UNIVERSITY NAME

DOCTORAL THESIS

Thesis Title

Author:
John SMITH

Supervisor:
Dr. James SMITH

A thesis submitted in fulfillment of the requirements
for the degree of Doctor of Philosophy

in the

Research Group Name
Department or School Name

April 28, 2021

"Thanks to my solid academic training, today I can write hundreds of words on virtually any topic without possessing a shred of information, which is how I got a good job in journalism."

Dave Barry

UNIVERSITY NAME

Abstract

Faculty Name
Department or School Name

Doctor of Philosophy

Thesis Title

by John SMITH

The Thesis Abstract is written here (and usually kept to just this page). The page is kept centered vertically so can expand into the blank space above the title too...

Acknowledgements

The acknowledgments and the people to thank go here, don't forget to include your project advisor...

Contents

List of Figures

List of Tables

For/Dedicated to/To my…

Chapter 1

Proving semantic preservation in HILECOP

- Change σ_{injr} and σ_{injf} into σ_i.
- Define the $\texttt{Inject}_{\downarrow}$ and $\texttt{Inject}_{\uparrow}$ relations.
- Keep the *sitpn* argument in the SITPN full execution relation, but remove it from the SITPN execution, cycle and state transition relations.
- Make a remark on the differentiation of boolean operators and intuitionistic logic operators
- Explain and illustrate the equivalence relation between SITPN and VHDL.

1.1 Preliminary Definitions

1.2 Behavior Preservation Theorem

1.3 Initial States

1.4 First Rising Edge

1.5 Rising Edge

1.6 Falling Edge

Definition 1 (Falling Edge Hypotheses). *Given an* $sitpn \in SITPN$, $d \in design$, $\gamma \in WM(sitpn, d)$, $E_c \in \mathbb{N} \to \mathcal{C} \to \mathbb{B}$, $\Delta \in ElDesign(d, \mathcal{D}_{\mathcal{H}})$, $E_p \in (\mathbb{N} \times \{\uparrow, \downarrow\}) \to Ins(\Delta) \to value$, $\tau \in \mathbb{N}$, $s, s' \in S(sitpn)$, $\sigma_e, \sigma, \sigma_i, \sigma_{\downarrow}, \sigma' \in \Sigma(\Delta)$, *assume that:*

- $\lfloor sitpn \rfloor_{\mathcal{H}} = (d, \gamma)$ *and* $\gamma \vdash E_p \overset{env}{=} E_c$ *and* $\mathcal{D}_{\mathcal{H}}, \emptyset \vdash \mathrm{d} \xrightarrow{elab} \Delta, \sigma_e$
- $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$
- $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$

- $\texttt{Inject}_{\downarrow}(\sigma, E_p, \tau, \sigma_i)$ *and* $\Delta, \sigma_i \vdash \text{d.cs} \xrightarrow{\downarrow} \sigma_{\downarrow}$ *and* $\Delta, \sigma_{\downarrow} \vdash \text{d.cs} \xrightarrow{\rightsquigarrow} \sigma'$
- *State* σ *is a stable design state:* $\mathcal{D}_{\mathcal{H}}, \Delta, \sigma \vdash \text{d.cs} \xrightarrow{comb} \sigma$

Lemma 1 (Falling Edge). *For all sitpn,* d, γ, Δ, σ_e, E_c, E_p, τ, s, s', σ, σ_i, $\sigma_{\downarrow}$, σ' *that verify the hypotheses of Def. 1, then* $\gamma \vdash s' \overset{\downarrow}{\sim} \sigma'$.

Proof. By definition of **??**, there are 12 points to prove.

1. $\forall p \in P, id_p \in Comps(\Delta)\ s.t.\ \gamma(p) = id_p,\ s'.M(p) = \sigma'(id_p)(\text{"s\_marking"})$.
2. $\forall t \in T_i, id_t \in Comps(\Delta)\ s.t.\ \gamma(t) = id_t,$
   $\big(upper(I_s(t)) = \infty \wedge s'.I(t) \leq lower(I_s(t)) \Rightarrow s'.I(t) = \sigma'(id_t)(\text{"s\_time\_counter"})\big)$
   $\wedge\big(upper(I_s(t)) = \infty \wedge s'.I(t) > lower(I_s(t)) \Rightarrow \sigma'(id_t)(\text{"s\_time\_counter"}) = lower(I_s(t))\big)$
   $\wedge\big(upper(I_s(t)) \neq \infty \wedge s'.I(t) > upper(I_s(t)) \Rightarrow \sigma'(id_t)(\text{"s\_time\_counter"}) = upper(I_s(t))\big)$
   $\wedge\big(upper(I_s(t)) \neq \infty \wedge s'.I(t) \leq upper(I_s(t)) \Rightarrow s'.I(t) = \sigma'(id_t)(\text{"s\_time\_counter"})\big)$.
3. $\forall t \in T_i, id_t \in Comps(\Delta)\ s.t.\ \gamma(t) = id_t, s'.reset_t(t) = \sigma'(id_t)(\text{"s\_reinit\_time\_counter"})$.
4. $\forall c \in \mathcal{C}, id_c \in Ins(\Delta)\ s.t.\ \gamma(c) = id_c,\ s'.cond(c) = \sigma'(id_c)$.
5. $\forall a \in \mathcal{A}, id_a \in Outs(\Delta)\ s.t.\ \gamma(a) = id_a,\ s'.ex(a) = \sigma'(id_a)$.
6. $\forall f \in \mathcal{F}, id_f \in Outs(\Delta)\ s.t.\ \gamma(f) = id_f,\ s'.ex(f) = \sigma'(id_f)$.
7. $\forall t \in T, id_t \in Comps(\Delta)\ s.t.\ \gamma(t) = id_t, t \in Firable(s') \Leftrightarrow \sigma'(id_t)(\text{"s\_firable"}) = \texttt{true}$.
8. $\forall t \in T, id_t \in Comps(\Delta)\ s.t.\ \gamma(t) = id_t, t \notin Firable(s') \Leftrightarrow \sigma'(id_t)(\text{"s\_firable"}) = \texttt{false}$.
9. $\forall t \in T, id_t \in Comps(\Delta)\ s.t.\ \gamma(t) = id_t, t \in Fired(s') \Leftrightarrow \sigma'(id_t)(\text{"fired"}) = \texttt{true}$.
10. $\forall t \in T, id_t \in Comps(\Delta)\ s.t.\ \gamma(t) = id_t, t \notin Fired(s') \Leftrightarrow \sigma'(id_t)(\text{"fired"}) = \texttt{false}$.
11. $\forall p \in P, id_p \in Comps(\Delta)\ s.t.\ \gamma(p) = id_p, \sum_{t \in Fired(s')} pre(p,t) = \sigma'(id_p)(\text{"s\_output\_token\_sum"})$.
12. $\forall p \in P, id_p \in Comps(\Delta)\ s.t.\ \gamma(p) = id_p, \sum_{t \in Fired(s')} post(t,p) = \sigma'(id_p)(\text{"s\_input\_token\_sum"})$.

Each point is proved by a separate lemma:

– Apply Lemma Falling Edge Equal Marking to solve 1.

– Apply Lemma Falling Edge Equal Time Counters to solve 2.

– Apply Lemma Falling Edge Equal Reset Orders to solve 3.

– Apply Lemma Falling Edge Equal Condition Values to solve 4.

– Apply Lemma Falling Edge Equal Action Executions to solve 5.

– Apply Lemma Falling Edge Equal Function Executions to solve 6.

– Apply Lemma Falling Edge Equal Firable to solve 7.

– Apply Lemma Falling Edge Equal Output Token Sum to solve 11.

– Apply Lemma Falling Edge Equal Input Token Sum to solve 12.

□

1.6.1 Falling Edge and marking

Lemma 2 (Falling Edge Equal Marking). *For all sitpn, d, γ, Δ, σ_e, E_c, E_p, τ, s, s', σ, σ_i, $\sigma_\downarrow$, σ' that verify the hypotheses of Def. 1, then $\forall p \in P, id_p \in Comps(\Delta)$ s.t. $\gamma(p) = id_p$, $s'.M(p) = \sigma'(id_p)(\text{"s\_marking"})$.*

Proof. Given a $p \in P$ and an $id \in Comps(\Delta)$ s.t. $\gamma(p) = id_p$, let us show
$\boxed{s'.M(p) = \sigma'(id_p)(\text{"s\_marking"}).}$
By definition of $E_c, \tau \vdash sitpn, s \xrightarrow{\downarrow} s'$:

$$s.M(p) = s'.M(p) \tag{1.1}$$

By property of the $\texttt{Inject}_\downarrow$ relation, the $\mathcal{H}$-VHDL falling edge relation, the stabilize relation and $\texttt{comp}(id_p, \text{"place"}, gm_p, ipm_p, opm_p) \in d.cs$:

$$\sigma'(id_p)(\text{"s\_marking"}) = \sigma(id_p)(\text{"s\_marking"}) \tag{1.2}$$

Rewriting the goal with (1.1) and (1.2): $\boxed{s.M(p) = \sigma(id_p)(\text{"s\_marking"}).}$
By definition of $\gamma, E_c, \tau \vdash s \overset{\downarrow}{\sim} \sigma$: $s.M(p) = \sigma(id_p)(\text{"s\_marking"})$.

□

Lemma 3 (Falling Edge Equal Output Token Sum). *For all sitpn, d, γ, Δ, σ_e, E_c, E_p, τ, s, s', σ, σ_i, $\sigma_\downarrow$, σ' that verify the hypotheses of Def. 1, then $\forall p, id_p$ s.t. $\gamma(p) = id_p$, $\sum_{t \in Fired(s')} pre(p,t) = \sigma'(id_p)(\text{"s\_output\_token\_sum"})$.*

Proof. Given a $p \in P$ and an $id_p \in Comps(\Delta)$, let us show
$\boxed{\sum_{t \in Fired(s')} pre(p,t) = \sigma'(id_p)(\text{"s\_output\_token\_sum"}).}$
By definition of id_p, there exist gm_p, ipm_p, opm_p s.t. $\texttt{comp}(id_p, \text{"place"}, gm_p, ipm_p, opm_p) \in d.cs$.
By property of the stabilize relation and $\texttt{comp}(id_p, \text{"place"}, gm_p, ipm_p, opm_p) \in d.cs$:

$$\sigma'(id_p)(\text{"sots"}) = \sum_{i=0}^{\Delta(id_p)(\text{"oan"})-1} \begin{cases} \sigma'(id_p)(\text{"oaw"})[i] \texttt{ if } (\sigma'(id_p)(\text{"otf"})[i] \\ \qquad\qquad . \sigma'(id_p)(\text{"oat"})[i] = \texttt{BASIC}) \\ 0 \textit{ otherwise} \end{cases} \tag{1.3}$$

Rewriting the goal with (1.3):

$$\boxed{\sum_{t \in Fired(s')} pre(p,t) = \sum_{i=0}^{\Delta(id_p)(\text{"oan"})-1} \begin{cases} \sigma'(id_p)(\text{"oaw"})[i] \texttt{ if } (\sigma'(id_p)(\text{"otf"})[i] \\ \qquad\qquad . \sigma'(id_p)(\text{"oat"})[i] = \texttt{BASIC}) \\ 0 \textit{ otherwise} \end{cases}}$$

Let us unfold the definition of the left sum term:

$$\sum_{t \in Fired(s')} \begin{cases} \omega \texttt{ if } pre(p,t) = (\omega, \texttt{basic}) \\ 0 \textit{ otherwise} \end{cases} = \sum_{i=0}^{\Delta(id_p)("oan")-1} \begin{cases} \sigma'(id_p)("oaw")[i] \texttt{ if } (\sigma'(id_p)("otf")[i] \\ \qquad\qquad\qquad\qquad . \sigma'(id_p)("oat")[i] = \texttt{BASIC}) \\ 0 \textit{ otherwise} \end{cases}$$

To ease the reading, let us define functions $f \in Fired(s') \to \mathbb{N}$ and $g \in [0, |output(p)| - 1] \to \mathbb{N}$ s.t.

$$f(t) = \begin{cases} \omega \texttt{ if } pre(p,t) = (\omega, \texttt{basic}) \\ 0 \textit{ otherwise} \end{cases} \quad \text{and } g(i) = \begin{cases} \sigma'(id_p)("oaw")[i] \texttt{ if } (\sigma'(id_p)("otf")[i] \\ \qquad\qquad\qquad\qquad . \sigma'(id_p)("oat")[i] = \texttt{BASIC}) \\ 0 \textit{ otherwise} \end{cases}$$

Then, the goal is: $\sum_{t \in Fired(s')} f(t) = \sum_{i=0}^{\Delta(id_p)("oan")-1} g(i)$

Let us perform case analysis on $output(p)$; there are two cases:

1. $output(p) = \emptyset$:

   By construction, $<\texttt{output\_arcs\_number} \Rightarrow 1> \in gm_p$, $<\texttt{output\_arcs\_types}(0) \Rightarrow \texttt{BASIC}> \in ipm_p$, $<\texttt{output\_transitions\_fired}(0) \Rightarrow \texttt{true}> \in ipm_p$, and $<\texttt{output\_arcs\_weights}(0) \Rightarrow 0> \in ipm_p$.

   By property of the elaboration relation and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$:

   $$\Delta(id_p)("oan") = 1 \tag{1.4}$$

   By property of the stabilize relation and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$:

   $$\sigma'(id_p)("oat")[0] = \texttt{BASIC} \tag{1.5}$$
   $$\sigma'(id_p)("otf")[0] = \texttt{true} \tag{1.6}$$
   $$\sigma'(id_p)("oaw")[0] = 0 \tag{1.7}$$

   By property of $output(p) = \emptyset$:

   $$\sum_{t \in Fired(s')} \begin{cases} \omega \texttt{ if } pre(p,t) = (\omega, \texttt{basic}) \\ 0 \textit{ otherwise} \end{cases} = 0 \tag{1.8}$$

   Rewriting the goal with (1.4), (1.5), (1.6), (1.7) and (1.8), tautology.

2. $output(p) \neq \emptyset$:

   By construction, $<\texttt{output\_arcs\_number} \Rightarrow |output(p)|> \in gm_p$, and by property of the elaboration relation:

   $$\Delta(id_p)("oan") = |output(p)| \tag{1.9}$$

Rewriting the goal with (1.9): $\boxed{\sum_{t \in Fired(s')} f(t) = \sum_{i=0}^{|output(p)|-1} g(i).}$

Let us reason by induction on the right sum term of the goal.

- **BASE CASE**:

  In that case, $0 > |output| - 1$ and $\sum_{i=0}^{|output(p)|-1} g(i) = 0$.

  As $0 > |output| - 1$, then $|output(p)| = 0$, thus contradicting $output(p) \neq \emptyset$.

- **INDUCTION CASE**:

  In that case, $0 \leq |output(p)| - 1$.

  $$\forall F \subseteq Fired(s'), g(0) + \sum_{t \in F} f(t) = g(0) + \sum_{i=1}^{|output(p)|-1} g(i)$$

  $$\boxed{\sum_{t \in Fired(s')} f(t) = g(0) + \sum_{i=1}^{|output(p)|-1} g(i)}$$

  By definition of g:

  $$g(0) = \begin{cases} \sigma'(id_p)(''oaw'')[0] \texttt{ if } (\sigma'(id_p)(''otf'')[0] \\ \qquad\qquad\qquad\qquad . \sigma'(id_p)(''oat'')[0] = \texttt{BASIC}) \\ 0 \ otherwise \end{cases} \tag{1.10}$$

  Let us perform case analysis on the value of $\sigma'(id_p)(''otf'')[0] \ . \ \sigma'(id_p)(''oat'')[0] = \texttt{BASIC}$; there are two cases:

  (a) $(\sigma'(id_p)(''otf'')[0] \ . \ \sigma'(id_p)(''oat'')[0] = \texttt{BASIC}) = \texttt{false}$:
  In that case, $g(0) = 0$, and then we can apply the induction hypothesis with $F = Fired(s')$ to solve the goal: $\sum_{t \in Fired(s')} f(t) = \sum_{i=1}^{|output(p)|-1} g(i).$

  (b) $(\sigma'(id_p)(''otf'')[0] \ . \ \sigma'(id_p)(''oat'')[0] = \texttt{BASIC}) = \texttt{true}$:
  In that case, $g(0) = \sigma'(id_p)(''oaw'')[0]$, $\sigma'(id_p)(''otf'')[0] = \texttt{true}$ and $\sigma'(id_p)(''oat'')[0] = \texttt{BASIC}$.
  By construction, there exist a $t \in output(t)$, $id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$. Let us take such a $t \in output(p)$.
  By definition of id_t, there exist gm_t, ipm_t, opm_t s.t. $\texttt{comp}(id_t, ''transition'', gm_t, ipm_t, opm_t) \in d.cs$.
  As $t \in output(p)$, there exist $\omega \in \mathbb{N}^*$ and $a \in \{\texttt{BASIC}, \texttt{TEST}, \texttt{INHIB}\}$ s.t. $pre(p,t) = (\omega, a)$. Let us take an ω and a s.t. $pre(p,t) = (\omega, a)$.
  By construction, $<\texttt{output\_arcs\_types}(0) \Rightarrow a> \in ipm_p$, $<\texttt{output\_arcs\_weights}(0) \Rightarrow \omega> \in ipm_p$, and there exists $id_{ft} \in Sigs(\Delta)$ s.t. $<\texttt{fired} \Rightarrow id_{ft}> \in opm_t$ and $<\texttt{output\_transitions\_fired}(0) \Rightarrow \texttt{id}_{\texttt{ft}}> \in ipm_p$

By property of the stabilize relation, $\sigma'(id_p)("oat")[0] = \texttt{BASIC}$ and $<\texttt{output\_arcs\_types(0)} \Rightarrow \texttt{a}> \in ipm_p$:

$$pre(p,t) = (\omega, \texttt{basic}) \tag{1.11}$$

By property of the stabilize relation, $<\texttt{fired} \Rightarrow \texttt{id}_{\texttt{ft}}> \in opm_t$, $<\texttt{output\_transitions\_fired(0)} \Rightarrow \texttt{id}_{\texttt{ft}}> \in ipm_p$ and $\sigma'(id_p)("otf")[0] = \texttt{true}$:

$$\sigma'(id_t)("fired") = \texttt{true} \tag{1.12}$$

Appealing to Lemma **??**, we know $t \in Fired(s')$.
As $t \in Fired(s')$, we can rewrite the left sum term of the goal as follows:

$$\boxed{f(t) + \sum_{t' \in Fired(s') \setminus \{t\}} f(t') = g(0) + \sum_{i=1}^{|output(p)|-1} g(i)}$$

We know that $g(0) = \sigma'(id_p)("oaw")[0]$, and by property of the stabilize relation and $<\texttt{output\_arcs\_weights(0)} \Rightarrow \omega> \in ipm_p$:

$$\sigma'(id_p)("oaw")[0] = \omega \tag{1.13}$$

Rewriting the goal with (1.13):

$$\boxed{f(t) + \sum_{t' \in Fired(s') \setminus \{t\}} f(t') = \omega + \sum_{i=1}^{|output(p)|-1} g(i)}$$

By definition of f, and as $pre(p,t) = (\omega, \texttt{basic})$, then $f(t) = \omega$; thus, rewriting the goal:

$$\boxed{\omega + \sum_{t' \in Fired(s') \setminus \{t\}} f(t') = \omega + \sum_{i=1}^{|output(p)|-1} g(i)}$$

Then, knowing that $g(0) = \omega$, we can apply the induction hypothesis with $F = Fired(s') \setminus \{t\}$: $g(0) + \sum_{t' \in Fired(s') \setminus \{t\}} f(t') = g(0) + \sum_{i=1}^{|output(p)|-1} g(i)$.

□

Lemma 4 (Falling Edge Equal Input Token Sum). *For all sitpn, d, γ, Δ, σ_e, E_c, E_p, τ, s, s', σ, σ_i, $\sigma_\downarrow$, σ' that verify the hypotheses of Def. 1, then $\forall p, id_p$ s.t. $\gamma(p) = id_p$, $\sum_{t \in Fired(s')} post(t,p) = \sigma'_p("s\_input\_token\_sum")$.*

Proof. Given a $p \in P$ and an $id_p \in Comps(\Delta)$, let us show

$$\boxed{\sum_{t \in Fired(s')} post(t,p) = \sigma'(id_p)("s\_input\_token\_sum").}$$

By definition of id_p, there exist gm_p, ipm_p, opm_p s.t. $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$.
By property of the stabilize relation and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$:

$$\sigma'(id_p)("sits") = \sum_{i=0}^{\Delta(id_p)("ian")-1} \begin{cases} \sigma'(id_p)("iaw")[i] \texttt{ if } \sigma'(id_p)("itf")[i] \\ 0 \textit{ otherwise} \end{cases} \tag{1.14}$$

Rewriting the goal with (1.14):

$$\sum_{t \in Fired(s')} post(t,p) = \sum_{i=0}^{\Delta(id_p)("ian")-1} \begin{cases} \sigma'(id_p)("iaw")[i] \texttt{ if } \sigma'(id_p)("otf")[i] \\ 0 \ otherwise \end{cases}$$

Let us unfold the definition of the left sum term:

$$\sum_{t \in Fired(s')} \begin{cases} \omega \texttt{ if } post(t,p) = \omega \\ 0 \ otherwise \end{cases} = \sum_{i=0}^{\Delta(id_p)("ian")-1} \begin{cases} \sigma'(id_p)("iaw")[i] \texttt{ if } \sigma'(id_p)("itf")[i] \\ 0 \ otherwise \end{cases}$$

Let us perform case analysis on $input(p)$; there are two cases:

1. $input(p) = \emptyset$:

   By construction, $<\texttt{input\_arcs\_number} \Rightarrow \texttt{1}> \in gm_p$, $<\texttt{input\_transitions\_fired(0)} \Rightarrow \texttt{true}> \in ipm_p$, and $<\texttt{input\_arcs\_weights(0)} \Rightarrow \texttt{0}> \in ipm_p$.
   By property of the elaboration relation and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$:

   $$\Delta(id_p)("ian") = 1 \tag{1.15}$$

   By property of the stabilize relation and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$:

   $$\sigma'(id_p)("itf")[0] = \texttt{true} \tag{1.16}$$
   $$\sigma'(id_p)("iaw")[0] = 0 \tag{1.17}$$

   By property of $input(p) = \emptyset$:

   $$\sum_{t \in Fired(s')} \begin{cases} \omega \texttt{ if } post(t,p) = \omega \\ 0 \ otherwise \end{cases} = 0 \tag{1.18}$$

   Rewriting the goal with (1.15), (1.16), (1.17), and (1.18), and simplifying the goal, tautology.

2. $input(p) \neq \emptyset$:

   By construction, $<\texttt{input\_arcs\_number} \Rightarrow |input(p)|> \in gm_p$, and by property of the elaboration relation:

   $$\Delta(id_p)("ian") = |input(p)| \tag{1.19}$$

   To ease the reading, let us define functions $f \in Fired(s') \to \mathbb{N}$ and $g \in [0, |input(p)| - 1] \to \mathbb{N}$ s.t. $f(t) = \begin{cases} \omega \texttt{ if } post(t,p) = \omega \\ 0 \ otherwise \end{cases}$ and
   $g(i) = \begin{cases} \sigma'(id_p)("iaw")[i] \texttt{ if } \sigma'(id_p)("itf")[i] \\ 0 \ otherwise \end{cases}$

Then, the goal is: $\boxed{\sum_{t \in Fired(s')} f(t) = \sum_{i=0}^{\Delta(id_p)("ian")-1} g(i)}$

Rewriting the goal with (1.19): $\boxed{\sum_{t \in Fired(s')} f(t) = \sum_{i=0}^{|input(p)|-1} g(i).}$

Let us reason by induction on the right sum term of the goal.

- **BASE CASE**:
  In that case, $0 > |input(p)| - 1$ and $\sum_{i=0}^{|input(p)|-1} g(i) = 0$.
  As $0 > |input(p)| - 1$, then $|input(p)| = 0$, thus contradicting $input(p) \neq \emptyset$.
- **INDUCTION CASE**:
  In that case, $0 \leq |input(p)| - 1$.

  $$\forall F \subseteq Fired(s'),\ g(0) + \sum_{t \in F} f(t) = g(0) + \sum_{i=1}^{|input(p)|-1} g(i)$$

  $$\boxed{\sum_{t \in Fired(s')} f(t) = g(0) + \sum_{i=1}^{|input(p)|-1} g(i)}$$

  By definition of g:

  $$g(0) = \begin{cases} \sigma'(id_p)("iaw")[0] \texttt{ if } \sigma'(id_p)("itf")[0] \\ 0 \ otherwise \end{cases} \tag{1.20}$$

  Let us perform case analysis on the value of $\sigma'(id_p)("itf")[0]$; there are two cases:

  (a) $\sigma'(id_p)("itf")[0] = \texttt{false}$:
  In that case, $g(0) = 0$, and then we can apply the induction hypothesis with $F = Fired(s')$ to solve the goal: $\sum_{t \in Fired(s')} f(t) = \sum_{i=1}^{|input(p)|-1} g(i).$

  (b) $\sigma'(id_p)("itf")[0] = \texttt{true}$:
  In that case, $g(0) = \sigma'(id_p)("iaw")[0]$ and $\sigma'(id_p)("itf")[0] = \texttt{true}$.
  By construction, there exist a $t \in input(t)$, $id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$. Let us take such a $t \in input(p)$.
  By definition of id_t, there exist gm_t, ipm_t, opm_t s.t. $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$.
  As $t \in input(p)$, there exist $\omega \in \mathbb{N}^*$ s.t. $post(t,p) = \omega$. Let us take an ω s.t. $post(t,p) = \omega$.
  By construction, $<\texttt{input\_arcs\_weights}(0) \Rightarrow \omega> \in ipm_p$, and there exists $id_{ft} \in Sigs(\Delta)$ s.t. $<\texttt{fired} \Rightarrow id_{ft}> \in opm_t$ and $<\texttt{input\_transitions\_fired}(0) \Rightarrow \texttt{id}_{\texttt{ft}}> \in ipm_p$
  By property of the stabilize relation and $<\texttt{input\_arcs\_types}(0) \Rightarrow \texttt{a}> \in ipm_p$:

  $$post(t,p) = \omega \tag{1.21}$$

By property of the stabilize relation, $<\texttt{fired} \Rightarrow \texttt{id}_{\texttt{ft}}> \in opm_t$,
$<\texttt{input\_transitions\_fired}(0) \Rightarrow \texttt{id}_{\texttt{ft}}> \in ipm_p$ and $\sigma'(id_p)("itf")[0] = \texttt{true}$:

$$\sigma'(id_t)("fired") = \texttt{true} \tag{1.22}$$

Appealing to Lemma **??** and (1.22), we know $t \in Fired(s')$.
As $t \in Fired(s')$, we can rewrite the left sum term of the goal as follows:

$$\boxed{f(t) + \sum_{t' \in Fired(s') \setminus \{t\}} f(t') = g(0) + \sum_{i=1}^{|input(p)|-1} g(i)}$$

We know that $g(0) = \sigma'(id_p)("iaw")[0]$, and by property of the stabilize relation and $<\texttt{input\_arcs\_weights}(0) \Rightarrow \omega> \in ipm_p$:

$$\sigma'(id_p)("iaw")[0] = \omega \tag{1.23}$$

Rewriting the goal with (1.23):

$$\boxed{f(t) + \sum_{t' \in Fired(s') \setminus \{t\}} f(t') = \omega + \sum_{i=1}^{|input(p)|-1} g(i)}$$

By definition of f, and as $post(t,p) = \omega$, then $f(t) = \omega$; thus, rewriting the goal:

$$\boxed{\omega + \sum_{t' \in Fired(s') \setminus \{t\}} f(t') = \omega + \sum_{i=1}^{|input(p)|-1} g(i)}$$

Then, knowing that $g(0) = \omega$, we can apply the induction hypothesis with $F = Fired(s') \setminus \{t\}$: $g(0) + \sum_{t' \in Fired(s') \setminus \{t\}} f(t') = g(0) + \sum_{i=1}^{|input(p)|-1} g(i).$

□

1.6.2 Falling edge and time counters

Lemma 5 (Falling Edge Equal Time Counters). *For all $sitpn$, d, γ, Δ, σ_e, E_c, E_p, τ, s, s', σ, σ_i, $\sigma_\downarrow$, σ' that verify the hypotheses of Def. 1, then $\forall t \in T_i, id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$,*
$\big(upper(I_s(t)) = \infty \wedge s'.I(t) \leq lower(I_s(t)) \Rightarrow s'.I(t) = \sigma'(id_t)("s\_time\_counter")\big)$
$\wedge\big(upper(I_s(t)) = \infty \wedge s'.I(t) > lower(I_s(t)) \Rightarrow \sigma'(id_t)("s\_time\_counter") = lower(I_s(t))\big)$
$\wedge\big(upper(I_s(t)) \neq \infty \wedge s'.I(t) > upper(I_s(t)) \Rightarrow \sigma'(id_t)("s\_time\_counter") = upper(I_s(t))\big)$
$\wedge\big(upper(I_s(t)) \neq \infty \wedge s'.I(t) \leq upper(I_s(t)) \Rightarrow s'.I(t) = \sigma'(id_t)("s\_time\_counter")\big)$.

Proof. Given a $t \in T_i$ and an $id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$, let us show

$$\boxed{\begin{array}{l}\big(upper(I_s(t)) = \infty \wedge s'.I(t) \leq lower(I_s(t)) \Rightarrow s'.I(t) = \sigma'(id_t)("s\_time\_counter")\big)\\ \wedge\big(upper(I_s(t)) = \infty \wedge s'.I(t) > lower(I_s(t)) \Rightarrow \sigma'(id_t)("s\_time\_counter") = lower(I_s(t))\big)\\ \wedge\big(upper(I_s(t)) \neq \infty \wedge s'.I(t) > upper(I_s(t)) \Rightarrow \sigma'(id_t)("s\_time\_counter") = upper(I_s(t))\big)\\ \wedge\big(upper(I_s(t)) \neq \infty \wedge s'.I(t) \leq upper(I_s(t)) \Rightarrow s'.I(t) = \sigma'(id_t)("s\_time\_counter")\big)\end{array}}$$

By definition of id_t, there exist gm_t, ipm_t, opm_t s.t. $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$.

By property of the elaboration, $\texttt{Inject}_{\downarrow}$, $\mathcal{H}$-VHDL rising edge and stabilize relations, and $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$:

$$\begin{aligned}\sigma(id_t)("se") = \texttt{true} \wedge \Delta(id_t)("tt") \neq \texttt{NOT\_TEMPORAL} \wedge \sigma(id_t)("srtc") = \texttt{false} \\ \wedge \sigma(id_t)("stc") < \Delta(id_t)("mtc") \Rightarrow \sigma'(id_t)("stc") = \sigma(id_t)("stc") + 1\end{aligned} \tag{1.24}$$

$$\begin{aligned}\sigma(id_t)("se") = \texttt{true} \wedge \Delta(id_t)("tt") \neq \texttt{NOT\_TEMPORAL} \wedge \sigma(id_t)("srtc") = \texttt{false} \\ \wedge \sigma(id_t)("stc") \geq \Delta(id_t)("mtc") \Rightarrow \sigma'(id_t)("stc") = \sigma(id_t)("stc")\end{aligned} \tag{1.25}$$

$$\begin{aligned}\sigma(id_t)("se") = \texttt{true} \wedge \Delta(id_t)("tt") \neq \texttt{NOT\_TEMPORAL} \\ \wedge \sigma(id_t)("srtc") = \texttt{true} \Rightarrow \sigma'(id_t)("stc") = 1\end{aligned} \tag{1.26}$$

$$\sigma(id_t)("se") = \texttt{false} \vee \Delta(id_t)("tt") = \texttt{NOT\_TEMPORAL} \Rightarrow \sigma'(id_t)("stc") = 0 \tag{1.27}$$

Then, there are 4 points to show:

1. $\boxed{upper(I_s(t)) = \infty \wedge s'.I(t) \leq lower(I_s(t)) \Rightarrow s'.I(t) = \sigma'(id_t)("s\_time\_counter")}$

   Assuming $upper(I_s(t)) = \infty$ and $s'.I(t) \leq lower(I_s(t))$, let us show $\boxed{s'.I(t) = \sigma'(id_t)("s\_time\_counter").}$

   Case analysis on $t \in Sens(s.M)$; there are two cases:

   (a) $t \notin Sens(s.M)$:

   By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $\sigma(id_t)("se") = \texttt{false}$ (1.28).
   Appealing to (1.27) and (1.28), we have $\sigma'(id_t)("stc") = 0$ (1.29).
   By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.I(t) = 0$ (1.30).
   Rewriting the goal with (1.29) and (1.30): tautology.

   (b) $t \in Sens(s.M)$:

   By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $\sigma(id_t)("se") = \texttt{true}$ (1.31).
   By construction, and as $upper(I_s(t)) = \infty$, $<\texttt{transition\_type} \Rightarrow \texttt{TEMP\_A\_INF}> \in gm_t$.
   By property of the elaboration relation, we have $\Delta(id_t)("tt") = \texttt{TEMP\_A\_INF}$ (1.32).
   Case analysis on $s.reset_t(t)$; there are two cases:

   i. $s.reset_t(t) = \texttt{true}$:

   By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, $\sigma(id_t)("srtc") = \texttt{true}$ (1.33).
   Appealing to (1.26), (1.31), (1.32) and (1.33), we have $\sigma'(id_t)("stc") = 1$ (1.34).
   By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.I(t) = 1$ (1.35).
   Rewriting the goal with (1.34) and (1.35): tautology.

   ii. $s.reset_t(t) = \texttt{false}$:

   By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $\sigma(id_t)("srtc") = \texttt{false}$ (1.36).

As $upper(I_s(t)) = \infty$, there exists an $a \in \mathbb{N}^*$ s.t. $I_s(t) = [a, \infty]$. Let us take such an $a \in \mathbb{N}^*$. By construction, $<\texttt{maximal\_time\_counter} \Rightarrow a> \in gm_t$, and by property of the elaboration relation, we have $\Delta(id_t)(''mtc'') = a$ (1.37).

By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, and knowing that $t \in Sens(s.M)$, $s.reset_t(t) = \texttt{false}$ and $upper(I_s(t)) = \infty$:

$$s'.I(t) = s.I(t) + 1 \tag{1.38}$$

Rewriting the goal with (1.38): $\boxed{s.I(t) + 1 = \sigma'(id_t)(''stc'').}$

We assumed that $s'.I(t) \leq lower(I_s(t))$, and as $s'.I(t) = s.I(t) + 1$, then $s.I(t) + 1 \leq lower(I_s(t))$, then $s.I(t) < lower(I_s(t))$, then $s.I(t) < a$ since $a = lower(I_s(t))$.

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, and knowing that $s.I(t) < lower(I_s(t))$ and $upper(I_s(t)) = \infty$:

$$s.I(t) = \sigma(id_t)(''stc'') \tag{1.39}$$

Appealing to (1.37), (1.39) and $s.I(t) < a$:

$$\sigma(id_t)(''stc'') < \Delta(id_t)(''mtc'') \tag{1.40}$$

Appealing to (1.24), (1.40), (1.36) and (1.31):

$$\sigma'(id_t)(''stc'') = \sigma(id_t)(''stc'') + 1 \tag{1.41}$$

Rewriting the goal with (1.41) and (1.39): tautology.

2. $\boxed{upper(I_s(t)) = \infty \wedge s'.I(t) > lower(I_s(t)) \Rightarrow \sigma'(id_t)(''s\_time\_counter'') = lower(I_s(t).}$

Assuming that $upper(I_s(t)) = \infty$ and $s'.I(t) > lower(I_s(t))$, let us show $\boxed{\sigma'(id_t)(''s\_time\_counter'') = lower(I_s(t)).}$

As $upper(I_s(t)) = \infty$, there exists an $a \in \mathbb{N}^*$ s.t. $I_s(t) = [a, \infty]$. Let us take such an $a \in \mathbb{N}^*$. By construction, $<\texttt{maximal\_time\_counter} \Rightarrow a> \in gm_t$, and $<\texttt{transition\_type} \Rightarrow \texttt{TEMP\_A\_INF}> \in gm_t$ by property of the elaboration relation:

$$\Delta(id_t)(''mtc'') = a \tag{1.42}$$
$$\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_INF} \tag{1.43}$$

Case analysis on $t \in Sens(s.M)$:

(a) $t \notin Sens(s.M)$:

By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, and knowing that $t \in Sens(s.M)$, then $s'.I(t) = 0$. Since $lower(I_s(t)) \in \mathbb{N}^*$, then $lower(I_s(t)) > 0$.

Contradicts $s'.I(t) > lower(I_s(t))$.

(b) $t \in Sens(s.M)$:

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$ and $t \in Sens(s.M)$:

$$\sigma(id_t)(''se'') = \texttt{true} \tag{1.44}$$

Case analysis on $s.reset_t(t)$; there are two cases:

i. $s.reset_t(t) = \texttt{true}$:

By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$: $s'.I(t) = 1$.
We assumed that $s'.I(t) > lower(I_s(t))$, then $1 > lower(I_s(t))$.
Contradicts $lower(I_s(t)) > 0$.

ii. $s.reset_t(t) = \texttt{false}$:

By property of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$ and $s.reset_t(t) = \texttt{false}$:

$$\sigma(id_t)(\text{"}srtc\text{"}) = \texttt{false} \tag{1.45}$$

By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, and knowing that $s'.I(t) > lower(I_s(t))$:

$$\begin{aligned} s'.I(t) = s.I(t) + 1 &\Rightarrow s.I(t) + 1 > lower(I_s(t)) \\ &\Rightarrow s.I(t) \geq lower(I_s(t)) \end{aligned} \tag{1.46}$$

Case analysis on $s.I(t) \geq lower(I_s(t))$:

A. $s.I(t) > lower(I_s(t))$: $\boxed{\sigma'(id_t)(\text{"}stc\text{"}) = lower(I_s(t)).}$

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$:

$$\sigma(id_t)(\text{"}stc\text{"}) = lower(I_s(t)) \tag{1.47}$$

Appealing to (1.25):

$$\sigma'(id_t)(\text{"}stc\text{"}) = \sigma(id_t)(\text{"}stc\text{"}) \tag{1.48}$$

Rewriting the goal with (1.47) and (1.48): tautology.

B. $s.I(t) = lower(I_s(t))$: $\boxed{\sigma'(id_t)(\text{"}stc\text{"}) = lower(I_s(t)).}$

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$:

$$s.I(t) = \sigma(id_t)(\text{"}stc\text{"}) \tag{1.49}$$

Appealing to (1.25):

$$\sigma'(id_t)(\text{"}stc\text{"}) = \sigma(id_t)(\text{"}stc\text{"}) \tag{1.50}$$

Rewriting the goal with (1.50), (1.49) and $s.I(t) = lower(I_s(t))$: tautology.

3. $\boxed{upper(I_s(t)) \neq \infty \wedge s'.I(t) > upper(I_s(t)) \Rightarrow \sigma'(id_t)(\text{"}s\_time\_counter\text{"}) = upper(I_s(t)).}$

Assuming that $upper(I_s(t)) \neq \infty$ and $s'.I(t) > upper(I_s(t))$, let us show
$\boxed{\sigma'(id_t)(\text{"}s\_time\_counter\text{"}) = upper(I_s(t)).}$

As $upper(I_s(t)) \neq \infty$, there exists an $a \in \mathbb{N}^*$, and a $b \in \mathbb{N}^*$ s.t. $I_s(t) = [a, b]$. Let us take such an a and b. By construction, there exists $tt \in \{\texttt{TEMP\_A\_A}, \texttt{TEMP\_A\_B}\}$ s.t. $<\texttt{maximal\_time\_counter} \Rightarrow b> \in gm_t$, and $<\texttt{transition\_type} \Rightarrow tt> \in gm_t$; by property of the elaboration relation:

$$\Delta(id_t)(\text{"}mtc\text{"}) = b = upper(I_s(t)) \tag{1.51}$$

$$\Delta(id_t)(\text{"}tt\text{"}) \neq \texttt{NOT\_TEMP} \tag{1.52}$$

Case analysis on $t \in Sens(s.M)$:

(a) $t \notin Sens(s.M)$:

By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, and knowing that $t \in Sens(s.M)$, then $s'.I(t) = 0$. Since $upper(I_s(t)) \in \mathbb{N}^*$, then $upper(I_s(t)) > 0$.

Contradicts $s'.I(t) > upper(I_s(t))$.

(b) $t \in Sens(s.M)$:

By definition of $\gamma, E_c, \tau \vdash s \overset{\updownarrow}{\sim} \sigma$ and $t \in Sens(s.M)$:

$$\sigma(id_t)(\text{"se"}) = \texttt{true} \tag{1.53}$$

Case analysis on $s.reset_t(t)$; there are two cases:

i. $s.reset_t(t) = \texttt{true}$:

By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$: $s'.I(t) = 1$.
We assumed that $s'.I(t) > upper(I_s(t))$, then $1 > upper(I_s(t))$.
Contradicts $upper(I_s(t)) > 0$.

ii. $s.reset_t(t) = \texttt{false}$:

By property of $\gamma, E_c, \tau \vdash s \overset{\updownarrow}{\sim} \sigma$ and $s.reset_t(t) = \texttt{false}$:

$$\sigma(id_t)(\text{"srtc"}) = \texttt{false} \tag{1.54}$$

Case analysis on $s.I(t) > upper(I_s(t))$ or $s.I(t) \leq upper(I_s(t))$:

A. $s.I(t) > upper(I_s(t))$: $\boxed{\sigma'(id_t)(\text{"stc"}) = upper(I_s(t)).}$

By definition of $\gamma, E_c, \tau \vdash s \overset{\updownarrow}{\sim} \sigma$:

$$s'.I(t) = s.I(t) \tag{1.55}$$

By definition of $\gamma, E_c, \tau \vdash s \overset{\updownarrow}{\sim} \sigma$:

$$\sigma(id_t)(\text{"stc"}) = upper(I_s(t)) \tag{1.56}$$

Appealing to (1.25), we have $\sigma'(id_t)(\text{"stc"}) = \sigma(id_t)(\text{"stc"})$.
Rewriting the goal with $\sigma'(id_t)(\text{"stc"}) = \sigma(id_t)(\text{"stc"})$ and (1.56): tautology.

B. $s.I(t) \leq upper(I_s(t))$: $\boxed{\sigma'(id_t)(\text{"stc"}) = upper(I_s(t)).}$

By definition of $\gamma, E_c, \tau \vdash s \overset{\updownarrow}{\sim} \sigma$:

$$s.I(t) = \sigma(id_t)(\text{"stc"}) \tag{1.57}$$

Case analysis on $s.I(t) \leq upper(I_s(t))$; there are two cases:

- $s.I(t) = upper(I_s(t))$:

Appealing to (1.51), (1.57) and $s.I(t) = upper(I_s(t))$:

$$\Delta(id_t)(\text{"mtc"}) \leq \sigma(id_t)(\text{"stc"}) \tag{1.58}$$

Appealing to (1.58) and (1.25):

$$\sigma'(id_t)(\text{"}stc\text{"}) = \sigma(id_t)(\text{"}stc\text{"}) \tag{1.59}$$

Rewriting the goal with (1.59), (1.57) and $s.I(t) = upper(I_s(t))$: tautology.

- $s.I(t) < upper(I_s(t))$:

  By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$:

  $$s'.I(t) = s.I(t) + 1 \tag{1.60}$$

  From (1.60) and $s.I(t) < upper(I_s(t))$, we can deduce $s'.I(t) \leq upper(I_s(t))$; contradicts $s'.I(t) > upper(I_s(t))$.

4. $\boxed{upper(I_s(t)) \neq \infty \wedge s'.I(t) \leq upper(I_s(t)) \Rightarrow s'.I(t) = \sigma'(id_t)(\text{"}s\_time\_counter\text{"}).}$

Assuming that $upper(I_s(t)) \neq \infty$ and $s'.I(t) \leq upper(I_s(t))$, let us show $\boxed{s'.I(t) = \sigma'(id_t)(\text{"}s\_time\_counter\text{"}).}$

As $upper(I_s(t)) \neq \infty$, there exists an $a \in \mathbb{N}^*$, and a $b \in \mathbb{N}^*$ s.t. $I_s(t) = [a, b]$. Let us take such an a and b. By construction, there exists $tt \in \{\texttt{TEMP\_A\_A}, \texttt{TEMP\_A\_B}\}$ s.t. $<\texttt{maximal\_time\_counter} \Rightarrow b> \in gm_t$, and $<\texttt{transition\_type} \Rightarrow tt> \in gm_t$; by property of the elaboration relation:

$$\Delta(id_t)(\text{"}mtc\text{"}) = b = upper(I_s(t)) \tag{1.61}$$

$$\Delta(id_t)(\text{"}tt\text{"}) \neq \texttt{NOT\_TEMP} \tag{1.62}$$

Case analysis on $t \in Sens(s.M)$:

(a) $t \notin Sens(s.M)$:

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $\sigma(id_t)(\text{"}se\text{"}) = \texttt{false}$ (1.63).
Appealing (1.27) and (1.63), we have $\sigma'(id_t)(\text{"}stc\text{"}) = 0$ (1.64).
By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.I(t) = 0$ (1.65).
Rewriting the goal with (1.64) and (1.65): tautology.

(b) $t \in Sens(s.M)$:

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $\sigma(id_t)(\text{"}se\text{"}) = \texttt{true}$ (1.66).
Case analysis on $s.reset_t(t)$:

i. $s.reset_t(t) = \texttt{true}$:

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $\sigma(id_t)(\text{"}srtc\text{"}) = \texttt{true}$ (1.67).
Appealing to (1.26), (1.62), (1.66) and (1.67), we have $\sigma'(id_t)(\text{"}stc\text{"}) = 1$ (1.68).
By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.I(t) = 1$ (1.69).
Rewriting the goal with (1.68) and (1.69), tautology.

ii. $s.reset_t(t) = \texttt{false}$:

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $\sigma(id_t)(\text{"}srtc\text{"}) = \texttt{false}$ (1.70).
Case analysis on $s.I(t) > upper(I_s(t))$ or $s.I(t) \leq upper(I_s(t))$:

A. $s.I(t) > upper(I_s(t))$:
By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s.I(t) = s'.I(t)$, and thus, $s'.I(t) > upper(I_s(t))$. Contradicts $s'.I(t) \leq upper(I_s(t))$.

B. $s.I(t) \leq upper(I_s(t))$:
By definition of $\gamma, E_c, \tau \vdash s \overset{\updownarrow}{\sim} \sigma$, we have $s.I(t) = \sigma(id_t)(''stc'')$ (1.71).

- $s.I(t) < upper(I_s(t))$:
From $s.I(t) < upper(I_s(t))$, (1.71) and (1.61), we can deduce $\sigma(id_t)(''stc'') < \Delta(id_t)(''mtc'')$ (1.72).
From (1.24), (1.66), (1.62), (1.70) and (1.72), we can deduce:

$$\sigma'(id_t)(''stc'') = \sigma(id_t)(''stc'') + 1 \tag{1.73}$$

By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$:

$$s'.I(t) = s.I(t) + 1 \tag{1.74}$$

Rewriting the goal with (1.73) and (1.74), tautology.

- $s.I(t) = upper(I_s(t))$:
By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we know that $s'.I(t) = s.I(t) + 1$. We assumed that $s'.I(t) \leq upper(I_s(t))$; thus, $s.I(t) + 1 \leq upper(I_s(t))$.
Contradicts $s.I(t) = upper(I_s(t))$.

□

1.6.3 Falling edge and reset orders

Lemma 6 (Falling Edge Equal Reset Orders). *For all sitpn, d, γ, Δ, σ_e, E_c, E_p, τ, s, s', σ, σ_i, $\sigma_\downarrow$, σ' that verify the hypotheses of Def. 1, then $\forall t \in T_i, id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$, $s'.reset_t(t) = \sigma'(id_t)(''s\_reinit\_time\_counter'')$.*

Proof. Given a $t \in T_i$ and an $id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$, let us show $s'.reset_t(t) = \sigma'(id_t)(''srtc'')$.
By definition of id_t, there exist gm_t, ipm_t, opm_t s.t. $\texttt{comp}(id_t, ''transition'', gm_t, ipm_t, opm_t) \in d.cs$.
By property of the stabilize relation and $\texttt{comp}(id_t, ''transition'', gm_t, ipm_t, opm_t) \in d.cs$:

$$\sigma'(id_t)(''srtc'') = \sum_{i=0}^{\Delta(id_t)(''ian'')-1} \sigma'(id_t)(''rt'')[i] \tag{1.75}$$

□

1.6.4 Falling edge and condition values

Lemma 7 (Falling Edge Equal Condition Values). *For all sitpn, d, γ, Δ, σ_e, E_c, E_p, τ, s, s', σ, σ_i, $\sigma_\downarrow$, σ' that verify the hypotheses of Def. 1, then $\forall c \in \mathcal{C}, id_c \in Ins(\Delta)$ s.t. $\gamma(c) = id_c$, $s'.cond(c) = \sigma'(id_c)$.*

Proof. Given a $c \in \mathcal{C}$ and an $id_c \in Ins(\Delta)$ s.t. $\gamma(c) = id_c$, let us show $s'.cond(c) = \sigma'(id_c)$.

By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.cond(c) = E_c(\tau, c)$ (1.76).
By property of the $\texttt{Inject}_{\downarrow}$, the $\mathcal{H}$-VHDL falling edge, the stabilize relations and $id_c \in Ins(\Delta)$, we have $\sigma'(id_c) = E_p(\tau, \downarrow)(id_c)$ (1.77).
Rewriting the goal with (1.76) and (1.77): $\boxed{E_c(\tau, c) = E_p(\tau, \downarrow)(id_c)}$
By definition of $\gamma \vdash E_p \overset{env}{=} E_c$: $E_c(\tau, c) = E_p(\tau, \downarrow)(id_c)$.

□

1.6.5 Falling and action executions

Lemma 8 (Falling Edge Equal Action Executions). *For all sitpn, d, γ, Δ, σ_e, E_c, E_p, τ, s, s', σ, σ_i, $\sigma_{\downarrow}$, σ' that verify the hypotheses of Def. 1, then $\forall a \in \mathcal{A}, id_a \in Outs(\Delta)$ s.t. $\gamma(a) = id_a$, $s'.ex(a) = \sigma'(id_a)$.*

Proof. Given an $a \in \mathcal{A}$ and an $id_a \in Outs(\Delta)$ s.t. $\gamma(a) = id_a$, let us show $\boxed{s'.ex(a) = \sigma'(id_a).}$
By property of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$:

$$s'.ex(a) = \sum_{p \in marked(s.M)} \mathbb{A}(p, a) \tag{1.78}$$

By construction, the ''`action`'' process is a part of design d's behavior, i.e there exist an $sl \subseteq Sigs(\Delta)$ and an $ss_a \in ss$ s.t. $\texttt{ps}(\text{"}action\text{"}, \emptyset, sl, ss) \in d.cs$.
By construction id_a is only assigned in the body of the ''`action`'' process. Let $pls(a)$ be the set of actions associated to action a, i.e $pls(a) = \{p \in P \mid \mathbb{A}(p, a) = true\}$. Then, depending on $pls(a)$, there are two cases of assignment of output port id_a:

- **CASE** $pls(a) = \emptyset$:
  By construction, $\texttt{id}_\texttt{a} \Leftarrow \texttt{false} \in ss_{a\downarrow}$ where $ss_{a\downarrow}$ is the part of the ''`action`'' process body executed during the falling edge phase.

  By property of the $\mathcal{H}$-VHDL falling edge, the stabilize relations and $\texttt{ps}(\text{"}action\text{"}, \emptyset, sl, ss_a) \in d.cs$:

  $$\sigma'(id_a) = false \tag{1.79}$$

  By property of $\sum_{p \in marked(s.M)} \mathbb{A}(p, a)$ and $pls(a) = \emptyset$:

  $$\sum_{p \in marked(s.M)} \mathbb{A}(p, a) = \texttt{false} \tag{1.80}$$

  Rewriting the goal with (1.78), (1.79) and (1.80), tautology.

- **CASE** $pls(a) \neq \emptyset$:
  By construction, $\texttt{id}_\texttt{a} \Leftarrow \texttt{id}_{\texttt{mp}_0} + \cdots + \texttt{id}_{\texttt{mp}_n} \in ss_{a\downarrow}$, where $id_{mp_i} \in Sigs(\Delta)$, $ss_{a\downarrow}$ is the part of the ''`action`'' process body executed during the falling edge phase, and $n = |pls(a)| - 1$.

  By property of the $\texttt{Inject}_{\downarrow}$, the $\mathcal{H}$-VHDL falling edge, the stabilize relations, and $\texttt{ps}(\text{"}action\text{"}, \emptyset, sl, ss) \in d.cs$:

  $$\sigma'(id_a) = \sigma(id_{mp_0}) + \cdots + \sigma(id_{mp_n}) \tag{1.81}$$

Rewriting the goal with (1.78) and (1.81), $\boxed{\sum_{p \in marked(s.M)} \mathbb{A}(p,a) = \sigma(id_{mp_0}) + \cdots + \sigma(id_{mp_n}).}$

Let us reason on the value of $\sigma(id_{mp_0}) + \cdots + \sigma(id_{mp_n})$; there are two cases:

- **CASE** $\sigma(id_{mp_0}) + \cdots + \sigma(id_{mp_n}) = \texttt{true}$:
  Then, we can rewrite the goal as follows: $\boxed{\sum_{p \in marked(s.M)} \mathbb{A}(p,a) = \texttt{true}.}$
  To prove the above goal, let us show $\boxed{\exists p \in marked(s.M)\ s.t.\ \mathbb{A}(p,a) = \texttt{true}.}$
  From $\sigma(id_{mp_0}) + \cdots + \sigma(id_{mp_n}) = \texttt{true}$, we can deduce that $\exists id_{mp_i}\ s.t.\ \sigma(id_{mp_i}) = \texttt{true}$.
  Let us take an id_{mp_i} s.t. $\sigma(id_{mp_i}) = \texttt{true}$.
  By construction, for all id_{mp_i}, there exist a $p_i \in pls(a)$, an $id_{p_i} \in Comps(\Delta)$, gm_{p_i}, ipm_{p_i} and opm_{p_i} s.t. $\gamma(p_i) = id_{p_i}$ and $\texttt{comp}(id_{p_i}, "place", gm_{p_i}, ipm_{p_i}, opm_{p_i}) \in d.cs$ and $<\texttt{marked} \Rightarrow \texttt{id}_{\texttt{mp}_\texttt{i}}> \in opm_{p_i}$. Let us take such a p_i, id_{p_i}, gm_{p_i}, ipm_{p_i} and opm_{p_i}.
  By property of stable σ, and $\texttt{comp}(id_{p_i}, "place", gm_{p_i}, ipm_{p_i}, opm_{p_i}) \in d.cs$:

$$\sigma(id_{mp_i}) = \sigma(id_{p_i})("marked") \tag{1.82}$$
$$\sigma(id_{p_i})("marked") = \sigma(id_{p_i})("sm") > 0 \tag{1.83}$$

  From (1.82), (1.83) and $\sigma(id_{mp_i}) = \texttt{true}$, we can deduce that $\sigma(id_{p_i})("marked") = \texttt{true}$ and $(\sigma(id_{p_i})("sm") > 0) = \texttt{true}$.
  By property of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$:

$$s.M(p_i) = \sigma(id_{p_i})("sm") \tag{1.84}$$

  From (1.84) and $(\sigma(id_{p_i})("sm") > 0) = \texttt{true}$, we can deduce $p_i \in marked(s.M)$, i.e $s.M(p_i) > 0$.
  Let us use p_i to prove the goal: $\boxed{\mathbb{A}(p,a) = \texttt{true}.}$
  By definition of $p_i \in pls(a)$, $\mathbb{A}(p,a) = \texttt{true}$.
- **CASE** $\sigma(id_{mp_0}) + \cdots + \sigma(id_{mp_n}) = \texttt{false}$:
  Then, we can rewrite the goal as follows: $\boxed{\sum_{p \in marked(s.M)} \mathbb{A}(p,a) = \texttt{false}.}$
  To prove the above goal, let us show $\boxed{\forall p \in marked(s.M)\ s.t.\ \mathbb{A}(p,a) = \texttt{false}.}$
  Given a $p \in marked(s.M)$, let us show $\boxed{\mathbb{A}(p,a) = \texttt{false}.}$
  Let us perform case analysis on $\mathbb{A}(p,a)$; there are 2 cases:
  - **CASE** $\mathbb{A}(p,a) = \texttt{false}$.
  - **CASE** $\mathbb{A}(p,a) = \texttt{true}$:
    By construction, for all $p \in P$ s.t. $\mathbb{A}(p,a) = \texttt{true}$, there exist an $id_p \in Comps(\Delta)$, gm_{tp}, ipm_p, opm_p and $id_{mp_i} \in Sigs(\Delta)$ s.t. $\gamma(p) = id_p$ and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$ and $<\texttt{marked} \Rightarrow \texttt{id}_{\texttt{mp}_\texttt{i}}> \in opm_p$. Let us take such a id_p, gm_p, ipm_p, opm_p and id_{mp_i}.

By property of stable σ and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$:

$$\sigma(id_{mp_i}) = \sigma(id_p)("marked") \tag{1.85}$$
$$\sigma(id_p)("marked") = \sigma(id_p)("sm") > 0 \tag{1.86}$$

From $\sigma(id_{mp_0}) + \cdots + \sigma(id_{mp_n}) = \texttt{false}$, we can deduce $\sigma(id_p)("marked") = \texttt{false}$, and thus that $(\sigma(id_p)("sm") > 0) = \texttt{false}$.

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $s.M(p) = \sigma(id_p)("sm")$, and thus, we can deduce that $s.M(p) = 0$ (equivalent to $(s.M(p) > 0) = \texttt{false}$).

Contradicts $p \in marked(s.M)$ (i.e, $s.M(p) > 0$).

□

1.6.6 Falling edge and function executions

Lemma 9 (Falling Edge Equal Function Executions). *For all $sitpn, d, \gamma, \Delta, \sigma_e, E_c, E_p, \tau, s, s', \sigma, \sigma_i, \sigma_\downarrow, \sigma'$ that verify the hypotheses of Def. 1, then $\forall f \in \mathcal{F}, id_f \in Outs(\Delta)$ s.t. $\gamma(f) = id_f$, $s'.ex(f) = \sigma'(id_f)$.*

Proof. Given an $f \in \mathcal{F}$ and an $id_f \in Outs(\Delta)$ s.t. $\gamma(f) = id_f$, let us show $\boxed{s'.ex(f) = \sigma'(id_f).}$

By property of $E_c, \tau \vdash s \overset{\downarrow}{\to} s'$:

$$s.ex(f) = s'.ex(f) \tag{1.87}$$

By construction, id_f is an output port identifier of boolean type in the $\mathcal{H}$-VHDL design d assigned by the ‘‘`function`’’ process only during a rising edge phase.
By property of the $\mathcal{H}$-VHDL $\texttt{Inject}_\uparrow$, rising edge, stabilize relations, and the ‘‘`function`’’ process:

$$\sigma(id_f) = \sigma'(id_f) \tag{1.88}$$

Rewriting the goal with (1.87) and (1.88), $\boxed{s.ex(f) = \sigma(id_f).}$

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, $s.ex(f) = \sigma(id_f)$. □

1.6.7 Falling edge and firable transitions

Lemma 10 (Falling Edge Equal Firable). *For all $sitpn$, d, γ, Δ, σ_e, E_c, E_p, τ, s, s', σ, σ_i, $\sigma_\downarrow$, σ' that verify the hypotheses of Def. 1, then $\forall t \in T, id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$, $t \in Firable(s') \Leftrightarrow \sigma'(id_t)("s\_firable") = \texttt{true}$.*

Proof. Given a $t \in T$ and $id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$, let us show that
$\boxed{t \in Firable(s') \Leftrightarrow \sigma'(id_t)("s\_firable") = \texttt{true}.}$

The proof is in two parts:

1. Assuming that $t \in Firable(s')$, let us show $\boxed{\sigma'(id_t)("s\_firable") = \texttt{true}.}$
   Apply Lemma Falling Edge Equal Firable 1 to solve the goal.
2. Assuming that $\sigma'(id_t)("s\_firable") = \texttt{true}$, let us show $\boxed{t \in Firable(s').}$
   Apply Lemma Falling Edge Equal Firable 2 to solve the goal.

□

Lemma 11 (Falling Edge Equal Firable 1). *For all sitpn, d, γ, Δ, σ_e, E_c, E_p, τ, s, s', σ, σ_i, $\sigma_\downarrow$, σ' that verify the hypotheses of Def. 1, then $\forall t \in T, id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$, $t \in Firable(s') \Rightarrow \sigma'(id_t)(\text{"}s\_firable\text{"}) = \texttt{true}$.*

Proof. Given a $t \in T$ and $id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$, and assuming that $t \in Firable(s')$, let us show $\boxed{\sigma'(id_t)(\text{"}s\_firable\text{"}) = \texttt{true}.}$

By definition of id_t, there exist gm_t, ipm_t, opm_t s.t. $\texttt{comp}(id_t, \text{"}transition\text{"}, gm_t, ipm_t, opm_t) \in d.cs$. By property of the $Inject_\downarrow$, the $\mathcal{H}$-VHDL falling edge, the stabilize relations and $\texttt{comp}(id_t, \text{"}transition\text{"}, gm_t, ipm_t, opm_t) \in d.cs$:

$$\sigma'(id_t)(\text{"}sfa\text{"}) = \sigma(id_t)(\text{"}se\text{"}) \,.\, \sigma(id_t)(\text{"}scc\text{"}) \,.\, \texttt{checktc}(\Delta(id_t), \sigma(id_t)) \tag{1.89}$$

Let us define term $\texttt{checktc}(\Delta(id_t), \sigma(id_t))$ as follows:

$$\begin{aligned}\texttt{checktc}(\Delta(id_t), \sigma(id_t)) = \Big(&\texttt{not}\ \sigma(id_t)(\text{"}srtc\text{"}) \,. \\ &\big[(\Delta(id_t)(\text{"}tt\text{"}) = \texttt{TEMP\_A\_B} \,.\, (\sigma(id_t)(\text{"}stc\text{"}) \geq \sigma(id_t)(\text{"}A\text{"}) - 1) \\ &\qquad .\, (\sigma(id_t)(\text{"}stc\text{"}) \leq \sigma(id_t)(\text{"}B\text{"}) - 1)) \\ &+ (\Delta(id_t)(\text{"}tt\text{"}) = \texttt{TEMP\_A\_A} \,.\, (\sigma(id_t)(\text{"}stc\text{"}) = \sigma(id_t)(\text{"}A\text{"}) - 1)) \\ &+ (\Delta(id_t)(\text{"}tt\text{"}) = \texttt{TEMP\_A\_INF} \,.\, (\sigma(id_t)(\text{"}stc\text{"}) \geq \sigma(id_t)(\text{"}A\text{"}) - 1))\big]\Big) \\ &+ \big(\sigma(id_t)(\text{"}srtc\text{"}) \,.\, \Delta(id_t)(\text{"}tt\text{"}) \neq \texttt{NOT\_TEMP} \,.\, \sigma(id_t)(\text{"}A\text{"}) = 1\big) \\ &+ \Delta(id_t)(\text{"}tt\text{"}) = \texttt{NOT\_TEMP}\end{aligned} \tag{1.90}$$

Rewriting the goal with (1.89): $\boxed{\sigma(id_t)(\text{"}se\text{"}) \,.\, \sigma(id_t)(\text{"}scc\text{"}) \,.\, \texttt{checktc}(\Delta(id_t), \sigma(id_t)) = \texttt{true}.}$
Then, there are three points to prove:

1. $\boxed{\sigma(id_t)(\text{"}se\text{"}) = \texttt{true}}$:

   From $t \in Firable(s')$, we can deduce $t \in Sens(s'.M)$. By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s.M = s'.M$, and thus, we can deduce $t \in Sens(s.M)$.

   By definition of $\gamma, E_c, \tau \vdash s \overset{\updownarrow}{\sim} \sigma$, we know that $t \in Sens(s.M)$ implies $\sigma(id_t)(\text{"}se\text{"}) = \texttt{true}.$

2. $\boxed{\sigma(id_t)(\text{"}scc\text{"}) = \texttt{true}}$:

   By definition of $\gamma, E_c, \tau \vdash s \overset{\updownarrow}{\sim} \sigma$:

   $$\sigma(id_t)(\text{"}scc\text{"}) = \prod_{c \in conds(t)} \begin{cases} E_c(\tau, c) & if\ \mathbb{C}(t,c) = 1 \\ \texttt{not}(E_c(\tau, c)) & if\ \mathbb{C}(t,c) = -1 \end{cases} \tag{1.91}$$

   where $conds(t) = \{c \in \mathcal{C} \mid \mathbb{C}(t,c) = 1 \vee \mathbb{C}(t,c) = -1\}$.

Rewriting the goal with (1.91): $\boxed{\prod_{c \in conds(t)} \begin{cases} E_c(\tau, c) & if\ \mathbb{C}(t,c) = 1 \\ \texttt{not}(E_c(\tau, c)) & if\ \mathbb{C}(t,c) = -1 \end{cases} = \texttt{true}.}$

To ease the reading, let us define $f(c) = \begin{cases} E_c(\tau, c) & if\ \mathbb{C}(t,c) = 1 \\ \texttt{not}(E_c(\tau, c)) & if\ \mathbb{C}(t,c) = -1 \end{cases}$.

Let us reason by induction on the left term of the goal:

- **BASE CASE**: $true = true.$
- **INDUCTION CASE**:

  $$\prod_{c' \in conds(t) \setminus \{c\}} f(c') = \texttt{true}$$

  $\boxed{f(c)\ .\ \prod_{c' \in conds(t) \setminus \{c\}} f(c') = \texttt{true}.}$

  Rewriting the goal with the induction hypothesis, and simplifying the goal, and unfolding the definition of $f(c)$: $\boxed{\begin{cases} E_c(\tau, c) & if\ \mathbb{C}(t,c) = 1 \\ \texttt{not}(E_c(\tau, c)) & if\ \mathbb{C}(t,c) = -1 \end{cases} = \texttt{true}.}$

  As $c \in conds(t)$, let us perform case analysis on $\mathbb{C}(t,c) = 1 \vee \mathbb{C}(t,c) = -1$:

  (a) $\mathbb{C}(t,c) = 1$: $\boxed{E_c(\tau, c) = \texttt{true}.}$

  By definition of $t \in Firable(s')$, we can deduce that $s'.cond(c) = \texttt{true}$. By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.cond(c) = E_c(\tau, c)$. Thus, $E_c(\tau, c) = \texttt{true}.$

  (b) $\mathbb{C}(t,c) = -1$: $\boxed{\texttt{not}\ E_c(\tau, c) = \texttt{true}.}$

  By definition of $t \in Firable(s')$, we can deduce that $s'.cond(c) = \texttt{false}$. By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.cond(c) = E_c(\tau, c)$. Thus, $\texttt{not}\ E_c(\tau, c) = \texttt{true}.$

3. $\boxed{\texttt{checktc}(\Delta(id_t), \sigma(id_t)) = \texttt{true}}$:

By definition of $t \in Firable(s')$, we have $t \notin T_i \vee s'.I(t) \in I_s(t)$. Let us perform case analysis on $t \notin T_i \vee s'.I(t) \in I_s(t)$:

(a) $t \notin T_i$:

By construction, $<\texttt{transition\_type} \Rightarrow \texttt{NOT\_TEMP}> \in gm_t$, and by property of the elaboration relation, we have $\Delta(id_t)(\text{"}tt\text{"}) = \texttt{NOT\_TEMP}$.
From $\Delta(id_t)(\text{"}tt\text{"}) = \texttt{NOT\_TEMP}$, and the definition of $\texttt{checktc}(\Delta(id_t), \sigma(id_t))$, we can deduce $\texttt{checktc}(\Delta(id_t), \sigma(id_t)) = \texttt{true}.$

(b) $s'.I(t) \in I_s(t)$:

From $s'.I(t) \in I_s(t)$, we can deduce that $t \in T_i$. Thus, by construction, there exists $tt \in \{\texttt{TEMP\_A\_B}, \texttt{TEMP\_A\_A}, \texttt{TEMP\_A\_INF}\}$ s.t. $<\texttt{transition\_type} \Rightarrow tt> \in gm_t$. By property of the elaboration relation, we have $\Delta(id_t)(''tt'') = tt$, and thus, we know $\Delta(id_t)(''tt'') \neq \texttt{NOT\_TEMP}$. Therefore, we can simplfy the term $\texttt{checktc}(\Delta(id_t), \sigma(id_t))$ as follows:

$$\begin{aligned}\texttt{checktc}(\Delta(id_t), \sigma(id_t)) = \Big(&\texttt{not}\ \sigma(id_t)(''srtc'')\ .\\ &\big[(\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_B}\ .\ (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1)\\ &\qquad .\ (\sigma(id_t)(''stc'') \leq \sigma(id_t)(''B'') - 1))\\ &+(\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_A}\ .\\ &\quad (\sigma(id_t)(''stc'') = \sigma(id_t)(''A'') - 1))\\ &+(\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_INF}\ .\\ &\quad (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1))\big]\Big)\\ &+ (\sigma(id_t)(''srtc'')\ .\ \sigma(id_t)(''A'') = 1)\end{aligned} \tag{1.92}$$

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $s.reset_t(t) = \sigma(id_t)(''srtc'')$.
Let us perform case analysis on the value $s.reset_t(t)$:

i. $s.reset_t(t) = \texttt{true}$:

Then, from $s.reset_t(t) = \sigma(id_t)(''srtc'')$, we can deduce that $\sigma(id_t)(''srtc'') = \texttt{true}$.
From $\sigma(id_t)(''srtc'') = \texttt{true}$, we can simplify the term $\texttt{checktc}(\Delta(id_t), \sigma(id_t))$ as follows:

$$\texttt{checktc}(\Delta(id_t), \sigma(id_t)) = (\sigma(id_t)(''A'') = 1) \tag{1.93}$$

Rewriting the goal with (1.93), and simplifying the goal: $\boxed{\sigma(id_t)(''A'') = 1.}$

By definition of $E_c, \tau \vdash s \overset{\downarrow}{\to} s'$, from $t \in Sens(s.M)$ and $s.reset_t(t) = \texttt{true}$, we can deduce $s'.I(t) = 1$. We know that $s'.I(t) \in I_s(t)$, and thus, we have $1 \in I_s(t)$. By definition of $1 \in I_s(t)$, there exist an $a \in \mathbb{N}^*$ and a $ni \in \mathbb{N}^* \sqcup \{\infty\}$ s.t. $I_s(t) = [a, ni]$ and $1 \in [a, ni]$.
By definition of $1 \in [a, ni]$, we have $a \leq 1$, and since $a \in \mathbb{N}^*$, we can deduce $a = 1$.
By construction, $<\texttt{time\_A\_value} \Rightarrow a> \in ipm_t$, and by property of stable σ, we have $\sigma(id_t)(''A'') = a = 1.$

ii. $s.reset_t(t) = \texttt{false}$:

Then, from $s.reset_t(t) = \sigma(id_t)(''srtc'')$, we can deduce that $\sigma(id_t)(''srtc'') = \texttt{false}$.

From $\sigma(id_t)(''srtc'') = \texttt{false}$, we can simplify the term $\texttt{checktc}(\Delta(id_t), \sigma(id_t))$ as follows:

$$\begin{array}{c} \texttt{checktc}(\Delta(id_t), \sigma(id_t)) \\ = \\ \begin{array}{l} (\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_B} \quad . (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1) \\ \qquad\qquad\qquad\qquad\quad\ . (\sigma(id_t)(''stc'') \leq \sigma(id_t)(''B'') - 1)) \\ +(\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_A} \,.\, (\sigma(id_t)(''stc'') = \sigma(id_t)(''A'') - 1)) \\ +(\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_INF} \,.\, (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1)) \end{array} \end{array} \tag{1.94}$$

Let us perform case analysis on $I_s(t)$; there are two cases:

- $I_s(t) = [a, b]$ where $a, b \in \mathbb{N}^*$; then, either $a = b$ or $a \neq b$:
  - $a = b$:
    Then, we have $I_s(t) = [a, a]$, and by construction $<\texttt{transition\_type} \Rightarrow \texttt{TEMP\_A\_A}> \in gm_t$. By property of the elaboration relation, we have $\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_A}$; thus we can simplify the term checktc as follows:

    $$\texttt{checktc}(\Delta(id_t), \sigma(id_t)) = (\sigma(id_t)(''stc'') = \sigma(id_t)(''A'') - 1) \tag{1.95}$$

    Rewriting the goal with (1.95), and simplifying the goal:
    $\boxed{\sigma(id_t)(''stc'') = \sigma(id_t)(''A'') - 1.}$
    From $s'.I(t) \in [a, a]$, we can deduce that $s'.I(t) = a$. Let us perform case analysis on $s.I(t) < upper(I_s(t))$ or $s.I(t) \geq upper(I_s(t))$:
    - $s.I(t) < upper(I_s(t))$:
      By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $s.I(t) = \sigma(id_t)(''stc'')$. By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.I(t) = s.I(t) + 1$. From $s'.I(t) = a$ and $s'.I(t) = s.I(t) + 1$, we can deduce $a - 1 = s.I(t)$.
      By construction, $<\texttt{time\_A\_value} \Rightarrow a> \in ipm_t$, and by property of stable σ, we have $\sigma(id_t)(''A'') = a$.
      Rewriting the goal with $\sigma(id_t)(''A'') = a$ and $s.I(t) = \sigma(id_t)(''stc'')$:
      $\sigma(id_t)(''stc'') = \sigma(id_t)(''A'') - 1.$
    - $s.I(t) \geq upper(I_s(t))$:
      In the case where $s.I(t) > upper(I_s(t))$, then $s.I(t) > a$. By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s.I(t) = s'.I(t) = a$. Then, $a > a$ is a contradiction.

      In the case where $s.I(t) = upper(I_s(t))$, then $s.I(t) = a$. By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.I(t) = s.I(t) + 1$. Then, we have $s'.I(t) = a$ and $s'.I(t) = a + 1$. Then, $a = a + 1$ is a contradiction.
  - $a \neq b$:
    Then, we have $I_s(t) = [a, b]$, and by construction $<\texttt{transition\_type} \Rightarrow \texttt{TEMP\_A\_B}> \in gm_t$. By property of the elaboration relation, we have

$\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_B}$; thus we can simplify the term `checktc` as follows:

$$\texttt{checktc}(\Delta(id_t), \sigma(id_t)) = (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1) \,.\, (\sigma(id_t)(''stc'') \leq \sigma(id_t)(''B'') - 1) \tag{1.96}$$

Rewriting the goal with (1.96), and simplifying the goal:
$\boxed{(\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1) \wedge (\sigma(id_t)(''stc'') \leq \sigma(id_t)(''B'') - 1).}$

Let us perform case analysis on $s.I(t) < upper(I_s(t))$ or $s.I(t) \geq upper(I_s(t))$:

* $s.I(t) < upper(I_s(t))$:
  By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $s.I(t) = \sigma(id_t)(''stc'')$. By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.I(t) = s.I(t) + 1$. By definition of $s'.I(t) \in [a, b]$:
  $\Rightarrow a \leq s'.I(t) \leq b$.
  $\Rightarrow a \leq s'.I(t) \wedge s'.I(t) \leq b$
  $\Rightarrow a \leq s.I(t) + 1 \wedge s.I(t) + 1 \leq b$
  $\Rightarrow a - 1 \leq s.I(t) \wedge s.I(t) \leq b - 1$
  By construction, $<\texttt{time\_A\_value} \Rightarrow a> \in ipm_t$ and $<\texttt{time\_B\_value} \Rightarrow b> \in ipm_t$, and by property of stable σ, we have $\sigma(id_t)(''A'') = a$ and $\sigma(id_t)(''B'') = b$.
  Rewriting the goal with $\sigma(id_t)(''A'') = a$, $\sigma(id_t)(''B'') = b$ and $s.I(t) = \sigma(id_t)(''stc'')$: $a - 1 \leq s.I(t) \wedge s.I(t) \leq b - 1$.
* $s.I(t) \geq upper(I_s(t))$:
  In the case where $s.I(t) > upper(I_s(t))$, then $s.I(t) > b$. By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s.I(t) = s'.I(t) = b$. Then, $b > b$ is a contradiction.

  In the case where $s.I(t) = upper(I_s(t))$, then $s.I(t) = b$. By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.I(t) = s.I(t) + 1$.
  By definition of $s'.I(t) \in [a, b]$, we have $s'.I(t) \leq b$:
  $\Rightarrow s.I(t) + 1 \leq b$
  $\Rightarrow$ $b + 1 \leq b$ is contradiction.

- $I_s(t) = [a, \infty]$ where $a \in \mathbb{N}^*$:
  By construction $<\texttt{transition\_type} \Rightarrow \texttt{TEMP\_A\_INF}> \in gm_t$. By property of the elaboration relation, we have $\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_INF}$; thus we can simplify the term `checktc` as follows:

$$\texttt{checktc}(\Delta(id_t), \sigma(id_t)) = (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1)) \tag{1.97}$$

  Rewriting the goal with (1.97), and simplifying the goal:
  $\boxed{\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1.}$
  From $s'.I(t) \in [a, \infty]$, we can deduce $a \leq s'.I(t)$. Then, let us perform case analysis on $s.I(t) \leq lower(I_s(t))$ or $s.I(t) > lower(I_s(t))$:
  – $s.I(t) \leq lower(I_s(t))$:
    By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $s.I(t) = \sigma(id_t)(''stc'')$.

By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.I(t) = s.I(t) + 1$:
$\Rightarrow a \leq s'.I(t)$
$\Rightarrow a \leq s.I(t) + 1$
$\Rightarrow a - 1 \leq s.I(t)$
By construction, <time_A_value $\Rightarrow a>$ $\in ipm_t$, and by property of stable σ, we have $\sigma(id_t)("A") = a$.
Rewriting the goal with $\sigma(id_t)("A") = a$ and $s.I(t) = \sigma(id_t)("stc")$:
$a - 1 \leq s.I(t)$.

– $s.I(t) > lower(I_s(t))$:
By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $\sigma(id_t)("stc") = lower(I_s(t)) = a$.
By construction, <time_A_value $\Rightarrow a>$ $\in ipm_t$, and by property of stable σ, we have $\sigma(id_t)("A") = a$.
Rewriting the goal with $\sigma(id_t)("stc") = a$ and $\sigma(id_t)("A") = a$: $a - 1 \leq a$.

□

Lemma 12 (Falling Edge Equal Firable 2)**.** *For all sitpn, d, γ, Δ, σ_e, E_c, E_p, τ, s, s', σ, σ_i, $\sigma_\downarrow$, σ' that verify the hypotheses of Def. 1, then $\forall t \in T, id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$, $\sigma'(id_t)("s\_firable") =$ `true` $\Rightarrow t \in Firable(s')$.*

Proof. Given a $t \in T$ and $id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$, and assuming that $\sigma'(id_t)("s\_firable") =$ `true`, let us show $\boxed{t \in Firable(s').}$

By definition of id_t, there exist gm_t, ipm_t, opm_t s.t. $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$.
By property of the $Inject_\downarrow$, the $\mathcal{H}$-VHDL falling edge, the stabilize relations and $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$:

$$\sigma'(id_t)("sfa") = \sigma(id_t)("se") \,.\, \sigma(id_t)("scc") \,.\, \texttt{checktc}(\Delta(id_t), \sigma(id_t)) = \texttt{true} \tag{1.98}$$

From (1.98), we can deduce:

$$\sigma(id_t)("se") = \texttt{true} \tag{1.99}$$
$$\sigma(id_t)("scc") = \texttt{true} \tag{1.100}$$
$$\texttt{checktc}(\Delta(id_t), \sigma(id_t)) = \texttt{true} \tag{1.101}$$

Term $\texttt{checktc}(\Delta(id_t), \sigma(id_t))$ as the same definition as in Lemma Falling Edge Equal Firable 1.
By definition of $t \in Firable(s')$, there are three points to prove:

1. $\boxed{t \in Sens(s'.M)}$
2. $\boxed{t \notin T_i \vee s'.I(t) \in I_s(t)}$
3. $\boxed{\forall c \in \mathcal{C},\ \mathbb{C}(t,c) = 1 \Rightarrow s'.cond(c) = \texttt{true} \text{ and } \mathbb{C}(t,c) = -1 \Rightarrow s'.cond(c) = \texttt{false}}$

Let us prove these three points:

1. $\boxed{t \in Sens(s'.M)}$:

By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s.M = s'.M$. Rewriting the goal with $s.M = s'.M$: $\boxed{t \in Sens(s.M).}$

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $\sigma(id_t)(\text{"se"}) = \texttt{true} \Leftrightarrow t \in Sens(s.M)$.

$t \in Sens(s.M)$.

2. $\boxed{\forall c \in \mathcal{C},\ \mathbb{C}(t,c) = 1 \Rightarrow s'.cond(c) = \texttt{true} \text{ and } \mathbb{C}(t,c) = -1 \Rightarrow s'.cond(c) = \texttt{false}}$

Given a $c \in \mathcal{C}$, there are two points to prove:

(a) $\boxed{\mathbb{C}(t,c) = 1 \Rightarrow s'.cond(c) = \texttt{true}.}$

(b) $\boxed{\mathbb{C}(t,c) = -1 \Rightarrow s'.cond(c) = \texttt{false}.}$

Let us prove these two points:

(a) Assuming that $\mathbb{C}(t,c) = 1$, let us show $\boxed{s'.cond(c) = \texttt{true}.}$

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have:

$$\sigma(id_t)(\text{"scc"}) = \prod_{c \in conds(t)} \begin{cases} E_c(\tau, c) & if\ \mathbb{C}(t,c) = 1 \\ \texttt{not}(E_c(\tau, c)) & if\ \mathbb{C}(t,c) = -1 \end{cases} = \texttt{true} \tag{1.102}$$

where $conds(t) = \{c \in \mathcal{C} \mid \mathbb{C}(t,c) = 1 \vee \mathbb{C}(t,c) = -1\}$.
As $c \in conds(t)$ and $\mathbb{C}(t,c) = 1$, and by definition of the product expression, we have:

$$E_c(\tau, c)\ .\ \prod_{c' \in conds(t) \setminus \{c\}} \begin{cases} E_c(\tau, c') & if\ \mathbb{C}(t,c') = 1 \\ \texttt{not}(E_c(\tau, c')) & if\ \mathbb{C}(t,c') = -1 \end{cases} = \texttt{true} \tag{1.103}$$

From (1.103), we can deduce that $E_c(\tau, c) = \texttt{true}$.
By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.cond(c) = E_c(\tau, c)$.
Rewriting the goal with $s'.cond(c) = E_c(\tau, c)$ and $E_c(\tau, c) = \texttt{true}$: tautology.

(b) Assuming that $\mathbb{C}(t,c) = -1$, let us show $\boxed{s'.cond(c) = \texttt{false}.}$

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have:

$$\sigma(id_t)(\text{"scc"}) = \prod_{c \in conds(t)} \begin{cases} E_c(\tau, c) & if\ \mathbb{C}(t,c) = 1 \\ \texttt{not}(E_c(\tau, c)) & if\ \mathbb{C}(t,c) = -1 \end{cases} = \texttt{true} \tag{1.104}$$

where $conds(t) = \{c \in \mathcal{C} \mid \mathbb{C}(t,c) = 1 \vee \mathbb{C}(t,c) = -1\}$.
As $c \in conds(t)$ and $\mathbb{C}(t,c) = -1$, and by definition of the product expression, we have:

$$\texttt{not}\ E_c(\tau, c)\ .\ \prod_{c' \in conds(t) \setminus \{c\}} \begin{cases} E_c(\tau, c') & if\ \mathbb{C}(t,c') = 1 \\ \texttt{not}(E_c(\tau, c')) & if\ \mathbb{C}(t,c') = -1 \end{cases} = \texttt{true} \tag{1.105}$$

From (1.105), we can deduce that $E_c(\tau, c) = \texttt{false}$.

By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.cond(c) = E_c(\tau, c)$.
Rewriting the goal with $s'.cond(c) = E_c(\tau, c)$ and $E_c(\tau, c) = \texttt{false}$: tautology.

3. $\boxed{t \notin T_i \vee s'.I(t) \in I_s(t)}$

Reasoning on $\texttt{checktc}(\Delta(id_t), \sigma(id_t)) = \texttt{true}$, there are 3 cases:

(a) $\Big(\texttt{not}\ \sigma(id_t)(''srtc'')\ .\ [\dots]\Big) = \texttt{true}$[1]

(b) $\big(\sigma(id_t)(''srtc'')\ .\ \Delta(id_t)(''tt'') \neq \texttt{NOT\_TEMP}\ .\ \sigma(id_t)(''A'') = 1\big) = \texttt{true}$

(c) $\big(\Delta(id_t)(''tt'') = \texttt{NOT\_TEMP}\big) = \texttt{true}$

(a) $\Big(\texttt{not}\ \sigma(id_t)(''srtc'')\ .\ [\dots]\Big) = \texttt{true}$:
Then, we can deduce $\texttt{not}\ \sigma(id_t)(''srtc'') = \texttt{true}$ and $[\dots] = \texttt{true}$. From $\texttt{not}\ \sigma(id_t)(''srtc'') = \texttt{true}$, we can deduce $\sigma(id_t)(''srtc'') = \texttt{false}$, and from $[\dots] = \texttt{true}$, we have three other cases:

i. $\big(\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_B}\ .\ (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1)\ .\ (\sigma(id_t)(''stc'') \leq \sigma(id_t)(''B'') - 1)\big) = \texttt{true}$
ii. $(\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_A}\ .\ (\sigma(id_t)(''stc'') = \sigma(id_t)(''A'') - 1)) = \texttt{true}$
iii. $(\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_INF}\ .\ (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1)) = \texttt{true}$

Let us prove the goal is these three contexts:

i. $\big(\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_B}\ .\ (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1)\ .\ (\sigma(id_t)(''stc'') \leq \sigma(id_t)(''B'') - 1)\big) = \texttt{true}$:
Then, converting boolean equalities into intuitionistic predicates, we have:
- $\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_B}$
- $\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1$
- $\sigma(id_t)(''stc'') \leq \sigma(id_t)(''B'') - 1$

By property of the elaboration relation, and $\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_B}$, there exist $a, b \in \mathbb{N}^*$ s.t. $I_s(t) = [a, b]$. Let us take such an a and b. Then, let us show $\boxed{s'.I(t) \in I_s(t).}$
Rewriting the goal with $I_s(t) = [a, b]$: $\boxed{s'.I(t) \in [a, b].}$
By construction, $<\texttt{time\_A\_value} \Rightarrow a>$ and $<\texttt{time\_B\_value} \Rightarrow b>$, and by property of stable σ, we have $\sigma(id_t)(''A'') = a$ and $\sigma(id_t)(''B'') = b$.
Rewriting the goal with $\sigma(id_t)(''A'') = a$ and $\sigma(id_t)(''B'') = b$, and by definition of $\in$: $\boxed{\sigma(id_t)(''A'') \leq s'.I(t) \leq \sigma(id_t)(''B'').}$
Now, let us perform case analysis on $s.I(t) \leq upper(I_s(t))$ or $s.I(t) > upper(I_s(t))$:
- $s.I(t) \leq upper(I_s(t))$:
  By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $s.I(t) = \sigma(id_t)(''stc'')$.
  From $\sigma(id_t)(''se'') = \texttt{true}$, we can deduce $t \in Sens(s.M)$, and from $\sigma(id_t)(''srtc'') = \texttt{false}$, we can deduce $s.reset_t(t) = \texttt{false}$. Then, by definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.I(t) = s.I(t) + 1$.

[1] See equation (1.90) for the full definition

$\Rightarrow$ $\boxed{\sigma(id_t)(''A'') \leq s.I(t) + 1 \leq \sigma(id_t)(''B'')}$ (by $s'.I(t) = s.I(t) + 1$)

$\Rightarrow$ $\boxed{\sigma(id_t)(''A'') \leq \sigma(id_t)(''stc'') + 1 \leq \sigma(id_t)(''B'')}$ (by $s.I(t) = \sigma(id_t)(''stc'')$)

$\Rightarrow$ $\sigma(id_t)(''A'') - 1 \leq \sigma(id_t)(''stc'') \leq \sigma(id_t)(''B'') - 1$

- $s.I(t) > upper(I_s(t))$:

  By definition of $\gamma, E_c, \tau \vdash s \overset{\updownarrow}{\sim} \sigma$, we have $\sigma(id_t)(''stc'') = upper(I_s(t)) = b$.
  Then, from $\sigma(id_t)(''stc'') \leq \sigma(id_t)(''B'') - 1$, $\sigma(id_t)(''stc'') = upper(I_s(t)) = b$ and $\sigma(id_t)(''B'') = b$, we can deduce the following contradiction:
  $\sigma(id_t)(''B'') \leq \sigma(id_t)(''B'') - 1$.

ii. $(\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_A} \,.\, (\sigma(id_t)(''stc'') = \sigma(id_t)(''A'') - 1)) = \texttt{true}$:
Then, converting boolean equalities into intuitionistic predicates, we have:

- $\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_A}$
- $\sigma(id_t)(''stc'') = \sigma(id_t)(''A'') - 1$

By property of the elaboration relation, and $\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_A}$, there exist $a \in \mathbb{N}^*$ s.t. $I_s(t) = [a, a]$. Let us take such an a. Then, let us show $\boxed{s'.I(t) \in I_s(t).}$
Rewriting the goal with $I_s(t) = [a, a]$: $\boxed{s'.I(t) \in [a, a].}$
By construction, $<\texttt{time\_A\_value} \Rightarrow a>$, and by property of stable σ, we have $\sigma(id_t)(''A'') = a$.
Rewriting the goal with $\sigma(id_t)(''A'') = a$, unfolding the definition of $\in$, and simplifying the goal: $\boxed{s'.I(t) = \sigma(id_t)(''A'').}$
Now, let us perform case analysis on $s.I(t) \leq upper(I_s(t))$ or $s.I(t) > upper(I_s(t))$:

- $s.I(t) \leq upper(I_s(t))$:

  By definition of $\gamma, E_c, \tau \vdash s \overset{\updownarrow}{\sim} \sigma$, we have $s.I(t) = \sigma(id_t)(''stc'')$.
  From $\sigma(id_t)(''se'') = \texttt{true}$, we can deduce $t \in Sens(s.M)$, and from $\sigma(id_t)(''srtc'') = \texttt{false}$, we can deduce $s.reset_t(t) = \texttt{false}$. Then, by definition of $E_c, \tau \vdash s \overset{\downarrow}{\rightarrow} s'$, we have $s'.I(t) = s.I(t) + 1$.

  $\Rightarrow$ $\boxed{s.I(t) + 1 = \sigma(id_t)(''A'')}$ (by $s'.I(t) = s.I(t) + 1$)

  $\Rightarrow$ $\boxed{\sigma(id_t)(''stc'') + 1 = \sigma(id_t)(''A'')}$ (by $s.I(t) = \sigma(id_t)(''stc'')$)

  $\Rightarrow$ $\sigma(id_t)(''stc'') = \sigma(id_t)(''A'') - 1$

- $s.I(t) > upper(I_s(t))$:

  By definition of $\gamma, E_c, \tau \vdash s \overset{\updownarrow}{\sim} \sigma$, we have $\sigma(id_t)(''stc'') = upper(I_s(t)) = a$.
  Then, from $\sigma(id_t)(''stc'') = \sigma(id_t)(''A'') - 1$, $\sigma(id_t)(''stc'') = upper(I_s(t)) = a$, $\sigma(id_t)(''A'') = a$, and $a \in \mathbb{N}^*$, we can deduce the following contradiction:
  $\sigma(id_t)(''A'') = \sigma(id_t)(''A'') - 1$.

iii. $(\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_INF} \,.\, (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1)) = \texttt{true}$:
Then, converting boolean equalities into intuitionistic predicates, we have:

- $\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_INF}$
- $\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1$

By property of the elaboration relation, and $\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_INF}$, there exist $a \in \mathbb{N}^*$ s.t. $I_s(t) = [a, \infty]$. Let us take such an a. Then, let us show $\boxed{s'.I(t) \in I_s(t).}$
Rewriting the goal with $I_s(t) = [a, \infty]$: $\boxed{s'.I(t) \in [a, \infty].}$

By construction, $<$`time_A_value` $\Rightarrow a>$, and by property of stable σ, we have $\sigma(id_t)(''A'') = a$.
Rewriting the goal with $\sigma(id_t)(''A'') = a$, unfolding the definition of $\in$, and simplifying the goal: $\boxed{\sigma(id_t)(''A'') \leq s'.I(t).}$
Now, let us perform case analysis on $s.I(t) \leq lower(I_s(t))$ or $s.I(t) > lower(I_s(t))$:

- $s.I(t) \leq lower(I_s(t))$:
  By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $s.I(t) = \sigma(id_t)(''stc'')$.
  From $\sigma(id_t)(''se'') =$ `true`, we can deduce $t \in Sens(s.M)$, and from $\sigma(id_t)(''srtc'') =$ `false`, we can deduce $s.reset_t(t) =$ `false`. Then, by definition of $E_c, \tau \vdash s \overset{\downarrow}{\rightarrow} s'$, we have $s'.I(t) = s.I(t) + 1$.
  $\Rightarrow$ $\boxed{\sigma(id_t)(''A'') \leq s.I(t) + 1}$ (by $s'.I(t) = s.I(t) + 1$)
  $\Rightarrow$ $\boxed{\sigma(id_t)(''A'') \leq \sigma(id_t)(''stc'') + 1}$ (by $s.I(t) = \sigma(id_t)(''stc'')$)
  $\Rightarrow$ $\sigma(id_t)(''A'') - 1 \leq \sigma(id_t)(''stc'')$
- $s.I(t) > lower(I_s(t))$:
  By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $\sigma(id_t)(''stc'') = lower(I_s(t)) = a$.
  From $\sigma(id_t)(''se'') =$ `true`, we can deduce $t \in Sens(s.M)$, and from $\sigma(id_t)(''srtc'') =$ `false`, we can deduce $s.reset_t(t) =$ `false`. Then, by definition of $E_c, \tau \vdash s \overset{\downarrow}{\rightarrow} s'$, we have $s'.I(t) = s.I(t) + 1$.
  $\Rightarrow$ $\boxed{\sigma(id_t)(''A'') \leq s.I(t) + 1}$ (by $s'.I(t) = s.I(t) + 1$)
  $\Rightarrow$ $\boxed{a \leq s.I(t) + 1}$ (by $\sigma(id_t)(''A'') = a$)
  $\Rightarrow$ $\boxed{a < s.I(t)}$
  $\Rightarrow$ $lower(I_s(t)) < s.I(t)$

(b) $\big(\sigma(id_t)(''srtc'') \,.\, \Delta(id_t)(''tt'') \neq$ `NOT_TEMP` $\,.\, \sigma(id_t)(''A'') = 1\big) =$ `true`
Then, converting boolean equalities into intuitionistic predicates, we have:

- $\sigma(id_t)(''srtc'') =$ `true`
- $\Delta(id_t)(''tt'') \neq$ `NOT_TEMP`
- $\sigma(id_t)(''A'') = 1$

By property of the elaboration relation, and $\Delta(id_t)(''tt'') \neq$ `NOT_TEMP`, there exist an $a \in \mathbb{N}^*$ and a $ni \in \mathbb{N}^* \sqcup \{\infty\}$ s.t. $I_s(t) = [a, ni]$. Let us take such an a and ni.
By construction, $<$`time_A_value` $\Rightarrow a> \in ipm_t$, and by property of stable σ, we have $\sigma(id_t)(''A'') = a$. Thus, we can deduce $a = 1$ and $I_s(t) = [1, ni]$.
By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, from $\sigma(id_t)(''se'') =$ `true`, we can deduce $t \in Sens(s.M)$, and from $\sigma(id_t)(''srtc'') =$ `true`, we can deduce $s.reset_t(t) =$ `true`.
By definition of $E_c, \tau \vdash s \overset{\downarrow}{\rightarrow} s'$, $t \in Sens(s.M)$ and $s.reset_t(t) =$ `true`, we have $s'.I(t) = 1$.
Now, let us show $\boxed{s'.I(t) \in I_s(t)}$.
Rewriting the goal with $s'.I(t) = 1$ and $I_s(t) = [1, ni]$: $1 \in [1, ni]$.

(c) $\big(\Delta(id_t)(''tt'') =$ `NOT_TEMP`$\big) =$ `true`
Let us show $\boxed{t \notin T_i.}$

By property of the elaboration relation and $\Delta(id_t)(\text{"}tt\text{"}) = \texttt{NOT\_TEMP}$, we have $t \notin T_i$.

□

1.7 A detailled proof: equivalence of fired transitions

Appendix A

Reminder on natural semantics

Appendix B

Reminder on induction principles

- Present all the material that will be used in the proof, and that needs clarifying for people who do not come from the field (e.g, automaticians and electronicians)
  - structural induction
  - induction on relations
  - ...