Automated Verification for Real-Time Systems via Implicit Clocks and an Extended Antimirov Algorithm (Supplementary Material (Appendix))

Yahui Song and Wei-Ngan Chin

School of Computing, National University of Singapore, Singapore
{yahuis,chinwn}@comp.nus.edu.sg

A Operational Semantics Rules for the Basic Statements

Rules $[v]$, $[assign]$, and $[ev]$ are axioms, which terminate immediately. We use $\mathcal{S}[\alpha]$ to update the environment $\mathcal{S}$ with the assignment α.

$$(\mathcal{S}, v) \xrightarrow{\tau} (\mathcal{S}, v)\ [v] \quad (\mathcal{S}, \alpha) \xrightarrow{\tau} (\mathcal{S}[\alpha], ())\ [assign] \quad (\mathcal{S}, \texttt{event}[\mathtt{A}(v, \alpha^*)]) \xrightarrow{\mathtt{A}(v)} (\mathcal{S}[\alpha^*], ())\ [ev]$$

In conditionals, if v is True in the environment, the first branch is executed. Otherwise, the other branch is executed. The rule $[call]$ retrieves the function body e of mn from the program, and executes e with instantiated arguments.

$$\frac{\mathcal{S}(v) = True}{(\mathcal{S}, if\ \ v\ \ e_1\ \ e_2) \xrightarrow{\tau} (\mathcal{S}, e_1)}[cond_1] \quad \frac{\mathcal{S}(v) = False}{(\mathcal{S}, if\ \ v\ \ e_1\ \ e_2) \xrightarrow{\tau} (\mathcal{S}, e_2)}[cond_2] \quad \frac{mn x^*\ \{e\} \in \mathcal{P} \quad (\mathcal{S}, e[v^*/x^*]) \xrightarrow{l} (\mathcal{S}', e')}{(\mathcal{S}, mn(v^*)) \xrightarrow{l} (\mathcal{S}', e')}[call]$$

Rules $[seq_1]$ and $[seq_2]$ state that e_1 takes the control when it still can behave; then the control transfers to e_2 when e_1 terminates. In process $e_1 || e_2$, if any of e_1 or e_2 can proceed, they proceed on their own. Rule $[par_3]$ states that if both branches can proceed with the same label, they proceed together.

$$\frac{(\mathcal{S}, e_1) \xrightarrow{l} (\mathcal{S}', e_1')}{(\mathcal{S}, e_1; e_2) \xrightarrow{l} (\mathcal{S}', e_1'; e_2)}[seq_1] \quad \frac{}{(\mathcal{S}, v; e_2) \xrightarrow{\tau} (\mathcal{S}, e_2)}[seq_2] \quad \frac{(\mathcal{S}, e_1) \xrightarrow{l} (\mathcal{S}', e_1')}{(\mathcal{S}, e_1 || e_2) \xrightarrow{l} (\mathcal{S}', e_1' || e_2)}[par_1]$$

$$\frac{(\mathcal{S}, e_1) \xrightarrow{l} (\mathcal{S}', v)}{(\mathcal{S}, e_1 || e_2) \xrightarrow{l} (\mathcal{S}', e_2)}[par_2] \qquad \frac{(\mathcal{S}, e_1) \xrightarrow{l} (\mathcal{S}, e_1') \qquad (\mathcal{S}, e_2) \xrightarrow{l} (\mathcal{S}, e_2')}{(\mathcal{S}, e_1 || e_2) \xrightarrow{l} (\mathcal{S}, e_1' || e_2')}[par_3]$$

B The Complete Forward Rules

Rule $[FV\text{-}Value]$ obtains the next state by inheriting the current state. Rule $[FV\text{-}Event]$ concatenates the event to the current state and update the environment for the subsequent statements.

$$\frac{}{\mathcal{S} \vdash \{\pi, \theta\}\ v\ \{\pi, \theta\}}\ [FV\text{-}Value] \qquad \frac{\theta' {=} \theta \cdot \mathtt{A}(v) \qquad \mathcal{S}[\alpha^*] \vdash \{\pi, \theta'\}\ e\ \{\Pi, \Theta\}}{\mathcal{S} \vdash \{\pi, \theta\}\ \mathtt{event}[\mathtt{A}(v, \alpha^*)]; e\ \{\Pi, \Theta\}}\ [FV\text{-}Event]$$

Rule $[FV\text{-}Call]$ first checks whether the instantiated precondition of callee, $\Phi_{pre}[v^*/x^*]$, is satisfied by the current program state. When the check is succeeded, the final states are formed by concatenating the instantiated postcondition to the current states. $\mathcal{P}$ denotes the program being checked.

$$\frac{\begin{array}{c} mn\ x^*\ \{\mathbf{req}\ \Phi_{pre}\ \mathbf{ens}\ \Phi_{post}\}\ \{e\} \in \mathcal{P} \\ \mathcal{S} \vdash \{\pi, \theta\} \sqsubseteq \Phi_{pre}[v^*/x^*] \qquad \Phi_f = \{\pi, \theta\} \cdot \Phi_{post}[v^*/x^*] \end{array}}{\mathcal{S} \vdash \{\pi, \theta\}\ mn(v^*)\ \{\Phi_f\}}\ [FV\text{-}Call]$$

Rule $[FV\text{-}Cond\text{-}Local]$ computes an over-approximation of the program states, by adding different constraints into different branches. $\pi \wedge v$ enforces v into the pure constraints of every trace in the state, same for $\pi \wedge \neg v$. Rule $[FV\text{-}Cond\text{-}Global]$ is applied when v is a global variable, the constraints are inserted as $\tau(\pi)$ events into the traces, which are determined when other threads are parallel composed.

$$\frac{\begin{array}{c}[FV\text{-}Cond\text{-}Local] \\ \mathcal{S} \vdash \{\pi \wedge v, \theta\}\ e_1\ \{\Pi_1, \Theta_1\} \qquad \mathcal{S} \vdash \{\pi \wedge \neg v, \theta\}\ e_2\ \{\Pi_2, \Theta_2\} \qquad (v\ is\ local)\end{array}}{\mathcal{S} \vdash \{\pi, \epsilon\}\ \mathbf{if}\ v\ \mathbf{then}\ e_1\ \mathbf{else}\ e_2\ \{\Pi_1, \Theta_1\} \cup \{\Pi_2, \Theta_2\}}$$

$$\frac{\begin{array}{c}[FV\text{-}Cond\text{-}Global] \\ \mathcal{S} \vdash \{\pi, \epsilon\}\ e_1\ \{\Pi_1, \Theta_1\} \qquad \mathcal{S} \vdash \{\pi, \theta\}\ e_2\ \{\Pi_2, \Theta_2\} \qquad (v\ is\ global)\end{array}}{\mathcal{S} \vdash \{\pi, \theta\}\ \mathbf{if}\ v\ \mathbf{then}\ e_1\ \mathbf{else}\ e_2\ \{\Pi_1, \theta \cdot \tau(v{=}True) \cdot \Theta_1\} \cup \{\Pi_2, \theta \cdot \tau(v{=}False) \cdot \Theta_2\}}$$

$[FV\text{-}Meth]$ initializes the state using the declared precondition, accumulates the effects from the method body, and checks the inclusion between the final state $\{\Pi, \Theta\}$ and the concatenation of the pre- and postcondition[1]. $[FV\text{-}Guard]$ computes the effects of e and concatenates $(v{=}True)?$ before e's effects.

$$\frac{\begin{array}{c}[FV\text{-}Meth] \\ \vdash \{\Phi_{pre}\}\ e\ \{\Pi, \Theta\} \qquad \{\Pi, \Theta\} \sqsubseteq \Phi_{pre} \cdot \Phi_{post}\end{array}}{\mathcal{S} \vdash\ mn\ x^*\ \{\mathbf{req}\ \Phi_{pre}\ \mathbf{ens}\ \Phi_{post}\}\ \{e\}} \qquad \frac{\begin{array}{c}[FV\text{-}Guard] \\ \mathcal{S} \vdash \{\pi, \epsilon\}\ e\ \{\Pi, \Theta\}\end{array}}{\mathcal{S} \vdash \{\pi, \theta\}\ [v]e\ \{\Pi, \theta \cdot (v{=}True)?\Theta\}}$$

$[FV\text{-}Seq]$ computes $\{\Pi_1, \Theta_1\}$ from e_1, then further gets $\{\Pi_2, \Theta_2\}$ by continuously computing the behaviors of e_2, to be the final state. $[FV\text{-}Par]$ computes behaviors for e_1 and e_2 independently, then parallel merges the effects.

$$\frac{\mathcal{S} \vdash \{\pi, \theta\}\ e_1\ \{\Pi_1, \Theta_1\} \qquad \mathcal{S} \vdash \{\Pi_1, \Theta_1\}\ e_2\ \{\Pi_2, \Theta_2\}}{\mathcal{S} \vdash \{\pi, \theta\}\ e_1; e_2\ \{\Pi_2, \Theta_2\}}\ [FV\text{-}Seq]$$

$$\frac{\mathcal{S} \vdash \{\pi, \theta\}\ e_1\ \{\Pi_1, \Theta_1\} \qquad \mathcal{S} \vdash \{\pi, \theta\}\ e_2\ \{\Pi_2, \Theta_2\}}{\mathcal{S} \vdash \{\pi, \theta\}\ e_1 || e_2\ \{\Pi_1 \wedge \Pi_2, \Theta_1 || \Theta_2\}}\ [FV\text{-}Par]$$

[1] Note that for succinctness, the user-provided Φ_{post} only denotes the *extension* of the effects from executing the method body.

C Soundness of the Forward Rules

Given any system configuration $\zeta{=}(\mathcal{S}, e)$, by applying the operational semantics rules, if $(\mathcal{S}, e){\rightarrow}^*(\mathcal{S}', v)$ has execution time d and produces event sequence φ; and for any history effect $\pi{\wedge}\theta$, such that $d_1, \mathcal{S}, \varphi_1{\models}(\pi{\wedge}\theta)$, and the forward verifier reasons $\mathcal{S}{\vdash}\{\pi, \theta\}\, e\, \{\Pi, \Theta\}$, then $\exists(\pi'{\wedge}\theta') \in \{\Pi, \Theta\}$ such that $(d_1{+}d), \mathcal{S}', (\varphi_1{+\!+}\varphi)$ ${\models}(\pi'{\wedge}\theta')$.

Proof. By induction on the structure of e:

1. **Value:** $(\mathcal{S}, v)\xrightarrow{\tau}(\mathcal{S}, v)$ [v]
When $((\mathcal{S}, v){\rightarrow}(\mathcal{S}, v))$, it takes 0 time and produces am empty sequence []. By rule [FV-Value], $\mathcal{S} \vdash \{\pi, \theta\}\ v\ \{\pi, \theta\}$, then the post effect is the witness that $(d_1{+}0), \mathcal{S}, (\varphi_1{+\!+}[]) \models \pi{\wedge}\theta$ is valid.

2. **Event:** $(\mathcal{S}, \mathtt{event}[\mathtt{A}(v, \alpha^*)])\xrightarrow{\mathtt{A}(v)}(\mathcal{S}[\alpha^*], ())$ $[ev]$
When $(\mathcal{S}, \mathtt{event}[\mathtt{A}(v, \alpha^*)]){\rightarrow}^*(\mathcal{S}[\alpha^*], ())$, it takes 0 time and produces the event sequence $[\mathtt{A}(v, \alpha^*)]$. By rule [FV-Value], $\mathcal{S} \vdash \{\pi, \theta\}\ \mathtt{A}(v, \alpha^*)\ \{\pi, \theta \cdot \mathtt{A}(v, \alpha^*)\}$, then the post effect is the witness that $(d_1{+}0), \mathcal{S}[\alpha^*], (\varphi_1{+\!+}[\mathtt{A}(v, \alpha^*)]) \models \pi \wedge \theta \cdot \mathtt{A}(v, \alpha^*)$.

3. **Guard:**

$$\frac{\mathcal{S} \models (v{=}true)}{(\mathcal{S}, [v]e) \xrightarrow{\tau} (\mathcal{S}, e)}[gu_1] \qquad \frac{\mathcal{S} \not\models (v{=}true)}{(\mathcal{S}, [v]e) \xrightarrow{\tau} (\mathcal{S}, [v]e)}[gu_2]$$

When $(\mathcal{S}, [v]e){\rightarrow}^*(\mathcal{S}, v')$, it produces the sequence $\varphi(e)$. By $[FV\text{-}Guard]$, $\mathcal{S} \vdash \{\pi, \theta\}\ [v]e\ \{\Pi, \theta \cdot (v{=}True)?\Theta\}$ where $\mathcal{S} \vdash \{\pi, \epsilon\}e\{\Pi, \Theta\}$. Then the post effect is the witness that $(d_1{+}d_{wait}{+}d_e), \mathcal{S}, (\varphi_1{+\!+}[\varphi(e)]) \models \Pi \wedge \theta \cdot (v{=}True)?\Theta$ is valid.

4. **Delay:**

$$\frac{\mathrm{d}{\leq}v}{(\mathcal{S}, \mathtt{delay}[v]) \xrightarrow{\mathrm{d}} (\mathcal{S}, \mathtt{delay}[v\text{-}\mathrm{d}])}\ [delay_1] \qquad \frac{}{(\mathcal{S}, \mathtt{delay}[0]) \xrightarrow{\tau} (\mathcal{S}, ())}\ [delay_2]$$

When $(\mathcal{S}, \mathtt{delay}[v]){\rightarrow}^*(\mathcal{S}, ())$, by applying rules $[delay_1]$, $[delay_2]$, it produces am empty sequence [], and takes time $\mathcal{S}(v)$. By $[FV\text{-}Delay]$, $\mathcal{S} \vdash \{\pi, \theta\}\ \mathtt{delay}[v]$ $\{\pi{\wedge}(t{=}d), \theta \cdot \epsilon\#t\}$. Then the post effect $\pi{\wedge}(t{=}d) \wedge \theta \cdot \epsilon\#t$ is the witness that $(d_1{+}\mathcal{S}(v)), \mathcal{S}, (\varphi_1{+\!+}[]) \models \pi{\wedge}(t{=}v) \wedge \theta \cdot \epsilon\#t$ is valid.

5. **Timeout:**

$$\frac{(\mathcal{S}, e_1) \xrightarrow{\mathtt{A}} (\mathcal{S}', e_1')}{(\mathcal{S}, e_1\ \mathtt{timeout}[v]\ e_2)\xrightarrow{\mathtt{A}}(\mathcal{S}', e_1')}[to_1] \frac{(\mathcal{S}, e_1) \xrightarrow{\tau} (\mathcal{S}', e_1')}{(\mathcal{S}, e_1\ \mathtt{timeout}[v]\ e_2)\xrightarrow{\tau}(\mathcal{S}', e_1'\ \mathtt{timeout}[v]e_2)}[to_2]$$

$$\frac{(\mathcal{S}, e_1) \xrightarrow{\mathrm{d}} (\mathcal{S}, e_1') \qquad (\mathrm{d}{\leq}v)}{(\mathcal{S}, e_1\ \mathtt{timeout}[v]\ e_2)\xrightarrow{\mathrm{d}}(\mathcal{S}, e_1'\ \mathtt{timeout}[v\text{-}\mathrm{d}]e_2)}[to_3] \frac{}{(\mathcal{S}, e_1\ \mathtt{timeout}[0]e_2)\xrightarrow{\tau}(\mathcal{S}, e_2)}[to_4]$$

When $(\mathcal{S}, e_1\ \texttt{timeout}[v]\ e_2){\rightarrow}^*(\mathcal{S}', v')$, there are two possibilities:
- e_1 started before time bound $\mathcal{S}(v)$: by applying rules $[to_2]$, $[to_3]$ and $[to_1]$, it produces the concrete sequence $[\texttt{A};\ tl(\varphi(e_1))]$, and $\texttt{A}$ takes t_1 time-units, which is less than $\mathcal{S}(v)$. By $[FV\text{-}Timeout]$, $\mathcal{S} \vdash \{\pi, \theta\}\ e_1\ \texttt{timeout}[v]\ e_2\ \{\Pi_1{\wedge}t_1{<}v, \theta \cdot (hd(\Theta_1)\texttt{\#}t_1){\cdot}tl(\Theta_1)\}$ where $\mathcal{S} \vdash \{\pi, \epsilon\} e_1 \{\Pi_1, \Theta_1\}$. Then the post effect is the witness such that $(d_1{+}t_1), \mathcal{S}', (\varphi_1\texttt{++}[\texttt{A};\ tl(\varphi(e_1))]) \models \Pi_1{\wedge}(t_1{<}v) \wedge \theta \cdot (hd(\Theta_1)\texttt{\#}t_1) \cdot tl(\Theta_1)$.
- e_1 never started, by applying rules $[to_4]$, it takes time d and produces the concrete sequence $[\varphi(e_2)]$. By $[FV\text{-}Timeout]$, $\mathcal{S} \vdash \{\pi, \theta\}\ e_1\ \texttt{timeout}[v]\ e_2\ \{\Pi_2{\wedge}t_2{=}v, \theta{\cdot}(\epsilon\texttt{\#}t_2) \cdot \Theta_2\}$ where $\mathcal{S} \vdash \{\pi, \epsilon\} e_2 \{\Pi_2, \Theta_2\}$. Then the post effect is the witness such that $(d_1{+}d), \mathcal{S}', (\varphi_1\texttt{++}[\varphi(e_2)]) \models \Pi_2{\wedge}t_2{=}v \wedge \theta \cdot (\epsilon\texttt{\#}t_2) \cdot \Theta_2$ is valid.

6. **Deadline:**

$$\frac{(\mathcal{S}, e) \xrightarrow{\texttt{A}/\tau} (\mathcal{S}', e')}{(\mathcal{S}, \texttt{deadline}[v]\ e) \xrightarrow{\texttt{A}/\tau} (\mathcal{S}', \texttt{deadline}[v]\ e')}[ddl_1]$$

$$\frac{(\mathcal{S}, e) \xrightarrow{l} (\mathcal{S}', v)}{(\mathcal{S}, \texttt{deadline}[v]\ e) \xrightarrow{l} (\mathcal{S}', v)}[ddl_2] \qquad \frac{(\mathcal{S}, e) \xrightarrow{\mathrm{d}} (\mathcal{S}, e') \quad (\mathrm{d}{\leq}v)}{(\mathcal{S}, \texttt{deadline}[v]\ e) \xrightarrow{\mathrm{d}} (\mathcal{S}, \texttt{deadline}[v\text{-}\mathrm{d}]\ e')}[ddl_3]$$

When $(\mathcal{S}, \texttt{deadline}[v]\ e){\rightarrow}^*(\mathcal{S}', v')$, by applying rules $[ddl_1]$, $[ddl_2]$ and $[ddl_3]$, it produces the concrete sequence $[\varphi(e)]$, and it takes d time-units which is less than $\mathcal{S}(v)$. By $[FV\text{-}Deadline]$, $\mathcal{S} \vdash \{\pi, \theta\}\ \texttt{deadline}[v]\ e\ \{\Pi_1{\wedge}(t{\leq}v), \theta{\cdot}(\Theta_1\texttt{\#}t)\}$ where $\mathcal{S} \vdash \{\pi, \epsilon\} e \{\Pi_1, \Theta_1\}$. Then the post effect is the witness such that $(d_1{+}d), \mathcal{S}', (\varphi_1\texttt{++}[\varphi(e)]) \models \Pi_1{\wedge}(t{\leq}v) \wedge \theta \cdot (\Theta_1\texttt{\#}t)$ is valid.

7. **Interrupt:**

$$\frac{(\mathcal{S}, e_1) \xrightarrow{\texttt{A}/\tau} (\mathcal{S}', e_1')}{(\mathcal{S}, e_1\ \texttt{interrupt}[v]\ e_2) \xrightarrow{\texttt{A}/\tau} (\mathcal{S}', e_1'\ \texttt{interrupt}[v]\ e_2)}[int_1]$$

$$\frac{(\mathcal{S}, e_1) \xrightarrow{l} (\mathcal{S}', v)}{(\mathcal{S}, e_1\ \texttt{interrupt}[v]\ e_2) \xrightarrow{l} (\mathcal{S}', v)}[int_2] \qquad \frac{}{(\mathcal{S}, e_1\ \texttt{interrupt}[0]\ e_2) \xrightarrow{\tau} (\mathcal{S}, e_2)}[int_3]$$

When $(\mathcal{S}, e_1\ \texttt{interrupt}[v]\ e_2){\rightarrow}^*(\mathcal{S}', v')$, by applying rules $[int_1]$, $[int_2]$ and $[int_3]$, it produces many possible sequences, which depends of how many events e_1 can trigger before time bound v. For example, - when there is only one event triggered before the time bound, by Algorithm 1, $\Delta{=}\pi{\wedge}(t{<}v) \wedge \theta \cdot hd(\varphi(e_1))\texttt{\#}t$. By $[FV\text{-}Interrupt]$, $\mathcal{S} \vdash \{\pi, \theta\}\ e_1\ \texttt{interrupt}[v]\ e_2\ \{\Pi', \theta{\cdot}\Theta'\}$ where $\mathcal{S} \vdash \{\Delta\}\ e_2\ \{\Pi', \Theta'\}$. Then the post effect is the witness such that
$(d_1{+}t{+}d_{e2}), \mathcal{S}', (\varphi_1\texttt{++}[hd(\varphi(e_1))]\texttt{++}[\varphi(e_2)]) \models \pi{\wedge}(t < v) \wedge \theta \cdot hd(\varphi(e_1))\texttt{\#}t \cdot \Theta'$. is valid. Similar proofs for other possibilities.

8. **Conditional:**

$$\frac{\mathcal{S}(v) = \mathit{True}}{(\mathcal{S}, \mathit{if}\ \ v\ \ e_1\ \ e_2) \xrightarrow{\tau} (\mathcal{S}, e_1)}\ [\mathit{cond_1}] \quad \frac{\mathcal{S}(v) = \mathit{False}}{(\mathcal{S}, \mathit{if}\ \ v\ \ e_1\ \ e_2) \xrightarrow{\tau} (\mathcal{S}, e_2)}\ [\mathit{cond_2}]$$

When $(\mathcal{S}, \mathit{if}\ \ v\ e_1\ \ e_2) \rightarrow^* (\mathcal{S}', v')$, there are two possibilities:
- when $\mathcal{S}(v){=}\mathit{True}$, it takes d_{e1} time units and produces sequence $varphi(e_1)$. By $[FV\text{-}Cond\text{-}Local]$, $\mathcal{S} \vdash \{\pi, \theta\}$ **if** v **then** e_1 **else** e_2 $\{\Pi_1, \theta \cdot \tau(v{=}\mathit{True}) \cdot \Theta_1\}$ where $\mathcal{S} \vdash \{\pi, \epsilon\}\ \ e_1\ \ \{\Pi_1, \Theta_1\}$. Then the post effect is the witness such that $(d_1{+}d_{e1}), \mathcal{S}', (\varphi_1{+}{+}[\varphi(e_1)]) \models \Pi_1, \theta \cdot \tau(v{=}\mathit{True}) \cdot \Theta_1$ is valid.
- when $\mathcal{S}(v){=}\mathit{False}$ it takes d_{e2} time units and produces sequence $varphi(e_2)$. By $[FV\text{-}Cond\text{-}Local]$, $\mathcal{S} \vdash \{\pi, \theta\}$ **if** v **then** e_1 **else** e_2 $\{\Pi_2, \theta \cdot \tau(v{=}\mathit{True}) \cdot \Theta_2\}$ where $\mathcal{S} \vdash \{\pi, \epsilon\}\ \ e_2\ \ \{\Pi_2, \Theta_2\}$. Then the post effect is the witness such that $(d_1{+}d_{e2}), \mathcal{S}', (\varphi_1{+}{+}[\varphi(e_2)]) \models \Pi_2, \theta \cdot \tau(v{=}\mathit{False}) \cdot \Theta_2$ is valid.

9. **Method Call:**

$$\frac{mn x^*\ \ \{e\} {\in} \mathcal{P} \quad (\mathcal{S}, e[v^*/x^*]) \xrightarrow{l} (\mathcal{S}', e')}{(\mathcal{S}, mn(v^*)) \xrightarrow{l} (\mathcal{S}', e')}\ [\mathit{call}]$$

When $(\mathcal{S}, mn(v^*)) \rightarrow^* (\mathcal{S}', v')$, it takes d_e time units and produces sequence $varphi(e)$. By $[FV\text{-}Call]$, $\mathcal{S} \vdash \{\pi, \theta\}\ mn(v^*)\ \{\Phi_f\}$ where $\Phi_f{=}\{\pi, \theta\} \cdot \Phi_{post}[v^*/x^*]$. The post effect is the witness of $(d_1{+}d_e), \mathcal{S}', (\varphi_1{+}{+}[\varphi(e)]) \models \{\pi, \theta\} \cdot \Phi_{post}[v^*/x^*]$.

D Termination of the TRS

The TRS is terminating.

Proof. Let Set$[\mathcal{I}]$ be a data structure representing the sets of inclusions. We use S to denote the inclusions to be proved, and H to accumulate "inductive hypotheses", i.e., $S, H \in \mathit{Set}[\mathcal{I}]$. Consider the following partial ordering $\succ$ on pairs $\langle S, H\rangle$: $\langle S_1, H_1\rangle \succ \langle S_2, H_2\rangle$ iff $|H_1| < |H_2| \vee (|H_1| = |H_2| \wedge |S_1| > |S_2|)$.

Here $|X|$ stands for the cardinality of a set X. Let $\Rightarrow$ denote the rewrite relation, then $\Rightarrow^*$ denotes its reflexive transitive closure. For any given S_0, H_0, this ordering is well founded on the set of pairs $\{\langle S, H\rangle \mid \langle S_0, H_0\rangle \Rightarrow^* \langle S, H\rangle\}$, due to the fact that H is a subset of the finite set of pairs of all possible derivatives in initial inclusion. Inference rules in our TRS given in Sec.5 transform current pairs $\langle S, H\rangle$ to new pairs $\langle S', H'\rangle$. And each rule either increases $|H|$ (Unfolding) or, otherwise, reduces $|S|$ (Axiom, Disprove, Prove), therefore the system is terminating.

E Soundness of the TRS

For each inference rules, if inclusions in their premises are valid, and their side conditions are satisfied, then goal inclusions in their conclusions are valid.

Proof. By case analysis for each inference rules:

1. **Axiom Rules:**

$$\frac{}{\Gamma \vdash \pi \wedge \bot \sqsubseteq \Phi}\ [\texttt{Bot-LHS}] \qquad \frac{\Phi \neq \pi \wedge \bot}{\Gamma \vdash \Phi \not\sqsubseteq \pi \wedge \bot}\ [\texttt{Bot-RHS}]$$

- It is easy to verify that antecedent of goal entailments in the rule [Bot-LHS] is unsatisfiable. Therefore, these entailments are evidently valid.
- It is easy to verify that consequent of goal entailments in the rule [Bot-RHS] is unsatisfiable. Therefore, these entailments are evidently invalid.

2. **Disprove Rules:**

$$\frac{\delta_{\pi_1}(\theta_1) \wedge \neg\delta_{\pi_2}(\theta_2)}{\Gamma \vdash \pi_1 \wedge \theta_1 \not\sqsubseteq \pi_2 \wedge \theta_2}\ [\texttt{DISPROVE}] \qquad \frac{\pi_1 \Rightarrow \pi_2 \qquad fst_{\pi_1}(\theta_1) = \{\}}{\Gamma \vdash \pi_1 \wedge \theta_1 \sqsubseteq \pi_2 \wedge \theta_2}\ [\texttt{PROVE}]$$

- It's straightforward to prove soundness of the rule [DISPROVE], Given that $\theta 1$ is nullable, while θ_2 is not nullable, thus clearly the antecedent contains more event traces than the consequent. Therefore, these entailments are evidently invalid.

3. **Prove Rules:**

$$\frac{(\pi_1{\wedge}\theta_1 \sqsubseteq \pi_3{\wedge}\theta_3) \in \Gamma \qquad (\pi_3{\wedge}\theta_3 \sqsubseteq \pi_4{\wedge}\theta_4) \in \Gamma \qquad (\pi_4{\wedge}\theta_4 \sqsubseteq \pi_2{\wedge}\theta_2) \in \Gamma}{\Gamma \vdash \pi_1 \wedge \theta_1 \sqsubseteq \pi_2 \wedge \theta_2}\ [\texttt{REOCCUR}]$$

- To prove soundness of the rule [PROVE], we consider an arbitrary model, $d, \mathcal{S}, \varphi$ such that: $d, \mathcal{S}, \varphi \models \pi_1 \wedge \theta_1$. Given the side conditions from the promises, we get $d, \mathcal{S}, \varphi \models \pi_2 \wedge \theta_2$. When the *fst* set of θ_1 is empty, θ_1 is possible $\bot$ or ϵ and $\pi_2 \wedge \theta_2$ is nullable. For both cases, the inclusion is valid.
- To prove soundness of the rule [REOCCUR], we consider an arbitrary model, $d, \mathcal{S}, \varphi$ such that: $d, \mathcal{S}, \varphi \models \pi_1 \wedge \theta_1$. Given the promises that $\pi_1 \wedge \theta_1 \sqsubseteq \pi_3 \wedge \theta_3$, we get $d, \mathcal{S}, \varphi \models \pi_3 \wedge \theta_3$; Given the promise that there exists a hypothesis $\pi_3 \wedge \theta_3 \sqsubseteq \pi_4 \wedge \theta_4$, we get $d, \mathcal{S}, \varphi \models \pi_4 \wedge \theta_4$; Given the promises that $\pi_4 \wedge \theta_4 \sqsubseteq \pi_2 \wedge \theta_2$, we get $d, \mathcal{S}, \varphi \models \pi_2 \wedge \theta_2$. Therefore, the inclusion is valid.

4. **Unfolding Rule:**

$$\frac{H{=}fst_{\pi_1}(\theta_1) \qquad \Gamma'{=}\Gamma, (\pi_1{\wedge}\theta_1 \sqsubseteq \pi_2{\wedge}\theta_2) \qquad \forall h{\in}H.\ (\Gamma' \vdash D_h^{\pi_1}(\theta_1) \sqsubseteq D_h^{\pi_2}(\theta_2))}{\Gamma \vdash \pi_1 \wedge \theta_1 \sqsubseteq \pi_2 \wedge \theta_2}[\texttt{UNFOLD}]$$

- To prove soundness of [UNFOLD], we consider an arbitrary model, $d_1, \mathcal{S}_1, \varphi_1$ and $d_2, \mathcal{S}_2, \varphi_2$ such that: $d_1, \mathcal{S}_1, \varphi_1 \models \pi_1 \wedge \theta_1$ and $d_2, \mathcal{S}_2, \varphi_2 \models \pi_2 \wedge \theta_2$. For an arbitrary event h, let $d_1', \mathcal{S}_1', {\varphi_1}' \models \mathtt{h}^{-1}[\![\pi_1 \wedge \theta_1]\!]$; and $d_2', \mathcal{S}_2', {\varphi_2}' \models \mathtt{h}^{-1}[\![\pi_2 \wedge \theta_2]\!]$.

Case 1), $\mathtt{h} \notin F$, $d_1', \varphi_1{}' \models \bot$, thus automatically $d_1', \varphi_1{}' \models D_{\mathtt{h}}^{\pi_2}(\theta_2)$;

Case 2), $\mathtt{h} \in F$, given that inclusions in the rule's premise is valid, then $d_1', \mathcal{S}_1', \varphi_1{}' \models D_{\mathtt{h}}^{\pi_2}(\theta_2)$.

By Definition 3, since for all h, $D_{\mathtt{h}}^{\pi_1}(\theta_1) \sqsubseteq D_{\mathtt{h}}^{\pi_2}(\theta_2)$, the conclusion is valid.

All the inference rules used in the TRS are sound, therefore the TRS is sound.