Detecting speculative leaks with compositional semantics - Technical Report

XAVER FABIAN, CISPA Helmholtz Center for Information Security, Germany and University of Trento, Italy
MARCO GUARNIERI, IMDEA Software Institute, Spain
BORIS KÖPF, Azure Research, Microsoft, UK
JOSE F. MORALES, IMDEA Software Institute, Spain
MARCO PATRIGNANI, University of Trento, Italy
JAN REINEKE, Saarland University, Germany
ANDRES SANCHEZ, Amazon, Spain

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

Additional Key Words and Phrases: Spectre; Speculative Execution; Speculative information flows; Speculative non-interference

Authors' addresses: Xaver Fabian, CISPA Helmholtz Center for Information Security, Saarbrücken, Germany, xaver.fabian@cispa.de and University of Trento, Trento, Italy; Marco Guarnieri, IMDEA Software Institute, Madrid, Spain, marco.guarnieri@imdea.org; Boris Köpf, Azure Research, Microsoft, UK; Jose F. Morales, IMDEA Software Institute, Madrid, Spain; Marco Patrignani, University of Trento, Trento, Italy, marco.patrignani@unitn.it; Jan Reineke, Saarland University, Saarbrücken, Germany; Andres Sanchez, Amazon, Madrid, Spain.

A TRACE PROJECTIONS

Here, we formalize the speculative projections $\upharpoonright_x$ for each of our semantics and the non-speculative projection $\upharpoonright_{ns}$.

Non-speculative Trace Projection. Given a trace τ, its non-speculative projection contains only the observations that are produced by committed transactions; in other words, rolled-back transactions are removed in the projection. Formally, $\tau\upharpoonright_{ns}$ is defined as follows:

Definition 1 (Non-speculative projection)**.** *We define the non-speculative projection mutually recursive as*

$$\begin{aligned}
\varepsilon\upharpoonright_{ns} &= \varepsilon \\
\overline{\tau} \cdot \texttt{commit}_x\ n\upharpoonright_{ns} &= \overline{\tau}\upharpoonright_{ns} \\
\overline{\tau} \cdot \texttt{start}_x\ n\upharpoonright_{ns} &= \overline{\tau}\upharpoonright_{ns} \\
\overline{\tau} \cdot \texttt{rlb}_x\ id\upharpoonright_{ns} &= helper(\overline{\tau}, id) \\
\overline{\tau} \cdot \tau\upharpoonright_{ns} &= \overline{\tau}\upharpoonright_{ns} \cdot \tau \text{ otherwise}
\end{aligned}$$

The helper() is defined as

$$\begin{aligned}
helper(\varepsilon, id) &= \varepsilon \\
helper(\overline{\tau} \cdot \texttt{start}_x\ id, id) &= \overline{\tau}\upharpoonright_{ns} \\
helper(\overline{\tau} \cdot \tau, id) &= helper(\overline{\tau}, id) \text{ otherwise}
\end{aligned}$$

Speculative Trace Projections. Given a speculative trace τ, its speculative projection contains only the observations produced by rolled-back transactions.

Definition 2 (Speculative Projection)**.**

$$\begin{aligned}
\varepsilon\upharpoonright_{se} &= \varepsilon \\
\overline{\tau} \cdot \texttt{rlb}_x\ i\upharpoonright_{se} &= helper_{se}(\overline{\tau}, i) \\
\overline{\tau} \cdot \tau\upharpoonright_{se} &= \overline{\tau}\upharpoonright_{se} \text{ otherwise}
\end{aligned}$$

$$\begin{aligned}
helper_{se}(\varepsilon, id) &= \varepsilon \\
helper_{se}(\overline{\tau} \cdot \texttt{start}_x\ id, id) &= \overline{\tau}\upharpoonright_{se} \\
helper_{se}(\overline{\tau} \cdot \texttt{start}_x\ id', id) &= helper_{se}(\overline{\tau}, id) \text{ if } id \neq id' \\
helper_{se}(\overline{\tau} \cdot \texttt{rlb}_x\ id', id) &= helper_{se}(\overline{\tau}, id) \text{ if } id \neq id' \\
helper_{se}(\overline{\tau} \cdot \texttt{commit}_x\ id', id) &= helper_{se}(\overline{\tau}, id) \\
helper_{se}(\overline{\tau} \cdot \tau, id) &= helper_{se}(\overline{\tau}, id) \cdot \tau \text{ otherwise}
\end{aligned}$$

B TECHNICAL REPORT

While the main paper simplifies notation for clarity, this document details the full operational semantics. These differences are purely cosmetic and do not affect the validity of the proofs. We outline the specific notational deviations below.

B.1 Differences in Oracle Semantics

$$\frac{\langle p, \sigma'' \rangle \xrightarrow{\tau} \langle p, \sigma''' \rangle \qquad (\sigma''' \neq \sigma'' \uplus \delta \text{ or } p, \sigma' \vdash \text{fin})}{\overline{\Psi}_x \cdot \langle p, ctr, \sigma, h, n, \cdots \rangle \cdot \langle p, ctr', \sigma', h', 0, \cdots \rangle^{\langle \sigma'', \delta \rangle} \cdot \overline{\Psi}_x{}' \overset{\texttt{rlb}_x\ ctr \cdot \tau}{\rightsquigarrow}{}^{O_x}_{x} \overline{\Psi}_x \cdot \langle p, ctr', \sigma''', h', n-1, \cdots \rangle} \text{ (O-Rollback)}$$

$$\frac{\langle p, \sigma'' \rangle \xrightarrow{\tau} \langle p, \sigma''' \rangle \qquad (\sigma''' = \sigma'' \uplus \delta \text{ or } p, \sigma' \vdash \text{fin})}{\overline{\Psi}_x \cdot \langle p, ctr, \sigma, h, n, \cdots \rangle \cdot \langle p, ctr', \sigma', h', 0, \cdots \rangle^{\langle \sigma'', \delta \rangle} \cdot \overline{\Psi}_x{}' \overset{\texttt{commit}_x\ ctr}{\rightsquigarrow}{}^{O_x}_{x} \overline{\Psi}_x \cdot \langle p, ctr', \sigma', h', n, \cdots \rangle \cdot \overline{\Psi}_x{}'} \text{ (O-Commit)}$$

The rules in the paper (restated here for clarity) delay the decision if a speculation was right (commit) or wrong (rollback).

Here in the technical report, we instead know this when starting speculation.

This is fine, since when speculation is started and the oracle gives its prediction, we can check if that prediction is correct or not by comparing the predicted state with the current state after a non-speculative step. We then decorate the new speculative transaction with a boolean indicating if this state will be rolled back or committed.

This results in simpler rollback/commit rules and a slightly more involved rule for starting speculation. Here are the examples for changes in comparison for S. Here, the start of speculation is encapsulated in two rules. One starts a transaction that will be rolled back, while the other starts one that will be committed.

$$\frac{n' = 0 \text{ or p is stuck}}{\overline{\Psi}_4 \cdot \langle p, ctr, \sigma, h, n \rangle \cdot \langle p, ctr', \sigma', h', n' \rangle^{true} \cdot \overline{\Psi}_4' \overset{\texttt{rlb}\ ctr}{\rightsquigarrow}{}^{O}_{\mathsf{S}} \overline{\Psi}_4 \cdot \langle p, ctr', \sigma, h, n \rangle} \text{ (S:Rollback)}$$

$$\frac{}{\overline{\Psi}_4 \cdot \langle p, ctr, \sigma, h, n \rangle^b \cdot \langle p, ctr', \sigma', h', 0 \rangle^{false} \cdot \overline{\Psi}_4{}' \overset{\texttt{commit}_{\mathsf{S}}\ ctr}{\rightsquigarrow}{}^{O}_{\mathsf{S}} \overline{\Psi}_4 \cdot \langle p, ctr', \sigma', h', n \rangle^b \cdot \overline{\Psi}_4{}'} \text{ (S:Commit)}$$

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

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

Next, in δ was used as a partial state to update the current state $\sigma \uplus \delta$. In the technical report, we do not use δ and instead directly write the state changes in the speculation rule. Similarly, the oracle does not output a δ, and instead, the specific thing required for speculation,i.e., for branch speculation, it will return the branch to jump to.

C GENERAL NON-INTERFERENCE PROOFS

General note: These proofs assume that the speculative semantics is a well-formed speculative semantics. This is given for all the semantics present in the paper.

Corollary 1 (GNI implies SNI)**.** *If $p \vdash_x$ GNI then $p \vdash_x$ SNI.*

Proof.

Assume that $p \vdash_x$ GNI.

Let σ, σ' be two arbitrary initial configurations such that $\sigma \backsim_\phi \sigma'$.

Thus, using $\sigma \backsim_\phi \sigma'$ and unfolding $p \vdash NI$ we get $Beh_x^\omega(p, \sigma) = Beh_x^\omega(p, \sigma')$.

Furthermore, we can conclude $Beh_x^\omega(p, \sigma)\upharpoonright_{ns} = Beh_x^\omega(p, \sigma')\upharpoonright_{ns}$ from $Beh_x^\omega(p, \sigma) = Beh_x^\omega(p, \sigma')$ since $\upharpoonright_{ns}$ is a subtrace by definition.

Since σ, σ' are two arbitrary states such that $\sigma \backsim_\phi \sigma'$ and we have $Beh_x^\omega(p, \sigma) = Beh_x^\omega(p, \sigma')$ and $Beh_x^\omega(p, \sigma)\upharpoonright_{ns} = Beh_x^\omega(p, \sigma')\upharpoonright_{ns}$ we have $p \vdash_x$ SNI. □

Proposition 1 (GNI Decomposition)**.** *Given a policy ϕ and a program p: $p \vdash SeqCT \wedge p \vdash_x SNI \Leftrightarrow p \vdash_x GNI$*

Proof.

$\Rightarrow$

Assume that $p \vdash$ SeqCT and $p \vdash_x$ SNI.

Let σ, σ' be two arbitrary initial configurations such that $\sigma \backsim_\phi \sigma'$.

From $\sigma \backsim_\phi \sigma'$ and $p \vdash SeqCT$ we get $Beh_{NS}(p, \sigma) = Beh_{NS}(p, \sigma')$.

From NS Consistency and $Beh_x^\omega(p)\upharpoonright_{ns} = Beh_{NS}(p) = Beh_x^O(p)\upharpoonright_{ns}$ we get $Beh_x^\omega(p, \sigma)\upharpoonright_{ns} = Beh_{NS}(p, \sigma)$ and $Beh_x^\omega(p, \sigma')\upharpoonright_{ns} = Beh_{NS}(p, \sigma')$

From $Beh_{NS}(p, \sigma) = Beh_{NS}(p, \sigma')$ we get $Beh_x^\omega(p, \sigma)\upharpoonright_{ns} = Beh_x^\omega(p, \sigma')\upharpoonright_{ns}$

Together with $p \vdash_x$ SNI for which we fulfil the premise, we get $Beh_x^\omega(p, \sigma) = Beh_x^\omega(p, \sigma')$.

Since σ, σ' are two arbitrary states such that $\sigma \backsim_\phi \sigma'$ we have

$\sigma \backsim_\phi \sigma' \implies Beh_x^\omega(p, \sigma) = Beh_x^\omega(p, \sigma')$, which is $p \vdash_x$ GNI.

$\Leftarrow$

Assume that $p \vdash_x$ GNI.

We get $p \vdash_x$ SNI by applying Corollary 1.

It remains to prove $p \vdash$ SeqCT.

Let σ, σ' be two arbitrary initial configurations such that $\sigma \backsim_\phi \sigma'$.

Thus, using $\sigma \backsim_\phi \sigma'$ and unfolding $p \vdash_x NI$ we get $Beh_x^\omega(p, \sigma) = Beh_x^\omega(p, \sigma')$.

Furthermore, we can conclude $Beh_x^\omega(p, \sigma)\upharpoonright_{ns} = Beh_x^\omega(p, \sigma')\upharpoonright_{ns}$ from $Beh_x^\omega(p, \sigma) = Beh_x^\omega(p, \sigma')$ since $\upharpoonright_{ns}$ is a subtrace by definition.

And from NS Consistency we can conclude $Beh_{NS}(p, \sigma) = Beh_{NS}(p, \sigma')$ as well.

Since σ, σ' are two arbitrary states such that $\sigma \backsim_\phi \sigma'$ we have

$\sigma \backsim_\phi \sigma' \implies Beh_{NS}(p, \sigma) = Beh_{NS}(p, \sigma')$, which is $p \vdash$ SeqCT.

□

D μASM AND NS-SEMANTICS

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

Basic Types

$$
\begin{array}{rccl}
\text{(Registers)} & x & \in & \mathit{Regs} \\
\text{(Values)} & n, l & \in & \mathit{Vals} = \mathbb{N} \cup \{\bot\}
\end{array}
$$

Syntax

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

Fig. 1. 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 3. *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 4. *An 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.

$\boxed{\textit{Judgements}}$

$\sigma \xrightarrow{\tau} \sigma'$	*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 $\overline{\tau}$.*
$((p, \sigma)) \Omega_{NS} \overline{\tau}$	*Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.*

Expression evaluation

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

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

$$\text{(Skip)}\ \frac{p(a(\mathbf{pc})) = \mathbf{skip}}{\langle p, m, a\rangle \to \langle p, m, a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1]\rangle} \qquad \text{(Endbr)}\ \frac{p(a(\mathbf{pc})) = \mathbf{endbr}}{\langle p, m, a\rangle \to \langle p, m, a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1]\rangle}$$

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

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

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

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

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

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

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

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

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

The evaluation relation $\to$ captures individual steps in the execution of a μAsm program.

Further, we define some shorthand notation for common interactions:

Definition 5. *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 $\sigma = \langle m, a\rangle$:

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

$$\langle m, a\rangle(l \mapsto y) := \langle m(l \mapsto y), a\rangle \textit{with } l \in Vals\ y \in Vals$$

Definition 6. *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

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

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

$$\boxed{(p \times \mathit{InitConf}) \rightsquigarrow_{NS} \overline{\tau}}$$

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

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.

D.1 Symbolic Non-Speculative Semantics

Note that we pushed the symbolic path condition $\mathtt{symPc}()$ 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 μ. Thus, there is no difference to the way it was presented in the paper.

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**.

$$\text{(Endbr-Symb)}\ \frac{p(sa(\mathbf{pc})) = \mathbf{endbr}}{\langle p, sm, sa, \delta^{\mathcal{S}} \rangle \to \langle p, sm, sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1], \delta^{\mathcal{S}} \rangle}$$

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

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

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

Symbolic expressions. Symbolic expressions represent computations over symbolic values. A *symbolic expression se* is a concrete value $n \in \mathit{Vals}$, a symbolic value $s \in \mathit{SymbVals}$, an if-then-else expression $\mathbf{ite}(se, se', se'')$, or the application of a unary $\ominus$ or a binary operator $\otimes$.

$$se := n \mid s \mid \mathbf{ite}(se, se', se'') \mid \ominus se \mid se \otimes se'$$

Symbolic memories. We model symbolic memories as symbolic arrays using the standard theory of arrays. That is, we model memory updates as triples of the form $\mathbf{write}(sm, se, se')$, which updates the symbolic memory *sm* by assigning the symbolic value se' to the symbolic location *se*, and memory reads as $\mathbf{read}(sm, se)$, which denote retrieving the value assigned to the symbolic expression *se*.

A *symbolic memory sm* is either a function $mem : \mathbb{N} \to \mathit{SymbVals}$ mapping memory addresses to symbolic values or a term $\mathbf{write}(sm, se, se')$, where *sm* is a symbolic memory and se, se' are symbolic expressions. To account for symbolic

Expression evaluation

$$\begin{array}{ll}
[\![n]\!](a) = n & \text{if } n \in \mathit{Vals} \\
[\![se]\!](a) = se & \text{if } sa \in \mathit{SymbExprs} \setminus \mathit{Vals} \\
[\![x]\!](a) = a(x) & \text{if } x \in \mathit{Regs} \\
[\![\ominus e]\!](a) = \mathit{apply}(\ominus, [\![e]\!](a)) & \text{if } [\![e]\!](a) \in \mathit{Vals} \\
[\![\ominus e]\!](a) = \ominus [\![e]\!](a) & \text{if } [\![e]\!](a) \in \mathit{SymbExprs} \setminus \mathit{Vals} \\
[\![e_1 \otimes e_2]\!](a) = \mathit{apply}(\otimes, [\![e_1]\!](a), [\![e_2]\!](a)) & \text{if } [\![e_1]\!](a), [\![e_2]\!](a) \in \mathit{Vals} \\
[\![e_1 \otimes e_2]\!](a) = [\![e_1]\!](a) \otimes [\![e_2]\!](a) & \text{if } [\![e_1]\!](a) \in \mathit{SymbExprs} \setminus \mathit{Vals} \\
[\![e_1 \otimes e_2]\!](a) = [\![e_1]\!](a) \otimes [\![e_2]\!](a) & \text{if } [\![e_2]\!](a) \in \mathit{SymbExprs} \setminus \mathit{Vals}
\end{array}$$

Instruction evaluation

Skip

$$\frac{p(sa(\mathbf{pc})) = \mathbf{skip}}{\langle p, sm, sa, \delta^{\mathcal{S}} \rangle \to_s \langle p, sm, sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1], \delta^{\mathcal{S}} \rangle}$$

Barrier

$$\frac{p(sa(\mathbf{pc})) = \mathbf{spbarr}}{\langle p, sm, sa, \delta^{\mathcal{S}} \rangle \to_s \langle p, sm, sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1], \delta^{\mathcal{S}} \rangle}$$

Assign

$$\frac{p(sa(\mathbf{pc})) = x \leftarrow e \qquad x \neq \mathbf{pc}}{\langle p, sm, sa, \delta^{\mathcal{S}} \rangle \to_s \langle p, sm, sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto [\![e]\!](sa)], \delta^{\mathcal{S}} \rangle}$$

ConditionalUpdate-Concr-Sat

$$\frac{p(sa(\mathbf{pc})) = x \xleftarrow{e'?} e \qquad [\![e']\!](sa) = 0 \qquad x \neq \mathbf{pc}}{\langle p, sm, sa, \delta^{\mathcal{S}} \rangle \to_s \langle p, sm, sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto [\![e]\!](sa)], \delta^{\mathcal{S}} \rangle}$$

ConditionalUpdate-Concr-Unsat

$$\frac{p(sa(\mathbf{pc})) = x \xleftarrow{e'?} e \qquad [\![e']\!](sa) = n \qquad n \in \mathit{Vals} \qquad n \neq 0 \qquad x \neq \mathbf{pc}}{\langle p, sm, sa, \delta^{\mathcal{S}} \rangle \to_s \langle p, sm, sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1], \delta^{\mathcal{S}} \rangle}$$

ConditionalUpdate-Symb

$$\frac{p(sa(\mathbf{pc})) = x \xleftarrow{e'?} e \qquad [\![e']\!](sa) = se \qquad se \notin \mathit{Vals} \qquad x \neq \mathbf{pc}}{\langle p, sm, sa, \delta^{\mathcal{S}} \rangle \to_s \langle p, sm, sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto \mathbf{ite}(se = 0, [\![e]\!](sa), sa(x))], \delta^{\mathcal{S}} \rangle}$$

Load-Symb

$$\frac{p(sa(\mathbf{pc})) = \mathbf{load}\ x, e \qquad x \neq \mathbf{pc} \qquad se = [\![e]\!](sa) \qquad se' = \mathbf{read}(sm, se)}{\langle p, sm, sa, \delta^{\mathcal{S}} \rangle \xrightarrow{\mathtt{load}\ se}_s \langle sm, sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto se'], \delta^{\mathcal{S}} \rangle}$$

Store-Symb

$$\frac{p(sa(\mathbf{pc})) = \mathbf{store}\ x, e \qquad se = [\![e]\!](sa) \qquad sm' = \mathbf{write}(sm, se, sa(x))}{\langle p, sm, sa, \delta^{\mathcal{S}} \rangle \xrightarrow{\mathtt{store}\ se}_s \langle p, sm', sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1], \delta^{\mathcal{S}} \rangle}$$

Beqz-Concr-Sat

$$\frac{p(sa(\mathbf{pc})) = \mathbf{beqz}\ x, \ell \qquad sa(x) = 0 \qquad sa(x) \in \mathit{Vals}}{\langle p, sm, sa, \delta^{\mathcal{S}} \rangle \xrightarrow{\mathtt{pc}\ \ell}_s \langle p, sm, sa[\mathbf{pc} \mapsto \ell], \delta^{\mathcal{S}} \cdot \mathtt{symPc}(\top) \rangle}$$

Beqz-Symb-Sat

$$\frac{p(sa(\mathbf{pc})) = \mathbf{beqz}\ x, \ell \qquad sa(x) \notin \mathit{Vals}}{\langle p, sm, sa, \delta^{\mathcal{S}} \rangle \xrightarrow{\mathtt{pc}\ \ell}_s \langle p, sm, sa[\mathbf{pc} \mapsto \ell], \delta^{\mathcal{S}} \cdot \mathtt{symPc}(sa(x) = 0) \rangle}$$

Beqz-Concr-Unsat

$$\frac{p(sa(\mathbf{pc})) = \mathbf{beqz}\ x, \ell \qquad sa(x) \neq 0 \qquad sa(x) \in \mathit{Vals}}{\langle p, sm, sa, \delta^{\mathcal{S}} \rangle \xrightarrow{\mathtt{pc}\ sa(\mathbf{pc})+1}_s \langle p, sm, sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1], \delta^{\mathcal{S}} \cdot \mathtt{symPc}(\top) \rangle}$$

Beqz-Symb-Unsat

$$\frac{p(sa(\mathbf{pc})) = \mathbf{beqz}\ x, \ell \qquad sa(x) \notin \mathit{Vals}}{\langle p, sm, sa, \delta^{\mathcal{S}} \rangle \xrightarrow{\mathtt{pc}\ sa(\mathbf{pc})+1}_s \langle p, sm, sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1], \delta^{\mathcal{S}} \cdot \mathtt{symPc}(sa(x) \neq 0) \rangle}$$

Jmp-Concr

$$\frac{p(sa(\mathbf{pc})) = \mathbf{jmp}\ e \qquad \ell = [\![e]\!](sa) \qquad \ell \in \mathit{Vals}}{\langle p, sm, sa, \delta^{\mathcal{S}} \rangle \xrightarrow{\mathtt{pc}\ \ell}_s \langle p, sm, sa[\mathbf{pc} \mapsto \ell], \delta^{\mathcal{S}} \cdot \mathtt{symPc}(\top) \rangle}$$

Jmp-Symb

$$\frac{p(sa(\mathbf{pc})) = \mathbf{jmp}\ e \qquad [\![e]\!](sa) \notin \mathit{Vals} \qquad \ell \in \mathit{Vals}}{\langle p, sm, sa, \delta^{\mathcal{S}} \rangle \xrightarrow{\mathtt{pc}\ \ell}_s \langle p, sm, sa[\mathbf{pc} \mapsto \ell], \delta^{\mathcal{S}} \cdot \mathtt{symPc}([\![e]\!](sa) = \ell) \rangle}$$

Terminate

$$\frac{p(sa(\mathbf{pc})) = \bot}{\langle p, sm, sa, \delta^{\mathcal{S}} \rangle \to_s \langle p, sm, sa[\mathbf{pc} \mapsto \bot], \delta^{\mathcal{S}} \rangle}$$

Fig. 2. μAsm symbolic non-speculative semantics for a program p

memories, we extend symbolic expressions with terms of the form $\mathbf{read}(sm, se)$, where sm is a symbolic memory and se is a symbolic expression, representing memory reads.

$$sm := mem \mid \mathbf{write}(sm, se, se')$$
$$se := \ldots \mid \mathbf{read}(sm, se)$$

Evaluating symbolic expressions. The value of a symbolic expression se depends on a *valuation* $\mu : SymbVals \to Vals$ mapping symbolic values to concrete ones:

$$\begin{aligned}
\mu(n) &= n \text{ if } n \in Vals \\
\mu(s) &= \mu(s) \text{ if } s \in SymbVals \\
\mu(\mathbf{ite}(se, se', se'')) &= \mu(se') \text{ if } \mu(se) \neq 0 \\
\mu(\mathbf{ite}(se, se', se'')) &= \mu(se'') \text{ if } \mu(se) = 0 \\
\mu(\ominus se) &= \ominus \mu(se) \\
\mu(se \otimes se') &= \mu(se) \otimes \mu(se') \\
\mu(mem) &= \mu \circ mem \\
\mu(\mathbf{write}(sm, se, se')) &= \mu(sm)[\mu(se) \mapsto \mu(se')] \\
\mu(\mathbf{read}(sm, se)) &= \mu(sm)(\mu(se))
\end{aligned}$$

An expression se is *satisfiable* if there is a valuation μ satisfying it, i.e., $\mu(se) \neq 0$.

Symbolic assignments. A *symbolic assignment* sa is a function mapping registers to symbolic expressions $sa : Regs \to SymbExprs$. Given a symbolic assignment sa and a valuation μ, $\mu(sa)$ denotes the assignment $\mu \circ sa$. We assume the program counter **pc** to always be concrete, i.e., $sa(\mathbf{pc}) \in Vals$.

Symbolic configurations. A *symbolic configuration* is a pair $\langle p, sm, sa \rangle$ consisting of a symbolic memory sm and a symbolic assignment sa. We lift speculative states to symbolic configurations.

Symbolic observations. When symbolically executing a program, we may produce observations whose value is symbolic. To account for this, we introduce symbolic observations of the form `load` se and `store` se, which are produced when symbolically executing **load** and **store** commands, and `symPc`(se), produced when symbolically evaluating branching instructions, where se is a symbolic expression. In our symbolic semantics, we use the observations `symPc`(se) to represent the symbolic path condition indicating when a path is feasible. Given a sequence of symbolic observations τ and a valuation μ, $\mu(\tau)$ denotes the trace obtained by (1) dropping all observations `symPc`(se), and (2) evaluating all symbolic observations different from `symPc`(se) under μ.

Symbolic semantics. The *non-speculative* semantics is captured by the relation $\to_s$ in Fig. 2.

Computing symbolic runs and traces. We now fix the symbolic values. The set *SymbVals* consists of a symbolic value x_s for each register identifier x and of a symbolic value mem_s^n for each memory address n. We also fix the initial symbolic memory $sm_0 = \lambda n \in \mathbb{N}.\ m_s^n$ and the symbolic assignment sa_0 such that $sa_0(\mathbf{pc}) = 0$ and $sa_0(x) = x_s$.

$$\boxed{\Sigma_{x_S}\ {}_{S}{\Downarrow}_{x}^{\overline{\tau_S}}\ \Sigma'_{x_S}}$$

$$\frac{}{\Sigma_{x_{\mathcal{S}}}\ {}_{\mathcal{S}}{\Downarrow}_x^{\varepsilon}\ \Sigma_{x_{\mathcal{S}}}}\ \text{(NS:Sym-Reflection)} \qquad \frac{\Sigma_{x_{\mathcal{S}}}\ {}_{\mathcal{S}}{\Downarrow}_x^{\overline{\tau_{\mathcal{S}}}}\ \Sigma''_{x_{\mathcal{S}}} \qquad \Sigma''_{x_{\mathcal{S}}} \overset{\tau_{\mathcal{S}}}{\text{👻}}{}_x^{\mathcal{S}}\ \Sigma'_{x_{\mathcal{S}}}}{\Sigma_{x_{\mathcal{S}}}\ {}_{\mathcal{S}}{\Downarrow}_x^{\overline{\tau_{\mathcal{S}}}\cdot\tau_{\mathcal{S}}}\ \Sigma'_{x_{\mathcal{S}}}}\ \text{(NS:Sym-Single)}$$

Helpers

$$\frac{\sigma_{\mathcal{S}} \in \mathit{InitConf}}{\vdash \Sigma_{x_{\mathcal{S}}} : \mathit{init}}\ \text{(NS:Sym-Init)} \qquad \frac{\sigma_{\mathcal{S}}(\mathbf{pc}) = \bot}{\vdash \sigma_{\mathcal{S}} : \mathit{fin}}\ \text{(NS-Sym-Fin)}$$

$$\frac{\exists \sigma'_{\mathcal{S}} \qquad \vdash \sigma_{\mathcal{S}}' : \mathit{fin} \qquad (p, \sigma_{\mathcal{S}})\ {}_{\mathcal{S}}{\Downarrow}_{\overline{\tau_{\mathcal{S}}}}\ \langle p, \sigma_{\mathcal{S}}' \rangle}{((p, \sigma_{\mathcal{S}}))\ \text{👻}_{NS}\overline{\tau_{\mathcal{S}}}}\ \text{(NS:Sym-Trace)} \qquad \frac{}{\mathit{Beh}_x^{\mathcal{S}}(p) = \{\overline{\tau_{\mathcal{S}}} \mid \forall \sigma_{\mathcal{S}} \in \mathit{InitConf}.\ (p, \sigma_{\mathcal{S}})\text{👻}_x^{\omega}\overline{\tau_{\mathcal{S}}}\}}\ \text{(NS:Sym-Beh)}$$

The set $\mathit{Beh}_{NS}^{\mathcal{S}}(p)$ contains all runs that can be derived using the symbolic non-speculative semantics starting from the initial configuration $\sigma_{\mathcal{S}}$.

E NS: RELATION SYMBOLIC AND CONCRETE NON-SPECULATIVE SEMANTICS

Theorem 1 (NS: Symbolic Consistency). *$\mathit{Beh}_{NS}(p) = \mu(\mathit{Beh}_{NS}^{\mathcal{S}}(p))$.*

Proof. Immediate from Lemma 2 (NS: Soundness Symbolic) and Lemma 4 (NS: Completeness Symbolic) □

E.1 Auxiliary lemmas

Lemma 1 provides some useful helping facts, which we will use throughout the soundness proof.

Lemma 1. *The following facts hold:*

1. *Given a symbolic assignment sa and a valuation $\mu : \mathit{SymbVals} \to \mathit{Vals}$, then $\mu(sa)(x) = \mu(sa(x))$ for all $x \in \mathit{Regs}$.*
2. *Given a symbolic memory sa and a valuation $\mu : \mathit{SymbVals} \to \mathit{Vals}$, then $\mu(sm)(n) = \mu(sm(n))$ for all $n \in \mathit{Addrs}$.*
3. *Given a symbolic assignment sa, an expression e, and a valuation $\mu : \mathit{SymbVals} \to \mathit{Vals}$, then $\mu([\![e]\!](sa)) = [\![e]\!](\mu(sa))$.*

Proof. Below we prove all our claims.

Proof of (1). Let sa be a symbolic assignment and $\mu : \mathit{SymbVals} \to \mathit{Vals}$. Then, $\mu(sa)$ is defined as $\mu \circ sa$. Hence, $\mu(sa)(x) = \mu(sa(x))$.

Proof of (2). Identical to (1).

Proof of (3). Let sa be a symbolic assignment, e be an expression, and $\mu : \mathit{SymbVals} \to \mathit{Vals}$. We show, by structural induction on e, that $\mu([\![e]\!](sa)) = [\![e]\!](\mu(sa))$. For the base case, there are two possibilities. If e is a value $n \in \mathit{Vals}$, then $[\![n]\!](sa) = n$, $[\![n]\!](\mu(sa)) = n$, and $\mu(n) = n$. Hence, $\mu([\![e]\!](sa)) = [\![e]\!](\mu(sa))$. If e is a register identifier $x \in \mathit{Regs}$, then $[\![x]\!](\mu(sa)) = \mu(sa)(x)$ and $\mu([\![e]\!](sa)) = \mu(sa(x))$. From this and (1), we get $\mu([\![e]\!](sa)) = [\![e]\!](\mu(sa))$. For the induction step, there two cases. If e is of the form $\ominus e'$, then $[\![\ominus e']\!](\mu(sa)) = \mathit{apply}(\ominus, [\![e']\!](\mu(sa)))$, whereas $\mu([\![\ominus e']\!](sa))$ is either $\mu(\mathit{apply}(\ominus, [\![e']\!](sa)))$ if $[\![e']\!](sa) \in \mathit{Vals}$ or $\mu(\ominus[\![e']\!](sa))$ otherwise. In the first case, $\mu(\mathit{apply}(\ominus, [\![e']\!](\mu(sa)))) = \mathit{apply}(\ominus, [\![e']\!](sa))$ (since we are dealing only with concrete values) and $[\![e']\!](\mu(sa)) = [\![e']\!](sa)$ since $[\![e']\!](sa) \in \mathit{Vals}$. Therefore, $\mu([\![e]\!](sa)) = [\![e]\!](\mu(sa))$. In the second case, $\mu(\ominus[\![e']\!](sa)) = \mathit{apply}(\ominus, \mu([\![e']\!](sa)))$. By applying the induction hypothesis ($[\![e']\!](\mu(sa)) = \mu([\![e']\!](sa))$, we obtain $\mu(\ominus[\![e']\!](sa)) = apply(\ominus, [\![e']\!](\mu(sa)))$. Hence, $\mu([\![e]\!](sa)) = [\![e]\!](\mu(sa))$. The proof for the second case (i.e., $e = e_1 \otimes e_2$) is similar. □

E.2 Soundness

Note that Soundness is split up into two lemmas: 2 and Lemma 3.

In Lemma 2, we prove the soundness of the symbolic non-speculative semantics.

Lemma 2 (NS: Soundness Symbolic)**.** *Let p be a program. Whenever $\langle sm, sa\rangle \xrightarrow{\tau}_s \langle sm', sa'\rangle$, then for all mappings $\mu : SymbVals \to Vals$ such that $\mu \models pthCnd(\tau)$, $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\mu(\tau)} \langle \mu(sm'), \mu(sa')\rangle$.*

Proof. Let p be a program. Assume that $\langle sm, sa\rangle \xrightarrow{\tau}_s \langle sm', sa'\rangle$ holds. We proceed by case distinction on the rules defining $\to_s$.

Rule Skip. Assume that $\langle sm, sa\rangle \xrightarrow{\tau}_s \langle sm', sa'\rangle$ has been derived using the Skip rule in the symbolic semantics. Then, $p(a(\mathbf{pc})) = \mathbf{skip}$, $sm' = sm$, $\tau = \varepsilon$, and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1]$. Let $\mu : SymbVals \to Vals$ be an arbitrary valuation satisfying $pthCnd(\tau)$ (since $pthCnd(\tau)$ is $\top$ all valuations are models of $pthCnd(\tau)$). Observe that $\mu(sa)(\mathbf{pc}) = sa(\mathbf{pc})$ since the program counter is always concrete. Hence, $p(\mu(sa)(\mathbf{pc})) = \mathbf{skip}$. Thus, we can apply the rule Skip of the concrete semantics starting from $\langle \mu(sm), \mu(sa)\rangle$. Hence, $\langle \mu(sm), \mu(sa)\rangle \to \langle \mu(sm), \mu(sa)[\mathbf{pc} \mapsto \mu(sa)(\mathbf{pc}) + 1]\rangle$. From this, $\mu(\tau) = \varepsilon$ (since $\tau = \varepsilon$), and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1]$, we have that $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\mu(\tau)} \langle \mu(sm'), \mu(sa')\rangle$.

Rule Barrier. The proof of this case is analogous to that of Skip.

Rule Assign. Assume that $\langle sm, sa\rangle \xrightarrow{\tau}_s \langle sm', sa'\rangle$ has been derived using the Assign rule in the symbolic semantics. Then, $p(a(\mathbf{pc})) = x \leftarrow e$, $x \neq \mathbf{pc}$, $sm' = sm$, $\tau = \varepsilon$, and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto [\![e]\!](sa)]$. Let $\mu : SymbVals \to Vals$ be an arbitrary valuation (since $pthCnd(\tau)$ is $\top$ all valuations are models of $pthCnd(\tau)$). Observe that $\mu(sa)(\mathbf{pc}) = sa(\mathbf{pc})$ since the program counter is always concrete. Hence, $p(\mu(sa)(\mathbf{pc})) = x \leftarrow e$. Thus, we can apply the rule Assign of the concrete semantics starting from $\langle \mu(sm), \mu(sa)\rangle$. Hence, $\langle \mu(sm), \mu(sa)\rangle \to \langle \mu(sm), \mu(sa)[\mathbf{pc} \mapsto \mu(sa)(\mathbf{pc}) + 1, x \mapsto [\![e]\!](\mu(sa))]\rangle$. From this, Lemma 1, $\mu(\tau) = \varepsilon$ (since $\tau = \varepsilon$), and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto [\![e]\!](sa)]$, we have that $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\mu(\tau)} \langle \mu(sm'), \mu(sa')\rangle$.

Rule ConditionalUpdate-Concr-Sat. Assume that $\langle sm, sa\rangle \xrightarrow{\tau}_s \langle sm', sa'\rangle$ has been derived using the ConditionalUpdate-Concr-Sat rule in the symbolic semantics. Then, $p(a(\mathbf{pc})) = x \xleftarrow{e'?} e$, $x \neq \mathbf{pc}$, $sm' = sm$, $\tau = \varepsilon$, $[\![e']\!](sa) = 0$, and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto [\![e]\!](sa)]$. Let $\mu : SymbVals \to Vals$ be an arbitrary valuation (since $pthCnd(\tau)$ is $\top$ all valuations are models of $pthCnd(\tau)$). Observe that $\mu(sa)(\mathbf{pc}) = sa(\mathbf{pc})$ since the program counter is always concrete. Hence, $p(\mu(sa)(\mathbf{pc})) = x \xleftarrow{e'?} e$. Thus, we can apply one of the rules ConditionalUpdate-Sat or ConditionalUpdate-Unsat of the concrete semantics starting from $\langle \mu(sm), \mu(sa)\rangle$. We claim that $[\![e']\!](\mu(sa)) = 0$. Therefore, we can apply the rule ConditionalUpdate-Sat. Hence, $\langle \mu(sm), \mu(sa)\rangle \to \langle \mu(sm), \mu(sa)[\mathbf{pc} \mapsto \mu(sa)(\mathbf{pc}) + 1, x \mapsto [\![e]\!](\mu(sa))]\rangle$. From this, Lemma 1, $\mu(\tau) = \varepsilon$ (since $\tau = \varepsilon$), and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto [\![e]\!](sa)]$, we have that $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\mu(\tau)} \langle \mu(sm'), \mu(sa')\rangle$.
We now show that $[\![e']\!](\mu(sa))$ is indeed 0. Since $[\![e']\!](sa) = 0$, the value of e' depends only on registers in sa whose value is concrete. Hence, for all these registers x, $\mu(sa)(x) = sa(x)$. Thus, $[\![e']\!](\mu(sa)) = [\![e']\!](sa) = 0$.

Rule ConditionalUpdate-Concr-Unsat. The proof of this case is analogous to that of ConditionalUpdate-Concr-Unsat.

Rule ConditionalUpdate-Symb. Assume that $\langle sm, sa\rangle \xrightarrow{\tau}_s \langle sm', sa'\rangle$ has been derived using the ConditionalUpdate-Symb rule in the symbolic semantics. Then, $p(a(\mathbf{pc})) = x \xleftarrow{e'?} e$, $x \neq \mathbf{pc}$, $sm' = sm$, $\tau = \varepsilon$, $[\![e']\!](sa) = se$, $se \notin \mathit{Vals}$, and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto \mathbf{ite}(se = 0, [\![e]\!](sa), sa(x))]$. Let $\mu : \mathit{SymbVals} \to \mathit{Vals}$ be an arbitrary valuation (since $\mathit{pthCnd}(\tau)$ is $\top$ all valuations are models of $\mathit{pthCnd}(\tau)$). Observe that $\mu(sa)(\mathbf{pc}) = sa(\mathbf{pc})$ since the program counter is always concrete. Hence, $p(\mu(sa)(\mathbf{pc})) = x \xleftarrow{e'?} e$.

There are two cases:

$\mu \models se = 0$: Then, $\mu(se) = 0$ and therefore $[\![e']\!](\mu(sa)) = 0$. Hence, we can apply the rule ConditionalUpdate-Sat starting from $\langle \mu(sm), \mu(sa)\rangle$. Therefore, we get $\langle \mu(sm), \mu(sa)\rangle \to \langle \mu(sm), \mu(sa)[\mathbf{pc} \mapsto \mu(sa)(\mathbf{pc}) + 1, x \mapsto [\![e]\!](\mu(sa))]\rangle$. To prove our claim, we have to show that $\mu(sa') = \mu(sa)[\mathbf{pc} \mapsto \mu(sa)(\mathbf{pc}) + 1, x \mapsto [\![e]\!](\mu(sa))]$. From $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto \mathbf{ite}(se = 0, [\![e]\!](sa), sa(x))]$, it is enough to show that $\mu(\mathbf{ite}(se = 0, [\![e]\!](sa), sa(x))) = [\![e]\!](\mu(sa))$. Since $\mu \models se = 0$, $\mu(\mathbf{ite}(se = 0, [\![e]\!](sa), sa(x)))$ is equivalent to $\mu([\![e]\!](sa))$. From this and Lemma 1, $\mu([\![e]\!](sa)) = [\![e]\!](\mu(sa))$. Hence, we have that $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\mu(\tau)} \langle \mu(sm'), \mu(sa')\rangle$.

$\mu \not\models se = 0$: Then, $\mu(se) \neq 0$ and therefore $[\![e']\!](\mu(sa)) \neq 0$. Hence, we can apply the rule ConditionalUpdate-Unsat starting from $\langle \mu(sm), \mu(sa)\rangle$. Therefore, we get $\langle \mu(sm), \mu(sa)\rangle \to \langle \mu(sm), \mu(sa)[\mathbf{pc} \mapsto \mu(sa)(\mathbf{pc}) + 1]\rangle$. To prove our claim, we have to show that $\mu(sa') = \mu(sa)[\mathbf{pc} \mapsto \mu(sa)(\mathbf{pc}) + 1]$. From $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto \mathbf{ite}(se = 0, [\![e]\!](sa), sa(x))]$, it is enough to show that $\mu(\mathbf{ite}(se = 0, [\![e]\!](sa), sa(x))) = \mu(sa)(x)$. Since $\mu \not\models se = 0$, $\mu(\mathbf{ite}(se = 0, [\![e]\!](sa), sa(x)))$ is equivalent to $\mu(sa(x))$. From this and Lemma 1, $\mu(sa(x)) = \mu(sa)(x)$. Hence, we have that $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\mu(\tau)} \langle \mu(sm'), \mu(sa')\rangle$.

This completes the proof of this case.

Rule Load-Symb. Assume that $\langle sm, sa\rangle \xrightarrow{\tau}_s \langle sm', sa'\rangle$ has been derived using the Load-Symb rule in the symbolic semantics. Then, $p(a(\mathbf{pc})) = \mathbf{load}\ x, e$, $x \neq \mathbf{pc}$, $sm' = sm$, $se = [\![e]\!](sa)$, $\tau = \texttt{load}\ se$, and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto \mathbf{read}(sm, se)]$. Let $\mu : \mathit{SymbVals} \to \mathit{Vals}$ be an arbitrary valuation (since $\mathit{pthCnd}(\tau) = \top$ all valuations μ are valid models). Observe that $\mu(sa)(\mathbf{pc}) = sa(\mathbf{pc})$ since the program counter is always concrete. Hence, $p(\mu(sa)(\mathbf{pc})) = \mathbf{load}\ x, e$ and $x \neq \mathbf{pc}$. Thus, we can apply the rule Load of the concrete semantics starting from $\langle \mu(sm), \mu(sa)\rangle$. Hence, $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\texttt{load}\ [\![e]\!](\mu(sa))} \langle \mu(sm), \mu(sa)[\mathbf{pc} \mapsto \mu(sa)(\mathbf{pc}) + 1, x \mapsto \mu(sm)([\![e]\!](\mu(sa)))]\rangle$.

Observe that $\mu([\![e]\!](sa)) = [\![e]\!](\mu(sa))$ (from Lemma 1), and therefore $\mu(\texttt{load}\ [\![e]\!](sa)) = \texttt{load}\ [\![e]\!](\mu(sa))$. We claim that $\mu(\mathbf{read}(sm, se)) = \mu(sm)([\![e]\!](\mu(sa)))$. From this, $\mu(sa)[\mathbf{pc} \mapsto \mu(sa)(\mathbf{pc})+1, x \mapsto \mu(sm)([\![e]\!](\mu(sa)))] = \mu(sa')$. Therefore, $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\mu(\tau)} \langle \mu(sm'), \mu(sa')\rangle$.

We now show that $\mu(\mathbf{read}(sm, se)) = \mu(sm)([\![e]\!](\mu(sa)))$. From the evaluation of symbolic expressions, we have that $\mu(\mathbf{read}(sm, se))$ is equivalent to $\mu(sm)(\mu(se))$. From this and $se = [\![e]\!](sa)$, we have $\mu(\mathbf{read}(sm, se)) = \mu(sm)(\mu([\![e]\!](sa)))$. From this and Lemma 1, we get $\mu(\mathbf{read}(sm, se)) = \mu(sm)([\![e]\!](\mu(sa)))$.

Rule Store-Symb. Assume that $\langle sm, sa\rangle \xrightarrow{\tau}_s \langle sm', sa'\rangle$ has been derived using the Store-Symb rule in the symbolic semantics. Then, $p(a(\mathbf{pc})) = \mathbf{store}\ x, e$, $se = [\![e]\!](sa)$, $sm' = \mathbf{write}(sm, se, sa(x))$, $\tau = \texttt{store}\ se$, and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1]$. Let $\mu : \mathit{SymbVals} \to \mathit{Vals}$ be an arbitrary valuation (since $\mathit{pthCnd}(\tau) = \top$ all valuations are valid models). Observe that $\mu(sa)(\mathbf{pc}) = sa(\mathbf{pc})$ since the program counter is always concrete. Hence, $p(\mu(sa)(\mathbf{pc})) = \mathbf{store}\ x, e$. Thus, we can apply the rule Store of the concrete semantics starting from $\langle \mu(sm), \mu(sa)\rangle$. Hence, $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\texttt{store}\ [\![e]\!](\mu(sa))} \langle \mu(sm)[[\![e]\!](\mu(sa)) \mapsto \mu(sa)(x)], \mu(sa)[\mathbf{pc} \mapsto \mu(sa)(\mathbf{pc}) + 1]\rangle$.

Observe that (1) $\mu(\llbracket e \rrbracket(sa)) = \llbracket e \rrbracket(\mu(sa))$ (from Lemma 1) and therefore $\mu(\texttt{store}\ \llbracket e \rrbracket(sa)) = \texttt{store}\ \llbracket e \rrbracket(\mu(sa))$, and (2) $\mu(sa)[\mathbf{pc} \mapsto \mu(sa)(\mathbf{pc}) + 1] = \mu(sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1])$. Moreover, we claim that $\mu(sm)[\llbracket e \rrbracket(\mu(sa)) \mapsto \mu(sa)(x)] = \mu(\mathbf{write}(sm, se, sa(x)))$. Therefore, $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\mu(\tau)} \langle \mu(sm'), \mu(sa')\rangle$.

We now prove our claim that $\mu(sm)[\llbracket e \rrbracket(\mu(sa)) \mapsto \mu(sa)(x)] = \mu(\mathbf{write}(sm, se, sa(x)))$. From the evaluation of symbolic expressions, we have that $\mu(\mathbf{write}(sm, se, sa(x)))$ is equivalent to $\mu(sm)[\mu(se) \mapsto \mu(sa(x))]$. From $se = \llbracket e \rrbracket(sa)$, we have $\mu(\mathbf{write}(sm, se, sa(x))) = \mu(sm)[\mu(\llbracket e \rrbracket(sa)) \mapsto \mu(sa(x))]$. From Lemma 1, we have $\mu(\mathbf{write}(sm, se, sa(x))) = \mu(sm)[\llbracket e \rrbracket(\mu(sa)) \mapsto \mu(sa)(x)]$.

Rule Beqz-Concr-Sat. Assume that $\langle sm, sa\rangle \xrightarrow{\tau}_s \langle sm', sa'\rangle$ has been derived using the Beqz-Concr-1 rule in the symbolic semantics. Then, $p(a(\mathbf{pc})) = \mathbf{beqz}\ x, \ell$, $sa(x) = 0$, $sa(x) \in \mathit{Vals}$, $sm' = sm$, $\tau = \texttt{symPc}(\top) \cdot \texttt{pc}\ \ell$, and $sa' = sa[\mathbf{pc} \mapsto \ell]$. Let $\mu : \mathit{SymbVals} \to \mathit{Vals}$ be an arbitrary valuation (since $\mathit{pthCnd}(\tau) = \top$ all valuations are valid models). Observe that $\mu(sa)(\mathbf{pc}) = sa(\mathbf{pc})$ since the program counter is always concrete. Hence, $p(\mu(sa)(\mathbf{pc})) = \mathbf{beqz}\ x, \ell$. Thus, we can apply one of the rules Beqz-Sat or Beqz-Unsat of the concrete semantics starting from $\langle \mu(sm), \mu(sa)\rangle$. We claim that $\mu(sa)(x) = 0$. Therefore, we can apply the Beqz-Sat rule. Hence, $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\texttt{pc}\ \ell} \langle \mu(sm), \mu(sa)[\mathbf{pc} \mapsto \ell]\rangle$. Therefore, $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\mu(\tau)} \langle \mu(sm'), \mu(sa')\rangle$ (since $\mu(\tau) = \mu(\texttt{symPc}(\top) \cdot \texttt{pc}\ \ell) = \texttt{pc}\ \ell$).

We now prove our claim that $\mu(sa)(x) = 0$. We know that $sa(x) = 0$. Hence, $\mu(sa(x)) = 0$ (since $sa(x)$ is a concrete value). From this and Lemma 1, $\mu(sa)(x) = 0$.

Rule Beqz-Symb-Sat. Assume that $\langle sm, sa\rangle \xrightarrow{\tau}_s \langle sm', sa'\rangle$ has been derived using the Beqz-Symb-Sat rule in the symbolic semantics. Then, $p(a(\mathbf{pc})) = \mathbf{beqz}\ x, \ell$, $sa(x) \notin \mathit{Vals}$, $sm' = sm$, $\tau = \texttt{symPc}(sa(x) = 0) \cdot \texttt{pc}\ \ell$, and $sa' = sa[\mathbf{pc} \mapsto \ell]$. Let $\mu : \mathit{SymbVals} \to \mathit{Vals}$ be an arbitrary valuation satisfying $\mathit{pthCnd}(\tau) = sa(x) = 0$. Observe that $\mu(sa)(\mathbf{pc}) = sa(\mathbf{pc})$ since the program counter is always concrete. Hence, $p(\mu(sa)(\mathbf{pc})) = \mathbf{beqz}\ x, \ell$. Thus, we can apply one of the rules Beqz-Sat or Beqz-Unsat of the concrete semantics starting from $\langle \mu(sm), \mu(sa)\rangle$. We claim that $\mu(sa)(x) = 0$. Therefore, we can apply the Beqz-Sat rule. Hence, $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\texttt{pc}\ \ell} \langle \mu(sm), \mu(sa)[\mathbf{pc} \mapsto \ell]\rangle$. Therefore, $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\mu(\tau)} \langle \mu(sm'), \mu(sa')\rangle$ (since $\mu(\tau) = \mu(\texttt{symPc}(sa(x) = 0) \cdot \texttt{pc}\ \ell) = \texttt{pc}\ \ell$).

We now prove our claim that $\mu(sa)(x) = 0$. We know that $sa(x) = se$ and $\mu \models se = 0$. Hence, $\mu(se) = 0$. Therefore, $\mu(sa(x)) = 0$. From this and Lemma 1, we have $\mu(sa)(x) = 0$.

Rule Beqz-Concr-Unsat. The proof of this case is similar to that of the Beqz-Concr-Sat rule.

Rule Beqz-Symb-Unsat. The proof of this case is similar to that of the Beqz-Symb-Sat rule.

Rule Jmp-Concr. Assume that $\langle sm, sa\rangle \xrightarrow{\tau}_s \langle sm', sa'\rangle$ has been derived using the Jmp-Concr rule in the symbolic semantics. Then, $p(a(\mathbf{pc})) = \mathbf{jmp}\ e$, $\ell = \llbracket e \rrbracket(sa)$, $\ell \in \mathit{Vals}$, $sm' = sm$, $\tau = \texttt{symPc}(\top) \cdot \texttt{pc}\ \ell$, and $sa' = sa[\mathbf{pc} \mapsto \ell]$. Let $\mu : \mathit{SymbVals} \to \mathit{Vals}$ be an arbitrary valuation (since $\mathit{pthCnd}(\tau) = \top$ all valuations are valid models). Observe that $\mu(sa)(\mathbf{pc}) = sa(\mathbf{pc})$ since the program counter is always concrete. Hence, $p(\mu(sa)(\mathbf{pc})) = \mathbf{jmp}\ e$. Thus, we can apply the Jmp rule of the concrete semantics starting from $\langle \mu(sm), \mu(sa)\rangle$. Observe that $\llbracket e \rrbracket(\mu(sa)) = \mu(\llbracket e \rrbracket(sa)) = \ell$. Hence, $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\texttt{pc}\ \ell} \langle \mu(sm), \mu(sa)[\mathbf{pc} \mapsto \ell]\rangle$. Therefore, $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\mu(\tau)} \langle \mu(sm'), \mu(sa')\rangle$ (since $\mu(\tau) = \mu(\texttt{symPc}(\top) \cdot \texttt{pc}\ \ell) = \texttt{pc}\ \ell$).

Rule Jmp-Symb. Assume that $\langle sm, sa\rangle \xrightarrow{\tau}_s \langle sm', sa'\rangle$ has been derived using the Jmp-Symb rule in the symbolic semantics. Then, $p(a(\mathbf{pc})) = \mathbf{jmp}\ e$, $\llbracket e \rrbracket(sa) \notin \mathit{Vals}$, $\ell \in \mathit{Vals}$, $sm' = sm$, $\tau = \texttt{symPc}(\llbracket e \rrbracket(sa) = \ell) \cdot \texttt{pc}\ \ell$, and $sa' = sa[\mathbf{pc} \mapsto \ell]$. Let $\mu : \mathit{SymbVals} \to \mathit{Vals}$ be an arbitrary valuation satisfying $\mathit{pthCnd}(\tau)$, that is, $\llbracket e \rrbracket(sa) = \ell$. Observe that $\mu(sa)(\mathbf{pc}) = sa(\mathbf{pc})$ since the program counter is always concrete. Hence, $p(\mu(sa)(\mathbf{pc})) = \mathbf{jmp}\ e$.

Thus, we can apply the Jmp rule of the concrete semantics starting from $\langle \mu(sm), \mu(sa)\rangle$. We claim $[\![e]\!](\mu(sa)) = \ell$. Hence, $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\texttt{pc}\ \ell} \langle \mu(sm), \mu(sa)[\mathbf{pc} \mapsto \ell]\rangle$. Therefore, $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\mu(\tau)} \langle \mu(sm'), \mu(sa')\rangle$ (since $\mu(\tau) = \mu(\texttt{symPc}([\![e]\!](sa) = \ell) \cdot \texttt{pc}\ \ell) = \texttt{pc}\ \ell$).

We now prove our claim that $[\![e]\!](\mu(sa)) = \ell$. We know that $[\![e]\!](sa) = se$ and $\mu \models se = \ell$. Hence, $\mu([\![e]\!](sa)) = \ell$. From this and Lemma 1, we have $[\![e]\!](\mu(sa)) = \ell$.

Rule Terminate. The proof of this case is similar to that of the Skip rule.

This completes the proof of our claim. □

E.2.1 Soundness: Added rules. These are the additional rules. Note that Soundness is split up into two lemmas: Lemma 2 and Lemma 3. 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 3 (NS: Soundness Symbolic Added rules)**.** *If*

(1) $\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$ *and*
(2) $\mu \models pthCnd(\tau_{\mathcal{S}})$

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 $p(sa(pc)) = \mathbf{call}\ f$ and since **pc** and function names f are always concrete $p(\mu\,\sigma_{\mathcal{S}}) = \mathbf{call}\ f$ as well. Furthermore, $sa' = sa[\mathbf{pc} \mapsto n, \mathbf{sp} \mapsto sa(\mathbf{sp}) - 8]$ and $sm' = \mathbf{write}(sm, sa(\mathbf{pc}) + 1, sa'(\mathbf{sp}))$ 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 $a' = \mu\, sa[\mathbf{pc} \mapsto n, \mathbf{sp} \mapsto \mu\, sa(\mathbf{sp}) - 8]$. From this and the fact that **sp** is always concrete we have $\mu\, sa' = a'$.

Now, $m' = \mu\, sm'[\mu\, sa'(\mathbf{sp}) \mapsto \mu\, sa(\mathbf{pc}) + 1]$ which again follows from **sp** and **pc** to be concrete.

Rule Ret-Concr Then $p(sa(pc)) = \mathbf{ret}$ and since **pc** is always concrete $p(\mu\,\sigma_{\mathcal{S}} = \mathbf{ret}$ as well.

We have $l = \mathbf{read}(sm, sa(\mathbf{sp}))$ and $l \in Vals$ and $sa' = sa[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto sa(\mathbf{sp}) + 8]$ and $\texttt{symPc}(\top)$. Let μ be an arbitrary valuation (since $\mu \models pthCnd(\tau_{\mathcal{S}}) = \top$).

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 $\mu\, sa' = \mu\, sa[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto \mu\, sa(\mathbf{sp})]$

We now have $\sigma' = \langle p, \langle \mu\, sm, \mu\, sa'\rangle\rangle$ and are finished.

Rule Ret-Symb Then $p(sa(pc)) = \mathbf{ret}$ and since **pc** is always concrete $p(\mu\,\sigma_{\mathcal{S}} = \mathbf{ret}$ as well.

We have $l = \mathbf{read}(sm, sa(\mathbf{sp}))$ and $l \notin Vals$ and $sa' = sa[\mathbf{pc} \mapsto l', \mathbf{sp} \mapsto sa(\mathbf{sp}) + 8]$ 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.

□

E.3 Completeness

Note that Completeness is split up into two lemmas: Lemma 4 and Lemma 5.

In Lemma 4, we prove the completeness of the non-speculative symbolic semantics.

Lemma 4 (NS: Completeness Symbolic)**.** *Let p be a program, sa be a symbolic assignment, and sm be a symbolic memory. Whenever $\langle m, a\rangle \xrightarrow{\tau} \langle m', a'\rangle$, then for all assignments $\mu : SymbVals \rightarrow Vals$ such that $\mu(sa) = a$ and $\mu(sm) = m$, then there exist τ', sm', sa' such that $\langle sm, sa\rangle \xrightarrow{\tau'}_s \langle sm', sa'\rangle$, $\mu(sm') = m'$, $\mu(sa') = a'$, $\mu(\tau') = \tau$, and $\mu \models pthCnd(\tau)$.*

Proof. Let p be a program, sa be a symbolic assignment, and sm be a symbolic memory. Moreover, assume that $\langle m, a\rangle \xrightarrow{\tau} \langle m', a'\rangle$ holds. Finally, let $\mu : SymbVals \rightarrow Vals$ be an arbitrary assignment such that $\mu(sa) = a$ and $\mu(sm) = m$. We proceed by case distinction on the rules defining $\rightarrow$.

Rule Skip. Assume that $\langle m, a\rangle \xrightarrow{\tau} \langle m', a'\rangle$ has been derived using the Skip rule in the concrete semantics. Then, $p(a(\mathbf{pc})) = \mathbf{skip}$, $m' = m$, $a' = a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1]$, and $\tau = \varepsilon$. From $p(a(\mathbf{pc})) = \mathbf{skip}$, $\mu(sa) = a$, and $\mathbf{pc}$ being always concrete, we have that $p(sa(\mathbf{pc})) = \mathbf{skip}$. Thus, we can apply the rule Skip of the symbolic semantics starting from $\langle sm, sa\rangle$. Hence, $\langle sm, sa\rangle \xrightarrow{\tau'}_s \langle sm', sa'\rangle$, where $\tau' = \varepsilon$, $sm' = sm$, $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1]$, and $\varphi' = \varphi$. From $m' = m$, $\mu(sm) = m$, and $sm' = sm$, we have that $\mu(sm') = m'$. From Lemma 1, $a' = a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1]$, $\mu(sa) = a$, and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1]$, we have that $\mu(sa') = \mu(sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1]) = \mu(sa)[\mathbf{pc} \mapsto \mu(sa(\mathbf{pc}))+1] = a[\mathbf{pc} \mapsto \mu(sa(\mathbf{pc}))+1] = a[\mathbf{pc} \mapsto \mu(sa)(\mathbf{pc})+1] = a[\mathbf{pc} \mapsto a(\mathbf{pc})+1] = a'$. From $\tau = \varepsilon$ and $\tau' = \varepsilon$, we have that $\mu(\tau') = \tau$. Finally, from $pthCnd(\tau') = \top$, we have that $\mu \models pthCnd(\tau)$.

Rule Barrier. The proof of this case is similar to that of **Rule Skip.**

Rule Assign. Assume that $\langle m, a\rangle \xrightarrow{\tau} \langle m', a'\rangle$ has been derived using the Assign rule in the concrete semantics. Then, $p(a(\mathbf{pc})) = x \leftarrow e$, $x \neq \mathbf{pc}$, $m' = m$, $a' = a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1, x \mapsto [\![x]\!](a)]$, and $\tau = \varepsilon$. From $p(a(\mathbf{pc})) = x \leftarrow e$, $\mu(sa) = a$, and $\mathbf{pc}$ being always concrete, we have that $p(sa(\mathbf{pc})) = x \leftarrow e$. Thus, we can apply the rule Assign of the symbolic semantics starting from $\langle sm, sa\rangle$. Hence, $\langle sm, sa\rangle \xrightarrow{\tau'}_s \langle sm', sa'\rangle$, where $\tau' = \varepsilon$, $sm' = sm$, and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto [\![e]\!](sa)]$. From $m' = m$, $\mu(sm) = m$, and $sm' = sm$, we have that $\mu(sm') = m'$. From Lemma 1, $a' = a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1, x \mapsto [\![e]\!](a)]$, $\mu(sa) = a$, and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto [\![e]\!](a)]$, we have that $\mu(sa') = \mu(sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto [\![e]\!](sa)]) = \mu(sa)[\mathbf{pc} \mapsto \mu(sa(\mathbf{pc})) + 1, x \mapsto \mu([\![e]\!](sa))] = \mu(sa)[\mathbf{pc} \mapsto \mu(sa)(\mathbf{pc}) + 1, x \mapsto [\![e]\!](\mu(sa))] = a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1, x \mapsto [\![e]\!](a)] = a'$. From $\tau = \varepsilon$ and $\tau' = \varepsilon$, we have that $\mu(\tau') = \tau$. Finally, from $pthCnd(\tau') = \top$, we have that $\mu \models pthCnd(\tau)$.

Rule ConditionalUpdate-Sat. Assume that $\langle m, a\rangle \xrightarrow{\tau} \langle m', a'\rangle$ has been derived using the ConditionalUpdate-Sat rule in the concrete semantics. Then, $p(a(\mathbf{pc})) = x \xleftarrow{e'?} e$, $x \neq \mathbf{pc}$, $[\![e']\!](a) = 0$, $m' = m$, $a' = a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1, x \mapsto [\![x]\!](a)]$, and $\tau = \varepsilon$. From $p(a(\mathbf{pc})) = x \xleftarrow{e'?} e$, $\mu(sa) = a$, and $\mathbf{pc}$ being always concrete, we have that $p(sa(\mathbf{pc})) = x \xleftarrow{e'?} e$. There are two cases:

$[\![e']\!](sa) \in Vals$: We claim that $[\![e']\!](sa) = 0$. Therefore, we can apply the rule ConditionalUpdate-Concr-Sat of the symbolic semantics starting from $\langle sm, sa\rangle$. Hence, $\langle sm, sa\rangle \xrightarrow{\tau'}_s \langle sm', sa'\rangle$, where $\tau' = \varepsilon$, $sm' = sm$, and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto [\![e]\!](sa)]$. From $m' = m$, $\mu(sm) = m$, and $sm' = sm$, we have that $\mu(sm') = m'$. From Lemma 1, $a' = a[\mathbf{pc} \mapsto a(\mathbf{pc})+1, x \mapsto [\![e]\!](a)]$, $\mu(sa) = a$, and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc})+1, x \mapsto [\![e]\!](a)]$, we have that $\mu(sa') = \mu(sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto [\![e]\!](sa)]) = \mu(sa)[\mathbf{pc} \mapsto \mu(sa(\mathbf{pc})) + 1, x \mapsto \mu([\![e]\!](sa))] = \mu(sa)[\mathbf{pc} \mapsto \mu(sa)(\mathbf{pc}) + 1, x \mapsto [\![e]\!](\mu(sa))] = a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1, x \mapsto [\![e]\!](a)] = a'$. From $\tau = \varepsilon$ and $\tau' = \varepsilon$, we have that $\mu(\tau') = \tau$. Finally, from $pthCnd(\tau') = \top$, we have that $\mu \models pthCnd(\tau)$. We now show that $[\![e']\!](sa) = 0$. From $[\![e']\!](sa) \in Vals$, it follows that all variables defining e' have concrete values in sa. From this and $\mu(sa) = a$, we have that all these variables agree in a and sa. Hence, $[\![e']\!](sa) = [\![e']\!](a) = 0$.

$[\![e']\!](sa) \notin Vals$: We can apply the rule ConditionalUpdate-Symb of the symbolic semantics starting from $\langle sm, sa\rangle$. Hence, $\langle sm, sa\rangle \xrightarrow{\tau'}_s \langle sm', sa'\rangle$, where $\tau' = \varepsilon$, $sm' = sm$, and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto \mathbf{ite}([\![e']\!](sa) = 0, [\![e]\!](sa), sa(x))]$. From $m' = m$, $\mu(sm) = m$, and $sm' = sm$, we have that $\mu(sm') = m'$. From $\tau = \varepsilon$ and $\tau' = \varepsilon$, we have that $\mu(\tau') = \tau$. Finally, from $pthCnd(\tau') = \top$, we have that $\mu \models pthCnd(\tau)$. Finally, to show that $a' = \mu(sa')$, we need to show that $\mu(\mathbf{ite}([\![e']\!](sa) = 0, [\![e]\!](sa), sa(x)))$ is equivalent to $[\![e]\!](sa)$. From the evaluation of symbolic expressions, $\mu(\mathbf{ite}([\![e']\!](sa) = 0, [\![e]\!](sa), sa(x)))$ is $\mu([\![e]\!](sa))$ if $\mu([\![e']\!](sa) = 0) \neq 0$, i.e., if $\mu([\![e']\!](sa)) = 0$, and $\mu(sa(x))$ otherwise. We now show that $\mu([\![e']\!](sa)) = 0$, from this we immediately get that $a' = \mu(sa')$. From Lemma 1, we have $\mu([\![e']\!](sa)) = [\![e']\!](\mu(sa))$. From this and $\mu(sa) = a$, we have $\mu([\![e']\!](sa)) = [\![e']\!](a)$. From this and $[\![e']\!](a) = 0$, we finally get $\mu([\![e']\!](sa)) = 0$.

This concludes the proof of this case.

Rule ConditionalUpdate-Unsat. The proof of this case is similar to that of **Rule ConditionalUpdate-Sat.**

Rule Load. Assume that $\langle m, a\rangle \xrightarrow{\tau} \langle m', a'\rangle$ has been derived using the Load rule in the concrete semantics. Then, $p(a(\mathbf{pc})) = \mathbf{load}\ x, e$, $x \neq \mathbf{pc}$, $m' = m$, $a' = a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1, x \mapsto m([\![e]\!](a))]$, and $\tau = \texttt{load}\ [\![e]\!](a)$. From $p(a(\mathbf{pc})) = \mathbf{load}\ x, e$, $\mu(sa) = a$, and $\mathbf{pc}$ being always concrete, we have that $p(sa(\mathbf{pc})) = \mathbf{load}\ x, e$. We proceed by applying the Load-Symb rule of the symbolic semantics starting from $\langle sm, sa, \varphi\rangle$. Hence, $\langle sm, sa\rangle \xrightarrow{\tau'}_s \langle sm', sa'\rangle$, where $se = [\![e]\!](sa)$, $se' = \mathbf{read}(sm, se)$, $\tau' = \texttt{load}\ se$, $sm' = sm$, and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto se']$. We claim that $\mu(se') = m([\![e]\!](a))$. From $m' = m$, $\mu(sm) = m$, and $sm' = sm$, we have that $\mu(sm') = m'$. From $a' = a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1, x \mapsto m([\![e]\!](a))]$, $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto se']$, and $\mu(se') = m([\![e]\!](a))$, we have that $\mu(sa') = \mu(sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1, x \mapsto se']) = \mu(sa)[\mathbf{pc} \mapsto \mu(sa(\mathbf{pc})) + 1, x \mapsto \mu(se')] = \mu(sa)[\mathbf{pc} \mapsto \mu(sa)(\mathbf{pc}) + 1, x \mapsto m([\![e]\!](a))] = a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1, x \mapsto m([\![e]\!](a))] = a'$ (by relying on $\mu(sa) = a$, $\mu(sm) = m$, our claim that $\mu(se') = m([\![e]\!](a))$, and Lemma 1). From $\tau = \texttt{load}\ [\![e]\!](a)$ and $\tau' = \texttt{load}\ [\![e]\!](sa)$, we have that $\mu(\tau') = \texttt{load}\ \mu([\![e]\!](sa)) = \texttt{load}\ [\![e]\!](\mu(sa)) = \texttt{load}\ [\![e]\!](a) = \tau$ (by applying Lemma 1 and relying on $\mu(sa) = a$). Finally, from $pthCnd(\tau) = \top$, we have that $\mu \models pthCnd(\tau)$.

We now prove our claim that $\mu(se') = m([\![e]\!](a))$. From $se' = \mathbf{read}(sm, se)$, we have that $\mu(se') = \mu(sm)(\mu(se))$ (from the evaluation of symbolic expressions). From this and $\mu(sm) = m$, we have that $\mu(se') = m(\mu(se))$. From $se = [\![e]\!](sa)$, $\mu(se) = \mu([\![e]\!](sa)) = [\![e]\!](\mu(sa)) = [\![e]\!](a)$ (from $\mu(sa) = a$ and Lemma 1). Therefore, $\mu(se') = m([\![e]\!](a))$.

Rule Store. Assume that $\langle m, a\rangle \xrightarrow{\tau} \langle m', a'\rangle$ has been derived using the Store rule in the concrete semantics. Then, $p(a(\mathbf{pc})) = \mathbf{store}\ x, e$, $m' = m[[\![e]\!](a) \mapsto a(x)]$, $a' = a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1]$, and $\tau = \texttt{store}\ [\![e]\!](a)$. From $p(a(\mathbf{pc})) = \mathbf{store}\ x, e$, $\mu(sa) = a$, and $\mathbf{pc}$ being always concrete, we have that $p(sa(\mathbf{pc})) = \mathbf{store}\ x, e$. We proceed by applying the Store-Symb rule of the symbolic semantics starting from $\langle sm, sa\rangle$. Hence, $\langle sm, sa\rangle \xrightarrow{\tau'}_s \langle sm', sa'\rangle$, where $se = [\![e]\!](sa)$, $\tau' = \texttt{store}\ se$, $sm' = \mathbf{write}(sm, se, sa(x))$, and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1]$. For showing that $\mu(sm') = m'$, we proceed as follows. From the evaluation of symbolic expressions, $\mu(sm') = \mu(\mathbf{write}(sm, se, sa(x))) = \mu(sm)[\mu(se) \mapsto \mu(sa(x))]$. From this, $\mu(sm) = m$, $\mu(sa) = a$, and Lemma 1, we have $\mu(sm)[\mu(se) \mapsto \mu(sa(x))] = m[\mu(se) \mapsto \mu(sa)(x)] = m[\mu(se) \mapsto a(x)]$. From this, $\mu(sa) = a$, $se = [\![e]\!](sa)$, and Lemma 1, we have $m[\mu(se) \mapsto a(x)] = m[\mu([\![e]\!](sa)) \mapsto a(x)] = m[[\![e]\!](\mu(sa)) \mapsto a(x)] = m[[\![e]\!](a) \mapsto a(x)]$. Therefore, $\mu(sm') = m[[\![e]\!](a) \mapsto a(x)]$. Since $m' = m[[\![e]\!](a) \mapsto a(x)]$, we proved that $\mu(sm') = m'$. From $a' = a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1]$ and $sa' = sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1]$, we have that $\mu(sa') = \mu(sa[\mathbf{pc} \mapsto sa(\mathbf{pc}) + 1]) = \mu(sa)[\mathbf{pc} \mapsto \mu(sa(\mathbf{pc})) + 1] = a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1] = a'$ (by relying on $\mu(sa) = a$ and Lemma 1). From $\tau = \texttt{store}\ [\![e]\!](a)$

and $\tau' = \texttt{store}\ [\![e]\!](sa)$, we have that $\mu(\tau') = \texttt{store}\ \mu([\![e]\!](sa)) = \texttt{store}\ [\![e]\!](\mu(sa)) = \texttt{store}\ [\![e]\!](a) = \tau$ (by applying Lemma 1 and relying on $\mu(sa) = a$). Finally, from $pthCnd(\tau) = \top$, we have $\mu \models pthCnd(\tau)$.

We now prove our claim that $\mu(se') = m([\![e]\!](a))$. From $se' = \mathbf{ite}(se = 0, sm(0), \mathbf{ite}(se = 1, sm(1), \ldots))$, we have that $\mu(se') = \mu(\mathbf{ite}(se = 0, sm(0), \mathbf{ite}(se = 1, sm(1), \ldots)))$. Hence, $\mu(se') = \mu(sm(\mu(se)))$ (by relying on the semantics of $\mathbf{ite}(se, se', se'')$). From this and $se = [\![e]\!](sa)$, we have that $\mu(se') = \mu(sm(\mu([\![e]\!](sa))))$. By applying Lemma 1, we have $\mu(se') = \mu(sm)([\![e]\!](\mu(sa)))$. From this, $\mu(sm) = m$, and $\mu(sa) = a$, we have $\mu(se') = m([\![e]\!](a))$.

Rule Beqz-Sat. Assume that $\langle m, a\rangle \xrightarrow{\tau} \langle m', a'\rangle$ has been derived using the Beqz-Sat rule in the concrete semantics. Then, $p(a(\mathbf{pc})) = \mathbf{beqz}\ x, \ell$, $a(x) = 0$, $m' = m$, $a' = a[\mathbf{pc} \mapsto \ell]$, and $\tau = \texttt{pc}\ \ell$. From $p(a(\mathbf{pc})) = \mathbf{beqz}\ x, \ell$, $\mu(sa) = a$, and $\mathbf{pc}$ being always concrete, we have that $p(sa(\mathbf{pc})) = \mathbf{beqz}\ x, \ell$. There are two cases:

- Assume that $sa(x) \in Vals$. From $a(x) = 0$ and $\mu(sa) = a$, we have that $sa(x) = 0$. Hence, we proceed by applying the Beqz-Concr-Sat rule of the symbolic semantics starting from $\langle sm, sa\rangle$. Hence, $\langle sm, sa\rangle \xrightarrow{\tau'}_s \langle sm', sa'\rangle$, where $\tau' = \texttt{symPc}(\top) \cdot \texttt{pc}\ \ell$, $sm' = sm$, and $sa' = sa[\mathbf{pc} \mapsto \ell]$. From $m' = m$, $\mu(sm) = m$, and $sm' = sm$, we have that $\mu(sm') = m'$. From $a' = a[\mathbf{pc} \mapsto \ell]$ and $sa' = sa[\mathbf{pc} \mapsto \ell]$, we have that $\mu(sa') = \mu(sa[\mathbf{pc} \mapsto \ell]) = \mu(sa)[\mathbf{pc} \mapsto \ell] = a[\mathbf{pc} \mapsto \ell] = a'$ (by relying on $\mu(sa) = a$ and Lemma 1). From $\tau = \texttt{pc}\ \ell$ and $\tau' = \texttt{symPc}(\top) \cdot \texttt{pc}\ \ell$, we have that $\mu(\tau') = \tau$. Finally, from $pthCnd(\tau') = \top$, we have that $\mu \models pthCnd(\tau')$.
- Assume that $sa(x) \notin Vals$ and let $se = sa(x)$. We proceed by applying the Beqz-Symb-Sat rule of the symbolic semantics starting from $\langle sm, sa\rangle$. Hence, $\langle sm, sa\rangle \xrightarrow{\tau'}_s \langle sm', sa'\rangle$, where $\tau' = \texttt{symPc}(sa(x) = 0) \cdot \texttt{pc}\ \ell$, $sm' = sm$, and $sa' = sa[\mathbf{pc} \mapsto \ell]$. From $m' = m$, $\mu(sm) = m$, and $sm' = sm$, we have that $\mu(sm') = m'$. From $a' = a[\mathbf{pc} \mapsto \ell]$ and $sa' = sa[\mathbf{pc} \mapsto \ell]$, we have that $\mu(sa') = \mu(sa[\mathbf{pc} \mapsto \ell]) = \mu(sa)[\mathbf{pc} \mapsto \ell] = a[\mathbf{pc} \mapsto \ell] = a'$ (by relying on $\mu(sa) = a$ and Lemma 1). From $\tau = \texttt{pc}\ \ell$ and $\tau' = \texttt{symPc}(sa(x) = 0) \cdot \texttt{pc}\ \ell$, we have that $\mu(\tau') = \tau$. We now show that $\mu \models pthCnd(\tau')$. Since $pthCnd(\tau')$ is $sa(x) = 0$, we need to show that $\mu(sa(x)) = 0$. From Lemma 1, $\mu(sa(x)) = \mu(sa)(x)$. From this and $\mu(sa) = a$, $\mu(sa(x)) = a(x)$. Therefore, $\mu(sa(x)) = 0$ since $a(x) = 0$. Hence, $\mu \models sa(x) = 0$, i.e., $\mu \models pthCnd(\tau')$.

Rule Beqz-Unsat. The proof of this case is similar to that of **Rule Beqz-Unsat.**

Rule Jmp. Assume that $\langle m, a\rangle \xrightarrow{\tau} \langle m', a'\rangle$ has been derived using the Jmp rule in the concrete semantics. Then, $p(a(\mathbf{pc})) = \mathbf{jmp}\ e$, $\ell = [\![e]\!](a)$, $m' = m$, $a' = a[\mathbf{pc} \mapsto \ell]$, and $\tau = \texttt{pc}\ \ell$. From $p(a(\mathbf{pc})) = \mathbf{jmp}\ e$, $\mu(sa) = a$, and $\mathbf{pc}$ being always concrete, we have that $p(sa(\mathbf{pc})) = \mathbf{jmp}\ e$. There are two cases:

- Assume that $[\![e]\!](sa) \in Vals$. We proceed by applying the Jmp-Concr rule of the symbolic semantics starting from $\langle sm, sa\rangle$. Hence, $\langle sm, sa\rangle \xrightarrow{\tau'}_s \langle sm', sa'\rangle$, where $\ell' = [\![e]\!](sa)$, $\tau' = \texttt{symPc}(\top) \cdot \texttt{pc}\ \ell'$, $sm' = sm$, and $sa' = sa[\mathbf{pc} \mapsto \ell']$. Observe that $\ell = \ell'$ (since $\ell' = [\![e]\!](sa)$ and $\mu(sa) = a$). From $m' = m$, $\mu(sm) = m$, and $sm' = sm$, we have that $\mu(sm') = m'$. From $a' = a[\mathbf{pc} \mapsto \ell]$, $sa' = sa[\mathbf{pc} \mapsto \ell']$, and $\ell = \ell'$, we have that $\mu(sa') = \mu(sa[\mathbf{pc} \mapsto \ell]) = \mu(sa)[\mathbf{pc} \mapsto \ell] = a[\mathbf{pc} \mapsto \ell] = a'$ (by relying on $\mu(sa) = a$ and Lemma 1). From $\tau = \texttt{pc}\ \ell$, $\tau' = \texttt{symPc}(\top) \cdot \texttt{pc}\ \ell'$, and $\ell = \ell'$, we have that $\mu(\tau') = \tau$. Finally, from $pthCnd(\tau') = \top$, we have that $\mu \models pthCnd(\tau')$.
- Assume that $[\![e]\!](sa) \notin Vals$ and let $se = [\![e]\!](sa)$. We proceed by applying the Jmp-Symb rule of the symbolic semantics starting from $\langle sm, sa\rangle$, where we pick ℓ as target label. Hence, $\langle sm, sa\rangle \xrightarrow{\tau'}_s \langle sm', sa'\rangle$, where $\tau' = \texttt{symPc}([\![e]\!](sa) = \ell) \cdot \texttt{pc}\ \ell$, $sm' = sm$, and $sa' = sa[\mathbf{pc} \mapsto \ell]$. From $m' = m$, $\mu(sm) = m$, and $sm' = sm$, we have that $\mu(sm') = m'$. From $a' = a[\mathbf{pc} \mapsto \ell]$ and $sa' = sa[\mathbf{pc} \mapsto \ell]$, we have

that $\mu(sa') = \mu(sa[\mathbf{pc} \mapsto \ell]) = \mu(sa)[\mathbf{pc} \mapsto \ell] = a[\mathbf{pc} \mapsto \ell] = a'$ (by relying on $\mu(sa) = a$ and Lemma 1). From $\tau = \texttt{pc}\ \ell$ and $\tau' = \texttt{symPc}(\llbracket e \rrbracket(sa) = \ell) \cdot \texttt{pc}\ \ell$, we have that $\mu(\tau') = \tau$. We now show that $\mu \models pthCnd(\tau')$. Since $pthCnd(\tau')$ is $\llbracket e \rrbracket(sa) = \ell$, we need to show that $\mu(\llbracket e \rrbracket(sa)) = \ell$. From Lemma 1, $\mu(\llbracket e \rrbracket(sa)) = \llbracket e \rrbracket(\mu(sa))$. From this and $\mu(sa) = a$, $\mu(\llbracket e \rrbracket(sa)) = \llbracket e \rrbracket(a)$. Therefore, $\mu(\llbracket e \rrbracket(sa)) = \ell$ since $\llbracket e \rrbracket(a) = \ell$. Hence, $\mu \models \llbracket e \rrbracket(sa) = \ell$, i.e., $\mu \models pthCnd(\tau')$.

Rule Terminate. The proof of this case is similar to that of **Rule Skip.**

This completes the proof of our claim. □

E.3.1 Completeness: Added rules. These are the additional rules. Note that Completeness is split up into two lemmas: Lemma 4 and Lemma 5.

Lemma 5 (NS : Completeness Symbolic Added)**.** *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 $\mu \models pthCnd(\tau_{\mathcal{S}})$

Proof. We proceed by inversion on $\sigma \xrightarrow{\tau} \sigma'$.

Rule Call Then $p(a(\mathbf{pc})) = \mathbf{call}\ f$, $\mathcal{F}(f) = n$, $a' = a[\mathbf{pc} \mapsto n, \mathbf{sp} \mapsto a(\mathbf{sp}) - 8]$ and $m' = m[a'(\mathbf{sp}) \mapsto a(\mathbf{pc}) + 1]$.

Since $\mathbf{pc}$ is always concrete, $p(sa(\mathbf{pc})) = \mathbf{call}\ f$ 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 $sa' = sa[\mathbf{pc} \mapsto n, \mathbf{sp} \mapsto sa(\mathbf{sp}) - 8]$ and $sm' = \mathbf{write}(sm, sa(\mathbf{pc}) + 1, sa'(\mathbf{sp}))$ and $\mu \models pthCnd(\sigma'_{\mathcal{S}}) = \top$.

Now applying Lemma 7 from Spectector we get $\mu\, sa' = \mu\, sa[\mathbf{pc} \mapsto \mu\, sa(\mathbf{pc} + 1)] = a[\mathbf{pc} \mapsto a(\mathbf{pc}) + 1]$. Now, again using Lemma 7, $\mu\, sm' = \mu\, \mathbf{write}(sm, sa(\mathbf{pc}) + 1, sa'(\mathbf{sp})) = \mu\, sm[\mu\, sa'\mathbf{sp} \mapsto \mu\, sa(\mathbf{pc}) + 1] = m[a'(\mathbf{sp}) \mapsto a(\mathbf{pc}) + 1]$

Rule Ret Then $p(a(\mathbf{pc})) = \mathbf{ret}$, $l = m(a(\mathbf{sp}))$ and $a' = a[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto a(\mathbf{sp}) + 8]$.

Since $\mathbf{pc}$ is always concrete, $p(sa(\mathbf{pc})) = \mathbf{ret}$ as well.

There are two cases now:

$l' = sm(sa(\mathbf{sp})) \in Vals$ 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 $\mu \models pthCnd(\sigma'_{\mathcal{S}}) = \top$.

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 $\mu\, sm' = m'$.

$l' = sm(sa(\mathbf{sp})) \notin Vals$ 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 $\mu \vDash pthCnd(\sigma'_S) = \texttt{symPc}(sm(sa(\mathbf{sp}) = l)$ (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.

□

F GENERAL FACTS

General definitions that we will use throughout the technical report. The lemmas in here hold for all our speculative semantics, so they are written with X_x in mind.

Definition 7 (Core state)**.** *Every state for a speculative semantics that we define will always contain these core elements: The program p, the counter ctr, the configuration σ and the speculation window n.*

Definition 8 (Dot notation)**.** *In the following, we use a dot notation to refer to components of a speculative instance Ψ_x/ Φ_x. For example, we write $\Psi_x.ctr$ to refer to ctr inside the instance Ψ_x.*

We lift this notation to speculative states X_x and Σ_x in the following way: we write $\Sigma_x \cdot \sigma$ to denote the configuration σ of the topmost speculative instance Φ_x of the speculative state Σ_x. For example if $\Sigma_S = \overline{\Phi}_x \cdot \Phi_x$ then $\Sigma_x.\sigma$ refers to $\Phi_x.\sigma$.

Definition 9 (Update notation)**.** *We use bracket notation to update a speculative instance Ψ_x. For example, $\Psi_x[n \mapsto 0]$ updates field n in Ψ_x to 0. For example, $\Psi'_x = \Psi_x[n \mapsto \Psi_x.n - 1]$*

Definition 10 (Tuple Equality)**.** *Two tuples $\langle t_1, \cdots, t_n\rangle$, $\langle t'_1, \cdots, t'_n\rangle$ are equal, iff $t_1 = t'_1, \cdots, t_n = t'_n$.*

Definition 11 (No ongoing transactions that will be rolled back)**.** *A speculative state X_x has no ongoing transactions that will be rolled back, iff*

$$\frac{\begin{array}{c}\exists X'_x \qquad \vdash X'_x : fin \qquad X_{x\overline{\rho}} \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}} X'_x \\ \forall \texttt{rlb}_x\ i \in \overline{\tau}.\ \exists \texttt{start}_x\ i \in \overline{\tau} \\ \nexists \texttt{start}_x\ id \in \overline{\rho}.\ \texttt{rlb}_x\ id \in \overline{\tau}\end{array}}{\vdash_O X_{x\overline{\rho}} : noongoing}\ \textit{(No-ongoing-transaction-rolled)}$$

The last premise tells us that all started speculative transactions that will be rolled back were created in the execution $X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}} X'_x$. Since X'_x 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_x because we did not find a $\texttt{rlb}_x\ i$ for that transaction in the trace $\overline{\tau}$. Note that the final state is unique by Lemma 6 (Uniqueness final state).

Definition 12 (Ongoing transactions that will be rolled back)**.** *A speculative execution $X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}} X''_x$ has ongoing transactions that will be rolled back, iff*

$$\frac{\begin{array}{c}\exists X'_x \qquad \vdash X'_x : fin \qquad X''_x \overset{O}{\rightsquigarrow}{}^{S}_{\overline{\tau}'} X'_x \\ \exists.\ \texttt{rlb}_x\ id' \in \overline{\tau}.\ \forall \texttt{start}_x\ id \in \overline{\tau}'\ id \neq id'\end{array}}{\vdash_O X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}} X''_x : ongoingtransactionrolledback}\ \textit{(Ongoing-transaction-rolled-closed)}$$

By Lemma 6 (Uniqueness final state) the state X'_x is unique for the given oracle O.

Definition 13 (Oldest ongoing transaction that will be rolled back)**.** *A speculative state X_x has an oldest ongoing transaction that will be rolled back, iff*

$$\frac{\exists X'_x \qquad \vdash X'_x : fin \qquad X''_x \overset{O}{\rightsquigarrow}\!{}^{\mathtt{S}}_{\overline{\tau}'} X'_x \quad \exists.\, \mathtt{rlb}_x\ id' \in \overline{\tau}. \forall \mathtt{start}_x\ id \in \overline{\tau}'\ id \neq id' \quad \forall\, \mathtt{rlb}_x\ j \nexists\, \mathtt{start}_x\ j \,\exists\, \mathtt{rlb}_x\ i \nexists\, \mathtt{start}_x\ i \wedge i \leq j}{\vdash^{i}_{O} X_x : biggestongoingtransactionirolledback}\ \textit{(Ongoing-transaction-rolled-closed-oldest)}$$

has to exist because traces are finite.

Definition 14 (Case when $\upharpoonright_{ns}$ is linear)**.**

$$\overline{\tau}\upharpoonright_{ns} \cdot \overline{\tau}'\upharpoonright_{ns} = \overline{\tau} \cdot \overline{\tau}'\upharpoonright_{ns}$$

iff, $\forall.\, \mathtt{rlb}_x\ id \in \overline{\tau}'.\, \mathtt{start}_x\ id \in \overline{\tau}'$.

Definition 15 (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, $\tau \neq \mathtt{rlb}_x\ id$ *forall* $id \in \mathbb{N}$.

Definition 16. *If* $\overline{\tau}'$ *is a prefix of* $\overline{\tau}$ *and* $X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}} X'_x$, *then there exists* X^1_x *such that* $X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}'} X^1_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}''} X'_x$, *where* $\overline{\tau} = \overline{\tau}' \cdot \overline{\tau}''$.

Definition 17. *A speculative state* X_x *either has no ongoing transactions that need to be rolled back or it has ongoing transactions that need to be rolled back.*

Definition 18 (Well orderedness of rollback and start)**.** *If there are* $\mathtt{start}_x\ i, \mathtt{rlb}_x\ i \in \overline{\tau}$, *Then* $\overline{\tau} = \overline{\tau}' \cdot \mathtt{rlb}_x\ i\overline{\tau}''$, *the* $\mathtt{start}_x\ i \in \overline{\tau}'$.

The $\mathtt{start}_x\ i$ *appears before the corresponding* $\mathtt{rlb}_x\ i$ *in the trace.*

Definition 19 (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 6 (Uniqueness final state)**.** *If*

(1) X_x *is a speculative state and*
(2) O *is an oracle and*
(3) There exists X'_x, X''_x *and*
(4) $\vdash X'_x : fin$ *and* $\vdash X''_x : fin$ *and*
(5) $X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}} X'_x$ *and* $X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}'} X''_x$

Then

I $X'_x = X''_x$

Proof. Since $\vdash X'_x : fin$ and $\vdash X''_x : fin$ we know by definition that $X'_x = \langle p, ctr', \sigma', h', \bot \rangle$ and $X''_x = \langle p, ctr'', \sigma'', h'', \bot \rangle$. We need to show

I $ctr' = ctr''$ and
II $h' = h''$ and
III $\sigma' = \sigma''$

Follows from the determinism of the languages ◻

Lemma 7 (Commits do not change the topmost configuration)**.** *If*

(1) $X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}} X'_x$ *and*
(2) $\overline{\tau} = \texttt{commit}\ id_1 \cdot \cdots \cdot \texttt{commit}\ id_n$ *for some* $n \geq 1$

Then

I $X_x.\sigma = X'_x.\sigma$ *and*
II $\overline{\tau}\upharpoonright_{ns} = \varepsilon$

Proof. We have

(1) $X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}} X'_x$ and
(2) $\overline{\tau} = \texttt{commit}\ id_1 \cdot \cdots \cdot \texttt{commit}\ id_n$ for some n

We now need to proof that $X_x.\sigma = X'_x.\sigma$ and $\overline{\tau}\upharpoonright_{ns} = \varepsilon$.

I $X_x.\sigma = X'_x.\sigma$ For $X_x.\sigma = X'_x.\sigma$ notice that $X'_x.\sigma$ is the configuration for the topmost instance in the state X'_x. 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 commit rules (like Rule S:Commit) only change the instance before the previous instance.

topmost instance was committed If the topmost instance in X'_x is committed, then the configuration $X'_x.\sigma$ is still at the top, because committing (like in Rule S:Commit) only updates the previous instance with the configuration σ, h and the ctr of the committed instance. We thus preserve $X'_x.\sigma$.

II $\overline{\tau}\upharpoonright_{ns} = \varepsilon$ Follows from the definition of $\upharpoonright_{ns}$.

This completes the proof. □

Lemma 8 (Reaching Final state from final configuration (Finish commit instances))**.** *If*

(1) $X_x.\sigma \in \mathit{FinalConf}$ *and*
(2) $\vdash X_x : \mathit{nounfinishedtransactionsrolledback}$ *and*
(3) $|X_x| \geq 1$

Then

I $X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}} X'_x$ *and*
II $\forall \tau \in \overline{\tau}.\ \tau = \texttt{commit}\ id$ *for some* $id \in \mathbb{N}$ *and*
III $\vdash X'_x : \mathit{fin}$
IV $X_x.\sigma = X'_x.\sigma$

Proof. Induction on the size of $|X_x|$.

$|X_x| = 1$ **I** Then we derive $X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}} X'_x$ by reflection (like Rule S:Reflection) and have $X'_x = X_x$.

II Trivial, since $\overline{\tau} = \varepsilon$.

III Since $|X_x| = 1$, we have $X_x.n = \bot$. We can now derive $\vdash X_x : \mathit{fin}$, since $X_x.\sigma \in \mathit{FinalConf}$. Because $X_x = X'_x$, we have $\vdash X'_x : \mathit{fin}$ and are finished.

IV Trivial, since $X_x = X'_x$.

$|X_x| = n + 1$ **with** $n > 0$ By $|X_x| > 1$ and $\vdash X_x : \mathit{nounfinishedtransactionsrolledback}$ we know that there are transactions that still need to be committed.

Since $X_x.\sigma \in \mathit{FinalConf}$, we know that the only rule that applies is Rule S:Commit. Thus, $X_x \overset{O_x}{\underset{x}{\xrightsquigarrow{\texttt{commit}\ id}}} X''_x$

Committing (like Rule S:Commit) does not change topmost configuration (Lemma 7 (Commits do not change the topmost configuration)). So, we have $X''_x.\sigma = X_x.\sigma$.

We now apply IH on X''_x, since $|X''_x| = n$. We get

(1) $X''_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}'} X'_x$ and
(2) $\forall \tau \in \overline{\tau}'.\ \tau = \texttt{commit}\ id$ for some $id \in \mathbb{N}$ and
(3) $\vdash X'_x : \mathit{fin}$

I We construct an execution $X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{X'_x}$ by Rule S:Single with $X_x \overset{\texttt{commit}\ id}{\rightsquigarrow}{}^{O_x}_{x} X''_x$ and $X''_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}'} X'_x$.

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 7 (Commits do not change the topmost configuration).

□

Definition 20 (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.

$$count() : X_x \mapsto \mathbb{N}$$

$$\begin{aligned} count(\varepsilon) &= 0 \\ count(\overline{\Psi}_x \cdot \Psi_x^{true}) &= count(\overline{\Psi}_x) + 1 \ \textit{where}\ \Psi_x.n = 0 \\ count(\overline{\Psi}_x \cdot \Psi_x) &= count(\overline{\Psi}_x) \end{aligned}$$

Lemma 9 (Executing a chain of commits). *If*

(1) no transaction that will be rolled back with speculation window 0 *in* X_x

Then there exists X'_x such that

(1) $X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}} X'_x$
(2) $minWndw(X'_x) > 0$
(3) $\forall \tau \in \overline{\tau}.\ \tau = \texttt{commit}\ id$ *for some* $id \in \mathbb{N}$
(4) $X_x.\sigma = X'_x.\sigma$

Proof. The proof proceeds in a similar fashion to Lemma 8 (Reaching Final state from final configuration (Finish commit instances)). By induction on the size of $count(X_x)$.

$count(X_x) = 0$ **I** Then we derive $X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}} X'_x$ by Rule S:Reflection and have $X'_x = X_x$.

II Because $\vdash_O X'_x : \mathit{noongoing}$ and $count(X'_x) = 0$, there cannot be a transaction with speculation window 0.

III Trivial, since $\overline{\tau} = \varepsilon$.

IV Trivial, since $X_x = X'_x$.

$count(X_x) = n + 1$ By $count(X_x) > 0$ we know that there are transactions that still need to be committed.

Then $minWndw(X_x) = 0$ and we know that the only rule that applies is Rule S:Commit. Thus, $X_x \overset{\texttt{commit}\ id}{\rightsquigarrow}{}^{O_x}_{x} X''_x$

Applying Rule S:Commit does not change topmost configuration (Lemma 7 (Commits do not change the topmost configuration)). So, we have $X''_x.\sigma = X_x.\sigma$.

We now apply IH on X''_x, since $count(X''_x) = n$. We get

(1) $X''_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}'} X'_x$ and
(2) $minWndw(X'_x) > 0$
(3) $\forall \tau \in \overline{\tau}'. \tau = \texttt{commit}\ id$ for some $id \in \mathbb{N}$ and
(4) $X_x.\sigma = X'_x.\sigma$

I We construct an execution $X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{X'_x}$ by Rule S:Single with $X_x \xrightarrow[x]{\texttt{commit}\ id\ O_x} X''_x$ and $X''_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}'} X'_x$.

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 7 (Commits do not change the topmost configuration).

□

We use the symbol Δ to present additional data in the speculative instance, ie.e, $\langle p, ctr, \sigma, n, \Delta\rangle$. For example, $\Delta = \mathbb{R}$ for $\mathcal{J}_{\mathrm{R}}$.

Definition 21 (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 22 (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 23 (AM: Similar speculative instances). *Two speculative instances $\langle p, ctr, \sigma, n, \Delta\rangle^b$ and $\langle p', ctr', \sigma', n', \Delta'\rangle^{b'}$ are similar, written $\langle p, ctr, \sigma, n, \Delta\rangle^b \simeq \langle p', ctr', \sigma', n', \Delta'\rangle^{b'}$ iff $p = p'$, $ctr = ctr'$, $n = n'$, $b = b'$, $\Delta = \Delta'$, $\sigma \sim_{\mathbf{pc}} \sigma'$ and $\sigma \sim_{next} \sigma'$.*

Definition 24 (Oracle: Similar speculative instances). *Two speculative instances $\langle p, ctr, \sigma, h, n, \Delta\rangle^b$ and $\langle p', ctr', \sigma', h', n', \Delta'\rangle^{b'}$ are similar, written $\langle p, ctr, \sigma, h, n, \Delta\rangle^b \simeq \langle p', ctr', \sigma', h,' n', \Delta'\rangle^{b'}$ iff $p = p'$, $ctr = ctr'$, $h = h'$, $n = n'$, $b = b'$, $\Delta = \Delta'$, $\sigma \sim_{\mathbf{pc}} \sigma'$ and $\sigma \sim_{next} \sigma'$.*

Definition 25 (Oracle: Similar speculative states). *Two speculative states $\overline{\Psi}_x \cdot \langle p, ctr, \sigma, h, n, Delta\rangle_{\overline{\rho}}$ $\overline{\Psi}'_x \cdot \langle p', ctr', \sigma', h', n', Delta'\rangle_{\overline{\rho}'}$ are similar, written $\overline{\Psi}_x \cdot \langle p, ctr, \sigma, h, n, \Delta\rangle_{\overline{\rho}} \cong \overline{\Psi}'_x \cdot \langle p', ctr, \sigma', h', n', \Delta'\rangle_{\overline{\rho}'}$ iff all the speculative instances in $\overline{\Psi}_x$ and $\overline{\Psi}'_x$ are similar speculative instances which is written $\overline{\Psi}_x \simeq \overline{\Psi}'_x$ and $ctr = ctr'$, $\sigma \sim_{\mathbf{pc}} \sigma'$, $n = n'$, $h = h'$, $\Delta = \Delta'$, $\overline{\rho} = \overline{\rho}'$ and $b = b'$.*

Definition 26 (commit-free projection). *The commit-free projection of our speculative state X is defined as follows:*

$$\begin{aligned}
\varepsilon\restriction_{com} =& \varepsilon \\
\overline{\Psi}_x \cdot \langle p, ctr, \sigma, h, n, \ldots\rangle^b\restriction_{com} =& \overline{\Psi}_x\restriction_{com} \cdot \langle p, ctr, \sigma, h, n, \ldots\rangle^b \text{ with } b \neq false \\
\overline{\Psi}_x \cdot \langle p, ctr, \sigma, h, n, \ldots\rangle\restriction_{com} =& \overline{\Psi}_4 \cdot \langle p, ctr, \sigma, h, n, \ldots\rangle \text{ where } |\overline{\Psi}_x| = 0 \\
\overline{\Psi}_x \cdot \langle p, ctr, \sigma, h, n, \ldots\rangle^b \cdot \langle p, ctr', \sigma', h', n', \ldots\rangle^{false}\restriction_{com} =& \overline{\Psi}_x \cdot \langle p, ctr', \sigma', h', n\rangle^b\restriction_{com}
\end{aligned}$$

This executes the committed speculative instance and changes the speculative state.

Definition 27 (Invariants). *We write $INV(\Sigma_x, X_x)$ iff $INV_h(\Sigma_x, X_x\restriction_{com})$ holds. $INV_h(\Sigma_x, X_x)$ holds if $|X_x| = |\Sigma_x|$ and for all $1 \leq i \leq |\Sigma_x|$, $minWndw(X^i_x) \leq wndw(\Sigma^i_x)$, where Σ^i_x denotes the prefix of Σ_x of length i.*

Definition 28 (Invariants2). *We write $INV2(\Sigma_x, X_x)$ iff $INV2_h(\Sigma_x, X_x\restriction_{com})$ holds. $INV2_h(\Sigma, X_x)$ holds if $|X_x| = |\Sigma_x|$ and $minWndw(X_x) = wndw(\Sigma_x)$*

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

Definition 29 (Decrease function)**.**

$$decr() : X_x \mapsto X_x$$

$$\begin{aligned}
decr(\varepsilon) &= \varepsilon \\
decr(\overline{\Psi_x} \cdot \Psi_x) &= decr(\overline{\Psi_x}) \cdot \Psi_x \ \mathit{if}\ \Psi_x.n = 0 \ \mathit{or}\ \Psi_x.n = \bot \\
decr(\overline{\Psi_x} \cdot \Psi_x) &= decr(\overline{\Psi_x}) \cdot \Psi'_x \,\mathit{if}\ \Psi_x.n > 0 \ \mathit{and\ where}\ \Psi'_x = \Psi_x[n \mapsto \Psi_x.n - 1]
\end{aligned}$$

Definition 30 (Zeroes function)**.**

$$zeroes() : X_x \mapsto X_x$$

$$\begin{aligned}
zeroes(\varepsilon) &= \varepsilon \\
zeroes(\overline{\Psi_x} \cdot \Psi_x) &= zeroes(\overline{\Psi_x}) \cdot \Psi_x \ \mathit{if}\ \Psi_x.n = 0 \ \mathit{or}\ \Psi_x.n = \bot \\
zeroes(\overline{\Psi_x} \cdot \Psi_x) &= zeroes(\overline{\Psi_x}) \cdot \Psi_x[n \mapsto 0]
\end{aligned}$$

Here is a short review of the rules of B

$$\boxed{\Sigma_{B} \overset{\tau}{\rightsquigarrow}_{B} \Sigma'_{B}}$$

(B:AM-Context)

$$\frac{\Phi_{B} \overset{\tau}{\rightsquigarrow}_{B} \overline{\Phi'_{B}}}{\overline{\Phi_{B}} \cdot \Phi_{B} \overset{\tau}{\rightsquigarrow}_{B} \overline{\Phi_{B}} \cdot \overline{\Phi'_{B}}}$$

(B:AM-Rollback)

$$\frac{n' = 0 \text{ or p is stuck}}{\overline{\Phi_{B}} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle \xrightarrow{\texttt{rlb}_{B}\ ctr}_{B} \overline{\Phi_{B}} \cdot \langle p, ctr', \sigma, n \rangle}$$

$$\boxed{\Phi_{B} \overset{\tau}{\rightsquigarrow}_{B} \overline{\Phi'_{B}}}$$

(B:AM-barr)

$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, \bot \rangle \overset{\tau}{\rightsquigarrow}_{B} \langle p, ctr, \sigma', \bot \rangle}$$

(B:AM-barr-spec)

$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, n+1 \rangle \overset{\tau}{\rightsquigarrow}_{B} \langle p, ctr, \sigma', 0 \rangle}$$

(AM-NoBranch)

$$\frac{p(\sigma(\mathbf{pc})) \neq \mathbf{beqz}\ x, l, \mathbf{spbarr}, Z \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, n+1 \rangle \overset{\tau}{\rightsquigarrow}_{B} \langle p, ctr, \sigma', n \rangle}$$

(B:AM-General)

$$\frac{\tau = \texttt{pc}\ n \mid \texttt{start}_{B}\ n}{\Phi_{B\,\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}_{B} \Phi_{B\,\overline{\rho}}}$$

(B:AM-Spec)

$$\frac{\begin{array}{ccc} p(\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell & (p, \sigma) \xrightarrow{\tau} (p, \sigma') & j = min(\omega, n) \\ \sigma'' = \sigma[\mathbf{pc} \mapsto l'] & l' = \begin{cases} \sigma(\mathbf{pc}) + 1 & \text{if } \sigma'(\mathbf{pc}) = l \\ l & \text{if } \sigma'(\mathbf{pc}) \neq l \end{cases} & \end{array}}{\langle p, ctr, \sigma, n+1 \rangle_{\overline{\rho}} \overset{\tau}{\rightsquigarrow}_{B} \langle p, ctr, \sigma', n \rangle_{\overline{\rho}} \cdot \langle p, ctr+1, \sigma'', j \rangle_{\overline{\rho}\cdot\texttt{pc}\ \sigma''(\mathbf{pc})\cdot\texttt{start}_{B}\ ctr}}$$

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

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

$$\boxed{(p \times InitConf) \curvearrowright_B^{\omega} \overline{\tau}}$$

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

G PROOFS FOR $\curvearrowright_B$:

Our main result for $\curvearrowright_B$ is the following

Theorem 2 ($\curvearrowright_B$ is *WFSS*). $\vdash \curvearrowright_B$ *WFSS*

Proof. Immediately follows from Theorem 5 (B: SNI of Oralce and AM), Proposition 3 (B: Symbolic Consistency), Theorem 4 (B: Behaviour of non-speculative semantics and AM semantics) and Theorem 3 (B SE: Behaviour of non-speculative and oracle semantics). □

G.1 B: Relating the speculative and non-speculative semantics

We start by spelling out the definition of $[\![p]\!]_O$. Given a program p and a prediction oracle O, we denote by $[\![p]\!]_O$ the set of all triples $\langle \sigma, \tau, \sigma' \rangle \in InitConf \times ExtObs^* \times FinalConf$ corresponding to executions $\langle 0, \sigma, \varepsilon, \varepsilon \rangle \overset{\tau}{\rightsquigarrow}^* \langle ctr, \sigma', \varepsilon, h \rangle$.

We are now ready to prove Theorem 3, which we restate here for simplicity:

Theorem 3 (B SE: Behaviour of non-speculative and oracle semantics). *Let p be a program and O be a prediction oracle. Then $Beh_{NS}(p) = Beh_B^O(p)\upharpoonright_{ns}$*

Proof. We prove the two directions separately.

($\Leftarrow$). Assume that $\langle \sigma, \tau', \sigma' \rangle \in [\![p]\!]_O$. From Lemma 10 (proved in Appendix G.1.1), it follows that $\langle \sigma, \tau\upharpoonright_{ns}, \sigma' \rangle \in (\!|p|\!)$.

($\Rightarrow$). Assume that $\langle \sigma, \tau, \sigma' \rangle \in (\!|p|\!)$. From Proposition 2 (proved in Appendix G.1.2), it follows that there exists a trace $\tau' \in ExtObs^*$ such that $\langle \sigma, \tau', \sigma' \rangle \in [\![p]\!]_O$ and $\tau'\upharpoonright_{ns} = \tau$. □

In the following, we rely on the concept of *rolled-back transactions* to denote portions of program executions associated with rolled-back speculative transactions. Concretely, an execution $\langle ctr_0, \sigma_0, s_0, h_0 \rangle \overset{\tau_0}{\rightsquigarrow} \langle ctr_1, \sigma_1, s_1, h_1 \rangle \overset{\tau_1}{\rightsquigarrow} \ldots \overset{\tau_{n-1}}{\rightsquigarrow} \langle ctr_n, \sigma_n, s_n, h_n \rangle \overset{\tau_n}{\rightsquigarrow} \langle ctr_{n+1}, \sigma_{n+1}, s_{n+1}, h_{n+1} \rangle$ is a *rolled back speculative transaction* iff there is an identifier $id \in \mathbb{N}$ and two labels $\ell, \ell' \in Vals$ such that $\tau_0 = \texttt{start}\ i \cdot \texttt{pc}\ \ell$ and $\tau_n = \texttt{rlb}\ i \cdot \texttt{pc}\ \ell'$.

G.1.1 Soundness of the speculative semantics.

Lemma 10 states that the speculative semantics does not introduce spurious non-speculative behaviors.

Lemma 10 (B: Soundness)**.** *Let p be a program and O be a prediction oracle. Whenever $\langle 0, \sigma, \varepsilon, \varepsilon \rangle \overset{\tau}{\rightsquigarrow}^* \langle ctr, \sigma', \varepsilon, h \rangle$, $\sigma \in InitConf$, and $\sigma' \in FinalConf$, then $\sigma \xrightarrow{\tau\upharpoonright_{ns}}^* \sigma'$.*

Proof. Let p be a program and O be a prediction oracle. Furthermore, let r be an execution $\langle 0, \sigma, \varepsilon, \varepsilon \rangle \overset{\tau}{\rightsquigarrow}^* \langle ctr, \sigma', \varepsilon, h \rangle$ such that $\sigma \in InitConf$ and $\sigma' \in FinalConf$. We denote by R the set of rolled back transactions and by C

the set containing all identifiers of transactions committed in r, i.e., $R = \{id \in \mathbb{N} \mid \exists i \in \mathbb{N}.\ \tau|_i = \texttt{rlb}\ id\}$ and $C = \{id \in \mathbb{N} \mid \exists i \in \mathbb{N}.\ \tau|_i = \texttt{commit}\ id\}$. We can incrementally construct the execution $\sigma \xrightarrow{\tau\upharpoonright_{ns}}{}^{*} \sigma'$ by applying Lemma 11–Lemma 14. In particular, for instructions that are not inside a speculative transaction, we apply Lemma 11. For branch instructions, there are two cases. If the associated speculative transaction is eventually rolled back (i.e., its identifier is in R), then we apply Lemma 14 to the whole rolled back transaction to generate the corresponding step in the non-speculative semantics. In contrast, if the speculative transaction is eventually committed (i.e., its identifier is in C), then we can apply Lemma 12 (in conjunction with Lemma 15) to generate the corresponding step in the non-speculative semantics as well as Lemma 11 for the other instructions in the transaction. Finally, we can simply ignore the steps associated with the Se-Commit rule (see Lemma 13). Observe that the resulting traces can be combined to obtain $\tau\upharpoonright_{ns}$ since $\langle 0, \sigma, \varepsilon, \varepsilon\rangle \overset{\tau}{\rightsquigarrow}{}^{*} \langle ctr, \sigma', \varepsilon, h\rangle$ is a terminated execution. ◻

The above proof relies on the auxiliary lemmas below to handle non-branch instructions (Lemma 11), committed transactions (Lemma 12, Lemma 13, and Lemma 15), and rolled back transactions (Lemma 14).

Lemma 11. *Let p be a program and O be a prediction oracle. Whenever $\langle ctr, \sigma, s, h\rangle \overset{\tau}{\rightsquigarrow} \langle ctr', \sigma', s', h'\rangle$, $p(\sigma(\mathbf{pc})) \neq \mathbf{beqz}\ x, \ell$, and $enabled(s)$, then $\sigma \xrightarrow{\tau} \sigma'$.*

Proof. Let p be a program and O be a prediction oracle. Assume that $\langle ctr, \sigma, s, h\rangle \overset{\tau}{\rightsquigarrow} \langle ctr', \sigma', s', h'\rangle$, $p(\sigma(\mathbf{pc})) \neq \mathbf{beqz}\ x, \ell$, and $enabled(s)$. From this and the Se-NoBranch rule, it follows $\sigma \xrightarrow{\tau} \sigma'$. ◻

Lemma 12. *Let p be a program and O be a prediction oracle. Whenever $\langle ctr, \sigma, s, h\rangle \overset{\tau}{\rightsquigarrow} \langle ctr', \sigma', s', h'\rangle$, $p(\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell$, $enabled(s)$, $O(p, h, \sigma(\mathbf{pc})) = \langle \ell', w\rangle$, $\sigma \xrightarrow{\texttt{pc}\ \ell'} \sigma''$, then $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma'$.*

Proof. Let p be a program and O be a prediction oracle. Assume that $\langle ctr, \sigma, s, h\rangle \overset{\tau}{\rightsquigarrow} \langle ctr', \sigma', s', h'\rangle$, $p(\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell$, $enabled(s)$, $O(p, h, \sigma(\mathbf{pc})) = \langle \ell', w\rangle$, $\sigma \xrightarrow{\texttt{pc}\ \ell'} \sigma''$. From this, the run was produced by applying the Se-Branch rule. Hence, $\sigma' = \sigma[\mathbf{pc} \mapsto \ell']$ and $\tau = \texttt{start}\ ctr \cdot \texttt{pc}\ \ell'$. From this, $\sigma \xrightarrow{\texttt{pc}\ \ell'} \sigma''$, $\tau\upharpoonright_{ns} = \texttt{pc}\ \ell'$, and $\sigma'' = \sigma[\mathbf{pc} \mapsto \ell']$, it follows that $\tau\upharpoonright_{ns} = \texttt{pc}\ \ell'$ and $\sigma' = \sigma''$. Hence, $\sigma \xrightarrow{\tau} \sigma'$. ◻

Lemma 13. *Let p be a program and O be a prediction oracle. Whenever $\langle ctr, \sigma, s, h\rangle \overset{\texttt{commit}\ id}{\rightsquigarrow} \langle ctr', \sigma', s', h'\rangle$, then $\sigma = \sigma'$.*

Proof. Let p be a program and O be a prediction oracle. Assume that $\langle ctr, \sigma, s, h\rangle \overset{\texttt{commit}\ id}{\rightsquigarrow} \langle ctr', \sigma', s', h'\rangle$. The only applicable rule is Se-Commit and $\sigma = \sigma'$ directly follows from the rule's definition. ◻

Lemma 14. *Let p be a μAsm program and O be a prediction oracle. Whenever $r := \langle ctr, \sigma, s, h\rangle \overset{\tau}{\rightsquigarrow}{}^{*} \langle ctr', \sigma', s', h'\rangle$, $enabled(s)$, $p(\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell$, and the run r is a rolled-back transaction, then $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma'$.*

Proof. Let p be a μAsm program and O be a prediction oracle. Assume that $r := \langle ctr, \sigma, s, h\rangle \overset{\tau}{\rightsquigarrow}{}^{*} \langle ctr', \sigma', s', h'\rangle$, $enabled(s)$, $p(\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell$, and the run r is a rolled-back transaction. Since r is a rolled back transaction, there is an identifier $id \in \mathbb{N}$ and two labels $\ell, \ell' \in Vals$ such that $\langle ctr, \sigma, s, h\rangle \overset{\texttt{start}\ id \cdot \texttt{pc}\ \ell}{\rightsquigarrow} \langle ctr_1, \sigma_1, s_1, h_1\rangle \overset{\tau_1}{\rightsquigarrow} \ldots \overset{\tau_{n-1}}{\rightsquigarrow} \langle ctr_n, \sigma_n, s_n, h_n\rangle \overset{\texttt{rlb}\ id \cdot \texttt{pc}\ \ell'}{\rightsquigarrow} \langle ctr_{n+1}, \sigma_{n+1}, s_{n+1}, h_{n+1}\rangle$.

First, observe that τ is $\texttt{start}\ i \cdot \texttt{pc}\ \ell \cdot \tau' \cdot \texttt{rlb}\ i \cdot \texttt{pc}\ \ell'$. From this, $\tau\upharpoonright_{ns} = \texttt{pc}\ \ell'\upharpoonright_{ns} = \texttt{pc}\ \ell'$.

Next, the first step in r is obtained by applying the Se-Branch rule (since it is the only rule producing $\texttt{start}\ id$ observations). Hence, the last transaction in s' is $\langle \sigma, ctr, w, \ell\rangle$, where $\langle \ell, w\rangle$ is the prediction produced by O, and $id = ctr$.

We never modify the identifier, label, and rollback state inside the speculative transaction during the execution up to the last step. Therefore, it follows (from the rules) that $\langle \sigma, ctr, 0, \ell \rangle$ is a transaction in s_n.

Finally, the last step is obtained by applying the Se-Rollback rule (since it is the only rule producing $\texttt{rlb}\ id$ observations). Hence, the rolled back transaction in s_n is $\langle \sigma, ctr, 0, \ell \rangle$. From this, we have $\sigma \xrightarrow{\texttt{pc}\ \ell'} \sigma_{n+1}$. From this, $\tau\upharpoonright_{ns} = \texttt{pc}\ \ell'$, and $\sigma' = \sigma_{n+1}$ (by construction), we have $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma'$. ◻

Lemma 15. *Let p be a program, O be a prediction oracle, and $\langle ctr_0, \sigma_0, s_0, h_0 \rangle \overset{\tau_0}{\rightsquigarrow} \langle ctr_1, \sigma_1, s_1, h_1 \rangle \overset{\tau_1}{\rightsquigarrow} \dots \overset{\tau_{n-1}}{\rightsquigarrow} \langle ctr_n, \sigma_n, s_n, h_n \rangle \overset{\tau_n}{\rightsquigarrow} \langle ctr_{n+1}, \sigma_{n+1}, s_{n+1}, h_{n+1} \rangle$ be an execution. For all identifiers $id \in \mathbb{N}$, if there is a index $0 \leq j \leq n$ such that $\tau_j = \texttt{commit}\ id$, then there exists an $0 \leq i < j$ and $w \in \mathbb{N}$ such that $\langle m, a \rangle \xrightarrow{\texttt{pc}\ \ell} \langle m, a[\mathbf{pc} \mapsto \ell] \rangle$, $\langle m, a \rangle = \sigma_i$, $\langle \ell, w \rangle = O(p, h_i, \sigma_i(\mathbf{pc}))$, and $\tau_i = \texttt{start}\ ctr_i \cdot \texttt{pc}\ \sigma_{i+1}(\mathbf{pc})$.*

Proof. Let p be a program, O be a prediction oracle, and $\langle ctr_0, \sigma_0, s_0, h_0 \rangle \overset{\tau_0}{\rightsquigarrow} \langle ctr_1, \sigma_1, s_1, h_1 \rangle \overset{\tau_1}{\rightsquigarrow} \dots \overset{\tau_{n-1}}{\rightsquigarrow} \langle ctr_n, \sigma_n, s_n, h_n \rangle \overset{\tau_n}{\rightsquigarrow} \langle ctr_{n+1}, \sigma_{n+1}, s_{n+1}, h_{n+1} \rangle$ be an execution. Let $id \in \mathbb{N}$ be an arbitrary identifier such that $\tau_j = \texttt{commit}\ id$ for some $0 \leq j \leq n$. The j-th step in the run has been produced by applying the Se-Commit rule, which is the only rule producing $\texttt{commit}\ id$ observations, while committing the the speculative transaction $\langle \langle m, a \rangle, id, 0, \ell \rangle$ in s_j. Hence, $\langle m, a \rangle \xrightarrow{\texttt{pc}\ \ell} \langle m, a[\mathbf{pc} \mapsto \ell] \rangle$ holds. Therefore, there is an $0 \leq i < j$ when we executed the Se-Branch rule for the identifier id. In particular, the rule created the speculative transaction $\langle \sigma_i, ctr_i, w, \ell' \rangle$ where $\langle \ell', w \rangle = O(p, h_i, \sigma_i(\mathbf{pc}))$, the observations are $\tau_i = \texttt{start}\ ctr_i \cdot \texttt{pc}\ \ell'$, and the next program counter is ℓ'. Since (1) we only modify the speculative windows inside the speculative transactions states, and (2) there is always only one speculative transaction per identifier, it follows that $ctr_i = id$, $\sigma_i = \langle m, a \rangle$, and $\ell' = \ell$. From this, $\langle m, a \rangle \xrightarrow{\texttt{pc}\ \ell} \langle m, a[\mathbf{pc} \mapsto \ell] \rangle$, $\langle m, a \rangle = \sigma_i$, $\langle \ell, w \rangle = O(p, h_i, \sigma_i(\mathbf{pc}))$, and $\tau_i = \texttt{start}\ ctr_i \cdot \texttt{pc}\ \sigma_{i+1}(\mathbf{pc})$. ◻

G.1.2 Completeness of the speculative semantics. Proposition 2 states that the speculative semantics models all behaviors of the non-speculative semantics (independently on the prediction oracle).

Proposition 2. *Let p be a program and O be a prediction oracle. Whenever $\sigma \xrightarrow{\tau}^{*} \sigma'$, $\sigma \in InitConf$, and $\sigma' \in FinalConf$, there are $\tau' \in ExtObs^*$, $ctr \in \mathbb{N}$, and $h \in \mathcal{H}$ such that $\langle 0, \sigma, \varepsilon, \varepsilon \rangle \overset{\tau'}{\rightsquigarrow}^{*} \langle ctr, \sigma', \varepsilon, h \rangle$ and $\tau = \tau'\upharpoonright_{ns}$.*

Proof. Let p be a program and O be a prediction oracle. Moreover, let r be an execution $\sigma_0 \xrightarrow{\tau_0} \sigma_1 \xrightarrow{\tau_1} \dots \sigma_n \xrightarrow{\tau_n} \sigma_{n+1}$ such that $\sigma_0 \in InitConf$ and $\sigma_{n+1} \in FinalConf$.

We now define a procedure $\textsc{expand}(\langle ctr, \sigma, s, h \rangle, \sigma \xrightarrow{\tau} \sigma')$ for constructing the execution under the speculative semantics as follows:

- If $p(\sigma(\mathbf{pc})) \neq \mathbf{beqz}\ x, \ell'$ and $enabled(s)$, then we apply the Se-NoBranch rule once. This produces the step $r' := \langle ctr, \sigma, s, h \rangle \overset{\tau}{\rightsquigarrow} \langle ctr, \sigma', decr(s), h' \rangle$. We return r'.
- If $p(\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell'$ and $enabled(s)$, there are two cases:
  - If $O(p, h, \sigma(\mathbf{pc})) = \langle \ell, w \rangle$ and $\ell = \sigma'(\mathbf{pc})$, then we correctly predict the outcome of the branch instruction. We produce the execution r' by applying the Se-Branch rule: $r' := \langle ctr, \sigma, s, h \rangle \overset{\texttt{start}\ ctr \cdot \texttt{pc}\ \ell}{\rightsquigarrow} \langle ctr + 1, \sigma', decr(s) \cdot \langle \sigma, ctr, w, \ell \rangle, h \cdot \langle \sigma(\mathbf{pc}), ctr, \ell \rangle \rangle$. Observe that this step starts a speculative transaction that will be committed (since $\ell = \sigma'(\mathbf{pc})$). We return r'.
  - If $O(p, h, \sigma(\mathbf{pc})) = \langle \ell, w \rangle$ and $\ell \neq \sigma'(\mathbf{pc})$, then we mispredict the outcome of the branch instruction.We produce the execution r' by (1) applying Se-Branch once to start the transaction ctr, (2) we repeatedly apply the speculative semantics rules until we roll back the transaction ctr. This is always possible since

speculative transactions always terminate. Hence, r' is $\langle ctr, \sigma, s, h\rangle \xrightarrow{\texttt{start}\ ctr\cdot\texttt{pc}\ \ell} \langle ctr+1, \sigma[\mathbf{pc} \mapsto \ell], decr(s) \cdot \langle \sigma, ctr, w, \ell\rangle, h \cdot \langle \sigma(\mathbf{pc}), ctr, \ell\rangle\rangle \xrightarrow{\tau'}{}^{*} \langle ctr'', \sigma'', s'' \cdot \langle \sigma, ctr, 0, \ell\rangle \cdot s''', h'\rangle \xrightarrow{\texttt{rlb}\ ctr\cdot\texttt{pc}\ \sigma'(\mathbf{pc})} \langle ctr'', \sigma', s'', h' \cdot \langle \sigma(\mathbf{pc}), ctr, \sigma'(\mathbf{pc})\rangle\rangle$. We return r'.

- If $\neg enabled(s)$, then there is a pending transaction (with identifier id) that has to be committed. In this case, we simply perform one step by applying the Se-Commit rule.

Finally, the execution r' is constructed by concatenating the partial executions $r_0, \ldots, r_n$, which are constructed as follows:

$$cfg_0 := \langle ctr_0, \sigma_0, \varepsilon, \varepsilon\rangle$$
$$r_i = \textsc{expand}(cfg_i, \sigma_i \xrightarrow{\tau_i} \sigma_{i+1})$$
$$cfg_i := last(r_{i-1}) \qquad \text{if } i > 0$$

From the construction, it immediately follows that the initial extended configuration in r' is $\langle ctr_0, \sigma_0, \varepsilon, \varepsilon\rangle$ and the final configuration is $\langle ctr, \sigma_0, \varepsilon, h\rangle$ (for some $ctr \in \mathbb{N}$ and $h \in \mathcal{H}$) since (1) r is a terminating run, (2) we always execute all transactions until completion, (3) speculative transactions always terminate given that speculative windows are decremented during execution, (4) rolled-back speculative transactions do not affect the configuration σ. Similarly, it is easy to see that $\tau\upharpoonright_{ns} = \tau_0 \cdot \ldots \cdot \tau_n$ since (1) the observations associated with committed steps are equivalent to those in the non-speculative semantics, (2) observations associated with rolled back transactions are removed by the projection (and we execute all transactions until termination, and (3) other extended observations are removed by the non-speculative projection. □

G.2 B: Relating the always-mispredict and non-speculative semantics

We start by spelling out the definition of $\{\!|p|\!\}_w$. Given a program p and a speculative window w, we denote by $\{\!|p|\!\}_w$ the set of all triples $\langle \sigma, \tau, \sigma'\rangle \in InitConf \times ExtObs^* \times FinalConf$ corresponding to executions $\langle 0, \sigma, \varepsilon\rangle \overset{\tau}{\Longrightarrow}{}^{*} \langle ctr, \sigma', \varepsilon\rangle$.

We are now ready to prove Theorem 4, which we restate here for simplicity:

Theorem 4 (B: Behaviour of non-speculative semantics and AM semantics). *Let p be a program. Then $Beh_{NS}(p) = Beh^{\omega}_{\mathrm{B}}(p)\upharpoonright_{ns}$*

Proof. The proposition can be proved in a similar way to Proposition 3. Specifically, the proof of the direction ($\Leftarrow$) is a simpler version of Lemma 10 (B: Soundness)'s proof since there are only rolled-back transactions. The proof of the direction ($\Rightarrow$), instead, is identical Proposition 2 ()'s proof. □

G.3 B: Relating concrete and symbolic always mispredict semantics

Below, we provide the proof of Proposition 3: We note that the path condition is here collected on the trace instead of in a separate structure $\delta^{\mathcal{S}}$ as we have shown previously.

Proposition 3 (B: Symbolic Consistency)**.** *Let p be a program and $w \in \mathbb{N}$ be a speculative window. Then, $\{\!|p|\!\}_w = \gamma(\{\!|p|\!\}^{symb}_w)$.*

Proof. The proposition follows from Proposition 4 (proved in Appendix G.3.2) and Proposition 5 (proved in Appendix G.3.3).

We now prove the two directions:

($\Rightarrow$) : Let $\langle \sigma, \tau, \sigma' \rangle$ be a run in $\{\!|p|\!\}_w$. From this, it follows that $\langle 0, \sigma, \varepsilon \rangle \overset{p}{\Longrightarrow} w\tau^* \langle ctr, \sigma', \varepsilon \rangle$. From Proposition 5 (proved in Appendix G.3.3), there is a valuation μ, a symbolic trace τ', and a final symbolic configuration σ'' such that $\langle 0, \langle sm_0, sa_0 \rangle, \varepsilon \rangle \overset{\tau'}{\Longrightarrow}_s^* \langle ctr, \sigma'', \varepsilon \rangle$, $\mu(\tau') = \tau$, $\mu(\langle sm_0, sa_0 \rangle) = \sigma$, $\mu(\sigma'') = \sigma'$, and $\mu \models pthCnd(\tau')$. Hence, $\langle \langle sm_0, sa_0 \rangle, \tau', \sigma'' \rangle \in symTraces_p(w)$ and $\langle \mu(\langle sm_0, sa_0 \rangle), \mu(\tau'), \mu(\sigma'') \rangle \in \gamma(\langle \langle sm_0, sa_0 \rangle, \tau', \sigma'' \rangle)$ (since $\mu \models pthCnd(\tau')$). Therefore, $\langle \mu(\langle sm_0, sa_0 \rangle), \mu(\tau'), \mu(\sigma'') \rangle \in \gamma(symTraces_p(w))$. From this and $\mu(\tau') = \tau$, $\mu(\langle sm_0, sa_0 \rangle) = \sigma$, $\mu(\sigma'') = \sigma'$, we have $\langle \sigma, \tau, \sigma' \rangle \in \gamma(symTraces_p(w))$.

($\Leftarrow$) : Let $\langle \sigma, \tau, \sigma' \rangle$ be a run in $\gamma(symTraces_p(w))$. From this, it follows that there is a symbolic run $\langle \sigma_s, \tau_s, \sigma'_s \rangle \in symTraces_p(w)$ and a valuation μ such that $\mu \models pthCnd(\tau_s)$ and $\mu(\sigma_s) = \sigma$, $\mu(\sigma'_s) = \sigma'$, and $\mu(\tau_s) = \tau$. From $\langle \sigma_s, \tau_s, \sigma'_s \rangle \in symTraces_p(w)$, we have that $\langle 0, \sigma_s, \varepsilon \rangle \overset{\tau_s}{\Longrightarrow}_s^* \langle ctr, \sigma'_s, \varepsilon \rangle$. From Proposition 4 (proved in Appendix G.3.2) and $\mu \models pthCnd(\tau_s)$, we have that $\langle 0, \mu(\sigma_s), \varepsilon \rangle \overset{p}{\Longrightarrow} w\mu(\tau_s)^* \langle ctr, \mu(\sigma'_s), \varepsilon \rangle$. Therefore, $\langle \mu(sigma_s), \mu(\tau_s), \mu(\sigma'_s) \rangle \in \{\!|p|\!\}_w$. From this and $\mu(\sigma_s) = \sigma$, $\mu(\sigma'_s) = \sigma'$, and $\mu(\tau_s) = \tau$, we have $\langle \sigma, \tau, \sigma' \rangle \in \{\!|p|\!\}_w$.

This completes the proof of our claim. ◻

G.3.1 Auxiliary definitions. Given a symbolic speculative state $\langle \sigma, id, w, \ell \rangle \in SpecS$, its *next-step mispredict path condition* $pthCnd(\langle \sigma, id, w, \ell \rangle)$ is the symbolic expression $pthCnd(\tau)$ such that $\sigma \overset{\tau}{\longrightarrow}_s \sigma'$ and $\sigma'(\mathbf{pc}) \neq \ell$ (if such a τ does not exists, then $pthCnd(s) = \top$). Given a sequence of symbolic speculative states $s \in SpecS^*$, its *next-step mispredict path condition* $pthCnd(s) = \bigwedge_{\langle \sigma, id, w, \ell \rangle \in s} pthCnd(\langle \sigma, id, w, \ell \rangle)$.

We say that a concrete speculative state $\langle \sigma, id, w, \ell \rangle \in SpecS$ is *next-step mispredict well-formed*, written $wf(\langle \sigma, id, w, \ell \rangle)$, if $\sigma \overset{\tau}{\longrightarrow}_s \sigma'$ and $\sigma'(\mathbf{pc}) \neq \ell$. We say that a sequence of speculative states $s \in SpecS^*$ is *next-step mispredict well-formed*, written $wf(s)$, if $\bigwedge_{\langle \sigma, id, w, \ell \rangle \in s} wf(\langle \sigma, id, w, \ell \rangle)$.

G.3.2 Soundness. In Proposition 4, we prove the soundness of the symbolic semantics.

Proposition 4. *Let p be a program and μ be a valuation. Whenever $\langle 0, \langle sm_0, sa_0 \rangle, \varepsilon \rangle \overset{\tau}{\Longrightarrow}_s^* \langle ctr, \langle sm, sa \rangle, \varepsilon \rangle$, $\langle sm, sa \rangle \in FinalConf$, and $\mu \models pthCnd(\tau)$, then $\langle 0, \langle \mu(sm_0), \mu(sa_0) \rangle, \varepsilon \rangle \overset{p}{\Longrightarrow} O\mu(\tau)^* \langle ctr, \langle \mu(sm), \mu(sa) \rangle, \varepsilon \rangle$.*

Proof. Let p be a program and μ be a valuation. Assume that, for some $n \in \mathbb{N}$, $\langle ctr_0, \langle sm_0, sa_0 \rangle, s_0 \rangle \overset{\tau_0}{\Longrightarrow}_s \langle ctr_1, \langle sm_1, sa_1 \rangle, s_1 \rangle \overset{\tau_1}{\Longrightarrow}_s \ldots \langle ctr_n, \langle sm_n, sa_n \rangle, s_n \rangle \overset{\tau_n}{\Longrightarrow}_s \langle ctr_{n+1}, \langle sm_{n+1}, sa_{n+1} \rangle, s_{n+1} \rangle$, where $ctr_0 = 0$, $s_0 = s_{n+1} = \varepsilon$, and $\langle sm_n, sa_n \rangle \in FinalConf$. Finally, assume that $\mu \models pthCnd(\tau_0 \cdot \tau_1 \cdot \ldots \cdot \tau_n)$. We claim that, for all $1 \leq i \leq n+1$, $\mu \models pthCnd(s_{i-1})$. We can obtain the concrete execution $\langle ctr_0, \langle \mu(sm_0), \mu(sa_0) \rangle, \mu(s_0) \rangle \overset{\mu(\tau_0 \cdot \tau_1 \cdot \ldots \cdot \tau_n)}{\rightsquigarrow}^n \langle ctr_{n+1}, \langle \mu(sm_{n+1}), \mu(sa_{n+1}) \rangle, \mu(s_{n+1}) \rangle$ by repeatedly applying Lemma 16 (since for all $1 \leq i \leq n+1$, $\mu \models pthCnd(s_{i-1}) \wedge pthCnd(\tau_i)$).

We now show that for all $0 \leq i \leq n+1$, $\mu \models pthCnd(s_i)$. We prove this by induction. For the base case of $i = 0$, the claim trivially holds since $s_0 = \varepsilon$ and therefore $pthCnd(s_0) = \top$. For the induction step, assume that the claim holds for all $j < i$. We now show that it holds for i as well. There are three cases:

- The i-th configuration has been derived using the Se-NoBranch rule. Then, s_{i-1} and s_i only differ in the length of the remaining speculation windows. Therefore, $pthCnd(s_{i-1}) = pthCnd(s_i)$. From the induction hypothesis, $\mu \models pthCnd(s_{i-1})$. Therefore, $\mu \models pthCnd(s_i)$.
- The i-th configuration has been derived using the Se-Branch rule. Then, $s_i = decr'(s_{i-1}) \cdot \langle \langle sm_{i-1}, sa_{i-1} \rangle, id, min(w, wndw(s) - 1), \ell \rangle$, where $p(sa_{i-1}(\mathbf{pc})) = \mathbf{beqz}\ x, \ell''$, $\langle sm_{i-1}, sa_{i-1} \rangle \xrightarrow{\texttt{symPc}(se) \cdot \texttt{pc}\ \ell'}_s \sigma'$,

$\ell = \begin{cases} sa_{i-1}(\mathbf{pc}) + 1 & \text{if } \ell' \neq sa_{i-1}(\mathbf{pc}) + 1 \\ \ell'' & \text{if } \ell' = sa_{i-1}(\mathbf{pc}) + 1 \end{cases}$, and $pthCnd(\tau_{i-1}) = se$. From this, it follows that $pthCnd(\langle\sigma, id, 0, \ell\rangle) = se$. From this, $pthCnd(\tau_{i-1}) = se$, and $\mu \models pthCnd(\tau_0 \cdot \tau_1 \cdot \ldots \cdot \tau_n)$, we have that $\mu \models se$. Moreover, from $pthCnd(s_i) = pthCnd(s_{i-1}) \wedge se$, $\mu \models se$, and the induction hypothesis, we have $\mu \models pthCnd(s_i)$.

- The i-th configuration has been derived using the Se-Rollback rule. Then, $s_{i-1} = s_i \cdot \langle\sigma, id, 0, \ell\rangle$ for some σ, id, and ℓ. Therefore, $pthCnd(s_{i-1}) = pthCnd(s_i) \wedge \varphi$ for some φ. From the induction hypothesis, $\mu \models pthCnd(s_{i-1})$. From this and $pthCnd(s_{i-1}) = pthCnd(s_i) \wedge \varphi$ for some φ, we have $\mu \models pthCnd(s_i)$.

This completes the proof of our claim. ◻

In Lemma 16, we prove the soundness of a single step of the symbolic always mispredict semantics.

Lemma 16. *Let p be a program. Whenever $\langle ctr, \langle sm, sa\rangle, s\rangle \overset{\tau}{\Longrightarrow}_s \langle ctr', \langle sm', sa'\rangle, s'\rangle$, then for all mappings $\mu : SymbVals \to Vals$ such that $\mu \models pthCnd(s) \wedge pthCnd(\tau)$, $\langle ctr, \langle \mu(sm), \mu(sa)\rangle, \mu(s)\rangle \overset{p}{\Longrightarrow} O\mu(\tau)\langle ctr', \langle \mu(sm'), \mu(sa')\rangle, \mu(s')\rangle$.*

Proof. Let $p \in Prg$ be a program. Moreover, assume that $\langle ctr, \langle sm, sa\rangle, s\rangle \overset{\tau}{\Longrightarrow}_s \langle ctr', \langle sm', sa'\rangle, s'\rangle$. We proceed by case distinction on the rules defining $\Longrightarrow_s$.

Rule Am-NoBranch. Assume that $\langle ctr, \langle sm, sa\rangle, s\rangle \overset{\tau}{\Longrightarrow}_s \langle ctr', \langle sm', sa'\rangle, s'\rangle$ has been derived using the Se-NoBranch rule in the symbolic semantics. Then, $\langle sm, sa\rangle \xrightarrow{\tau}_s \langle sm', sa'\rangle$, $p(sa(\mathbf{pc})) \neq \mathbf{beqz}\ x, \ell$, $enabled'(s)$, $ctr' = ctr$, and $s' = decr'(s)$. Let $\mu : SymbVals \to Vals$ be an arbitrary valuation that satisfies $pthCnd(s) \wedge pthCnd(\tau)$. Observe that μ also satisfies $pthCnd(\tau)$. Therefore, we can apply Lemma 2 to $\langle sm, sa\rangle \xrightarrow{\tau}_s \langle sm', sa'\rangle$ to derive $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\mu(\tau)} \langle \mu(sm'), \mu(sa')\rangle$. Moreover, we immediately have that $enabled'(s)$ iff $enabled'(\mu(s))$ and $p(sa(\mathbf{pc})) \neq \mathbf{beqz}\ x, \ell$, iff $p(\mu(sa)(\mathbf{pc})) \neq \mathbf{beqz}\ x, \ell$,. Thus, we can apply the rule Am-NoBranch of the concrete semantics starting from $\langle ctr, \langle \mu(sm), \mu(sa)\rangle, \mu(s)\rangle$. Therefore, $\langle ctr, \langle \mu(sm), \mu(sa)\rangle, \mu(s)\rangle \overset{p}{\Longrightarrow} O\mu(\tau)\langle ctr, \langle \mu(sm'), \mu(sa')\rangle, \mu(s')\rangle$.

Rule Am-Branch. Assume that $\langle ctr, \langle sm, sa\rangle, s\rangle \overset{\tau}{\Longrightarrow}_s \langle ctr', \langle sm', sa'\rangle, s'\rangle$ has been derived using the Se-Branch rule in the symbolic semantics. Then, $p(sa(\mathbf{pc})) = \mathbf{beqz}\ x, \ell''$, $enabled'(s)$, $\langle sm, sa\rangle \xrightarrow{\mathtt{symPc}(se) \cdot \mathtt{pc}\ \ell'}_s \sigma'$, $\ell = \begin{cases} sa(\mathbf{pc}) + 1 & \text{if } \ell' \neq sa(\mathbf{pc}) + 1 \\ \ell'' & \text{if } \ell' = sa(\mathbf{pc}) + 1 \end{cases}$, $ctr' = ctr + 1$, $sm' = sm$, $sa' = sa[\mathbf{pc} \mapsto \ell]$, $s' = s \cdot \langle\langle sm, sa\rangle, ctr, min(w, wndw(s) - 1), \ell\rangle$, and $\tau = \mathtt{symPc}(se) \cdot \mathtt{start}\ ctr \cdot \mathtt{pc}\ \ell$. Let $\mu : SymbVals \to Vals$ be an arbitrary valuation satisfying $pthCnd(s) \wedge pthCnd(\tau)$. Observe that μ also satisfies $pthCnd(\tau)$, i.e., $\mu \models se$. We can apply Lemma 2 to $\langle sm, sa\rangle \xrightarrow{\mathtt{symPc}(se) \cdot \mathtt{pc}\ \ell'}_s \sigma'$ to derive $\langle \mu(sm), \mu(sa)\rangle \xrightarrow{\mu(\tau)} \mu(\sigma')$. Observe that $\mu(\sigma')(\mathbf{pc}) = \ell'$ and $enabled'(s)$ holds iff $enabled'(\mu(s))$ does. Therefore, we can apply the rule Am-Branch of the concrete semantics starting from $\langle ctr, \langle \mu(sm), \mu(sa)\rangle, \mu(s)\rangle$. We have $\langle ctr, \langle \mu(sm), \mu(sa)\rangle, \mu(s)\rangle \overset{p}{\Longrightarrow} O_n \mathtt{start}\ ctr \cdot \mathtt{pc}\ \ell'''\langle ctr + 1, \langle \mu(sm), \mu(sa)[\mathbf{pc} \mapsto \ell''']\rangle, \mu(s) \cdot \langle\langle \mu(sm), \mu(sa)\rangle, ctr, min(w, wndw(\mu(s)) - 1), \ell'''\rangle\rangle$. We claim that $\ell = \ell'''$. Hence, $\langle ctr, \langle \mu(sm), \mu(sa)\rangle, \mu(s)\rangle \overset{p}{\Longrightarrow} O\mu(\tau)\langle ctr', \langle \mu(sm'), \mu(sa')\rangle, \mu(s')\rangle$.

We now show that $\ell = \ell'''$. There are two cases:

$\ell = sa(\mathbf{pc}) + 1$: Then, $\ell' \neq sa(\mathbf{pc}) + 1$. There are two cases:

- The step $\langle sm, sa\rangle \xrightarrow{\mathtt{symPc}(se) \cdot \mathtt{pc}\ \ell'}_s \sigma'$ has been derived using the Beqz-Concr-Sat rule from the symbolic non-speculative semantics. Then, $sa(x) = 0$. Therefore, $\mu(sa)(x) = 0$ and $\ell''' = \mu(sa)(\mathbf{pc})+1$ by construction. Hence, $\ell = \ell'''$.

 * The step $\langle sm, sa\rangle \xrightarrow{\texttt{symPc}(se)\cdot\texttt{pc}\ \ell'}_s \sigma'$ has been derived using the BEQZ-SYMB-SAT rule from the symbolic non-speculative semantics. Then, se is $sa(x) = 0$. From this and $\mu \models se$, we have that $\mu(sa)(x) = 0$ and, therefore, $\ell''' = \mu(sa)(\mathbf{pc}) + 1$ by construction. Hence, $\ell = \ell'''$.

This completes the proof of this case.

$\ell = \ell''$: Then, $\ell' = sa(\mathbf{pc}) + 1$. There are two cases:

 * The step $\langle sm, sa\rangle \xrightarrow{\texttt{symPc}(se)\cdot\texttt{pc}\ \ell'}_s \sigma'$ has been derived using the BEQZ-CONCR-UNSAT rule from the symbolic non-speculative semantics. Then, $sa(x) \neq 0$. Therefore, $\mu(sa)(x) \neq 0$ and $\ell''' = \ell''$ by construction. Hence, $\ell = \ell'''$.
 * The step $\langle sm, sa\rangle \xrightarrow{\texttt{symPc}(se)\cdot\texttt{pc}\ \ell'}_s \sigma'$ has been derived using the BEQZ-SYMB-UNSAT rule from the symbolic non-speculative semantics. Then, se is $sa(x) \neq 0$. From this and $\mu \models se$, we have that $\mu(sa)(x) \neq 0$ and, therefore, $\ell''' = \ell''$ by construction. Hence, $\ell = \ell'''$.

This completes the proof of this case.

This completes the proof of our claim.

Rule AM-ROLLBACK. Assume that $\langle ctr, \langle sm, sa\rangle, s\rangle \overset{\tau}{\Longrightarrow}_s \langle ctr', \langle sm', sa'\rangle, s'\rangle$ has been derived using the SE-ROLLBACK rule in the symbolic semantics. Then, $s = s_B \cdot \langle \sigma, id, 0, \ell\rangle$, $\sigma \xrightarrow{\tau'}_s \sigma'$, $ctr' = ctr$, $\sigma' = \langle sm', sa'\rangle$, $s' = s_B$, $sa'(\mathbf{pc}) \neq \ell$, and $\tau = \texttt{rlb}\ id \cdot \texttt{pc}\ \sigma'(\mathbf{pc})$. Let $\mu : SymbVals \to Vals$ be an arbitrary valuation satisfying $pthCnd(s) \wedge pthCnd(\tau)$. We claim that $\mu \models pthCnd(\tau')$. Therefore, Lemma 2 to $\sigma \xrightarrow{\tau'}_s \sigma'$ to derive $\mu(\sigma) \xrightarrow{\mu(\tau')} \mu(\sigma')$. By applying the rule AM-ROLLBACK of the concrete semantics starting from $\langle ctr, \langle \mu(sm), \mu(sa)\rangle, \mu(s)\rangle$, we obtain $\langle ctr, \langle \mu(sm), \mu(sa)\rangle, \mu(s_B) \cdot \langle \sigma, id, 0, \ell\rangle\rangle \overset{p}{\Longrightarrow} \mathcal{O}_n \texttt{rlb}\ id \cdot \texttt{pc}\ \sigma'(\mathbf{pc}) \langle ctr, \mu(\sigma'), \mu(s_B)\rangle$. Since $\sigma'(\mathbf{pc}) = \mu(\sigma')(\mathbf{pc}) = \ell$ (since the program counter is always concrete), we have that $\langle ctr, \langle \mu(sm), \mu(sa)\rangle, \mu(s)\rangle \overset{p}{\Longrightarrow} \mathcal{O}\mu(\tau)\langle ctr', \langle \mu(sm'), \mu(sa')\rangle, \mu(s')\rangle$.

We now prove our claim that $\mu \models pthCnd(\tau')$. There are four cases:

 – The step $\sigma \xrightarrow{\tau'}_s \sigma'$ has been derived using the BEQZ-CONCR-SAT rule from the symbolic non-speculative semantics. Then, $pthCnd(\tau') = \top$ and the claim trivially holds.
 – The step $\sigma \xrightarrow{\tau'}_s \sigma'$ has been derived using the BEQZ-CONCR-UNSAT rule from the symbolic non-speculative semantics. Then, $pthCnd(\tau') = \top$ and the claim trivially holds.
 – The step $\sigma \xrightarrow{\tau'}_s \sigma'$ has been derived using the BEQZ-SYMB-SAT rule from the symbolic non-speculative semantics. Then, $pthCnd(\tau')$ is $sa(x) = 0$. Observe that $sa(x) = 0$ is one of the conjuncts of $pthCnd(s)$ by construction. Therefore, $\mu \models pthCnd(\tau')$ since $\mu \models pthCnd(s)$.
 – The step $\sigma \xrightarrow{\tau'}_s \sigma'$ has been derived using the BEQZ-SYMB-UNSAT rule from the symbolic non-speculative semantics. Then, $pthCnd(\tau')$ is $sa(x) \neq 0$. Observe that $sa(x) \neq 0$ is one of the conjuncts of $pthCnd(s)$ by construction. Therefore, $\mu \models pthCnd(\tau')$ since $\mu \models pthCnd(s)$.

This completes the proof of our claim.

This completes the proof of our claim. ◻

G.3.3 Completeness. In Proposition 5 we prove the completeness of our symbolic semantics.

Proposition 5. *Let p be a program. Whenever $\langle 0, \sigma, \varepsilon\rangle \overset{p}{\Longrightarrow} \mathcal{O}\tau'^{*}\langle ctr, \sigma', \varepsilon\rangle$, $\sigma \in InitConf$, and $\sigma' \in FinalConf$, then there is a valuation μ, a symbolic trace τ', and a final symbolic configuration $\langle sm, sa\rangle$ such that $\langle 0, \langle sm_0, sa_0\rangle, \varepsilon, \top\rangle \overset{\tau'}{\Longrightarrow}_s^{*} \langle ctr, \langle sm, sa\rangle, \varepsilon\rangle$, $\mu(\langle sm_0, sa_0\rangle) = \sigma$, $\mu(\langle sm, sa\rangle) = \sigma'$, $\mu(\tau') = \tau$, and $\mu \models pthCnd(\tau')$.*

Proof. Let p be a program and $\langle ctr_0, \sigma_0, s_0\rangle \overset{p}{\Longrightarrow} O\tau_0\langle ctr_1, \sigma_1, s_1\rangle \overset{p}{\Longrightarrow} O\tau_1 \ldots \langle ctr_n, \sigma_n, s_n\rangle \overset{p}{\Longrightarrow} O\tau_n\langle ctr_{n+1}, \sigma_{n+1}, s_{n+1}\rangle$ be a concrete execution, where $ctr_0 = 0$, $s_0 = s_{n+1} = \varepsilon$, $\sigma_0 \in InitConf$, and $\sigma_{n+1} \in FinalConf$. We claim that $wf(s_i)$ holds for all $0 \le i \le n+1$. Furthermore, let μ be a valuation such that $\mu(\langle sm_0, sa_0\rangle) = \sigma_0$. We can construct the symbolic execution $\langle 0, \langle sm_0, sa_0\rangle, \varepsilon, \top\rangle \overset{\tau'}{\Longrightarrow}_s^* \langle ctr, \langle sm, sa\rangle, \varepsilon\rangle$ by repeatedly applying Lemma 17. From the same Lemma, we also obtain that $\mu(\langle sm_0, sa_0\rangle) = \sigma_0$, $\mu(\langle sm, sa\rangle) = \sigma_{n+1}$, $\mu(\tau') = \tau_0 \cdot \ldots \cdot \tau_n$, and $\mu \models pthCnd(\tau')$.

We prove by induction that $wf(s_i)$ holds for all $0 \le i \le n+1$. For the base case $i = 0$, $s_0 = \varepsilon$ and $wf(s_0)$ holds trivially. For the induction step, we assume that $wf(s_j)$ holds for all $j < i$ and we show that it holds also for s_j. There are three cases:

- The i-th configuration has been derived using the Am-NoBranch rule. Then, s_{i-1} and s_i only differ in the length of the remaining speculation windows. Therefore, $wf(s_i)$ holds iff $wf(s_{i-1})$ does. From the induction hypothesis, $wf(s_{i-1})$ holds and therefore $wf(s_i)$ holds.
- The i-th configuration has been derived using the Am-Branch rule. Then, $s_i = decr'(s_{i-1}) \cdot \langle \sigma_{i-1}, ctr, min(w, wndw(s) - 1), \ell\rangle$, where $p(\sigma_{i-1}(\mathbf{pc})) = \mathbf{beqz}\ x, \ell''$, $\sigma_{i-1} \xrightarrow{\mathsf{pc}\ \ell'} \sigma'$, and $\ell = \begin{cases} \sigma_{i-1}(\mathbf{pc}) + 1 & \text{if } \sigma_{i-1}(x) = 0 \\ \ell' & \text{if } \sigma_{i-1}(x) \neq 0 \end{cases}$. From this, $wf(s_i)$ holds iff both $wf(s_{i-1})$ and $wf(\langle \sigma_{i-1}, ctr, min(w, wndw(s) - 1), \ell\rangle)$ hold. The former follows from the induction hypothesis, the latter follows from $\sigma_{i-1} \xrightarrow{\mathsf{pc}\ \ell'} \sigma'$ and $\ell = \begin{cases} \sigma_{i-1}(\mathbf{pc}) + 1 & \text{if } \sigma_{i-1}(x) = 0 \\ \ell' & \text{if } \sigma_{i-1}(x) \neq 0 \end{cases}$.
- The i-th configuration has been derived using the Am-Rollback rule. Then, $s_{i-1} = s_i \cdot \langle \sigma, id, 0, \ell\rangle$ for some σ, id, and ℓ, i.e., if $wf(s_{i-1})$ holds, then $wf(s_i)$ holds as well. From the induction hypothesis, $wf(s_{i-1})$ holds and, thus, $wf(s_i)$ holds.

This completes the proof of our claim.

□

In Lemma 17, we prove the completeness of one step of the symbolic semantics.

Lemma 17. *Let p be a program, sa be a symbolic assignment, sm be a symbolic memory, and ss be a sequence of symbolic speculative states. Whenever $\langle ctr, \langle m, a\rangle, s\rangle \overset{p}{\Longrightarrow} O_n\tau\langle ctr', \langle m', a'\rangle, s'\rangle$ and $wf(s)$, then for all valuations $\mu : SymbVals \to Vals$ such that $\mu(sa) = a$, $\mu(sm) = m$, and $\mu(ss) = s$, then there are τ', ctr', sm', sa' such that $\langle ctr, \langle sm, sa\rangle, ss\rangle \overset{\tau'}{\Longrightarrow}_s \langle ctr', \langle sm', sa'\rangle, ss'\rangle$, $\mu(sm') = m'$, $\mu(sa') = a'$, $\mu(ss') = s'$, $\mu(\tau') = \tau$, and $\mu \models pthCnd(\tau')$.*

Proof. Let p be a program, sa be a symbolic assignment, sm be a symbolic memory, ss be a symbolic speculative state. Moreover, assume that $\langle ctr, \langle m, a\rangle, s\rangle \overset{p}{\Longrightarrow} O_n\tau\langle ctr', \langle m', a'\rangle, s'\rangle$ holds and $wf(s)$. Finally, let $\mu : SymbVals \to Vals$ be an arbitrary valuation such that $\mu(sa) = a$, $\mu(sm) = m$, and $\mu(ss) = s$. We proceed by case distinction on the rules defining $\overset{p}{\Longrightarrow} O_n$.

Rule Am-NoBranch. Assume that $\langle ctr, \langle m, a\rangle, s\rangle \overset{p}{\Longrightarrow} O_n\tau\langle ctr', \langle m', a'\rangle, s'\rangle$ has been derived using the Se-NoBranch rule in the concrete semantics. Then, $p(a(\mathbf{pc})) \neq \mathbf{beqz}\ x, \ell$, $\langle m, a\rangle \xrightarrow{\tau} \langle m', a'\rangle$, $enabled'(s)$, $ctr' = ctr$, and $s' = decr'(s)$. Observe that $p(sa(\mathbf{pc})) \neq \mathbf{beqz}\ x, \ell$, and $enabled'(ss)$ immediately follow from $p(a(\mathbf{pc})) \neq \mathbf{beqz}\ x, \ell$ and $enabled'(s)$ respectively. We can apply Lemma 4 to $\langle m, a\rangle \xrightarrow{\tau} \langle m', a'\rangle$. Therefore, for all valuation μ such that $\mu(sa) = a$ and $\mu(sm) = m$, there are sm', sa', τ' such that $\langle sm, sa\rangle \xrightarrow{\tau'}_s \langle sm', sa'\rangle$, $\mu(sm') = m'$, $\mu(sa') = a'$, $\mu(\tau') = \tau$, and $\mu \models pthCnd(\tau')$. Since μ is a valuation for which $\mu(sa) = a$ and $\mu(sm) = m$, we therefore have that

$\langle sm, sa\rangle \xrightarrow{\tau'}_s \langle sm', sa'\rangle$, $\mu(sm') = m'$, $\mu(sa') = a'$, $\mu(\tau') = \tau$, and $\mu \models pthCnd(\tau')$. Hence, we can apply the Am-NoBranch rule in the symbolic semantics to $\langle ctr, \langle sm, sa\rangle, ss\rangle$. Thus, $\langle ctr, \langle sm, sa\rangle, ss\rangle \overset{\tau'}{\Longrightarrow}_s \langle ctr'', \langle sm', sa'\rangle, ss'\rangle$, where $ctr'' = ctr$. We have already established that $\mu(sm') = m'$, $\mu(sa') = a'$, and $\mu(\tau') = \tau$, and $\mu \models pthCnd(\tau')$ (which all follow from the application of Lemma 4). We still have to show $\mu(ss') = s'$. This immediately follows from $\mu(ss) = s$, $s' = \begin{cases} decr'(s) & \text{if } p(a(\mathbf{pc})) \neq \mathbf{spbarr} \\ zeroes'(s) & \text{otherwise} \end{cases}$, $ss' = \begin{cases} decr'(ss) & \text{if } p(sa(\mathbf{pc})) \neq \mathbf{spbarr} \\ zeroes'(ss) & \text{otherwise} \end{cases}$, and $sa(\mathbf{pc}) = a(\mathbf{pc})$.

Rule Am-Branch. Assume that $\langle ctr, \langle m, a\rangle, s\rangle \overset{p}{\Longrightarrow} O_n\tau\langle ctr', \langle m', a'\rangle, s'\rangle$ has been derived using the Se-Branch rule in the concrete semantics. Then, $p(a(\mathbf{pc})) = \mathbf{beqz}\ x, \ell'$, $enabled'(s)$, $\ell = \begin{cases} a(\mathbf{pc}) + 1 & \text{if } a(x) = 0 \\ \ell' & \text{if } a(x) \neq 0 \end{cases}$, $\tau = \texttt{start}\ ctr \cdot \texttt{pc}\ \ell$, $m' = m$, $a' = a[\mathbf{pc} \mapsto \ell]$, $ctr' = ctr + 1$, and $s' = decr'(s) \cdot \langle\langle m, a\rangle, ctr, min(w, wndw(s) - 1), \ell\rangle$. Observe that $enabled'(ss)$ directly follows from $\mu(ss) = s$ and $enabled'(s)$ and $p(sa(\mathbf{pc})) = \mathbf{beqz}\ x, \ell'$ follows from $\mathbf{pc}$ being always concrete and $\mu(sa) = a$. Observe also that $\langle m, a\rangle \xrightarrow{\texttt{pc}\ \ell''} \langle m, a[\mathbf{pc} \mapsto \ell'']\rangle$ holds where $\ell'' \in \{\ell', a(\mathbf{pc})+1\} \setminus \{\ell\}$. We can apply Lemma 4 to $\langle m, a\rangle \xrightarrow{\texttt{pc}\ \ell''} \langle m, a[\mathbf{pc} \mapsto \ell'']\rangle$. Therefore, for all valuations μ such that $\mu(sa) = a$ and $\mu(sm) = m$, $\langle sm, sa\rangle \xrightarrow{\tau'}_s \langle sm', sa'\rangle$, $\mu(sm') = m$, $\mu(sa') = a[\mathbf{pc} \mapsto \ell'']$, $\mu(\tau') = \texttt{pc}\ \ell''$, and $\mu \models pthCnd(\tau')$. Since $\mu(sa) = a$ and $\mu(sm) = m$, we thus have that $\langle sm, sa\rangle \xrightarrow{\tau''}_s \langle sm', sa'\rangle$, $\mu(sm') = m$, $\mu(sa') = a[\mathbf{pc} \mapsto \ell'']$, $\mu(\tau'') = \texttt{pc}\ \ell''$, and $\mu \models pthCnd(\tau'')$. Observe that, since $p(sa(\mathbf{pc})) = \mathbf{beqz}\ x, \ell'$, τ' is of the form $\texttt{symPc}(se) \cdot \texttt{pc}\ \ell''$. Therefore, we can apply the Am-Branch-Symb rule in the symbolic semantics to $\langle ctr, \langle sm, sa\rangle, ss\rangle$ to derive $\langle ctr, \langle sm, sa\rangle, ss\rangle \overset{p}{\Longrightarrow} w\tau'\langle ctr + 1, \langle sm', sa'\rangle, ss'\rangle$, where $\tau' = \texttt{symPc}(se) \cdot \texttt{start}\ id \cdot \texttt{pc}\ \ell'''$, $sm' = sm$, $sa' = sa[\mathbf{pc} \mapsto \ell''']$, $\ell''' = \begin{cases} \sigma(\mathbf{pc}) + 1 & \text{if } \ell'' \neq sa(\mathbf{pc}) + 1 \\ \ell' & \text{if } \ell'' = sa(\mathbf{pc}) + 1 \end{cases}$, $ss' = decr'(ss) \cdot \langle\langle sm, sa\rangle, ctr, min(w, wndw(ss) - 1), \ell'''\rangle$, and $id = ctr$. We claim that $\ell''' = \ell$. From $\mu(sm) = m$ and $m' = m$, we get that $\mu(sm') = \mu(sm) = m = m'$. From $\mu(sa) = a$, $a' = a[\mathbf{pc} \mapsto \ell]$, $sa' = sa[\mathbf{pc} \mapsto \ell''']$, and $\ell = \ell'''$, we have that $\mu(sa') = \mu(sa[\mathbf{pc} \mapsto \ell''']) = \mu(sa)[\mathbf{pc} \mapsto \ell'''] = a[\mathbf{pc} \mapsto \ell'''] = a[\mathbf{pc} \mapsto \ell] = a'$. From $\tau = \texttt{start}\ ctr \cdot \texttt{pc}\ \ell$, $\tau' = \texttt{symPc}(se) \cdot \texttt{start}\ id \cdot \texttt{pc}\ \ell'''$, and $\ell = \ell'''$, we have $\mu(\tau') = \tau$. From $\mu(ss) = s$, $\mu(sa) = a$, $\mu(sm) = m$, $s' = decr'(s) \cdot \langle\langle m, a\rangle, ctr, min(w, wndw(s) - 1), \ell\rangle$, $ss' = decr'(ss) \cdot \langle\langle sm, sa\rangle, ctr, min(w, wndw(ss) - 1), \ell'''\rangle$, and $\ell = \ell'''$, we have $\mu(ss') = \mu(decr'(ss) \cdot \langle\langle sm, sa\rangle, ctr, min(w, wndw(ss) - 1), \ell'''\rangle) = decr'(\mu(ss)) \cdot \langle\langle \mu(sm), \mu(sa)\rangle, ctr, min(w, wndw(\mu(ss)) - 1), \ell'''\rangle = decr'(s) \cdot \langle\langle m, a\rangle, ctr, min(w, wndw(s) - 1), \ell'''\rangle = decr'(s) \cdot \langle\langle m, a\rangle, ctr, min(w, wndw(s) - 1), \ell\rangle = s'$. Finally, $\mu \models pthCnd(\tau')$ immediately follows from $\tau' = \texttt{symPc}(se) \cdot \texttt{start}\ id \cdot \texttt{pc}\ \ell'''$, $\tau'' = \texttt{symPc}(se) \cdot \texttt{pc}\ \ell''$, and $\mu \models pthCnd(\tau'')$.

We now prove our claim that $\ell = \ell'''$. There are two cases:

$a(x) = 0$: Then, $\ell = a(\mathbf{pc}) + 1$. Therefore, $\ell'' = \ell'$. From this and p's well-formedness, it follows that $\ell'' \neq sa(\mathbf{pc}) + 1$ (since we consider only μAsm programs such that $p(\ell) = \mathbf{beqz}\ x, \ell'$ and $\ell' \neq \ell + 1$). Hence, $\ell''' = sa(\mathbf{pc}) + 1$. From this and $sa(\mathbf{pc}) = a(\mathbf{pc})$, we have that $\ell = \ell'''$.

$a(x) \neq 0$: Then, $\ell = \ell'$. Therefore, $\ell'' = a(\mathbf{pc}) + 1$. From this and p's well-formedness, $\ell''' = \ell$. Hence, $\ell = \ell'''$.

Rule Am-Rollback. Assume that $\langle ctr, \langle m, a\rangle, s\rangle \overset{p}{\Longrightarrow} O_n\tau\langle ctr', \langle m', a'\rangle, s'\rangle$ has been derived using the Am-Rollback rule in the concrete semantics. Then, $s = s_B \cdot \langle id, 0, \ell, \langle m'', a''\rangle\rangle$, $\tau = \texttt{rlb}\ id \cdot \texttt{pc}\ a'(\mathbf{pc})$, $\langle m'', a''\rangle \xrightarrow{\tau''} \langle m''', a'''\rangle$, $ctr' = ctr$, $m' = m'''$, $a' = a'''$, and $s' = s_B$. From $\mu(ss) = s$ and $s = s_B \cdot \langle id, 0, \ell, \langle m'', a''\rangle\rangle$, it follows that $ss = ss_B \cdot \langle id, 0, \ell, \langle sm'', sa''\rangle\rangle$ and $\mu(sa'') = a''$ and $\mu(sm'') = m''$. Since $\mu(sa'') = a''$ and $\mu(sm'') = m''$, we can apply Lemma 4 to $\langle m'', a'' \rangle \xrightarrow{\tau''} \langle m''', a''' \rangle$. We, therefore, obtain that there are sm''', sa''', τ''' such that $\langle sm'', sa'' \rangle \xrightarrow{\tau'}_s \langle sm''', sa''' \rangle$, $\mu(sm''') = m'''$, $\mu(sa''') = a'''$, $\mu(\tau''') = \tau''$, and $\mu \models pthCnd(\tau''')$. We claim that $sa'''(\mathbf{pc}) \neq \ell$. Hence, we can apply the Am-Rollback rule in the symbolic semantics to $\langle ctr, \langle sm, sa \rangle, ss \rangle$. Thus, $\langle ctr, \langle sm, sa \rangle, ss \rangle \xRightarrow{\tau'}_s \langle ctr'', \langle sm', sa' \rangle, ss' \rangle$, where $ctr'' = ctr$, $sm' = sm'''$, $sa' = sa'''$, and $ss' = ss_B$. From $ctr'' = ctr$ and $ctr' = ctr$, we have $ctr' = ctr''$. From $\mu(sa''') = a'''$, $a' = a'''$, and $sa' = sa'''$, we have $\mu(sa') = a'$. From $\mu(sm''') = m'''$, $m' = m'''$, and $sm' = sm'''$, we have $\mu(sm') = m'$. From $\tau = \texttt{rlb}\ id \cdot \texttt{pc}\ a'(\mathbf{pc})$ and $\tau' = \texttt{rlb}\ id \cdot \texttt{pc}\ sa'(\mathbf{pc})$, we have $\mu(\tau') = \tau$ and $\mu \models pthCnd(\tau')$. Finally, from $s' = s_B$ and $ss' = ss_B$, we have $\mu(ss') = \mu(ss_B) = s_B$ (thanks to $\mu(ss) = s$) and $\mu \models pthCnd(ss')$ (thanks to $\mu \models pthCnd(ss)$).

We now prove our claim that $sa'''(\mathbf{pc}) \neq \ell$. From $s = s_B \cdot \langle id, 0, \ell, \langle m'', a'' \rangle \rangle$, $\langle m'', a'' \rangle \xrightarrow{\tau''} \langle m''', a''' \rangle$, and $wf(s)$, we immediately have that $a'''(\mathbf{pc}) \neq \ell$. From this and $sa'''(\mathbf{pc}) = a'''(\mathbf{pc})$, we have $sa'''(\mathbf{pc}) \neq \ell$.

This completes the proof of our claim. □

G.4 B: Relating speculative and always mispredict semantics

Below, we provide the proof of Theorem 5, which we restate here for simplicity:

Theorem 5 (B: SNI of Oralce and AM). *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 $((p, \sigma)) \text{👻}_{NS} \overline{\tau}$, $((p, \sigma')) \text{👻}_{NS} \overline{\tau}$, then $((p, \sigma)) \text{👻}^{\omega}_{B} \overline{\tau}''$, $((p, \sigma')) \text{👻}^{\omega}_{B} \overline{\tau}''$*

Proof. Let p be a program, P be a policy, and $w \in \mathbb{N}$ be a speculative window. We prove the two directions separately.

($\Rightarrow$). Assume that p satisfies SNI for P and all prediction oracles O with speculative window at most w. Then, for all O with speculative window at most w, for all initial configurations $\sigma, \sigma' \in InitConf$, if $\sigma \sim_P \sigma'$ and $(\!|p|\!)(\sigma) = (\!|p|\!)(\sigma')$, then $[\![p]\!]_O(\sigma) = [\![p]\!]_O(\sigma')$. From this and Proposition 6 (proved below), we have that for all initial configurations $\sigma, \sigma' \in InitConf$, if $\sigma \sim_P \sigma'$ and $(\!|p|\!)(\sigma) = (\!|p|\!)(\sigma')$, then $\{\!|p|\!\}_w(\sigma) = \{\!|p|\!\}_w(\sigma')$.

($\Leftarrow$). Assume that p is such that for all initial configurations $\sigma, \sigma' \in InitConf$, if $\sigma \sim_P \sigma'$ and $(\!|p|\!)(\sigma) = (\!|p|\!)(\sigma')$, then $\{\!|p|\!\}_w(\sigma) = \{\!|p|\!\}_w(\sigma')$. Let O be an arbitrary prediction oracle with speculative window at most w. From Proposition 6 (proved below), we have that for all initial configurations $\sigma, \sigma' \in InitConf$, if $\sigma \sim_P \sigma'$ and $(\!|p|\!)(\sigma) = (\!|p|\!)(\sigma')$, then $[\![p]\!]_O(\sigma) = [\![p]\!]_O(\sigma')$. Therefore, p satisfies SNI w.r.t. P and O. Since O is an arbitrary predictor with speculation window at most w, then p satisfies SNI for P and all prediction oracles O with speculative window at most w. □

The proof of Theorem 5 depends on Proposition 6, which we restate here for simplicity:

Proposition 6. *Let p be a program, $w \in \mathbb{N}$ be a speculative window, and $\sigma, \sigma' \in InitConf$ be initial configurations. $\{\!|p|\!\}_w(\sigma) = \{\!|p|\!\}_w(\sigma')$ iff $[\![p]\!]_O(\sigma) = [\![p]\!]_O(\sigma')$ for all prediction oracles O with speculative window at most w.*

Proof. The proposition follows immediately from Proposition 7 (proved in Appendix G.4.2) and Proposition 8 (proved in Appendix G.4.3). □

G.4.1 Auxiliary definitions. Before proving Proposition 7 and Proposition 8, we introduce some auxiliary definitions.

pc-*similar configurations.* Two configurations $\sigma, \sigma' \in Conf$ are **pc**-*similar*, written $\sigma \sim_{\mathbf{pc}} \sigma'$, iff $\sigma(\mathbf{pc}) = \sigma'(\mathbf{pc})$.

Next-step agreeing configurations. Two configurations $\sigma, \sigma' \in \mathit{Conf}$ are *next-step agreeing*, written $\sigma \sim_{next} \sigma'$, iff there are $\sigma_1, \sigma'_1 \in \mathit{Conf}$ such that $\sigma \xrightarrow{\tau} \sigma_1$, $\sigma' \xrightarrow{\tau} \sigma'_1$, and $\sigma_1 \sim_{\mathbf{pc}} \sigma'_1$.

Similar extended configurations. Two speculative states $\langle \sigma, id, w, \ell \rangle$ and $\langle \sigma', id', w', \ell' \rangle$ in *SpecS* are *similar*, written $\langle \sigma, id, w, \ell \rangle \cong \langle \sigma', id', w', \ell' \rangle$, iff $id = id'$, $w = w'$, $\ell = \ell'$, $\sigma \sim_{\mathbf{pc}} \sigma'$, and $\sigma \sim_{next} \sigma'$.

Two sequences of speculative states s and s' in SpecS^* are *similar*, written $s \cong s'$, iff all their speculative states are similar. Formally, $\varepsilon \cong \varepsilon$ and $s \cdot \langle \sigma, id, w, \ell \rangle \cong s' \cdot \langle \sigma', id', w', \ell' \rangle$ iff $s \cong s'$ and $\langle \sigma, id, w, \ell \rangle \cong \langle \sigma', id', w', \ell' \rangle$.

Two extended configurations $\langle ctr, \sigma, s \rangle, \langle ctr', \sigma', s' \rangle$ are *similar*, written $\langle ctr, \sigma, s \rangle \cong \langle ctr', \sigma', s' \rangle$, iff $ctr = ctr'$, $\sigma \sim_{\mathbf{pc}} \sigma'$, and $s \cong s'$. Similarly, $\langle ctr, \sigma, s, h \rangle \cong \langle ctr', \sigma', s', h' \rangle$ iff $ctr = ctr'$, $\sigma \sim_{\mathbf{pc}} \sigma'$, $s \cong s'$, and $h = h'$.

Commit-free projection. The commit-free projection of a sequence of speculative state $s \in \mathit{SpecS}^*$, written $s\upharpoonright_{com}$, is as follows: $\varepsilon\upharpoonright_{com} = \varepsilon$, $s \cdot \langle \sigma, id, w, \ell \rangle\upharpoonright_{com} = s\upharpoonright_{com} \cdot \langle \sigma, id, w, \ell \rangle$ if $\sigma \xrightarrow{\tau} \sigma'$ and $\sigma'(\mathbf{pc}) \neq \ell$, and $s \cdot \langle \sigma, id, w, \ell \rangle\upharpoonright_{com} = s\upharpoonright_{com}$ if $\sigma \xrightarrow{\tau} \sigma'$ and $\sigma'(\mathbf{pc}) = \ell$.

Mirrored configurations. Two speculative states $\langle \sigma, id, w, \ell \rangle$ and $\langle \sigma, id', w', \ell' \rangle$ in *SpecS* are *mirrors* if $\sigma = \sigma'$ and $\ell = \ell'$. Two sequences of speculative states s and s' in SpecS^* are *mirrors*, written $s||s'$, if $|s| = |s'|$ and their speculative states are pairwise mirrors. Finally, $\langle ctr, \sigma, s \rangle || \langle ctr', \sigma', s', h' \rangle$ iff $\sigma = \sigma'$ and $s||s'\upharpoonright_{com}$.

Auxiliary functions for handling transactions' lenghts. The $wndw(\cdot) : \mathit{SpecS}^* \to \mathbb{N} \cup \{\infty\}$ function is defined as follows: $wndw(\varepsilon) = \infty$ and $wndw(s \cdot \langle ctr, w, n, \sigma \rangle) = w$. The $minWndw(\cdot) : \mathit{SpecS}^* \to \mathbb{N} \cup \{\infty\}$ function is defined as follows: $minWndw(\varepsilon) = \infty$ and $minWndw(s \cdot \langle ctr, w, n, \sigma \rangle) = min(w, minWndw(s))$.

Invariants. We denote by $INV(s, s')$, where $s, s' \in \mathit{SpecS}^*$, the fact that $|s| = |s'|$ and for all $1 \leq i \leq |s|$, $minWndw(s'^i) \leq wndw(s^i)$, where s^i denotes the prefix of s of length i. Additionally, $INV(\langle ctr, \sigma, s \rangle, \langle ctr', \sigma', s', h' \rangle)$, where $\langle ctr, \sigma, s \rangle$ is an extended configuration for the always mispredict semantics whereas $\langle ctr', \sigma', s', h' \rangle$ is an extended configuration for the speculative semantics, holds iff $INV(s, s'\upharpoonright_{com})$ does.

We denote by $INV2(s, s')$, where $s, s' \in \mathit{SpecS}^*$, the fact that $|s| = |s'|$ and for all $1 \leq i \leq |s|$, $minWndw(s'^i) = wndw(s^i)$, where s^i denotes the prefix of s of length i. Moreover, $INV2(\langle ctr, \sigma, s \rangle, \langle ctr', \sigma', s', h' \rangle)$, where $\langle ctr, \sigma, s \rangle$ is an extended configuration for the always mispredict semantics whereas $\langle ctr', \sigma', s', h' \rangle$ is an extended configuration for the speculative semantics, holds iff $INV2(s, s'\upharpoonright_{com})$ does.

Notation for runs and traces. For simplicity, we restate here the definitions of $\{\!|p|\!\}_w(\sigma)$ and $[\![p]\!]_{\mathcal{O}}(\sigma)$. Let p be a program, $w \in \mathbb{N}$ be a speculative window, $\mathcal{O}$ be a prediction oracle, and $\sigma \in \mathit{InitConf}$ be an initial configuration. Then, $\{\!|p|\!\}_w(\sigma)$ denotes the trace $\tau \in \mathit{ExtObs}^*$ such that there is a final configuration $\sigma' \in \mathit{FinalConf}$ such that $\langle \sigma, \tau, \sigma' \rangle \in \{\!|p|\!\}_w$, whereas $[\![p]\!]_w(\sigma)$ denotes the trace $\tau \in \mathit{ExtObs}^*$ such that there is a final configuration $\sigma' \in \mathit{FinalConf}$ such that $\langle \sigma, \tau, \sigma' \rangle \in [\![p]\!]_{\mathcal{O}}$. If there is no such τ, then we write $\{\!|p|\!\}_w(\sigma) = \bot$ (respectively $[\![p]\!]_w(\sigma) = \bot$).

G.4.2 Soundness. In Proposition 7 , we prove the soundness of the always mispredict semantics w.r.t. the speculative semantics.

Proposition 7. *Let p be a program, $w \in \mathbb{N}$ be a speculative window, and $\sigma, \sigma' \in \mathit{InitConf}$ be two initial configurations. If $\{\!|p|\!\}_w(\sigma) = \{\!|p|\!\}_w(\sigma')$, then $[\![p]\!]_{\mathcal{O}}(\sigma) = [\![p]\!]_{\mathcal{O}}(\sigma')$ for all prediction oracle $\mathcal{O}$ with speculation window at most w.*

Proof. Let $w \in \mathbb{N}$ be a speculative window and $\sigma, \sigma' \in \mathit{InitConf}$ be two initial configurations such that $\{\!|p|\!\}_w(\sigma) = \{\!|p|\!\}_w(\sigma')$. Moreover, let O be an arbitrary prediction oracle with speculative window at most w. If $\{\!|p|\!\}_w(\sigma) = \bot$, then the computation does not terminate in σ and σ'. Since speculation does not introduce non-termination, the computation does not terminate according to $\rightsquigarrow$ as well. Hence, $[\![p]\!]_O(\sigma) = [\![p]\!]_O(\sigma') = \bot$. If $\{\!|p|\!\}_w(\sigma) \neq \bot$, then we can obtain the runs for $\rightsquigarrow$ by repeatedly applying Appendix G.4.2 (proved below) to the runs corresponding to $\{\!|p|\!\}_w(\sigma)$ and $\{\!|p|\!\}_w(\sigma')$. Observe that we can apply the Appendix G.4.2 because (I) $\{\!|p|\!\}_w(\sigma) = \{\!|p|\!\}_w(\sigma')$, (II) $\{\!|p|\!\}_w(\sigma) \neq \bot$, (III) the initial configurations $\langle 0, \sigma, \varepsilon\rangle$, $\langle 0, \sigma', \varepsilon\rangle$, $\langle 0, \sigma, \varepsilon, \varepsilon\rangle$, $\langle 0, \sigma', \varepsilon, \varepsilon\rangle$ trivially satisfy conditions (1)–(4), and (IV) the application of Appendix G.4.2 preserves (1)–(4). From the point (g) in Appendix G.4.2, we immediately have that the runs have the same traces. Hence, $[\![p]\!]_O(\sigma) = [\![p]\!]_O(\sigma')$. □

We now prove Appendix G.4.2.

Let p be a program, $w \in \mathbb{N}$ be a speculative window, O be a prediction oracle with speculative window at most w, am_0, am'_0 be two extended speculative configurations for the always mispredict semantics, and sp_0, sp'_0 be two extended speculative configurations for the speculative semantics.

If the following conditions hold:

(1) $am_0 \cong am'_0$,
(2) $sp_0 \cong sp'_0$,
(3) $am_0 || sp_0 \wedge am'_0 || sp'_0$,
(4) $INV(am_0, sp_0) \wedge INV(am'_0, sp'_0)$,
(5) $\{\!|p|\!\}_w(am_0) \neq \bot$,
(6) $\{\!|p|\!\}_w(am_0) = \{\!|p|\!\}_w(am'_0)$,

then there are configurations am_1, am'_1 (for the always mispredict semantics), sp_1, sp'_1 (for the speculative semantics), and $n \in \mathbb{N}$ such that:

(a) $am_0 \overset{\tau_0}{\Longrightarrow}{}^n\ am_1 \wedge am'_0 \overset{\tau_0}{\Longrightarrow}{}^n\ am'_1$,
(b) $sp_0 \overset{\tau}{\rightsquigarrow} sp_1 \wedge sp'_0 \overset{\tau'}{\rightsquigarrow} sp'_1$,
(c) $am_1 \cong am'_1$,
(d) $sp_1 \cong sp'_1$,
(e) $am_1 || sp_1 \wedge am'_1 || sp'_1$,
(f) $INV(am_1, sp_1) \wedge INV(am'_1, sp'_1)$, and
(g) $\tau = \tau'$.

Proof. Let p be a program, $w \in \mathbb{N}$ be a speculative window, O be a prediction oracle with speculative window at most w, am_0, am'_0 be two extended speculative configurations for the "always mispredict" semantics, and sp_0, sp'_0 be two extended speculative configurations for the speculative semantics.

In the following, we use a dot notation to refer to the components of the extended configurations. For instance, we write $am_0.\sigma$ to denote the configuration σ in am_0. We also implicitly lift functions like $minWndw(\cdot)$ and $wndw(\cdot)$ to extended configurations.

Assume that (1)–(6) hold. Observe that, from (2), it follows $minWndw(sp_0) = minWndw(sp'_0)$. We proceed by case distinction on $minWndw(sp_0)$:

$minWndw(sp_0) > 0$: From $minWndw(sp_0) > 0$, (1), (2), and (4), we also get that $wndw(am_0) > 0$ and $wndw(am'_0) > 0$ (this follows from $sp_0.s = sp_0.s^{|sp_0.s|}$ and (4)). From $minWndw(sp_0) > 0$ and (2), it follows that $enabled(sp_0)$ and $enabled(sp'_0)$ hold. Additionally, from $wndw(am_0) > 0$ and (1), we also get $enabled'(am_0)$ and $enabled'(am_1)$.

That is, we can apply only the rules Se-NoBranch and Se-Branch according to both semantics. Observe that $sp_0.\sigma(\mathbf{pc}) = sp'_0.\sigma(\mathbf{pc})$ (from (2)) and $am_0.\sigma(\mathbf{pc}) = am'_0.\sigma(\mathbf{pc})$ (from (1)). Moreover, $am_0.\sigma(\mathbf{pc}) = sp_0.\sigma(\mathbf{pc})$ and $am'_0.\sigma(\mathbf{pc}) = sp'_0.\sigma(\mathbf{pc})$ (from (3)). Hence, the program counters in the four states point to the same instructions. There are two cases:

$p(sp_0.\sigma(\mathbf{pc}))$ **is a branch instruction beqz** x, n: Observe that $O(sp_0.\sigma, p, sp_0.h) = O(sp'_0.\sigma, p, sp'_0.h)$ since $am_0.\sigma(\mathbf{pc}) = sp_0.\sigma(\mathbf{pc})$, $sp_0.h = sp'_0.h$ (from (2)), and O is a prediction oracle. Let $\langle m, w'\rangle$ be the corresponding prediction.

There are two cases:

$\langle \ell', w'\rangle$ **is a correct prediction w.r.t.** sp_0: We first show that $\langle \ell', w'\rangle$ is a correct prediction w.r.t. sp'_0 as well. From (6), we know that the trace produced starting from am_0 and am'_0 are the same. From this, $am_0.\sigma(\mathbf{pc}) = sp_0.\sigma(\mathbf{pc})$, and $p(sp_0.\sigma(\mathbf{pc}))$ is a branch instruction, we have that the always mispredict semantics modifies the program counter **pc** in the same way in am_0 and am'_0 when applying the Se-Branch in$\Longrightarrow$. Hence, $am_0.\sigma(x) = am'_0.\sigma(x)$. From this and (3), we also have $sp_0.\sigma(x) = sp'_0.\sigma(x)$. Thus, $\langle \ell', w'\rangle$ is a correct prediction w.r.t. sp'_0 as well.

According to the always mispredict semantics, there are k, k' such that:

$$r := am_0 \xRightarrow{\texttt{start}\ am_0.ctr\cdot\texttt{pc}\ \ell_0} am_2 \xRightarrow{v}{}^{k}\ am_3 \xRightarrow{\texttt{rlb}\ am_0.ctr\cdot\texttt{pc}\ \ell_1} am_1$$
$$r' := am'_0 \xRightarrow{\texttt{start}\ am'_0.ctr\cdot\texttt{pc}\ \ell'_0} am'_2 \xRightarrow{v'}{}^{k'}\ am'_3 \xRightarrow{\texttt{rlb}\ am'_0.ctr\cdot\texttt{pc}\ \ell'_1} am'_1$$

From (1) and (6), we immediately have that $am_0.ctr = am'_0.ctr$, $\ell_0 = \ell'_0$, $k = k'$, $v = v'$, and $\ell_1 = \ell'_1$. Moreover, since $\langle \ell', w'\rangle$ is a correct prediction we also have that $\ell_1 = \ell'$ and $\ell'_1 = \ell'$. Hence, we pick n to be $k + 2$.

Additionally, by applying the rule Se-Branch once in $\rightsquigarrow$ we also get $sp_0 \overset{\tau}{\rightsquigarrow} sp_1$ and $sp'_0 \overset{\tau'}{\rightsquigarrow} sp'_1$.

We have already shown that (a) and (b) hold. We now show that (c)–(g) hold as well.

(c): To show that $am_1 \cong am'_1$, we need to show $am_1.ctr = am'_1.ctr$, $am_1.\sigma \sim_{\mathbf{pc}} am'_1.\sigma$, and $am_1.s \cong am'_1.s$. First, $am_1.ctr = am'_1.ctr$ immediately follows from $v = v'$ and (1) (that is, $am_0.ctr = am'_0.ctr$ and during the mispredicted branch we created the same transactions in both runs). Second, $am_1.\sigma \sim_{\mathbf{pc}} am'_1.\sigma$ follows from $\ell_1 = \ell'_1$ (since $am_1.\sigma = am_0.\sigma[\mathbf{pc} \mapsto \ell_1]$ and $am'_1.\sigma = am'_0.\sigma[\mathbf{pc} \mapsto \ell'_1]$). Finally, $am_1.s \cong am'_1.s$ immediately follows from $am_1.s = am_0.s$, $am'_1.s = am_0.s$, and (1).

(d): To show that $sp_1 \cong sp'_1$, we need to show $sp_1.ctr = sp'_1.ctr$, $sp_1.\sigma \sim_{\mathbf{pc}} sp'_1.\sigma$, $sp_1.s \cong sp'_1.s$, and $sp_1.h = sp'_1.h$. First, $sp_1.ctr = sp'_1.ctr$ immediately follows from $sp_1.ctr = sp_0.ctr + 1$, $sp'_1.ctr = sp'_0.ctr + 1$, and (2). Second, $sp_1.\sigma \sim_{\mathbf{pc}} sp'_1.\sigma$ follows from (2) and $O(sp_0.\sigma, p, sp_0.h) = O(sp'_0.\sigma, p, sp'_0.h)$ (so the program counter is updated in the same way in both configurations). Third, $sp_1.s \cong sp'_1.s$ follows from (2), $sp_1.s$ being $decr(sp_0.s) \cdot \langle sp_0.\sigma, sp_0.ctr, w', \ell'\rangle$, $sp'_1.s$ being $decr(sp'_0.s) \cdot \langle sp'_0.\sigma, sp'_0.ctr, w', \ell'\rangle$, $sp_0.ctr = sp'_0.ctr$ (from (2)), $sp_0.\sigma \sim_{\mathbf{pc}} sp'_0.\sigma$ (from (2)), and $sp_0.\sigma \sim_{next} sp'_0.\sigma$ (we proved above that $sp_0.\sigma(x) = sp'_0.\sigma(x)$; from this, it follows that the outcome of the branch instruction w.r.t. the non-speculative semantics is the same). Finally, $sp_1.h = sp'_1.h$ immediately follows from (2), $sp_1.h = sp_0.h \cdot \langle sp_0.\sigma(\mathbf{pc}), sp_0.ctr, \ell'\rangle$, $sp'_1.,h = sp'_0.h \cdot \langle sp'_0.\sigma(\mathbf{pc}), sp'_0.ctr, \ell'\rangle$, $sp_0.ctr = sp'_0.ctr$ (from (2)), and $sp_0.\sigma(\mathbf{pc}) = sp'_0.\sigma(\mathbf{pc})$ (from (2)).

(e): We show only $am_1||sp_1$ (the proof for $am_1'||sp_1'$ is similar). To show $am_1||sp_1$, we need to show $am_1.\sigma = sp_1.\sigma$ and $am_1.s||sp_1.s\upharpoonright_{com}$. From the Se-Branch rule in $\rightsquigarrow$, we have that $sp_1.\sigma = sp_0.\sigma[\mathbf{pc} \mapsto \ell']$. The last step in r is obtained by applying the rule Se-Rollback in$\Longrightarrow$. From this rule, $am_1.\sigma$ is the configuration obtained by executing one step of the non-speculative semantics starting from $am_0.\sigma$. From (3), we have that $am_0.\sigma = sp_0.\sigma$. Moreover, since $\langle \ell', w' \rangle$ is a correct prediction for sp_0, we have that $am_1.\sigma = am_0.\sigma[\mathbf{pc} \mapsto \ell']$. Hence, $am_1.\sigma = sp_1.\sigma$.

We now show that $am_1.s||sp_1.s\upharpoonright_{com}$. From the Se-Branch rule in $\rightsquigarrow$, we have that $sp_1.s = decr(sp_0.s)\cdot\langle sp_0.\sigma, sp_0.ctr, w', \ell' \rangle$. Since $\langle \ell', w' \rangle$ is a correct prediction for sp_0, however, $sp_1.s\upharpoonright_{com} = decr(sp_0.s)\upharpoonright_{com} = decr(sp_0.s\upharpoonright_{com})$. Moreover, from r, it follows that $am_1.s = am_0.s$. Hence, $am_1.s||sp_1.s\upharpoonright_{com}$ follows from (3), $am_1.s = am_0.s$, and $sp_1.s\upharpoonright_{com} = decr(sp_0.s)\upharpoonright_{com}$.

(f): Here we prove that $INV(am_1, sp_1)$ holds. $INV(am_1', sp_1')$ can be proved in a similar way. To show $INV(am_1, sp_1)$, we need to show that $|am_1.s| = |sp_1.s\upharpoonright_{com}|$ and for all $i \leq i \leq |am_1.s|$, $minWndw(sp_1.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$.

We first prove $|am_1.s| = |sp_1.s\upharpoonright_{com}|$. From (4), we have $|am_0.s| = |sp_0.s\upharpoonright_{com}|$. From the run r, we have that $am_1.s = am_0.s$ and, therefore, $|am_1.s| = |am_0.s|$. From the Se-Branch rule in $\rightsquigarrow$, we have that $sp_1.s = decr(sp_0.s) \cdot \langle sp_0.\sigma, sp_0.ctr, w', \ell' \rangle$. Since $\langle \ell', w' \rangle$ is a correct prediction for sp_0, we have that $sp_1.s\upharpoonright_{com} = decr(sp_0.s)\upharpoonright_{com}$. Hence, $|sp_1.s\upharpoonright_{com}| = |sp_0.s\upharpoonright_{com}|$. From $|am_0.s| = |sp_0.s\upharpoonright_{com}|$, $|sp_1.s\upharpoonright_{com}| = |sp_0.s\upharpoonright_{com}|$, and $|am_1.s| = |am_0.s|$, we therefore have that $|am_1.s| = |sp_1.s\upharpoonright_{com}|$.

We now show that for all $1 \leq i \leq |am_1.s|$, $minWndw(sp_1.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$. Observe that $am_1.s = am_0.s$ and $sp_1.s = decr(sp_0.s) \cdot \langle sp_0.\sigma, sp_0.ctr, w', \ell' \rangle$. Since $\langle \ell', w' \rangle$ is a correct prediction for sp_0, we have that $sp_1.s\upharpoonright_{com} = decr(sp_0.s)\upharpoonright_{com}$. Let i be an arbitrary value such that $1 \leq i \leq |am_1.s|$. Then, $wndw(am_1.s^i) = wndw(am_0.s^i)$ and $minWndw(sp_1.s\upharpoonright_{com}{}^i) = minWndw(decr(sp_0.s)\upharpoonright_{com}{}^i)$. From (4), we have that $minWndw(sp_0.s\upharpoonright_{com}{}^i) \leq wndw(am_0.s^i)$. From this and $wndw(am_1.s^i) = wndw(am_0.s^i)$, we get $minWndw(sp_0.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$. From the definition of $decr(\cdot)$, we also have $minWndw(decr(sp_0.s)\upharpoonright_{com}{}^i) \leq minWndw(sp_0.s\upharpoonright_{com}{}^i)$. From this and $minWndw(sp_0.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$, we have $minWndw(decr(sp_0.s)\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$. Hence, $minWndw(sp_1.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$ for all $1 \leq i \leq |am_1.s|$ (since we have proved it for an arbitrary i).

(g): The observations are $\tau = \texttt{start}\ sp_0.ctr \cdot \texttt{pc}\ \ell'$ and $\tau = \texttt{start}\ sp_0'.ctr \cdot \texttt{pc}\ \ell'$. From this, $O(sp_0.\sigma, p, sp_0.h) = O(sp_0'.\sigma, p, sp_0'.h)$, and $sp_0.ctr = sp_0'.ctr$ (from (2)), we get $\tau = \tau'$.

This completes the proof of this case.

$\langle \ell', w' \rangle$ **is a misprediction w.r.t.** sp_0: We first show that $\langle \ell', w' \rangle$ is a misprediction w.r.t. sp_0' as well. From (6), we know that the trace produced starting from am_0 and am_0' are the same. From this, $am_0.\sigma(\mathbf{pc}) = sp_0.\sigma(\mathbf{pc})$, and $p(sp_0.\sigma(\mathbf{pc}))$ is a branch instruction, we have that the always mispredict semantics modifies the program counter $\mathbf{pc}$ in the same way in am_0 and am_0' when applying the Se-Branch in$\Longrightarrow$. Hence, $am_0.\sigma(x) = am_0'.\sigma(x)$. From this and (3), we also have $sp_0.\sigma(x) = sp_0'.\sigma(x)$. Thus, $\langle \ell', w' \rangle$ is a misprediction w.r.t. sp_0' as well.

Let $n = 1$. We obtain $am_0 \overset{\tau_0}{\Longrightarrow}{}^{n}\ am_1$ and $am'_0 \overset{\tau'_0}{\Longrightarrow}{}^{n}\ am'_1$ by applying once the rule Se-Branch in $\Longrightarrow$. From (5) and (6), we have that $\tau_0 = \tau'_0$. Moreover, by applying the rule Se-Branch once in $\rightsquigarrow$ we also get $sp_0 \overset{\tau}{\rightsquigarrow} sp_1$ and $sp'_0 \overset{\tau'}{\rightsquigarrow} sp'_1$.

We have already shown that (a) and (b) hold. We now show that (c)–(g) hold as well.

(c): To show that $am_1 \cong am'_1$, we need to show $am_1.ctr = am'_1.ctr$, $am_1.\sigma \sim_{\mathbf{pc}} am'_1.\sigma$, and $am_1.s \cong am'_1.s$. First, $am_1.ctr = am'_1.ctr$ immediately follows from $am_0.ctr + 1 = am_1.ctr$, $am'_0.ctr + 1 = am'_1.ctr$, and (1). Second, $am_1.\sigma \sim_{\mathbf{pc}} am'_1.\sigma$ follows from $\tau_0 = \tau'_0$ (i.e., the program counter is modified in the same ways in both runs). Finally, to show that $am_1.s \cong am'_1.s$, we need to show that $am_0.ctr = am'_0.ctr$, $min(w, wndw(am_0.s) - 1) = min(w, wndw(am'_0.s) - 1)$, $n_0 = n'_0$, $am_0.\sigma \sim_{\mathbf{pc}} am'_0.\sigma$, and $am_0.\sigma \sim_{next} am'_0.\sigma$ (since $am_1.s = am_0.s \cdot \langle am_0.\sigma, am_0.ctr, min(w, wndw(am_0.s) - 1), n_0\rangle$ and $am'_1.s = am'_0.s \cdot \langle am'_0.\sigma, am'_0.ctr, min(w, wndw(am'_0.s) - 1), n'_0\rangle$). Observe that $am_0.ctr = am'_0.ctr$ follows from (1), $min(w, wndw(am_0.s) - 1) = min(w, wndw(am'_0.s) - 1)$ also follow from (1), $n_0 = n'_0$ follows from $\tau_0 = \tau'_0$ (which indicates that $\mathbf{pc}$ is modified in a similar way), $am_0.\sigma \sim_{\mathbf{pc}} am'_0.\sigma$ follows from (1), and $am_0.\sigma \sim_{next} am'_0.\sigma$ follows from $\tau_0 = \tau'_0$ (i.e., since we mispredict in the same direct, then the outcome of the branch instruction must be the same according to the non-speculative semantics).

(d): To show that $sp_1 \cong sp'_1$, we need to show $sp_1.ctr = sp'_1.ctr$, $sp_1.\sigma \sim_{\mathbf{pc}} sp'_1.\sigma$, $sp_1.s \cong sp'_1.s$, and $sp_1.h = sp'_1.h$. First, $sp_1.ctr = sp'_1.ctr$ immediately follows from $sp_1.ctr = sp_0.ctr + 1$, $sp'_1.ctr = sp'_0.ctr + 1$, and (2). Second, $sp_1.\sigma \sim_{\mathbf{pc}} sp'_1.\sigma$ follows from (2) and $O(sp_0.\sigma, p, sp_0.h) = O(sp'_0.\sigma, p, sp'_0.h)$ (so the program counter is updated in the same way in both configurations). Third, $sp_1.s \cong sp'_1.s$ follows from (2), $sp_1.s$ being $decr(sp_0.s) \cdot \langle sp_0.\sigma, sp_0.ctr, w', \ell'\rangle$, $sp'_1.s$ being $decr(sp'_0.s) \cdot \langle sp'_0.\sigma, sp'_0.ctr, w', \ell'\rangle$, $sp_0.ctr = sp'_0.ctr$ (from (2)), $sp_0.\sigma \sim_{\mathbf{pc}} sp'_0.\sigma$ (from (2)), and $sp_0.\sigma \sim_{next} sp'_0.\sigma$ (we proved above that $sp_0.\sigma(x) = sp'_0.\sigma(x)$; from this, it follows that the outcome of the branch instruction w.r.t. the non-speculative semantics is the same). Finally, $sp_1.h = sp'_1.h$ immediately follows from (2), $sp_1.h = sp_0.h \cdot \langle sp_0.\sigma(\mathbf{pc}), sp_0.ctr, \ell'\rangle$, $sp'_1., h = sp'_0.h \cdot \langle sp'_0.\sigma(\mathbf{pc}), sp'_0.ctr, \ell'\rangle$, $sp_0.ctr = sp'_0.ctr$ (from (2)), and $sp_0.\sigma(\mathbf{pc}) = sp'_0.\sigma(\mathbf{pc})$ (from (2)).

(e): To show $am_1||sp_1 \wedge am'_1||sp'_1$, we need to show $am_1.\sigma = sp_1.\sigma$, $am'_1.\sigma = sp'_1.\sigma$, $am_1.s||sp_1.s\upharpoonright_{com}$, and $am'_1.s||sp'_1.s\upharpoonright_{com}$. In the following, we show only $am_1.\sigma = sp_1.\sigma$ and $am_1.s||sp_1.s\upharpoonright_{com}$ ($am'_1.\sigma = sp'_1.\sigma$ and $sp'_1.s\upharpoonright_{com}$ can be derived in the same way). The Se-Branch rule in both semantics only modify the program counter. From this and (3), for showing $am_1.\sigma = sp_1.\sigma$, it is enough to show $am_1.\sigma(\mathbf{pc}) = sp_1.\sigma(\mathbf{pc})$. From the Se-Branch rule in the speculative semantics $\rightsquigarrow$, we have that $sp_1.\sigma(\mathbf{pc}) = \ell'$. There are two cases:

$sp_0.\sigma(x) = 0$: From this and $\langle \ell', w'\rangle$ being a misprediction for sp_0, it follows that $\ell' = sp_0.\sigma(\mathbf{pc})+1$. Moreover, from $sp_0.\sigma(x) = 0$ and (3), we also have that $am_0.\sigma(x) = 0$. From this and the Se-Branch rule in $\Longrightarrow$, we have $am_1.\sigma(\mathbf{pc}) = am_0.\sigma(\mathbf{pc})+1$. Therefore, $am_1.\sigma(\mathbf{pc}) = sp_0.\sigma(\mathbf{pc})+1$ (because $am_0.\sigma(\mathbf{pc}) = sp_0.\sigma(\mathbf{pc})$ follows from (3)). Hence, $am_1.\sigma(\mathbf{pc}) = sp_1.\sigma(\mathbf{pc})$. Thus, $am_1.\sigma = sp_1.\sigma$.

$sp_0.\sigma(x) \neq 0$: From this and $\langle \ell', w'\rangle$ being a misprediction for sp_0, it follows that $\ell' = \ell$. Moreover, from $sp_0.\sigma(x) \neq 0$ and (3), we also have that $am_0.\sigma(x) \neq 0$. From this and the Se-Branch rule in $\Longrightarrow$, we have $am_1.\sigma(\mathbf{pc}) = \ell$. Hence, $am_1.\sigma(\mathbf{pc}) = sp_1.\sigma(\mathbf{pc})$. Thus, $am_1.\sigma = sp_1.\sigma$.

We still have to show that $am_1.s||sp_1.s\upharpoonright_{com}$. From the Se-Branch rule in$\Longrightarrow$, we have that $am_1.s = am_0.s \cdot \langle am_0.\sigma, am_0.ctr, min(w, wndw(am_0.s)-1), \ell' \rangle$ (note that the prediction is ℓ' as we showed above). In contrast, from the Se-Branch rule in $\rightsquigarrow$, we have that $sp_1.s = decr(sp_0.s) \cdot \langle sp_0.\sigma, sp_0.ctr, w', \ell' \rangle$. Since $\langle \ell', w' \rangle$ is a misprediction for sp_0, we have that $sp_1.s\upharpoonright_{com} = decr(sp_0.s)\upharpoonright_{com} \cdot \langle sp_0.\sigma, sp_0.ctr, w', \ell' \rangle$. Observe that $am_0.s||decr(sp_0.s)\upharpoonright_{com}$ immediately follows from (3). Hence, we just have to show that $\langle am_0.\sigma, am_0.ctr, min(w, wndw(am_0.s)-1), \ell' \rangle || \langle sp_0.\sigma, sp_0.ctr, w', \ell' \rangle$. Since the prediction is the same in both speculative states, this requires only to show that $am_0.\sigma = sp_0.\sigma$, which follows from (3).

(f): Here we prove that $INV(am_1, sp_1)$ holds. $INV(am_1', sp_1')$ can be proved in a similar way. To show $INV(am_1, sp_1)$, we need to show that $|am_1.s| = |sp_1.s\upharpoonright_{com}|$ and for all $i \leq i \leq |am_1.s|$, $minWndw(sp_1.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$.

We first prove $|am_1.s| = |sp_1.s\upharpoonright_{com}|$. From (4), we have $|am_0.s| = |sp_0.s\upharpoonright_{com}|$. From the Se-Branch rule in$\Longrightarrow$, we have that $am_1.s = am_0.s \cdot \langle am_0.\sigma, am_0.ctr, min(w, wndw(am_0.s)-1), \ell' \rangle$ (note that the prediction is ℓ' as we showed above). Hence, $|am_1.s| = |am_0.s| + 1$. From the Se-Branch rule in $\rightsquigarrow$, we have that $sp_1.s = decr(sp_0.s) \cdot \langle sp_0.\sigma, sp_0.ctr, w', \ell' \rangle$. Since $\langle \ell', w' \rangle$ is a misprediction for sp_0, we have that $sp_1.s\upharpoonright_{com} = decr(sp_0.s)\upharpoonright_{com} \cdot \langle sp_0.\sigma, sp_0.ctr, w', \ell' \rangle$. Hence, $|sp_1.s\upharpoonright_{com}| = |sp_0.s\upharpoonright_{com}| + 1$. From $|am_0.s| = |sp_0.s\upharpoonright_{com}|$, $|am_1.s| = |am_0.s| + 1$, and $|sp_1.s\upharpoonright_{com}| = |sp_0.s\upharpoonright_{com}| + 1$, we therefore have $|am_1.s| = |sp_1.s\upharpoonright_{com}|$.

We now show that for all $i \leq i \leq |am_1.s|$, $minWndw(sp_1.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$. Observe that $am_1.s = am_0.s \cdot \langle am_0.\sigma, am_0.ctr, min(w, wndw(am_0.s)-1), \ell' \rangle$ and $sp_1.s = decr(sp_0.s) \cdot \langle sp_0.\sigma, sp_0.ctr, w', \ell' \rangle$. Since $\langle \ell', w' \rangle$ is a misprediction for sp_0, we have that $sp_1.s\upharpoonright_{com} = decr(sp_0.s)\upharpoonright_{com} \cdot \langle sp_0.\sigma, sp_0.ctr, w', \ell' \rangle$. There are two cases:

$i = |am_1.s|$: From the Se-Branch rule in$\Longrightarrow$, we have that $wndw(am_1.s^i) = min(w, wndw(am_0.s)-1)$. From the Se-Branch rule in $\rightsquigarrow$, we also have that $minWndw(sp_1.s\upharpoonright_{com}{}^i) = min(minWndw(sp_0.s\upharpoonright_{com}{}^i)-1, w')$. Moreover, we have that (1) $w' \leq w$ (since O has speculative window at most w), and (2) $minWndw(sp_0.s\upharpoonright_{com}{}^i) - 1 \leq wndw(am_0.s) - 1$ (since we have $minWndw(sp_0.s\upharpoonright_{com}{}^i) \leq wndw(am_0.s)$ from (4) because $am_0.s = am_0.s^i$). As a result, we immediately have that $min(minWndw(sp_0.s\upharpoonright_{com}{}^i)-1, w') \leq min(w, wndw(am_0.s)-1)$. Hence, $minWndw(sp_1.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$.

$i < |am_1.s|$: We have $wndw(am_1.s^i) = wndw(am_0.s^i)$ (because $am_1.s^i = am_0.s^i$) and $minWndw(sp_1.s\upharpoonright_{com}{}^i) = minWndw(sp_0.s\upharpoonright_{com}{}^i) - 1$ (because $sp_1.s\upharpoonright_{com}{}^i = decr(sp_0.s\upharpoonright_{com}{}^i)$). From (4), we also have that $minWndw(sp_0.s\upharpoonright_{com}{}^i) \leq wndw(am_0.s^i)$. Therefore, $minWndw(sp_0.s\upharpoonright_{com}{}^i)-1 \leq wndw(am_0.s^i)$. From this, $wndw(am_1.s^i) = wndw(am_0.s^i)$, and $minWndw(sp_1.s\upharpoonright_{com}{}^i) = minWndw(sp_0.s\upharpoonright_{com}{}^i)-1$, we have $minWndw(sp_1.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$.

(g): The observations are $\tau = \texttt{start}\ sp_0.ctr \cdot \texttt{pc}\ \ell'$ and $\tau = \texttt{start}\ sp_0'.ctr \cdot \texttt{pc}\ \ell'$. From this, $O(sp_0.\sigma, p, sp_0.h) = O(sp_0'.\sigma, p, sp_0'.h)$, and $sp_0.ctr = sp_0'.ctr$ (from (2)), we get $\tau = \tau'$.

This completes the proof of this case.

This completes the proof of this case.

$p(sp_0.\sigma(\mathbf{pc}))$ **is not a branch instruction**: Let $n = 1$. We obtain $am_0 \overset{\tau_0}{\Longrightarrow}^n am_1$ and $am'_0 \overset{\tau'_0}{\Longrightarrow}^n am'_1$ by applying once the rule SE-NoBranch in $\Longrightarrow$. From (5) and (6), we have that $\tau_0 = \tau'_0$. Moreover, by applying the rule SE-NoBranch once in $\rightsquigarrow$ we also get $sp_0 \overset{\tau}{\rightsquigarrow} sp_1$ and $sp'_0 \overset{\tau'}{\rightsquigarrow} sp'_1$.

We have already shown that (a) and (b) hold. We now show that (c)–(g) hold as well.

(c): To show that $am_1 \cong am'_1$, we need to show $am_1.ctr = am'_1.ctr$, $am_1.\sigma \sim_{\mathbf{pc}} am'_1.\sigma$, and $am_1.s \cong am'_1.s$. First, $am_1.ctr = am'_1.ctr$ immediately follows from $am_0.ctr = am_1.ctr$, $am'_0.ctr = am'_1.ctr$, and (1). Second, $am_1.\sigma \sim_{\mathbf{pc}} am'_1.\sigma$ follows from (1) and the fact that $\rightarrow$ modifies the program counters in $am_0.\sigma$ and $am'_0.\sigma$ in the same way (if the current instruction is not a jump, both program counters are incremented by 1 and if the instruction is a jump, the target is the same since $\tau_0 = \tau'_0$). Finally, $am_1.s \cong am'_1.s$ follows from (1), $am_1.s$ being either $decr'(am_0.s)$ or $zeroes'(am_0.s)$ (depending on $am_0.\mathbf{pc}$), and $am'_1.s$ being either $decr'(am'_0.s)$ or $zeroes'(am'_0.s)$ (depending on $am'_0.\mathbf{pc}$).

(d): To show that $sp_1 \cong sp'_1$, we need to show $sp_1.ctr = sp'_1.ctr$, $sp_1.\sigma \sim_{\mathbf{pc}} sp'_1.\sigma$, $sp_1.s \cong sp'_1.s$, and $sp_1.h = sp'_1.h$. First, $sp_1.ctr = sp'_1.ctr$ immediately follows from $sp_0.ctr = sp_1.ctr$, $sp'_0.ctr = sp'_1.ctr$, and (2). Second, $sp_1.\sigma \sim_{\mathbf{pc}} sp'_1.\sigma$ follows from (2) and the fact that $\rightarrow$ modifies the program counters in $sp_0.\sigma$ and $sp'_0.\sigma$ in the same way (if the current instruction is not a jump, both program counters are incremented by 1 and if the instruction is a jump, the target is the same since $\tau = \tau'$, which we prove in (g) below). Third, $sp_1.s \cong sp'_1.s$ follows from (2), $sp_1.s$ being either $decr(sp_0.s)$ or $zeroes(sp_0.s)$ (depending on $sp_0.\mathbf{pc}$), and $sp'_1.s$ being either $decr(sp'_0.s)$ or $zeroes(sp'_0.s)$ (depending on $sp'_0.\mathbf{pc}$). Finally, $sp_1.h = sp'_1.h$ immediately follows from (2), $sp_1.h = sp_0.h$, and $sp'_1.h = sp'_0.h$.

(e): To show $am_1 || sp_1 \wedge am'_1 || sp'_1$, we need to show $am_1.\sigma = sp_1.\sigma$, $am'_1.\sigma = sp'_1.\sigma$, $am_1.s || sp_1.s\upharpoonright_{com}$, and $am'_1.s || sp'_1.s\upharpoonright_{com}$. From the SE-NoBranch, we have that $am_0.\sigma \xrightarrow{\tau_0} am_1.\sigma$, $am'_0.\sigma \xrightarrow{\tau'_0} am'_1.\sigma$, $sp_0.\sigma \xrightarrow{\tau} sp_1.\sigma$, $sp'_0.\sigma \xrightarrow{\tau'} sp'_1.\sigma$. From this and (3), we have that $am_1.\sigma = sp_1.\sigma$ and $am'_1.\sigma = sp'_1.\sigma$ (since $am_0.\sigma = sp_0.\sigma$, $am'_0.\sigma = sp'_0.\sigma$). Moreover, $am_1.s || sp_1.s\upharpoonright_{com}$, and $am'_1.s || sp'_1.s\upharpoonright_{com}$ immediately follow from (3), $sp_1.s$ being either $decr(sp_0.s)$ or $zeroes(sp_0.s)$ (depending on $sp_0.\mathbf{pc}$), and $sp'_1.s$ being either $decr(sp'_0.s)$ or $zeroes(sp'_0.s)$ (depending on $sp'_0.\mathbf{pc}$), which only modify the speculation windows.

(f): For simplicity, we show only $INV(am_1, sp_1)$, the proof for $INV(am'_1, sp'_1)$ is analogous. To show $INV(am_1, sp_1)$, we need to show that $|am_1.s| = |sp_1.s\upharpoonright_{com}|$ (which immediately follows from $INV(am_0, sp_0)$ and the fact that we do not add or remove speculative states) and for all $i \leq i \leq |am_1.s|$, $minWndw(sp_1.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$. There are two cases:

$i = |am_1.s|$: If the instruction is not **spbarr**, then $wndw(am_1.s^i) = wndw(am_0.s^i) - 1$ and $minWndw(sp_1.s\upharpoonright_{com}{}^i) = minWndw(sp_0.s\upharpoonright_{com}{}^i) - 1$. From (4), we also have that $minWndw(sp_0.s\upharpoonright_{com}{}^i) \leq wndw(am_0.s^i)$. Hence, $minWndw(sp_1.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$.

If the executed instruction is **spbarr**, then $wndw(am_1.s^i) = 0$ and $minWndw(sp_1.s\upharpoonright_{com}{}^i) = 0$. Therefore, $minWndw(sp_1.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$.

$i < |am_1.s|$: If the executed instruction is not **spbarr**, then $wndw(am_1.s^i) = wndw(am_0.s^i)$ (because $am_1.s^i = am_0.s^i$) and $minWndw(sp_1.s\upharpoonright_{com}{}^i) = minWndw(sp_0.s\upharpoonright_{com}{}^i) - 1$. From (4), we also have that $minWndw(sp_0.s\upharpoonright_{com}{}^i) \leq wndw(am_0.s^i)$. Therefore, $minWndw(sp_0.s\upharpoonright_{com}{}^i) - 1 \leq wndw(am_0.s^i)$. From this, $wndw(am_1.s^i) = wndw(am_0.s^i)$, and $minWndw(sp_1.s\upharpoonright_{com}{}^i) = minWndw(sp_0.s\upharpoonright_{com}{}^i) - 1$, we have $minWndw(sp_1.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$.

If the executed instruction is **spbarr**, then $wndw(am_1.s^i) = wndw(am_0.s^i)$ (because $am_1.s^i = am_0.s^i$) and $minWndw(sp_1.s\upharpoonright_{com}{}^i) = 0$. From this, we immediately have $minWndw(sp_1.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$.

(g): From (3), we have that $am_0.\sigma = sp_0.\sigma$ and $am'_0.\sigma = sp'_0.\sigma$. From the SE-NOBRANCH, we have that $am_0.\sigma \xrightarrow{\tau_0} am_1.\sigma$, $am'_0.\sigma \xrightarrow{\tau'_0} am'_1.\sigma$, $sp_0.\sigma \xrightarrow{\tau} sp_1.\sigma$, $sp'_0.\sigma \xrightarrow{\tau'} sp'_1.\sigma$. That is, $\tau_0 = \tau$ and $\tau'_0 = \tau'$. From this and $\tau_0 = \tau'_0$, we get $\tau = \tau'$.

This completes the proof of this case.

This completes the proof of this case.

$minWndw(sp_0) = 0$: Let i, i' be the largest values such that $minWndw(sp_0.s^i) > 0$ and $minWndw(sp'_0.s^{i'}) > 0$. We now show that $i = i'$. From (2), we have that $sp_0.s \cong sp'_0.s$ which means that the speculative states in $sp_0.s$ and $sp'_0.s$ are pairwise similar. As a result, the remaining speculative windows are pairwise the same. Hence, $minWndw(sp_0.s^i) = minWndw(sp'_0.s^{i'})$ for all $1 \leq i \leq |sp_0.s|$. Observe also that each pair of speculative states in $sp_0.s$ and $sp'_0.s$ results either in two commits or two rollbacks (again from (2)).

There are two cases:

We can apply the SE-COMMIT rule in sp_0: Hence, $sp_0.s = s_0 \cdot \langle \sigma_0, id_0, 0, \ell_0 \rangle \cdot s_1$, $\sigma_0 \xrightarrow{\rho} \sigma_1$, $enabled(s_1)$, and $\sigma_1(\mathbf{pc}) = \ell_0$. From (2), we have that $sp'_0.s = s'_0 \cdot \langle \sigma'_0, id'_0, 0, \ell'_0 \rangle \cdot s'_1$, $enabled(s'_1)$, $\sigma'_0 \xrightarrow{\rho'} \sigma'_1$, $\ell_0 = \ell'_0$, $id_0 = id'_0$, and $\sigma'_1(\mathbf{pc}) = \ell'_0$. As a result, we can apply the SE-COMMIT rule also to sp'_0. Therefore, we have $sp_0 \overset{\texttt{rlb}\ id_0 \cdot \texttt{pc}\ \sigma_1(\mathbf{pc})}{\rightsquigarrow} sp_1$ and $sp'_0 \overset{\texttt{rlb}\ id'_0 \cdot \texttt{pc}\ \sigma'_1(\mathbf{pc})}{\rightsquigarrow} sp'_1$.

Let $n = 0$. Therefore, we have $am_0 \Longrightarrow^0 am_1$, $am'_0 \Longrightarrow^0 am'_1$, $am_0 = am_1$, and $am'_0 = am'_1$.

We have already shown that (a) and (b) hold. We now show that (c)-(g) hold as well.

(c): $am_1 \cong am'_1$ immediately follows from (1), $am_0 = am_1$, and $am'_0 = am'_1$.

(d): To show that $sp_1 \cong sp'_1$, we need to show $sp_1.ctr = sp'_1.ctr$, $sp_1.\sigma \sim_{\mathbf{pc}} sp'_1.\sigma$, $sp_1.s \cong sp'_1.s$, and $sp_1.h = sp'_1.h$. First, $sp_1.ctr = sp'_1.ctr$ immediately follows from $sp_0.ctr = sp_1.ctr$, $sp'_0.ctr = sp'_1.ctr$, and (2). Second, $sp_1.\sigma \sim_{\mathbf{pc}} sp'_1.\sigma$ follows from (2), $sp_1.\sigma = sp_0.\sigma$, and $sp'_1.\sigma = sp'_0.\sigma$. Third, $sp_1.s \cong sp'_1.s$ follows from (2), $sp_1 = s_0 \cdot s_1$, and $sp'_1 = s'_0 \cdot s'_1$. Finally, $sp_1.h = sp'_1.h$ immediately follows from (2), $sp_1.h = sp_0.h \cdot \langle \sigma_0(\mathbf{pc}), id_0, \sigma_1(\mathbf{pc}) \rangle$, and $sp'_1.h = sp'_0.h \cdot \langle \sigma'_0(\mathbf{pc}), id'_0, \sigma'_1(\mathbf{pc}) \rangle$, $id_0 = id'_0$ (from (2)), $\sigma_0(\mathbf{pc}) = \sigma'_0(\mathbf{pc})$ (since all configurations in the speculative states are pairwise $\mathbf{pc}$-agreeing), and $\sigma_1(\mathbf{pc}) = \sigma'_1(\mathbf{pc})$ (since all configurations in the speculative states are pairwise next-step agreeing).

(e): Here we prove only $am_1 || sp_1$ ($am'_1 || sp'_1$ can be proved in the same way). To show $am_1 || sp_1$, we need to show $am_1.\sigma = sp_1.\sigma$ and $am_1.s || sp_1.s\upharpoonright_{com}$. From the SE-COMMIT rule in $\rightsquigarrow$, we have that $sp_1.\sigma = sp_0.\sigma_1$. Moreover, $am_1 = am_0$ and, therefore, $am_1.\sigma = am_0.\sigma$. From (3), $sp_1.\sigma = sp_0.\sigma_1$, and $am_1.\sigma = am_0.\sigma$, we have $am_1.\sigma = sp_1.\sigma$. Observe also that $am_1.s || sp_1.s\upharpoonright_{com}$ follows from $am_1.s = am_0.s$ (since $am_1 = am_0$) and $sp_1.s\upharpoonright_{com} = sp_0.s\upharpoonright_{com}$ (since the removed speculative state is one leading to a commit).

(f): For simplicity, we show only $INV(am_1, sp_1)$, the proof for $INV(am'_1, sp'_1)$ is analogous. To show $INV(am_1, sp_1)$, we need to show that $|am_1.s| = |sp_1.s\upharpoonright_{com}|$ and for all $i \leq i \leq |am_1.s|$, $minWndw(sp_1.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$. Observe that $am_1.s = am_0.s$ (because $am_1 = am_0$) and $sp_1.s\upharpoonright_{com} = sp_0.s\upharpoonright_{com}$ (because we remove a committed speculative state). As a result, both $|am_1.s| = |sp_1.s\upharpoonright_{com}|$ and $minWndw(sp_1.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$ for all $i \leq i \leq |am_1.s|$ immediately follow from (4).

(g): The observations τ_0 and τ'_0 are respectively $\texttt{commit}\ id_0$ and $\texttt{commit}\ id'_0$. From (2), we have that $sp_0.s \cong sp'_0.s$ which implies $id_0 = id'_0$. Hence, $\tau_0 = \tau'_0$.

This completes the proof of this case.

We can apply the Se-Rollback rule in sp_0: Hence, $sp_0.s = s_0 \cdot \langle \sigma_0, id_0, 0, \ell_0 \rangle \cdot s_1$, $\sigma_0 \xrightarrow{\rho} \sigma_1$, $enabled(s_1)$, and $\sigma_1(\mathbf{pc}) \neq \ell_0$. From (2), we have that $sp_0'.s = s_0' \cdot \langle \sigma_0', id_0', 0, \ell_0' \rangle \cdot s_1'$, $enabled(s_1')$, $\sigma_0' \xrightarrow{\rho'} \sigma_1'$, $\ell_0 = \ell_0'$, $id_0 = id_0'$, and $\sigma_1'(\mathbf{pc}) \neq \ell_0'$. As a result, we can apply the Se-Rollback rule also to sp_0'. Therefore, we have $sp_0 \overset{\texttt{rlb}\ id_0 \cdot \texttt{pc}\ \sigma_1(\mathbf{pc})}{\rightsquigarrow} sp_1$ and $sp_0' \overset{\texttt{rlb}\ id_0' \cdot \texttt{pc}\ \sigma_1'(\mathbf{pc})}{\rightsquigarrow} sp_1'$.

In the following, we denote by **idx** the index of $sp_0.s$'s $i+1$-th speculative state (i.e., the one that we are rolling back) inside its commit-free projection $sp_0.s\upharpoonright_{com}$, i.e., the $i+1$-th speculative state in sp_0 is the **idx**-th state in $sp_0.s\upharpoonright_{com}$. Observe that **idx** is also the index of $sp_0'.s$'s $i+1$-th speculative state, which we are rolling back, inside $sp_0'.s\upharpoonright_{com}$.

Let id be the transaction identifier in the **idx**-th speculative state in $am_0.s$. From (1), it follows that id is also the identifier in the **idx**-th speculative state in $am_0'.s$. According to the always mispredict semantics, there are k, k' such that:

$$r := am_0 \overset{v}{\Longrightarrow}^{k} am_2 \xRightarrow{\texttt{rlb}\ id \cdot \texttt{pc}\ \ell_1} am_1$$

$$r' := am_0' \overset{v'}{\Longrightarrow}^{k'} am_2' \xRightarrow{\texttt{rlb}\ id \cdot \texttt{pc}\ \ell_1'} am_1'$$

From (1) and (6), we immediately have that $k = k'$, $v = v'$, and $\ell_1 = \ell_1'$. Hence, we pick n to be $k+1$.

We have already shown that (a) and (b) hold. We now show that (c)-(g) hold as well.

(c): To show that $am_1 \cong am_1'$, we need to show $am_1.ctr = am_1'.ctr$, $am_1.\sigma \sim_{\mathbf{pc}} am_1'.\sigma$, and $am_1.s \cong am_1'.s$. First, $am_1.ctr = am_1'.ctr$ follows from (1) and $v = v'$. Second, $am_1.\sigma \sim_{\mathbf{pc}} am_1'.\sigma$ follows from (1) (since the configurations in the speculative states in $am_0.s$ and $am_0'.s$ are pairwise next-step agreeing and no intermediate steps in r, r' has modified the state that we are rolling back in the last step). Finally, $am_1.s \cong am_1'.s$ follows from (1), $am_1.s = am_0.s^{\mathbf{idx}-1}$, and $am_1'.s = am_0'.s^{\mathbf{idx}-1}$.

(d): To show that $sp_1 \cong sp_1'$, we need to show $sp_1.ctr = sp_1'.ctr$, $sp_1.\sigma \sim_{\mathbf{pc}} sp_1'.\sigma$, $sp_1.s \cong sp_1'.s$, and $sp_1.h = sp_1'.h$. First, $sp_1.ctr = sp_1'.ctr$ immediately follows from $sp_0.ctr = sp_1.ctr$, $sp_0'.ctr = sp_1'.ctr$, and (2). Second, $sp_1.\sigma \sim_{\mathbf{pc}} sp_1'.\sigma$ follows from (2) (since the configurations in the speculative states are pairwise next-step agreeing). Third, $sp_1.s \cong sp_1'.s$ follows from (2), $sp_1.s = sp_0.s^i$, and $sp_1'.s = sp_0'.s^i$. Finally, $sp_1.h = sp_1'.h$ immediately follows from (2), $sp_1.h = sp_0.h \cdot \langle \sigma_0(\mathbf{pc}), id_0, \sigma_1(\mathbf{pc}) \rangle$, and $sp_1'.h = sp_0'.h \cdot \langle \sigma_0'(\mathbf{pc}), id_0', \sigma_1'(\mathbf{pc}) \rangle$, $id_0 = id_0'$ (from (2)), $\sigma_0(\mathbf{pc}) = \sigma_0'(\mathbf{pc})$ (since all configurations in the speculative states are pairwise $\mathbf{pc}$-agreeing), and $\sigma_1(\mathbf{pc}) = \sigma_1'(\mathbf{pc})$ (since all configurations in the speculative states are pairwise next-step agreeing).

(e): Here we prove only $am_1 || sp_1$ ($am_1' || sp_1'$ can be proved in the same way). To show $am_1 || sp_1$, we need to show $am_1.\sigma = sp_1.\sigma$ and $am_1.s || sp_1.s\upharpoonright_{com}$. From the Se-Rollback rule in $\rightsquigarrow$, we have that $sp_1.\sigma = \sigma_1$, which is the configuration obtained by executing one step starting from the configuration σ_0 in the $i+1$-th speculative state in $sp_0.s$. From the run r, am_1 is obtained by applying the Se-Rollback rule in$\Longrightarrow$. As a result, $am_1.\sigma$ is the configuration obtained by executing one step starting from the configuration in **idx**-th speculative state in $am_0.s$. Observe that, from (3), σ_0 is exactly the configuration in the **idx**-th speculative state in $am_0.s$ (because the $i+1$-th state in $sp_0.s$ that we are rolling back is also the **idx**-th state in $sp_0.s\upharpoonright_{com}$). Hence, $am_1.\sigma = sp_1.\sigma$. Moreover, observe that $am_1.s || sp_1.s\upharpoonright_{com}$ immediately follows from (3), $am_1.s$ being $am_0.s^{\mathbf{idx}-1}$, $sp_1.s\upharpoonright_{com} = sp_0.s^i\upharpoonright_{com}$.

(f): For simplicity, we show only $INV(am_1, sp_1)$, the proof for $INV(am'_1, sp'_1)$ is analogous. To show $INV(am_1, sp_1)$, we need to show that $|am_1.s| = |sp_1.s\upharpoonright_{com}|$ and for all $i \leq i \leq |am_1.s|$, $minWndw(sp_1.s\upharpoonright_{com}{}^i) \leq wndw(am_1.s^i)$.

First, $|am_1.s| = |sp_1.s\upharpoonright_{com}|$ follows from (4), $am_1.s = am_0.s^{\mathbf{idx}-1}$ (because we are rolling back the **idx**-th transaction in the speculative state and the semantics only modifies the last speculative state), $sp_1.s\upharpoonright_{com} = sp_0.s^i\upharpoonright_{com}$, and $|sp_0.s^i\upharpoonright_{com}| = \mathbf{idx}-1$ (because $sp_0.s$'s i+1-th speculative state corresponds to $sp_0.s\upharpoonright_{com}$'s **idx**-th state by construction).

We now show that for all $1 \leq j \leq |am_1.s|$, $minWndw(sp_1.s\upharpoonright_{com}{}^j) \leq wndw(am_1.s^j)$. Let j be an arbitrary value such that $1 \leq j \leq |am_1.s|$. Observe that $am_1.s^j = am_0.s^j$ and $sp_1.s\upharpoonright_{com}{}^j = sp_0.s\upharpoonright_{com}{}^j$ (since $j \leq |am_1.s| < \mathbf{idx}$). From this and (4), we therefore immediately have that $minWndw(sp_1.s\upharpoonright_{com}{}^j) \leq wndw(am_1.s^j)$.

(g): The observations τ_0 and τ'_0 are respectively $\texttt{rlb}\ id_0 \cdot \texttt{pc}\ \sigma_1(\mathbf{pc})$ and $\texttt{rlb}\ id'_0 \cdot \texttt{pc}\ \sigma'_1(\mathbf{pc})$. From (2), we have that $sp_0.s \cong sp'_0.s$ which implies $id_0 = id'_0$. Moreover, we also have that $\sigma_0 \sim_{next} \sigma'_0$ and, therefore, $\sigma_1(\mathbf{pc}) = \sigma'_1(\mathbf{pc})$. Hence, $\tau_0 = \tau'_0$.

This completes the proof of this case.

This completes the proof of this case.

This completes the proof of our claim. □

G.4.3 Completeness. In Proposition 8, we prove the completeness of the always mispredict semantics w.r.t. the speculative semantics.

Proposition 8. *Let $w \in \mathbb{N}$ be a speculative window and $\sigma, \sigma' \in InitConf$ be two initial configurations. If $\{\!|p|\!\}_w(\sigma) \neq \{\!|p|\!\}_w(\sigma')$, then there exists a prediction oracle O with speculation window at most w such that $[\![p]\!]_O(\sigma) \neq [\![p]\!]_O(\sigma')$.*

Proof. Let $w \in \mathbb{N}$ be a speculative window and $\sigma, \sigma' \in InitConf$ be two initial configurations such that $\{\!|p|\!\}_w(\sigma) \neq \{\!|p|\!\}_w(\sigma')$.

We first analyze the case when the program does not terminate. There are two cases: either $\{\!|p|\!\}_w(\sigma) = \bot \wedge \{\!|p|\!\}_w(\sigma') \neq \bot$ or $\{\!|p|\!\}_w(\sigma) \neq \bot \wedge \{\!|p|\!\}_w(\sigma') = \bot$. Consider the first case $\{\!|p|\!\}_w(\sigma) = \bot \wedge \{\!|p|\!\}_w(\sigma') \neq \bot$ (the proof for the second case is similar). Since speculative execution does not introduce or prevent non-termination, we have that $[\![p]\!]_O(\sigma) = \bot \wedge [\![p]\!]_O(\sigma') \neq \bot$ for all prediction oracles O. Hence, there is a prediction oracle with speculative window at most w such that $[\![p]\!]_O(\sigma) \neq [\![p]\!]_O(\sigma')$.

We now consider the case where both $\{\!|p|\!\}_w(\sigma) \neq \bot$ and $\{\!|p|\!\}_w(\sigma') \neq \bot$. From this and $\{\!|p|\!\}_w(\sigma) \neq \{\!|p|\!\}_w(\sigma')$, it follows that there are $n, k, k' \in \mathbb{N}$, extended configurations am_1, am_2, am'_1, am'_2, final extended configurations am_3, am'_3, and sequences of observations $\tau, \tau_{am,1}, \tau_{am,2}, \tau'_{am,1}, \tau'_{am,2}$ such that $\tau_{am,1} \neq \tau'_{am,1}$, $am_1 \cong am'_1$ and:

$$\langle 0, \sigma, \varepsilon\rangle \overset{\tau}{\Longrightarrow}{}^n\ am_1 \xRightarrow{\tau_{am,1}} am_2 \xRightarrow{\tau_{am,2}}{}^k\ am_3$$

$$\langle 0, \sigma, \varepsilon\rangle \overset{\tau}{\Longrightarrow}{}^n\ am'_1 \xRightarrow{\tau'_{am,1}} am'_2 \xRightarrow{\tau'_{am,2}}{}^{k'}\ am'_3$$

We claim that there is a prediction oracle O with speculative window at most w such that (1) $\langle 0, \sigma, \varepsilon, \varepsilon\rangle \overset{v}{\rightsquigarrow}{}^* sp_1$ and $sp_1.\sigma = am_1.\sigma$ and $INV2(sp_1, am_1)$, and (2) $\langle 0, \sigma', \varepsilon, \varepsilon\rangle \overset{v}{\rightsquigarrow}{}^* sp'_1$ and $sp'_1.\sigma = am'_1.\sigma$ and $INV2(sp'_1, am'_1)$, and (3) $sp_1 \cong sp'_1$.

We now proceed by case distinction on the rule in $\Longrightarrow$ used to derive $am_1 \xRightarrow{\tau_{am,1}} am_2$. Observe that from $am_1 \cong am'_1$ and $\tau_{am,1} \neq \tau'_{am,1}$, it follows that the only possible rules are Se-NoBranch and Se-Branch (since applying the Se-Rollback rule would lead to $\tau_{am,1} = \tau'_{am,1}$):

Se-NoBranch: From the rule, we have that $p(am_1.\sigma(\mathbf{pc})) \neq \mathbf{beqz}\ x, \ell$, $enabled'(am_1.s)$, and $am_1.\sigma \xrightarrow{\tau_{am,1}} am_2.\sigma$. From $am_1 \cong am'_1$, we also have $p(am'_1.\sigma(\mathbf{pc})) \neq \mathbf{beqz}\ x, \ell$ (since $am_1.\sigma(\mathbf{pc}) = am'_1.\sigma(\mathbf{pc})$) and $enabled'(am'_1.s)$ (since $am'_1.s \cong am_1.s$). Hence, also $am'_1 \xRightarrow{\tau'_{am,1}} am'_2$ is obtained by applying the Se-NoBranch rule. Therefore, $am'_1.\sigma \xrightarrow{\tau_{am,1}} am'_2.\sigma$.
From our claim, we have (1) $\langle 0, \sigma, \varepsilon, \varepsilon\rangle \overset{v}{\rightsquigarrow}^* sp_1$, $sp_1.\sigma = am_1.\sigma$, and $INV2(sp_1, am_1)$, and (2) $\langle 0, \sigma', \varepsilon, \varepsilon\rangle \overset{v}{\rightsquigarrow}^* sp'_1$ and $sp'_1.\sigma = am'_1.\sigma$ and $INV2(sp'_1, am'_1)$. From $sp_1.\sigma = am_1.\sigma$, $sp'_1.\sigma = am'_1.\sigma$, $p(am'_1.\sigma(\mathbf{pc})) \neq \mathbf{beqz}\ x, \ell$, and $p(am_1.\sigma(\mathbf{pc})) \neq \mathbf{beqz}\ x, \ell$, we immediately have $p(sp'_1.\sigma(\mathbf{pc})) \neq \mathbf{beqz}\ x, \ell$, and $p(sp_1.\sigma(\mathbf{pc})) \neq \mathbf{beqz}\ x, \ell$. Moreover, from $enabled'(am_1.s)$, $enabled'(am'_1.s)$, $INV2(sp_1, am_1)$, and $INV2(sp'_1, am'_1)$, we also have $enabled(sp_1)$ and $enabled(sp'_1)$. Hence, we can apply to both configurations the Se-NoBranch rule in $\rightsquigarrow$. As a result, $sp_1 \overset{\tau_{sp,1}}{\rightsquigarrow} sp_2$ and $sp'_1 \overset{\tau'_{sp,1}}{\rightsquigarrow} sp'_2$ where the traces are derived using the non-speculative semantics $sp_1.\sigma \xrightarrow{\tau_{sp,1}} sp_2.\sigma$ and $sp'_1.\sigma \xrightarrow{\tau'_{sp,1}} sp'_2.\sigma$. From this, $sp_1.\sigma = am_1.\sigma$, $sp'_1.\sigma = am'_1.\sigma$, and the determinism of the non-speculative semantics, we have that $\tau_{sp,1} = \tau_{am,1}$ and $\tau'_{sp,1} = \tau'_{am,1}$. This, together with $\tau_{am,1} \neq \tau'_{am,1}$, leads to $\tau_{sp,1} \neq \tau'_{sp,1}$. Observe also that both $\tau_{sp,1}$ and $\tau'_{sp,1}$ are observations in *ExtObs*. Therefore, there are sequences of observations ρ, ρ' such that $[\![p]\!]_O(\sigma) = v \cdot \tau_{sp,1} \cdot \rho$ and $[\![p]\!]_O(\sigma') = v \cdot \tau'_{sp,1} \cdot \rho'$. As a result, $[\![p]\!]_O(\sigma) \neq [\![p]\!]_O(\sigma')$.

Se-Branch: From the rule, we have that $p(am_1.\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell''$ and $enabled'(am_1.s)$. From $am_1 \cong am'_1$, we also have $p(am'_1.\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell''$ (since $am_1.\sigma(\mathbf{pc}) = am'_1.\sigma(\mathbf{pc})$) and $enabled'(am'_1.s)$ (since $am'_1.s \cong am_1.s$). Hence, also $am'_1 \xRightarrow{\tau'_{am,1}} am'_2$ is obtained by applying the Se-Branch rule. Therefore, $\tau_{am,1} = \texttt{start}\ am_1.ctr \cdot \texttt{pc}\ \ell$ and $\tau'_{am,1} = \texttt{start}\ am'_1.ctr \cdot \texttt{pc}\ \ell'$, where $\ell = \begin{cases} \ell'' & \text{if } am_1.\sigma(x) \neq 0 \\ am_1.\sigma(\mathbf{pc}) + 1 & \text{if } am_1.\sigma(x) = 0 \end{cases}$
and $\ell' = \begin{cases} \ell'' & \text{if } am'_1.\sigma(x) \neq 0 \\ am'_1.\sigma(\mathbf{pc}) + 1 & \text{if } am'_1.\sigma(x) = 0 \end{cases}$. Since $am_1.ctr = am_1.ctr$ (from $am'_1.s \cong am_1.s$) and $\tau_{am,1} \neq \tau'_{am,1}$, we have that either $am_1.\sigma(x) = 0 \wedge am'_1.\sigma(x) \neq 0$ or $am_1.\sigma(x) \neq 0 \wedge am'_1.\sigma(x) = 0$. Without loss of generality, we assume that $am_1.\sigma(x) = 0 \wedge am'_1.\sigma(x) \neq 0$ (the proof for the other case is analogous).
We now executes two steps starting from sp_1 and sp'_1 with respect to $\rightsquigarrow$, and we construct $sp_1 \overset{\tau_{sp,1}}{\rightsquigarrow} sp_2 \overset{\tau_{sp,2}}{\rightsquigarrow} sp_3$ and $sp'_1 \overset{\tau'_{sp,1}}{\rightsquigarrow} sp'_2 \overset{\tau'_{sp,2}}{\rightsquigarrow} sp'_3$. From our claim, we have (1) $\langle 0, \sigma, \varepsilon, \varepsilon\rangle \overset{v}{\rightsquigarrow}^* sp_1$, $sp_1.\sigma = am_1.\sigma$, and $INV2(sp_1, am_1)$, and (2) $\langle 0, \sigma', \varepsilon, \varepsilon\rangle \overset{v}{\rightsquigarrow}^* sp'_1$ and $sp'_1.\sigma = am'_1.\sigma$ and $INV2(sp'_1, am'_1)$, and (3) $|sp_1.h| = |sp'_1.h|$. From $sp_1.\sigma = am_1.\sigma$, $sp'_1.\sigma = am'_1.\sigma$, $p(am'_1.\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell''$, and $p(am_1.\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell''$, we immediately have $O(sp_1.\sigma, p, sp_1.h) \neq \bot$, $O(sp'_1.\sigma, p, sp'_1.h) \neq \bot$, $p(sp'_1.\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell''$, and $p(sp_1.\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell''$. Moreover, from $enabled'(am_1.s)$, $enabled'(am'_1.s)$, $INV2(sp_1, am_1)$, and $INV2(sp'_1, am'_1)$, we also have $enabled(sp_1)$ and $enabled(sp'_1)$. Hence, we can apply to both configurations the Se-Branch rule in $\rightsquigarrow$. From $sp_1.\sigma = am_1.\sigma$, $sp'_1.\sigma = am'_1.\sigma$, and $am_1 \cong am'_1$, we immediately have that $sp_1.\sigma(\mathbf{pc}) = sp'_1.\sigma(\mathbf{pc})$. From this, (3), and the way in which we construct O (see below), we have that $O(sp_1.\sigma, p, sp_1.h) = O(sp'_1.\sigma, p, sp'_1.h) = \langle \ell'', 0\rangle$. By applying the Se-Branch rule to sp_1 we get $sp_1 \overset{\tau_{sp,1}}{\rightsquigarrow} sp_2$, where $\tau_{sp,1} = \texttt{start}\ sp_1.ctr \cdot \texttt{pc}\ \ell''$, $sp_2.ctr = sp_1.ctr + 1$, $sp_2.\sigma = sp_1.\sigma[\mathbf{pc} \mapsto \ell'']$, $sp_2.s = decr(sp_1.s) \cdot \langle sp_1.\sigma, sp_1.id, 0, \ell''\rangle$, and $sp_2.h = sp_1.h \cdot \langle sp_1.\sigma(\mathbf{pc}), sp_1.id, \ell''\rangle$.

Similarly, by applying the Se-Branch rule to sp'_1 we get $sp'_1 \overset{\tau'_{sp,1}}{\rightsquigarrow} sp'_2$, where $\tau'_{sp,1} = \texttt{start}\ sp'_1.ctr \cdot \texttt{pc}\ \ell''$, $sp'_2.ctr = sp'_1.ctr + 1$, $sp'_2.\sigma = sp'_1.\sigma[\mathbf{pc} \mapsto \ell'']$, $sp'_2.s = decr(sp'_1.s) \cdot \langle sp'_1.\sigma, sp'_1.id, 0, \ell''\rangle$, and $sp'_2.h = sp'_1.h \cdot \langle sp'_1.\sigma(\mathbf{pc}), sp'_1.id, \ell''\rangle$. Observe that $\tau_{sp,1} = \tau'_{sp,1}$ immediately follows from (3).

Since $sp_2.s = decr(sp_1.s) \cdot \langle sp_1.id, 0, n, sp_1.\sigma\rangle$ and $sp'_2.s = decr(sp'_1.s) \cdot \langle sp'_1.id, 0, n, sp'_1.\sigma\rangle$, we can commit or rollback the transactions associated with the last speculative states in $sp_2.s$ and $sp'_2.s$ (i.e., the transactions we started in the step $sp_1 \overset{\tau_{sp,1}}{\rightsquigarrow} sp_2$ and $sp'_1 \overset{\tau'_{sp,1}}{\rightsquigarrow} sp'_2$). We start by considering sp_2. From $am_1.\sigma(x) = 0$ and $sp_1.\sigma = am_1.\sigma$, we have that $sp_1.\sigma(x) = 0$. From this, $p(sp_1.\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell''$, and $O(sp_1.\sigma, p, sp_1.h) = \langle \ell'', 0\rangle$, the configuration σ obtained as $sp_1.\sigma \xrightarrow{\tau} \sigma$ is such that $\sigma(\mathbf{pc}) = \ell''$. Hence, we can apply the Se-Commit rule to sp_2 and obtain $sp_2 \overset{\tau_{sp,2}}{\rightsquigarrow} sp_3$, where $\tau_{sp,2} = \texttt{commit}\ sp_1.ctr$, $sp_3.ctr = sp_2.ctr$, $sp_3.\sigma = sp_2.\sigma$, $sp_3.s = decr(sp_1.s)$, and $sp_3.h = sp_2.h$. Consider now sp'_2. From $am'_1.\sigma(x) \neq 0$ and $sp'_1.\sigma = am'_1.\sigma$, we have that $sp'_1.\sigma(x) \neq 0$. From this, $p(sp'_1.\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell''$, and $O(sp'_1.\sigma, p, sp'_1.h) = \langle \ell'', 0\rangle$, the configuration σ' obtained as $sp'_1.\sigma \xrightarrow{\tau} \sigma'$ is such that $\sigma'(\mathbf{pc}) = sp'_1.\sigma(\mathbf{pc}) + 1$. From this and the well-formedness of p, we have that $\sigma'(\mathbf{pc}) \neq \ell''$. Hence, we can apply the Se-Rollback rule to sp'_2 and obtain $sp'_2 \overset{\tau'_{sp,2}}{\rightsquigarrow} sp'_3$, where $\tau'_{sp,2} = \texttt{rlb}\ sp'_1.ctr \cdot \texttt{pc}\ \sigma'(\mathbf{pc})$, $sp'_3.ctr = sp'_2.ctr$, $sp'_3.\sigma = \sigma'$, $sp'_3.s = decr(sp'_1.s)$, and $sp'_3.h = sp'_2.h \cdot \langle sp'_1.\sigma(\mathbf{pc}), sp'_1.ctr, \sigma'(\mathbf{pc})\rangle$. Therefore, there are sequences of observations ρ, ρ' such that $[\![p]\!]_O(\sigma) = v \cdot \tau_{sp,1} \cdot \tau_{sp,2} \cdot \rho$ and $[\![p]\!]_O(\sigma') = v \cdot \tau'_{sp,1} \cdot \tau'_{sp,2} \cdot \rho'$, where $\tau_{sp,1} = \tau'_{sp,1}$ and $\tau_{sp,2} \neq \tau'_{sp,2}$. As a result, $[\![p]\!]_O(\sigma) \neq [\![p]\!]_O(\sigma')$.

This completes the proof our claim.

Constructing the prediction oracle O. Here we prove our claim that there is a prediction oracle O with speculative window at most w such that (1) $\langle 0, \sigma, \varepsilon, \varepsilon\rangle \overset{v}{\rightsquigarrow}{}^* sp_1$ and $sp_1.\sigma = am_1.\sigma$ and $INV2(sp_1, am_1)$, and (2) $\langle 0, \sigma', \varepsilon, \varepsilon\rangle \overset{v}{\rightsquigarrow}{}^* sp'_1$ and $sp'_1.\sigma = am'_1.\sigma$ and $INV2(sp'_1, am'_1)$, and (3) $sp_1 \cong sp'_1$.

We denote by RB the set of transaction identifiers that occur $am_1.s$. Observe that from $\langle 0, \sigma, \varepsilon\rangle \overset{\tau}{\Longrightarrow}{}^n am_1$ and $\langle 0, \sigma, \varepsilon\rangle \overset{\tau}{\Longrightarrow}{}^n am'_1$ it follows that RB is also the set of transaction identifiers occurring in $am'_1.s$. The set RB identifies which branch instructions we must mispredict to reach the configuration am_1.

We now construct a list of predictions $\langle \ell, w\rangle$. In the following, we write am_0 instead of $\langle 0, \sigma, \varepsilon\rangle$. We construct the list by analyzing the execution $am_0 \overset{\tau}{\Longrightarrow}{}^n am_1$ (observe that deriving the list from $\langle 0, \sigma', \varepsilon\rangle \overset{\tau}{\Longrightarrow}{}^n am'_1$ would result in the same list). The list L is iteratively constructed as follows. During the execution, we denote by $\mathbf{idx}$ the position of the configuration in the execution from which we should continue the construction. Initially, $\mathbf{idx} = 0$. At each iteration, we find the smallest $\mathbf{idx'} \in \mathbb{N}$ such that $\mathbf{idx} \leq \mathbf{idx'} < n$ and the extended configuration $am_{\mathbf{idx'}}$ is such that $am_0 \overset{\tau_1}{\Longrightarrow}{}^{\mathbf{idx'}} am_{\mathbf{idx'}}$, and $p(am_{\mathbf{idx'}}.\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell$ and $enabled'(am_{\mathbf{idx'}}.s)$ (i.e., the next step in the execution is obtained using the Se-Branch rule). Next, we proceed as follows:

$\mathbf{am_{idx'}}.ctr \in \mathbf{RB}$ In this case, we mispredict the outcome of the corresponding branch instruction. The prediction associated with the branch instruction is $\langle \ell'', w\rangle$, where $\ell'' = am_{\mathbf{idx'}}.\sigma(\mathbf{pc}) + 1$ if $am_{\mathbf{idx'}}.\sigma(x) = 0$ and $\ell'' = \ell$ otherwise. Concretely, we update L by appending $\langle \ell'', w\rangle$ and setting $\mathbf{idx}$ to $\mathbf{idx'}+1$ (i.e., we continue constructing L by analyzing the next step in the execution).

$\mathbf{am_{idx'}}.ctr \notin \mathbf{RB}$ In this case, we correctly predict the outcome of the corresponding branch instruction. The prediction associated with the branch instruction is $\langle \ell'', 0\rangle$, where $\ell'' = \ell$ if $am_{\mathbf{idx'}}.\sigma(x) = 0$ and $\ell'' = am_{\mathbf{idx'}}.\sigma(\mathbf{pc}) + 1$ otherwise. Concretely, we update L by appending $\langle \ell'', 0\rangle$ and we update the index $\mathbf{idx}$ to $\mathbf{idx'} + k + 2$ where the value $k \in \mathbb{N}$ is such that $am_0 \overset{\tau_1}{\Longrightarrow}{}^{\mathbf{idx'}} am_{\mathbf{idx'}} \xRightarrow{\texttt{start}\ am_{\mathbf{idx'}}.ctr \cdot \texttt{pc}\ \ell'} am_{\mathbf{idx'}+1} \overset{v}{\Longrightarrow}{}^k am_{\mathbf{idx'}+k+1} \xRightarrow{\texttt{rlb}\ am_{\mathbf{idx'}}.ctr \cdot \texttt{pc}\ \ell''} am_{\mathbf{idx'}+k+2}$. That is, we ignore the portion of the execution associated with the speculative transaction $am_{\mathbf{idx'}}.ctr$

and we continue constructing L after the transaction $am_{\mathbf{idx}'}.ctr$ has been rolled back. Observe also that $\mathbf{idx}' + k + 2 \leq n$ (otherwise $am_{\mathbf{idx}'}.ctr$ would have been included into RB).

Finally, if the configuration am_1 in $\langle 0, \sigma, \varepsilon \rangle \overset{\tau}{\Longrightarrow}^{n} am_1$ is such that $p(am_1.\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell$ and $enabled'(am_1.s)$, we append to L the prediction $\langle \ell, 0 \rangle$.

The prediction oracle O is defined as follows, where $\#(h)$ is the number of unique transaction identifiers in h:

$$O(\sigma, p, h) := \begin{cases} \langle \ell', w' \rangle & \text{if } \#(h) + 1 \leq |L| \wedge L|_{\#(h)+1} = \langle \ell', w' \rangle \wedge (p(\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell' \vee \ell' = \sigma(\mathbf{pc}) + 1) \\ \langle \ell, 0 \rangle & \text{otherwise (where } p(\sigma(\mathbf{pc})) = \mathbf{beqz}\ x, \ell) \end{cases}$$

Observe that O is a prediction oracle as it depends only on the program counter, the program itself, and the length of the history. Moreover, its speculative window is at most w (since the predictions contain either w or 0 as speculative window). The key property of O is that "when the execution starts from σ (or σ'), O follows the predictions in L for the first $|L|$ branch instructions and afterwards always predicts the branch as taken".

From $\langle 0, \sigma, \varepsilon \rangle \overset{\tau}{\Longrightarrow}^{n} am_1$, $\langle 0, \sigma, \varepsilon \rangle \overset{\tau}{\Longrightarrow}^{n} am_1'$, and the way in which we constructed O, we have that (1) $\langle 0, \sigma, \varepsilon, \varepsilon \rangle \overset{\nu}{\rightsquigarrow}^{*} sp_1$ and $sp_1.\sigma = am_1.\sigma$ and $INV2(sp_1, am_1)$, and (2) $\langle 0, \sigma', \varepsilon, \varepsilon \rangle \overset{\nu}{\rightsquigarrow}^{*} sp_1'$ and $sp_1'.\sigma = am_1'.\sigma$ and $INV2(sp_1', am_1')$, and (3) $sp_1 \cong sp_1'$. The proof of this statement is similar to the proof of Appendix G.4.2. ◻

Lemma 18 (B: AM and Oracle coincide)**.** *If*

(1) $\Sigma_{B} \approx^{\Sigma^{States}}_{O_{am}} X_{B}$ *by Base and*

(2) $\Sigma_{B} \overset{\tau}{\Rightarrow}_{B} \Sigma_{B}'$ *and*

(3) $minWndw(\Sigma_{B}) > 0$

(4) $X_{B}.\overline{\rho} = \emptyset$

Then

(1) $X_{B} \overset{\tau}{\rightsquigarrow}^{O}_{B} X_{B}'$

Proof. Since $minWndw(\Sigma_{B}) > 0$ we know that the next step is not a rollback. From $minWndw(\Sigma_{B}) > 0$ and $\Sigma_{B} \approx^{\Sigma^{States}}_{O_{am}} X_{B}$ we have $INV2(\Sigma_{B}, X_{B})$ and we get $minWndw(X_{B}) > 0$ as well.

We proceed by inversion on $\Sigma_{B} \overset{\tau}{\Rightarrow}_{B} \Sigma_{B}'$:

Rule AM-NoBranch From the rule, we have that $\Sigma_{B}.\sigma \xrightarrow{\tau} \Sigma_{B}'.\sigma$.

The case is analogous to the corresponding case in Lemma 67 (S: AM and Oracle coincide).

Rule B:AM-barr-spec, Rule B:AM-barr From the rule, we have that $\Sigma_{B}.\sigma \rightarrow \Sigma_{B}'.\sigma$.

The case is analogous to the case above.

Rule B:AM-Spec Then, τ is generated by the step $\Sigma_{B}.\sigma \xrightarrow{\tau} \Sigma_{B}'.\sigma$ generated by Rule B:AM-Spec.

The case is analogous to the corresponding case in Lemma 67 (S: AM and Oracle coincide).

◻

H SEMANTICS FOR Ω_{J}

H.1 Ω_{J}: Always Mispredict Semantics

Speculative program states Σ_{J} are defined as stacks of Speculative instances $\overline{\Phi}_{J}$. A speculation instance $\Phi_{J} = \langle p, ctr, \sigma, n \rangle$ 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 $\perp$ when there is no speculative transaction ongoing.

$$\textit{Speculative States } \Sigma_{\mathcal{J}} ::= \overline{\Phi}_{\mathcal{J}}$$

$$\textit{Speculative Instance } \Phi_{\mathcal{J}} ::= \langle p, ctr, \sigma, n\rangle_{\overline{\rho}}$$

$$\tau ::= \texttt{start}_{\mathcal{J}}\ ctr \mid \texttt{rlb}_{\mathcal{J}}\ ctr$$

First, we keep track of all possible allowed jump targets in the program. We collect the instruction number for each **endbr** instruction into a labelset L defined as follows: $L_p = \{i \mid \forall i \in \mathbb{N}.\ p(i) = \textbf{endbr}\}$. We will omit p in L_p if it is clear from context and we assume L_p is ordered.

We use $\exists x \subset e.\ x \in Regs$ to indicate that the jump is really indirect. This means one subexpression of e is a register.

$\boxed{\textit{Judgements}}$

$\Sigma_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$	State $\Sigma_{\mathcal{J}}$ small-steps to $\Sigma'_{\mathcal{J}}$ and emits observation τ.
$\Phi_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \overline{\Phi}'_{\mathcal{J}}$	Speculative instance $\Phi_{\mathcal{J}}$ small-steps to $\overline{\Phi}_{\mathcal{J}}'$ and emits observation τ.
$\Sigma_{\mathcal{J}} \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$	State $\Sigma_{\mathcal{J}}$ big-steps to $\Sigma'_{\mathcal{J}}$ and emits a list of observations $\overline{\tau}$.
$p \times \textit{InitConf} \rightsquigarrow^{\omega}_{\mathcal{J}} \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$\boxed{\Sigma_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}}}$

($\mathcal{J}$:AM-Context)
$$\frac{\Phi_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \overline{\Phi}'_{\mathcal{J}}}{\overline{\Phi}_{\mathcal{J}} \cdot \Phi_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \overline{\Phi}_{\mathcal{J}} \cdot \overline{\Phi}'_{\mathcal{J}}}$$

($\mathcal{J}$:AM-Rollback)
$$\frac{n' = 0 \text{ or p is stuckif } ctr \geq ctr' \text{ then } ctr'' = ctr \text{ else } ctr'' = ctr'}{\overline{\Phi}_{\mathcal{J}} \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle \overset{\texttt{rlb}_{\mathcal{J}}\ ctr}{\rightsquigarrow}_{\mathcal{J}} \overline{\Phi}_{\mathcal{J}} \cdot \langle p, ctr'', \sigma, n\rangle}$$

$\boxed{\Phi_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \overline{\Phi}'_{\mathcal{J}}}$

($\mathcal{J}$:AM-barr)
$$\frac{p(\sigma(\mathbf{pc})) = \textbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, \bot\rangle \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \langle p, ctr, \sigma', \bot\rangle}$$

($\mathcal{J}$:AM-barr-spec)
$$\frac{p(\sigma(\mathbf{pc})) = \textbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, n+1\rangle \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \langle p, ctr, \sigma', 0\rangle}$$

($\mathcal{J}$:AM-NoSpec)
$$\frac{p(\sigma(\mathbf{pc})) \neq \textbf{jmp}\ x, \textbf{spbarr}, Z \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, n+1\rangle \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \langle p, ctr, \sigma', n\rangle}$$

($\mathcal{J}$:AM-General)
$$\frac{\tau = \texttt{pc}\ n \mid \texttt{start}_{\mathcal{J}}\ n}{\Phi_{\mathcal{J}\,\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Phi_{\mathcal{J}\,\overline{\rho}}}$$

($\mathcal{J}$:AM-Spec)
$$\frac{\begin{array}{c} p(\sigma(\mathbf{pc})) = \textbf{jmp}\ x \qquad \sigma \xrightarrow{\tau} \sigma' \qquad j = min(\omega, n) \\ \exists x \subset e.\ x \in Regs \qquad \langle p, ctr+1, \sigma, j\rangle \vdash^{L\setminus\{\sigma'.\mathbf{pc}\}} \overline{\Phi}_{\mathcal{J}} \\ \overline{\Phi}_{\mathcal{J}} = \overline{\Phi}'_{\mathcal{J}} \cdot \Phi_{\mathcal{J}} \end{array}}{\langle p, ctr, \sigma, n+1\rangle_{\varepsilon} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \langle p, ctr, \sigma', n\rangle_{\varepsilon} \cdot \overline{\Phi}'_{\mathcal{J}} \cdot \Phi_{\mathcal{J}\,\varepsilon\cdot\texttt{pc}\ \sigma'(\mathbf{pc})\cdot\texttt{start}_{\mathcal{J}}\ ctr}}$$

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

$$\frac{}{\Sigma_{\mathcal{J}} \Downarrow^{\varepsilon}_{\mathcal{J}} \Sigma_{\mathcal{J}}}\ (\mathcal{J}\text{:AM-Reflection}) \qquad \frac{\Sigma_{\mathcal{J}} \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma''_{\mathcal{J}} \quad \Sigma''_{\mathcal{J}} \xrightarrow{\tau}_{\mathcal{J}} \Sigma'_{\mathcal{J}}}{\Sigma_{\mathcal{J}} \Downarrow^{\overline{\tau}\cdot\tau}_{\mathcal{J}} \Sigma'_{\mathcal{J}}}\ (\mathcal{J}\text{:AM-Single})$$

Helpers

$$\frac{}{\langle p, ctr, \sigma, n\rangle \vdash^{\varnothing} \varnothing}\ (\text{Helper-Base}) \qquad \frac{l \in S \quad \langle p, ctr, \sigma, n\rangle \vdash^{S\setminus l} \overline{\Phi}_{\mathcal{J}}}{\langle p, ctr, \sigma, n\rangle \vdash^{S} \langle p, ctr, \sigma[\mathbf{pc} \mapsto l], n\rangle \cdot \overline{\Phi}_{\mathcal{J}}}\ (\text{Helper-Ind})$$

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

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

$$\frac{}{\langle p, ctr, \sigma, n\rangle \vdash^{[\,]} \varnothing}\ (\text{Helper-Base}) \qquad \frac{\langle p, ctr+1, \sigma, n\rangle \vdash^{S'} \overline{\Phi}_{\mathcal{J}}}{\langle p, ctr, \sigma, n\rangle \vdash^{[l::S']} \langle p, ctr+1, \sigma[\mathbf{pc} \mapsto l]\rangle \cdot \overline{\Phi}_{\mathcal{J}}}\ (\text{Helper-Ind})$$

Notie the helper predicate Rule Helper-Ind generating all speculative states needed in Rule $\mathcal{J}$:AM-Spec

$p \times \mathit{InitConf} \leadsto^{\omega}_{\mathcal{J}} \overline{\tau}$

$$\frac{\exists \Sigma'_{\mathcal{J}} \quad \vdash \Sigma'_{\mathcal{J}} \colon \mathit{fin} \quad \Sigma^{0}_{\mathcal{J}}(p, \sigma) \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}}}{p, \sigma \leadsto^{\omega}_{\mathcal{J}} \overline{\tau}}\ (\mathcal{J}\text{:AM-Trace}) \qquad \frac{}{\mathit{Beh}^{\omega}_{\mathcal{J}}(p) = \{\overline{\tau} \mid \forall \sigma \in \mathit{InitConf}.\ p, \sigma \leadsto^{\omega}_{\mathcal{J}} \overline{\tau}\}}\ (\mathcal{J}\text{:AM-Beh})$$

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

H.2 $\leadsto_{\mathcal{J}}$: Oracle Semantics

We use an oracle O to decide where to jump to 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:

$$\begin{aligned} \mathit{Speculative\ States}\ X_{\mathcal{J}} &::= \overline{\Psi}_{\mathcal{J}} \\ \mathit{Speculative\ Instance}\ \Psi_{\mathcal{J}} &::= \langle p, ctr, \sigma, h, n\rangle^{b}_{\rho} \text{ where } b \in \{\text{true}, \text{false}, \varepsilon\} \\ \tau &::= ..\ \mid \texttt{commit}_{\mathcal{J}}\ ctr \end{aligned}$$

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.

Judgements

$X_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}}$	State $X_{\mathcal{J}}$ small-steps to $X'_{\mathcal{J}}$ and emits observation τ.
$\Phi_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} \overline{\Phi}'_{\mathcal{J}}$	Speculative instance $\Psi_{\mathcal{J}}$ small-steps to $\overline{\Psi}_{\mathcal{J}}'$ and emits observation τ.
$X_{\mathcal{J}} \;{}^{O}\!\Downarrow^{\mathcal{J}}_{\overline{\tau}} X'_{\mathcal{J}}$	State $X_{\mathcal{J}}$ big-steps to $X'_{\mathcal{J}}$ and emits a list of observations $\overline{\tau}$.
$p \times InitConf \;\Omega^{O}_{\mathcal{J}}\; \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$\boxed{X_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}}}$

($\mathcal{J}$:SE-Context)

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

($\mathcal{J}$:Rollback)

$$\frac{n' = 0 \text{ or p is stuck}}{\overline{\Psi}_{\mathcal{J}} \cdot \langle p, ctr, \sigma, h, n\rangle \cdot \langle p, ctr', \sigma', h', n'\rangle^{false} \cdot \overline{\Psi}'_{\mathcal{J}} \overset{\texttt{rlb}_{\mathcal{J}}\; ctr}{\rightsquigarrow}{}^{O}_{\mathcal{J}} \overline{\Psi}_{\mathcal{J}} \cdot \langle p, ctr', \sigma, h, n\rangle}$$

($\mathcal{J}$:Commit)

$$\frac{}{\overline{\Psi}_{\mathcal{J}} \cdot \langle p, ctr, \sigma, h, n\rangle^{b} \cdot \langle p, ctr', \sigma', h', 0\rangle^{true} \cdot \overline{\Psi}_{\mathcal{J}}{}' \overset{\texttt{commit}_{\mathcal{J}}\; ctr}{\rightsquigarrow}{}^{O}_{\mathcal{J}} \overline{\Psi}_{\mathcal{J}} \cdot \langle p, ctr', \sigma', h', n\rangle^{b} \cdot \overline{\Psi}_{\mathcal{J}}{}'}$$

($\mathcal{J}$:General)

$$\frac{\tau = \texttt{pc}\; n \mid \texttt{start}_{\mathcal{J}}\; n}{\overline{\Psi}_{\mathcal{J}} \cdot \Psi_{\mathcal{J}\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} \overline{\Psi}_{\mathcal{J}} \cdot \Psi_{\mathcal{J}\overline{\rho}}}$$

$\boxed{\Psi_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} \Psi'_{\mathcal{J}}}$

($\mathcal{J}$:barr)

$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, h, \bot\rangle \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} \langle p, ctr, \sigma', h, \bot\rangle}$$

($\mathcal{J}$:barr-spec)

$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, h, n+1\rangle \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} \langle p, ctr, \sigma, h, 0\rangle}$$

($\mathcal{J}$:NoSpec)

$$\frac{p(\sigma(\mathbf{pc})) \neq \mathbf{jmp}\; x, \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, h, n+1\rangle \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} \langle p, ctr, \sigma', h, n\rangle}$$

($\mathcal{J}$:Spec)

$$\frac{\begin{array}{ccc} p(\sigma(\mathbf{pc})) = \mathbf{jmp}\; e & \sigma \xrightarrow{\tau} \sigma' & O(p, n, h) = (l, \omega) \\ \exists x \subset e.\, x \in Regs \quad [\![e]\!](a) \neq l & \sigma'' = \sigma[\mathbf{pc} \mapsto l] & h' = h \cdot \langle \sigma(\mathbf{pc}), l\rangle \end{array}}{\langle p, ctr, \sigma, h, n+1\rangle \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} \langle p, ctr, \sigma', h', n\rangle \cdot \langle p, ctr+1, \sigma'', h', \omega\rangle^{true}_{\texttt{pc}\; \sigma''(\mathbf{pc}) \cdot \texttt{st}\; (ctr)}}$$

($\mathcal{J}$:Spec-Exe)

$$\frac{\begin{array}{ccc} p(\sigma(\mathbf{pc})) = \mathbf{jmp}\; e & \sigma \xrightarrow{\tau} \sigma' & O(p, n, h) = (l, \omega) \\ \exists x \subset e.\, x \in Regs & [\![e]\!](a) = l & h' = h \cdot \langle \sigma(\mathbf{pc}), l\rangle \end{array}}{\langle p, ctr, \sigma, h, n+1\rangle \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} \langle p, ctr, \sigma', h, n\rangle \cdot \langle p, ctr+1, \sigma', h', \omega\rangle^{false}_{\texttt{st}\; (ctr)}}$$

$\boxed{X_{\mathcal{J}} \;{}^{O}\!\Downarrow^{\mathcal{J}}_{\overline{\tau}} X'_{\mathcal{J}}}$

$$\frac{}{X_{\mathcal{J}} \overset{O}{\leadsto}{}^{\mathcal{J}}_{\varepsilon} X_{\mathcal{J}}}\ (\mathcal{J}\text{:Reflection}) \qquad \frac{X_{\mathcal{J}} \overset{O}{\leadsto}{}^{\mathcal{J}}_{\overline{\tau}} X''_{\mathcal{J}} \qquad X''_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}}}{X_{\mathcal{J}} \overset{O}{\leadsto}{}^{\mathcal{J}}_{\overline{\tau}\cdot\tau} X'_{\mathcal{J}}}\ (\mathcal{J}\text{:Single})$$

$\boxed{Helpers}$

$$\frac{X_{\mathcal{J}} = \langle p, 0, \sigma, \varepsilon, \bot\rangle \qquad \sigma \in InitConf}{\vdash X_{\mathcal{J}} \colon init}\ (\mathcal{J}\text{:SE-Init}) \qquad \frac{X_{\mathcal{J}} = \langle p, ctr, \sigma, h, \bot\rangle \qquad \sigma(\mathbf{pc}) = \bot}{\vdash X_{\mathcal{J}} \colon fin}\ (\mathcal{J}\text{:SE-Fin})$$

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

$\boxed{p \times InitConf \ \Downarrow^{O}_{\mathcal{J}}\ \overline{\tau}}$

$$\frac{\exists X'_{\mathcal{J}} \qquad \vdash X'_{\mathcal{J}} \colon fin \qquad X^{init}_{\mathsf{S}}(p, \sigma) \overset{O}{\leadsto}{}^{\mathcal{J}}_{\overline{\tau}} X'_{\mathcal{J}}}{(p, \sigma) \Downarrow^{O}_{\mathcal{J}} \overline{\tau}}\ (\mathcal{J}\text{:SE-Trace}) \qquad \frac{}{Beh^{O}_{\mathcal{J}}(p) = \{\overline{\tau} \mid \forall \sigma \in InitConf.\ (p, \sigma) \Downarrow^{O}_{\mathcal{J}} \overline{\tau}\}}\ (\mathcal{J}\text{:SE-Beh})$$

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

H.3 $\Downarrow_{\mathcal{J}}$: 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 $\to_{\mathcal{S}}$. The symbolic states $\Sigma^{\mathcal{S}}_{\mathcal{J}}$.

$\boxed{\Sigma^{\mathcal{S}}_{\mathcal{J}} \overset{\tau}{\Rightarrow}{}^{\mathcal{S}}_{\mathcal{J}} \Sigma^{\mathcal{S}\prime}_{\mathcal{J}}}$

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

$$\frac{n' = 0 \text{ or p is stuck}}{\overline{\Phi}_{\mathcal{J}\mathcal{S}} \cdot \langle p, ctr, \sigma_{\mathcal{S}}, n\rangle \cdot \langle p, ctr', \sigma'_{\mathcal{S}}, n'\rangle \xRightarrow{\texttt{rlb}_{\mathcal{J}}\ ctr}{}^{\mathcal{S}}_{\mathcal{J}} \overline{\Phi}_{\mathcal{J}\mathcal{S}} \cdot \langle p, ctr', \sigma_{\mathcal{S}}, n\rangle}\ (\mathcal{J}\text{:Sym-Rollback})$$

$\boxed{\Phi^{\mathcal{S}}_{\mathcal{J}} \overset{\tau}{\Rightarrow}_{\mathcal{J}} \overline{\Phi}'_{\mathcal{J}\mathcal{S}}}$

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

$$\frac{p(\sigma(\mathbf{pc})) \neq \mathbf{jmp}\ e, \mathbf{spbarr}, Z \qquad \sigma_{\mathcal{S}} \xrightarrow{\tau}_{\mathcal{S}} \sigma'_{\mathcal{S}}}{\langle p, ctr, \sigma_{\mathcal{S}}, n+1\rangle \overset{\tau}{\Rightarrow}{}^{\mathcal{S}}_{\mathcal{J}} \langle p, ctr, \sigma'_{\mathcal{S}}, n\rangle}\ (\mathcal{J}\text{:Sym-NoSpec}) \qquad \frac{\tau = \texttt{pc}\ n \mid \texttt{start}_{\mathcal{J}}\ n}{\Phi^{\mathcal{S}}_{\mathcal{J}\ \overline{p}\cdot\tau} \overset{\tau}{\Rightarrow}{}^{\mathcal{S}}_{\mathcal{J}} \Phi^{\mathcal{S}}_{\mathcal{J}\ \overline{p}}}\ (\mathcal{J}\text{:Sym-General})$$

(J:Sym-Spec)

$$\frac{\begin{array}{c} p(\sigma(\mathbf{pc})) = \mathbf{jmp}\ e \quad \sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}} \quad j = min(\omega, n) \\ \sigma''_{\mathcal{S}}.\delta^{\mathcal{S}} = \sigma'_{\mathcal{S}}.\delta^{\mathcal{S}} \qquad \exists x \subset e.\, x \in Regs \\ \langle p, ctr, \sigma''_{\mathcal{S}}, j\rangle \vdash^{L \setminus \{\sigma'_{\mathcal{S}}\cdot\mathbf{pc}\}} \overline{\Phi}_{\mathcal{J}_{\mathcal{S}}} \\ \overline{\Phi}_{\mathcal{J}_{\mathcal{S}}} = \overline{\Phi}'_{\mathcal{J}_{\mathcal{S}}} \cdot \Phi^{\mathcal{S}}_{\mathcal{J}} \end{array}}{\langle p, ctr, \sigma_{\mathcal{S}}, n+1\rangle \overset{\tau}{=}\!\!\rightsquigarrow^{\mathcal{S}}_{\mathcal{J}} \langle p, ctr, \sigma'_{\mathcal{S}}, n\rangle \cdot \overline{\Phi}'_{\mathcal{J}_{\mathcal{S}}} \cdot \Phi^{\mathcal{S}}_{\mathcal{J}\ \mathtt{pc}\ \sigma'_{\mathcal{S}}(\mathbf{pc})\cdot\mathtt{start}_{\mathcal{J}}\ ctr}}$$

$\boxed{\Sigma^{\mathcal{S}}_{\mathcal{J}}\ {}_{\mathcal{S}}\!\Downarrow^{\overline{\tau}}_{\mathcal{J}}\ \Sigma^{\mathcal{S}\prime}_{\mathcal{J}}}$

(J:Sym-Reflection)

$$\frac{}{\Sigma^{\mathcal{S}}_{\mathcal{J}}\ {}_{\mathcal{S}}\!\Downarrow^{\varepsilon}_{\mathcal{J}}\ \Sigma^{\mathcal{S}}_{\mathcal{J}}}$$

(J:Sym-Single)

$$\frac{\Sigma^{\mathcal{S}}_{\mathcal{J}}\ {}_{\mathcal{S}}\!\Downarrow^{\overline{\tau}}_{\mathcal{J}}\ \Sigma^{\mathcal{S}\prime\prime}_{\mathcal{J}} \qquad \Sigma^{\mathcal{S}\prime\prime}_{\mathcal{J}} \overset{\tau}{=}\!\!\rightsquigarrow^{\mathcal{S}}_{\mathcal{J}} \Sigma^{\mathcal{S}\prime}_{\mathcal{J}}}{\Sigma^{\mathcal{S}}_{\mathcal{J}}\ {}_{\mathcal{S}}\!\Downarrow^{\overline{\tau}\cdot\tau_{\mathcal{S}}}_{\mathcal{J}}\ \Sigma^{\mathcal{S}\prime}_{\mathcal{J}}}$$

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

$\boxed{Helpers}$

(J:Sym-Init)

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

(J:Sym-Fin)

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

(J:Sym-Initial-State)

$$\frac{}{\Sigma^{\mathcal{S}\,init}_{\mathcal{J}}(p, \sigma_{\mathcal{S}}) \coloneqq \langle p, 0, \sigma_{\mathcal{S}}, \bot\rangle}$$

$\boxed{(p \times InitConf)\ \ {}_{\mathcal{S}}\!\Omega^{\omega}_{\mathcal{J}}\ \overline{\tau}}$

(J:Sym-Trace)

$$\frac{\exists \Sigma^{\mathcal{S}\prime}_{\mathcal{J}} \qquad \vdash \Sigma^{\mathcal{S}\prime}_{\mathcal{J}} : fin \qquad \Sigma^{0}_{\mathcal{J}}(p, \sigma_{\mathcal{S}})\ {}_{\mathcal{S}}\!\Downarrow^{\overline{\tau}}_{\mathcal{J}}\ \Sigma^{\mathcal{S}\prime}_{\mathcal{J}}}{(p, \sigma_{\mathcal{S}})\ \ {}_{\mathcal{S}}\!\Omega^{\omega}_{\mathcal{J}}\ \overline{\tau}}$$

(J:Sym-Beh)

$$\frac{}{Beh^{\mathcal{S}}_{\mathcal{J}}(p) = \{\overline{\tau} \mid \forall \sigma_{\mathcal{S}} \in InitConf.\ (p, \sigma)\ \ {}_{\mathcal{S}}\!\Omega^{\omega}_{\mathcal{J}}\ \overline{\tau}\}}$$

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

I PROOFS FOR $\rightsquigarrow_{\mathcal{J}}$:

Our main result for $\rightsquigarrow_{\mathcal{J}}$ is the following

Theorem 6 ($\rightsquigarrow_{\mathcal{J}}$ is *WFSS*). $\vdash \rightsquigarrow_{\mathcal{J}}$ *WFSS*

Proof. Immediately follows from Theorem 10 ($\mathcal{J}$: Oracle Overapproximation), Theorem 9 ($\mathcal{J}$: Symbolic Consistency), Theorem 8 ($\mathcal{J}$: Behaviour of non-speculative semantics and AM semantics) and Theorem 7 ($\mathcal{J}$ SE: Behaviour of non-speculative and oracle semantics). ◻

I.1 $\mathcal{J}$: Relating Non-speculative and Oracle Semantics

Theorem 7 ($\mathcal{J}$ SE: Behaviour of non-speculative and oracle semantics)

- Lemma 23 ($\mathcal{J}$ SE: Completeness of the speculative semantics)
  - Lemma 24 ($\mathcal{J}$ SE: Non-speculative execution for rolled back transactions)
- Lemma 25 ($\mathcal{J}$ AM : Soundness of the AM semantics w.r.t. non-speculative semantics)
  - Lemma 20 ($\mathcal{J}$ SE: Soundness single step No Speculation)
    - Lemma 21 ($\mathcal{J}$ SE: Single Step Instance Non Speculative)
  - Lemma 22 ($\mathcal{J}$ SE: Single Step Speculation)

Theorem 7 ($\mathcal{J}$ SE: Behaviour of non-speculative and oracle semantics). *Let p be a program and O be a prediction oracle. Then $Beh_{NS}(p) = Beh^{O}_{\mathcal{J}}(p)\upharpoonright_{ns}$*

Proof. We prove the two directions separately:

$\Leftarrow$ By the definition of $Beh^{O}_{\mathcal{J}}(p)$ we have an initial configuration σ such that $(p,\sigma)\ \Omega^{O}_{\mathcal{J}}\ \overline{\tau}$.

By definition of $(p,\sigma)\ \Omega^{O}_{\mathcal{J}}\ \overline{\tau}$, we know there exists a state $X'_{\mathcal{J}}$ such that $\vdash X'_{\mathcal{J}}$: *fin* and an initial state $X^{init}_{\mathcal{J}}(p,\sigma)$ such that $X^{init}_{\mathcal{J}}(p,\sigma) \overset{O}{\rightsquigarrow}{}^{\mathcal{J}}_{\overline{\tau}} X'_{\mathcal{J}}$.

Analogous to the corresponding case in Theorem 12 ($\mathcal{S}$ SE: Behaviour of non-speculative and oracle semantics) by using Lemma 19 ($\mathcal{J}$ SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

We thus have $((p,\sigma))\ \Omega_{NS}\overline{\tau}\upharpoonright_{ns} \in Beh_{NS}(p)$ by Rule NS-Trace.

$\Rightarrow$ Assume that $((p,\sigma))\ \Omega_{NS}\overline{\tau} \in Beh_{NS}(p)$. We thus know there exists $\sigma' \in FinalConf$ such that $\sigma \Downarrow_{\overline{\tau}} \sigma'$.

Analogous to the corresponding case in Theorem 12 ($\mathcal{S}$ SE: Behaviour of non-speculative and oracle semantics) by using Lemma 23 ($\mathcal{J}$ SE: Completeness of the speculative semantics).

We thus have $(p,\sigma)\ \Omega^{O}_{\mathcal{J}}\ \overline{\tau}' \cdot \overline{\tau}'' \in Beh^{O}_{\mathcal{J}}(p)$, where $\overline{\tau}''\upharpoonright_{ns} = \varepsilon$.

□

I.2 Soundness

Lemma 19 ($\mathcal{J}$ SE: Soundness of the speculative semantics w.r.t. non-speculative semantics). *If*

(1) $X_{\mathcal{J}}.\sigma = \sigma$ and

(2) $\vdash_O X_{\mathcal{J}}$: noongoing and

(3) $X_{\mathcal{J}} \overset{O}{\rightsquigarrow}{}^{\mathcal{J}}_{\overline{\tau}} X'_{\mathcal{J}}$

Then there exists σ' such that

I if $\vdash_O X'_J$*: noongoing then* $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}\sigma'}$ *and* $X'_J.\sigma = \sigma'$ *and*

II if $\vdash^i_O X'_J$*: 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 $X_J \overset{O}{\leadsto}{}^J_{\overline{\tau}} X'_J$

Rule J:Reflection Then we have $X_J \overset{O}{\leadsto}{}^J_{\varepsilon} X_J$ with $X'_J = X_J$ and by Rule NS-Reflection we have

I $\sigma \Downarrow_{\varepsilon\upharpoonright_{ns}} \sigma'$ with $\sigma = \sigma'$.

II $\sigma \Downarrow_{helper(\varepsilon,i)} \sigma'$ with $\sigma = \sigma'$.

Rule J:Single We have $X_J \overset{O}{\leadsto}{}^J_{\overline{\tau}'\cdot\tau} X'_J$ and by Rule J:Single we get $X_J \overset{O}{\leadsto}{}^J_{\overline{\tau}'} X''_J$ and $X''_J \overset{\tau}{\rightsquigarrow}{}^O_S X'_J$.

We need to proof

I if $\vdash_O X'_J$: *noongoing* then $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ and $X'_J.\sigma = \sigma'$

II if $\vdash^i_O X'_J$: *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 $X_J \overset{O}{\leadsto}{}^J_{\overline{\tau}'} X''_J$ and have a σ'' where σ'' is the configuration for some instance in X''_J such that.

I' if $\vdash_O X''_J$: *noongoing* then $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}\sigma''}$ and $X''_J.\sigma = \sigma''$

II' if $\vdash^j_O X''_J$: *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''_J.

no ongoing transactions in X''_J Then X''_J has no ongoing transactions, meaning $\vdash_O X''_J$: *noongoing* and we have $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}} \sigma''$ and $X''_J.\sigma = \sigma''$ by IH.

I Then $\vdash_O X'_J$: *noongoing* and we need to prove $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ and $X'_J.\sigma = \sigma'$. We now proceed by inversion on $X''_J \overset{\tau}{\rightsquigarrow}{}^O_J X'_J$:

Rule J:Rollback Analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

Rule J:Spec The contradiction is analogous to the case of Rule S:Store-Skip in Lemma 45 (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 $\sigma'' = X''_J.\sigma$. Since $\vdash_O X''_J$: *noongoing*, there no ongoing transactions that need to be rolled back.

Furthermore, no transaction that will be rolled back is created in the step $X''_J \overset{\tau}{\rightsquigarrow}{}^O_J X'_J$, because $\vdash_O X'_J$: *noongoing*.

The case is analogous to Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) by using Lemma 20 (J SE: Soundness single step No Speculation).

II Then X'_J has ongoing transactions, meaning $\vdash^i_O X'_J$: *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 $X''_J \overset{\tau}{\rightsquigarrow}{}^O_J X'_J$:

Rule $\mathcal{J}$:Spec Since we know a new transaction was created that will be rolled back, we also know that $id = i$.

We know that, because $\vdash_O X''_{\mathcal{J}}$: *noongoing*, so there was not another ongoing transaction.

The case is analogous to Lemma 45 ($\mathcal{S}$ SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) together with Lemma 22 ($\mathcal{J}$ SE: Single Step Speculation).

otherwise By definition of $\vdash^i_O X'_{\mathcal{J}}$: *biggestongoingtransactionirolledback* we know that there exists a $\texttt{rlb}_{\mathcal{J}}\ i$ in the execution $X'_{\mathcal{J}} \overset{O}{\underset{\overline{\tau}_{fin}}{\leadsto}}{}^{\mathcal{J}} X_{\mathcal{J}fin}$ 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 45 ($\mathcal{S}$ SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

ongoing transactions in $X''_{\mathcal{J}}$ Then $X''_{\mathcal{J}}$ has ongoing transactions, meaning $\vdash^j_O X''_{\mathcal{J}}$: *biggestongoingtransactionirolledback* and we have $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$ and σ'' is the configuration for the instance with $ctr = j$.

I Then $\vdash_O X'_{\mathcal{J}}$: *noongoing* and we need to prove $\sigma \Downarrow_{\overline{\tau}\cdot\tau\restriction_{ns}\sigma'}$ and $X'_{\mathcal{J}}.\sigma = \sigma'$. We now proceed by inversion on $X''_{\mathcal{J}} \overset{\tau}{\leadsto}{}^O_{\mathcal{J}} X'_{\mathcal{J}}$:

Rule $\mathcal{J}$:Rollback and $\tau = \texttt{rlb}_{\mathcal{J}}\ j$ 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 45 ($\mathcal{S}$ SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Then $\tau \neq \texttt{rlb}_{\mathcal{J}}\ j$.

Deriving the contradiction is analogous to the corresponding case in Lemma 45 ($\mathcal{S}$ SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

II Then $\vdash^i_O X'_{\mathcal{J}}$: *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 $X''_{\mathcal{J}} \overset{\tau}{\leadsto}{}^O_{\mathcal{J}} X'_{\mathcal{J}}$:

Rule $\mathcal{J}$:Rollback Then $\tau = \texttt{rlb}_{\mathcal{J}}\ id$. We do a case analysis if $id = j$ or not.

$id = j$ Contradiction, analogous to the corresponding case in Lemma 45 ($\mathcal{S}$ SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

$id \neq j$ Analogous to the corresponding case in Lemma 45 ($\mathcal{S}$ SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Then $\tau \neq \texttt{rlb}_{\mathcal{J}}\ id$.

Then $helper(\overline{\tau} \cdot \tau, i) = helper(\overline{\tau}, i)$

We choose $\sigma' = \sigma''$ and derive a step by Rule NS-Reflection.

The rest is analogous to Lemma 45 ($\mathcal{S}$ SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

□

Lemma 20 ($\mathcal{J}$ SE: Soundness single step No Speculation). *If*

(1) $\vdash_O X_{\mathcal{J}}$: *noongoing and*
(2) $X_{\mathcal{J}} \overset{\tau}{\leadsto}{}^O_{\mathcal{J}} X'_{\mathcal{J}}$ *and*
(3) $\vdash_O X'_{\mathcal{J}}$: *noongoing and*
(4) $\sigma = X_{\mathcal{J}}.\sigma$

Then there exists σ' *such that*

I $\sigma \Downarrow_{\tau\restriction_{ns}} \sigma'$ *and*
II $X'_{\mathcal{J}}.\sigma = \sigma'$

Proof. We proceed by inversion on $X_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}}$:

Rule $\mathcal{J}$:General Thus, we have $X_{\mathcal{J}} = \overline{\Psi}_{\mathcal{J}} \cdot \Psi_{\mathcal{J}_{\overline{\rho}\cdot\tau}}$ and $X'_{\mathcal{J}} = \overline{\Psi}_{\mathcal{J}} \cdot \Psi_{\mathcal{J}_{\overline{\rho}}}$ with $\Psi_{\mathcal{J}}.\sigma = \sigma$.

By the definition of $\overset{\tau}{\rightsquigarrow}{}^{O}_{S}$ only Rule $\mathcal{J}$:Spec and Rule $\mathcal{J}$:Spec-Exe add observations to $\overline{\rho}$.

These observations are either `start` *id* or `bypass` *n*.

By the definition of $\restriction_{ns}$, we have $\tau\restriction_{ns} = \varepsilon$.

Thus, we have $\sigma \Downarrow_{\varepsilon\restriction_{ns}} \sigma$ by Rule NS-Reflection.

Rule $\mathcal{J}$: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 $X_{\mathcal{J}}.\sigma = X'_{\mathcal{J}}.\sigma$ and with this we get $X'_{\mathcal{J}}.\sigma = \sigma$.

Thus, we can derive $\sigma \Downarrow_{\texttt{commit}\ id\restriction_{ns}} \sigma$.

Rule $\mathcal{J}$:Rollback Contradiction, since $\vdash_O X_{\mathcal{J}}$: *noongoing* and Definition 18 (Well orderedness of rollback and start).

Rule $\mathcal{J}$:SE-Context We have $X_{\mathcal{J}} = \overline{\Psi}_{\mathcal{J}} \cdot \Psi_{\mathcal{J}}$ and $X'_{\mathcal{J}} = \overline{\Psi}''_{\mathcal{J}} \cdot \overline{\Psi}'_{\mathcal{J}}$ with $\Psi_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} \overline{\Psi}'_{\mathcal{J}}$. By Lemma 21 ($\mathcal{J}$ SE: Single Step Instance Non Speculative) we have $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ with $\sigma = \Psi_{\mathcal{J}}.\sigma$ and $\overline{\Psi}'_{\mathcal{J}}.\sigma = \sigma'$.

□

Lemma 21 ($\mathcal{J}$ SE: Single Step Instance Non Speculative)**.** *If*

(1) $X_{\mathcal{J}} = \overline{\Psi}_{\mathcal{J}} \cdot \Psi_{\mathcal{J}}$ *and*
(2) $X'_{\mathcal{J}} = \overline{\Psi}_{\mathcal{J}} \cdot \overline{\Psi}'_{\mathcal{J}}$ *and* $\vdash_O X'_{\mathcal{J}}$: *noongoing and*
(3) $\Psi_S \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} \overline{\Psi}'_{\mathcal{J}}$ *and*
(4) $\sigma = \Psi_{\mathcal{J}}.\sigma$

Then there is a σ' *such that*

I $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ *and*
II $\overline{\Psi}'_{\mathcal{J}}.\sigma = \sigma$

Proof. We proceed by case analysis on the rule used to derive $\Psi_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} \Psi'_{\mathcal{J}}$.

Rule $\mathcal{J}$:barr or Rule $\mathcal{J}$:barr-spec Thus, we have $p(\sigma(\mathbf{pc})) \neq \mathbf{jmp}$ and $n \neq 0$. We show the proof for Rule $\mathcal{J}$:barr, the proof for Rule $\mathcal{J}$:barr-spec is analogous.

By Rule $\mathcal{J}$:barr we know $\sigma \xrightarrow{\tau} \sigma'$ and $\Psi'_{\mathcal{J}} = \langle p, ctr, \sigma', h, n-1\rangle$.

Thus $\sigma' = \Psi'_{\mathcal{J}}.\sigma$ and $\tau = \varepsilon = \varepsilon\restriction_{ns}$.

Rule $\mathcal{J}$:NoSpec We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule and $\Psi'_{\mathcal{J}} = \langle p, ctr, \sigma', h, n-1\rangle$.

Thus, $\sigma' = \Psi'_{\mathcal{J}}.\sigma$.

Because the rule used the observation received from the step $\sigma \xrightarrow{\tau} \sigma'$, we have $\tau\restriction_{ns} = \tau$ and are finished.

Rule $\mathcal{J}$:Spec Contradiction, because there are no ongoing transactions in $X'_{\mathcal{J}}$ by the fact $\vdash_O X'_{\mathcal{J}}$: *noongoing*.

Rule $\mathcal{J}$:Spec-Exe By definition $\overline{\Psi}'_4 = \langle p, ctr, \sigma', h, n\rangle \cdot \langle p, ctr', \sigma', h', n'\rangle_{\overline{\rho}}$. 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 $\overline{\Psi}'_4.\sigma = \sigma'$.

□

Lemma 22 ($\mathcal{J}$SE: Single Step Speculation)**.** *If*

(1) $X_{\mathcal{J}} = \overline{\Psi}_{\mathcal{J}} \cdot \Psi_{\mathcal{J}}$ *and* $\vdash_{O} X_{\mathcal{J}}$: *noongoing*
(2) $X'_{\mathcal{J}} = \overline{\Psi}_{\mathcal{J}} \cdot \overline{\Psi}'_{\mathcal{J}}$ *and* $\vdash^{i}_{O} X'_{\mathcal{J}}$: *biggestongoingtransactionirolledback and*
(3) $\Psi_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} \overline{\Psi}'_{\mathcal{J}}$ *and*
(4) $\sigma = \Psi_{\mathcal{J}}.\sigma$

Then

I $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma'$ *and*
II σ' *is the configuration for the instance with* $ctr = i$ *in* $X'_{\mathcal{J}}$

Proof. We proceed by inversion on $\Psi_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} \overline{\Psi}'_{\mathcal{J}}$:

Rule $\mathcal{J}$:AM-Spec Then we have

$$\frac{\sigma \xrightarrow{\tau} \sigma'}{\overline{\Psi}'_{\mathcal{J}} = \langle p, ctr, \sigma', n\rangle \cdot \Psi'^{\,l}_{\mathcal{J}\,\texttt{pc}\ \sigma'(\mathbf{pc})\cdot \texttt{start}_{\mathcal{J}}\ ctr}}$$

We have $\sigma \xrightarrow{\tau} \sigma'$.
Since $\vdash_{O} X_{\mathcal{J}}$: *noongoing* we know that $\tau\upharpoonright_{ns} = \tau = \texttt{pc}\ \sigma'(\mathbf{pc})$.
Since a transaction with $id = ctr$ was started and we have $\vdash_{O} X_{\mathcal{J}}$: *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 $\vdash_{O} X_{\mathcal{J}}$: *noongoing* and $\vdash^{i}_{O} X'_{\mathcal{J}}$: *biggestongoingtransactionirolledback*, we know that a transaction has to be started that will be rolled back.

□

I.3 Completeness

Lemma 23 ($\mathcal{J}$SE: Completeness of the speculative semantics)**.** *If*

(1) $\sigma \in InitConf$ *and*
(2) $\sigma \Downarrow_{\overline{\tau}} \sigma'$ *and*
(3) $X_{\mathcal{J}} = X^{init}_{\mathcal{J}}(\sigma)$

Then

I $X_{\mathcal{J}} \overset{O}{\leadsto}{}^{\mathcal{J}}_{\overline{\tau}'} X'_{\mathcal{J}\,\rho}$ *and*
II $\vdash_{O} X'_{\mathcal{J}}$: *noongoing and*
III $\sigma' = X'_{\mathcal{J}}.\sigma$ *and*
IV $\overline{\tau} = \overline{\tau}'\upharpoonright_{ns}$ *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 $\mathcal{J}$:Reflection we have $X_{\mathcal{J}} \overset{O}{\leadsto}{}^{\mathcal{J}}_{\varepsilon} X_{\mathcal{J}}$.

By construction $\vdash_O X_{\mathcal{J}}$: *noongoing* and $X_{\mathcal{J}}.\sigma = \sigma$.

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 $X_{\mathcal{J}} \overset{O}{\leadsto}{}^{\mathcal{J}}_{\overline{\tau}' \cdot \tau'} X'_{\mathcal{J}}$ and

II $\vdash_O X'_{\mathcal{J}}$: *noongoing* and

III $\sigma' = X'_{\mathcal{J}}.\sigma$ 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' $X_{\mathcal{J}} \overset{O}{\leadsto}{}^{\mathcal{J}}_{\overline{\tau}'} X''_{\mathcal{J}\,\rho}$ and

II' $\vdash_O X''_{\mathcal{J}\,\rho}$: *noongoing* and

III' $\sigma'' = X''_{\mathcal{J}}.\sigma$ and

IV' $\overline{\tau} = \overline{\tau}' \restriction_{ns}$

V' $\rho = \varepsilon$

To account for possible outstanding commits, we use Lemma 9 (Executing a chain of commits) on $X''_{\mathcal{J}}$ and get

a) $X''_{\mathcal{J}} \overset{O}{\leadsto}{}^{\mathcal{J}}_{\overline{\tau}'''} X'''_{\mathcal{J}}$

b) $minWndw(X'''_{\mathcal{J}}) > 0$

c) $\forall \tau \in \overline{\tau}'''.\ \tau = \texttt{commit}\ id$ for some $id \in \mathbb{N}$

d) $X''_{\mathcal{J}}.\sigma = X'''_{\mathcal{J}}.\sigma$

By c) and the definition of $\restriction_{ns}$ we have $\overline{\tau}''' \restriction_{ns} = \varepsilon$.

Because only Rule $\mathcal{J}$:Commit was used we have $X'''_{\mathcal{J}\,\rho} = X''_{\mathcal{J}\,\rho}$. We now do a case analysis on the instruction $p(\sigma''(\mathbf{pc}))$:

$p(\sigma''(\mathbf{pc})) \neq \mathbf{jmp}$ Then either Rule $\mathcal{J}$:barr, Rule $\mathcal{J}$:barr-spec or Rule $\mathcal{J}$:NoSpec in conjunction with Rule $\mathcal{J}$:SE-Context was used to derive the step $X'''_{\mathcal{J}} \overset{\tau'}{\rightsquigarrow}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}}$.

Here, τ' is generated from $X'''_{\mathcal{J}}.\sigma \xrightarrow{\tau'} \sigma'$ and $X'_{\mathcal{J}}.\sigma = \sigma'$ Analogous to the corresponding case in Lemma 100 (SLS SE: Completeness of the speculative semantics).

$p(\sigma''(\mathbf{pc})) = \mathbf{jmp}$ Then depending on the oracle decision, either Rule $\mathcal{J}$:Spec or Rule $\mathcal{J}$:Spec-Exe is used in conjunction with Rule $\mathcal{J}$:SE-Context:

$O(p, n, h) = (l, \omega)$ **(Rule $\mathcal{J}$:Spec-Exe)** Then we jump to the original target.

We derive $X''_{\mathcal{J}} \overset{\tau \cdot \texttt{start}_{\mathcal{J}}\ id}{\rightsquigarrow}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}}$ by using Rule $\mathcal{J}$:Spec-Exe and produce the observation $\tau' = \tau$, where $\tau = \texttt{pc}\ l \in Obs$.

Analogous to the corresponding case in Lemma 100 (SLS SE: Completeness of the speculative semantics).

$O(p, n, h) = (l', \omega)$ **(Rule $\mathcal{J}$:Spec)** Then we jump to a different target l'. We derive a step by using Rule $\mathcal{J}$:Spec. This produces the observation τ'', where $\tau'' = \texttt{pc}\ l$ and the step $X'''_{\mathcal{J}}.\sigma \xrightarrow{\tau''} \sigma'''$ is made.

Analogous to the corresponding case in Lemma 100 (SLS SE: Completeness of the speculative semantics).

Notice that ρ is empty for all the cases, because we discharge all the observations immediately using Rule $\mathcal{J}$:General.

□

Lemma 24 ($\mathcal{J}$ SE: Non-speculative execution for rolled back transactions.). *If*

(1) $X_{\mathcal{J}} \overset{O}{\rightsquigarrow}{}^{\mathcal{J}}_{\overline{\tau}} X'_{\mathcal{J}}$ *and*

(2) $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$ *and*

(3) $\sigma = X_{\mathcal{J}}.\sigma$

Then

I *there is a configurations* σ' *with* $X'_{\mathcal{J}}.\sigma = \sigma'$ *and*

II $\sigma \xrightarrow{\overline{\tau}\upharpoonright_{ns}} \sigma'$ *and*

III $\overline{\tau}\upharpoonright_{ns} = \tau$

Proof. Let $X_{\mathcal{J}} \overset{O}{\rightsquigarrow}{}^{\mathcal{J}}_{\overline{\tau}} X'_{\mathcal{J}}$ be an execution with trace $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$. Let $\sigma = X_{\mathcal{J}}.\sigma$

We know Rule $\mathcal{J}$:Spec 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 $\upharpoonright_{ns}$ we have $\overline{\tau}\upharpoonright_{ns} = \tau\upharpoonright_{ns} = \tau$, where the last steps is because of the fact $\tau \in Obs$.

Thus, we have $\sigma \xrightarrow{\overline{\tau}\upharpoonright_{ns}} \sigma'$.

Now we need to show that $\sigma' = X'_{\mathcal{J}}.\sigma$, which is analogous to Lemma 50 (S SE: Non-speculative execution for rolled back transactions). □

I.4 $\mathcal{J}$: Relating Non-speculative and AM Semantics

Theorem 8 ($\mathcal{J}$: Behaviour of non-speculative semantics and AM semantics)

Lemma 28 ($\mathcal{J}$ AM: Completeness of the speculative AM semantics)

Lemma 25 ($\mathcal{J}$ AM : Soundness of the AM semantics w.r.t. non-speculative semantics)

Lemma 29 ($\mathcal{J}$ AM: Non-speculative execution for rolled back transactions)

Lemma 26 ($\mathcal{J}$ AM: Soundness single step No Speculation)

Lemma 27 ($\mathcal{J}$ AM: Single Step Speculation)

Theorem 8 ($\mathcal{J}$: Behaviour of non-speculative semantics and AM semantics). *Let p be a program. Then* $Beh_{NS}(p) = Beh^{\omega}_{\mathcal{J}}(p)\upharpoonright_{ns}$

Proof. The proposition can be proven in similar fashion to Theorem 12 (S SE: Behaviour of non-speculative and oracle semantics). We prove the two directions separately:

$\Leftarrow$ Assume that $\overline{\tau} \in Beh^{\omega}_{\mathcal{J}}(p)$.

By the definition of $Beh^{\omega}_{\mathcal{J}}(p)$ we have an initial configuration σ such that $(p, \sigma) \Downarrow^{\omega}_{\mathcal{J}} \overline{\tau}$.

The proof proceeds in similar fashion to the analogous case in Theorem 7 ($\mathcal{J}$ SE: Behaviour of non-speculative and oracle semantics) by using Lemma 51 ($\mathcal{S}$ AM : Soundness of the AM semantics w.r.t. non-speculative semantics).

We can now conclude that $((p, \sigma))\, ⍾_{NS} \overline{\tau}\upharpoonright_{ns} \in Beh_{NS}(p)$ by Rule NS-Trace.

$\Rightarrow$ Assume that $((p, \sigma))\, ⍾_{NS} \overline{\tau} \in Beh_{NS}(p)$.

We thus know there exists $\sigma' \in \mathit{FinalConf}$ such that $\sigma \Downarrow_{\overline{\tau}} \sigma'$.

We apply Lemma 28 ($\mathcal{J}$ AM: Completeness of the speculative AM semantics) with $\Sigma_{\mathcal{J}} = \Sigma^{init}_{\mathcal{J}} p, \sigma$ and get $\Sigma^{init}_{\mathcal{J}} p, \sigma \Downarrow^{\overline{\tau}'}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$ with $\vdash_O \Sigma'_{\mathcal{J}}$: *noongoing*, $\sigma' = \Sigma'_{\mathcal{J}}.\sigma$ and $\overline{\tau} = \overline{\tau}'\upharpoonright_{ns}$.

Because of $\vdash_O \Sigma'_{\mathcal{J}}$: *noongoing* and $\sigma' = \Sigma'_{\mathcal{J}}.\sigma$ we know that $\vdash \Sigma'_{\mathcal{J}}$: *fin*.

We thus have $(p, \sigma)\, ⍾^{\omega}_{\mathcal{J}}\, \overline{\tau}' \in Beh^{\omega}_{\mathcal{J}}(p)$.

□

I.4.1 Soundness.

Lemma 25 ($\mathcal{J}$ AM : Soundness of the AM semantics w.r.t. non-speculative semantics)**.** *If*

(1) $\Sigma_{\mathcal{J}}.\sigma = \sigma$ *and*
(2) $\vdash_O \Sigma_{\mathcal{J}}$: *noongoing and*
(3) $\Sigma_{\mathcal{J}} \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$

Then there exists σ' *such that*

I *if* $\vdash_O \Sigma'_{\mathcal{J}}$: *noongoing then* $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}\sigma'}$ *and* $\Sigma'_{\mathcal{J}}.\sigma = \sigma'$ *and*

II *if* $\vdash^i_O \Sigma'_{\mathcal{J}}$: *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 $\Sigma_{\mathcal{J}} \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$

Rule $\mathcal{J}$:AM-Reflection Then we have $\Sigma_{\mathcal{J}} \Downarrow^{\varepsilon}_{\mathcal{J}} \Sigma_{\mathcal{J}}$ with $\Sigma'_{\mathcal{J}} = \Sigma_{\mathcal{J}}$ and by Rule NS-Reflection we have

I $\sigma \Downarrow_{\varepsilon\upharpoonright_{ns}} \sigma'$ with $\sigma = \sigma'$.
II $\sigma \Downarrow_{helper(\varepsilon,i)} \sigma'$ with $\sigma = \sigma'$.

Rule $\mathcal{J}$:AM-Single We have $\Sigma_{\mathcal{J}} \Downarrow^{\overline{\tau}'\cdot\tau}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$ and by Rule $\mathcal{J}$:AM-Single we get $\Sigma_{\mathcal{J}} \Downarrow^{\overline{\tau}'}_{\mathcal{J}} \Sigma''_{\mathcal{J}}$ and $\Sigma''_{\mathcal{J}} \xrightarrow{\tau}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$.

We need to prove

I if $\vdash_O \Sigma'_{\mathcal{J}}$: *noongoing* then $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ and $\Sigma'_{\mathcal{J}}.\sigma = \sigma'$

II if $\vdash^i_O \Sigma'_{\mathcal{J}}$: *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 $\Sigma_{\mathcal{J}} \Downarrow^{\overline{\tau}'}_{\mathcal{J}} \Sigma''_{\mathcal{J}}$ and have a σ'' where σ'' is the configuration for some instance in $\Sigma''_{\mathcal{J}}$ such that.

I' if $\vdash_O \Sigma''_{\mathcal{J}}$: *noongoing* then $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}\sigma''}$ and $\Sigma''_{\mathcal{J}}.\sigma = \sigma''$

II' if $\vdash^j_O \Sigma''_{\mathcal{J}}$: *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 $\Sigma''_{\mathcal{J}}$.

no ongoing transactions in $\Sigma''_{\mathcal{J}}$ Then $\Sigma''_{\mathcal{J}}$ has no ongoing transactions, meaning $\vdash_O \Sigma''_{\mathcal{J}} : noongoing$ and we have $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}} \sigma''$ and $\Sigma''_{\mathcal{J}}.\sigma = \sigma''$ by IH.

I Then $\vdash_O \Sigma'_{\mathcal{J}}$: *noongoing* and we need to prove $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ and $\Sigma'_{\mathcal{J}}.\sigma = \sigma'$. We now proceed by inversion on $\Sigma''_{\mathcal{J}} \xrightarrow{\tau}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$:

Rule $\mathcal{J}$:AM-Rollback Then $\tau = \texttt{rlb}_{\mathcal{J}}\ id$.

Contradiction. Analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

Rule $\mathcal{J}$:AM-Spec Contradiction. Analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise We know that $\sigma'' = \Sigma''_{\mathcal{J}}.\sigma$.

Furthermore, no transaction that will be rolled back is created in the step $\Sigma''_{\mathcal{J}} \xrightarrow{\tau}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$, because $\vdash_O \Sigma'_{\mathcal{J}}$: *noongoing*.

We can now apply Lemma 26 ($\mathcal{J}$ AM: Soundness single step No Speculation) with $\Sigma''_{\mathcal{J}} \xrightarrow{\tau}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$ and get

$$\sigma'' \Downarrow_{\tau\upharpoonright_{ns}} \sigma'$$
$$\Sigma'_{\mathcal{J}}.\sigma = \sigma'$$

Since $\overline{\tau}\upharpoonright_{ns} \cdot \tau\upharpoonright_{ns} = \overline{\tau} \cdot \tau\upharpoonright_{ns}$ (because $\tau \neq \texttt{rlb}_{\mathcal{J}}\ id$), we are finished.

II Then $\Sigma'_{\mathcal{J}}$ has ongoing transactions, meaning $\vdash^i_O \Sigma'_{\mathcal{J}}$: *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 $\Sigma''_{\mathcal{J}} \xrightarrow{\tau}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$:

Rule $\mathcal{J}$:AM-Spec Analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) together with Lemma 27 ($\mathcal{J}$ AM: Single Step Speculation).

otherwise By definition of $\vdash^i_O \Sigma'_{\mathcal{J}}$: *biggestongoingtransactionirolledback* we know that there exists a $\texttt{rlb}_{\mathcal{J}}\ i$ in the execution $\Sigma'_{\mathcal{J}} \Downarrow^{\overline{\tau}_{fin}}_{\mathcal{J}} \Sigma_{\mathcal{J}fin}$ with no matching $\texttt{start}_{\mathcal{J}}\ i$ observation in that execution. Contradiction, analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

ongoing transactions in $\Sigma''_{\mathcal{J}}$ Then $\Sigma''_{\mathcal{J}}$ has ongoing transactions, meaning $\vdash^j_O \Sigma''_{\mathcal{J}}$: *biggestongoingtransactionirolledback* and we have $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$ and σ'' is the configuration for the instance with $ctr = j$.

I Then $\vdash_O \Sigma'_{\mathcal{J}}$: *noongoing* and we need to prove $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ and $\Sigma'_{\mathcal{J}}.\sigma = \sigma'$. We now proceed by inversion on $\Sigma''_{\mathcal{J}} \xrightarrow{\tau}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$:

Rule $\mathcal{J}$:AM-Rollback and $\tau = \texttt{rlb}_{\mathcal{J}}\ j$ Choose $\sigma' = \sigma''$. Analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Then $\tau \neq \texttt{rlb}_{\mathcal{J}}\ j$.

Contradiction, analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

II Then $\vdash^i_O \Sigma'_{\mathcal{J}}$: *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 $\Sigma''_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$:

Rule $\mathcal{J}$:AM-Rollback Then $\tau = \texttt{rlb}\ id$. We do a case analysis if $id = j$ or not.

$id = j$ Contradiction, analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

$id \neq j$ Analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Then $\tau \neq \texttt{rlb}_{\mathcal{J}}\ id$.

Then $helper(\overline{\tau} \cdot \tau, i) = helper(\overline{\tau}, i)$

We choose $\sigma' = \sigma''$ and derive a step by Rule NS-Reflection.

The rest is analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

$\square$

Lemma 26 ($\mathcal{J}$ AM: Soundness single step No Speculation)**.** *If*

(1) $\vdash_O \Sigma_{\mathcal{J}}$: *noongoing and*
(2) $\Sigma_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$ *and*
(3) $\vdash_O \Sigma'_{\mathcal{J}}$: *noongoing and*
(4) $\sigma = \Sigma_{\mathcal{J}}.\sigma$

Then there exists σ' *such that*

I $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ *and*
II $\Sigma'_{\mathcal{J}}.\sigma = \sigma'$

Proof. We proceed by inversion on $\Sigma_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$:

Rule $\mathcal{J}$:AM-General Thus, we have $\Sigma_{\mathcal{J}} = \overline{\Phi}_{\mathcal{J}} \cdot \Phi_{\mathcal{J}\overline{\rho}' \cdot \tau}$. Contradiction. By the definition of $\overset{\tau}{\rightsquigarrow}_{\mathcal{J}}$ only Rule $\mathcal{J}$:AM-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 $\vdash_O \Sigma_{\mathcal{J}}$: *noongoing*.

Rule $\mathcal{J}$:AM-Rollback Contradiction, since $\vdash_O \Sigma_{\mathcal{J}}$: *noongoing* and Definition 18 (Well orderedness of rollback and start).

Rule $\mathcal{J}$:AM-Context We have $\Sigma_{\mathcal{J}} = \overline{\Phi}_{\mathcal{J}} \cdot \Phi_{\mathcal{J}}$ and $\Sigma'_{\mathcal{J}} = \overline{\Phi}''_{\mathcal{J}} \cdot \overline{\Phi}'_{\mathcal{J}}$ with $\Phi_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \overline{\Phi}'_{\mathcal{J}}$.

We proceed by case analysis on the rule used to derive $\Phi_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Phi'_{\mathcal{J}}$.

Rule $\mathcal{J}$:AM-Spec Contradiction, because this starts a speculative transaction that needs to be rolled back. This cannot happen because of $\vdash_O \Sigma'_{\mathcal{J}}$: *noongoing*.

Rule $\mathcal{J}$:AM-barr or Rule $\mathcal{J}$:AM-barr-spec Thus, we have $p(\sigma(\mathbf{pc})) \neq \mathbf{jmp}$ and $n \neq 0$. We show the proof for Rule $\mathcal{J}$:AM-barr, the proof for Rule $\mathcal{J}$:AM-barr-spec is analogous.

By Rule $\mathcal{J}$:AM-barr we know $\sigma \xrightarrow{\varepsilon} \sigma'$ and $\overline{\Phi}'_{\mathcal{J}} = \langle p, ctr, \sigma', n-1 \rangle$.

Thus $\sigma' = \overline{\Phi}'_{\mathcal{J}}.\sigma$ and $\tau = \varepsilon = \varepsilon\restriction_{ns}$.

Thus, we have an execution $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ and $\sigma' = \Sigma'_{\mathcal{J}}.\sigma$ as needed.

Rule $\mathcal{J}$:AM-NoSpec Thus, we have $p(\sigma(\mathbf{pc})) \neq \mathbf{jmp}$ and $n \neq 0$. We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule Rule $\mathcal{J}$:AM-NoSpec and $\overline{\Phi}'_{\mathcal{J}} = \langle p, ctr, \sigma', n-1 \rangle$.
Thus, choose $\sigma' = \overline{\Phi}'_{\mathcal{J}}.\sigma$.
Because the rule used the observation received from the derived step $\sigma \xrightarrow{\tau} \sigma'$, we already get $\tau\restriction_{ns} = \tau$ and are finished.

□

Lemma 27 ($\mathcal{J}$ AM: Single Step Speculation). *If*

(1) $\Sigma_{\mathcal{J}} = \overline{\Phi}_{\mathcal{J}} \cdot \Phi_{\mathcal{J}}$ *and* $\vdash_O \Sigma_{\mathcal{J}}$: *noongoing*
(2) $\Sigma'_{\mathcal{J}} = \overline{\Phi}_{\mathcal{J}} \cdot \overline{\Phi}'_{\mathcal{J}}$ *and* $\vdash^i_O \Sigma'_{\mathcal{J}}$: *biggestongoingtransactionirolledback and*
(3) $\Phi_{\mathcal{J}} \overset{\tau}{\leadsto}_{\mathcal{J}} \overline{\Phi}'_{\mathcal{J}}$ *and*
(4) $\sigma = \Phi_{\mathcal{J}}.\sigma$

Then

I $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ *and*
II σ' *is the configuration for the instance with ctr* $= i$ *in* $\Sigma'_{\mathcal{J}}$

Proof. We proceed by inversion on $\Phi_{\mathcal{J}} \overset{\tau}{\leadsto}_{\mathcal{J}} \overline{\Phi}'_{\mathcal{J}}$:

Rule $\mathcal{J}$:AM-Spec Then we have

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

$$\overline{\Phi}'_{\mathcal{J}} = \langle p, ctr, \sigma', n \rangle \cdot \overline{\Phi}'_{\mathcal{J}}$$

We have $\sigma \xrightarrow{\tau} \sigma'$.
Since $\vdash_O \Sigma_{\mathcal{J}}$: *noongoing* we know that $\tau\restriction_{ns} = \tau = \mathsf{pc}\ n$.
Since a transaction with $id = ctr$ was started and we have $\vdash_O \Sigma_{\mathcal{J}}$: *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 $\vdash_O \Sigma_{\mathcal{J}}$: *noongoing* and $\vdash^i_O \Sigma'_{\mathcal{J}}$: *biggestongoingtransactionirolledback*, we know that a transaction has to be started that will be rolled back.

□

I.4.2 Completeness.

Lemma 28 ($\mathcal{J}$ AM: Completeness of the speculative AM semantics). *If*

(1) $\sigma \in InitConf$ *and*
(2) $\sigma \Downarrow_{\overline{\tau}} \sigma'$ *and*
(3) $\Sigma_{\mathcal{J}} = \Sigma^{init}_{\mathcal{J}}\sigma$

Then

I $\Sigma_{\mathcal{J}} \Downarrow^{\overline{\tau}'}_{\mathcal{J}} \Sigma'_{\mathcal{J}_\rho}$ *and*
II $\vdash_O \Sigma'_{\mathcal{J}}$: *noongoing and*
III $\sigma' = \Sigma'_{\mathcal{J}}.\sigma$ *and*

IV $\overline{\tau} = \overline{\tau}' \upharpoonright_{ns}$ *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 $\mathcal{J}$:AM-Reflection we have $\Sigma_{\mathcal{J}} \Downarrow_{\mathcal{J}}^{\varepsilon} \Sigma_{\mathcal{J}}$. By construction $\vdash_O \Sigma_{\mathcal{J}}$: *noongoing* and $\Sigma_{\mathcal{J}}.\sigma = \sigma$. Since $\varepsilon \upharpoonright_{ns} = \varepsilon$ we are finished.

Rule NS-Single Then we have $\sigma \Downarrow_{\overline{\tau}} \sigma''$ and $\sigma'' \xrightarrow{\tau} \sigma'$.

We need to show

I $\Sigma_{\mathcal{J}} \Downarrow_{\mathcal{J}}^{\overline{\tau}' \cdot \tau'} \Sigma'_{\mathcal{J}}$ and

II $\vdash_O \Sigma'_{\mathcal{J}}$: *noongoing* and

III $\sigma' = \Sigma'_{\mathcal{J}}.\sigma$ and

IV $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \upharpoonright_{ns}$

We apply the IH on $\sigma \Downarrow_{\overline{\tau}} \sigma''$ we get

I' $\Sigma_{\mathcal{J}} \Downarrow_{\mathcal{J}}^{\overline{\tau}'} \Sigma''_{\mathcal{J}\,\rho}$ and

II' $\vdash_O \Sigma''_{\mathcal{J}\,\rho}$: *noongoing* and

III' $\sigma'' = \Sigma''_{\mathcal{J}}.\sigma$ and

IV' $\overline{\tau} = \overline{\tau}' \upharpoonright_{ns}$

V' $\rho = \varepsilon$

We now do a case analysis on the instruction $p(\sigma(\mathbf{pc}))$:

$p(\sigma(\mathbf{pc})) \neq \mathbf{jmp}$ Analogous to the corresponding case in Lemma 23 ($\mathcal{J}$ SE: Completeness of the speculative semantics).

$p(\sigma(\mathbf{pc})) = \mathbf{jmp}$ Analogous to the corresponding case Lemma 23 ($\mathcal{J}$ SE: Completeness of the speculative semantics), which is when the oracle mispredicted in the proof, together with Lemma 29 ($\mathcal{J}$ AM: Non-speculative execution for rolled back transactions).

□

Lemma 29 ($\mathcal{J}$ AM: Non-speculative execution for rolled back transactions.). *If*

(1) $\Sigma_{\mathcal{J}} \Downarrow_{\mathcal{J}}^{\overline{\tau}} \Sigma'_{\mathcal{J}}$ *and*

(2) $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$ *and*

(3) $\sigma = \Sigma_{\mathcal{J}}.\sigma$

Then there exists a configuration σ' *such that*

I $\Sigma'_{\mathcal{J}}.\sigma = \sigma'$ *and*

II $\sigma \xrightarrow{\overline{\tau}\upharpoonright_{ns}} \sigma'$ *and*

III $\overline{\tau}\upharpoonright_{ns} = \tau$

Proof. Let $\Sigma_{\mathcal{J}} \Downarrow_{\mathcal{J}}^{\overline{\tau}} \Sigma'_{\mathcal{J}}$ be an execution with trace $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$. Let $\sigma = \Sigma_{\mathcal{J}}.\sigma$.
The proof proceeds analogously to Lemma 29 ($\mathcal{J}$ AM: Non-speculative execution for rolled back transactions).

□

I.5 $\mathcal{J}$: Relating Symbolic and AM semantics

Theorem 9 ($\mathcal{J}$: Symbolic Consistency). $Beh^{\omega}_{\mathcal{J}}(p) = \mu(Beh^{S}_{\mathcal{J}}(p))$

Proof. The proof is analogous to Proposition 3 ($\mathcal{B}$: Symbolic Consistency) using Lemma 30 ($\mathcal{J}$: Soundness of the AM semantics w.r.t. symbolic semantics) and Lemma 32 ($\mathcal{J}$: Completeness of the symbolic semantics). □

Theorem 9 ($\mathcal{J}$: Symbolic Consistency)

Lemma 30 ($\mathcal{J}$: Soundness of the AM semantics w.r.t. symbolic semantics) Lemma 32 ($\mathcal{J}$: Completeness of the symbolic semantics)

Lemma 31 ($\mathcal{J}$: Soundness single step) Lemma 33 ($\mathcal{J}$: Completeness single step)

I.5.1 Soundness.

Lemma 30 ($\mathcal{J}$: Soundness of the AM semantics w.r.t. symbolic semantics). *If*

(1) $\Sigma^{S}_{\mathcal{J}} \; {}_{S}\Downarrow^{\overline{\tau_S}}_{\mathcal{J}} \; \Sigma^{S'}_{\mathcal{J}}$ *and*
(2) $\mu \vDash pthCnd(\Sigma^{S'}_{\mathcal{J}})$

Then

I $\mu(\Sigma^{S}_{\mathcal{J}}) \Downarrow^{\mu(\overline{\tau_S})}_{\mathcal{J}} \; \mu(\Sigma^{S'}_{\mathcal{J}})$

Proof. We proceed by induction on $\Sigma^{S}_{\mathcal{J}} \; {}_{S}\Downarrow^{\overline{\tau_S}}_{\mathcal{J}} \; \Sigma^{S'}_{\mathcal{J}}$

Rule $\mathcal{J}$:Sym-Reflection Then we have $\Sigma^{S}_{\mathcal{J}} \; {}_{S}\Downarrow^{\varepsilon}_{\mathcal{J}} \Sigma^{S'}_{\mathcal{J}}$ with $\Sigma^{S'}_{\mathcal{J}} = \Sigma^{S}_{\mathcal{J}}$. Using Rule $\mathcal{J}$:AM-Reflection we get $\mu(\Sigma^{S}_{\mathcal{J}}) \; {}_{S}\Downarrow^{\mu(\varepsilon)}_{\mathcal{J}} \; \mu(\Sigma^{S'}_{\mathcal{J}})$ and are finished.

Rule $\mathcal{J}$:Sym-Single We have $\Sigma^{S}_{\mathcal{J}} \; {}_{S}\Downarrow^{\overline{\tau_S}' \cdot \tau_S}_{\mathcal{J}} \; \Sigma^{S'}_{\mathcal{J}}$ and by Rule $\mathcal{J}$:Sym-Single we get $\Sigma^{S}_{\mathcal{J}} \; {}_{S}\Downarrow^{\overline{\tau_S}'}_{\mathcal{J}} \; \Sigma^{S''}_{\mathcal{J}}$ and $\Sigma^{S''}_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}^{S}_{\mathcal{J}} \Sigma^{S'}_{\mathcal{J}}$.

We need to prove

(1) $\mu(\Sigma^{S}_{\mathcal{J}}) \Downarrow^{\mu(\overline{\tau} \cdot \tau_S)}_{\mathcal{J}} \; \mu(\Sigma^{S'}_{\mathcal{J}})$

We apply the IH on $\Sigma^{S}_{\mathcal{J}} \; {}_{S}\Downarrow^{\overline{\tau_S}}_{\mathcal{J}} \; \Sigma^{S''}_{\mathcal{J}}$ and have a $\Sigma''_{\mathcal{J}} = \mu(\Sigma^{S''}_{\mathcal{J}})$ such that:

(1) $\mu(\Sigma^{S}_{\mathcal{J}}) \Downarrow^{\mu(\overline{\tau_S})}_{\mathcal{J}} \; \Sigma''_{\mathcal{J}}$ and

The result follows by applying Lemma 31 ($\mathcal{J}$: Soundness single step) on $\Sigma^{S''}_{\mathcal{J}} \overset{\tau_S}{\rightsquigarrow}^{S}_{\mathcal{J}} \; \Sigma^{S'}_{\mathcal{J}}$ and get a step $\Sigma''_{\mathcal{J}} \overset{\mu(\tau_S)}{\rightsquigarrow}_{\mathcal{J}} \mu(\Sigma^{S'}_{\mathcal{J}})$.

We now use Rule $\mathcal{J}$:AM-Single and get an execution $\mu(\Sigma^{S}_{\mathcal{J}}) \Downarrow^{\mu(\overline{\tau_S}) \cdot \mu(\tau_S)}_{\mathcal{J}} \; \mu(\Sigma^{S'}_{\mathcal{J}})$ as required.

□

Lemma 31 ($\mathcal{J}$: Soundness single step). *If*

(1) $\Sigma^{S}_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}^{S}_{\mathcal{J}} \Sigma^{S'}_{\mathcal{J}}$ *and*
(2) $\mu \vDash pthCnd(\Sigma^{S'}_{\mathcal{J}})$

Then

I $\mu(\Sigma^{S}_{\mathcal{J}}) \overset{\mu(\tau)}{\rightsquigarrow}_{\mathcal{J}} \mu(\Sigma^{S'}_{\mathcal{J}})$

Proof. We proceed by inversion on $\Sigma^{S}_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}^{S}_{\mathcal{J}} \Sigma^{S'}_{\mathcal{J}}$:

Rule $\mathcal{J}$**:Sym-Rollback** Analogous to the corresponding case in Lemma 108 (SLS: Soundness single step).

Rule $\mathcal{J}$**:Sym-Context** We then have $\Phi_{\mathcal{J}}^{\mathcal{S}} \overset{\tau}{\leadsto}_{\mathcal{J}}^{\mathcal{S}} \overline{\Phi}'_{\mathcal{J}_{\mathcal{S}}}$. Thus, we know $\Phi_{\mathcal{J}}^{\mathcal{S}}.n > 0$ and $\mu(\Phi_{\mathcal{J}}^{\mathcal{S}}).n > 0$ as well. We proceed by inversion on $\Phi_{\mathcal{J}}^{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\leadsto}_{\mathcal{J}}^{\mathcal{S}} \overline{\Phi}'_{\mathcal{J}_{\mathcal{S}}}$:

Rule $\mathcal{J}$**:Sym-General** Analogous to the corresponding case in Lemma 108 (SLS: Soundness single step).

Rule $\mathcal{J}$**:Sym-NoSpec** Analogous to the corresponding case in Lemma 108 (SLS: Soundness single step).

Rule $\mathcal{J}$**:Sym-barr** Then we have $\Phi_{\mathcal{J}}^{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\leadsto}_{\mathcal{J}}^{\mathcal{S}} \Phi_{\mathcal{J}}^{\mathcal{S}\prime}$ where $\Phi_{\mathcal{J}}^{\mathcal{S}\prime} = \langle p, \Phi_{\mathcal{J}}^{\mathcal{S}}.ctr, \Phi_{\mathcal{J}}^{\mathcal{S}}.\sigma'_{\mathcal{S}}, \Phi_{\mathcal{J}}^{\mathcal{S}}.n{-}1\rangle$ with $\Phi_{\mathcal{J}}^{\mathcal{S}}.\sigma \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$. Analogous to Rule $\mathcal{J}$:Sym-NoSpec using Rule $\mathcal{J}$:AM-barr.

Rule $\mathcal{J}$**:Sym-barr-spec** Then we have $\Phi_{\mathcal{J}}^{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\leadsto}_{\mathcal{J}}^{\mathcal{S}} \Phi_{\mathcal{J}}^{\mathcal{S}\prime}$ where $\Phi_{\mathcal{J}}^{\mathcal{S}\prime} = \langle p, \Phi_{\mathcal{J}}^{\mathcal{S}}.ctr, \Phi_{\mathcal{J}}^{\mathcal{S}}.\sigma'_{\mathcal{S}}, \Phi_{\mathcal{J}}^{\mathcal{S}}.n{-}1\rangle$ with $\Phi_{\mathcal{J}}^{\mathcal{S}}.\sigma \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$. Analogous to case Rule $\mathcal{J}$:Sym-NoSpec using Rule $\mathcal{J}$:AM-barr-spec.

Rule $\mathcal{J}$**:Sym-Spec** We have $\Phi_{\mathcal{J}}^{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\leadsto}_{\mathcal{J}}^{\mathcal{S}} \overline{\Phi}_{\mathcal{J}_{\mathcal{S}}}$ (Note that multiple speculative instances are created). Let $\overline{\Phi}_{\mathcal{J}_{\mathcal{S}}} = \Phi_{\mathcal{J}}^{\mathcal{S}0} \cdot \Phi_{\mathcal{J}}^{\mathcal{S}1} \cdots \Phi_{\mathcal{J}}^{\mathcal{S}n}$. Furthermore, we have $\Phi_{\mathcal{J}}^{\mathcal{S}}.\sigma \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$ with $\Phi_{\mathcal{J}}^{\mathcal{S}0}.\sigma_{\mathcal{S}} = \sigma'_{\mathcal{S}}$ and for each $l \in L$ we have $\sigma^i_{\mathcal{S}} = \sigma_{\mathcal{S}}[\mathbf{pc} \mapsto l]$, (note that l is always concrete).

We use Lemma 3 (NS: Soundness Symbolic Added rules) on $\Phi_{\mathcal{J}}^{\mathcal{S}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$ and get $\mu(\Phi_{\mathcal{J}}^{\mathcal{S}}.\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_{\mathcal{S}})} \mu(\sigma'_{\mathcal{S}})$. Let $\sigma' = \mu(\sigma'_{\mathcal{S}})$.
Choose $\Phi_{\mathcal{J}} = \mu(\Phi_{\mathcal{J}}^{\mathcal{S}})$ and note that a **jmp** instruction is executed.

We now derive a step using Rule $\mathcal{J}$:AM-Spec $\Phi_{\mathcal{J}} \overset{\mu(\tau_{\mathcal{S}})}{\leadsto}_{\mathcal{J}} \overline{\Phi}_{\mathcal{J}}$ together with the non-speculative step $\mu(\Phi_{\mathcal{J}}^{\mathcal{S}}.\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_{\mathcal{S}})} \mu(\sigma'_{\mathcal{S}})$ above and define for each $l \in L$ $\sigma^i = \mu(\sigma_{\mathcal{S}})[\mathbf{pc} \mapsto l]$.
We now show that $\mu(\overline{\Phi}_{\mathcal{J}_{\mathcal{S}}}) = \overline{\Phi}_{\mathcal{J}}$. Since l is concrete and $\mu(\Phi_{\mathcal{J}}^{\mathcal{S}}.\sigma_{\mathcal{S}}) = \sigma$, it follow by definition that $\mu(\sigma^{i)}_{\mathcal{S}} = \sigma^i$ for all $l \in L$.
By $\mu(\Phi_{\mathcal{J}}^{\mathcal{S}}) = \Phi_{\mathcal{J}}$ we have $\Phi_{\mathcal{J}}^{\mathcal{S}}.ctr = \Phi_{\mathcal{J}}.ctr$ and $\Phi_{\mathcal{J}}^{\mathcal{S}}.n = \Phi_{\mathcal{J}}.n$.

Now, we have $\mu(\overline{\Phi}_{\mathcal{J}_{\mathcal{S}}}) = \overline{\Phi}_{\mathcal{J}}$ and thus $\mu(\Phi_{\mathcal{J}}^{\mathcal{S}}) \overset{\mu(\tau_{\mathcal{S}})}{\leadsto}_{\mathcal{J}} \mu(\overline{\Phi}_{\mathcal{J}_{\mathcal{S}}})$ as needed.

□

I.5.2 Completeness.

Lemma 32 (J: Completeness of the symbolic semantics)**.** *If*

(1) $\Sigma_{\mathcal{J}} \Downarrow_{\mathcal{J}}^{\overline{\tau}} \Sigma'_{\mathcal{J}}$ *and*
(2) $\Sigma_{\mathcal{J}} = \mu(\Sigma_{\mathcal{J}}^{\mathcal{S}})$

Then there is a valuation μ*, a symbolic trace* $\overline{\tau_{\mathcal{S}}}'$ *and a final state* $\Sigma_{\mathcal{J}}^{\mathcal{S}\prime}$ *such that*

I $\Sigma_{\mathcal{J}}^{\mathcal{S}}\ {}_{\mathcal{S}}\Downarrow_{\mathcal{J}}^{\overline{\tau_{\mathcal{S}}}'} \Sigma_{\mathcal{J}}^{\mathcal{S}\prime}$ *and*
II $\Sigma'_{\mathcal{J}} = \mu(\Sigma_{\mathcal{J}}^{\mathcal{S}\prime})$ *and* $\overline{\tau} = \mu(\overline{\tau_{\mathcal{S}}}')$ *and*
III $\mu \vDash pthCnd(\Sigma_{\mathcal{J}}^{\mathcal{S}\prime})$

Proof. We proceed by induction on $\Sigma_{\mathsf{S}} \Downarrow_{\mathcal{J}}^{\overline{\tau}} \Sigma'_{\mathsf{S}}$

Rule $\mathcal{J}$**:AM-Reflection** Then we have $\Sigma_{\mathsf{S}} \Downarrow_{\mathcal{J}}^{\varepsilon} \Sigma'_{\mathsf{S}}$ with $\Sigma_{\mathsf{S}} = \Sigma'_{\mathsf{S}}$.

I - III By Rule $\mathcal{J}$:Sym-Reflection we have $\Sigma_{\mathcal{J}}^{\mathcal{S}}\ {}_{\mathcal{S}}\Downarrow_{\mathcal{J}}^{\varepsilon} \Sigma_{\mathcal{J}}^{\mathcal{S}\prime}$. By construction $\Sigma_{\mathcal{J}}^{\mathcal{S}\prime} = \Sigma_{\mathcal{J}}^{\mathcal{S}\prime}$. We now trivially satisfy all conditions.

Rule $\mathcal{J}$:AM-Single We have $\Sigma_{S} \Downarrow_{\mathcal{J}}^{\overline{\tau}' \cdot \tau} \Sigma'_{S}$ and by Rule S:AM-Single we get $\Sigma_{S} \Downarrow_{\mathcal{J}}^{\overline{\tau_S}'} \Sigma''_{S}$ and $\Sigma''_{S} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}}^{\mathcal{S}} \Sigma'_{S}$.

We need to prove

(1) $\Sigma_{\mathcal{J}}^{\mathcal{S}} \; {}_{\mathcal{S}}\Downarrow_{\mathcal{J}}^{\overline{\tau_{\mathcal{S}}}' \cdot \tau_{\mathcal{S}}} \Sigma_{\mathcal{J}}^{\mathcal{S}\prime}$ and

(2) $\Sigma'_{\mathcal{J}} = \mu(\Sigma_{\mathcal{J}}^{\mathcal{S}\prime})$ and $\overline{\tau}' \cdot \tau = \mu(\overline{\tau_{\mathcal{S}}}' \cdot \tau_{\mathcal{S}})$ and

(3) $\mu \vDash pthCnd(\Sigma_{\mathcal{J}}^{\mathcal{S}\prime})$

We apply the IH on $\Sigma_{\mathcal{J}} \Downarrow_{\mathcal{J}}^{\overline{\tau_S}'} \Sigma''_{\mathcal{J}}$ and obtain a $\Sigma_{\mathcal{J}}^{\mathcal{S}\prime\prime}$ such that:

(1) $\Sigma_{\mathcal{J}}^{\mathcal{S}} \; {}_{\mathcal{S}}\Downarrow_{\mathcal{J}}^{\overline{\tau_{\mathcal{S}}}'} \Sigma_{\mathcal{J}}^{\mathcal{S}\prime\prime}$ and

(2) $\Sigma''_{\mathcal{J}} = \mu(\Sigma_{\mathcal{J}}^{\mathcal{S}\prime\prime})$ and $\overline{\tau}' = \mu(\overline{\tau_{\mathcal{S}}}')$ and

(3) $\mu \vDash pthCnd(\Sigma_{\mathcal{J}}^{\mathcal{S}\prime\prime})$

The result follows from applying Lemma 33 ($\mathcal{J}$: Completeness single step) on $\Sigma''_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$: □

Lemma 33 ($\mathcal{J}$: Completeness single step)**.** *If*

(1) $\Sigma_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$ *and*

(2) $\mu(\Sigma_{\mathcal{J}}^{\mathcal{S}}) = \Sigma_{\mathcal{J}}$ *and*

(3) $\mu \vDash pthCnd(\Sigma_{\mathcal{J}}^{\mathcal{S}})$

Then

I $\Sigma_{\mathcal{J}}^{\mathcal{S}} \overset{\tau'}{\rightsquigarrow}_{\mathcal{J}}^{\mathcal{S}} \Sigma_{\mathcal{J}}^{\mathcal{S}\prime}$ *and*

II $\mu(\Sigma_{\mathcal{J}}^{\mathcal{S}\prime}) = \Sigma'_{\mathcal{J}}$ *and*

III $\mu \vDash pthCnd(\Sigma_{\mathcal{J}}^{\mathcal{S}\prime})$ *and* $\mu(\tau') = \tau$

Proof. We proceed by inversion on $\Sigma_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$:

Rule $\mathcal{J}$:AM-Rollback Since μ does not change the speculation window and ctr and $\mu(\Sigma_{\mathcal{J}}^{\mathcal{S}}) = \Sigma_{\mathcal{J}}$, we have $\Sigma_{\mathcal{J}}.n = \Sigma_{\mathcal{J}}^{\mathcal{S}}.n = 0$ and $\Sigma_{\mathcal{J}}.ctr = \Sigma_{\mathcal{J}}^{\mathcal{S}}.ctr$.

Analogous to the corresponding case in Lemma 111 (SLS: Completeness single step).

Rule $\mathcal{J}$:AM-Context We then have $\Phi_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \overline{\Phi}'_{\mathcal{J}}$. Note that $\Phi_{\mathcal{J}}.n > 0$ and as such for all symbolic states where $\mu(\Phi_{\mathcal{J}}^{\mathcal{S}}) = \Phi_{\mathcal{J}}$ as well. We proceed by inversion on $\Phi_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \overline{\Phi}'_{\mathcal{J}}$:

Rule $\mathcal{J}$:AM-General Analogous to the corresponding case in Lemma 111 (SLS: Completeness single step).

Rule $\mathcal{J}$:AM-barr Analogous to the corresponding case in Lemma 111 (SLS: Completeness single step).

Rule $\mathcal{J}$:AM-barr-spec Analogous to the barrier case above.

Rule $\mathcal{J}$:AM-NoSpec The case is analogous to Rule $\mathcal{J}$:AM-barr above using Rule $\mathcal{J}$:Sym-NoSpec.

Rule $\mathcal{J}$:AM-Spec We have $\Phi_{\mathcal{J}}^{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}_{\mathcal{J}}^{\mathcal{S}} \overline{\Phi}_{\mathcal{J}_{\mathcal{S}}}$ (Note that multiple speculative instances are created). Let $\overline{\Phi}_{\mathcal{J}} = \Phi_{\mathcal{J}}^{0} \cdot \Phi_{\mathcal{J}}^{1} \cdots \Phi_{\mathcal{J}}^{n}$.

Furthermore, we have $\Phi_{\mathcal{J}}.\sigma \xrightarrow{\tau} \sigma'$ and with $\Phi_{\mathcal{J}}^{0}.\sigma = \sigma'$ and for each $l \in L$ we have $\sigma^{i} = \sigma[\mathbf{pc} \mapsto l]$, (note that l is always concrete).

We use Lemma 5 (NS : Completeness Symbolic Added) on $\Phi_{\mathcal{J}}.\sigma \xrightarrow{\tau} \sigma'$ and get $\Phi_{\mathcal{J}}^{\mathcal{S}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$, where $\mu(\Phi_{\mathcal{J}}^{\mathcal{S}}) = \Phi_{\mathcal{J}}$ as per assumption, $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu(\sigma'_{\mathcal{S}}) = \sigma'$.

Choose $\Phi_{\mathcal{J}} = \mu(\Phi_{\mathcal{J}}^{\mathcal{S}})$ and note that a **jmp** instruction is executed.

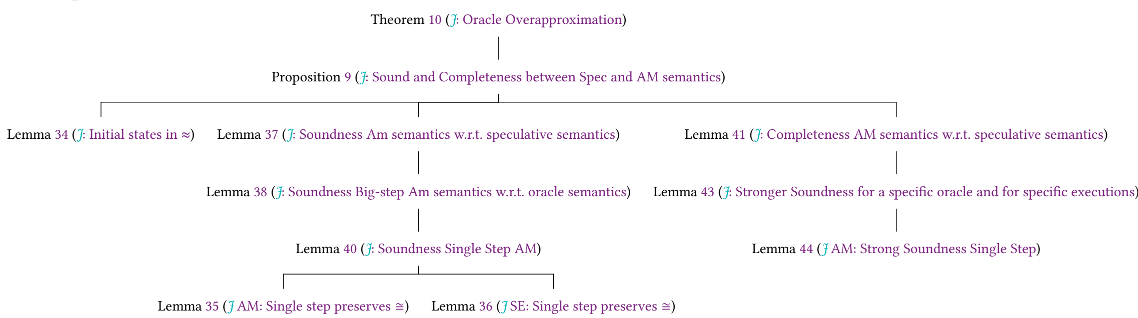
We now derive a step using Rule $\mathcal{J}$:Sym-Spec $\Phi^{\mathcal{S}}_{\mathcal{J}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathcal{J}} \overline{\Phi}_{\mathcal{J}_{\mathcal{S}}}$ together with the non-speculative step $\Phi^{\mathcal{S}}_{\mathcal{J}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$ above and define for each $l \in L$ $\sigma^i = \mu(\sigma_{\mathcal{S}})[\mathbf{pc} \mapsto l]$.
We now show that $\mu(\overline{\Phi}_{\mathcal{J}_{\mathcal{S}}}) = \overline{\Phi}_{\mathcal{J}}$. Since l is concrete and $\mu(\Phi^{\mathcal{S}}_{\mathcal{J}}.\sigma_{\mathcal{S}}) = \sigma$, it follow by definition that $\mu(\sigma^{i)}_{\mathcal{S}} = \sigma^i$ for all $l \in L$.
By $\mu(\Phi^{\mathcal{S}}_{\mathcal{J}}) = \Phi_{\mathcal{J}}$ we have $\Phi^{\mathcal{S}}_{\mathcal{J}}.ctr = \Phi_{\mathcal{J}}.ctr$ and $\Phi^{\mathcal{S}}_{\mathcal{J}}.n = \Phi_{\mathcal{J}}.n$.
Now, we have $\mu(\overline{\Phi}_{\mathcal{J}_{\mathcal{S}}}) = \overline{\Phi}_{\mathcal{J}}$ and thus $\Phi^{\mathcal{S}}_{\mathcal{J}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathcal{J}} \overline{\Phi}_{\mathcal{J}_{\mathcal{S}}}$ as needed.
It remains to show that $\mu \vDash pthCnd(\overline{\Phi}_{\mathcal{J}_{\mathcal{S}}})$. Since $\Phi^{\mathcal{S}^0}_{\mathcal{J}}.\delta^{\mathcal{S}} = \sigma'_{\mathcal{S}}.\delta^{\mathcal{S}}$ and we have $\mu \vDash pthCnd(\sigma'_{\mathcal{S}})$ from above we get $\mu \vDash pthCnd(\Phi^{\mathcal{S}^0}_{\mathcal{J}})$.
For the remaining $\Phi^{\mathcal{S}^i}_{\mathcal{J}}$ we have $\Phi^{\mathcal{S}^i}_{\mathcal{J}}.\sigma_{\mathcal{S}}.\delta^{\mathcal{S}} = \sigma_{\mathcal{S}}\delta^{\mathcal{S}}$. Since $\mu \vDash pthCnd(\sigma_{\mathcal{S}})$ we have $\mu \vDash pthCnd(\Phi^{\mathcal{S}}_{\mathcal{J}})^i$ and combined we have $\mu \vDash pthCnd(\overline{\Phi}_{\mathcal{J}_{\mathcal{S}}})$.

□

I.6 $\mathcal{J}$: Relating Oracle and AM semantics via SNI

First the definition of the element function we are gonna use: elem_of_states$(\langle p, ctr, \sigma, n\rangle) = \langle p, ctr, \sigma\rangle$

The proof structure looks like this:



Theorem 10 ($\mathcal{J}$: Oracle Overapproximation). *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 $((p,\sigma)) \Downarrow_{NS} \overline{\tau}$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}$, then $(p,\sigma) \Downarrow^{\omega}_{\mathcal{J}} \overline{\tau}''$, $(p,\sigma') \Downarrow^{\omega}_{\mathcal{J}} \overline{\tau}''$*

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) $((p,\sigma)) \Downarrow_{NS} \overline{\tau}'$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}'$ 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 $(p,\sigma) \Downarrow^{\omega}_{\mathcal{J}} \overline{\tau}''$, $(p,\sigma') \Downarrow^{\omega}_{\mathcal{J}} \overline{\tau}''$ 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 $((p,\sigma)) \Downarrow_{NS} \overline{\tau}$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}$, then $(p,\sigma) \Downarrow^{O}_{\mathcal{J}} \overline{\tau}'$ and $(p,\sigma') \Downarrow^{O}_{\mathcal{J}} \overline{\tau}'$.
We fulfill all premises of SNI by 1) and 2) for p and get $(p,\sigma) \Downarrow^{O}_{\mathcal{J}} \overline{\tau}'$ and $(p,\sigma') \Downarrow^{O}_{\mathcal{J}} \overline{\tau}'$.
We use Proposition 9 ($\mathcal{J}$: Sound and Completeness between Spec and AM semantics) with $(p,\sigma) \Downarrow^{O}_{\mathcal{J}} \overline{\tau}'$ and $(p,\sigma') \Downarrow^{O}_{\mathcal{J}} \overline{\tau}'$ to get $(p,\sigma) \Downarrow^{\omega}_{\mathcal{J}} \overline{\tau}''$, $(p,\sigma') \Downarrow^{\omega}_{\mathcal{J}} \overline{\tau}''$. This completes the proof.

($\Leftarrow$) We have

(1) $\sigma \sim_P \sigma'$ and
(2) $((p,\sigma)) \Downarrow_{NS} \overline{\tau}'$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}'$ and
(3) if $\sigma \sim_P \sigma'$ and $((p,\sigma)) \Downarrow_{NS} \overline{\tau}$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}$, then $(p,\sigma) \Downarrow_{\mathcal{J}}^{\omega} \overline{\tau}''$, $(p,\sigma') \Downarrow_{\mathcal{J}}^{\omega} \overline{\tau}''$

Note that we got assumptions 1) and 2) by the unfolding of the definition of SNI. We need to show that $(p,\sigma) \Downarrow_{\mathcal{J}}^{O} \overline{\tau}'$ and $(p,\sigma') \Downarrow_{\mathcal{J}}^{O} \overline{\tau}'$ holds.

By using assumption 1) and 2) for assumption 3), we get $(p,\sigma) \Downarrow_{\mathcal{J}}^{\omega} \overline{\tau}''$, $(p,\sigma') \Downarrow_{\mathcal{J}}^{\omega} \overline{\tau}''$.

Let O be an arbitrary prediction oracle with speculative window at most ω.

From Proposition 9 ($\mathcal{J}$: Sound and Completeness between Spec and AM semantics) with $(p,\sigma) \Downarrow_{\mathcal{J}}^{\omega} \overline{\tau}''$, $(p,\sigma') \Downarrow_{\mathcal{J}}^{\omega} \overline{\tau}''$ we get back $(p,\sigma) \Downarrow_{\mathcal{J}}^{O} \overline{\tau}$, $(p,\sigma') \Downarrow_{\mathcal{J}}^{O} \overline{\tau}$. 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 9 ($\mathcal{J}$: 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 $(p,\sigma) \Downarrow_{\mathcal{J}}^{\omega} \overline{\tau}$ and $(p,\sigma') \Downarrow_{\mathcal{J}}^{\omega} \overline{\tau}$ iff $(p,\sigma) \Downarrow_{\mathcal{J}}^{O} \overline{\tau}'$, $(p,\sigma) \Downarrow_{\mathcal{J}}^{O} \overline{\tau}'$ for all prediction oracles O with speculative window at most ω.*

Proof. The proposition immediately follows from Lemma 37 ($\mathcal{J}$: Soundness Am semantics w.r.t. speculative semantics) and Lemma 41 ($\mathcal{J}$: Completeness AM semantics w.r.t. speculative semantics) □

Lemma 34 ($\mathcal{J}$: Initial states in $\approx$). *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) $\Sigma_{\mathcal{J}}^{init} p, \sigma$ and $\Sigma_{\mathcal{J}}^{init} p, \sigma'$ and
(3) $X_{\mathcal{J}}^{init}(p,\sigma)$ and $X_{\mathcal{J}}^{init}(p,\sigma')$

Then

(1) $X_{\mathcal{J}}^{init}(p,\sigma) \cong X_{\mathcal{J}}^{init}(p,\sigma')$ and
(2) $\Sigma_{\mathcal{J}}^{init} p, \sigma \cong \Sigma_{\mathcal{J}}^{init} p, \sigma'$ and
(3) $\Sigma_{\mathcal{J}}^{init} p, \sigma \approx X_{\mathcal{J}}^{init}(p,\sigma)$ and $\Sigma_{\mathcal{J}}^{init} p, \sigma' \approx X_{\mathcal{J}}^{init}(p,\sigma')$ by Rule Single-Base and

Proof. We have

(1) $\sigma, \sigma' \in InitConf$ and
(2) $\Sigma_{\mathcal{J}}^{init} p, \sigma$ and $\Sigma_{\mathcal{J}}^{init} p, \sigma'$ and
(3) $X_{\mathcal{J}}^{init}(p,\sigma)$ and $X_{\mathcal{J}}^{init}(p,\sigma')$

Notice that by definition of $X_{\mathcal{J}}^{init}()$ and $\Sigma_{\mathcal{J}}^{init}$ we have:

$$X_{\mathcal{J}}^{init}(p,\sigma) = \langle p, 0, \sigma, \emptyset, \bot\rangle$$
$$X_{\mathcal{J}}^{init}(p,\sigma') = \langle p, 0, \sigma, \emptyset, \bot\rangle$$
$$\Sigma_{\mathcal{J}}^{init} p, \sigma = \langle p, 0, \sigma, \bot\rangle$$
$$\Sigma_{\mathcal{J}}^{init} p, \sigma' = \langle p, 0, \sigma, \bot\rangle$$

I Immediate

II Immediate

III Immediate using Rule Single-Base

∎

Lemma 35 ($\mathcal{J}$ AM: Single step preserves $\cong$)**.** *If*

(1) $\Sigma_{\mathcal{J}_1} \cong \Sigma_{\mathcal{J}_2}$ *and*

(2) $\Sigma_{\mathcal{J}_1} \overset{\tau}{\Rrightarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$ *and* $\Sigma_{\mathcal{J}_2} \overset{\tau}{\Rrightarrow}_{\mathcal{J}} \Sigma''_{\mathcal{J}}$

Then

(1) $\Sigma'_{\mathcal{J}} \cong \Sigma''_{\mathcal{J}}$

Proof. We have

(1) $\Sigma_{\mathcal{J}_1} \cong \Sigma_{\mathcal{J}_2}$ and

(2) $\Sigma_{\mathcal{J}_1} \overset{\tau}{\Rrightarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$ and $\Sigma_{\mathcal{J}_2} \overset{\tau'}{\Rrightarrow}_{\mathcal{J}} \Sigma''_{\mathcal{J}}$

Because of (1), we know that the same rule was used to derive the steps $\Sigma_{\mathcal{J}_1} \overset{\tau}{\Rrightarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$ and $\Sigma_{\mathcal{J}_2} \overset{\tau}{\Rrightarrow}_{\mathcal{J}} \Sigma''_{\mathcal{J}}$.

We know that $\Sigma'_{\mathcal{J}}.ctr = \Sigma''_{\mathcal{J}}.ctr$, $\Sigma'_{\mathcal{J}}.n = \Sigma''_{\mathcal{J}}.n$, $\Sigma'_{\mathcal{J}}.b = \Sigma''_{\mathcal{J}}.b$, because of (1) and the fact that the same rule was used to derive the step.

The proof is analogous to Lemma 60 ($\mathbb{S}$ AM: Single step preserves $\cong$).

∎

Lemma 36 ($\mathcal{J}$ SE: Single step preserves $\cong$)**.** *If*

(1) $X_{\mathcal{J}_1} \cong X_{\mathcal{J}_2}$ *and*

(2) $X_{\mathcal{J}_1} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}}$ *and* $X_{\mathcal{J}_2} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} X''_{\mathcal{J}}$

Then

(1) $X'_{\mathcal{J}} \cong X''_{\mathcal{J}}$ *and*

Proof. We have

(1) $X_{\mathcal{J}_1} \cong X_{\mathcal{J}_2}$ and

(2) $X_{\mathcal{J}_1} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}}$ and $X_{\mathcal{J}_2} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} X''_{\mathcal{J}}$

Because of (1), we know that the same rule was used to derive the steps $X_{\mathcal{J}_1} \overset{\tau}{\Rrightarrow}_{\mathcal{J}} X'_{\mathcal{J}}$ and $X_{\mathcal{J}_2} \overset{\tau}{\Rrightarrow}_{\mathcal{J}} X''_{\mathcal{J}}$.

We know that $X'_{\mathcal{J}}.ctr = X''_{\mathcal{J}}.ctr$, $X'_{\mathcal{J}}.n = X''_{\mathcal{J}}.n$, $X'_{\mathcal{J}}.b = X''_{\mathcal{J}}.b$ (where b marks if it is a misprediction or not), because of (1) and the fact that the same rule was used to derive the step.

The proof is analogous to Lemma 61 ($\mathbb{S}$ SE: Single step preserves $\cong$). ∎

I.7 Soundness

Lemma 37 ($\mathcal{J}$: 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) $(p, \sigma) \Cap^{\omega}_{\mathcal{J}} \overline{\tau}, (p, \sigma') \Cap^{\omega}_{\mathcal{J}} \overline{\tau}$

Then for all prediction oracles O with speculation window at most ω.

I $(p, \sigma) \Cap^{O}_{\mathcal{J}} \overline{\tau}', (p, \sigma) \Cap^{O}_{\mathcal{J}} \overline{\tau}'$

Proof. Let $\omega \in \mathbb{N}$ be a speculation window and $\sigma, \sigma' \in \mathit{InitConf}$ be two initial configurations. We have:

(1) $(p, \sigma) \Cap^{\omega}_{\mathcal{J}} \overline{\tau}, (p, \sigma') \Cap^{\omega}_{\mathcal{J}} \overline{\tau}$

Furthermore, let O be an arbitrary prediction oracle with speculative window at most ω.

The reasoning ins analogous to Lemma 63 ($\mathcal{S}$: Soundness Am semantics w.r.t. speculative semantics) using Lemma 38 ($\mathcal{J}$: Soundness Big-step Am semantics w.r.t. oracle semantics) together with Lemma 34 ($\mathcal{J}$: Initial states in $\approx$).

∎

Lemma 38 ($\mathcal{J}$: Soundness Big-step Am semantics w.r.t. oracle semantics)**.** *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*

If

(1) $\Sigma_{\mathcal{J}_1} \cong \Sigma_{\mathcal{J}_2}$

(2) $X_{\mathcal{J}_1} \cong X_{\mathcal{J}_2}$ *and* $\overline{\rho} = \varnothing$

(3) $\Sigma_{\mathcal{J}_1} \approx X_{\mathcal{J}_1}$ *and* $\Sigma_{\mathcal{J}_2} \approx X_{\mathcal{J}_2}$

(4) $\Sigma_{\mathcal{J}_1} \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$ *and* $\Sigma_{\mathcal{J}_2} \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}_2}$

Then for all prediction oracles O with speculation window at most ω.

I $X_{\mathcal{J}_1} \overset{O}{\rightsquigarrow}{}^{\mathcal{J}}_{\overline{\tau}'} X'_{\mathcal{J}_1}, X_{\mathcal{J}_2} \overset{O}{\rightsquigarrow}{}^{\mathcal{J}}_{\overline{\tau}''} X'_{\mathcal{J}_2}$

II $\Sigma'_{\mathcal{J}_1} \cong \Sigma'_{\mathcal{J}_2}$

III $X'_{\mathcal{J}_1} \cong X'_{\mathcal{J}_2}$ *and* $\overline{\rho} = \varnothing$

IV $\Sigma'_{\mathcal{J}_1} \approx X'_{\mathcal{J}_1}$ *and* $\Sigma'_{\mathcal{J}_2} \approx X'_{\mathcal{J}_2}$

V $\overline{\tau}' = \overline{\tau}''$

Proof. By Induction on $\Sigma_{\mathcal{J}_1} \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$ and $\Sigma_{\mathcal{J}_2} \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}_2}$.

Rule $\mathcal{J}$:AM-Reflection We have $\Sigma_{\mathcal{J}_1} \Downarrow^{\varepsilon}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$ and $\Sigma_{\mathcal{J}_2} \Downarrow^{\varepsilon}_{\mathcal{J}} \Sigma'_{\mathcal{J}_2}$, where $\Sigma'_{\mathcal{J}_1} = \Sigma_{\mathcal{J}_1}$ and $\Sigma'_{\mathcal{J}_2} = \Sigma_{\mathcal{J}_2}$.

Furthermore, we use Rule $\mathcal{J}$:Reflection to derive $X_{\mathcal{J}_1} \overset{O}{\rightsquigarrow}{}^{\mathcal{J}}_{\varepsilon} X'_{\mathcal{J}_1}, X_{\mathcal{J}_2} \overset{O}{\rightsquigarrow}{}^{\mathcal{J}}_{\varepsilon} X'_{\mathcal{J}_2}$ with $X'_{\mathcal{J}_1} = X_{\mathcal{J}_1}$ and $X'_{\mathcal{J}_2} = X_{\mathcal{J}_2}$.

We now trivially satisfy all conclusions.

Rule $\mathcal{J}$:AM-Single We have $\Sigma_{\mathcal{J}_1} \Downarrow^{\overline{\tau}''}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$ with $\Sigma'_{\mathcal{J}} \overset{\tau}{\Cap}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$ and $\Sigma_{\mathcal{J}_2} \Downarrow^{\overline{\tau}''}_{\mathcal{J}} \Sigma''_{\mathcal{J}}$ and $\Sigma''_{\mathcal{J}} \overset{\tau}{\Cap}_{\mathcal{J}} \Sigma'_{\mathcal{J}_2}$.

We now apply IH on $\Sigma_{\mathcal{J}_1} \Downarrow^{\overline{\tau}''}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$ and $\Sigma_{\mathcal{J}_2} \Downarrow^{\overline{\tau}''}_{\mathcal{J}} \Sigma''_{\mathcal{J}}$ and get

(a) $X_{\mathcal{J}_1} \overset{O}{\rightsquigarrow}{}^{\mathcal{J}}_{\overline{\tau}'} X'_{\mathcal{J}}, X_{\mathcal{J}_2} \overset{O}{\rightsquigarrow}{}^{\mathcal{J}}_{\overline{\tau}''} X''_{\mathcal{J}}$

(b) $\Sigma'_{\mathcal{J}} \cong \Sigma''_{\mathcal{J}}$

(c) $X'_{\mathcal{J}} \cong X''_{\mathcal{J}}$ and $\overline{\rho}' = \varnothing$

(d) $\Sigma'_{\mathcal{J}} \approx X'_{\mathcal{J}}$ and $\Sigma''_{\mathcal{J}} \approx X''_{\mathcal{J}}$

(e) $\overline{\tau}' = \overline{\tau}''$

We proceed by inversion on $\approx$ in $\Sigma'_{\mathcal{J}} \approx X'_{\mathcal{J}}$ and $\Sigma''_{\mathcal{J}} \approx X''_{\mathcal{J}}$:

com-single-base We thus have $\Sigma'_{\mathcal{J}} \sim X'_{\mathcal{J}} \upharpoonright_{com}$ and $\mathit{INV}(\Sigma'_{\mathcal{J}}, X'_{\mathcal{J}})$ (Similar for $\Sigma''_{\mathcal{J}}$ and $X''_{\mathcal{J}}$).

We only show the proof for $X'_{\mathcal{J}}$ here. The proof for $X''_{\mathcal{J}}$ is analogous, because of $X'_{\mathcal{J}} \cong X''_{\mathcal{J}}$.

Notice that if $minWndw(X'_{\mathcal{J}}) = 0$ 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 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states) using Lemma 40 ($\mathcal{J}$: Soundness Single Step AM).

com-single-oracle We thus have

$$\begin{aligned}
X'_{\mathcal{J}} =& X_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma, h, n''' \rangle^{l} \\
\Sigma'_{\mathcal{J}} =& \Sigma_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle \cdot \Sigma_{\mathcal{J}_4} \\
X_{\mathcal{J}} =& X_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \\
\Sigma_{\mathcal{J}} =& \Sigma_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma, n \rangle \\
\Sigma_{\mathcal{J}} \sim& X_{\mathcal{J}} \upharpoonright_{com}
\end{aligned}$$

The form of $X''_{\mathcal{J}}$ and $\Sigma''_{\mathcal{J}}$ is analogous.

The case is analogous to the corresponding case in Lemma 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

com-single-rollback We have

$$\begin{aligned}
X'_{\mathcal{J}} =& X_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma'', h', 0 \rangle^{l} \cdot X_{\mathcal{J}_4} \\
\Sigma'_{\mathcal{J}} =& \Sigma_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle^{false} \cdot \Sigma_{\mathcal{J}_4} \\
X_{\mathcal{J}} =& X_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \\
\Sigma_{\mathcal{J}} =& \Sigma_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma, n \rangle \\
\Sigma_{\mathcal{J}} \sim& X_{\mathcal{J}} \upharpoonright_{com} \\
n' \geq& 0
\end{aligned}$$

The form of $X''_{\mathcal{J}}$ and $\Sigma''_{\mathcal{J}}$ is analogous.

Additionally, we know that the transaction terminates in some state $\Sigma_{\mathcal{J}} \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'''_{\mathcal{J}}$. There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma'_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$ is not a rollback for *ctr* and Rule $\mathcal{J}$:AM-Context or Rule $\mathcal{J}$:AM-Rollback for a different transaction with a different *ctr* was used.

The case is analogous to the corresponding case in Lemma 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

$n' = 0$ Then we know that $\Sigma'_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$ was created by Rule $\mathcal{J}$:AM-Rollback and is a rollback for *ctr*.

I Here we prove that $X'_{\mathcal{J}} \xrightsquigarrow{\tau_0}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}_1}$ and $X''_{\mathcal{J}} \xrightsquigarrow{\tau_1}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}_2}$.

Since in $X'_{\mathcal{J}}$ and $X''_{\mathcal{J}}$ we have a state with $n = 0$ and we mispredicted, we know that Rule $\mathcal{J}$:Rollback applies.

So $X'_{\mathcal{J}} \xrightsquigarrow{\tau_0}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}_1}$ and $X''_{\mathcal{J}} \xrightsquigarrow{\tau_1}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}_2}$ are derived by Rule $\mathcal{J}$:Rollback.

The rest of the case is analogous to the corresponding case Lemma 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

$\square$

Since the Oracle semantics creates only one speculative state depending on the oracle and the AM semantics creates all possible speculative states depending on L, we need to be careful on how to relate them.
In our relation, we have an invariant on the speculative states when speculation is started.
We notice that in the AM semantics we can reorder the created speculative states. The same actions are visible on the trace, just in a different order. This way, we can put the speculative state in the AM semantics that jumps to the same location as the oracle speculative state, in the desired position in the AM state. This again allows us to relate the AM state and Oracle state.

Lemma 39 ($\mathcal{J}$: Reorder of the speculative states)**.** *If*

(1) $\Phi_{\mathcal{J}} \Longrightarrow_{\mathcal{J}} \Phi'_{\mathcal{J}} \cdot \overline{\Phi}'_{\mathcal{J}}$ *and*
(2) $\overline{\Phi}'_{\mathcal{J}} = \Phi^1_{\mathcal{J}} \cdot \ldots \cdot \Phi^n_{\mathcal{J}_{\overline{P}}}$

Then for all permutations of the state $\overline{\Phi}''_{\mathcal{J}} = perm(\overline{\Phi}'_{\mathcal{J}})$ *we have:*

(1) $\Phi'_{\mathcal{J}} \cdot \overline{\Phi}'_{\mathcal{J}} \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Phi''_{\mathcal{J}}$ *and*
(2) $\Phi'_{\mathcal{J}} \cdot \overline{\Phi}''_{\mathcal{J}} \Downarrow^{\overline{\tau}''}_{\mathcal{J}} \Phi''_{\mathcal{J}}$ *and*
(3) $\Phi''_{\mathcal{J}} = \Phi'_{\mathcal{J}}[ctr \mapsto ctr'']$
(4) there exists a permutation f such that $f(\overline{\tau}) = \overline{\tau}'$

Proof. NS trace is the same. So it does not influence the architectural execution.

We know that all speculative transactions terminate. Thus, all speculative transactions in $\overline{\Phi}'_{\mathcal{J}}$ and $\overline{\Phi}''_{\mathcal{J}}$ are terminated by Rule $\mathcal{J}$:AM-Rollback.

Thus, after all speculative transactions are terminated, we have $\Phi'_{\mathcal{J}}$ left. Rule $\mathcal{J}$:AM-Rollback only changes the counter of the state below. So we know that the new counter of $\Phi''_{\mathcal{J}}$ is the counter of the last speculative transaction that is rolled back.

Thus, the same state is reached after speculation.

Next, the same speculative states $\Phi^{\dagger}_{\mathcal{J}}$ are in $\overline{\Phi}'_{\mathcal{J}}$ and $\overline{\Phi}''_{\mathcal{J}}$. Since the semantics is deterministic, we know that each speculative state generates one trace $\overline{\tau}^{\dagger}$ which is pairwise equivalent between the permutation and the original order for each $\Phi^{\dagger}_{\mathcal{J}}$.

Thus, the same actions are generated. Just in a different order. □

Lemma 40 ($\mathcal{J}$: 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,* $\Sigma_{\mathcal{J}_1} = \Sigma'_{\mathcal{J}} \cdot \Phi'_{\mathcal{J}}$, $\Sigma_{\mathcal{J}_2} = \Sigma''_{\mathcal{J}} \cdot \Phi''_{\mathcal{J}}$ *be two speculative states for the always mispredict semantics and* $X_{\mathcal{J}_1}, X_{\mathcal{J}_2}$*, be two speculative states for the speculative semantics.*

If the following conditions hold:

(1) $\Sigma_{\mathcal{J}_1} \cong \Sigma_{\mathcal{J}_2}$
(2) $X_{\mathcal{J}_1} \cong X_{\mathcal{J}_2}$ *and* $\overline{p} = \emptyset$
(3) $\Sigma_{\mathcal{J}_1} \approx X_{\mathcal{J}_1}$ *and* $\Sigma_{\mathcal{J}_2} \approx X_{\mathcal{J}_2}$
(4) $\Phi'_{\mathcal{J}} \overset{\tau''}{\Longrightarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$ *and* $\Phi''_{\mathcal{J}} \overset{\tau''}{\Longrightarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}_2}$

then there are instances $X'_{\mathcal{J}_1}, X'_{\mathcal{J}_2}$ *for the speculative semantics such that:*

I $X_{\mathcal{J}_1} \overset{O}{\leadsto}{}^{\mathcal{J}}_{\tau} X'_{\mathcal{J}_1}$ *and* $X_{\mathcal{J}_2} \overset{O}{\leadsto}{}^{\mathcal{J}}_{\tau'} X'_{\mathcal{J}_2}$
II $\Sigma'_{\mathcal{J}_1} \cong \Sigma'_{\mathcal{J}_2}$
III $X'_{\mathcal{J}_1} \cong X'_{\mathcal{J}_2}$ *and* $\overline{\rho} = \emptyset$
IV $\Sigma'_{\mathcal{J}_1} \approx X'_{\mathcal{J}_1}$ *and* $\Sigma'_{\mathcal{J}_2} \approx X'_{\mathcal{J}_2}$
V $\tau = \tau'$

Proof. We proceed by inversion on $\Phi'_{\mathcal{J}} \overset{\tau''}{\Longrightarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$ and $\Phi''_{\mathcal{J}} \overset{\tau''}{\Longrightarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}_2}$:

Rule $\mathcal{J}$:AM-General We choose $X'_{\mathcal{J}_1} = X'_{\mathcal{J}}$ and $X'_{\mathcal{J}_2} = X''_{\mathcal{J}}$. The case is analogous to the corresponding case in Lemma 65 (S: Soundness Single Step AM).

Rule $\mathcal{J}$:AM-Spec There are two cases depending on the output of the oracle O.

(ω, l) **and correct prediction w.r.t** $X'_{\mathcal{J}}$ The execution jumps to the correct address

I We use Rule $\mathcal{J}$:Spec-Exe to derive the steps $X_{\mathcal{J}_1} \overset{\tau_0}{\leadsto}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}}$ and $X_{\mathcal{J}_2} \overset{\tau_1}{\leadsto}{}^{O}_{\mathcal{J}} X''_{\mathcal{J}}$.
Furthermore, we execute Rule $\mathcal{J}$:General once, because Rule $\mathcal{J}$:Spec-Exe creates one observations in $\overline{\rho}$. We now have $X'_{\mathcal{J}_1} = X'_{\mathcal{J}}$ 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 $X_{\mathcal{J}_1} \overset{O}{\leadsto}{}^{\mathcal{J}}_{\overline{\tau}} X'_{\mathcal{J}_1}$ and $X_{\mathcal{J}_2} \overset{O}{\leadsto}{}^{\mathcal{J}}_{\overline{\tau}'} X'_{\mathcal{J}_2}$.

II By Lemma 35 ($\mathcal{J}$ AM: Single step preserves $\cong$).

III By Lemma 36 ($\mathcal{J}$ SE: Single step preserves $\cong$) for $X_{\mathcal{J}_1} \overset{\tau_0}{\leadsto}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}}$ and $X_{\mathcal{J}_2} \overset{\tau_1}{\leadsto}{}^{O}_{\mathcal{J}} X''_{\mathcal{J}}$ and the fact that the use of Rule $\mathcal{J}$: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 $\mathcal{J}$:General twice.

IV We have

$$
\begin{aligned}
X'_{\mathcal{J}_1} &= X'_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma', h, n\rangle \cdot \langle p, ctr', \sigma', h', n_0\rangle \\
\Sigma'_{\mathcal{J}_1} &= \Sigma_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma', n_1\rangle \cdot \overline{\Phi}'_{\mathcal{J}} \\
X'_{\mathcal{J}_4} &= X'_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma', h, n\rangle \\
\Sigma'_{\mathcal{J}_4} &= \Sigma_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma', n_1\rangle
\end{aligned}
$$

The case is analogous to the Rule S:AM-Store-Spec correct prediction case in Lemma 65 (S: Soundness Single Step AM),

V The observations are $\overline{\tau} = \texttt{pc}\ l \cdot \texttt{start}\ ctr_1$ and $\overline{\tau}' = \texttt{pc}\ l \cdot \texttt{start}\ ctr_2$.
The case is analogous to the Rule S:AM-Store-Spec correct prediction case in Lemma 65 (S: Soundness Single Step AM).

(ω, l) **wrong prediction w.r.t** $X'_{\mathcal{J}}$ The indirect jump jumps to the wrong target.

a) We use Rule $\mathcal{J}$:Spec to derive the steps $X'_{\mathcal{J}} \overset{\tau_0}{\leadsto}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}_1}$ and $X''_{\mathcal{J}} \overset{\tau_1}{\leadsto}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}_2}$.
Furthermore, we execute Rule $\mathcal{J}$:General once, because Rule $\mathcal{J}$:Spec creates one observations in $\overline{\rho}$. We now have $X'_{\mathcal{J}_1} = X'_{\mathcal{J}}$ 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 $X_{\mathcal{J}_1} \overset{O}{\leadsto}{}^{\mathcal{J}}_{\overline{\tau}} X'_{\mathcal{J}_1}$ and $X_{\mathcal{J}_2} \overset{O}{\leadsto}{}^{\mathcal{J}}_{\overline{\tau}'} X'_{\mathcal{J}_2}$.
Notice that the observations in $\overline{\rho}$ are equal between $X_{\mathcal{J}_1}$ and $X_{\mathcal{J}_2}$, because of (2). We have $X_{\mathcal{J}_1}.ctr = X_{\mathcal{J}_2}.ctr$ and $X_{\mathcal{J}_1}.\sigma \sim_{\mathbf{pc}} X_{\mathcal{J}_2}.\sigma$ from our relation.

b) By Lemma 35 ($\mathcal{J}$ AM: Single step preserves $\cong$).

c) By Lemma 36 ($\mathcal{J}$ SE: Single step preserves $\cong$) for Rule $\mathcal{J}$:Spec and Rule $\mathcal{J}$:General twice. Notice that $\overline{\rho}$ is empty now.

d) We have:

$$\begin{aligned}
X'_{\mathcal{J}_1} =& X'_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma', h, n\rangle \cdot \langle p, ctr', \sigma''', h', n_0\rangle \\
\Sigma'_{\mathcal{J}_1} =& \Sigma_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma', n_1\rangle \cdot \overline{\Phi}_{\mathcal{J}} \\
X'_{\mathcal{J}_4} =& X'_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma', h, n\rangle \\
\Sigma'_{\mathcal{J}_4} =& \Sigma_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma', n_1\rangle
\end{aligned}$$

We now use Lemma 39 ($\mathcal{J}$: Reorder of the speculative states) to reorder the speculative states created in $\Sigma'_{\mathcal{J}_1}$ and $\Sigma'_{\mathcal{J}_2}$ which are $\overline{\Phi}_{\mathcal{J}}$ to have the speculative instance with $\sigma'''.\mathbf{pc} = l$ (which exists since $l \in L$) to be last. I.e. $\overline{\Phi}_{\mathcal{J}} = \Phi_{\mathcal{J}} \cdot \overline{\Phi}''_{\mathcal{J}}$ where $\Phi_{\mathcal{J}}.\mathbf{pc} = l$.

Now, we can again instantiate the relation The rest of the case is analogous to the Rule S:AM-Store-Spec wrong prediction case in Lemma 65 (S: Soundness Single Step AM).

e) The observations are

$$\begin{aligned}
\overline{\tau} =& \texttt{pc}\ \sigma'(\mathbf{pc}) \cdot \texttt{start}\ X_{\mathcal{J}_1}.ctr \\
\overline{\tau}' =& \texttt{pc}\ \sigma'(\mathbf{pc}) \cdot \texttt{start}\ X_{\mathcal{J}_2}.ctr
\end{aligned}$$

The case is analogous to the misprediction case in Lemma 65 (S: Soundness Single Step AM).

Rule $\mathcal{J}$:AM-barr and Rule $\mathcal{J}$:AM-barr-spec We prove this for Rule $\mathcal{J}$:AM-barr-spec. The proof for Rule $\mathcal{J}$:AM-barr is analogous.

The proof is analogous to the corresponding case in Lemma 65 (S: Soundness Single Step AM) using Lemma 35 ($\mathcal{J}$ AM: Single step preserves $\cong$) and Lemma 36 ($\mathcal{J}$ SE: Single step preserves $\cong$),

Rule $\mathcal{J}$:AM-NoSpec 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 $INV(\Sigma'_{\mathcal{J}_1}, X'_{\mathcal{J}_1})$ is is analogous to the corresponding case in Lemma 65 (S: Soundness Single Step AM).

□

I.8 Completeness

Definition 31 ($\mathcal{J}$: Constructing the AM Oracle)**.** *Constructing the prediction oracle $O_{am}{}^{\mathcal{J}}$. We build our oracle based on the executions $\Sigma^{init}_{\mathcal{J}} p, \sigma \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma_{\mathcal{J}_1} \xrightarrow{\tau_{am}}_{\mathcal{J}} \Sigma_{\mathcal{J}_2}, \Sigma^{init}_{\mathcal{J}} p, \sigma' \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1} \xrightarrow{\tau'_{am}}_{\mathcal{J}} \Sigma'_{\mathcal{J}_2}$ where $\tau_{am} \neq \tau'_{am}$.*

Let us denote by the set (RB, l) the ids and jump locations l of the path of nested speculative transactions in $\Sigma_{\mathcal{J}_1}$ that were made to reach the difference. Since $\Sigma_{\mathcal{J}_1} \cong \Sigma'_{\mathcal{J}_1}$ we know that the same transaction ids are still ongoing in $\Sigma'_{\mathcal{J}_1}$ as well. The set RB describes the jump instructions that we need to mispredict to reach the difference in the trace.

We write $(RB, l)^1$ to indicate the first projection applied to every element in the set. Our oracle is now defined as follows:

$$O_{am}{}^{\mathcal{J}}(p, n, h) = \begin{cases} (l, \omega) \ \textit{if}\ |h| \in (RB, l)^1 \wedge p(\sigma(\mathbf{pc})) = \mathbf{jmp}\ xe \\ (l', 0) \ \textit{otherwise (where } p(\sigma(\mathbf{pc})) = \mathbf{jmp}\ xe\textit{)} \end{cases}$$

Lemma 41 ($\mathcal{J}$: 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) $p, \sigma \; ⎍^{\omega}_{\mathcal{J}} \; \overline{\tau}$ and $p, \sigma' \; ⎍^{\omega}_{\mathcal{J}} \; \overline{\tau}'$ and
(2) $\overline{\tau} \neq \overline{\tau}'$

Then there exists an oracle O such that

I $p, \sigma \; ⎍^{O}_{\mathcal{J}} \; \overline{\tau}_1$ and $p, \sigma' \; ⎍^{O}_{\mathcal{J}} \; \overline{\tau}'_1$ 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) $p, \sigma \; ⎍^{\omega}_{\mathcal{J}} \; \overline{\tau}$ and $p, \sigma' \; ⎍^{\omega}_{\mathcal{J}} \; \overline{\tau}'$ and
(2) $\overline{\tau} \neq \overline{\tau}'$

By definition of $⎍^{\omega}_{\mathcal{J}}$ we have two final states $\Sigma_{\mathcal{J}F}$ and $\Sigma'_{\mathcal{J}F}$ such that $\Sigma^{init}_{\mathcal{J}} p, \sigma \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma_{\mathcal{J}F}$ $\Sigma^{init}_{\mathcal{J}} p, \sigma' \Downarrow^{\overline{\tau}'}_{\mathcal{J}} \Sigma'_{\mathcal{J}F}$. Combined with the fact that $\overline{\tau} \neq \overline{\tau}'$, it follows that there are speculative states $\Sigma_{\mathcal{J}_1}, \Sigma_{\mathcal{J}}, \Sigma'_{\mathcal{J}_1}, \Sigma'_{\mathcal{J}_2}$ and sequences of observations $\overline{\tau}, \overline{\tau}_{end}, \overline{\tau}'_{end}, \tau_{am}, \tau'_{am}$ such that $\tau_{am} \neq \tau'_{am}$, $\Sigma_{\mathcal{J}_1} \cong \Sigma'_{\mathcal{J}_1}$ and:

$$\Sigma^{init}_{\mathcal{J}} p, \sigma \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma_{\mathcal{J}_1} \overset{\tau_{am}}{\rightsquigarrow}_{\mathcal{J}} \Sigma_{\mathcal{J}_2} \Downarrow^{\overline{\tau}_{end}}_{\mathcal{J}} \Sigma_{\mathcal{J}F}$$
$$\Sigma^{init}_{\mathcal{J}} p, \sigma' \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1} \overset{\tau'_{am}}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}_2} \Downarrow^{\overline{\tau}'_{end}}_{\mathcal{J}} \Sigma'_{\mathcal{J}F}$$

We claim that there is a prediction oracle O with a speculative window at most ω such that

a $X^{init}_{\mathcal{J}}(p, \sigma) \overset{O}{\rightsquigarrow}{}^{\mathcal{J}}_{v} X_{\mathcal{J}_1}$ and $X_{\mathcal{J}_1}.\sigma = \Sigma_{\mathcal{J}_1}.\sigma$ and $INV2(X_{\mathcal{J}_1}, \Sigma_{\mathcal{J}_1})$ and
b $X^{init}_{\mathcal{J}}(p, \sigma') \overset{O}{\rightsquigarrow}{}^{\mathcal{J}}_{v} X'_{\mathcal{J}_1}$ and $X'_{\mathcal{J}_1}.\sigma = \Sigma'_{\mathcal{J}_1}.\sigma$ and $INV2(X'_{\mathcal{J}_1}, \Sigma'_{\mathcal{J}_1})$
c $X_{\mathcal{J}_1} \cong X'_{\mathcal{J}_1}$

We get this by applying Lemma 43 ($\mathcal{J}$: Stronger Soundness for a specific oracle and for specific executions) on the Am execution up to the point of the difference $\Sigma^{init}_{\mathcal{J}} p, \sigma \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma_{\mathcal{J}_1}$ with the $O_{am}{}^{\mathcal{J}}$ and Σ^{States}_1 being all the states in $\Sigma^{init}_{\mathcal{J}} p, \sigma \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma_{\mathcal{J}_1}$ (similar for Σ^{States}_2 for $\Sigma^{init}_{\mathcal{J}} p, \sigma' \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$)..

We now show that $\Sigma_{\mathcal{J}_1} \approx_{O_{am}} X_{\mathcal{J}_1}$ is derived by Rule Single-Base-Oracle (similar for $\Sigma_{\mathcal{J}_2} \approx^{\Sigma^{States}_2}_{O_{am}{}^{\mathcal{J}}} X_{\mathcal{J}_2}$).

We do a case distinction if there are ongoing transactions in $X_{\mathcal{J}_1}$ or not

no ongoing transactions in $X_{\mathcal{J}_1}$ Then $\Sigma_{\mathcal{J}_1} \approx_{O_{am}} X_{\mathcal{J}_1}$ can only be derived Rule Single-Base-Oracle and $\Sigma_{\mathcal{J}_1}$ has no ongoing transactions as well. Then we have by $INV2(\Sigma_{\mathcal{J}_1}, X_{\mathcal{J}_1})$ and $\Sigma_{\mathcal{J}_1}.n = \bot$ that $X_{\mathcal{J}_1}.n = \bot$.

ongoing transactions in $X_{\mathcal{J}}$ 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 $X_{\mathcal{J}}$.

Furthermore, we know that $X_{\mathcal{J}_1}.n \geq minWndw(X_{\mathcal{J}_1})$ by definition of the oracle $O_{am}{}^{\mathcal{J}}$ and $minWndw()$.

Since the next rule cannot be Rule $\mathcal{J}$:AM-Rollback, we know that $\Sigma_{\mathcal{J}_1}.n > 0$ and by $INV2(\Sigma_{\mathcal{J}_1}, X_{\mathcal{J}_1})$ we get $minWndw(X_{\mathcal{J}_1}) > 0$ (Similar for $X'_{\mathcal{J}_1}$ because of $\Sigma_{\mathcal{J}_1} \cong \Sigma'_{\mathcal{J}_1}$).

If $\Sigma_{\mathcal{J}_1} \approx_{O_{am}} X_{\mathcal{J}_1}$ by rollback rule, we would have a contradiction because we would need the topmost speculation window of $X_{\mathcal{J}_1}.n = 0$. But we know that $minWndw(X_{\mathcal{J}_1}) > 0$, because the speculation window of the topmost instance was created with a speculation window of ω.

we know that $X_{\mathcal{J}_1} \approx_{O_{am}} \Sigma_{\mathcal{J}_1}$ by Rule Single-Base-Oracle.

We now proceed by case analysis on the rule in $\Rrightarrow_{\mathcal{J}}$ used to derive $\Sigma_{\mathcal{J}_1} \stackrel{\tau_{am}}{\Rrightarrow}_{\mathcal{J}} \Sigma_{\mathcal{J}_2}$. Because $\Sigma_{\mathcal{J}_1} \cong \Sigma'_{\mathcal{J}_1}$ and $\overline{\tau}_1 = \overline{\tau}'_1$, we know that the same rule was used in $\Sigma'_{\mathcal{J}_1} \stackrel{\tau'_{am}}{\Rrightarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}_2}$ as well.

Rule $\mathcal{J}$:AM-Rollback Contradiction. Because $\Sigma_{\mathcal{J}_1} \cong \Sigma'_{\mathcal{J}_1}$ 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 $\mathcal{J}$:AM-Context By inversion on Rule $\mathcal{J}$:AM-Context for the step $\Sigma_{\mathcal{J}_1} \stackrel{\tau_{am}}{\Rrightarrow}_{\mathcal{J}} \Sigma_{\mathcal{J}_2}$ we have $\Sigma_{\mathcal{J}_1} = \overline{\Phi}_{\mathcal{J}} \cdot \Phi_{\mathcal{J}}$ and $\Sigma_{\mathcal{J}_2} = \overline{\Phi}_{\mathcal{J}} \cdot \overline{\Phi}'_{\mathcal{J}}$ with $\Phi_{\mathcal{J}} \stackrel{\tau_{am}}{\Rrightarrow}_{\mathcal{J}} \overline{\Phi}'_{\mathcal{J}}$.

We now do inversion on $\Sigma_{\mathcal{J}_1} \stackrel{\tau_{am}}{\Rrightarrow}_{\mathcal{J}} \Sigma_{\mathcal{J}_2}$ and $\Phi_{\mathcal{J}} \stackrel{\tau_{am}}{\Rrightarrow}_{\mathcal{J}} \overline{\Phi}'_{\mathbb{S}}$:

Rule $\mathcal{J}$:AM-General Contradiction. By $\Sigma_{\mathcal{J}_1} \cong \Sigma'_{\mathcal{J}_1}$ we know that $\Sigma_{\mathcal{J}_1}.\overline{\rho} = \Sigma'_{\mathcal{J}_1}.\overline{\rho}$.

This immediately implies that $\tau_{am} = \tau_{am'}$, which is not true by assumption.

Rule $\mathcal{J}$:AM-barr-spec, Rule $\mathcal{J}$:AM-barr Contradiction. Since these rules do not generate any observation by definition.

This leads to $\tau_{am} = \tau_{am'}$.

Rule $\mathcal{J}$:AM-NoSpec, Rule $\mathcal{J}$:AM-Spec We fulfil all assumptions for Lemma 42 ($\mathcal{J}$: AM and Oracle coincide) and get $X_{\mathbb{S}1} \overset{\tau_{am}}{\rightsquigarrow}{}^{O}_{\mathbb{S}} X_{\mathbb{S}2}$ and $X'_{\mathbb{S}1} \overset{\tau'_{am}}{\rightsquigarrow}{}^{O}_{\mathbb{S}} X'_{\mathbb{S}2}$.

Since $\tau_{am} \neq \tau'_{am}$ by assumption we are finished.

This completes the proof of our claim.

□

Lemma 42 ($\mathcal{J}$: AM and Oracle coincide). *If*

(1) $\Sigma_{\mathcal{J}} \approx^{\Sigma^{States}_{X_{\mathcal{J}}}}_{O_{am}{}^{\mathcal{J}}}$ *by Base and*

(2) $\Sigma_{\mathcal{J}} \stackrel{\tau}{\Rrightarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$ *and*

(3) $minWndw(\Sigma_{\mathcal{J}}) > 0$

(4) $X_{\mathcal{J}}.\overline{\rho} = \emptyset$

Then

(1) $X_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathcal{J}} X'_{\mathcal{J}}$

Proof. Since $minWndw(\Sigma_{\mathcal{J}}) > 0$ we know that the next step is not a rollback. From $minWndw(\Sigma_{\mathcal{J}}) > 0$ and $\Sigma_{\mathcal{J}} \approx^{\Sigma^{States}}_{O_{am}} X_{\mathcal{J}}$ we have $INV2(\Sigma_{\mathcal{J}}, X_{\mathcal{J}})$ and we get $minWndw(X_{\mathcal{J}}) > 0$ as well.

We proceed by inversion on $\Sigma_{\mathcal{J}} \stackrel{\tau}{\Rrightarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$:

Rule $\mathcal{J}$:AM-NoSpec From the rule, we have that $\Sigma_{\mathcal{J}}.\sigma \xrightarrow{\tau} \Sigma'_{\mathcal{J}}.\sigma$.

The case is analogous to the corresponding case in Lemma 67 ($\mathbb{S}$: AM and Oracle coincide).

Rule $\mathcal{J}$:AM-barr-spec, Rule $\mathcal{J}$:AM-barr From the rule, we have that $\Sigma_{\mathcal{J}}.\sigma \rightarrow \Sigma'_{\mathcal{J}}.\sigma$.

The case is analogous to the case above.

Rule $\mathcal{J}$:AM-Spec Then, τ is generated by the step $\Sigma_{\mathcal{J}}.\sigma \xrightarrow{\tau} \Sigma'_{\mathcal{J}}.\sigma$ generated by Rule $\mathcal{J}$:AM-Spec.

The case is analogous to the corresponding case in Lemma 67 ($\mathbb{S}$: AM and Oracle coincide).

□

Lemma 43 ($\mathcal{J}$: Stronger Soundness for a specific oracle and for specific executions). *Specific executions mean that there is a difference in the trace but before there is none. We use the oracle $O_{am}{}^{\mathsf{S}}$ as it is defined by Definition 31 ($\mathcal{J}$: Constructing the AM Oracle) for the given execution. If*

(1) $\Sigma_{\mathcal{J}_1} \cong \Sigma_{\mathcal{J}_2}$
(2) $X_{\mathcal{J}_1} \cong X_{\mathcal{J}_2}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma_{\mathcal{J}_1} \approx^{\Sigma_1^{States}}_{O_{am}{}^{\mathcal{J}}} X_{\mathcal{J}_1}$ *and* $\Sigma_{\mathcal{J}_2} \approx^{\Sigma_2^{States}}_{O_{am}{}^{\mathcal{J}}} X_{\mathcal{J}_2}$
(4) $\Sigma_{\mathcal{J}_1} \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$ *and* $\Sigma_{\mathcal{J}_2} \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}_2}$
(5) $\Sigma_1^{States} = \Sigma_{\mathcal{J}_1} \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$ *and* $\Sigma_2^{States} = \Sigma_{\mathcal{J}_2} \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}_2}$

and our oracle is constructed in the way described above Then

I $X_{\mathcal{J}_1} \overset{O}{\rightsquigarrow}{}^{\mathcal{J}}_{\overline{\tau}'} X'_{\mathcal{J}_1}, X_{\mathcal{J}_2} \overset{O}{\rightsquigarrow}{}^{\mathcal{J}}_{\overline{\tau}''} X'_{\mathcal{J}_2}$
II $\Sigma'_{\mathcal{J}_1} \cong \Sigma'_{\mathcal{J}_2}$
III $X'_{\mathcal{J}_1} \cong X'_{\mathcal{J}_2}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{\mathcal{J}_1} \approx^{\Sigma_1^{States}}_{O_{am}{}^{\mathcal{J}}} X'_{\mathcal{J}_1}$ *and* $\Sigma'_{\mathcal{J}_2} \approx^{\Sigma_2^{States}}_{O_{am}{}^{\mathcal{J}}} X'_{\mathcal{J}_2}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. Notice that the proof is very similar to Lemma 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states). The only different thing 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*$(\Sigma_{\mathcal{J}}, X_{\mathcal{J}})$

For these reasons, we will only argue why *INV2*$(\Sigma'_{\mathcal{J}_1}, X'_{\mathcal{J}_1})$ holds in the different cases and leave the rest to the old soundness proof.

By Induction on $\Sigma_{\mathcal{J}_1} \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$ and $\Sigma_{\mathcal{J}_2} \Downarrow^{\overline{\tau}}_{\mathcal{J}} \Sigma'_{\mathcal{J}_2}$.

Rule $\mathcal{J}$:AM-Reflection Analogous to Lemma 68 (S: Stronger Soundness for a specific oracle and for specific executions).

Rule S:AM-Single We have $\Sigma_{\mathcal{J}_1} \Downarrow^{\overline{\tau}''}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$ with $\Sigma'_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$ and $\Sigma_{\mathcal{J}_2} \Downarrow^{\overline{\tau}''}_{\mathcal{J}} \Sigma''_{\mathcal{J}}$ and $\Sigma''_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}_2}$.

We now apply IH on $\Sigma_{\mathcal{J}_1} \Downarrow^{\overline{\tau}''}_{\mathcal{J}} \Sigma'_{\mathcal{J}}$ and $\Sigma_{\mathcal{J}_2} \Downarrow^{\overline{\tau}''}_{\mathcal{J}} \Sigma''_{\mathcal{J}}$ and get

(a) $X_{\mathcal{J}_1} \overset{O}{\rightsquigarrow}{}^{\mathcal{J}}_{\overline{\tau}'} X'_{\mathcal{J}}, X_{\mathcal{J}_2} \overset{O}{\rightsquigarrow}{}^{\mathcal{J}}_{\overline{\tau}''} X''_{\mathcal{J}}$
(b) $\Sigma'_{\mathcal{J}} \cong \Sigma''_{\mathcal{J}}$
(c) $X'_{\mathcal{J}} \cong X''_{\mathcal{J}}$ and $\overline{\rho}' = \varnothing$
(d) $\Sigma'_{\mathcal{J}} \approx^{\Sigma_1^{States}}_{O_{am}{}^{\mathcal{J}}} X'_{\mathcal{J}}$ and $\Sigma''_{\mathcal{J}} \approx^{\Sigma_2^{States}}_{O_{am}{}^{\mathcal{J}}} X''_{\mathcal{J}}$
(e) $\overline{\tau}' = \overline{\tau}''$

We do a case distinction on $\approx^{\Sigma^{States}}_{O_{am}{}^{\mathcal{J}}}$ in $\Sigma'_{\mathcal{J}} \approx^{\Sigma_1^{States}}_{O_{am}{}^{\mathcal{J}}} X'_{\mathcal{J}}$ and $\Sigma''_{\mathcal{J}} \approx^{\Sigma_2^{States}}_{O_{am}{}^{\mathcal{J}}} X''_{\mathcal{J}}$ by inversion:

Rule Single-Base-Oracle We thus have $\Sigma'_{\mathcal{J}} \sim X'_{\mathcal{J}}\restriction_{com}$, $minWndw(X'_{\mathcal{J}}) > 0$ and *INV2*$(\Sigma'_{\mathcal{J}}, X'_{\mathcal{J}})$ (Similar for $\Sigma''_{\mathcal{J}}$ and $X''_{\mathcal{J}}$).

We now proceed by inversion on the derivation $\Sigma'_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$ and $\Sigma''_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}_2}$.

Rule $\mathcal{J}$:AM-Rollback Contradiction, because of $minWndw(X'_{\mathcal{J}}) > 0$ and *INV2*$(\Sigma'_{\mathcal{J}}, X'_{\mathcal{J}})$.

Rule $\mathcal{J}$:AM-General *INV2*() trivially holds, because it does not change the speculation window of the states.

Rule $\mathcal{J}$:AM-Context We have $\Phi_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \overline{\Phi}_{S}$ and $\Phi'_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \overline{\Phi}'_{S}$. We fulfil all conditions for Lemma 44 ($\mathcal{J}$ AM: Strong Soundness Single Step) which gives us the desired result. Especially, that the resulting state is in Σ_1^{States}, which follows by definition of Σ^{States}

Rule Single-Transaction-Rollback-Oracle We have

$$
\begin{aligned}
X'_{\mathcal{J}} =& X_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma'', h', 0 \rangle^{false} \cdot X_{\mathcal{J}_4} \\
\Sigma'_{\mathcal{J}} =& \Sigma_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle^{false} \cdot \Sigma_{\mathcal{J}_4} \\
X_{\mathcal{J}} =& X_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \\
\Sigma_{\mathcal{J}} =& \Sigma_{\mathcal{J}_3} \cdot \langle p, ctr, \sigma, n \rangle \\
\Sigma_{\mathcal{J}} \sim& X_{\mathcal{J}} \upharpoonright_{com} \\
& INV2(\Sigma_{\mathcal{J}}, X_{\mathcal{J}}) \\
n' \geq& 0
\end{aligned}
$$

The form of $X''_{\mathcal{J}}$ and $\Sigma''_{\mathcal{J}}$ is analogous.

Additionally, we know that the transaction terminates in some state $\Sigma_{\mathcal{J}} \Downarrow_{\mathcal{J}}^{\overline{\tau}} \Sigma'''_{\mathcal{J}}$. There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma'_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$ is not a rollback. Because $\Sigma_{\mathcal{J}}$ and $X_{\mathcal{J}}$ do not change, $INV2(\Sigma_{\mathcal{J}}, X_{\mathcal{J}})$ does not change as well.

The states are still related by Rule Single-Transaction-Rollback-Oracle after the step.

$n' = 0$ Then we know that $\Sigma'_{\mathcal{J}} \overset{\tau}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$ was created by Rule S:AM-Rollback and is a rollback for ctr. Notice, that the only difference between $X_{\mathcal{J}}$ and $\Sigma_{\mathcal{J}}$ is the updated ctr, because of the rollback. Updating the counter does not change the invariant $INV2()$. This means $INV2(\Sigma_{\mathcal{J}}, X_{\mathcal{J}})$ (with updated ctr) still holds.

□

Lemma 44 ($\mathcal{J}$ AM: 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, $\Sigma_{\mathcal{J}_1} = \Sigma'_{\mathcal{J}} \cdot \Phi'_{\mathcal{J}}$, $\Sigma_{\mathcal{J}_2} = \Sigma''_{\mathcal{J}} \cdot \Phi''_{\mathcal{J}}$ be two speculative states for the always mispredict semantics and $X_{\mathcal{J}_1}, X_{\mathcal{J}_2}$, be two speculative states for the speculative semantics.*

If the following conditions hold:

(1) $\Sigma_{\mathcal{J}_1} \cong \Sigma_{\mathcal{J}_2}$

(2) $X_{\mathcal{J}_1} \cong X_{\mathcal{J}_2}$ *and* $\overline{p} = \varnothing$

(3) $\Sigma_{\mathcal{J}_1} \approx_{O_{am}\mathcal{J}}^{\Sigma_1^{States}} X_{\mathcal{J}_1}$ *and* $\Sigma_{\mathcal{J}_2} \approx_{O_{am}\mathcal{J}}^{\Sigma_2^{States}} X_{\mathcal{J}_2}$

(4) $\Phi'_{\mathcal{J}} \overset{\tau''}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}_1}$ *and* $\Phi''_{\mathcal{J}} \overset{\tau''}{\rightsquigarrow}_{\mathcal{J}} \Sigma'_{\mathcal{J}_2}$ *and*

(5) $\Sigma'_{\mathcal{J}_1} \in \Sigma_1^{States}$ *and* $\Sigma'_{\mathcal{J}_2} \in \Sigma_2^{States}$

then there are instances $X'_{\mathcal{J}_1}, X'_{\mathcal{J}_2}$ for the speculative semantics such that:

I $X_{\mathcal{J}_1} \overset{O}{\leadsto}{}_{\tau}^{\mathcal{J}} X'_{\mathcal{J}_1}$ *and* $X_{\mathcal{J}_2} \overset{O}{\leadsto}{}_{\tau'}^{\mathcal{J}} X'_{\mathcal{J}_2}$

II $\Sigma'_{\mathcal{J}_1} \cong \Sigma'_{\mathcal{J}_2}$

III $X'_{\mathcal{J}_1} \cong X'_{\mathcal{J}_2}$ *and* $\overline{p} = \varnothing$

$IV\ \Sigma'_{\mathcal{J}_1} \approx^{\Sigma_1^{States}}_{O_{am}\mathcal{J}} X'_{\mathcal{J}_1}$ $and\ \Sigma'_{\mathcal{J}_2} \approx^{\Sigma_2^{States}}_{O_{am}\mathcal{J}} X'_{\mathcal{J}_2}$
$V\ \ \tau = \tau'$

Proof. The proof is very similar to Lemma 65 (S: Soundness Single Step AM). The only different thing 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., $INV2(\Sigma_{\mathcal{J}}, X_{\mathcal{J}})$

For these reasons, we will only argue why $INV2(\Sigma'_{\mathcal{J}_1}, X'_{\mathcal{J}_1})$ holds in the different cases and leave the rest to the old soundness proof.

Now we do case distinction on the instruction executed:

not indirect jump instruction Analogous to the corresponding case "not store instruction" in Lemma 69 (S AM: Strong Soundness Single Step)

Rule $\mathcal{J}$:AM-Spec We know that our oracle only mispredicts. That is why only rule $\mathcal{J}$:Spec will be used for oracle states.

$$
\begin{aligned}
X'_{\mathcal{J}_1} &= X'''_{\mathcal{J}} \cdot \Psi_{\mathcal{J}}\\
minWndw(X'''_{\mathcal{J}}) &= minWndw(decr(X'_{\mathcal{J}})) = minWndw(X'_{\mathcal{J}}) - 1\\
X'_{\mathcal{J}}.\sigma &\xrightarrow{\tau} X'''_{\mathcal{J}}.\sigma\\
\Sigma'_{\mathcal{J}_1} &= \Sigma'''_{\mathcal{J}} \cdot \Phi_{\mathcal{J}}\\
\Sigma'''_{\mathcal{J}}.n &= \Sigma'_{\mathcal{J}}.n - 1\\
\Sigma'_{\mathcal{J}}.\sigma &\xrightarrow{\tau} \Sigma'''_{\mathcal{J}}.\sigma
\end{aligned}
$$

Note that the step $minWndw(decr(X'_{\mathcal{J}})) = minWndw(X'_{\mathcal{J}}) - 1$ comes from the fact that $minWndw(X'_{\mathcal{J}}) = \Sigma'_{\mathcal{J}}.n$ and $\Sigma_{\mathcal{J}}.n > 0$ by assumption.

Depending on the output of the oracle we switch the relation

$O(p, \sigma, h) = (l, 0)$ We need to show that $INV2(\Sigma'''_{\mathcal{J}}, X'''_{\mathcal{J}})$ holds. The argument is the same as above for not indirect jump instruction. We now fulfil all premises to relate by Rule Single-Transaction-Rollback-Oracle.

$O(p, \sigma, h) = (l, \omega)$ We need to show that $INV2(\Sigma'''_{\mathcal{J}} \cdot \Phi_{\mathcal{J}}, X'''_{\mathcal{J}} \cdot \Phi_{\mathcal{J}})$ holds. The argument for $INV2(\Sigma'''_{\mathcal{J}}, X'''_{\mathcal{J}})$ is the same as above.

Furthermore, we know that $\Psi_{\mathcal{J}}.n = \omega$ by the output of the oracle and $\Phi_{\mathcal{J}}.n = \min(\omega, \Sigma'_{\mathcal{J}}.n - 1)$.

There are two cases depending on $\min(\omega, \Sigma_{\mathcal{J}}.n - 1)$.

$\Phi_{\mathcal{J}}.n = \omega$ Then by definition $\Sigma'_{\mathcal{J}}.n = \bot$ and from $\Sigma'_{\mathcal{J}} \sim X'_{\mathcal{J}}$ we get $|\Sigma'_{\mathcal{J}}| = |X'_{\mathcal{J}}| = 1$ and $X'_{\mathcal{J}}.n = \bot$. Otherwise, they would not be related.

Since $\bot > \omega$ and $\bot - 1 = \bot$, we have $minWndw(X'_{\mathcal{J}_1}) = \omega$ and $\Sigma'_{\mathcal{J}_1}.n = \omega$ and are finished.

$\Phi_{\mathcal{J}}.n = \Sigma'_{\mathcal{J}}.n - 1$ Then $n \neq \bot$ and we know that $\Sigma'''_{\mathcal{J}}.n = \Sigma'_{\mathcal{J}}.n - 1$.

Furthermore we know that $INV2(\Sigma'''_{\mathcal{J}}, X'''_{\mathcal{J}})$ holds.

So $minWndw(X'''_{\mathcal{J}}) = \Sigma'''_{\mathcal{J}}.n$. Since $\Sigma'''_{\mathcal{J}}.n < \omega$ we know that $minWndw(X'''_{\mathcal{J}}) < \omega$.

From this we can follow that $minWndw(X'_{\mathcal{J}_1}) < \omega$ (because $\Psi_{\mathcal{J}}.n = \omega$).

Now we have $minWndw(X'_{\mathcal{J}_1}) = minWndw(X'''_{\mathcal{J}} \cdot \Psi_{\mathcal{J}}) = minWndw(X'''_{\mathcal{J}})$ and $\Sigma'_{\mathcal{J}_1}.n = \Sigma'_{\mathcal{J}}.n - 1 = \Sigma'''_{\mathcal{J}}.n$.

Thus, by $INV2(\Sigma'''_{\mathcal{J}}, X'''_{\mathcal{J}})$ we have $INV2(\Sigma'_{\mathcal{J}_1}, X'_{\mathcal{J}_1})$

We can relate by Rule Single-Transaction-Rollback-Oracle.

□

J SEMANTICS FOR $\ghost_{S}$

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.

J.1 $\ghost_{S}$: Always Mispredict Semantics

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 `start` ctr and `rlb` ctr are now indexed by the speculative semantics they came from

Judgements

$\Sigma_{S} \xrightarrow{\tau}_{\ghost_{S}} \Sigma'_{S}$	State Σ_{S} small-steps to Σ'_{S} and emits observation τ.
$\Phi_{S} \xrightarrow{\tau}_{\ghost_{S}} \overline{\Phi}'_{S}$	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 $\overline{\tau}$.
$(p \times InitConf)\ \ghost^{\omega}_{S} \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$\boxed{\Sigma_{S} \xrightarrow{\tau}_{\ghost_{S}} \Sigma'_{S}}$

(S:AM-Context)
$$\frac{\Phi_{S} \xrightarrow{\tau}_{\ghost_{S}} \overline{\Phi}'_{S}}{\overline{\Phi}_{S} \cdot \Phi_{S} \xrightarrow{\tau}_{\ghost_{S}} \overline{\Phi}_{S} \cdot \overline{\Phi}'_{S}}$$

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

$\boxed{\Phi_{S} \xrightarrow{\tau}_{\ghost_{S}} \overline{\Phi}'_{S}}$

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

$$\frac{p(\sigma(\mathbf{pc})) \neq \mathbf{store}\ x, e, \mathbf{spbarr}, Z \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, n+1\rangle \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \langle p, ctr, \sigma', n\rangle}\ (\mathsf{S}\text{:AM-NoBranch}) \qquad \frac{\tau = \mathtt{bypass}\ n \mid \mathtt{start}_{\mathsf{S}}\ n}{\Phi_{\mathsf{S}}{}_{\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Phi_{\mathsf{S}}{}_{\overline{\rho}}}\ (\mathsf{S}\text{:AM-General})$$

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

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.

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

$$\frac{}{\Sigma_{\mathsf{S}} \Downarrow^{\varepsilon}_{\mathsf{S}} \Sigma_{\mathsf{S}}}\ (\mathsf{S}\text{:AM-Reflection}) \qquad \frac{\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}}_{\mathsf{S}} \Sigma''_{\mathsf{S}} \qquad \Sigma''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Sigma'_{\mathsf{S}}}{\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}\cdot\tau}_{\mathsf{S}} \Sigma'_{\mathsf{S}}}\ (\mathsf{S}\text{:AM-Single})$$

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

$\boxed{Helpers}$

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

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

$\boxed{(p \times InitConf) \Downarrow^{\omega}_{\mathsf{S}} \overline{\tau}}$

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

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

J.2 $\rightsquigarrow_{\mathsf{S}}$: Oracle Semantics

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:

$$\textit{Speculative States } X_{\mathsf{S}} ::= \overline{\Psi}_4$$

$$\textit{Speculative Instance } \Psi_{\mathsf{S}} ::= \langle p, ctr, \sigma, h, n\rangle^{b}_{\overline{\rho}} \text{ where } b \in \{\text{true}, \text{false}, \varepsilon\}$$

$$\tau ::= .. \mid \texttt{commit}_{\mathsf{S}}\ ctr$$

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 $\texttt{commit}_{\mathsf{S}}\ ctr$ observation. The ctr is used to annotate traces so one can find $\texttt{start}_{\mathsf{S}}\ ctr$, $\texttt{rlb}_{\mathsf{S}}\ ctr$ and $\texttt{commit}_{\mathsf{S}}\ ctr$ pairs.

Judgements

$X_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X'_{\mathsf{S}}$	State X_{S} small-steps to X'_{S} and emits observation τ.
$\Phi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} \overline{\Phi}'_{\mathsf{S}}$	Speculative instance Ψ_{S} small-steps to $\overline{\Psi}_4{}'$ and emits observation τ.
$X_{\mathsf{S}} \ {}^{O}\Downarrow^{\mathsf{S}}_{\overline{\tau}} X'_{\mathsf{S}}$	State X_{S} big-steps to X'_{S} and emits a list of observations $\overline{\tau}$.
$(p \times \mathit{InitConf}) \Downarrow^{O}_{\mathsf{S}} \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$\boxed{X_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X'_{\mathsf{S}}}$

(S:SE-Context)

$$\frac{\Psi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} \overline{\Psi}_4{}' \qquad \Psi_{\mathsf{S}} = \langle p, ctr, \sigma, h, n\rangle \qquad \text{if } p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \text{ then } \overline{\Psi}_{41} = \mathit{zeroes}(\overline{\Psi}_4) \text{ else } \overline{\Psi}_{41} = \mathit{decr}(\overline{\Psi}_4)}{\overline{\Psi}_4 \cdot \Psi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} \overline{\Psi}_{41} \cdot \overline{\Psi}_4{}'}$$

(S:Rollback)

$$\frac{n' = 0 \text{ or p is stuck}}{\overline{\Psi}_4 \cdot \langle p, ctr, \sigma, h, n\rangle \cdot \langle p, ctr', \sigma', h', n'\rangle^{true} \cdot \overline{\Psi}'_4 \overset{\texttt{rlb}\ ctr}{\rightsquigarrow}{}^{O}_{\mathsf{S}} \overline{\Psi}_4 \cdot \langle p, ctr', \sigma, h, n\rangle}$$

(S:Commit)

$$\frac{}{\overline{\Psi}_4 \cdot \langle p, ctr, \sigma, h, n\rangle^{b} \cdot \langle p, ctr', \sigma', h', 0\rangle^{false} \cdot \overline{\Psi}_4{}' \overset{\texttt{commit}_{\mathsf{S}}\ ctr}{\rightsquigarrow}{}^{O}_{\mathsf{S}} \overline{\Psi}_4 \cdot \langle p, ctr', \sigma', h', n\rangle^{b} \cdot \overline{\Psi}_4{}'}$$

(S:General)

$$\frac{\tau = \texttt{bypass}\ n \mid \texttt{start}\ n}{\overline{\Psi}_4 \cdot \Psi_{\mathsf{S}\,\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} \overline{\Psi}_4 \cdot \Psi_{\mathsf{S}\,\overline{\rho}}}$$

$\boxed{\Psi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} \Psi'_{\mathsf{S}}}$

(S:barr)

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

(S:barr-spec)

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

(S:NoBranch)

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

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

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

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

$$\boxed{X_{\mathsf{S}} \ {}^{O}\!\!\Downarrow^{\mathsf{S}}_{\overline{\tau}} X'_{\mathsf{S}}}$$

$$\frac{}{X_{\mathsf{S}} \ {}^{O}\!\!\Downarrow^{\mathsf{S}}_{\varepsilon} X_{\mathsf{S}}} \ (\mathsf{S}\text{:Reflection}) \qquad \frac{X_{\mathsf{S}} \ {}^{O}\!\!\Downarrow^{\mathsf{S}}_{\overline{\tau}} X''_{\mathsf{S}} \quad X''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X'_{\mathsf{S}}}{X_{\mathsf{S}} \ {}^{O}\!\!\Downarrow^{\mathsf{S}}_{\overline{\tau} \cdot \tau} X'_{\mathsf{S}}} \ (\mathsf{S}\text{:Single})$$

where $X_{\mathsf{S}} \ {}^{O}\!\!\Downarrow^{\mathsf{S}}_{\overline{\tau}} X'_{\mathsf{S}}$ 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.

$$\boxed{Helpers}$$

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

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

$$\boxed{(p \times InitConf) \ \Omega^{O}_{\mathsf{S}} \overline{\tau}}$$

$$\frac{\exists X'_{\mathsf{S}} \quad \vdash X'_{\mathsf{S}} : fin \quad X^{init}_{\mathsf{S}}(p, \sigma) \ {}^{O}\!\!\Downarrow^{\mathsf{S}}_{\overline{\tau}} X'_{\mathsf{S}}}{(p, \sigma) \ \Omega^{O}_{\mathsf{S}} \overline{\tau}} \ (\mathsf{S}\text{:SE-Trace}) \qquad \frac{}{Beh^{O}_{\mathsf{S}}(p) = \{\overline{\tau} \mid \forall \sigma \in InitConf.\ (p, \sigma) \ \Omega^{O}_{\mathsf{S}} \overline{\tau}\}} \ (\mathsf{S}\text{:SE-Beh})$$

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

J.3 Ω_{S}: 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 $\Sigma^{\mathcal{S}}_{\mathsf{S}}$.

$$\boxed{\Sigma^{\mathcal{S}}_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}\Omega^{\mathcal{S}}_{\mathsf{S}} \ \Sigma^{\mathcal{S}\prime}_{\mathsf{S}}}$$

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

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

$$\boxed{\Phi^{\mathcal{S}}_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \overline{\Phi}'_{\mathsf{S}_{\mathcal{S}}}}$$

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

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

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

(S:Sym-General)
$$\frac{\tau = \mathtt{bypass}\ n \mid \mathtt{start}_{\mathsf{S}}\ n}{\Phi^{\mathcal{S}}_{\mathsf{S}\ \overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathsf{S}} \Phi^{\mathcal{S}}_{\mathsf{S}\ \overline{\rho}}}$$

(S:Sym-Store-Spec)
$$\frac{\begin{array}{cc} p(\sigma(\mathbf{pc})) = \mathbf{store}\ x, e & \sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}} \\ \sigma''_{\mathcal{S}} = \sigma[\mathbf{pc} \mapsto \sigma(\mathbf{pc}) + 1] \quad \sigma''_{\mathcal{S}}.\delta^{\mathcal{S}} = \sigma'_{\mathcal{S}}.\delta^{\mathcal{S}} & j = min(\omega, n) \end{array}}{\langle p, ctr, \sigma_{\mathcal{S}}, n+1\rangle_{\overline{\rho}} \overset{\tau}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathsf{S}} \langle p, ctr, \sigma'_{\mathcal{S}}, n\rangle_{\overline{\rho}} \cdot \langle p, ctr+1, \sigma'', j\rangle_{\overline{\rho}\cdot\mathtt{bypass}\ \sigma(\mathbf{pc})\cdot\mathtt{start}_{\mathsf{S}}\ ctr}}$$

$$\boxed{\Sigma^{\mathcal{S}}_{\mathsf{S}}\ {}_{\mathcal{S}}{\Downarrow}^{\overline{\tau}}_{\mathsf{S}}\ \Sigma^{\mathcal{S}\prime}_{\mathsf{S}}}$$

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

(S:Sym-Single)
$$\frac{\Sigma_{\mathsf{S}}\ {}_{\mathcal{S}}{\Downarrow}^{\overline{\tau}}_{\mathsf{S}}\ \Sigma''_{\mathsf{S}} \qquad \Sigma''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathsf{S}} \Sigma'_{\mathsf{S}}}{\Sigma^{\mathcal{S}}_{\mathsf{S}}\ {}_{\mathcal{S}}{\Downarrow}^{\overline{\tau}\cdot\tau_{\mathcal{S}}}_{\mathsf{S}}\ \Sigma^{\mathcal{S}\prime}_{\mathsf{S}}}$$

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

$$\boxed{Helpers}$$

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

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

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

$$\boxed{(p \times InitConf)\ {}_{\mathcal{S}}\Omega^{\omega}_{\mathsf{S}}\ \overline{\tau}}$$

(S:Sym-Trace)
$$\frac{\exists\Sigma'_{\mathsf{S}} \qquad \vdash \Sigma'_{\mathsf{S}} : fin \qquad \Sigma^{0}_{\mathsf{S}}(p, \sigma)\ {}_{\mathcal{S}}{\Downarrow}^{\overline{\tau}}_{\mathsf{S}}\ \Sigma'_{\mathsf{S}}}{(p, \sigma_{\mathcal{S}})\ {}_{\mathcal{S}}\Omega^{\omega}_{\mathsf{S}}\ \overline{\tau}}$$

(S:Sym-Beh)
$$\frac{}{Beh^{\mathcal{S}}_{\mathsf{S}}(p) = \{\overline{\tau} \mid \forall\sigma_{\mathcal{S}} \in InitConf.\ (p, \sigma)\ {}_{\mathcal{S}}\Omega^{\omega}_{\mathsf{S}}\ \overline{\tau}\}}$$

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

K PROOFS FOR 👻$_{\mathsf{S}}$:

Our main result for 👻$_{\mathsf{S}}$ is the following

Theorem 11 (👻$_{\mathsf{S}}$ is *WFSS*). $\vdash$ 👻$_{\mathsf{S}}$ *WFSS*

Proof. Immediately follows from Theorem 15 (S: Oracle Overapproximation), Theorem 14 (S: Behaviour of AM and symbolic semantics), Theorem 13 (S AM: Behaviour of non-speculative semantics and AM semantics) and Theorem 12 (S SE: Behaviour of non-speculative and oracle semantics). □

K.1 S: Relating Non-speculative and Oracle Semantics

- Theorem 12 (S SE: Behaviour of non-speculative and oracle semantics)
  - Lemma 49 (S SE: Completeness of the speculative semantics)
    - Lemma 50 (S SE: Non-speculative execution for rolled back transactions)
  - Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics)
    - Lemma 46 (S SE: Soundness single step No Speculation)
      - Lemma 47 (S SE: Single Step Instance Non Speculative)
    - Lemma 48 (S SE: Store step)

Theorem 12 (S SE: Behaviour of non-speculative and oracle semantics). *Let p be a program and O be a prediction oracle. Then $Beh_{NS}(p) = Beh^{O}_{\mathsf{S}}(p)\restriction_{ns}$*

Proof. We prove the two directions separately:

$\Leftarrow$ Assume that $\overline{\tau} \in Beh^{O}_{\mathsf{S}}(p)$.

By the definition of $Beh^{O}_{\mathsf{S}}(p)$ we have an initial configuration σ such that $((p,\sigma))$ 👻$^{O}_{\mathsf{S}}\overline{\tau}$.

By definition of (p,σ) 👻$^{O}_{\mathsf{S}}\overline{\tau}$, we know there exists a state X'_{S} such that $\vdash X'_{\mathsf{S}}: \mathit{fin}$ and an initial state $\Sigma^{init}_{\mathsf{S}}(p,\sigma)$ such that $\Sigma^{init}_{\mathsf{S}}(p,\sigma) \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}} X'_{\mathsf{S}}$.

We apply Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) with $\Sigma^{init}_{\mathsf{S}}(p,\sigma) \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}} X'_{\mathsf{S}}$, because $\Sigma^{init}_{\mathsf{S}}(p,\sigma)$ 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 $\vdash_{O} X'_{\mathsf{S}}: \mathit{noongoing}$ then $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}} \sigma'$ and
(3) if $\vdash^{i}_{O} X'_{\mathsf{S}}: \mathit{biggestongoingtransactionirolledback}$ 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 $\vdash X'_{\mathsf{S}} : \mathit{fin}$, we have $\vdash_O X'_{\mathsf{S}} : \mathit{noongoing}$ and as such $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}} \sigma'$ by 2).
Since X'_{S} has only one instance, we have $X'_{\mathsf{S}}.\sigma = \sigma'$.
Furthermore, because of $\vdash X'_{\mathsf{S}} : \mathit{fin}$, we know $X'_{\mathsf{S}}.\sigma \in \mathit{FinalConf}$.
We can now conclude that $((p,\sigma))\,⍾_{NS}\overline{\tau}\upharpoonright_{ns} \in \mathit{Beh}_{NS}(p)$ by Rule NS-Trace.

$\Rightarrow$ Assume that $((p,\sigma))\,⍾^{O}_{\mathsf{S}}\overline{\tau} \in \mathit{Beh}_{NS}(p)$. We thus know there exists $\sigma' \in \mathit{FinalConf}$ such that $\sigma \Downarrow_{\overline{\tau}} \sigma'$.

Let $X_{\mathsf{S}} = X^{\mathit{init}}_{\mathsf{S}}(p,\sigma)$. We now apply Lemma 49 (S SE: Completeness of the speculative semantics) and get

(1) X'_{S} with $\vdash_O X_{\mathsf{S}} : \mathit{noongoing}$
(2) $\sigma' = X'_{\mathsf{S}}.\sigma$
(3) $X_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}'} X'_{\mathsf{S}}$ and
(4) $\overline{\tau} = \overline{\tau}'\upharpoonright_{ns}$.

Since $\sigma' \in \mathit{FinalConf}$, we know that $X'_{\mathsf{S}}.\sigma \in \mathit{FinalConf}$.
We now show how we can reach a final state X''_{S}. We apply Lemma 8 (Reaching Final state from final configuration (Finish commit instances)) on X'_{S} and get

(1) $X'_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}''} X''_{\mathsf{S}}$
(2) $\forall \tau \in \overline{\tau}''.\ \tau = \texttt{commit}\ \mathit{id}$ for some $\mathit{id} \in \mathbb{N}$
(3) $\vdash X''_{\mathsf{S}} : \mathit{fin}$
(4) $X'_{\mathsf{S}}.\sigma = X''_{\mathsf{S}}.\sigma$

We now have an execution $X_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}'\cdot\overline{\tau}''} X''_{\mathsf{S}}$, since the oracle semantics are deterministic.
Note that by 2) we have $\overline{\tau}''\upharpoonright_{ns} = \varepsilon$ and thus $\overline{\tau}'\cdot\overline{\tau}''\upharpoonright_{ns} = \overline{\tau}'\upharpoonright_{ns}$.
By 3) we have that $\vdash X''_{\mathsf{S}} : \mathit{fin}$.
We thus have $((p,\sigma))\,⍾^{O}_{\mathsf{S}}\overline{\tau}'\cdot\overline{\tau}'' \in \mathit{Beh}^{O}_{\mathsf{S}}(p)$.

□

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.

K.1.1 Soundness.

Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics)**.** *If*

(1) $X_{\mathsf{S}}.\sigma = \sigma$ *and*
(2) $\vdash_O X_{\mathsf{S}} : \mathit{noongoing}$ *and*
(3) $X_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}} X'_{\mathsf{S}}$

Then there exists σ' *such that*

I if $\vdash_O X'_{\mathsf{S}} : \mathit{noongoing}$ *then* $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}\sigma'}$ *and (if* $\texttt{start}\ \mathit{id} \in X'_{\mathsf{S}}.\overline{p}$ *then* $X'_{\mathsf{S}} = \overline{\Psi}_4 \cdot \langle p, \mathit{ctr}, \sigma', h, n\rangle$ *and* $\overline{\Phi}_{\mathsf{S}}.\sigma = \sigma'$ *else* $X'_{\mathsf{S}}.\sigma = \sigma'$*) and*

II if $\vdash^{i}_{O} X'_{\mathsf{S}}$: 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 with the instance with ctr = i.

Proof. We proceed by induction on $X_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}} X'_{\mathsf{S}}$

Rule S:Reflection Then we have $X_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\varepsilon} X_{\mathsf{S}}$ with $X'_{\mathsf{S}} = X_{\mathsf{S}}$ 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:Single We have $X_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}'\cdot\tau} X'_{\mathsf{S}}$ and by Rule S:Single we get $X_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}'} X''_{\mathsf{S}}$ and $X''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X'_{\mathsf{S}}$.

We need to prove

I if $\vdash_{O} X'_{\mathsf{S}}$: *noongoing* then $\sigma \Downarrow_{\overline{\tau}\cdot\tau\restriction_{ns}\sigma'}$ and $X'_{\mathsf{S}}.\sigma = \sigma'$

II if $\vdash^{i}_{O} X'_{\mathsf{S}}$: *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 $X_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}'} X''_{\mathsf{S}}$ and have a σ'' where σ'' is the configuration for some instance in X''_{S} such that.

I' if $\vdash_{O} X''_{\mathsf{S}}$: *noongoing* then $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}\sigma''}$ and $X''_{\mathsf{S}}.\sigma = \sigma''$

II' if $\vdash^{j}_{O} X''_{\mathsf{S}}$: *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 X''_{S}.

no ongoing transactions in X''_{S} Then X''_{S} has no ongoing transactions, meaning $\vdash_{O} X''_{\mathsf{S}}$: *noongoing* and we have $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}} \sigma''$ and $X''_{\mathsf{S}}.\sigma = \sigma''$ by IH.

I Then $\vdash_{O} X'_{\mathsf{S}}$: *noongoing* and we need to proof $\sigma \Downarrow_{\overline{\tau}\cdot\tau\restriction_{ns}\sigma'}$ and $X'_{\mathsf{S}}.\sigma = \sigma'$. We now proceed by inversion on $X''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X'_{\mathsf{S}}$:

Rule S:Rollback Then $\tau = \texttt{rlb}$ *id*.

Contradiction. Since $\vdash_{O} X''_{\mathsf{S}}$: *noongoing* there does not exists a `rlb` *id* observation that does not have a corresponding `start` *id* observation in the execution $X_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}} X''_{\mathsf{S}}$. So $\tau \neq \texttt{rlb}$ *id*.

Rule S:Store-Skip Then we know that $\overline{\rho} = \texttt{bypass}\ X''_{\mathsf{S}}.\sigma(\mathbf{pc}) \cdot \texttt{start}\ id$ for X'_{S}. Contradiction. Since $\vdash_{O} X'_{\mathsf{S}}$: *noongoing*, there exists a `start` *id* for every `rlb` *id* in the execution $X'_{\mathsf{S}\overline{\rho}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}_{fin}} X_{\mathsf{S}fin}$ and $\nexists \texttt{start}\ id \in \overline{\rho}.\ \texttt{rlb}\ id \in \overline{\tau}$

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 $\sigma'' = X''_{\mathsf{S}}.\sigma$.

Since $\vdash_{O} X''_{\mathsf{S}}$: *noongoing*, there no ongoing transactions that need to be rolled back.

Furthermore, no transaction that will be rolled back is created in the step $X''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X'_{\mathsf{S}}$, because $\vdash_{O} X'_{\mathsf{S}}$: *noongoing*.

We can now apply Lemma 46 (S SE: Soundness single step No Speculation) with $X''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X'_{\mathsf{S}}$ and get

$$\sigma'' \Downarrow_{\tau\upharpoonright_{ns}} \sigma'$$
$$X'_{\mathsf{S}}.\sigma = \sigma'$$

Since $\overline{\tau}\upharpoonright_{ns} \cdot \tau\upharpoonright_{ns} = \overline{\tau} \cdot \tau\upharpoonright_{ns}$ (because $\tau \neq \texttt{rlb}\ id$), we are finished.

II Then X'_{S} has ongoing transactions, meaning $\vdash^{i}_{O} X'_{\mathsf{S}} :$ *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 $X''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X'_{\mathsf{S}}$:

Rule S:Store-Skip Then we know that $\overline{p} = \texttt{bypass}\ X''_{\mathsf{S}}.\sigma(\mathbf{pc}) \cdot \texttt{start}\ id$ 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 $\vdash_{O} X''_{\mathsf{S}} :$ *noongoing*, so there was not another ongoing transaction.

We can now apply Lemma 48 (S SE: Store step) and get

$$\sigma'' \xrightarrow{\texttt{store}\ m\upharpoonright_{ns}} \sigma'$$

σ' is the configuration for the instance with $ctr = i$ in X'_{S}

By IH we have $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}} \sigma''$ where $X''_{\mathsf{S}}.\sigma = \sigma''$.

Using $\sigma'' \xrightarrow{\texttt{store}\ m\upharpoonright_{ns}} \sigma'$ we get $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}\cdot\texttt{store}\ m\upharpoonright_{ns}} \sigma'$.

Since $\vdash_{O} X''_{\mathsf{S}} :$ *noongoing* we have $\texttt{store}\ m\upharpoonright_{ns} = \texttt{store}\ m$ and thus $\overline{\tau}\upharpoonright_{ns} \cdot \texttt{store}\ m = \overline{\tau} \cdot \texttt{store}\ m\upharpoonright_{ns}$.

We are now finished.

otherwise By definition of $\vdash^{i}_{O} X'_{\mathsf{S}} :$ *biggestongoingtransactionirolledback* we know that there exists a $\texttt{rlb}\ i$ in the execution $X'_{\mathsf{S}} \overset{O}{\Downarrow}{}^{\mathsf{S}}_{\overline{\tau}_{fin}} X_{\mathsf{S}fin}$ with no matching $\texttt{start}\ i$ observation in that execution.

This means the $\texttt{start}\ i$ has to happen before in the execution $X_{\mathsf{S}} \overset{O}{\Downarrow}{}^{\mathsf{S}}_{\overline{\tau}\cdot\tau} X'_{\mathsf{S}}$.

By definition of $\vdash_{O} X''_{\mathsf{S}} :$ *noongoing*, we have that all $\texttt{rlb}\ id'$ have a matching $\texttt{start}\ id'$ in the execution $X''_{\mathsf{S}} \overset{O}{\Downarrow}{}^{\mathsf{S}}_{\tau\cdot\overline{\tau}_{fin}} X_{\mathsf{S}fin}$.

Now we have a contradiction, since $\texttt{rlb}\ i$ does not have a matching $\texttt{start}\ i$.

ongoing transactions in X''_{S} Then X''_{S} has ongoing transactions, meaning $\vdash^{j}_{O} X''_{\mathsf{S}} :$ *biggestongoingtransactionirolledback* and we have $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$ and σ'' is the configuration for the instance with $ctr = j$.

I Then $\vdash_{O} X'_{\mathsf{S}} :$ *noongoing* and we need to prove $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ and $X'_{\mathsf{S}}.\sigma = \sigma'$. We now proceed by inversion on $X''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X'_{\mathsf{S}}$:

Rule S:Rollback and $\tau = \texttt{rlb}\ j$ Choose $\sigma' = \sigma''$. Since $\overline{\tau} \cdot \tau\upharpoonright_{ns} = helper(\overline{\tau}, j)$ we can use IH $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$ and Rule NS-Reflection.

The rollback 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 rollback.

So $X'_{\mathsf{S}}.\sigma = \sigma''$ and we are finished.

otherwise Then $\tau \neq \texttt{rlb}\ j$.

Since $\vdash_O X'_{\mathsf{S}}$: *noongoing*, there does not exists `rlb` *id* without matching `start` *id* in the execution $X'_{\mathsf{S}} \overset{O}{\Downarrow}{}^{\mathsf{S}}_{\overline{\tau}_{fin}} X_{\mathsf{S}}fin$.

Because $\vdash^j_O X''_{\mathsf{S}}$: *biggestongoingtransactionirolledback*, there exists a a smallest `rlb` j that does not have a `start` j in the execution $X''_{\mathsf{S}} \overset{O}{\Downarrow}{}^{\mathsf{S}}_{\tau\cdot\overline{\tau}_{fin}} X_{\mathsf{S}}fin$.

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 $X'_{\mathsf{S}} \overset{O}{\Downarrow}{}^{\mathsf{S}}_{\overline{\tau}_{fin}} X_{\mathsf{S}}fin$.

II Then $\vdash^i_O X'_{\mathsf{S}}$: *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 $X''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X'_{\mathsf{S}}$:

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 46 (S SE: Soundness single step No Speculation)**.** *If*

(1) $\vdash_O X_{\mathsf{S}}$: *noongoing and*
(2) $X_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X'_{\mathsf{S}}$ *and*
(3) $\vdash_O X'_{\mathsf{S}}$: *noongoing and*
(4) $\sigma = X_{\mathsf{S}}.\sigma$

Then there exists σ' *such that*

I $\sigma \Downarrow_{\tau\restriction_{ns}} \sigma'$ *and*
II $X'_{\mathsf{S}}.\sigma = \sigma'$

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 $X_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X'_{\mathsf{S}}$:

Rule S:General Thus we have $X_{\mathsf{S}} = \overline{\Psi}_4 \cdot \Psi_{\mathsf{S}\overline{\rho}\cdot\tau}$ and $X'_{\mathsf{S}} = \overline{\Psi}_4 \cdot \Psi_{\mathsf{S}\overline{\rho}}$ with $\Psi_{\mathsf{S}}.\sigma = \sigma$.

By the definition of $\Psi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X_{\mathsf{S}}$ only Rule S:Store-Skip and Rule S:Store-Exe add observations to $\overline{\rho}$.

These observations are either $\texttt{start}_{\mathsf{S}}$ *id* or $\texttt{bypass}$ *n*.

By the definition of $\upharpoonright_{ns}$ we have $\tau\upharpoonright_{ns} = \varepsilon$ and we have $\sigma \Downarrow_{\varepsilon\upharpoonright_{ns}} \sigma$ by Rule NS-Reflection.

Rule S:Commit Then the generated observation is $\tau = \texttt{commit}\ id$. Furthermore, $\texttt{commit}\ id\upharpoonright_{ns} = \varepsilon$

By the definition of the rule, we have $X_{\mathsf{S}}.\sigma = X'_{\mathsf{S}}.\sigma$ and with this we get $X'_{\mathsf{S}}.\sigma = \sigma$.

Thus, we can derive $\sigma \Downarrow_{\texttt{commit}\ id\upharpoonright_{ns}} \sigma$.

Rule S:Rollback Contradiction, since $\vdash_O X_{\mathsf{S}}$: *noongoing* and Definition 18 (Well orderedness of rollback and start).

Rule S:SE-Context Thus we have $X_{\mathsf{S}} = \overline{\Psi}_4 \cdot \Psi_{\mathsf{S}}$ and $X'_{\mathsf{S}} = \overline{\Psi}_4 \cdot \overline{\Psi}'_4$ with $\Psi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} \overline{\Psi}'_4$. By Lemma 47 (S SE: Single Step Instance Non Speculative) we have $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma$ with $\sigma = \Psi_{\mathsf{S}}.\sigma$ and $\overline{\Psi}'_4.\sigma = \sigma$.

□

Lemma 47 (S SE: Single Step Instance Non Speculative)**.** *If*

(1) $X_{\mathsf{S}} = \overline{\Psi}_4 \cdot \Psi_{\mathsf{S}}$ *and*
(2) $X'_{\mathsf{S}} = \overline{\Psi}_4 \cdot \overline{\Psi}'_4$ *and* $\vdash_O X'_{\mathsf{S}}$: *noongoing and*
(3) $\Psi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} \overline{\Psi}'_4$ *and*
(4) $\sigma = \Psi_{\mathsf{S}}.\sigma$

Then there is a σ' such that

I $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma'$ *and*
II $\overline{\Psi}'_4.\sigma = \sigma$

Proof. We proceed by case analysis on the rule used to derive $\Psi''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} \Psi'_{\mathsf{S}}$.

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 $\overline{\Psi}'_4 = \langle p, ctr, \sigma', h, n-1\rangle$.

Thus $\sigma' = \overline{\Psi}'_4.\sigma$ and $\tau = \varepsilon = \varepsilon\upharpoonright_{ns}$.

Rule S:NoBranch We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule and $\overline{\Psi}'_4 = \langle p, ctr, \sigma', h, n-1\rangle$.

Thus, $\sigma' = \overline{\Psi}'_4.\sigma$.

Because the rule used the observation received from the step $\sigma \xrightarrow{\tau} \sigma'$, we have $\tau\upharpoonright_{ns} = \tau$ and are finished.

Rule S:Store-Skip Contradiction, because there are no ongoing transactions in X'_{S} by the fact $\vdash_O X'_{\mathsf{S}}$: *noongoing*.

Rule S:Store-Exe By definition $\overline{\Psi}'_4 = \langle p, ctr, \sigma', h, n\rangle \cdot \langle p, ctr', \sigma', h', n'\rangle_{\overline{\rho}}$. By premise of the rule we do the step $\sigma \xrightarrow{\tau'} \sigma'$.

The generated trace is $\tau = \tau'$ and $\tau\upharpoonright_{ns} = \tau'$. Thus the step $\sigma \xrightarrow{\tau'} \sigma'$ is what we look for and by construction $\overline{\Psi}'_4.\sigma = \sigma'$.

□

Lemma 48 (S SE: Store step)**.** *If*

(1) $X_{\mathsf{S}} = \overline{\Psi}_4 \cdot \Psi_{\mathsf{S}}$ *and* $\vdash_O X_{\mathsf{S}}$: *noongoing*
(2) $X'_{\mathsf{S}} = \overline{\Psi}_4 \cdot \overline{\Psi}'_4$ *and* $\vdash^i_O X'_{\mathsf{S}}$: *biggestongoingtransactionirolledback and*

(3) $\Psi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} \overline{\Psi}'_4$ *and*

(4) $\sigma = \Psi_{\mathsf{S}}.\sigma$

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 $\Psi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{S}} \overline{\Psi}'_4$:

Rule S:Store-Skip By definition $\overline{\Psi}'_4 = \langle p, ctr, \sigma_1, h, n\rangle \cdot \langle p, ctr+1, \sigma_2, h', n'\rangle_{\texttt{start}\ ctr \cdot \texttt{bypass}\ \sigma_1(\mathbf{pc})} \cdot$

By premise of the rule we do the step $\sigma \xrightarrow{\texttt{store}\ m} \sigma_1$ for some $m \in \mathbb{N}$. Since $\vdash_O X_{\mathsf{S}} :$ *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 $\vdash_O X_{\mathsf{S}} :$ *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 $\vdash_O X_{\mathsf{S}} :$ *noongoing* and $\vdash^i_O X'_{\mathsf{S}} :$ *biggestongoingtransactionirolledback*, we know that a transaction has to be started that will be rolled back.

□

K.1.2 Completeness.

Lemma 49 (S SE: Completeness of the speculative semantics)**.** *If*

(1) $\sigma \in$ *InitConf and*

(2) $\sigma \Downarrow_{\overline{\tau}} \sigma'$ *and*

(3) $X_{\mathsf{S}} = X^{init}_{\mathsf{S}}(p, \sigma)$

Then

I $X_{\mathsf{S}} \overset{O}{\Downarrow}{}^{\mathsf{S}}_{\overline{\tau}'} X'_{\mathsf{S}_\rho}$ *and*

II $\vdash_O X'_{\mathsf{S}} :$ *noongoing and*

III $\sigma' = X'_{\mathsf{S}}.\sigma$ *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 $X_{\mathsf{S}} \overset{O}{\Downarrow}{}^{\mathsf{S}}_{\varepsilon} X_{\mathsf{S}}$. By construction $\vdash_O X_{\mathsf{S}} :$ *noongoing* and $X_{\mathsf{S}}.\sigma = \sigma$. 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 $X_{\mathsf{S}} \overset{O}{\Downarrow}{}^{\mathsf{S}}_{\overline{\tau}' \cdot \tau'} X'_{\mathsf{S}}$ and

II $\vdash_O X'_{\mathsf{S}} :$ *noongoing* and

III $\sigma' = X'_{\mathsf{S}}.\sigma$ and

IV $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \upharpoonright_{ns}$

We apply the IH on $\sigma \Downarrow_{\overline{\tau}} \sigma''$ we get

I' $X_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}'} X''_{\mathsf{S}\;\rho}$ and

II' $\vdash_O X''_{\mathsf{S}\;\rho}$: *noongoing* and

III' $\sigma'' = X''_{\mathsf{S}}.\sigma$ and

IV' $\overline{\tau} = \overline{\tau}' \upharpoonright_{ns}$

V' $\rho = \varepsilon$

To account for possible outstanding commits, we use Lemma 9 (Executing a chain of commits) on X''_{S} and get

a) $X''_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}'''} X'''_{\mathsf{S}}$

b) $minWndw(X'''_{\mathsf{S}}) > 0$

c) $\forall \tau \in \overline{\tau}'''. \tau = \texttt{commit}\ id$ for some $id \in \mathbb{N}$

d) $X''_{\mathsf{S}}.\sigma = X'''_{\mathsf{S}}.\sigma$

By c) and the definition of $\upharpoonright_{ns}$ we have $\overline{\tau}''' \upharpoonright_{ns} = \varepsilon$.

Because only Rule S:Commit was used we have $X'''_{\mathsf{S}} \cdot \overline{\rho} = X''_{\mathsf{S}} \cdot \overline{\rho}$.

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 $X'''_{\mathsf{S}} \overset{\tau'}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X^n_{\mathsf{S}}$.

Here, τ' is generated from $X'''_{\mathsf{S}}.\sigma \xrightarrow{\tau'} \sigma'$ and $X^n_{\mathsf{S}}.\sigma = \sigma'$

Since $\rightarrow$ is deterministic, we know that $\tau' = \tau$.

II Since no speculative transaction is started and we have $\vdash_O X''_{\mathsf{S}}$: *noongoing* by IH, we have $\vdash_O X^n_{\mathsf{S}}$: *noongoing*.

III By definition and determinism of $\rightarrow$.

IV Now we have $X''_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau'} X^n_{\mathsf{S}}$. Looking at the trace that is generated we have

$$\begin{aligned}
&\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau' \upharpoonright_{ns} \tau' = \tau \\
=&\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau \upharpoonright_{ns} \tau \text{ generated by} \rightarrow \\
=&\overline{\tau}' \cdot \overline{\tau}''' \upharpoonright_{ns} \cdot \tau\ \overline{\tau}''' \upharpoonright_{ns} = \varepsilon \\
=&\overline{\tau}' \upharpoonright_{ns} \cdot \tau \text{ by IH} \\
=&\overline{\tau} \cdot \tau
\end{aligned}$$

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 $X''_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\tau \cdot \texttt{start}\ id} X^n_{\mathsf{S}}$ 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 $X'''_{\mathsf{S}}.\sigma \xrightarrow{\tau} \sigma'$ is made.

II No speculative transaction was started that needs to be rolled back. By $\vdash_O X''_{\mathsf{S}}$: *noongoing* and $\vdash_O X'''_{\mathsf{S}}$: *noongoing* we get $\vdash_O X^n_{\mathsf{S}}$: *noongoing*.

III By definition and determinism of $\longrightarrow$.

IV We now have:

$$\begin{aligned}
&\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau' \cdot \texttt{start}\ id \upharpoonright_{ns} \text{Def. and } \overline{\tau}''' \upharpoonright_{ns} = \varepsilon \\
&= \overline{\tau}' \cdot \tau' \upharpoonright_{ns} \tau' = \tau \\
&= \overline{\tau}' \cdot \tau \upharpoonright_{ns} \tau \text{ generated by} \longrightarrow \\
&= \overline{\tau}' \upharpoonright_{ns} \cdot \tau \text{ by IH} \\
&= \overline{\tau} \cdot \tau
\end{aligned}$$

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 $X'''_{\mathsf{S}}.\sigma \xrightarrow{\tau''} \sigma'''$ is made.

Since $\longrightarrow$ is deterministic and the fact that $\sigma'' \xrightarrow{\tau''} \sigma'''$, $\sigma'' \xrightarrow{\tau} \sigma'$ and $X'''_{\mathsf{S}}.\sigma = \sigma''$, 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 $X'''_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\tau' \cdot \texttt{start}\ id \cdot \texttt{bypass}\ n} X_{\mathsf{S}3}$.

Since all transactions are eventually closed, we know there exists X^n_{S} such that $X^3_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}^n \cdot \texttt{rlb}\ id} X^n_{\mathsf{S}}$.

We now apply Lemma 50 (S SE: Non-speculative execution for rolled back transactions) on the execution $X'''_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\tau' \cdot \texttt{start}\ id \cdot \texttt{bypass}\ n \cdot \overline{\tau}^n \cdot \texttt{rlb}\ id} X^n_{\mathsf{S}}$ and get $\sigma'' \xrightarrow{\tau''} \sigma'''$ and $X^n_{\mathsf{S}}.\sigma = \sigma''$.

II Since the speculative transaction that was started was also rolled back and the fact that $\vdash_O X''_{\mathsf{S}}$: *noongoing* by IH and $\vdash_O X'''_{\mathsf{S}}$: *noongoing*, we have $\vdash_O X^n_{\mathsf{S}}$: *noongoing*.

III Follows by definition and I).

IV By definition $\tau'' \cdot \texttt{start}\ id \cdots \texttt{rlb}\ id \upharpoonright_{ns} = \tau'' \upharpoonright_{ns} = \tau''$.

$$\begin{aligned}
&\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau'' \cdot \texttt{start}\ id \cdot \overline{\tau}^n \cdot \texttt{rlb}\ id \upharpoonright_{ns} \text{Def. and } \overline{\tau}''' \upharpoonright_{ns} = \varepsilon \\
&= \overline{\tau}' \cdot \tau' \upharpoonright_{ns} \tau'' = \tau \\
&= \overline{\tau}' \cdot \tau \upharpoonright_{ns} \tau \text{ generated by} \longrightarrow \\
&= \overline{\tau}' \upharpoonright_{ns} \cdot \tau \text{ by IH} \\
&= \overline{\tau} \cdot \tau
\end{aligned}$$

Note that $\overline{\rho}$ is empty for all the cases, because we discharge all the observations immediately using Rule S:General.

□

Lemma 50 (S SE: Non-speculative execution for rolled back transactions.). *If*

(1) $X_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}} X'_{\mathsf{S}}$ *and*

(2) $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$ *and*

(3) $\sigma = X_{\mathsf{S}}.\sigma$

Then

I there is a configurations σ' *with* $X'_{\mathsf{S}}.\sigma = \sigma'$ *and*

II $\sigma \xrightarrow{\overline{\tau}\upharpoonright_{ns}} \sigma'$ *and*

III $\overline{\tau}\upharpoonright_{ns} = \tau$

Proof. Let $X_{\mathsf{S}} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}} X'_{\mathsf{S}}$ be an execution with trace $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$. Let $\sigma = X_{\mathsf{S}}.\sigma$

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 $\upharpoonright_{ns}$ we have $\overline{\tau}\upharpoonright_{ns} = \tau\upharpoonright_{ns} = \tau$, where the last steps is because of the fact that τ was generated by $\rightarrow$.

Thus, we have $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}} \sigma'$ by Rule NS-Reflection and $\sigma \xrightarrow{\tau} \sigma'$.

Now, we need to show that $\sigma' = X'_{\mathsf{S}}.\sigma$. 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 $X_{\mathsf{S}}.\overline{\Psi}_4 \cdot \Psi_{\mathsf{S}} \cdot \Psi'_{\mathsf{S}}$ 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 $X'_{\mathsf{S}}.\sigma = \Psi_{\mathsf{S}}.\sigma = \sigma'$ and we are finished. ◻

K.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 13 (S AM: Behaviour of non-speculative semantics and AM semantics)

Lemma 54 (S AM: Completeness of the speculative semantics) Lemma 51 (S AM : Soundness of the AM semantics w.r.t. non-speculative semantics)

Lemma 55 (S AM: Non-speculative execution for rolled back transactions)

Lemma 52 (S AM: Soundness single step No Speculation) Lemma 53 (S AM: Single Step Speculation)

Theorem 13 (S AM: Behaviour of non-speculative semantics and AM semantics). *Let p be a program. Then* $Beh_{NS}(p) = Beh^{\omega}_{\mathsf{S}}(p)\upharpoonright_{ns}$

Proof. The proposition can be proven in similar fashion to Theorem 12 (S SE: Behaviour of non-speculative and oracle semantics). We prove the two directions separately:

$\Leftarrow$ Assume that $\overline{\tau} \in Beh^{\omega}_{\mathsf{S}}(p)$.

By the definition of $Beh^{\omega}_{\mathsf{S}}(p)$ we have an initial configuration σ such that $((p, \sigma)) \rightsquigarrow^{\omega}_{\mathsf{S}} \overline{\tau}$.

The proof proceeds in similar fashion to the analogous case in Theorem 12 (S SE: Behaviour of non-speculative and oracle semantics) by using Lemma 51 (S AM : Soundness of the AM semantics w.r.t. non-speculative semantics).

We can now conclude that $((p, \sigma)) \rightsquigarrow_{NS} \overline{\tau}\restriction_{ns} \in Beh_{NS}(p)$ by Rule NS-Trace.

$\Rightarrow$ Assume that $((p, \sigma)) \rightsquigarrow_{NS} \overline{\tau} \in Beh_{NS}(p)$.

We thus know there exists $\sigma' \in FinalConf$ such that $\sigma \Downarrow_{\overline{\tau}} \sigma'$.

We apply Lemma 54 (S AM: Completeness of the speculative semantics) with $\Sigma_{\mathsf{S}} = \Sigma^{init}_{\mathsf{S}}(p, \sigma)$ and get $\Sigma^{init}_{\mathsf{S}}(p, \sigma) \Downarrow^{\overline{\tau}'}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ 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 $((p, \sigma)) \rightsquigarrow^{\omega}_{\mathsf{S}} \overline{\tau}' \in Beh^{\omega}_{\mathsf{S}}(p)$.

$\square$

K.2.1 Soundness.

Lemma 51 (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) $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$

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* $\vdash^{i}_{O} \Sigma'_{\mathsf{S}} :$ *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 $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$

Rule S:AM-Reflection Then we have $\Sigma_{\mathsf{S}} \Downarrow^{\varepsilon}_{\mathsf{S}} \Sigma_{\mathsf{S}}$ 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 $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}' \cdot \tau}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ and by Rule S:AM-Single we get $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}'}_{\mathsf{S}} \Sigma''_{\mathsf{S}}$ and $\Sigma''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$.

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 $\vdash^{i}_{O} \Sigma'_{\mathsf{S}} :$ *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 $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}'}_{\mathsf{S}} \Sigma''_{\mathsf{S}}$ 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 $\vdash^{j}_{O} \Sigma''_{S}$: *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 $\vdash_{O} \Sigma''_{S}$: *noongoing* and we have $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}} \sigma''$ and $\Sigma''_{S}.\sigma = \sigma''$ by IH.

I Then $\vdash_{O} \Sigma'_{S}$: *noongoing* and we need to prove $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ and $\Sigma'_{S}.\sigma = \sigma'$. We now proceed by inversion on $\Sigma''_{S} \overset{\tau}{\rightsquigarrow}^{O}_{S} \Sigma'_{S}$:

Rule S:AM-Rollback Then $\tau = \texttt{rlb}\ id$.

Analogous to the corresponding case in Lemma 45 (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 45 (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 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) together with Lemma 52 (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 $\Sigma''_{S} \overset{\tau}{=\!\!\rightsquigarrow}_{S} \Sigma'_{S}$:

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 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) together with Lemma 53 (S AM: Single Step Speculation).

otherwise By definition of $\vdash^{i}_{O} \Sigma'_{S}$: *biggestongoingtransactionirolledback* we know that there exists a $\texttt{rlb}\ i$ in the execution $\Sigma'_{S} \Downarrow^{\overline{\tau}_{fin}}_{S} \Sigma_{S_{fin}}$ with no matching $\texttt{start}\ i$ observation in that execution. Analogous to the corresponding case in Lemma 45 (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 $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ 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 $\tau = \texttt{rlb}\ j$ Analogous to the corresponding case in Lemma 45 (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 45 (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 $\Sigma''_{S} \overset{\tau}{=\!\!\rightsquigarrow}_{S} \Sigma'_{S}$:

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 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

$id \neq j$ Analogous to the corresponding case in Lemma 45 (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 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics)

□

Lemma 52 (S AM: Soundness single step No Speculation)**.** *If*

(1) $\vdash_O \Sigma_S : noongoing$ *and*

(2) $\Sigma_S \overset{\tau}{\rightsquigarrow}_S \Sigma'_S$ *and*

(3) $\vdash_O \Sigma'_S : noongoing$ *and*

(4) $\sigma = \Sigma_S.\sigma$

Then there exists σ' *such that*

I $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma'$ *and*

II $\Sigma'_S.\sigma = \sigma'$

and σ' *is the configuration for some instance in* Σ'_S*.*

Proof. We proceed by inversion on $\Sigma_S \overset{\tau}{\rightsquigarrow}_S \Sigma'_S$:

Rule S:AM-General Thus, we have $\Sigma_S = \overline{\Phi}_S \cdot \Phi_{S_{\overline{p}'\cdot\tau}}$. Contradiction. By the definition of $\overset{\tau}{\rightsquigarrow}_S$ only Rule S:AM-Store-Spec adds observations to $\overline{p}$.

Since $\overline{p} = \overline{p}' \cdot \tau$ 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 18 (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 $\Phi_S \overset{\tau}{\rightsquigarrow}_S \overline{\Phi}'_S$.

We proceed by case analysis on the rule used to derive $\Phi_S \overset{\tau}{\rightsquigarrow}_S \Phi'_S$.

Rule S:AM-barr-spec, Rule S:AM-barr We have $p(\sigma(\mathbf{pc})) \neq \mathbf{store}\ x, e$ and $n \neq 0$: We show the proof for Rule S:AM-barr, the proof for Rule S:AM-barr-spec is analogous.

By Rule S:AM-barr we know $\sigma \xrightarrow{\varepsilon} \sigma'$ and $\overline{\Phi}'_S = \langle p, ctr, \sigma', n-1\rangle$.

Thus $\sigma' = \overline{\Phi}'_S.\sigma$ and $\tau = \varepsilon = \varepsilon\upharpoonright_{ns}$.

Thus, we have an execution $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma'$ and $\sigma' = \Sigma'_j.\sigma$ as needed.

Rule S:AM-NoBranch Thus, we have $p(\sigma(\mathbf{pc})) \neq \mathbf{jmp}$ and $n \neq 0$. We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule Rule S:AM-NoBranch and $\overline{\Phi}'_S = \langle p, ctr, \sigma', n-1\rangle$.

Thus, choose $\sigma' = \overline{\Phi}'_S.\sigma$.

Because the rule used the observation received from the derived step $\sigma \xrightarrow{\tau} \sigma'$, we already get $\tau\upharpoonright_{ns} = \tau$ and are finished.

Rule S:AM-Store-Spec Contradiction, because there are no ongoing transactions in Σ'_S by the fact $\vdash_O \Sigma'_S : noongoing$.

□

Lemma 53 (S AM: Single Step Speculation). *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) $\Phi_S \overset{\tau}{=\!\!\rightsquigarrow}_S \overline{\Phi}'_S$ *and*
(4) $\sigma = \Phi_S.\sigma$

Then

I $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma'$ *and*
II σ' *is the configuration for the instance with* $ctr = i$ *in* Σ'_S

Proof. We proceed by inversion on $\Phi_S \overset{\tau}{=\!\!\rightsquigarrow}_S \overline{\Phi}'_S$:

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 48 (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.

□

K.2.2 Completeness.

Lemma 54 (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 $\overline{\tau} = \overline{\tau}'\upharpoonright_{ns}$ *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 $\varepsilon\upharpoonright_{ns} = \varepsilon$ we are finished.

Rule NS-Single Then we have $\sigma \Downarrow_{\overline{\tau}} \sigma''$ and $\sigma'' \xrightarrow{\tau} \sigma'$.

We need to show

I $\Sigma_S \Downarrow^{\overline{\tau}'\cdot\tau'}_S \Sigma'_S$ and
II $\vdash_O \Sigma'_S : noongoing$ and

III $\sigma' = \Sigma'_{\mathsf{S}}.\sigma$ and

IV $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \upharpoonright_{ns}$

V $\rho = \varepsilon$

We apply the IH on $\sigma \Downarrow_{\overline{\tau}} \sigma''$ we get

I' $\Sigma_{\mathsf{S}} \Downarrow_{\mathsf{S}}^{\overline{\tau}'} \Sigma''_{\mathsf{S}\ \rho}$ and

II' $\vdash_O \Sigma''_{\mathsf{S}\ \rho} : \mathit{noongoing}$ and

III' $\sigma'' = \Sigma''_{\mathsf{S}}.\sigma$ and

IV' $\overline{\tau} = \overline{\tau}' \upharpoonright_{ns}$

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 49 (S SE: Completeness of the speculative semantics).

$p(\sigma(\mathbf{pc})) = \mathbf{store}\ x, e$ Analogous to the corresponding case Lemma 49 (S SE: Completeness of the speculative semantics), which is when the oracle mispredicted in the proof, together with Lemma 55 (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 55 (S AM: Non-speculative execution for rolled back transactions.)**.** *If*

(1) $\Sigma_{\mathsf{S}} \Downarrow_{\mathsf{S}}^{\overline{\tau}} \Sigma'_{\mathsf{S}}$ *and*

(2) $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$ *and*

(3) $\sigma = \Sigma_{\mathsf{S}}.\sigma$

Then

I there is a configurations σ' *with* $\Sigma'_{\mathsf{S}}.\sigma = \sigma'$ *and*

II $\sigma \xrightarrow{\overline{\tau}\upharpoonright_{ns}} \sigma'$ *and*

III $\overline{\tau}\upharpoonright_{ns} = \tau$

Proof. Let $\Sigma_{\mathsf{S}} \Downarrow_{\mathsf{S}}^{\overline{\tau}} \Sigma'_{\mathsf{S}}$ be an execution with trace $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$. Let $\sigma = \Sigma_{\mathsf{S}}.\sigma$
The proof proceeds analogously to Lemma 50 (S SE: Non-speculative execution for rolled back transactions). □

K.3 S: Relating Symbolic and AM semantics

Theorem 14 (S: Behaviour of AM and symbolic semantics). $Beh^{\omega}_{\mathsf{S}}(p) = \mu(Beh^{\mathcal{S}}_{\mathsf{S}}(p))$

Theorem 14 (S: Behaviour of AM and symbolic semantics)

Lemma 56 (S: Soundness of the AM semantics w.r.t. symbolic semantics) Lemma 58 (S: Completeness of the symbolic semantics)

Lemma 57 (S: Soundness single step) Lemma 59 (S: Completeness single step)

Now onto theorems for the new speculative semantics. We want to show Soundness and Completeness.
We lift μ to speculative states $\Sigma^{\mathcal{S}}_{\mathsf{S}}$ in the following way by applying μ pointwise for each instance in the state $\Sigma^{\mathcal{S}}_{\mathsf{S}}$.

K.3.1 Soundness.

Lemma 56 (S: Soundness of the AM semantics w.r.t. symbolic semantics)**.** *If*

(1) $\Sigma_{\mathsf{S}}^{\mathcal{S}} \ {}_{\mathcal{S}}\Downarrow_{\mathsf{S}}^{\overline{\tau_{\mathcal{S}}}} \ \Sigma_{\mathsf{S}}^{\mathcal{S}'}$ *and*
(2) $\mu \vDash pthCnd(\Sigma_{\mathsf{S}}^{\mathcal{S}'})$

Then

I $\mu(\Sigma_{\mathsf{S}}^{\mathcal{S}}) \Downarrow_{\mathsf{S}}^{\mu(\overline{\tau_{\mathcal{S}}})} \ \mu(\Sigma_{\mathsf{S}}^{\mathcal{S}'})$ *and*

Proof. We proceed by induction on $\Sigma_{\mathsf{S}}^{\mathcal{S}} \ {}_{\mathcal{S}}\Downarrow_{\mathsf{S}}^{\overline{\tau_{\mathcal{S}}}} \ \Sigma_{\mathsf{S}}^{\mathcal{S}'}$

Rule S:Sym-Reflection Then we have $\Sigma_{\mathsf{S}}^{\mathcal{S}} \ {}_{\mathcal{S}}\Downarrow_{\mathsf{S}}^{\varepsilon} \Sigma_{\mathsf{S}}^{\mathcal{S}'}$ with $\Sigma_{\mathsf{S}}^{\mathcal{S}'} = \Sigma_{\mathsf{S}}^{\mathcal{S}}$. Using Rule S:AM-Reflection we get $\mu(\Sigma_{\mathsf{S}}^{\mathcal{S}}) \ {}_{\mathcal{S}}\Downarrow_{\mathsf{S}}^{\mu(\varepsilon)} \ \mu(\Sigma_{\mathsf{S}}^{\mathcal{S}'})$ and are finished.

Rule S:Sym-Single We have $\Sigma_{\mathsf{S}}^{\mathcal{S}} \ {}_{\mathcal{S}}\Downarrow_{\mathsf{S}}^{\overline{\tau_{\mathcal{S}}}'\cdot\tau_{\mathcal{S}}} \ \Sigma_{\mathsf{S}}^{\mathcal{S}'}$ and by Rule S:Sym-Single we get $\Sigma_{\mathsf{S}}^{\mathcal{S}} \ {}_{\mathcal{S}}\Downarrow_{\mathsf{S}}^{\overline{\tau_{\mathcal{S}}}'} \ \Sigma_{\mathsf{S}}^{\mathcal{S}''}$ and $\Sigma_{\mathsf{S}}^{\mathcal{S}''} \xrightarrow{\tau}_{\mathsf{S}}^{\mathcal{S}} \Sigma_{\mathsf{S}}^{\mathcal{S}'}$.
We need to prove
(1) $\mu(\Sigma_{\mathsf{S}}^{\mathcal{S}}) \Downarrow_{\mathsf{S}}^{\mu(\overline{\tau}\cdot\tau_{\mathcal{S}})} \ \mu(\Sigma_{\mathsf{S}}^{\mathcal{S}'})$
We apply the IH on $\Sigma_{\mathsf{S}}^{\mathcal{S}} \ {}_{\mathcal{S}}\Downarrow_{\mathsf{S}}^{\overline{\tau_{\mathcal{S}}}} \ \Sigma_{\mathsf{S}}^{\mathcal{S}''}$ and have a $\Sigma_{\mathsf{S}}'' = \mu(\Sigma_{\mathsf{S}}^{\mathcal{S}''})$ such that:
(1) $\mu(\Sigma_{\mathsf{S}}^{\mathcal{S}}) \Downarrow_{\mathsf{S}}^{\mu(\overline{\tau_{\mathcal{S}}})} \ \Sigma_{\mathsf{S}}''$ and
The result follows by applying Lemma 57 (S: Soundness single step) on $\Sigma_{\mathsf{S}}^{\mathcal{S}''} \xrightarrow{\tau_{\mathcal{S}}}_{\mathsf{S}}^{\mathcal{S}} \ \Sigma_{\mathsf{S}}^{\mathcal{S}'}$ and get a step $\Sigma_{\mathsf{S}}'' \xrightarrow{\mu(\tau_{\mathcal{S}})}_{\mathsf{S}} \mu(\Sigma_{\mathsf{S}}^{\mathcal{S}'})$. We now use Rule S:AM-Single and get an execution $\mu(\Sigma_{\mathsf{S}}^{\mathcal{S}}) \Downarrow_{\mathsf{S}}^{\mu(\overline{\tau_{\mathcal{S}}})\cdot\mu(\tau_{\mathcal{S}})} \ \mu(\Sigma_{\mathsf{S}}^{\mathcal{S}'})$ as required.

□

Lemma 57 (S: Soundness single step)**.** *If*

(1) $\Sigma_{\mathsf{S}}^{\mathcal{S}} \xrightarrow{\tau}_{\mathsf{S}}^{\mathcal{S}} \Sigma_{\mathsf{S}}^{\mathcal{S}}$ *and*
(2) $\mu \vDash pthCnd(\Sigma_{\mathsf{S}}^{\mathcal{S}'})$

Then

I $\mu(\Sigma_{\mathsf{S}}^{\mathcal{S}}) \xrightarrow{\mu(\tau)}_{\mathsf{S}} \mu(\Sigma_{\mathsf{S}}^{\mathcal{S}'})$

Proof. We proceed by inversion on $\Sigma_{\mathsf{S}}^{\mathcal{S}} \xrightarrow{\tau}_{\mathsf{S}}^{\mathcal{S}} \Sigma_{\mathsf{S}}^{\mathcal{S}'}$:

Rule S:Sym-Rollback Since μ does not change the speculation window and *ctr* and $\mu(\Sigma_{\mathsf{S}}^{\mathcal{S}}) = \Sigma_{\mathsf{S}}$, we have $\Sigma_{\mathsf{S}}.n = \Sigma_{\mathsf{S}}^{\mathcal{S}}.n = 0$ and $\Sigma_{\mathsf{S}}.ctr = \Sigma_{\mathsf{S}}^{\mathcal{S}}.ctr$.
$\Sigma_{\mathsf{S}} \xrightarrow{\tau'}_{\mathsf{S}} \Sigma_{\mathsf{S}}^{\mathcal{S}'}$ We can use Rule S:AM-Rollback to derive $\Sigma_{\mathsf{S}} \xrightarrow{\tau'}_{\mathsf{S}} \Sigma_{\mathsf{S}}'$.
$\mu(\Sigma_{\mathsf{S}}^{\mathcal{S}'}) = \Sigma_{\mathsf{S}}'$ The rule only deletes the topmost instance and changes the *ctr* of the instance below. Since $\Sigma_{\mathsf{S}}.ctr = \Sigma_{\mathsf{S}}^{\mathcal{S}}.ctr$, we have $\mu(\Sigma_{\mathsf{S}}^{\mathcal{S}'}) = \Sigma_{\mathsf{S}}'$
$\mu \vDash pthCnd(\Sigma_{\mathsf{S}}^{\mathcal{S}'})$ **and** $\mu(\tau') = \tau$ Since the $\Sigma_{\mathsf{S}}.ctr = \Sigma_{\mathsf{S}}^{\mathcal{S}}.ctr$ we already have $\mu(\tau') = \tau$. For $\mu \vDash pthCnd(\Sigma_{\mathsf{S}}^{\mathcal{S}'})$, notice that $\mu \vDash pthCnd(\Sigma_{\mathsf{S}}^{\mathcal{S}'}) = \mu \vDash pthCnd(\Sigma_{\mathsf{S}}^{\mathcal{S}})$ because the rule only deletes a speculative instance. Thus, we are finished.

Rule S:Sym-Context We then have $\Phi_{\mathsf{S}}^{\mathcal{S}} \xrightarrow{\tau}_{\mathsf{S}}^{\mathcal{S}} \overline{\Phi}'_{\mathsf{S}_{\mathcal{S}}}$. Thus, we know $\Phi_{\mathsf{S}}^{\mathcal{S}} > 0$ and $\mu(\Phi_{\mathsf{S}}^{\mathcal{S}}) > 0$ as well. We proceed by inversion on $\Phi_{\mathsf{S}}^{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathsf{S}}^{\mathcal{S}} \overline{\Phi}'_{\mathsf{S}_{\mathcal{S}}}$:

Rule S:Sym-General Then $\Phi_{\mathsf{S}}^{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}{}_{\mathsf{S}}^{\mathcal{S}} \Phi_{\mathsf{S}\overline{\rho_{\mathcal{S}}}\backslash\tau_{\mathcal{S}}}$. By $\mu(\Phi_{\mathsf{S}}^{\mathcal{S}}) = \Phi_{\mathsf{S}}$ 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 $\Phi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Phi_{\mathsf{S}\overline{\rho}\backslash\tau}$.
Now we have $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu(\Phi_{\mathsf{S}}^{\mathcal{S}}{}_{\overline{\rho_{\mathcal{S}}}\backslash\tau_{\mathcal{S}})} = \Phi_{\mathsf{S}\overline{\rho}\backslash\tau}$ by construction.

Rule S:Sym-NoBranch Then we have $\Phi_{\mathsf{S}}^{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}{}_{\mathsf{S}}^{\mathcal{S}} \Phi_{\mathsf{S}}^{\mathcal{S}\prime}$ where $\Phi_{\mathsf{S}}^{\mathcal{S}\prime} = \langle p, \Phi_{\mathsf{S}}^{\mathcal{S}}.ctr, \Phi_{\mathsf{S}}^{\mathcal{S}}.\sigma'_{\mathcal{S}}, \Phi_{\mathsf{S}}^{\mathcal{S}}.n - 1\rangle$ with $\Phi_{\mathsf{S}}^{\mathcal{S}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$.
Since we have $\mu \vDash pthCnd(\overline{\Phi}_{\mathsf{S}_{\mathcal{S}}}.\sigma_{\mathcal{S}})$ (by assumption) we can use Lemma 3 (NS: Soundness Symbolic Added rules) on $\Phi_{\mathsf{S}}^{\mathcal{S}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$ and get $\mu(\Phi_{\mathsf{S}}^{\mathcal{S}}\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_{\mathcal{S}})} \mu(\sigma'_{\mathcal{S}})$, where $\mu(\Phi_{\mathsf{S}}.\sigma_{\mathcal{S}}) = \Phi_{\mathsf{S}}.\sigma$ as per assumption.
Now choose $\Phi_{\mathsf{S}}^{\mathcal{S}\prime}.\sigma = \sigma'_{\mathcal{S}}$ and let it otherwise be equal to Φ'_{S}. We can now use Rule S:Sym-NoBranch to derive the step $\Phi_{\mathsf{S}}^{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}{}_{\mathsf{S}}^{\mathcal{S}} \Phi_{\mathsf{S}}^{\mathcal{S}\prime}$ using the derived $\rightarrow_{\mathcal{S}}$ step and trivially satisfy $\mu(\Phi_{\mathsf{S}}^{\mathcal{S}\prime}) = \Phi'_{\mathsf{S}}$.

Rule S:Sym-barr Then we have $\Phi_{\mathsf{S}}^{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}{}_{\mathsf{S}}^{\mathcal{S}} \Phi_{\mathsf{S}}^{\mathcal{S}\prime}$ where $\Phi_{\mathsf{S}}^{\mathcal{S}\prime} = \langle p, \Phi_{\mathsf{S}}^{\mathcal{S}}.ctr, \Phi_{\mathsf{S}}^{\mathcal{S}}.\sigma'_{\mathcal{S}}, \Phi_{\mathsf{S}}^{\mathcal{S}}.n - 1\rangle$ with $\Phi_{\mathsf{S}}^{\mathcal{S}}.\sigma \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$. Analogous to Rule S:Sym-NoBranch using Rule S:AM-barr.

Rule S:Sym-barr-spec Then we have $\Phi_{\mathsf{S}}^{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}{}_{\mathsf{S}}^{\mathcal{S}} \Phi_{\mathsf{S}}^{\mathcal{S}\prime}$ where $\Phi_{\mathsf{S}}^{\mathcal{S}\prime} = \langle p, \Phi_{\mathsf{S}}^{\mathcal{S}}.ctr, \Phi_{\mathsf{S}}^{\mathcal{S}}.\sigma'_{\mathcal{S}}, \Phi_{\mathsf{S}}^{\mathcal{S}}.n - 1\rangle$ with $\Phi_{\mathsf{S}}^{\mathcal{S}}.\sigma \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$. Analogous to case Rule S:Sym-NoBranch using Rule S:AM-barr-spec.

Rule S:Sym-Store-Spec We have $\Phi_{\mathsf{S}}^{\mathcal{S}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}{}_{\mathsf{S}}^{\mathcal{S}} \overline{\Phi}_{\mathsf{S}_{\mathcal{S}}\overline{\rho_{\mathcal{S}}}\cdot\mathtt{bypass}\ \Phi_{\mathsf{S}}^{\mathcal{S}}.\mathbf{pc}\cdot\mathtt{start}\ \Phi_{\mathsf{S}}^{\mathcal{S}}.ctr}$ where $\overline{\Phi}_{\mathsf{S}_{\mathcal{S}}} = \langle p, \Phi_{\mathsf{S}}^{\mathcal{S}}.ctr, \sigma'_{\mathcal{S}}, \Phi_{\mathsf{S}}^{\mathcal{S}}.n - 1\rangle \cdot \langle p, \Phi_{\mathsf{S}}^{\mathcal{S}}.ctr + 1, \sigma''_{\mathcal{S}}, \min \Phi_{\mathsf{S}}^{\mathcal{S}}.n, \omega\rangle$. Furthermore, we have $\Phi_{\mathsf{S}}^{\mathcal{S}}.\sigma \xrightarrow{\tau_{\mathcal{S}}} \sigma'_{\mathcal{S}}$ and $\sigma''_{\mathcal{S}} = \sigma_{\mathcal{S}}[\mathbf{pc} \mapsto \Phi_{\mathsf{S}}^{\mathcal{S}}.\sigma_{\mathcal{S}}(\mathbf{pc}) + 1]$ (note that **pc** is always concrete).
We use Lemma 3 (NS: Soundness Symbolic Added rules) on $\Phi_{\mathsf{S}}^{\mathcal{S}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$ and get $\mu(\Phi_{\mathsf{S}}^{\mathcal{S}}.\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_{\mathcal{S}})}_{\mathcal{S}} \mu(\sigma'_{\mathcal{S}})$.
Choose $\Phi_{\mathsf{S}} = \mu(\Phi_{\mathsf{S}}^{\mathcal{S}})$ 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 $\mu(\Phi_{\mathsf{S}}^{\mathcal{S}}.\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_{\mathcal{S}})}_{\mathcal{S}} \mu(\sigma'_{\mathcal{S}})$ above and define $\sigma'' = \sigma[\mathbf{pc} \mapsto \sigma(\mathbf{pc}) + 1]$: $\Phi_{\mathsf{S}} \overset{\mu(\tau_{\mathcal{S}})}{\rightsquigarrow}_{\mathsf{S}} \overline{\Phi}_{\mathsf{S}}$ with $\overline{\Phi}_{\mathsf{S}} = \langle p, \Phi_{\mathsf{S}}.ctr, \sigma', \Phi_{\mathsf{S}}.n - 1\rangle \cdot \langle p, \Phi_{\mathsf{S}}.ctr + 1, \sigma'', \min \Phi_{\mathsf{S}}.n, \omega\rangle$.
We now show that $\mu(\overline{\Phi}_{\mathsf{S}_{\mathcal{S}}}) = \overline{\Phi}_{\mathsf{S}}$. Since **pc** is concrete and $\mu(\Phi_{\mathsf{S}}^{\mathcal{S}}.\sigma) = \sigma$, it follow that $\mu(\sigma''_{\mathcal{S}}) = \sigma''$.
By $\mu(\Phi_{\mathsf{S}}^{\mathcal{S}}) = \Phi_{\mathsf{S}}$ we have $\Phi_{\mathsf{S}}^{\mathcal{S}}.ctr = \Phi_{\mathsf{S}}.ctr$ and $\Phi_{\mathsf{S}}^{\mathcal{S}}.n = \Phi_{\mathsf{S}}.n$.
Now, we have $\mu(\overline{\Phi}_{\mathsf{S}_{\mathcal{S}}}) = \overline{\Phi}_{\mathsf{S}}$ and thus $\mu(\Phi_{\mathsf{S}}^{\mathcal{S}}) \overset{\mu(\tau_{\mathcal{S}})}{\rightsquigarrow}_{\mathsf{S}} \mu(\overline{\Phi}_{\mathsf{S}_{\mathcal{S}}})$ as needed.

□

K.3.2 Completeness.

Lemma 58 (S: Completeness of the symbolic semantics)**.** *If*

(1) $\Sigma_{\mathsf{S}} \Downarrow_{\mathsf{S}}^{\overline{\tau}} \Sigma'_{\mathsf{S}}$ *and*
(2) $\Sigma_{\mathsf{S}} = \mu(\Sigma_{\mathsf{S}}^{\mathcal{S}})$

Then there is a valuation μ*, a symbolic trace* $\overline{\tau}'$ *and a final state* $\Sigma_{\mathsf{S}}^{\mathcal{S}\prime}$ *such that*

I $\Sigma_{\mathsf{S}}^{\mathcal{S}}\ {}_{\mathcal{S}}\Downarrow_{\mathsf{S}}^{\overline{\tau}'} \Sigma_{\mathsf{S}}^{\mathcal{S}\prime}$ *and*
II $\Sigma'_{\mathsf{S}} = \mu(\Sigma_{\mathsf{S}}^{\mathcal{S}\prime})$ *and* $\overline{\tau} = \mu(\overline{\tau}')$ *and*
III $\mu \vDash pthCnd(\Sigma_{\mathsf{S}}^{\mathcal{S}\prime})$

Proof. We proceed by induction on $\Sigma_{\mathsf{S}} \Downarrow_{\mathsf{S}}^{\overline{\tau}} \Sigma'_{\mathsf{S}}$

Rule S:AM-Reflection Then we have $\Sigma_{\mathsf{S}} \Downarrow^{\varepsilon}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ with $\Sigma_{\mathsf{S}} = \Sigma'_{\mathsf{S}}$.

I - III By Rule S:Sym-Reflection we have $\Sigma^{\mathcal{S}}_{\mathsf{S}}\ {}_{\mathcal{S}}\Downarrow^{\varepsilon}_{\mathsf{S}}\ \Sigma^{\mathcal{S}'}_{\mathsf{S}}$. By construction $\Sigma^{\mathcal{S}'}_{\mathsf{S}} = \Sigma^{\mathcal{S}'}_{\mathsf{S}}$. We now trivially satisfy all conditions.

Rule S:AM-Single We have $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}'\cdot\tau}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ and by Rule S:AM-Single we get $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau_{\mathcal{S}}}'}_{\mathsf{S}} \Sigma''_{\mathsf{S}}$ and $\Sigma''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$.

We need to prove

(1) $\Sigma^{\mathcal{S}}_{\mathsf{S}}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau_{\mathcal{S}}}'\cdot\tau_{\mathcal{S}}}_{\mathsf{S}}\ \Sigma^{\mathcal{S}'}_{\mathsf{S}}$ and

(2) $\Sigma'_{\mathsf{S}} = \mu(\Sigma^{\mathcal{S}'}_{\mathsf{S}})$ and $\overline{\tau}'\cdot\tau = \mu(\overline{\tau_{\mathcal{S}}}'\cdot\tau_{\mathcal{S}})$ and

(3) $\mu \vDash pthCnd(\Sigma^{\mathcal{S}'}_{\mathsf{S}})$

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

(1) $\Sigma^{\mathcal{S}}_{\mathsf{S}}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau_{\mathcal{S}}}'}_{\mathsf{S}}\ \Sigma^{\mathcal{S}''}_{\mathsf{S}}$ and

(2) $\Sigma''_{\mathsf{S}} = \mu(\Sigma^{\mathcal{S}''}_{\mathsf{S}})$ and $\overline{\tau}' = \mu(\overline{\tau_{\mathcal{S}}}')$ and

(3) $\mu \vDash pthCnd(\Sigma^{\mathcal{S}''}_{\mathsf{S}})$

The result follows from applying Lemma 59 (S: Completeness single step) on $\Sigma''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$:

□

Lemma 59 (S: Completeness single step)**.** *If*

(1) $\Sigma_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ *and*

(2) $\mu(\Sigma^{\mathcal{S}}_{\mathsf{S}}) = \Sigma_{\mathsf{S}}$ *and*

(3) $\mu \vDash pthCnd(\Sigma^{\mathcal{S}}_{\mathsf{S}})$

Then

I $\Sigma^{\mathcal{S}}_{\mathsf{S}} \overset{\tau'}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathsf{S}} \Sigma^{\mathcal{S}'}_{\mathsf{S}}$ *and*

II $\mu(\Sigma^{\mathcal{S}'}_{\mathsf{S}}) = \Sigma'_{\mathsf{S}}$ *and*

III $\mu \vDash pthCnd(\Sigma^{\mathcal{S}'}_{\mathsf{S}})$ *and* $\mu(\tau') = \tau$

Proof. We proceed by inversion on $\Sigma_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$:

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

$\Sigma^{\mathcal{S}}_{\mathsf{S}} \overset{\tau'}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathsf{S}} \Sigma^{\mathcal{S}'}_{\mathsf{S}}$ We can use the rule Rule S:Sym-Rollback in the symbolic semantics to derive $\Sigma^{\mathcal{S}}_{\mathsf{S}} \overset{\tau'}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathsf{S}} \Sigma^{\mathcal{S}'}_{\mathsf{S}}$.

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

$\mu \vDash pthCnd(\tau')$ **and** $\mu(\tau') = \tau$ Since the $\Sigma_{\mathsf{S}}.ctr = \Sigma^{\mathcal{S}}_{\mathsf{S}}.ctr$ we already have $\mu(\tau') = \tau$. For $\mu \vDash pthCnd(\Sigma^{\mathcal{S}'}_{\mathsf{S}})$, notice that $\mu \vDash pthCnd(\Sigma^{\mathcal{S}'}_{\mathsf{S}}) = \mu \vDash pthCnd(\Sigma^{\mathcal{S}}_{\mathsf{S}})$ because the rule only deletes a speculative instance. Thus, we are finished.

Rule S:AM-Context We then have $\Phi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \overline{\Phi}'_{\mathsf{S}}$. Note that $\Phi_{\mathsf{S}}.n > 0$ and as such for all symbolic states where $\mu(\Phi^{\mathcal{S}}_{\mathsf{S}}) = \Phi_{\mathsf{S}}$ as well. We proceed by inversion on $\Phi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \overline{\Phi}'_{\mathsf{S}}$:

Rule S:AM-General Then $\Phi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Phi_{\mathsf{S}\,\overline{\rho}\backslash\tau}$. By $\mu(\Phi^{\mathcal{S}}_{\mathsf{S}}) = \Phi_{\mathsf{S}}$ 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 $\Phi^{\mathcal{S}}_{\mathsf{S}}$ except for $\overline{\rho}$ we have $\Phi^{\mathcal{S}}_{\mathsf{S}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathsf{S}} \Phi^{\mathcal{S}}_{\mathsf{S}\,\overline{\rho_{\mathcal{S}}}\backslash\tau_{\mathcal{S}}}$.

Now we have $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu(\Phi^{\mathcal{S}}_{\mathsf{S}})_{\overline{\rho}\backslash\tau_{\mathcal{S}}} = \Phi_{\mathsf{S}\,\overline{\rho}\backslash\tau}$ by construction.

Rule S:AM-barr Then we have $\Phi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Phi'_{\mathsf{S}}$ where $\Phi'_{\mathsf{S}} = \langle p, \Phi_{\mathsf{S}}.ctr, \Phi_{\mathsf{S}}.\sigma', \Phi_{\mathsf{S}}.n - 1\rangle$ with $\Phi_{\mathsf{S}}.\sigma \xrightarrow{\tau} \sigma'$. We use Lemma 5 (NS : Completeness Symbolic Added) on $\Phi_{\mathsf{S}}.\sigma \rightarrow \sigma'$ and get $\Phi^{\mathcal{S}}_{\mathsf{S}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$, where $\mu(\Phi_{\mathsf{S}}) = \Phi_{\mathsf{S}}$ as per assumption, $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu(\sigma'_{\mathcal{S}}) = \sigma'$. Now choose $\Phi^{\mathcal{S}'}_{\mathsf{S}}.\sigma = \sigma'_{\mathcal{S}}$ and let it otherwise be equal to Φ'_{S}. We can now use Rule S:Sym-barr to derive the step $\Phi^{\mathcal{S}}_{\mathsf{S}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}^{\mathcal{S}}_{\mathsf{S}} \Phi^{\mathcal{S}'}_{\mathsf{S}}$ using the derived $\rightarrow_{\mathcal{S}}$ step and trivially satisfy $\mu(\Phi^{\mathcal{S}'}_{\mathsf{S}}) = \Phi'_{\mathsf{S}}$.

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.

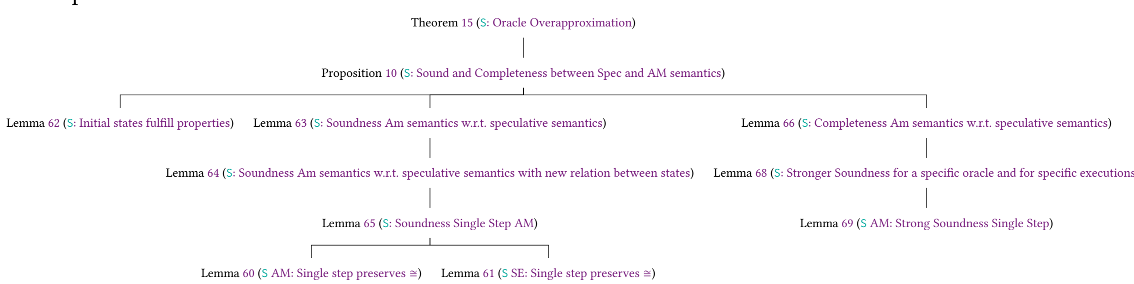
Rule S:AM-Store-Spec We have $\Phi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \overline{\Phi}_{\mathsf{S}}{}_{\overline{p}\cdot\texttt{bypass}\ \Phi_{\mathsf{S}}.\mathbf{pc}\cdot\texttt{start}\ \Phi_{\mathsf{S}}.ctr}$ where $\overline{\Phi}_{\mathsf{S}} = \langle p, \Phi_{\mathsf{S}}.ctr, \sigma', \Phi_{\mathsf{S}}.n-1\rangle \cdot \langle p, \Phi_{\mathsf{S}}.ctr+1, \sigma'', \min \Phi_{\mathsf{S}}.n, \omega\rangle$. Furthermore, we have $\Phi_{\mathsf{S}}.\sigma \rightarrow \sigma'$ and $\sigma'' = \sigma[\mathbf{pc} \mapsto \Phi_{\mathsf{S}}.\sigma(\mathbf{pc}) + 1]$
We use Lemma 5 (NS : Completeness Symbolic Added) on $\Phi_{\mathsf{S}}.\sigma \xrightarrow{\tau} \sigma'$ and get $\Phi^{\mathcal{S}}_{\mathsf{S}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$, where $\mu(\Phi^{\mathcal{S}}_{\mathsf{S}}) = \Phi_{\mathsf{S}}$ as per assumption, $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu(\sigma'_{\mathcal{S}}) = \sigma'$.
Next, we define $\sigma''_{\mathcal{S}} = \Phi^{\mathcal{S}}_{\mathsf{S}}.\sigma_{\mathcal{S}}[\mathbf{pc} \mapsto \Phi_{\mathsf{S}}.\sigma(\mathbf{pc}) + 1]$ (per assumption **pc** is concrete).
It follows that $\mu(\sigma''_{\mathcal{S}}) = \sigma''$ by $\mu(\Phi^{\mathcal{S}}_{\mathsf{S}}.\sigma) = \sigma$.
Since a **store** is executed, we can use Rule S:Sym-Store-Spec to derive a step and get $\Phi^{\mathcal{S}}_{\mathsf{S}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}^{\mathcal{S}}_{\mathsf{S}} \langle p, \Phi^{\mathcal{S}}_{\mathsf{S}}.ctr+1, \Phi^{\mathcal{S}}_{\mathsf{S}}.\sigma_{\mathcal{S}}, \Phi^{\mathcal{S}}_{\mathsf{S}}.n - 1\rangle \cdot \langle p, \Phi^{\mathcal{S}}_{\mathsf{S}}.ctr + 1, \sigma''_{\mathcal{S}}, \min \Phi^{\mathcal{S}}_{\mathsf{S}}.n, \omega\rangle_{\overline{p}\cdot\texttt{bypass}\ \Phi^{\mathcal{S}}_{\mathsf{S}}.\mathbf{pc}\cdot\texttt{start}\ \Phi^{\mathcal{S}}_{\mathsf{S}}.ctr}$.
By $\mu(\Phi^{\mathcal{S}}_{\mathsf{S}}) = \Phi_{\mathsf{S}}$ we have $\Phi^{\mathcal{S}}_{\mathsf{S}}.ctr = \Phi_{\mathsf{S}}.ctr$ and $\Phi^{\mathcal{S}}_{\mathsf{S}}.n = \Phi_{\mathsf{S}}.n$.
Now, we have $\mu(\overline{\Phi}_{\mathsf{S}_{\mathcal{S}}}) = \overline{\Phi}_{\mathsf{S}}$ and $\mu(\tau_{\mathcal{S}}) = \tau$.
It remains to show that $\mu \vDash pthCnd(\overline{\Phi}_{\mathsf{S}_{\mathcal{S}}})$. Since $\overline{\Phi}_{\mathsf{S}_{\mathcal{S}}}.\sigma_{\mathcal{S}} = \sigma''_{\mathcal{S}}$, $\sigma''_{\mathcal{S}}.\delta^{\mathcal{S}} = \sigma'_{\mathcal{S}}.\delta^{\mathcal{S}}$ and we have $\mu \vDash pthCnd(\sigma'_{\mathcal{S}})$ from above we have $\mu \vDash pthCnd(\overline{\Phi}_{\mathsf{S}_{\mathcal{S}}})$.

□

K.4 S: Relating Oracle and AM semantics via SNI

First the definition of the element function we are gonna use: elem_of_states$(\langle p, ctr, \sigma, n\rangle) = \langle p, ctr, \sigma\rangle$

The proof structure looks like this:



We define a few Lemmas

Lemma 60 (S AM: Single step preserves ≅). *If*

(1) $\Sigma_{\mathsf{S}1} \cong \Sigma_{\mathsf{S}2}$ *and*
(2) $\Sigma_{\mathsf{S}1} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ *and* $\Sigma_{\mathsf{S}2} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Sigma''_{\mathsf{S}}$

Then

(1) $\Sigma'_{\mathsf{S}} \cong \Sigma''_{\mathsf{S}}$

Proof. We have

(1) $\Sigma_{S1} \cong \Sigma_{S2}$ and
(2) $\Sigma_{S1} \overset{\tau}{\Rightarrow}_{S} \Sigma'_{S}$ and $\Sigma_{S2} \overset{\tau'}{\Rightarrow}_{S} \Sigma''_{S}$

Because of (1), we know that the same rule was used to derive the steps $\Sigma_{S1} \overset{\tau}{\Rightarrow}_{S} \Sigma'_{S}$ and $\Sigma_{S2} \overset{\tau}{\Rightarrow}_{S} \Sigma''_{S}$.

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 61 (S SE: Single step preserves $\cong$). *If*

(1) $X_{S1} \cong X_{S2}$ *and*
(2) $X_{S1} \overset{\tau}{\rightsquigarrow}{}^{O}_{S} X'_{S}$ *and* $X_{S2} \overset{\tau}{\rightsquigarrow}{}^{O}_{S} X''_{S}$

Then

(1) $X'_{S} \cong X''_{S}$ *and*

Proof. We have

(1) $X_{S1} \cong X_{S2}$ and
(2) $X_{S1} \overset{\tau}{\rightsquigarrow}{}^{O}_{S} X'_{S}$ and $X_{S2} \overset{\tau}{\rightsquigarrow}{}^{O}_{S} X''_{S}$

Because of (1), we know that the same rule was used to derive the steps $X_{S1} \overset{\tau}{\Rightarrow}_{S} X'_{S}$ and $X_{S2} \overset{\tau}{\Rightarrow}_{S} X''_{S}$.

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 15 (S: Oracle Overapproximation). *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 $((p,\sigma)) \Downarrow_{NS} \overline{\tau}$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}$, then $((p,\sigma)) \Downarrow^{\omega}_{S} \overline{\tau}''$, $((p,\sigma')) \Downarrow^{\omega}_{S} \overline{\tau}''$*

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) $((p,\sigma)) \Downarrow_{NS} \overline{\tau}'$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}'$ 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 $((p,\sigma)) \Downarrow^{\omega}_{S} \overline{\tau}''$, $((p,\sigma')) \Downarrow^{\omega}_{S} \overline{\tau}''$ 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 $((p,\sigma)) \Downarrow_{NS} \overline{\tau}$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}$, then $((p,\sigma)) \Downarrow^{O}_{S} \overline{\tau}'$ and $((p,\sigma')) \Downarrow^{O}_{S} \overline{\tau}'$.

We fulfill all premises of SNI by a) and b) for p and get $((p,\sigma)) \Downarrow^{O}_{S} \overline{\tau}'$ and $((p,\sigma')) \Downarrow^{O}_{S} \overline{\tau}'$.

We use Proposition 10 (S: Sound and Completeness between Spec and AM semantics) with $((p, \sigma)) \rightsquigarrow_S^{O} \overline{\tau}'$ and $((p, \sigma')) \rightsquigarrow_S^{O} \overline{\tau}'$ to get $((p, \sigma)) \rightsquigarrow_S^{\omega} \overline{\tau}''$, $((p, \sigma')) \rightsquigarrow_S^{\omega} \overline{\tau}''$. This completes the proof.

($\Leftarrow$) We have

(1) $\sigma \sim_P \sigma'$ and
(2) $((p, \sigma)) \rightsquigarrow_{NS} \overline{\tau}'$, $((p, \sigma')) \rightsquigarrow_{NS} \overline{\tau}'$ and
(3) if $\sigma \sim_P \sigma'$ and $((p, \sigma)) \rightsquigarrow_{NS} \overline{\tau}$, $((p, \sigma')) \rightsquigarrow_{NS} \overline{\tau}$, then $((p, \sigma)) \rightsquigarrow_S^{\omega} \overline{\tau}''$, $((p, \sigma')) \rightsquigarrow_S^{\omega} \overline{\tau}''$

Note that we got assumptions a) and b) by the unfolding of the definition of SNI. We need to show that $((p, \sigma)) \rightsquigarrow_S^{O} \overline{\tau}'$ and $((p, \sigma')) \rightsquigarrow_S^{O} \overline{\tau}'$ holds.

By using assumption a) and b) for assumption c), we get $((p, \sigma)) \rightsquigarrow_S^{\omega} \overline{\tau}''$, $((p, \sigma')) \rightsquigarrow_S^{\omega} \overline{\tau}''$.

Let O be an arbitrary prediction oracle with speculative window at most ω.

From Proposition 10 (S: Sound and Completeness between Spec and AM semantics) with $((p, \sigma)) \rightsquigarrow_S^{\omega} \overline{\tau}''$, $((p, \sigma')) \rightsquigarrow_S^{\omega} \overline{\tau}''$ we get back $((p, \sigma)) \rightsquigarrow_S^{O} \overline{\tau}$, $((p, \sigma')) \rightsquigarrow_S^{O} \overline{\tau}$. 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 10 (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 $((p, \sigma)) \rightsquigarrow_S^{\omega} \overline{\tau}$ and $((p, \sigma')) \rightsquigarrow_S^{\omega} \overline{\tau}$ iff $((p, \sigma)) \rightsquigarrow_S^{O} \overline{\tau}'$, $((p, \sigma)) \rightsquigarrow_S^{O} \overline{\tau}'$ for all prediction oracles O with speculative window at most ω.*

Proof. The proposition immediately follows from Lemma 63 (S: Soundness Am semantics w.r.t. speculative semantics) and Lemma 66 (S: Completeness Am semantics w.r.t. speculative semantics) □

Definition 32 (S: Relation between AM and spec for all oracles). *We define two relations between AM and oracle semantics. ≈ ∼*

$$\boxed{\Sigma_S \approx X_S}$$

$$\text{(Base)}\ \frac{}{\varnothing \approx \varnothing} \qquad \text{(Single-Base)}\ \frac{\Sigma_S \sim X_S\upharpoonright_{com} \quad INV(\Sigma_S, X_S)}{\Sigma_S \approx X_S}$$

$$\text{(Single-OracleTrue)}\ \frac{\begin{array}{c}\Sigma_S \sim X_S\upharpoonright_{com} \quad \Sigma_S'' \Downarrow_S^{\overline{\tau}} \Sigma_S''' \textit{ where transaction with id ctr is rolled back} \\ X_S = X_S' \cdot \langle p, ctr, \sigma, h, n'' \rangle \quad \Sigma_S = \Sigma_S' \cdot \langle p, ctr, \sigma, n \rangle \quad INV(\Sigma_S, X_S)\end{array}}{\Sigma_S' \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle \cdot \Sigma_{S1} \approx X_S' \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma, h, n''' \rangle^{true}}$$

$$\text{(Single-Transaction-Rollback)}\ \frac{\begin{array}{c}\Sigma_S'' \sim X_S''\upharpoonright_{com} \quad n' \geq 0 \quad \Sigma_S'' \Downarrow_S^{\overline{\tau}} \Sigma_S''' \textit{ where transaction with id ctr is rolled back} \\ X_S = X_S' \cdot \langle p, ctr, \sigma, h, n'' \rangle \quad \Sigma_S = \Sigma_S' \cdot \langle p, ctr, \sigma, n \rangle \quad INV(\Sigma_S, X_S)\end{array}}{\Sigma_S' \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle^{false} \cdot \Sigma_{S1} \approx X_S' \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma'', h', 0 \rangle^{false} \cdot X_{S1}}$$

$$\boxed{\Sigma_S \sim X_S}$$

$$\text{(Base)}\ \frac{}{\varnothing \sim \varnothing} \qquad \text{(Single)}\ \frac{|\Sigma_S'| = |X_S'| \quad \Sigma_S' \sim X_S'}{\Sigma_S' \cdot \langle p, ctr, \sigma, n \rangle^b \sim X_S' \cdot \langle p, ctr', \sigma, h, n' \rangle^b}$$

Later on, we will use the more general definition of $\approx$ defined in Definition 41 (Relation between AM and Oracle States General). We can recover $\Sigma_{\mathsf{S}} \approx X_{\mathsf{S}}$ by instantiating the general relation with a definition of elem_of_states found in Appendix R.15.

Lemma 62 (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) $\Sigma_{\mathsf{S}}^{init}(p, \sigma)$ and $\Sigma_{\mathsf{S}}^{init}(p, \sigma')$ and
(3) $X_{\mathsf{S}}^{init}(p, \sigma)$ and $X_{\mathsf{S}}^{init}(p, \sigma')$

Then

(1) $X_{\mathsf{S}}^{init}(p, \sigma) \cong X_{\mathsf{S}}^{init}(p, \sigma')$ and
(2) $\Sigma_{\mathsf{S}}^{init}(p, \sigma) \cong \Sigma_{\mathsf{S}}^{init}(p, \sigma')$ and
(3) $\Sigma_{\mathsf{S}}^{init}(p, \sigma) \approx X_{\mathsf{S}}^{init}(p, \sigma)$ and $\Sigma_{\mathsf{S}}^{init}(p, \sigma') \approx X_{\mathsf{S}}^{init}(p, \sigma')$ by Rule Single-Base

Proof. We have

(1) $\sigma, \sigma' \in InitConf$ and
(2) $\Sigma_{\mathsf{S}}^{init}(p, \sigma)$ and $\Sigma_{\mathsf{S}}^{init}(p, \sigma')$ and
(3) $X_{\mathsf{S}}^{init}(p, \sigma)$ and $X_{\mathsf{S}}^{init}(p, \sigma')$

Notice that by definition of $X_{\mathsf{S}}^{init}()$ and $\Sigma_{\mathsf{S}}^{init}()$ we have:

$$\begin{aligned}
X_{\mathsf{S}}^{init}(p, \sigma) &= \langle p, 0, \sigma, \emptyset, \bot\rangle \\
X_{\mathsf{S}}^{init}(p, \sigma') &= \langle p, 0, \sigma, \emptyset, \bot\rangle \\
\Sigma_{\mathsf{S}}^{init}(p, \sigma) &= \langle p, 0, \sigma, \bot\rangle \\
\Sigma_{\mathsf{S}}^{init}(p, \sigma') &= \langle p, 0, \sigma, \bot\rangle
\end{aligned}$$

I Immediate
II Immediate
III Immediate using Rule Single-Base

□

Lemma 63 (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) $((p, \sigma)) \Downarrow_{\mathsf{S}}^{\omega} \overline{\tau}$, $((p, \sigma')) \Downarrow_{\mathsf{S}}^{\omega} \overline{\tau}$

Then for all prediction oracles O with speculation window at most ω.

I $((p, \sigma)) \Downarrow_{\mathsf{S}}^{O} \overline{\tau}'$, $((p, \sigma)) \Downarrow_{\mathsf{S}}^{O} \overline{\tau}'$

Proof. Let $\omega \in \mathbb{N}$ be a speculation window and $\sigma, \sigma' \in InitConf$ be two initial configurations. We have:

(1) $((p, \sigma)) \Downarrow_{\mathsf{S}}^{\omega} \overline{\tau}$, $((p, \sigma')) \Downarrow_{\mathsf{S}}^{\omega} \overline{\tau}$

Furthermore, let O be an arbitrary prediction oracle with speculative window at most ω. Then we know there are executions $\Sigma^{init}_{\mathsf{S}}((p,\sigma)\Downarrow^{\overline{\tau}}_{\mathsf{S}}\Sigma'_{\mathsf{S}}$ and $\Sigma^{init}_{\mathsf{S}}(p,\sigma')\ {}^{O}\!\!\rightsquigarrow^{\mathsf{S}}_{\overline{\tau}}\Sigma''_{\mathsf{S}}$ where $\vdash \Sigma'_{\mathsf{S}} : \mathit{fin}$ and $\vdash \Sigma''_{\mathsf{S}} : \mathit{fin}$.

We unfold the definition of $()\ \text{👻}^{O}_{\mathsf{S}}$ and get $X^{init}_{\mathsf{S}}(p,\sigma)$ and $X^{init}_{\mathsf{S}}(p,\sigma')$ as initial states.

We need to find $\vdash X'_{\mathsf{S}} : \mathit{fin}, \vdash X''_{\mathsf{S}} : \mathit{fin}$ such that $X^{init}_{\mathsf{S}}(p,\sigma)\Downarrow^{\overline{\tau}}_{\mathsf{S}} X'_{\mathsf{S}}$ and $X^{init}_{\mathsf{S}}(p,\sigma')\ {}^{O}\!\!\rightsquigarrow^{\mathsf{S}}_{\overline{\tau}} X''_{\mathsf{S}}$.

Since we know by Lemma 62 (S: Initial states fulfill properties) that our initial states fulfill all the premises for Lemma 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states) we get:

(1) $X^{init}_{\mathsf{S}}(p,\sigma)\ {}^{O}\!\!\rightsquigarrow^{\mathsf{S}}_{\overline{\tau}'} X'_{\mathsf{S}1}$, $X^{init}_{\mathsf{S}}(p,\sigma')\ {}^{O}\!\!\rightsquigarrow^{\mathsf{S}}_{\overline{\tau}''} X'_{\mathsf{S}2}$
(2) $\Sigma'_{\mathsf{S}} \cong \Sigma''_{\mathsf{S}}$
(3) $X'_{\mathsf{S}1} \cong X'_{\mathsf{S}2}$ and $\overline{\rho} = \varnothing$
(4) $\Sigma'_{\mathsf{S}} \approx X'_{\mathsf{S}1}$ and $\Sigma'_{\mathsf{S}} \approx X'_{\mathsf{S}2}$
(5) $\overline{\tau}' = \overline{\tau}''$

We now argue, how we obtain final states from the oracle states $X'_{\mathsf{S}1}$ and $X'_{\mathsf{S}2}$.

Notice that because of $\vdash \Sigma'_{\mathsf{S}} : \mathit{fin}$ and $\vdash \Sigma''_{\mathsf{S}} : \mathit{fin}$ that $\Sigma'_{\mathsf{S}} \approx X'_{\mathsf{S}1}$ and $\Sigma'_{\mathsf{S}} \approx X'_{\mathsf{S}2}$ 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 $X'_{\mathsf{S}1}$ and $X'_{\mathsf{S}2}$. Since $X'_{\mathsf{S}1} \cong X'_{\mathsf{S}2}$, we know that $|X'_{\mathsf{S}1}| = |X'_{\mathsf{S}2}|$.

$|X'_{\mathsf{S}1}| = 1$ We know that $\Sigma'_{\mathsf{S}} \approx X'_{\mathsf{S}1}$ and $\vdash \Sigma'_{\mathsf{S}} : \mathit{fin}$.

Because of $\vdash \Sigma'_{\mathsf{S}} : \mathit{fin}$, we know that $\Sigma'_{\mathsf{S}}.\sigma \in \mathit{FinalConf}$.

Thus, by $\Sigma'_{\mathsf{S}} \approx X'_{\mathsf{S}1}$ we have $X'_{\mathsf{S}1}.\sigma \in \mathit{FinalConf}$ since $X'_{\mathsf{S}1}.\sigma = \Sigma'_{\mathsf{S}}.\sigma$.

Because $|X'_{\mathsf{S}1}| = 1$, we also have $X'_{\mathsf{S}1}.n = \bot$.

We can now conclude that $\vdash X'_{\mathsf{S}1} : \mathit{fin}$.

$|X'_{\mathsf{S}1}| > 1$ We know that $\Sigma'_{\mathsf{S}} \approx X'_{\mathsf{S}1}$ and $\vdash \Sigma'_{\mathsf{S}} : \mathit{fin}$.

Because of $\vdash \Sigma'_{\mathsf{S}} : \mathit{fin}$, we know that $\Sigma'_{\mathsf{S}}.\sigma \in \mathit{FinalConf}$ and $\vdash_O \Sigma'_{\mathsf{S}} : \mathit{noongoing}$

Thus, by $\Sigma'_{\mathsf{S}} \approx X'_{\mathsf{S}1}$ we have $X'_{\mathsf{S}1}.\sigma \in \mathit{FinalConf}$ since $X'_{\mathsf{S}1}.\sigma = \Sigma'_{\mathsf{S}}.\sigma$ and $\vdash_O X'_{\mathsf{S}1} : \mathit{noongoing}$,

Since $X'_{\mathsf{S}1}.\sigma \in \mathit{FinalConf}$ and $|X'_{\mathsf{S}1}| > 1$, we know there are speculative instances that need to be committed.

We can now apply Lemma 8 (Reaching Final state from final configuration (Finish commit instances)):

(1) $X'_{\mathsf{S}1}\ {}^{O}\!\!\rightsquigarrow^{\mathsf{S}}_{\overline{\tau}''} X'_{\mathsf{S}}$
(2) $\forall \tau \in \overline{\tau}^{\dagger}.\ \tau = \texttt{commit}\ \mathit{id}$ for some $\mathit{id} \in \mathbb{N}$
(3) $\vdash X'_{\mathsf{S}} : \mathit{fin}$
(4) $X'_{\mathsf{S}}.\sigma = X'_{\mathsf{S}1}.\sigma$

Because of $X'_{\mathsf{S}1} \cong X'_{\mathsf{S}2}$, we know that $X'_{\mathsf{S}2}$ generates the same trace with the same *ids* for the commits. Thus, $\vdash X'_{\mathsf{S}} : \mathit{fin}$.

The case for $X'_{\mathsf{S}2}$ are analogous and not shown here.

Thus, $((p,\sigma))\ \text{👻}^{O}_{\mathsf{S}}\overline{\tau}' \cdot \overline{\tau}^{\dagger}$, $((p,\sigma'))\ \text{👻}^{O}_{\mathsf{S}}\overline{\tau}' \cdot \overline{\tau}^{\dagger}$. ◻

Lemma 64 (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) $\Sigma_{\mathsf{S}1} \cong \Sigma_{\mathsf{S}2}$
(2) $X_{\mathsf{S}1} \cong X_{\mathsf{S}2}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma_{\mathsf{S}1} \approx X_{\mathsf{S}1}$ *and* $\Sigma_{\mathsf{S}2} \approx X_{\mathsf{S}2}$

(4) $\Sigma_{S1} \Downarrow_{S}^{\overline{\tau}} \Sigma'_{S1}$ *and* $\Sigma_{S2} \Downarrow_{S}^{\overline{\tau}} \Sigma'_{S2}$

Then for all prediction oracles O *with speculation window at most* ω.

I $X_{S1} \overset{O}{\rightsquigarrow}{}^{S}_{\overline{\tau}'} X'_{S1}, X_{S2} \overset{O}{\rightsquigarrow}{}^{S}_{\overline{\tau}''} X'_{S2}$
II $\Sigma'_{S1} \cong \Sigma'_{S2}$
III $X'_{S1} \cong X'_{S2}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{S1} \approx X'_{S1}$ *and* $\Sigma'_{S2} \approx X'_{S2}$
V $\overline{\tau}' = \overline{\tau}''$

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 $\Sigma_{S1} \Downarrow_{S}^{\varepsilon} \Sigma'_{S1}$ and $\Sigma_{S2} \Downarrow_{S}^{\varepsilon} \Sigma'_{S2}$, where $\Sigma'_{S1} = \Sigma_{S1}$ and $\Sigma'_{S2} = \Sigma_{S2}$.

Furthermore, we use Rule S:Reflection to derive $X_{S1} \overset{O}{\rightsquigarrow}{}^{S}_{\varepsilon} X'_{S1}, X_{S2} \overset{O}{\rightsquigarrow}{}^{S}_{\varepsilon} X'_{S2}$ 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 $\Sigma'_{S} \overset{\tau}{\rightsquigarrow}_{S} \Sigma'_{S1}$ and $\Sigma_{S2} \Downarrow_{S}^{\overline{\tau}''} \Sigma''_{S}$ and $\Sigma''_{S} \overset{\tau}{\rightsquigarrow}_{S} \Sigma'_{S2}$.

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) $X_{S1} \overset{O}{\rightsquigarrow}{}^{S}_{\overline{\tau}'} X'_{S}, X_{S2} \overset{O}{\rightsquigarrow}{}^{S}_{\overline{\tau}''} X''_{S}$
(b) $\Sigma'_{S} \cong \Sigma''_{S}$
(c) $X'_{S} \cong X''_{S}$ and $\overline{\rho}' = \varnothing$
(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 $\Sigma'_{S} \sim X'_{S}\upharpoonright_{com}$ and $INV(\Sigma'_{S}, X'_{S})$ (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 $minWndw(X'_{S}) = 0$ 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 9 (Executing a chain of commits) on X''_{S} and get

f) $X'_{S} \overset{O}{\rightsquigarrow}{}^{S}_{\overline{\tau}'''} X'''_{S}$
g) $minWndw(X'''_{S}) > 0$
h) $\forall \tau \in \overline{\tau}'''. \tau =$ `commit` id for some $id \in \mathbb{N}$
i) $X'_{S}.\sigma = X'''_{S}.\sigma$

By h) and the definition of $\upharpoonright_{ns}$ we have $\overline{\tau}''' \upharpoonright_{ns} = \varepsilon$.

Furthermore, $X'_{S}\upharpoonright_{com} = X'''_{S}\upharpoonright_{com}$ by definition of $\upharpoonright_{com}$ (we only executed commits) and $|X'_{S}\upharpoonright_{com}| = |X'''_{S}\upharpoonright_{com}|$.

Thus, $\Sigma'_{S} \sim X'''_{S}\upharpoonright_{com}$, $INV(\Sigma'_{S}, X'''_{S})$ and we have $\Sigma'_{S} \approx X'''_{S}$ by Rule Single-Base.

We now proceed by inversion on the derivations $\Sigma'_{S} \overset{\tau}{\rightsquigarrow}_{S} \Sigma'_{S1}$ and $\Sigma''_{S} \overset{\tau}{\rightsquigarrow}_{S} \Sigma'_{S2}$.

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 $\Psi'_{S} \overset{\tau}{\rightsquigarrow}_{S} \overline{\Psi}'_{4}$ and $\Psi''_{S} \overset{\tau}{\rightsquigarrow} \overline{\Psi}'''_{4}$ where $\Sigma'_{S} = \overline{\Psi}_{4} \cdot \Psi'_{S}$ and $\Sigma''_{S} = \overline{\Psi}''_{4} \cdot \Psi''_{S}$.

Furthermore, note that all states point to the same instruction by b)-d).

Using Lemma 65 (S: Soundness Single Step AM) on $\Psi'_{\mathsf{S}} \xrightarrow{\tau}_{\mathsf{S}} \overline{\Psi}'_4$ and $\Psi''_{\mathsf{S}} \xrightarrow{\tau} \overline{\Psi}'''_4$ we get the desired result.

Rule S:AM-Rollback Contradiction, because $minWndw(X'''_{\mathsf{S}}) > 0$ and $INV(\Sigma'_{\mathsf{S}}, X'''_{\mathsf{S}})$.

v4-com-single-oracle We thus have

$$X'_{\mathsf{S}} = X_{\mathsf{S}3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma, h, n''' \rangle^{true}$$
$$\Sigma'_{\mathsf{S}} = \Sigma_{\mathsf{S}3} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle \cdot \Sigma_{\mathsf{S}4}$$
$$X_{\mathsf{S}} = X_{\mathsf{S}3} \cdot \langle p, ctr, \sigma, h, n'' \rangle$$
$$\Sigma_{\mathsf{S}} = \Sigma_{\mathsf{S}3} \cdot \langle p, ctr, \sigma, n \rangle$$
$$\Sigma_{\mathsf{S}} \sim X_{\mathsf{S}} \upharpoonright_{com}$$
$$INV(\Sigma_{\mathsf{S}}, X_{\mathsf{S}})$$

The form of X''_{S} and Σ''_{S} is analogous. We now apply inversion on $\Sigma'_{\mathsf{S}} \xrightarrow{\tau}_{\mathsf{S}} \Sigma'_{\mathsf{S}1}$.

Rule S:AM-Context We choose $X'_{\mathsf{S}1} = X'_{\mathsf{S}}$ and $X'_{\mathsf{S}2} = X''_{\mathsf{S}}$.

I By IH a)

II By Lemma 60 (S AM: Single step preserves $\cong$).

III Since $X'_{\mathsf{S}1} = X'_{\mathsf{S}}$ and $X'_{\mathsf{S}2} = X''_{\mathsf{S}}$, we are finished using IH c).

IV We show that $X'_{\mathsf{S}1} \approx \Sigma'_{\mathsf{S}1}$ by Rule Single-OracleTrue. The proof for $X'_{\mathsf{S}2} \approx \Sigma'_{\mathsf{S}2}$ 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 $\Sigma_{\mathsf{S}} \sim X_{\mathsf{S}} \upharpoonright_{com}$ and $INV(\Sigma_{\mathsf{S}}, X_{\mathsf{S}}) X_{\mathsf{S}} \upharpoonright_{com}$ 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 $X'_{\mathsf{S}1} = X'_{\mathsf{S}}$ and $X'_{\mathsf{S}2} = X''_{\mathsf{S}}$.

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 $X'_{\mathsf{S}1} = X'_{\mathsf{S}}$ and $X'_{\mathsf{S}2} = X''_{\mathsf{S}}$

I By IH a)

IV Here, we only show $\Sigma'_{\mathsf{S}1} \approx X'_{\mathsf{S}1}$ by Rule Single-Base. The proof for $\Sigma'_{\mathsf{S}2} \approx X'_{\mathsf{S}2}$ is analogous.

Notice that $\Sigma'_{\mathsf{S}1} = \Sigma_{\mathsf{S}3} \cdot \langle p, ctr'', \sigma, n \rangle$ (updated *ctr*) after the rollback.

Combined with the constructed $X'_{\mathsf{S}1}$, we have $\Sigma'_{\mathsf{S}1} \sim X'_{\mathsf{S}1} \upharpoonright_{com}$ and $INV(\Sigma'_{\mathsf{S}1}, X'_{\mathsf{S}1})$ by our assumptions.

So we can use Rule Single-Base and have $\Sigma'_{\mathsf{S}1} \approx X'_{\mathsf{S}1}$.

V By IH e)

v4-com-single-rollback We have

$$\begin{aligned}
X'_{\mathsf{S}} =& X_{\mathsf{S}3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma'', h', 0 \rangle^{false} \cdot X_{\mathsf{S}4} \\
\Sigma'_{\mathsf{S}} =& \Sigma_{\mathsf{S}3} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle^{false} \cdot \Sigma_{\mathsf{S}4} \\
X_{\mathsf{S}} =& X_{\mathsf{S}3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \\
\Sigma_{\mathsf{S}} =& \Sigma_{\mathsf{S}3} \cdot \langle p, ctr, \sigma, n \rangle \\
\Sigma_{\mathsf{S}} \sim& X_{\mathsf{S}} \upharpoonright_{com} \\
& INV(\Sigma_{\mathsf{S}}, X_{\mathsf{S}}) \\
n' \geq& 0
\end{aligned}$$

The form of X''_{S} and Σ''_{S} is analogous.

Additionally, we know that the transaction terminates in some state $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}}_{\mathsf{S}} \Sigma'''_{\mathsf{S}}$. There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma'_{\mathsf{S}} \overset{\tau}{=\!\!\Omega}_{\mathsf{S}} \Sigma'_{\mathsf{S}1}$ 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 $\Sigma''_{\mathsf{S}} \overset{\tau}{=\!\!\Omega}_{\mathsf{S}} \Sigma'_{\mathsf{S}2}$ as well.

We choose $X'_{\mathsf{S}1} = X'_{\mathsf{S}}$ and $X'_{\mathsf{S}2} = X''_{\mathsf{S}}$.

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 $\Sigma'_{\mathsf{S}} \overset{\tau}{=\!\!\Omega}_{\mathsf{S}} \Sigma'_{\mathsf{S}1}$ was created by Rule S:AM-Rollback and is a rollback for *ctr*.

I Here we prove that $X'_{\mathsf{S}} \overset{\tau_0}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X'_{\mathsf{S}1}$ and $X''_{\mathsf{S}} \overset{\tau_1}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X'_{\mathsf{S}2}$.

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 $X'_{\mathsf{S}} \overset{\tau_0}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X'_{\mathsf{S}1}$ and $X''_{\mathsf{S}} \overset{\tau_1}{\rightsquigarrow}{}^{O}_{\mathsf{S}} X'_{\mathsf{S}2}$ are derived by Rule S:Rollback.

II By Lemma 60 (S AM: Single step preserves ≅)

III By Lemma 61 (S SE: Single step preserves ≅) with fact V).

IV Here, we only show $\Sigma'_{\mathsf{S}1} \approx X'_{\mathsf{S}1}$ by Rule Single-Base. The proof for $\Sigma'_{\mathsf{S}2} \approx X'_{\mathsf{S}2}$ is analogous.

We know that the states after rollback are

$$\begin{aligned}
X'_{\mathsf{S}1} &= X_{\mathsf{S}3} \cdot \langle p, ctr', \sigma, h', n'' \rangle \\
\Sigma'_{\mathsf{S}1} &= \Sigma_{\mathsf{S}3} \cdot \langle p, ctr', \sigma, n \rangle
\end{aligned}$$

Notice, that the only difference to X_{S} and Σ_{S} is the updated *ctr*. We also know by assumption that $\Sigma_{\mathsf{S}} \sim X_{\mathsf{S}} \upharpoonright_{com}$ and $INV(\Sigma_{\mathsf{S}}, X_{\mathsf{S}})$.

By construction of $X'_{\mathsf{S}1}$ and $\Sigma'_{\mathsf{S}1}$, we can conclude that $\Sigma'_{\mathsf{S}} \sim X'_{\mathsf{S}1} \upharpoonright_{com}$ and $INV(\Sigma'_{\mathsf{S}1}, X'_{\mathsf{S}1})$.

This allows us to use Rule Single-Base to derive $\Sigma'_{\mathsf{S}1} \approx X'_{\mathsf{S}1}$.

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 65 (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, $\Sigma_{S1} = \Sigma'_S \cdot \Phi'_S$, $\Sigma_{S2} = \Sigma''_S \cdot \Phi''_S$ 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) $\Sigma_{S1} \approx X_{S1}$ *and* $\Sigma_{S2} \approx X_{S2}$
(4) $\Phi'_S \overset{\tau''}{\Longrightarrow}_S \Sigma'_{S1}$ *and* $\Phi''_S \overset{\tau''}{\Longrightarrow}_S \Sigma'_{S2}$

then there are instances X'_{S1}, X'_{S2} for the speculative semantics such that:

I $X_{S1} \overset{O}{\rightsquigarrow}{}^{S}_{\tau} X'_{S1}$ *and* $X_{S2} \overset{O}{\rightsquigarrow}{}^{S}_{\tau'} X'_{S2}$
II $\Sigma'_{S1} \cong \Sigma'_{S2}$
III $X'_{S1} \cong X'_{S2}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{S1} \approx X'_{S1}$ *and* $\Sigma'_{S2} \approx X'_{S2}$
V $\tau = \tau'$

Proof. We proceed by inversion on $\Phi'_S \overset{\tau''}{\Longrightarrow}_S \Sigma'_{S1}$ and $\Phi''_S \overset{\tau''}{\Longrightarrow}_S \Sigma'_{S2}$:

Rule S:AM-General We choose $X'_{S1} = X'_S$ and $X'_{S2} = X''_S$.

- **I** By Rule S:Reflection.
- **II** Notice that by Rule S:AM-General we have $\Sigma'_{S1} = \Sigma_{S1}$ and $\Sigma'_{S2} = \Sigma_{S2}$, because the rule only emits the observations in $\overline{\rho}$. We are finished by using assumption 1).
- **III** Since $X'_{S1} = X'_S$ and $X'_{S2} = X''_S$, we are finished using assumption 3).
- **IV** Here, we only show $\Sigma'_{S1} \approx X'_{S1}$ by Rule Single-Base. The proof for $\Sigma'_{S2} \approx X'_{S2}$ is analogous.
  The use of Rule S:AM-General does not change the state. That is why $\Sigma'_{S1} = \Sigma_{S1\rho\backslash\tau}$.
  By our assumptions we have $\Sigma_{S1} \sim X_{S1}\upharpoonright_{com}$ and $INV(\Sigma_{S1}, X_{S1})$.
  After substitution we have $\Sigma'_{S1} \sim X'_{S1}\upharpoonright_{com}$ and $INV(\Sigma'_{S1}, X'_{S1})$. Thus, we fulfill all premises for Rule Single-Base and $\Sigma'_{S1} \approx X'_{S1}$.
- **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.

$(true, \omega)$ **correct prediction w.r.t X'_S** The store instruction is not skipped and is executed normally.

- **I** We use Rule S:Store-Exe to derive the steps $X_{S1} \overset{\tau_0}{\rightsquigarrow}{}^{O}_{S} X'_S$ and $X_{S2} \overset{\tau_1}{\rightsquigarrow}{}^{O}_{S} X''_S$.
  Furthermore, we execute Rule S:General once, because Rule S:Store-Exe created one observation in $\overline{\rho}$. We now have $X'_{S1} = X'_S$ 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 $X_{S1} \overset{O}{\rightsquigarrow}{}^{S}_{\overline{\tau}} X'_{S1}$ and $X_{S2} \overset{O}{\rightsquigarrow}{}^{S}_{\overline{\tau'}} X'_{S2}$.
- **II** By Lemma 60 (S AM: Single step preserves $\cong$)
- **III** By Lemma 61 (S SE: Single step preserves $\cong$) for $X_{S1} \overset{\tau_0}{\rightsquigarrow}{}^{O}_{S} X'_S$ and $X_{S2} \overset{\tau_1}{\rightsquigarrow}{}^{O}_{S} X''_S$ 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

$$X'_{S1} = X'_{S3} \cdot \langle p, ctr, \sigma', h, n\rangle \cdot \langle p, ctr', \sigma', h', n_0\rangle^{true}$$
$$\Sigma'_{S1} = \Sigma_{S3} \cdot \langle p, ctr, \sigma', n_1\rangle \cdot \langle p, ctr', \sigma'', n_2\rangle$$
$$X'_{S4} = X'_{S3} \cdot \langle p, ctr, \sigma', h, n\rangle$$
$$\Sigma'_{S4} = \Sigma_{S3} \cdot \langle p, ctr, \sigma'', n_1\rangle$$

We now show that $\Sigma'_{S4} \sim X'_{S4}$.

$|\Sigma'_{S4}| = |X'_{S4}\upharpoonright_{com}|$ First, notice that $|X_{S1}\upharpoonright_{com}| = |X'_{S4}\upharpoonright_{com}|$, because the rule does not change b. Similarly, $|\Sigma_{S1}| = |\Sigma'_{S4}|$ and by our assumption $|\Sigma_{S1}| = |X_{S1}\upharpoonright_{com}|$ we get after substitution: $|\Sigma'_{S4}| = |X'_{S4}\upharpoonright_{com}|$.

$\sigma' = \sigma''$ We know that $X_{S1}.\sigma \xrightarrow{\tau_0} X'_{S4}.\sigma$ and $\Sigma'_{S}.\sigma \xrightarrow{\tau} \Sigma'_{S4}.\sigma$. Because of $\Sigma_{S1} \approx X_{S1}$ and the fact that $\rightarrow$ is deterministic, we know that $\Sigma'_{S4}.\sigma = X'_{S4}.\sigma$. Thus, $\sigma' = \sigma''$

We can now conclude that $\Sigma'_{S4} \sim X'_{S4}\upharpoonright_{com}$.

We now show that $INV(\Sigma'_{S4}, X'_{S4})$ holds.

$|\Sigma'_{S4}| = |X'_{S4}\upharpoonright_{com}|$ Already shown above.

$1 \le i \le |\Sigma'_{S4}|$, $minWndw(X'_{S4}\upharpoonright_{com}{}^{i}) \le \Sigma'_{S4}{}^{i}.n$ There are two cases: Either $\Sigma'_{S4}{}^{i}.n = \Sigma_{S1}.n - 1$ (if $i = |\Sigma'_{S4}|$) or $\Sigma'_{S4}{}^{i}.n = \Sigma_{S1}.n$. We will prove it for $\Sigma'_{S4}{}^{i}.n = \Sigma_{S1}.n - 1$, because that automatically yields us the the result for $\Sigma'_{S4}{}^{i}.n = \Sigma_{S1}.n$.
From Rule S:Store-Exe (which does not change older labels b) and the fact that we have a correct prediction we have $minWndw(X'_{S4}\upharpoonright_{com}{}^{i}) = minWndw(decr(X_{S1})\upharpoonright_{com}{}^{i})$.
From the definition of $decr()$ we get $minWndw(decr(X_{S1})\upharpoonright_{com}{}^{i}) \le minWndw(X_{S1}\upharpoonright_{com}{}^{i})$.
Also, $minWndw(decr(X_{S1})\upharpoonright_{com}{}^{i}) \le \Sigma_{S1}.n - 1$, because $n > 0$ and $INV(\Sigma_{S1}, X_{S1})$. If n was 0, we would have executed Rule S:AM-Rollback instead of the store. Now we get:

$$minWndw(X_{S1}\upharpoonright_{com}{}^{i}) \le \Sigma_{S1}{}^{i}.n$$
$$minWndw(decr(X_{S1})\upharpoonright_{com}{}^{i}) \le \Sigma_{S1}{}^{i}.n - 1$$
$$minWndw(decr(X_{S1})\upharpoonright_{com}{}^{i}) \le \Sigma'_{S4}{}^{i}.n$$
$$minWndw(X'_{S4}\upharpoonright_{com}{}^{i}) \le \Sigma'_{S4}{}^{i}.n$$

which proves our claim.

We now show by which rule $\Sigma'_{S1} \approx X'_{S1}$ are related.
For that, we do a case distinction if there are transactions that need to be rolled back or not in X'_{S1}. We have to do this, because we only know that $minWndw(X_{S1}) > 0$ *before* we did the step. So it could happen that $minWndw(X'_{S1}) = 0$ 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'_{S1} 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 $X'_{\mathsf{S}1}$ with window 0 Then we relate by Rule Single-Transaction-Rollback, because there is an instance in $X'_{\mathsf{S}1}$ 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 fulfil 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 $X_{\mathsf{S}1} \cong X_{\mathsf{S}2}$ we know that $X_{\mathsf{S}1}.\sigma(\mathbf{pc}) = X_{\mathsf{S}2}.\sigma(\mathbf{pc})$ and $X_{\mathsf{S}1}.ctr = X_{\mathsf{S}2}.ctr$.

As a result, by $X_{\mathsf{S}1}.ctr = ctr_1$ and $X_{\mathsf{S}2}.ctr = ctr_2$ we have $ctr_1 = ctr_2$.

Since $\Sigma_{\mathsf{S}1} \approx X_{\mathsf{S}1}$, we have $\Sigma_{\mathsf{S}1}.\sigma = X_{\mathsf{S}1}.\sigma$ (similar for $\Sigma_{\mathsf{S}2}$ and $X_{\mathsf{S}2}$).

We know that the observation $\tau'' = \texttt{store}\ m$ is generated by $\Sigma_{\mathsf{S}1}.\sigma \xrightarrow{\tau''} \Sigma'_{\mathsf{S}1}.\sigma$ and $\Sigma_{\mathsf{S}2}.\sigma \xrightarrow{\tau''} \Sigma'_{\mathsf{S}2}.\sigma$ in the step Rule S:AM-Store-Spec and similarly $X_{\mathsf{S}1}.\sigma \xrightarrow{\texttt{store}\ m} X'_{\mathsf{S}1}.\sigma$ and $X_{\mathsf{S}2}.\sigma \xrightarrow{\texttt{store}\ m'} X'_{\mathsf{S}2}.\sigma$

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.

$(false, \omega)$ **wrong prediction w.r.t X'_{S}** The store instruction is skipped.

I We use Rule S:Store-Skip to derive the steps $X'_{\mathsf{S}} \overset{\tau_0}{\rightsquigarrow}{}^{O}_{\mathsf{S}}\ X'_{\mathsf{S}1}$ and $X''_{\mathsf{S}} \overset{\tau_1}{\rightsquigarrow}{}^{O}_{\mathsf{S}}\ X'_{\mathsf{S}2}$.

Furthermore, we execute Rule S:General twice, because Rule S:Store-Exe created two observations in $\overline{\rho}$. We now have $X'_{\mathsf{S}1} = X'_{\mathsf{S}}$ 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 $X_{\mathsf{S}1} \ {}^{O}\!\!\rightsquigarrow^{\mathsf{S}}_{\overline{\tau}} X'_{\mathsf{S}1}$ and $X_{\mathsf{S}2} \ {}^{O}\!\!\rightsquigarrow^{\mathsf{S}}_{\overline{\tau}'} X'_{\mathsf{S}2}$.

Notice that the observations in $\overline{\rho}$ are equal between $X_{\mathsf{S}1}$ and $X_{\mathsf{S}2}$, because of (2). We have $X_{\mathsf{S}1}.ctr = X_{\mathsf{S}2}.ctr$ and $X_{\mathsf{S}1}.\sigma \sim_{\mathbf{pc}} X_{\mathsf{S}2}.\sigma$ from our relation.

II By Lemma 60 (S AM: Single step preserves $\cong$)

III By Lemma 61 (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:

$$
\begin{aligned}
X'_{\mathsf{S}1} =& X'_{\mathsf{S}3} \cdot \langle p, ctr, \sigma', h, n\rangle \cdot \langle p, ctr', \sigma''', h', n_0\rangle^{false}\\
\Sigma'_{\mathsf{S}1} =& \Sigma_{\mathsf{S}3} \cdot \langle p, ctr, \sigma', n_1\rangle \cdot \langle p, ctr', \sigma'', n_2\rangle\\
X'_{\mathsf{S}4} =& X'_{\mathsf{S}3} \cdot \langle p, ctr, \sigma', h, n\rangle\\
\Sigma'_{\mathsf{S}4} =& \Sigma_{\mathsf{S}3} \cdot \langle p, ctr, \sigma', n_1\rangle
\end{aligned}
$$

We now show that $\Sigma'_{\mathsf{S}1} \sim X'_{\mathsf{S}1}$ and $INV(\Sigma'_{\mathsf{S}1}, X'_{\mathsf{S}1})$ hold.

Notice that we assume $\Sigma'_{\mathsf{S}4} \sim X'_{\mathsf{S}4}\restriction_{com}$ and $INV(\Sigma'_{\mathsf{S}4}, X'_{\mathsf{S}4})$, because the proofs are exactly the same as above.

We start by showing $\Sigma'_{\mathsf{S}1} \sim X'_{\mathsf{S}1}$:

$|\Sigma'_{\mathsf{S}1}| = |X'_{\mathsf{S}1}\restriction_{com}|$ We have $|X'_{\mathsf{S}1}\restriction_{com}| = |X'_{\mathsf{S}4}\restriction_{com}| + 1$ and $|\Sigma'_{\mathsf{S}1}| = |\Sigma'_{\mathsf{S}4}| + 1$, because we mispredict. By assumption $\Sigma'_{\mathsf{S}4} \sim X'_{\mathsf{S}4}$ we have $|\Sigma'_{\mathsf{S}4}| = |X'_{\mathsf{S}4}\restriction_{com}|$ and are thus finished.

$\sigma''' = \sigma''$ Since the rules applied, changed $X_{\mathsf{S}1}.\sigma$ and $\Sigma_{\mathsf{S}1}.\sigma$ in the same way and the fact that $X_{\mathsf{S}1}.\sigma = \Sigma_{\mathsf{S}1}.\sigma$ we get $\sigma''' = \sigma''$.

We can now conclude that $\Sigma'_{S1} \sim X'_{S1}\upharpoonright_{com}$.

Now for $INV(\Sigma'_{S1}, X'_{S1})$:

$|\Sigma'_{S1}| = |X'_{S1}\upharpoonright_{com}|$ Already shown above.

$1 \leq i \leq |\Sigma'_{S1}|$, $minWndw(X'_{S1}\upharpoonright_{com}{}^{i}) \leq \Sigma'_{S1}{}^{i}.n$ There are two cases:

Either $\Sigma'_{S1}{}^{i}.n = \min(\Sigma'_{S4}.n + 1, \omega)$ (if $i = |\Sigma'_{S1}|$) or $\Sigma'_{S1}{}^{i}.n = \Sigma_{S1}.n$.

We will prove it for $\Sigma'_{S1}{}^{i}.n = \min(\Sigma'_{S4}.n + 1, \omega)$, because we have the result for $i \leq |\Sigma'_{S1}|$ by assumption $INV(\Sigma'_{S4}, X'_{S4})$.

By $INV(\Sigma'_{S4}, X'_{S4})$ we know this holds for Σ'_{S4} and X'_{S4}.

Notice that $minWndw(X'_{S1}\upharpoonright_{com}) \leq minWndw(X'_{S4}\upharpoonright_{com})$.

Furthermore, $\Sigma'_{S4}.n \leq \Sigma'_{S1}.n$ (the 1 comes from the fact that the window is reduced when executing the store normally), because $\Sigma'_{S1} = \min(\Sigma'_{S4}.n + 1, \omega)$ and the fact that all possible values for n are bound by ω.

Now we have:

$$minWndw(X_{S1}\upharpoonright_{com}{}^{i}) \leq \Sigma_{S1}{}^{i}.n$$

$$minWndw(decr(X_{S1})\upharpoonright_{com}{}^{i}) \leq \Sigma_{S1}{}^{i}.n - 1$$

$$minWndw(decr(X_{S1})\upharpoonright_{com}{}^{i}) \leq \Sigma'_{S4}{}^{i}.n$$

$$minWndw(X'_{S4}\upharpoonright_{com}{}^{i}) \leq \Sigma'_{S4}{}^{i}.n \; minWndw(X'_{S1}\upharpoonright_{com}) \leq minWndw(X'_{S4}\upharpoonright_{com})$$

$$minWndw(X'_{S1}\upharpoonright_{com}{}^{i}) \leq \Sigma'_{S4}{}^{i}.n \; \Sigma'_{S4}.n \leq \Sigma'_{S1}.n$$

$$minWndw(X'_{S1}\upharpoonright_{com}{}^{i}) \leq \Sigma'_{S1}{}^{i}.n$$

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'_{S1}.

No Transaction that needs to be rolled back in X'_{S1} 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'_{S1} 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

$$\overline{\tau} = \texttt{store}\ m \cdot \texttt{start}\ X_{S1}.ctr \cdot \texttt{bypass}\ X_{S1}.\sigma(\mathbf{pc})$$

$$\overline{\tau}' = \texttt{store}\ m' \cdot \texttt{start}\ X_{S2}.ctr \cdot \texttt{bypass}\ X_{S2}.\sigma(\mathbf{pc})$$

for some $m, m' \in Vals$.

From (2) we have $X_{S1}.ctr = X_{S2}.ctr$ and $X_{S1}.\sigma \sim_{\mathbf{pc}} X_{S2}.\sigma$.

We know that the observation $\tau'' = \texttt{store}\ m$ is generated by $\Sigma_{S1}.\sigma \xrightarrow{\tau''} \Sigma'_{S1}.\sigma$ and $\Sigma_{S2}.\sigma \xrightarrow{\tau''} \Sigma'_{S2}.\sigma$ in the step Rule S:AM-Store-Spec and similarly $X_{S1}.\sigma \xrightarrow{\texttt{store}\ m'} X'_{S1}.\sigma$ and $X_{S2}.\sigma \xrightarrow{\texttt{store}\ m'} X'_{S2}.\sigma$.

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_{S1} and X_{S2}.

We get $X'_S \overset{\tau_0}{\rightsquigarrow}{}_S^O X'_{S1}$ and $X''_S \overset{\tau_0}{\rightsquigarrow}{}_S^O X'_{S2}$.

II By Lemma 60 (S AM: Single step preserves ≅).

III By Lemma 61 (S SE: Single step preserves ≅).

IV After the **spbarr** instruction, we know that there could be speculative transactions in X'_{S1} that has a speculation window of 0.

We prove that $\Sigma'_{S1} \sim X'_{S1}\upharpoonright_{com}$. The proof for $\Sigma'_{S2} \sim X'_{S2}\upharpoonright_{com}$ is analogous.

$\Sigma'_{S1}.\sigma = X'_{S1}.\sigma$ We know by 3) that $\Sigma_{S1}.\sigma = X_{S1}.\sigma$.

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.

$|X'_{S1}\upharpoonright_{com}| = |\Sigma'_{S1}|$ Since the executed rule does not add or remove speculative instances, we know that this holds by assumption.

We prove $INV(\Sigma'_{S1}, X'_{S1})$ still holds. The proof for $INV(\Sigma'_{S2}, X'_{S2})$ is analogous.

We need to show that $|\Sigma'_{S1}| = |X'_{S1}\upharpoonright_{com}|$ and for all $1 \leq i \leq |\Sigma'_{S1}|$, $minWndw(X'_{S1}\upharpoonright_{com}{}^{i}) \leq \Sigma'_{S1}{}^{i}.n$.

$|\Sigma'_{S1}| = |X'_{S1}\upharpoonright_{com}|$ Follows from above.

$1 \leq i \leq |\Sigma'_S|$, $minWndw(X'_S\upharpoonright_{com}{}^{i}) \leq \Sigma'_{S1}{}^{i}.n$ Since the executed instruction was a barrier instruction, we know that $minWndw(X'_S\upharpoonright_{com}{}^{i}) = 0$.

There are two cases dependent on the chosen i:

$i = |\Sigma'_{S1}|$ Then $\Sigma'_{S1}{}^{i}.n = 0$, because of the **spbarr** instruction and therefore $minWndw(X'_{S1}\upharpoonright_{com}{}^{i}) \leq \Sigma'_{S1}{}^{i}.n$.

$i < |\Sigma'_{S1}|$ Then $\Sigma'_{S1}.n = \Sigma'_S.n$ and we have $minWndw(X'_{S1}\upharpoonright_{com}{}^{i}) \leq \Sigma'_{S1}{}^{i}.n$, since $minWndw(X'_{S1}\upharpoonright_{com}{}^{i}) = 0$.

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'_{S1}. Note that by assumption 1) that a similar transaction exists then in X'_{S2} as well.

no transaction with speculation window 0 Then we have $\Sigma'_{S1} \approx X'_{S1}$ by Rule Single-Base using the facts $\Sigma'_{S1} \sim X'_{S1}\upharpoonright_{com}$ and $INV(\Sigma'_{S1}, X'_{S1})$.

transaction with speculation window 0 We know by construction, that there exists a speculative transaction in Σ'_{S1} with the same transaction id. We showed that $\Sigma'_{S1} \sim X'_{S1}\upharpoonright_{com}$ and $INV(\Sigma'_{S1}, X'_{S1})$ 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 $\Sigma_{S1}.\sigma \xrightarrow{\tau''} \Sigma'_{S1}$ and $X_{S1}.\sigma \xrightarrow{\tau_0} X'_{S1}$. Similarly, $\Sigma_{S2}.\sigma \xrightarrow{\tau''} \Sigma'_{S2}$ and $X_{S2}.\sigma \xrightarrow{\tau_1} X'_{S2}.\sigma$.

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 $INV(\Sigma'_{S1}, X'_{S1})$ is the same as for the store instructions above.

□

Definition 33 (Constructing the Oracle). *Constructing the prediction oracle ${O_{am}}^{\mathsf{S}}$. We build our oracle based on the executions $\Sigma_{\mathsf{S}}^{init}(p,\sigma) \Downarrow_{\mathsf{S}}^{\overline{\tau}} \Sigma_{\mathsf{S}1} \overset{\tau_{am}}{=\!=\!\Rightarrow}_{\mathsf{S}} \Sigma_{\mathsf{S}2}, \Sigma_{\mathsf{S}}^{init}(p,\sigma') \Downarrow_{\mathsf{S}}^{\overline{\tau}} \Sigma'_{\mathsf{S}1} \overset{\tau'_{am}}{=\!=\!\Rightarrow}_{\mathsf{S}} \Sigma'_{\mathsf{S}2}$ where $\tau_{am} \neq \tau'_{am}$.*

Let us denote by the set RB the ids of all ongoing transaction ids in $\Sigma_{\mathsf{S}1}$. Since $\Sigma_{\mathsf{S}1} \cong \Sigma'_{\mathsf{S}1}$ we know that the same transaction ids are still ongoing in $\Sigma'_{\mathsf{S}1}$ 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:

$$
{O_{am}}^{\mathsf{S}}(p,n,h) = \begin{cases} (false, \omega) \text{ if } |h| \in RB \wedge p(\sigma(\mathbf{pc})) = \mathbf{store}\ x, e \\ (false, 0) \text{ otherwise (where } p(\sigma(\mathbf{pc})) = \mathbf{store}\ x, e) \end{cases}
$$

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 store at line 1000 is vulnerable to a V4 Spectre attack. The misprediction of the store at line 1 does not influence 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.*

For a given execution $\Sigma_x \Downarrow_{xy}^{\overline{\tau}} \Sigma'_x$ we can extract all the states into a set Σ^{States}.

Definition 34 (S: Relation between AM and Spec for oracles that only mispredict). *We define one relation, $\approx_{{O_{am}}^{\mathsf{S}}}^{\Sigma^{States}}$, between AM and oracle semantics. Note that $\approx_{{O_{am}}^{\mathsf{S}}}^{\Sigma^{States}}$ is indexed by an oracle and only holds for a specific part of an execution indexed by Σ^{States}. This oracle has to always mispredict.*

$$\boxed{\Sigma_{\mathsf{S}} \approx_{{O_{am}}^{\mathsf{S}}}^{\Sigma^{States}} X_{\mathsf{S}}}$$

$$
\text{(Base-Oracle)}\ \frac{}{\varnothing \approx_{{O_{am}}^{\mathsf{S}}}^{\Sigma^{States}} \varnothing}
\qquad
\text{(Single-Base-Oracle)}\ \frac{\Sigma_{\mathsf{S}} \sim X_{\mathsf{S}}\upharpoonright_{com} \quad INV2(\Sigma_{\mathsf{S}}, X_{\mathsf{S}}) \quad minWndw(X_{\mathsf{S}}) > 0 \quad \Sigma_{\mathsf{S}} \in \Sigma^{States}}{\Sigma_{\mathsf{S}} \approx_{{O_{am}}^{\mathsf{S}}}^{\Sigma^{States}} X_{\mathsf{S}}}
$$

$$
\text{(Single-Transaction-Rollback-Oracle)}\ \frac{\begin{array}{c}\Sigma''_{\mathsf{S}} \sim X''_{\mathsf{S}}\upharpoonright_{com} \quad n' \geq 0 \quad \Sigma''_{\mathsf{S}} \Downarrow_{\mathsf{S}}^{\overline{\tau}} \Sigma'''_{\mathsf{S}} \text{ where transaction with id ctr is rolled back} \\ X_{\mathsf{S}} = X'_{\mathsf{S}} \cdot \langle p, ctr, \sigma, h, n''\rangle \quad \Sigma_{\mathsf{S}} = \Sigma'_{\mathsf{S}} \cdot \langle p, ctr, \sigma, n\rangle \quad INV2(\Sigma_{\mathsf{S}}, X_{\mathsf{S}}) \\ \Sigma'_{\mathsf{S}} \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle^{false} \cdot \Sigma_{\mathsf{S}1} \in \Sigma^{States}\end{array}}{\Sigma'_{\mathsf{S}} \cdot \langle p, ctr, \sigma, n\rangle \cdot \langle p, ctr', \sigma', n'\rangle^{false} \cdot \Sigma_{\mathsf{S}1} \approx_{{O_{am}}^{\mathsf{S}}}^{\Sigma^{States}} X'_{\mathsf{S}} \cdot \langle p, ctr, \sigma, h, n''\rangle \cdot \langle p, ctr', \sigma'', h', 0\rangle^{false}}
$$

Why is the relation indexed by the oracle and a specific execution? We prove Completeness via the contrapositive. Thus, we have two AM executions that differ in their traces and need to find two Oracle executions that differ as well for a specific oracle. We use the AM execution to guide the oracle to the difference in the trace. This means that the oracle always mispredicts. Furthermore, the relation we define only holds up to that point of the AM execution where the difference is. The reason has to do with how in the Oracle semantics the speculation window is reduced for all states per step, instead of only the topmost one. This results in *INV2*() not being provable after the difference in the traces. Otherwise, we could not instantiate *INV2*() after doing the single step in Lemma 69 (S AM: Strong Soundness Single Step).

We again, showed here an instantiated version of a more general version of the relation for easier explanation. The more general version can be found in Definition 44 (Relation between AM and Spec for oracles that only mispredict).

Lemma 66 (S: 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) $(p, \sigma) \rightsquigarrow_{\mathsf{S}}^{\omega} \overline{\tau}$ and $(p, \sigma') \rightsquigarrow_{\mathsf{S}}^{\omega} \overline{\tau}'$ and
(2) $\overline{\tau} \neq \overline{\tau}'$

Then there exists an oracle O such that

I $(p, \sigma) \rightsquigarrow_{\mathsf{S}}^{O} \overline{\tau}_1$ and $(p, \sigma') \rightsquigarrow_{\mathsf{S}}^{O} \overline{\tau}_1'$ 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) $(p, \sigma) \rightsquigarrow_{\mathsf{S}}^{\omega} \overline{\tau}$ and $(p, \sigma') \rightsquigarrow_{\mathsf{S}}^{\omega} \overline{\tau}'$ and
(2) $\overline{\tau} \neq \overline{\tau}'$

By definition of $() \rightsquigarrow_{\mathsf{S}}^{\omega}$ we have two final states $\Sigma_{\mathsf{S}F}$ and $\Sigma'_{\mathsf{S}F}$ such that $\Sigma_{\mathsf{S}}^{init}(p, \sigma) \Downarrow_{\mathsf{S}}^{\overline{\tau}} \Sigma_{\mathsf{S}F}$ $\Sigma_{\mathsf{S}}^{init}(p, \sigma') \Downarrow_{\mathsf{S}}^{\overline{\tau}'} \Sigma'_{\mathsf{S}F}$. Combined with the fact that $\overline{\tau} \neq \overline{\tau}'$, it follows that there are speculative states $\Sigma_{\mathsf{S}1}, \Sigma_{\mathsf{S}}, \Sigma'_{\mathsf{S}1}, \Sigma'_{\mathsf{S}2}$ and sequences of observations $\overline{\tau}, \overline{\tau}_{end}, \overline{\tau}'_{end}, \tau_{am}, \tau'_{am}$ such that $\tau_{am} \neq \tau'_{am}$, $\Sigma_{\mathsf{S}1} \cong \Sigma'_{\mathsf{S}1}$ and:

$$\Sigma_{\mathsf{S}}^{init}(p, \sigma) \Downarrow_{\mathsf{S}}^{\overline{\tau}} \Sigma_{\mathsf{S}1} \xrightarrow{\tau_{am}}_{\mathsf{S}} \Sigma_{\mathsf{S}2} \Downarrow_{\mathsf{S}}^{\overline{\tau}_{end}} \Sigma_{\mathsf{S}F}$$

$$\Sigma_{\mathsf{S}}^{init}(p, \sigma') \Downarrow_{\mathsf{S}}^{\overline{\tau}} \Sigma'_{\mathsf{S}1} \xrightarrow{\tau'_{am}}_{\mathsf{S}} \Sigma'_{\mathsf{S}2} \Downarrow_{\mathsf{S}}^{\overline{\tau}'_{end}} \Sigma'_{\mathsf{S}F}$$

We claim that there is a prediction oracle O with speculative window at most ω such that

a $X_{\mathsf{S}}^{init}(p, \sigma) \overset{O}{\rightsquigarrow}{}_{v}^{\mathsf{S}} X_{\mathsf{S}1}$ and $X_{\mathsf{S}1}.\sigma = \Sigma_{\mathsf{S}1}.\sigma$ and $INV2(X_{\mathsf{S}1}, \Sigma_{\mathsf{S}1})$ and
b $X_{\mathsf{S}}^{init}(p, \sigma') \overset{O}{\rightsquigarrow}{}_{v}^{\mathsf{S}} X'_{\mathsf{S}1}$ and $X'_{\mathsf{S}1}.\sigma = \Sigma'_{\mathsf{S}1}.\sigma$ and $INV2(X'_{\mathsf{S}1}, \Sigma'_{\mathsf{S}1})$
c $X_{\mathsf{S}1} \cong X'_{\mathsf{S}1}$

We get this by applying Lemma 68 (S: Stronger Soundness for a specific oracle and for specific executions) on the Am execution up to the point of the difference $\Sigma_{\mathsf{S}}^{init}(p, \sigma) \Downarrow_{\mathsf{S}}^{\overline{\tau}} \Sigma_{\mathsf{S}1}$ with the $O_{am}{}^{\mathsf{S}}$ and Σ_1^{States} being all the states in $\Sigma_{\mathsf{S}}^{init}(p, \sigma) \Downarrow_{\mathsf{S}}^{\overline{\tau}} \Sigma_{\mathsf{S}1}$ (similar for Σ_2^{States} for $\Sigma_{\mathsf{S}}^{init}(p, \sigma') \Downarrow_{\mathsf{S}}^{\overline{\tau}} \Sigma'_{\mathsf{S}1}$).

We now show that $\Sigma_{\mathsf{S}1} \approx_{O_{am}{}^{\mathsf{S}}}^{\Sigma_1^{States}} X_{\mathsf{S}1}$ is derived by Rule Single-Base-Oracle (similar for $\Sigma_{\mathsf{S}2} \approx_{O_{am}{}^{\mathsf{S}}}^{\Sigma_2^{States}} X_{\mathsf{S}2}$).

We do a case distinction if there are ongoing transactions in $X_{\mathsf{S}1}$ or not

no ongoing transactions in X_{S1} Then $\Sigma_{S1} \approx^{\Sigma_1^{States}}_{O_{am}{}^{S}} X_{S1}$ can only be derived Rule Single-Base-Oracle and Σ_{S1} has no ongoing transactions as well. Then we have by $INV2(\Sigma_{S1}, X_{S1})$ and $\Sigma_{S1}.n = \bot$ that $X_{S1}.n = \bot$.

ongoing transactions in X_S By the definition of the oracle O, we know that 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 $X_{S1}.n \geq minWndw(X_{S1})$ by definition of the oracle $O_{am}{}^{S}$ and $minWndw()$.

Since the next rule cannot be Rule S:AM-Rollback, we know that $\Sigma_{S1}.n > 0$ and by $INV2(\Sigma_{S1}, X_{S1})$ we get $minWndw(X_{S1}) > 0$ (Similar for X'_{S1} because of $\Sigma_{S1} \cong \Sigma'_{S1}$).

If $\Sigma_{S1} \approx^{\Sigma_1^{States}}_{O_{am}{}^{S}} X_{S1}$ by rollback rule, we would have a contradiction because we would need the topmost speculation window of $X_{S1}.n = 0$. But we know that $minWndw(X_{S1}) > 0$, because the speculation window of the topmost instance was created with a speculation window of ω.

Thus, we know that $X_{S1} \approx^{\Sigma_1^{States}}_{O_{am}{}^{S}} \Sigma_{S1}$ by Rule Single-Base-Oracle.

We now proceed by case analysis on the rule in $\Downarrow_S$ used to derive $\Sigma_{S1} \overset{\tau_{am}}{\Downarrow}_S \Sigma_{S2}$. Because $\Sigma_{S1} \cong \Sigma'_{S1}$ and $\overline{\tau}_1 = \overline{\tau}'_1$, we know that the same rule was used in $\Sigma'_{S1} \overset{\tau'_{am}}{\Downarrow}_S \Sigma'_{S2}$ 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 $\Sigma_{S1} \overset{\tau_{am}}{\Downarrow}_S \Sigma_{S2}$ we have $\Sigma_{S1} = \overline{\Phi}_S \cdot \Phi_S$ and $\Sigma_{S2} = \overline{\Phi}_S \cdot \overline{\Phi}'_S$ with $\Phi_S \overset{\tau_{am}}{\Downarrow}_S \overline{\Phi}'_S$.

We now do inversion on $\Sigma_{S1} \overset{\tau_{am}}{\Downarrow}_S \Sigma_{S2}$ and $\Phi_S \overset{\tau_{am}}{\Downarrow}_S \overline{\Phi}'_S$:

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, Rule S:AM-Store-Spec We fulfill all assumptions for Lemma 67 (S: AM and Oracle coincide) and get $X_{S1} \overset{\tau_{am}}{\rightsquigarrow}{}^{O}_{S} X_{S2}$ and $X'_{S1} \overset{\tau'_{am}}{\rightsquigarrow}{}^{O}_{S} X'_{S2}$.

Since $\tau_{am} \neq \tau'_{am}$ by assumption we are finished.

This completes the proof of our claim.

$\square$

Lemma 67 (S: AM and Oracle coincide)**.** *If*

(1) $\Sigma_S \approx^{\Sigma_{X_S}^{States}}_{O_{am}{}^{S}}$ *by Base and*

(2) $\Sigma_S \overset{\tau}{\Downarrow}_S \Sigma'_S$ *and*

(3) $minWndw(\Sigma_S) > 0$

(4) $X_S.\overline{\rho} = \emptyset$

Then

(1) $X_S \overset{\tau}{\rightsquigarrow}{}^{O}_{S} X'_S$

Proof. Since $minWndw(\Sigma_S) > 0$ we know that the next step is not a rollback. From $minWndw(\Sigma_S) > 0$ and $\Sigma_S \approx^{\Sigma^{States}}_{O_{am}} X_S$ we have $INV2(\Sigma_S, X_S)$ and we get $minWndw(X_S) > 0$ as well.

We proceed by inversion on $\Sigma_S \xrightarrow{\tau}_S \Sigma'_S$:

Rule S:AM-NoBranch From the rule, we have that $\Sigma_S.\sigma \xrightarrow{\tau} \Sigma'_S.\sigma$.

From $X_S.\sigma = \Sigma_S.\sigma$, we have that Rule S:NoBranch was used to derive $X_S \overset{O}{\underset{\tau'}{\rightsquigarrow}}_S X'_S$. From Rule S:NoBranch we have that τ' comes from $X_S.\sigma \xrightarrow{\tau} X_S.\sigma$.

Combined with $X_S.\sigma = \Sigma_S.\sigma$, and the determinism of the non-speculative semantics we have $\tau = \tau'$.

Rule S:AM-barr-spec, Rule S:AM-barr From the rule, we have that $\Sigma_S.\sigma \rightarrow \Sigma'_S.\sigma$.

The case is analogous to the case above.

Rule S:AM-Store-Spec Then, τ is generated by the step $\Sigma_S.\sigma \xrightarrow{\tau} \Sigma'_S.\sigma$ generated by Rule S:AM-Store-Spec.

From the fact that $X_S.\sigma = \Sigma_S.\sigma$, $INV2(X_S, \Sigma_S)$, and from the way we construct the oracle (see above), we have that $O(p, X_S.\sigma(pc), X_S.h) = (false, \omega)$ and it follows that Rule S:Store-Skip applies to X_S.

From Rule S:Store-Skip, we have $X_S \overset{O}{\underset{\tau'}{\rightsquigarrow}}_S X'_S$ and we know that $X_S.\sigma \xrightarrow{\tau'} X'_S.\sigma/$

Because the non-speculative semantics $\rightarrow$ is deterministic, we have $\tau = \tau'$

□

Lemma 68 (S: 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 33 (Constructing the Oracle) for the given execution. If*

(1) $\Sigma_{S1} \cong \Sigma_{S2}$
(2) $X_{S1} \cong X_{S2}$ *and* $\overline{p} = \emptyset$
(3) $\Sigma_{S1} \approx^{\Sigma_1^{States}}_{O_{am}{}^{S}} X_{S1}$ *and* $\Sigma_{S2} \approx^{\Sigma_2^{States}}_{O_{am}{}^{S}} X_{S2}$
(4) $\Sigma_{S1} \Downarrow^{\overline{\tau}}_S \Sigma'_{S1}$ *and* $\Sigma_{S2} \Downarrow^{\overline{\tau}}_S \Sigma'_{S2}$
(5) $\Sigma_1^{States} = \Sigma_{S1} \Downarrow^{\overline{\tau}}_S \Sigma'_{S1}$ *and* $\Sigma_2^{States} = \Sigma_{S2} \Downarrow^{\overline{\tau}}_S \Sigma'_{S2}$

and our oracle is constructed in the way described above Then

I $X_{S1} \overset{O}{\rightsquigarrow}{}^{S}_{\overline{\tau}'} X'_{S1}, X_{S2} \overset{O}{\rightsquigarrow}{}^{S}_{\overline{\tau}''} X'_{S2}$
II $\Sigma'_{S1} \cong \Sigma'_{S2}$
III $X'_{S1} \cong X'_{S2}$ *and* $\overline{p} = \emptyset$
IV $\Sigma'_{S1} \approx^{\Sigma_1^{States}}_{O_{am}{}^{S}} X'_{S1}$ *and* $\Sigma'_{S2} \approx^{\Sigma_2^{States}}_{O_{am}{}^{S}} X'_{S2}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. Notice that the proof is very similar to Lemma 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states). The only different thing 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 $\Sigma_{S1} \Downarrow^{\overline{\tau}}_S \Sigma'_{S1}$ and $\Sigma_{S2} \Downarrow^{\overline{\tau}}_S \Sigma'_{S2}$.

Rule S:AM-Reflection We have $\Sigma_{S1} \Downarrow^{\varepsilon}_S \Sigma'_S$ and $\Sigma_{S2} \Downarrow^{\varepsilon}_S \Sigma''_S$, 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 $X_{\mathsf{S}1} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\varepsilon} X'_{\mathsf{S}1}, X_{\mathsf{S}2} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\varepsilon} X'_{\mathsf{S}2}$ with $X'_{\mathsf{S}1} = X_{\mathsf{S}1}$ and $X'_{\mathsf{S}2} = X_{\mathsf{S}2}$. We now trivially satisfy all conclusions.

Rule S:AM-Single We have $\Sigma_{\mathsf{S}1} \Downarrow^{\overline{\tau}''}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ with $\Sigma'_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Sigma'_{\mathsf{S}1}$ and $\Sigma_{\mathsf{S}2} \Downarrow^{\overline{\tau}''}_{\mathsf{S}} \Sigma''_{\mathsf{S}}$ and $\Sigma''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Sigma'_{\mathsf{S}2}$.

We now apply IH on $\Sigma_{\mathsf{S}1} \Downarrow^{\overline{\tau}''}_{\mathsf{S}} \Sigma'_{\mathsf{S}}$ and $\Sigma_{\mathsf{S}2} \Downarrow^{\overline{\tau}''}_{\mathsf{S}} \Sigma''_{\mathsf{S}}$ and get

(a) $X_{\mathsf{S}1} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}'} X'_{\mathsf{S}}, X_{\mathsf{S}2} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\overline{\tau}''} X''_{\mathsf{S}}$
(b) $\Sigma'_{\mathsf{S}} \cong \Sigma''_{\mathsf{S}}$
(c) $X'_{\mathsf{S}} \cong X''_{\mathsf{S}}$ and $\overline{\rho}' = \varnothing$
(d) $\Sigma'_{\mathsf{S}} \approx^{\Sigma_1^{States}}_{O_{am}{}^{\mathsf{S}}} X'_{\mathsf{S}}$ and $\Sigma''_{\mathsf{S}} \approx^{\Sigma_2^{States}}_{O_{am}{}^{\mathsf{S}}} X''_{\mathsf{S}}$
(e) $\overline{\tau}' = \overline{\tau}''$

We do a case distinction on $\approx^{\Sigma^{States}}_{O_{am}{}^{\mathsf{S}}}$ in $\Sigma'_{\mathsf{S}} \approx^{\Sigma_1^{States}}_{O_{am}{}^{\mathsf{S}}} X'_{\mathsf{S}}$ and $\Sigma''_{\mathsf{S}} \approx^{\Sigma_2^{States}}_{O_{am}{}^{\mathsf{S}}} X''_{\mathsf{S}}$ by inversion:

Rule Single-Base-Oracle We thus have $\Sigma'_{\mathsf{S}} \sim X'_{\mathsf{S}}\restriction_{com}$, $minWndw(X'_{\mathsf{S}}) > 0$ and $INV2(\Sigma'_{\mathsf{S}}, X'_{\mathsf{S}})$ (Similar for Σ''_{S} and X''_{S}).

We now proceed by inversion on the derivation $\Sigma'_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Sigma'_{\mathsf{S}1}$ and $\Sigma''_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Sigma'_{\mathsf{S}2}$.

Rule S:AM-Rollback Contradiction, because of $minWndw(X'_{\mathsf{S}}) > 0$ and $INV2(\Sigma'_{\mathsf{S}}, X'_{\mathsf{S}})$.

Rule S:AM-General $INV2()$ trivially holds, because it does not change the speculation window of the states.

Rule S:AM-Context: We have $\Phi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \overline{\Phi}_{\mathsf{S}}$ and $\Phi'_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \overline{\Phi}'_{\mathsf{S}}$. We fulfill all conditions for Lemma 69 (S AM: Strong Soundness Single Step) which gives us the desired result. Especially, that the resulting state is in Σ_1^{States}, which follows by definition of Σ^{States}

Rule Single-Transaction-Rollback-Oracle We have

$$
\begin{aligned}
X'_{\mathsf{S}} =& X_{\mathsf{S}3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma'', h', 0 \rangle^{false} \cdot X_{\mathsf{S}4} \\
\Sigma'_{\mathsf{S}} =& \Sigma_{\mathsf{S}3} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle^{false} \cdot \Sigma_{\mathsf{S}4} \\
X_{\mathsf{S}} =& X_{\mathsf{S}3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \\
\Sigma_{\mathsf{S}} =& \Sigma_{\mathsf{S}3} \cdot \langle p, ctr, \sigma, n \rangle \\
\Sigma_{\mathsf{S}} \sim& X_{\mathsf{S}}\restriction_{com} \\
& INV2(\Sigma_{\mathsf{S}}, X_{\mathsf{S}}) \\
n' \geq& 0
\end{aligned}
$$

The form of X''_{S} and Σ''_{S} is analogous.

Additionally, we know that the transaction terminates in some state $\Sigma_{\mathsf{S}} \Downarrow^{\overline{\tau}}_{\mathsf{S}} \Sigma'''_{\mathsf{S}}$. There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma'_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Sigma'_{\mathsf{S}1}$ is not a roll back. Because Σ_{S} and X_{S} do not change, $INV2(\Sigma_{\mathsf{S}}, X_{\mathsf{S}})$ does not change as well.

The states are still related by Rule Single-Transaction-Rollback after the step.

$n' = 0$ Then we know that $\Sigma'_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Sigma'_{\mathsf{S}1}$ 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 $INV2(\Sigma_{\mathsf{S}}, X_{\mathsf{S}})$ (with updated ctr) still holds.

$\square$

Lemma 69 (S AM: 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, $\Sigma_{\mathsf{S}1} = \Sigma'_{\mathsf{S}} \cdot \Phi'_{\mathsf{S}}$, $\Sigma_{\mathsf{S}2} = \Sigma''_{\mathsf{S}} \cdot \Phi''_{\mathsf{S}}$ be two speculative states for the always mispredict semantics and $X_{\mathsf{S}1}, X_{\mathsf{S}2}$, be two speculative states for the speculative semantics.*

If the following conditions hold:

(1) $\Sigma_{\mathsf{S}1} \cong \Sigma_{\mathsf{S}2}$
(2) $X_{\mathsf{S}1} \cong X_{\mathsf{S}2}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma_{\mathsf{S}1} \approx^{\Sigma_1^{States}}_{O_{am}\,\mathsf{S}} X_{\mathsf{S}1}$ *and* $\Sigma_{\mathsf{S}2} \approx^{\Sigma_2^{States}}_{O_{am}\,\mathsf{S}} X_{\mathsf{S}2}$
(4) $\Phi'_{\mathsf{S}} \overset{\tau''}{=\!\!=\!\!\Omega}_{\mathsf{S}} \Sigma'_{\mathsf{S}1}$ *and* $\Phi''_{\mathsf{S}} \overset{\tau''}{=\!\!=\!\!\Omega}_{\mathsf{S}} \Sigma'_{\mathsf{S}2}$ *and*
(5) $\Sigma'_{\mathsf{S}1} \in \Sigma_1^{States}$ *and* $\Sigma'_{\mathsf{S}1} \in \Sigma_2^{States}$

then there are instances $X'_{\mathsf{S}1}, X'_{\mathsf{S}2}$ for the speculative semantics such that:

I $X_{\mathsf{S}1} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\tau} X'_{\mathsf{S}1}$ *and* $X_{\mathsf{S}2} \overset{O}{\rightsquigarrow}{}^{\mathsf{S}}_{\tau'} X'_{\mathsf{S}2}$
II $\Sigma'_{\mathsf{S}1} \cong \Sigma'_{\mathsf{S}2}$
III $X'_{\mathsf{S}1} \cong X'_{\mathsf{S}2}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{\mathsf{S}1} \approx^{\Sigma_1^{States}}_{O_{am}\,\mathsf{S}} X'_{\mathsf{S}1}$ *and* $\Sigma'_{\mathsf{S}2} \approx^{\Sigma_2^{States}}_{O_{am}\,\mathsf{S}} X'_{\mathsf{S}2}$
V $\tau = \tau'$

Proof. The proof is very similar to Lemma 65 (S: Soundness Single Step AM). The only different thing 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*$(\Sigma_{\mathsf{S}}, X_{\mathsf{S}})$

For these reasons, we will only argue why *INV2*$(\Sigma'_{\mathsf{S}1}, X'_{\mathsf{S}1})$ 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*$(\Sigma'_{\mathsf{S}1}, X'_{\mathsf{S}1})$ still holds. The proof for *INV2*$(\Sigma'_{\mathsf{S}2}, X'_{\mathsf{S}2})$ is analogous.

Note that $|X_{\mathsf{S}}\upharpoonright_{com}| = |X_{\mathsf{S}}|$ for all states X_{S}, because our oracle only mispredicts. We need to show that $|\Sigma'_{\mathsf{S}1}| = |X'_{\mathsf{S}1}|$ and $minWndw(X'_{\mathsf{S}1}) = \Sigma'_{\mathsf{S}1}.n$.

$|\Sigma'_{\mathsf{S}1}| = |X'_{\mathsf{S}1}|$ Since the rules that apply here do not create or remove a speculative instance we have

$$|\Sigma'_{\mathsf{S}1}| = |X'_{\mathsf{S}1}|$$
$$|\Sigma'_{\mathsf{S}}| = |X'_{\mathsf{S}}|$$

which we know by the assumption *INV2*$(\Sigma'_{\mathsf{S}}, X'_{\mathsf{S}})$.

$minWndw(X'_{\mathsf{S}}) = \Sigma'_{\mathsf{S}1}.n$ Since the executed instruction was not a store instruction instruction, we have two cases

barrier instruction Then $minWndw(X'_{\mathsf{S}1}) = minWndw(zeroes(X'_{\mathsf{S}})) = 0$ and $\Sigma'_{\mathsf{S}1}.n = 0$ and we satisfy *INV2*$(\Sigma'_{\mathsf{S}1}, X'_{\mathsf{S}1})$.

not barrier Then $minWndw(X'_{\mathsf{S}1}) = minWndw(decr(X'_{\mathsf{S}}))$ and $\Sigma'_{\mathsf{S}1}.n = \Sigma'_{\mathsf{S}}.n - 1$.

By definition of *INV2*$(\Sigma'_{\mathsf{S}}, X'_{\mathsf{S}})$ we have $minWndw(X'_{\mathsf{S}}) = \Sigma'_{\mathsf{S}}.n$ and by $\approx^{\Sigma^{States}}_{O_{am}\,\mathsf{S}}$ 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 $minWndw(decr(X'_S)) = minWndw(X'_S) - 1$.

$$\begin{aligned} minWndw(X'_S) &= \Sigma'_S.n \\ minWndw(X'_S) - 1 &= \Sigma'_S.n - 1 \\ minWndw(decr(X'_S)) &= \Sigma'_{S1}.n \\ minWndw(X'_{S1}) &= \Sigma'_{S1}.n \end{aligned}$$

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.

$$\begin{aligned} X'_{S1} &= X'''_S \cdot \Psi_S \\ minWndw(X'''_S) &= minWndw(decr(X'_S)) = minWndw(X'_S) - 1 \\ X'_S.\sigma &\xrightarrow{\tau} X'''_S.\sigma \\ \Sigma'_{S1} &= \Sigma'''_S \cdot \Phi_S \\ \Sigma'''_S.n &= \Sigma'_S.n - 1 \\ \Sigma'_S.\sigma &\xrightarrow{\tau} \Sigma'''_S.\sigma \end{aligned}$$

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 $minWndw(X'_{S1}) = \omega$ and $\Sigma'_{S1}.n = \omega$ 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 $minWndw(X'_{S1}) < \omega$ (because $\Psi_S.n = \omega$).

Now we have $minWndw(X'_{S1}) = minWndw(X'''_S \cdot \Psi_S) = minWndw(X'''_S)$ and $\Sigma'_{S1}.n = \Sigma'_S.n - 1 = \Sigma'''_S.n$.

Thus, by $INV2(\Sigma'''_S, X'''_S)$ we have $INV2(\Sigma'_{S1}, X'_{S1})$

We can relate by Rule Single-Base-Oracle.

□

L SEMANTICS FOR $\mathcal{G}_{\mathsf{R}}$

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

$$\textit{Speculative State } \Sigma_{\mathsf{R}} ::= \Phi_{\mathsf{R}}$$

$$\textit{Speculative Instance } \Phi_{\mathsf{R}} ::= \langle p, ctr, \sigma, \mathbb{R}, n \rangle_{\overline{\rho}}$$

$$\tau ::= \texttt{start}_{\mathsf{R}}\ ctr \mid \texttt{rlb}_{\mathsf{R}}\ ctr$$

L.1 $\mathcal{G}_{\mathsf{R}}$: Always Mispredict Semantics

$\boxed{\textit{Judgements}}$

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

$\boxed{\Sigma_{\mathsf{R}} \overset{\tau}{\Rrightarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}}}$

(R:AM-Context)
$$\frac{\Phi_{\mathsf{R}} \overset{\tau}{\Rrightarrow}_{\mathsf{R}} \overline{\Phi}'_{\mathsf{R}}}{\overline{\Phi}_{\mathsf{R}} \cdot \Phi_{\mathsf{R}} \overset{\tau}{\Rrightarrow}_{\mathsf{R}} \overline{\Phi}_{\mathsf{R}} \cdot \overline{\Phi}'_{\mathsf{R}}}$$

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

$\boxed{\Phi_{\mathsf{R}} \overset{\tau}{\Rrightarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}}}$

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

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

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

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

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

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

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

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

$$\frac{\tau = \texttt{ret}\ n \mid \texttt{start}_{\mathsf{R}}\ n}{\Phi_{\mathsf{R}\overline{p}\cdot\tau} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \Phi_{\mathsf{R}\overline{p}}}\ (\mathsf{R}\text{:AM-General})$$

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

$$\frac{}{\Sigma_{\mathsf{R}} \Downarrow^{\varepsilon}_{\mathsf{R}} \Sigma_{\mathsf{R}}}\ (\mathsf{R}\text{:AM-Reflection}) \qquad \frac{\Sigma_{\mathsf{R}} \Downarrow^{\overline{\tau}}_{\mathsf{R}} \Sigma''_{\mathsf{R}} \qquad \Sigma''_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}}}{\Sigma_{\mathsf{R}} \Downarrow^{\overline{\tau}\cdot\tau}_{\mathsf{R}} \Sigma'_{\mathsf{R}}}\ (\mathsf{R}\text{:AM-Single})$$

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

$$\boxed{Helpers}$$

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

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

$$\boxed{(p \times InitConf) \rightsquigarrow^{\omega}_{\mathsf{R}} \overline{\tau}}$$

$$\frac{\exists \Sigma'_{\mathsf{R}} \qquad \vdash \Sigma'_{\mathsf{R}} : fin \qquad \Sigma^{init}_{\mathsf{R}}(()p, \sigma) \Downarrow^{\overline{\tau}}_{\mathsf{R}} \Sigma'_{\mathsf{R}}}{(p, \sigma) \rightsquigarrow^{\omega}_{\mathsf{R}} \overline{\tau}}\ (\mathsf{R}\text{:AM-Trace}) \qquad \frac{}{Beh^{\omega}_{\mathsf{R}}(p) = \{\overline{\tau} \mid \forall \sigma \in InitConf.\ (p, \sigma) \rightsquigarrow^{\omega}_{\mathsf{R}} \overline{\tau}\}}\ (\mathsf{R}\text{:AM-Beh})$$

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

L.2 $\rightsquigarrow_{\mathsf{R}}$: Oracle Semantics

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 the jump location l because we need them for SE-Commit and SE-Rollback to check if the jump location with correct (rule R:SE-Commit) or not (rule R:SE-Rollback).

$$Speculative\ State\ X_{\mathsf{R}} ::= \Psi_{\mathsf{R}}$$

$$Speculative\ Instance\ \Psi_{\mathsf{R}} ::= \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle^{l}_{p}\ l \in \mathbb{N} \text{ or } l = \varepsilon$$

$$\tau ::= .. \mid \texttt{commit}_{\mathsf{R}}\ ctr$$

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

$\boxed{\textit{Judgements}}$

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

$\boxed{X_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} X'_{\mathsf{R}}}$

(R:SE-Context)

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

(R:SE-Rollback)

$$\frac{n' = 0 \qquad \text{or p is stuck}}{\overline{\Psi}_{\mathsf{R}} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}, h', n'\rangle^{\mathit{false}} \cdot \overline{\Psi}_{\mathsf{R}}' \xrightarrow[\mathsf{R}]{\mathtt{rlb}_{\mathsf{R}}\ ctr \quad O} \overline{\Psi}_{\mathsf{R}} \cdot \langle p, ctr', \sigma, \mathbb{R}, h, n\rangle}$$

(R:SE-Commit)

$$\frac{}{\overline{\Psi}_{\mathsf{R}} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle^{l} \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0\rangle^{\mathit{true}} \cdot \overline{\Phi}_{\mathsf{R}}' \xrightarrow[\mathsf{R}]{\mathtt{commit}_{\mathsf{R}}\ ctr \quad O} \overline{\Psi}_{\mathsf{R}} \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n\rangle^{l} \cdot \overline{\Psi}_{\mathsf{R}}'}$$

(R:SE-General)

$$\frac{\tau = \mathtt{ret}\ n \mid \mathtt{start}_{\mathsf{R}}\ n}{\overline{\Psi}_{\mathsf{R}} \cdot \Psi_{\mathsf{R}\,\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} \overline{\Psi}_{\mathsf{R}} \cdot \Psi_{\mathsf{R}\,\overline{\rho}}}$$

$\boxed{\Psi_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} \Psi'_{\mathsf{R}}}$

(R:SE-barr)

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

(R:SE-barr-spec)

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

(R:SE-NoBranch)

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

(R:SE-Ret)

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

(R:SE-Ret-Empty)

$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{ret} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, \emptyset, h, n+1\rangle \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} \langle p, ctr, \sigma', \emptyset, h, n\rangle}$$

(R:SE-Call-Full)

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

(R:SE-Call)

$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{call}\ f \qquad \sigma \xrightarrow{\tau} \sigma' \\ \mathbb{R}' = \mathbb{R} \cdot (a(\mathbf{pc}) + 1) \qquad |\mathbb{R}| < RSB_{size}}{\langle p, ctr, \sigma, \mathbb{R}, n+1\rangle \overset{\tau}{\Rightarrow}_{\mathsf{R}} \langle p, ctr, \sigma', \mathbb{R}', n\rangle}$$

$$\boxed{\Sigma_{\mathsf{R}} \overset{O}{\rightsquigarrow}{}^{\mathsf{R}}_{\overline{\tau}} \Sigma'_{\mathsf{R}}}$$

(R:SE-Reflection)
$$\frac{}{\Sigma_{\mathsf{R}} \overset{O}{\rightsquigarrow}{}^{\mathsf{R}}_{\varepsilon} \Sigma_{\mathsf{R}}}$$

(R:SE-Single)
$$\frac{\Sigma_{\mathsf{R}} \Downarrow^{\overline{\tau}}_{\mathsf{R}} \Sigma''_{\mathsf{R}} \qquad \Sigma''_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} \Sigma'_{\mathsf{R}}}{\Sigma_{\mathsf{R}} \overset{O}{\rightsquigarrow}{}^{\mathsf{R}}_{\overline{\tau}\cdot\tau} \Sigma'_{\mathsf{R}}}$$

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

$$\boxed{Helpers}$$

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

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

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

$$\boxed{(p \times InitConf) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}}$$

(R:SE-Trace)
$$\frac{\exists X'_{\mathsf{R}} \qquad \vdash X'_{\mathsf{R}} : fin \qquad X^{init}_{\mathsf{R}}(p,\sigma) \overset{O}{\rightsquigarrow}{}^{\mathsf{R}}_{\overline{\tau}} \Psi'_{\mathsf{R}}}{(p,\sigma) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}}$$

(R:SE-Beh-V4)
$$\frac{}{Beh^{O}_{\mathsf{R}}(p) = \{\overline{\tau} \mid \forall \sigma \in InitConf.\ ((p,\sigma)) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}\}}$$

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

L.3 $\Downarrow_{\mathsf{R}}$: Symbolic semantics

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

$$\boxed{\Sigma^{S}_{\mathsf{R}} \overset{\tau_S}{\Longrightarrow}{}^{S}_{\mathsf{R}} \Sigma^{S}{}'_{\mathsf{R}}}$$

(R:Sym-Context)
$$\frac{\Phi^{S}_{\mathsf{R}} \overset{\tau}{\Longrightarrow}{}^{S}_{\mathsf{R}} \overline{\Phi^{S}}'_{\mathsf{R}}}{\overline{\Phi^{S}}_{\mathsf{R}} \cdot \Phi^{S}_{\mathsf{R}} \overset{\tau_S}{\Longrightarrow}{}^{S}_{\mathsf{R}} \overline{\Phi^{S}}_{\mathsf{R}} \cdot \overline{\Phi^{S}}'_{\mathsf{R}}}$$

(R:Sym-Rollback)
$$\frac{n' = 0 \text{ or p is stuck}}{\overline{\Phi^{S}}_{\mathsf{R}} \cdot \langle p, ctr, \sigma_S, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma'_S, \mathbb{R}, n'\rangle^{l} \overset{\mathtt{rlb}_{\mathsf{R}}\ ctr}{\Longrightarrow}{}^{S}_{\mathsf{R}} \overline{\Phi^{S}}_{\mathsf{R}} \cdot \langle p, ctr', \sigma_S, \mathbb{R}, n\rangle}$$

$$\boxed{\Phi^{S}_{\mathsf{R}} \overset{\tau}{\Longrightarrow}{}^{S}_{\mathsf{R}} \Sigma^{S}{}'_{\mathsf{R}}}$$

(R:Sym:AM-barr)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma_S \xrightarrow{\tau_S}_S \sigma'_S}{\langle p, ctr, \sigma_S, \mathbb{R}, \bot\rangle \overset{\tau_S}{\Longrightarrow}{}^{S}_{\mathsf{R}} \langle p, ctr, \sigma'_S, \mathbb{R}, \bot\rangle}$$

(R:Sym-barr-spec)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma_S \xrightarrow{\tau_S}_S \sigma'_S}{\langle p, ctr, \sigma_S, \mathbb{R}, n+1\rangle \overset{\tau_S}{\Longrightarrow}{}^{S}_{\mathsf{R}} \langle p, ctr, \sigma'_S, \mathbb{R}, n\rangle}$$

(R:Sym-NoBranch)

$$\frac{p(\sigma(\mathbf{pc})) \neq \mathbf{ret}, \mathbf{spbarr}, \mathbf{call}\ f, Z \qquad \sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}}{\langle p, ctr, \sigma_{\mathcal{S}}, \mathbb{R}, n+1\rangle \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathsf{R}} \langle p, ctr, \sigma'_{\mathcal{S}}, \mathbb{R}, n\rangle}$$

(R:Sym-Ret-Spec)

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

(R:Sym-Ret-Same)

$$\frac{\begin{array}{c} p(\sigma(\mathbf{pc})) = \mathbf{ret} \quad \sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}} \quad \mathbb{R} = \mathbb{R}'; l \\ l = \mathbf{read}(sm, sa(\mathbf{sp}))) \end{array}}{\langle p, ctr, \sigma, \mathbb{R}, n+1\rangle \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathsf{R}} \langle p, ctr, \sigma', \mathbb{R}, n\rangle}$$

(R:Sym-Ret-Empty)

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

(R:Sym-Call-Full)

$$\frac{\begin{array}{c} p(\sigma(\mathbf{pc})) = \mathbf{call}\ f \quad \sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}} \\ |\mathbb{R}| \geq RSB_{size} \end{array}}{\langle p, ctr, \sigma_{\mathcal{S}}, \mathbb{R}, n+1\rangle \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathsf{R}} \langle p, ctr, \sigma'_{\mathcal{S}}, \mathbb{R}, n\rangle}$$

(R:Sym-Call)

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

(R:Sym-General)

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

$\boxed{\Sigma^{\mathcal{S}}_{\mathsf{R}}\ {}_{\mathcal{S}}\!\Downarrow^{\overline{\tau}}_{\mathsf{R}}\ \Sigma^{\mathcal{S}\prime}_{\mathsf{R}}}$

(R:Sym-Reflection)

$$\frac{}{\Sigma^{\mathcal{S}}_{\mathsf{R}}\ {}_{\mathcal{S}}\!\Downarrow^{\varepsilon}_{\mathsf{R}}\ \Sigma^{\mathcal{S}}_{\mathsf{R}}}$$

(R:Sym-Single)

$$\frac{\Sigma^{\mathcal{S}}_{\mathsf{R}}\ {}_{\mathcal{S}}\!\Downarrow^{\overline{\tau_{\mathcal{S}}}}_{\mathsf{R}}\ \Sigma^{\mathcal{S}\prime\prime}_{\mathsf{R}} \qquad \Sigma^{\mathcal{S}\prime\prime}_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathsf{R}} \Sigma^{\mathcal{S}\prime}_{\mathsf{R}}}{\Sigma^{\mathcal{S}}_{\mathsf{R}}\ {}_{\mathcal{S}}\!\Downarrow^{\overline{\tau_{\mathcal{S}}} \cdot \tau_{\mathcal{S}}}_{\mathsf{R}}\ \Sigma^{\mathcal{S}\prime}_{\mathsf{R}}}$$

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

$\boxed{Helpers}$

(R:Sym-Init)

$$\frac{\Sigma^{\mathcal{S}}_{\mathsf{R}} = \langle p, 0, \sigma_{\mathcal{S}}, \mathbb{R}, \bot\rangle \qquad \sigma_{\mathcal{S}} \in InitConf}{\vdash \Sigma^{\mathcal{S}}_{\mathsf{R}} : init}$$

(R:Sym-Fin)

$$\frac{\Sigma^{\mathcal{S}}_{\mathsf{R}} = \langle p, ctr, \sigma, \mathbb{R}, \bot\rangle \qquad \sigma_{\mathcal{S}}(\mathbf{pc}) = \bot}{\vdash \Sigma^{\mathcal{S}}_{\mathsf{R}} : fin}$$

(R:Sym-Initial-State)

$$\frac{}{\Sigma^{\mathcal{S}\,init}_{\mathsf{R}}(p, \sigma) := \langle p, 0, \sigma_{\mathcal{S}}, \varepsilon, \bot\rangle}$$

$\boxed{(p \times InitConf) \curvearrowright^{\omega}_{\mathsf{R}} \overline{\tau}}$

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

M PROOFS FOR $\Game_{R}$:

Our main result for $\Game_{R}$ is the following

Theorem 16 ($\Game_{R}$ is *WFSS*). $\vdash \Game_{R}$ *WFSS*

Proof. Immediately follows from Theorem 20 (R: Oracle Overapproximation), Theorem 19 ($\Game_{R}$: Behaviour of AM and symbolic semantics), Theorem 18 (R AM: Behaviour of non-speculative semantics and AM semantics) and Theorem 17 (R SE: Behaviour of non-speculative and oracle semantics). □

M.1 R: Relating Non-speculative and Oracle Semantics

- Theorem 17 (R SE: Behaviour of non-speculative and oracle semantics)
  - Lemma 75 (R SE: Completeness of the speculative semantics)
    - Lemma 76 (R SE: Non-speculative execution for rolled back transactions)
  - Lemma 70 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics)
    - Lemma 71 (R SE: Soundness single step No Speculation)
      - Lemma 72 (R SE: Single Step Instance Non Speculative)
    - Lemma 74 (R SE: Return step Speculation)

Theorem 17 (R SE: Behaviour of non-speculative and oracle semantics). *Let p be a program and O be a prediction oracle. Then $Beh_{NS}(p) = Beh^{O}_{R}(p)\restriction_{ns}$*

Proof. We prove the two directions separately:

$\Leftarrow$ By the definition of $Beh^{O}_{R}(p)$ we have an initial configuration σ such that $((p,\sigma)) \leadsto^{O}_{R} \overline{\tau}$.

By definition of $((p,\sigma)) \leadsto^{O}_{R} \overline{\tau}$, we know there exists a state X'_{R} such that $\vdash X'_{R} : fin$ and an initial state $\Sigma^{init}_{R}(p,\sigma)$ such that $\Sigma^{init}_{R}(p,\sigma) \ {}^{O}\!\!\Downarrow^{R}_{\overline{\tau}} X'_{R}$.

Analogous to the corresponding case in Theorem 12 (S SE: Behaviour of non-speculative and oracle semantics) by using Lemma 70 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

We thus have $((p,\sigma)) \leadsto_{NS} \overline{\tau}\restriction_{ns} \in Beh_{NS}(p)$ by Rule NS-Trace.

$\Rightarrow$ Assume that $((p,\sigma)) \leadsto_{NS} \overline{\tau} \in Beh_{NS}(p)$. We thus know there exists $\sigma' \in FinalConf$ such that $\sigma \Downarrow_{\overline{\tau}} \sigma'$.

Analogous to the corresponding case in Theorem 12 (S SE: Behaviour of non-speculative and oracle semantics) by using Lemma 75 (R SE: Completeness of the speculative semantics).
We thus have $((p,\sigma)) \Downarrow^{O}_{\mathrm{R}} \overline{\tau}' \cdot \overline{\tau}'' \in Beh^{O}_{\mathrm{R}}(p)$.

□

Lemma 70 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics)**.** *If*

(1) $X_{\mathrm{R}}.\sigma = \sigma$ *and*
(2) $\vdash_O X_{\mathrm{R}} :$ *noongoing and*
(3) $X_{\mathrm{R}} \; {}^{O}\!\!\rightsquigarrow^{\mathrm{R}}_{\overline{\tau}} X'_{\mathrm{R}}$

Then there exists σ' *such that*

I *if* $\vdash_O X'_{\mathrm{R}} :$ *noongoing then* $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}\sigma'}$ *and* $X'_{\mathrm{R}}.\sigma = \sigma'$ *and*
II *if* $\vdash^{i}_{O} X'_{\mathrm{R}} :$ *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 $X_{\mathrm{R}} \; {}^{O}\!\!\rightsquigarrow^{\mathrm{R}}_{\overline{\tau}} X'_{\mathrm{R}}$

Rule R:SE-Reflection Then we have $X_{\mathrm{R}} \; {}^{O}\!\!\rightsquigarrow^{\mathrm{R}}_{\varepsilon} X_{\mathrm{R}}$ with $X'_{\mathrm{R}} = X_{\mathrm{R}}$ and by Rule NS-Reflection we have

I $\sigma \Downarrow_{\varepsilon\upharpoonright_{ns}} \sigma'$ with $\sigma = \sigma'$.
II $\sigma \Downarrow_{helper(\varepsilon,i)} \sigma'$ with $\sigma = \sigma'$.

Rule R:SE-Single We have $X_{\mathrm{R}} \; {}^{O}\!\!\rightsquigarrow^{\mathrm{R}}_{\overline{\tau}'\cdot\tau} X'_{\mathrm{R}}$ and by Rule R:SE-Single we get $X_{\mathrm{R}} \; {}^{O}\!\!\rightsquigarrow^{\mathrm{R}}_{\overline{\tau}'} X''_{\mathrm{R}}$ and $X''_{\mathrm{R}} \xrightarrow{\tau}{}^{O}_{\mathrm{R}} X'_{\mathrm{R}}$.

We need to proof

I if $\vdash_O X'_{\mathrm{R}} :$ *noongoing* then $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ and $X'_{\mathrm{R}}.\sigma = \sigma'$
II if $\vdash^{i}_{O} X'_{\mathrm{R}} :$ *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 $X_{\mathrm{R}} \; {}^{O}\!\!\rightsquigarrow^{\mathrm{R}}_{\overline{\tau}'} X''_{\mathrm{R}}$ and have a σ'' where σ'' is the configuration for some instance in X''_{R} such that.

I' if $\vdash_O X''_{\mathrm{R}} :$ *noongoing* then $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}\sigma''}$ and $X''_{\mathrm{R}}.\sigma = \sigma''$
II' if $\vdash^{j}_{O} X''_{\mathrm{R}} :$ *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 $\vdash_O X''_{\mathrm{R}} :$ *noongoing* and we have $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}} \sigma''$ and $X''_{\mathrm{R}}.\sigma = \sigma''$ by IH.

I Then $\vdash_O X'_{\mathrm{R}} :$ *noongoing* and we need to prove $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ and $X'_{\mathrm{R}}.\sigma = \sigma'$. We now proceed by inversion on $X''_{\mathrm{R}} \xrightarrow{\tau}{}^{O}_{\mathrm{R}} X'_{\mathrm{R}}$:

Rule R:SE-Rollback Analogous to the corresponding case in Lemma 45 (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 $\overline{p} =$ `ret` $l \cdot$ `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 45 (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 $\sigma'' = X''_{\mathsf{R}}.\sigma$. Since $\vdash_O X''_{\mathsf{R}} : \mathit{noongoing}$, there no ongoing transactions that need to be rolled back.

Furthermore, no transaction that will be rolled back is created in the step $X''_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} X'_{\mathsf{R}}$, because $\vdash_O X'_{\mathsf{R}} : \mathit{noongoing}$.

The case is analogous to Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) by using Lemma 71 (R SE: Soundness single step No Speculation).

II Then X'_{R} has ongoing transactions, meaning $\vdash^i_O X'_{\mathsf{R}} : \mathit{biggestongoingtransactionirolledback}$ 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 $X''_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} X'_{\mathsf{R}}$:

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 $\overline{p} = \mathtt{ret}\ l \cdot \mathtt{start}\ id$ 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 $\vdash_O X''_{\mathsf{R}} : \mathit{noongoing}$, so there was not another ongoing transaction.

The case is analogous to Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) together with Lemma 74 (R SE: Return step Speculation).

otherwise By definition of $\vdash^i_O X'_{\mathsf{R}} : \mathit{biggestongoingtransactionirolledback}$ we know that there exists a $\mathtt{rlb}\ i$ in the execution $X'_{\mathsf{R}} \overset{O}{\Downarrow}{}^{\mathsf{R}}_{\overline{\tau}_{fin}} X_{\mathsf{R}fin}$ with no matching $\mathtt{start}\ i$ observation in that execution.

The contradiction can be derived in the same way as in the analogous case in Lemma 45 (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 $\vdash^j_O X''_{\mathsf{R}} : \mathit{biggestongoingtransactionirolledback}$ and we have $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$ and σ'' is the configuration for the instance with $ctr = j$.

I Then $\vdash_O X'_{\mathsf{R}} : \mathit{noongoing}$ and we need to prove $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ and $X'_{\mathsf{R}}.\sigma = \sigma'$. We now proceed by inversion on $X''_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} X'_{\mathsf{R}}$:

Rule R:SE-Rollback and $\tau = \mathtt{rlb}\ j$ Choose $\sigma' = \sigma''$. Since $\overline{\tau}\cdot\tau\upharpoonright_{ns} = helper(\overline{\tau}, j)$ we can use IH $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$.

Analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Then $\tau \neq \mathtt{rlb}\ j$.

Deriving the contradiction is analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

II Then $\vdash^i_O X'_{\mathsf{R}} : \mathit{biggestongoingtransactionirolledback}$ 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 $X''_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} X'_{\mathsf{R}}$:

Rule R:SE-Rollback Then $\tau = \mathtt{rlb}\ id$. We do a case analysis if $id = j$ or not.

$id = j$ Analogous to Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

$id \neq j$ Analogous to Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Analogous to Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

□

Lemma 71 (R SE: Soundness single step No Speculation). *If*

(1) $\vdash_O X_{\mathsf{R}}$: *noongoing and*
(2) $X_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} X'_{\mathsf{R}}$ *and*
(3) $\vdash_O X'_{\mathsf{R}}$: *noongoing and*
(4) $\sigma = X_{\mathsf{R}}.\sigma$

Then there exists σ' *such that*

I $\sigma \Downarrow_{\tau\restriction_{ns}} \sigma'$ *and*
II $X'_{\mathsf{R}}.\sigma = \sigma'$

Proof. We proceed by inversion on $X_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} X'_{\mathsf{R}}$:

Rule R:SE-General Thus we have $X_{\mathsf{R}} = \overline{\Psi}_{\mathsf{R}} \cdot \Psi_{\mathsf{R}\overline{\rho}\cdot\tau}$ and $X'_{\mathsf{R}} = \overline{\Psi}_{\mathsf{R}} \cdot \Psi_{\mathsf{R}\overline{\rho}}$ with $\Psi_{\mathsf{R}}.\sigma = \sigma$.
By the definition of $\Psi_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} X_{\mathsf{R}}$ 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 $X_{\mathsf{R}}.\sigma = X'_{\mathsf{R}}.\sigma$ and with this we get $X'_{\mathsf{R}}.\sigma = \sigma$.
Thus, we can derive $\sigma \Downarrow_{\texttt{commit}\ id\restriction_{ns}} \sigma$.

Rule R:SE-Rollback Contradiction, since $\vdash_O X_{\mathsf{R}}$: *noongoing* and Definition 18 (Well orderedness of rollback and start).

Rule R:SE-Context We have $X_{\mathsf{R}} = \overline{\Psi}_{\mathsf{R}} \cdot \Psi_{\mathsf{R}}$ and $X'_{\mathsf{R}} = \overline{\Psi}''_{\mathsf{R}} \cdot \overline{\Psi}'_{\mathsf{R}}$ with $\Psi_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} \overline{\Psi}'_{\mathsf{R}}$. By Lemma 72 (R SE: Single Step Instance Non Speculative) we have $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ with $\sigma = \Psi_{\mathsf{R}}.\sigma$ and $\overline{\Psi}'_{\mathsf{R}}.\sigma = \sigma'$.

□

Lemma 72 (R SE: Single Step Instance Non Speculative). *If*

(1) $X_{\mathsf{R}} = \overline{\Psi}_{\mathsf{R}} \cdot \Psi_{\mathsf{R}}$ *and*
(2) $X'_{\mathsf{R}} = \overline{\Psi}_{\mathsf{R}} \cdot \overline{\Psi}'_{\mathsf{R}}$ *and* $\vdash_O X'_{\mathsf{R}}$: *noongoing and*
(3) $\Psi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} \overline{\Psi}'_{\mathsf{R}}$ *and*
(4) $\sigma = \Psi_{\mathsf{R}}.\sigma$

Then there is a σ' *such that*

I $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ *and*
II $\overline{\Psi}'_{\mathsf{R}}.\sigma = \sigma$

Proof. We proceed by case analysis on the rule used to derive $\Psi_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} \Psi'_{\mathsf{R}}$.

Rule R:**SE-Ret** Then we have:

$$\sigma \xrightarrow{\tau} \sigma'$$
$$\mathbb{R} = \mathbb{R}' \cdot l$$
$$\sigma'' = \sigma[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto a(\mathbf{sp}) + 8]$$
$$\overline{\Psi}_{\mathsf{R}} = \langle p, ctr, \sigma', \mathbb{R}', h', n\rangle \cdot \langle p, ctr+1, \sigma'', \mathbb{R}', h', \omega\rangle^{l}_{\mathtt{ret}\ l\cdot\mathtt{start}\ ctr}$$

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 $\overline{\Psi}_{\mathsf{R}} = \langle p, ctr, \sigma', \mathbb{R}', h', n\rangle \cdot \langle p, ctr+1, \sigma'', \mathbb{R}', h', \omega\rangle^{l}_{\mathtt{ret}\ l\cdot\mathtt{st}\ (ctr)}$.

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 $p(\sigma(\mathbf{pc})) = \mathbf{ret}$ 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, $\sigma' = \overline{\Psi}'_{\mathsf{R}}.\sigma$.

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 $\vdash_{O} X'_{\mathsf{R}} : noongoing$.

Rule R:**SE-Ret-Empty** We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule and $\overline{\Psi}'_{\mathsf{R}} = \langle p, ctr, \sigma', \mathbb{R}, h, n-1\rangle$.

Thus, $\sigma' = \overline{\Psi}'_{\mathsf{R}}.\sigma$.

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 $p(\sigma(\mathbf{pc})) \neq \mathbf{ret}$ and $n \neq 0$ and can apply Lemma 73 (R SE: no Ret speculation). We get get an execution $\sigma \xrightarrow{\tau\restriction_{ns}} \sigma'$ and $\sigma' = X'_{\mathsf{R}}.\sigma$.

□

Lemma 73 (R SE: no Ret speculation). *Let p be a program, O be a prediction oracle. If*

(1) $\Psi_{\mathsf{R}} = \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle$ *and*
(2) $\Psi_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} \overline{\Psi}'_{\mathsf{R}}$, *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) $\Psi_{\mathsf{R}} = \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle$ and
(2) $\Psi_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} \overline{\Psi}'_{\mathsf{R}}$ and
(3) $p(\sigma(\mathbf{pc})) \neq \mathbf{ret}$ and
(4) $n \neq 0$

By inversion on $\Psi_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} X'_{\mathsf{R}}$ 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 $\tau = \varepsilon = \varepsilon\upharpoonright_{ns}$.

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 $\tau\upharpoonright_{ns} = \tau$ 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 74 (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 $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma'$ *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 $\tau\upharpoonright_{ns} = \tau = \texttt{ret}\ l$.

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.

□

M.1.1 Completeness. We proceed with the Completeness direction

Lemma 75 (R SE: Completeness of the speculative semantics)**.** *If*

(1) $\sigma \in InitConf$ *and*

(2) $\sigma \Downarrow_{\overline{\tau}} \sigma'$ *and*

(3) $X_{\mathrm{R}} = X_{\mathrm{R}}^{init}(\sigma)$

Then

I $X_{\mathrm{R}} \overset{O}{\rightsquigarrow}{}^{\mathrm{R}}_{\overline{\tau}'} X'_{\mathrm{R}\,\rho}$ *and*

II $\vdash_O X'_{\mathrm{R}} : noongoing$ *and*

III $\sigma' = X'_{\mathrm{R}}.\sigma$ *and*

IV $\overline{\tau} = \overline{\tau}' \upharpoonright_{ns}$ *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 $X_{\mathrm{R}} \overset{O}{\rightsquigarrow}{}^{\mathrm{R}}_{\varepsilon} X_{\mathrm{R}}$. By construction $\vdash_O X_{\mathrm{R}} : noongoing$ and $X_{\mathrm{R}}.\sigma = \sigma$. Since $\varepsilon \upharpoonright_{ns} = \varepsilon$ we are finished.

Rule NS-Single Then we have $\sigma \Downarrow_{\overline{\tau}} \sigma''$ and $\sigma'' \xrightarrow{\tau} \sigma'$.

We need to show

I $X_{\mathrm{R}} \overset{O}{\rightsquigarrow}{}^{\mathrm{R}}_{\overline{\tau}' \cdot \tau'} X'_{\mathrm{R}}$ and

II $\vdash_O X'_{\mathrm{R}} : noongoing$ and

III $\sigma' = X'_{\mathrm{R}}.\sigma$ and

IV $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \upharpoonright_{ns}$

We apply the IH on $\sigma \xrightarrow{\overline{\tau}} \sigma''$ we get

I' $X_{\mathrm{R}} \overset{O}{\rightsquigarrow}{}^{\mathrm{R}}_{\overline{\tau}'} X''_{\mathrm{R}\,\rho}$ and

II' $\vdash_O X''_{\mathrm{R}\,\rho} : noongoing$ and

III' $\sigma'' = X''_{\mathrm{R}}.\sigma$ and

IV' $\overline{\tau} = \overline{\tau}' \upharpoonright_{ns}$

V' $\rho = \varepsilon$

To account for possible outstanding commits, we use Lemma 9 (Executing a chain of commits) on X''_{R} and get

a) $X''_{\mathrm{R}} \overset{O}{\rightsquigarrow}{}^{\mathrm{R}}_{\overline{\tau}'''} X'''_{\mathrm{R}}$

b) $minWndw(X'''_{\mathrm{R}}) > 0$

c) $\forall \tau \in \overline{\tau}'''. \tau =$ `commit` id for some $id \in \mathbb{N}$

d) $X''_{\mathrm{R}}.\sigma = X'''_{\mathrm{R}}.\sigma$

By c) and the definition of $\upharpoonright_{ns}$ we have $\overline{\tau}''' \upharpoonright_{ns} = \varepsilon$.

Because only Rule R:SE-Commit was used we have $X'''_{\mathrm{R}\,\rho} = X''_{\mathrm{R}\,\rho}$. 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 $X'''_{\mathrm{R}} \overset{O}{\underset{}{\xrightarrow{\tau'}}}{}_{\mathrm{R}} X^{n}_{\mathrm{R}}$.

Here, τ' is generated from $X'''_{\mathrm{R}}.\sigma \xrightarrow{\tau'} \sigma'$.

Since $\rightarrow$ is deterministic, we know that $\tau' = \tau$.

II Since no speculative transaction is started and we have $\vdash_O X''_{\mathsf{R}} : noongoing$ by IH, we have $\vdash_O X^n_{\mathsf{R}} : noongoing$.

III By definition and determinism of $\rightarrow$.

IV Now we have $X''_{\mathsf{R}} \overset{O}{\rightsquigarrow}{}^{\mathsf{R}}_{\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau'} X^n_{\mathsf{R}}$. Looking at the trace that is generated we have

$$
\begin{aligned}
&\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau' \upharpoonright_{ns} \overline{\tau}''' \upharpoonright_{ns} = \varepsilon \\
&= \overline{\tau}' \cdot \tau' \upharpoonright_{ns} \tau' = \tau \\
&= \overline{\tau}' \cdot \tau \upharpoonright_{ns} \tau \text{ generated by} \rightarrow \\
&= \overline{\tau}' \upharpoonright_{ns} \cdot \tau \text{ by IH} \\
&= \overline{\tau} \cdot \tau
\end{aligned}
$$

and thus, are finished.

$p(\sigma(\mathbf{pc})) = \mathbf{ret}$ 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 $X''_{\mathsf{R}} \overset{O}{\rightsquigarrow}{}^{\mathsf{R}}_{\tau \cdot \mathtt{start}\ id} X^n_{\mathsf{R}}$ by using Rule R:SE-Ret in conjunction with Rule R:SE-Context and produce the observation $\tau' = \tau$, where $\tau = \mathtt{ret}\ l$.

Afterwards, we need to discharge the observation in $\overline{\rho}$ that was generated by Rule R:SE-Ret (which is always a $\mathtt{start}\ id$).

The only rule that can be used when $\overline{\rho}$ is non-empty is Rule R:SE-General, which produces $\mathtt{start}\ id$.

By Rule R:SE-Ret, we know that the step $X'''_{\mathsf{R}}.\sigma \xrightarrow{\tau} \sigma'$ is made.

II No speculative transaction was started that needs to be rolled back. By $\vdash_O X''_{\mathsf{R}} : noongoing$ and $\vdash_O X'''_{\mathsf{R}} : noongoing$ we get $\vdash_O X^n_{\mathsf{R}} : noongoing$.

III By definition and determinism of $\rightarrow$.

IV We now have:

$$
\begin{aligned}
&\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau' \cdot \mathtt{start}\ id \upharpoonright_{ns} \text{Def. and } \overline{\tau}''' \upharpoonright_{ns} = \varepsilon \\
&= \overline{\tau}' \cdot \tau' \upharpoonright_{ns} \tau' = \tau \\
&= \overline{\tau}' \cdot \tau \upharpoonright_{ns} \tau \text{ generated by} \rightarrow \\
&= \overline{\tau}' \upharpoonright_{ns} \cdot \tau \text{ by IH} \\
&= \overline{\tau} \cdot \tau
\end{aligned}
$$

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 $\tau'' = \mathtt{store}\ m$ and the step $X'''_{\mathsf{R}}.\sigma \xrightarrow{\tau''} \sigma'''$ is made.

Since $\rightarrow$ is deterministic and the fact that $\sigma'' \xrightarrow{\tau''} \sigma'''$, $\sigma'' \xrightarrow{\tau} \sigma'$ and $X'''_{\mathrm{R}}.\sigma = \sigma''$, 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 $X'''_{\mathrm{R}} \overset{O}{\rightsquigarrow}{}^{\mathrm{R}}_{\tau'\cdot\texttt{start}\ id\cdot\texttt{ret}\ l} X_{\mathrm{R}}3$.

Since all transactions are eventually closed, we know there exists X^n_{R} such that $X^3_{\mathrm{R}} \overset{O}{\rightsquigarrow}{}^{\mathrm{R}}_{\overline{\tau}^n\cdot\texttt{rlb}\ id} X^n_{\mathrm{R}}$.

We now apply Lemma 76 (R SE: Non-speculative execution for rolled back transactions) on the execution $X'''_{\mathrm{R}} \overset{O}{\rightsquigarrow}{}^{\mathrm{R}}_{\tau'\cdot\texttt{start}\ id\cdot\texttt{bypass}\ n\cdot\overline{\tau}^n\cdot\texttt{rlb}\ id} X^n_{\mathrm{R}}$ and get $\sigma'' \xrightarrow{\tau''} \sigma'''$ and $X^n_{\mathrm{R}}.\sigma = \sigma''$.

II Since the speculative transaction that was started was also rolled back and the fact that $\vdash_O X''_{\mathrm{R}} : \mathit{noongoing}$ by IH and $\vdash_O X'''_{\mathrm{R}} : \mathit{noongoing}$, we have $\vdash_O X^n_{\mathrm{R}} : \mathit{noongoing}$.

III Follows by definition and I).

IV By definition $\tau'' \cdot \texttt{start}\ id \cdots \texttt{rlb}\ id {\upharpoonright_{ns}} = \tau'' {\upharpoonright_{ns}} = \tau''$.

$$
\begin{aligned}
&\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau'' \cdot \texttt{start}\ id \cdot \overline{\tau}^n \cdot \texttt{rlb}\ id {\upharpoonright_{ns}} \text{ Def. and } \overline{\tau}''' {\upharpoonright_{ns}} = \varepsilon\\
=&\overline{\tau}' \cdot \tau' {\upharpoonright_{ns}} \ \tau'' = \tau\\
=&\ \overline{\tau}' \cdot \tau {\upharpoonright_{ns}} \ \tau \text{ generated by} \rightarrow\\
=&\ \overline{\tau}' {\upharpoonright_{ns}} \cdot \tau \text{ by IH}\\
=&\ \overline{\tau} \cdot \tau
\end{aligned}
$$

Notice that ρ is empty for all the cases, because we discharge all the observations immediately using Rule R:SE-General.

□

Lemma 76 (R SE: Non-speculative execution for rolled back transactions.). *If*

(1) $X_{\mathrm{R}} \overset{O}{\rightsquigarrow}{}^{\mathrm{R}}_{\overline{\tau}} X'_{\mathrm{R}}$ *and*

(2) $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$ *and*

(3) $\sigma = X_{\mathrm{R}}.\sigma$

Then

I there is a configurations σ' *with* $X'_{\mathrm{R}}.\sigma = \sigma'$ *and*

II $\sigma \xrightarrow{\overline{\tau}{\upharpoonright_{ns}}} \sigma'$ *and*

III $\overline{\tau}{\upharpoonright_{ns}} = \tau$

Proof. Let $X_{\mathrm{R}} \overset{O}{\rightsquigarrow}{}^{\mathrm{R}}_{\overline{\tau}} X'_{\mathrm{R}}$ be an execution with trace $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$. Let $\sigma = X_{\mathrm{R}}.\sigma$

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 ${\upharpoonright_{ns}}$ we have $\overline{\tau}{\upharpoonright_{ns}} = \tau{\upharpoonright_{ns}} = \tau$, where the last steps is because of the fact $\tau \in \mathit{Obs}$.

Thus, we have $\sigma \Downarrow_{\overline{\tau}{\upharpoonright_{ns}}} \sigma'$ by Rule NS-Reflection and $\sigma \xrightarrow{\tau} \sigma'$.

Now we need to show that $\sigma' = X'_{\mathrm{R}}.\sigma$, which is analogous to Lemma 50 (S SE: Non-speculative execution for rolled back transactions). □

M.2 R: Relating Non-speculative and AM Semantics

- Theorem 18 (R AM: Behaviour of non-speculative semantics and AM semantics)
  - Lemma 80 (R AM: Completeness of the speculative AM semantics)
    - Lemma 81 (R AM: Non-speculative execution for rolled back transactions)
  - Lemma 77 (R AM : Soundness of the AM semantics w.r.t. non-speculative semantics)
    - Lemma 78 (R AM: Soundness single step No Speculation)
    - Lemma 79 (R AM: Single Step Speculation)

Theorem 18 (R AM: Behaviour of non-speculative semantics and AM semantics). *Let p be a program. Then* $Beh_{NS}(p) = Beh^{\omega}_{\mathsf{R}}(p)\restriction_{ns}$

Proof. The lemma can be proven in a similar fashion to Theorem 13 (S AM: Behaviour of non-speculative semantics and AM semantics). We prove the two directions separately:

$\Leftarrow$ Assume that $\overline{\tau} \in Beh^{\omega}_{\mathsf{R}}(p)$.

By the definition of $Beh^{\omega}_{\mathsf{R}}(p)$ we have an initial configuration σ such that $((p,\sigma))\,\Omega^{\omega}_{\mathsf{R}}\overline{\tau}$.

The proof proceeds in similar fashion to the analogous case in Theorem 13 (S AM: Behaviour of non-speculative semantics and AM semantics) by using Lemma 77 (R AM : Soundness of the AM semantics w.r.t. non-speculative semantics).

We can now conclude that $(p,\sigma)\,\Omega_{NS}\overline{\tau}\restriction_{ns} \in Beh_{NS}(p)$ by Rule NS-Trace.

$\Rightarrow$ Assume that $(p,\sigma)\,\Omega_{NS}\overline{\tau} \in Beh_{NS}(p)$. We thus know there exists $\sigma' \in FinalConf$ such that $\sigma \Downarrow_{\overline{\tau}} \sigma'$.

We can now apply Lemma 80 (R AM: Completeness of the speculative AM semantics) and get $\Sigma^{init}_{\mathsf{R}}(p,\sigma) \Downarrow^{\overline{\tau}'}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$ with $\vdash_O \Sigma'_{\mathsf{R}}$: *noongoing*, $\sigma' = \Sigma'_{\mathsf{R}}.\sigma$ and $\overline{\tau} = \overline{\tau}'\restriction_{ns}$.

Because of $\vdash_O \Sigma'_{\mathsf{R}}$: *noongoing* and $\sigma' = \Sigma'_{\mathsf{R}}.\sigma$ we know that $\vdash \Sigma'_{\mathsf{R}}$: *fin*.

We thus have $((p,\sigma))\,\Omega^{\omega}_{\mathsf{R}}\overline{\tau}' \in Beh^{\omega}_{\mathsf{R}}(p)$.

□

Lemma 77 (R AM : Soundness of the AM semantics w.r.t. non-speculative semantics). *If*

(1) $\Sigma_{\mathsf{R}}.\sigma = \sigma$ *and*
(2) $\vdash_O \Sigma_{\mathsf{R}}$: *noongoing and*
(3) $\Sigma_{\mathsf{R}} \Downarrow^{\overline{\tau}}_{\mathsf{S}} \Sigma'_{\mathsf{R}}$

Then there exists σ' *such that*

I if $\vdash_O \Sigma'_{\mathsf{R}}$: *noongoing then* $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}\sigma'}$ *and* $\Sigma'_{\mathsf{R}}.\sigma = \sigma'$ *and*

II if $\vdash^{i}_{O} \Sigma'_{\mathsf{R}}$: 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 $\Sigma_{\mathsf{R}} \Downarrow^{\overline{\tau}}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$

Rule R:AM-Reflection Then we have $\Sigma_{\mathsf{R}} \Downarrow^{\varepsilon}_{\mathsf{R}} \Sigma_{\mathsf{R}}$ with $\Sigma'_{\mathsf{R}} = \Sigma_{\mathsf{R}}$ 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 $\Sigma_{\mathsf{R}} \Downarrow^{\overline{\tau}'\cdot\tau}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$ and by Rule R:AM-Single we get $\Sigma_{\mathsf{R}} \Downarrow^{\overline{\tau}'}_{\mathsf{R}} \Sigma''_{\mathsf{R}}$ and $\Sigma''_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$.

We need to prove

I if $\vdash_{O} \Sigma'_{\mathsf{R}}$: *noongoing* then $\sigma \Downarrow_{\overline{\tau}\cdot\tau\restriction_{ns}\sigma'}$ and $\Sigma'_{\mathsf{R}}.\sigma = \sigma'$

II if $\vdash^{i}_{O} \Sigma'_{\mathsf{R}}$: *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 $\Sigma_{\mathsf{R}} \Downarrow^{\overline{\tau}'}_{\mathsf{R}} \Sigma''_{\mathsf{R}}$ and have a σ'' where σ'' is the configuration for some instance in Σ''_{R} such that.

I' if $\vdash_{O} \Sigma''_{\mathsf{R}}$: *noongoing* then $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}\sigma''}$ and $\Sigma''_{\mathsf{R}}.\sigma = \sigma''$

II' if $\vdash^{j}_{O} \Sigma''_{\mathsf{R}}$: *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 $\vdash_{O} \Sigma''_{\mathsf{R}}$: *noongoing* and we have $\sigma \Downarrow_{\overline{\tau}\restriction_{ns}} \sigma''$ and $\Sigma''_{\mathsf{R}}.\sigma = \sigma''$ by IH.

I Then $\vdash_{O} \Sigma'_{\mathsf{R}}$: *noongoing* and we need to proof $\sigma \Downarrow_{\overline{\tau}\cdot\tau\restriction_{ns}\sigma'}$ and $\Sigma'_{\mathsf{R}}.\sigma = \sigma'$. We now proceed by inversion on $\Sigma''_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$:

Rule R:AM-Rollback Then $\tau =$ `rlb` *id*.

Analogous to the corresponding case in Lemma 70 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

Rule R:AM-Ret-Spec Then we know that $\overline{p} =$ `ret` $l \cdot$ `start` *id* for Σ'_{R}.

Analogous to the corresponding case in Lemma 70 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise We know that $\sigma'' = \Sigma''_{\mathsf{R}}.\sigma$.

Analogous to the corresponding case in Lemma 70 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) together with Lemma 78 (R AM: Soundness single step No Speculation) with $\Sigma''_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$.

II Then Σ'_{R} has ongoing transactions, meaning $\vdash^{i}_{O} \Sigma'_{\mathsf{R}}$: *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 $\Sigma''_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$:

Rule R:AM-Ret-Spec Then we know that $\overline{p} =$ `ret` $l \cdot$ `start` *id* for Σ'_{R}.

Analogous to the corresponding case in Lemma 70 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) together with Lemma 79 (R AM: Single Step Speculation).

otherwise By definition of $\vdash^{i}_{O} \Sigma'_{R}$: *biggestongoingtransactionirolledback* we know that there exists a `rlb` i in the execution $\Sigma'_{R} \Downarrow^{\overline{\tau}_{fin}}_{R} \Sigma_{R fin}$ with no matching `start` i observation in that execution. Analogous to the corresponding case in Lemma 70 (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 $\Sigma''_{R} \xrightarrow{\tau}{}^{O}_{S} \Sigma'_{R}$:

Rule R:AM-Rollback and $\tau =$ `rlb` j Analogous to the corresponding case in Lemma 70 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Then $\tau \neq$ `rlb` j.

Analogous to the corresponding case in Lemma 70 (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 $\Sigma''_{R} \overset{\tau}{\leadsto}_{R} \Sigma'_{R}$:

Rule R:AM-Rollback Then $\tau =$ `rlb` id. We do a case analysis if $id = j$ or not.

$id = j$ Analogous to the corresponding case in Lemma 70 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

$id \neq j$ Analogous to the corresponding case in Lemma 70 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Then $\tau \neq$ `rlb` id.

Analogous to the corresponding case in Lemma 70 (R SE: Soundness of the speculative semantics w.r.t. non-speculative semantics)

□

Lemma 78 (R AM: Soundness single step No Speculation)**.** *If*

(1) $\vdash_{O} \Sigma_{R}$: *noongoing and*
(2) $\Sigma_{R} \overset{\tau}{\leadsto}_{R} \Sigma'_{R}$ *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 $\Sigma_{R} \overset{\tau}{\leadsto}_{R} \Sigma'_{R}$:

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 $\Phi_{R}.\sigma = \sigma$. Contradiction. By the definition of $\overset{\tau}{\leadsto}_{S}$ only Rule R:AM-Ret-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 $\vdash_{O} \Sigma_{R}$: *noongoing*.

Rule R:AM-Rollback Contradiction, since $\vdash_O \Sigma_R :$ *noongoing* and Definition 18 (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 $\Phi_R \xrightarrow{\tau}_R \overline{\Phi}'_R$.

We proceed by case analysis on the rule used to derive $\Phi_R \xrightarrow{\tau}_R \Phi'_R$.

Rule R:AM-Ret-Spec 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-barr or Rule R:AM-barr-spec We have $p(\sigma(\mathbf{pc})) \neq \mathbf{ret}$ and $n \neq 0$.

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 $\tau = \varepsilon = \varepsilon\upharpoonright_{ns}$.

Rule R:AM-NoBranch We have $p(\sigma(\mathbf{pc})) \neq \mathbf{ret}$ and $n \neq 0$.

We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule and $\overline{\Psi}'_4 = \langle p, ctr, \sigma', \mathbb{R}, h, n-1 \rangle$.

Thus, $\sigma' = \overline{\Phi}'_R.\sigma$.

Because the rule used the observation received from the step $\sigma \xrightarrow{\tau} \sigma'$, we have $\tau\upharpoonright_{ns} = \tau$ 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.

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 step $\sigma \xrightarrow{\tau} \sigma'$, we have $\tau\upharpoonright_{ns} = \tau$ 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.

□

Lemma 79 (R AM: Single 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) $\Phi_R \xrightarrow{\tau}_R \overline{\Phi}'_R$ *and*
(4) $\sigma = \Phi_R.\sigma$

Then

I $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma'$ *and*
II σ' *is the configuration for the instance with* $ctr = i$ *in* Σ'_R

Proof. We proceed by inversion on $\Phi_R \xrightarrow{\tau}_R \overline{\Phi}'_R$:

Rule R:AM-Ret-Spec Then we have

$$\sigma \xrightarrow{\tau} \sigma'$$
$$\mathbb{R} = \mathbb{R}' \cdot l$$
$$m(a(\mathbf{sp})) \neq l$$
$$\sigma'' = \sigma[\mathbf{pc} \mapsto l, \mathbf{sp} \mapsto a(\mathbf{sp}) + 8]$$
$$\overline{\Phi}_{\mathrm{R}} = \langle p, ctr, \sigma', \mathbb{R}', h', n\rangle \cdot \langle p, ctr+1, \sigma'', \mathbb{R}', h', \omega\rangle^{l}_{\mathtt{ret}\ l \cdot \mathtt{st}\ (ctr)}$$

We have $\sigma \xrightarrow{\tau} \sigma'$.

Since $\vdash_O \Sigma_{\mathrm{R}} : noongoing$ we know that $\tau\restriction_{ns} = \tau = \mathtt{ret}\ l$.

Since a transaction with $id = ctr$ was started and we have $\vdash_O \Sigma_{\mathrm{R}} : noongoing$, 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 $\vdash_O \Sigma_{\mathrm{R}} : noongoing$ and $\vdash^i_O \Sigma'_{\mathrm{R}} : biggestongoingtransactionirolledback$, we know that a transaction has to be started that will be rolled back.

□

M.2.1 Completeness.

Lemma 80 (R AM: Completeness of the speculative AM semantics)**.** *If*

(1) $\sigma \in InitConf$ *and*

(2) $\sigma \Downarrow_{\overline{\tau}} \sigma'$ *and*

(3) $\Sigma_{\mathrm{R}} = \Sigma^{init}_{\mathrm{R}}(\sigma)$

Then

I $\Sigma_{\mathrm{R}} \Downarrow^{\overline{\tau}'}_{\mathrm{R}} \Sigma'_{\mathrm{R}\rho}$ *and*

II $\vdash_O \Sigma'_{\mathrm{R}} : noongoing$ *and*

III $\sigma' = \Sigma'_{\mathrm{R}}.\sigma$ *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 $\Sigma_{\mathrm{R}} \Downarrow^{\varepsilon}_{\mathrm{R}} \Sigma_{\mathrm{R}}$. By construction $\vdash_O \Sigma_{\mathrm{R}} : noongoing$ and $\Sigma_{\mathrm{R}}.\sigma = \sigma$. 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 $\Sigma_{\mathrm{R}} \Downarrow^{\overline{\tau}' \cdot \tau'}_{\mathrm{R}} \Sigma'_{\mathrm{R}}$ and

II $\vdash_O \Sigma'_{\mathrm{R}} : noongoing$ and

III $\sigma' = \Sigma'_{\mathrm{R}}.\sigma$ 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' $\Sigma_{\mathsf{R}} \Downarrow^{\overline{\tau}'}_{\mathsf{R}} \Sigma''_{\mathsf{R}\,\rho}$ and

II' $\vdash_{O} \Sigma''_{\mathsf{R}\,\rho}$: *noongoing* and

III' $\sigma'' = \Sigma''_{\mathsf{R}}.\sigma$ and

IV' $\overline{\tau} = \overline{\tau}' \upharpoonright_{ns}$

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 75 (R SE: Completeness of the speculative semantics).

$p(\sigma(\mathbf{pc})) = \mathbf{ret}$ Analogous to the corresponding case Lemma 75 (R SE: Completeness of the speculative semantics), which is when the oracle mispredicted in the proof, together with Lemma 81 (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 81 (R AM: Non-speculative execution for rolled back transactions.). *If*

(1) $\Sigma_{\mathsf{R}} \Downarrow^{\overline{\tau}}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$ *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 $\Sigma'_{\mathsf{R}}.\sigma = \sigma'$ *and*

II $\sigma \xrightarrow{\overline{\tau}\upharpoonright_{ns}} \sigma'$ *and*

III $\overline{\tau}\upharpoonright_{ns} = \tau$

Proof. Let $\Sigma_{\mathsf{R}} \Downarrow^{\overline{\tau}}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$ be an execution with trace $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$. Let $\sigma = \Sigma_{\mathsf{R}}.\sigma$

The proof proceeds analogously to Lemma 76 (R SE: Non-speculative execution for rolled back transactions). □

M.3 R: Relating Symbolic and AM semantics

These proofs are conceptually very similar to the proofs of S.

Theorem 19 (R: Behaviour of AM and symbolic semantics). $Beh^{\omega}_{\mathsf{R}}(p) = \mu(Beh^{\mathcal{S}}_{\mathsf{R}}(p))$

Theorem 19 (R: Behaviour of AM and symbolic semantics)

Lemma 82 (R: Soundness of the AM semantics w.r.t. symbolic semantics) Lemma 84 (R: Completeness of the symbolic semantics)

Lemma 83 (R: Soundness single step) Lemma 85 (R: Completeness single step)

Now onto theorems for the new speculative semantics. We want to show Soundness and Completeness.

M.3.1 Soundness.

Lemma 82 (R: Soundness of the AM semantics w.r.t. symbolic semantics)**.** *If*

(1) $\Sigma^{\mathcal{S}}_{R}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau}}_{R}\ \Sigma^{\mathcal{S}\prime}_{R}$ *and*
(2) $\mu \vDash pthCnd(\Sigma^{\mathcal{S}\prime}_{R})$

Then

$I\ \ \mu(\Sigma^{\mathcal{S}}_{R}) \Downarrow^{\mu(\overline{\tau})}_{R}\ \mu(\Sigma^{\mathcal{S}\prime}_{R})$ *and*

Proof. We proceed by induction on $\Sigma^{\mathcal{S}}_{R}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau_{\mathcal{S}}}}_{R}\ \Sigma^{\mathcal{S}\prime}_{R}$

Rule R:Sym-Reflection Then we have $\Sigma^{\mathcal{S}}_{R}\ {}_{\mathcal{S}}\Downarrow^{\varepsilon}_{R}\ \Sigma^{\mathcal{S}\prime}_{R}$ with $\Sigma^{\mathcal{S}\prime}_{R} = \Sigma^{\mathcal{S}}_{R}$. Using Rule R:AM-Reflection we get $\mu(\Sigma^{\mathcal{S}}_{R})\ {}_{\mathcal{S}}\Downarrow^{\mu(\varepsilon)}_{R}\ \mu(\Sigma^{\mathcal{S}\prime}_{R})$ and are finished.

Rule R:Sym-Single We have $\Sigma^{\mathcal{S}}_{R}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau_{\mathcal{S}}}'\cdot\tau_{\mathcal{S}}}_{R}\ \Sigma^{\mathcal{S}\prime}_{R}$ and by Rule R:Sym-Single we get $\Sigma^{\mathcal{S}}_{R}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau_{\mathcal{S}}}'}_{R}\ \Sigma^{\mathcal{S}\prime\prime}_{R}$ and $\Sigma^{\mathcal{S}\prime\prime}_{R} \xrightarrow{\tau}{}^{\mathcal{S}}_{R}\ \Sigma^{\mathcal{S}\prime}_{R}$.
We need to prove
(1) $\mu(\Sigma^{\mathcal{S}}_{R}) \Downarrow^{\mu(\overline{\tau}\cdot\tau_{\mathcal{S}})}_{R}\ \mu(\Sigma^{\mathcal{S}\prime}_{R})$
We apply the IH on $\Sigma^{\mathcal{S}}_{R}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau_{\mathcal{S}}}}_{R}\ \Sigma^{\mathcal{S}\prime\prime}_{R}$ and have a $\Sigma''_{R} = \mu(\Sigma^{\mathcal{S}\prime\prime}_{R})$ such that:
(1) $\mu(\Sigma^{\mathcal{S}}_{R}) \Downarrow^{\mu(\overline{\tau_{\mathcal{S}}})}_{R}\ \Sigma''_{R}$ and
(2) $\mu \vDash pthCnd(\Sigma^{\mathcal{S}\prime\prime}_{R})$
The result follows by applying Lemma 83 (R: Soundness single step) on $\Sigma^{\mathcal{S}\prime\prime}_{R} \xrightarrow{\tau_{\mathcal{S}}}{}^{\mathcal{S}}_{R}\ \Sigma^{\mathcal{S}\prime}_{R}$ and get a step $\Sigma''_{R} \xrightarrow{\mu(\tau_{\mathcal{S}})}_{R}\ \mu(\Sigma^{\mathcal{S}}_{R})$. We now use Rule R:AM-Single and get an execution $\mu(\Sigma^{\mathcal{S}}_{R}) \Downarrow^{\mu(\overline{\tau_{\mathcal{S}}})\cdot\mu(\tau_{\mathcal{S}})}_{R}\ \mu(\Sigma^{\mathcal{S}\prime}_{R})$ as required.

□

Lemma 83 (R: Soundness single step)**.** *If*

(1) $\Sigma^{\mathcal{S}}_{R} \xrightarrow{\tau_{\mathcal{S}}}{}^{\mathcal{S}}_{R}\ \Sigma^{\mathcal{S}}_{R}$ *and*
(2) $\mu \vDash pthCnd(\Sigma^{\mathcal{S}\prime}_{R})$

Then

$I\ \ \mu(\Sigma^{\mathcal{S}}_{R}) \xrightarrow{\mu(\tau_{\mathcal{S}})}_{R}\ \mu(\Sigma^{\mathcal{S}\prime}_{R})$

Proof. We proceed by inversion on $\Sigma^{\mathcal{S}}_{R} \xrightarrow{\tau}{}^{\mathcal{S}}_{R}\ \Sigma^{\mathcal{S}\prime}_{R}$:

Rule R:Sym-Rollback Since μ does not change the speculation window and ctr and $\mu(\Sigma^{\mathcal{S}}_{R}) = \Sigma_{R}$, we have $\Sigma_{R}.n = \Sigma^{\mathcal{S}}_{R}.n = 0$ and $\Sigma_{R}.ctr = \Sigma^{\mathcal{S}}_{R}.ctr$.
Analogous to Lemma 57 using Rule R:AM-Rollback.

Rule R:Sym-Context We then have $\Phi^{\mathcal{S}}_{R} \xrightarrow{\tau}{}^{\mathcal{S}}_{R}\ \overline{\Phi^{\mathcal{S}\prime}}_{R}$. Thus, we know $\Phi^{\mathcal{S}}_{R} > 0$ and $\mu(\Phi^{\mathcal{S}}_{R}) > 0$ as well. We proceed by inversion on $\Phi^{\mathcal{S}}_{R} \xrightarrow{\tau_{\mathcal{S}}}{}^{\mathcal{S}}_{R}\ \overline{\Phi^{\mathcal{S}\prime}}_{R}$:

Rule R:Sym-General Then $\Phi^{\mathcal{S}}_{R} \xrightarrow{\tau_{\mathcal{S}}}{}^{\mathcal{S}}_{R}\ \Phi^{\mathcal{S}}_{R\ \overline{p_{\mathcal{S}}}\setminus\tau_{\mathcal{S}}}$. Analogous to Lemma 57 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, Ru

Then we have $\Phi^{\mathcal{S}}_{R} \xrightarrow{\tau_{\mathcal{S}}}{}^{\mathcal{S}}_{R}\ \Phi^{\mathcal{S}\prime}_{R}$ where $\Phi^{\mathcal{S}\prime}_{R} = \langle p, \Phi^{\mathcal{S}}_{R}.ctr, \Phi^{\mathcal{S}}_{R}.\sigma'_{\mathcal{S}}, \Phi^{\mathcal{S}}_{R}.\mathbb{R}, \Phi^{\mathcal{S}}_{R}.n - 1\rangle$ with $\Phi^{\mathcal{S}}_{R}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$.
Since we have $\mu \vDash pthCnd(\overline{\Phi^{\mathcal{S}}}_{R}.\sigma_{\mathcal{S}})$ (by assumption) we can use Lemma 3 (NS: Soundness Symbolic Added rules) on $\Phi^{\mathcal{S}}_{R}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$ and get $\mu(\Phi^{\mathcal{S}}_{R}\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_{\mathcal{S}})} \mu(\sigma'_{\mathcal{S}})$, where $\mu(\Phi_{S}.\sigma_{\mathcal{S}}) = \Phi_{S}.\sigma$ as per assumption.

Now choose $\Phi_{\mathsf{R}}^{\mathcal{S}'}.\sigma = \sigma'_{\mathcal{S}}$ and let it otherwise be equal to Φ'_{S}. We can now use Rule S:Sym-NoBranch to derive the step $\Phi_{\mathsf{R}}^{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}{}_{\mathsf{R}}^{\mathcal{S}} \Phi_{\mathsf{R}}^{\mathcal{S}'}$ using the derived $\rightarrow_{\mathcal{S}}$ step and trivially satisfy $\mu(\Phi_{\mathsf{R}}^{\mathcal{S}'}) = \Phi'_{\mathsf{S}}$.

Rule R:AM-Call Then we have $\Phi_{\mathsf{R}}^{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}{}_{\mathsf{R}}^{\mathcal{S}} \Phi_{\mathsf{R}}^{\mathcal{S}'}$ where $\Phi_{\mathsf{R}}^{\mathcal{S}'} = \langle p, \Phi_{\mathsf{R}}^{\mathcal{S}}.ctr, \Phi_{\mathsf{R}}^{\mathcal{S}}.\sigma', \mathbb{R}', \Phi_{\mathsf{R}}^{\mathcal{S}}.n{-}1\rangle$ with $\Phi_{\mathsf{R}}^{\mathcal{S}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$ and $\mathbb{R}' = \Phi_{\mathsf{R}}^{\mathcal{S}}.\mathbb{R}.\Phi_{\mathsf{R}}^{\mathcal{S}}.\sigma_{\mathcal{S}}(\mathbf{pc}) + 1$. 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 57 (S: Soundness single step).

Rule R:Sym-Ret-Spec We have $\Phi_{\mathsf{R}}^{\mathcal{S}}.\mathbb{R} = \mathbb{R}' \cdot l$ and $\Phi_{\mathsf{R}}^{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}{}_{\mathsf{R}}^{\mathcal{S}} \overline{\Phi^{\mathcal{S}}}_{\mathsf{R}\,\overline{\rho_{\mathcal{S}}}\cdot\mathtt{ret}\ l\cdot\mathtt{start}_{\mathsf{R}}\ \Phi_{\mathsf{R}}^{\mathcal{S}}.ctr}$ where $\overline{\Phi^{\mathcal{S}}}_{\mathsf{R}} = \langle p, \Phi_{\mathsf{R}}^{\mathcal{S}}.ctr, \sigma'_{\mathcal{S}}, \Phi_{\mathsf{R}}^{\mathcal{S}}.\mathbb{R}, \Phi_{\mathsf{R}}^{\mathcal{S}}.n - 1\rangle \cdot \langle p, \Phi_{\mathsf{R}}^{\mathcal{S}}.ctr + 1, \sigma''_{\mathcal{S}}, \mathbb{R}', \min \Phi_{\mathsf{R}}^{\mathcal{S}}.n, \omega\rangle$.
Furthermore, we have $\Phi_{\mathsf{R}}^{\mathcal{S}}.\sigma \xrightarrow{\tau_{\mathcal{S}}} \sigma'_{\mathcal{S}}$ and $\sigma''_{\mathcal{S}} = \sigma_{\mathcal{S}}[\mathbf{pc} \mapsto l, ' \rightarrow sa(\mathbf{sp}) + 8]$.
We use Lemma 3 (NS: Soundness Symbolic Added rules) on $\Phi_{\mathsf{R}}^{\mathcal{S}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$ and get $\mu(\Phi_{\mathsf{R}}^{\mathcal{S}}.\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_{\mathcal{S}})}_{\mathcal{S}} \mu(\sigma'_{\mathcal{S}})$.
Choose $\Phi_{\mathsf{R}} = \mu(\Phi_{\mathsf{R}}^{\mathcal{S}})$ 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 $\mu(\Phi_{\mathsf{R}}^{\mathcal{S}}.\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_{\mathcal{S}})}_{\mathcal{S}} \mu(\sigma'_{\mathcal{S}})$ above and $\sigma'' = \sigma[\mathbf{pc} \mapsto l, ' \rightarrow a(\mathbf{sp}) + 8]$: $\Phi_{\mathsf{R}} \xrightarrow{\mu(\tau_{\mathcal{S}})}{}_{\mathsf{R}} \overline{\Phi}_{\mathsf{R}}$ with $\overline{\Phi}_{\mathsf{R}} = \langle p, \Phi_{\mathsf{R}}.ctr, \mu(\sigma'_{\mathcal{S}}), \Phi_{\mathsf{R}}.n - 1\rangle \cdot \langle p, \Phi_{\mathsf{R}}.ctr + 1, \sigma'', \min \Phi_{\mathsf{R}}.n, \omega\rangle$.
By definition we have $\mu(\sigma''_{\mathcal{S}}) = \sigma''$, because **pc** and **sp** are always concrete. We now show that $\mu(\overline{\Phi^{\mathcal{S}}}_{\mathsf{R}}) = \overline{\Phi}_{\mathsf{R}}$. By $\mu(\Phi_{\mathsf{R}}^{\mathcal{S}}) = \Phi_{\mathsf{R}}$ we have $\Phi_{\mathsf{R}}^{\mathcal{S}}.ctr = \Phi_{\mathsf{R}}.ctr$ and $\Phi_{\mathsf{R}}^{\mathcal{S}}.n = \Phi_{\mathsf{R}}.n$ and by construction $\mu(\overline{\Phi^{\mathcal{S}}}_{\mathsf{R}}) = \overline{\Phi}_{\mathsf{R}}$ and thus $\mu(\Phi_{\mathsf{R}}^{\mathcal{S}}) \xrightarrow{\mu(\tau_{\mathcal{S}})}{}_{\mathsf{R}} \mu(\overline{\Phi^{\mathcal{S}}}_{\mathsf{R}})$ as needed.

□

M.3.2 *Completeness.*

Lemma 84 (R: Completeness of the symbolic semantics)**.** *If*

(1) $\Sigma_{\mathsf{R}} \Downarrow_{\mathsf{R}}^{\overline{\tau}} \Sigma'_{\mathsf{R}}$ *and*
(2) $\Sigma_{\mathsf{R}} = \mu(\Sigma_{\mathsf{R}}^{\mathcal{S}})$

Then there is a valuation μ, a symbolic trace $\overline{\tau}'$ and a final state $\Sigma_{\mathsf{R}}^{\mathcal{S}'}$ such that

I $\Sigma_{\mathsf{R}}^{\mathcal{S}}\ {}_{\mathcal{S}}\Downarrow_{\mathsf{R}}^{\overline{\tau}'} \Sigma_{\mathsf{R}}^{\mathcal{S}'}$ *and*
II $\Sigma'_{\mathsf{R}} = \mu(\Sigma_{\mathsf{R}}^{\mathcal{S}'})$ *and* $\overline{\tau} = \mu(\overline{\tau}')$ *and*
III $\mu \vDash pthCnd(\Sigma_{\mathsf{R}}^{\mathcal{S}'})$

Proof. We proceed by induction on $\Sigma_{\mathsf{R}} \Downarrow_{\mathsf{R}}^{\overline{\tau}} \Sigma'_{\mathsf{R}}$

Rule R:AM-Reflection Then we have $\Sigma_{\mathsf{R}} \Downarrow_{\mathsf{R}}^{\varepsilon} \Sigma'_{\mathsf{R}}$ with $\Sigma_{\mathsf{R}} = \Sigma'_{\mathsf{R}}$.

I - III By Rule R:Sym-Reflection we have $\Sigma_{\mathsf{R}}^{\mathcal{S}}\ {}_{\mathcal{S}}\Downarrow_{\mathsf{R}}^{\varepsilon} \Sigma_{\mathsf{R}}^{\mathcal{S}'}$. By construction $\Sigma_{\mathsf{R}}^{\mathcal{S}'} = \Sigma_{\mathsf{R}}^{\mathcal{S}'}$. We now trivially satisfy all conditions.

Rule R:AM-Single We have $\Sigma_{\mathsf{R}} \Downarrow_{\mathsf{R}}^{\overline{\tau}'\cdot\tau} \Sigma'_{\mathsf{R}}$ and by Rule R:AM-Single we get $\Sigma_{\mathsf{R}} \Downarrow_{\mathsf{R}}^{\overline{\tau_{\mathcal{S}}}'} \Sigma''_{\mathsf{R}}$ and $\Sigma''_{\mathsf{R}} \xrightarrow{\tau}{}_{\mathsf{R}}^{\mathcal{S}} \Sigma'_{\mathsf{R}}$.

We need to prove

(1) $\Sigma_{\mathsf{R}}^{\mathcal{S}}\ {}_{\mathcal{S}}\Downarrow_{\mathsf{R}}^{\overline{\tau_{\mathcal{S}}}'\cdot\tau_{\mathcal{S}}} \Sigma_{\mathsf{R}}^{\mathcal{S}'}$ and
(2) $\Sigma'_{\mathsf{R}} = \mu(\Sigma_{\mathsf{R}}^{\mathcal{S}'})$ and $\overline{\tau}' \cdot \tau = \mu(\overline{\tau_{\mathcal{S}}}' \cdot \tau_{\mathcal{S}})$ and
(3) $\mu \vDash pthCnd(\Sigma_{\mathsf{R}}^{\mathcal{S}'})$

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

(1) $\Sigma^{\mathcal{S}}_{\mathsf{R}} \ {}_{\mathcal{S}}{\Downarrow}^{\overline{\tau_{\mathcal{S}}}'}_{\mathsf{R}} \ \Sigma^{\mathcal{S}''}_{\mathsf{R}}$ and
(2) $\Sigma''_{\mathsf{R}} = \mu(\Sigma^{\mathcal{S}''}_{\mathsf{R}})$ and $\overline{\tau}' = \mu(\overline{\tau_{\mathcal{S}}}')$ and
(3) $\mu \vDash pthCnd(\Sigma^{\mathcal{S}''}_{\mathsf{R}})$

The result follows from applying Lemma 85 (R: Completeness single step) on $\Sigma''_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$ and get a step $\Sigma^{\mathcal{S}''}_{\mathsf{R}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}^{\mathcal{S}}_{\mathsf{R}} \Sigma^{\mathcal{S}}_{\mathsf{R}}$. We now use Rule R:Sym-Single and get an execution $\Sigma^{\mathcal{S}}_{\mathsf{R}} \ {}_{\mathcal{S}}{\Downarrow}^{\overline{\tau_{\mathcal{S}}}\cdot\tau_{\mathcal{S}}}_{\mathsf{R}} \ \mu(\Sigma^{\mathcal{S}'}_{\mathsf{R}})$ as required.

□

Lemma 85 (R: Completeness single step). *If*

(1) $\Sigma_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$ *and* $\mu(\Sigma^{\mathcal{S}}_{\mathsf{R}}) = \Sigma_{\mathsf{R}}$ *and*
(2) $\mu \vDash pthCnd(\Sigma^{\mathcal{S}}_{\mathsf{R}})$

Then

I $\Sigma^{\mathcal{S}}_{\mathsf{R}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}^{\mathcal{S}}_{\mathsf{R}} \Sigma^{\mathcal{S}'}_{\mathsf{R}}$ *and*
II $\mu(\Sigma^{\mathcal{S}'}_{\mathsf{R}}) = \Sigma'_{\mathsf{R}}$ *and*
III $\mu \vDash pthCnd(\Sigma^{\mathcal{S}'}_{\mathsf{R}})$ *and* $\mu(\tau_{\mathcal{S}}) = \tau$

Proof. We proceed by inversion on $\Sigma_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$:

Rule R:AM-Rollback Since μ does not change the speculation window and ctr and $\mu(\Sigma^{\mathcal{S}}_{\mathsf{R}}) = \Sigma_{\mathsf{R}}$, we have $\Sigma_{\mathsf{R}}.n = \Sigma^{\mathcal{S}}_{\mathsf{R}}.n = 0$ and $\Sigma_{\mathsf{R}}.ctr = \Sigma^{\mathcal{S}}_{\mathsf{R}}.ctr$. The rest of the proof is analogous to the corresponding case in Lemma 59 (S: Completeness single step)

Rule R:AM-Context We then have $\Phi_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \overline{\Phi}'_{\mathsf{R}}$. Note that $\Phi_{\mathsf{R}}.n > 0$ and as such for all symbolic states where $\mu(\Phi^{\mathcal{S}}_{\mathsf{R}}) = \Phi_{\mathsf{R}}$ as well. We proceed by inversion on $\Phi_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \overline{\Phi}'_{\mathsf{R}}$:

Rule R:AM-General Analogous to the corresponding case in Lemma 59 (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

Then we have $\Phi_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \Phi'_{\mathsf{R}}$ where $\Phi'_{\mathsf{R}} = \langle p, \Phi_{\mathsf{R}}.ctr, \Phi_{\mathsf{R}}.\sigma', \Phi_{\mathsf{R}}.\mathbb{R}, \Phi_{\mathsf{R}}.n - 1\rangle$ with $\Phi_{\mathsf{R}}.\sigma \xrightarrow{\tau} \sigma'$. Analogous to the corresponding case in Lemma 59 (S: Completeness single step).

Rule R:AM-Call Then we have $\Phi_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \Phi'_{\mathsf{R}}$ where $\Phi'_{\mathsf{R}} = \langle p, \Phi_{\mathsf{R}}.ctr, \Phi_{\mathsf{R}}.\sigma', \mathbb{R}', \Phi_{\mathsf{R}}.n - 1\rangle$ with $\Phi_{\mathsf{R}}.\sigma \xrightarrow{\tau} \sigma'$ and $\mathbb{R}' = \Phi_{\mathsf{R}}.\mathbb{R}.\Phi_{\mathsf{R}}.\sigma(\mathbf{pc}) + 1$. 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 59 (S: Completeness single step).

Rule R:AM-Ret-Spec We have $\Phi_{\mathsf{R}}.\mathbb{R} = \mathbb{R}' \cdot l$ and $\Phi_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \overline{\Phi}_{\mathsf{R}}{}_{\overline{\rho}\cdot\mathtt{ret}\ l\cdot\mathtt{start}_{\mathsf{R}}\ \Phi_{\mathsf{R}}.ctr}$ where $\overline{\Phi}_{\mathsf{R}} = \langle p, \Phi_{\mathsf{R}}.ctr, \sigma', \Phi_{\mathsf{R}}.\mathbb{R}, \Phi_{\mathsf{R}}.n - 1\rangle \cdot \langle p, \Phi_{\mathsf{R}}.ctr + 1, \sigma'', \mathbb{R}', \min \Phi^{\mathcal{S}}_{\mathsf{R}}.n, \omega\rangle$.
Furthermore, we have $\Phi_{\mathsf{R}}.\sigma \xrightarrow{\tau} \sigma'$ and $\sigma'' = \sigma[\mathbf{pc} \mapsto l, ' \to a(\mathbf{sp}) + 8]$.
We use Lemma 5 (NS : Completeness Symbolic Added) on $\Phi_{\mathsf{R}}.\sigma \xrightarrow{\tau} \sigma'$ and get $\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$ with $\mu(\sigma_{\mathcal{S}}) = \sigma$, $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu(\sigma'_{\mathcal{S}}) = \sigma'$ and $\mu \vDash pthCnd(\sigma'_{\mathcal{S}})$.
Choose $\Phi_{\mathsf{R}} = \mu(\Phi^{\mathcal{S}}_{\mathsf{R}})$ 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 $\mu(\Phi^{\mathcal{S}}_{\mathsf{R}}.\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_{\mathcal{S}})}_{\mathcal{S}} \mu(\sigma'_{\mathcal{S}})$ above and $\sigma'' = \sigma[\mathbf{pc} \mapsto \sigma(\mathbf{pc}) + 1]$:
$\Phi^{\mathcal{S}}_{\mathsf{R}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}^{\mathcal{S}}_{\mathsf{R}} \overline{\Phi^{\mathcal{S}}}_{\mathsf{R}}$ with $\overline{\Phi^{\mathcal{S}}}_{\mathsf{R}} = \langle p, \Phi^{\mathcal{S}}_{\mathsf{R}}.ctr, \sigma'_{\mathcal{S}}, \Phi^{\mathcal{S}}_{\mathsf{R}}.\mathbb{R}, \Phi_{\mathsf{R}}.n - 1\rangle \cdot \langle p, \Phi^{\mathcal{S}}_{\mathsf{R}}.ctr + 1, \sigma'', \Phi^{\mathcal{S}}_{\mathsf{R}}.\mathbb{R}', \min \Phi^{\mathcal{S}}_{\mathsf{R}}.n, \omega\rangle$.
By definition we have $\mu(\sigma''_{\mathcal{S}}) = \sigma''$, because **pc** and **sp** are always concrete. We now show that $\mu(\overline{\Phi^{\mathcal{S}}}_{\mathsf{R}}) = \overline{\Phi}_{\mathsf{R}}$.

By $\mu(\Phi^{\mathcal{S}}_{R}) = \Phi_{R}$ we have $\Phi^{\mathcal{S}}_{R}.ctr = \Phi_{R}.ctr$ and $\Phi^{\mathcal{S}}_{R}.n = \Phi_{R}.n$ and by construction $\mu(\overline{\Phi^{\mathcal{S}}}_{R}) = \overline{\Phi}_{R}$ and thus $\mu(\Phi^{\mathcal{S}}_{R}) \overset{\mu(\tau_S)}{\rightsquigarrow}_{R} \mu(\overline{\Phi^{\mathcal{S}}}_{R})$ as needed.
Since $\overline{\Phi^{\mathcal{S}}}_{R}.\sigma = \sigma''$ and $\sigma''.\delta^{\mathcal{S}} = \sigma'.\delta^{\mathcal{S}}$ we have $\mu \vDash pthCnd(\sigma'')$ by $\mu \vDash pthCnd(\sigma')$ from above.

□

M.4 R: Relating Oracle and AM semantics via SNI

First the definition of the element function we are gonna use: elem_of_states$(\langle p, ctr, \sigma, \mathbb{R}, n\rangle) = \langle p, ctr, \sigma, \mathbb{R}\rangle$

The proof structure looks like this:

- Theorem 20 (R: Oracle Overapproximation)
  - Proposition 11 (R: Sound and Completeness between Spec and AM semantics)
    - Lemma 88 (R: Initial states fulfill properties)
    - Lemma 89 (R: Soundness Am semantics w.r.t. speculative semantics)
      - Lemma 90 (R: Soundness Am semantics w.r.t. speculative semantics with new relation between states)
        - Lemma 91 (R: Soundness Single Step AM)
          - Lemma 86 (R AM: Single step preserves ≅)
          - Lemma 87 (R SE: Single step preserves ≅)
    - Lemma 92 (R: Completeness AM semantics w.r.t. speculative semantics)
      - Lemma 94 (R:Stronger Soundness for a specific oracle and for specific executions)
        - Lemma 95 (R AM: Strong Soundness Single Step)

We define a few Lemmas

Lemma 86 (R AM: Single step preserves ≅). *If*

(1) $\Sigma_{R1} \cong \Sigma_{R2}$ *and*
(2) $\Sigma_{R1} \overset{\tau}{\rightsquigarrow}_{R} \Sigma'_{R}$ *and* $\Sigma_{R2} \overset{\tau}{\rightsquigarrow}_{R} \Sigma''_{R}$

Then

(1) $\Sigma'_{R} \cong \Sigma''_{R}$

Proof. We have

(1) $\Sigma_{R1} \cong \Sigma_{R2}$ and
(2) $\Sigma_{R1} \overset{\tau}{\rightsquigarrow}_{R} \Sigma'_{R}$ and $\Sigma_{R2} \overset{\tau'}{\rightsquigarrow}_{R} \Sigma''_{R}$

Because of (1), we know that the same rule was used to derive the steps $\Sigma_{R1} \overset{\tau}{\rightsquigarrow}_{R} \Sigma'_{R}$ and $\Sigma_{R2} \overset{\tau}{\rightsquigarrow}_{R} \Sigma''_{R}$.

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 60 (S AM: Single step preserves ≅).

□

Lemma 87 (R SE: Single step preserves ≅). *If*

(1) $X_{R1} \cong X_{R2}$ *and*
(2) $X_{R1} \xrightarrow{\tau}{}^{O}_{R} X'_{R}$ *and* $X_{R2} \xrightarrow{\tau}{}^{O}_{R} X''_{R}$

Then

(1) $X'_{R} \cong X''_{R}$ *and*

Proof. We have

(1) $X_{\mathsf{R}1} \cong X_{\mathsf{R}2}$ and
(2) $X_{\mathsf{R}1} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} X'_{\mathsf{R}}$ and $X_{\mathsf{R}2} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} X''_{\mathsf{R}}$

Because of (1), we know that the same rule was used to derive the steps $X_{\mathsf{R}1} \overset{\tau}{\Rightarrow}_{\mathsf{R}} X'_{\mathsf{R}}$ and $X_{\mathsf{R}2} \overset{\tau}{\Rightarrow}_{\mathsf{R}} X''_{\mathsf{R}}$.

We know that $X'_{\mathsf{R}}.ctr = X''_{\mathsf{R}}.ctr$, $X'_{\mathsf{R}}.n = X''_{\mathsf{R}}.n$, $X'_{\mathsf{R}}.l = X''_{\mathsf{R}}.l$, because of (1) and the fact that the same rule was used to derive the step.

The proof is analogous to Lemma 61 (S SE: Single step preserves $\cong$). ◻

Theorem 20 (R: Oracle Overapproximation). *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 $((p,\sigma)) \Downarrow_{NS} \overline{\tau}$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}$, then $((p,\sigma)) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}''$, $((p,\sigma')) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}''$*

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.

($\Rightarrow$) We have

(1) $\sigma \sim_P \sigma'$ and
(2) $((p,\sigma)) \Downarrow_{NS} \overline{\tau}'$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}'$ 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 $((p,\sigma)) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}''$, $((p,\sigma')) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}''$ 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 $((p,\sigma)) \Downarrow_{NS} \overline{\tau}$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}$, then $((p,\sigma)) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}'$ and $((p,\sigma')) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}'$.
We fulfill all premises of SNI by 1) and 2) for p and get $((p,\sigma)) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}'$ and $((p,\sigma')) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}'$.
We use Proposition 11 (R: Sound and Completeness between Spec and AM semantics) with $((p,\sigma)) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}'$ and $((p,\sigma')) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}'$ to get $((p,\sigma)) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}''$, $((p,\sigma')) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}''$. This completes the proof.

($\Leftarrow$) We have

(1) $\sigma \sim_P \sigma'$ and
(2) $((p,\sigma)) \Downarrow_{NS} \overline{\tau}'$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}'$ and
(3) if $\sigma \sim_P \sigma'$ and $((p,\sigma)) \Downarrow_{NS} \overline{\tau}$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}$, then $((p,\sigma)) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}''$, $((p,\sigma')) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}''$

Note that we got assumptions 1) and 2) by the unfolding of the definition of SNI. We need to show that $((p,\sigma)) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}'$ and $((p,\sigma')) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}'$ holds.
By using assumption 1) and 2) for assumption 3), we get $((p,\sigma)) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}''$, $((p,\sigma')) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}''$.
Let O be an arbitrary prediction oracle with speculative window at most ω.
From Proposition 11 (R: Sound and Completeness between Spec and AM semantics) with $((p,\sigma)) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}''$, $((p,\sigma')) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}''$ we get back $((p,\sigma)) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}$, $((p,\sigma')) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}$. 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 11 (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 $((p,\sigma)) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}$ and $((p,\sigma')) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}$ iff $((p,\sigma)) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}'$, $((p,\sigma)) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}'$ for all prediction oracles O with speculative window at most ω.*

Proof. The proposition immediately follows from Lemma 89 (R: Soundness Am semantics w.r.t. speculative semantics) and Lemma 92 (R: Completeness AM semantics w.r.t. speculative semantics) ◻

Definition 35 (V5: Relation between AM and spec for all oracles). *We define two relations between AM and oracle semantics.* $\approx$ $\sim$

$$\boxed{\Sigma_{\mathrm{R}} \approx X_{\mathrm{R}}}$$

$$\text{(Base)}\ \frac{}{\varnothing \approx \varnothing} \qquad \text{(Single-Base)}\ \frac{\Sigma_{\mathrm{R}} \sim X_{\mathrm{R}}\upharpoonright_{com} \qquad INV(\Sigma_{\mathrm{R}}, X_{\mathrm{R}})}{\Sigma_{\mathrm{R}} \approx X_{\mathrm{R}}}$$

$$\text{(Single-OracleTrue)}\ \frac{\begin{array}{c}\Sigma_{\mathrm{R}} \sim X_{\mathrm{R}}\upharpoonright_{com} \qquad \Sigma''_{\mathrm{R}} \Downarrow^{\overline{\tau}}_{\mathrm{R}} \Sigma'''_{\mathrm{R}} \textit{ where transaction with id ctr is rolled back}\\ X_{\mathrm{R}} = X'_{\mathrm{R}} \cdot \langle p, ctr, \sigma, h, n''\rangle \qquad \Sigma_{\mathrm{R}} = \Sigma'_{\mathrm{R}} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \qquad INV(\Sigma_{\mathrm{R}}, X_{\mathrm{R}})\end{array}}{\Sigma'_{\mathrm{R}} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n'\rangle \cdot \Sigma_{\mathrm{R}1} \approx X'_{\mathrm{R}} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n''\rangle \cdot \langle p, ctr', \sigma, \mathbb{R}', h, n'''\rangle^{true}}$$

$$\text{(Single-Transaction-Rollback)}\ \frac{\begin{array}{c}\Sigma''_{\mathrm{R}} \sim X''_{\mathrm{R}}\upharpoonright_{com} \qquad n' \geq 0 \qquad \Sigma''_{\mathrm{R}} \Downarrow^{\overline{\tau}}_{\mathrm{R}} \Sigma'''_{\mathrm{R}} \textit{ where transaction with id ctr is rolled back}\\ X_{\mathrm{R}} = X'_{\mathrm{R}} \cdot \langle p, ctr, \sigma, h, n''\rangle \qquad \Sigma_{\mathrm{R}} = \Sigma'_{\mathrm{R}} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \qquad INV(\Sigma_{\mathrm{R}}, X_{\mathrm{R}})\end{array}}{\Sigma'_{\mathrm{R}} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}'n'\rangle^{false} \cdot \Sigma_{\mathrm{R}1} \approx X'_{\mathrm{R}} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n''\rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0\rangle^{false} \cdot X_{\mathrm{R}1}}$$

$$\boxed{\Sigma_{\mathrm{R}} \sim X_{\mathrm{R}}}$$

$$\text{(Base)}\ \frac{}{\varnothing \sim \varnothing} \qquad \text{(Single)}\ \frac{|\Sigma'_{\mathrm{R}}| = |X'_{\mathrm{R}}| \qquad \Sigma'_{\mathrm{R}} \sim X'_{\mathrm{R}}}{\Sigma'_{\mathrm{R}} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle^{b} \sim X'_{\mathrm{R}} \cdot \langle p, ctr', \sigma, \mathbb{R}, h, n'\rangle^{b}}$$

Lemma 88 (R: 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) $\Sigma^{init}_{\mathrm{R}}(p, \sigma)$ and $\Sigma^{init}_{\mathrm{R}}(p, \sigma')$ and
(3) $X^{init}_{\mathrm{R}}(p, \sigma)$ and $X^{init}_{\mathrm{R}}(p, \sigma')$

Then

(1) $X^{init}_{\mathrm{R}}(p, \sigma) \cong X^{init}_{\mathrm{R}}(p, \sigma')$ and
(2) $\Sigma^{init}_{\mathrm{R}}(p, \sigma) \cong \Sigma^{init}_{\mathrm{R}}(p, \sigma')$ and
(3) $\Sigma^{init}_{\mathrm{R}}(p, \sigma) \approx X^{init}_{\mathrm{R}}(p, \sigma)$ and $\Sigma^{init}_{\mathrm{R}}(p, \sigma') \approx X^{init}_{\mathrm{R}}(p, \sigma')$ by Rule Single-Base and

Proof. We have

(1) $\sigma, \sigma' \in InitConf$ and
(2) $\Sigma^{init}_{\mathrm{R}}(p, \sigma)$ and $\Sigma^{init}_{\mathrm{R}}(p, \sigma')$ and
(3) $X^{init}_{\mathrm{R}}(p, \sigma)$ and $X^{init}_{\mathrm{R}}(p, \sigma')$

Notice that by definition of $X^{init}_{\mathrm{R}}()$ and $\Sigma^{init}_{\mathrm{R}}()$ we have:

$$\begin{aligned} X^{init}_{\mathrm{R}}(p, \sigma) &= \langle p, 0, \sigma, \varnothing, \bot\rangle \\ X^{init}_{\mathrm{R}}(p, \sigma') &= \langle p, 0, \sigma, \varnothing, \bot\rangle \\ \Sigma^{init}_{\mathrm{R}}(p, \sigma) &= \langle p, 0, \sigma, \bot\rangle \\ \Sigma^{init}_{\mathrm{R}}(p, \sigma') &= \langle p, 0, \sigma, \bot\rangle \end{aligned}$$

I Immediate

II Immediate

III Immediate using Rule Single-Base

□

Lemma 89 (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) $((p, \sigma)) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}$, $((p, \sigma')) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}$

Then for all prediction oracles O with speculation window at most ω.

I $((p, \sigma)) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}'$, $((p, \sigma)) \Downarrow^{O}_{\mathsf{R}} \overline{\tau}'$

Proof. Let $\omega \in \mathbb{N}$ be a speculation window and $\sigma, \sigma' \in InitConf$ be two initial configurations. We have:

(1) $((p, \sigma)) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}$, $((p, \sigma')) \Downarrow^{\omega}_{\mathsf{R}} \overline{\tau}$

Furthermore, let O be an arbitrary prediction oracle with speculative window at most ω.

The reasoning ins analogous to Lemma 63 (S: Soundness Am semantics w.r.t. speculative semantics) using Lemma 90 (R: Soundness Am semantics w.r.t. speculative semantics with new relation between states) together with Lemma 88 (R: Initial states fulfill properties).

□

Lemma 90 (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) $\Sigma_{\mathsf{R}1} \cong \Sigma_{\mathsf{R}2}$

(2) $X_{\mathsf{R}1} \cong X_{\mathsf{R}2}$ and $\overline{\rho} = \varnothing$

(3) $\Sigma_{\mathsf{R}1} \approx X_{\mathsf{R}1}$ and $\Sigma_{\mathsf{R}2} \approx X_{\mathsf{R}2}$

(4) $\Sigma_{\mathsf{R}1} \Downarrow^{\overline{\tau}}_{\mathsf{R}} \Sigma'_{\mathsf{R}1}$ and $\Sigma_{\mathsf{R}2} \Downarrow^{\overline{\tau}}_{\mathsf{R}} \Sigma'_{\mathsf{R}2}$

Then for all prediction oracles O with speculation window at most ω.

I $X_{\mathsf{R}1} \; {}^{O}\!\!\leadsto^{\mathsf{R}}_{\overline{\tau}'} X'_{\mathsf{R}1}$, $X_{\mathsf{R}2} \; {}^{O}\!\!\leadsto^{\mathsf{R}}_{\overline{\tau}''} X'_{\mathsf{R}2}$

II $\Sigma'_{\mathsf{R}1} \cong \Sigma'_{\mathsf{R}2}$

III $X'_{\mathsf{R}1} \cong X'_{\mathsf{R}2}$ and $\overline{\rho} = \varnothing$

IV $\Sigma'_{\mathsf{R}1} \approx X'_{\mathsf{R}1}$ and $\Sigma'_{\mathsf{R}2} \approx X'_{\mathsf{R}2}$

V $\overline{\tau}' = \overline{\tau}''$

Proof. By Induction on $\Sigma_{\mathsf{R}1} \Downarrow^{\overline{\tau}}_{\mathsf{R}} \Sigma'_{\mathsf{R}1}$ and $\Sigma_{\mathsf{R}2} \Downarrow^{\overline{\tau}}_{\mathsf{R}} \Sigma'_{\mathsf{R}2}$.

Rule R:AM-Reflection We have $\Sigma_{\mathsf{R}1} \Downarrow^{\varepsilon}_{\mathsf{R}} \Sigma'_{\mathsf{R}1}$ and $\Sigma_{\mathsf{R}2} \Downarrow^{\varepsilon}_{\mathsf{R}} \Sigma'_{\mathsf{R}2}$, where $\Sigma'_{\mathsf{R}1} = \Sigma_{\mathsf{R}1}$ and $\Sigma'_{\mathsf{R}2} = \Sigma_{\mathsf{R}2}$.

Furthermore, we use Rule R:SE-Reflection to derive $X_{\mathsf{R}1} \; {}^{O}\!\!\leadsto^{\mathsf{R}}_{\varepsilon} X'_{\mathsf{R}1}$, $X_{\mathsf{R}2} \; {}^{O}\!\!\leadsto^{\mathsf{R}}_{\varepsilon} X'_{\mathsf{R}2}$ with $X'_{\mathsf{R}1} = X_{\mathsf{R}1}$ and $X'_{\mathsf{R}2} = X_{\mathsf{R}2}$.

We now trivially satisfy all conclusions.

Rule R:AM-Single We have $\Sigma_{\mathsf{R}1} \Downarrow^{\overline{\tau}''}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$ with $\Sigma'_{\mathsf{R}} \xrightarrow{\tau}_{\mathsf{R}} \Sigma'_{\mathsf{R}1}$ and $\Sigma_{\mathsf{R}2} \Downarrow^{\overline{\tau}''}_{\mathsf{R}} \Sigma''_{\mathsf{R}}$ and $\Sigma''_{\mathsf{R}} \xrightarrow{\tau}_{\mathsf{R}} \Sigma'_{\mathsf{R}2}$.

We now apply IH on $\Sigma_{\mathsf{R}1} \Downarrow^{\overline{\tau}''}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$ and $\Sigma_{\mathsf{R}2} \Downarrow^{\overline{\tau}''}_{\mathsf{R}} \Sigma''_{\mathsf{R}}$ and get

(a) $X_{\mathsf{R}1} \overset{O}{\rightsquigarrow}{}^{\mathsf{R}}_{\overline{\tau}'} X'_{\mathsf{R}}$, $X_{\mathsf{R}2} \overset{O}{\rightsquigarrow}{}^{\mathsf{R}}_{\overline{\tau}''} X''_{\mathsf{R}}$
(b) $\Sigma'_{\mathsf{R}} \cong \Sigma''_{\mathsf{R}}$
(c) $X'_{\mathsf{R}} \cong X''_{\mathsf{R}}$ and $\overline{\rho}' = \varnothing$
(d) $\Sigma'_{\mathsf{R}} \approx X'_{\mathsf{R}}$ and $\Sigma''_{\mathsf{R}} \approx X''_{\mathsf{R}}$
(e) $\overline{\tau}' = \overline{\tau}''$

We proceed by inversion on $\approx$ in $\Sigma'_{\mathsf{R}} \approx X'_{\mathsf{R}}$ and $\Sigma''_{\mathsf{R}} \approx X''_{\mathsf{R}}$:

v5-com-single-base We thus have $\Sigma'_{\mathsf{R}} \sim X'_{\mathsf{R}} \restriction_{com}$ and $INV(\Sigma'_{\mathsf{R}}, X'_{\mathsf{R}})$ (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 $X'_{\mathsf{R}} \cong X''_{\mathsf{R}}$.

Notice that if $minWndw(X'_{\mathsf{R}}) = 0$ 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 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states) using Lemma 91 (R: Soundness Single Step AM).

v5-com-single-oracle We thus have

$$\begin{aligned}
X'_{\mathsf{R}} =& X_{\mathsf{R}3} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \cdot \langle p, ctr', \sigma, \mathbb{R}', h, n''' \rangle^{l} \\
\Sigma'_{\mathsf{R}} =& \Sigma_{\mathsf{R}3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle \cdot \Sigma_{\mathsf{R}4} \\
X_{\mathsf{R}} =& X_{\mathsf{R}3} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \\
\Sigma_{\mathsf{R}} =& \Sigma_{\mathsf{R}3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \\
\Sigma_{\mathsf{R}} \sim& X_{\mathsf{R}} \restriction_{com}
\end{aligned}$$

The form of X''_{R} and Σ''_{R} is analogous.

The case is analogous to the corresponding case in Lemma 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

v5-com-single-rollback We have

$$\begin{aligned}
X'_{\mathsf{R}} =& X_{\mathsf{R}3} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0 \rangle^{l} \cdot X_{\mathsf{R}4} \\
\Sigma'_{\mathsf{R}} =& \Sigma_{\mathsf{R}3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle^{l} \cdot \Sigma_{\mathsf{R}4} \\
X_{\mathsf{R}} =& X_{\mathsf{R}3} \cdot \langle p, ctr, \sigma, h, \mathbb{R}, n'' \rangle \\
\Sigma_{\mathsf{R}} =& \Sigma_{\mathsf{R}3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \\
\Sigma_{\mathsf{R}} \sim& X_{\mathsf{R}} \restriction_{com} \\
n' \geq& 0
\end{aligned}$$

The form of X''_{R} and Σ''_{R} is analogous.

Additionally we know that the transaction terminates in some state $\Sigma_{\mathsf{R}} \Downarrow^{\overline{\tau}}_{\mathsf{R}} \Sigma'''_{\mathsf{R}}$. There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma'_{\mathsf{R}} \overset{\tau}{=\!\!\!\rightsquigarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}1}$ 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 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

$n' = 0$ Then we know that $\Sigma'_{\mathsf{R}} \overset{\tau}{=\!\!\!\rightsquigarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}1}$ was created by Rule R:AM-Rollback and is a rollback for ctr.

I Here we prove that $X'_{\mathsf{R}} \overset{O}{\xrightsquigarrow{\tau_0}}_{\mathsf{R}} X'_{\mathsf{R}1}$ and $X''_{\mathsf{R}} \overset{O}{\xrightsquigarrow{\tau_1}}_{\mathsf{R}} X'_{\mathsf{R}2}$.

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 $X'_{\mathsf{R}} \overset{O}{\xrightsquigarrow{\tau_0}}_{\mathsf{R}} X'_{\mathsf{R}1}$ and $X''_{\mathsf{R}} \overset{O}{\xrightsquigarrow{\tau_1}}_{\mathsf{R}} X'_{\mathsf{R}2}$ are derived by Rule R:SE-Rollback.

The rest of the case is analogous to the corresponding case Lemma 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

□

Lemma 91 (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, $\Sigma_{\mathsf{R}1} = \Sigma'_{\mathsf{R}} \cdot \Phi'_{\mathsf{R}}$, $\Sigma_{\mathsf{R}2} = \Sigma''_{\mathsf{R}} \cdot \Phi''_{\mathsf{R}}$ be two speculative states for the always mispredict semantics and $X_{\mathsf{R}1}, X_{\mathsf{R}2}$, be two speculative states for the speculative semantics.*

If the following conditions hold:

(1) $\Sigma_{\mathsf{R}1} \cong \Sigma_{\mathsf{R}2}$
(2) $X_{\mathsf{R}1} \cong X_{\mathsf{R}2}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma_{\mathsf{R}1} \approx X_{\mathsf{R}1}$ *and* $\Sigma_{\mathsf{R}2} \approx X_{\mathsf{R}2}$
(4) $\Phi'_{\mathsf{R}} \overset{\tau''}{\Longrightarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}1}$ *and* $\Phi''_{\mathsf{R}} \overset{\tau''}{\Longrightarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}2}$

then there are instances $X'_{\mathsf{R}1}, X'_{\mathsf{R}2}$ for the speculative semantics such that:

I $X_{\mathsf{R}1} \overset{O}{\underset{\tau}{\rightsquigarrow}}{}_{\mathsf{R}} X'_{\mathsf{R}1}$ *and* $X_{\mathsf{R}2} \overset{O}{\underset{\tau'}{\rightsquigarrow}}{}_{\mathsf{R}} X'_{\mathsf{R}2}$
II $\Sigma'_{\mathsf{R}1} \cong \Sigma'_{\mathsf{R}2}$
III $X'_{\mathsf{R}1} \cong X'_{\mathsf{R}2}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{\mathsf{R}1} \approx X'_{\mathsf{R}1}$ *and* $\Sigma'_{\mathsf{R}2} \approx X'_{\mathsf{R}2}$
V $\tau = \tau'$

Proof. We proceed by inversion on $\Phi'_{\mathsf{R}} \overset{\tau''}{\Longrightarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}1}$ and $\Phi''_{\mathsf{R}} \overset{\tau''}{\Longrightarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}2}$:

Rule R:AM-General We choose $X'_{\mathsf{R}1} = X'_{\mathsf{R}}$ and $X'_{\mathsf{R}2} = X''_{\mathsf{R}}$. The case is analogous to the corresponding case in Lemma 65 (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 $X_{\mathsf{R}1} \overset{O}{\xrightsquigarrow{\tau_0}}_{\mathsf{R}} X'_{\mathsf{R}}$ and $X_{\mathsf{R}2} \overset{O}{\xrightsquigarrow{\tau_1}}_{\mathsf{R}} X''_{\mathsf{R}}$.

Furthermore, we execute Rule R:SE-General twice, because Rule R:SE-Ret created two observations in $\overline{\rho}$. We now have $X'_{\mathsf{R}1} = X'_{\mathsf{R}}$ 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 $X_{\mathsf{R}1} \overset{O}{\underset{\tau}{\rightsquigarrow}}{}_{\mathsf{R}} X'_{\mathsf{R}1}$ and $X_{\mathsf{R}2} \overset{O}{\underset{\tau'}{\rightsquigarrow}}{}_{\mathsf{R}} X'_{\mathsf{R}2}$.

II By Lemma 86 (R AM: Single step preserves ≅).

III By Lemma 87 (R SE: Single step preserves ≅) for $X_{\mathsf{R}1} \overset{O}{\xrightsquigarrow{\tau_0}}_{\mathsf{R}} X'_{\mathsf{R}}$ and $X_{\mathsf{R}2} \overset{O}{\xrightsquigarrow{\tau_1}}_{\mathsf{R}} X''_{\mathsf{R}}$ 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

$$
\begin{aligned}
X'_{\text{R}1} =& X'_{\text{R}3} \cdot \langle p, ctr, \sigma', \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n_0\rangle \\
\Sigma'_{\text{R}1} =& \Sigma_{\text{R}3} \cdot \langle p, ctr, \sigma', \mathbb{R}, n_1\rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', n_2\rangle \\
X'_{\text{R}4} =& X'_{\text{R}3} \cdot \langle p, ctr, \sigma', \mathbb{R}, h, n\rangle \\
\Sigma'_{\text{R}4} =& \Sigma_{\text{R}3} \cdot \langle p, ctr, \sigma', \mathbb{R}, n_1\rangle
\end{aligned}
$$

The case is analogous to the Rule S:AM-Store-Spec correct prediction case in Lemma 65 (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 $m, m' \in \mathit{Vals}$.

The case is analogous to the Rule S:AM-Store-Spec correct prediction case in Lemma 65 (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 $X'_{\text{R}} \overset{\tau_0}{\rightsquigarrow}{}^{O}_{\text{R}} X'_{\text{R}1}$ and $X''_{\text{R}} \overset{\tau_1}{\rightsquigarrow}{}^{O}_{\text{R}} X'_{\text{R}2}$.

Furthermore, we execute Rule R:SE-General twice, because Rule R:SE-Ret created two observations in $\overline{\rho}$. We now have $X'_{\text{R}1} = X'_{\text{R}}$ 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 $X_{\text{R}1} \;{}^{O}\!\!\rightsquigarrow^{\text{R}}_{\overline{\tau}} X'_{\text{R}1}$ and $X_{\text{R}2} \;{}^{O}\!\!\rightsquigarrow^{\text{R}}_{\overline{\tau}'} X'_{\text{R}2}$.

Notice that the observations in $\overline{\rho}$ are equal between $X_{\text{R}1}$ and $X_{\text{R}2}$, because of (2). We have $X_{\text{R}1}.ctr = X_{\text{R}2}.ctr$ and $X_{\text{R}1}.\sigma \sim_{\mathbf{pc}} X_{\text{R}2}.\sigma$ from our relation.

b) By Lemma 86 (R AM: Single step preserves $\cong$).

c) By Lemma 87 (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:

$$
\begin{aligned}
X'_{\text{R}1} =& X'_{\text{R}3} \cdot \langle p, ctr, \sigma', \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma''', \mathbb{R}', h', n_0\rangle \\
\Sigma'_{\text{R}1} =& \Sigma_{\text{R}3} \cdot \langle p, ctr, \sigma', \mathbb{R}, n_1\rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', n_2\rangle \\
X'_{\text{R}4} =& X'_{\text{R}3} \cdot \langle p, ctr, \sigma', \mathbb{R}, h, n\rangle \\
\Sigma'_{\text{R}4} =& \Sigma_{\text{R}3} \cdot \langle p, ctr, \sigma', \mathbb{R}, n_1\rangle
\end{aligned}
$$

The case is analogous to the Rule S:AM-Store-Spec correct prediction case in Lemma 65 (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

$$
\begin{aligned}
\overline{\tau} =& \texttt{ret}\ m \cdot \texttt{start}\ X_{\text{R}1}.ctr \cdot \texttt{ret}\ X_{\text{R}1}.\sigma(\mathbf{pc}) \\
\overline{\tau}' =& \texttt{ret}\ m' \cdot \texttt{start}\ X_{\text{R}2}.ctr \cdot \texttt{ret}\ X_{\text{R}2}.\sigma(\mathbf{pc})
\end{aligned}
$$

for some $m, m' \in \mathit{Vals}$.

The case is analogous to the misprediction case in Lemma 65 (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 65 (S: Soundness Single Step AM) using Lemma 86 (R AM: Single step preserves $\cong$) and Lemma 87 (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 $INV(\Sigma'_{\mathsf{R}1}, X'_{\mathsf{R}1})$ is analogous to the corresponding case in Lemma 65 (S: Soundness Single Step AM).

□

Definition 36 (R: Constructing the Oracle)**.** *Constructing the prediction oracle $O_{am}{}^{\mathsf{R}}$. We build our oracle based on the executions $\Sigma^{init}_{\mathsf{R}}(p,\sigma) \Downarrow^{\overline{\tau}}_{\mathsf{R}} \Sigma_{\mathsf{R}1} \overset{\tau_{am}}{\rightsquigarrow}_{\mathsf{R}} \Sigma_{\mathsf{R}2}, \Sigma^{init}_{\mathsf{R}}(p,\sigma') \Downarrow^{\overline{\tau}}_{\mathsf{R}} \Sigma'_{\mathsf{R}1} \overset{\tau'_{am}}{\rightsquigarrow}_{\mathsf{R}} \Sigma'_{\mathsf{R}2}$ where $\tau_{am} \neq \tau'_{am}$.*

Let us denote by the set RB the ids of all ongoing transaction ids in $\Sigma_{\mathsf{R}1}$. Since $\Sigma_{\mathsf{R}1} \cong \Sigma'_{\mathsf{R}1}$ we know that the same transaction ids are still ongoing in $\Sigma'_{\mathsf{R}1}$ 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:

$$O_{am}{}^{\mathsf{R}}(p,n,h) = \begin{cases} (\omega) \ \textit{if}\ |h| \in RB \wedge p(\sigma(\mathbf{pc})) = \mathbf{ret} \\ (0) \ \textit{otherwise (where } p(\sigma(\mathbf{pc})) = \mathbf{ret}) \end{cases}$$

Note that we use the length of h to reconstruct the ctr. Both start at 0 and are increased when 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 37 (R: Relation between AM and Spec for oracles that only mispredict)**.** *We define a relation $\approx^{\Sigma States}_{O_{am}{}^{\mathsf{R}}}$ between AM and oracle semantics.*

$$\boxed{\Sigma_{\mathsf{R}} \approx^{\Sigma States}_{O_{am}{}^{\mathsf{R}}} X_{\mathsf{R}}}$$

$$\textit{(Base-Oracle)}\ \frac{}{\varnothing \approx^{\Sigma States}_{O_{am}{}^{\mathsf{R}}} \varnothing} \qquad \textit{(Single-Base-Oracle)}\ \frac{\Sigma_{\mathsf{R}} \sim X_{\mathsf{R}}\restriction_{com} \quad INV2(\Sigma_{\mathsf{R}}, X_{\mathsf{R}}) \quad minWndw(X_{\mathsf{R}}) > 0}{\Sigma_{\mathsf{R}} \approx^{\Sigma States}_{O_{am}{}^{\mathsf{R}}} X_{\mathsf{R}}}$$

$$\textit{(Single-Transaction-Rollback-Oracle)}\ \frac{\begin{array}{c}\Sigma''_{\mathsf{R}} \sim X''_{\mathsf{R}}\restriction_{com} \quad n' \geq 0 \quad \Sigma''_{\mathsf{R}} \Downarrow^{\overline{\tau}}_{\mathsf{R}} \Sigma'''_{\mathsf{R}} \textit{ where transaction with id ctr is rolled back} \\ X_{\mathsf{R}} = X'_{\mathsf{R}} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \quad \Sigma_{\mathsf{R}} = \Sigma'_{\mathsf{R}} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \quad INV2(\Sigma_{\mathsf{R}}, X_{\mathsf{R}})\end{array}}{\Sigma'_{\mathsf{R}} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}' n' \rangle^{false} \cdot \Sigma_{\mathsf{R}1} \approx^{\Sigma States}_{O_{am}{}^{\mathsf{R}}} X'_{\mathsf{R}} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0 \rangle^{false}}$$

We again, showed here an instantiated version of a more general version of the relation for easier explanation. The more general version can be found in Definition 44 (Relation between AM and Spec for oracles that only mispredict).

Lemma 92 (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) $(p, \sigma) \Omega_{R}^{\omega} \overline{\tau}$ *and* $(p, \sigma') \Omega_{R}^{\omega} \overline{\tau}'$ *and*
(2) $\overline{\tau} \neq \overline{\tau}'$

Then there exists an oracle O *such that*

I $(p, \sigma) \Omega_{R}^{O} \overline{\tau}_1$ *and* $(p, \sigma') \Omega_{R}^{O} \overline{\tau}'_1$ *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) $(p, \sigma) \Omega_{R}^{\omega} \overline{\tau}$ and $(p, \sigma') \Omega_{R}^{\omega} \overline{\tau}'$ and
(2) $\overline{\tau} \neq \overline{\tau}'$

By definition of $() \Omega_{R}^{\omega}$ 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:

$$\Sigma_{R}^{init}(p, \sigma) \Downarrow_{R}^{\overline{\tau}} \Sigma_{R1} \xrightarrow{\tau_{am}}_{R} \Sigma_{R2} \Downarrow_{R}^{\overline{\tau}_{end}} \Sigma_{RF}$$

$$\Sigma_{R}^{init}(p, \sigma') \Downarrow_{R}^{\overline{\tau}} \Sigma'_{R1} \xrightarrow{\tau'_{am}}_{R} \Sigma'_{R2} \Downarrow_{R}^{\overline{\tau}'_{end}} \Sigma'_{RF}$$

We claim that there is a prediction oracle O with a 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 $INV2(X_{R1}, \Sigma_{R1})$ and
b $X_{R}^{init}(p, \sigma') \overset{O}{\rightsquigarrow}_{v}^{R} X'_{R1}$ and $X'_{R1}.\sigma = \Sigma'_{R1}.\sigma$ and $INV2(X'_{R1}, \Sigma'_{R1})$
c $X_{R1} \cong X'_{R1}$

We get this by applying Lemma 94 (R:Stronger Soundness for a specific oracle and for specific executions) on the Am execution up to the point of the difference i.e., $\Sigma_{R}^{init}(p, \sigma) \Downarrow_{R}^{\overline{\tau}} \Sigma_{R1}$ and Σ_1^{States} being all the states in $\Sigma_{R}^{init}(p, \sigma) \Downarrow_{R}^{\overline{\tau}} \Sigma_{R1}$ (similar for Σ_2^{States} for $\Sigma_{R}^{init}(p, \sigma') \Downarrow_{R}^{\overline{\tau}} \Sigma'_{R1}$).

We now show that $\Sigma_{R1} \approx_{O_{am}{}^{R}}^{\Sigma_1^{States}} X_{R1}$ is derived by Rule Single-Base-Oracle (similar for $\Sigma_{R2} \approx_{O_{am}{}^{R}}^{\Sigma_2^{States}} X_{R2}$).

We do a case distinction if there are ongoing transactions in X_{R1} or not

no ongoing transactions in X_{R1} Then $\Sigma_{R1} \approx_{O_{am}{}^{R}}^{\Sigma_1^{States}} X_{R1}$ can only be derived Rule Single-Base-Oracle and Σ_{R1} has no ongoing transactions as well. Then we have by $INV2(\Sigma_{R1}, X_{R1})$ 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 $O_{am}{}^{R}$ 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 $\Sigma_{R1} \approx_{O_{am}{}^{R}}^{\Sigma_1^{States}} X_{R1}$ 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 $X_{R1} \approx_{O_{am}{}^{R}}^{\Sigma_1^{States}} \Sigma_{R1}$ by Rule Single-Base-Oracle.

We now proceed by case analysis on the rule in $\overset{}{\rightsquigarrow}_{\mathsf{R}}$ used to derive $\Sigma_{\mathsf{R}1} \xrightarrow{\tau_{am}}_{\mathsf{R}} \Sigma_{\mathsf{R}2}$. Because $\Sigma_{\mathsf{R}1} \cong \Sigma'_{\mathsf{R}1}$ and $\overline{\tau}_1 = \overline{\tau}'_1$, we know that the same rule was used in $\Sigma'_{\mathsf{R}1} \xrightarrow{\tau'_{am}}_{\mathsf{R}} \Sigma'_{\mathsf{R}2}$ as well.

Rule R:AM-Rollback Contradiction. Because $\Sigma_{\mathsf{R}1} \cong \Sigma'_{\mathsf{R}1}$ 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 $\Sigma_{\mathsf{R}1} \xrightarrow{\tau_{am}}_{\mathsf{R}} \Sigma_{\mathsf{R}2}$ we have $\Sigma_{\mathsf{R}1} = \overline{\Phi}_{\mathsf{R}} \cdot \Phi_{\mathsf{R}}$ and $\Sigma_{\mathsf{R}2} = \overline{\Phi}_{\mathsf{R}} \cdot \overline{\Phi}'_{\mathsf{R}}$ with $\Phi_{\mathsf{R}} \xrightarrow{\tau_{am}}_{\mathsf{R}} \overline{\Phi}'_{\mathsf{R}}$.

We now do inversion on $\Sigma_{\mathsf{R}1} \xrightarrow{\tau_{am}}_{\mathsf{R}} \Sigma_{\mathsf{R}2}$ and $\Phi_{\mathsf{R}} \xrightarrow{\tau_{am}}_{\mathsf{R}} \overline{\Phi}'_{\mathsf{S}}$:

Rule R:AM-General Contradiction. By $\Sigma_{\mathsf{R}1} \cong \Sigma'_{\mathsf{R}1}$ we know that $\Sigma_{\mathsf{R}1}.\overline{\rho} = \Sigma'_{\mathsf{R}1}.\overline{\rho}$.

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-Ret-Same, Rule R:AM-Ret-Empty, Rule R:AM-Call-Full, Rule R:AM-Call Contradiction.

Since $\Sigma_{\mathsf{R}1} \cong \Sigma'_{\mathsf{R}1}$ we know the same instruction is executed.

However Rule R:AM-Ret-Same, Rule R:AM-Ret-Empty only produce `ret` observations, which would contradict $\tau_{am} \neq \tau'_{am}$.

Similarly, Rule R:AM-Call-Full, Rule R:AM-Call produce `call` f observations again contradicting our assumption $\tau_{am} \neq \tau'_{am}$.

Rule R:AM-NoBranch and Rule R:AM-Ret-Spec We fulfill all assumptions for Lemma 93 (R: AM and Oracle coincide) and get $X_{\mathsf{R}1} \overset{\tau_{am}}{\rightsquigarrow}{}^{O}_{\mathsf{R}} X_{\mathsf{R}2}$ and $X'_{\mathsf{R}1} \overset{\tau'_{am}}{\rightsquigarrow}{}^{O}_{\mathsf{R}} X'_{\mathsf{R}2}$.

Since $\tau_{am} \neq \tau'_{am}$ by assumption we are finished.

This completes the proof of our claim.

□

Lemma 93 (R: AM and Oracle coincide). *If*

(1) $\Sigma_{\mathsf{R}} \approx^{\Sigma^{States}_{X_{\mathsf{R}}}}_{O_{am}\,\mathsf{R}}$ *by Base and*

(2) $\Sigma_{\mathsf{R}} \xrightarrow{\tau}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$ *and*

(3) $minWndw(\Sigma_{\mathsf{R}}) > 0$

(4) $X_{\mathsf{R}}.\overline{\rho} = \varnothing$

Then

(1) $X_{\mathsf{R}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{R}} X'_{\mathsf{R}}$

Proof. Since $minWndw(\Sigma_{\mathsf{R}}) > 0$ we know that the next step is not a rollback. From $minWndw(\Sigma_{\mathsf{R}}) > 0$ and $\Sigma_{\mathsf{R}} \approx^{\Sigma^{States}}_{O_{am}} X_{\mathsf{R}}$ we have $INV2(\Sigma_{\mathsf{R}}, X_{\mathsf{R}})$ and we get $minWndw(X_{\mathsf{R}}) > 0$ as well.

We proceed by inversion on $\Sigma_{\mathsf{R}} \xrightarrow{\tau}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$:

Rule R:AM-NoBranch From the rule, we have that $\Sigma_{\mathsf{R}}.\sigma \xrightarrow{\tau} \Sigma'_{\mathsf{R}}.\sigma$.

The case is analogous to the corresponding case in Lemma 67 (S: AM and Oracle coincide).

Rule R:AM-barr-spec, Rule R:AM-barr, Rule R:AM-Ret-Same, Rule R:AM-Ret-Empty, Rule R:AM-Call-Full, Rule R:AM-Call

From the rule, we have that $\Sigma_{\mathsf{R}}.\sigma \rightarrow \Sigma'_{\mathsf{R}}.\sigma$.

The case is analogous to the case above.

Rule R:AM-Ret-Spec Then, τ is generated by the step $\Sigma_{R}.\sigma \xrightarrow{\tau} \Sigma'_{R}.\sigma$ generated by Rule R:AM-Ret-Spec.

The case is analogous to the corresponding case in Lemma 67 (S: AM and Oracle coincide) using Rule R:SE-Ret

□

Lemma 94 (R: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 $O_{am}{}^{R}$ as it is defined by Definition 36 (R: 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) $\Sigma_{R1} \approx^{\Sigma_1^{States}}_{O_{am}{}^{R}} X_{R1}$ *and* $\approx^{\Sigma_1^{States}}_{O_{am}{}^{R}} \approx^{\Sigma_2^{States}}_{O_{am}{}^{R}} X_{R2}$

(4) $\Sigma_{R1} \Downarrow^{\overline{\tau}}_{R} \Sigma'_{R1}$ *and* $\Sigma_{R2} \Downarrow^{\overline{\tau}}_{R} \Sigma'_{R2}$

(5) $\Sigma_1^{States} = \Sigma_{SLS1} \Downarrow^{\overline{\tau}}_{SLS} \Sigma'_{SLS1}$ *and* $\Sigma_2^{States} = \Sigma_{SLS2} \Downarrow^{\overline{\tau}}_{SLS} \Sigma'_{SLS2}$

and our oracle is constructed in the way described above Then

I $X_{R1} \overset{O}{\rightsquigarrow}{}^{R}_{\overline{\tau}'} X'_{R1}, X_{R2} \overset{O}{\rightsquigarrow}{}^{R}_{\overline{\tau}''} X'_{R2}$

II $\Sigma'_{R1} \cong \Sigma'_{R2}$

III $X'_{R1} \cong X'_{R2}$ *and* $\overline{\rho} = \varnothing$

IV $\Sigma'_{R1} \approx^{\Sigma_1^{States}}_{O_{am}{}^{R}} X'_{R1}$ *and* $\Sigma'_{R2} \approx^{\Sigma_2^{States}}_{O_{am}{}^{R}} X'_{R2}$

V $\overline{\tau}' = \overline{\tau}''$

Proof. Notice that the proof is very similar to Lemma 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states). The only different thing 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 $\Sigma_{R1} \Downarrow^{\varepsilon}_{R} \Sigma'_{R}$ and $\Sigma_{R2} \Downarrow^{\varepsilon}_{R} \Sigma''_{R}$, 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 $X_{R1} \overset{O}{\rightsquigarrow}{}^{R}_{\varepsilon} X'_{R1}, X_{R2} \overset{O}{\rightsquigarrow}{}^{R}_{\varepsilon} X'_{R2}$ 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 $\Sigma'_{R} \overset{\tau}{\rightsquigarrow}_{R} \Sigma'_{R1}$ and $\Sigma_{R2} \Downarrow^{\overline{\tau}''}_{R} \Sigma''_{R}$ and $\Sigma''_{R} \overset{\tau}{\rightsquigarrow}_{R} \Sigma'_{R2}$.

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) $X_{R1} \overset{O}{\rightsquigarrow}{}^{R}_{\overline{\tau}'} X'_{R}, X_{R2} \overset{O}{\rightsquigarrow}{}^{R}_{\overline{\tau}''} X''_{R}$

(b) $\Sigma'_{R} \cong \Sigma''_{R}$

(c) $X'_{R} \cong X''_{R}$ and $\overline{\rho}' = \varnothing$

(d) $\Sigma'_{R} \approx^{\Sigma_1^{States}}_{O_{am}{}^{R}} X'_{R}$ and $\Sigma''_{R} \approx^{\Sigma_2^{States}}_{O_{am}{}^{R}} X''_{R}$

(e) $\overline{\tau}' = \overline{\tau}''$

We do a case distinction on $\approx^{\Sigma_1^{States}}_{O_{am}{}^{R}}$ in $\Sigma'_{R} \approx_{O_{am}} X'_{R}$ and $\Sigma''_{R} \approx^{\Sigma_2^{States}}_{O_{am}{}^{R}} X''_{R}$ by inversion:

v5-com-single-base We thus have $\Sigma'_{R} \sim X'_{R}\upharpoonright_{com}$, $minWndw(X'_{R}) > 0$ and $INV2(\Sigma'_{R}, X'_{R})$ (Similar for Σ''_{R} and X''_{R}).

We now proceed by inversion on the derivation $\Sigma'_{R} \stackrel{\tau}{\Longrightarrow}_{R} \Sigma'_{R1}$.

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 $\Phi_{R} \stackrel{\tau}{\Longrightarrow}_{R} \overline{\Phi}_{R}$ and $\Phi'_{R} \stackrel{\tau}{\Longrightarrow}_{R} \overline{\Phi}'_{R}$. We fulfill all conditions for Lemma 95 (R AM: Strong Soundness Single Step) which gives us the desired result.

v5-com-single-rollback We have

$$X'_{R} = X_{R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n'' \rangle \cdot \langle p, ctr', \sigma'', \mathbb{R}', h', 0 \rangle \cdot X_{R4}$$

$$\Sigma'_{R} = \Sigma_{R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle \cdot \Sigma_{R4}$$

$$X_{R} = X_{R3} \cdot \langle p, ctr, \sigma, h, n'' \rangle$$

$$\Sigma_{R} = \Sigma_{R3} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle$$

$$\Sigma_{R} \sim X_{R} \upharpoonright_{com}$$

$$INV2(\Sigma_{R}, X_{R})$$

$$n' \geq 0$$

The form of X''_{R} and Σ''_{R} is analogous.

The case is analogous to the corresponding case in Lemma 68 (S: Stronger Soundness for a specific oracle and for specific executions).

□

Lemma 95 (R AM: 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* $\overline{p} = \varnothing$
(3) $\Sigma_{R1} \approx^{\Sigma_1^{States}}_{O_{am}\,R} X_{R1}$ *and* $\Sigma_{R2} \approx^{\Sigma_2^{States}}_{O_{am}\,R} X_{R2}$
(4) $\Phi'_{R} \stackrel{\tau''}{\Longrightarrow}_{R} \Sigma'_{R1}$ *and* $\Phi''_{R} \stackrel{\tau''}{\Longrightarrow}_{R} \Sigma'_{R2}$
(5) $\Sigma'_{R1} \in \Sigma_1^{States}$ *and* $\Sigma'_{R1} \in \Sigma_2^{States}$

then there are instances X'_{R1}, X'_{R2} for the speculative semantics such that:

I $X_{R1} \overset{O}{\rightsquigarrow}{}^{R}_{\tau} X'_{R1}$ *and* $X_{R2} \overset{O}{\rightsquigarrow}{}^{R}_{\tau'} X'_{R2}$
II $\Sigma'_{R1} \cong \Sigma'_{R2}$
III $X'_{R1} \cong X'_{R2}$ *and* $\overline{p} = \varnothing$
IV $\Sigma'_{R1} \approx^{\Sigma_1^{States}}_{O_{am}\,R} X'_{R1}$ *and* $\Sigma'_{R2} \approx^{\Sigma_2^{States}}_{O_{am}\,R} X'_{R2}$
V $\tau = \tau'$

Proof. The proof is very similar to Lemma 65 (S: Soundness Single Step AM). The only different thing 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 $\mathit{INV2}(\Sigma'_{\mathsf{R}1}, X'_{\mathsf{R}1})$ holds in the different cases and leave the rest to the old soundness proof.

Now we do case distinction on the instruction executed:

not 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 $\mathit{INV2}(\Sigma'_{\mathsf{R}1}, X'_{\mathsf{R}1})$ still holds. The proof for $\mathit{INV2}(\Sigma'_{\mathsf{R}2}, X'_{\mathsf{R}2})$ is analogous.

The proof is analogous to the corresponding case 'not store instruction' in Lemma 68 (S: 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:

$$\begin{aligned}
X'_{\mathsf{R}1} =& X'''_{\mathsf{R}} \cdot \Psi_{\mathsf{R}} \\
minWndw(X'''_{\mathsf{R}}) =& minWndw(decr(X'_{\mathsf{R}})) = minWndw(X'_{\mathsf{R}}) - 1 \\
X'_{\mathsf{R}}.\sigma \xrightarrow{\tau}& X'''_{\mathsf{R}}.\sigma \\
\Sigma'_{\mathsf{R}1} =& \Sigma'''_{\mathsf{R}} \cdot \Phi_{\mathsf{R}} \\
\Sigma'''_{\mathsf{R}}.n =& \Sigma'_{\mathsf{R}}.n - 1 \\
\Sigma'_{\mathsf{R}}.\sigma \xrightarrow{\tau}& \Sigma'''_{\mathsf{R}}.\sigma
\end{aligned}$$

Note that the step $minWndw(decr(X'_{\mathsf{R}})) = minWndw(X'_{\mathsf{R}}) - 1$ comes from the fact that $minWndw(X'_{\mathsf{R}}) = \Sigma'_{\mathsf{R}}.n$ and $\Sigma_{\mathsf{R}}.n > 0$ by assumption.

Depending on the output of the oracle we switch the relation

$O(p, \sigma, h) = 0$ We need to show that $\mathit{INV2}(\Sigma'''_{\mathsf{R}}, X'''_{\mathsf{R}})$ holds. The argument is the same as above for not **ret** instructions.

$O(p, \sigma, h) = \omega$ We need to show that $\mathit{INV2}(\Sigma'''_{\mathsf{R}} \cdot \Phi_{\mathsf{R}}, X'''_{\mathsf{R}} \cdot \Phi_{\mathsf{R}})$ holds.

The case is analogous to the corresponding case (store misprediction) in Lemma 68 (S: Stronger Soundness for a specific oracle and for specific executions).

□

N SEMANTICS FOR $\mathcal{Q}_{\mathsf{SLS}}$

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.

N.1 $\rightsquigarrow_{\mathsf{SLS}}$: Always Mispredict Semantics

Speculative program states Σ_{SLS} are defined as stacks of Speculative instances $\overline{\Phi}_{\mathsf{SLS}}$. A speculation instance $\Phi_{\mathsf{SLS}} = \langle p, ctr, \sigma, n\rangle$ 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 $\perp$ when there is no speculative transaction ongoing.

$$\textit{Speculative States } \Sigma_{\mathsf{SLS}} ::= \overline{\Phi}_{\mathsf{SLS}}$$

$$\textit{Speculative Instance } \Phi_{\mathsf{SLS}} ::= \langle p, ctr, \sigma, n\rangle_{\overline{\rho}}$$

$$\tau ::= \mathtt{bypass}\ n \mid \mathtt{start}_{\mathsf{SLS}}\ ctr \mid \mathtt{rlb}_{\mathsf{SLS}}\ ctr$$

Judgements

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

Rule SLS:AM-Rollback only triggers when the $\overline{\rho}$ is empty.

$\boxed{\Sigma_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}}$

(SLS:AM-Context)
$$\frac{\Phi_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \overline{\Phi}'_{\mathsf{SLS}}}{\overline{\Phi}_{\mathsf{SLS}} \cdot \Phi_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \overline{\Phi}_{\mathsf{SLS}} \cdot \overline{\Phi}'_{\mathsf{SLS}}}$$

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

$\boxed{\Phi_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \overline{\Phi}'_{\mathsf{SLS}}}$

(SLS:AM-barr)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, \perp\rangle \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \langle p, ctr, \sigma', \perp\rangle}$$

(SLS:AM-barr-spec)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, n+1\rangle \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \langle p, ctr, \sigma', 0\rangle}$$

(SLS:AM-NoSpec)
$$\frac{p(\sigma(\mathbf{pc})) \neq \mathbf{ret}, \mathbf{spbarr}, Z \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, n+1\rangle \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \langle p, ctr, \sigma', n\rangle}$$

(SLS:AM-General)
$$\frac{\tau = \mathtt{bypass}\ n \mid \mathtt{start}_{\mathsf{SLS}}\ n}{\Phi_{\mathsf{SLS}\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \Phi_{\mathsf{SLS}\overline{\rho}}}$$

(SLS:AM-Spec)
$$\frac{\begin{array}{cc} p(\sigma(\mathbf{pc})) = \mathbf{ret} & \sigma \xrightarrow{\tau} \sigma' \\ \sigma'' = \sigma[\mathbf{pc} \mapsto \sigma(\mathbf{pc}) + 1] & j = min(\omega, n) \end{array}}{\langle p, ctr, \sigma, n+1\rangle_{\varepsilon} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \langle p, ctr, \sigma', n\rangle_{\varepsilon} \cdot \langle p, ctr+1, \sigma'', j\rangle_{\varepsilon\cdot\mathtt{bypass}\ \sigma(\mathbf{pc})\cdot\mathtt{start}_{\mathsf{SLS}}\ ctr}}$$

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

(SLS:AM-Reflection)
$$\frac{}{\Sigma_{\mathsf{SLS}} \Downarrow^{\varepsilon}_{\mathsf{SLS}} \Sigma_{\mathsf{SLS}}}$$

(SLS:AM-Single)
$$\frac{\Sigma_{\mathsf{SLS}} \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma''_{\mathsf{SLS}} \qquad \Sigma''_{\mathsf{SLS}} \xrightarrow{\tau}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}}{\Sigma_{\mathsf{SLS}} \Downarrow^{\overline{\tau}\cdot\tau}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}}$$

$\boxed{Helpers}$

(SLS:AM-Init)
$$\frac{\Sigma_{\mathsf{SLS}} = \langle p, 0, \sigma, \bot\rangle \qquad \sigma \in \mathit{InitConf}}{\vdash \Sigma_{\mathsf{SLS}} : \mathit{init}}$$

(SLS:AM-Fin)
$$\frac{\Sigma_{\mathsf{SLS}} = \langle p, \mathit{ctr}, \sigma, \bot\rangle \qquad \sigma(\mathbf{pc}) = \bot}{\vdash \Sigma_{\mathsf{SLS}} : \mathit{fin}}$$

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

$\boxed{p \times \mathit{InitConf} \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}}$

(SLS:AM-Trace)
$$\frac{\exists \Sigma'_{\mathsf{SLS}} \qquad \vdash \Sigma'_{\mathsf{SLS}} : \mathit{fin} \qquad \Sigma^{0}_{\mathsf{SLS}}(p, \sigma) \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}}{p, \sigma \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}}$$

(SLS:AM-Beh)
$$\frac{}{\mathit{Beh}^{\omega}_{\mathsf{SLS}}(p) = \{\overline{\tau} \mid \forall \sigma \in \mathit{InitConf}.\ p, \sigma \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}\}}$$

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

N.2 $\rightsquigarrow_{\mathsf{SLS}}$: Oracle Semantics

We use an oracle O to decide if a **ret** 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:

$$\mathit{Speculative\ States}\ X_{\mathsf{SLS}} ::= \overline{\Psi}_{\mathsf{SLS}}$$

$$\mathit{Speculative\ Instance}\ \Psi_{\mathsf{SLS}} ::= \langle p, \mathit{ctr}, \sigma, h, n\rangle^{b}_{p} \text{ where } b \in \{\text{true}, \text{false}, \varepsilon\}$$

$$\tau ::= ..\ |\ \mathtt{commit}_{\mathsf{SLS}}\ \mathit{ctr}$$

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.

$\boxed{Judgements}$

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

$\boxed{X_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X'_{\mathsf{SLS}}}$

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

(SLS:Rollback)
$$\frac{n' = 0 \text{ or p is stuck}}{\overline{\Psi}_{\mathsf{SLS}} \cdot \langle p, ctr, \sigma, h, n \rangle \cdot \langle p, ctr', \sigma', h', n' \rangle^{true} \cdot \overline{\Psi}'_{\mathsf{SLS}} \xrightarrow{\mathtt{rlb}_{\mathsf{SLS}}\ ctr}{}^{O}_{\mathsf{SLS}} \overline{\Psi}_{\mathsf{SLS}} \cdot \langle p, ctr', \sigma, h, n \rangle}$$

(SLS:Commit)
$$\frac{}{\overline{\Psi}_{\mathsf{SLS}} \cdot \langle p, ctr, \sigma, h, n \rangle^{b} \cdot \langle p, ctr', \sigma', h', 0 \rangle^{false} \cdot \overline{\Psi}_{\mathsf{SLS}}{}' \xrightarrow{\mathtt{commit}_{\mathsf{SLS}}\ ctr}{}^{O}_{\mathsf{SLS}} \overline{\Psi}_{\mathsf{SLS}} \cdot \langle p, ctr', \sigma', h', n \rangle^{b} \cdot \overline{\Psi}_{\mathsf{SLS}}{}'}$$

(SLS:General)
$$\frac{\tau = \mathtt{bypass}\ n \mid \mathtt{start}_{\mathsf{SLS}}\ n}{\overline{\Psi}_{\mathsf{SLS}} \cdot \Psi_{\mathsf{SLS}\overline{\rho}\cdot\tau} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} \overline{\Psi}_{\mathsf{SLS}} \cdot \Psi_{\mathsf{SLS}\overline{\rho}}}$$

$\boxed{\Psi_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} \Psi'_{\mathsf{SLS}}}$

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

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

(SLS:NoSpec)
$$\frac{p(\sigma(\mathbf{pc})) \neq \mathbf{ret}, \mathbf{spbarr} \qquad \sigma \xrightarrow{\tau} \sigma'}{\langle p, ctr, \sigma, h, n+1 \rangle \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} \langle p, ctr, \sigma', h, n \rangle}$$

(SLS:Spec)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{ret} \qquad \sigma \xrightarrow{\tau} \sigma' \qquad O(p, n, h) = (true, \omega) \\ l = \sigma(\mathbf{pc}) + 1 \qquad \sigma'' = \sigma[\mathbf{pc} \mapsto l] \qquad h' = h \cdot \langle \sigma(\mathbf{pc}), true \rangle}{\langle p, ctr, \sigma, h, n+1 \rangle \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} \langle p, ctr, \sigma', h', n \rangle \cdot \langle p, ctr+1, \sigma'', h', \omega \rangle^{true}_{\mathtt{bypass}\ \sigma(\mathbf{pc}) \cdot \mathtt{st}\ (ctr)}}$$

(SLS:Spec-Exe)
$$\frac{p(\sigma(\mathbf{pc})) = \mathbf{ret} \qquad \sigma \xrightarrow{\tau} \sigma' \qquad O(p, n, h) = (false, \omega) \\ h' = h \cdot \langle \sigma(\mathbf{pc}), false \rangle}{\langle p, ctr, \sigma, h, n+1 \rangle \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} \langle p, ctr, \sigma', h, n \rangle \cdot \langle p, ctr+1, \sigma', h', \omega \rangle^{false}_{\mathtt{st}\ (ctr)}}$$

$\boxed{X_{\mathsf{SLS}}\ {}^{O}\!\!\rightsquigarrow^{\mathsf{SLS}}_{\overline{\tau}} X'_{\mathsf{SLS}}}$

(SLS:Reflection)
$$\frac{}{X_{\mathsf{SLS}}\ {}^{O}\!\!\rightsquigarrow^{\mathsf{SLS}}_{\varepsilon} X_{\mathsf{SLS}}}$$

(SLS:Single)
$$\frac{X_{\mathsf{SLS}}\ {}^{O}\!\!\rightsquigarrow^{\mathsf{SLS}}_{\overline{\tau}} X''_{\mathsf{SLS}} \qquad X''_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X'_{\mathsf{SLS}}}{X_{\mathsf{SLS}}\ {}^{O}\!\!\rightsquigarrow^{\mathsf{SLS}}_{\overline{\tau}\cdot\tau} X'_{\mathsf{SLS}}}$$

$\boxed{Helpers}$

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

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

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

$$\boxed{p \times InitConf \Downarrow^{O}_{\mathsf{SLS}} \overline{\tau}}$$

(SLS:SE-Trace)
$$\frac{\exists X'_{\mathsf{SLS}} \quad \vdash X'_{\mathsf{SLS}} : \mathit{fin} \qquad X^{init}_{\mathsf{S}}(p,\sigma) \;{}^{O}\!\rightsquigarrow^{\mathsf{SLS}}_{\overline{\tau}}\; X'_{\mathsf{SLS}}}{p, \sigma \Downarrow^{O}_{\mathsf{SLS}} \overline{\tau}}$$

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

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

N.3 $\Downarrow_{\mathsf{SLS}}$: 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 $\Sigma^{\mathcal{S}}_{\mathsf{SLS}}$.

$$\boxed{\Sigma^{\mathcal{S}}_{\mathsf{SLS}} \xRightarrow{\tau}{}^{\mathcal{S}}_{\mathsf{SLS}} \Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}'}$$

(SLS:Sym-Context)
$$\frac{\Phi^{\mathcal{S}}_{\mathsf{SLS}} \xRightarrow{\tau}{}^{\mathcal{S}}_{\mathsf{SLS}} \overline{\Phi}'_{\mathsf{SLS}_{\mathcal{S}}}}{\overline{\Phi}_{\mathsf{SLS}_{\mathcal{S}}} \cdot \Phi^{\mathcal{S}}_{\mathsf{SLS}} \xRightarrow{\tau}{}^{\mathcal{S}}_{\mathsf{SLS}} \overline{\Phi}_{\mathsf{SLS}_{\mathcal{S}}} \cdot \overline{\Phi}'_{\mathsf{SLS}_{\mathcal{S}}}}$$

(SLS:Sym-Rollback)
$$\frac{n' = 0 \text{ or p is stuck}}{\overline{\Phi}_{\mathsf{SLS}_{\mathcal{S}}} \cdot \langle p, ctr, \sigma_{\mathcal{S}}, n\rangle \cdot \langle p, ctr', \sigma'_{\mathcal{S}}, n'\rangle \xRightarrow{\texttt{rlb}_{\mathsf{SLS}}\ ctr}{}^{\mathcal{S}}_{\mathsf{SLS}} \overline{\Phi}_{\mathsf{SLS}_{\mathcal{S}}} \cdot \langle p, ctr', \sigma_{\mathcal{S}}, n\rangle}$$

$$\boxed{\Phi^{\mathcal{S}}_{\mathsf{SLS}} \xRightarrow{\tau}{}_{\mathsf{SLS}} \overline{\Phi}'_{\mathsf{SLS}_{\mathcal{S}}}}$$

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

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

(SLS:Sym-NoSpec)
$$\frac{p(\sigma(\mathbf{pc})) \neq \mathbf{ret}, \mathbf{spbarr}, Z \qquad \sigma_{\mathcal{S}} \xrightarrow{\tau}_{\mathcal{S}} \sigma'_{\mathcal{S}}}{\langle p, ctr, \sigma_{\mathcal{S}}, n+1\rangle \xRightarrow{\tau}{}^{\mathcal{S}}_{\mathsf{SLS}} \langle p, ctr, \sigma'_{\mathcal{S}}, n\rangle}$$

(SLS:Sym-General)
$$\frac{\tau = \texttt{bypass}\ n \mid \texttt{start}_{\mathsf{SLS}}\ n}{\Phi^{\mathcal{S}}_{\mathsf{SLS}\,\overline{p}\cdot\tau} \xRightarrow{\tau}{}^{\mathcal{S}}_{\mathsf{SLS}} \Phi^{\mathcal{S}}_{\mathsf{SLS}\,\overline{p}}}$$

(SLS:Sym-Spec)
$$\frac{\begin{array}{cc} p(\sigma(\mathbf{pc})) = \mathbf{ret} & \sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}} \\ \sigma''_{\mathcal{S}} = \sigma[\mathbf{pc} \mapsto \sigma(\mathbf{pc})+1] \qquad \sigma''_{\mathcal{S}}.\delta^{\mathcal{S}} = \sigma'_{\mathcal{S}}.\delta^{\mathcal{S}} & j = min(\omega, n) \end{array}}{\langle p, ctr, \sigma_{\mathcal{S}}, n+1\rangle_{\overline{p}} \xRightarrow{\tau}{}^{\mathcal{S}}_{\mathsf{SLS}} \langle p, ctr, \sigma'_{\mathcal{S}}, n\rangle_{\overline{p}} \cdot \langle p, ctr+1, \sigma'', j\rangle_{\overline{p}\cdot\texttt{bypass}\ \sigma(\mathbf{pc})\cdot\texttt{start}_{\mathsf{SLS}}\ ctr}}$$

$$\boxed{\Sigma^{\mathcal{S}}_{\mathsf{SLS}}\ {}_{\mathcal{S}}\!\Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}'}$$

(SLS:Sym-Reflection)
$$\frac{}{\Sigma^{\mathcal{S}}_{\mathsf{SLS}}\ {}_{\mathcal{S}}\!\Downarrow^{\varepsilon}_{\mathsf{SLS}} \Sigma^{\mathcal{S}}_{\mathsf{SLS}}}$$

(SLS:Sym-Single)
$$\frac{\Sigma_{\mathsf{SLS}}\ {}_{\mathcal{S}}\!\Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma''_{\mathsf{SLS}} \qquad \Sigma''_{\mathsf{SLS}} \xRightarrow{\tau}{}^{\mathcal{S}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}}{\Sigma^{\mathcal{S}}_{\mathsf{SLS}}\ {}_{\mathcal{S}}\!\Downarrow^{\overline{\tau}\cdot\tau_{\mathcal{S}}}_{\mathsf{SLS}} \Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}'}$$

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

$\boxed{Helpers}$

$$\frac{\Sigma^{\mathcal{S}}_{\mathsf{SLS}} = \langle p, 0, \sigma_{\mathcal{S}}, \bot\rangle \qquad \sigma_{\mathcal{S}} \in \mathit{InitConf}}{\vdash \Sigma^{\mathcal{S}}_{\mathsf{SLS}} : \mathit{init}}\ (\mathsf{SLS}\text{:Sym-Init}) \qquad \frac{\Sigma^{\mathcal{S}}_{\mathsf{SLS}} = \langle p, \mathit{ctr}, \sigma_{\mathcal{S}}, \bot\rangle \qquad \sigma_{\mathcal{S}}(\mathbf{pc}) = \bot}{\vdash \Sigma^{\mathcal{S}}_{\mathsf{SLS}} : \mathit{fin}}\ (\mathsf{SLS}\text{:Sym-Fin})$$

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

$\boxed{(p \times \mathit{InitConf})\ {}_{\mathcal{S}}\text{👻}^{\omega}_{\mathsf{SLS}}\ \overline{\tau}}$

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

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

O PROOFS FOR 👻_{SLS}:

Our main result for 👻_{SLS} is the following

Theorem 21 (👻_{SLS} is *WFSS*). $\vdash \text{👻}_{\mathsf{SLS}}$ *WFSS*

Proof. Immediately follows from Theorem 25 (SLS: Oracle Overapproximation), Theorem 24 (SLS: Symbolic Consistency), Theorem 23 (SLS: Behaviour of non-speculative semantics and AM semantics) and Theorem 22 (SLS SE: Behaviour of non-speculative and oracle semantics). ◻

O.1 SLS: Relating Non-speculative and Oracle Semantics

- Theorem 22 (SLS SE: Behaviour of non-speculative and oracle semantics)
  - Lemma 100 (SLS SE: Completeness of the speculative semantics)
    - Lemma 101 (SLS SE: Non-speculative execution for rolled back transactions)
  - Lemma 96 (SLS SE: Soundness of the speculative semantics w.r.t. non-speculative semantics)
    - Lemma 97 (SLS SE: Soundness single step No Speculation)
      - Lemma 98 (SLS SE: Single Step Instance Non Speculative)
    - Lemma 99 (SLS SE: Single Step Speculation)

Theorem 22 (SLS SE: Behaviour of non-speculative and oracle semantics). *Let p be a program and O be a prediction oracle. Then $Beh_{NS}(p) = Beh^{O}_{SLS}(p)\upharpoonright_{ns}$*

Proof. We prove the two directions separately:

$\Leftarrow$ By the definition of $Beh^{O}_{SLS}(p)$ we have an initial configuration σ such that $(p,\sigma)\ \Downarrow^{O}_{SLS}\ \overline{\tau}$.

By definition of $(p,\sigma)\ \Downarrow^{O}_{SLS}\ \overline{\tau}$, we know there exists a state X'_{SLS} such that $\vdash X'_{SLS} : fin$ and an initial state $X^{init}_{SLS}(p,\sigma)$ such that $X^{init}_{SLS}(p,\sigma)\ \overset{O}{\rightsquigarrow}{}^{SLS}_{\overline{\tau}} X'_{SLS}$.

Analogous to the corresponding case in Theorem 12 (S SE: Behaviour of non-speculative and oracle semantics) by using Lemma 96 (SLS SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

We thus have $((p,\sigma))\ \Downarrow_{NS}\overline{\tau}\upharpoonright_{ns} \in Beh_{NS}(p)$ by Rule NS-Trace.

$\Rightarrow$ Assume that $((p,\sigma))\ \Downarrow_{NS}\overline{\tau} \in Beh_{NS}(p)$. We thus know there exists $\sigma' \in FinalConf$ such that $\sigma \Downarrow_{\overline{\tau}} \sigma'$.

Analogous to the corresponding case in Theorem 12 (S SE: Behaviour of non-speculative and oracle semantics) by using Lemma 100 (SLS SE: Completeness of the speculative semantics).

We thus have $(p,\sigma)\ \Downarrow^{O}_{SLS}\ \overline{\tau}'\cdot\overline{\tau}'' \in Beh^{O}_{SLS}(p)$, where $\overline{\tau}''\upharpoonright_{ns} = \varepsilon$.

□

O.1.1 Soundness.

Lemma 96 (SLS SE: Soundness of the speculative semantics w.r.t. non-speculative semantics). *If*

(1) $X_{SLS}.\sigma = \sigma$ and

(2) $\vdash_O X_{SLS} : noongoing$ and

(3) $X_{SLS}\ \overset{O}{\rightsquigarrow}{}^{SLS}_{\overline{\tau}} X'_{SLS}$

Then there exists σ' such that

I if $\vdash_O X'_{SLS} : noongoing$ then $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}\sigma'}$ and $X'_{SLS}.\sigma = \sigma'$ and

II if $\vdash^{i}_{O} X'_{SLS} : biggestongoingtransactionirolledback$ 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 $X_{SLS}\ \overset{O}{\rightsquigarrow}{}^{SLS}_{\overline{\tau}} X'_{SLS}$

Rule SLS:Reflection Then we have $X_{SLS}\ \overset{O}{\rightsquigarrow}{}^{SLS}_{\varepsilon} X_{SLS}$ with $X'_{SLS} = X_{SLS}$ and by Rule NS-Reflection we have

I $\sigma \Downarrow_{\varepsilon\upharpoonright_{ns}} \sigma'$ with $\sigma = \sigma'$.

II $\sigma \Downarrow_{helper(\varepsilon,i)} \sigma'$ with $\sigma = \sigma'$.

Rule SLS:Single We have $X_{SLS}\ \overset{O}{\rightsquigarrow}{}^{SLS}_{\overline{\tau}'\cdot\tau} X'_{SLS}$ and by Rule SLS:Single we get $X_{SLS}\ \overset{O}{\rightsquigarrow}{}^{SLS}_{\overline{\tau}'} X''_{SLS}$ and $X''_{SLS} \overset{\tau}{\rightsquigarrow}{}^{O}_{SLS} X'_{SLS}$.

We need to proof

I if $\vdash_O X'_{SLS} : noongoing$ then $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ and $X'_{SLS}.\sigma = \sigma'$

II if $\vdash^{i}_{O} X'_{SLS} : biggestongoingtransactionirolledback$ 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 $X_{SLS}\ \overset{O}{\rightsquigarrow}{}^{SLS}_{\overline{\tau}'} X''_{SLS}$ and have a σ'' where σ'' is the configuration for some instance in X''_{SLS} such that.

I' if $\vdash_O X''_{SLS} : noongoing$ then $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}\sigma''}$ and $X''_{SLS}.\sigma = \sigma''$

II' if $\vdash^{j}_{O} X''_{\mathsf{SLS}}$: *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''_{SLS}.

no ongoing transactions in X''_{SLS} Then X''_{SLS} has no ongoing transactions, meaning $\vdash_{O} X''_{\mathsf{SLS}}$: *noongoing* and we have $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}} \sigma''$ and $X''_{\mathsf{SLS}}.\sigma = \sigma''$ by IH.

I Then $\vdash_{O} X'_{\mathsf{SLS}}$: *noongoing* and we need to prove $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ and $X'_{\mathsf{SLS}}.\sigma = \sigma'$. We now proceed by inversion on $X''_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X'_{\mathsf{SLS}}$:

Rule SLS:Rollback Analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

Rule SLS:Spec The contradiction is analogous to the case of Rule S:Store-Skip in Lemma 45 (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 $\sigma'' = X''_{\mathsf{SLS}}.\sigma$. Since $\vdash_{O} X''_{\mathsf{SLS}}$: *noongoing*, there no ongoing transactions that need to be rolled back.

Furthermore, no transaction that will be rolled back is created in the step $X''_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X'_{\mathsf{SLS}}$, because $\vdash_{O} X'_{\mathsf{SLS}}$: *noongoing*.

The case is analogous to Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) by using Lemma 97 (SLS SE: Soundness single step No Speculation).

II Then X'_{SLS} has ongoing transactions, meaning $\vdash^{i}_{O} X'_{\mathsf{SLS}}$: *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 $X''_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X'_{\mathsf{SLS}}$:

Rule SLS:Spec Since we know a new transaction was created that will be rolled back, we also know that $id = i$.

We know that, because $\vdash_{O} X''_{\mathsf{SLS}}$: *noongoing*, so there was not another ongoing transaction.

The case is analogous to Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) together with Lemma 99 (SLS SE: Single Step Speculation).

otherwise By definition of $\vdash^{i}_{O} X'_{\mathsf{SLS}}$: *biggestongoingtransactionirolledback* we know that there exists a $\texttt{rlb}_{\mathsf{SLS}}$ i in the execution $X'_{\mathsf{SLS}} \overset{O}{\Downarrow}{}^{\mathsf{SLS}}_{\overline{\tau}_{fin}} X_{\mathsf{SLS}\,fin}$ 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 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

ongoing transactions in X''_{SLS} Then X''_{SLS} has ongoing transactions, meaning $\vdash^{j}_{O} X''_{\mathsf{SLS}}$: *biggestongoingtransactionirolledback* and we have $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$ and σ'' is the configuration for the instance with $ctr = j$.

I Then $\vdash_{O} X'_{\mathsf{SLS}}$: *noongoing* and we need to prove $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ and $X'_{\mathsf{SLS}}.\sigma = \sigma'$. We now proceed by inversion on $X''_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X'_{\mathsf{SLS}}$:

Rule SLS:Rollback and $\tau = \texttt{rlb}_{\mathsf{SLS}}\ j$ Choose $\sigma' = \sigma''$. Since $\overline{\tau} \cdot \tau\upharpoonright_{ns} = helper(\overline{\tau}, j)$ we can use IH $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$.

Analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Then $\tau \neq \texttt{rlb}_{\mathsf{SLS}}\ j$.

Deriving the contradiction is analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

II Then $\vdash^{i}_{O} X'_{\mathsf{SLS}}$: *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 $X''_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X'_{\mathsf{SLS}}$:

Rule SLS:Rollback Then $\tau = \texttt{rlb}_{\mathsf{SLS}}\ id$. We do a case analysis if $id = j$ or not.

$id = j$ Contradiction, analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

$id \neq j$ Analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Then $\tau \neq \texttt{rlb}_{\mathsf{SLS}}\ id$.

Then $helper(\overline{\tau}\cdot\tau, i) = helper(\overline{\tau}, i)$

We choose $\sigma' = \sigma''$ and derive a step by Rule NS-Reflection.

The rest is analogous to Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

□

Lemma 97 (SLS SE: Soundness single step No Speculation)**.** *If*

(1) $\vdash_{O} X_{\mathsf{SLS}}$: *noongoing and*
(2) $X_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X'_{\mathsf{SLS}}$ *and*
(3) $\vdash_{O} X'_{\mathsf{SLS}}$: *noongoing and*
(4) $\sigma = X_{\mathsf{SLS}}.\sigma$

Then there exists σ' *such that*

I $\sigma \Downarrow_{\tau\upharpoonright_{ns}} \sigma'$ *and*
II $X'_{\mathsf{SLS}}.\sigma = \sigma'$

Proof. We proceed by inversion on $X_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X'_{\mathsf{SLS}}$:

Rule SLS:General Thus we have $X_{\mathsf{SLS}} = \overline{\Psi}_{\mathsf{SLS}} \cdot \Psi_{\mathsf{SLS}\overline{\rho}\cdot\tau}$ and $X'_{\mathsf{SLS}} = \overline{\Psi}_{\mathsf{SLS}} \cdot \Psi_{\mathsf{SLS}\overline{\rho}}$ with $\Psi_{\mathsf{SLS}}.\sigma = \sigma$.

By the definition of $\overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}}$ only Rule SLS:Spec and Rule SLS:Spec-Exe add observations to $\overline{\rho}$.

These observations are either $\texttt{start}\ id$ or $\texttt{bypass}\ n$.

By the definition of $\upharpoonright_{ns}$, we have $\tau\upharpoonright_{ns} = \varepsilon$.

Thus, we have $\sigma \Downarrow_{\varepsilon\upharpoonright_{ns}} \sigma$ by Rule NS-Reflection.

Rule SLS:Commit Then the generated observation is $\tau = \texttt{commit}\ id$. Furthermore, $\texttt{commit}\ id\upharpoonright_{ns} = \varepsilon$.

By the definition of the rule, we have $X_{\mathsf{SLS}}.\sigma = X'_{\mathsf{SLS}}.\sigma$ and with this we get $X'_{\mathsf{SLS}}.\sigma = \sigma$.

Thus, we can derive $\sigma \Downarrow_{\texttt{commit}\ id\upharpoonright_{ns}} \sigma$.

Rule SLS:Rollback Contradiction, since $\vdash_{O} X_{\mathsf{SLS}}$: *noongoing* and Definition 18 (Well orderedness of rollback and start).

Rule SLS:SE-Context We have $X_{\mathsf{SLS}} = \overline{\Psi}_{\mathsf{SLS}} \cdot \Psi_{\mathsf{SLS}}$ and $X'_{\mathsf{SLS}} = \overline{\Psi}''_{\mathsf{SLS}} \cdot \overline{\Psi}'_{\mathsf{SLS}}$ with $\Psi_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} \overline{\Psi}'_{\mathsf{SLS}}$. By Lemma 98 (SLS SE: Single Step Instance Non Speculative) we have $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma'$ with $\sigma = \Psi_{\mathsf{SLS}}.\sigma$ and $\overline{\Psi}'_{\mathsf{SLS}}.\sigma = \sigma'$.

□

Lemma 98 (SLS SE: Single Step Instance Non Speculative)**.** *If*

(1) $X_{\mathsf{SLS}} = \overline{\Psi}_{\mathsf{SLS}} \cdot \Psi_{\mathsf{SLS}}$ *and*
(2) $X'_{\mathsf{SLS}} = \overline{\Psi}_{\mathsf{SLS}} \cdot \overline{\Psi}'_{\mathsf{SLS}}$ *and* $\vdash_O X'_{\mathsf{SLS}} : noongoing$ *and*
(3) $\Psi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} \overline{\Psi}'_{\mathsf{SLS}}$ *and*
(4) $\sigma = \Psi_{\mathsf{SLS}}.\sigma$

Then there is a σ' *such that*

I $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma'$ *and*
II $\overline{\Psi}'_{\mathsf{SLS}}.\sigma = \sigma$

Proof. We proceed by case analysis on the rule used to derive $\Psi_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} \Psi'_{\mathsf{SLS}}$.

Rule SLS:barr or Rule SLS:barr-spec We have $p(\sigma(\mathbf{pc})) \neq \mathbf{ret}$ and $n \neq 0$. We show the proof for Rule SLS:barr, the proof for Rule SLS:barr-spec is analogous.
By Rule SLS:barr we know $\sigma \xrightarrow{\tau} \sigma'$ and $\Psi'_{\mathsf{SLS}} = \langle p, ctr, \sigma', h, n-1\rangle$.
Thus $\sigma' = \Psi'_{\mathsf{SLS}}.\sigma$ and $\tau = \varepsilon = \varepsilon\upharpoonright_{ns}$.

Rule SLS:NoSpec We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule and $\Psi'_{\mathsf{SLS}} = \langle p, ctr, \sigma', h, n-1\rangle$.
Thus, $\sigma' = \Psi'_{\mathsf{SLS}}.\sigma$.
Because the rule used the observation received from the step $\sigma \xrightarrow{\tau} \sigma'$, we have $\tau\upharpoonright_{ns} = \tau$ and are finished.

Rule SLS:Spec Contradiction, because there are no ongoing transactions in X'_{SLS} by the fact $\vdash_O X'_{\mathsf{SLS}} : noongoing$.

Rule SLS:Spec-Exe By definition $\overline{\Psi}'_4 = \langle p, ctr, \sigma', h, n\rangle \cdot \langle p, ctr', \sigma', h', n'\rangle_{\overline{p}}$. By premise of the rule we do the step $\sigma \xrightarrow{\tau'} \sigma'$.
The generated trace is $\tau = \tau'$ and $\tau\upharpoonright_{ns} = \tau'$.
Thus, the step $\sigma \xrightarrow{\tau'} \sigma'$ is what we look for and by construction $\overline{\Psi}'_4.\sigma = \sigma'$.

□

Lemma 99 (SLS SE: Single Step Speculation)**.** *If*

(1) $X_{\mathsf{SLS}} = \overline{\Psi}_{\mathsf{SLS}} \cdot \Psi_{\mathsf{SLS}}$ *and* $\vdash_O X_{\mathsf{SLS}} : noongoing$
(2) $X'_{\mathsf{SLS}} = \overline{\Psi}_{\mathsf{SLS}} \cdot \overline{\Psi}'_{\mathsf{SLS}}$ *and* $\vdash^i_O X'_{\mathsf{SLS}} : biggestongoingtransactionirolledback$ *and*
(3) $\Psi_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} \overline{\Psi}'_{\mathsf{SLS}}$ *and*
(4) $\sigma = \Psi_{\mathsf{SLS}}.\sigma$

Then

I $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma'$ *and*
II σ' *is the configuration for the instance with* $ctr = i$ *in* X'_{SLS}

Proof. We proceed by inversion on $\Psi_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} \overline{\Psi}'_{\mathsf{SLS}}$:

Rule SLS:AM-Spec Then we have

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

$$\overline{\Psi}'_{\mathsf{SLS}} = \langle p, ctr, \sigma', n\rangle \cdot \Psi'^{\;l}_{\mathsf{SLS}\,\mathtt{bypass}\ \sigma(\mathbf{pc})\cdot\mathtt{start}_{\mathsf{SLS}}\ ctr}$$

We have $\sigma \xrightarrow{\tau} \sigma'$.

Since $\vdash_{O} X_{\mathsf{SLS}}:$ *noongoing* we know that $\tau\upharpoonright_{ns} = \tau = \texttt{ret}\ l$.

Since a transaction with $id = ctr$ was started and we have $\vdash_{O} X_{\mathsf{SLS}}:$ *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 $\vdash_{O} X_{\mathsf{SLS}}:$ *noongoing* and $\vdash^{i}_{O} X'_{\mathsf{SLS}}:$ *biggestongoingtransactionirolledback*, we know that a transaction has to be started that will be rolled back.

□

O.1.2 Completeness.

Lemma 100 (SLS SE: Completeness of the speculative semantics)**.** *If*

(1) $\sigma \in InitConf$ *and*

(2) $\sigma \Downarrow_{\overline{\tau}} \sigma'$ *and*

(3) $X_{\mathsf{SLS}} = X^{init}_{\mathsf{SLS}}(\sigma)$

Then

I $X_{\mathsf{SLS}} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}'} X'_{\mathsf{SLS}\,\rho}$ *and*

II $\vdash_{O} X'_{\mathsf{SLS}}:$ *noongoing and*

III $\sigma' = X'_{\mathsf{SLS}}.\sigma$ *and*

IV $\overline{\tau} = \overline{\tau}'\upharpoonright_{ns}$ *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 SLS:Reflection we have $X_{\mathsf{SLS}} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\varepsilon} X_{\mathsf{SLS}}$.

By construction $\vdash_{O} X_{\mathsf{SLS}}:$ *noongoing* and $X_{\mathsf{SLS}}.\sigma = \sigma$.

Since $\varepsilon\upharpoonright_{ns} = \varepsilon$ we are finished.

Rule NS-Single Then we have $\sigma \Downarrow_{\overline{\tau}} \sigma''$ and $\sigma'' \xrightarrow{\tau} \sigma'$.

We need to show

I $X_{\mathsf{SLS}} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}'\cdot\tau'} X'_{\mathsf{SLS}}$ and

II $\vdash_{O} X'_{\mathsf{SLS}}:$ *noongoing* and

III $\sigma' = X'_{\mathsf{SLS}}.\sigma$ and

IV $\overline{\tau}\cdot\tau = \overline{\tau}'\cdot\tau'\upharpoonright_{ns}$

We apply the IH on $\sigma \Downarrow_{\overline{\tau}} \sigma''$ we get

I' $X_{\mathsf{SLS}} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}'} X''_{\mathsf{SLS}\,\rho}$ and

II' $\vdash_{O} X''_{\mathsf{SLS}\,\rho}:$ *noongoing* and

III' $\sigma'' = X''_{\mathsf{SLS}}.\sigma$ and

IV' $\overline{\tau} = \overline{\tau}'\upharpoonright_{ns}$

V' $\rho = \varepsilon$

To account for possible outstanding commits, we use Lemma 9 (Executing a chain of commits) on X''_{SLS} and get

a) $X''_{\mathsf{SLS}} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}'''} X'''_{\mathsf{SLS}}$

b) $minWndw(X'''_{\mathsf{SLS}}) > 0$

c) $\forall \tau \in \overline{\tau}'''. \tau = \texttt{commit}\ id$ for some $id \in \mathbb{N}$

d) $X''_{\mathsf{SLS}}.\sigma = X'''_{\mathsf{SLS}}.\sigma$

By c) and the definition of $\upharpoonright_{ns}$ we have $\overline{\tau}''' \upharpoonright_{ns} = \varepsilon$.

Because only Rule SLS:Commit was used we have $X'''_{\mathsf{SLS}\rho} = X''_{\mathsf{SLS}\rho}$. We now do a case analysis on the instruction $p(\sigma''(\mathbf{pc}))$:

$p(\sigma''(\mathbf{pc})) \neq \mathbf{ret}$ **I** Then either Rule SLS:barr, Rule SLS:barr-spec or Rule SLS:NoSpec in conjunction with Rule SLS:SE-Context was used to derive the step $X'''_{\mathsf{SLS}} \xrightarrow{\tau'}\!\!\!\rightsquigarrow^{O}_{\mathsf{SLS}} X'_{\mathsf{SLS}}$.

Here, τ' is generated from $X'''_{\mathsf{SLS}}.\sigma \xrightarrow{\tau'} \sigma'$ and $X'_{\mathsf{SLS}}.\sigma = \sigma'$

Since $\rightarrow$ is deterministic, we know that $\tau' = \tau$.

II Since no speculative transaction is started and we have $\vdash_O X''_{\mathsf{SLS}} : noongoing$ by IH and $\vdash_O X'''_{\mathsf{SLS}} : noongoing$, we have $\vdash_O X'_{\mathsf{SLS}} : noongoing$.

III By definition and determinism of $\rightarrow$.

IV Now we have $X''_{\mathsf{SLS}} \;{}^{O}\!\!\rightsquigarrow^{\mathsf{SLS}}_{\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau'} X'_{\mathsf{S}}$. Looking at the trace that is generated we have

$$
\begin{aligned}
& \overline{\tau}' \cdot \overline{\tau}''' \cdot \tau' \upharpoonright_{ns} \tau' = \tau \\
= & \overline{\tau}' \cdot \overline{\tau}''' \cdot \tau \upharpoonright_{ns} \tau \text{ generated by} \rightarrow \\
= & \overline{\tau}' \cdot \overline{\tau}''' \upharpoonright_{ns} \cdot \tau\ \overline{\tau}''' \upharpoonright_{ns} = \varepsilon \\
= & \overline{\tau}' \upharpoonright_{ns} \cdot \tau \text{ by IH} \\
= & \overline{\tau} \cdot \tau
\end{aligned}
$$

and thus, are finished.

$p(\sigma''(\mathbf{pc})) = \mathbf{ret}$ Then depending on the oracle decision, either Rule SLS:Spec or Rule SLS:Spec-Exe is used in conjunction with Rule SLS:SE-Context:

$O(p, n, h) = (false, \omega)$ **(Rule SLS:Spec-Exe)** Then we do not skip the **ret** instruction.

I We derive $X''_{\mathsf{SLS}} \;{}^{O}\!\!\rightsquigarrow^{\mathsf{SLS}}_{\tau \cdot \texttt{start}_{\mathsf{SLS}}\ id} X'_{\mathsf{SLS}}$ by using Rule SLS:Spec-Exe and produce the observation $\tau' = \tau$, where $\tau = \texttt{ret}\ l \in Obs$.

Afterwards, we need to discharge the observation in $\overline{\rho}$ that was generated by Rule SLS:Spec-Exe (which is always a $\texttt{start}_{\mathsf{SLS}}\ id$) using Rule SLS:General.

By Rule SLS:Spec-Exe, we know that the step $X'''_{\mathsf{SLS}}.\sigma \xrightarrow{\tau'} \sigma'$ is made.

II No speculative transaction was started that needs to be rolled back. By $\vdash_O X''_{\mathsf{SLS}} : noongoing$ and $\vdash_O X'''_{\mathsf{SLS}} : noongoing$ we get $\vdash_O X'_{\mathsf{SLS}} : noongoing$.

III By definition and determinism of $\rightarrow$.

IV We now have:

$$\begin{aligned}
&\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau' \cdot \texttt{start}_{\mathsf{SLS}}\ id \upharpoonright_{ns} \text{ Def. and } \overline{\tau}''' \upharpoonright_{ns} = \varepsilon \\
&= \overline{\tau}' \cdot \tau' \upharpoonright_{ns} \tau' = \tau \\
&= \overline{\tau}' \cdot \tau \upharpoonright_{ns} \tau \text{ generated by} \rightarrow \\
&= \overline{\tau}' \upharpoonright_{ns} \cdot \tau \text{ by IH} \\
&= \overline{\tau} \cdot \tau
\end{aligned}$$

and are finished.

$O(p, n, h) = (true, \omega)$ **(Rule SLS:Spec)** Then we skip the **ret** instruction.

I We derive a step by using Rule SLS:Spec.

This produces the observation τ'', where $\tau'' = \texttt{ret}\ m$ and the step $X'''_{\mathsf{SLS}}.\sigma \xrightarrow{\tau''} \sigma'''$ is made.

Since $\rightarrow$ is deterministic and the fact that $\sigma'' \xrightarrow{\tau''} \sigma'''$, $\sigma'' \xrightarrow{\tau} \sigma'$ and $X'''_{\mathsf{SLS}}.\sigma = \sigma''$, we have $\sigma''' = \sigma'$ and $\tau'' = \tau$.

Since Rule SLS:Spec pushes two observations into $\overline{\rho}$, Rule SLS:General applies twice and produces $\texttt{bypass}\ id$ and $\texttt{start}_{\mathsf{SLS}}\ id$.

We thus have $X'''_{\mathsf{SLS}} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\tau' \cdot \texttt{start}_{\mathsf{SLS}}\ id \cdot \texttt{bypass}\ n} X_{\mathsf{SLS}}3$.

Since all transactions are eventually closed, we know there exists X'_{SLS} such that $X^3_{\mathsf{SLS}} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}^n \cdot \texttt{rlb}_{\mathsf{SLS}}\ id} X'_{\mathsf{SLS}}$.

We now apply Lemma 101 (SLS SE: Non-speculative execution for rolled back transactions) on the execution $X'''_{\mathsf{SLS}} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\tau' \cdot \texttt{start}_{\mathsf{SLS}}\ id \cdot \texttt{bypass}\ n \cdot \overline{\tau}^n \cdot \texttt{rlb}_{\mathsf{SLS}}\ id} X'_{\mathsf{SLS}}$ and get $X'''_{\mathsf{SLS}}.\sigma \xrightarrow{\tau''} \sigma'$ and $X'_{\mathsf{SLS}}.\sigma = \sigma''$.

II Since the speculative transaction that was started was also rolled back and the fact that $\vdash_O X''_{\mathsf{SLS}} : noongoing$ by IH and $\vdash_O X'''_{\mathsf{SLS}} : noongoing$, we have $\vdash_O X'_{\mathsf{SLS}} : noongoing$.

III Follows by definition and I).

IV By definition $\tau'' \cdot \texttt{start}_{\mathsf{SLS}}\ id \cdots \texttt{rlb}_{\mathsf{SLS}}\ id \upharpoonright_{ns} = \tau'' \upharpoonright_{ns} = \tau''$.

$$\begin{aligned}
&\overline{\tau}' \cdot \overline{\tau}''' \cdot \tau'' \cdot \texttt{start}_{\mathsf{SLS}}\ id \cdot \overline{\tau}^n \cdot \texttt{rlb}_{\mathsf{SLS}}\ id \upharpoonright_{ns} \text{ Def. and } \overline{\tau}''' \upharpoonright_{ns} = \varepsilon \\
&= \overline{\tau}' \cdot \tau' \upharpoonright_{ns} \tau'' = \tau \\
&= \overline{\tau}' \cdot \tau \upharpoonright_{ns} \tau \text{ generated by} \rightarrow \\
&= \overline{\tau}' \upharpoonright_{ns} \cdot \tau \text{ by IH} \\
&= \overline{\tau} \cdot \tau
\end{aligned}$$

Notice that ρ is empty for all the cases, because we discharge all the observations immediately using Rule SLS:General.

□

Lemma 101 (SLS SE: Non-speculative execution for rolled back transactions.). *If*

(1) $X_{\mathsf{SLS}} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}} X'_{\mathsf{SLS}}$ *and*
(2) $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$ *and*
(3) $\sigma = X_{\mathsf{SLS}}.\sigma$

Then

I there is a configurations σ' *with* $X'_{\mathsf{SLS}}.\sigma = \sigma'$ *and*

II $\sigma \xrightarrow{\overline{\tau}\restriction_{ns}} \sigma'$ *and*

III $\overline{\tau}\restriction_{ns} = \tau$

Proof. Let $X_{\mathsf{SLS}} \overset{O}{\rightsquigarrow}^{\mathsf{SLS}}_{\overline{\tau}} X'_{\mathsf{SLS}}$ be an execution with trace $\overline{\tau} = \tau \cdot \mathtt{start}_{\mathsf{SLS}}\ id \cdot \overline{\tau}' \cdot \mathtt{rlb}_{\mathsf{SLS}}\ id$. Let $\sigma = X_{\mathsf{SLS}}.\sigma$
We know Rule SLS:Spec 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 $\sigma \xrightarrow{\overline{\tau}\restriction_{ns}} \sigma'$.
Now we need to show that $\sigma' = X'_{\mathsf{SLS}}.\sigma$, which is analogous to Lemma 50 (S SE: Non-speculative execution for rolled back transactions). □

O.2 SLS: Relating Non-speculative and AM Semantics

Theorem 23 (SLS: Behaviour of non-speculative semantics and AM semantics)

Lemma 105 (SLS AM: Completeness of the speculative AM semantics)

Lemma 106 (SLS AM: Non-speculative execution for rolled back transactions)

Lemma 102 (SLS AM : Soundness of the AM semantics w.r.t. non-speculative semantics)

Lemma 103 (SLS AM: Soundness single step No Speculation)

Lemma 104 (SLS AM: Single Step Speculation)

Theorem 23 (SLS: Behaviour of non-speculative semantics and AM semantics). $Beh_{NS}(p) = Beh^{\omega}_{\mathsf{SLS}}(p)\restriction_{ns}$

Proof. We prove the two directions separately:

$\Leftarrow$ Assume that $\overline{\tau} \in Beh^{\omega}_{\mathsf{SLS}}(p)$.
By the definition of $Beh^{\omega}_{\mathsf{SLS}}(p)$ we have an initial configuration σ such that (p, σ) 👻$^{\omega}_{\mathsf{SLS}}$ $\overline{\tau}$.
The proof proceeds in a similar fashion to the analogous case in Theorem 12 (S SE: Behaviour of non-speculative and oracle semantics) by using Lemma 102 (SLS AM : Soundness of the AM semantics w.r.t. non-speculative semantics).
We can now conclude that $((p, \sigma))$ 👻$_{NS}\overline{\tau}\restriction_{ns} \in Beh_{NS}(p)$ by Rule NS-Trace.

$\Rightarrow$ Assume that $((p, \sigma))$ 👻$_{NS}\overline{\tau} \in Beh_{NS}(p)$.
We thus know there exists $\sigma' \in FinalConf$ such that $\sigma \Downarrow_{\overline{\tau}} \sigma'$.
We apply Lemma 105 (SLS AM: Completeness of the speculative AM semantics) with $\Sigma_{\mathsf{SLS}} = \Sigma^{init}_{\mathsf{SLS}} p, \sigma$ and get $\Sigma^{init}_{\mathsf{SLS}} p, \sigma \Downarrow^{\overline{\tau}'}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$ with $\vdash_O \Sigma'_{\mathsf{SLS}} : noongoing$, $\sigma' = \Sigma'_{\mathsf{SLS}}.\sigma$ and $\overline{\tau} = \overline{\tau}'\restriction_{ns}$.
Because of $\vdash_O \Sigma'_{\mathsf{SLS}} : noongoing$ and $\sigma' = \Sigma'_{\mathsf{SLS}}.\sigma$ we know that $\vdash \Sigma'_{\mathsf{SLS}} : fin$.

We thus have $(p, \sigma) \Downarrow^{\omega}_{\text{SLS}} \overline{\tau}' \in Beh^{\omega}_{\text{SLS}}(p)$.

$\square$

O.2.1 Soundness.

Lemma 102 (SLS AM : Soundness of the AM semantics w.r.t. non-speculative semantics)**.** *If*

(1) $\Sigma_{\text{SLS}}.\sigma = \sigma$ *and*

(2) $\vdash_O \Sigma_{\text{SLS}} :$ *noongoing and*

(3) $\Sigma_{\text{SLS}} \Downarrow^{\overline{\tau}}_{\text{SLS}} \Sigma'_{\text{SLS}}$

Then there exists σ' *such that*

I if $\vdash_O \Sigma'_{\text{SLS}} :$ *noongoing then* $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}\sigma'}$ *and* $\Sigma'_{\text{SLS}}.\sigma = \sigma'$ *and*

II if $\vdash^i_O \Sigma'_{\text{SLS}} :$ *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 $\Sigma_{\text{SLS}} \Downarrow^{\overline{\tau}}_{\text{SLS}} \Sigma'_{\text{SLS}}$

Rule SLS:AM-Reflection Then we have $\Sigma_{\text{SLS}} \Downarrow^{\varepsilon}_{\text{SLS}} \Sigma_{\text{SLS}}$ with $\Sigma'_{\text{SLS}} = \Sigma_{\text{SLS}}$ and by Rule NS-Reflection we have

I $\sigma \Downarrow_{\varepsilon\upharpoonright_{ns}} \sigma'$ with $\sigma = \sigma'$.

II $\sigma \Downarrow_{helper(\varepsilon,i)} \sigma'$ with $\sigma = \sigma'$.

Rule SLS:AM-Single We have $\Sigma_{\text{SLS}} \Downarrow^{\overline{\tau}'\cdot\tau}_{\text{SLS}} \Sigma'_{\text{SLS}}$ and by Rule SLS:AM-Single we get $\Sigma_{\text{SLS}} \Downarrow^{\overline{\tau}'}_{\text{SLS}} \Sigma''_{\text{SLS}}$ and $\Sigma''_{\text{SLS}} \xrightarrow{\tau}_{\text{SLS}} \Sigma'_{\text{SLS}}$.

We need to prove

I if $\vdash_O \Sigma'_{\text{SLS}} :$ *noongoing* then $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ and $\Sigma'_{\text{SLS}}.\sigma = \sigma'$

II if $\vdash^i_O \Sigma'_{\text{SLS}} :$ *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 $\Sigma_{\text{SLS}} \Downarrow^{\overline{\tau}'}_{\text{SLS}} \Sigma''_{\text{SLS}}$ and have a σ'' where σ'' is the configuration for some instance in Σ''_{SLS} such that.

I' if $\vdash_O \Sigma''_{\text{SLS}} :$ *noongoing* then $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}\sigma''}$ and $\Sigma''_{\text{SLS}}.\sigma = \sigma''$

II' if $\vdash^j_O \Sigma''_{\text{SLS}} :$ *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''_{SLS}.

no ongoing transactions in Σ''_{SLS} Then Σ''_{SLS} has no ongoing transactions, meaning $\vdash_O \Sigma''_{\text{SLS}} :$ *noongoing* and we have $\sigma \Downarrow_{\overline{\tau}\upharpoonright_{ns}} \sigma''$ and $\Sigma''_{\text{SLS}}.\sigma = \sigma''$ by IH.

I Then $\vdash_O \Sigma'_{\text{SLS}} :$ *noongoing* and we need to prove $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ and $\Sigma'_{\text{SLS}}.\sigma = \sigma'$. We now proceed by inversion on $\Sigma''_{\text{SLS}} \xrightarrow{\tau}_{\text{SLS}} \Sigma'_{\text{SLS}}$:

Rule SLS:AM-Rollback Then $\tau = \texttt{rlb}\ id$.

Contradiction. Analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

Rule SLS:AM-Spec Then we know that $\overline{\rho} = \texttt{ret}\ l \cdot \texttt{start}\ id$ for Σ'_{SLS}.

Contradiction. Analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise We know that $\sigma'' = \Sigma''_{SLS}.\sigma$.

Furthermore, no transaction that will be rolled back is created in the step $\Sigma''_{SLS} \overset{\tau}{\rightsquigarrow}_{SLS} \Sigma'_{SLS}$, because $\vdash_O \Sigma'_{SLS} : noongoing$.

We can now apply Lemma 103 (SLS AM: Soundness single step No Speculation) with $\Sigma''_{SLS} \overset{\tau}{\rightsquigarrow}_{SLS} \Sigma'_{SLS}$ and get

$$\sigma'' \Downarrow_{\tau\upharpoonright_{ns}} \sigma'$$
$$\Sigma'_{SLS}.\sigma = \sigma'$$

Since $\overline{\tau}\upharpoonright_{ns} \cdot \tau\upharpoonright_{ns} = \overline{\tau} \cdot \tau\upharpoonright_{ns}$ (because $\tau \neq \texttt{rlb}_{SLS}\ id$), we are finished.

II Then Σ'_{SLS} has ongoing transactions, meaning $\vdash^i_O \Sigma'_{SLS} : biggestongoingtransactionirolledback$ 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 $\Sigma''_{SLS} \overset{\tau}{\rightsquigarrow}_{SLS} \Sigma'_{SLS}$:

Rule SLS:AM-Spec Then we know that $\overline{\rho} = \texttt{ret}\ l \cdot \texttt{start}_{SLS}\ id$ for Σ'_{SLS}.

Analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics) together with Lemma 104 (SLS AM: Single Step Speculation).

otherwise By definition of $\vdash^i_O \Sigma'_{SLS} : biggestongoingtransactionirolledback$ we know that there exists a $\texttt{rlb}_{SLS}\ i$ in the execution $\Sigma'_{SLS} \Downarrow^{\overline{\tau}_{fin}}_{SLS} \Sigma_{SLS\,fin}$ with no matching $\texttt{start}_{SLS}\ i$ observation in that execution.

Contradiction, analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

ongoing transactions in Σ''_{SLS} Then Σ''_{SLS} has ongoing transactions, meaning $\vdash^j_O \Sigma''_{SLS} : biggestongoingtransactionirolledback$ and we have $\sigma \Downarrow_{helper(\overline{\tau},j)} \sigma''$ and σ'' is the configuration for the instance with $ctr = j$.

I Then $\vdash_O \Sigma'_{SLS} : noongoing$ and we need to prove $\sigma \Downarrow_{\overline{\tau}\cdot\tau\upharpoonright_{ns}\sigma'}$ and $\Sigma'_{SLS}.\sigma = \sigma'$. We now proceed by inversion on $\Sigma''_{SLS} \overset{\tau}{\rightsquigarrow}_{SLS} \Sigma'_{SLS}$:

Rule SLS:AM-Rollback and $\tau = \texttt{rlb}_{SLS}\ j$ Choose $\sigma' = \sigma''$. Analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Then $\tau \neq \texttt{rlb}_{SLS}\ j$.

Contradiction, analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

II Then $\vdash^i_O \Sigma'_{SLS} : biggestongoingtransactionirolledback$ 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 $\Sigma''_{SLS} \overset{\tau}{\rightsquigarrow}_{SLS} \Sigma'_{SLS}$:

Rule SLS:AM-Rollback Then $\tau = \texttt{rlb}\ id$. We do a case analysis if $id = j$ or not.

$id = j$ Contradiction, analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

$id \neq j$ Analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

otherwise Then $\tau \neq \texttt{rlb}_{\mathsf{SLS}}\ id$.
Then $helper(\overline{\tau} \cdot \tau, i) = helper(\overline{\tau}, i)$
We choose $\sigma' = \sigma''$ and derive a step by Rule NS-Reflection.
The rest is analogous to the corresponding case in Lemma 45 (S SE: Soundness of the speculative semantics w.r.t. non-speculative semantics).

□

Lemma 103 (SLS AM: Soundness single step No Speculation)**.** *If*

(1) $\vdash_O \Sigma_{\mathsf{SLS}} : noongoing$ *and*
(2) $\Sigma_{\mathsf{SLS}} \overset{\tau}{\Rrightarrow}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$ *and*
(3) $\vdash_O \Sigma'_{\mathsf{SLS}} : noongoing$ *and*
(4) $\sigma = \Sigma_{\mathsf{SLS}}.\sigma$

Then there exists σ' *such that*

I $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma'$ *and*
II $\Sigma'_{\mathsf{SLS}}.\sigma = \sigma'$

Proof. We proceed by inversion on $\Sigma_{\mathsf{SLS}} \overset{\tau}{\Rrightarrow}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$:

Rule SLS:AM-General Thus, we have $\Sigma_{\mathsf{SLS}} = \overline{\Phi}_{\mathsf{SLS}} \cdot \Phi_{\mathsf{SLS}\,\overline{\rho}'\cdot\tau}$. Contradiction. By the definition of $\overset{\tau}{\Rrightarrow}_{\mathsf{SLS}}$ only Rule SLS:AM-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 $\vdash_O \Sigma_{\mathsf{SLS}} : noongoing$.

Rule SLS:AM-Rollback Contradiction, since $\vdash_O \Sigma_{\mathsf{SLS}} : noongoing$ and Definition 18 (Well orderedness of rollback and start).

Rule SLS:AM-Context We have $\Sigma_{\mathsf{SLS}} = \overline{\Phi}_{\mathsf{SLS}} \cdot \Phi_{\mathsf{SLS}}$ and $\Sigma'_{\mathsf{SLS}} = \overline{\Phi}''_{\mathsf{SLS}} \cdot \overline{\Phi}'_{\mathsf{SLS}}$ with $\Phi_{\mathsf{SLS}} \overset{\tau}{\Rrightarrow}_{\mathsf{SLS}} \overline{\Phi}'_{\mathsf{SLS}}$.
We proceed by case analysis on the rule used to derive $\Phi_{\mathsf{SLS}} \overset{\tau}{\Rrightarrow}_{\mathsf{SLS}} \Phi'_{\mathsf{SLS}}$.

Rule SLS:AM-Spec Contradiction, because this starts a speculative transaction that needs to be rolled back.
This cannot happen because of $\vdash_O \Sigma'_{\mathsf{SLS}} : noongoing$.

Rule SLS:AM-barr or Rule SLS:AM-barr-spec Thus, we have $p(\sigma(\mathbf{pc})) \neq \mathbf{ret}$ and $n \neq 0$. We show the proof for Rule SLS:AM-barr, the proof for Rule SLS:AM-barr-spec is analogous.
By Rule SLS:AM-barr we know $\sigma \xrightarrow{\varepsilon} \sigma'$ and $\overline{\Phi}'_{\mathsf{SLS}} = \langle p, ctr, \sigma', n-1 \rangle$.
Thus $\sigma' = \overline{\Phi}'_{\mathsf{SLS}}.\sigma$ and $\tau = \varepsilon = \varepsilon\upharpoonright_{ns}$.
Thus, we have an execution $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma'$ and $\sigma' = \Sigma'_{\mathsf{SLS}}.\sigma$ as needed.

Rule SLS:AM-NoSpec Thus, we have $p(\sigma(\mathbf{pc})) \neq \mathbf{ret}$ and $n \neq 0$. We have $\sigma \xrightarrow{\tau} \sigma'$ as premise of the applied rule Rule SLS:AM-NoSpec and $\overline{\Phi}'_{\mathsf{SLS}} = \langle p, ctr, \sigma', n-1 \rangle$.
Thus, choose $\sigma' = \overline{\Phi}'_{\mathsf{SLS}}.\sigma$.
Because the rule used the observation received from the derived step $\sigma \xrightarrow{\tau} \sigma'$, we already get $\tau\upharpoonright_{ns} = \tau$ and are finished.

□

Lemma 104 (SLS AM: Single Step Speculation)**.** *If*

(1) $\Sigma_{SLS} = \overline{\Phi}_{SLS} \cdot \Phi_{SLS}$ *and* $\vdash_O \Sigma_{SLS} :$ *noongoing*

(2) $\Sigma'_{SLS} = \overline{\Phi}_{SLS} \cdot \overline{\Phi}'_{SLS}$ *and* $\vdash^i_O \Sigma'_{SLS} :$ *biggestongoingtransactionirolledback and*

(3) $\Phi_{SLS} \overset{\tau}{\Rightarrow}\!\!\!\Omega_{SLS}\ \overline{\Phi}'_{SLS}$ *and*

(4) $\sigma = \Phi_{SLS}.\sigma$

Then

I $\sigma \xrightarrow{\tau\upharpoonright_{ns}} \sigma'$ *and*

II σ' *is the configuration for the instance with* $ctr = i$ *in* Σ'_{SLS}

Proof. We proceed by inversion on $\Phi_{SLS} \overset{\tau}{\Rightarrow}\!\!\!\Omega_{SLS}\ \overline{\Phi}'_{SLS}$:

Rule SLS:AM-Spec Then we have

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

$$\overline{\Phi}'_{SLS} = \langle p, ctr, \sigma', n \rangle \cdot \Phi'_{SLS} {}^{\;\;l}_{\texttt{bypass}}\ \sigma(\mathbf{pc}) \cdot \texttt{start}_{SLS}\ ctr$$

We have $\sigma \xrightarrow{\tau} \sigma'$.

Since $\vdash_O \Sigma_{SLS} :$ *noongoing* we know that $\tau\upharpoonright_{ns} = \tau = \texttt{ret}\ l$.

Since a transaction with $id = ctr$ was started and we have $\vdash_O \Sigma_{SLS} :$ *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 $\vdash_O \Sigma_{SLS} :$ *noongoing* and $\vdash^i_O \Sigma'_{SLS} :$ *biggestongoingtransactionirolledback*, we know that a transaction has to be started that will be rolled back.

□

O.2.2 Completeness.

Lemma 105 (SLS AM: Completeness of the speculative AM semantics)**.** *If*

(1) $\sigma \in InitConf$ *and*

(2) $\sigma \Downarrow_{\overline{\tau}} \sigma'$ *and*

(3) $\Sigma_{SLS} = \Sigma^{init}_{SLS}\sigma$

Then

I $\Sigma_{SLS} \Downarrow^{\overline{\tau}'}_{SLS} \Sigma'_{SLS\,\rho}$ *and*

II $\vdash_O \Sigma'_{SLS} :$ *noongoing and*

III $\sigma' = \Sigma'_{SLS}.\sigma$ *and*

IV $\overline{\tau} = \overline{\tau}'\upharpoonright_{ns}$ *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 SLS:AM-Reflection we have $\Sigma_{SLS} \Downarrow^{\varepsilon}_{SLS} \Sigma_{SLS}$. By construction $\vdash_O \Sigma_{SLS} :$ *noongoing* and $\Sigma_{SLS}.\sigma = \sigma$. Since $\varepsilon\upharpoonright_{ns} = \varepsilon$ we are finished.

Rule NS-Single Then we have $\sigma \Downarrow_{\overline{\tau}} \sigma''$ and $\sigma'' \xrightarrow{\tau} \sigma'$.

We need to show

I $\Sigma_{SLS} \Downarrow_{SLS}^{\overline{\tau}'\cdot\tau'} \Sigma'_{SLS}$ and

II $\vdash_O \Sigma'_{SLS}$: *noongoing* and

III $\sigma' = \Sigma'_{SLS}.\sigma$ and

IV $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \upharpoonright_{ns}$

We apply the IH on $\sigma \Downarrow_{\overline{\tau}} \sigma''$ we get

I' $\Sigma_{SLS} \Downarrow_{SLS}^{\overline{\tau}'} \Sigma''_{SLS\rho}$ and

II' $\vdash_O \Sigma''_{SLS\rho}$: *noongoing* and

III' $\sigma'' = \Sigma''_{SLS}.\sigma$ and

IV' $\overline{\tau} = \overline{\tau}' \upharpoonright_{ns}$

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 100 (SLS SE: Completeness of the speculative semantics).

$p(\sigma(\mathbf{pc})) = \mathbf{ret}$ Analogous to the corresponding case Lemma 100 (SLS SE: Completeness of the speculative semantics), which is when the oracle mispredicted in the proof, together with Lemma 106 (SLS AM: Non-speculative execution for rolled back transactions).

□

Lemma 106 (SLS AM: Non-speculative execution for rolled back transactions.)**.** *If*

(1) $\Sigma_{SLS} \Downarrow_{SLS}^{\overline{\tau}} \Sigma'_{SLS}$ *and*

(2) $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$ *and*

(3) $\sigma = \Sigma_{SLS}.\sigma$

Then there exists a configuration σ' *such that*

I $\Sigma'_{SLS}.\sigma = \sigma'$ *and*

II $\sigma \xrightarrow{\overline{\tau}\upharpoonright_{ns}} \sigma'$ *and*

III $\overline{\tau}\upharpoonright_{ns} = \tau$

Proof. Let $\Sigma_{SLS} \Downarrow_{SLS}^{\overline{\tau}} \Sigma'_{SLS}$ be an execution with trace $\overline{\tau} = \tau \cdot \texttt{start}\ id \cdot \overline{\tau}' \cdot \texttt{rlb}\ id$. Let $\sigma = \Sigma_{SLS}.\sigma$.

Let $\Sigma_{SLS} = \overline{\Phi}_{SLS} \cdot \Phi_{SLS}$ Because of $\texttt{start}$ *id* in the trace, we know that Rule SLS:AM-Spec was used to start the speculative transaction.

This rule has the premise $\sigma \xrightarrow{\tau} \sigma'$ for some configuration σ'.

Thus $\Sigma''_{SLS} = \overline{\Phi}_{SLS} \cdot \Phi'_{SLS} \cdot \Phi''_{SLS}$ with $\Phi'_{SLS}.\sigma = \sigma'$.

By definition of $\upharpoonright_{ns}$ we have $\overline{\tau}\upharpoonright_{ns} = \tau\upharpoonright_{ns} = \tau$, where the last steps follows because of the fact that τ was generated by $\rightarrow$.

Thus, we have $\sigma \xrightarrow{\overline{\tau}\upharpoonright_{ns}} \sigma'$.

Now, we need to show that $\sigma' = \Sigma'_{SLS}.\sigma$. We know that Rule SLS:AM-Spec created a new speculative instance Φ'_{S} used for speculation that is at the top.

Thus the state after Rule SLS:AM-Spec is of the form $\overline{\Phi}_{SLS} \cdot \Phi'_{SLS} \cdot \Phi''_{SLS}$ and since Rule SLS:AM-Rollback deletes the instance Φ''_{SLS}, we have Φ'_{SLS} at the top of the stack.

Now $\Sigma'_{\textsf{SLS}}.\sigma = \Phi'_{\textsf{SLS}}.\sigma = \sigma'$ and we are finished.

□

O.3 SLS: Relating Symbolic and AM semantics

- Theorem 24 (SLS: Symbolic Consistency)
  - Lemma 107 (SLS: Soundness of the AM semantics w.r.t. symbolic semantics)
    - Lemma 108 (SLS: Soundness single step)
  - Lemma 109 (SLS: Completeness of the symbolic semantic
    - Lemma 111 (SLS: Completeness single step)

Theorem 24 (SLS: Symbolic Consistency). $Beh^{\omega}_{\textsf{SLS}}(p) = \mu(Beh^{\mathcal{S}}_{\textsf{SLS}}(p))$

Proof. We prove the two directions separately:

$\Leftarrow$ Assume that $\overline{\tau} \in Beh^{\mathcal{S}}_{\textsf{SLS}}(p)$.

By the definition of $Beh^{\mathcal{S}}_{\textsf{SLS}}(p)$ we have an initial configuration $\sigma_{\mathcal{S}}$ such that $(p, \sigma_{\mathcal{S}})\ {}_{\mathcal{S}}\Cap^{\omega}_{\textsf{SLS}}\ \overline{\tau_{\mathcal{S}}}$.
We thus know there exists $\vdash \Sigma^{\mathcal{S}}_{\textsf{SLS}}{}' : \mathit{fin}$ such that $\Sigma^{\mathit{init}}_{\textsf{SLS}}(p, \sigma_{\mathcal{S}})\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau_{\mathcal{S}}}}_{\textsf{SLS}}\ \Sigma^{\mathcal{S}}_{\textsf{SLS}}{}'$ and $\mu \vDash \mathit{pthCnd}(\overline{\tau_{\mathcal{S}}})$.
We now apply Lemma 107 (SLS: Soundness of the AM semantics w.r.t. symbolic semantics) on $\Sigma^{\mathit{init}}_{\textsf{SLS}}(p, \sigma_{\mathcal{S}})\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau_{\mathcal{S}}}}_{\textsf{SLS}}\ \Sigma^{\mathcal{S}}_{\textsf{SLS}}{}'$ and get $\Sigma_{\textsf{SLS}} \Downarrow^{\overline{\tau}}_{\textsf{SLS}} \Sigma'_{\textsf{SLS}}$, where $\mu(\Sigma^{\mathcal{S}}_{\textsf{SLS}}{}') = \Sigma'_{\textsf{SLS}}$ and $\mu(\overline{\tau_{\mathcal{S}}}) = \overline{\tau}$
Since $\vdash \Sigma^{\mathcal{S}}_{\textsf{SLS}}{}' : \mathit{fin}$ and $\mu(\Sigma^{\mathcal{S}}_{\textsf{SLS}}{}') = \Sigma'_{\textsf{SLS}}$ we have $\vdash \Sigma'_{\textsf{SLS}} : \mathit{fin}$ as well.
We can now conclude that $(p, \mu(\sigma_{\mathcal{S}}))\ \Cap^{\omega}_{\textsf{SLS}}\ \mu(\overline{\tau_{\mathcal{S}}})\restriction_{ns} \in Beh^{\omega}_{\textsf{SLS}}(p)$ by Rule SLS:AM-Trace.

$\Rightarrow$ Assume that $(p, \sigma)\ \Cap^{\omega}_{\textsf{SLS}}\ \overline{\tau} \in Beh^{\omega}_{\textsf{SLS}}(p)$. We thus know there exists $\vdash \Sigma'_{\textsf{SLS}} : \mathit{fin}$ such that $\Sigma^{\mathit{init}}_{\textsf{SLS}}(p, \sigma) \Downarrow^{\overline{\tau}}_{\textsf{SLS}} \Sigma'_{\textsf{SLS}}$.

We now apply Lemma 109 (SLS: Completeness of the symbolic semantics) on $\Sigma^{\mathit{init}}_{\textsf{SLS}}(p, \sigma) \Downarrow^{\overline{\tau}}_{\textsf{SLS}} \Sigma'_{\textsf{SLS}}$ and get

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

Since $\vdash \Sigma'_{\textsf{SLS}} : \mathit{fin}$ and $\mu(\Sigma^{\mathcal{S}}_{\textsf{SLS}}{}') = \Sigma'_{\textsf{SLS}}$ we have $\vdash \Sigma^{\mathcal{S}}_{\textsf{SLS}}{}' : \mathit{fin}$ as well.
Thus, $(p, \sigma_{\mathcal{S}})\ {}_{\mathcal{S}}\Cap^{\omega}_{\textsf{SLS}}\ \overline{\tau_{\mathcal{S}}} \in Beh^{\mathcal{S}}_{\textsf{SLS}}(p)$.

□

O.3.1 *Soundness.*

Lemma 107 (SLS: Soundness of the AM semantics w.r.t. symbolic semantics)**.** *If*

(1) $\Sigma^{\mathcal{S}}_{\textsf{SLS}}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau_{\mathcal{S}}}}_{\textsf{SLS}}\ \Sigma^{\mathcal{S}}_{\textsf{SLS}}{}'$ *and*
(2) $\mu \vDash \mathit{pthCnd}(\Sigma^{\mathcal{S}}_{\textsf{SLS}}{}')$

Then

I $\mu(\Sigma^{\mathcal{S}}_{\textsf{SLS}}) \Downarrow^{\mu(\overline{\tau_{\mathcal{S}}})}_{\textsf{SLS}} \mu(\Sigma^{\mathcal{S}}_{\textsf{SLS}}{}')$

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

Rule SLS:Sym-Reflection Then we have $\Sigma^{\mathcal{S}}_{\mathsf{SLS}}\ {}_{\mathcal{S}}{\Downarrow}^{\varepsilon}_{\mathsf{SLS}}\ \Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}'$ with $\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}' = \Sigma^{\mathcal{S}}_{\mathsf{SLS}}$. Using Rule SLS:AM-Reflection we get $\mu(\Sigma^{\mathcal{S}}_{\mathsf{SLS}})\ {}_{\mathcal{S}}{\Downarrow}^{\mu(\varepsilon)}_{\mathsf{SLS}}\ \mu(\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}')$ and are finished.

Rule SLS:Sym-Single We have $\Sigma^{\mathcal{S}}_{\mathsf{SLS}}\ {}_{\mathcal{S}}{\Downarrow}^{\overline{\tau_{\mathcal{S}}}'\cdot\tau_{\mathcal{S}}}_{\mathsf{SLS}}\ \Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}'$ and by Rule SLS:Sym-Single we get $\Sigma^{\mathcal{S}}_{\mathsf{SLS}}\ {}_{\mathcal{S}}{\Downarrow}^{\overline{\tau_{\mathcal{S}}}'}_{\mathsf{SLS}}\ \Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}''$ and $\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}''\ \overset{\tau}{\leadsto}{}^{\mathcal{S}}_{\mathsf{SLS}}\ \Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}'$.

We need to prove

(1) $\mu(\Sigma^{\mathcal{S}}_{\mathsf{SLS}})\ {\Downarrow}^{\mu(\overline{\tau}\cdot\tau_{\mathcal{S}})}_{\mathsf{SLS}}\ \mu(\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}')$

We apply the IH on $\Sigma^{\mathcal{S}}_{\mathsf{SLS}}\ {}_{\mathcal{S}}{\Downarrow}^{\overline{\tau_{\mathcal{S}}}}_{\mathsf{SLS}}\ \Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}''$ and have a $\Sigma''_{\mathsf{SLS}} = \mu(\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}'')$ such that:

(1) $\mu(\Sigma^{\mathcal{S}}_{\mathsf{SLS}})\ {\Downarrow}^{\mu(\overline{\tau_{\mathcal{S}}})}_{\mathsf{SLS}}\ \Sigma''_{\mathsf{SLS}}$ and

The result follows by applying Lemma 108 (SLS: Soundness single step) on $\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}''\ \overset{\tau_{\mathcal{S}}}{\leadsto}{}^{\mathcal{S}}_{\mathsf{SLS}}\ \Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}'$ and get a step $\Sigma''_{\mathsf{SLS}}\ \overset{\mu(\tau_{\mathcal{S}})}{\leadsto}{}_{\mathsf{SLS}}\ \mu(\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}')$.

We now use Rule SLS:AM-Single and get an execution $\mu(\Sigma^{\mathcal{S}}_{\mathsf{SLS}})\ {\Downarrow}^{\mu(\overline{\tau_{\mathcal{S}}})\cdot\mu(\tau_{\mathcal{S}})}_{\mathsf{SLS}}\ \mu(\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}')$ as required.

□

Lemma 108 (SLS: Soundness single step). *If*

(1) $\Sigma^{\mathcal{S}}_{\mathsf{SLS}}\ \overset{\tau}{\leadsto}{}^{\mathcal{S}}_{\mathsf{SLS}}\ \Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}'$ *and*

(2) $\mu\ \vDash pthCnd(\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}')$

Then

I $\mu(\Sigma^{\mathcal{S}}_{\mathsf{SLS}})\ \overset{\mu(\tau)}{\leadsto}{}_{\mathsf{SLS}}\ \mu(\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}')$

Proof. We proceed by inversion on $\Sigma^{\mathcal{S}}_{\mathsf{SLS}}\ \overset{\tau}{\leadsto}{}^{\mathcal{S}}_{\mathsf{SLS}}\ \Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}'$:

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

$\Sigma_{\mathsf{SLS}}\ \overset{\tau'}{\leadsto}{}_{\mathsf{SLS}}\ \Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}'$ We can use Rule SLS:AM-Rollback to derive $\Sigma_{\mathsf{SLS}}\ \overset{\tau'}{\leadsto}{}_{\mathsf{SLS}}\ \Sigma'_{\mathsf{SLS}}$.

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

$\mu\ \vDash pthCnd(\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}')$ **and** $\mu(\tau') = \tau$ Since the $\Sigma_{\mathsf{SLS}}.ctr = \Sigma^{\mathcal{S}}_{\mathsf{SLS}}.ctr$ we already have $\mu(\tau') = \tau$. For $\mu\ \vDash pthCnd(\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}')$, notice that $\mu\ \vDash pthCnd(\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}') = \mu\ \vDash pthCnd(\Sigma^{\mathcal{S}}_{\mathsf{SLS}})$ because the rule only deletes a speculative instance. Thus, we are finished.

Rule SLS:Sym-Context We then have $\Phi^{\mathcal{S}}_{\mathsf{SLS}}\ \overset{\tau}{\leadsto}{}^{\mathcal{S}}_{\mathsf{SLS}}\ \overline{\Phi}'_{\mathsf{SLS}_{\mathcal{S}}}$. Thus, we know $\Phi^{\mathcal{S}}_{\mathsf{SLS}}.n > 0$ and $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}}).n > 0$ as well. We proceed by inversion on $\Phi^{\mathcal{S}}_{\mathsf{SLS}}\ \overset{\tau_{\mathcal{S}}}{\leadsto}{}^{\mathcal{S}}_{\mathsf{SLS}}\ \overline{\Phi}'_{\mathsf{SLS}_{\mathcal{S}}}$:

Rule SLS:Sym-General Then $\Phi^{\mathcal{S}}_{\mathsf{SLS}}\ \overset{\tau_{\mathcal{S}}}{\leadsto}{}^{\mathcal{S}}_{\mathsf{SLS}}\ \Phi_{\mathsf{SLS}\overline{\rho_{\mathcal{S}}}\backslash\tau_{\mathcal{S}}}$. By $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}}) = \Phi_{\mathsf{SLS}}$ 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 and Rule SLS:AM-General applies.

Since that rule does not change the state Φ_{SLS} except for $\overline{\rho}$ we have $\Phi_{\mathsf{SLS}}\ \overset{\tau}{\leadsto}{}_{\mathsf{SLS}}\ \Phi_{\mathsf{SLS}\overline{\rho}\backslash\tau}$.

Now we have $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}\overline{\rho_{\mathcal{S}}}\backslash\tau_{\mathcal{S}})} = \Phi_{\mathsf{SLS}\overline{\rho}\backslash\tau}$ by construction.

Rule SLS:Sym-NoSpec Then we have $\Phi^{\mathcal{S}}_{\mathsf{SLS}}\ \overset{\tau_{\mathcal{S}}}{\leadsto}{}^{\mathcal{S}}_{\mathsf{SLS}}\ \Phi^{\mathcal{S}}_{\mathsf{SLS}}{}'$ where $\Phi^{\mathcal{S}}_{\mathsf{SLS}}{}' = \langle p, \Phi^{\mathcal{S}}_{\mathsf{SLS}}.ctr, \Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma'_{\mathcal{S}}, \Phi^{\mathcal{S}}_{\mathsf{SLS}}.n - 1\rangle$ with $\Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$.

Since we have $\mu \vDash pthCnd(\overline{\Phi}_{\mathsf{SLS}_{\mathcal{S}}}.\sigma_{\mathcal{S}})$ (by assumption) we can use Lemma 3 (NS: Soundness Symbolic Added rules) on $\Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$ and get $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}}\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_{\mathcal{S}})} \mu(\sigma'_{\mathcal{S}})$, where $\mu(\Phi_{\mathsf{SLS}}.\sigma_{\mathcal{S}}) = \Phi_{\mathsf{SLS}}.\sigma$ as per assumption.

We can now use Rule SLS:AM-NoSpec to derive the step $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}}) \overset{\mu(\tau_{\mathcal{S}})}{=\!=\!\Rightarrow}_{\mathsf{SLS}} \Phi'_{\mathsf{SLS}}$ using the derived $\rightarrow$ step and satisfy $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}}{}') = \Phi'_{\mathsf{SLS}}$ by determinism of $\rightarrow$.

Rule SLS:Sym-barr Then we have $\Phi^{\mathcal{S}}_{\mathsf{SLS}} \overset{\tau_{\mathcal{S}}}{=\!=\!\Rightarrow}^{\mathcal{S}}_{\mathsf{SLS}} \Phi^{\mathcal{S}}_{\mathsf{SLS}}{}'$ where $\Phi^{\mathcal{S}}_{\mathsf{SLS}}{}' = \langle p, \Phi^{\mathcal{S}}_{\mathsf{SLS}}.ctr, \Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma'_{\mathcal{S}}, \Phi^{\mathcal{S}}_{\mathsf{SLS}}.n-1\rangle$ with $\Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$. Analogous to Rule SLS:Sym-NoSpec using Rule SLS:AM-barr.

Rule SLS:Sym-barr-spec Then we have $\Phi^{\mathcal{S}}_{\mathsf{SLS}} \overset{\tau_{\mathcal{S}}}{=\!=\!\Rightarrow}^{\mathcal{S}}_{\mathsf{SLS}} \Phi^{\mathcal{S}}_{\mathsf{SLS}}{}'$ where $\Phi^{\mathcal{S}}_{\mathsf{SLS}}{}' = \langle p, \Phi^{\mathcal{S}}_{\mathsf{SLS}}.ctr, \Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma'_{\mathcal{S}}, \Phi^{\mathcal{S}}_{\mathsf{SLS}}.n-1\rangle$ with $\Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$. Analogous to case Rule SLS:Sym-NoSpec using Rule SLS:AM-barr-spec.

Rule SLS:Sym-Spec We have $\Phi^{\mathcal{S}}_{\mathsf{SLS}} \overset{\tau_{\mathcal{S}}}{=\!=\!\Rightarrow}^{\mathcal{S}}_{\mathsf{SLS}} \overline{\Phi}_{\mathsf{SLS}_{\mathcal{S}}\overline{\rho_{\mathcal{S}}}\cdot \mathtt{bypass}\ \Phi^{\mathcal{S}}_{\mathsf{SLS}}.\mathbf{pc}\cdot \mathtt{start}\ \Phi^{\mathcal{S}}_{\mathsf{SLS}}.ctr}$ where $\overline{\Phi}_{\mathsf{SLS}_{\mathcal{S}}} = \langle p, \Phi^{\mathcal{S}}_{\mathsf{SLS}}.ctr, \sigma'_{\mathcal{S}}, \Phi^{\mathcal{S}}_{\mathsf{SLS}}.n-1\rangle \cdot \langle p, \Phi^{\mathcal{S}}_{\mathsf{SLS}}.ctr+1, \sigma''_{\mathcal{S}}, \min \Phi^{\mathcal{S}}_{\mathsf{SLS}}.n, \omega\rangle$. Furthermore, we have $\Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$ and $\sigma''_{\mathcal{S}} = \sigma_{\mathcal{S}}[\mathbf{pc} \mapsto \Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma_{\mathcal{S}}(\mathbf{pc})+1]$ (note that **pc** is always concrete).

We use Lemma 3 (NS: Soundness Symbolic Added rules) on $\Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$ and get $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_{\mathcal{S}})} \mu(\sigma'_{\mathcal{S}})$. Let $\sigma' = \mu(\sigma'_{\mathcal{S}})$.
Choose $\Phi_{\mathsf{SLS}} = \mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}})$ and note that a **ret** instruction is executed.

We now derive a step using Rule SLS:AM-Spec together with the non-speculative step $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma_{\mathcal{S}}) \xrightarrow{\mu(\tau_{\mathcal{S}})} \mu(\sigma'_{\mathcal{S}})$ above and define $\sigma'' = \sigma[\mathbf{pc} \mapsto \sigma(\mathbf{pc})+1]$.
$\Phi_{\mathsf{SLS}} \overset{\mu(\tau_{\mathcal{S}})}{=\!=\!\Rightarrow}_{\mathsf{SLS}} \overline{\Phi}_{\mathsf{SLS}}$ with $\overline{\Phi}_{\mathsf{SLS}} = \langle p, \Phi_{\mathsf{SLS}}.ctr, \mu(\sigma'_{\mathcal{S}}), \Phi_{\mathsf{SLS}}.n-1\rangle \cdot \langle p, \Phi_{\mathsf{SLS}}.ctr+1, \sigma'', \min \Phi_{\mathsf{SLS}}.n, \omega\rangle$.
We now show that $\mu(\overline{\Phi}_{\mathsf{SLS}_{\mathcal{S}}}) = \overline{\Phi}_{\mathsf{SLS}}$. Since **pc** is concrete and $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma) = \sigma$, it follow that $\mu(\sigma''_{\mathcal{S}}) = \sigma''$.
By $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}}) = \Phi_{\mathsf{SLS}}$ we have $\Phi^{\mathcal{S}}_{\mathsf{SLS}}.ctr = \Phi_{\mathsf{SLS}}.ctr$ and $\Phi^{\mathcal{S}}_{\mathsf{SLS}}.n = \Phi_{\mathsf{SLS}}.n$.

Now, we have $\mu(\overline{\Phi}_{\mathsf{SLS}_{\mathcal{S}}}) = \overline{\Phi}_{\mathsf{SLS}}$ and thus $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}}) \overset{\mu(\tau_{\mathcal{S}})}{=\!=\!\Rightarrow}_{\mathsf{SLS}} \mu(\overline{\Phi}_{\mathsf{SLS}_{\mathcal{S}}})$ as needed.

□

O.3.2 Completeness.

Lemma 109 (SLS: Completeness of the symbolic semantics)**.** *If*

(1) $\Sigma_{\mathsf{SLS}} \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$ *and*
(2) $\Sigma_{\mathsf{SLS}} = \mu(\Sigma^{\mathcal{S}}_{\mathsf{SLS}})$

Then there is a valuation μ*, a symbolic trace* $\overline{\tau_{\mathcal{S}}}'$ *and a final state* $\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}'$ *such that*

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

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

Rule SLS:AM-Reflection Then we have $\Sigma_{\mathsf{SLS}} \Downarrow^{\varepsilon}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$ with $\Sigma_{\mathsf{SLS}} = \Sigma'_{\mathsf{SLS}}$.

I - III By Rule SLS:Sym-Reflection we have $\Sigma^{\mathcal{S}}_{\mathsf{SLS}}\ {}_{\mathcal{S}}\Downarrow^{\varepsilon}_{\mathsf{SLS}} \Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}'$. By construction $\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}' = \Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}'$. We now trivially satisfy all conditions.

Rule SLS:AM-Single We have $\Sigma_{\mathsf{SLS}} \Downarrow^{\overline{\tau}'\cdot\tau}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$ and by Rule SLS:AM-Single we get $\Sigma_{\mathsf{SLS}} \Downarrow^{\overline{\tau_{\mathcal{S}}}'}_{\mathsf{SLS}} \Sigma''_{\mathsf{SLS}}$ and $\Sigma''_{\mathsf{SLS}} \overset{\tau}{=\!\!\!\curvearrowright}{}^{\mathcal{S}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$.

We need to prove

(1) $\Sigma^{\mathcal{S}}_{\mathsf{SLS}} \;{}_{\mathcal{S}}\!\Downarrow^{\overline{\tau_{\mathcal{S}}}'\cdot\tau_{\mathcal{S}}}_{\mathsf{SLS}} {\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}'$ and

(2) $\Sigma'_{\mathsf{SLS}} = \mu({\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}')$ and $\overline{\tau}' \cdot \tau = \mu(\overline{\tau_{\mathcal{S}}}' \cdot \tau_{\mathcal{S}})$ and

(3) $\mu \vDash pthCnd({\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}')$

We apply the IH on $\Sigma_{\mathsf{SLS}} \Downarrow^{\overline{\tau_{\mathcal{S}}}'}_{\mathsf{SLS}} \Sigma''_{\mathsf{SLS}}$ and obtain a ${\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}''$ such that:

(1) $\Sigma^{\mathcal{S}}_{\mathsf{SLS}} \;{}_{\mathcal{S}}\!\Downarrow^{\overline{\tau_{\mathcal{S}}}'}_{\mathsf{SLS}} {\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}''$ and

(2) $\Sigma''_{\mathsf{SLS}} = \mu({\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}'')$ and $\overline{\tau}' = \mu(\overline{\tau_{\mathcal{S}}}')$ and

(3) $\mu \vDash pthCnd({\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}'')$

The result follows from applying Lemma 111 (SLS: Completeness single step) on $\Sigma''_{\mathsf{SLS}} \overset{\tau}{=\!\!\!\curvearrowright}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$:

□

Lemma 110 (SLS: Completeness single step). *If*

(1) $\Sigma_{\mathsf{SLS}} \overset{\tau}{=\!\!\!\curvearrowright}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$ *and*

(2) $\mu(\Sigma^{\mathcal{S}}_{\mathsf{SLS}}) = \Sigma_{\mathsf{SLS}}$ *and*

(3) $\mu \vDash pthCnd(\Sigma^{\mathcal{S}}_{\mathsf{SLS}})$

Then

I $\Sigma^{\mathcal{S}}_{\mathsf{SLS}} \overset{\tau'}{=\!\!\!\curvearrowright}{}^{\mathcal{S}}_{\mathsf{SLS}} {\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}'$ *and*

II $\mu({\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}') = \Sigma'_{\mathsf{SLS}}$ *and*

III $\mu \vDash pthCnd({\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}')$ *and* $\mu(\tau') = \tau$

Lemma 111 (SLS: Completeness single step). *If*

(1) $\Sigma_{\mathsf{SLS}} \overset{\tau}{=\!\!\!\curvearrowright}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$ *and*

(2) $\mu(\Sigma^{\mathcal{S}}_{\mathsf{SLS}}) = \Sigma_{\mathsf{SLS}}$ *and*

(3) $\mu \vDash pthCnd(\Sigma^{\mathcal{S}}_{\mathsf{SLS}})$

Then

I $\Sigma^{\mathcal{S}}_{\mathsf{SLS}} \overset{\tau'}{=\!\!\!\curvearrowright}{}^{\mathcal{S}}_{\mathsf{SLS}} {\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}'$ *and*

II $\mu({\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}') = \Sigma'_{\mathsf{SLS}}$ *and*

III $\mu \vDash pthCnd({\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}')$ *and* $\mu(\tau') = \tau$

Proof. We proceed by inversion on $\Sigma_{\mathsf{SLS}} \overset{\tau}{=\!\!\!\curvearrowright}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$:

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

$\Sigma^{\mathcal{S}}_{\mathsf{SLS}} \overset{\tau'}{=\!\!\!\curvearrowright}{}^{\mathcal{S}}_{\mathsf{SLS}} {\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}'$ We can use the rule Rule SLS:Sym-Rollback in the symbolic semantics to derive $\Sigma^{\mathcal{S}}_{\mathsf{SLS}} \overset{\tau'}{=\!\!\!\curvearrowright}{}^{\mathcal{S}}_{\mathsf{SLS}} {\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}'$.

$\mu({\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}') = \Sigma'_{\mathsf{SLS}}$ The rule Rule SLS:Sym-Rollback only deletes the topmost instance and changes the ctr of the instance below. Since $\Sigma_{\mathsf{SLS}}.ctr = \Sigma^{\mathcal{S}}_{\mathsf{SLS}}.ctr$, we have $\mu({\Sigma^{\mathcal{S}}_{\mathsf{SLS}}}') = \Sigma'_{\mathsf{SLS}}$

$\mu \vDash pthCnd(\tau')$ **and** $\mu(\tau') = \tau$ Since the $\Sigma_{\mathsf{SLS}}.ctr = \Sigma^{\mathcal{S}}_{\mathsf{SLS}}.ctr$ we already have $\mu(\tau') = \tau$. For $\mu \vDash pthCnd(\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}')$, notice that $\mu \vDash pthCnd(\Sigma^{\mathcal{S}}_{\mathsf{SLS}}{}') = \mu \vDash pthCnd(\Sigma^{\mathcal{S}}_{\mathsf{SLS}})$ because the rule only deletes a speculative instance. Thus, we are finished.

Rule SLS:AM-Context We then have $\Phi_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \overline{\Phi}'_{\mathsf{SLS}}$. Note that $\Phi_{\mathsf{SLS}}.n > 0$ and as such for all symbolic states where $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}}) = \Phi_{\mathsf{SLS}}$ as well. We proceed by inversion on $\Phi_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \overline{\Phi}'_{\mathsf{SLS}}$:

Rule SLS:AM-General Then $\Phi_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \Phi_{\mathsf{SLS}\overline{\rho}\backslash\tau}$. By $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}}) = \Phi_{\mathsf{SLS}}$ 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 SLS:Sym-General applies. Since that rule does not change the state $\Phi^{\mathcal{S}}_{\mathsf{SLS}}$ except for $\overline{\rho}$ we have $\Phi^{\mathcal{S}}_{\mathsf{SLS}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathsf{SLS}} \Phi^{\mathcal{S}}_{\mathsf{SLS}\overline{\rho_{\mathcal{S}}}\backslash\tau_{\mathcal{S}}}$. Now we have $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}})_{\overline{\rho}\backslash\tau_{\mathcal{S}}} = \Phi_{\mathsf{SLS}\overline{\rho}\backslash\tau}$ by construction.

Rule SLS:AM-barr Then we have $\Phi_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \Phi'_{\mathsf{SLS}}$ where $\Phi'_{\mathsf{SLS}} = \langle p, \Phi_{\mathsf{SLS}}.ctr, \Phi_{\mathsf{SLS}}.\sigma', \Phi_{\mathsf{SLS}}.n - 1\rangle$ with $\Phi_{\mathsf{SLS}}.\sigma \xrightarrow{\tau} \sigma'$. We use Lemma 5 (NS : Completeness Symbolic Added) on $\Phi_{\mathsf{SLS}}.\sigma \to \sigma'$ and get $\Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$, where $\mu(\Phi_{\mathsf{SLS}}) = \Phi_{\mathsf{SLS}}$ as per assumption, $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu(\sigma'_{\mathcal{S}}) = \sigma'$. Now choose $\Phi^{\mathcal{S}}_{\mathsf{SLS}}{}'.\sigma = \sigma'_{\mathcal{S}}$ and let it otherwise be equal to Φ_{SLS}. We can now use Rule SLS:Sym-barr to derive the step $\Phi^{\mathcal{S}}_{\mathsf{SLS}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathsf{SLS}} \Phi^{\mathcal{S}}_{\mathsf{SLS}}{}'$ using the derived $\to_{\mathcal{S}}$ step and trivially satisfy $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}}{}') = \Phi'_{\mathsf{SLS}}$.

Rule SLS:AM-barr-spec Analogous to the barrier case above.

Rule SLS:AM-NoSpec The case is analogous to Rule SLS:AM-barr above using Rule SLS:Sym-NoSpec.

Rule SLS:AM-Spec We have $\Phi_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \overline{\Phi}_{\mathsf{SLS}\overline{\rho}\cdot\mathtt{bypass}\ \Phi_{\mathsf{SLS}}.\mathbf{pc}\cdot\mathtt{start}\ \Phi_{\mathsf{SLS}}.ctr}$ where $\overline{\Phi}_{\mathsf{SLS}} = \langle p, \Phi_{\mathsf{SLS}}.ctr, \sigma', \Phi_{\mathsf{SLS}}.n - 1\rangle \cdot \langle p, \Phi_{\mathsf{SLS}}.ctr + 1, \sigma'', \min \Phi_{\mathsf{SLS}}.n, \omega\rangle$. Furthermore, we have $\Phi_{\mathsf{SLS}}.\sigma \to \sigma'$ and $\sigma'' = \sigma[\mathbf{pc} \mapsto \Phi_{\mathsf{SLS}}.\sigma(\mathbf{pc}) + 1]$

We use Lemma 5 (NS : Completeness Symbolic Added) on $\Phi_{\mathsf{SLS}}.\sigma \xrightarrow{\tau} \sigma'$ and get $\Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma_{\mathcal{S}} \xrightarrow{\tau_{\mathcal{S}}}_{\mathcal{S}} \sigma'_{\mathcal{S}}$, where $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}}) = \Phi_{\mathsf{SLS}}$ as per assumption, $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu(\sigma'_{\mathcal{S}}) = \sigma'$.

Next, we define $\sigma''_{\mathcal{S}} = \Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma_{\mathcal{S}}[\mathbf{pc} \mapsto \Phi_{\mathsf{SLS}}.\sigma(\mathbf{pc}) + 1]$ (per assumption **pc** is concrete).

It follows that $\mu(\sigma''_{\mathcal{S}}) = \sigma''$ by $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma) = \sigma$.

Since a **ret** is executed, we can use Rule SLS:Sym-Spec to derive a step and get

$$\Phi^{\mathcal{S}}_{\mathsf{SLS}} \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}{}^{\mathcal{S}}_{\mathsf{SLS}} \langle p, \Phi^{\mathcal{S}}_{\mathsf{SLS}}.ctr + 1, \Phi^{\mathcal{S}}_{\mathsf{SLS}}.\sigma_{\mathcal{S}}, \Phi^{\mathcal{S}}_{\mathsf{SLS}}.n - 1\rangle \cdot \langle p, \Phi^{\mathcal{S}}_{\mathsf{SLS}}.ctr + 1, \sigma''_{\mathcal{S}}, \min \Phi^{\mathcal{S}}_{\mathsf{SLS}}.n, \omega\rangle_{\overline{\rho}\cdot\mathtt{bypass}\ \Phi^{\mathcal{S}}_{\mathsf{SLS}}.\mathbf{pc}\cdot\mathtt{start}\ \Phi^{\mathcal{S}}_{\mathsf{SLS}}.ctr}.$$

By $\mu(\Phi^{\mathcal{S}}_{\mathsf{SLS}}) = \Phi_{\mathsf{SLS}}$ we have $\Phi^{\mathcal{S}}_{\mathsf{SLS}}.ctr = \Phi_{\mathsf{SLS}}.ctr$ and $\Phi^{\mathcal{S}}_{\mathsf{SLS}}.n = \Phi_{\mathsf{SLS}}.n$.

Now, we have $\mu(\overline{\Phi}_{\mathsf{SLS}_{\mathcal{S}}}) = \overline{\Phi}_{\mathsf{SLS}}$ and $\mu(\tau_{\mathcal{S}}) = \tau$.

It remains to show that $\mu \vDash pthCnd(\overline{\Phi}_{\mathsf{SLS}_{\mathcal{S}}})$. Since $\overline{\Phi}_{\mathsf{SLS}_{\mathcal{S}}}.\sigma_{\mathcal{S}} = \sigma''_{\mathcal{S}}$, $\sigma''_{\mathcal{S}}.\delta^{\mathcal{S}} = \sigma'_{\mathcal{S}}.\delta^{\mathcal{S}}$ and we have $\mu \vDash pthCnd(\sigma'_{\mathcal{S}})$ from above we have $\mu \vDash pthCnd(\overline{\Phi}_{\mathsf{SLS}_{\mathcal{S}}})$.

□

O.4 SLS: Relating Oracle and AM semantics via SNI

First the definition of the element function we are gonna use: $\text{elem\_of\_states}(\langle p, ctr, \sigma, n\rangle) = \langle p, ctr, \sigma\rangle$

The proof structure looks like this:

- Theorem 25 (SLS: Oracle Overapproximation)
  - Proposition 12 (SLS: Sound and Completeness between Spec and AM semantics)
    - Lemma 112 (SLS: Initial states in $\approx$)
    - Lemma 115 (SLS: Soundness Am semantics w.r.t. speculative semantics)
      - Lemma 116 (SLS: Soundness Big-step Am semantics w.r.t. oracle semantics)
        - Lemma 117 (SLS: Soundness Single Step AM)
          - Lemma 113 (SLS AM: Single step preserves $\cong$)
          - Lemma 114 (SLS SE: Single step preserves $\cong$)
    - Lemma 118 (SLS: Completeness AM semantics w.r.t. speculative semantics)
      - Lemma 120 (SLS: Stronger Soundness for a specific oracle and for specific executions)
        - Lemma 121 (SLS AM: Strong Soundness Single Step)

Theorem 25 (SLS: Oracle Overapproximation). *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 $((p,\sigma)) \Downarrow_{NS} \overline{\tau}$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}$, then $(p,\sigma) \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}''$, $(p,\sigma') \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}''$*

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) $((p,\sigma)) \Downarrow_{NS} \overline{\tau}'$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}'$ 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 $(p,\sigma) \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}''$, $(p,\sigma') \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}''$ 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 $((p,\sigma)) \Downarrow_{NS} \overline{\tau}$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}$, then $(p,\sigma) \Downarrow^{O}_{\mathsf{SLS}} \overline{\tau}'$ and $(p,\sigma') \Downarrow^{O}_{\mathsf{SLS}} \overline{\tau}'$.

We fulfill all premises of SNI by 1) and 2) for p and get $(p,\sigma) \Downarrow^{O}_{\mathsf{SLS}} \overline{\tau}'$ and $(p,\sigma') \Downarrow^{O}_{\mathsf{SLS}} \overline{\tau}'$.

We use Proposition 12 (SLS: Sound and Completeness between Spec and AM semantics) with $(p,\sigma) \Downarrow^{O}_{\mathsf{SLS}} \overline{\tau}'$ and $(p,\sigma') \Downarrow^{O}_{\mathsf{SLS}} \overline{\tau}'$ to get $(p,\sigma) \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}''$, $(p,\sigma') \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}''$. This completes the proof.

($\Leftarrow$) We have

(1) $\sigma \sim_P \sigma'$ and

(2) $((p,\sigma)) \Downarrow_{NS} \overline{\tau}'$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}'$ and

(3) if $\sigma \sim_P \sigma'$ and $((p,\sigma)) \Downarrow_{NS} \overline{\tau}$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}$, then $(p,\sigma) \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}''$, $(p,\sigma') \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}''$

Note that we got assumptions 1) and 2) by the unfolding of the definition of SNI. We need to show that $(p,\sigma) \Downarrow^{O}_{\mathsf{SLS}} \overline{\tau}'$ and $(p,\sigma') \Downarrow^{O}_{\mathsf{SLS}} \overline{\tau}'$ holds.

By using assumption 1) and 2) for assumption 3), we get $(p,\sigma) \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}''$, $(p,\sigma') \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}''$.

Let O be an arbitrary prediction oracle with speculative window at most ω.

From Proposition 12 (SLS: Sound and Completeness between Spec and AM semantics) with $(p,\sigma) \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}''$, $(p,\sigma') \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}''$ we get back $(p,\sigma) \Downarrow^{O}_{\mathsf{SLS}} \overline{\tau}$, $(p,\sigma') \Downarrow^{O}_{\mathsf{SLS}} \overline{\tau}$. 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 12 (SLS: 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 $(p,\sigma) \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}$ and $(p,\sigma') \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}$ iff $(p,\sigma) \Downarrow^{O}_{\mathsf{SLS}} \overline{\tau}'$, $(p,\sigma) \Downarrow^{O}_{\mathsf{SLS}} \overline{\tau}'$ for all prediction oracles O with speculative window at most ω.*

Proof. The proposition immediately follows from Lemma 115 (SLS: Soundness Am semantics w.r.t. speculative semantics) and Lemma 118 (SLS: Completeness AM semantics w.r.t. speculative semantics) □

Lemma 112 (SLS: Initial states in $\approx$). *Let p be a program, ω be a speculation window and O be an oracle with speculation window at most ω. If*

(1) $\sigma, \sigma' \in \mathit{InitConf}$ *and*
(2) $\Sigma^{init}_{\mathsf{SLS}} p, \sigma$ *and* $\Sigma^{init}_{\mathsf{SLS}} p, \sigma'$ *and*
(3) $X^{init}_{\mathsf{SLS}}(p, \sigma)$ *and* $X^{init}_{\mathsf{SLS}}(p, \sigma')$

Then

(1) $X^{init}_{\mathsf{SLS}}(p, \sigma) \cong X^{init}_{\mathsf{SLS}}(p, \sigma')$ *and*
(2) $\Sigma^{init}_{\mathsf{SLS}} p, \sigma \cong \Sigma^{init}_{\mathsf{SLS}} p, \sigma'$ *and*
(3) $\Sigma^{init}_{\mathsf{SLS}} p, \sigma \approx X^{init}_{\mathsf{SLS}}(p, \sigma)$ *and* $\Sigma^{init}_{\mathsf{SLS}} p, \sigma' \approx X^{init}_{\mathsf{SLS}}(p, \sigma')$ *by sls-com-single-base*

Proof. We have

(1) $\sigma, \sigma' \in \mathit{InitConf}$ and
(2) $\Sigma^{init}_{\mathsf{SLS}} p, \sigma$ and $\Sigma^{init}_{\mathsf{SLS}} p, \sigma'$ and
(3) $X^{init}_{\mathsf{SLS}}(p, \sigma)$ and $X^{init}_{\mathsf{SLS}}(p, \sigma')$

Notice that by definition of $X^{init}_{\mathsf{SLS}}()$ and $\Sigma^{init}_{\mathsf{SLS}}$ we have:

$$X^{init}_{\mathsf{SLS}}(p, \sigma) = \langle p, 0, \sigma, \emptyset, \bot\rangle$$
$$X^{init}_{\mathsf{SLS}}(p, \sigma') = \langle p, 0, \sigma, \emptyset, \bot\rangle$$
$$\Sigma^{init}_{\mathsf{SLS}} p, \sigma = \langle p, 0, \sigma, \bot\rangle$$
$$\Sigma^{init}_{\mathsf{SLS}} p, \sigma' = \langle p, 0, \sigma, \bot\rangle$$

I Immediate
II Immediate
III Immediate using Rule Single-Base

□

Lemma 113 (SLS AM: Single step preserves $\cong$). *If*

(1) $\Sigma_{\mathsf{SLS}1} \cong \Sigma_{\mathsf{SLS}2}$ *and*
(2) $\Sigma_{\mathsf{SLS}1} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$ *and* $\Sigma_{\mathsf{SLS}2} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \Sigma''_{\mathsf{SLS}}$

Then

(1) $\Sigma'_{\mathsf{SLS}} \cong \Sigma''_{\mathsf{SLS}}$

Proof. We have

(1) $\Sigma_{\mathsf{SLS}1} \cong \Sigma_{\mathsf{SLS}2}$ and
(2) $\Sigma_{\mathsf{SLS}1} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$ and $\Sigma_{\mathsf{SLS}2} \overset{\tau'}{\rightsquigarrow}_{\mathsf{SLS}} \Sigma''_{\mathsf{SLS}}$

Because of (1), we know that the same rule was used to derive the steps $\Sigma_{\mathsf{SLS}1} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$ and $\Sigma_{\mathsf{SLS}2} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \Sigma''_{\mathsf{SLS}}$.

We know that $\Sigma'_{\mathsf{SLS}}.ctr = \Sigma''_{\mathsf{SLS}}.ctr$, $\Sigma'_{\mathsf{SLS}}.n = \Sigma''_{\mathsf{SLS}}.n$, $\Sigma'_{\mathsf{SLS}}.b = \Sigma''_{\mathsf{SLS}}.b$, because of (1) and the fact that the same rule was used to derive the step.

The proof is analogous to Lemma 60 (S AM: Single step preserves $\cong$).

∎

Lemma 114 (SLS SE: Single step preserves $\cong$). *If*

(1) $X_{\mathsf{SLS}1} \cong X_{\mathsf{SLS}2}$ *and*
(2) $X_{\mathsf{SLS}1} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X'_{\mathsf{SLS}}$ *and* $X_{\mathsf{SLS}2} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X''_{\mathsf{SLS}}$

Then

(1) $X'_{\mathsf{SLS}} \cong X''_{\mathsf{SLS}}$ *and*

Proof. We have

(1) $X_{\mathsf{SLS}1} \cong X_{\mathsf{SLS}2}$ and
(2) $X_{\mathsf{SLS}1} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X'_{\mathsf{SLS}}$ and $X_{\mathsf{SLS}2} \overset{\tau}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X''_{\mathsf{SLS}}$

Because of (1), we know that the same rule was used to derive the steps $X_{\mathsf{SLS}1} \overset{\tau}{\Rightarrow}_{\mathsf{SLS}} X'_{\mathsf{SLS}}$ and $X_{\mathsf{SLS}2} \overset{\tau}{\Rightarrow}_{\mathsf{SLS}} X''_{\mathsf{SLS}}$.

We know that $X'_{\mathsf{SLS}}.ctr = X''_{\mathsf{SLS}}.ctr$, $X'_{\mathsf{SLS}}.n = X''_{\mathsf{SLS}}.n$, $X'_{\mathsf{SLS}}.b = X''_{\mathsf{SLS}}.b$ (where b marks if it is a misprediction or not), because of (1) and the fact that the same rule was used to derive the step.

The proof is analogous to Lemma 61 (S SE: Single step preserves $\cong$). ∎

O.5 Soundness

Lemma 115 (SLS: Soundness Am semantics w.r.t. speculative semantics). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*

If

(1) $\sigma, \sigma' \in \mathit{InitConf}$ *and*
(2) $(p, \sigma) \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}$, $(p, \sigma') \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}$

Then for all prediction oracles O with speculation window at most ω.

I $(p, \sigma) \Downarrow^{O}_{\mathsf{SLS}} \overline{\tau}'$, $(p, \sigma) \Downarrow^{O}_{\mathsf{SLS}} \overline{\tau}'$

Proof. Let $\omega \in \mathbb{N}$ be a speculation window and $\sigma, \sigma' \in \mathit{InitConf}$ be two initial configurations. We have:

(1) $(p, \sigma) \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}$, $(p, \sigma') \Downarrow^{\omega}_{\mathsf{SLS}} \overline{\tau}$

Furthermore, let O be an arbitrary prediction oracle with speculative window at most ω.

The reasoning ins analogous to Lemma 63 (S: Soundness Am semantics w.r.t. speculative semantics) using Lemma 116 (SLS: Soundness Big-step Am semantics w.r.t. oracle semantics) together with Lemma 112 (SLS: Initial states in $\approx$).

∎

Lemma 116 (SLS: Soundness Big-step Am semantics w.r.t. oracle semantics). *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window.*

If

(1) $\Sigma_{\mathsf{SLS}1} \cong \Sigma_{\mathsf{SLS}2}$
(2) $X_{\mathsf{SLS}1} \cong X_{\mathsf{SLS}2}$ *and* $\overline{p} = \emptyset$
(3) $\Sigma_{\mathsf{SLS}1} \approx X_{\mathsf{SLS}1}$ *and* $\Sigma_{\mathsf{SLS}2} \approx X_{\mathsf{SLS}2}$
(4) $\Sigma_{\mathsf{SLS}1} \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1}$ *and* $\Sigma_{\mathsf{SLS}2} \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}2}$

Then for all prediction oracles O with speculation window at most ω.

I $X_{\mathsf{SLS}1} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}'} X'_{\mathsf{SLS}1}, X_{\mathsf{SLS}2} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}''} X'_{\mathsf{SLS}2}$
II $\Sigma'_{\mathsf{SLS}1} \cong \Sigma'_{\mathsf{SLS}2}$
III $X'_{\mathsf{SLS}1} \cong X'_{\mathsf{SLS}2}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{\mathsf{SLS}1} \approx X'_{\mathsf{SLS}1}$ *and* $\Sigma'_{\mathsf{SLS}2} \approx X'_{\mathsf{SLS}2}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. By Induction on $\Sigma_{\mathsf{SLS}1} \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1}$ and $\Sigma_{\mathsf{SLS}2} \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}2}$.

Rule SLS:AM-Reflection We have $\Sigma_{\mathsf{SLS}1} \Downarrow^{\varepsilon}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1}$ and $\Sigma_{\mathsf{SLS}2} \Downarrow^{\varepsilon}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}2}$, where $\Sigma'_{\mathsf{SLS}1} = \Sigma_{\mathsf{SLS}1}$ and $\Sigma'_{\mathsf{SLS}2} = \Sigma_{\mathsf{SLS}2}$.
Furthermore, we use Rule SLS:Reflection to derive $X_{\mathsf{SLS}1} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\varepsilon} X'_{\mathsf{SLS}1}, X_{\mathsf{SLS}2} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\varepsilon} X'_{\mathsf{SLS}2}$ with $X'_{\mathsf{SLS}1} = X_{\mathsf{SLS}1}$ and $X'_{\mathsf{SLS}2} = X_{\mathsf{SLS}2}$.
We now trivially satisfy all conclusions.

Rule SLS:AM-Single We have $\Sigma_{\mathsf{SLS}1} \Downarrow^{\overline{\tau}''}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$ with $\Sigma'_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1}$ and $\Sigma_{\mathsf{SLS}2} \Downarrow^{\overline{\tau}''}_{\mathsf{SLS}} \Sigma''_{\mathsf{SLS}}$ and $\Sigma''_{\mathsf{SLS}} \overset{\tau}{\rightsquigarrow}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}2}$.
We now apply IH on $\Sigma_{\mathsf{SLS}1} \Downarrow^{\overline{\tau}''}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$ and $\Sigma_{\mathsf{SLS}2} \Downarrow^{\overline{\tau}''}_{\mathsf{SLS}} \Sigma''_{\mathsf{SLS}}$ and get

(a) $X_{\mathsf{SLS}1} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}'} X'_{\mathsf{SLS}}, X_{\mathsf{SLS}2} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}''} X''_{\mathsf{SLS}}$
(b) $\Sigma'_{\mathsf{SLS}} \cong \Sigma''_{\mathsf{SLS}}$
(c) $X'_{\mathsf{SLS}} \cong X''_{\mathsf{SLS}}$ and $\overline{\rho}' = \varnothing$
(d) $\Sigma'_{\mathsf{SLS}} \approx X'_{\mathsf{SLS}}$ and $\Sigma''_{\mathsf{SLS}} \approx X''_{\mathsf{SLS}}$
(e) $\overline{\tau}' = \overline{\tau}''$

We proceed by inversion on $\approx$ in $\Sigma'_{\mathsf{SLS}} \approx X'_{\mathsf{SLS}}$ and $\Sigma''_{\mathsf{SLS}} \approx X''_{\mathsf{SLS}}$:

com-single-base We thus have $\Sigma'_{\mathsf{SLS}} \sim X'_{\mathsf{SLS}} \restriction_{com}$ and $INV(\Sigma'_{\mathsf{SLS}}, X'_{\mathsf{SLS}})$ (Similar for Σ''_{SLS} and X''_{SLS}).
We only show the proof for X'_{SLS} here. The proof for X''_{SLS} is analogous, because of $X'_{\mathsf{SLS}} \cong X''_{\mathsf{SLS}}$.
Notice that if $minWndw(X'_{\mathsf{SLS}}) = 0$ 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 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states) using Lemma 117 (SLS: Soundness Single Step AM).

com-single-oracle We thus have

$$\begin{aligned}
X'_{\mathsf{SLS}} =& X_{\mathsf{SLS}3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma, h, n''' \rangle^{l} \\
\Sigma'_{\mathsf{SLS}} =& \Sigma_{\mathsf{SLS}3} \cdot \langle p, ctr, \sigma n \rangle \cdot \langle p, ctr', \sigma', n' \rangle \cdot \Sigma_{\mathsf{SLS}4} \\
X_{\mathsf{SLS}} =& X_{\mathsf{SLS}3} \cdot \langle p, ctr, \sigma h, n'' \rangle \\
\Sigma_{\mathsf{SLS}} =& \Sigma_{\mathsf{SLS}3} \cdot \langle p, ctr, \sigma n \rangle \\
\Sigma_{\mathsf{SLS}} \sim& X_{\mathsf{SLS}} \restriction_{com}
\end{aligned}$$

The form of X''_{SLS} and Σ''_{SLS} is analogous.
The case is analogous to the corresponding case in Lemma 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

com-single-rollback We have

$$\begin{aligned}
X'_{\mathsf{SLS}} =& X_{\mathsf{SLS}3} \cdot \langle p, ctr, \sigma h, n'' \rangle \cdot \langle p, ctr', \sigma'', h', 0 \rangle^{true} \cdot X_{\mathsf{SLS}4} \\
\Sigma'_{\mathsf{SLS}} =& \Sigma_{\mathsf{SLS}3} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', n' \rangle \cdot \Sigma_{\mathsf{SLS}4} \\
X_{\mathsf{SLS}} =& X_{\mathsf{SLS}3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \\
\Sigma_{\mathsf{SLS}} =& \Sigma_{\mathsf{SLS}3} \cdot \langle p, ctr, \sigma, n \rangle \\
\Sigma_{\mathsf{SLS}} \sim& X_{\mathsf{SLS}} \upharpoonright_{com} \\
n' \geq& 0
\end{aligned}$$

The form of X''_{SLS} and Σ''_{SLS} is analogous.

Additionally, we know that the transaction terminates in some state $\Sigma_{\mathsf{SLS}} \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma'''_{\mathsf{SLS}}$. There are two cases depending on n'.

$n' > 0$ Then we know that $\Sigma'_{\mathsf{SLS}} \overset{\tau}{=\!\!\Omega}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1}$ is not a rollback for ctr and Rule SLS:AM-Context or Rule SLS:AM-Rollback for a different transaction with a different ctr was used.

The case is analogous to the corresponding case in Lemma 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

$n' = 0$ Then we know that $\Sigma'_{\mathsf{SLS}} \overset{\tau}{=\!\!\Omega}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1}$ was created by Rule SLS:AM-Rollback and is a rollback for ctr.

I Here we prove that $X'_{\mathsf{SLS}} \overset{\tau_0}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X'_{\mathsf{SLS}1}$ and $X''_{\mathsf{SLS}} \overset{\tau_1}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X'_{\mathsf{SLS}2}$.

Since in X'_{SLS} and X''_{SLS} we have a state with $n = 0$ and we mispredicted, we know that Rule SLS:Rollback applies.

So $X'_{\mathsf{SLS}} \overset{\tau_0}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X'_{\mathsf{SLS}1}$ and $X''_{\mathsf{SLS}} \overset{\tau_1}{\rightsquigarrow}{}^{O}_{\mathsf{SLS}} X'_{\mathsf{SLS}2}$ are derived by Rule SLS:Rollback.

The rest of the case is analogous to the corresponding case Lemma 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states).

□

Lemma 117 (SLS: 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, $\Sigma_{\mathsf{SLS}1} = \Sigma'_{\mathsf{SLS}} \cdot \Phi'_{\mathsf{SLS}}$, $\Sigma_{\mathsf{SLS}2} = \Sigma''_{\mathsf{SLS}} \cdot \Phi''_{\mathsf{SLS}}$ be two speculative states for the always mispredict semantics and $X_{\mathsf{SLS}1}, X_{\mathsf{SLS}2}$, be two speculative states for the speculative semantics.*

If the following conditions hold:

(1) $\Sigma_{\mathsf{SLS}1} \cong \Sigma_{\mathsf{SLS}2}$

(2) $X_{\mathsf{SLS}1} \cong X_{\mathsf{SLS}2}$ *and* $\overline{p} = \emptyset$

(3) $\Sigma_{\mathsf{SLS}1} \approx X_{\mathsf{SLS}1}$ *and* $\Sigma_{\mathsf{SLS}2} \approx X_{\mathsf{SLS}2}$

(4) $\Phi'_{\mathsf{SLS}} \overset{\tau''}{=\!\!\Omega}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1}$ *and* $\Phi''_{\mathsf{SLS}} \overset{\tau''}{=\!\!\Omega}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}2}$

then there are instances $X'_{\mathsf{SLS}1}, X'_{\mathsf{SLS}2}$ for the speculative semantics such that:

I $X_{\mathsf{SLS}1} \;{}^{O}\!\!\downarrow^{\mathsf{SLS}}_{\tau} X'_{\mathsf{SLS}1}$ *and* $X_{\mathsf{SLS}2} \;{}^{O}\!\!\downarrow^{\mathsf{SLS}}_{\tau'} X'_{\mathsf{SLS}2}$

II $\Sigma'_{\mathsf{SLS}1} \cong \Sigma'_{\mathsf{SLS}2}$

III $X'_{\mathsf{SLS}1} \cong X'_{\mathsf{SLS}2}$ *and* $\overline{p} = \emptyset$

IV $\Sigma'_{\mathsf{SLS}1} \approx X'_{\mathsf{SLS}1}$ *and* $\Sigma'_{\mathsf{SLS}2} \approx X'_{\mathsf{SLS}2}$

V $\tau = \tau'$

Proof. We proceed by inversion on $\Phi'_{\mathsf{SLS}} \overset{\tau''}{\Longrightarrow}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1}$ and $\Phi''_{\mathsf{SLS}} \overset{\tau''}{\Longrightarrow}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}2}$:

Rule SLS:AM-General We choose $X'_{\mathsf{SLS}1} = X'_{\mathsf{SLS}}$ and $X'_{\mathsf{SLS}2} = X''_{\mathsf{SLS}}$. The case is analogous to the corresponding case in Lemma 65 (S: Soundness Single Step AM).

Rule SLS:AM-Spec There are two cases depending on the output of the oracle O.

($false, \omega$) **correct prediction w.r.t X'_{SLS}** The return instruction is not skipped.

I We use Rule SLS:Spec-Exe to derive the steps $X_{\mathsf{SLS}1} \overset{O}{\underset{}{\xrightarrow{\tau_0}}}_{\mathsf{SLS}} X'_{\mathsf{SLS}}$ and $X_{\mathsf{SLS}2} \overset{O}{\xrightarrow{\tau_1}}_{\mathsf{SLS}} X''_{\mathsf{SLS}}$.
Furthermore, we execute Rule SLS:General twice, because Rule SLS:Spec-Exe created two observations in $\overline{\rho}$. We now have $X'_{\mathsf{SLS}1} = X'_{\mathsf{SLS}}$ 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 $X_{\mathsf{SLS}1} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}} X'_{\mathsf{SLS}1}$ and $X_{\mathsf{SLS}2} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}'} X'_{\mathsf{SLS}2}$.

II By Lemma 113 (SLS AM: Single step preserves $\cong$).

III By Lemma 114 (SLS SE: Single step preserves $\cong$) for $X_{\mathsf{SLS}1} \overset{O}{\xrightarrow{\tau_0}}_{\mathsf{SLS}} X'_{\mathsf{SLS}}$ and $X_{\mathsf{SLS}2} \overset{O}{\xrightarrow{\tau_1}}_{\mathsf{SLS}} X''_{\mathsf{SLS}}$ and the fact that the use of Rule SLS: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 SLS:General twice.

IV We have

$$
\begin{aligned}
X'_{\mathsf{SLS}1} =& X_{\mathsf{SLS}}{}'_3 \cdot \langle p, ctr, \sigma', h, n\rangle \cdot \langle p, ctr', \sigma', h', n_0\rangle \\
\Sigma'_{\mathsf{SLS}1} =& \Sigma_{\mathsf{SLS}3} \cdot \langle p, ctr, \sigma', n_1\rangle \cdot \langle p, ctr', \sigma'', n_2\rangle \\
X'_{\mathsf{SLS}4} =& X_{\mathsf{SLS}}{}'_3 \cdot \langle p, ctr, \sigma', h, n\rangle \\
\Sigma'_{\mathsf{SLS}4} =& \Sigma_{\mathsf{SLS}3} \cdot \langle p, ctr, \sigma', n_1\rangle
\end{aligned}
$$

The case is analogous to the Rule S:AM-Store-Spec correct prediction case in Lemma 65 (S: Soundness Single Step AM)/

V The observations are $\overline{\tau} = \texttt{ret}\ m \cdot \texttt{start}_{\mathsf{SLS}}\ ctr_1$ and $\overline{\tau}' = \texttt{ret}\ m' \cdot \texttt{start}_{\mathsf{SLS}}\ ctr_2$ for some $m, m' \in Vals$.
The case is analogous to the Rule S:AM-Store-Spec correct prediction case in Lemma 65 (S: Soundness Single Step AM).

($false, \omega$) **wrong prediction w.r.t X'_{SLS}** The return instruction is skipped

a) We use Rule SLS:Spec to derive the steps $X'_{\mathsf{SLS}} \overset{O}{\xrightarrow{\tau_0}}_{\mathsf{SLS}} X'_{\mathsf{SLS}1}$ and $X''_{\mathsf{SLS}} \overset{O}{\xrightarrow{\tau_1}}_{\mathsf{SLS}} X'_{\mathsf{SLS}2}$.
Furthermore, we execute Rule SLS:General twice, because Rule SLS:Spec created two observations in $\overline{\rho}$. We now have $X'_{\mathsf{SLS}1} = X'_{\mathsf{SLS}}$ 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 $X_{\mathsf{SLS}1} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}} X'_{\mathsf{SLS}1}$ and $X_{\mathsf{SLS}2} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}'} X'_{\mathsf{SLS}2}$.
Notice that the observations in $\overline{\rho}$ are equal between $X_{\mathsf{SLS}1}$ and $X_{\mathsf{SLS}2}$, because of (2). We have $X_{\mathsf{SLS}1}.ctr = X_{\mathsf{SLS}2}.ctr$ and $X_{\mathsf{SLS}1}.\sigma \sim_{\mathbf{pc}} X_{\mathsf{SLS}2}.\sigma$ from our relation.

b) By Lemma 113 (SLS AM: Single step preserves $\cong$).

c) By Lemma 114 (SLS 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:

$$\begin{aligned}X'_{\mathsf{SLS}1} =& X_{\mathsf{SLS}}{}'_3 \cdot \langle p, ctr, \sigma', h, n\rangle \cdot \langle p, ctr', \sigma''', h', n_0\rangle\\ \Sigma'_{\mathsf{SLS}1} =& \Sigma_{\mathsf{SLS}3} \cdot \langle p, ctr, \sigma', n_1\rangle \cdot \langle p, ctr', \sigma'', n_2\rangle\\ X'_{\mathsf{SLS}4} =& X_{\mathsf{SLS}}{}'_3 \cdot \langle p, ctr, \sigma', h, n\rangle\\ \Sigma'_{\mathsf{SLS}4} =& \Sigma_{\mathsf{SLS}3} \cdot \langle p, ctr, \sigma', n_1\rangle\end{aligned}$$

The case is analogous to the Rule S:AM-Store-Spec wrong prediction case in Lemma 65 (S: Soundness Single Step AM).

V) The observations are

$$\begin{aligned}\overline{\tau} =& \texttt{ret}\ m \cdot \texttt{start}\ X_{\mathsf{SLS}1}.ctr \cdot \texttt{bypass}\ X_{\mathsf{SLS}1}.\sigma(\mathbf{pc})\\ \overline{\tau}' =& \texttt{ret}\ m' \cdot \texttt{start}\ X_{\mathsf{SLS}2}.ctr \cdot \texttt{bypass}\ X_{\mathsf{SLS}2}.\sigma(\mathbf{pc})\end{aligned}$$

for some $m, m' \in Vals$.

The case is analogous to the misprediction case in Lemma 65 (S: Soundness Single Step AM).

Rule SLS:AM-barr and Rule SLS:AM-barr-spec We prove this for Rule SLS:AM-barr-spec. The proof for Rule SLS:AM-barr is analogous.

The proof is analogous to the corresponding case in Lemma 65 (S: Soundness Single Step AM) using Lemma 113 (SLS AM: Single step preserves ≅) and Lemma 114 (SLS SE: Single step preserves ≅),

Rule SLS:AM-NoSpec 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 $INV(\Sigma'_{\mathsf{SLS}1}, X'_{\mathsf{SLS}1})$ is analogous to the corresponding case in Lemma 65 (S: Soundness Single Step AM).

□

O.6 Completeness

Definition 38 (Constructing the Oracle $O_{am}{}^{\mathsf{SLS}}$)**.** *The oracle is built upon a specific executions:* $\Sigma^{init}_{\mathsf{SLS}} p, \sigma \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma_{\mathsf{SLS}1} \xrightarrow{\tau_{am}}_{\mathsf{SLS}} \Sigma_{\mathsf{SLS}2}$, $\Sigma^{init}_{\mathsf{SLS}} p, \sigma' \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1} \xrightarrow{\tau'_{am}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}2}$ *where* $\tau_{am} \neq \tau'_{am}$.

Let us denote by the set RB the ids of all ongoing transaction ids in $\Sigma_{\mathsf{SLS}1}$*. Since* $\Sigma_{\mathsf{SLS}1} \cong \Sigma'_{\mathsf{SLS}1}$ *we know that the same transaction ids are still ongoing in* $\Sigma'_{\mathsf{SLS}1}$ *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:

$$O_{am}{}^{\mathsf{SLS}}(p, n, h) = \begin{cases}(false, \omega) \text{ if } |h| \in RB \land p(\sigma(\mathbf{pc})) = \mathbf{ret}\\ (true, 0) \text{ otherwise (where } p(\sigma(\mathbf{pc})) = \mathbf{ret})\end{cases}$$

Lemma 118 (SLS: 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) $p, \sigma \Omega^{\omega}_{\mathsf{SLS}}\ \overline{\tau}$ *and* $p, \sigma' \Omega^{\omega}_{\mathsf{SLS}}\ \overline{\tau}'$ *and*
(2) $\overline{\tau} \neq \overline{\tau}'$

Then there exists an oracle O such that

I $p, \sigma \Omega^{O}_{\mathsf{SLS}}\ \overline{\tau}_1$ *and* $p, \sigma' \Omega^{O}_{\mathsf{SLS}}\ \overline{\tau}'_1$ *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. We have If

(1) $p, \sigma \; \Omega^{\omega}_{\mathsf{SLS}} \; \overline{\tau}$ and $p, \sigma' \; \Omega^{\omega}_{\mathsf{SLS}} \; \overline{\tau}'$ and
(2) $\overline{\tau} \neq \overline{\tau}'$

By definition of $\Omega^{\omega}_{\mathsf{SLS}}$ we have two final states $\Sigma_{\mathsf{SLS}F}$ and $\Sigma'_{\mathsf{SLS}F}$ such that $\Sigma^{init}_{\mathsf{SLS}} p, \sigma \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma_{\mathsf{SLS}F}$ $\Sigma^{init}_{\mathsf{SLS}} p, \sigma' \Downarrow^{\overline{\tau}'}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}F}$. Combined with the fact that $\overline{\tau} \neq \overline{\tau}'$, it follows that there are speculative states $\Sigma_{\mathsf{SLS}1}, \Sigma_{\mathsf{SLS}}, \Sigma'_{\mathsf{SLS}1}, \Sigma'_{\mathsf{SLS}2}$ and sequences of observations $\overline{\tau}, \overline{\tau}_{end}, \overline{\tau}'_{end}, \tau_{am}, \tau'_{am}$ such that $\tau_{am} \neq \tau'_{am}$, $\Sigma_{\mathsf{SLS}1} \cong \Sigma'_{\mathsf{SLS}1}$ and:

$$\Sigma^{init}_{\mathsf{SLS}} p, \sigma \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma_{\mathsf{SLS}1} \xrightarrow{\tau_{am}}_{\mathsf{SLS}} \Sigma_{\mathsf{SLS}2} \Downarrow^{\overline{\tau}_{end}}_{\mathsf{SLS}} \Sigma_{\mathsf{SLS}F}$$

$$\Sigma^{init}_{\mathsf{SLS}} p, \sigma' \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1} \xrightarrow{\tau'_{am}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}2} \Downarrow^{\overline{\tau}'_{end}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}F}$$

We claim that there is a prediction oracle ${O_{am}}^{\mathsf{SLS}}$ with a speculative window at most ω such that

a $X^{init}_{\mathsf{SLS}}(p, \sigma) \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{v} X_{\mathsf{SLS}1}$ and $X_{\mathsf{SLS}1}.\sigma = \Sigma_{\mathsf{SLS}1}.\sigma$ and $\mathit{INV2}(X_{\mathsf{SLS}1}, \Sigma_{\mathsf{SLS}1})$ and
b $X^{init}_{\mathsf{SLS}}(p, \sigma') \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{v} X'_{\mathsf{SLS}1}$ and $X'_{\mathsf{SLS}1}.\sigma = \Sigma'_{\mathsf{SLS}1}.\sigma$ and $\mathit{INV2}(X'_{\mathsf{SLS}1}, \Sigma'_{\mathsf{SLS}1})$
c $X_{\mathsf{SLS}1} \cong X'_{\mathsf{SLS}1}$

We get this by applying Lemma 120 (SLS: Stronger Soundness for a specific oracle and for specific executions) on the Am execution up to the point of the difference i.e., $\Sigma^{init}_{\mathsf{SLS}} p, \sigma \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma_{\mathsf{SLS}1}$ with the ${O_{am}}^{\mathsf{SLS}}$ and Σ^{States}_1 being all the states in $\Sigma^{init}_{\mathsf{SLS}} p, \sigma \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma_{\mathsf{SLS}1}$ (similar for Σ^{States}_2 for $\Sigma^{init}_{\mathsf{SLS}} p, \sigma' \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1}$).

We now show that $\Sigma_{\mathsf{SLS}1} \approx^{\Sigma^{States}_1}_{{O_{am}}^{\mathsf{SLS}}} X_{\mathsf{SLS}1}$ is derived by Rule Single-Base-Oracle (similar for $\Sigma_{\mathsf{SLS}2} \approx^{\Sigma^{States}_2}_{{O_{am}}^{\mathsf{SLS}}} X_{\mathsf{SLS}2}$).

We do a case distinction if there are ongoing transactions in $X_{\mathsf{SLS}1}$ or not

no ongoing transactions in $X_{\mathsf{SLS}1}$ Then $\Sigma_{\mathsf{SLS}1} \approx^{\Sigma^{States}_1}_{{O_{am}}^{\mathsf{SLS}}} X_{\mathsf{SLS}1}$ can only be derived Rule Single-Base-Oracle and $\Sigma_{\mathsf{SLS}1}$ has no ongoing transactions as well. Then we have by $\mathit{INV2}(\Sigma_{\mathsf{SLS}1}, X_{\mathsf{SLS}1})$ and $\Sigma_{\mathsf{SLS}1}.n = \bot$ that $X_{\mathsf{SLS}1}.n = \bot$.

ongoing transactions in X_{SLS} By the definition of the oracle O, we know that 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_{SLS}.

Furthermore, we know that $X_{\mathsf{SLS}1}.n \geq \mathit{minWndw}(X_{\mathsf{SLS}1})$ by definition of the oracle ${O_{am}}^{\mathsf{SLS}}$ and $\mathit{minWndw}()$. Since the next rule cannot be Rule SLS:AM-Rollback, we know that $\Sigma_{\mathsf{SLS}1}.n > 0$ and by $\mathit{INV2}(\Sigma_{\mathsf{SLS}1}, X_{\mathsf{SLS}1})$ we get $\mathit{minWndw}(X_{\mathsf{SLS}1}) > 0$ (Similar for $X'_{\mathsf{SLS}1}$ because of $\Sigma_{\mathsf{SLS}1} \cong \Sigma'_{\mathsf{SLS}1}$).

If $\Sigma_{\mathsf{SLS}1} \approx^{\Sigma^{States}}_{{O_{am}}^{\mathsf{SLS}}} X_{\mathsf{SLS}1}$ by rollback rule, we would have a contradiction because we would need the topmost speculation window of $X_{\mathsf{SLS}1}.n = 0$. But we know that $\mathit{minWndw}(X_{\mathsf{SLS}1}) > 0$, because the speculation window of the topmost instance was created with a speculation window of ω.

Thus, we know that $X_{\mathsf{SLS}1} \approx^{\Sigma^{States}_1}_{{O_{am}}^{\mathsf{SLS}}} \Sigma_{\mathsf{SLS}1}$ by Rule Single-Base-Oracle.

We now proceed by case analysis on the rule in $\xrightarrow{}_{\mathsf{SLS}}$ used to derive $\Sigma_{\mathsf{SLS}1} \xrightarrow{\tau_{am}}_{\mathsf{SLS}} \Sigma_{\mathsf{SLS}2}$. Because $\Sigma_{\mathsf{SLS}1} \cong \Sigma'_{\mathsf{SLS}1}$ and $\overline{\tau}_1 = \overline{\tau}'_1$, we know that the same rule was used in $\Sigma'_{\mathsf{SLS}1} \xrightarrow{\tau'_{am}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}2}$ as well.

Rule SLS:AM-Rollback Contradiction. Because $\Sigma_{\mathsf{SLS}1} \cong \Sigma'_{\mathsf{SLS}1}$ 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 SLS:AM-Context By inversion on Rule SLS:AM-Context for the step $\Sigma_{SLS1} \overset{\tau_{am}}{=\!\!\!=\!\!\!\rightsquigarrow}_{SLS} \Sigma_{SLS2}$ we have $\Sigma_{SLS1} = \overline{\Phi}_{SLS} \cdot \Phi_{SLS}$ and $\Sigma_{SLS2} = \overline{\Phi}_{SLS} \cdot \overline{\Phi}'_{SLS}$ with $\Phi_{SLS} \overset{\tau_{am}}{=\!\!\!=\!\!\!\rightsquigarrow}_{SLS} \overline{\Phi}'_{SLS}$.

We now do inversion on $\Sigma_{SLS1} \overset{\tau_{am}}{=\!\!\!=\!\!\!\rightsquigarrow}_{SLS} \Sigma_{SLS2}$ and $\Phi_{SLS} \overset{\tau_{am}}{=\!\!\!=\!\!\!\rightsquigarrow}_{SLS} \overline{\Phi}'_{S}$:

Rule SLS:AM-General Contradiction. By $\Sigma_{SLS1} \cong \Sigma'_{SLS1}$ we know that $\Sigma_{SLS1}.\overline{\rho} = \Sigma'_{SLS1}.\overline{\rho}$.

This immediately implies that $\tau_{am} = \tau_{am'}$, which is not true by assumption.

Rule SLS:AM-barr-spec, Rule SLS:AM-barr Contradiction. Since these rules do not generate any observation by definition.

This leads to $\tau_{am} = \tau_{am'}$.

Rule SLS:AM-NoSpec and Rule SLS:AM-Spec We fulfil all assumptions for Lemma 119 (SLS: AM and Oracle coincide) and get $X_{S1} \overset{\tau_{am}}{\rightsquigarrow}{}^{O}_{S} X_{S2}$ and $X'_{S1} \overset{\tau'_{am}}{\rightsquigarrow}{}^{O}_{S} X'_{S2}$.

Since $\tau_{am} \neq \tau'_{am}$ by assumption we are finished.

This completes the proof of our claim.

□

Lemma 119 (SLS: AM and Oracle coincide)**.** *If*

(1) $\Sigma_{SLS} \approx^{\Sigma^{States}_{X_{SLS}}}_{O_{am}{}^{SLS}}$ *by Base and*
(2) $\Sigma_{SLS} \overset{\tau}{=\!\!\!\rightsquigarrow}_{SLS} \Sigma'_{SLS}$ *and*
(3) $minWndw(\Sigma_{SLS}) > 0$
(4) $X_{SLS}.\overline{\rho} = \varnothing$

Then

(1) $X_{SLS} \overset{\tau}{\rightsquigarrow}{}^{O}_{SLS} X'_{SLS}$

Proof. Since $minWndw(\Sigma_{SLS}) > 0$ we know that the next step is not a rollback. From $minWndw(\Sigma_{SLS}) > 0$ and $\Sigma_{SLS} \approx^{\Sigma^{States}}_{O_{am}} X_{SLS}$ we have *INV2*(Σ_{SLS}, X_{SLS}) and we get $minWndw(X_{SLS}) > 0$ as well.

We proceed by inversion on $\Sigma_{SLS} \overset{\tau}{=\!\!\!\rightsquigarrow}_{SLS} \Sigma'_{SLS}$:

Rule SLS:AM-NoSpec From the rule, we have that $\Sigma_{SLS}.\sigma \xrightarrow{\tau} \Sigma'_{SLS}.\sigma$.

The case is analogous to the corresponding case in Lemma 67 (S: AM and Oracle coincide).

Rule SLS:AM-barr-spec, Rule SLS:AM-barr From the rule, we have that $\Sigma_{SLS}.\sigma \rightarrow \Sigma'_{SLS}.\sigma$.

The case is analogous to the case above.

Rule SLS:AM-Spec Then, τ is generated by the step $\Sigma_{SLS}.\sigma \xrightarrow{\tau} \Sigma'_{SLS}.\sigma$ generated by Rule SLS:AM-Spec.

The case is analogous to the corresponding case in Lemma 67 (S: AM and Oracle coincide).

□

Lemma 120 (SLS: 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 $O_{am}{}^{SLS}$ as it is defined by Definition 38 (Constructing the Oracle $O_{am}{}^{SLS}$) for the given execution. If*

(1) $\Sigma_{SLS1} \cong \Sigma_{SLS2}$
(2) $X_{SLS1} \cong X_{SLS2}$ *and* $\overline{\rho} = \varnothing$
(3) $\Sigma_{SLS1} \approx^{\Sigma^{States}_{1}}_{O_{am}{}^{SLS}} X_{SLS1}$ *and* $\Sigma_{SLS2} \approx^{\Sigma^{States}_{2}}_{O_{am}{}^{SLS}} X_{SLS2}$

(4) $\Sigma_{\mathsf{SLS}1} \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1}$ *and* $\Sigma_{\mathsf{SLS}2} \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}2}$
(5) $\Sigma^{States}_{1} = \Sigma_{\mathsf{SLS}1} \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1}$ *and* $\Sigma^{States}_{2} = \Sigma_{\mathsf{SLS}2} \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}2}$

and our oracle is constructed in the way described above Then

I $X_{\mathsf{SLS}1} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}'} X'_{\mathsf{SLS}1}, X_{\mathsf{SLS}2} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}''} X'_{\mathsf{SLS}2}$
II $\Sigma'_{\mathsf{SLS}1} \cong \Sigma'_{\mathsf{SLS}2}$
III $X'_{\mathsf{SLS}1} \cong X'_{\mathsf{SLS}2}$ *and* $\overline{\rho} = \varnothing$
IV $\Sigma'_{\mathsf{SLS}1} \approx^{\Sigma^{States}_1}_{O_{am}}{}^{\mathsf{SLS}} X'_{\mathsf{SLS}1}$ *and* $\Sigma'_{\mathsf{SLS}2} \approx^{\Sigma^{States}_2}_{O_{am}}{}^{\mathsf{SLS}} X'_{\mathsf{SLS}2}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. Notice that the proof is very similar to Lemma 64 (S: Soundness Am semantics w.r.t. speculative semantics with new relation between states). The only different thing 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 $INV2(\Sigma'_{\mathsf{SLS}1}, X'_{\mathsf{SLS}1})$ holds in the different cases and leave the rest to the old soundness proof.

By Induction on $\Sigma_{\mathsf{SLS}1} \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1}$ and $\Sigma_{\mathsf{SLS}2} \Downarrow^{\overline{\tau}}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}2}$.

Rule SLS:AM-Reflection We have $\Sigma_{\mathsf{SLS}1} \Downarrow^{\varepsilon}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$ and $\Sigma_{\mathsf{SLS}2} \Downarrow^{\varepsilon}_{\mathsf{SLS}} \Sigma''_{\mathsf{SLS}}$, where $\Sigma'_{\mathsf{SLS}} = \Sigma_{\mathsf{SLS}1}$ and $\Sigma''_{\mathsf{SLS}} = \Sigma_{\mathsf{SLS}2}$. We choose $\Sigma'_{\mathsf{SLS}1} = \Sigma'_{\mathsf{SLS}}$ and $\Sigma'_{\mathsf{SLS}2} = \Sigma''_{\mathsf{SLS}}$.

We further use Rule SLS:Reflection to derive $X_{\mathsf{SLS}1} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\varepsilon} X'_{\mathsf{SLS}1}, X_{\mathsf{SLS}2} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\varepsilon} X'_{\mathsf{SLS}2}$ with $X'_{\mathsf{SLS}1} = X_{\mathsf{SLS}1}$ and $X'_{\mathsf{SLS}2} = X_{\mathsf{SLS}2}$. We now trivially satisfy all conclusions.

Rule SLS:AM-Single We have $\Sigma_{\mathsf{SLS}1} \Downarrow^{\overline{\tau}''}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$ with $\Sigma'_{\mathsf{SLS}} \overset{\tau}{\Rightarrow}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1}$ and $\Sigma_{\mathsf{SLS}2} \Downarrow^{\overline{\tau}''}_{\mathsf{SLS}} \Sigma''_{\mathsf{SLS}}$ and $\Sigma''_{\mathsf{SLS}} \overset{\tau}{\Rightarrow}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}2}$.

We now apply IH on $\Sigma_{\mathsf{SLS}1} \Downarrow^{\overline{\tau}''}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}}$ and $\Sigma_{\mathsf{SLS}2} \Downarrow^{\overline{\tau}''}_{\mathsf{SLS}} \Sigma''_{\mathsf{SLS}}$ and get

(a) $X_{\mathsf{SLS}1} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}'} X'_{\mathsf{SLS}}, X_{\mathsf{SLS}2} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\overline{\tau}''} X''_{\mathsf{SLS}}$
(b) $\Sigma'_{\mathsf{SLS}} \cong \Sigma''_{\mathsf{SLS}}$
(c) $X'_{\mathsf{SLS}} \cong X''_{\mathsf{SLS}}$ and $\overline{\rho}' = \varnothing$
(d) $\Sigma'_{\mathsf{SLS}} \approx^{\Sigma^{States}_1}_{O_{am}}{}^{\mathsf{SLS}} X'_{\mathsf{SLS}}$ and $\Sigma''_{\mathsf{SLS}} \approx^{\Sigma^{States}_2}_{O_{am}}{}^{\mathsf{SLS}} X''_{\mathsf{SLS}}$
(e) $\overline{\tau}' = \overline{\tau}''$

We do a case distinction on $\approx^{\Sigma^{States}_1}_{O_{am}}{}^{\mathsf{SLS}}$ in $\Sigma'_{\mathsf{SLS}} \approx^{\Sigma^{States}_1}_{O_{am}}{}^{\mathsf{SLS}} X'_{\mathsf{SLS}}$ and $\Sigma''_{\mathsf{SLS}} \approx^{\Sigma^{States}_2}_{O_{am}}{}^{\mathsf{SLS}} X''_{\mathsf{SLS}}$ by inversion:

sls-com-single-base We thus have $\Sigma'_{\mathsf{SLS}} \sim X'_{\mathsf{SLS}}\upharpoonright_{com}$, $minWndw(X'_{\mathsf{SLS}}) > 0$ and $INV2(\Sigma'_{\mathsf{SLS}}, X'_{\mathsf{SLS}})$ (Similar for Σ''_{SLS} and X''_{SLS}).

We now proceed by inversion on the derivation $\Sigma'_{\mathsf{SLS}} \overset{\tau}{\Rightarrow}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1}$.

Rule SLS:AM-Rollback Contradiction, because of $minWndw(X'_{\mathsf{SLS}}) > 0$ and $INV2(\Sigma'_{\mathsf{SLS}}, X'_{\mathsf{SLS}})$.

Rule SLS:AM-General $INV2()$ trivially holds, because it does not change the speculation window of the states.

Rule SLS:AM-Context We have $\Phi_{\mathsf{SLS}} \overset{\tau}{\Rightarrow}_{\mathsf{SLS}} \overline{\Phi}_{\mathsf{SLS}}$ and $\Phi'_{\mathsf{SLS}} \overset{\tau}{\Rightarrow}_{\mathsf{SLS}} \overline{\Phi}'_{\mathsf{SLS}}$. We fulfil all conditions for Lemma 121 (SLS AM: Strong Soundness Single Step) which gives us the desired result.

sls-com-single-rollback We have

$$\begin{aligned}
X'_{\mathsf{SLS}} =& X_{\mathsf{SLS}3} \cdot \langle p, ctr, \sigma, h, n'' \rangle \cdot \langle p, ctr', \sigma'', h', 0 \rangle \cdot X_{\mathsf{SLS}4}\\
\Sigma'_{\mathsf{SLS}} =& \Sigma_{\mathsf{SLS}3} \cdot \langle p, ctr, \sigma, n \rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', n' \rangle \cdot \Sigma_{\mathsf{SLS}4}\\
X_{\mathsf{SLS}} =& X_{\mathsf{SLS}3} \cdot \langle p, ctr, \sigma, h, n'' \rangle\\
\Sigma_{\mathsf{SLS}} =& \Sigma_{\mathsf{SLS}3} \cdot \langle p, ctr, \sigma, n \rangle\\
\Sigma_{\mathsf{SLS}} \sim& X_{\mathsf{SLS}} \upharpoonright_{com}\\
& \mathit{INV2}(\Sigma_{\mathsf{SLS}}, X_{\mathsf{SLS}})\\
n' \geq& 0
\end{aligned}$$

The form of X''_{SLS} and Σ''_{SLS} is analogous.

The case is analogous to the corresponding case in Lemma 68 (S: Stronger Soundness for a specific oracle and for specific executions).

□

Lemma 121 (SLS AM: 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, $\Sigma_{\mathsf{SLS}1} = \Sigma'_{\mathsf{SLS}} \cdot \Phi'_{\mathsf{SLS}}$, $\Sigma_{\mathsf{SLS}2} = \Sigma''_{\mathsf{SLS}} \cdot \Phi''_{\mathsf{SLS}}$ be two speculative states for the always mispredict semantics and $X_{\mathsf{SLS}1}, X_{\mathsf{SLS}2}$, be two speculative states for the speculative semantics.*

If the following conditions hold:

(1) $\Sigma_{\mathsf{SLS}1} \cong \Sigma_{\mathsf{SLS}2}$

(2) $X_{\mathsf{SLS}1} \cong X_{\mathsf{SLS}2}$ *and* $\overline{p} = \varnothing$

(3) $\Sigma_{\mathsf{SLS}1} \approx^{\Sigma_1^{States}}_{O_{am}{}^{\mathsf{SLS}}} X_{\mathsf{SLS}1}$ *and* $\Sigma_{\mathsf{SLS}2} \approx^{\Sigma_2^{States}}_{O_{am}{}^{\mathsf{SLS}}} X_{\mathsf{SLS}2}$

(4) $\Phi'_{\mathsf{SLS}} \overset{\tau''}{\Longrightarrow}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}1}$ *and* $\Phi''_{\mathsf{SLS}} \overset{\tau''}{\Longrightarrow}_{\mathsf{SLS}} \Sigma'_{\mathsf{SLS}2}$

(5) $\Sigma'_{\mathsf{SLS}1} \in \Sigma_1^{States}$ *and* $\Sigma'_{\mathsf{SLS}1} \in \Sigma_2^{States}$

then there are instances $X'_{\mathsf{SLS}1}, X'_{\mathsf{SLS}2}$ for the speculative semantics such that:

I $X_{\mathsf{SLS}1} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\tau} X'_{\mathsf{SLS}1}$ *and* $X_{\mathsf{SLS}2} \overset{O}{\rightsquigarrow}{}^{\mathsf{SLS}}_{\tau'} X'_{\mathsf{SLS}2}$

II $\Sigma'_{\mathsf{SLS}1} \cong \Sigma'_{\mathsf{SLS}2}$

III $X'_{\mathsf{SLS}1} \cong X'_{\mathsf{SLS}2}$ *and* $\overline{p} = \varnothing$

IV $\Sigma'_{\mathsf{SLS}1} \approx^{\Sigma_1^{States}}_{O_{am}{}^{\mathsf{SLS}}} X'_{\mathsf{SLS}1}$ *and* $\Sigma'_{\mathsf{SLS}2} \approx^{\Sigma_2^{States}}_{O_{am}{}^{\mathsf{SLS}}} X'_{\mathsf{SLS}2}$

V $\tau = \tau'$

Proof. The proof is very similar to Lemma 65 (S: Soundness Single Step AM). The only different thing 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., $\mathit{INV2}(\Sigma_{\mathsf{SLS}}, X_{\mathsf{SLS}})$

For these reasons, we will only argue why $\mathit{INV2}(\Sigma'_{\mathsf{SLS}1}, X'_{\mathsf{SLS}1})$ holds in the different cases and leave the rest to the old soundness proof.

Now we do case distinction on the instruction executed:

not ret instruction This includes the rules Rule SLS:NoSpec. We prove that $\mathit{INV2}(\Sigma'_{\mathsf{SLS}1}, X'_{\mathsf{SLS}1})$ still holds. The proof for $\mathit{INV2}(\Sigma'_{\mathsf{SLS}2}, X'_{\mathsf{SLS}2})$ is analogous.

The proof is analogous to the corresponding case 'not store instruction' in Lemma 68 (S: Stronger Soundness for a specific oracle and for specific executions).

Rule SLS:AM-Spec We know that our oracle only mispredicts. That is why only rule SLS:Spec will be used for oracle states. We know that rule SLS:Spec applies since it is a **ret** instruction. We have:

$$X'_{\mathsf{SLS}1} = X'''_{\mathsf{SLS}} \cdot \Psi_{\mathsf{SLS}}$$
$$minWndw(X'''_{\mathsf{SLS}}) = minWndw(decr(X'_{\mathsf{SLS}})) = minWndw(X'_{\mathsf{SLS}}) - 1$$
$$X'_{\mathsf{SLS}}.\sigma \xrightarrow{\tau} X'''_{\mathsf{SLS}}.\sigma$$
$$\Sigma'_{\mathsf{SLS}1} = \Sigma'''_{\mathsf{SLS}} \cdot \Phi_{\mathsf{SLS}}$$
$$\Sigma'''_{\mathsf{SLS}}.n = \Sigma'_{\mathsf{SLS}}.n - 1$$
$$\Sigma'_{\mathsf{SLS}}.\sigma \xrightarrow{\tau} \Sigma'''_{\mathsf{SLS}}.\sigma$$

Note that the step $minWndw(decr(X'_{\mathsf{SLS}})) = minWndw(X'_{\mathsf{SLS}}) - 1$ comes from the fact that $minWndw(X'_{\mathsf{SLS}}) = \Sigma'_{\mathsf{SLS}}.n$ and $\Sigma_{\mathsf{SLS}}.n > 0$ by assumption.

Depending on the output of the oracle we switch the relation

$O(p, \sigma, h) = (true, 0)$ We need to show that $INV2(\Sigma'''_{\mathsf{SLS}}, X'''_{\mathsf{SLS}})$ holds. The argument is the same as above for not **ret** instructions.

$O(p, \sigma, h) = (true, \omega)$ We need to show that $INV2(\Sigma'''_{\mathsf{SLS}} \cdot \Phi_{\mathsf{SLS}}, X'''_{\mathsf{SLS}} \cdot \Phi_{\mathsf{SLS}})$ holds.

The case is analogous to the corresponding case (store misprediction) in Lemma 68 (S: Stronger Soundness for a specific oracle and for specific executions).

□

P SPECTECTOR'S SOUNDNESS AND COMPLETENESS

Below, we provide the proof of Theorem 26, which we restate here for simplicity:

Theorem 26 (Correctness Spectector). *If Spectector(p, P, w) terminates, then Spectector(p, P, w) = Secure iff the program p satisfies speculative non-interference w.r.t. the policy P, , a secure speculative semantics ⊢ x WFSS and all prediction oracles O with speculative window at most w.*

Proof. Theorem 26 immediately follows from Spectector's soundness (see Lemma 122) and completeness (see Lemma 123). □

These proofs rely on the definition of secure speculative semantics, which we restate here for simplicity: A speculative semantics $\mathcal{Q}_x$ is secure (denoted $\vdash \mathcal{Q}_x$ *WFSS*) if:

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

Lemma 122 states that if Spectector determines a program to be secure, the program is speculatively non-interferent.

Lemma 122. *Whenever Spectector(p, P, w) = Secure, the program p satisfies speculative non-interference w.r.t. the policy P, a secure speculative semantics ⊢ x WFSS and any oracle O with speculative window at most w.*

Proof. If $\textsc{Spectector}(p, P, w) = \textsc{Secure}$, then for all symbolic traces τ, $\textsc{MemLeak}(\tau) = \bot$ and $\textsc{CtrlLeak}(\tau) = \bot$. Let σ and σ' be two arbitrary P-indistinguishable initial configurations producing the same concrete non-speculative trace τ. From **NS Consistency**, σ and σ' result in two concrete speculative traces τ_c and τ_c' with the same non-speculative projection. From **Symbolic Consistency**, τ_c and τ_c' correspond to two symbolic traces τ_s and τ_s'. Since $\textsc{CtrlLeak}(\tau_s) = \bot$, $\textsc{CtrlLeak}(\tau_s') = \bot$, and $\tau_c \upharpoonright_{ns} = \tau_c' \upharpoonright_{ns}$, speculatively executed control-flow instructions produce the same outcome in τ_c and τ_c'. Hence, the same code is executed in both traces and $\tau_s = \tau_s'$. From $\textsc{MemLeak}(\tau_s) = \bot$, the observations produced by speculatively executed **load** and **store** instructions are the same. Thus, $\tau_c = \tau_c'$. Hence, whenever two initial configurations result in the same non-speculative traces, then they produce the same speculative traces. Therefore, p satisfies speculative non-interference w.r.t. the always-mispredict semantics with speculative window w. From this and **Oracle Overapproximation**, p satisfies speculative non-interference w.r.t. any prediction oracle with speculative window at most w. ◻

Lemma 123 states that the leaks found by Spectector are valid counterexamples to speculative non-interference.

Lemma 123. *Whenever $\textsc{Spectector}(p, P, w) = \textsc{Insecure}$, there is an oracle O with speculative window at most w such that program p does not satisfy speculative non-interference w.r.t. O and the policy P.*

Proof. If $\textsc{Spectector}(p, P) = \textsc{Insecure}$, there is a symbolic trace τ for which either $\textsc{MemLeak}(\tau) = \top$ or $\textsc{CtrlLeak}(\tau) = \top$. In the first case, $pthCnd(\tau) \wedge polEqv(P) \wedge obsEqv(\tau \upharpoonright_{ns}) \wedge \neg obsEqv(\tau \upharpoonright_{se})$ is satisfiable. Then, there are two models for the symbolic trace τ that (1) satisfy the path condition encoded in τ, (2) agree on the non-sensitive registers and memory locations in P, (3) produce the same non-speculative projection, and (4) the speculative projections differ on a **load** or **store** observation. From **Symbolic Consistency**, the two concretizations correspond to two concrete runs, with different traces, whose non-speculative projection are the same. By combining this with **NS Consistency**, there are two configurations that produce the same non-speculative trace but different speculative traces. This is a violation of speculative non-interference.

In the second case, there is a prefix $v \cdot \texttt{symPc}(se)$ of $\tau \upharpoonright_{se}$ such that $pthCnd(\tau \upharpoonright_{ns} \cdot v) \wedge polEqv(P) \wedge obsEqv(\tau \upharpoonright_{ns}) \wedge \neg(se_1 \leftrightarrow se_2)$ is satisfiable. Hence, there are two symbolic traces τ and τ' that produce the same non-speculative observations but differ on a program counter observation $\texttt{pc}\ n$ in their speculative projections. Again, this implies, through **Symbolic Consistency** and **NS Consistency**, that there are two P-indistinguishable initial configurations producing the same non-speculative traces but distinct speculative traces, leading to a violation of speculative non-interference.

In both cases, p does not satisfy speculative non-interference w.r.t. the always-mispredict semantics with speculative window w. From this and **Oracle Overapproximation**, there is a prediction oracle O with speculative window at most w such that p does not satisfy speculative non-interference w.r.t. O. ◻

Thus, the proof is true for every secure speculative semantics.

Q FRAMEWORK DEFINITION

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

Q.1 Union of States

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

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

Q.2 Unified Trace Model

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

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

Q.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 $\upharpoonleft_{xy}$ as the inverse of the join function:

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

We require that

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

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

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

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

Q.4 AM Semantics

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

(AM-Context-xy)

$$\frac{\Phi_{xy} \overset{\tau}{\rightsquigarrow}_{xy} \overline{\Phi}'_{xy}}{\overline{\Phi}_{xy} \cdot \Phi_{xy} \overset{\tau}{\rightsquigarrow}_{xy} \overline{\Phi}_{xy} \cdot \overline{\Phi}'_{xy}}$$

(AM-x-Rollback-xy)

$$\frac{\begin{array}{cc} n' = 0 \text{ or p is stuck} & \overline{\Phi}_{xy} \cdot \Phi_{xy} \cdot \Phi'_{xy} \upharpoonleft^x_{xy} \xRightarrow{\texttt{rlb}_x\ ctr}_x \overline{\Phi}_{xy} \cdot \Phi''_{xy} \upharpoonleft^x_{xy} \\ \Phi''_{xy} = \Phi_{xy} & \Phi''_{xy}.ctr = \Phi'_{xy}.ctr \end{array}}{\overline{\Phi}_{xy} \cdot \Phi_{xy} \cdot \Phi'_{xy} \xRightarrow{\texttt{rlb}_x\ ctr}_{xy} \overline{\Phi}_{xy} \cdot \Phi''_{xy}}$$

(AM-y-Rollback-xy)

$$\frac{\begin{array}{c}\Phi'_{xy}.n = 0 \text{ or p is stuck} \\ \Phi''_{xy} = \Phi_{xy}\end{array} \qquad \begin{array}{c}\overline{\Phi}_{xy} \cdot \Phi_{xy} \cdot \Phi'_{xy}\restriction^{y}_{xy} \overset{\mathtt{rlb}_y\ ctr}{\rightsquigarrow}_y \overline{\Phi}_{xy} \cdot \Phi''_{xy}\restriction^{y}_{xy} \\ \Phi''_{xy}.ctr = \Phi'_{xy}.ctr\end{array}}{\overline{\Phi}_{xy} \cdot \Phi_{xy} \cdot \Phi'_{xy} \overset{\mathtt{rlb}_y\ ctr}{\rightsquigarrow}_{xy} \overline{\Phi}_{xy} \cdot \Phi''_{xy}}$$

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

(AM-x-step)

$$\frac{\Phi_{xy}\restriction^{x}_{xy} \overset{\tau}{\rightsquigarrow}_{x}^{Z_{xy}\restriction^{x}_{xy}} \overline{\Phi}'_{xy}\restriction^{x}_{xy}}{\Phi_{xy} \overset{\tau}{\rightsquigarrow}_{xy} \overline{\Phi}'_{xy}}$$

(AM-y-step)

$$\frac{\Phi_{xy}\restriction^{y}_{xy} \overset{\tau}{\rightsquigarrow}_{y}^{Z_{xy}\restriction^{y}_{xy}} \overline{\Phi}'_{xy}\restriction^{y}_{xy}}{\Phi_{xy} \overset{\tau}{\rightsquigarrow}_{xy} \overline{\Phi}'_{xy}}$$

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

(AM-Reflection-xy)

$$\frac{}{\Sigma_{xy} \Downarrow^{\varepsilon}_{xy} \Sigma_{xy}}$$

(AM-Single-xy)

$$\frac{\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma''_{xy} \qquad \Sigma''_{xy} \overset{\tau}{\rightsquigarrow}_{xy} \Sigma'_{xy}}{\Sigma_{xy} \Downarrow^{\overline{\tau}\cdot\tau}_{xy} \Sigma'_{xy}}$$

Q.5 Symbolic Semantics

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

(Sym-Context-xy)

$$\frac{\Phi^{S}_{xy} \overset{\tau_S}{\rightsquigarrow}^{S}_{xy} \overline{\Phi^{S}_{xy}}'}{\overline{\Phi^{S}_{xy}} \cdot \Phi^{S}_{xy} \overset{\tau_S}{\rightsquigarrow}^{S}_{xy} \overline{\Phi^{S}_{xy}} \cdot \overline{\Phi^{S}_{xy}}'}$$

(Sym-x-Rollback-xy)

$$\frac{\begin{array}{c}n' = 0 \text{ or p is stuck} \\ \Phi^{S\prime\,\prime}_{xy} = \Phi^{S}_{xy}\end{array} \qquad \begin{array}{c}\overline{\Phi^{S}_{xy}} \cdot \Phi^{S}_{xy} \cdot \Phi^{S\prime}_{xy}\restriction^{x}_{xy} \overset{\mathtt{rlb}_x\ ctr}{\rightsquigarrow}^{S}_{x} \overline{\Phi^{S}_{xy}} \cdot \Phi^{S\prime\,\prime}_{xy}\restriction^{x}_{xy} \\ \Phi^{S\prime\,\prime}_{xy}.ctr = \Phi^{S\prime}_{xy}.ctr\end{array}}{\overline{\Phi^{S}_{xy}} \cdot \Phi^{S}_{xy} \cdot \Phi^{S\prime}_{xy} \overset{\mathtt{rlb}_x\ ctr}{\rightsquigarrow}^{S}_{xy} \overline{\Phi^{S}_{xy}} \cdot \Phi^{S\prime\,\prime}_{xy}}$$

(Sym-y-Rollback-xy)

$$\frac{\begin{array}{c}\Phi'_{xy}.n = 0 \text{ or p is stuck} \\ \Phi^{S\prime\,\prime}_{xy} = \Phi^{S}_{xy}\end{array} \qquad \begin{array}{c}\overline{\Phi^{S}_{xy}} \cdot \Phi^{S}_{xy} \cdot \Phi^{S\prime}_{xy}\restriction^{y}_{xy} \overset{\mathtt{rlb}_y\ ctr}{\rightsquigarrow}^{S}_{y} \overline{\Phi^{S}_{xy}} \cdot \Phi^{S\prime\,\prime}_{xy}\restriction^{y}_{xy} \\ \Phi^{S\prime\,\prime}_{xy}.ctr = \Phi^{S\prime}_{xy}.ctr\end{array}}{\overline{\Phi^{S}_{xy}} \cdot \Phi^{S}_{xy} \cdot \Phi^{S\prime}_{xy} \overset{\mathtt{rlb}_y\ ctr}{\rightsquigarrow}^{S}_{xy} \overline{\Phi^{S}_{xy}} \cdot \Phi^{S\prime\,\prime}_{xy}}$$

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

(Sym-x-step)

$$\frac{\Phi^{S}_{xy}\restriction^{x}_{xy} \overset{\tau_S}{\rightsquigarrow}_{x}^{Z_{xy}\restriction^{x}_{xy}\,S} \overline{\Phi^{S}_{xy}}'\restriction^{x}_{xy}}{\Phi^{S}_{xy} \overset{\tau_S}{\rightsquigarrow}^{S}_{xy} \overline{\Phi^{S}_{xy}}'}$$

(Sym-y-step)

$$\frac{\Phi^{S}_{xy}\restriction^{y}_{xy} \overset{\tau_S}{\rightsquigarrow}_{y}^{Z_{xy}\restriction^{y}_{xy}\,S} \overline{\Phi^{S}_{xy}}'\restriction^{y}_{xy}}{\Phi^{S}_{xy} \overset{\tau}{\rightsquigarrow}^{S}_{xy} \overline{\Phi^{S}_{xy}}'}$$

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

(Sym-Reflection-xy)

$$\frac{}{\Sigma^{\mathcal{S}}_{xy}\ {}_{\mathcal{S}}\Downarrow^{\varepsilon}_{xy}\ \Sigma^{\mathcal{S}}_{xy}}$$

(Sym-Single-xy)

$$\frac{\Sigma^{\mathcal{S}}_{xy}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau}}_{xy}\ \Sigma^{\mathcal{S}'}_{xy}{}' \qquad \Sigma^{\mathcal{S}'}_{xy}{}' \overset{\tau_{\mathcal{S}}}{\rightsquigarrow}{}^{\mathcal{S}}_{xy}\ \Sigma^{\mathcal{S}'}_{xy}}{\Sigma^{\mathcal{S}}_{xy}\ {}_{\mathcal{S}}\Downarrow^{\overline{\tau}\cdot\tau_{\mathcal{S}}}_{xy}\ \Sigma^{\mathcal{S}'}_{xy}}$$

Q.6 Oracle semantics

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

(SE-Context-xy)

$$\frac{\Psi_{xy} \overset{\tau}{\rightsquigarrow}{}^{O_{xy}}_{xy} \overline{\Psi}'_{xy} \qquad minWndw(\overline{\Psi}_{xy}\cdot\Psi_{xy}) > 0 \qquad \text{if } p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \text{ then } \overline{\Psi}_{xy}'' = zeroes(\overline{\Psi}_{xy}) \text{ else } \overline{\Psi}_{xy}'' = decr(\overline{\Psi}_{xy})}{\overline{\Psi}_{xy}\cdot\Psi_{xy} \overset{\tau}{\rightsquigarrow}{}^{O_{xy}}_{xy} \overline{\Psi}_{xy}''\cdot\overline{\Psi}'_{xy}}$$

(SE-General-x)

$$\frac{\overline{\Psi}_{xy}\cdot\Psi_{xy_{\overline{\rho}\cdot\tau}}\upharpoonright^{x}_{xy} \overset{\tau}{\rightsquigarrow}{}^{O_x}_{x} \overline{\Psi}_{xy}\cdot\Psi_{xy_{\overline{\rho}}}\upharpoonright^{x}_{xy}}{\overline{\Psi}_{xy}\cdot\Psi_{xy_{\overline{\rho}\cdot\tau}} \overset{\tau}{\rightsquigarrow}{}^{O_{xy}}_{xy} \overline{\Psi}_{xy}\cdot\Psi_{xy_{\overline{\rho}}}}$$

(SE-General-y)

$$\frac{\overline{\Psi}_{xy}\cdot\Psi_{xy_{\overline{\rho}\cdot\tau}}\upharpoonright^{y}_{xy} \overset{\tau}{\rightsquigarrow}{}^{O_y}_{y} \overline{\Psi}_{xy}\cdot\Psi_{xy_{\overline{\rho}}}\upharpoonright^{y}_{xy}}{\overline{\Psi}_{xy}\cdot\Psi_{xy_{\overline{\rho}\cdot\tau}} \overset{\tau}{\rightsquigarrow}{}^{O_{xy}}_{xy} \overline{\Psi}_{xy}\cdot\Psi_{xy_{\overline{\rho}}}}$$

(SE-Rollback-x)

$$\frac{n' = 0 \text{ or } p \text{ is stuck} \qquad \Psi_{xy}\cdot\Psi'_{xy}\upharpoonright^{x}_{xy} \overset{\mathtt{rlb}_x\ ctr}{\rightsquigarrow}{}^{O_x}_{x} \Psi''_{xy}\upharpoonright^{x}_{xy} \qquad \Psi''_{xy} = \Psi_{xy}[ctr \mapsto \Psi'_{xy}.ctr]}{\overline{\Psi}_{xy}\cdot\Psi_{xy}\cdot\Psi'_{xy}\cdot\overline{\Psi}'_{xy} \overset{\mathtt{rlb}_x\ ctr}{\rightsquigarrow}{}^{O_{xy}}_{xy} \overline{\Psi}_{xy}\cdot\Psi''_{xy}}$$

(SE-Rollback-y)

$$\frac{n' = 0 \text{ or } p \text{ is stuck} \qquad \Psi_{xy}\cdot\Psi'_{xy}\upharpoonright^{y}_{xy} \overset{\tau}{\rightsquigarrow}{}^{O_y}_{y} \Psi''_{xy}\upharpoonright^{y}_{xy} \qquad \Psi''_{xy} = \Psi_{xy}[ctr \mapsto \Psi'_{xy}.ctr]}{\overline{\Psi}_{xy}\cdot\Psi_{xy}\cdot\Psi'_{xy}\cdot\overline{\Psi}'_{xy} \overset{\tau}{\rightsquigarrow}{}^{O_{xy}}_{xy} \overline{\Psi}_{xy}\cdot\Psi''_{xy}}$$

(SE-Commit-x)

$$\frac{\Psi_{xy}\cdot\Psi'_{xy}\upharpoonright^{x}_{xy} \overset{\tau}{\rightsquigarrow}{}^{O_x}_{x} \Psi''_{xy}\upharpoonright^{x}_{xy}}{\overline{\Psi}_{xy}\cdot\Psi_{xy}\cdot\Psi'_{xy}\cdot\overline{\Psi}_{xy}' \overset{\tau}{\rightsquigarrow}{}^{O_{xy}}_{xy} \overline{\Psi}_{xy}\cdot\Psi''_{xy}\cdot\overline{\Psi}_{xy}'}$$

(SE-Commit-y)

$$\frac{\Psi_{xy}\cdot\Psi'_{xy}\upharpoonright^{y}_{xy} \overset{\tau}{\rightsquigarrow}{}^{O_y}_{y} \Psi''_{xy}\upharpoonright^{y}_{xy}}{\overline{\Psi}_{xy}\cdot\Psi_{xy}\cdot\Psi'_{xy}\cdot\overline{\Psi}_{xy}' \overset{\tau}{\rightsquigarrow}{}^{O_{xy}}_{xy} \overline{\Psi}_{xy}\cdot\Psi''_{xy}\cdot\overline{\Psi}_{xy}'}$$

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

(SE-x-step)

$$\frac{O_{xy} = (O_x, O_y) \qquad \Psi_{xy}\upharpoonright^{x}_{xy} \overset{\tau}{\rightsquigarrow}{}^{O_x}_{x} \overline{\Psi}'_{xy}\upharpoonright^{x}_{xy}}{\Psi_{xy} \overset{\tau}{\rightsquigarrow}{}^{O_{xy}}_{xy} \overline{\Psi}'_{xy}}$$

(SE-y-step)

$$\frac{O_{xy} = (O_x, O_y) \qquad \Psi_{xy}\upharpoonright^{y}_{xy} \overset{\tau}{\rightsquigarrow}{}^{O_y}_{y} \overline{\Psi}'_{xy}\upharpoonright^{y}_{xy}}{\Psi_{xy} \overset{\tau}{\rightsquigarrow}{}^{O_{xy}}_{xy} \overline{\Psi}'_{xy}}$$

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

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

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

$\boxed{\textit{Helpers}}$

$$\frac{X_{xy} = \Psi_{xy} \quad \Psi_{xy}\upharpoonright_{xy} = (\Psi_x, \Psi_y) \quad \vdash \Psi_x : init \quad \vdash \Psi_y : init}{\vdash X_{xy} : init}\;\text{(Comb-SE:Init)}$$

$$\frac{X_{xy} = \Psi_{xy} \quad \Psi_{xy}\upharpoonright_{xy} = (\Psi_x, \Psi_y) \quad \vdash \Psi_x : fin \quad \vdash \Psi_y : fin}{\vdash X_{xy} : fin}\;\text{(Comb-SE:Fin)}$$

$$\frac{}{X^{init}_{xy}(p,\sigma) \coloneqq \sqcup_{xy}(X^{init}_x(p,\sigma), X^{init}_y(p,\sigma))}\;\text{(Comb-SE-Initial-State)}$$

Q.7 Main definitions from the paper

Here we restate the main definitions of the paper.

Definition 39 (Secure Speculative Semantics)**.** *A semantics $\mathcal{Q}_x$ is secure (denoted $\vdash \mathcal{Q}_x$ WFSS) if:*

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

Definition 40 (Well-formed composition)**.** *A composition $\mathcal{Q}_{xy}$ of two speculative semantics $\mathcal{Q}_x$ and $\mathcal{Q}_y$ is well-formed, denoted with $\vdash \mathcal{Q}_{xy}$: WFC if:*

1. *(Confluence) Whenever $\Sigma_{xy} \overset{\tau}{=\!\!\Rightarrow}\mathcal{Q}_{xy}\, \Sigma'_{xy}$ and $\Sigma_{xy} \overset{\tau}{=\!\!\Rightarrow}\mathcal{Q}_{xy}\, \Sigma''_{xy}$, then $\Sigma'_{xy} = \Sigma''_{xy}$.*
2. *(Projection preservation) For all programs p, $Beh^{\omega}_x(p) = Beh^{\omega}_{xy}((p))\upharpoonright^{x}_{xy}$ and $Beh^{\omega}_y(p) = Beh^{\omega}_{xy}((p))\upharpoonright^{y}_{xy}$.*
3. *(Relation preservation) If $\Sigma_{xy} \approx_{xy} X_{xy}$ and $\Sigma_{xy} \overset{\overline{\tau}}{=\!\!\Rightarrow}\mathcal{Q}^{*}_{xy}\, \Sigma'_{xy}$ then $X_{xy} \overset{\overline{\tau}'}{\rightsquigarrow}{}^{O_{xy}}_{xy}{}^{*}\, X'_{xy}$ and $\Sigma'_{xy} \approx_{xy} X'_{xy}$.*
4. *(Symbolic Preservation) If $\Sigma^{S}_{xy} \overset{\tau_S}{=\!\!\Rightarrow}\mathcal{Q}^{S}_{xy}\, \Sigma^{S'}_{xy}$ and $\mu(\Sigma^{S}_{xy}) = \Sigma_{xy}$ and $\mu \vDash pthCnd(\tau_S)$ Then there exists Σ'_{xy} such that $\Sigma_{xy} \overset{\mu(\tau)}{=\!\!\Rightarrow}\mathcal{Q}_{xy}\, \Sigma'_{xy}$ and $\mu(\Sigma^{S'}_{xy}) = \Sigma'_{xy}$. Furthermore, if $\Sigma_{xy} \overset{\tau}{=\!\!\Rightarrow}\mathcal{Q}_{xy}\, \Sigma'_{xy}$ and $\mu(\Sigma^{S}_{xy}) = \Sigma_{xy}$ then $\Sigma^{S}_{xy} \overset{\tau'}{=\!\!\Rightarrow}\mathcal{Q}^{S}_{xy}\, \Sigma^{S'}_{xy}$, $\mu(\Sigma^{S'}_{xy}) = \Sigma'_{xy}$, $\mu \vDash pthCnd(\tau')$ and $\mu(\tau') = \tau$*

Q.8 Main result

Here is the main result of the paper again.

Theorem 27 ($\mathcal{Q}_{xy}$ is *WFSS*). *if $\vdash \mathcal{Q}_x$ WFSS and $\vdash \mathcal{Q}_y$ WFSS and $\vdash \mathcal{Q}_{xy}$: WFC then $\vdash \mathcal{Q}_{xy}$ WFSS.*

Proof. Immediate from Theorem 28 (NS Consistency) and Theorem 29 (Symbolic Consistency).

Note that the last of *WFSS* is missing (overapproximation of oracle). Since this is technical, we delay the presentation and refer the reader to each of the combinations. ◻

Now here is one of the main results for the general case that follows from just well-formedness:

Corollary 2 (Security Decomposition)**.** *Let* $\vdash \mathcal{J}_{xy} : \mathit{WFC}$ *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.

From $p \vdash_x$ SNI and $p \vdash_y$ SNI we get:

$$\sigma, \sigma' \in \mathit{InitConf}$$

$$\sigma \sim_P \sigma'$$

$$((p, \sigma)) \Downarrow_{NS} \overline{\tau}', \big((p, \sigma')\big) \Downarrow_{NS} \overline{\tau}'$$

for some policy P.

We need to show that

(1) $((p, \sigma)) \Downarrow_x^{\omega} \overline{\tau}_x$, $((p, \sigma')) \Downarrow_x^{\omega} \overline{\tau}_x$
(2) $((p, \sigma)) \Downarrow_y^{\omega} \overline{\tau}_y$, $((p, \sigma')) \Downarrow_y^{\omega} \overline{\tau}_y$

From Projection Preservation of $\vdash \mathcal{J}_{xy} : \mathit{WFC}$ we get $\mathit{Beh}_x^{\omega}(p) = \mathit{Beh}_{xy}^{\omega}((p)) \upharpoonright_{xy}^{x}$ and $\mathit{Beh}_y^{\omega}(p) = \mathit{Beh}_{xy}^{\omega}((p)) \upharpoonright_{xy}^{y}$. We show the proof for 1) via the projection to x. The proof for 2) is analogous using the projection to y.

Unfolding the definition of $p \vdash_{xy}$ SNI we get:

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

After initialization with our assumptions we have $((p, \sigma)) \Downarrow_{xy}^{\omega} \overline{\tau}_{xy}$, $((p, \sigma')) \Downarrow_{xy}^{\omega} \overline{\tau}_{xy}$.

By the projection to x assumption we have $((p, \sigma)) \Downarrow_x^{\omega} \overline{\tau}_{xy} \upharpoonright_{xy}^{x} \in \mathit{Beh}_x^{\omega}(p)$ and $((p, \sigma')) \Downarrow_x^{\omega} \overline{\tau}_{xy} \upharpoonright_{xy}^{x} \in \mathit{Beh}_x^{\omega}(p)$, which is what we needed to show.

□

Corollary 3 (Leakage Preservation)**.** *Let* $\vdash \mathcal{J}_{xy} : \mathit{WFC}$ *and let* p *be a program and* ω *be a speculation window. If* $p \nvdash_x$ *SNI or* $p \nvdash_y$ *SNI, then* $p \nvdash_{xy}$ *SNI.*

Proof. By contrapositive. The contrapositive is: $p \vdash_{xy}$ SNI then $p \vdash_x$ SNI and $p \vdash_y$ SNI This is exactly Security Decomposition. □

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

Q.9 NS Consistency for the general combination

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

Theorem 28 (NS Consistency). *If*

(1) $\vdash \mathcal{J}_{xy} : \mathit{WFC}$ *and*
(2) $\mathit{Beh}_{NS}(p) = \mathit{Beh}_x^{\omega}(p) \upharpoonright_{ns}$ *and*
(3) $\mathit{Beh}_{NS}(p) = \mathit{Beh}_y^{\omega}(p) \upharpoonright_{ns}$

Then

I $\mathit{Beh}_{NS}(p) = \mathit{Beh}_{xy}^{\omega}(p) \upharpoonright_{ns}$.

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

From $\vdash \mathcal{Q}_{xy} : \mathit{WFC}$, we have that $Beh^{\omega}_{xy}(p)\upharpoonright^{y}_{xy} = Beh^{\omega}_{y}(p)$.

Again by definition, we get $Beh^{\omega}_{y}(p)\upharpoonright^{x}_{xy} = Beh^{\omega}_{y}(p)\upharpoonright_{ns}$ ($Beh^{\omega}_{y}(p)$ only has transactions of type y).

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

Combining these facts we get:

$$
\begin{aligned}
& Beh^{\omega}_{xy}(p)\upharpoonright_{ns} \\
&= Beh^{\omega}_{xy}(p)\upharpoonright^{y}_{xy}\upharpoonright^{x}_{xy} \\
&= Beh^{\omega}_{y}(p)\upharpoonright^{x}_{xy} \\
&= Beh^{\omega}_{y}(p)\upharpoonright_{ns} \\
&= Beh_{NS}(p)
\end{aligned}
$$

and are finished. □

Q.9.1 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: $Beh^{\omega}_{x}(p) = \mu(Beh^{S}_{x}(p))$ 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.

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];
```

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. Assumption 1 (Symbolic Soundness x) 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.

Q.10 Symbolic Consistency for the general combination

Theorem 29 (Symbolic Consistency). *If $\vdash \mathcal{Q}_{xy} : \mathit{WFC}$, then $\forall p.\, Beh^{\omega}_{xy}(p) = \mu(Beh^{S}_{xy}(p))$.*

Proof. We prove the two directions separately:

$\Leftarrow$ Assume that $(p, \sigma_{\mathcal{S}}) \ {}_{\mathcal{S}}\!\leadsto^{\omega}_{xy} \overline{\tau} \in Beh^{\mathcal{S}}_{xy}(p)$. 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 $\mu \vDash pthCnd(\overline{\tau_{\mathcal{S}}})$. We now apply Lemma 124 (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 $\mu(\overline{\tau_{\mathcal{S}}}) = \overline{\tau}$
Since $\vdash \Sigma^{\mathcal{S}'}_{xy} : fin$ and $\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$ we have $\vdash \Sigma'_{xy} : fin$ as well.
Thus, $((p, \mu(\sigma_{\mathcal{S}}))) \leadsto^{\omega}_{xy} \mu(\overline{\tau_{\mathcal{S}}}) \in Beh^{\mathcal{S}}_{xy}(p)$.

$\Rightarrow$ Assume that $((p, \sigma)) \leadsto^{\omega}_{xy} \overline{\tau} \in Beh^{\omega}_{xy}(p)$. We thus know there exists $\vdash \Sigma'_{xy} : fin$ such that $\Sigma^{init}_{xy}((p, \sigma)) \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}$.
We now apply Lemma 125 (Completeness Symbolic Combination) on $\Sigma^{init}_{xy}((p, \sigma)) \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}$ and get

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

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

□

Lemma 124 (Soundness Symbolic Combination)**.** *If*

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

Then

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

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

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 fulfil all conditions.

Rule Sym-Single-xy We have $\Sigma^{\mathcal{S}}_{xy} \ {}_{\mathcal{S}}\!\Downarrow^{\overline{\tau_{\mathcal{S}}}' \cdot \tau_{\mathcal{S}}}_{xy} \Sigma^{\mathcal{S}'}_{xy}$ and by Rule Sym-Single-xy we get $\Sigma^{\mathcal{S}}_{xy} \ {}_{\mathcal{S}}\!\Downarrow^{\overline{\tau_{\mathcal{S}}}'}_{xy} \Sigma^{\mathcal{S}'}_{xy}{}'$ and $\Sigma^{\mathcal{S}'}_{xy}{}' \xrightarrow{\tau_{\mathcal{S}}} \leadsto^{\mathcal{S}}_{xy} \Sigma^{\mathcal{S}'}_{xy}$.
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 $\mu(\overline{\tau_{\mathcal{S}}} \cdot \tau_{\mathcal{S}}) = \overline{\tau} \cdot \tau$ and
We apply the IH on $\Sigma^{\mathcal{S}}_{xy} \ {}_{\mathcal{S}}\!\Downarrow^{\overline{\tau_{\mathcal{S}}}'}_{xy} \Sigma^{\mathcal{S}'}_{xy}{}'$ 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 $\mu(\overline{\tau_{\mathcal{S}}}) = \overline{\tau}$ and

We use Symbolic Preservation (In lemma form here: Lemma 126 (Comb: Soundness single step symbolic)) from $\vdash \mathcal{Q}_{xy} : \mathit{WFC}$ on $\Sigma_{xy}^{\mathcal{S}'\prime} \xrightarrow{\tau_{\mathcal{S}}}{}_{\mathcal{Q}}{}_{xy}^{\mathcal{S}} \Sigma_{xy}^{\mathcal{S}'}$ and get $\Sigma_{xy}'' \xrightarrow{\tau}{}_{\mathcal{Q}}{}_{xy} \Sigma_{xy}'$ and $\mu(\Sigma_{xy}^{\mathcal{S}'}) = \Sigma_{xy}'$ and $\mu(\tau_{\mathcal{S}}) = \tau$.

We now use Rule AM-Single-xy on $\Sigma_{xy} \Downarrow_{xy}^{\overline{\tau}} \Sigma_{xy}''$ and $\Sigma_{xy}'' \xrightarrow{\tau}{}_{\mathcal{Q}}{}_{xy} \Sigma_{xy}'$ and get the desired result.

□

Lemma 125 (Completeness Symbolic Combination)**.** *If*

(1) $\Sigma_{xy} \Downarrow_{xy}^{\overline{\tau}} \Sigma_{xy}'$ *and*
(2) $\vdash \mathcal{Q}_{xy} : \mathit{WFC}$

Then there is a valuation μ*, a symbolic trace* $\overline{\tau}'$ *and a final state* $\Sigma_{xy}^{\mathcal{S}'}$ *such that*

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

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

Rule AM-Reflection-xy Then we have $\Sigma_{xy} \Downarrow_{xy}^{\varepsilon} \Sigma_{xy}'$ with $\Sigma_{xy}' = \Sigma_{xy}'$.

I - IV By Rule Sym-Reflection-xy we have $\Sigma_{xy}^{\mathcal{S}} \; {}_{\mathcal{S}}\Downarrow_{xy}^{\varepsilon} \Sigma_{xy}$. 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 $\Sigma_{xy} \Downarrow_{xy}^{\overline{\tau_{\mathcal{S}}}'} \Sigma_{xy}''$ and $\Sigma_{xy}'' \xrightarrow{\tau}{}_{\mathcal{Q}}{}_{xy}^{\mathcal{S}} \Sigma_{xy}'$.

We need to prove

I $\Sigma_{xy} = \mu(\Sigma_{xy}^{\mathcal{S}})$ and
II $\Sigma_{xy}^{\mathcal{S}} \; {}_{\mathcal{S}}\Downarrow_{xy}^{\overline{\tau_{\mathcal{S}}}'\cdot\tau_{\mathcal{S}}} \Sigma_{xy}^{\mathcal{S}'}$ and
III $\Sigma_{xy}' = \mu(\Sigma_{xy}^{\mathcal{S}'})$ and $\overline{\tau}' \cdot \tau = \mu(\overline{\tau_{\mathcal{S}}}' \cdot \tau_{\mathcal{S}})$ and
IV $\mu \vDash \mathit{pthCnd}(\overline{\tau_{\mathcal{S}}}' \cdot \tau_{\mathcal{S}})$

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

(1) $\Sigma_{xy} = \mu(\Sigma_{xy}^{\mathcal{S}})$ and
(2) $\Sigma_{xy}^{\mathcal{S}} \; {}_{\mathcal{S}}\Downarrow_{xy}^{\overline{\tau_{\mathcal{S}}}'} \Sigma_{xy}^{\mathcal{S}'\prime}$ and
(3) $\Sigma_{xy}'' = \mu(\Sigma_{xy}^{\mathcal{S}'})'$ and $\overline{\tau}' = \mu(\overline{\tau_{\mathcal{S}}}')$ and
(4) $\mu \vDash \mathit{pthCnd}(\overline{\tau_{\mathcal{S}}}')$

We use Symbolic Preservation (In lemma form here: Lemma 127 (Comb: Completeness single step)) from $\vdash \mathcal{Q}_{xy}$: WFC on $\Sigma_{xy}'' \xrightarrow{\tau}{}_{\mathcal{Q}}{}_{xy} \Sigma_{xy}'$ and get $\Sigma_{xy}^{\mathcal{S}'\prime} \xrightarrow{\tau_{\mathcal{S}}}{}_{\mathcal{Q}}{}_{xy}^{\mathcal{S}} \Sigma_{xy}^{\mathcal{S}'}$ and $\mu(\Sigma_{xy}^{\mathcal{S}'}) = \Sigma_{xy}'$ and $\mu(\tau_{\mathcal{S}}) = \tau$ and $\mu \vDash \mathit{pthCnd}(\tau_{\mathcal{S}})$.

By definition, we have $\mu \vDash \mathit{pthCnd}(\overline{\tau_{\mathcal{S}}}')$ since $\mu \vDash \mathit{pthCnd}(\tau_{\mathcal{S}}')$ and $\mu \vDash \mathit{pthCnd}(\overline{\tau_{\mathcal{S}}}')$.

We now use Rule Sym-Single-xy on $\Sigma_{xy}^{\mathcal{S}} \; {}_{\mathcal{S}}\Downarrow_{xy}^{\overline{\tau_{\mathcal{S}}}'} \Sigma_{xy}^{\mathcal{S}'\prime}$ and $\Sigma_{xy}^{\mathcal{S}'\prime} \xrightarrow{\tau_{\mathcal{S}}}{}_{\mathcal{Q}}{}_{xy}^{\mathcal{S}} \Sigma_{xy}^{\mathcal{S}'}$ and get the desired result.

□

Q.11 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 (Assumption 1 and Assumption 2 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 V1, V2, V4, V5 and SLS (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.
This similarly holds for 3) of the WFC as we will see later.

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

Assumption 1 (Symbolic Soundness x)**.** *If*

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

Then

(1) $\Sigma_{x_\mathcal{S}} \overset{\tau_\mathcal{S}}{=\!\!\Omega}{}^\mathcal{S}_x \Sigma'_{x_\mathcal{S}}$ *and*
(2) $\mu(\Sigma'_{x_\mathcal{S}}) = \Sigma'_x$ *and*
(3) $\mu(\tau_\mathcal{S}) = \tau$

Assumption 2 (Symbolic Completeness x)**.** *If*

(1) $\Sigma_{x_\mathcal{S}} \overset{\tau_\mathcal{S}}{=\!\!\Omega}{}^\mathcal{S}_x \Sigma'_{x_\mathcal{S}}$ *and*
(2) $\mu(\Sigma_{x_\mathcal{S}}) = \Sigma_x$

Then

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

Lemma 126 (Comb: Soundness single step symbolic)**.** *If*

(1) $\Sigma^\mathcal{S}_{xy} \overset{\tau_\mathcal{S}}{=\!\!\Omega}{}^\mathcal{S}_{xy} \Sigma^{\mathcal{S}'}_{xy}$ *and*
(2) $\mu(\Sigma^\mathcal{S}_{xy}) = \Sigma_{xy}$
(3) $\mu \models pthCnd(\tau_\mathcal{S})$

Then there exists Σ'_{xy} *such that*

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

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

Rule Sym-x-Rollback-xy Since μ 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 $\Sigma_{xy}.ctr = \Sigma^{\mathcal{S}}_{xy}.ctr$.

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

$\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$ **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 $\Phi^{\mathcal{S}}_{xy} \xrightarrow{\tau_{\mathcal{S}}}{}^{\mathcal{S}}_{xy} \overline{\Phi^{\mathcal{S}}_{xy}}'$. We proceed by inversion on $\Phi^{\mathcal{S}}_{xy} \xrightarrow{\tau_{\mathcal{S}}}{}^{\mathcal{S}}_{xy} \overline{\Phi^{\mathcal{S}}_{xy}}'$:

Rule Sym-x-step Then we have $\Phi^{\mathcal{S}}_{xy}\upharpoonright^{x}_{xy} \xrightarrow{\tau_{\mathcal{S}}}{}^{Z_{xy}\upharpoonright^{x}_{xy}\,\mathcal{S}}_{x} \overline{\Phi^{\mathcal{S}}_{xy}}'\upharpoonright^{x}_{xy}$. Note that $\mu(\Phi^{\mathcal{S}}_{xy})\upharpoonright^{x}_{xy} = \Phi_{xy}\upharpoonright^{x}_{xy}$ 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 $\mathbf{pc}$ is concrete. That means the same instruction is executed.

Now we use Assumption 1 (Symbolic Soundness x) and get $\Phi_{xy}\upharpoonright^{x}_{xy} \xrightarrow{\tau}_{x} \overline{\Phi}'_{xy}\upharpoonright^{x}_{xy}$ with $\mu(\overline{\Phi^{\mathcal{S}}_{xy}}')\upharpoonright^{x}_{xy} = \overline{\Phi}'_{xy}\upharpoonright^{x}_{xy}$ and $\mu(\tau_{\mathcal{S}}) = \tau$.

From $\mu(\overline{\Phi^{\mathcal{S}}_{xy}}')\upharpoonright^{x}_{xy} = \overline{\Phi}'_{xy}\upharpoonright^{x}_{xy}$ 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 $\Phi_{xy}\upharpoonright^{x}_{xy} \xrightarrow{\tau}_{x} \overline{\Phi}'_{xy}\upharpoonright^{x}_{xy}$ and get $\Phi_{xy} \xrightarrow{\tau}_{xy} \overline{\Phi}'_{xy}$ and are finished.

Rule Sym-y-step Then we have $\Phi^{\mathcal{S}}_{xy}\upharpoonright^{y}_{xy} \xrightarrow{\tau_{\mathcal{S}}}{}^{Z_{xy}\upharpoonright^{y}_{xy}\,\mathcal{S}}_{y} \overline{\Phi^{\mathcal{S}}_{xy}}'\upharpoonright^{y}_{xy}$. Note that $\mu(\Phi^{\mathcal{S}}_{xy})\upharpoonright^{y}_{xy} = \Phi_{xy}\upharpoonright^{y}_{xy}$ because of $\mu(\Sigma^{\mathcal{S}}_{xy}) = \Sigma_{xy}$.

The proof is analogous to the case above using Assumption 1 (Symbolic Soundness x).

□

Lemma 127 (Comb: Completeness single step)**.** *If*

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

Then

I $\Sigma^{\mathcal{S}}_{xy} \xrightarrow{\tau'}{}^{\mathcal{S}}_{xy} \Sigma^{\mathcal{S}'}_{xy}$ *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 $\Sigma_{xy} \xrightarrow{\tau}_{xy} \Sigma'_{xy}$:

Rule AM-x-Rollback-xy Since μ 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 $\Sigma_{xy}.ctr = \Sigma^{\mathcal{S}}_{xy}.ctr$.

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

$\mu(\Sigma^{\mathcal{S}'}_{xy}) = \Sigma'_{xy}$ 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 $\mathbf{pc}$ is concrete. That means the same instruction is executed.

Now we use Assumption 2 (Symbolic Completeness x) and get $\Phi^{\mathcal{S}}_{xy}\restriction^{x}_{xy} \overset{\tau_{\mathcal{S}}}{\Longrightarrow}^{\mathcal{S}}_{x} \overline{\Phi^{\mathcal{S}}_{xy}}'\restriction^{x}_{xy}$ 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 $\Phi^{\mathcal{S}}_{xy}\restriction^{x}_{xy} \overset{\tau}{\Longrightarrow}^{\mathcal{S}}_{x} \overline{\Phi^{\mathcal{S}}_{xy}}'\restriction^{x}_{xy}$ and get $\Phi^{\mathcal{S}}_{xy} \overset{\tau_{\mathcal{S}}}{\Longrightarrow}^{\mathcal{S}}_{xy} \overline{\Phi^{\mathcal{S}}_{xy}}'$ and are finished.

Rule AM-y-step Analogous to the case above using Assumption 2 (Symbolic Completeness x) for the y-step.

□

R WFC OF ALL THE REMAINING COMBINATIONS

In this section, we show that our combined semantics fulfil our well-formedness condition defined in Appendix Q. As a reminder, here is the definition of well-formedness.

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

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

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

(4) *(Relation Preservation new)* $\forall \approx_{xy} \in \{\approx, \approx^{\Sigma^{States}}_{O_{am}}\}$, If $\Sigma_{xy} \cong \Sigma^{\dagger}_{xy}$ and $X_{xy} \cong X^{\dagger}_{xy}$ and $\Sigma_{xy} \approx_{xy} X_{xy}$ and $\Sigma_{xy} \overset{\overline{\tau}}{\Longrightarrow}^{*}_{xy} \Sigma'_{xy}$ and $\Sigma^{\dagger}_{xy} \overset{\overline{\tau}}{\Longrightarrow}^{*}_{xy} \Sigma^{\dagger\dagger}_{xy}$ then $X_{xy} \overset{\overline{\tau}'}{\rightsquigarrow}^{O_{xy}}_{xy}{}^{*} X'_{xy}$ $X^{\dagger}_{xy} \overset{\overline{\tau}'}{\rightsquigarrow}^{O_{xy}}_{xy}{}^{*} X^{\dagger\dagger}_{xy}$ and $\Sigma'_{xy} \approx_{xy} X'_{xy}$ and $\Sigma'_{xy} \cong \Sigma^{\dagger\dagger}_{xy}$ and $X'_{xy} \cong X^{\dagger\dagger}_{xy}$.

AM and Oracle coincide If $\Sigma_{xy} \approx^{\Sigma^{States}}_{O_{am}} X_{xy}$ by Base and $\Sigma_{xy} \overset{\tau}{\Longrightarrow}_{xy} \Sigma'_{xy}$ and $minWndw(\Sigma_{xy}) > 0$ and $X_{xy}.\overline{p} = \varnothing$ then $X_{xy} \overset{\tau}{\rightsquigarrow}^{O_{xy}}_{xy} X'_{xy}$

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

In general, Confluence follows from the correct instantiation of the metaparameter Z. Our AM semantics delegate back to the non-speculative semantics in all cases not related to speculation. Since the non-speculative semantics is deterministic, all the rules delegating back are confluent. The only difference in the execution can appear if speculation is started. However, then the metaparamter restricts the no-branching rule of the other semantics part of the combination and it cannot be used. Thus, speculation is always started and only one rule is possible, contradicting the assumption of Confluence. For a concrete proof we refer to Lemma 142 (V45 AM: Confluence). So in the remainder, we will not reference Confluence for each of the combination but rely on this meta-argument above.

For Symbolic Preservation, we rely on our general construction in Appendix Q.11, where we need to fulfil the assumptions made, which we will provide now

$\mathcal{Q}_{B}$ The lemmas needed are Appendix G.4.2 (Soundness) and Proposition 8 ().

$\mathcal{Q}_{J}$ The lemmas needed are Lemma 31 (J: Soundness single step) and Lemma 33 (J: Completeness single step).

$\mathcal{Q}_{S}$ The lemmas needed are Lemma 57 (S: Soundness single step) and Lemma 59 (S: Completeness single step).

$\mathcal{Q}_{R}$ The lemmas needed are Lemma 83 (R: Soundness single step) and Lemma 85 (R: Completeness single step).

$\mathcal{Q}_{SLS}$ The lemmas needed are Lemma 108 (SLS: Soundness single step) and Lemma 111 (SLS: Completeness single step).

Thus, all of the combinations will fulfil Symbolic Preservation because all the source semantics for the combinations fulfil the assumptions needed to derive it generally.

For Relation Preservation, we also rely on our general construction in Appendix R.15, where we need to fulfil the assumptions made, which we will provide now:

$\mathcal{Q}_{B}$ The lemmas needed are Appendix G.4.2 (Soundness) and Proposition 8 ().

$\mathcal{Q}_{J}$ The lemmas needed are Lemma 40 ($\mathcal{J}$: Soundness Single Step AM) and Lemma 43 ($\mathcal{J}$: Stronger Soundness for a specific oracle and for specific executions).

$\mathcal{Q}_{S}$ The lemmas needed are Lemma 65 (S: Soundness Single Step AM) and Lemma 68 (S: Stronger Soundness for a specific oracle and for specific executions).

$\mathcal{Q}_{R}$ The lemmas needed are Lemma 91 (R: Soundness Single Step AM) and Lemma 94 (R:Stronger Soundness for a specific oracle and for specific executions).

$\mathcal{Q}_{SLS}$ The lemmas needed are Lemma 117 (SLS: Soundness Single Step AM) and Lemma 120 (SLS: Stronger Soundness for a specific oracle and for specific executions).

For the condition or AM and Oracle coincide we again rely on the general construction found in Appendix R.15:

$\mathcal{Q}_{B}$ The lemma needed is Lemma 18 (B: AM and Oracle coincide)

$\mathcal{Q}_{J}$ The lemma needed is Lemma 42 ($\mathcal{J}$: AM and Oracle coincide)

$\mathcal{Q}_{S}$ The lemma needed is Lemma 67 (S: AM and Oracle coincide)

$\mathcal{Q}_{R}$ The lemma needed is Lemma 93 (R: AM and Oracle coincide)

$\mathcal{Q}_{SLS}$ The lemma needed is Lemma 119 (SLS: AM and Oracle coincide)

The remaining proofs for Projection Preservation follow a very similar structure and we only describe the difference in the relevant cases. For a complete proof, we refer to Appendix T.

> The idea for Projection Preservation is this. We create a new relation that is very strong, i.e. the relevant parts of the state of the combination and the specific source variant are the same and one where speculation of the other source is happening. When the combination does a step, it can either be an x step or a y step. If it is an x-step and we relate to source x semantics, then we do the same step in the source. If it is a y-step, we know by Confluence that it only matters if a new speculative transaction is started, since this speculation does not happen in the x semantics. However, this is speculation and is removed by the projection function. In this case we wait until speculation is over and continue in the relation.

R.1 $\mathcal{Q}_{B+J}$

R.1.1 Projection Preservation.

Theorem 30 (B + $\mathcal{J}$: Relating V1 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{B}(p) = Beh^{B+R}_{\omega}(p)\upharpoonright^{B}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). ◻

Theorem 31 (B + $\mathcal{J}$: Relating V2 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathcal{J}}(p) = Beh^{B+R}_{\omega}(p)\upharpoonright^{\mathcal{J}}$.*

Proof. The proof is analogous to Theorem 70 (V45: Relating V5 with projection of combined). ◻

R.2 $\mathcal{Q}_{B+SLS}$

R.2.1 Projection Preservation.

Theorem 32 (B + SLS: Relating V1 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{B}(p) = Beh^{B+SLS}_{\omega}(p)\upharpoonright^{B}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). ◻

Theorem 33 (B + SLS: Relating SLS with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{SLS}(p) = Beh^{B+SLS}_{\omega}(p)\upharpoonright^{SLS}$.*

Proof. The proof is analogous to Theorem 70 (V45: Relating V5 with projection of combined). ◻

R.3 $\mathcal{Q}_{J+S}$

R.3.1 Projection Preservation.

Theorem 34 ($\mathcal{J}$+ S: Relating V2 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathcal{J}}(p) = Beh^{\mathcal{J}+S}_{\omega}(p)\upharpoonright^{\mathcal{J}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). ◻

Theorem 35 ($\mathcal{J}$+ S: Relating V4 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{S}(p) = Beh^{\mathcal{J}+S}_{\omega}(p)\upharpoonright^{S}$.*

Proof. The proof is analogous to Theorem 70 (V45: Relating V5 with projection of combined). ◻

R.4 $\mathcal{Q}_{S+SLS}$

R.4.1 Projection Preservation.

Theorem 36 (S + SLS: Relating V4 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{S}(p) = Beh^{S+SLS}_{\omega}(p)\upharpoonright^{S}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). ◻

Theorem 37 (S + SLS: Relating SLS with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{SLS}(p) = Beh^{S+SLS}_{\omega}(p)\upharpoonright^{SLS}$.*

Proof. The proof is analogous to Theorem 70 (V45: Relating V5 with projection of combined). ◻

R.5 $\mathcal{Q}_{\mathcal{J}+\mathsf{R}}$

R.5.1 Projection Preservation.

Theorem 38 ($\mathcal{J}$+ R: Relating V2 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathcal{J}}(p) = Beh^{\mathcal{J}+\mathsf{R}}_{\omega}(p)\upharpoonright^{\mathcal{J}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). □

Theorem 39 ($\mathcal{J}$+ R: Relating V5 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{R}}(p) = Beh^{\mathcal{J}+\mathsf{R}}_{\omega}(p)\upharpoonright^{\mathsf{R}}$.*

Proof. The proof is analogous to Theorem 70 (V45: Relating V5 with projection of combined). □

R.6 $\mathcal{Q}_{\mathcal{J}+\mathsf{SLS}}$

R.6.1 Projection Preservation.

Theorem 40 ($\mathcal{J}$ + SLS: Relating V2 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathcal{J}}(p) = Beh^{\mathcal{J}+\mathsf{SLS}}_{\omega}(p)\upharpoonright^{\mathcal{J}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). □

Theorem 41 ($\mathcal{J}$ + SLS: Relating SLS with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{SLS}}(p) = Beh^{\mathcal{J}+\mathsf{SLS}}_{\omega}(p)\upharpoonright^{\mathsf{SLS}}$.*

Proof. The proof is analogous to Theorem 70 (V45: Relating V5 with projection of combined). □

R.7 $\mathcal{Q}_{\mathsf{B}+\mathcal{J}+\mathsf{S}}$

R.7.1 Projection Preservation.

Theorem 42 (B + $\mathcal{J}$+ S: Relating V1 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{B}}(p) = Beh^{\mathsf{B}+\mathcal{J}+\mathsf{S}}_{\omega}(p)\upharpoonright^{\mathsf{B}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). □

Theorem 43 (B + $\mathcal{J}$+ S: Relating V2 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathcal{J}}(p) = Beh^{\mathsf{B}+\mathcal{J}+\mathsf{S}}_{\omega}(p)\upharpoonright^{\mathcal{J}}$.*

Proof. The proof is analogous to Theorem 70 (V45: Relating V5 with projection of combined). □

Theorem 44 (B + $\mathcal{J}$+ S: Relating V4 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{S}}(p) = Beh^{\mathsf{B}+\mathcal{J}+\mathsf{S}}_{\omega}(p)\upharpoonright^{\mathsf{S}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). □

R.8 $\mathcal{Q}_{\mathsf{B}+\mathcal{J}+\mathsf{R}}$

R.8.1 Projection Preservation.

Theorem 45 (B + $\mathcal{J}$+ R: Relating V1 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{B}}(p) = Beh^{\mathsf{B}+\mathcal{J}+\mathsf{R}}_{\omega}(p)\upharpoonright^{\mathsf{B}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). □

Theorem 46 (B + $\mathcal{J}$ + R: Relating V2 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathcal{J}}(p) = Beh^{\mathsf{B}+\mathcal{J}+\mathsf{R}}_{\omega}(p)\restriction^{\mathcal{J}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). □

Theorem 47 (B + $\mathcal{J}$ + R: Relating V5 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{R}}(p) = Beh^{\mathsf{B}+\mathcal{J}+\mathsf{R}}_{\omega}(p)\restriction^{\mathsf{R}}$.*

Proof. The proof is analogous to Theorem 70 (V45: Relating V5 with projection of combined). □

R.9 $_{\mathsf{B}+\mathcal{J}+\mathsf{SLS}}$

R.9.1 Projection Preservation.

Theorem 48 (B + $\mathcal{J}$ + SLS: Relating V1 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{B}}(p) = Beh^{\mathsf{B}+\mathcal{J}+\mathsf{SLS}}_{\omega}(p)\restriction^{\mathsf{B}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). □

Theorem 49 (B + $\mathcal{J}$ + SLS: Relating V2 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathcal{J}}(p) = Beh^{\mathsf{B}+\mathcal{J}+\mathsf{SLS}}_{\omega}(p)\restriction^{\mathcal{J}}$.*

Proof. The proof is analogous to Theorem 70 (V45: Relating V5 with projection of combined). □

Theorem 50 (B + $\mathcal{J}$ + SLS: Relating SLS with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{SLS}}(p) = Beh^{\mathsf{B}+\mathcal{J}+\mathsf{SLS}}_{\omega}(p)\restriction^{\mathsf{SLS}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). □

R.10 $_{\mathcal{J}+\mathsf{S}+\mathsf{R}}$

R.10.1 Projection Preservation.

Theorem 51 ($\mathcal{J}$ + S + R: Relating V2 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathcal{J}}(p) = Beh^{\mathcal{J}+\mathsf{S}+\mathsf{R}}_{\omega}(p)\restriction^{\mathcal{J}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). □

Theorem 52 ($\mathcal{J}$ + S + R: Relating V4 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{S}}(p) = Beh^{\mathcal{J}+\mathsf{S}+\mathsf{R}}_{\omega}(p)\restriction^{\mathsf{S}}$.*

Proof. The proof is analogous to Theorem 70 (V45: Relating V5 with projection of combined). □

Theorem 53 ($\mathcal{J}$ + S + R: Relating V5 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{R}}(p) = Beh^{\mathcal{J}+\mathsf{S}+\mathsf{R}}_{\omega}(p)\restriction^{\mathsf{R}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). □

R.11 $\mathcal{Q}_{\mathcal{J}+\mathsf{S}+\mathsf{SLS}}$

R.11.1 Projection Preservation.

Theorem 54 ($\mathcal{J}$ + S + SLS: Relating V2 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathcal{J}}(p) = Beh^{\mathcal{J}+\mathsf{S}+\mathsf{SLS}}_{\omega}(p)\upharpoonright^{\mathcal{J}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). □

Theorem 55 ($\mathcal{J}$ + S + SLS: Relating V4 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{S}}(p) = Beh^{\mathcal{J}+\mathsf{S}+\mathsf{SLS}}_{\omega}(p)\upharpoonright^{\mathsf{S}}$.*

Proof. The proof is analogous to Theorem 70 (V45: Relating V5 with projection of combined). □

Theorem 56 ($\mathcal{J}$ + S + SLS: Relating SLS with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{SLS}}(p) = Beh^{\mathcal{J}+\mathsf{S}+\mathsf{SLS}}_{\omega}(p)\upharpoonright^{\mathsf{SLS}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). □

R.12 $\mathcal{Q}_{\mathsf{B}+\mathsf{S}+\mathsf{SLS}}$

Theorem 57 (B + S + SLS: Relating V1 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{B}}(p) = Beh^{\mathsf{B}+\mathsf{S}+\mathsf{SLS}}_{\omega}(p)\upharpoonright^{\mathsf{B}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). □

Theorem 58 (B + S + SLS: Relating V4 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{S}}(p) = Beh^{\mathsf{B}+\mathsf{S}+\mathsf{SLS}}_{\omega}(p)\upharpoonright^{\mathsf{S}}$.*

Proof. The proof is analogous to Theorem 70 (V45: Relating V5 with projection of combined). □

Theorem 59 (B + S + SLS: Relating SLS with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{SLS}}(p) = Beh^{\mathsf{B}+\mathsf{S}+\mathsf{SLS}}_{\omega}(p)\upharpoonright^{\mathsf{SLS}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). □

R.13 $\mathcal{Q}_{\mathsf{B}+\mathcal{J}+\mathsf{S}+\mathsf{R}}$

R.13.1 Projection Preservation.

Theorem 60 (B + $\mathcal{J}$ + S + R: Relating V1 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{B}}(p) = Beh^{\mathsf{B}+\mathcal{J}+\mathsf{S}+\mathsf{R}}_{\omega}(p)\upharpoonright^{\mathsf{B}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). □

Theorem 61 (B + $\mathcal{J}$ + S + R: Relating V2 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathcal{J}}(p) = Beh^{\mathsf{B}+\mathcal{J}+\mathsf{S}+\mathsf{R}}_{\omega}(p)\upharpoonright^{\mathcal{J}}$.*

Proof. The proof is analogous to Theorem 70 (V45: Relating V5 with projection of combined). □

Theorem 62 (B + $\mathcal{J}$ + S + R: Relating V4 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{\mathsf{S}}(p) = Beh^{\mathsf{B}+\mathcal{J}+\mathsf{S}+\mathsf{R}}_{\omega}(p)\upharpoonright^{\mathsf{S}}$.*

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). ◻

Theorem 63 (B + J + S + R: Relating V5 with projection of combined). *Let p be a program and ω be a speculation window. Then* $Beh^{\omega}_{R}(p) = Beh^{B+J+S+R}_{\omega}(p)\restriction^{R}$.

Proof. The proof is analogous to Theorem 70 (V45: Relating V5 with projection of combined). ◻

R.14 $\text{👻}_{B+J+S+SLS}$

R.14.1 Projection Preservation.

Theorem 64 (B + J + S + SLS: Relating V1 with projection of combined). *Let p be a program and ω be a speculation window. Then* $Beh^{\omega}_{B}(p) = Beh^{B+J+S+R}_{\omega}(p)\restriction^{B}$.

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). ◻

Theorem 65 (B + J + S + SLS: Relating V2 with projection of combined). *Let p be a program and ω be a speculation window. Then* $Beh^{\omega}_{J}(p) = Beh^{B+J+S+SLS}_{\omega}(p)\restriction^{J}$.

Proof. The proof is analogous to Theorem 70 (V45: Relating V5 with projection of combined). ◻

Theorem 66 (B + J + S + SLS: Relating V4 with projection of combined). *Let p be a program and ω be a speculation window. Then* $Beh^{\omega}_{S}(p) = Beh^{B+J+S+SLS}_{\omega}(p)\restriction^{S}$.

Proof. The proof is analogous to Theorem 69 (V45: Relating V4 with projection of combined). ◻

Theorem 67 (B + J + S + SLS: Relating SLS with projection of combined). *Let p be a program and ω be a speculation window. Then* $Beh^{\omega}_{SLS}(p) = Beh^{B+J+S+SLS}_{\omega}(p)\restriction^{SLS}$.

Proof. The proof is analogous to Theorem 70 (V45: Relating V5 with projection of combined). ◻

The combinations not possible are:

(1) 2 combinations: 👻_{R+SLS}
(2) 3 combinations: $\text{👻}_{J+R+SLS}$, $\text{👻}_{B+R+SLS}$, $\text{👻}_{S+R+SLS}$
(3) 4 combinations: $\text{👻}_{B+J+R+SLS}$, $\text{👻}_{B+S+R+SLS}$, $\text{👻}_{J+S+R+SLS}$
(4) 5 combinations: $\text{👻}_{B+J+S+R+SLS}$

R.15 Oracle Overapproximation for the general combination

Theorem 68 (Oracle Overapproximation). *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 $((p,\sigma))\,\text{👻}_{NS}\overline{\tau}$, $((p,\sigma'))\,\text{👻}_{NS}\overline{\tau}$, then $((p,\sigma))\,\text{👻}^{\omega}_{xy}\overline{\tau}''$, $((p,\sigma'))\,\text{👻}^{\omega}_{xy}\overline{\tau}''$*

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) $((p,\sigma))\,\text{👻}_{NS}\overline{\tau}'$, $((p,\sigma'))\,\text{👻}_{NS}\overline{\tau}'$ 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 $((p,\sigma)) \Downarrow^{\omega}_{xy} \overline{\tau}''$, $((p,\sigma')) \Downarrow^{\omega}_{xy} \overline{\tau}''$ 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 $((p,\sigma)) \Downarrow_{NS} \overline{\tau}$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}$, then $(p,\sigma) \Downarrow^{O}_{xy} \overline{\tau}'$ and $(p,\sigma') \Downarrow^{O}_{xy} \overline{\tau}'$.

We fulfill all premises of SNI by a) and b) for p and get $(p,\sigma) \Downarrow^{O}_{xy} \overline{\tau}'$ and $(p,\sigma') \Downarrow^{O}_{xy} \overline{\tau}'$.

We use Proposition 13 (Combined: Sound and Completeness between Spec and AM semantics) with $(p,\sigma) \Downarrow^{O}_{xy} \overline{\tau}'$ and $(p,\sigma') \Downarrow^{O}_{xy} \overline{\tau}'$ to get $((p,\sigma)) \Downarrow^{\omega}_{xy} \overline{\tau}''$, $((p,\sigma')) \Downarrow^{\omega}_{xy} \overline{\tau}''$. This completes the proof.

($\Leftarrow$) We have

(1) $\sigma \sim_P \sigma'$ and
(2) $((p,\sigma)) \Downarrow_{NS} \overline{\tau}'$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}'$ and
(3) if $\sigma \sim_P \sigma'$ and $((p,\sigma)) \Downarrow_{NS} \overline{\tau}$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}$, then $((p,\sigma)) \Downarrow^{\omega}_{xy} \overline{\tau}''$, $((p,\sigma')) \Downarrow^{\omega}_{xy} \overline{\tau}''$

Note that we got assumptions a) and b) by the unfolding of the definition of SNI. We need to show that $(p,\sigma) \Downarrow^{O}_{xy} \overline{\tau}'$ and $(p,\sigma') \Downarrow^{O}_{xy} \overline{\tau}'$ holds.

By using assumption a) and b) for assumption c), we get $((p,\sigma)) \Downarrow^{\omega}_{xy} \overline{\tau}''$, $((p,\sigma')) \Downarrow^{\omega}_{xy} \overline{\tau}''$.

Let O be an arbitrary prediction oracle with speculative window at most ω.

From Proposition 13 (Combined: Sound and Completeness between Spec and AM semantics) with $((p,\sigma)) \Downarrow^{\omega}_{xy} \overline{\tau}''$, $((p,\sigma')) \Downarrow^{\omega}_{xy} \overline{\tau}''$ we get back $(p,\sigma) \Downarrow^{O}_{xy} \overline{\tau}$, $(p,\sigma') \Downarrow^{O}_{xy} \overline{\tau}$. 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 13 (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 $((p,\sigma)) \Downarrow^{\omega}_{xy} \overline{\tau}$ and $((p,\sigma')) \Downarrow^{\omega}_{xy} \overline{\tau}$ iff $(p,\sigma) \Downarrow^{O}_{xy} \overline{\tau}'$, $(p,\sigma) \Downarrow^{O}_{xy} \overline{\tau}'$ for all prediction oracles O with speculative window at most ω.*

Proof. The proposition immediately follows from Lemma 129 (Comb: Soundness Am semantics w.r.t. speculative semantics) and Lemma 130 (Comb: Completeness Am semantics w.r.t. Oracle semantics) □

R.15.1 Soundness.

Definition 41 (Relation between AM and Oracle States General)**.** *We define two relations between AM and oracle semantics.* $\approx$ $\sim$

$\boxed{\Sigma_{xy} \approx X_{xy}}$

$$\frac{}{\varnothing \approx \varnothing}\ \text{(Base)} \qquad \frac{\Sigma_{xy} \sim X_{xy}\restriction_{com} \qquad INV(\Sigma_{xy}, X_{xy})}{\Sigma_x \approx X_{xy}}\ \text{(Single-Base)}$$

$$\frac{\begin{array}{ccc}\Sigma_{xy} \sim X_{xy}\restriction_{com} \quad \text{elem\_of\_states}(\Phi_{xy}) = \text{elem\_of\_states}(\Psi_{xy}) & \Phi_{xy}.ctr = \Psi_{xy}.ctr & \Phi'_{xy}.ctr = \Psi'_{xy}.ctr \\ X_{xy} = X'_{xy} \cdot \Psi_{xy} \qquad \Sigma_{xy} = \Sigma'_{xy} \cdot \Phi_{xy} & & INV(\Sigma_{xy}, X_{xy})\end{array}}{\Sigma'_{xy} \cdot \Phi_{xy} \cdot \Phi'_{xy} \cdot \Sigma''_{xy} \approx X'_x \cdot \Psi_x \cdot \Psi_x^{false}}\ \text{(Single-OracleTrue)}$$

$$\frac{\begin{array}{c}\Sigma_{xy} \sim X_{xy}\restriction_{com} \quad \text{elem\_of\_states}(\Phi_{xy}) = \text{elem\_of\_states}(\Psi_{xy}) \quad \Phi_{xy}.ctr = \Psi_{xy}.ctr \quad \Phi'_{xy}.ctr = \Psi'_{xy}.ctr \\ \Psi'_{xy}.n = 0 \quad \text{is\_mispred}(\Psi'_{xy}) \quad \Phi_{xy}.n' \geq 0 \quad X_{xy} = X'_{xy} \cdot \Psi_{xy} \quad \Sigma_{xy} = \Sigma'_{xy} \cdot \Phi_{xy} \quad INV(\Sigma_{xy}, X_{xy})\end{array}}{\Sigma'_{xy} \cdot \Phi_{xy} \cdot \Phi'_{xy} \cdot \Sigma''_{xy} \approx X'_{xy} \cdot \Psi_{xy} \cdot \Psi'_{xy} \cdot X''_{xy}}\ \text{(Single-Transaction-Rollback)}$$

$\boxed{\Sigma_{xy} \sim X_{xy}}$

$$\frac{}{\varnothing \sim \varnothing}\ \text{(Base)} \qquad \frac{|\Sigma'_{xy}| = |X'_{xy}| \qquad \Sigma'_{xy} \sim X'_{xy} \qquad \text{elem\_of\_states}(\Phi_{xy}) = \text{elem\_of\_states}(\Psi_{xy})}{\Sigma'_{xy} \cdot \Phi_{xy} \sim X'_{xy} \cdot \Psi_{xy}}\ \text{(Single)}$$

Here are the defintion of elem_of_states for the different concrete states:

$$\text{elem\_of\_states}(\Sigma_x) = \langle p, ctr, \sigma \rangle$$

$$\text{elem\_of\_states}(X_x) = \langle p, ctr, \sigma \rangle \text{where } x \in \{\mathsf{B}, \mathcal{J}, \mathsf{S}, \mathsf{SLS}\}$$

$$\text{elem\_of\_states}(\Sigma_{\mathsf{R}}) = \langle p, ctr, \sigma, \mathbb{R} \rangle$$

$$\text{elem\_of\_states}(X_{\mathsf{R}}) = \langle p, ctr, \sigma, \mathbb{R} \rangle$$

Definition 42 (Comb: Comparison of elem_of_states)**.** elem_of_states Σ_{xy} = elem_of_states $X_{xy} \stackrel{\text{def}}{=}$ elem_of_states $\Sigma_{xy}\restriction^{x}_{xy}$ = elem_of_states $X_{xy}\restriction^{x}_{xy}$ *and* elem_of_states $\Sigma_{xy}\restriction^{y}_{xy}$ = elem_of_states $X_{xy}\restriction^{y}_{xy}$

elem_of_states$(\Sigma_x) \subseteq$ elem_of_states(Σ_{xy})

elem_of_states$(\Sigma_{xy}) \setminus$ elem_of_states(Σ_x) elem_of_states$(\Sigma_{xy}\restriction^{x}_{xy}) \notin$ elem_of_states$(\Sigma_{xy}) \setminus$ elem_of_states(Σ_x)

The predicate is_mispred states if the speculative instance was created by a misprediction or a commit action. A correct decision (commit) is annotated with *false*, while an incorrect decision (will rolled back) is annotated with *true*. This is uniform with all the source semantics. We can uniformly represent the decision with a boolean.

We define one relation for all of these proofs. Note that this relation differentiates between rolled back, committed and a base case. The only dependent here is on σ and n. Nothing more is needed. All our semantics share this structure. Thus we define a base relation here. This is possible because we can represent if a state needs to be rolled back or committed with a boolean on the state for all speculative semantics.

True means speculation started and mispredicted. False means the transaction will be committed.

Related to the combination. The combination tracks from where every instance in the state is coming from. So it is always clear which commit rule needs to be used.

Lemma 128 (Comb: Intial states in $\approx$). *Let p be a program, ω be a speculation window and O be an oracle with speculation window at most ω. If*

(1) $\sigma, \sigma' \in \mathit{InitConf}$ *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) $X^{init}_{xy}(p, \sigma) \cong X^{init}_{xy}(p, \sigma')$ *and*
(2) $\Sigma^{init}_{xy}(p, \sigma) \cong \Sigma^{init}_{xy}(p, \sigma')$ *and*
(3) $\Sigma^{init}_{xy}(p, \sigma) \approx X^{init}_{xy}(p, \sigma)$ *and* $\Sigma^{init}_{xy}(p, \sigma') \approx X^{init}_{xy}(p, \sigma')$ *by Rule Single-Base*

Proof. We have

(1) $\sigma, \sigma' \in \mathit{InitConf}$ and
(2) $\Sigma^{init}_{xy}(p, \sigma)$ and $\Sigma^{init}_{xy}(p, \sigma')$ and
(3) $X^{init}_{xy}(p, \sigma)$ and $X^{init}_{xy}(p, \sigma')$

All follow from the definition of $X^{init}_{xy}()$ and $\Sigma^{init}_{xy}()$:

I Immediate
II Immediate
III Immediate using Rule Single-Base

□

Lemma 129 (Comb: Soundness Am semantics w.r.t. speculative semantics). *If*

(1) $\vdash \text{👻}_{xy} : \mathit{WFC}$
(2) $\sigma, \sigma' \in \mathit{InitConf}$ *and*
(3) $((p, \sigma))\, \text{👻}^{\omega}_{xy} \overline{\tau}, ((p, \sigma'))\, \text{👻}^{\omega}_{xy} \overline{\tau}$

Then for all prediction oracles O with speculation window at most ω.

I $(p, \sigma)\, \text{👻}^{O}_{xy}\, \overline{\tau}', (p, \sigma)\, \text{👻}^{O}_{xy}\, \overline{\tau}'$

Proof. Let $\omega \in \mathbb{N}$ be a speculation window and $\sigma, \sigma' \in \mathit{InitConf}$ be two initial configurations. We have:

(1) $((p, \sigma))\, \text{👻}^{\omega}_{xy} \overline{\tau}, ((p, \sigma'))\, \text{👻}^{\omega}_{xy} \overline{\tau}$

Furthermore, let O be an arbitrary prediction oracle with speculative window at most ω.

Then we know there are executions $\Sigma^{init}_{xy}((p, \sigma) \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}$ and $\Sigma^{init}_{xy}(p, \sigma') \Downarrow^{\overline{\tau}}_{xy} \Sigma''_{xy}$ where $\vdash \Sigma'_{xy} : \mathit{fin}$ and $\vdash \Sigma''_{xy} : \mathit{fin}$.

We unfold the definition of 👻^{O}_{xy} and get $X^{init}_{xy}(p, \sigma)$ and $X^{init}_{xy}(p, \sigma')$ as initial states.

We need to find $\vdash X'_{xy} : \mathit{fin}, \vdash X''_{xy} : \mathit{fin}$ such that $X^{init}_{xy}(p, \sigma) \Downarrow^{\overline{\tau}}_{xy} X'_{xy}$ and $X^{init}_{xy}(p, \sigma') \overset{O_{xy}}{\rightsquigarrow}{}^{xy}_{\overline{\tau}} X''_{xy}$.

Since we know by Lemma 128 (Comb: Intial states in $\approx$) that our initial states fulfill all the premises for applying $\vdash \text{👻}_{xy} : \mathit{WFC}$ Relation Preservation and we get:

(1) $X^{init}_{xy}(p,\sigma) \overset{O_{xy}}{\leadsto}{}^{xy}_{\overline{\tau}'} X'_{xy_1}$, $X^{init}_{xy}(p,\sigma') \overset{O_{xy}}{\leadsto}{}^{xy}_{\overline{\tau}''} X'_{xy_2}$
(2) $\Sigma'_{xy} \cong \Sigma''_{xy}$
(3) $X'_{xy_1} \cong X'_{xy_2}$ and $\overline{\rho} = \varnothing$
(4) $\Sigma'_{xy} \approx X'_{xy_1}$ and $\Sigma'_{xy} \approx X'_{xy_2}$
(5) $\overline{\tau}' = \overline{\tau}''$

We now argue, how we obtain final states from the oracle states X'_{xy_1} and X'_{xy_2}.

Notice that because of $\vdash \Sigma'_{xy} : fin$ and $\vdash \Sigma''_{xy} : fin$ that $\Sigma'_{xy} \approx X'_{xy_1}$ and $\Sigma'_{xy} \approx X'_{xy_2}$ can only be related by Rule Single-Base, because there are no ongoing transactions in Σ'_{xy} and Σ''_{xy}.

We now do a case analysis on the length of X'_{xy_1} and X'_{xy_2}. Since $X'_{xy_1} \cong X'_{xy_2}$, we know that $|X'_{xy_1}| = |X'_{xy_2}|$.

$|X'_{xy_1}| = 1$ We know that $\Sigma'_{xy} \approx X'_{xy_1}$ and $\vdash \Sigma'_{xy} : fin$.

Because of $\vdash \Sigma'_{xy} : fin$, we know that $\Sigma'_{xy}.\sigma \in \mathit{FinalConf}$.

Thus, by $\Sigma'_{xy} \approx X'_{xy_1}$ we have $X'_{xy_1}.\sigma \in \mathit{FinalConf}$ since $X'_{xy_1}.\sigma = \Sigma'_{xy}.\sigma$.

Because $|X'_{xy_1}| = 1$, we also have $X'_{xy_1}.n = \bot$.

We can now conclude that $\vdash X'_{xy_1} : fin$.

$|X'_{xy_1}| > 1$ We know that $\Sigma'_{xy} \approx X'_{xy_1}$ and $\vdash \Sigma'_{xy} : fin$.

Because of $\vdash \Sigma'_{xy} : fin$, we know that $\Sigma'_{xy}.\sigma \in \mathit{FinalConf}$ and $\vdash_O \Sigma'_{xy} : noongoing$

Thus, by $\Sigma'_{xy} \approx X'_{xy_1}$ we have $X'_{xy_1}.\sigma \in \mathit{FinalConf}$ since $X'_{xy_1}.\sigma = \Sigma'_{xy}.\sigma$ and $\vdash_O X'_{xy_1} : noongoing$,

Since $X'_{xy_1}.\sigma \in \mathit{FinalConf}$ and $|X'_{xy_1}| > 1$, we know there are speculative instances that need to be committed.

We can now apply Lemma 8 (Reaching Final state from final configuration (Finish commit instances)):

(1) $X'_{xy_1} \overset{O_{xy}}{\leadsto}{}^{xy}_{\overline{\tau}''} X'_{xy}$
(2) $\forall \tau \in \overline{\tau}^{\dagger}.\ \tau = \texttt{commit}\ id$ for some $id \in \mathbb{N}$
(3) $\vdash X'_{xy} : fin$
(4) $X'_{xy}.\sigma = X'_{xy_1}.\sigma$

Because of $X'_{xy_1} \cong X'_{xy_2}$, we know that X'_{xy_2} generates the same trace with the same *id*s for the commits. Thus, $\vdash X'_{xy} : fin$.

The case for X'_{xy_2} are analogous and not shown here.

Thus, $(p,\sigma)\ \Omega^{O}_{xy}\ \overline{\tau}' \cdot \overline{\tau}^{\dagger}$, $(p,\sigma')\ \Omega^{O}_{xy}\ \overline{\tau}' \cdot \overline{\tau}^{\dagger}$. □

R.15.2 Completeness.

Definition 43 (Combined: 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.

For a given $\Sigma_{xy} \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy}$ we can extract all the states into a set Σ^{States}

Definition 44 (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 AM oracle and a set of stats on which the relation will hold. This oracle has to always mispredict.*

$$\boxed{\Sigma_x \approx^{\Sigma^{States}}_{O^{xy}_{am}} X_x}$$

$$\frac{}{\varnothing \approx^{\Sigma^{States}}_{O^{xy}_{am}} \varnothing}\ \textit{(Base-Oracle)} \qquad \frac{\Sigma_x \sim X_x\upharpoonright_{com} \quad \mathit{INV2}(\Sigma_x, X_x) \quad \mathit{minWndw}(X_x) > 0 \quad \Sigma_x \in \Sigma^{States}}{\Sigma_x \approx^{\Sigma^{States}}_{O^{xy}_{am}} X_x}\ \textit{(Single-Base-Oracle)}$$

$$\frac{\begin{array}{ccc} \Sigma''_x \sim X''_x\upharpoonright_{com} & \Phi'_x.n \geq 0 & \text{elem\_of\_states}(\Phi_x) = \text{elem\_of\_states}(\Psi_x) \\ X''_x = X'_x \cdot \Psi_x & \Phi'_x.ctr = \Psi'_x.ctr & \Psi'_x.n = 0 \\ \Sigma''_x = \Sigma'_x \cdot \Phi_x & \mathit{INV2}(\Sigma_x, X_x) & \Sigma'_{xy} \cdot \Phi_x \cdot \Phi^{false'}_x \cdot \Sigma_{x1} \in \Sigma^{States} \end{array}}{\Sigma'_{xy} \cdot \Phi_x \cdot \Phi^{true'}_x \cdot \Sigma_{x1} \approx^{\Sigma^{States}}_{O^{xy}_{am}} X'_x \cdot \Psi_x \cdot \Psi^{true'}_x}\ \textit{(Single-Transaction-Rollback-Oracle)}$$

Lemma 130 (Comb: Completeness Am semantics w.r.t. Oracle semantics)**.** *Let p be a program, $\omega \in \mathbb{N}$ be a speculative window, $\sigma, \sigma' \in \mathit{InitConf}$ be two initial configurations. If*

(1) $((p, \sigma)) \Downarrow^{\omega}_{xy} \overline{\tau}$ and $((p, \sigma')) \Downarrow^{\omega}_{xy} \overline{\tau}'$ 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, $\sigma, \sigma' \in \mathit{InitConf}$ 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 $((p, \sigma)) \Downarrow^{\omega}_{xy} \overline{\tau}$ 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:

$$\Sigma^{init}_{xy}(p, \sigma) \Downarrow^{\overline{\tau}}_{xy} \Sigma^*_{xy} \xrightarrow{\tau_{am}}_{xy} \Sigma^{**}_{xy} \Downarrow^{\overline{\tau}_{end}}_{xy} \Sigma_{xy_F}$$

$$\Sigma^{init}_{xy}(p, \sigma') \Downarrow^{\overline{\tau}}_{xy} \Sigma^{\dagger}_{xy} \xrightarrow{\tau'_{am}}_{xy} \Sigma^{\dagger\dagger}_{xy} \Downarrow^{\overline{\tau}'_{end}}_{xy} \Sigma'_{xy_F}$$

We claim that there is a prediction oracle O with speculative window at most ω such that

a) $X^{init}_{xy}(p, \sigma) \ {}^{O_{xy}}\!\rightsquigarrow^{xy}_{v} X^*_{xy}$ and $X^*_{xy}.\sigma = \Sigma^*_{xy}.\sigma$ and $\mathit{INV2}(X^*_{xy}, \Sigma^*_{xy})$ and
b) $X^{init}_{xy}(p, \sigma') \ {}^{O_{xy}}\!\rightsquigarrow^{xy}_{v} X^{\dagger}_{xy}$ and $X^{\dagger}_{xy}.\sigma = \Sigma^{\dagger}_{xy}.\sigma$ and $\mathit{INV2}(X^{\dagger}_{xy}, \Sigma^{\dagger}_{xy})$
c) $X^*_{xy} \cong_{xy} X^{\dagger}_{xy}$

We achieve this by applying $\vdash \rightsquigarrow_{xy}$: *WFC* Relation Preservation AM on the AM execution up to the point of the difference $\Sigma^{init}_{xy}(p, \sigma) \Downarrow^{\overline{\tau}}_{xy} \Sigma_{xy_1}$ with the O^{xy}_{am} and Σ^{States}_1 being all the states in $\Sigma^{init}_{xy}(p, \sigma) \Downarrow^{\overline{\tau}}_{xy} \Sigma_{xy_1}$ (similar for Σ^{States}_2 for $\Sigma^{init}_{xy}(p, \sigma') \Downarrow^{\overline{\tau}}_{xy} \Sigma'_{xy_1}$).

We now show that $\Sigma^*_{xy} \approx^{\Sigma^{States}}_{O^{xy}_{am}} X^*_{xy}$ and $\Sigma^{\dagger}_{xy} \approx^{\Sigma^{States}}_{O^{xy}_{am}} X^{\dagger}_{xy}$ is derived by Rule Single-Base-Oracle.

We only show and $\Sigma^*_{xy} \approx^{\Sigma^{States}}_{O^{xy}_{am}} X^*_{xy}$ since and $\Sigma^{\dagger}_{xy} \approx^{\Sigma^{States}}_{O^{xy}_{am}} X^{\dagger}_{xy}$ is analogous 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 $\mathit{INV2}(\Sigma^*_{xy}, X^*_{xy})$ and $\Sigma^*_{xy}.n = \bot$ that $X^*_{xy}.n = \bot$ that $\Sigma^*_{xy} \approx^{\Sigma^{States}}_{O^{xy}_{am}} X^*_{xy}$ can only be derived Rule 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*(Σ^*_{xy}, X^*_{xy}) we get $minWndw(X^*_{xy}) > 0$ (Similar for $X^\dagger_{xy}$ because of $\Sigma^*_{xy} \cong \Sigma^\dagger_{xy}$).
If $\Sigma^*_{xy} \approx^{\Sigma^{States}}_{O^{xy}_{am}} X^*_{xy}$ 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 $X^*_{xy} \approx^{\Sigma^{States}}_{O^{xy}_{am}} \Sigma^*_{xy}$ by Rule Single-Base-Oracle.

We can now use Lemma 139 (Comb: AM and Oracle coincide) with $\Sigma^*_{xy} \overset{\tau_{am}}{\Longrightarrow\Omega}_{xy} \Sigma^{**}_{xy}$ and $X^*_{xy} \approx^{\Sigma^{States}}_{O^{xy}_{am}} \Sigma^*_{xy}$ and get $X^*_{xy} \overset{O_{xy}}{\underset{xy}{\overset{\tau_{am}}{\rightsquigarrow}}} X^{**}_{xy}$.

Similar we apply Lemma 139 (Comb: AM and Oracle coincide) with $\Sigma^\dagger_{xy} \overset{\tau'_{am}}{\Longrightarrow\Omega}_{xy} \Sigma^{\dagger\dagger}_{xy}$ and $X^\dagger_{xy} \approx^{\Sigma^{States}}_{O^{xy}_{am}} \Sigma^\dagger_{xy}$ and get $X^\dagger_{xy} \overset{O_{xy}}{\underset{xy}{\overset{\tau'_{am}}{\rightsquigarrow}}} X^{\dagger\dagger}_{xy}$.

We are now done because we found a difference in the oracle execution since $\tau_{am} \neq \tau'_{am}$.

□

R.16 Proving Relation Preservation for a combination

We can derive the 3rd and 5th condition of WFC in general. We use assumptions about the source semantics (fulfilled by all our semantics) to derive WFC 3 generally.

Assumption 3 (Relation Preservation x)**.** *If*

(1) $\Sigma_x \approx_x X_x$ *and* $\Sigma^\dagger_x \approx_x X^\dagger_x$ *and*
(2) $\Sigma_x \overset{\overline{\tau}}{\Longrightarrow\Omega}_x \Sigma'_x$ *and* $\Sigma^\dagger_x \overset{\tau}{\Longrightarrow\Omega}_x \Sigma^{\dagger\dagger}_x$
(3) $\Sigma_x \cong \Sigma^\dagger_x$ *and* $X_x \cong X^\dagger_x$

Then there exists X'_x *and* $X^{\dagger\dagger}_x$

I $X_x \;{}^{O_x}\!\!\wr\tfrac{x}{\overline{\tau}'} X'_x$ *and* $X^\dagger_x \;{}^{O_x}\!\!\wr\tfrac{x}{\overline{\tau}'} X^{\dagger\dagger}_x$
II $\Sigma'_x \approx_x X'_x$ *and* $\Sigma^{\dagger\dagger}_x \approx_x X^{\dagger\dagger}_x$ *and*
III $\Sigma'_x \cong \Sigma^{\dagger\dagger}_x$ *and* $X'_x \cong X^{\dagger\dagger}_x$

Assumption 4 (Relation Preservation y)**.** *If*

(1) $\Sigma_y \approx X_y$ *and* $\Sigma^\dagger_y \approx_y X^\dagger_y$ *and*
(2) $\Sigma_y \overset{\overline{\tau}}{\Longrightarrow\Omega}_y \Sigma'_y$ *and* $\Sigma^\dagger_y \overset{\tau}{\Longrightarrow\Omega}_y \Sigma^{\dagger\dagger}_y$
(3) $\Sigma_y \cong \Sigma^\dagger_y$ *and* $X_y \cong X^\dagger_y$

Then

I $X_y \;{}^{O_y}\!\!\wr\tfrac{y}{\overline{\tau}'} X'_y$ *and* $X^\dagger_y \;{}^{O_y}\!\!\wr\tfrac{y}{\overline{\tau}'} X^{\dagger\dagger}_y$
II $\Sigma'_y \approx_y X'_y$ *and* $\Sigma^{\dagger\dagger}_y \approx_y X^{\dagger\dagger}_x$ *and*
III $\Sigma'_y \cong \Sigma^{\dagger\dagger}_y$ *and* $X'_y \cong X^{\dagger\dagger}_y$

Lemma 131 (Relation Preservation : Soundness big-step). *If*

(1) $\Sigma_{xy_1} \cong \Sigma_{xy_2}$
(2) $X_{xy_1} \cong X_{xy_2}$ *and* $\overline{\rho} = \emptyset$
(3) $\Sigma_{xy_1} \approx X_{xy_1}$ *and* $\Sigma_{xy_2} \approx X_{xy_2}$
(4) $\Sigma_{xy_1} \Downarrow_{xy}^{\overline{\tau}} \Sigma'_{xy_1}$ *and* $\Sigma_{xy_2} \Downarrow_{xy}^{\overline{\tau}} \Sigma'_{xy_2}$

Then for all prediction oracles O with speculation window at most ω.

I $X_{xy_1} \ {}^{O_{xy}}\!\!\downarrow_{\overline{\tau}'}^{xy} X'_{xy_1}, X_{xy_2} \ {}^{O_{xy}}\!\!\downarrow_{\overline{\tau}''}^{xy} X'_{xy_2}$
II $\Sigma'_{xy_1} \cong \Sigma'_{xy_2}$
III $X'_{xy_1} \cong X'_{xy_2}$ *and* $\overline{\rho} = \emptyset$
IV $\Sigma'_{xy_1} \approx X'_{xy_1}$ *and* $\Sigma'_{xy_2} \approx X'_{xy_2}$
V $\overline{\tau}' = \overline{\tau}''$

Proof. **Rule AM-Reflection-xy** We have $\Sigma_{xy_1} \Downarrow_{xy}^{\varepsilon} \Sigma'_{xy_1}$ and $\Sigma_{xy_2} \Downarrow_{xy}^{\varepsilon} \Sigma'_{xy_2}$, where $\Sigma'_{xy_1} = \Sigma_{xy_1}$ and $\Sigma'_{xy_2} = \Sigma_{xy_2}$.

Furthermore, we use Rule SE-Reflection-xy to derive $X_{xy_1} \ {}^{O_{xy}}\!\!\downarrow_{\varepsilon}^{xy} X'_{xy_1}, X_{xy_2} \ {}^{O_{xy}}\!\!\downarrow_{\varepsilon}^{xy} X'_{xy_2}$ with $X'_{xy_1} = X_{xy_1}$ and $X'_{xy_2} = X_{xy_2}$.

We now trivially satisfy all conclusions.

Rule AM-Single-xy We have $\Sigma_{xy_1} \Downarrow_{xy}^{\overline{\tau}''} \Sigma'_{xy}$ with $\Sigma'_{xy} \overset{\tau}{\Rightarrow}_{xy} \Sigma'_{xy_1}$ and $\Sigma_{xy_2} \Downarrow_{xy}^{\overline{\tau}''} \Sigma''_{xy}$ and $\Sigma''_{xy} \overset{\tau}{\Rightarrow}_{xy} \Sigma'_{xy_2}$.

We now apply IH on $\Sigma_{xy_1} \Downarrow_{xy}^{\overline{\tau}''} \Sigma'_{xy}$ and $\Sigma_{xy_2} \Downarrow_{xy}^{\overline{\tau}''} \Sigma''_{xy}$ and get

(a) $X_{xy_1} \ {}^{O_{xy}}\!\!\downarrow_{\overline{\tau}'}^{xy} X'_{xy}, X_{xy_2} \ {}^{O_{xy}}\!\!\downarrow_{\overline{\tau}''}^{xy} X''_{xy}$
(b) $\Sigma'_{xy} \cong \Sigma''_{xy}$
(c) $X'_{xy} \cong X''_{xy}$ and $\overline{\rho}' = \emptyset$
(d) $\Sigma'_{xy} \approx X'_{xy}$ and $\Sigma''_{xy} \approx X''_{xy}$
(e) $\overline{\tau}' = \overline{\tau}''$

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 $X'_{xy} \cong X''_{xy}$.

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 Single-Transaction-Rollback.

To account for possible outstanding commits, we can use Lemma 9 (Executing a chain of commits) on X''_{xy} and get

f) $X'_{xy} \ {}^{O_{xy}}\!\!\downarrow_{\overline{\tau}'''}^{xy} X'''_{xy}$
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 $|X'_{xy}\restriction_{com}| = |X'''_{xy}\restriction_{com}|$.

Thus, $\Sigma'_{xy} \sim X'''_{xy}\restriction_{com}$, $INV(\Sigma'_{xy}, X'''_{xy})$ and we have $\Sigma'_{S} \approx X'''_{xy}$ by Rule Single-Base.

We now proceed by inversion on the derivations $\Sigma'_{xy} \overset{\tau}{\Rightarrow}_{xy} \Sigma'_{xy_1}$ and $\Sigma''_{xy} \overset{\tau}{\Rightarrow}_{xy} \Sigma'_{xy_2}$.

Rule AM-Context-xy We have $\Psi'_{xy} \overset{\tau}{\rightsquigarrow}_{xy} \overline{\Psi}'_{xy}$ and $\Psi''_{xy} \overset{\tau}{\rightsquigarrow}_{xy} \overline{\Psi}'''_{xy}$ where $\Sigma'_{xy} = \overline{\Psi}_{xy} \cdot \Psi'_{xy}$ and $\Sigma''_{xy} = \overline{\Psi}''_{xy} \cdot \Psi''_{xy}$.

Using Lemma 132 (Relation Preservation : Soundness Single Step) we get the desired result.

Rule AM-x-Rollback-xy and Rule AM-y-Rollback-xy Contradiction, because $minWndw(X'''_{xy}) > 0$ and $INV(\Sigma'_{xy}, X'''_{xy})$.

Oracle We now apply inversion on $\Sigma'_{xy} \overset{\tau}{\rightsquigarrow}_{xy} \Sigma'_{xy_1}$.

Rule AM-Context-xy We choose $X'_{xy_1} = X'_{xy}$ and $X'_{xy_2} = X''_{xy}$.

Rollback

□

Lemma 132 (Relation Preservation : Soundness Single Step)**.** *If*

(1) $\Sigma_{xy} \cong \Sigma^{\dagger}_{xy}$ *and* $X_{xy} \cong X^{\dagger}_{xy}$
(2) $\Sigma_{xy} \approx_{xy} X_{xy}$ *and* $\Sigma^{\dagger}_{xy} \approx_{xy} X^{\dagger}_{xy}$ *by Base and*
(3) $\Sigma_{xy} \overset{\tau}{\rightsquigarrow}_{xy} \Sigma'_{xy}$ *and* $\Sigma^{\dagger}_{xy} \overset{\tau}{\rightsquigarrow}_{xy} \Sigma^{\dagger\dagger}_{xy}$
(4) $minWndw(X_{xy}) > 0$

then

(1) $X_{xy} \overset{O_{xy}}{\rightsquigarrow}{}^{xy}_{\overline{\tau}'} X'_{xy}$ *and* $X^{\dagger}_{xy} \overset{O_{xy}}{\rightsquigarrow}{}^{xy}_{\overline{\tau}'} X^{\dagger\dagger}_{xy}$
(2) $\Sigma'_{xy} \approx_{xy} X'_{xy}$ *and* $\Sigma^{\dagger\dagger}_{xy} \approx_{xy} X^{\dagger\dagger}_{xy}$ *and*
(3) $\Sigma'_{xy} \cong \Sigma^{\dagger\dagger}_{xy}$ *and* $X'_{xy} \cong X^{\dagger\dagger}_{xy}$

Proof. We proceed by case distinction on $\Sigma_{xy} \approx_{xy} X_{xy}$ and $\Sigma^{\dagger}_{xy} \approx_{xy} X^{\dagger}_{xy}$:

We proceed by inversion on $\Sigma_{xy} \overset{\tau}{\rightsquigarrow}_{xy} \Sigma'_{xy}$ and $\Sigma^{\dagger}_{xy} \overset{\tau}{\rightsquigarrow}_{xy} \Sigma^{\dagger\dagger}_{xy}$:

Rule AM-x-step Then we have $\Phi_x \upharpoonright^{x}_{xy} \overset{\tau}{\rightsquigarrow}_{x} \overline{\Phi}'_{x}$.

Let $X_{xy} = \overline{\Psi}_{xy} \cdot \Psi_{xy}$. By definition, we know $\Phi_{xy} \approx_{xy} \Psi_{xy}$. We can apply Assumption 3 (Relation Preservation x) and get:

$$\Sigma'_x \approx_{xy} X'_x$$
$$\Sigma^{\dagger\dagger}_x \approx_{xy} X^{\dagger\dagger}_x$$
$$X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}} X'_x$$
$$X^{\dagger}_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}} X^{\dagger\dagger}_x$$
$$X'_x \cong X^{\dagger\dagger}_x$$
$$\Sigma'_x \cong \Sigma_x\dagger\dagger$$

By Lemma 135 (Comb AM: Single step preserves ≅) we get $\Sigma'_{xy} \cong \Sigma^{\dagger\dagger}_{xy}$.

Next, we apply Lemma 137 (Recomposition x) on $\Sigma'_x \approx_{xy} X'_x$ and $\Sigma^{\dagger\dagger}_x \approx_{xy} X^{\dagger\dagger}_x$ and get $\Sigma'_{xy} \approx_{xy} X'_{xy}$ and $\Sigma^{\dagger\dagger}_{xy} \approx_{xy} X^{\dagger\dagger}_{xy}$.

Next, we check if a new speculative transaction was started.

We now argue how we get an execution for oracle states such that $X'_x = X'_{xy} \upharpoonright^{x}_{xy}$.

First, we proceed by Case distinction on the found derivation of $X_x \overset{O_{xy}}{\rightsquigarrow}{}^{xy}_{\overline{\tau}} X'_x$

Rule AM-Reflection-xy Then we have $X_x \overset{O_{xy}}{\rightsquigarrow}{}^{xy}_{\varepsilon} X'_x$.

Then we derive $X_{xy} \overset{O_{xy}}{\rightsquigarrow}{}^{xy}_{\varepsilon} X'_{xy}$ by Rule SE-Reflection-xy.

Thus, $X_{xy} = X'_{xy}$ and $X'_{xy} \upharpoonright^{x}_{xy} = X'_x$.

Rule AM-Single-xy

Since $\Sigma_{xy} \approx_{xy} X_{xy}$ by base we know $\Sigma_{xy}.\sigma = X_{xy}.\sigma$. Since $minWndw(X_{xy}) > 0$ we know that X_{xy} can take a step that is not a commit or rollback using x-step (modulo Confluence).

$X_{xy} \xrightarrow{\tau}_{xy} X''_{xy}$ by $\Psi_{xy} \upharpoonright^{x}_{xy} \xrightarrow{\tau}_{x} \overline{\Psi}''_x$. The same holds for $X^{\dagger}_{xy}$.

Thus we can apply Lemma 136 (Comb SE: Single step preserves $\cong$) and get $X''_{xy} \cong X^{*}_{xy}$

Since was done in the x semantics and the semantics is deterministic, we know that this step needs to exist in $X_x \overset{O_{xy}}{\rightsquigarrow}{}^{xy}_{\overline{\tau}} X'_x$ as well. Thus, there exists X''_x in $X_x \overset{O_{xy}}{\rightsquigarrow}{}^{xy}_{\overline{\tau}} X'_x$ such that $X''_{xy} \upharpoonright^{x}_{xy} = X''_x$.

We now do a case distinction if $X''_x = X'_x$ or not:

$X''_x = X'_x$ Then we have $X'_x = X''_{xy} \upharpoonright^{x}_{xy}$ and we are done. Then the execution is just an application of Rule SE-Single-xy with $X_{xy} \xrightarrow{\tau}_{xy} X''_{xy}$ and with Rule SE-Reflection-xy to get $X_{xy} \overset{O_{xy}}{\rightsquigarrow}{}^{xy}_{\overline{\tau}} X'_{xy}$.

$X''_x \neq X'_x$ This means there are additional steps from $X''_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}'} X'_x$.

We now argue that the only rule that is applicable here is the General rule.

Independent of the state we know that the sigma of the original states before execution at the top match. This means this sigma needs to be untouched otherwise $\approx_x$ would not hold.

Other things cannot be executed in X''_x since $\approx_x$ would not hold to Φ'_x.

Thus, this means a new speculative state was created. This implies that $\overline{\rho}$ is not empty for X'_x and additional steps were made to execute them.

This also means that X''_{xy} has a new speculative state and $\overline{\rho}$ is non-empty as well. We execute those as well.

Since these applications do not change anything of the state we have $X'_x = X'_{xy} \upharpoonright^{x}_{xy}$.

Since these observations are generated by $\overline{\rho}$ which come from X''_x and $X''_x = X''_{xy} \upharpoonright^{x}_{xy}$ we know the same observations were made.

Rule AM-y-step Then we have $\Phi_x \upharpoonright^{x}_{xy} \xrightarrow{\tau}_{x} \overline{\Phi}'_x$ and $\Phi^{\dagger}_x \upharpoonright^{x}_{xy} \xrightarrow{\tau}_{x} \overline{\Phi}^{\dagger\dagger}_x$. The proof is analogous to Rule AM-x-step using Assumption 3 (Relation Preservation x) and Lemma 137 (Recomposition x).

∎

Lemma 133 (Relation Preservation : Strong Soundness Single Step). *If*

(1) $\Sigma_{xy} \cong \Sigma^{\dagger}_{xy}$ *and* $X_{xy} \cong X^{\dagger}_{xy}$

(2) $\Sigma_{xy} \approx^{\Sigma^{States}}_{O^{xy}_{am}} X_{xy}$ *and* $\Sigma^{\dagger}_{xy} \approx^{\Sigma^{States}}_{O^{xy}_{am}} X^{\dagger}_{xy}$ *by Base and*

(3) $\Sigma_{xy} \xrightarrow{\tau}_{xy} \Sigma'_{xy}$ *and* $\Sigma^{\dagger}_{xy} \xrightarrow{\tau}_{xy} \Sigma^{\dagger\dagger}_{xy}$

(4) $minWndw(X_{xy}) > 0$

then

(1) $X_{xy} \overset{O_{xy}}{\rightsquigarrow}{}^{xy}_{\overline{\tau}'} X'_{xy}$ *and* $X^{\dagger}_{xy} \overset{O_{xy}}{\rightsquigarrow}{}^{xy}_{\overline{\tau}'} X^{\dagger\dagger}_{xy}$

(2) $\Sigma'_{xy} \approx^{\Sigma^{States}}_{O^{xy}_{am}} X'_{xy}$ *and* $\Sigma^{\dagger\dagger}_{xy} \approx^{\Sigma^{States}}_{O^{xy}_{am}} X^{\dagger\dagger}_{xy}$ *and*

(3) $\Sigma'_{xy} \cong \Sigma^{\dagger\dagger}_{xy}$ *and* $X'_{xy} \cong X^{\dagger\dagger}_{xy}$

R.16.1 Handling the $\cong$ relation. There are multiple ways to define it: One here

Definition 45 (Comb : $\cong_{xy}$)**.** *We define $\Sigma_{xy} \cong_{xy} \Sigma'_{xy}$ by reusing its parts:*

$\Sigma_{xy} \cong_{xy} \Sigma'_{xy} \stackrel{\text{def}}{=} \Sigma_{xy}\upharpoonright^{x}_{xy} \cong_{x} \Sigma'_{xy}\upharpoonright^{x}_{xy} \wedge \Sigma_{xy}\upharpoonright^{y}_{xy} \cong_{y} \Sigma'_{xy}\upharpoonright^{y}_{xy}.$

or because the relation $\cong$ is independent of the state (relates everything in the state by equality and σ with $\sigma \sim_{\mathbf{pc}} \sigma'$). Thus, we can reuse $\cong$ for the definition and relate to sources via the following 3 lemmas:

Lemma 134 (Comb: Coincide on $\cong$ for projections)**.** *If*

(1) $\Sigma_{xy} \cong X_{xy}$

Then

(1) $\Sigma_{xy}\upharpoonright^{x}_{xy} \cong X_{xy}\upharpoonright^{x}_{xy}$ *and*
(2) $\Sigma_{xy}\upharpoonright^{y}_{xy} \cong X_{xy}\upharpoonright^{y}_{xy}$

Proof. The projection function does not change the values of the instances in the state. Thus, $\Sigma_{xy}\upharpoonright^{x}_{xy} \cong X_{xy}\upharpoonright^{x}_{xy}$ and $\Sigma_{xy}\upharpoonright^{y}_{xy} \cong X_{xy}\upharpoonright^{y}_{xy}$ trivially holds. □

Lemma 135 (Comb AM: Single step preserves $\cong$)**.** *If*

(1) $\Sigma_{xy} \cong \Sigma^{\dagger}_{xy}$ *and*
(2) $\Sigma_{xy} \xrightarrow{\tau}_{xy} \Sigma'_{xy}$ *and* $\Sigma^{\dagger}_{xy} \xrightarrow{\tau}_{xy} \Sigma^{\dagger\dagger}_{xy}$

Then

(1) $\Sigma'_{xy} \cong \Sigma^{\dagger\dagger}_{xy}$

Proof. The proof is analogous to Lemma 60 (S AM: Single step preserves $\cong$). □

Lemma 136 (Comb SE: Single step preserves $\cong$)**.** *If*

(1) $X_{xy} \cong X^{\dagger}_{xy}$ *and*
(2) $X_{xy} \overset{\tau}{\rightsquigarrow}{}^{O_{xy}}_{xy} X'_{xy}$ *and* $X^{\dagger}_{xy} \overset{\tau}{\rightsquigarrow}{}^{O_{xy}}_{xy} X^{\dagger\dagger}_{xy}$

Then

(1) $X'_{xy} \cong X^{\dagger\dagger}_{xy}$ *and*

Proof. The proof is analogous to Lemma 61 (S SE: Single step preserves $\cong$). □

Definition 46 (commit-free projection)**.** *The commit-free projection of our speculative state X is defined as follows:*

$$\begin{aligned}
\varepsilon\upharpoonright_{com} &= \varepsilon \\
\overline{\Psi}_x \cdot \Psi^{b}\upharpoonright_{com} &= \overline{\Psi}_x\upharpoonright_{com} \cdot \Psi^{b}_x \text{ with } b \neq \mathit{false} \\
\overline{\Psi}_x \cdot \Psi_x\upharpoonright_{com} &= \overline{\Psi}_x \cdot \Psi_x \text{ where } |\overline{\Psi}_x| = 0 \\
\overline{\Psi}_x \cdot \Psi^{b}_x \cdot \Psi^{\mathit{true}'}_x\upharpoonright_{com} &= \overline{\Psi}_x \cdot \Psi^{b''}_x\upharpoonright_{com} \text{ where } \Psi''_x = \Psi'_x[n \mapsto \Psi_x.n]
\end{aligned}$$

This executes the committed speculative instance and changes the speculative state.

Lemma 137 (Recomposition x)**.** *If*

(1) $\Sigma_{xy} \approx_{xy} X_{xy}$ *by Base and*
(2) $\Sigma_x \approx_x X_x$ *and*
(3) $\Sigma_x = \Sigma_{xy}\upharpoonright^{x}_{xy}$ *and*

(4) $X_x = X_{xy}\restriction^{x}_{xy}$ *and*
(5) $\Phi_x \overset{\tau}{\rightsquigarrow}_x \overline{\Phi}'_x$ *and*
(6) $X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}} \overline{\Psi}'_x$
(7) $\overline{\Phi}'_x \approx_x \overline{\Psi}'_x$ *and*
(8) $\overline{\Phi}'_{xy} = \overline{\Phi}'_x\restriction^{x}_{xy}$ *and* $X'_x = X'_{xy}\restriction^{x}_{xy}$

Then

(1) $\Sigma'_{xy} \approx_{xy} X'_{xy}$

Proof. Since $\Phi_x \overset{\tau}{\rightsquigarrow}_x \overline{\Phi}'_x$ we know that only the topmost state Φ_x of Σ_x did change. Similar for Σ_{xy}.

Furthermore, we know for all remaining elements of the state not in $\Sigma_{xy}\restriction^{x}_{xy}$ that they remain unchanged and are equal to the parts of Σ'_{xy}.

First, we check if $minWndw(X_x) = 0$. If that is the case then their is at least one outstanding commit, otherwise the states would not be related by Base. We first, execute this possible chain of commits and reach X''_x with $X_x \overset{O_x}{\rightsquigarrow}{}^{x}_{\overline{\tau}} X''_x$ where $\forall \tau \in \overline{\tau}. \exists id, \tau =$ `commit` id and $minWndw(X''_x) > 0$.

Furthermore, we have $\Sigma_x \approx_x X''_x$ because only committed states were removed and these were already ignored in $\Sigma_x \sim X_x\restriction_{com}$.

Next, we know that X''_x step will involve the SE-Context rule since no commit or rollback can executed. Let $X''_x = \overline{\Psi}''_x \cdot \Psi''_x$. Thus, depending on the executed instruction we have $decr(\overline{\Psi}_x)$ or $zeroes(\overline{\Psi}_x)$.

First, we know that and

Let us gather all the facts:

$$\Sigma_{xy} = \overline{\Phi}_{xy} \cdot \Phi_{xy}$$
$$X''_{xy} = \overline{\Psi}_{xy} \cdot \Psi_{xy}$$
$$\Sigma'_{xy} = \overline{\Phi}_{xy} \cdot \overline{\Phi}'_{xy}$$
$$X'_{xy} = f(\overline{\Psi}_{xy}) \cdot \overline{\Psi}'_{xy} \text{ where } f \text{ is either } decr() \text{ or } zeroes()$$
$$\overline{\Phi}_{xy} \cdot \Phi_{xy} \sim \overline{\Psi}_{xy} \cdot \Psi_{xy} \text{and} INV(\overline{\Phi}_{xy} \cdot \Phi_{xy}, \overline{\Psi}_{xy} \cdot \Psi_{xy})$$
$$\overline{\Phi}_{xy} \sim f(\overline{\Psi}_{xy}) \text{and} INV(\overline{\Phi}_{xy}, f(\overline{\Psi}_{xy}))$$

We proceed by case distinction on $\overline{\Phi}'_x \approx_x \overline{\Psi}'_x$:

Base Then we have $\overline{\Phi}'_x \sim \overline{\Psi}'_x\restriction_{com}$ and $INV(\overline{\Phi}'_x, \overline{\Psi}'_x)$.

Since the parts not in the projection $\restriction^{x}_{xy}$ do not change, we have $\overline{\Phi}'_{xy} \sim \overline{\Psi}'_{xy}\restriction_{com}$ and $INV(\overline{\Phi}'_{xy}, \overline{\Psi}'_{xy})$ from $\Phi_{xy} \sim \Psi_{xy}$

Since the remaining parts of the combined state did not change (except for the reduced n in $\overline{\Psi}_{xy}$), we have $\overline{\Phi}_{xy} \sim \overline{\Psi}_{xy}$ and $INV(\overline{\Phi}_{xy}, \overline{\Psi}_{xy})$ as well.

Together we have $\overline{\Phi}_{xy} \cdot \overline{\Phi}'_{xy} \sim \overline{\Psi}_{xy} \cdot \overline{\Psi}'_{xy}$ and $INV(\overline{\Phi}_{xy} \cdot \overline{\Phi}'_{xy}, \overline{\Psi}_{xy} \cdot \overline{\Psi}'_{xy})$

Because of $f(\overline{\Psi}_{xy})$ we may now have $minWndw(X'_{xy}) = 0$.

No transaction that needs to be rolled back in X'_{xy} Then we relate by Rule Single Base for the reasons above.

Trasaction that needs to be rolled back in X'_{xy} Then we relate bu Rule Single Transaction Rollback, since we fulfil all premises for above.

OracleTrue Then an oracle predicted the correct non-speculative location and a new speculative instance was created that will be committed.

Furthermore, a new speculative instance was created in the AM semantics as well.

First, we know that $\overline{\Phi}_{xy} \sim \overline{\Psi}_{xy}$ and $INV(\overline{\Phi}_{xy}, \overline{\Psi}_{xy})$ Next, form $\Sigma'_x \approx_x X'_x$ we get. $\Phi_x.ctr = \Psi_x.ctr$, $\Phi'_x.ctr = \Psi'_x.ctr$ and elem_of_states Φ_x = elem_of_states Ψ_x, $INV(\Phi_x, \Psi_x)$. From this, we can follow that $\Phi_{xy}.ctr = \Psi_{xy}.ctr$, $\Phi'_{xy}.ctr = \Psi'_{xy}.ctr$ and elem_of_states Φ_{xy} = elem_of_states Ψ_{xy}, $INV(\Phi_{xy}, \Psi_{xy})$. Together, we get $\overline{\Phi}_{xy} \cdot \Phi_{xy} \sim \overline{\Psi}_{xy} \cdot \Psi_{xy}$ and $INV(\overline{\Phi}_{xy} \cdot \Phi_{xy}, \overline{\Psi}_{xy} \cdot \Psi_{xy})$.

The remaining parts of Σ_{xy} and X_{xy} do not change. Except for the speculation window of X_{xy} because of SE-Context-xy. This means, we may now have $minWndw(X'_{xy}) = 0$.

Because of $f(\overline{\Psi}_{xy})$ we may now have $minWndw(X'_{xy}) = 0$.

No transaction that needs to be rolled back in X'_{xy} Thus, $\Sigma'_{xy} \approx_{xy} X'_{xy}$ by Oracle True for the reasons above

Transaction that needs to be rolled back in X'_{xy} Then we relate bu Rule Single Transaction Rollback, since we fulfil all premises from above.

Single-Transaction-Rollback Next, form $\Sigma'_x \approx_x X'_x$ we get. $\Phi_x.ctr = \Psi_x.ctr$, $\Phi'_x.ctr = \Psi'_x.ctr$ and elem_of_states Φ_x = elem_of_states Ψ_x, $INV(\Phi_x, \Psi_x)$. From this, we can follow that $\Phi_{xy}.ctr = \Psi_{xy}.ctr$, $\Phi'_{xy}.ctr = \Psi'_{xy}.ctr$ and elem_of_states Φ_{xy} = elem_of_states Ψ_{xy}, $INV(\Phi_{xy}, \Psi_{xy})$. Together, we get $\overline{\Phi}_{xy} \cdot \Phi_{xy} \sim \overline{\Psi}_{xy} \cdot \Psi_{xy}$ and $INV(\overline{\Phi}_{xy} \cdot \Phi_{xy}, \overline{\Psi}_{xy} \cdot \Psi_{xy})$.

Thus, we fulfill all conditions for Single Transaction rollback.

□

Lemma 138 (Recomposition y)**.** *If*

(1) $\Sigma_{xy} \approx_{xy} X_{xy}$ *by Base and*
(2) $\Sigma_x \approx_y X_x$ *and*
(3) $\Sigma_y = \Sigma_{xy}\restriction^{y}_{xy}$ *and*
(4) $X_y = X_{xy}\restriction^{y}_{xy}$ *and*
(5) $\Phi_y \overset{\tau}{\leadsto}_y \overline{\Phi}'_y$ *and*
(6) $X_y \overset{O_y}{\rightsquigarrow}{}^{y}_{\overline{\tau}} \overline{\Psi}'_y$
(7) $\overline{\Phi}'_y \approx_y \overline{\Psi}'_y$ *and*
(8) $\overline{\Phi}'_{xy} = \overline{\Phi}'_y\restriction^{y}_{xy}$ *and* $X'_y = X'_{xy}\restriction^{y}_{xy}$

Then

(1) $\Sigma'_{xy} \approx_{xy} X'_{xy}$

Proof. The proof is analogous to Lemma 137 (Recomposition x). □

These assumptions for x and y are what one already needs to prove in the Completeness direction of Oracle Overapproximation.

Assumption 5 (Comb: AM and Oracle coincide for x)**.** *If*

(1) $\Sigma_x \approx^{\Sigma^{States}}_{O_{am}} X_x$ *by Base and*
(2) $\Sigma_x \overset{\tau}{\Longrightarrow}_x \Sigma'_x$ *and*
(3) $minWndw(\Sigma_x) > 0$

Then

(1) $X_x \overset{\tau}{\rightsquigarrow}^{O_x}_x X'_x$

Assumption 6 (Comb: AM and Oracle coincide for y)**.** *If*

(1) $\Sigma_y \approx^{\Sigma^{States}}_{O_{am}} X_y$ *by Base and*
(2) $\Sigma_y \overset{\tau}{\Longrightarrow}_y \Sigma'_y$ *and*
(3) $minWndw(\Sigma_y) > 0$

Then

(1) $X_y \overset{\tau}{\rightsquigarrow}^{O_y}_y X'_y$

Lemma 139 (Comb: AM and Oracle coincide)**.** *If*

(1) $\Sigma_{xy} \approx^{\Sigma^{States}}_{O_{am}} X_{xy}$ *by Base and*
(2) $\Sigma_{xy} \overset{\tau}{\Longrightarrow}_{xy} \Sigma'_{xy}$ *and*
(3) $minWndw(\Sigma_{xy}) > 0$
(4) $X_{xy}.\overline{\rho} = \emptyset$

Then

(1) $X_{xy} \overset{\tau}{\rightsquigarrow}^{O_{xy}}_{xy} X'_{xy}$

Proof. Since $minWndw(\Sigma_{xy}) > 0$ we know that the next step is not a rollback. From $minWndw(\Sigma_{xy}) > 0$ and $\Sigma_{xy} \approx^{\Sigma^{States}}_{O_{am}} X_{xy}$ we have *INV2*(Σ_{xy}, X_{xy}) and we get $minWndw(X_{xy}) > 0$ as well.

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

Rule AM-x-step Then we have $\Phi_x \upharpoonright^x_{xy} \overset{\tau}{\Longrightarrow}_x \overline{\Phi}'_x$. Thus, we can apply Assumption 5 (Comb: AM and Oracle coincide for x) and get $X_x \overset{\tau}{\rightsquigarrow}^{O_x} X'_x$ with $X_{xy} \upharpoonright^x_{xy} = X_x$.

Since $minWndw(X_{xy} > 0)$ we know that no rollback or commit can be executed and by $X_{xy}.\overline{\rho} = \emptyset$ we know that a general step cannot be made.

Thus, the step $X_{xy} \overset{\tau}{\rightsquigarrow}^{O_{xy}}_{xy} X'_{xy}$ has to be derived by Rule SE-Context-xy and we need to find a step $\Psi_{xy} \overset{\tau}{\rightsquigarrow}^{O_{xy}}_{xy} \overline{\Psi}'_{xy}$ with $X_{xy} = \overline{\Psi}_{xy} \cdot \Psi_{xy}$.

Similarly, the step $X_x \overset{\tau}{\rightsquigarrow}^{O_x}_x X'_x$ has to be made by the context rule as well. Thus, we know $\Psi_x \overset{\tau}{\Longrightarrow}_x \overline{\Psi}'_x$ with $\Psi_{xy} \upharpoonright^x_{xy} = \Psi_x$.

Since $\Sigma_{xy}.\sigma = X_{xy}.\sigma$ and an x-step was done in Σ_{xy}, we know that an x-step is possible in X_{xy} as well (modulo Confluence).

Now, we can use Rule SE-x-step with $\Psi_x \overset{\tau}{\Longrightarrow}_x \overline{\Psi}'_x$ to derive $\Psi_{xy} \overset{\tau}{\Longrightarrow}_{xy} \overline{\Psi}'_{xy}$ which we can use together with Rule SE-Context-xy to derive $X_{xy} \overset{\tau}{\Longrightarrow}_{xy} X'_{xy}$.

Rule AM-y-step Then we have $\Phi_y \upharpoonright^{y}_{xy} \overset{\tau}{\Rrightarrow}_y \overline{\Phi}'_y$. Thus, we can apply Assumption 6 (Comb: AM and Oracle coincide for y) and get $X_y \overset{\tau}{\rightsquigarrow}^{O_y}_y X'_y$ as required.

□

R.16.2 Some infos on cong. Old relations defined per combination

Here is the old definition of ≅

Definition 47 (AM: Similar speculative instances)**.** *Two speculative instances $\langle p, ctr, \sigma, n, \Delta\rangle^b$ and $\langle p', ctr', \sigma', n', \Delta'\rangle^{b'}$ are similar, written $\langle p, ctr, \sigma, n, \Delta\rangle^b \cong \langle p', ctr', \sigma', n', \Delta'\rangle^{b'}$ iff $p = p'$, $ctr = ctr'$, $n = n'$, $b = b'$, $\Delta = \Delta'$, $\sigma \sim_{\mathbf{pc}} \sigma'$ and $\sigma \sim_{next} \sigma'$.*

Definition 48 (Oracle: Similar speculative instances)**.** *Two speculative instances $\langle p, ctr, \sigma, h, n, \Delta\rangle^b$ and $\langle p', ctr', \sigma', h', n', \Delta'\rangle^{b'}$ are similar, written $\langle p, ctr, \sigma, h, n, \Delta\rangle^b \cong \langle p', ctr', \sigma', h,' n', \Delta'\rangle^{b'}$ iff $p = p'$, $ctr = ctr'$, $h = h'$, $n = n'$, $b = b'$, $\Delta = \Delta'$, $\sigma \sim_{\mathbf{pc}} \sigma'$ and $\sigma \sim_{next} \sigma'$.*

This should hold for combination and should be easily derivable form

Lemma 140. *If*

(1) $\Sigma_x \overset{\tau}{\Rrightarrow}_x \Sigma'_x$ and
(2) $\Sigma_x \cong \Sigma^{\dagger}_x$

Then

(1) $\Sigma^{\dagger}_x \overset{\tau}{\Rrightarrow}_x \Sigma^{\dagger\dagger}_x$ and
(2) $\Sigma^{\dagger\dagger}_x \cong \Sigma'_x$

and similar for oracle.

However ≅ the next part does not hold for the topmost state! only the pc similar part does. And this is good, otherwise the completeness proof for SNI would not work since next would force that the non-speculative step is actually equal, even though it should be unequal

Next-Sim was only because of rollbacks. They did an extra step in the original semantics

S SEMANTICS FOR $\Rrightarrow_{\mathsf{S+R}}$

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

Let us first define a speculative state and a speculative instance. Speculative instances are the union of their parts. So here $\Phi_{\mathsf{S+R}} \in \Phi_{\mathsf{S}} \cup \Phi_{\mathsf{R}}$.

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

Definition 49 (Projection to R)**.** *We define a projection function $\upharpoonright^{\mathsf{R}} : \Phi_{\mathsf{S+R}} \to \Phi_{\mathsf{R}}$ as:*

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

We lift the function to speculative states $\Sigma_{\mathsf{S+R}}$ in the following way:

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

Definition 50 (Projection to S)**.** *We define a projection function $\upharpoonright^{\mathsf{S}} : \Phi_{\mathsf{S+R}} \to \Phi_{\mathsf{S}} \times \mathbb{R}$ as:*

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

We lift the function to speculative states $\Sigma_{\mathsf{S+R}}$ in the following way:

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

Judgements

$\Sigma_{\mathsf{S+R}} \overset{\tau}{\rightsquigarrow}_{S+R} \Sigma'_{\mathsf{S+R}}$	State $\Sigma_{\mathsf{S+R}}$ small-steps to $\Sigma'_{\mathsf{S+R}}$ and emits observation τ.
$\Phi_{\mathsf{S+R}} \overset{\tau}{\rightsquigarrow}_{S+R} \overline{\Phi}'_{\mathsf{S+R}}$	Speculative instance $\Phi_{\mathsf{S+R}}$ small-steps to $\overline{\Phi}_{\mathsf{S+R}}{}'$ and emits observation τ.
$\Sigma_{\mathsf{S+R}} \Downarrow^{\overline{\tau}}_{45} \Sigma'_{\mathsf{S+R}}$	State $\Sigma_{\mathsf{S+R}}$ big-steps to $\Sigma'_{\mathsf{S+R}}$ and emits a list of observations $\overline{\tau}$.
$p \times InitConf \;\Omega^{\omega}_{45}\; \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$\boxed{\Sigma_{\mathsf{S+R}} \overset{\tau}{\rightsquigarrow}_{S+R} \Sigma'_{\mathsf{S+R}}}$

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

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

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

$\boxed{\Phi_{\mathsf{S+R}} \overset{\tau}{\rightsquigarrow}_{S+R} \Phi'_{\mathsf{S+R}}}$

(AM-v4-step-V45)
$$\frac{\begin{array}{c} \Phi_{\mathsf{S+R}}\upharpoonright^{\mathsf{S}} = (\Phi_{\mathsf{S}}, \mathbb{R}) \quad \Phi_{\mathsf{S}} \overset{\tau}{\rightsquigarrow}_{\mathsf{S}} \overline{\Phi}'_{\mathsf{S}} \\ \overline{\Phi}'_{\mathsf{S+R}}\upharpoonright^{\mathsf{S}} = (\overline{\Phi}'_{\mathsf{S}}, \mathbb{R}) \end{array}}{\Phi_{\mathsf{S+R}} \overset{\tau}{\rightsquigarrow}_{S+R} \overline{\Phi}'_{\mathsf{S+R}}}$$

(AM-v5-step-V45)
$$\frac{\Phi_{\mathsf{S+R}}\upharpoonright^{\mathsf{R}} \overset{\tau}{\rightsquigarrow}_{\mathsf{R}} \overline{\Phi}'_{\mathsf{R}} \quad \overline{\Phi}'_{\mathsf{S+R}}\upharpoonright^{\mathsf{R}} = \overline{\Phi}'_{\mathsf{R}}}{\Phi_{\mathsf{S+R}} \overset{\tau}{\rightsquigarrow}_{S+R} \overline{\Phi}'_{\mathsf{S+R}}}$$

$$\boxed{\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{45} \Sigma'_{S+R}}$$

$$\text{(AM-Reflection-V45)}\ \frac{}{\Sigma_{S+R} \Downarrow^{\varepsilon}_{45} \Sigma_{S+R}} \qquad \text{(AM-Single-V45)}\ \frac{\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{45} \Sigma''_{S+R} \quad \Sigma''_{S+R} \overset{\tau}{\rightsquigarrow}_{S+R} \Sigma'_{S+R}}{\Sigma_{S+R} \Downarrow^{\overline{\tau}\cdot\tau}_{45} \Sigma'_{S+R}}$$

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

$$\boxed{\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{45} \Sigma'_{S+R}}$$

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

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

$$\boxed{p \times \mathit{InitConf} \,\Omega^{\omega}_{45}\, \overline{\tau}}$$

$$\text{(AM-Trace-V45)}\ \frac{\exists \Sigma'_{S+R} \quad \vdash \Sigma'_{S+R} : \mathit{fin} \quad \Sigma^{\mathit{init}}_{S+R}(p, \sigma) \Downarrow^{\overline{\tau}}_{45} \Sigma'_{S+R}}{(p, \sigma)\,\Omega^{\omega}_{45}\, \overline{\tau}} \qquad \text{(AM-Beh-V45)}\ \frac{}{\mathit{Beh}^{S+R}_{\omega}(p) = \{\overline{\tau} \mid \forall \sigma \in \mathit{InitConf}.\ (p, \sigma)\,\Omega^{\omega}_{45}\, \overline{\tau}\}}$$

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

S.1 Combined oracle semantics V4 V5

Note that we now need our labels l and b again. This could make this a little bit harder For example the projection to 4 needs to extract the l again and reattach it later but only to the old state if there is one.

$$\text{Spec. States } X_{45} ::= \overline{\Psi}_{45}$$

$$\text{Spec. Instance } \Psi_{45} ::= \langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, n\rangle^{b+l}_{\rho} \text{with } b = \{\mathit{true}, \mathit{false}, \varepsilon\} \text{ and } l \in \mathbb{N} \cup \{\varepsilon\}$$

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

Definition 51 (Projection to R). *We define a projection function* $\upharpoonright^{R} : \Psi_{45} \to \Psi_R$ *as:*

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

We lift the function to speculative states X_{45} *in the following way:*

$$\varepsilon \upharpoonright^{R} = \varepsilon$$

$$\overline{\Psi}_{45} \cdot \langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, n\rangle \upharpoonright^{R} = \overline{\Psi}_{45} \upharpoonright^{R} \cdot \langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, n\rangle$$

Definition 52 (Projection to S). *We define a projection function* $\upharpoonright^{S} : \Psi_{45} \to \Psi_S \times \mathbb{R}$ *as:*

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

We lift the function to speculative states X_{45} in the following way:

$$\varepsilon \upharpoonright^{S} = \varepsilon$$
$$\overline{\Psi}_{45} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \upharpoonright^{S} = \overline{\Psi}_{45} \upharpoonright^{S} \cdot (\langle p, ctr, \sigma, h, n\rangle, \mathbb{R})$$

Judgements

$X_{45} \overset{O_{S+R}}{\underset{45}{\overset{\tau}{\rightsquigarrow}}} X'_{45}$	State X_{45} small-steps to X'_{45} and emits observation τ.
$\Psi_{45} \overset{O_{S+R}}{\underset{45}{\overset{\tau}{\rightsquigarrow}}} \overline{\Psi}'_{45}$	Speculative instance Ψ_{45} small-steps to $\overline{\Psi}_{45}{}'$ and emits observation τ.
$X_{45} \; {}^{O_{S+R}}\Downarrow^{45}_{\overline{\tau}} X'_{45}$	State X_{45} big-steps to X'_{45} and emits a list of observations $\overline{\tau}$.
$p \times InitConf \; \Downarrow^{O}_{45} \overline{\tau}$	Program p and initial configuration σ produce the observations $\overline{\tau}$ during execution.

$\boxed{X_{45} \overset{O_{S+R}}{\underset{45}{\overset{\tau}{\rightsquigarrow}}} X'_{45}}$

(S + R-SE-Context)
$$\frac{\Psi_{45} \overset{O_{S+R}}{\underset{45}{\overset{\tau}{\rightsquigarrow}}} \overline{\Psi}'_{45} \qquad \Psi_{45} = \langle p, ctr, \sigma, \mathbb{R}, h, n+1\rangle \\ \text{if } p(\sigma(\mathbf{pc})) = \mathbf{spbarr} \text{ then } \overline{\Psi}_{45}{}'' = zeroes(\overline{\Psi}_{45}) \text{ else } \overline{\Psi}_{45}{}'' = decr(\overline{\Psi}_{45})}{\overline{\Psi}_{45} \cdot \Psi_{45} \overset{O_{S+R}}{\underset{45}{\overset{\tau}{\rightsquigarrow}}} \overline{\Psi}_{45}{}'' \cdot \overline{\Psi}'_{45}}$$

(S + R-SE:v4-General)
$$\frac{\overline{\Psi}_{45} \cdot \Psi_{45\,\overline{\rho}\cdot\tau} \upharpoonright^{S} \overset{O_S}{\underset{S}{\overset{\tau}{\rightsquigarrow}}} \overline{\Psi}_{45} \cdot \Psi_{45\,\overline{\rho}} \upharpoonright^{S}}{\overline{\Psi}_{45} \cdot \Psi_{45\,\overline{\rho}\cdot\tau} \overset{O_{S+R}}{\underset{45}{\overset{\tau}{\rightsquigarrow}}} \overline{\Psi}_{45} \cdot \Psi_{45\,\overline{\rho}}}$$

(S + R-SE:v5-General)
$$\frac{\overline{\Psi}_{45} \cdot \Psi_{45\,\overline{\rho}\cdot\tau} \upharpoonright^{R} \overset{O_R}{\underset{R}{\overset{\tau}{\rightsquigarrow}}} \overline{\Psi}_{45} \cdot \Psi_{45\,\overline{\rho}} \upharpoonright^{R}}{\overline{\Psi}_{45} \cdot \Psi_{45\,\overline{\rho}\cdot\tau} \overset{O_{S+R}}{\underset{45}{\overset{\tau}{\rightsquigarrow}}} \overline{\Psi}_{45} \cdot \Psi_{45\,\overline{\rho}}}$$

(S + R-SE:v4-Rollback)
$$\frac{n' = 0 \text{ or } p \text{ is stuck} \qquad \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n'\rangle^{true} \upharpoonright^{S} \overset{O_S}{\underset{S}{\overset{\tau}{\rightsquigarrow}}} \langle p, ctr', \sigma, \mathbb{R}, h, n\rangle \upharpoonright^{S}}{\overline{\Psi}_{45} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n'\rangle^{(S,true)} \cdot \overline{\Psi}'_{45} \overset{O_{S+R}}{\underset{45}{\overset{\tau}{\rightsquigarrow}}} \overline{\Psi}_{45} \cdot \langle p, ctr', \sigma, \mathbb{R}, h, n\rangle}$$

(S + R-SE:v5-Rollback)
$$\frac{n' = 0 \text{ or } p \text{ is stuck} \qquad \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n'\rangle^{m} \upharpoonright^{R} \overset{O_R}{\underset{R}{\overset{\tau}{\rightsquigarrow}}} \langle p, ctr', \sigma, \mathbb{R}, h, n\rangle \upharpoonright^{R}}{\overline{\Psi}_{45} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n'\rangle^{(R,m)} \cdot \overline{\Psi}'_{45} \overset{O_{S+R}}{\underset{45}{\overset{\tau}{\rightsquigarrow}}} \overline{\Psi}_{45} \cdot \langle p, ctr', \sigma, \mathbb{R}, h, n\rangle}$$

(S + R-SE:v4-Commit)
$$\frac{\langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0\rangle^{false} \upharpoonright^{S} \overset{O_S}{\underset{S}{\overset{\tau}{\rightsquigarrow}}} \langle p, ctr', \sigma', \mathbb{R}', h', n\rangle \upharpoonright^{S}}{\overline{\Psi}_{45} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0\rangle^{(S,false)} \cdot \overline{\Psi}_{45}{}' \overset{O_{S+R}}{\underset{45}{\overset{\tau}{\rightsquigarrow}}} \overline{\Psi}_{45} \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n\rangle \cdot \overline{\Psi}_{45}{}'}$$

(S + R-SE:v5-Commit)
$$\frac{\langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0\rangle^{m} \upharpoonright^{R} \overset{O_R}{\underset{R}{\overset{\tau}{\rightsquigarrow}}} \langle p, ctr', \sigma', \mathbb{R}', h', n\rangle \upharpoonright^{R}}{\overline{\Psi}_{45} \cdot \langle p, ctr, \sigma, \mathbb{R}, h, n\rangle \cdot \langle p, ctr', \sigma', \mathbb{R}', h', 0\rangle^{(R,m)} \cdot \overline{\Psi}_{45}{}' \overset{O_{S+R}}{\underset{45}{\overset{\tau}{\rightsquigarrow}}} \overline{\Psi}_{45} \cdot \langle p, ctr', \sigma', \mathbb{R}', h', n\rangle \cdot \overline{\Psi}_{45}{}'}$$

$\boxed{\Psi_{45} \overset{O_{S+R}}{\underset{45}{\overset{\tau}{\rightsquigarrow}}} \Psi'_{45}}$

(S + R-SE:v4-step)
$$\frac{O_{S+R} = (O, O_R) \qquad \Psi_{45} \upharpoonright^{S} \overset{O_S}{\underset{S}{\overset{\tau}{\rightsquigarrow}}} \overline{\Psi}'_{45} \upharpoonright^{S}}{\Psi_{45} \overset{O_{S+R}}{\underset{45}{\overset{\tau}{\rightsquigarrow}}} \overline{\Psi}'_{45}}$$

(S + R-SE:v5-step)
$$\frac{O_{S+R} = (O_S, O) \qquad \Psi_{45} \upharpoonright^{R} \overset{O_R}{\underset{R}{\overset{\tau}{\rightsquigarrow}}} \overline{\Psi}'_{45} \upharpoonright^{S}}{\Psi_{45} \overset{O_{S+R}}{\underset{45}{\overset{\tau}{\rightsquigarrow}}} \overline{\Psi}'_{45}}$$

$\boxed{X_{45} \; {}^{O_{S+R}}\Downarrow^{45}_{\overline{\tau}} X'_{45}}$

$$\frac{}{X_{45} \;{}^{O_{S+R}}\!\wr^{45}_{\varepsilon} X_{45}} \;(\text{SE-Reflection-V45}) \qquad \frac{X_{45} \;{}^{O_{S+R}}\!\wr^{45}_{\overline{\tau}} X''_{45} \qquad X''_{45} \overset{\tau}{\rightsquigarrow}{}^{O_{S+R}}_{45} X'_{45}}{X_{45} \;{}^{O_{S+R}}\!\wr^{45}_{\overline{\tau}\cdot\tau} X'_{45}} \;(\text{SE-Single-V45})$$

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

$\boxed{\mathit{Helpers}}$

$$\frac{X_{45} = \langle p, 0, \sigma, \varepsilon, \varepsilon, \bot\rangle \qquad \sigma \in \mathit{InitConf}}{\vdash X_{45} : \mathit{init}} \;(\text{SE-Init-V45}) \qquad \frac{X_{45} = \langle p, \mathit{ctr}, \sigma, \mathbb{R}, h, \bot\rangle \qquad \sigma(\mathbf{pc}) = \bot}{\vdash X_{45} : \mathit{fin}} \;(\text{SE-Fin-V45})$$

$$\frac{}{X^{\mathit{init}}_{45}(p, \sigma) \coloneqq \langle p, 0, \sigma, \varepsilon, \varepsilon, \bot\rangle} \;(\text{S} + \text{R:SE-Initial-State})$$

$\boxed{p \times \mathit{InitConf} \;\Omega^{O}_{45}\; \overline{\tau}}$

$$\frac{\exists X'_{45} \qquad \vdash X'_{45} : \mathit{fin} \qquad X^{\mathit{init}}_{45}(p, \sigma) \;{}^{O_{S+R}}\!\wr^{45}_{\overline{\tau}} X'_{45}}{(p, \sigma) \;\Omega^{O}_{45}\; \overline{\tau}} \;(\text{SE-Trace-V45}) \qquad \frac{}{\mathit{Beh}^{S+R}_{\omega}(p) = \{\overline{\tau} \mid \forall \sigma \in \mathit{InitConf}.\ (p, \sigma) \;\Omega^{O}_{45}\; \overline{\tau}\}} \;(\text{SE-Beh-V45})$$

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

T S + R : PROJECTION PRESERVATION AND CONFLUENCE IN DETAIL

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.

$$t_{v45} \coloneqq \cdots \texttt{start}_{S}\ i \ldots \texttt{start}_{R}\ i+1 \texttt{start}_{R}\ i+2 \cdots \texttt{rlb}_{R}\ i+1 \cdot \texttt{rlb}_{S}\ i \cdots \texttt{start}_{S}\ i+3$$

$$t_{v4} \coloneqq \ldots \texttt{start}_{S}\ i \cdots \texttt{rlb}_{S}\ i \cdots \texttt{start}_{S}\ i+1$$

$$t_{v45}\!\upharpoonright^{S} \coloneqq \cdots \texttt{start}_{S}\ i \cdot \texttt{rlb}_{S}\ i \cdots \texttt{start}_{S}\ i+3$$

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 141 (V45: Relating speculative projections to non-speculative projection). *Let $(p, \sigma) \Downarrow_{45}^{\omega} \overline{\tau}$. Then $\overline{\tau}\upharpoonright^{S}\upharpoonright^{R} = \overline{\tau}\upharpoonright_{ns}$.*

We now describe a very important fact about our semantics, Namely that it is confluent.

Lemma 142 (V45 AM: Confluence). *If*

(1) $\Sigma_{S+R} \overset{\tau}{\Longrightarrow}_{S+R} \Sigma'_{S+R}$ and
(2) $\Sigma_{S+R} \overset{\tau}{\Longrightarrow}_{S+R} \Sigma''_{S+R}$ 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 $\Sigma'_{S+R} = \Sigma''_{S+R}$.

□

T.1 Relating the semantics on their projections with combined.

Lemma 143 (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 $\Sigma_{S}^{init}()$, $\Sigma_{S+R}^{init}()$ and Rule V45-V4:Single-Base. □

Theorem 69 (V45: Relating V4 with projection of combined). *Let p be a program and ω be a speculation window. Then $Beh_{S}^{\omega}(p) = Beh_{\omega}^{S+R}(p)\upharpoonright^{S}$.*

Proof. The proposition can be proven in similar fashion to Theorem 13 (S AM: Behaviour of non-speculative semantics and AM semantics). We prove the two directions separately:

$\Leftarrow$ Assume that $(p,\sigma)\ \Omega^{\omega}_{45}\ \overline{\tau} \in Beh^{S+R}_{\omega}(p)$.

By the definition of $Beh^{S+R}_{\omega}(p)$ we have an initial configuration σ such that $(p,\sigma)\ \Omega^{\omega}_{45}\ \overline{\tau}$.

The proof proceeds in similar fashion to the analogous case in Theorem 13 (S AM: Behaviour of non-speculative semantics and AM semantics) by using Lemma 144 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

We can now conclude that $(p,\sigma)\ \Omega^{\omega}_{S}\overline{\tau}\upharpoonright^{S} \in Beh^{\omega}_{S}(p)$ by Rule S:AM-Trace.

$\Rightarrow$ Assume that $((p,\sigma))\ \Omega^{\omega}_{S}\overline{\tau} \in Beh^{\omega}_{S}(p)$. We thus know there exists $\vdash \Sigma'_{S} : fin$ such that $\Sigma^{init}_{S}(p,\sigma) \Downarrow^{\overline{\tau}}_{S} \Sigma'_{S}$.

Let $\Sigma_{S} = \Sigma^{init}_{S}(p,\sigma)$ and $\Sigma_{S+R} = \Sigma^{init}_{S+R}(p,\sigma)$. By Lemma 143 we have $\Sigma_{S} \approx \Sigma_{S+R}$.

We can now We apply Lemma 147 (V45 AM: Completeness w.r.t V4 and projection) and get $\Sigma_{S+R} \Downarrow^{\overline{\tau}'}_{45} \Sigma'_{S+R}$ with $\Sigma'_{S} \approx \Sigma'_{S+R}$ by Rule V45-V4:Single-Base and $\overline{\tau} = \overline{\tau}'\upharpoonright^{S}$.

Because of $\vdash \Sigma'_{S} : fin$ and $\Sigma'_{S} \approx \Sigma'_{S+R}$, we know that $\vdash \Sigma'_{S+R} : fin$.

We thus have $(p,\sigma)\ \Omega^{\omega}_{45}\ \overline{\tau}'\upharpoonright^{S} \in Beh^{S+R}_{\omega}(p)$.

$\square$

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 output of a $\texttt{start}_{R}$ *id* observation using the general rule. So starting a speculation actually takes two turns, until it is visible in the trace. This is exactly what this state in the relation is for.

$\boxed{\Sigma_{S} \approx \Sigma_{S+R}}$

$$\text{(V45-V4:Base)}\ \frac{}{\varnothing \approx \varnothing} \qquad \text{(V45-V4:Single-Base)}\ \frac{\Sigma'_{S} \sim \Sigma'_{S+R}}{\Sigma'_{S} \cdot \langle p, ctr, \sigma, n\rangle \approx \Sigma'_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}$$

$$\text{(V45-V4:Single-Speculation-Start)}\ \frac{\begin{array}{ll}\Sigma_{S} \sim \Sigma_{S+R} & \Sigma''_{S+R} \Downarrow^{\overline{\tau}}_{45} \Sigma'''_{S+R} \text{where transaction with id } ctr \text{ is rolled back}\\ \Sigma_{S} = \Sigma'_{S} \cdot \langle p, ctr', \sigma, n\rangle & \Sigma_{S+R} = \Sigma'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle\end{array}}{\Sigma'_{S} \cdot \langle p, ctr', \sigma, n\rangle \approx \Sigma'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^{v5}_{\texttt{ret}\ l\cdot\texttt{start}\ ctr}}$$

$$\text{(V45-V4:Single-Speculation-Diff)}\ \frac{\begin{array}{ll}\Sigma_{S} \sim \Sigma_{S+R} & \Sigma''_{S+R} \Downarrow^{\overline{\tau}}_{45} \Sigma'''_{S+R} \text{where transaction with id } ctr \text{ is rolled back}\\ \Sigma_{S} = \Sigma'_{S} \cdot \langle p, ctr', \sigma, n\rangle & \Sigma_{S+R} = \Sigma'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle\end{array}}{\Sigma'_{S} \cdot \langle p, ctr', \sigma, n\rangle \approx \Sigma'_{S+R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^{v5} \cdot \Sigma_{S+R1}}$$

$\boxed{\Sigma_{S} \sim \Sigma_{S+R}}$

$$\text{(V45-V4:Base)}\ \frac{}{\varnothing \sim \varnothing} \qquad \text{(V45-V4:Single)}\ \frac{|\Sigma'_{S}| = |\Sigma'_{S+R}| \quad \Sigma'_{S} \sim \Sigma'_{S+R}}{\Sigma'_{S} \cdot \langle p, ctr, \sigma, n\rangle \sim \Sigma'_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}$$

Lemma 144 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics). *If*

(1) $\Sigma_{S} \approx \Sigma_{S+R}$ *and*

(2) $\Sigma_{S+R} \Downarrow_{45}^{\overline{\tau}} \Sigma'_{S+R}$

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* $\Sigma_S \Downarrow_S^{\overline{\tau}\restriction^S} \Sigma'_S$ *and*

III *if* $\Sigma'_S \approx \Sigma'_{S+R}$ *by Rule V45-V4:Single-Speculation-Start then* $\Sigma_S \Downarrow_S^{\overline{\tau}\restriction^S} \Sigma'_S$ *and*

IV *if* $\Sigma'_S \approx \Sigma'_{S+R}$ *by Rule V45-V4:Single-Speculation-Diff* $\Sigma_S \Downarrow_S^{helpers_S(\overline{\tau},i)} \Sigma'_S$, *where* $i = ctr'$ *by unpacking* Σ'_{S+R} *according to Rule V45-V4:Single-Speculation-Diff*

Proof. By Induction on $\Sigma_{S+R} \Downarrow_{45}^{\overline{\tau}} \Sigma'_{S+R}$.

Rule AM-Reflection-V45 Then we have $\Sigma_{S+R} \Downarrow_S^{\varepsilon} \Sigma_{S+R}$ with $\Sigma'_{S+R} = \Sigma_{S+R}$ and by Rule AM-Reflection-V45 we have

I $\Sigma_S \Downarrow_S^{\varepsilon\restriction^S} \Sigma'_S$ with $\Sigma_S = \Sigma'_S$.

II $\Sigma_S \Downarrow_S^{helpers_S(\varepsilon,i)} \Sigma'_S$ with $\Sigma_S = \Sigma'_S$.

III $\Sigma'_S \approx \Sigma'_{S+R}$

Rule AM-Single-V45 We have $\Sigma_{S+R} \Downarrow_{45}^{\overline{\tau}''} \Sigma''_{S+R}$ with $\Sigma''_{S+R} \xrightarrow{\tau}_{S+R} \Sigma'_{S+R}$.

We now apply IH on $\Sigma''_{S+R} \Downarrow_{45}^{\overline{\tau}''} \Sigma''_{S+R}$ and get

(a) $\Sigma''_S \approx \Sigma''_{S+R}$

(b) if $\Sigma''_S \approx \Sigma''_{S+R}$ by Rule V45-V4:Single-Base then $\Sigma_S \Downarrow_S^{\overline{\tau}\restriction^S} \Sigma''_S$ and

(c) if $\Sigma''_S \approx \Sigma''_{S+R}$ by Rule V45-V4:Single-Speculation-Start then $\Sigma_S \Downarrow_S^{\overline{\tau}\restriction^S} \Sigma''_S$ and

(d) if $\Sigma''_S \approx \Sigma''_{S+R}$ by Rule V45-V4:Single-Speculation-Diff then $\Sigma_S \Downarrow_S^{helpers_S(\overline{\tau},i)} \Sigma''_S$, 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

$$\Sigma_S \Downarrow_S^{\overline{\tau}\restriction^S} \Sigma''_S$$
$$\Sigma''_S = \Sigma'''_S \cdot \langle p, ctr, \sigma, n \rangle_{\overline{\rho}}$$
$$\Sigma''_{S+R} = \Sigma'''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n \rangle_{\overline{\rho}}$$
$$\Sigma'''_S \sim \Sigma'''_{S+R}$$

We proceed by inversion on the derivation $\Sigma''_{S+R} \xrightarrow{\tau}_{S+R} \Sigma'_{S+R}$.

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 $\Sigma''_S \xrightarrow{\mathtt{rlb}_S\ ctr}_S \Sigma'_S$ 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 $\overline{\tau} \cdot \tau \upharpoonright^{S} = \overline{\tau}\upharpoonright^{S} \cdot \tau$ by definition of $\upharpoonright^{S}$ and thus have $\Sigma_S \Downarrow_S^{\overline{\tau}\cdot\tau\upharpoonright^S} \Sigma'_S$.

Rule AM-Context-V45 We have $\Phi_{S+R} \xrightarrow{\tau}_{S+R} \overline{\Phi}'_{S+R}$ and $n > 0$.

We now use inversion on $\Phi_{S+R} \xrightarrow{\tau}_{S+R} \overline{\Phi}_{S+R}$:

Rule AM-v4-step-V45 Then we have $\Phi_{S+R}\upharpoonright^{S} = (\Phi_S, \mathbb{R})$ and $\Phi_S \xrightarrow{\tau}_S \overline{\Phi}'_S$.

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 $\rightsquigarrow_S$: $\Sigma''_S \xrightarrow{\tau'}_S \Sigma'_S$.

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 $\overline{\tau} \cdot \tau'\upharpoonright^{S} = \overline{\tau}\upharpoonright^{S} \cdot \tau$.

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 $\texttt{start}_R$ *id* or $\texttt{rlb}_R$ *id* observation, we have $\overline{\tau}\cdot\tau\upharpoonright^{S} = \overline{\tau}\upharpoonright^{S}\cdot\tau$ by definition of $\upharpoonright^{S}$.

This means we have $\Sigma_S \Downarrow_S^{\overline{\tau}\cdot\tau\upharpoonright^S} \Sigma'_S$ as needed to show.

Rule AM-v5-step-V45 Then we have $\Phi_{S+R}\upharpoonright^{R} \xrightarrow{\tau}_R \overline{\Phi}'_R$.

By inversion on $\Phi_{S+R}\upharpoonright^{R} \xrightarrow{\tau}_R \overline{\Phi}'_R$ we get:

Rule R:AM-Ret-Spec We use Lemma 145 (V45: V4 step) and get $\Sigma''_S \xrightarrow{\tau\upharpoonright^S}_S \Sigma'_S$ 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 $\overline{\tau} \cdot \tau\upharpoonright^{S} = \overline{\tau}\upharpoonright^{S} \cdot \tau$.

We know that $\tau\upharpoonright^{S} = \tau$ and since τ is not a $\texttt{start}$ *id* or $\texttt{rlb}$ *id* observation, we have $\overline{\tau} \cdot \tau\upharpoonright^{S} = \overline{\tau}\upharpoonright^{S} \cdot \tau$.

This means we have $\Sigma_S \Downarrow_S^{\overline{\tau}\cdot\tau\upharpoonright^S} \Sigma'_S$ as needed to show.

otherwise We use Lemma 145 (V45: V4 step) and get $\Sigma''_S \xrightarrow{\tau\upharpoonright^S}_S \Sigma'_S$, $\tau\upharpoonright^{S} = \tau$ 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 $\overline{\tau} \cdot \tau\upharpoonright^{S} = \overline{\tau}\upharpoonright^{S} \cdot \tau$.

We know that $\tau\upharpoonright^{S} = \tau$ and have $\overline{\tau} \cdot \tau\upharpoonright^{S} = \overline{\tau}\upharpoonright^{S} \cdot \tau$ by definition of $\upharpoonright^{S}$.

This means we have $\Sigma_S \Downarrow_S^{\overline{\tau}\cdot\tau\upharpoonright^S} \Sigma'_S$ as needed to show.

Rule V45-V4:Single-Speculation-Start We have:

$$\begin{aligned}
\Sigma_S &\Downarrow_S^{\overline{\tau}\upharpoonright^S} \Sigma''_S \\
\Sigma''_S &= \Sigma'''_S \cdot \langle p, ctr, \sigma, n\rangle \\
\Sigma''_{S+R} &= \Sigma'''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle_{\texttt{ret}\ l\cdot\texttt{start}_R\ ctr'} \\
\Sigma'''_S \cdot \langle p, ctr, \sigma, n\rangle &\sim \Sigma'''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle
\end{aligned}$$

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 $\Phi_{S+R} \stackrel{\tau}{=\!\!\!\rightsquigarrow}_{S+R} \overline{\Phi}'_{S+R}$.

We now use inversion on $\Phi_{S+R} \stackrel{\tau}{=\!\!\!\rightsquigarrow}_{S+R} \overline{\Phi}_{S+R}$:

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 $\Phi_{S+R}\upharpoonright^{R} \stackrel{\tau}{=\!\!\!\rightsquigarrow}_{R} \overline{\Phi}'_{R}$.

By inversion on $\Phi_{S+R}\upharpoonright^{R} \stackrel{\tau}{=\!\!\!\rightsquigarrow}_{R} \overline{\Phi}'_{R}$ 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 $\Sigma''_S \Downarrow^{\varepsilon}_S \Sigma'_S$ 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:

$$\begin{aligned} &\overline{\tau}\upharpoonright^{S} && \text{Definition } helpers_S() \\ =\ & helpers_S(\overline{\tau}\cdot \texttt{start}_R\ ctr', ctr') && \tau = \texttt{start}_R\ ctr' \\ =\ & helpers_S(\overline{\tau}\cdot\tau, i) \end{aligned}$$

and we have $\overline{\tau}\upharpoonright^{S}$ by IH.

Since $\Sigma'_S = \Sigma''_S$ and IH $\Sigma_S \Downarrow_S^{\overline{\tau}\upharpoonright^{S}} \Sigma''_S$, 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 $helpers_S(\overline{\tau}\cdot \texttt{rlb}_R\ id, j) = helpers_S(\overline{\tau}, j)$.

By IH we have $\Sigma_S \Downarrow_S^{helpers_S(\overline{\tau},j)} \Sigma''_S$.

Combined with $\Sigma''_S = \Sigma'_S$ we get $\Sigma_S \Downarrow_S^{helpers_S(\overline{\tau},j)} \Sigma'_S$ 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 $\overline{\tau} \cdot \texttt{rlb}_{R}\ j \upharpoonright^{S} = helpers_{S}(\overline{\tau}, j)$ by definition of $\upharpoonright^{S}$ and $id = j$.
Since by IH we know $\Sigma_{S} \Downarrow^{helpers_{S}(\overline{\tau},j)}_{S} \Sigma''_{S}$ 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 underlying semantics just uses the no Branching rule, which is always there.

Lemma 145 (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) $\Phi_{S+R} \upharpoonright^{R} \xrightarrow{\tau}_{R} \overline{\Phi}'_{R}$ *and*

Then

(1) $\Sigma_{S} \xrightarrow{\tau\upharpoonright^{S}}_{S} \Sigma'_{S}$ *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 $\approx$:

$$\Sigma_{S} = \Sigma''_{S} \cdot \langle p, ctr, \sigma, n\rangle$$
$$\Sigma_{S+R} = \Sigma''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle$$
$$\Sigma''_{S} \sim \Sigma''_{S+R}$$

We proceed by inversion on $\Phi_{S+R} \upharpoonright^{R} \xrightarrow{\tau}_{R} \overline{\Phi}'_{R}$:

Rule R:AM-Ret-Spec Then we use Rule S:AM-NoBranch to derive a step $\Sigma_S \xrightarrow{\tau}_S \Sigma'_S$.

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 $\Sigma'_{S+R} = \overline{\Phi}_{S+R} \cdot \langle p, ctr, \sigma', \mathbb{R}', n\rangle \cdot \langle p, ctr+1, \sigma'', \mathbb{R}', n'\rangle_{\texttt{ret}\ l \cdot \texttt{start}_R\ ctr}$.

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, $\tau\upharpoonright^S = \tau$ by definition of $\upharpoonright^S$.

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 142 (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 $\Sigma_S \xrightarrow{\tau}_S \Sigma'_S$ 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 $\tau\upharpoonright^S = \tau$ by definition of $\upharpoonright^S$.

Rule R:AM-General Contradiction. This means that $\Sigma_{S+R}.\overline{p}$ 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 $\Sigma_S.\overline{p}$ contains one of these observations as well.

This is impossible, because they cannot be generated according to $\rightsquigarrow_S$, 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 $\Sigma_S \xrightarrow{\tau}_S \Sigma'_S$.

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 $\tau\upharpoonright^S = \tau$ by definition of $\upharpoonright^S$.

□

Lemma 146 (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) $\Phi_{S+R}\upharpoonright^S \xrightarrow{\tau}_S \overline{\Phi}'_S$ *and*

Then

(1) $\Sigma_R \xrightarrow{\tau\upharpoonright^R}_R \Sigma'_R$ *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 $\approx$:

$$\Sigma_{R} = \Sigma''_{R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n \rangle$$
$$\Sigma_{S+R} = \Sigma''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n \rangle$$
$$\Sigma''_{R} \sim \Sigma''_{S+R}$$

We proceed by inversion on $\Phi_{S+R} \upharpoonright^{S} \overset{\tau}{\rightsquigarrow}_{S} \overline{\Phi}'_{R}$:

Rule S:AM-Store-Spec Then we use Rule R:AM-NoBranch to derive a step $\Sigma_{R} \overset{\tau}{\rightsquigarrow}_{R} \Sigma'_{R}$.
The case is analogous to the corresponding case of Rule R:AM-Ret-Spec in Lemma 145 (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 145 (V45: V4 step).

□

Completeness

Lemma 147 (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 $\Sigma_{S+R} \Downarrow^{\overline{\tau}'}_{45} \Sigma'_{S+R}$ *and*
III $\overline{\tau} = \overline{\tau}' \upharpoonright^{S}$

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 $\Sigma_{S+R} \Downarrow^{\overline{\tau}'}_{45} \Sigma'_{S+R}$ 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 $\varepsilon \upharpoonright^{S} = \varepsilon$ we are finished.

Rule AM-Single-V45 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 $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \upharpoonright^{S}$
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' $\overline{\tau} = \overline{\tau}' \upharpoonright^{S}$

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 $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \upharpoonright^{S}$.

We have $\tau \upharpoonright^{S} = \tau$ by definition of $\upharpoonright^{S}$ and the fact that $\tau' = \texttt{rlb}_{S}\ ctr$.

This means we have:

$$\begin{aligned}&\overline{\tau}' \cdot \tau \upharpoonright^{S} && \text{Definition } \upharpoonright^{S} \\ &= \overline{\tau}' \upharpoonright^{S} \cdot \tau' && \text{by IH} \\ &= \overline{\tau} \cdot \tau' && \tau = \tau' \\ &= \overline{\tau} \cdot \tau\end{aligned}$$

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 $\Sigma''_{S+R} \Downarrow_{45}^{\tau \cdot \texttt{start}\ id \cdot \overline{\tau}'' \cdot \texttt{rlb}\ id} \Sigma'_{S+R}$ 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 $\Sigma'_{\mathsf{S}} \approx \Sigma'_{\mathsf{S+R}}$ by Rule V45-V4:Single-Base by determinism of the non-speculative semantics.
Next, we need to show that $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau' \cdot \mathtt{start}_{\mathsf{R}}\ id \cdot \overline{\tau}'' \cdot \mathtt{rlb}_{\mathsf{R}}\ id\upharpoonright^{\mathsf{S}}$.
Notice that $\tau' \cdot \mathtt{start}_{\mathsf{R}}\ id \cdot \overline{\tau}'' \cdot \mathtt{rlb}_{\mathsf{R}}\ id\upharpoonright^{\mathsf{S}} = \tau'\upharpoonright^{\mathsf{S}} = \tau'$ by definition of $\upharpoonright^{\mathsf{S}}$ and the fact that $\Sigma''_{\mathsf{S+R}} \approx \Sigma''_{\mathsf{S}}$.
This means we have:

$$\begin{aligned}
&\overline{\tau}' \cdot \tau' \cdot \mathtt{start}_{\mathsf{R}}\ id \cdot \overline{\tau}'' \cdot \mathtt{rlb}_{\mathsf{R}}\ id\upharpoonright^{\mathsf{S}} \\
&= \overline{\tau}' \cdot \tau'\upharpoonright^{\mathsf{S}} \text{ Definition } \upharpoonright^{\mathsf{S}} \\
&= \overline{\tau}'\upharpoonright^{\mathsf{S}} \cdot \tau' \ \tau = \tau' \text{ and IH} \\
&= \overline{\tau} \cdot \tau
\end{aligned}$$

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 $\Sigma''_{\mathsf{S+R}} \overset{\tau'}{\rightsquigarrow}_{S+R} \Sigma'_{\mathsf{S+R}}$.
From the determinism of the non-speculative semantics and $\Sigma''_{\mathsf{S}} \approx \Sigma''_{\mathsf{S+R}}$ we can conclude that $\Sigma'_{\mathsf{S}} \approx \Sigma'_{\mathsf{S+R}}$ by Rule V45-V4:Single-Base.
Next, we need to show that $\overline{\tau} \cdot \tau = \overline{\tau}' \cdot \tau'\upharpoonright^{\mathsf{S}}$.
Since the observation τ' was generated by the non-speculative semantics and there is no ongoing transaction of V5 (because $\Sigma'_{\mathsf{S}} \approx \Sigma'_{\mathsf{S+R}}$) we have $\tau'\upharpoonright^{\mathsf{S}} = \tau$.
Furthermore, by determinism of $\rightarrow$ we have $\tau' = \tau$. This means we have:

$$\begin{aligned}
&\overline{\tau}' \cdot \tau\upharpoonright^{\mathsf{S}} \text{ Definition } \upharpoonright^{\mathsf{S}} \\
&= \overline{\tau}'\upharpoonright^{\mathsf{S}} \cdot \tau' \text{ by IH} \\
&= \overline{\tau} \cdot \tau' \ \tau = \tau' \\
&= \overline{\tau} \cdot \tau
\end{aligned}$$

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 142 (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 $\Sigma''_{S+R} \overset{\tau'}{\rightsquigarrow}_{S+R} \Sigma'_{S+R}$.

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 $\tau' \upharpoonright^{S} = \tau'$.

This means we have

$$
\begin{aligned}
&\overline{\tau}' \cdot \tau \upharpoonright^{S} && \text{Definition } \upharpoonright^{S}\\
&= \overline{\tau}' \upharpoonright^{S} \cdot \tau' && \text{by IH}\\
&= \overline{\tau} \cdot \tau' && \tau = \tau'\\
&= \overline{\tau} \cdot \tau
\end{aligned}
$$

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.

□

T.2 Combination V45 and projection to V5

THEOREM 70 (V45: RELATING V5 WITH PROJECTION OF COMBINED). *Let p be a program and ω be a speculation window. Then $Beh^{\omega}_{R}(p) = Beh^{S+R}_{\omega}(p) \upharpoonright^{R}$.*

PROOF. The proposition can be proven in similar fashion to Theorem 69 (V45: Relating V4 with projection of combined). We prove the two directions separately:

$\Leftarrow$ Assume that $(p, \sigma) \Downarrow^{\omega}_{45} \overline{\tau} \in Beh^{S+R}_{\omega}(p)$.

By the definition of $Beh^{S+R}_{\omega}(p)$ we have an initial state $\Sigma_{S+R} = \Sigma^{init}_{S+R}(p, \sigma)$ such that $(p, \sigma) \Downarrow^{\omega}_{45} \overline{\tau}$.

The proof proceeds in similar fashion to the analogous case in Theorem 69 (V45: Relating V4 with projection of combined) by using Lemma 148 (V45: Soundness of the AM speculative semantics w.r.t. AM v5 semantics).

We can now conclude that $((p, \sigma)) \Downarrow^{\omega}_{R} \overline{\tau} \upharpoonright^{R} \in Beh^{\omega}_{R}(p)$ by Rule R:AM-Trace.

$\Rightarrow$ Assume that $((p, \sigma)) \Downarrow^{\omega}_{R} \overline{\tau} \in Beh^{\omega}_{R}(p)$. 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 69 (V45: Relating V4 with projection of combined) by using Lemma 149 (V45 AM: Completeness w.r.t V5 and projection).

We thus have $(p, \sigma) \Downarrow^{\omega}_{45} \overline{\tau}' \in Beh^{S+R}_{\omega}(p)$ with $\overline{\tau}' \upharpoonright^{R} = \overline{\tau}$.

□

$$\boxed{\Sigma_{R} \approx \Sigma_{S+R}}$$

$$\text{(V45-V5:Base)}\ \frac{}{\varnothing \approx \varnothing} \qquad \text{(V45-V5:Single-Base)}\ \frac{|\Sigma'_{S}| = |X'_{S}| \qquad \Sigma'_{R} \sim \Sigma'_{S+R}}{\Sigma'_{R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle^{b} \approx \Sigma'_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle^{b}}$$

$$\text{(V45-V5:Single-Transaction-Start)}\ \frac{\begin{array}{c}\Sigma_{R} \sim \Sigma_{S+R} \qquad n' \geq 0 \qquad \Sigma''_{S} \Downarrow^{\overline{\tau}}_{S} \Sigma'''_{S} \text{where transaction with id } ctr \text{ is rolled back} \\ \Sigma_{R} = \Sigma'_{R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \qquad \Sigma_{S+R} = \Sigma'_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\end{array}}{\Sigma'_{R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \approx \Sigma'_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^{false}_{\texttt{bypass}\ n\cdot\texttt{start}_{S}\ ctr}}$$

$$\text{(V45-V5:Single-Transaction-Rollback)}\ \frac{\begin{array}{c}\Sigma_{R} \sim \Sigma_{S+R} \qquad n' \geq 0 \qquad \Sigma''_{S} \Downarrow^{\overline{\tau}}_{S} \Sigma'''_{S} \text{where transaction with id } ctr \text{ is rolled back} \\ \Sigma_{R} = \Sigma'_{R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \qquad \Sigma_{S+R} = \Sigma'_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle\end{array}}{\Sigma'_{R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \approx \Sigma'_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle^{false} \cdot \Sigma_{S+R1}}$$

$$\boxed{\Sigma_{R} \sim \Sigma_{S+R}}$$

$$\text{(V45-V5:Base)}\ \frac{}{\varnothing \sim \varnothing} \qquad \text{(V45-V5:Single)}\ \frac{|\Sigma'_{R}| = |\Sigma'_{S+R}| \qquad \Sigma'_{R} \sim \Sigma'_{S+R}}{\Sigma'_{R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \sim \Sigma'_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle}$$

Lemma 148 (V45: Soundness of the AM speculative semantics w.r.t. AM v5 semantics). *If*

(1) $\Sigma_{R} \approx \Sigma_{S+R}$ *and*
(2) $\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{45} \Sigma'_{S+R}$

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* $\Sigma_{R} \Downarrow^{\overline{\tau}\upharpoonright^{R}}_{R} \Sigma'_{R}$ *and*
III if $\Sigma'_{R} \approx \Sigma'_{S+R}$ *by Rule V45-V5:Single-Transaction-Start then* $\Sigma_{R} \Downarrow^{\overline{\tau}\upharpoonright^{R}}_{R} \Sigma'_{R}$ *and*
IV if $\Sigma'_{R} \approx \Sigma'_{S+R}$ *by Rule V45-V5:Single-Transaction-Rollback* $\Sigma_{R} \Downarrow^{helper_{R}(\overline{\tau},i)}_{R} \Sigma'_{R}$, *where* $i = ctr'$ *by unpacking* Σ'_{S+R} *according to Rule V45-V5:Single-Transaction-Rollback.*

Proof. By Induction on $\Sigma_{S+R} \Downarrow^{\overline{\tau}}_{45} \Sigma'_{S+R}$.

Rule AM-Reflection-V45 Then we have $\Sigma_{S+R} \Downarrow^{\varepsilon}_{45} \Sigma_{S+R}$ with $\Sigma'_{S+R} = \Sigma_{S+R}$ and by Rule AM-Reflection-V45 we have

I $\Sigma'_{R} \approx \Sigma'_{S+R}$
II $\Sigma_{R} \Downarrow^{\varepsilon\upharpoonright^{R}}_{R} \Sigma'_{R}$ with $\Sigma_{R} = \Sigma'_{R}$.
III $\Sigma_{R} \Downarrow^{helper_{R}(\varepsilon,i)}_{R} \Sigma'_{R}$ 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 $\Sigma_{S+R} \Downarrow^{\overline{\tau}''}_{45} \Sigma''_{S+R}$ with $\Sigma''_{S+R} \overset{\tau}{\rightsquigarrow}_{S+R} \Sigma'_{S+R}$.

We now apply IH on $\Sigma''_{S+R} \Downarrow^{\overline{\tau}''}_{45} \Sigma''_{S+R}$ and get

(a) $\Sigma''_{S} \approx \Sigma''_{S+R}$
(b) if $\Sigma''_{R} \approx \Sigma''_{S+R}$ by Rule V45-V5:Single-Base then $\Sigma_{R} \Downarrow^{\overline{\tau}\upharpoonright^{R}}_{S} \Sigma''_{R}$ and
(c) if $\Sigma''_{R} \approx \Sigma''_{S+R}$ by Rule V45-V5:Single-Transaction-Start then $\Sigma_{R} \Downarrow^{\overline{\tau}\upharpoonright^{R}}_{R} \Sigma''_{R}$ and

(d) if $\Sigma''_{\mathsf{R}} \approx \Sigma''_{\mathsf{S+R}}$ by Rule V45-V5:Single-Transaction-Rollback $\Sigma_{\mathsf{R}} \Downarrow_{\mathsf{S}}^{helper_R(\overline{\tau},j)} \Sigma''_{\mathsf{R}}$, where $j = ctr'$ by unpacking $\Sigma''_{\mathsf{S+R}}$ according to Rule V45-V5:Single-Transaction-Rollback

We do a case distinction on $\approx$ in $\Sigma''_{\mathsf{R}} \approx \Sigma''_{\mathsf{S+R}}$:

Rule V45-V5:Single-Base We have

$$\Sigma_{\mathsf{R}} \Downarrow_{\mathsf{S}}^{\overline{\tau}\restriction^{\mathsf{R}}} \Sigma''_{\mathsf{R}}$$

$$\Sigma''_{\mathsf{R}} = \Sigma'''_{\mathsf{R}} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle_{\overline{\rho}}$$

$$\Sigma''_{\mathsf{S+R}} = \Sigma'''_{\mathsf{S+R}} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle_{\overline{\rho}}$$

$$\Sigma'''_{\mathsf{R}} \sim \Sigma'''_{\mathsf{S+R}}$$

We now proceed by inversion on the derivation $\Sigma''_{\mathsf{S+R}} \overset{\tau}{=\!\!\!\Omega}_{S+R} \Sigma'_{\mathsf{S+R}}$:

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 $\Sigma''_{\mathsf{R}} \xrightarrow{\mathtt{rlb}_{\mathsf{R}}\ ctr}_{\mathsf{R}} \Sigma'_{\mathsf{R}}$ by Rule R:AM-Rollback, since n is equal between the two states. The rest of the case is analogous to Lemma 144 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

Rule AM-v4-Rollback-V45 Since $\Sigma''_{\mathsf{R}} \approx \Sigma''_{\mathsf{S+R}}$ by Rule V45-V5:Single-Base, there cannot be a roll back of V4.

Rule AM-Context-V45 We have $\Phi_{\mathsf{S+R}} \overset{\tau}{=\!\!\!\Omega}_{S+R} \overline{\Phi}'_{\mathsf{S+R}}$.

We now use inversion on $\Phi_{\mathsf{S+R}} \overset{\tau}{=\!\!\!\Omega}_{S+R} \overline{\Phi}_{\mathsf{S+R}}$:

Rule AM-v4-step-V45 Then we have $\Phi_{\mathsf{S+R}}\restriction^{\mathsf{S}} \overset{\tau}{=\!\!\!\Omega}_{\mathsf{S}} \overline{\Phi}'_{\mathsf{S}}$.

By inversion on $\Phi_{\mathsf{S+R}}\restriction^{\mathsf{S}} \overset{\tau}{=\!\!\!\Omega}_{\mathsf{S}} \overline{\Phi}'_{\mathsf{S}}$ 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 144 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) using Lemma 146 (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 144 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics) using Lemma 146 (V45: V5 step) and the fact that Rule S:AM-Store-Spec was not used.

Rule AM-v5-step-V45 Then we have $\Phi_{\mathsf{S+R}}\restriction^{\mathsf{R}} \overset{\tau}{=\!\!\!\Omega}_{\mathsf{R}} \overline{\Phi}'_{\mathsf{R}}$.

The case is analogous to the corresponding case Rule AM-v4-step-V45 in Lemma 144 (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 $\mathtt{start}_{\mathsf{R}}$ *id* or $\mathtt{rlb}_{\mathsf{R}}$ *id* observation.

Rule V45-V5:Single-Transaction-Start We have:

$$\Sigma_{R} \Downarrow_{R}^{\overline{\tau}\upharpoonright^{R}} \Sigma''_{R}$$
$$\Sigma''_{R} = \Sigma'''_{R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle$$
$$\Sigma''_{S+R} = \Sigma'''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr'', \sigma', \mathbb{R}', n'\rangle_{\mathtt{bypass}\ n\cdot\mathtt{start}_{S}\ ctr'}$$
$$\Sigma'''_{R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \sim \Sigma'''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle$$

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 $\Phi_{S+R}\upharpoonright^{S} \overset{\tau}{\rightsquigarrow}_{S} \overline{\Phi}'_{R}$.

By inversion on $\Phi_{S+R}\upharpoonright^{S} \overset{\tau}{\rightsquigarrow}_{S} \overline{\Phi}'_{S}$ we get:

Rule S:AM-General By definition we have $\tau = \mathtt{start}_{S}\ ctr'$. Since Rule S:AM-General does not modify the state, we have $\Sigma'_{S+R} = \Sigma''_{S+R\,\mathtt{bypass}\ n}$.

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:

$\overline{\tau}\upharpoonright^{R}$	Definition $helper_{R}()$
$= helper_{R}(\overline{\tau}\cdot \mathtt{start}_{S}\ ctr', ctr')$	$\tau = \mathtt{start}_{S}\ ctr'$
$= helper_{R}(\overline{\tau}\cdot\tau, ctr')$	

and we have $\overline{\tau}\upharpoonright^{R}$ by IH.

Since $\Sigma'_{R} = \Sigma''_{R}$ and IH $\Sigma_{R} \Downarrow_{R}^{\overline{\tau}\upharpoonright^{R}} \Sigma''_{R}$, 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 $\mathtt{start}_{S}\ id$ observations.

Rule V45-V5:Single-Transaction-Rollback We have:

$$\Sigma_{R} \Downarrow_{S}^{helper_{R}(\overline{\tau}, j)} \Sigma''_{R}$$
$$\Sigma''_{R} = \Sigma'''_{R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle$$
$$\Sigma''_{S+R} = \Sigma'''_{S+R} \cdot \langle p, ctr'', \sigma, \mathbb{R}, n\rangle \cdot \langle p, ctr''', \sigma'', \mathbb{R}'', n''\rangle \cdot \Sigma^{\dagger}_{S+R}$$
$$\Sigma'''_{R} \cdot \langle p, ctr, \sigma, \mathbb{R}, n\rangle \sim \Sigma'''_{S+R} \cdot \langle p, ctr', \sigma, \mathbb{R}, n\rangle$$
$$j = ctr'$$

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 $\Sigma''_{R} \Downarrow^{\varepsilon}_{R} \Sigma'_{R}$ by Rule R:AM-Reflection.

The case is analogous to the corresponding case in Lemma 144 (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 $\Sigma''_{R} \Downarrow^{\varepsilon}_{R} \Sigma'_{R}$ 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 144 (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 144 (V45: Soundness of the AM speculative semantics w.r.t. AM v4 semantics).

□

Lemma 149 (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 $\Sigma_{S+R} \Downarrow^{\overline{\tau}'}_{45} \Sigma'_{S+R}$ *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 $\Sigma_{S+R} \Downarrow^{\overline{\tau}'}_{45} \Sigma'_{S+R}$ 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 $\Sigma''_{R} \overset{\tau}{\rightsquigarrow}_{R} \Sigma'_{R}$.

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' $\Sigma_{S+R} \Downarrow^{\overline{\tau}'}_{45} \Sigma''_{S+R}$ and

II' $\Sigma''_{R} \approx \Sigma''_{S+R}$ by Rule V45-V5:Single-Base and

IV' $\overline{\tau} = \overline{\tau}' \upharpoonright^{R}$

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 $\Sigma''_{R} \overset{\tau}{\Longrightarrow}_{R} \Sigma'_{R}$:

Rule R:AM-Rollback The case is analogous to the corresponding case in Lemma 147 (V45 AM: Completeness w.r.t V4 and projection) using Rule AM-v5-Rollback-V45.

Rule R:AM-Context We then have $\langle p, ctr, \sigma, \mathbb{R}, n \rangle \overset{\tau}{\Longrightarrow}_{R} \overline{\Phi}'_{R}$ and $n > 0$.

By $\Sigma''_{R} \approx \Sigma''_{S+R}$ we know that Rule AM-Context-V45 applies for the step $\Sigma''_{S+R} \overset{\tau'}{\Longrightarrow}_{S+R} \Sigma'_{S+R}$ as well.

We now need to find a derivation for the step $\langle p, ctr', \sigma, \mathbb{R}, n \rangle \overset{\tau'}{\Longrightarrow}_{S+R} \overline{\Phi}'_{S+R}$ according to Rule AM-Context-V45.

We proceed by inversion on $\langle p, ctr, \sigma, \mathbb{R}, n \rangle \overset{\tau}{\Longrightarrow}_{R} \overline{\Phi}'_{R}$:

Rule R:AM-NoBranch Then $n > 0$ and $\langle p, ctr, \sigma, \mathbb{R}, n \rangle \overset{\tau}{\Longrightarrow}_{R} \overline{\Phi}'_{R}$ 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 147 (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 142 (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 $\Sigma''_{S+R} \overset{\tau'}{\Longrightarrow}_{S+R} \Sigma'_{S+R}$.

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 $\tau' \upharpoonright^{R} = \tau$.

This means we have

$$
\begin{aligned}
&\overline{\tau}' \cdot \tau \upharpoonright^{R} \text{ Definition } \upharpoonright^{R} \\
&= \overline{\tau}' \upharpoonright^{R} \cdot \tau' \text{ by IH} \\
&= \overline{\tau} \cdot \tau' \;\; \tau = \tau' \\
&= \overline{\tau} \cdot \tau
\end{aligned}
$$

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 4 (V45: Relating Combined to non-speculative)**.** *Let p be a program and ω be a speculation window. Then $Beh_{NS}(p) = Beh_{\omega}^{S+R}(p)\upharpoonright_{ns}$.*

Proof. By Lemma 141 (V45: Relating speculative projections to non-speculative projection), we have $Beh_{\omega}^{S+R}(p)\upharpoonright_{ns} = Beh_{\omega}^{S+R}(p)\upharpoonright^{S}\upharpoonright^{R}$.

By Theorem 69 (V45: Relating V4 with projection of combined), we have that $Beh_{\omega}^{S+R}(p)\upharpoonright^{S} = Beh_{S}^{\omega}(p)$.

By Theorem 17 (R SE: Behaviour of non-speculative and oracle semantics), we get $Beh_{R}^{\omega}(p)\upharpoonright^{R} = Beh_{R}^{\omega}(p)\upharpoonright_{ns}$.

By Theorem 12 (S SE: Behaviour of non-speculative and oracle semantics), we know that $Beh_{S}^{\omega}(p)\upharpoonright_{ns} = Beh_{NS}(p)$.

Combining these facts we get:

$$
\begin{aligned}
&Beh_{\omega}^{S+R}(p)\upharpoonright_{ns} \\
&= Beh_{\omega}^{S+R}(p)\upharpoonright^{S}\upharpoonright^{R} \\
&= Beh_{S}^{\omega}(p)\upharpoonright^{R} \\
&= Beh_{S}^{\omega}(p)\upharpoonright_{ns} \\
&= Beh_{NS}(p)
\end{aligned}
$$

and are finished. □

Corollary 5 (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 $((p,\sigma)) \Downarrow_{NS} \overline{\tau}'$, $((p,\sigma')) \Downarrow_{NS} \overline{\tau}'$.

We need to show that

(1) $((p,\sigma)) \Downarrow_{S}^{\omega} \overline{\tau}_s$, $((p,\sigma')) \Downarrow_{S}^{\omega} \overline{\tau}_s$

(2) $((p,\sigma)) \Downarrow_{R}^{\omega} \overline{\tau}_r$, $((p,\sigma')) \Downarrow_{R}^{\omega} \overline{\tau}_r$

We show the proof for 1). The proof for 2) is analogous using Theorem 70 (V45: Relating V5 with projection of combined).

Unfolding the definition of SNI for the combination we get:

(1) if $\sigma \sim_P \sigma'$ and $((p, \sigma)) \mathrel{\text{👻}}_{NS} \overline{\tau}$, $((p, \sigma')) \mathrel{\text{👻}}_{NS} \overline{\tau}$, then $(p, \sigma) \mathrel{\text{👻}}^{\omega}_{45} \overline{\tau}_{sr}$, $(p, \sigma') \mathrel{\text{👻}}^{\omega}_{45} \overline{\tau}_{sr}$

After initialization we have $(p, \sigma) \mathrel{\text{👻}}^{\omega}_{45} \overline{\tau}_{sr}$, $(p, \sigma') \mathrel{\text{👻}}^{\omega}_{45} \overline{\tau}_{sr}$.

By Theorem 69 (V45: Relating V4 with projection of combined) we have $((p, \sigma)) \mathrel{\text{👻}}^{\omega}_{\mathsf{S}} (\overline{\tau}_{sr} \restriction^{\mathsf{S}}) \in Beh^{\omega}_{\mathsf{S}}(p)$ and $(p, \sigma') \mathrel{\text{👻}}^{\omega}_{\mathsf{S}} (\overline{\tau}_{sr} \restriction^{\mathsf{S}}) \in Beh^{\omega}_{\mathsf{S}}(p)$, which is what we needed to show.

□