sigma''_{B+S+R} \cong \Sigma^{*}_{B+S+R}$ and the fact the same traces are generated, we know that the same rule was used to derive the step.

Rule AM-Context-V145 We now have $\Phi'_{B+S+R} \overset{\tau}{\twoheadrightarrow}_{B+S+R} \overline{\Phi}'_{B+S+R}$ and $\Phi''_{B+S+R} \overset{\tau}{\twoheadrightarrow}_{B+S+R} \overline{\Phi}'''_{B+S+R}$ where $\Sigma''_{B+S+R} = \overline{\Phi}_{B+S+R} \cdot \Phi'_{B+S+R}$ and $\Sigma^{*}_{B+S+R} = \overline{\Phi}''_{B+S+R} \cdot \Phi''_{B+S+R}$.
Furthermore, $n > 0$ and note that all states point to the same instruction by b-d.

Rule AM-v5-step-V145 Then, we have $\Phi_{B+S+R}\restriction^{R} \overset{\tau}{\twoheadrightarrow}_{R} \overline{\Phi}'_{B+S+R}\restriction^{R}$
We use Lemma 168 (V145: V5 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule AM-v4-step-V145 Then, we have $\Phi_{B+S+R}\restriction^{S} \overset{\tau}{\twoheadrightarrow}_{S} \overline{\Phi}'_{B+S+R}\restriction^{S}$
We use Lemma 170 (V145: V4 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule AM-v1-step-V145 Then we have $\Phi_{B+S+R}\restriction^{B} \overset{\tau}{\twoheadrightarrow}_{B} \overline{\Phi}'_{B+S+R}\restriction^{B}$.
We use Lemma 169 (V145: V1 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule AM-v1-Rollback-V145 Contradiction, because $minWndw(X^{**}_{B+S+R}) > 0$ and $INV(\Sigma''_{B+S+R}, X^{**}_{B+S+R})$.
Rule AM-v4-Rollback-V145 Contradiction, because $minWndw(X^{**}_{B+S+R}) > 0$ and $INV(\Sigma''_{B+S+R}, X^{**}_{B+S+R})$.
Rule AM-v5-Rollback-V145 Contradiction, because $minWndw(X^{**}_{B+S+R}) > 0$ and $INV(\Sigma''_{B+S+R}, X^{**}_{B+S+R})$.

Rule V145:Single-OracleTrue We thus have

$$
\begin{aligned}
X''_{B+S+R} &= X_{B+S+R3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma, h, n''' \rangle^{false} \\
\Sigma''_{B+S+R} &= \Sigma_{B+S+R3} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle \cdot \Sigma_{B+S+R4} \\
X_{B+S+R} &= X_{B+S+R3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \\
\Sigma_{B+S+R} &= \Sigma_{B+S+R3} \cdot \langle p, ctr, \sigma, n \rangle \\
\Sigma_{B+S+R} &\sim X_{B+S+R}\restriction_{com}
\end{aligned}
$$

The form of X^{*}_{B+S+R} and Σ^{*}_{B+S+R} is analogous. We now apply inversion on $\Sigma''_{B+S+R} \overset{\tau}{\twoheadrightarrow}_{B+S+R} \Sigma'_{B+S+R}$.

Rule AM-Context-V145 We choose $X'_{B+S+R} = X''_{B+S+R}$ and $X^{\dagger\dagger}_{B+S+R} = X^{*}_{B+S+R}$.

I By IH a) and Rule V145-SE:Reflection
II By Lemma 164 (V145AM: Single step preserves $\cong$).
III Since $X'_{B+S+R} = X''_{B+S+R}$ and $X^{\dagger\dagger}_{B+S+R} = X^{*}_{B+S+R}$, we are finished using IH c).
IV We show that $X'_{B+S+R} \approx_{B+S+R} \Sigma'_{B+S+R}$ by Rule V145:Single-OracleTrue. The proof for $X^{\dagger\dagger}_{B+S+R} \approx \Sigma^{\dagger\dagger}_{B+S+R}$ is analogous.
Since we did not roll back the transaction with *id ctr'* we have that Σ_{B+S+R} does not change.
Since X_{B+S+R} remains the same as well, we have $\Sigma_{B+S+R} \sim X_{B+S+R}\restriction_{com}$ and $INV(\Sigma_{B+S+R}, X_{B+S+R}) X_{B+S+R}\restriction_{com}$.
Thus, we fulfill all premises for Rule V145:Single-OracleTrue.
V By IH e).

Rule AM-v5-Rollback-V145 There are two cases depending on the transaction *id* of the rolled back transaction:

id > ctr Then an inner transaction w.r.t our *ctr* transaction was finished. We choose $X'_{B+S+R} = X_{B+S+R}$ and $X^{\dagger\dagger}_{B+S+R} = X^{\dagger}_{B+S+R}$. The rest of the proof proceeds similar to the context case above.

id = ctr Most cases are similar to the context case above. Only the relation changes. We choose $X'_{B+S+R} = X_{B+S+R}$ and $X^{\dagger\dagger}_{B+S+R} = X^{\dagger}_{B+S+R}$. The case is analogous to the corresponding case in Lemma 167 (V145: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

Rule AM-v1-Rollback-V145 and Rule AM-v4-Rollback-V145 The case is analogous to the case Rule AM-v5-Rollback-V145 above.

Rule V145:Single-Transaction-Rollback We have

$$
\begin{aligned}
X''_{B+S+R} &= X_{B+S+R3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma'', h', 0 \rangle^{true} \cdot X_{B+S+R4} \\
\Sigma''_{B+S+R} &= \Sigma_{B+S+R3} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle^{true} \cdot \Sigma_{B+S+R4} \\
X_{B+S+R} &= X_{B+S+R3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \\
\Sigma_{B+S+R} &= \Sigma_{B+S+R3} \cdot \langle p, ctr, \sigma, n \rangle \\
\Sigma_{B+S+R} &\sim X_{B+S+R} \restriction_{com} \\
n' &\geq 0
\end{aligned}
$$

The form of X^{*}_{B+S+R} and Σ^{*}_{B+S+R} is analogous.
There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma''_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \Sigma'_{B+S+R}$ is not a rollback for *ctr*. The case is analogous to the corresponding case in Lemma 98 (V45: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

$n' = 0$ Then we know that $\Sigma''_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \Sigma'_{B+S+R}$ was created by either Rule AM-v1-Rollback-V145 or Rule AM-v5-Rollback-V145 and is a rollback for *ctr*.
We do the proof for Rule AM-v5-Rollback-V145, since the case for Rule AM-v1-Rollback-V145 and Rule AM-v4-Rollback-V145 is analogous.
The proof obligations are analogous to the corresponding case in Lemma 98 (V45: Soundness Am semantics w.r.t. speculative semantics with new relation between states) using Lemma 164 (V145AM: Single step preserves ≅) for II and Lemma 165 (V145SE: Single step preserves ≅) for III.

□

Lemma 168 (V145: V5 Soundness Single step)**.** *If*

(1) $\Sigma_{B+S+R} \approx_{B+S+R} X_{B+S+R}$ *and* $\Sigma^{\dagger}_{B+S+R} \approx_{B+S+R} X^{\dagger}_{B+S+R}$ *by Rule V145:Single-Base and*
(2) $\Sigma_{B+S+R} \cong \Sigma^{\dagger}_{B+S+R}$ *and* $X_{B+S+R} \cong X^{\dagger}_{B+S+R}$ *and*
(3) $\Phi_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \overline{\Phi}'_{B+S+R}$ *and* $\Phi^{\dagger}_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \overline{\Phi}^{\dagger\dagger}_{B+S+R}$ *by*
(4) $\Phi_{B+S+R} \restriction^{R} \overset{\tau}{\dashrightarrow}_{R} \overline{\Phi}'_{B+S+R} \restriction^{R}$ *and* $\Phi^{\dagger}_{B+S+R} \restriction^{R} \overset{\tau}{\dashrightarrow}_{R} \overline{\Phi}^{\dagger\dagger}_{B+S+R} \restriction^{R}$

Then

(1) $\Psi_{B+S+R} \overset{\tau', O_{B+S+R}}{\rightsquigarrow}_{B+S+R} \overline{\Psi}'_{B+S+R}$ *and* $\Psi^{\dagger}_{B+S+R} \overset{\tau', O_{B+S+R}}{\rightsquigarrow}_{B+S+R} \overline{\Psi}^{\dagger\dagger}_{B+S+R}$ *in combination with Context rule*
(2) $\Psi_{B+S+R} \restriction^{R} \overset{\tau, O}{\rightsquigarrow}_{R} \overline{\Psi}'_{B+S+R} \restriction^{R}$ *and* $\Psi^{\dagger}_{B+S+R} \restriction^{R} \overset{\tau, O}{\rightsquigarrow}_{R} \overline{\Psi}^{\dagger\dagger}_{B+S+R} \restriction^{R}$
(3) $\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$ *and* $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ *and*
(4) $\Sigma'_{B+S+R} \approx_{B+S+R} X'_{B+S+R}$ *and* $\Sigma^{\dagger\dagger}_{B+S+R} \approx_{B+S+R} X^{\dagger\dagger}_{B+S+R}$

Proof. By Rule V145:Single-Base and $X_{B+S+R} \cong X^{\dagger}_{B+S+R}$ we know that $minWndw(X_{B+S+R}) > 0$ (similar for $X^{\dagger}_{B+S+R}$). This means Rule V145-SE-Context applies. We now need to find a step $\Psi_{B+S+R} \overset{\tau'}{\dashrightarrow}_{B+S+R} \overline{\Psi}'_{B+S+R}$ and $\Psi^{\dagger}_{B+S+R} \overset{\tau'}{\dashrightarrow}_{B+S+R} \overline{\Psi}^{\dagger\dagger}_{B+S+R}$. Note that Rule V145-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 162 and Lemma 161 we get $\Sigma_{B+S+R} \restriction^{R} \approx_{R} X_{B+S+R} \restriction^{R}$ and $\Sigma_{B+S+R} \restriction^{R} \cong \Sigma^{\dagger}_{B+S+R} \restriction^{R}$.

Because of $\Phi_{B+S+R} \restriction^{R} \overset{\tau}{\dashrightarrow}_{R} \overline{\Phi}'_{B+S+R} \restriction^{R}$ and $\Phi^{\dagger}_{B+S+R} \restriction^{R} \overset{\tau}{\dashrightarrow}_{R} \overline{\Phi}^{\dagger\dagger}_{B+S+R} \restriction^{R}$ and Rule V145:Single-Base, we fulfill all premises for Lemma 79 (R: Soundness Single Step AM) and derive a step in the oracle semantics:

a) $\Sigma'_{B+S+R} \restriction^{R} \cong \Sigma^{\dagger\dagger}_{B+S+R} \restriction^{R}$ and $X'_{B+S+R} \restriction^{R} \cong X^{\dagger\dagger}_{B+S+R} \restriction^{R}$
b) $\Sigma'_{B+S+R} \restriction^{R} \approx_{R} X'_{B+S+R} \restriction^{R}$ and $\Sigma^{\dagger\dagger}_{B+S+R} \restriction^{R} \approx_{R} X^{\dagger\dagger}_{B+S+R} \restriction^{R}$
c) $\Psi_{B+S+R} \restriction^{R} \overset{\tau}{\dashrightarrow}_{R} \overline{\Psi}'_{B+S+R} \restriction^{R'}$ and $\Psi^{\dagger}_{B+S+R} \restriction^{R} \overset{\tau}{\dashrightarrow}_{R} \overline{\Psi}^{\dagger}_{B+S+R} \restriction^{R}$ the step of the oracle

Since we have $\Psi_{B+S+R}\restriction^{R} \overset{O}{\underset{R}{\rightsquigarrow}} \overline{\Psi}'_{B+S+R}\restriction^{R'}$ we can derive a step $\Psi_{B+S+R} \overset{\tau', O_{B+S+R}}{\underset{B+S+R}{\rightsquigarrow}} \overline{\Psi}'_{B+S+R}$ using Rule V145-SE:v5-step (or another applicable rule by Lemma 160 (V145SE: Confluence)).

Let us collect what we already have:

$$\begin{aligned} X'_{B+S+R} &= X''_{B+S+R} \cdot \overline{\Psi}'_{B+S+R} \\ \Sigma'_{B+S+R} &= \Sigma''_{B+S+R} \cdot \overline{\Phi}'_{B+S+R} \\ X^{\dagger\dagger}_{B+S+R} &= X^{*}_{B+S+R} \cdot \overline{\Psi}^{\dagger\dagger}_{B+S+R} \\ \Sigma^{\dagger\dagger}_{B+S+R} &= \Sigma^{*}_{B+S+R} \cdot \overline{\Phi}^{\dagger\dagger}_{B+S+R} \end{aligned}$$

We now need to show that $\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$ and $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ and $\Sigma'_{B+S+R} \approx_{B+S+R} X'_{B+S+R}$ and $\Sigma^{\dagger\dagger}_{B+S+R} \approx_{B+S+R} X^{\dagger\dagger}_{B+S+R}$ hold.

$\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$ and $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ The proof for $\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$ and $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ is analogous to the corresponding case in Lemma 99 (V45: V4 Soundness Single step).

$\Sigma'_{B+S+R} \approx_{B+S+R} X'_{B+S+R}$ and $\Sigma^{\dagger\dagger}_{B+S+R} \approx_{B+S+R} X^{\dagger\dagger}_{B+S+R}$ We want to show that $\Sigma'_{B+S+R} \approx_{B+S+R} X'_{B+S+R}$. The case for $\Sigma^{\dagger\dagger}_{B+S+R} \approx_{B+S+R} X^{\dagger\dagger}_{B+S+R}$ is analogous.

We first check if there is a transaction of V5 that needs to be rolled back in X'_{B+S+R}, since the speculation window of each instance was reduced.

This has to be done, because we only know that $minWndw(X'_{B+S+R}) > 0$ *before* we did the step. So it could happen that $minWndw(X'_{B+S+R}) = 0$ for some transaction of V1 that needs to be rolled back.

Transaction of V1 or V4 that needs to be rolled back in X'_{B+S+R} with window 0 The step made cannot create a new speculative instance of V5 that would be on top. This means we can derive all premises of Rule V145:Single-Transaction-Rollback just from $\Sigma_{B+S+R} \approx_{B+S+R} X_{B+S+R}$. Thus, we have $\Sigma'_{B+S+R} \approx_{B+S+R} X'_{B+S+R}$ by Rule V145:Single-Transaction-Rollback.

No V1 or V5 Transaction that needs to be rolled back in X'_{B+S+R} with window 0 Since the speculation window was reduced for all entries in X'_{B+S+R} and only for the topmost entry in Σ_{B+S+R} and we had $INV(\Sigma_{B+S+R}, X_{B+S+R})$ from $\Sigma_{B+S+R} \approx_{B+S+R} X_{B+S+R}$, we have $INV(\Sigma'_{B+S+R}, X'_{B+S+R})$ again. This reasoning extends to newly created instances by speculation as well.

We do a case distinction on $\approx_R$:

Rule Single-Base Analogous to the corresponding cases in Lemma 99 (V45: V4 Soundness Single step).

Rule Single-OracleTrue Then, the oracle predicted correctly. Analogous to the corresponding cases in Lemma 99 (V45: V4 Soundness Single step). Rule V145:Single-OracleTrue and have $\Sigma'_{B+S+R} \approx_{B+S+R} X'_{B+S+R}$.

Rule Single-Transaction-Rollback Then one of the instances in $X'_{B+S+R}\restriction^{R}$ needs to be rolled back.

This means the same instance in X'_{B+S+R} needs to be rolled back as well.

We do a case distinction if the instance is part of $\overline{\Psi}'_{B+S+R}$ or not. These cases are analogous to the corresponding cases in Lemma 99 (V45: V4 Soundness Single step).

□

Lemma 169 (V145: V1 Soundness Single step)**.** *If*

(1) $\Sigma_{B+S+R} \approx_{B+S+R} X_{B+S+R}$ *and* $\Sigma^{\dagger}_{B+S+R} \approx_{B+S+R} X^{\dagger}_{B+S+R}$ *by Rule V145:Single-Base and*
(2) $\Sigma_{B+S+R} \cong \Sigma^{\dagger}_{B+S+R}$ *and* $X_{B+S+R} \cong X^{\dagger}_{B+S+R}$ *and*
(3) $\Phi_{B+S+R} \overset{\tau}{\not\rightsquigarrow}_{B+S+R} \overline{\Phi}'_{B+S+R}$ *and* $\Phi^{\dagger}_{B+S+R} \overset{\tau}{\not\rightsquigarrow}_{B+S+R} \overline{\Phi}^{\dagger\dagger}_{B+S+R}$ *by*
(4) $\Phi_{B+S+R}\restriction^{B} \overset{\tau}{\not\rightsquigarrow}_{B} \overline{\Phi}'_{B+S+R}\restriction^{B}$ *and* $\Phi^{\dagger}_{B+S+R}\restriction^{B} \overset{\tau}{\not\rightsquigarrow}_{B} \overline{\Phi}^{\dagger\dagger}_{B+S+R}\restriction^{B}$

Then

(1) $\Psi_{B+S+R} \overset{\tau', O_{B+S+R}}{\underset{B+S+R}{\rightsquigarrow}} \overline{\Psi}'_{B+S+R}$ *and* $\Psi^{\dagger}_{B+S+R} \overset{\tau', O_{B+S+R}}{\underset{B+S+R}{\rightsquigarrow}} \overline{\Psi}^{\dagger\dagger}_{B+S+R}$ *in combination with Context rule*
(2) $\Psi_{B+S+R}\restriction^{B} \overset{\tau}{\underset{B}{\rightsquigarrow}}{}^{O} \overline{\Psi}'_{B+S+R}\restriction^{B}$ *and* $\Psi^{\dagger}_{B+S+R}\restriction^{B} \overset{\tau}{\underset{B}{\rightsquigarrow}}{}^{O} \overline{\Psi}^{\dagger\dagger}_{B+S+R}\restriction^{B}$
(3) $\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$ *and* $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ *and*
(4) $\Sigma'_{B+S+R} \approx_{B+S+R} X'_{B+S+R}$ *and* $\Sigma^{\dagger\dagger}_{B+S+R} \approx_{B+S+R} X^{\dagger\dagger}_{B+S+R}$

Proof. The proof is very similar to Lemma 168 (V145: V5 Soundness Single step). We only discuss the key aspects.

By Rule V145:Single-Base and $X_{B+S+R} \cong X^{\dagger}_{B+S+R}$ we know that $minWndw(X_{B+S+R}) > 0$ (similar for $X^{\dagger}_{B+S+R}$). This means Rule V145-SE-Context applies. We now need to find a step $\Psi_{B+S+R} \overset{\tau'}{\not\rightsquigarrow}_{B+S+R} \overline{\Psi}'_{B+S+R}$ and $\Psi^{\dagger}_{B+S+R} \overset{\tau'}{\not\rightsquigarrow}_{B+S+R} \overline{\Psi}^{\dagger\dagger}_{B+S+R}$. Note that Rule V145-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 162 and Lemma 161 we get $\Sigma_{B+S+R}\restriction^{B} \approx_{B} X_{B+S+R}\restriction^{B}$ and $\Sigma_{B+S+R}\restriction^{B} \cong \Sigma^{\dagger}_{B+S+R}\restriction^{B}$.

Combined with Rule V145:Single-Base, we fulfill all premises for Lemma 52 (B: Soundness Single Step AM) and derive a step in the oracle semantics:

a) $\Sigma'_{B+S+R}\restriction^B \cong \Sigma^{\dagger\dagger}_{B+S+R}\restriction^B$ and $X'_{B+S+R}\restriction^B \cong X^{\dagger\dagger}_{B+S+R}\restriction^B$
b) $\Sigma'_{B+S+R}\restriction^B \approx_B X'_{B+S+R}\restriction^B$ and $\Sigma^{\dagger\dagger}_{B+S+R}\restriction^B \approx_B X^{\dagger\dagger}_{B+S+R}\restriction^B$
c) $\Psi_{B+S+R}\restriction^B \xrightarrow{\tau}_B \overline{\Psi}'_{B+S+R}\restriction^{B'}$ and $\Psi^{\dagger}_{B+S+R}\restriction^B \xrightarrow{\tau}_B \overline{\Psi}^{\dagger}_{B+S+R}\restriction^B$ the step of the oracle

Since we have $\Psi_{B+S+R}\restriction^R \xrightarrow{\tau}_R \overline{\Psi}'_{B+S+R}\restriction^{R'}$ we can derive a step $\Psi_{B+S+R} \xrightarrow{\tau'}_{B+S+R} \overline{\Psi}'_{B+S+R}$ using Rule V145-SE:v1-step (or another applicable rule by Lemma 160 (V145SE: Confluence)).

Let us collect what we already have:

$$\begin{aligned}
X'_{B+S+R} &= X''_{B+S+R} \cdot \overline{\Psi}'_{B+S+R}\\
\Sigma'_{B+S+R} &= \Sigma''_{B+S+R} \cdot \overline{\Phi}'_{B+S+R}\\
X^{\dagger\dagger}_{B+S+R} &= X^{*}_{B+S+R} \cdot \overline{\Psi}^{\dagger\dagger}_{B+S+R}\\
\Sigma^{\dagger\dagger}_{B+S+R} &= \Sigma^{*}_{B+S+R} \cdot \overline{\Phi}^{\dagger\dagger}_{B+S+R}
\end{aligned}$$

We now need to show that $\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$ and $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ and $\Sigma'_{B+S+R} \approx_{B+S+R} X'_{B+S+R}$ and $\Sigma^{\dagger\dagger}_{B+S+R} \approx_{B+S+R} X^{\dagger\dagger}_{B+S+R}$ hold.

$\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$ **and** $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ The proof for $\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$ and $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ is analogous to the corresponding case in Lemma 99 (V45: V4 Soundness Single step).

$\Sigma'_{B+S+R} \approx_{B+S+R} X'_{B+S+R}$ **and** $\Sigma^{\dagger\dagger}_{B+S+R} \approx_{B+S+R} X^{\dagger\dagger}_{B+S+R}$ We first check if there is a transaction of V4 that needs to be rolled back in X'_{B+S+R}, since the speculation window of each instance was reduced.

This has to be done, because we only know that $minWndw(X'_{B+S+R}) > 0$ *before* we did the step. So it could happen that $minWndw(X'_{B+S+R}) = 0$ for some transaction of V4 or V5 that needs to be rolled back.

Transaction of V4 or V5 that needs to be rolled back in X'_{B+S+R} with window 0 The step made cannot create a new speculative instance of V4. This means we can derive all premises of Rule V145:Single-Transaction-Rollback just from $\Sigma_{B+S+R} \approx_{B+S+R} X_{B+S+R}$. Thus, we have $\Sigma'_{B+S+R} \approx_{B+S+R} X'_{B+S+R}$ by Rule V145:Single-Transaction-Rollback.

No V4 or V5 Transaction that needs to be rolled back in X'_{B+S+R} with window 0 Since the speculation window was reduced for all entries in X'_{B+S+R} and only for the topmost entry in Σ_{B+S+R} and we had $INV(\Sigma_{B+S+R}, X_{B+S+R})$ from $\Sigma_{B+S+R} \approx_{B+S+R} X_{B+S+R}$, we have $INV(\Sigma'_{B+S+R}, X'_{B+S+R})$ again. This reasoning extends to newly created instances by speculation as well.

We do a case distinction on $\approx_B$:

Rule V1:Single-Base Analogous to the corresponding case in Lemma 99 (V45: V4 Soundness Single step).

Rule V1:Single-OracleTrue Analogous to the corresponding case in Lemma 99 (V45: V4 Soundness Single step).

Rule V1:Single-Transaction-Rollback Then one of the instances in $X'_{B+S+R}\restriction^B$ needs to be rolled back.

This means the same instance in X'_{B+S+R} needs to be rolled back as well.

We do a case distinction if the instance is part of $\overline{\Psi}'_{B+S+R}$ or not.

These cases are analogous to the corresponding cases in Lemma 99 (V45: V4 Soundness Single step).

□

Lemma 170 (V145: V4 Soundness Single step)**.** *If*

(1) $\Sigma_{B+S+R} \approx_{B+S+R} X_{B+S+R}$ *and* $\Sigma^{\dagger}_{B+S+R} \approx_{B+S+R} X^{\dagger}_{B+S+R}$ *by Rule V145:Single-Base and*
(2) $\Sigma_{B+S+R} \cong \Sigma^{\dagger}_{B+S+R}$ *and* $X_{B+S+R} \cong X^{\dagger}_{B+S+R}$ *and*
(3) $\Phi_{B+S+R} \xrightarrow{\tau}_{B+S+R} \overline{\Phi}'_{B+S+R}$ *and* $\Phi^{\dagger}_{B+S+R} \xrightarrow{\tau}_{B+S+R} \overline{\Phi}^{\dagger\dagger}_{B+S+R}$ *by*
(4) $\Phi_{B+S+R}\restriction^S \xrightarrow{\tau}_S \overline{\Phi}'_{B+S+R}\restriction^S$ *and* $\Phi^{\dagger}_{B+S+R}\restriction^S \xrightarrow{\tau}_S \overline{\Phi}^{\dagger\dagger}_{B+S+R}\restriction^S$

Then

(1) $\Psi_{B+S+R} \xrightarrow{\tau', O_{B+S+R}}_{B+S+R} \overline{\Psi}'_{B+S+R}$ *and* $\Psi^{\dagger}_{B+S+R} \xrightarrow{\tau', O_{B+S+R}}_{B+S+R} \overline{\Psi}^{\dagger\dagger}_{B+S+R}$ *in combination with Context rule*
(2) $\Psi_{B+S+R}\restriction^S \xrightarrow{\tau, O}_S \overline{\Psi}'_{B+S+R}\restriction^S$ *and* $\Psi^{\dagger}_{B+S+R}\restriction^S \xrightarrow{\tau, O}_S \overline{\Psi}^{\dagger\dagger}_{B+S+R}\restriction^S$
(3) $\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$ *and* $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ *and*
(4) $\Sigma'_{B+S+R} \approx_{B+S+R} X'_{B+S+R}$ *and* $\Sigma^{\dagger\dagger}_{B+S+R} \approx_{B+S+R} X^{\dagger\dagger}_{B+S+R}$

Proof. By Rule V145:Single-Base and $X_{B+S+R} \cong X^{\dagger}_{B+S+R}$ we know that $minWndw(X_{B+S+R}) > 0$ (similar for $X^{\dagger}_{B+S+R}$). This means Rule V145-SE-Context applies. We now need to find a step $\Psi_{B+S+R} \xrightarrow{\tau'}_{B+S+R} \overline{\Psi}'_{B+S+R}$ and $\Psi^{\dagger}_{B+S+R} \xrightarrow{\tau'}_{B+S+R} \overline{\Psi}^{\dagger\dagger}_{B+S+R}$. Note that Rule V145-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 162 and Lemma 161 we get $\Sigma_{B+S+R}\restriction^S \approx_S X_{B+S+R}\restriction^S$ and $\Sigma_{B+S+R}\restriction^S \cong \Sigma^{\dagger}_{B+S+R}\restriction^S$.

Because of $\Phi_{B+S+R}\restriction^S \overset{\tau}{\Rightarrow}_S \overline{\Phi}'_{B+S+R}\restriction^S$ and $\Phi^{\dagger}_{B+S+R}\restriction^S \overset{\tau}{\Rightarrow}_S \overline{\Phi}^{\dagger\dagger}_{B+S+R}\restriction^S$ and Rule V145:Single-Base, we fulfill all premises for Lemma 48 (S: Soundness Single Step AM) and derive a step in the oracle semantics:

a) $\Sigma'_{B+S+R}\restriction^S \cong \Sigma^{\dagger\dagger}_{B+S+R}\restriction^S$ and $X'_{B+S+R}\restriction^S \cong X^{\dagger\dagger}_{B+S+R}\restriction^S$
b) $\Sigma'_{B+S+R}\restriction^S \approx_S X'_{B+S+R}\restriction^S$ and $\Sigma^{\dagger\dagger}_{B+S+R}\restriction^S \approx_S X^{\dagger\dagger}_{B+S+R}\restriction^S$
c) $\Psi_{B+S+R}\restriction^S \overset{\tau}{\Rightarrow}_S \overline{\Psi}'_{B+S+R}\restriction^{S'}$ and $\Psi^{\dagger}_{B+S+R}\restriction^S \overset{\tau}{\Rightarrow}_S \overline{\Psi}^{\dagger}_{B+S+R}\restriction^S$ the step of the oracle

Since we have $\Psi_{B+S+R}\restriction^S \overset{\tau}{\rightsquigarrow}^{O}_{S} \overline{\Psi}'_{B+S+R}\restriction^{S'}$ we can derive a step $\Psi_{B+S+R} \overset{\tau}{\rightsquigarrow}^{O_{B+S+R}}_{B+S+R} \overline{\Psi}'_{B+S+R}$ using Rule V145-SE:v4-step (or another applicable rule by Lemma 160 (V145SE: Confluence)).

Let us collect what we already have:

$$X'_{B+S+R} = X''_{B+S+R} \cdot \overline{\Psi}'_{B+S+R}$$
$$\Sigma'_{B+S+R} = \Sigma''_{B+S+R} \cdot \overline{\Phi}'_{B+S+R}$$
$$X^{\dagger\dagger}_{B+S+R} = X^{*}_{B+S+R} \cdot \overline{\Psi}^{\dagger\dagger}_{B+S+R}$$
$$\Sigma^{\dagger\dagger}_{B+S+R} = \Sigma^{*}_{B+S+R} \cdot \overline{\Phi}^{\dagger\dagger}_{B+S+R}$$

We now need to show that $\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$ and $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ and $\Sigma'_{B+S+R} \approx_{B+S+R} X'_{B+S+R}$ and $\Sigma^{\dagger\dagger}_{B+S+R} \approx_{B+S+R} X^{\dagger\dagger}_{B+S+R}$ hold.

The rest of the proof is analogous to Lemma 99 (V45: V4 Soundness Single step).

□

N.6 Completeness

Definition 74 (V145: Relation between AM and Spec for oracles that only mispredict). $\boxed{\Sigma_{B+S+R} \approx^{O_{am}}_{B+S+R} X_{B+S+R}}$

$$\frac{}{\varnothing \approx^{O_{am}}_{B+S+R} \varnothing}\ \textit{(V145:Base-Oracle)} \qquad \frac{\Sigma_{B+S+R} \sim X_{B+S+R}\restriction_{com} \quad INV2(\Sigma_{B+S+R}, X_{B+S+R}) \quad minWndw(X_{B+S+R}) > 0}{\Sigma_{B+S+R} \approx^{O_{am}}_{B+S+R} X_{B+S+R}}\ \textit{(V145:Single-Base-Oracle)}$$

$$\frac{\begin{array}{c}\Sigma''_{B+S+R} \sim X''_{B+S+R}\restriction_{com} \quad n' \geq 0 \quad \Sigma''_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma'''_{B+S+R}\ \textit{where transaction with id ctr is rolled back} \quad x = (S, true) \vee (B, m) \\ X_{B+S+R} = X'_{B+S+R} \cdot \langle p, ctr, \sigma, h, n'' \rangle \qquad \Sigma_{B+S+R} = \Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, n \rangle \qquad INV2(\Sigma_{B+S+R}, X_{B+S+R})\end{array}}{\Sigma'_{B+S+R} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle^x \cdot \Sigma_{S1} \approx^{O_{am}}_{B+S+R} X'_{B+S+R} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0 \rangle^x}\ \textit{(V145:Single-Transaction-Rollback-Oracle)}$$

Lemma 171 (V145: Coincide on $\approx^{O_{am}}_{B+S+R}$ for projections). *If*

(1) $\Sigma_{B+S+R} \approx^{O_{am}}_{B+S+R} X_{B+S+R}$ *by Rule V145:Single-Base*

Then

(1) $\Sigma_{B+S+R}\restriction^R \approx^{O_{am}}_{R} X_{B+S+R}\restriction^R$ *by Rule Single-Base-Oracle and*
(2) $\Sigma_{B+S+R}\restriction^S \approx^{O_{am}}_{S} X_{B+S+R}\restriction^S$ *by Rule Single-Base-Oracle and*
(3) $\Sigma_{B+S+R}\restriction^B \approx^{O_{am}}_{B} X_{B+S+R}\restriction^B$ *by Rule Single-Base-Oracle*

Proof. The proof is analogous to Lemma 101 (V45: Coincide on $\approx^{O_{am}}_{S+R}$ for projections). □

Definition 75 (V145: Constructing the AM Oracle). *We rely for the construction of the oracle O^{B+S+R}_{am} on the construction of its parts. Here Definition 58 (Constructing the AM Oracle), Definition 56 (Constructing the Oracle) and Definition 62 (R: Constructing the Oracle).*

Thus, we have: $O^{B+S+R}_{am} = (O_{amB}, O_{amS}, O_{amR})$ for the speculative oracle combined semantics.

Lemma 172 (V145: Completeness Am semantics w.r.t. speculative semantics). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, $\sigma, \sigma' \in InitConf$ be two initial configurations. If*

(1) $(p, \sigma) \Uparrow^{\omega}_{B+S+R} \overline{\tau}$ *and* $(p, \sigma') \Uparrow^{\omega}_{B+S+R} \overline{\tau}'$ *and*
(2) $\overline{\tau} \neq \overline{\tau}'$

Then there exists an oracle O such that

I $(p, \sigma) \Uparrow^{O}_{B+S+R} \overline{\tau}_1$ *and* $(p, \sigma') \Uparrow^{O}_{B+S+R} \overline{\tau}'_1$ *and*
II $\overline{\tau}_1 \neq \overline{\tau}'_1$

Proof. Let $\omega \in \mathbb{N}$ be a speculative window, $\sigma, \sigma' \in \mathit{InitConf}$ be two initial configurations. If

(1) (p,σ) $\text{🕮}^{\omega}_{\mathrm{B+S+R}}$ $\overline{\tau}$ and (p,σ') $\text{🕮}^{\omega}_{\mathrm{B+S+R}}$ $\overline{\tau}'$ and
(2) $\overline{\tau} \neq \overline{\tau}'$

By definition of $\text{🕮}^{\omega}_{\mathrm{B+S+R}}$ we have two final states $\Sigma_{\mathrm{B+S+R}F}$ and $\Sigma'_{\mathrm{B+S+R}F}$ such that $\Sigma^{init}_{\mathrm{B+S+R}}(p,\sigma) \Downarrow^{\overline{\tau}}_{\mathrm{B+S+R}} \Sigma_{\mathrm{B+S+R}F}$ $\Sigma^{init}_{\mathrm{S}} p, \sigma' \Downarrow^{\overline{\tau}'}_{\mathrm{B+S+R}} \Sigma'_{\mathrm{B+S+R}F}$. Combined with the fact that $\overline{\tau} \neq \overline{\tau}'$, it follows that there are speculative states $\Sigma^{*}_{\mathrm{B+S+R}}, \Sigma^{**}_{\mathrm{B+S+R}}, \Sigma^{\dagger}_{\mathrm{B+S+R}}, \Sigma^{\dagger\dagger}_{\mathrm{B+S+R}}$ and sequences of observations $\overline{\tau}, \overline{\tau}_{end}, \overline{\tau}'_{end}, \tau_{am}, \tau'_{am}$ such that $\tau_{am} \neq \tau'_{am}$, $\Sigma^{*}_{\mathrm{B+S+R}} \cong \Sigma^{\dagger}_{\mathrm{B+S+R}}$ and:

$$\Sigma^{init}_{\mathrm{B+S+R}}(p,\sigma) \Downarrow^{\overline{\tau}}_{\mathrm{B+S+R}} \Sigma^{*}_{\mathrm{B+S+R}} \xrightarrow{\tau_{am}}_{\mathrm{B+S+R}} \Sigma^{**}_{\mathrm{B+S+R}} \Downarrow^{\overline{\tau}_{end}}_{\mathrm{B+S+R}} \Sigma_{\mathrm{B+S+R}F}$$

$$\Sigma^{init}_{\mathrm{B+S+R}}(p,\sigma') \Downarrow^{\overline{\tau}}_{\mathrm{B+S+R}} \Sigma^{\dagger}_{\mathrm{B+S+R}} \xrightarrow{\tau'_{am}}_{\mathrm{B+S+R}} \Sigma^{\dagger\dagger}_{\mathrm{B+S+R}} \Downarrow^{\overline{\tau}'_{end}}_{\mathrm{B+S+R}} \Sigma'_{\mathrm{B+S+R}F}$$

We claim that there is a prediction oracle O with speculative window at most ω such that

a) $X^{init}_{\mathrm{B+S+R}}(p,\sigma)$ $\overset{O_{\mathrm{B+R}}}{\wr}{}^{\mathrm{B+S+R}}_{v}$ $X^{*}_{\mathrm{B+S+R}}$ and $X^{*}_{\mathrm{B+S+R}}.\sigma = \Sigma^{*}_{\mathrm{B+S+R}}.\sigma$ and $\mathit{INV2}(X^{*}_{\mathrm{B+S+R}}, \Sigma^{*}_{\mathrm{B+S+R}})$ and
b) $X^{init}_{\mathrm{B+S+R}}(p,\sigma')$ $\overset{O_{\mathrm{B+R}}}{\wr}{}^{\mathrm{B+S+R}}_{v}$ $X^{\dagger}_{\mathrm{B+S+R}}$ and $X^{\dagger}_{\mathrm{B+S+R}}.\sigma = \Sigma^{\dagger}_{\mathrm{B+S+R}}.\sigma$ and $\mathit{INV2}(X^{\dagger}_{\mathrm{B+S+R}}, \Sigma^{\dagger}_{\mathrm{B+S+R}})$
c) $X^{*}_{\mathrm{B+S+R}} \cong X^{\dagger}_{\mathrm{B+S+R}}$

We achieve this by applying Lemma 173 (V145: Stronger Soundness for a specific oracle and for specific executions) on the AM execution up to the point of the difference i.e., $\Sigma^{init}_{\mathrm{B+S+R}}(p,\sigma) \Downarrow^{\overline{\tau}}_{\mathrm{B+S+R}} \Sigma^{*}_{\mathrm{B+S+R}}$ and $\Sigma^{init}_{\mathrm{B+S+R}}(p,\sigma') \Downarrow^{\overline{\tau}}_{\mathrm{B+S+R}} \Sigma^{\dagger}_{\mathrm{B+S+R}}$.

The argument why $\Sigma^{*}_{\mathrm{B+S+R}} \approx^{O_{am}}_{\mathrm{B+S+R}} X^{*}_{\mathrm{B+S+R}}$ is derived by Rule V145:Single-Base-Oracle is analogous to Lemma 102 (V45: Completeness Am semantics w.r.t. speculative semantics).

We proceed by case analysis on the rule in $\xrightarrow{\ }_{\mathrm{B+S+R}}$ used to derive $\Sigma^{*}_{\mathrm{B+S+R}} \xrightarrow{\tau_{am}}_{\mathrm{B+S+R}} \Sigma^{**}_{\mathrm{B+S+R}}$. Because $\Sigma^{*}_{\mathrm{B+S+R}} \cong \Sigma^{\dagger}_{\mathrm{B+S+R}}$ and $\overline{\tau}_1 = \overline{\tau}'_1$, we know that the same rule was used in $\Sigma^{\dagger}_{\mathrm{B+S+R}} \xrightarrow{\tau'_{am}}_{\mathrm{R}} \Sigma^{\dagger\dagger}_{\mathrm{B+S+R}}$ as well.

Rule AM-v5-Rollback-V145 Contradiction. Because $\Sigma^{*}_{\mathrm{B+S+R}} \cong \Sigma^{\dagger}_{\mathrm{B+S+R}}$ we have for all instances $\Phi_1.\mathit{ctr} = \Phi'_1.\mathit{ctr}$.
Since the same instance would be rolled back, we have $\tau_{am} = \tau'_{am}$.

Rule AM-v1-Rollback-V145 and Rule AM-v4-Rollback-V145 Analogous to the case above.

Rule AM-Context-V145 By inversion on Rule AM-Context-V145 for the step $\Sigma^{*}_{\mathrm{B+S+R}} \xrightarrow{\tau_{am}}_{\mathrm{B+S+R}} \Sigma^{**}_{\mathrm{B+S+R}}$ we have $\Sigma^{*}_{\mathrm{B+S+R}} = \overline{\Phi}_{\mathrm{B+S+R}} \cdot \Phi_{\mathrm{B+S+R}}$ and $\Sigma^{**}_{\mathrm{B+S+R}} = \overline{\Phi}_{\mathrm{B+S+R}} \cdot \overline{\Phi}'_{\mathrm{B+S+R}}$ with $\Phi_{\mathrm{B+S+R}} \xrightarrow{\tau_{am}}_{\mathrm{B+S+R}} \overline{\Phi}'_{\mathrm{B+S+R}}$.
We now do inversion on $\Phi_{\mathrm{B+S+R}} \xrightarrow{\tau_{am}}_{\mathrm{B+S+R}} \overline{\Phi}'_{\mathrm{B+S+R}}$:

Rule AM-v5-step-V145 Then we have $\Phi_{\mathrm{B+S+R}} \restriction^{R} \xrightarrow{\tau}_{\mathrm{R}} \overline{\Phi}'_{\mathrm{S}} \restriction^{R}$.
The case is analogous to Lemma 80 (R: Completeness AM semantics w.r.t. speculative semantics) in the Rule R:AM-Context case.

Rule AM-v4-step-V145 Then we have $\Phi_{\mathrm{B+S+R}} \restriction^{S} \xrightarrow{\tau}_{\mathrm{S}} \overline{\Phi}'_{\mathrm{S}} \restriction^{S}$.
The case is analogous to Lemma 49 (Completeness Am semantics w.r.t. speculative semantics) in the Rule S:AM-Context case.

Rule AM-v1-step-V145 Then we have $\Phi_{\mathrm{B+S+R}} \restriction^{B} \xrightarrow{\tau}_{\mathrm{B}} \overline{\Phi}'_{\mathrm{B+S+R}} \restriction^{B}$.
The case is analogous to Lemma 54 (B: Completeness Am semantics w.r.t. speculative semantics) in the Rule B:AM-Context case.

This completes the proof of our claim.

□

Lemma 173 (V145: Stronger Soundness for a specific oracle and for specific executions)**.** *Specific executions means that there is a difference in the trace but before there is none. We use the oracle O_{am} as it is defined by Definition 75 (V145: Constructing the AM Oracle) for the given execution. If*

(1) $\Sigma_{\mathrm{B+S+R}} \cong \Sigma^{\dagger}_{\mathrm{B+S+R}}$
(2) $X_{\mathrm{B+S+R}} \cong X^{\dagger}_{\mathrm{B+S+R}}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma_{\mathrm{B+S+R}} \approx^{O_{am}} X_{\mathrm{B+S+R}}$ *and* $\Sigma^{\dagger}_{\mathrm{B+S+R}} \approx^{O_{am}} X^{\dagger}_{\mathrm{B+S+R}}$
(4) $\Sigma_{\mathrm{B+S+R}} \Downarrow^{\overline{\tau}}_{\mathrm{B+S+R}} \Sigma'_{\mathrm{B+S+R}}$ *and* $\Sigma^{\dagger}_{\mathrm{B+S+R}} \Downarrow^{\overline{\tau}}_{\mathrm{B+S+R}} \Sigma^{\dagger\dagger}_{\mathrm{B+S+R}}$

and our oracle is constructed in the way described above Then

I $X_{\mathrm{B+S+R}}$ $\overset{O_{\mathrm{B+R}}}{\downarrow}{}^{\mathrm{B+S+R}}_{\overline{\tau}'}$ $X'_{\mathrm{B+S+R}}, X^{\dagger}_{\mathrm{B+S+R}}$ $\overset{O}{\downarrow}{}^{\mathrm{R}}_{\overline{\tau}''}$ $X^{\dagger\dagger}_{\mathrm{B+S+R}}$
II $\Sigma'_{\mathrm{B+S+R}} \cong \Sigma^{\dagger\dagger}_{\mathrm{B+S+R}}$
III $X'_{\mathrm{B+S+R}} \cong X^{\dagger\dagger}_{\mathrm{B+S+R}}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{\mathrm{B+S+R}} \approx^{O_{am}} X'_{\mathrm{B+S+R}}$ *and* $\Sigma^{\dagger\dagger}_{\mathrm{B+S+R}} \approx^{O_{am}} X^{\dagger\dagger}_{\mathrm{B+S+R}}$

$V\ \overline{\tau}' = \overline{\tau}''$

Proof. Notice that the proof is very similar to Lemma 167 (V145: Soundness Am semantics w.r.t. speculative semantics with new relation between states). The only thing that is different is that (1) the specific oracle only mispredicts so there is one less case in the relation and (2) we have a different invariant for that specific oracle i.e., $INV2(\Sigma_{B+S+R}, X_{B+S+R})$

For these reasons we will only argue why $INV2(\Sigma^{\dagger}_{B+S+R}, X'_{B+S+R})$ holds in the different cases and leave the rest to the old soundness proof.

By Induction on $\Sigma_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma'_{B+S+R}$ and $\Sigma^{\dagger}_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma^{\dagger\dagger}_{B+S+R}$.

Rule AM-Reflection-V145 We have $\Sigma_{B+S+R} \Downarrow^{\varepsilon}_{B+S+R} \Sigma'_{B+S+R}$ and $\Sigma^{\dagger}_{B+S+R} \Downarrow^{\varepsilon}_{B+S+R} \Sigma''_{B+S+R}$, where $\Sigma'_{B+S+R} = \Sigma_{B+S+R}$ and $\Sigma''_{B+S+R} = \Sigma^{\dagger}_{B+S+R}$.

We choose $\Sigma'_{B+S+R} = \Sigma'_{B+S+R}$ and $\Sigma^{\dagger\dagger}_{B+S+R} = \Sigma''_{B+S+R}$.

We further use Rule V145-SE:Reflection to derive $X_{B+S+R} \overset{O_{B+R}}{\wr}{}^{B+S+R}_{\varepsilon} X'_{B+S+R}, X^{\dagger}_{B+S+R} \overset{O_{B+R}}{\wr}{}^{B+S+R}_{\varepsilon} X^{\dagger\dagger}_{B+S+R}$ with $X'_{B+S+R} = X_{B+S+R}$ and $X^{\dagger\dagger}_{B+S+R} = X^{\dagger}_{B+S+R}$. We now trivially satisfy all conclusions.

Rule AM-Single-V145 We have $\Sigma_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma''_{B+S+R}$ with $\Sigma''_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \Sigma'_{B+S+R}$ and $\Sigma^{\dagger}_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma^{*}_{B+S+R}$ and $\Sigma^{*}_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \Sigma^{\dagger\dagger}_{B+S+R}$.

We now apply IH on $\Sigma_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma''_{B+S+R}$ and $\Sigma^{\dagger}_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma^{*}_{B+S+R}$ and get

(a) $X_{B+S+R} \overset{O_{B+R}}{\wr}{}^{B+S+R}_{\overline{\tau}'} X''_{B+S+R}, X^{\dagger}_{B+S+R} \overset{O_{B+R}}{\wr}{}^{B+S+R}_{\overline{\tau}''} X^{*}_{B+S+R}$
(b) $\Sigma''_{B+S+R} \cong \Sigma^{*}_{B+S+R}$
(c) $X''_{B+S+R} \cong X^{*}_{B+S+R}$ and $\overline{\rho}' = \varnothing$
(d) $\Sigma''_{B+S+R} \approx^{O_{am}}_{B+S+R} X''_{B+S+R}$ and $\Sigma^{*}_{B+S+R} \approx^{O_{am}}_{B+S+R} X^{*}_{B+S+R}$
(e) $\overline{\tau}' = \overline{\tau}''$

We do a case distinction on $\approx^{O_{am}}_{B+S+R}$ in $\Sigma''_{B+S+R} \approx^{O_{am}}_{B+S+R} X''_{B+S+R}$ and $\Sigma^{*}_{B+S+R} \approx^{O_{am}}_{B+S+R} X^{*}_{B+S+R}$:

Rule V145:Single-Base-Oracle We thus have $\Sigma''_{B+S+R} \sim X''_{B+S+R}\restriction_{com}$, $minWndw(X''_{B+S+R}) > 0$ and $INV2(\Sigma''_{B+S+R}, X''_{B+S+R})$ (Similar for Σ^{*}_{B+S+R} and X^{*}_{B+S+R}).

We now proceed by inversion on the derivation $\Sigma''_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \Sigma'_{B+S+R}$:

Rule AM-v5-Rollback-V145 Contradiction, since $minWndw(X''_{S}) > 0$ and $INV2(\Sigma''_{B+S+R}, X''_{B+S+R})$.

Rule AM-v4-Rollback-V145 and Rule AM-v1-Rollback-V145 Analogous to above.

Rule AM-Context-V145 We have $\Phi_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \overline{\Phi}'_{B+S+R}$ and $n > 0$.

We now use inversion on $\Phi_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \overline{\Phi}_{B+S+R}$:

Rule AM-v5-step-V145 Then, we have $\Phi_{B+S+R}\restriction^{R} \overset{\tau}{\dashrightarrow}_{R} \overline{\Phi}'_{B+S+R}\restriction^{R}$
We use Lemma 168 (V145: V5 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule AM-v4-step-V145 Then, we have $\Phi_{B+S+R}\restriction^{S} \overset{\tau}{\dashrightarrow}_{S} \overline{\Phi}'_{B+S+R}\restriction^{S}$
We use Lemma 170 (V145: V4 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule AM-v1-step-V145 Then, we have $\Phi_{B+S+R}\restriction^{B} \overset{\tau}{\dashrightarrow}_{B} \overline{\Phi}'_{B+S+R}\restriction^{B}$
We use Lemma 169 (V145: V1 Soundness Single step) to derive a step in the oracle semantics and fulfill all conditions.

Rule V145:Single-Transaction-Rollback-Oracle We have

$$
\begin{aligned}
X''_{B+S+R} &= X_{B+S+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0 \rangle^{x} \cdot X_{B+S+R4} \\
\Sigma''_{B+S+R} &= \Sigma_{B+S+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle^{x} \cdot \Sigma_{B+S+R4} \\
X_{B+S+R} &= X_{B+S+R3} \cdot \langle p, ctr, \sigma, h, \mathbb{R}, n'' \rangle \\
\Sigma_{B+S+R} &= \Sigma_{B+S+R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \\
\Sigma_{B+S+R} &\sim X_{B+S+R}\restriction_{com} \\
INV2(\Sigma_{B+S+R}, X_{B+S+R}) & \\
n' &\geq 0
\end{aligned}
$$

The form of X^{*}_{B+S+R} and Σ^{*}_{B+S+R} is analogous.

Additionally we know that the transaction terminates in some state $\Sigma_{B+S+R} \Downarrow^{\overline{\tau}}_{B+S+R} \Sigma'''_{B+S+R}$. There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma''_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \Sigma'_{B+S+R}$ is not a roll back. Because Σ_{B+S+R} and X_{B+S+R} do not change, $INV2(\Sigma_{B+S+R}, X_{B+S+R})$ does not change as well.

$n' = 0$ Then we know that $\Sigma''_{B+S+R} \overset{\tau}{\dashrightarrow}_{B+S+R} \Sigma'_{B+S+R}$ was created by Rule AM-v5-Rollback-V145, Rule AM-v4-Rollback-V145 or Rule AM-v1-Rollback-V145 and is a rollback for *ctr*.

Notice, that the only difference to X_{B+S+R} and Σ_{B+S+R} is the updated *ctr*, because of the roll back. Updating the counter does not change the invariant *INV2*(). This means $INV2(\Sigma_{B+S+R}, X_{B+S+R})$ (with updated *ctr*) still holds.

□

Lemma 174 (V145: Stronger V5 Soundness Single step)**.** *If*

(1) $\Sigma_{B+S+R} \approx^{O_{am}}_{B+S+R} X_{B+S+R}$ *and* $\Sigma^{\dagger}_{B+S+R} \approx^{O_{am}}_{B+S+R} X^{\dagger}_{B+S+R}$ *by Rule V145:Single-Base-Oracle and*
(2) $\Sigma_{B+S+R} \cong \Sigma^{\dagger}_{B+S+R}$ *and* $X_{B+S+R} \cong X^{\dagger}_{B+S+R}$ *and*
(3) $\Phi_{B+S+R} \xrightarrow{\tau}_{B+S+R} \overline{\Phi}'_{B+S+R}$ *and* $\Phi^{\dagger}_{B+S+R} \xrightarrow{\tau}_{B+S+R} \overline{\Phi}^{\dagger\dagger}_{B+S+R}$ *by*
(4) $\Phi_{B+S+R}\restriction^{R} \xrightarrow{\tau}_{R} \overline{\Phi}'_{B+S+R}\restriction^{R}$ *and* $\Phi^{\dagger}_{B+S+R}\restriction^{R} \xrightarrow{\tau}_{R} \overline{\Phi}^{\dagger\dagger}_{B+S+R}\restriction^{R}$

Then

(1) $\Psi_{B+S+R} \overset{\tau', O_{B+S+R}}{\rightsquigarrow}_{B+S+R} \overline{\Psi}'_{B+S+R}$ *and* $\Psi^{\dagger}_{B+S+R} \overset{\tau', O_{B+S+R}}{\rightsquigarrow}_{B+S+R} \overline{\Psi}^{\dagger\dagger}_{B+S+R}$ *in combination with Context rule*
(2) $\Psi_{B+S+R} \overset{\tau, O_{B+S+R}}{\rightsquigarrow}_{B+S+R} \overline{\Psi}'_{B+S+R}$ *and* $\Psi^{\dagger}_{B+S+R} \overset{\tau, O_{B+S+R}}{\rightsquigarrow}_{B+S+R} \overline{\Psi}^{\dagger\dagger}_{B+S+R}$
(3) $\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$ *and* $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ *and*
(4) $\Sigma'_{B+S+R} \approx^{O_{am}}_{B+S+R} X'_{B+S+R}$ *and* $\Sigma^{\dagger\dagger}_{B+S+R} \approx^{O_{am}}_{B+S+R} X^{\dagger\dagger}_{B+S+R}$

Proof. By Rule V145:Single-Base-Oracle and $X_{B+S+R} \cong X^{\dagger}_{B+S+R}$ we know that $minWndw(X_{B+S+R}) > 0$ (similar for $X^{\dagger}_{B+S+R}$). This means Rule V145-SE-Context applies. We now need to find a step $\Psi_{B+S+R} \xrightarrow{\tau'}_{B+S+R} \overline{\Psi}'_{B+S+R}$ and $\Psi^{\dagger}_{B+S+R} \xrightarrow{\tau'}_{B+S+R} \overline{\Psi}^{\dagger\dagger}_{B+S+R}$. Note that Rule V145-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 162 and Lemma 171 we get $\Sigma_{B+S+R}\restriction^{R} \approx_{R} X_{B+S+R}\restriction^{R}$ and $\Sigma_{B+S+R}\restriction^{R} \cong \Sigma^{\dagger}_{B+S+R}\restriction^{R}$.

Because of $\Phi_{B+S+R}\restriction^{R} \xrightarrow{\tau}_{R} \overline{\Phi}'_{B+S+R}\restriction^{R}$ and $\Phi^{\dagger}_{B+S+R}\restriction^{R} \xrightarrow{\tau}_{R} \overline{\Phi}^{\dagger\dagger}_{B+S+R}\restriction^{R}$ and Rule V145:Single-Base-Oracle, we fulfill all premises for Lemma 81 (Stronger Soundness for a specific oracle and for specific executions) and derive a step in the oracle semantics:

a) $\Sigma'_{B+S+R}\restriction^{R} \cong \Sigma^{\dagger\dagger}_{B+S+R}\restriction^{R}$ and $X'_{B+S+R}\restriction^{R} \cong X^{\dagger\dagger}_{B+S+R}\restriction^{R}$
b) $\Sigma'_{B+S+R}\restriction^{R} \approx^{O_{am}}_{R} X'_{B+S+R}\restriction^{R}$ and $\Sigma^{\dagger\dagger}_{B+S+R}\restriction^{R} \approx^{O_{am}}_{R} X^{\dagger\dagger}_{B+S+R}\restriction^{R}$
c) $\Psi_{B+S+R}\restriction^{R} \xrightarrow{\tau}_{R} \overline{\Psi}'_{B+S+R}\restriction^{R'}$ and $\Psi^{\dagger}_{B+S+R}\restriction^{R} \xrightarrow{\tau}_{R} \overline{\Psi}^{\dagger}_{B+S+R}\restriction^{R}$ the step of the oracle

Since we have $\Psi_{B+S+R}\restriction^{R} \xrightarrow{\tau}_{R} \overline{\Psi}'_{B+S+R}\restriction^{R'}$ we can derive a step $\Psi_{B+S+R} \xrightarrow{\tau'}_{B+S+R} \overline{\Psi}'_{B+S+R}$ using Rule V145-SE:v5-step (or another applicable rule by Lemma 160 (V145SE: Confluence)).

Let us collect what we already have:

$$X'_{B+S+R} = X''_{B+S+R} \cdot \overline{\Psi}'_{B+S+R}$$
$$\Sigma'_{B+S+R} = \Sigma''_{B+S+R} \cdot \overline{\Phi}'_{B+S+R}$$
$$X^{\dagger\dagger}_{B+S+R} = X^{*}_{B+S+R} \cdot \overline{\Psi}^{\dagger\dagger}_{B+S+R}$$
$$\Sigma^{\dagger\dagger}_{B+S+R} = \Sigma^{*}_{B+S+R} \cdot \overline{\Phi}^{\dagger\dagger}_{B+S+R}$$

We now need to show that $\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$ and $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ and $\Sigma'_{B+S+R} \approx^{O_{am}}_{B+S+R} X'_{B+S+R}$ and $\Sigma^{\dagger\dagger}_{B+S+R} \approx^{O_{am}}_{B+S+R} X^{\dagger\dagger}_{B+S+R}$ hold.

The rest of the proof is analogous to Lemma 104 (V45: Stronger V4 Soundness Single step).

□

Lemma 175 (V145: Stronger V1 Soundness Single step)**.** *If*

(1) $\Sigma_{B+S+R} \approx^{O_{am}}_{B+S+R} X_{B+S+R}$ *and* $\Sigma^{\dagger}_{B+S+R} \approx^{O_{am}}_{B+S+R} X^{\dagger}_{B+S+R}$ *by Rule V145:Single-Base-Oracle and*
(2) $\Sigma_{B+S+R} \cong \Sigma^{\dagger}_{B+S+R}$ *and* $X_{B+S+R} \cong X^{\dagger}_{B+S+R}$ *and*
(3) $\Phi_{B+S+R} \xrightarrow{\tau}_{B+S+R} \overline{\Phi}'_{B+S+R}$ *and* $\Phi^{\dagger}_{B+S+R} \xrightarrow{\tau}_{B+S+R} \overline{\Phi}^{\dagger\dagger}_{B+S+R}$ *by*
(4) $\Phi_{B+S+R}\restriction^{B} \xrightarrow{\tau}_{B} \overline{\Phi}'_{B+S+R}\restriction^{B}$ *and* $\Phi^{\dagger}_{B+S+R}\restriction^{B} \xrightarrow{\tau}_{B} \overline{\Phi}^{\dagger\dagger}_{B+S+R}\restriction^{B}$

Then

(1) $\Psi_{B+S+R} \overset{\tau', O_{B+S+R}}{\rightsquigarrow}_{B+S+R} \overline{\Psi}'_{B+S+R}$ *and* $\Psi^{\dagger}_{B+S+R} \overset{\tau', O_{B+S+R}}{\rightsquigarrow}_{B+S+R} \overline{\Psi}^{\dagger\dagger}_{B+S+R}$ *in combination with Context rule*
(2) $\Psi_{B+S+R} \overset{\tau, O_{B+S+R}}{\rightsquigarrow}_{B+S+R} \overline{\Psi}'_{B+S+R}$ *and* $\Psi^{\dagger}_{B+S+R} \overset{\tau, O_{B+S+R}}{\rightsquigarrow}_{B+S+R} \overline{\Psi}^{\dagger\dagger}_{B+S+R}$
(3) $\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$ *and* $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ *and*
(4) $\Sigma'_{B+S+R} \approx^{O_{am}}_{B+S+R} X'_{B+S+R}$ *and* $\Sigma^{\dagger\dagger}_{B+S+R} \approx^{O_{am}}_{B+S+R} X^{\dagger\dagger}_{B+S+R}$

Proof. By Rule V145:Single-Base-Oracle and $X_{B+S+R} \cong X^{\dagger}_{B+S+R}$ we know that $minWndw(X_{B+S+R}) > 0$ (similar for $X^{\dagger}_{B+S+R}$). This means Rule V145-SE-Context applies. We now need to find a step $\Psi_{B+S+R} \xrightarrow{\tau'} \overline{\Psi}'_{B+S+R}$ and $\Psi^{\dagger}_{B+S+R} \xrightarrow{\tau'} \overline{\Psi}^{\dagger\dagger}_{B+S+R}$. Note that Rule V145-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 162 (V145: Coincide on $\cong$ for projections) and Lemma 171 (V145: Coincide on $\approx^{O_{am}}_{B+S+R}$ for projections) we get $\Sigma_{B+S+R}\restriction^R \approx^{O_{am}}_{R} X_{B+S+R}\restriction^R$ and $\Sigma_{B+S+R}\restriction^R \cong \Sigma^{\dagger}_{B+S+R}\restriction^R$.

Because of $\Phi_{B+S+R}\restriction^B \xrightarrow{\tau}_B \overline{\Phi}'_{B+S+R}\restriction^B$ and $\Phi^{\dagger}_{B+S+R}\restriction^B \xrightarrow{\tau}_B \overline{\Phi}^{\dagger\dagger}_{B+S+R}\restriction^B$ and Rule V145:Single-Base-Oracle, we fulfill all premises for Lemma 53 (B: Stronger Soundness for a specific oracle and for specific executions) and derive a step in the oracle semantics:

a) $\Sigma'_{B+S+R}\restriction^B \cong \Sigma^{\dagger\dagger}_{B+S+R}\restriction^B$ and $X'_{B+S+R}\restriction^B \cong X^{\dagger\dagger}_{B+S+R}\restriction^B$
b) $\Sigma'_{B+S+R}\restriction^B \approx^{O_{am}}_{B} X'_{B+S+R}\restriction^B$ and $\Sigma^{\dagger\dagger}_{B+S+R}\restriction^B \approx^{O_{am}}_{B} X^{\dagger\dagger}_{B+S+R}\restriction^B$
c) $\Psi_{B+S+R}\restriction^B \xrightarrow{\tau}_B \overline{\Psi}'_{B+S+R}\restriction^{B'}$ and $\Psi^{\dagger}_{B+S+R}\restriction^B \xrightarrow{\tau}_B \overline{\Psi}^{\dagger}_{B+S+R}\restriction^B$ the step of the oracle

Since we have $\Psi_{B+S+R}\restriction^B \xrightarrow{\tau}_B \overline{\Psi}'_{B+S+R}\restriction^{B'}$ we can derive a step $\Psi_{B+S+R} \xrightarrow{\tau'} \overline{\Psi}'_{B+S+R}$ using Rule V145-SE:v5-step (or another applicable rule by Lemma 160 (V145SE: Confluence)).

Let us collect what we already have:

$$
\begin{aligned}
X'_{B+S+R} &= X''_{B+S+R} \cdot \overline{\Psi}'_{B+S+R} \\
\Sigma'_{B+S+R} &= \Sigma''_{B+S+R} \cdot \overline{\Phi}'_{B+S+R} \\
X^{\dagger\dagger}_{B+S+R} &= X^{*}_{B+S+R} \cdot \overline{\Psi}^{\dagger\dagger}_{B+S+R} \\
\Sigma^{\dagger\dagger}_{B+S+R} &= \Sigma^{*}_{B+S+R} \cdot \overline{\Phi}^{\dagger\dagger}_{B+S+R}
\end{aligned}
$$

We now need to show that $\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$ and $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ and $\Sigma'_{B+S+R} \approx^{O_{am}}_{B+S+R} X'_{B+S+R}$ and $\Sigma^{\dagger\dagger}_{B+S+R} \approx^{O_{am}}_{B+S+R} X^{\dagger\dagger}_{B+S+R}$ hold.

The rest of the proof is analogous to Lemma 104 (V45: Stronger V4 Soundness Single step).

□

Lemma 176 (V145: Stronger V4 Soundness Single step)**.** *If*

(1) $\Sigma_{B+S+R} \approx^{O_{am}}_{B+S+R} X_{B+S+R}$ *and* $\Sigma^{\dagger}_{B+S+R} \approx^{O_{am}}_{B+S+R} X^{\dagger}_{B+S+R}$ *by Rule V145:Single-Base-Oracle and*
(2) $\Sigma_{B+S+R} \cong \Sigma^{\dagger}_{B+S+R}$ *and* $X_{B+S+R} \cong X^{\dagger}_{B+S+R}$ *and*
(3) $\Phi_{B+S+R} \xrightarrow{\tau} \overline{\Phi}'_{B+S+R}$ *and* $\Phi^{\dagger}_{B+S+R} \xrightarrow{\tau} \overline{\Phi}^{\dagger\dagger}_{B+S+R}$ *by*
(4) $\Phi_{B+S+R}\restriction^S \xrightarrow{\tau}_S \overline{\Phi}'_{B+S+R}\restriction^S$ *and* $\Phi^{\dagger}_{B+S+R}\restriction^S \xrightarrow{\tau}_S \overline{\Phi}^{\dagger\dagger}_{B+S+R}\restriction^S$

Then

(1) $\Psi_{B+S+R} \xrightarrow{\tau', O_{B+S+R}} \overline{\Psi}'_{B+S+R}$ *and* $\Psi^{\dagger}_{B+S+R} \xrightarrow{\tau', O_{B+S+R}} \overline{\Psi}^{\dagger\dagger}_{B+S+R}$ *in combination with Context rule*
(2) $\Psi_{B+S+R} \xrightarrow{\tau, O_{B+S+R}} \overline{\Psi}'_{B+S+R}$ *and* $\Psi^{\dagger}_{B+S+R} \xrightarrow{\tau, O_{B+S+R}} \overline{\Psi}^{\dagger\dagger}_{B+S+R}$
(3) $\Sigma'_{B+S+R} \cong \Sigma^{\dagger\dagger}_{B+S+R}$ *and* $X'_{B+S+R} \cong X^{\dagger\dagger}_{B+S+R}$ *and*
(4) $\Sigma'_{B+S+R} \approx^{O_{am}}_{B+S+R} X'_{B+S+R}$ *and* $\Sigma^{\dagger\dagger}_{B+S+R} \approx^{O_{am}}_{B+S+R} X^{\dagger\dagger}_{B+S+R}$

Proof. By Rule V145:Single-Base-Oracle and $X_{B+S+R} \cong X^{\dagger}_{B+S+R}$ we know that $minWndw(X_{B+S+R}) > 0$ (similar for $X^{\dagger}_{B+S+R}$). This means Rule V145-SE-Context applies. We now need to find a step $\Psi_{B+S+R} \xrightarrow{\tau'} \overline{\Psi}'_{B+S+R}$ and $\Psi^{\dagger}_{B+S+R} \xrightarrow{\tau'} \overline{\Psi}^{\dagger\dagger}_{B+S+R}$. Note that Rule V145-SE-Context reduces the window of all states by 1 or zeroes the speculation window if the instruction was a barrier.

By Lemma 162 and Lemma 171 we get $\Sigma_{B+S+R}\restriction^S \approx_S X_{B+S+R}\restriction^S$ and $\Sigma_{B+S+R}\restriction^S \cong \Sigma^{\dagger}_{B+S+R}\restriction^S$.

Because of $\Phi_{B+S+R}\restriction^S \xrightarrow{\tau}_S \overline{\Phi}'_{B+S+R}\restriction^S$ and $\Phi^{\dagger}_{B+S+R}\restriction^S \xrightarrow{\tau}_S \overline{\Phi}^{\dagger\dagger}_{B+S+R}\restriction^S$ and Rule V145:Single-Base-Oracle, we fulfill all premises for Lemma 50 (Stronger Soundness for a specific oracle and for specific executions) and derive a step in the oracle semantics:

a) $\Sigma'_{B+S+R}\restriction^S \cong \Sigma^{\dagger\dagger}_{B+S+R}\restriction^S$ and $X'_{B+S+R}\restriction^S \cong X^{\dagger\dagger}_{B+S+R}\restriction^S$
b) $\Sigma'_{B+S+R}\restriction^S \approx^{O_{am}}_{S} X'_{B+S+R}\restriction^S$ and $\Sigma^{\dagger\dagger}_{B+S+R}\restriction^S \approx^{O_{am}}_{S} X^{\dagger\dagger}_{B+S+R}\restriction^S$
c) $\Psi_{B+S+R}\restriction^S \xrightarrow{\tau}_S \overline{\Psi}'_{B+S+R}\restriction^{S'}$ and $\Psi^{\dagger}_{B+S+R}\restriction^S \xrightarrow{\tau}_S \overline{\Psi}^{\dagger}_{B+S+R}\restriction^S$ the step of the oracle

Since we have $\Psi_{B+S+R}\restriction^S \xrightarrow{\tau}_S \overline{\Psi}'_{B+S+R}\restriction^{S'}$ we can derive a step $\Psi_{B+S+R} \xrightarrow{\tau'} \overline{\Psi}'_{B+S+R}$ using Rule V145-SE:v4-step (or another applicable rule by Lemma 113 (V14SE: Confluence)).

Let us collect what we already have:

$$X'_{\mathrm{B+S+R}} = X''_{\mathrm{B+S+R}} \cdot \overline{\Psi}'_{\mathrm{B+S+R}}$$
$$\Sigma'_{\mathrm{B+S+R}} = \Sigma''_{\mathrm{B+S+R}} \cdot \overline{\Phi}'_{\mathrm{B+S+R}}$$
$$X^{\dagger\dagger}_{\mathrm{B+S+R}} = X^{*}_{\mathrm{B+S+R}} \cdot \overline{\Psi}^{\dagger\dagger}_{\mathrm{B+S+R}}$$
$$\Sigma^{\dagger\dagger}_{\mathrm{B+S+R}} = \Sigma^{*}_{\mathrm{B+S+R}} \cdot \overline{\Phi}^{\dagger\dagger}_{\mathrm{B+S+R}}$$

We now need to show that $\Sigma'_{\mathrm{B+S+R}} \cong \Sigma^{\dagger\dagger}_{\mathrm{B+S+R}}$ and $X'_{\mathrm{B+S+R}} \cong X^{\dagger\dagger}_{\mathrm{B+S+R}}$ and $\Sigma'_{\mathrm{B+S+R}} \approx^{O_{am}}_{\mathrm{B+S+R}} X'_{\mathrm{B+S+R}}$ and $\Sigma^{\dagger\dagger}_{\mathrm{B+S+R}} \approx^{O_{am}}_{\mathrm{B+S+R}} X^{\dagger\dagger}_{\mathrm{B+S+R}}$ hold.

The rest of the proof is analogous to Lemma 104 (V45: Stronger V4 Soundness Single step).

□

N.7 Framework: Oracle overapproximation

Here are the remaining proofs for the general framework definitions for Oracle overapproximation.

Definition 76 (Comb : $\cong_{xy}$)**.** *We define $\Sigma_{xy} \cong_{xy} \Sigma'_{xy}$ by reusing its parts:*
$\Sigma_{xy} \cong_{xy} \Sigma'_{xy} = \Sigma_{xy}\restriction^{x}_{xy} \cong_{x} \Sigma'_{xy}\restriction^{x}_{xy} \wedge \Sigma_{xy}\restriction^{y}_{xy} \cong_{y} \Sigma'_{xy}\restriction^{y}_{xy}$.

Definition 77 (Comb: Relation between AM and spec for all oracles)**.** *We define two relations between AM and oracle semantics. $\approx_{xy}$ ~ In the combination we need to decide if the speculative instance was created by predicting correctly or not. That is possible upon creation of the speculative instance by looking at the instance below the speculative created one. If there is a difference in the configuration σ then the speculative instance was created by misprediction and otherwise (if there is no difference) then the instance was created by predicting correctly. Here we assume a boolean encoding of this information in the combination.*

$\boxed{\Sigma_{xy} \approx_{xy} X_{xy}}$

$$\frac{}{\varnothing \approx_{xy} \varnothing}\ (Comb{:}Base) \qquad \frac{\Sigma_{xy} \sim X_{xy}\restriction_{com} \quad INV(\Sigma_{xy}, X_{xy})}{\Sigma_{xy} \approx_{xy} X_{xy}}\ (Comb{:}Single\text{-}Base)$$

$$\frac{\begin{array}{cc}\Sigma_{xy} \sim X_{xy}\restriction_{com} & \Sigma''_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'''_{xy} \text{ where transaction with id ctr is rolled back} \\ X_{xy} = X'_{xy} \cdot \Psi_{xy} & z = (x, false) \vee (y, false) \\ \Sigma_{xy} = \Sigma'_{xy} \cdot \Phi_{xy} & INV(\Sigma_{xy}, X_{xy})\end{array}}{\Sigma'_{xy} \cdot \Phi_{xy} \cdot \Phi'_{xy} \cdot \Sigma_{xy_1} \approx_{xy} X'_{xy} \cdot \Psi_{xy} \cdot \Psi'^{z}_{xy}}\ (Comb{:}Single\text{-}OracleTrue)$$

$$\frac{\begin{array}{ccc}\Sigma''_{xy} \sim X''_{xy}\restriction_{com} & \Phi'_{xy}.n \geq 0 & \Sigma''_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'''_{xy} \text{ where transaction with id ctr is rolled back} \\ X_{xy} = X'_{xy} \cdot \Psi_{xy} & \Sigma_{xy} = \Sigma'_{xy} \cdot \Phi_{xy} & x = (x, true) \vee (y, true) \\ & & INV(\Sigma_{xy}, X_{xy})\end{array} \quad \Psi'_{xy}.n = 0}{\Sigma'_{xy} \cdot \Phi_{xy} \cdot \Phi'_{xy} \cdot \Sigma_{xy_1} \approx_{xy} X'_{xy} \cdot \Psi_{xy} \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0\rangle^{z} \cdot X_{xy_1}}\ (Comb{:}Single\text{-}Transaction\text{-}Rollback)$$

$\boxed{\Sigma_{xy} \sim X_{xy}}$

$$\frac{}{\varnothing \sim \varnothing}\ (Comb{:}Base) \qquad \frac{\begin{array}{cc}|\Sigma'_{xy}| = |X'_{xy}| & \Sigma'_{xy} \sim X'_{xy} \\ \Phi_{xy}\restriction^{x}_{xy} \sim_{x} \Psi_{xy}\restriction^{y}_{xy} & \Phi_{xy}\restriction^{x}_{xy} \sim_{y} \Psi_{xy}\restriction^{y}_{xy}\end{array}}{\Sigma'_{xy} \cdot \Phi_{xy} \sim X'_{xy} \cdot \Psi_{xy}}\ (Comb{:}Single)$$

Lemma 177 (Combined: Coincide on $\cong_{xy}$ for projections)**.** *If*

(1) $\Sigma_{xy} \cong_{xy} X_{xy}$

Then

(1) $\Sigma_{xy}\restriction^{x}_{xy} \cong_{x} X_{xy}\restriction^{x}_{xy}$ and
(2) $\Sigma_{xy}\restriction^{y}_{xy} \cong_{y} X_{xy}\restriction^{y}_{xy}$

Proof. The projection functions do not change the values of the instances in the state. Follows from the definition of $\cong_{xy}$. □

Lemma 178 (Combined: Initial states fulfill properties)**.** *Let p be a program, ω be a speculation window and O be an oracle with speculation window at most ω. If*

(1) $\sigma, \sigma' \in InitConf$ and
(2) $\Sigma^{init}_{xy}(p, \sigma)$ and $\Sigma^{init}_{xy}(p, \sigma')$ and
(3) $X^{init}_{xy}(p, \sigma)$ and $X^{init}_{xy}(p, \sigma')$

Then

(1) $X^{init}_{xy}(p, \sigma) \cong_{xy} X^{init}_{xy}(p, \sigma')$ and
(2) $\Sigma^{init}_{xy}(p, \sigma) \cong_{xy} \Sigma^{init}_{xy}(p, \sigma')$ and
(3) $\Sigma^{init}_{xy}(p, \sigma) \approx_{xy} X^{init}_{xy}(p, \sigma)$ and $\Sigma^{init}_{xy}(p, \sigma') \approx_{xy} X^{init}_{xy}(p, \sigma')$ by Rule Comb:Single-Base and

Proof. The proof follows by the definitions of $\Sigma^{init}_{xy}()$, $X^{init}_{xy}()$, $\approx_{xy}$ and $\cong_{xy}$. □

Note that this assumes that the source semantics preserve $\cong$ (which they do because otherwise proofs like SNI overapproximation would not work). Since the combined semantics delegates to either of the source semantics and they preserve their part of $\cong$ we get this general result.

Lemma 179 (Combined AM: Single step preserves $\cong$). *If*

(1) $\Sigma_{xy} \cong_{xy} \Sigma^{\dagger}_{xy}$ *and*

(2) $\Sigma_{xy} \overset{\tau}{\rightarrow\!\!\!\!\!\!\cdot}_{xy} \Sigma'_{xy}$ *and* $\Sigma^{\dagger}_{xy} \overset{\tau}{\rightarrow\!\!\!\!\!\!\cdot}_{xy} \Sigma^{\dagger\dagger}_{xy}$

Then

(1) $\Sigma'_{xy} \cong_{xy} \Sigma^{\dagger\dagger}_{xy}$

Proof. Because of (1), we know that the same rule was used (up to Confluence) to derive the steps $\Sigma_{xy} \overset{\tau}{\rightarrow\!\!\!\!\!\!\cdot}_{xy} \Sigma'_{xy}$ and $\Sigma^{\dagger}_{xy} \overset{\tau}{\rightarrow\!\!\!\!\!\!\cdot}_{xy} \Sigma^{\dagger\dagger}_{xy}$. Follows from the fact that the source semantics preserve $\cong_x$ and $\cong_y$ and the fact that the combined semantics delegates back to one of the source semantics.

□

Lemma 180 (Combined SE: Single step preserves $\cong_{xy}$). *If*

(1) $X_{xy} \cong_{xy} X^{\dagger}_{xy}$ *and*

(2) $X_{xy} \overset{\tau}{\rightarrow}^{O_{xy}}_{xy} X'_{xy}$ *and* $X^{\dagger}_{xy} \overset{\tau}{\rightarrow}^{O_{xy}}_{xy} X^{\dagger\dagger}_{xy}$

Then

(1) $X'_{xy} \cong_{xy} X^{\dagger\dagger}_{xy}$ *and*

Proof. Because of (1), we know that the same rule (up to Confluence) was used to derive the steps $X_{xy} \overset{\tau}{\rightarrow}^{O_{xy}}_{xy} X'_{xy}$ and $X^{\dagger}_{xy} \overset{\tau}{\rightarrow}^{O_{xy}}_{xy} X^{\dagger\dagger}_{xy}$.
Follows from the fact that the source semantics preserve $\cong_x$ and $\cong_y$ and the fact that the combined semantics delegates back to one of the source semantics. □

This is the main result needed for Oracle overapproximation.

Theorem 43 (Combined SNI). *A program p satisfies SNI for a security policy P and all prediction oracles O with speculative window at most ω iff for all initial configurations $\sigma, \sigma' \in InitConf$, if $\sigma \sim_P \sigma'$ and (p,σ) $\mathbb{A}^{O}_{NS}$ $\overline{\tau}$, (p,σ') $\mathbb{A}^{O}_{NS}$ $\overline{\tau}$, then (p,σ) $\mathbb{A}^{\omega}_{xy}$ $\overline{\tau}''$, (p,σ') $\mathbb{A}^{\omega}_{xy}$ $\overline{\tau}''$*

Proof. Let p be a program, P be a policy and $\omega \in \mathbb{N}$ be a speculative window. We prove the two directions separately.

($\Rightarrow$) We have
(1) $\sigma \sim_P \sigma'$ and
(2) (p,σ) $\mathbb{A}^{O}_{NS}$ $\overline{\tau}'$, (p,σ') $\mathbb{A}^{O}_{NS}$ $\overline{\tau}'$ and
(3) p satisfies SNI for policy P and all prediction oracles O with speculative window at most ω
and we need to show that (p,σ) $\mathbb{A}^{\omega}_{xy}$ $\overline{\tau}''$, (p,σ') $\mathbb{A}^{\omega}_{xy}$ $\overline{\tau}''$ holds.
We unfold the definition of SNI and have for all O with speculation window at most ω, for all initial configurations σ, σ', if $\sigma \sim_P \sigma'$ and (p,σ) $\mathbb{A}^{O}_{NS}$ $\overline{\tau}$, (p,σ') $\mathbb{A}^{O}_{NS}$ $\overline{\tau}$, then (p,σ) $\mathbb{A}^{O}_{xy}$ $\overline{\tau}'$ and (p,σ') $\mathbb{A}^{O}_{xy}$ $\overline{\tau}'$.
We fulfill all premises of SNI by a) and b) for p and get (p,σ) $\mathbb{A}^{O}_{xy}$ $\overline{\tau}'$ and (p,σ') $\mathbb{A}^{O}_{xy}$ $\overline{\tau}'$.
We use Proposition 3 (Combined: Sound and Completeness between Spec and AM semantics) with (p,σ) $\mathbb{A}^{O}_{xy}$ $\overline{\tau}'$ and (p,σ') $\mathbb{A}^{O}_{xy}$ $\overline{\tau}'$ to get (p,σ) $\mathbb{A}^{\omega}_{xy}$ $\overline{\tau}''$, (p,σ') $\mathbb{A}^{\omega}_{xy}$ $\overline{\tau}''$. This completes the proof.

($\Leftarrow$) We have
(1) $\sigma \sim_P \sigma'$ and
(2) (p,σ) $\mathbb{A}^{O}_{NS}$ $\overline{\tau}'$, (p,σ') $\mathbb{A}^{O}_{NS}$ $\overline{\tau}'$ and
(3) if $\sigma \sim_P \sigma'$ and (p,σ) $\mathbb{A}^{O}_{NS}$ $\overline{\tau}$, (p,σ') $\mathbb{A}^{O}_{NS}$ $\overline{\tau}$, then (p,σ) $\mathbb{A}^{\omega}_{xy}$ $\overline{\tau}''$, (p,σ') $\mathbb{A}^{\omega}_{xy}$ $\overline{\tau}''$
Note that we got assumptions a) and b) by the unfolding of the definition of SNI. We need to show that (p,σ) $\mathbb{A}^{O}_{xy}$ $\overline{\tau}'$ and (p,σ') $\mathbb{A}^{O}_{xy}$ $\overline{\tau}'$ holds.
By using assumption a) and b) for assumption c), we get (p,σ) $\mathbb{A}^{\omega}_{xy}$ $\overline{\tau}''$, (p,σ') $\mathbb{A}^{\omega}_{xy}$ $\overline{\tau}''$.
Let O be an arbitrary prediction oracle with speculative window at most ω.
From Proposition 3 (Combined: Sound and Completeness between Spec and AM semantics) with (p,σ) $\mathbb{A}^{\omega}_{xy}$ $\overline{\tau}''$, (p,σ') $\mathbb{A}^{\omega}_{xy}$ $\overline{\tau}''$ we get back (p,σ) $\mathbb{A}^{O}_{xy}$ $\overline{\tau}$, (p,σ') $\mathbb{A}^{O}_{xy}$ $\overline{\tau}$. Consequently, p satisfies SNI w.r.t. P and O.
Since O was an arbitrary prediction oracle with speculation window at most ω, then p satisfies SNI for P and all prediction oracles with speculation window at most ω.

□

Proposition 3 (Combined: Sound and Completeness between Spec and AM semantics)**.** *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, $\sigma, \sigma' \in InitConf$ be two initial configurations. We have $(p,\sigma) \mathbin{\text{ᗣ}}^{\omega}_{xy} \overline{\tau}$ and $(p,\sigma') \mathbin{\text{ᗣ}}^{\omega}_{xy} \overline{\tau}$ iff $(p,\sigma) \mathbin{\text{ᗣ}}^{O}_{xy} \overline{\tau}'$, $(p,\sigma) \mathbin{\text{ᗣ}}^{O}_{xy} \overline{\tau}'$ for all prediction oracles O with speculative window at most ω.*

Proof. The proposition immediately follows from Lemma 181 (Comb: Soundness Big-step) and Lemma 183 (Comb: Completeness Am semantics w.r.t. speculative semantics) □

N.7.1 Soundness Proof.

Lemma 181 (Comb: Soundness Big-step)**.** *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*
If
(1) $\sigma, \sigma' \in InitConf$ and
(2) $(p,\sigma) \mathbin{\text{ᗣ}}^{\omega}_{xy} \overline{\tau}$, $(p,\sigma') \mathbin{\text{ᗣ}}^{\omega}_{xy} \overline{\tau}$
Then for all prediction oracles O_{xy} with speculation window at most ω.
I $(p,\sigma) \mathbin{\text{ᗣ}}^{O}_{xy} \overline{\tau}'$, $(p,\sigma) \mathbin{\text{ᗣ}}^{O}_{xy} \overline{\tau}'$

Proof. The proof is analogous to Lemma 46 (S: Soundness Am semantics w.r.t. speculative semantics) using Lemma 178 (Combined: Initial states fulfill properties) to show that our initial states fulfill all the premises for Lemma 182 (Comb: Soundness Am semantics w.r.t. speculative semantics with new relation between states). □

Lemma 182 (Comb: Soundness Am semantics w.r.t. speculative semantics with new relation between states)**.** *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*
If
(1) $\Sigma_{xy} \cong_{xy} \Sigma^{\dagger}_{xy}$
(2) $X_{xy} \cong_{xy} X^{\dagger}_{xy}$ and $\overline{\rho} = \emptyset$
(3) $\Sigma^{\dagger}_{xy} \approx_{xy} X_{xy}$ and $\Sigma^{\dagger}_{xy} \approx_{xy} X^{\dagger}_{xy}$
(4) $\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}$ and $\Sigma^{\dagger}_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma^{\dagger\dagger}_{xy}$
Then for all prediction oracles O with speculation window at most ω.
I $X_{xy} \overset{O_{xy} \wr^{xy}_{\overline{\tau}'}}{\Downarrow} X'_{xy}, X^{\dagger}_{xy} \overset{O_{xy} \wr^{xy}_{\overline{\tau}''}}{\Downarrow} X^{\dagger\dagger}_{xy}$
II $\Sigma'_{xy} \cong_{xy} \Sigma^{\dagger\dagger}_{xy}$
III $X'_{xy} \cong_{xy} X^{\dagger\dagger}_{xy}$ and $\overline{\rho} = \emptyset$
IV $\Sigma'_{xy} \approx_{xy} X'_{xy}$ and $\Sigma^{\dagger\dagger}_{xy} \approx_{xy} X^{\dagger\dagger}_{xy}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. By Induction on $\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}$ and $\Sigma^{\dagger}_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma^{\dagger\dagger}_{xy}$.

Rule AM-Reflection-xy We have $\Sigma_{xy} \Downarrow^{\varepsilon}_{xy} \Sigma'_{xy}$ and $\Sigma^{\dagger}_{xy} \Downarrow^{\varepsilon}_{xy} \Sigma''_{xy}$, where $\Sigma'_{xy} = \Sigma_{xy}$ and $\Sigma''_{xy} = \Sigma^{\dagger}_{xy}$. We choose $\Sigma'_{xy} = \Sigma'_{xy}$ and $\Sigma^{\dagger\dagger}_{xy} = \Sigma''_{xy}$.
We further use Rule SE-Reflection-xy to derive $X_{xy} \overset{O_{xy} \wr^{xy}_{\varepsilon}}{\Downarrow} X'_{xy}, X^{\dagger}_{xy} \overset{O_{xy} \wr^{xy}_{\varepsilon}}{\Downarrow} X^{\dagger\dagger}_{xy}$ with $X'_{xy} = X_{xy}$ and $X^{\dagger\dagger}_{xy} = X^{\dagger}_{xy}$. We now trivially satisfy all conclusions.

Rule AM-Single-xy We have $\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma''_{xy}$ with $\Sigma''_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma'_{xy}$ and $\Sigma^{\dagger}_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'''_{xy}$ and $\Sigma'''_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma^{\dagger\dagger}_{xy}$.
We now apply IH on $\Sigma_{xy} \Downarrow^{\overline{\tau}''}_{xy} \Sigma''_{xy}$ and $\Sigma^{\dagger}_{xy} \Downarrow^{\overline{\tau}'''}_{xy} \Sigma^{*}_{xy}$ and get
(a) $X_{xy} \overset{O_{xy} \wr^{xy}_{\overline{\tau}'}}{\Downarrow} X''_{xy}, X^{\dagger}_{xy} \overset{O_{xy} \wr^{xy}_{\overline{\tau}''}}{\Downarrow} X^{*}_{xy}$
(b) $\Sigma''_{xy} \cong_{xy} \Sigma^{*}_{xy}$
(c) $X''_{xy} \cong_{xy} X^{*}_{xy}$ and $\overline{\rho}' = \emptyset$
(d) $\Sigma''_{xy} \approx_{xy} X''_{xy}$ and $\Sigma^{*}_{xy} \approx_{xy} X^{*}_{xy}$
(e) $\overline{\tau}' = \overline{\tau}''$
We do a case distinction on $\approx_{xy}$ in $\Sigma''_{xy} \approx_{xy} X''_{xy}$ and $\Sigma^{*}_{xy} \approx_{xy} X^{*}_{xy}$:
Rule Comb:Single-Base We thus have $\Sigma''_{xy} \sim X''_{xy}\restriction_{com}$ and $INV(\Sigma''_{xy}, X''_{xy})$ (Similar for Σ^{*}_{xy} and X^{*}_{xy}).
We only show the proof for X''_{xy} here. The proof for X^{*}_{xy} is analogous, because of $X''_{xy} \cong_{xy} X^{*}_{xy}$.
Notice that if $minWndw(X''_{xy}) = 0$ then the transaction with $n = 0$ has to be one that will be committed. Otherwise they would be related by Rule Comb:Single-Transaction-Rollback. To account for possible outstanding commits, we use a lemma similar to Lemma 23 (V45: Executing a chain of commits) on X''_{xy} and get

f) $X''_{xy} \overset{O_{xy}}{\underset{\overline{\tau}'''}{\wr^{xy}}} X^{**}_{xy}$
g) $minWndw(X^{**}_{xy}) > 0$
h) $\forall \tau \in \overline{\tau}'''.\ \tau = \texttt{commit}\ id$ for some $id \in \mathbb{N}$
i) $X''_{xy}.\sigma = X^{**}_{xy}.\sigma$

By h) and the definition of $\restriction_{ns}$ we have $\overline{\tau}''' \restriction_{ns} = \varepsilon$.
Furthermore, $X''_{xy} \restriction_{com} = X^{**}_{xy} \restriction_{com}$ by definition of $\restriction_{com}$ (we only executed commits) and we have $|X''_{xy} \restriction_{com}| = |X^{**}_{xy} \restriction_{com}|$.
Thus, $\Sigma''_{xy} \sim X^{**}_{xy} \restriction_{com}$ and $INV(\Sigma''_{xy}, X^{**}_{xy})$ and we have $\Sigma''_{xy} \approx_{xy} X^{**}_{xy}$ by Rule Comb:Single-Base.

We now proceed by inversion on the derivations $\Sigma''_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma'_{xy}$ and $\Sigma^{*}_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma^{\dagger\dagger}_{xy}$.
Note that by $\Sigma''_{xy} \cong_{xy} \Sigma^{*}_{xy}$ and the fact the same traces are generated, we know that the same rule (up to Confluence) was used to derive the step.

Rule AM-Context-xy We now have $\Phi'_{xy} \overset{\tau}{\dashrightarrow}_{xy} \overline{\Phi}'_{xy}$ and $\Phi''_{xy} \overset{\tau}{\dashrightarrow}_{xy} \overline{\Phi}'''_{xy}$ where $\Sigma''_{xy} = \overline{\Phi}_{xy} \cdot \Phi'_{xy}$ and $\Sigma^{*}_{xy} = \overline{\Phi}''_{xy} \cdot \Phi''_{xy}$.
Furthermore, $n > 0$ and note that all states point to the same instruction by b-d. Because of $\vdash \wr_{xy} : WFC$ we have *Relation Preservation.* Directly follows from Relation Preservation and Lemma 179 (Combined AM: Single step preserves $\cong$) and Lemma 180 (Combined SE: Single step preserves $\cong_{xy}$). Furthermore $\tau' = \tau''$ follows from the fact that the oracle steps were derived by the same rule (up to Confluence) and the fact that the AM steps produce the same observation. If $\tau' \neq \tau''$ then this directly implies that the AM steps produce different observations (since they are related by Rule Comb:Single-Base before the step was made).

Rule AM-x-Rollback-xy Contradiction, because $minWndw(X'''_{xy}) > 0$ and $INV(\Sigma'_{xy}, X'''_{xy})$.

Rule AM-y-Rollback-xy Contradiction, because $minWndw(X'''_{xy}) > 0$ and $INV(\Sigma'_{xy}, X'''_{xy})$.

Rule Comb:Single-OracleTrue We thus have

$$\begin{aligned}
X''_{xy} &= X_{xy_3} \cdot \Psi_{xy} \cdot \Psi''_{xy} \\
\Sigma''_{xy} &= \Sigma_{xy_3} \cdot \Phi_{xy} \cdot \Phi''_{xy} \cdot \Sigma_{xy_4} \\
X_{xy} &= X_{xy_3} \cdot \Psi_{xy} \\
\Sigma_{xy} &= \Sigma_{xy_3} \cdot \Phi_{xy} \\
\Sigma_{xy} &\sim X_{xy} \restriction_{com} \\
\Phi''_{xy}.ctr &= \Psi''_{xy}.ctr
\end{aligned}$$

The form of X^{*}_{xy} and Σ^{*}_{xy} is analogous. We now apply inversion on $\Sigma''_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma'_{xy}$.

Rule AM-Context-xy We choose $X'_{xy} = X''_{xy}$ and $X^{\dagger\dagger}_{xy} = X^{*}_{xy}$.

I By IH a) and Rule SE-Reflection-xy

II By Lemma 179 (Combined AM: Single step preserves $\cong$).

III Since $X'_{xy} = X''_{xy}$ and $X^{\dagger\dagger}_{xy} = X^{*}_{xy}$, we are finished using IH c).

IV We show that $X'_{xy} \approx_{xy} \Sigma'_{xy}$ by Rule Comb:Single-OracleTrue. The proof for $X^{\dagger\dagger}_{xy} \approx \Sigma^{\dagger\dagger}_{xy}$ is analogous.
Since we did not roll back the transaction with *id ctr'* we have that Σ_{xy} does not change.
Since X_{xy} remains the same as well, we have $\Sigma_{xy} \sim X_{xy} \restriction_{com}$ and $INV(\Sigma_{xy}, X_{xy}) X_{xy} \restriction_{com}$.
Thus, we fulfill all premises for Rule Comb:Single-OracleTrue.

V By IH e).

Rule AM-x-Rollback-xy There are two cases depending on the transaction *id* of the rolled back transaction:

id > ctr Then an inner transaction w.r.t our *ctr* transaction was finished. Similar to before, only Σ''_{xy} and Σ^{*}_{xy} do a step. We choose $X'_{xy} = X''_{xy}$ and $X^{\dagger\dagger}_{xy} = X^{*}_{xy}$. The rest of the proof proceeds analogous to the context case above.

id = ctr Most cases are similar to the context case above. Only the relation changes. We choose $X'_{xy} = X''_{xy}$ and $X^{\dagger\dagger}_{xy} = X^{*}_{xy}$

I By IH a) and Rule SE-Reflection-xy

IV Here, we only show $\Sigma'_{xy} \approx_{xy} X'_{xy}$ by Rule Comb:Single-Base. The proof for $\Sigma^{\dagger\dagger}_{xy} \approx X^{\dagger\dagger}_{xy}$ is analogous.
Rolling back only updates the counter *ctr* which was equal beforehand.
Combined with the constructed X'_{xy} we have $\Sigma'_{xy} \sim X'_{xy} \restriction_{com}$ and $INV(\Sigma'_{xy}, X'_{xy})$ by our assumptions.
So we can use Rule Comb:Single-Base and have $\Sigma'_{xy} \approx X'_{xy}$.

V By IH e)

Rule AM-y-Rollback-xy The case is analogous to the case Rule AM-x-Rollback-xy above.

Rule Comb:Single-Transaction-Rollback We have

$$\begin{aligned}
X''_{xy} &= X_{xy_3} \cdot \Psi_{xy} \cdot \Psi'_{xy} \cdot X_{xy_4} \\
\Sigma''_{xy} &= \Sigma_{xy_3} \cdot \Phi_{xy} \cdot \Phi'_{xy} \cdot \Sigma_{xy_4} \\
X_{xy} &= X_{xy_3} \cdot \Psi_{xy} \\
\Sigma_{xy} &= \Sigma_{xy_3} \cdot \Phi_{xy} \\
\Sigma_{xy} &\sim X_{xy}\restriction_{com} \\
n' &\geq 0
\end{aligned}$$

The form of X^*_{xy} and Σ^*_{xy} is analogous.

Additionally, we know that the transaction terminates in some state $\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'''_{xy}$. There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma''_{xy} \overset{\tau}{\doteq\!\!\text{Q}}_{xy} \Sigma'_{xy}$ is not a rollback for *ctr* and Rule AM-Context-xy was used.

Because of IH b), we know that the same rule was used for $\Sigma^{\dagger}_{xy} \overset{\tau}{\doteq\!\!\text{Q}}_{xy} \Sigma^{\dagger\dagger}_{xy}$ as well. We choose $X'_{xy} = X''_{xy}$ and $X^{\dagger\dagger}_{xy} = X^*_{xy}$. The resulting proof obligations are exactly the same to the context case of the oracle above.

$n' = 0$ Then we know that $\Sigma''_{xy} \overset{\tau}{\doteq\!\!\text{Q}}_{xy} \Sigma'_{xy}$ was created by either Rule AM-x-Rollback-xy or Rule AM-y-Rollback-xy and is a rollback for *ctr*.

We do the proof for Rule AM-x-Rollback-xy, since the case for Rule AM-y-Rollback-xy is analogous.

I Here we prove that $X''_{xy} \overset{\tau_0}{\rightsquigarrow}^{O_{xy}}_{xy} X'_{xy}$ and $X^*_{xy} \overset{\tau_1}{\rightsquigarrow}^{O_{xy}}_{xy} X^{\dagger\dagger}_{xy}$.
Since in X''_{xy} and X^*_{xy} we have a state that needs to be rolled back for the same *ctr*, we know that Rule SE-x-Rollback applies.
So $X''_{xy} \overset{\tau_0}{\rightsquigarrow}^{O_{xy}}_{xy} X'_{xy}$ and $X^*_{xy} \overset{\tau_1}{\rightsquigarrow}^{O_{xy}}_{xy} X^{\dagger\dagger}_{xy}$ are derived by Rule SE-x-Rollback.

II By Lemma 179 (Combined AM: Single step preserves $\cong$)

III By Lemma 180 (Combined SE: Single step preserves $\cong_{xy}$) with fact V).

IV Here, we only show $\Sigma'_{xy} \approx X'_{xy}$ by Rule Comb:Single-Base. The proof for $\Sigma^{\dagger\dagger}_{xy} \approx X^{\dagger\dagger}_{xy}$ is analogous.
Rolling back only updates the *ctr* field in both states. Since the updated value is the same (comes from the relation), we are finished.
We also know by assumption that $\Sigma''_{xy} \sim X''_{xy}\restriction_{com}$ and $INV(\Sigma''_{xy}, X''_{xy})$.
By construction of X'_{xy} and Σ'_{xy}, we can conclude that $\Sigma'_{xy} \sim X'_{xy}\restriction_{com}$ and $INV(\Sigma'_{xy}, X'_{xy})$.
This allows us to use Rule Comb:Single-Base to derive $\Sigma'_{xy} \approx_{xy} X'_{xy}$.

V Here $\tau_0 = \texttt{rlb}_x\ ctr'$ and $\tau_1 = \texttt{rlb}_x\ ctr''$. Because of IH b) we know that $ctr' = ctr''$ and thus $\tau_0 = \tau_1$.

□

N.7.2 Completeness Proof.

Definition 78 (Combined: Relation between AM and Spec for oracles that only mispredict)**.** *We define two relations, $\approx^{O_{am}}$ and $\sim$, between AM and oracle semantics. Note that $\approx^{O_{am}}$ is indexed by an oracle. This oracle has to always mispredict.*

$$\boxed{\Sigma_{xy} \approx^{O_{am}}_{xy} X_{xy}}$$

$$\frac{\text{(Comb:Base-Oracle)}}{\varnothing \approx^{O_{am}}_{xy} \varnothing} \qquad \frac{\Sigma_{xy} \sim X_{xy}\restriction_{com} \quad INV2(\Sigma_{xy}, X_{xy}) \quad minWndw(X_{xy}) > 0}{\Sigma_{xy} \approx^{O_{am}}_{xy} X_{xy}}\ \text{(Comb:Single-Base-Oracle)}$$

$$\frac{\begin{array}{ccc} \Sigma''_{xy} \sim X''_{xy}\restriction_{com} & \Phi'_{xy}.n' \geq 0 & \Sigma''_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'''_{xy} \text{ where transaction with id ctr is rolled back} \quad z = (x, true) \vee (y, true) \\ X_{xy} = X'_{xy} \cdot \Psi_{xy} & & \Sigma_{xy} = \Sigma'_{xy} \cdot \Phi_{xy} \qquad INV2(\Sigma_{xy}, X_{xy}) \end{array}}{\Sigma'_{xy} \cdot \Phi_{xy} \cdot \Phi'^{z}_{xy} \cdot \Sigma_{xy_1} \approx^{O_{am}}_{xy} X'_{xy} \cdot \Psi_{xy} \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0\rangle^z}\ \text{(Comb:Single-Transaction-Rollback-Oracle)}$$

Definition 79 (Comb: Constructing the AM Oracle)**.** *We rely for the construction of the oracle O^{xy}_{am} on the construction of its parts. Thus, we have: $O^{xy}_{am} = (O^{x}_{am}, O^{y}_{am})$ for the speculative oracle combined semantics.*

Lemma 183 (Comb: Completeness Am semantics w.r.t. speculative semantics)**.** *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, $\sigma, \sigma' \in InitConf$ be two initial configurations. If*

(1) (p, σ) Q^{ω}_{xy} $\overline{\tau}$ and (p, σ') Q^{ω}_{xy} $\overline{\tau}'$ and
(2) $\overline{\tau} \neq \overline{\tau}'$

Then there exists an oracle O such that

I $(p,\sigma) \Downarrow^{O}_{xy} \overline{\tau}_1$ *and* $(p,\sigma') \Downarrow^{O}_{xy} \overline{\tau}'_1$ *and*

II $\overline{\tau}_1 \neq \overline{\tau}'_1$

Proof. Let $\omega \in \mathbb{N}$ be a speculative window, $\sigma, \sigma' \in InitConf$ be two initial configurations. We have If

(1) $(p,\sigma) \Downarrow^{\omega}_{xy} \overline{\tau}$ and $(p,\sigma') \Downarrow^{\omega}_{xy} \overline{\tau}'$ and
(2) $\overline{\tau} \neq \overline{\tau}'$

By definition of $() \Downarrow^{\omega}_{xy}$ we have two final states Σ_{xy_F} and Σ'_{xy_F} such that $\Sigma^{init}_{xy}(p,\sigma) \Downarrow^{\overline{\tau}}_{xy} \Sigma_{xy_F}$ $\Sigma^{init}_{xy}(p,\sigma') \Downarrow^{\overline{\tau}'}_{xy} \Sigma'_{xy_F}$. Combined with the fact that $\overline{\tau} \neq \overline{\tau}'$, it follows that there are speculative states $\Sigma^{*}_{xy}, \Sigma^{**}_{xy}, \Sigma^{\dagger}_{xy}, \Sigma^{\dagger\dagger}_{xy}$ and sequences of observations $\overline{\tau}, \overline{\tau}_{end}, \overline{\tau}'_{end}, \tau_{am}, \tau'_{am}$ such that $\tau_{am} \neq \tau'_{am}$, $\Sigma^{*}_{xy} \cong \Sigma^{\dagger}_{xy}$ and:

$$\Sigma^{init}_{xy}(p,\sigma) \Downarrow^{\overline{\tau}}_{xy} \Sigma^{*}_{xy} \overset{\tau_{am}}{\Longrightarrow}_{xy} \Sigma^{**}_{xy} \Downarrow^{\overline{\tau}_{end}}_{xy} \Sigma_{xy_F}$$

$$\Sigma^{init}_{xy}(p,\sigma') \Downarrow^{\overline{\tau}}_{xy} \Sigma^{\dagger}_{xy} \overset{\tau'_{am}}{\Longrightarrow}_{xy} \Sigma^{\dagger\dagger}_{xy} \Downarrow^{\overline{\tau}'_{end}}_{xy} \Sigma'_{xy_F}$$

We claim that there is a prediction oracle O with speculative window at most ω such that

a) $X^{init}_{xy}(p,\sigma) \;{}^{O_{xy}}\!\Downarrow^{xy}_{v} X^{*}_{xy}$ and $X^{*}_{xy}.\sigma = \Sigma^{*}_{xy}.\sigma$ and $INV2(X^{*}_{xy}, \Sigma^{*}_{xy})$ and
b) $X^{init}_{xy}(p,\sigma') \;{}^{O_{xy}}\!\Downarrow^{xy}_{v} X^{\dagger}_{xy}$ and $X^{\dagger}_{xy}.\sigma = \Sigma^{\dagger}_{xy}.\sigma$ and $INV2(X^{\dagger}_{xy}, \Sigma^{\dagger}_{xy})$
c) $X^{*}_{xy} \cong_{xy} X^{\dagger}_{xy}$

We achieve this by applying Lemma 184 (Comb: Stronger Soundness for a specific oracle and for specific executions) on the AM execution up to the point of the difference i.e., $\Sigma^{init}_{xy}(p,\sigma) \Downarrow^{\overline{\tau}}_{xy} \Sigma^{*}_{xy}$ and $\Sigma^{init}_{xy}(p,\sigma') \Downarrow^{\overline{\tau}}_{xy} \Sigma^{\dagger}_{xy}$.

We now show that $\Sigma^{*}_{xy} \approx^{O_{am}}_{xy} X^{*}_{xy}$ is derived by Rule Comb:Single-Base-Oracle.

We do a case distinction if there are ongoing speculative transactions in X^{*}_{xy} or not:

no ongoing transactions in X^{*}_{xy} Then, Σ^{*}_{xy} has no ongoing transactions as well and we have by $INV2(\Sigma^{*}_{xy}, X^{*}_{xy})$ and $\Sigma^{*}_{xy}.n = \bot$ that $X^{*}_{xy}.n = \bot$ that $\Sigma^{*}_{xy} \approx^{O_{am}}_{xy} X^{*}_{xy}$ can only be derived Rule Comb:Single-Base-Oracle .

ongoing transactions in X^{*}_{xy} By the definition of the oracle O, we know that the for the transaction id where the difference $\tau_{am} \neq \tau_{am'}$ happens, the oracle mispredicted with a speculation window of ω. This is also the topmost transaction in X_{xy}.

Furthermore, we know that $X^{*}_{xy}.n \geq minWndw(X^{*}_{xy})$ by definition of the oracle O^{xy}_{am} and $minWndw()$.

Since the next rule cannot be Rule AM-x-Rollback-xy or Rule AM-y-Rollback-xy, we know that $\Sigma^{*}_{xy}.n > 0$ and by $INV2(\Sigma^{*}_{xy}, X^{*}_{xy})$ we get $minWndw(X^{*}_{xy}) > 0$ (Similar for $X^{\dagger}_{xy}$ because of $\Sigma^{*}_{xy} \cong \Sigma^{\dagger}_{xy}$).

If $\Sigma^{*}_{xy} \approx^{O_{am}} X^{*}_{xy}$ by rollback rule, we would have a contradiction because we would need the topmost speculation window of $X^{*}_{xy}.n = 0$. But we know that $minWndw(X^{*}_{xy}) > 0$, because the speculation window of the topmost instance was created with a speculation window of ω.

Now we know that $X^{*}_{xy} \approx^{O_{am}} \Sigma^{*}_{xy}$ by Rule Comb:Single-Base-Oracle.

We proceed by case analysis on the rule in $\Longrightarrow_{xy}$ used to derive $\Sigma^{*}_{xy} \overset{\tau_{am}}{\Longrightarrow}_{xy} \Sigma^{**}_{xy}$. Because $\Sigma^{*}_{xy} \cong_{xy} \Sigma^{\dagger}_{xy}$, we know that the same rule was used in $\Sigma^{\dagger}_{xy} \overset{\tau'_{am}}{\Longrightarrow}_{xy} \Sigma^{\dagger\dagger}_{xy}$ as well.

Rule AM-x-Rollback-xy Contradiction. Because $\Sigma^{*}_{xy} \cong_{xy} \Sigma^{\dagger}_{xy}$ we have for all instances $\Phi_1.ctr = \Phi'_1.ctr$.
Since the same instance would be rolled back, we have $\tau_{am} = \tau'_{am}$.

Rule AM-y-Rollback-xy Analogous to the case above.

Rule AM-Context-xy By inversion on Rule AM-Context-xy for the step $\Sigma^{*}_{xy} \overset{\tau_{am}}{\Longrightarrow}_{xy} \Sigma^{**}_{xy}$ we have $\Sigma^{*}_{xy} = \overline{\Phi}_{xy} \cdot \Phi_{xy}$ and $\Sigma^{**}_{xy} = \overline{\Phi}_{xy} \cdot \overline{\Phi}'_{xy}$ with $\Phi_{xy} \overset{\tau_{am}}{\Longrightarrow}_{xy} \overline{\Phi}'_{xy}$.

By Relation Preservation we can find $X^{*}_{xy} \;{}^{O_{xy}}\!\Downarrow^{xy}_{\overline{\tau}^{*}} X^{**}_{xy}$ and have $\Sigma^{**}_{xy} \approx^{O_{am}}_{xy} X^{**}_{xy}$. Since $X^{*}_{xy} \approx_{xy} \Sigma^{*}_{xy}$ is related by Rule Comb:Single-Base-Oracle that $X^{*}_{xy} \;{}^{O_{xy}}\!\Downarrow^{xy}_{\overline{\tau}^{*}} X^{**}_{xy}$ was derived by Rule SE-Single-xy (otherwise $\Sigma^{**}_{xy} \approx^{O_{am}}_{xy} X^{**}_{xy}$ cannot hold) and as such we have $X^{*}_{xy} \overset{\tau_{sp}}{\rightsquigarrow}{}^{O_{xy}}_{xy} X^{**}_{xy}$.

This holds similar for $X^{\dagger}_{xy}$ such that we have $X^{\dagger}_{xy} \overset{\tau_{sp'}}{\rightsquigarrow}{}^{O_{xy}}_{xy} X^{\dagger\dagger}_{xy}$.

By applying Assumption 1 (Oracle and AM steps in Lockstep produce the same observation) on $\Sigma^{*}_{xy} \overset{\tau_{am}}{\Longrightarrow}_{xy} \Sigma^{**}_{xy}$ and $X^{*}_{xy} \overset{\tau_{sp}}{\rightsquigarrow}{}^{O_{xy}}_{xy} X^{**}_{xy}$ we get that $\tau_{am} = \tau_{sp}$.

We can apply Assumption 1 (Oracle and AM steps in Lockstep produce the same observation) again on the steps $\Sigma^{\dagger}_{xy} \xrightarrow{\tau'_{am}}_{xy} \Sigma^{\dagger\dagger}_{xy}$ and $X^{*}_{xy} \overset{\tau_{sp'}}{\rightsquigarrow}_{xy}^{O_{xy}} X^{\dagger\dagger}_{xy}$.
Since $\tau_{am} \neq \tau_{am'}$ we can conclude that $\tau_{sp} \neq \tau_{sp'}$.

This completes the proof of our claim.

□

This assumption gives us the fact that the AM semantics and the Oracle semantics behave similar when they are in lock-step. Lockstep is enforced by Rule Comb:Single-Base-Oracle which essentially enforces a equality between the states. If the states are equal then they should do related things. Note that even if speculation starts and the Oracle is invoked, the underlying non-speculative step should be shown on the trace! Furthermore, this only holds for oracles that only mispredict. This essentially enforces a certain well behavedness of the Oracle and the AM semantics. They certainly should behave the same way, when they do not start speculating. Other edge cases are rolling back and committing but then the states would not be in lock step (covered by INV2), which enforces that $n > 0$. Furthermore, we know that overapproximation of the Oracle by the AM semantics holds in the source semantics when proving this assumption.-

Assumption 1 (Oracle and AM steps in Lockstep produce the same observation)**.** *If*

(1) $\Sigma_{xy} \approx^{O_{am}}_{xy} X_{xy}$ *by Rule Comb:Single-Base-Oracle*
(2) $\Sigma_{xy} \xrightarrow{\tau_{am}}_{xy} \Sigma'_{xy}$ *and* $X_{xy} \overset{\tau_{sp}}{\rightsquigarrow}_{xy}^{O_{xy}} X'_{xy}$

Then

(1) $\tau_{am} = \tau_{sp}$ *and*
(2) $\Sigma'_{xy} \approx^{O_{am}}_{xy} X'_{xy}$

We assume that the AM source semantics reduce the speculation window by 1 when executing an instruction, except when a barrier encountered, which sets the speculation window to 0. Furthermore, upon speculation the new speculation window is set to the minimum of the maximal speculation window ω and the previous speculation window j, that is $min(\omega, j)$.

Lemma 184 (Comb: Stronger Soundness for a specific oracle and for specific executions)**.** *Specific executions means that there is a difference in the trace but before there is none. We use the oracle O_{am} as it is defined by Definition 79 (Comb: Constructing the AM Oracle) for the given execution. If*

(1) $\Sigma_{xy} \cong_{xy} \Sigma^{\dagger}_{xy}$
(2) $X_{xy} \cong_{xy} X^{\dagger}_{xy}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma_{xy} \approx^{O_{am}}_{xy} X_{xy}$ *and* $\Sigma^{\dagger}_{xy} \approx^{O_{am}}_{xy} X^{\dagger}_{xy}$
(4) $\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}$ *and* $\Sigma^{\dagger}_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma^{\dagger\dagger}_{xy}$

and our oracle is constructed in the way described above Then

I $X_{xy} \overset{O_{xy}}{\downarrow}^{xy}_{\overline{\tau}'} X'_{xy}, X^{\dagger}_{xy} \overset{O_{xy}}{\downarrow}^{xy}_{\overline{\tau}''} X^{\dagger\dagger}_{xy}$
II $\Sigma'_{xy} \cong \Sigma^{\dagger\dagger}_{xy}$
III $X'_{xy} \cong_{xy} X^{\dagger\dagger}_{xy}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{xy} \approx^{O_{am}} X'_{xy}$ *and* $\Sigma^{\dagger\dagger}_{xy} \approx^{O_{am}} X^{\dagger\dagger}_{xy}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. Notice that the proof is very similar to Lemma 98 (V45: Soundness Am semantics w.r.t. speculative semantics with new relation between states). The only thing that is different is that (1) the specific oracle only mispredicts so there is one less case in the relation and (2) we have a different invariant for that specific oracle i.e., $INV2(\Sigma_{xy}, X_{xy})$ encoded in the new relation.

For these reasons we will only argue why $INV2(\Sigma^{\dagger}_{xy}, X'_{xy})$ holds in the different cases and leave the rest to the old soundness proof.

By Induction on $\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}$ and $\Sigma^{\dagger}_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma^{\dagger\dagger}_{xy}$.

Rule AM-Reflection-xy We have $\Sigma_{xy} \Downarrow^{\varepsilon}_{xy} \Sigma'_{xy}$ and $\Sigma^{\dagger}_{xy} \Downarrow^{\varepsilon}_{xy} \Sigma''_{xy}$, where $\Sigma'_{xy} = \Sigma_{xy}$ and $\Sigma''_{xy} = \Sigma^{\dagger}_{xy}$. We choose $\Sigma'_{xy} = \Sigma'_{xy}$ and $\Sigma^{\dagger\dagger}_{xy} = \Sigma''_{xy}$.
We further use Rule SE-Reflection-xy to derive $X_{xy} \overset{O_{xy}}{\downarrow}^{xy}_{\varepsilon} X'_{xy}, X^{\dagger}_{xy} \overset{O_{xy}}{\downarrow}^{xy}_{\varepsilon} X^{\dagger\dagger}_{xy}$ with $X'_{xy} = X_{xy}$ and $X^{\dagger\dagger}_{xy} = X^{\dagger}_{xy}$. We now trivially satisfy all conclusions.

Rule AM-Single-xy We have $\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma''_{xy}$ with $\Sigma''_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma'_{xy}$ and $\Sigma^{\dagger}_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma^{*}_{xy}$ and $\Sigma^{*}_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma^{\dagger\dagger}_{xy}$.

We now apply IH on $\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma''_{xy}$ and $\Sigma^{\dagger}_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma^{*}_{xy}$ and get

(a) $X_{xy} \overset{O_{xy} \wr\!\downarrow^{xy}_{\overline{\tau}'}}{} X''_{xy}, X^{\dagger}_{xy} \overset{O_{xy} \wr\!\downarrow^{xy}_{\overline{\tau}''}}{} X^{*}_{xy}$
(b) $\Sigma''_{xy} \cong \Sigma^{*}_{xy}$
(c) $X''_{xy} \cong X^{*}_{xy}$ and $\overline{\rho}' = \emptyset$
(d) $\Sigma''_{xy} \approx^{O_{am}}_{xy} X''_{xy}$ and $\Sigma^{*}_{xy} \approx^{O_{am}}_{xy} X^{*}_{xy}$
(e) $\overline{\tau}' = \overline{\tau}''$

We do a case distinction on $\approx^{O_{am}}_{xy}$ in $\Sigma''_{xy} \approx^{O_{am}}_{xy} X''_{xy}$ and $\Sigma^{*}_{xy} \approx^{O_{am}} X^{*}_{xy}$:

Rule Comb:Single-Base-Oracle We thus have $\Sigma''_{xy} \sim X''_{xy}\restriction_{com}$, $minWndw(X''_{xy}) > 0$ and $INV2(\Sigma''_{xy}, X''_{xy})$ (Similar for Σ^{*}_{xy} and X^{*}_{xy}).

We now proceed by inversion on the derivation $\Sigma''_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma'_{xy}$:

Rule AM-x-Rollback-xy Contradiction, since $minWndw(X''_{xy}) > 0$ and $INV2(\Sigma''_{xy}, X''_{xy})$.

Rule AM-y-Rollback-xy Analogous to above.

Rule AM-Context-xy We have $\Phi_{xy} \overset{\tau}{\dashrightarrow}_{xy} \overline{\Phi}'_{xy}$ and $\overline{\Phi}'_{xy}.n > 0$.

By Relation Preservation we can find $X''_{xy} \overset{O_{xy} \wr\!\downarrow^{xy}_{\overline{\tau}^*}}{} X'_{xy}$ and have $\Sigma'_{xy} \approx_{xy} X'_{xy}$. Since $\Sigma''_{xy} \approx^{O_{am}}_{xy} X''_{xy}$ is related by Rule Comb:Single-Base-Oracle that $X''_{xy} \overset{O_{xy} \wr\!\downarrow^{xy}_{\overline{\tau}^*}}{} X'_{xy}$ was derived by Rule SE-Single-xy (otherwise $\Sigma'_{xy} \approx^{O_{am}}_{xy} X'_{xy}$ cannot hold) and as such we have $X''_{xy} \overset{\tau_{sp}}{\rightsquigarrow}{}^{O_{xy}}_{xy} X'_{xy}$.

This holds similar for $X^{\dagger}_{xy}$ such that we have $X^{*}_{xy} \overset{\tau_{sp'}}{\rightsquigarrow}{}^{O_{xy}}_{xy} X^{\dagger\dagger}_{xy}$.

By applying Assumption 1 (Oracle and AM steps in Lockstep produce the same observation) on $\Sigma^{*}_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma^{**}_{xy}$ and $X^{*}_{xy} \overset{\tau_{sp}}{\rightsquigarrow}{}^{O_{xy}}_{xy} X^{**}_{xy}$ we get that $\tau = \tau_{sp}$.

We can apply Assumption 1 (Oracle and AM steps in Lockstep produce the same observation) again on the steps $\Sigma''_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma'_{xy}$ and $X^{*}_{xy} \overset{\tau_{sp'}}{\rightsquigarrow}{}^{O_{xy}}_{xy} X^{\dagger}_{xy}$ with $\tau = \tau_{sp'}$. Since $\tau = \tau_{sp} = \tau_{sp'}$ we can conclude that $\tau_{sp} = \tau_{sp'}$.

The speculation window is reduced depending on the instruction that was executed in the step. If it was not a barrier instruction it is reduced by 1. Otherwise it is zeroed or if a new speculative instance is created, then the Oracle semantics uses the O^{xy}_{am} and the AM semantics the minimum between the maximal speculation window ω and the speculation window of the previous instance j. We refer the reader to Lemma 51 (V4AM: Strong Soundness Single Step) since the argument why $INV2()$ holds is the same. The combined oracle semantic reduces the speculation window in a similar fashion to the semantics described in the linked theorem.

Furthermore, it is trivial to derive $\Sigma'_{xy} \approx^{O_{am}}_{xy} X'_{xy}$ from $\Sigma'_{xy} \approx_{xy} X'_{xy}$ and the fact of $INV2(\Sigma'_{xy}, X'_{xy})$ as described above.

Rule Comb:Single-Transaction-Rollback-Oracle We have

$$\begin{aligned} X''_{xy} &= X_{xy_3} \cdot \Psi_{xy} \cdot \Psi'_{xy} \cdot X_{xy_4} \\ \Sigma''_{xy} &= \Sigma_{xy_3} \cdot \Phi_{xy} \cdot \Phi'_{xy} \cdot \Sigma_{xy_4} \\ X_{xy} &= X_{xy_3} \cdot \Psi_{xy} \\ \Sigma_{xy} &= \Sigma_{xy_3} \cdot \Phi_{xy} \\ \Sigma_{xy} &\sim X_{xy}\restriction_{com} \\ INV2(\Sigma_{xy}, X_{xy}) & \\ n' &\geq 0 \end{aligned}$$

The form of X^{*}_{xy} and Σ^{*}_{xy} is analogous.

Additionally, we know that the transaction terminates in some state $\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'''_{xy}$. There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma''_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma'_{xy}$ is not a roll back. Because Σ_{xy} and X_{xy} do not change, $INV2(\Sigma_{xy}, X_{xy})$ does not change as well.

$n' = 0$ Then we know that $\Sigma''_{xy} \overset{\tau}{\dashrightarrow}_{xy} \Sigma'_{xy}$ was created by Rule AM-x-Rollback-xy or Rule AM-y-Rollback-xy and is a rollback for ctr.

Notice, that the only difference to X_{xy} and Σ_{xy} is the updated ctr, because of the roll back. Updating the counter does not change the invariant $INV2()$. This means $INV2(\Sigma_{xy}, X_{xy})$ (with updated ctr) still holds.

□