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 23, 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.

1.1 Preliminary Definitions

1.2 Behavior Preservation Theorem

1.3 Initial States

1.4 First Rising Edge

1.5 Rising Edge

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

- $\lfloor sitpn \rfloor_{\mathcal{H}} = (d, \gamma)$ *and* $\gamma \vdash E_p \overset{env}{=} E_c$ *and* $\mathcal{D}_{\mathcal{H}}, \emptyset \vdash \mathrm{d} \xrightarrow{elab} \Delta, \sigma_e$
- $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$
- $E_c, \tau \vdash s \xrightarrow{\uparrow} s'$
- $\texttt{Inject}_{\uparrow}(\sigma, E_p, \tau, \sigma_i)$ *and* $\mathcal{D}_{\mathcal{H}}, \Delta, \sigma_i \vdash \mathrm{d.cs} \xrightarrow{\uparrow} \sigma_\uparrow$ *and* $\mathcal{D}_{\mathcal{H}}, \Delta, \sigma_\uparrow \vdash \mathrm{d.cs} \xrightarrow{\rightsquigarrow} \sigma'$
- *State* σ *is a stable design state:* $\mathcal{D}_{\mathcal{H}}, \Delta, \sigma \vdash \mathrm{d.cs} \xrightarrow{comb} \sigma$

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

Proof. By definition of **??**, there are 7 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. $\forall a \in \mathcal{A}, id_a \in Outs(\Delta)\ s.t.\ \gamma(a) = id_a,\ s'.ex(a) = \sigma'(id_a)$.
5. $\forall f \in \mathcal{F}, id_f \in Outs(\Delta)\ s.t.\ \gamma(f) = id_f,\ s'.ex(f) = \sigma'(id_f)$.
6. $\forall t \in T, id_t \in Comps(\Delta)\ s.t.\ \gamma(t) = id_t, t \in Sens(s'.M) \Leftrightarrow \sigma'(id_t)(\text{"s\_enabled"}) = \texttt{true}$.
7. $\forall t \in T, id_t \in Comps(\Delta)\ s.t.\ \gamma(t) = id_t, t \notin Sens(s'.M) \Leftrightarrow \sigma'(id_t)(\text{"s\_enabled"}) = \texttt{false}$.
8. $\forall t \in T, id_t \in Comps(\Delta)\ s.t.\ \gamma(t) = id_t,$
   $\sigma'(id_t)(\text{"s\_condition\_combination"}) = \prod_{c \in conds(t)} \begin{cases} E_c(\tau, c) & if\ \mathbb{C}(t,c) = 1 \\ \texttt{not}(E_c(\tau,c)) & if\ \mathbb{C}(t,c) = -1 \end{cases}$
   where $conds(t) = \{c \in \mathcal{C} \mid \mathbb{C}(t,c) = 1 \vee \mathbb{C}(t,c) = -1\}$.

Each point is proved by a separate lemma:

- Apply Lemma Rising Edge Equal Marking to solve 1.
- Apply Lemma Rising Edge Equal Time Counters lemma to solve 2.
- Apply Lemma Rising Edge Equal Reset Orders to solve 3.
- Apply Lemma Rising Edge Equal Action Executions to solve 4.
- Apply Lemma Rising Edge Equal Function Executions to solve 5.
- Apply Lemma Rising Edge Equal Sensitized to solve 6.
- Apply Lemma Rising Edge Equal Not Sensitized to solve 7.
- Apply Lemma Rising Edge Equal Condition Combination to solve 8.

□

1.5.1 Rising Edge and Marking

Lemma 2 (Rising Edge Equal Marking). *For all sitpn, $d, \gamma, E_c, E_p, \tau, \Delta, \sigma_e, s, s', \sigma, \sigma_i, \sigma_\uparrow, \sigma'$ that verify the hypotheses of Def. 1, then $\forall p, id_p$ s.t. $\gamma(p) = id_p$ and $\sigma'(id_p) = \sigma'_p$, $s'.M(p) = \sigma'_p(\text{"s\_marking"})$.*

Proof. Given a $p \in P$, let us show $\boxed{s'.M(p) = \sigma'(id_p)(\text{"s\_marking"})}$.

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 definition of the SITPN state transition relation on rising edge:

$$s'.M(p) = s.M(p) - \sum_{t \in Fired(s)} pre(p,t) + \sum_{t \in Fired(s)} post(t,p) \tag{1.1}$$

By property of the $\texttt{Inject}_{\uparrow}$, the $\mathcal{H}$-VHDL rising edge and the stabilize relations, and $\texttt{comp}(id_p, "place", gm_p, ipm$ $d.cs$:

$$\begin{aligned}\sigma'(id_p)("sm") = \sigma(id_p)("sm") - \sigma(id_p)("s\_output\_token\_sum") \\ +\sigma(id_p)("s\_input\_token\_sum")\end{aligned} \tag{1.2}$$

By the definition of **??** relation:

$$s.M(p) = \sigma(id_p)("sm") \tag{1.3}$$

$$\sum_{t \in Fired(s)} pre(p,t) = \sigma(id_p)("sots") \tag{1.4}$$

$$\sum_{t \in Fired(s)} post(t,p) = \sigma(id_p)("sits") \tag{1.5}$$

Rewriting the goal with 1.1, 1.2, 1.3, 1.4 and 1.5, tautology .

□

1.5.2 Rising edge and condition combination

Lemma 3 (Rising Edge Equal Condition Combination). *For all sitpn, d, γ, E_c, E_p, τ, Δ, σ_e, s, s', σ, σ_i, $\sigma_{\uparrow}$, σ' that verify the hypotheses of Def. 1, then*
$\forall t \in T, id_t \in Comps(\Delta)$ *s.t.* $\gamma(t) = id_t$,

$$\sigma'(id_t)("s\_condition\_combination") = \prod_{c \in conds(t)} \begin{cases} E_c(\tau,c) & if\ \mathbb{C}(t,c) = 1 \\ \texttt{not}(E_c(\tau,c)) & if\ \mathbb{C}(t,c) = -1 \end{cases}$$

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

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

$$\boxed{\sigma'(id_t)("s\_condition\_combination") = \prod_{c \in conds(t)} \begin{cases} E_c(\tau,c) & if\ \mathbb{C}(t,c) = 1 \\ \texttt{not}(E_c(\tau,c)) & if\ \mathbb{C}(t,c) = -1 \end{cases}.}$$

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 $\mathcal{H}$-VHDL stabilize relation, and
$\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$:

$$\sigma'(id_t)("scc") = \prod_{i=0}^{\Delta(id_t)("conditions\_number")-1} \sigma'(id_t)("input\_conditions")[i] \tag{1.6}$$

Rewriting the goal with 1.6,

$$\boxed{\prod_{i=0}^{\Delta(id_t)("cn")-1} \sigma'(id_t)("ic")[i] = \prod_{c \in conds(t)} \begin{cases} E_c(\tau,c) & if\ \mathbb{C}(t,c) = 1 \\ \texttt{not}(E_c(\tau,c)) & if\ \mathbb{C}(t,c) = -1 \end{cases}.}$$

Case analysis on $conds(t)$ (2 CASES):

- **CASE** $conds(t) = \emptyset$:

$$\boxed{\prod_{i=0}^{\Delta(id_t)(\text{"}cn\text{"})-1} \sigma'(id_t)(\text{"}ic\text{"})[i] = \texttt{true}.}$$

By construction, $<\texttt{conditions\_number} \Rightarrow \texttt{1}> \in gm_t$ and $<\texttt{input\_conditions}(\texttt{0}) \Rightarrow \texttt{true}> \in ipm_t$.

By property of the stabilize relation, $<\texttt{conditions\_number} \Rightarrow \texttt{1}> \in gm_t$ and $<\texttt{input\_conditions}(\texttt{0}) \Rightarrow \texttt{tr}$ ipm_t:

$$\Delta(id_t)(\text{"}cn\text{"}) = 1 \tag{1.7}$$
$$\sigma'(id_t)(\text{"}ic\text{"})[0] = \texttt{true} \tag{1.8}$$

Rewriting the goal with 1.7 and 1.8, tautology.

- **CASE** $conds(t) \neq \emptyset$:
By construction, $<\texttt{conditions\_number} \Rightarrow |\texttt{conds(t)}|> \in gm_t$, and by property of the stabilize relation:

$$\Delta(id_t)(\text{"}cn\text{"}) = |conds(t)| \tag{1.9}$$

Rewriting the goal with (1.9),

$$\boxed{\prod_{i=0}^{|conds(t)|-1} \sigma'(id_t)(\text{"}ic\text{"})[i] = \prod_{c \in conds(t)} \begin{cases} E_c(\tau, c) & if\ \mathbb{C}(t,c) = 1 \\ \texttt{not}(E_c(\tau, c)) & if\ \mathbb{C}(t,c) = -1 \end{cases}.}$$

Applying Theorem **??**, there are two points to prove:

1. $|conds(t)| = |conds(t)|$
2. $\exists$ an injection $\iota \in [0, |conds(t)| - 1] \to conds(t)$ s.t.
$\forall i \in [0, |conds(t)| - 1]$, $\sigma'(id_t)(\text{"}ic\text{"})[i] = \begin{cases} E_c(\tau, \iota(i)) & if\ \mathbb{C}(t,\iota(i)) = 1 \\ \texttt{not}(E_c(\tau, \iota(i))) & if\ \mathbb{C}(t,\iota(i)) = -1 \end{cases}$

By construction, there exists a bijection $\beta \in [0, |conds(t)| - 1] \to conds(t)$ such that for all $i \in [0, |conds(t)| - 1]$, there exists an $id_c \in Ins(\Delta)$ and:

- $\gamma(\beta(i)) = id_c$
- $\mathbb{C}(t, \beta(i)) = 1$ implies $<\texttt{input\_conditions(i)} \Rightarrow \texttt{id}_\texttt{c}> \in ipm_t$
- $\mathbb{C}(t, \beta(i)) = -1$ implies $<\texttt{input\_conditions(i)} \Rightarrow \texttt{not id}_\texttt{c}> \in ipm_t$

Let us take such a bijection β to prove the goal. Then, given an $i \in [0, |conds(t)| - 1]$, let us show $\boxed{\sigma'(id_t)(\text{"}ic\text{"})[i] = \begin{cases} E_c(\tau, \beta(i)) & if\ \mathbb{C}(t,\beta(i)) = 1 \\ \texttt{not}(E_c(\tau, \beta(i))) & if\ \mathbb{C}(t,\beta(i)) = -1 \end{cases}}$

By definition of $\beta(i) \in conds(t)$:

$$\mathbb{C}(t, \beta(i)) = 1 \vee \mathbb{C}(t, \beta(i)) = -1 \tag{1.10}$$

Case analysis on (1.10):

– **CASE** $\mathbb{C}(t, \beta(i)) = 1$: $\boxed{\sigma'(id_t)(''ic'')[i] = E_c(\tau, \beta(i))}$

By property of β, there exists $id_c \in Ins(\Delta)$ s.t. $\gamma(\beta(i)) = id_c$ and
$<\texttt{input\_conditions(i)} \Rightarrow \texttt{id}_\texttt{c}> \in ipm_t$.
By property of the stabilize relation and $<\texttt{input\_conditions(i)} \Rightarrow \texttt{id}_\texttt{c}> \in ipm_t$:

$$\sigma'(id_t)(''ic'')[i] = \sigma'(id_c) \tag{1.11}$$

By property of the $\mathcal{H}$-VHDL rising edge and stabilize relations, and $id_c \in Ins(\Delta)$:

$$\sigma'(id_c) = \sigma_i(id_c) \tag{1.12}$$

By property of the $\texttt{Inject}_\uparrow$ relation and $id_c \in Ins(\Delta)$:

$$\sigma_i(id_c) = E_p(\tau, \uparrow)(id_c) \tag{1.13}$$

By property of $\gamma \vdash E_p \overset{env}{=} E_c$:

$$E_p(\tau, \uparrow)(id_c) = E_c(\tau, c) \tag{1.14}$$

Rewriting the goal with (1.11), (1.12), (1.13), (1.14), tautology.

– **CASE** $\mathbb{C}(t, c) = -1$: $\boxed{\sigma'(id_t)(''ic'')[i] = \texttt{not } E_c(\tau, \beta(i))}$
By property of β, there exists $id_c \in Ins(\Delta)$ s.t. $\gamma(\beta(i)) = id_c$ and
$<\texttt{input\_conditions(i)} \Rightarrow \texttt{not id}_\texttt{c}> \in ipm_t$.
By property of the stabilize relation and $<\texttt{input\_conditions(i)} \Rightarrow \texttt{not id}_\texttt{c}> \in ipm_t$:

$$\sigma'(id_t)(''ic'')[i] = \texttt{not } \sigma'(id_c) \tag{1.15}$$

Then, equations (1.12), (1.13) and (1.14) also hold this case.
Rewriting the goal with (1.15), (1.12), (1.13) and (1.14), tautology.

□

1.5.3 Rising edge and time counters

Lemma 4 (Rising Edge Equal Time Counters). *For all sitpn, d, γ, E_c, E_p, τ, Δ, σ_e, s, s', σ, σ_i, $\sigma_\uparrow$, 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

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

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

Then, there are 4 points to show:

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

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

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

   $$\sigma'(id_t)(\text{"s\_time\_counter"}) = \sigma(id_t)(\text{"s\_time\_counter"}) \tag{1.16}$$

   By property of $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$:

   $$\sigma(id_t)(\text{"s\_time\_counter"}) = lower(I_s(t)) \tag{1.17}$$

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

2. Proved in the same fashion as 1.
3. Proved in the same fashion as 1.
4. Proved in the same fashion as 1.

□

1.5.4 Rising edge and reset orders

Lemma 5 (Rising Edge Equal Reset Orders). *For all $sitpn$, d, γ, E_c, E_p, τ, Δ, σ_e, s, s', σ, σ_i, $\sigma_{\uparrow}$, σ' that verify the hypotheses of Def. 1, then*
$\forall t \in T_i, id_t \in Comps(\Delta)$ *s.t.* $\gamma(t) = id_t, s'.reset_t(t) = \sigma'(id_t)(\text{"s\_reinit\_time\_counter"})$

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

$$\sigma'(id_t)(\text{"srtc"}) = \sum_{i=0}^{\Delta(id_t)(\text{"input\_arcs\_number"})-1} \sigma'(id_t)(\text{"reinit\_time"})[i] \tag{1.18}$$

Rewriting the goal with (1.18), $\boxed{s'.reset_t(t) = \sum_{i=0}^{\Delta(id_t)("ian")-1} \sigma'(id_t)("rt")[i].}$

Case analysis on $input(t)$ (2 CASES):

- **CASE** $input(t) = \emptyset$:

  By construction, $<\texttt{input\_arcs\_number} \Rightarrow \texttt{1}> \in gm_t$, and by property of the elaboration relation:

  $$\Delta(id_t)("ian") = 1 \tag{1.19}$$

  By construction, there exists an $id_{ft} \in Sigs(\Delta)$ s.t. $<\texttt{reinit\_time(0)} \Rightarrow \texttt{id}_{\texttt{ft}}> \in ipm_t$ and $<\texttt{fired} \Rightarrow \texttt{id}_{\texttt{ft}}> \in opm_t$, and by property of the $\mathcal{H}$-VHDL stabilize relation and $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$:

  $$\sigma'(id_t)("rt")[0] = \sigma'(id_{ft}) \tag{1.20}$$
  $$\sigma'(id_{ft}) = \sigma'(id_t)("fired") \tag{1.21}$$
  $$\sigma'(id_t)("fired") = \sigma'(id_t)("s\_fired") \tag{1.22}$$
  $$\sigma'(id_t)("s\_fired") = \sigma'(id_t)("s\_firable").\sigma'(id_t)("s\_priority\_combination") \tag{1.23}$$

  Rewriting the goal with (1.20), (1.35), (1.22) and (1.23),
  $\boxed{s'.reset_t(t) = \sigma'(id_t)("s\_firable").\sigma'(id_t)("s\_priority\_combination").}$
  By property of the stabilize relation, and $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$:

  $$\sigma'(id_t)("spc") = \prod_{i=0}^{\Delta(id_t)("ian")-1} \sigma'(id_t)("priority\_authorizations")[i] \tag{1.24}$$

  By construction, $<\texttt{priority\_authorizations(0)} \Rightarrow \texttt{true}> \in ipm_t$, and by property of the stabilize relation and $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$:

  $$\sigma'(id_t)("priority\_authorizations")[0] = true \tag{1.25}$$

  Rewriting the goal with (1.19), (1.24) and (1.25), and simplifying the equation,
  $\boxed{s'.reset_t(t) = \sigma'(id_t)("s\_firable").}$
  Case analysis on $t \in Fired(s)$ or $t \notin Fired(s)$:

  - **CASE** $t \in Fired(s)$:

    By property of $E_c, \tau \vdash s \xrightarrow{\uparrow} s'$:

    $$s'.reset_t(t) = \texttt{true} \tag{1.26}$$

    Rewriting the goal with (1.26), $\boxed{\sigma'(id_t)("s\_firable") = \texttt{true}.}$
    By property of the stabilize, the $\mathcal{H}$-VHDL rising edge and the $\texttt{Inject}_{\uparrow}$ relations, and $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$:

    $$\sigma(id_t)("s\_firable") = \sigma'(id_t)("s\_firable") \tag{1.27}$$

Rewriting the goal with (1.27), $\boxed{\sigma(id_t)(\text{"}s\_firable\text{"}) = \texttt{true}.}$

By property of $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$:

$$t \in Firable(s) \Leftrightarrow \sigma(id_t)(\text{"}sfa\text{"}) = \texttt{true} \tag{1.28}$$

Rewriting the goal with (1.28), $\boxed{t \in Firable(s).}$

By property of $t \in Fired(s)$, $t \in Firable(s)$.

– **CASE** $t \notin Fired(s)$:
By property of $input(t) = \emptyset$, there does not exist any input place connected to t by a `basic` or `test` arc. Thus, by property of $E_c, \tau \vdash s \xrightarrow{\uparrow} s'$:

$$s'.reset_t(t) = \texttt{false} \tag{1.29}$$

Rewriting the goal with (1.29), $\boxed{\sigma'(id_t)(\text{"}s\_firable\text{"}) = \texttt{false}.}$
By property of the stabilize, the $\mathcal{H}$-VHDL rising edge and the $\texttt{Inject}_{\uparrow}$ relations, and $\texttt{comp}(id_t, \text{"}transition\text{"}, gm_t, ipm_t, opm_t) \in d.cs$, equation (1.27) holds.
Rewriting the goal with (1.27), $\boxed{\sigma(id_t)(\text{"}s\_firable\text{"}) = false.}$

By property of $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$:

$$t \notin Firable(s) \Leftrightarrow \sigma(id_t)(\text{"}sfa\text{"}) = \texttt{false} \tag{1.30}$$

By property of $t \notin Fired(s)$ and $input(t) = \emptyset$, $t \notin Firable(s)$.

- **CASE** $input(t) \neq \emptyset$:

By construction, $<\texttt{input\_arcs\_number} \Rightarrow |input(t)|> \in gm_t$, and by property of the $\mathcal{H}$-VHDL elaboration relation:

$$\Delta(id_t)(\text{"}ian\text{"}) = |input(t)| \tag{1.31}$$

Rewriting the goal with (1.31), $\boxed{s'.reset_t(t) = \sum_{i=0}^{|input(t)|-1} \sigma'(id_t)(\text{"}rt\text{"})[i].}$

Case analysis on $t \in Fired(s)$ or $t \notin Fired(s)$:

– **CASE** $t \in Fired(s)$:

By property of $E_c, \tau \vdash s \xrightarrow{\uparrow} s'$, equation (1.26) holds.

Rewriting the goal with (1.26), $\boxed{\sum_{i=0}^{|input(t)|-1} \sigma'(id_t)(\text{"}rt\text{"})[i] = \texttt{true}.}$

To prove the goal, let us show $\boxed{\exists i \in [0, |input(t)| - 1] \text{ s.t. } \sigma'(id_t)(\text{"}rt\text{"})[i] = \texttt{true}.}$

By construction, and $input(t) \neq \emptyset$, there exist $p \in input(t)$ and $id_p \in Comps(\Delta)$ s.t. $\gamma(p) = id_p$.

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 construction, there exist an $i \in [0, |input(t)| - 1]$, a $j \in [0, |output(p)| - 1]$ and $id_{ji} \in Sigs(\Delta)$ s.t. $<\texttt{reinit\_transition\_time(j)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in opm_p$ and $<\texttt{reinit\_time(i)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in ipm_t$. Let us take such an i, j and id_{ji}, and let us use i to prove the goal: $\boxed{\sigma'(id_t)("rt")[i] = \texttt{true}.}$

By property of the stabilize relation, $<\texttt{reinit\_transition\_time(j)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in opm_p$ and $<\texttt{reinit\_time(i)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in ipm_t$:

$$\sigma'(id_t)("rt")[i] = \sigma'(id_{ji}) = \sigma'(id_p)("rtt")[j] \tag{1.32}$$

Rewriting the goal with (1.32), $\boxed{\sigma'(id_p)("rtt")[j] = \texttt{true}.}$

By property of the $\texttt{Inject}_{\uparrow}$, the $\mathcal{H}$-VHDL rising edge and the stabilize relations:

$$\begin{aligned}\sigma'(id_p)("rtt")[j] = &((\sigma(id_p)("oat")[j] = \texttt{BASIC} + \sigma(id_p)("oat")[j] = \texttt{TEST})\\ &.(\sigma(id_p)("sm") - \sigma(id_p)("sots") < \sigma(id_p)("oaw")[j])\\ &.(\sigma(id_p)("sots") > 0))\\ &+ \sigma(id_p)("otf")[j]\end{aligned} \tag{1.33}$$

Rewriting the goal with (1.33),

$$\boxed{\begin{aligned}\texttt{true} = &((\sigma(id_p)("oat")[j] = \texttt{BASIC} + \sigma(id_p)("oat")[j] = \texttt{TEST})\\ &.(\sigma(id_p)("sm") - \sigma(id_p)("sots") < \sigma(id_p)("oaw")[j])\\ &.(\sigma(id_p)("sots") > 0))\\ &+ (\sigma(id_p)("otf")[j])\end{aligned}}$$

By construction, there exists $id_{ft} \in Sigs(\Delta)$ s.t. $<\texttt{output\_transitions\_fired(j)} \Rightarrow \texttt{id}_{\texttt{ft}}> \in ipm_p$ and $<\texttt{fired} \Rightarrow \texttt{id}_{\texttt{ft}}> \in opm_t$. By property of state σ as being a stable state:

$$\sigma(id_t)("fired") = \sigma(id_{ft}) = \sigma(id_p)("otf")[j] \tag{1.34}$$

Rewriting the goal with (1.34),

$$\boxed{\begin{aligned}\texttt{true} = &((\sigma(id_p)("oat")[j] = \texttt{BASIC} + \sigma(id_p)("oat")[j] = \texttt{TEST})\\ &.(\sigma(id_p)("sm") - \sigma(id_p)("sots") < \sigma(id_p)("oaw")[j])\\ &.(\sigma(id_p)("sots") > 0))\\ &+ \sigma(id_t)("fired")\end{aligned}}$$

By property of $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$:

$$t \in Fired(s) \Leftrightarrow \sigma(id_t)("fired") = \texttt{true} \tag{1.35}$$

Knowing that $t \in Fired(s)$, we can rewrite the goal with the right side of (1.35) and simplify the goal (i.e, $\forall b \in \mathbb{B},\ b + \texttt{true} = \texttt{true}$), then tautology.

– **CASE** $t \notin Fired(s)$: Then, there are two cases that will determine the value of $s'.reset_t(t)$. Either there exists a place p with an output token sum greater than zero, that is connected to t by an `basic` or `test` arc, and such that the transient marking of p disables t; or such a place does not exist (the predicate is decidable).

  * **CASE** there exists such a place p as described above:

    Then, let us take such a place p and $\omega \in \mathbb{N}^*$ s.t.:
    1. $\sum_{t_i \in Fired(s)} pre(p, t_i) > 0$
    2. $pre(p,t) = (\omega, \texttt{basic}) \vee pre(p,t) = (\omega, \texttt{test})$
    3. $s.M(p) - \sum_{t_i \in Fired(s)} pre(p, t_i) < \omega$

    We will only consider the case where $pre(p,t) = (\omega, \texttt{basic})$; the proof is the similar when $pre(p,t) = (\omega, \texttt{test})$.
    Assuming that p exists, and by property of $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$:

    $$s'.reset_t(t) = \texttt{true} \tag{1.36}$$

    Rewriting the goal with (1.36), $\boxed{\sum_{i=0}^{|input(t)|-1} \sigma'(id_t)(''rt'')[i] = \texttt{true}.}$
    To prove the goal, let us show $\boxed{\exists i \in [0, |input(t)| - 1] \text{ s.t. } \sigma'(id_t)(''rt'')[i] = \texttt{true}.}$
    By construction, there exists $id_p \in Comps(\Delta)$ s.t. $\gamma(p) = id_p$.
    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 construction, there exist an $i \in [0, |input(t)| - 1]$, a $j \in [0, |output(p)| - 1]$ and $id_{ji} \in Sigs(\Delta)$ s.t. $<\texttt{reinit\_transition\_time(j)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in opm_p$ and $<\texttt{reinit\_time(i)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in ipm_t$. Let us take such an i, j and id_{ji}, and let us use i to prove the goal: $\boxed{\sigma'(id_t)(''rt'')[i] = \texttt{true}.}$
    By property of the stabilize relation, $<\texttt{reinit\_transition\_time(j)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in opm_p$ and $<\texttt{reinit\_time(i)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in ipm_t$:

    $$\sigma'(id_t)(''rt'')[i] = \sigma'(id_{ji}) = \sigma'(id_p)(''rtt'')[j] \tag{1.37}$$

    Rewriting the goal with (1.37), $\boxed{\sigma'(id_p)(''rtt'')[j] = \texttt{true}.}$
    By property of the $\texttt{Inject}_\uparrow$, the $\mathcal{H}$-VHDL rising edge and the stabilize relations:

    $$\begin{aligned}\sigma'(id_p)(''rtt'')[j] = &\big((\sigma(id_p)(''oat'')[j] = \texttt{BASIC} + \sigma(id_p)(''oat'')[j] = \texttt{TEST})\\ &.(\sigma(id_p)(''sm'') - \sigma(id_p)(''sots'') < \sigma(id_p)(''oaw'')[j])\\ &.(\sigma(id_p)(''sots'') > 0)\big)\\ &+ \sigma(id_p)(''otf'')[j]\end{aligned} \tag{1.38}$$

Rewriting the goal with (1.38),

$$\boxed{\begin{aligned}\texttt{true} =&((\sigma(id_p)(''oat'')[j] = \texttt{BASIC} + \sigma(id_p)(''oat'')[j] = \texttt{TEST})\\ &.(\sigma(id_p)(''sm'') - \sigma(id_p)(''sots'') < \sigma(id_p)(''oaw'')[j])\\ &.(\sigma(id_p)(''sots'') > 0))\\ &+\sigma(id_p)(''otf'')[j]\end{aligned}}$$

By construction, $<\texttt{output\_arcs\_types(j)} \Rightarrow \texttt{BASIC}> \in ipm_p$ and $<\texttt{output\_arcs\_weights(j)} \Rightarrow \omega> \in ipm_p$.
By property of the stabilize relation and $\texttt{comp}(id_p, ''place'', gm_p, ipm_p, opm_p) \in d.cs$:

$$\sigma'(id_p)(''oat'')[j] = \texttt{BASIC} \tag{1.39}$$
$$\sigma'(id_p)(''oaw'')[j] = \omega \tag{1.40}$$

By property of $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$:

$$\sigma(id_p)(''sm'') = s.M(p) \tag{1.41}$$
$$\sigma(id_p)(''sots'') = \sum_{t_i \in Fired(s)} pre(p, t_i) \tag{1.42}$$

Rewriting the goal with (1.39), (1.40), (1.41) and (1.42), and simplifying the goal:

$$\boxed{(s.M(p) - \sum_{t_i \in Fired(s)} pre(p, t_i) < \omega \,.\, \sum_{t_i \in Fired(s)} pre(p, t_i) > 0)) + \sigma(id_t)(''fired'') = \texttt{true}}$$

Thanks to the hypotheses 1 and 3:

$$s.M(p) - \sum_{t_i \in Fired(s)} pre(p, t_i) < \omega = \texttt{true} \tag{1.43}$$
$$\sum_{t_i \in Fired(s)} pre(p, t_i) > 0 = \texttt{true} \tag{1.44}$$
$$\tag{1.45}$$

Rewriting the goal with (1.43) and (1.44), and simplifying the goal, tautology.

* **CASE** such a place does not exist:
Then, let us assume that, for all place $p \in P$
  1. $\sum_{t_i \in Fired(s)} pre(p, t_i) = 0$
  2. or $\forall \omega \in \mathbb{N}^*,\ pre(p,t) = (\omega, \texttt{basic}) \vee pre(p,t) = (\omega, \texttt{test}) \Rightarrow s.M(p) - \sum_{t_i \in Fired(s)} pre(p, t_i) \geq \omega$.

In that case, by property of $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$:

$$s'.reset_t(t) = \texttt{false} \tag{1.46}$$

Rewriting the goal with (1.46): $\boxed{\sum_{i=0}^{|input(t)|-1} \sigma'(id_t)(''rt'')[i] = \texttt{false}.}$

To prove the goal, let us show $\boxed{\forall i \in [0, |input(t)| - 1],\ \sigma'(id_t)(''rt'')[i] = \texttt{false}.}$
Given an $i \in [0, |input(t)| - 1]$, let us show $\boxed{\sigma'(id_t)(''rt'')[i] = \texttt{false}.}$

By construction, there exist a $p \in input(t)$, an $id_p \in Comps(\Delta)$, gm_p, ipm_p, opm_p, a $j \in [0, |output(p)| - 1]$, an $id_{ji} \in Sigs(\Delta)$ s.t. $\gamma(p) = id_p$ and $\texttt{comp}(id_p, ''place'', gm_p, ipm_p, opm_p) \in d.cs$ and $<\texttt{reinit\_transition\_time(j)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in opm_p$ and $<\texttt{reinit\_time(i)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in ipm_t$. Let us take such a p, id_p, gm_p, ipm_p, opm_p, j and id_{ji}.
By property of the stabilize relation, $<\texttt{reinit\_transition\_time(j)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in opm_p$ and $<\texttt{reinit\_time(i)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in ipm_t$:

$$\sigma'(id_t)(''rt'')[i] = \sigma'(id_{ji}) = \sigma'(id_p)(''rtt'')[j] \tag{1.47}$$

Rewriting the goal with (1.47): $\boxed{\sigma'(id_p)(''rtt'')[j] = \texttt{false}.}$

By property of the $\texttt{Inject}_{\uparrow}$, the $\mathcal{H}$-VHDL rising edge and the stabilize relations:

$$\begin{aligned}\sigma'(id_p)(''rtt'')[j] = &\big((\sigma(id_p)(''oat'')[j] = \texttt{BASIC} + \sigma(id_p)(''oat'')[j] = \texttt{TEST})\\ &.(\sigma(id_p)(''sm'') - \sigma(id_p)(''sots'') < \sigma(id_p)(''oaw'')[j])\\ &.(\sigma(id_p)(''sots'') > 0)\big)\\ &+ \sigma(id_p)(''otf'')[j]\end{aligned} \tag{1.48}$$

Rewriting the goal with (1.48),

$$\boxed{\begin{aligned}\texttt{false} = &((\sigma(id_p)(''oat'')[j] = \texttt{BASIC} + \sigma(id_p)(''oat'')[j] = \texttt{TEST})\\ &.(\sigma(id_p)(''sm'') - \sigma(id_p)(''sots'') < \sigma(id_p)(''oaw'')[j])\\ &.(\sigma(id_p)(''sots'') > 0))\\ &+ \sigma(id_p)(''otf'')[j])\end{aligned}}$$

By construction, there exists $id_{ft} \in Sigs(\Delta)$ s.t. $<\texttt{output\_transitions\_fired(j)} \Rightarrow \texttt{id}_{\texttt{ft}}> \in ipm_p$ and $<\texttt{fired} \Rightarrow \texttt{id}_{\texttt{ft}}> \in opm_t$. By property of state σ as being a stable state:

$$\sigma(id_t)(''fired'') = \sigma(id_{ft}) = \sigma(id_p)(''otf'')[j] \tag{1.49}$$

Rewriting the goal with (1.49),

$$\boxed{\begin{aligned}\texttt{false} = &((\sigma(id_p)(''oat'')[j] = \texttt{BASIC} + \sigma(id_p)(''oat'')[j] = \texttt{TEST})\\ &.(\sigma(id_p)(''sm'') - \sigma(id_p)(''sots'') < \sigma(id_p)(''oaw'')[j])\\ &.(\sigma(id_p)(''sots'') > 0))\\ &+ \sigma(id_t)(''fired'')\end{aligned}}$$

By property of $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$:

$$t \notin Fired(s) \Leftrightarrow \sigma(id_t)(''fired'') = \texttt{false} \tag{1.50}$$

Knowing that $t \notin Fired(s)$, we can rewrite the goal with the right side of (1.50) and simplify the goal (i.e, $\forall b \in \mathbb{B},\ b + \texttt{false} = b$):

$$\begin{aligned}\texttt{false} =&((\sigma(id_p)(''oat'')[j] = \texttt{BASIC} + \sigma(id_p)(''oat'')[j] = \texttt{TEST})\\ &.(\sigma(id_p)(''sm'') - \sigma(id_p)(''sots'') < \sigma(id_p)(''oaw'')[j])\\ &.(\sigma(id_p)(''sots'') > 0))\end{aligned}$$

Then, there are two cases:

1. **CASE** $\sum_{t_i \in Fired(s)} pre(p, t_i) = 0$:

   By property of $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$:

   $$\sum_{t_i \in Fired(s)} pre(p, t_i) = \sigma(id_p)(''sots'') \tag{1.51}$$

   Rewriting the goal with (1.51) and $\sum_{t_i \in Fired(s)} pre(p, t_i) = 0$, simplifying the goal:

   tautology.

2. **CASE** $\forall \omega \in \mathbb{N}^*,\ pre(p,t) = (\omega, \texttt{basic}) \vee pre(p,t) = (\omega, \texttt{test}) \Rightarrow s.M(p) - \sum_{t_i \in Fired(s)} pre(p, t_i) \geq \omega$:

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

   (a) **CASE** $pre(p,t) = (\omega, \texttt{basic})$ or $pre(p,t) = (\omega, \texttt{basic})$:
   By construction, $<\texttt{output\_arcs\_weights(j)} \Rightarrow \omega> \in ipm_p$.
   By property of stable state σ and $\texttt{comp}(id_p, ''place'', gm_p, ipm_p, opm_p) \in d.cs$:

   $$\sigma(id_p)(''oaw'')[j] = \omega \tag{1.52}$$

   By property of $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$:

   $$\sigma(id_p)(''sm'') = s.M(p) \tag{1.53}$$
   $$\sigma(id_p)(''sots'') = \sum_{t_i \in Fired(s)} pre(p, t_i) \tag{1.54}$$

   By hypothesis, we know that $s.M(p) - \sum_{t_i \in Fired(s)} pre(p, t_i) \geq \omega$, and then we can deduce:

   $$s.M(p) - \sum_{t_i \in Fired(s)} pre(p, t_i) < \omega = \texttt{false} \tag{1.55}$$

   Rewriting the goal with (1.52), (1.53), (1.54), and (1.55), and simplifying the goal, tautology.

   (b) **CASE** $pre(p,t) = (\omega, \texttt{inhib})$:
   By construction, $<\texttt{output\_arcs\_types(j)} \Rightarrow \texttt{INHIB}> \in ipm_p$.
   By property of stable state σ and $\texttt{comp}(id_p, ''place'', gm_p, ipm_p, opm_p) \in d.cs$:

   $$\sigma(id_p)(''oat'')[j] = \texttt{INHIB} \tag{1.56}$$

Rewriting the goal with (1.56), and simplifying the goal, tautology.

□

1.5.5 Rising edge and action executions

Lemma 6 (Rising Edge Equal Action Executions). *For all sitpn, d, γ, E_c, E_p, τ, Δ, σ_e, s, s', σ, σ_i, $\sigma_\uparrow$, 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 $E_c, \tau \vdash s \xrightarrow{\uparrow} s'$:

$$s.ex(a) = s'.ex(a) \tag{1.57}$$

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

$$\sigma(id_a) = \sigma'(id_a) \tag{1.58}$$

Rewriting the goal with (1.57) and (1.58), $\boxed{s.ex(a) = \sigma(id_a).}$

By property of $E_c, \tau \vdash s \xrightarrow{\uparrow} s'$, $s.ex(a) = \sigma(id_a)$. □

1.5.6 Rising edge and function executions

Lemma 7 (Rising Edge Equal Function Executions). *For all sitpn, d, γ, E_c, E_p, τ, Δ, σ_e, s, s', σ, σ_i, $\sigma_\uparrow$, σ' 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 $E_c, \tau \vdash s \xrightarrow{\uparrow} s'$:

$$s'.ex(f) = \sum_{t \in Fired(s)} \mathbb{F}(t, f) \tag{1.59}$$

By construction, the ''`function`'' process is a part of design d's behavior, i.e
$\texttt{ps}(''function'', \emptyset, sl, ss) \in d.cs$.
By construction id_f is an output port of design d, and it is only assigned in the body of the ''`function`'' process. Let $trs(f)$ be the set of transitions associated to function f, i.e $trs(f) = \{t \in T \mid \mathbb{F}(t, f) = true\}$. Then, depending on $trs(f)$, there are two cases of assignment of output port id_f:

- **CASE** $trs(f) = \emptyset$:
  By construction, $\texttt{id}_\texttt{f} \Leftarrow \texttt{false} \in ss_\uparrow$ where $ss_\uparrow$ is the part of the ''`function`'' process body executed during the rising edge phase.

  By property of the $\mathcal{H}$-VHDL rising edge, the stabilize relations and $\texttt{ps}(''function'', \emptyset, sl, ss) \in d.cs$:

  $$\sigma'(id_f) = false \tag{1.60}$$

By property of $\sum_{t \in Fired(s)} \mathbb{F}(t,f)$ and $trs(f) = \emptyset$:

$$\sum_{t \in Fired(s)} \mathbb{F}(t,f) = \texttt{false} \tag{1.61}$$

Rewriting the goal with (1.59), (1.60) and (1.61), tautology.

- **CASE** $trs(f) \neq \emptyset$:
  By construction, $\texttt{id}_\texttt{f} \Leftarrow \texttt{id}_{\texttt{ft}_0} + \cdots + \texttt{id}_{\texttt{ft}_n} \in ss_\uparrow$, where $id_{ft_i} \in Sigs(\Delta)$, $ss_\uparrow$ is the part of the "`function`" process body executed during the rising edge phase, and $n = |trs(f)| - 1$.

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

$$\sigma'(id_f) = \sigma(id_{ft_0}) + \cdots + \sigma(id_{ft_n}) \tag{1.62}$$

  Rewriting the goal with (1.59) and (1.62), $\boxed{\sum_{t \in Fired(s)} \mathbb{F}(t,f) = \sigma(id_{ft_0}) + \cdots + \sigma(id_{ft_n}).}$

  Let us reason on the value of $\sigma(id_{ft_0}) + \cdots + \sigma(id_{ft_n})$; there are two cases:

  - **CASE** $\sigma(id_{ft_0}) + \cdots + \sigma(id_{ft_n}) = \texttt{true}$:
    Then, we can rewrite the goal as follows: $\boxed{\sum_{t \in Fired(s)} \mathbb{F}(t,f) = \texttt{true}.}$

    To prove the above goal, let us show $\boxed{\exists t \in Fired(s)\ s.t.\ \mathbb{F}(t,f) = \texttt{true}.}$

    Knowing that $\sigma(id_{ft_0}) + \cdots + \sigma(id_{ft_n}) = \texttt{true}$, then $\exists id_{ft_i}\ s.t.\ \sigma(id_{ft_i}) = \texttt{true}$. Let us take such an id_{ft_i}.

    By construction, for all id_{ft_i}, there exist a $t_i \in trs(f)$, an $id_{t_i} \in Comps(\Delta)$, gm_{t_i}, ipm_{t_i} and opm_{t_i} s.t. $\gamma(t_i) = id_{t_i}$ and $\texttt{comp}(id_{t_i}, "transition", gm_{t_i}, ipm_{t_i}, opm_{t_i}) \in d.cs$ and $<\texttt{fired} \Rightarrow \texttt{id}_{\texttt{ft}_\texttt{i}}> \in opm_{t_i}$. Let us take such a t_i, id_{t_i}, gm_{t_i}, ipm_{t_i} and opm_{t_i}.

    By property of σ as being a stable design state, and $\texttt{comp}(id_{t_i}, "transition", gm_{t_i}, ipm_{t_i}, opm_{t_i}) \in d.cs$:

$$\sigma(id_{t_i})("fired") = \sigma(id_{ft_i}) \tag{1.63}$$

    Thanks to (1.63) and $\sigma(id_{ft_i}) = \texttt{true}$, we can deduce that $\sigma(id_{t_i})("fired") = \texttt{true}$.

    By property of $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$:

$$t_i \in Fired(s) \Leftrightarrow \sigma(id_{t_i})("fired") = \texttt{true} \tag{1.64}$$

    Thanks to (1.64), we can deduce $t_i \in Fired(s)$.

    Let us use t_i to prove the goal: $\boxed{\mathbb{F}(t,f) = \texttt{true}.}$

    By definition of $t_i \in trs(f)$, $\mathbb{F}(t,f) = \texttt{true}$.
  - **CASE** $\sigma(id_{ft_0}) + \cdots + \sigma(id_{ft_n}) = \texttt{false}$:
    Then, we can rewrite the goal as follows: $\boxed{\sum_{t \in Fired(s)} \mathbb{F}(t,f) = \texttt{false}.}$

To prove the above goal, let us show $\boxed{\forall t \in Fired(s)\ s.t.\ \mathbb{F}(t,f) = \texttt{false}.}$

Given a $t \in Fired(s)$, let us show $\boxed{\mathbb{F}(t,f) = \texttt{false}.}$

Let us perform case analysis on $\mathbb{F}(t,f)$; there are 2 cases:

* **CASE** $\mathbb{F}(t,f) = \texttt{false}.$
* **CASE** $\mathbb{F}(t,f) = \texttt{true}$:
  By construction, for all $t \in T$ s.t. $\mathbb{F}(t,f) = \texttt{true}$, there exist an $id_t \in Comps(\Delta)$, gm_t, ipm_t, opm_t and $id_{ft_i} \in Sigs(\Delta)$ s.t. $\gamma(t) = id_t$ and $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$ and $<\texttt{fired} \Rightarrow \texttt{id}_{\texttt{ft}_\texttt{i}}> \in opm_t$. Let us take such a id_t, gm_t, ipm_t, opm_t and id_{ft_i}.
  By property of stable design state σ and $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$, equation (1.63) holds.

  By property of $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$, equation (1.64) holds.
  Thanks to (1.63) and (1.64), we can deduce that $\sigma(id_{ft_i}) = \texttt{true}$.
  Then, $\sigma(id_{ft_i}) = \texttt{true}$ contradicts $\sigma(id_{ft_0}) + \cdots + \sigma(id_{ft_n}) = \texttt{false}.$

□

1.5.7 Rising edge and sensitization

Lemma 8 (Rising Edge Equal Sensitized). *For all sitpn, d, γ, E_c, E_p, τ, Δ, σ_e, s, s', σ, σ_i, $\sigma_\uparrow$, σ' that verify the hypotheses of Def. 1, then*
$\forall t \in T, id_t \in Comps(\Delta)\ s.t.\ \gamma(t) = id_t, t \in Sens(s'.M) \Leftrightarrow \sigma'(id_t)("s\_enabled") = \texttt{true}.$

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

By definition of id_t, there exist gm_t, ipm_t, opm_t s.t. $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$.
Then, the proof is in two parts:

1. Assuming that $t \in Sens(s'.M)$, let us show $\boxed{\sigma'(id_t)("s\_enabled") = \texttt{true}.}$

   By property of the stabilize relation and $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$:

   $$\sigma'(id_t)("se") = \prod_{i=0}^{\Delta(id_t)("ian")-1} \sigma'(id_t)("input\_arcs\_valid")[i] \tag{1.65}$$

   Rewriting the goal with (1.65), $\boxed{\prod_{i=0}^{\Delta(id_t)("ian")-1} \sigma'(id_t)("iav")[i] = \texttt{true}.}$

   To prove the goal, let us show that $\boxed{\forall i \in [0, \Delta(id_t)("ian") - 1],\ \sigma'(id_t)("iav")[i] = \texttt{true}.}$

   Given an $i \in [0, \Delta(id_t)("ian") - 1]$, let us show $\boxed{\sigma'(id_t)("iav")[i] = \texttt{true}.}$

   Let us perform case analysis on $input(t)$.

   - **CASE** $input(t) = \emptyset$:
     By construction, $<\texttt{input\_arcs\_number} \Rightarrow \texttt{1}> \in gm_t$ and
     $<\texttt{input\_arcs\_valid(0)} \Rightarrow \texttt{true}> \in ipm_t$.

By property of the elaboration and stabilize relations and $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$:

$$\Delta(id_t)("ian") = 1 \tag{1.66}$$
$$\sigma'(id_t)("iav")[0] = \texttt{true} \tag{1.67}$$

Thanks to (1.66), we can deduce that $i = 0$. Rewriting the goal with (1.67), tautology.

- **CASE** $input(t) \neq \emptyset$:
  By construction, $<\texttt{input\_arcs\_number} \Rightarrow |input(t)|> \in gm_t$.
  By property of the elaboration relation and $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$:

$$\Delta(id_t)("ian") = |input(t)| \tag{1.68}$$

  Thanks to (1.68), we know that $i \in [0, |input(t)| - 1]$.
  By construction, there exist a $p \in input(t)$, $id_p \in Comps(\Delta)$, gm_p, ipm_p, opm_p, $j \in [0, |output(p)| - 1]$ and $id_{ji} \in Sigs(\Delta)$ s.t. $\gamma(p) = id_p$ and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$ and $<\texttt{output\_arcs\_valid(j)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in opm_p$ and $<\texttt{input\_arcs\_valid(i)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in ipm_t$.
  By property of the stabilize relation, $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$ and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$:

$$\sigma'(id_t)("iav")[i] = \sigma'(id_{ji}) = \sigma'(id_p)("oav")[j] \tag{1.69}$$

  Rewriting the goal with (1.69), $\boxed{\sigma'(id_p)("oav")[j] = \texttt{true}.}$
  By property of the stabilize relation and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$:

$$\begin{aligned}\sigma'(id_p)("oav")[j] = &\big((\sigma'(id_p)("oat")[j] = \texttt{BASIC} + \sigma'(id_p)("oat")[j] = \texttt{TEST}) \\ &. \sigma'(id_p)("sm") \geq \sigma'(id_p)("oaw")[j]\big) \\ &+ \big(\sigma'(id_p)("oat")[j] = \texttt{INHIB} \,.\, \sigma'(id_p)("sm") < \sigma'(id_p)("oaw")[j]\big)\end{aligned} \tag{1.70}$$

  Rewriting the goal with (1.70),

$$\boxed{\begin{aligned}\texttt{true} = &\big((\sigma'(id_p)("oat")[j] = \texttt{BASIC} + \sigma'(id_p)("oat")[j] = \texttt{TEST}) \\ &. \sigma'(id_p)("sm") \geq \sigma'(id_p)("oaw")[j]\big) \\ &+ \big(\sigma'(id_p)("oat")[j] = \texttt{INHIB} \,.\, \sigma'(id_p)("sm") < \sigma'(id_p)("oaw")[j]\big)\end{aligned}}$$

  Let us perform case analysis on $pre(p, t)$; there are 3 cases:
  - **CASE** $pre(p, t) = (\omega, \texttt{BASIC})$:

    By construction, $<\texttt{output\_arcs\_types(j)} \Rightarrow \texttt{BASIC}> \in ipm_p$ and $<\texttt{output\_arcs\_weights(j)} \Rightarrow \omega> \in ipm_p$.

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

$$\sigma'(id_p)("oat")[j] = \texttt{BASIC} \quad (1.71)$$
$$\sigma'(id_p)("oaw")[j] = \omega \quad (1.72)$$

Rewriting the goal with (1.71) and (1.72), and simplifying the goal:
$\boxed{\sigma'(id_p)("sm") \geq \omega = \texttt{true}.}$
Appealing to Lemma Rising Edge Equal Marking:

$$s'.M(p) = \sigma'(id_p)("sm") \quad (1.73)$$

Rewriting the goal with (1.73): $\boxed{s'.M(p) \geq \omega = \texttt{true}.}$
By definition of $t \in Sens(s'.M)$, $s'.M(p) \geq \omega = \texttt{true}.$ [1]

– **CASE** $pre(p,t) = (\omega, \texttt{TEST})$: same as the preceding case.
– **CASE** $pre(p,t) = (\omega, \texttt{INHIB})$:
By construction, $<\texttt{output\_arcs\_types(j)} \Rightarrow \texttt{INHIB}> \in ipm_p$ and
$<\texttt{output\_arcs\_weights(j)} \Rightarrow \omega> \in ipm_p$.
By property of the stabilize relation and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$:

$$\sigma'(id_p)("oat")[j] = \texttt{INHIB} \quad (1.74)$$
$$\sigma'(id_p)("oaw")[j] = \omega \quad (1.75)$$

Rewriting the goal with (1.74) and (1.75), and simplifying the goal:
$\boxed{\sigma'(id_p)("sm") < \omega = \texttt{true}.}$
Appealing to Lemma Rising Edge Equal Marking, equation (1.73) holds.
Rewriting the goal with (1.73): $\boxed{s'.M(p) < \omega = \texttt{true}.}$
By definition of $t \in Sens(s'.M)$, $s'.M(p) < \omega = \texttt{true}.$

2. Assuming that $\sigma'(id_t)("s\_enabled") = \texttt{true}$, let us show $\boxed{t \in Sens(s'.M).}$
By definition of $t \in Sens(s'.M)$, let us show

$$\boxed{\forall p \in P, \omega \in \mathbb{N}^*,\ \big(pre(p,t) = (\omega, \texttt{basic}) \vee pre(p,t) = (\omega, \texttt{test}) \Rightarrow s'.M(p) \geq \omega\big) \wedge \big(pre(p,t) = (\omega, \texttt{inhib}) \Rightarrow s'.M(p) < \omega\big)}$$

Given a $p \in P$ and an $\omega \in \mathbb{N}^*$, let us show
$\boxed{pre(p,t) = (\omega, \texttt{basic}) \vee pre(p,t) = (\omega, \texttt{test}) \Rightarrow s'.M(p) \geq \omega}$ and
$\boxed{pre(p,t) = (\omega, \texttt{inhib}) \Rightarrow s'.M(p) < \omega.}$

(a) Assuming $pre(p,t) = (\omega, \texttt{basic}) \vee pre(p,t) = (\omega, \texttt{test})$, let us show $\boxed{s'.M(p) \geq \omega.}$
The proceeding is the same for $pre(p,t) = (\omega, \texttt{basic})$ and $pre(p,t) = (\omega, \texttt{test})$. Therefore, we will only cover the case where $pre(p,t) = (\omega, \texttt{basic})$.

[1] Here $\geq$ denotes a boolean operator, i.e $\geq \in \mathbb{N} \to \mathbb{N} \to \mathbb{B}$. As the $\geq \subseteq (\mathbb{N} \times \mathbb{B})$ relation is decidable for all pairs of natural numbers, we can interchange an expression $a \geq b = \texttt{true}$ with $a \geq b$ where $a, b \in \mathbb{N}$.

By property of the stabilize relation and $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$, equation (1.65) holds.

Rewriting $\sigma'(id_t)("se") = \texttt{true}$ with (1.65), $\prod_{i=0}^{\Delta(id_t)("ian")-1} \sigma'(id_t)("input\_arcs\_valid")[i] = \texttt{true}$.

Then, we can deduce that $\forall i \in [0, \Delta(id_t)("ian") - 1],\ \sigma'(id_t)("iav")[i] = \texttt{true}$.

By construction, there exist an $id_p \in Comps(\Delta)$, $gm_p, ipm_p, opm_p, i \in [0, |input(t)| - 1]$, $j \in [0, |output(p)| - 1]$ and $id_{ji} \in Sigs(\Delta)$ s.t. $\gamma(p) = id_p$ and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$ and $<\texttt{output\_arcs\_valid(j)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in opm_p$ and $<\texttt{input\_arcs\_valid(i)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in ipm_t$. Let us take such an $id_p \in Comps(\Delta)$, $gm_p, ipm_p, opm_p, i \in [0, |input(t)| - 1], j \in [0, |output(p)| - 1]$ and $id_{ji} \in Sigs(\Delta)$.

By construction, $<\texttt{input\_arcs\_number} \Rightarrow |input(t)|> \in gm_t$.

By property of the elaboration relation and $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$, equation (1.68) holds.

Thanks to (1.68), we can deduce that $\forall i \in [0, |input(t)| - 1],\ \sigma'(id_t)("iav")[i] = \texttt{true}$.

Having such an $i \in [0, |input(t)| - 1]$, we can deduce that $\sigma'(id_t)("iav")[i] = \texttt{true}$.

By property of the stabilize relation, $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$ and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$, equation (1.69) holds.

Thanks to (1.69), we can deduce that $\sigma'(id_p)("oav")[j] = \texttt{true}$.

By property of the stabilize relation and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$, equation (1.70) holds. Thanks to (1.70), we can deduce that:

$$\begin{aligned}\texttt{true} = &\big((\sigma'(id_p)("oat")[j] = \texttt{BASIC} + \sigma'(id_p)("oat")[j] = \texttt{TEST})\\ &\quad . \sigma'(id_p)("sm") \geq \sigma'(id_p)("oaw")[j]\big)\\ &+ \big(\sigma'(id_p)("oat")[j] = \texttt{INHIB} \,.\, \sigma'(id_p)("sm") < \sigma'(id_p)("oaw")[j]\big)\end{aligned}$$

By construction, $<\texttt{output\_arcs\_types(j)} \Rightarrow \texttt{BASIC}> \in ipm_p$ and $<\texttt{output\_arcs\_weights(j)} \Rightarrow \omega> \in ipm_p$.

By property of the stabilize relation and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$, equations (1.71) and (1.72) hold.

Thanks to (1.71) and (1.72), we can deduce that $\sigma'(id_p)("sm") \geq \omega = \texttt{true}$.

Appealing to Lemma Rising Edge Equal Marking, $s'.M(p) \geq \omega$.

(b) Assuming $pre(p, t) = (\omega, \texttt{inhib})$, let us show $\boxed{s'.M(p) < \omega.}$

The proceeding is the same as the preceding case. Here, we will start the proof where the two cases are diverging, i.e:

By construction, $<\texttt{output\_arcs\_types(j)} \Rightarrow \texttt{INHIB}> \in ipm_p$ and $<\texttt{output\_arcs\_weights(j)} \Rightarrow \omega> \in ipm_p$.

By property of the stabilize relation and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$, equations (1.74) and (1.72) hold.

Thanks to (1.74) and (1.72), we can deduce that $\sigma'(id_p)("sm") < \omega = \texttt{true}$.

Appealing to Lemma Rising Edge Equal Marking, $s'.M(p) < \omega$.

□

Lemma 9 (Rising Edge Equal Not Sensitized). *For all* $sitpn$, d, γ, E_c, E_p, τ, Δ, σ_e, s, s', σ, σ_i, $\sigma_\uparrow$, σ' *that verify the hypotheses of Def. 1, then*
$\forall t \in T, id_t \in Comps(\Delta)\ s.t.\ \gamma(t) = id_t, t \notin Sens(s'.M) \Leftrightarrow \sigma'(id_t)(\text{"}s\_enabled\text{"}) = \texttt{false}$.

Proof. For all $sitpn \in SITPN$, $s \in S(sitpn)$ and $t \in T$, $t \in Sens(s'.M)$ is decidable. Therefore, proving the above lemma is trivial by appealing to Lemma Rising Edge Equal Sensitized and by reasoning on contrapositives.

□

1.6 Falling Edge

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
  - ...