THÈSE POUR OBTENIR LE GRADE DE DOCTEUR
DE L'UNIVERSITÉ DE MONTPELLIER

En Informatique

École doctorale : Information, Structures, Systèmes

Unité de recherche LIRMM

Vérification d'une méthodologie pour la conception de systèmes numériques critiques

Présenté par Vincent IAMPIETRO

Le Date de la soutenance

Sous la direction de David Delahaye et David Andreu

Devant le jury composé de

[Nom Prénom], [Titre], [Labo]	[Statut jury]
[Nom Prénom], [Titre], [Labo]	[Statut jury]
[Nom Prénom], [Titre], [Labo]	[Statut jury]

UNIVERSITÉ DE MONTPELLIER

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

List of Abbreviations

SITPN	**S**ynchronously executed **I**nterpreted **T**ime **P**etri **N**et with priorities
VHDL	**V**ery high speed integrated circuit **H**ardware **D**escription **L**anguage
PCI	**P**lace **C**omponent **I**nstance
TCI	**T**ransition **C**omponent **I**nstance
GPL	**G**eneric **P**rogramming **L**anguage
HDL	**H**ardware **D**escription **L**anguage

For/Dedicated to/To my…

Appendix A

Semantic preservation proof

Constants and signals reference			
Full name	*Alias*	*Category*	*Type*
$''input\_conditions''$	$''ic''$	input port (T)	$\mathbb{B}$
$''reinit\_time''$	$''rt''$	input port (T)	$\mathbb{B}$
$''input\_arcs\_valid''$	$''iav''$	input port (T)	$\mathbb{B}$
$''fired''$	$''f''$	output port (T)	$\mathbb{B}$
$''s\_condition\_combination''$	$''scc''$	internal signal (T)	$\mathbb{B}$
$''s\_reinit\_time\_counter''$	$''srtc''$	internal signal (T)	$\mathbb{B}$
$''s\_priority\_combination''$	$''spc''$	internal signal (T)	$\mathbb{B}$
$''s\_fired''$	$''sf''$	internal signal (T)	$\mathbb{B}$
$''s\_firable''$	$''sfa''$	internal signal (T)	$\mathbb{B}$
$''s\_enabled''$	$''se''$	internal signal (T)	$\mathbb{B}$
$''input\_arcs\_number''$	$''ian''$	generic constant (T)	$\mathbb{N}$
$''transition\_type''$	$''tt''$	generic constant (T)	$\{\mathtt{NOT\_TEMP}, \mathtt{TEMP\_A\_B}, \mathtt{TEMP\_A\_A}, \mathtt{TEMP\_A\_INF}\}$
$''conditions\_number''$	$''cn''$	generic constant (T)	$\mathbb{N}$
$''maximal\_time\_counter''$	$''mtc''$	generic constant (T)	$\mathbb{N}$
$''s\_marking''$	$''sm''$	internal signal (P)	$\mathbb{N}$
$''s\_output\_token\_sum''$	$''sots''$	internal signal (P)	$\mathbb{N}$
$''s\_input\_token\_sum''$	$''sits''$	internal signal (P)	$\mathbb{N}$
$''reinit\_transition\_time''$	$''rtt''$	output port (P)	$\mathbb{B}$
$''output\_arcs\_types''$	$''oat''$	input port (P)	$\{\mathtt{BASIC}, \mathtt{TEST}, \mathtt{INHIB}\}$
$''output\_arcs\_weights''$	$''oaw''$	input port (P)	$\mathbb{N}$
$''output\_transition\_fired''$	$''otf''$	input port (P)	$\mathbb{B}$
$''input\_arcs\_weights''$	$''iaw''$	input port (P)	$\mathbb{N}$
$''input\_transition\_fired''$	$''itf''$	input port (P)	$\mathbb{B}$

TABLE A.1: Constants and signals reference for the $\mathcal{H}$-VHDL transition and place designs

A.1 Initial States

Definition 1 (Initial state hypotheses). *Given an* $sitpn \in SITPN$, $d \in design$, $\gamma \in WM(sitpn, d)$, $\Delta \in ElDesign(d, \mathcal{D}_{\mathcal{H}})$, $\sigma_e, \sigma_0 \in \Sigma(\Delta)$, *assume that:*

- *SITPN sitpn translates into design d:* $\lfloor sitpn \rfloor_{\mathcal{H}} = (d, \gamma)$

- *Δ is the elaborated version of d, σ_e is the default state of Δ, i.e, state of Δ where all signals have their default value:*

  $\mathcal{D}_{\mathcal{H}}, \emptyset \vdash d \xrightarrow{elab} (\Delta, \sigma_e)$

- *σ_0 is the initial state of Δ: $\Delta, \sigma_e \vdash d.cs \xrightarrow{init} \sigma_0$*

Lemma 1 (Similar Initial States). *For all $sitpn \in SITPN$, $d \in design$, $\gamma \in WM(sitpn, d)$, $\Delta \in ElDesign(d, \mathcal{D}_{\mathcal{H}}), \sigma_e, \sigma_0 \in \Sigma(\Delta)$ that verify the hypotheses of Definition 1, then $\gamma \vdash s_0 \sim \sigma_0$.*

Proof. By definition of the **??** relation, there are 6 points to prove.

1. $\forall p \in P, id_p \in Comps(\Delta)\ s.t.\ \gamma(p) = id_p,\ s_0.M(p) = \sigma_0(id_p)(\text{"}s\_marking\text{"})$.
2. $\forall t \in T_i, id_t \in Comps(\Delta)\ s.t.\ \gamma(t) = id_t,$
   $(upper(I_s(t)) = \infty \wedge s_0.I(t) \leq lower(I_s(t)) \Rightarrow s_0.I(t) = \sigma_0(id_t)(\text{"}s\_time\_counter\text{"}))$
   $\wedge(upper(I_s(t)) = \infty \wedge s_0.I(t) > lower(I_s(t)) \Rightarrow \sigma_0(id_t)(\text{"}s\_time\_counter\text{"}) = lower(I_s(t)))$
   $\wedge(upper(I_s(t)) \neq \infty \wedge s_0.I(t) > upper(I_s(t)) \Rightarrow \sigma_0(id_t)(\text{"}s\_time\_counter\text{"}) = upper(I_s(t)))$
   $\wedge(upper(I_s(t)) \neq \infty \wedge s_0.I(t) \leq upper(I_s(t)) \Rightarrow s_0.I(t) = \sigma_0(id_t)(\text{"}s\_time\_counter\text{"}))$.
3. $\forall t \in T_i, id_t \in Comps(\Delta)\ s.t.\ \gamma(t) = id_t, s_0.reset_t(t) = \sigma_0(id_t)(\text{"}s\_reinit\_time\_counter\text{"})$.
4. $\forall c \in \mathcal{C}, id_c \in Ins(\Delta)\ s.t.\ \gamma(c) = id_c,\ s_0.cond(c) = \sigma_0(id_c)$.
5. $\forall a \in \mathcal{A}, id_a \in Outs(\Delta)\ s.t.\ \gamma(a) = id_a,\ s_0.ex(a) = \sigma_0(id_a)$.
6. $\forall f \in \mathcal{F}, id_f \in Outs(\Delta)\ s.t.\ \gamma(f) = id_f,\ s_0.ex(f) = \sigma_0(id_f)$.

- Apply the Initial States Equal Marking lemma to solve 1.
- Apply the Initial States Equal Time Counters lemma to solve 2.
- Apply the Initial States Equal Reset Orders lemma to solve 3.
- Apply the Initial States Equal Condition Values lemma to solve 4.
- Apply the Initial States Equal Action Executions lemma to solve 5.
- Apply the Initial States Equal Function Executions lemma to solve 6.

□

A.1.1 Initial states and marking

Lemma 2 (Initial States Equal Marking). *For all $sitpn \in SITPN$, $d \in design$, $\gamma \in WM(sitpn, d)$, $\Delta \in ElDesign(d, \mathcal{D}_{\mathcal{H}}), \sigma_e, \sigma_0 \in \Sigma(\Delta)$ that verify the hypotheses of Definition 1, then $\forall p \in P, id_p \in Comps(\Delta)\ s.t.\ \gamma(p) = id_p$, then $s_0.M(p) = \sigma_0(id_p)(\text{"}s\_marking\text{"})$.*

Proof. Given a $p \in P$ and an $id_p \in Comps(\Delta)$ s.t. $\gamma(p) = id_p$, let us show that
$\boxed{s_0.M(p) = \sigma_0(id_p)(\text{"}s\_marking\text{"}).}$

By construction and 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 $\mathcal{H}$-VHDL initialization relation, $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$, and through the examination of the `marking` process defined in the place design architecture, we can deduce $\sigma_0(id_p)("s\_marking") = \sigma_0(id_p)("initial\_marking")$.
Rewriting $\sigma_0(id_p)("s\_marking")$ as $\sigma_0(id_p)("initial\_marking")$, $\boxed{\sigma_p^0("initial\_marking") = s_0.M(p).}$
By construction, $<\texttt{initial\_marking} \Rightarrow M_0(p)> \in ipm_p$.
By property of the $\mathcal{H}$-VHDL initialization relation, and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$, then $\sigma_0(id_p)("initial\_marking") = M_0(p)$. Rewriting $\sigma_0(id_p)("initial\_marking")$ as $M_0(p)$ in the current goal: $\boxed{M_0(p) = s_0.M(p).}$
By definition of s_0, we can rewrite $s_0.M(p)$ as $M_0(p)$ in the current goal, tautology.

□

A.1.2 Initial states and time counters

Lemma 3 (Initial States Equal Time Counters)**.** *For all* $sitpn \in SITPN, d \in design, \gamma \in WM(sitpn, d)$, $\Delta \in ElDesign(d, \mathcal{D_H}), \sigma_e, \sigma_0 \in \Sigma(\Delta)$ *that verify the hypotheses of Definition 1, then* $\forall t \in T_i, id_t \in Comps(\Delta)$ *s.t.* $\gamma(t) = id_t$,
$upper(I_s(t)) = \infty \wedge s_0.I(t) \leq lower(I_s(t)) \Rightarrow s_0.I(t) = \sigma_0(id_t)("s\_time\_counter") \wedge$
$upper(I_s(t)) = \infty \wedge s_0.I(t) > lower(I_s(t)) \Rightarrow \sigma_0(id_t)("s\_time\_counter") = lower(I_s(t)) \wedge$
$upper(I_s(t)) \neq \infty \wedge s_0.I(t) > upper(I_s(t)) \Rightarrow \sigma_0(id_t)("s\_time\_counter") = upper(I_s(t)) \wedge$
$upper(I_s(t)) \neq \infty \wedge s_0.I(t) \leq upper(I_s(t)) \Rightarrow s_0.I(t) = \sigma_0(id_t)("s\_time\_counter")$.

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

1. $\boxed{upper(I_s(t)) = \infty \wedge s_0.I(t) \leq lower(I_s(t)) \Rightarrow s_0.I(t) = \sigma_0(id_t)("s\_time\_counter")}$

2. $\boxed{upper(I_s(t)) = \infty \wedge s_0.I(t) > lower(I_s(t)) \Rightarrow \sigma_0(id_t)("s\_time\_counter") = lower(I_s(t))}$

3. $\boxed{upper(I_s(t)) \neq \infty \wedge s_0.I(t) > upper(I_s(t)) \Rightarrow \sigma_0(id_t)("s\_time\_counter") = upper(I_s(t))}$

4. $\boxed{upper(I_s(t)) \neq \infty \wedge s_0.I(t) \leq upper(I_s(t)) \Rightarrow s_0.I(t) = \sigma_0(id_t)("s\_time\_counter")}$

By construction and by definition of id_p, there exist gm_p, ipm_p, opm_p s.t. $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$.
Then, let us show the 4 previous points.

1. Assuming that $upper(I_s(t)) = \infty \wedge s_0.I(t) \leq lower(I_s(t))$, then let us show $\boxed{s_0.I(t) = \sigma_0(id_t)("s\_time\_counter").}$

   Rewriting $s_0.I(t)$ as 0, by definition of s_0, $\boxed{\sigma_0(id_t)("s\_time\_counter") = 0.}$

   By property of the $\mathcal{H}$-VHDL initialization relation, $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$, and through the examination of the `time_counter` process defined in the transition design architecture, we can deduce $\sigma_0(id_t)("s\_time\_counter") = 0$.

2. Assuming that $upper(I_s(t)) = \infty$ and $s_0.I(t) > lower(I_s(t))$, let us show $\boxed{\sigma_0(id_t)(\text{"}s\_time\_counter\text{"}) = lower(I_s(t))}$.

   By definition, $lower(I_s(t)) \in \mathbb{N}^*$ and $s_0.I(t) = 0$. Then, $lower(I_s(t)) < 0$ is a contradiction.

3. Assuming that $upper(I_s(t)) \neq \infty$ and $s_0.I(t) > upper(I_s(t))$, let us show $\boxed{\sigma_0(id_t)(\text{"}s\_time\_counter\text{"}) = upper(I_s(t))}$.

   By definition, $upper(I_s(t)) \in \mathbb{N}^*$ and $s_0.I(t) = 0$. Then, $upper(I_s(t)) < 0$ is a contradiction.

4. Assuming that $upper(I_s(t)) \neq \infty$ and $s_0.I(t) \leq upper(I_s(t))$, let us show $\boxed{s_0.I(t) = \sigma_0(id_t)(\text{"}s\_time\_counter\text{"})}$.

   Rewriting $s_0.I(t)$ as 0, by definition of s_0, $\boxed{\sigma_0(id_t)(\text{"}s\_time\_counter\text{"}) = 0.}$

   By property of the $\mathcal{H}$-VHDL initialization relation, $\texttt{comp}(id_t, \text{"}transition\text{"}, gm_t, ipm_t, opm_t) \in d.cs$, and through the examination of the `time_counter` process defined in the transition design architecture, we can deduce $\sigma_0(id_t)(\text{"}s\_time\_counter\text{"}) = 0$.

□

A.1.3 Initial states and reset orders

Lemma 4 (Initial States Equal Reset Orders). *For all $sitpn \in SITPN, d \in design, \gamma \in WM(sitpn, d)$, $\Delta \in ElDesign(d, \mathcal{D}_{\mathcal{H}}), \sigma_e, \sigma_0 \in \Sigma(\Delta)$ that verify the hypotheses of Definition 1, then $\forall t \in T_i, id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$, $s_0.reset_t(t) = \sigma_0(id_t)(\text{"}s\_reinit\_time\_counter\text{"})$.*

Proof. Given a $t \in T_i$ and an $id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$, let us show that $\boxed{s_0.reset_t(t) = \sigma_0(id_t)(\text{"}s\_reinit\_time\_counter\text{"}).}$
Rewriting $s_0.reset_t(t)$ as $false$, by definition of s_0, $\boxed{\sigma_0(id_t)(\text{"}s\_reinit\_time\_counter\text{"}) = false.}$

By construction and 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 $\mathcal{H}$-VHDL initialization relation, $\texttt{comp}(id_t, \text{"}transition\text{"}, gm_t, ipm_t, opm_t) \in d.cs$, and through the examination of the `reinit_time_counter_evaluation` process defined in the transition design architecture

we can deduce $\sigma_0(id_t)(\text{"}s\_reinit\_time\_counter\text{"}) = \prod_{i=0}^{\Delta(id_t)(\text{"}ian\text{"})-1} \sigma_0(id_t)(\text{"}rt\text{"})[i]$.

Rewriting $\sigma_0(id_t)(\text{"}s\_reinit\_time\_counter\text{"})$ as $\prod_{i=0}^{\Delta(id_t)(\text{"}ian\text{"})-1} \sigma_0(id_t)(\text{"}rt\text{"})[i]$,

$$\boxed{\prod_{i=0}^{\Delta(id_t)(\text{"}ian\text{"})-1} \sigma_0(id_t)(\text{"}rt\text{"})[i] = false.}$$

For all $t \in T$ (resp. $p \in P$), let $input(t)$ (resp. $input(p)$) be the set of input places of t (resp. input transitions of p), and let $output(t)$ (resp. $output(p)$) be the set of output places of t (resp. output transitions of p).

Let us perform case analysis on $input(t)$; there are 2 cases:

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

  By construction, <input_arcs_number $\Rightarrow$1> $\in gm_t$, and by property of the elaboration relation, and comp$(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$, we can deduce $\Delta(id_t)("ian") = 1$.

  By construction, < reinit_time(0) $\Rightarrow false$ >$\in ipm_t$, and by property of the initialization relation and comp$(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$, we can deduce $\sigma_0(id_t)("rt")[0] = false$.

  Rewriting $\Delta(id_t)("ian")$ as 1 and $\sigma_0(id_t)("rt")[0]$ as $false$, tautology.

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

  To prove the current goal, we can equivalently prove that
  $\boxed{\exists i \in [0, \Delta(id_t)("ian") - 1] \ s.t.\ \sigma_0(id_t)("rt")[i] = false.}$

  Since $input(t) \neq \emptyset$, $\exists p \ s.t.\ p \in input(t)$. Let us take such a $p \in input(t)$.

  By construction, for all $p \in P$, there exist $id_p \ s.t.\ \gamma(p) = id_p$.

  By construction and by definition of id_p, there exist gm_p, ipm_p, opm_p s.t. comp$(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$.

  By construction, there exist $i \in [0, |input(t)| - 1]$, $j \in [0, |output(p)| - 1]$, $id_{ji} \in Sigs(\Delta)$ s.t. <reinit_transitions_time(j) $\Rightarrow id_{ji}$> $\in opm_p$ and <reinit_time(i) $\Rightarrow id_{ji}$> $\in ipm_t$. Let us take such a i, j and id_{ji}.

  By construction and $input(t) \neq \emptyset$, <input_arcs_number $\Rightarrow |input(t)|$> $\in gm_t$.

  By property of the $\mathcal{H}$-VHDL elaboration relation and <input_arcs_number $\Rightarrow |input(t)|$> $\in gm_t$, we can deduce $\Delta(id_t)("ian") = |input(t)|$.

  Since $\Delta(id_t)("ian") = |input(t)|$ and we have an $i \in [0, |input(t)| - 1]$, then, we have an $i \in [0, \Delta(id_t)("ian") - 1]$. Let us take that i to prove the goal.

  Then, we must show $\boxed{\sigma_0(id_t)("rt")[i] = false.}$

  By property of the $\mathcal{H}$-VHDL initialization relation and <reinit_time(i) $\Rightarrow id_{ji}$> $\in ipm_t$, we can deduce $\sigma_0(id_t)("rt")[i] = \sigma_0("id_{ji}")$.

  Rewriting $\sigma_0(id_t)("rt")[i]$ as $\sigma_0("id_{ji}")$, $\boxed{\sigma_0("id_{ji}") = false.}$

  By property of the $\mathcal{H}$-VHDL initialization relation and < reinit_transitions_time(j) $\Rightarrow id_{ji}$ >$\in opm_p$, we can deduce $\sigma_0("id_{ji}") = \sigma_0(id_p)("rtt")[j]$.

  Rewriting $\sigma_0("id_{ji}")$ as $\sigma_0(id_p)("rtt")[j]$, $\boxed{\sigma_p^0("rtt")[j] = false.}$

  Since $t \in output(p)$, then we know that $output(p) \neq \emptyset$.

  Then, by construction, <output_arcs_number $\Rightarrow |output(p)|$> $\in gm_p$.

  By property of the elaboration relation and <output_arcs_number $\Rightarrow$ $|output(p)|$> $\in gm_p$, we can deduce that $\Delta(id_p)("oan") = |output(p)|$.

  Since $\Delta(id_p)("oan") = |output(p)|$ and $j \in [0, |output(p)| - 1]$, then $j \in [0, \Delta(id_p)("oan") - 1]$.

  By property of the $\mathcal{H}$-VHDL initialization relation, comp$(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$, through the examination of the reinit_transitions_time_evaluation process defined in the place design architecture, and since $j \in [0, \Delta(id_p)("oan") - 1]$, $\sigma_0(id_p)("rtt")(j) = false$.

$\square$

A.1.4 Initial states and condition values

Lemma 5 (Initial States Equal Condition Values). *For all* $sitpn \in SITPN, d \in design, \gamma \in WM(sitpn, d)$, $\Delta \in ElDesign(d, \mathcal{D}_{\mathcal{H}}), \sigma_e, \sigma_0 \in \Sigma(\Delta)$ *that verify the hypotheses of Definition 1, then* $\forall c \in \mathcal{C}, id_c \in Ins(\Delta)$ *s.t.* $\gamma(c) = id_c$, $s_0.cond(c) = \sigma_0(id_c)$.

Proof. Given a $c \in \mathcal{C}$ and an $id_c \in Ins(\Delta)$ *s.t.* $\gamma(c) = id_c$, let's show that $\boxed{s_0.cond(c) = \sigma_0(id_c).}$

Rewriting $s_0.cond(c)$ as $false$, by definition of s_0, $\boxed{\sigma_0(id_c) = false.}$
By construction, id_c is an input port identifier of boolean type in the $\mathcal{H}$-VHDL design d.
By property, of the $\mathcal{H}$-VHDL elaboration relation, $\sigma_e(id_c) = false$, where $false$ is the default value associated to signals of the boolean type during the elaboration (see definition of default value in chapter $\mathcal{H}$-VHDL semantics).
By property of the $\mathcal{H}$-VHDL initialization relation, we have $\sigma_e(id_c) = \sigma_0(id_c)$ (i.e, input ports are not assigned during the initialization phase).
Rewriting $\sigma_e(id_c)$ as $false$, $\sigma_0(id_c) = false.$

□

A.1.5 Initial states and action executions

Correction: id_f is assigned by the reset block of the function process

Lemma 6 (Initial States Equal Action Executions). *For all* $sitpn \in SITPN$, $d \in design$, $\gamma \in WM(sitpn, d)$, $\Delta \in ElDesign(d, \mathcal{D}_{\mathcal{H}}), \sigma_e, \sigma_0 \in \Sigma(\Delta)$ *that verify the hypotheses of Definition 1, then* $\forall a \in \mathcal{A}, id_a \in Outs(\Delta)$ *s.t.* $\gamma(a) = id_a$, $s_0.ex(a) = \sigma_0(id_a)$.

Proof. Given a $a \in \mathcal{A}$ and an $id_a \in Outs(\Delta)$ *s.t.* $\gamma(a) = id_a$, let's show that $\boxed{s_0.ex(a) = \sigma_0(id_a).}$

Rewriting $s_0.ex(a)$ as $false$, by definition of s_0, $\boxed{\sigma_0(id_a) = false.}$
By construction, id_a is an output port identifier of boolean type in the $\mathcal{H}$-VHDL design d.
By property, of the $\mathcal{H}$-VHDL elaboration relation, $\sigma_e(id_a) = false$, where $false$ is the default value associated to signals of the boolean type during the elaboration (see definition of default value in chapter $\mathcal{H}$-VHDL semantics).
By construction, we know that the output port identifier id_a is assigned in the generated `action` process, only at the falling edge phase of the simulation cycle (i.e, the assignment takes place in a `falling` statement block).
By property of the $\mathcal{H}$-VHDL initialization relation, and we have $\sigma_e(id_a) = \sigma_0(id_a)$ (i.e, process `action` is idle during the initialization phase).
Rewriting $\sigma_e(id_a)$ as $false$, $\sigma_0(id_a) = false.$

□

A.1.6 Initial states and function executions

Correction: id_f is assigned by the reset block of the function process

Lemma 7 (Initial States Equal Function Executions). *For all* $sitpn \in SITPN$, $d \in design$, $\gamma \in WM(sitpn, d)$, $\Delta \in ElDesign(d, \mathcal{D}_{\mathcal{H}}), \sigma_e, \sigma_0 \in \Sigma(\Delta)$ *that verify the hypotheses of Definition 1, then* $\forall f \in \mathcal{F}, id_f \in Outs(\Delta)$ *s.t.* $\gamma(f) = id_f$, $s_0.ex(f) = \sigma_0(id_f)$.

Proof. Given a $f \in \mathcal{F}$ and an $id_f \in Outs(\Delta)$ $s.t.$ $\gamma(f) = id_f$, let's show that $\boxed{s_0.ex(f) = \sigma_0(id_f).}$

Rewriting $s_0.ex(f)$ as $false$, by definition of s_0, $\boxed{\sigma_0(id_f) = false.}$
By construction, id_f is an output port identifier of boolean type in the $\mathcal{H}$-VHDL design d.
By property, of the $\mathcal{H}$-VHDL elaboration relation, $\sigma_e(id_f) = false$, where $false$ is the default value associated to signals of the boolean type during the elaboration (see definition of default value in chapter $\mathcal{H}$-VHDL semantics).
By construction, we know that the output port identifier id_f is assigned in the generated `function` process (i.e, `function` is the process identifier), only at the rising edge phase of the simulation cycle (i.e, the assignment takes place in a `rising` statement block).
By property of the $\mathcal{H}$-VHDL initialization relation, and we have $\sigma_e(id_f) = \sigma_0(id_f)$ (i.e, process `function` is idle during the initialization phase).
Rewriting $\sigma_e(id_f)$ as $false$, $\sigma_0(id_f) = false.$

□

A.2 First Rising Edge

Definition 2 (First Rising Edge Hypotheses). *Given an $sitpn \in SITPN, d \in design, \gamma \in WM(sitpn, d), \Delta \in ElDesign(d, \mathcal{D}_{\mathcal{H}}), \sigma_e, \sigma_0, \sigma_i, \sigma_{\uparrow}, \sigma \in \Sigma(\Delta)$, $E_c \in \mathbb{N} \to \mathcal{C} \to \mathbb{B}$, $E_p \in (\mathbb{N} \times \{\uparrow, \downarrow\}) \to Ins(\Delta) \to value$, $\tau \in \mathbb{N}$, assume that:*

- $\lfloor sitpn \rfloor_{\mathcal{H}} = (d, \gamma)$ *and* $\mathcal{D}_{\mathcal{H}}, \emptyset \vdash d \xrightarrow{elab} (\Delta, \sigma_e)$ *and* $\gamma \vdash E_p \stackrel{env}{=} E_c$
- σ_0 *is the initial state of* Δ: $\Delta, \sigma_e \vdash d.cs \xrightarrow{init} \sigma_0$
- $E_c, \tau \vdash s_0 \xrightarrow{\uparrow_0} s_0$
- $\mathtt{Inject}_{\uparrow}(\sigma_0, E_p, \tau, \sigma_i)$ *and* $\Delta, \sigma_i \vdash \mathrm{d.cs} \xrightarrow{\uparrow} \sigma_{\uparrow}$ *and* $\Delta, \sigma_{\uparrow} \vdash \mathrm{d.cs} \xrightarrow{\theta} \sigma$

Lemma 8 (First Rising Edge). *For all $sitpn, d, \gamma, \Delta, \sigma_e, \sigma_0, \sigma_i, \sigma_{\uparrow}, \sigma, E_c, E_p, \tau$ that verify the hypotheses of Def. 2, then $\gamma, E_c, \tau \vdash s_0 \stackrel{\uparrow}{\sim} \sigma$.*

Proof. By definition of **??**, 6 subgoals.

1. $\forall p \in P, id_p \in Comps(\Delta), \sigma_p \in \Sigma(\Delta(id_p))$ $s.t.$ $\gamma(p) = id_p$ and $\sigma(id_p) = \sigma_p$, $s_0.M(p) = \sigma_p(''s\_marking'')$.
2. $\forall t \in T_i, id_t \in Comps(\Delta), \sigma_t \in \Sigma(\Delta(id_t))$ $s.t.$ $\gamma(t) = id_t$ and $\sigma(id_t) = \sigma_t$,
$upper(I_s(t)) = \infty \wedge s_0.I(t) \leq lower(I_s(t)) \Rightarrow s_0.I(t) = \sigma_t(''s\_tc'') \wedge$
$upper(I_s(t)) = \infty \wedge s_0.I(t) > lower(I_s(t)) \Rightarrow \sigma_t(''s\_tc'') = lower(I_s(t)) \wedge$
$upper(I_s(t)) \neq \infty \wedge s_0.I(t) > upper(I_s(t)) \Rightarrow \sigma_t(''s\_tc'') = upper(I_s(t)) \wedge$
$upper(I_s(t)) \neq \infty \wedge s_0.I(t) \leq upper(I_s(t)) \Rightarrow s_0.I(t) = \sigma_t(''s\_tc'')$.
3. $\forall t \in T_i, id_t \in Comps(\Delta), \sigma_t \in \Sigma(\Delta(id_t))$ $s.t.$ $\gamma(t) = id_t$ and $\sigma(id_t) = \sigma_t$, $s_0.reset_t(t) = \sigma_t(''s\_reinit\_time\_counter'')$.
4. $\forall a \in \mathcal{A}, id_a \in Outs(\Delta)$ $s.t.$ $\gamma(a) = id_a$, $s_0.ex(a) = \sigma(id_a)$.

5. $\forall f \in \mathcal{F}, id_f \in Outs(\Delta)$ *s.t.* $\gamma(f) = id_f$, $s_0.ex(f) = \sigma(id_f)$.

6. $\forall t \in T_i, id_t \in Comps(\Delta)$ *s.t.* $\gamma(t) = id_t$,
$t \in Sens(s.M) \Leftrightarrow \sigma(id_t)(\text{"}s\_enabled\text{"}) = \mathtt{true}$.

7. $\forall t \in T, id_t \in Comps(\Delta)$ *s.t.* $\gamma(t) = id_t$,
$$\sigma(id_t)(\text{"}s\_condition\_combination\text{"}) = \prod_{c \in conds(t)} \begin{cases} E_c(\tau, c) & if\ \mathbb{C}(t,c) = 1 \\ \mathtt{not}(E_c(\tau, c)) & if\ \mathbb{C}(t,c) = -1 \end{cases}$$
where $conds(t) = \{c \in \mathcal{C} \mid \mathbb{C}(t,c) = 1 \vee \mathbb{C}(t,c) = -1\}$.

– Apply Lemma First Rising Edge Equal Marking to solve 1.

– Apply Lemma First Rising Edge Equal Time Counters to solve 2.

– Apply Lemma First Rising Edge Equal Reset Orders to solve 3.

– Apply Lemma "First Rising Edge Equal Action Executions" to solve 4.

– Apply Lemma "First Rising Edge Equal Function Executions " to solve 5.

– Apply Lemma "Rising Edge Equal Sensitized" to solve 6.

– Apply Lemma "Rising Edge Equal Condition Combination" to solve 7.

□

A.2.1 First rising edge and marking

Lemma 9 (First Rising Edge Equal Marking). *For all* $sitpn, d, \gamma, \Delta$, $\sigma_e, \sigma_0, \sigma_i, \sigma_\uparrow, \sigma$, E_c, E_p, τ *that verify the hypotheses of Def.* 2, *then* $\forall p \in P, id_p \in Comps(\Delta), \sigma_p \in \Sigma(\Delta(id_p))$ *s.t.* $\gamma(p) = id_p$ *and* $\sigma(id_p) = \sigma_p$, $s_0.M(p) = \sigma_p(\text{"}s\_marking\text{"})$.

Proof. Given a p, id_p, σ_p s.t. $\gamma(p) = id_p$ and $\sigma(id_p) = \sigma_p$, let us show that $\boxed{s_0.M(p) = \sigma_p(\text{"}s\_marking\text{"}).}$
By definition of id_p, there exist gm_p, ipm_p, opm_p *s.t.* $\mathtt{comp}(id_p, \text{"}place\text{"}, gm_p, ipm_p, opm_p) \in d.cs$.

By property of the $\mathcal{H}$-VHDL elaboration relation, the $\mathcal{H}$-VHDL initialization relation, the $\mathtt{Inject}_\uparrow$ relation, the $\mathcal{H}$-VHDL rising edge relation and $\mathtt{comp}(id_p, \text{"}place\text{"}, gm_p, ipm_p, opm_p) \in d.cs$, there exist a $\sigma_p^e, \sigma_p^0, \sigma_p^{injr}, \sigma_p^r \in \Sigma(\Delta)$ s.t. $\sigma_e(id_p) = \sigma_p^e$ and $\sigma_0(id_p) = \sigma_p^0$ and $\sigma_i(id_p) = \sigma_p^{injr}$ and $\sigma_r(id_p) = \sigma_p^r$
.

> From the elaboration to the end of the first rising edge phase, an internal state is associated with the P component instance id_p in the component store of the top-level design d.

By property of the $\mathcal{H}$-VHDL rising edge relation, the P design behavior (process "$\mathtt{marking}$"), and $\mathtt{comp}(id_p, \text{"}place\text{"}, gm_p, ipm_p, opm_p) \in d.cs$, then
$\sigma_p^r(\text{"}s\_marking\text{"}) = \sigma_p^{injr}(\text{"}s\_marking\text{"}) + \sigma_p^{injr}(\text{"}s\_input\_token\_sum\text{"}) - \sigma_p^{injr}(\text{"}s\_output\_token\_sum\text{"})$.

> Result of the execution of the process "$\mathtt{marking}$" that performs the signal assignment
> $\mathtt{s\_marking} \Leftarrow \mathtt{s\_marking} + \mathtt{s\_input\_token\_sum} - \mathtt{s\_output\_token\_sum}$.

By property of the $\mathcal{H}$-VHDL stabilize relation, the P design behavior (process "$\mathtt{marking}$"), and $\mathtt{comp}(id_p, \text{"}place\text{"}, gm_p, ipm_p, opm_p) \in d.cs$, then $\sigma_p^r(\text{"}s\_marking\text{"}) = \sigma_p(\text{"}s\_marking\text{"})$.

As it is only assigned by the process “`marking`”, and as the process “`marking`” is never executed during the stabilization phase, the “`s_marking`” signal has an invariant value during the stabilization phase.

Rewriting $\sigma_p(\text{"}s\_marking\text{"})$ as $\sigma_p^r(\text{"}s\_marking\text{"})$, and $\sigma_p^r(\text{"}s\_marking\text{"})$ as $\sigma_p^{injr}(\text{"}s\_marking\text{"}) + \sigma_p^{injr}(\text{"}s\_input\_token\_sum\text{"}) - \sigma_p^{injr}(\text{"}s\_output\_token\_sum\text{"})$, $\boxed{s_0.M(p) = \sigma_p^{injr}(\text{"}s\_marking\text{"}) + \sigma_p^{injr}(\text{"}s\_input\_token\_sum\text{"}) - \sigma_p^{injr}(\text{"}s\_output\_token\_sum\text{"}).}$

By property of the $\texttt{Inject}_\uparrow$ relation, $\sigma_p^{injr}(\text{"}s\_marking\text{"}) = \sigma_p^0(\text{"}s\_marking\text{"})$ and $\sigma_p^{injr}(\text{"}s\_input\_token\_sum\text{"}) = \sigma_p^0(\text{"}s\_input\_token\_sum\text{"})$ and $\sigma_p^{injr}(\text{"}s\_output\_token\_sum\text{"}) = \sigma_p^0(\text{"}s\_output\_token\_sum\text{"})$. Rewriting the above, $\boxed{s_0.M(p) = \sigma_p^0(\text{"}s\_marking\text{"}) + \sigma_p^0(\text{"}s\_input\_token\_sum\text{"}) - \sigma_p^0(\text{"}s\_output\_token\_sum\text{"}).}$

Detail the two lemmas giving this property.

By property of the $\mathcal{H}$-VHDL initialization relation, $\sigma_p^0(\text{"}s\_input\_token\_sum\text{"}) = 0$ and $\sigma_p^0(\text{"}s\_output\_token\_sum\text{"}) = 0$. Rewriting the above, $\boxed{s_0.M(p) = \sigma_p^0(\text{"}s\_marking\text{"}).}$

Applying the Initial States Equal Marking lemma, $s_0.M(p) = \sigma_p^0(\text{"}s\_marking\text{"})$. □

A.2.2 First rising edge and time counters

Lemma 10 (First Rising Edge Equal Time Counters). *For all $sitpn, d, \gamma, \Delta, \sigma_e, \sigma_0, \sigma_i, \sigma_\uparrow, \sigma, E_c, E_p, \tau$ that verify the hypotheses of Def. 2, then*
$\forall t \in T_i, id_t \in Comps(\Delta), \sigma_t \in \Sigma(\Delta(id_t))$ *s.t.* $\gamma(t) = id_t$ *and* $\sigma(id_t) = \sigma_t$,
$upper(I_s(t)) = \infty \wedge s_0.I(t) \leq lower(I_s(t)) \Rightarrow s_0.I(t) = \sigma_t(\text{"}s\_tc\text{"}) \wedge$
$upper(I_s(t)) = \infty \wedge s_0.I(t) > lower(I_s(t)) \Rightarrow \sigma_t(\text{"}s\_tc\text{"}) = lower(I_s(t)) \wedge$
$upper(I_s(t)) \neq \infty \wedge s_0.I(t) > upper(I_s(t)) \Rightarrow \sigma_t(\text{"}s\_tc\text{"}) = upper(I_s(t)) \wedge$
$upper(I_s(t)) \neq \infty \wedge s_0.I(t) \leq upper(I_s(t)) \Rightarrow s_0.I(t) = \sigma_t(\text{"}s\_tc\text{"})$.

Proof. Given a $t \in T_i$, an $id_t \in Comps(\Delta)$ and a $\sigma_t \in \Sigma(\Delta(id_t))$ s.t. $\gamma(t) = id_t$ and $\sigma(id_t) = \sigma_t$, let's show that:

1. $\boxed{upper(I_s(t)) = \infty \wedge s_0.I(t) \leq lower(I_s(t)) \Rightarrow s_0.I(t) = \sigma_t(\text{"}s\_tc\text{"})}$
2. $\boxed{upper(I_s(t)) = \infty \wedge s_0.I(t) > lower(I_s(t)) \Rightarrow \sigma_t(\text{"}s\_tc\text{"}) = lower(I_s(t))}$
3. $\boxed{upper(I_s(t)) \neq \infty \wedge s_0.I(t) > upper(I_s(t)) \Rightarrow \sigma_t(\text{"}s\_tc\text{"}) = upper(I_s(t))}$
4. $\boxed{upper(I_s(t)) \neq \infty \wedge s_0.I(t) \leq upper(I_s(t)) \Rightarrow s_0.I(t) = \sigma_t(\text{"}s\_tc\text{"})}$

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 $\mathcal{H}$-VHDL elaboration relation, the $\mathcal{H}$-VHDL initialization relation, the $\texttt{Inject}_\uparrow$ relation, the $\mathcal{H}$-VHDL rising edge relation and $\texttt{comp}(id_t, \text{"}transition\text{"}, gm_t, ipm_t, opm_t) \in d.cs$, there exist a $\sigma_t^e, \sigma_t^0, \sigma_t^{injr}, \sigma_t^r \in \Sigma(\Delta)$ s.t. $\sigma_e(id_t) = \sigma_t^e$ and $\sigma_0(id_t) = \sigma_t^0$ and $\sigma_i(id_t) = \sigma_t^{injr}$ and $\sigma_r(id_t) = \sigma_t^r$
.

> From the elaboration to the end of the first rising edge phase, an internal state is associated with the T component instance id_t in the component store of the top-level design d.

Then, let's show the 4 previous subgoals.

1. Assume $upper(I_s(t)) = \infty \wedge s_0.I(t) \leq lower(I_s(t))$, then show $\boxed{s_0.I(t) = \sigma_t(''s\_tc'').}$
   By property of the $\texttt{Inject}_{\uparrow}$ relation, the $\mathcal{H}$-VHDL rising edge and stabilize relations, and $\texttt{comp}(id_t, ''transition'', gm_t, ipm_t, opm_t) \in d.cs$, $\sigma_t(''s\_tc'') = \sigma_t^0(''s\_tc'')$.

   > The above equality is deduced from the two following facts:
   >
   > - The process "`time_counter`" is the only process that assigns signal `s_tc` in the T component behavior, and it is never executed during the rising edge and stabilization phases.
   > - The values of component instances' internal signals are invariant through the $\texttt{Inject}_{\uparrow}$ relation.

   Rewriting $\sigma_t(''s\_tc'')$ as $\sigma_t^0(''s\_tc'')$, $\boxed{s_0.I(t) = \sigma_t^0(''s\_tc'').}$

   Applying the Initial States Equal Time Counters lemma, $s_0.I(t) = \sigma_t^0(''s\_tc'')$.

2. Assume $upper(I_s(t)) = \infty \wedge s_0.I(t) > lower(I_s(t))$, then show $\boxed{\sigma_t(''s\_tc'') = lower(I_s(t))}$. By definition, $lower(I_s(t)) \in \mathbb{N}^*$ and $s_0.I(t) = 0$. Then, $lower(I_s(t)) < 0$ is a contradiction.

3. Assume $upper(I_s(t)) \neq \infty \wedge s_0.I(t) > upper(I_s(t))$, then show $\boxed{\sigma_t(''s\_tc'') = upper(I_s(t))}$. By definition, $upper(I_s(t)) \in \mathbb{N}^*$ and $s_0.I(t) = 0$. Then, $upper(I_s(t)) < 0$ is a contradiction.

4. Assume $upper(I_s(t)) \neq \infty \wedge s_0.I(t) \leq upper(I_s(t))$, then show $\boxed{s_0.I(t) = \sigma_t(''s\_tc'')}$.

   By property of the $\texttt{Inject}_{\uparrow}$ relation, the $\mathcal{H}$-VHDL rising edge and stabilize relations, and $\texttt{comp}(id_t, ''transition'', gm_t, ipm_t, opm_t) \in d.cs$, $\sigma_t(''s\_tc'') = \sigma_t^0(''s\_tc'')$.

   Rewriting $\sigma_t(''s\_tc'')$ as $\sigma_t^0(''s\_tc'')$, $\boxed{s_0.I(t) = \sigma_t^0(''s\_tc'').}$

   Applying the Initial States Equal Time Counters lemma, $s_0.I(t) = \sigma_t^0(''s\_tc'')$.

□

A.2.3 First rising edge and reset orders

Lemma 11 (First Rising Edge Equal Reset Orders). *For all $sitpn, d, \gamma, \Delta, \sigma_e, \sigma_0, \sigma_i, \sigma_{\uparrow}, \sigma, E_c, E_p, \tau$ that verify the hypotheses of Def. 2, then*
$\forall t \in T, id_t \in Comps(\Delta)$ *s.t.* $\gamma(t) = id_t$,
$s_0.reset_t(t) = \sigma(id_t)(''s\_reinit\_time\_counter'')$.

Proof. Given a $t \in T$ and an $id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$, let us show that $\boxed{s_0.reset_t(t) = \sigma(id_t)(''srtc'').}$
By construction and 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 $\texttt{comp}(id_t, ''transition'', gm_t, ipm_t, opm_t) \in d.cs$, then $\sigma(id_t)(''srtc'') = \sum_{i=0}^{\Delta(id_t)(''input\_arcs\_number'')-1} \sigma(id_t)(''reinit\_time'')[i]$.

$$\boxed{s_0.reset_t(t) = \sum_{i=0}^{\Delta(id_t)(''ian'')-1} \sigma(id_t)(''rt'')[i].}$$

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 $\mathcal{H}$-VHDL elaboration relation, then $\Delta(id_t)(''ian'') = 1$. By construction, $< \texttt{reinit\_time(0)} \Rightarrow \texttt{false} > \in ipm_t$, and by property of the $\mathcal{H}$-VHDL stabilize relation, $\sigma(id_t)(''rt'')[0] = false$.

  Rewriting $\Delta(id_t)(''ian'')$ as 1 and $\sigma(id_t)(''rt'')[0]$ as $false$, and by definition of s_0, $s_0.reset_t(t) = \sum_{i=0}^{\Delta(''ian'')-1} \sigma(id_t$

- **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, then $\Delta(id_t)(''ian'') = |input(t)|$.

  Rewriting $\Delta(id_t)(''ian'')$ as $|input(t)|$, $\boxed{s_0.reset_t(t) = \sum_{i=0}^{|input(t)|-1} \sigma(id_t)(''rt'')[i].}$

  By definition of s_0, $s_0.reset_t(t) = false$. Rewriting $s_0.reset_t(t)$ as $false$, $\boxed{\sum_{i=0}^{|input(t)|-1} \sigma(id_t)(''rt'')[i] = false.}$

  Given a $i \in [0, |input(t)| - 1]$, let us show $\boxed{\sigma(id_t)(''rt'')[i] = false.}$

  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 construction and 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 for all $i \in [0, |input(t)| - 1]$, there exist $j \in [0, |output(p)| - 1]$ and $id_{ji} \in Sigs(\Delta)$ s.t. $<\texttt{reinit\_transition\_time(j)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in opm_p$ and $<\texttt{reinit\_time(i)} \Rightarrow \texttt{id}_{\texttt{ji}}>$ ipm_t.

  By property of the $\mathcal{H}$-VHDL stabilize relation, $<\texttt{reinit\_transition\_time(j)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in opm_p$ and $<\texttt{reinit\_time(i)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in ipm_t$, then $\sigma(id_t)(''rt'')[i] = \sigma(id_{ji}) = \sigma(id_p)(''rtt'')[j]$.

  Rewriting $\sigma(id_t)(''rt'')[i]$ as $\sigma(id_{ji})$ and $\sigma(id_{ji})$ as $\sigma(id_p)(''rtt'')[j]$, $\boxed{\sigma(id_p)(''rtt'')[j] = false.}$

  By property of the $\mathcal{H}$-VHDL rising edge and stabilize relations,

$$\begin{aligned}\sigma(id_p)(''rtt'')[j] =& ((\sigma_0(id_p)(''oat'')[j] = \texttt{BASIC} + \sigma_0(id_p)(''oat'')[j] = \texttt{TEST}) \\ & .(\sigma_0(id_p)(''sm'') - \sigma_0(id_p)(''sots'') < \sigma_0(id_p)(''oaw'')[j]) \\ & .(\sigma_0(id_p)(''sots'') > 0)) \\ & + (\sigma_0(id_p)(''otf'')[j])\end{aligned}$$

Rewriting the goal with the above equation,

$$\boxed{\begin{aligned} false =&((\sigma_0(id_p)(''oat'')[j] = \texttt{BASIC} + \sigma_0(id_p)(''oat'')[j] = \texttt{TEST})\\ &.(\sigma_0(id_p)(''sm'') - \sigma_0(id_p)(''sots'') < \sigma_0(id_p)(''oaw'')[j])\\ &.(\sigma_0(id_p)(''sots'') > 0))\\ &+ (\sigma_0(id_p)(''otf'')[j]) \end{aligned}}$$

Add a lemma + proof in section initial states for fired = false after initialization.

By property of the $\mathcal{H}$-VHDL initialization and the $\texttt{Inject}_{\uparrow}$ relations, then $\sigma_0(id_p)(''otf'')[j] = false$. Rewriting $\sigma_0(id_p)(''otf'')[j]$ as $false$ and simplifying the goal,

$$\boxed{\begin{aligned} false =&((\sigma_0(id_p)(''oat'')[j] = \texttt{BASIC} + \sigma_0(id_p)(''oat'')[j] = \texttt{TEST})\\ &.(\sigma_0(id_p)(''sm'') - \sigma_0(id_p)(''sots'') < \sigma_0(id_p)(''oaw'')[j])\\ &.(\sigma_0(id_p)(''sots'') > 0)) \end{aligned}}$$

Add a lemma + proof in section initial states for output token sum = 0 after initialization.

By property of the $\mathcal{H}$-VHDL initialization and the $\texttt{Inject}_{\uparrow}$ relations, then $\sigma_0(id_p)(''sots'') = 0$. Rewriting $\sigma_0(id_p)(''sots'')$ as 0 and simplifying the goal, $false = false$

□

A.2.4 First rising edge and action executions

Lemma 12 (First Rising Edge Equal Action Executions)**.** *For all $sitpn, d, \gamma, \Delta, \sigma_e, \sigma_0, \sigma_i, \sigma_{\uparrow}, \sigma, E_c, E_p, \tau$ that verify the hypotheses of Def. 2, then*
$\forall a \in \mathcal{A}, id_a \in Outs(\Delta)$ *s.t.* $\gamma(a) = id_a,\ s_0.ex(a) = \sigma(id_a)$.

Proof. Given an $a \in \mathcal{A}$ and an $id_a \in Outs(\Delta)$ s.t. $\gamma(a) = id_a$, let us show that $\boxed{s_0.ex(a) = \sigma(id_a).}$

Rewriting $s_0.ex(a)$ as $false$, by definition of s_0, $\boxed{\sigma(id_a) = false.}$
By construction, id_a is an output port identifier of boolean type in the $\mathcal{H}$-VHDL design d assigned only during a falling edge phase in the ‘‘`action`’’ process.
By property of the $\mathcal{H}$-VHDL $\texttt{Inject}_{\uparrow}$, rising edge and stabilize relations, then $\sigma(id_a) = \sigma_0(id_a)$.
Thanks to the Lemma Initial States Equal Action Executions, $\sigma_0(id_a) = false$.
Rewriting $\sigma(id_a)$ as $\sigma_0(id_a)$, and $\sigma_0(id_a)$ as $false$, $false = false.$

□

A.2.5 First rising edge and function executions

Lemma 13 (First Rising Edge Equal Function Executions)**.** *For all $sitpn, d, \gamma, \Delta, \sigma_e, \sigma_0, \sigma_i, \sigma_{\uparrow}, \sigma, E_c, E_p, \tau$ that verify the hypotheses of Def. 2, then*
$\forall f \in \mathcal{F}, id_f \in Outs(\Delta)$ *s.t.* $\gamma(f) = id_f,\ s_0.ex(f) = \sigma(id_f)$.

Proof. Given an $f \in \mathcal{F}$ and an $id_f \in Outs(\Delta)$ s.t. $\gamma(f) = id_f$, let us show that $\boxed{s_0.ex(f) = \sigma(id_f).}$

Rewriting $s_0.ex(f)$ as $false$, by definition of s_0, $\boxed{\sigma(id_f) = false.}$

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 and the stabilize relation, then
  $\sigma(id_f) = false.$

- **CASE** $trs(f) \neq \emptyset$:
  By construction, $\texttt{id}_\texttt{f} \Leftarrow \texttt{id}_{\texttt{ft}_\texttt{0}} + \cdots + \texttt{id}_{\texttt{ft}_\texttt{n}} \in ss_\uparrow$ where $ss_\uparrow$ is the part of the ‘‘`function`’’ process body executed during the rising edge phase, and $n = |trs(f)| - 1$, and for all $i \in [0, n-1]$, id_{ft_i} is a internal signal of design d.

  By property of the $\texttt{Inject}_\uparrow$, the $\mathcal{H}$-VHDL rising edge and stabilize relation, then $\sigma(id_f) = \sigma_0(id_{ft_0}) + \cdots + \sigma_0(id_{ft_n})$.

  Rewriting $\sigma(id_f)$ as $\sigma_0(id_{ft_0}) + \cdots + \sigma_0(id_{ft_n})$, then
  $\boxed{\sigma_0(id_{ft_0}) + \cdots + \sigma_0(id_{ft_n}) = false.}$

  By construction, for all id_{ft_i}, there exist a $t_i \in trs(f)$ and an id_{t_i} s.t. $\gamma(t_i) = id_{t_i}$.

  By definition of id_{t_i}, there exist gm_{t_i}, ipm_{t_i} and opm_{t_i} s.t. $\texttt{comp}(id_{t_i}, ''transition'', gm_{t_i}, ipm_{t_i}, opm_{t_i}) \in d.cs$.

  By construction, $<\texttt{fired} \Rightarrow \texttt{id}_{\texttt{ft}_\texttt{i}}> \in opm_{t_i}$, and by property of the initialization relation $\sigma_0(id_{ft_i}) = \sigma_0(id_{t_i})(''fired'')$.

  Rewriting $\sigma_0(id_{ft_i})$ as $\sigma_0(id_{t_i})(''fired'')$, then
  $\boxed{\sigma_0(id_{t_0})(''fired'') + \cdots + \sigma_0(id_{t_n})(''fired'') = false.}$

  By property of the initialization relation, we know that for all $t \in T$ and $id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$, then $\sigma_0(id_t)(''fired'') = false$.

  Rewriting all $\sigma_0(id_{t_i})(''fired'')$ as $false$ and simplifying the goal, then
  $false = false.$

□

A.3 Rising Edge

Definition 3 (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* $\mathcal{D}_{\mathcal{H}}, \emptyset \vdash \mathrm{d} \xrightarrow{elab} \Delta, \sigma_e$
- $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$
- $E_c, \tau \vdash s \xrightarrow{\uparrow} s'$
- $\mathtt{Inject}_{\uparrow}(\sigma, E_p, \tau, \sigma_i)$ *and* $\mathcal{D}_{\mathcal{H}}, \Delta, \sigma_i \vdash \mathrm{d.cs} \xrightarrow{\uparrow} \sigma_{\uparrow}$ *and* $\mathcal{D}_{\mathcal{H}}, \Delta, \sigma_{\uparrow} \vdash \mathrm{d.cs} \xrightarrow{\leadsto} \sigma'$
- *State* σ *is a stable design state:* $\mathcal{D}_{\mathcal{H}}, \Delta, \sigma \vdash \mathrm{d.cs} \xrightarrow{comb} \sigma$

A.3.1 Rising Edge and Marking

Lemma 14 (Rising Edge Equal Marking)**.** *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. 3, then* $\forall p, id_p$ *s.t.* $\gamma(p) = id_p$ *and* $\sigma'(id_p) = \sigma'_p$, $s'.M(p) = \sigma'_p(''s\_marking'')$.

Proof. Given a $p \in P$, let us show $\boxed{s'.M(p) = \sigma'(id_p)(''s\_marking'').}$
By construction and by definition of id_p, there exist gm_p, ipm_p, opm_p s.t. $\mathtt{comp}(id_p, ''place'', gm_p, ipm_p, opm_p) \in d.cs$.By definition of the SITPN state transition relation on rising edge:

$$s'.M(p) = s.M(p) - \sum_{t \in Fired(s)} pre(p,t) + \sum_{t \in Fired(s)} post(t,p) \tag{A.1}$$

By property of the $\mathtt{Inject}_{\uparrow}$, the $\mathcal{H}$-VHDL rising edge and the stabilize relations, and $\mathtt{comp}(id_p, ''place'', gm_p, ipm_p, opm_p) \in d.cs$:

$$\begin{aligned} \sigma'(id_p)(''sm'') = \sigma(id_p)(''sm'') - \sigma(id_p)(''s\_output\_token\_sum'') \\ +\sigma(id_p)(''s\_input\_token\_sum'') \end{aligned} \tag{A.2}$$

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

$$s.M(p) = \sigma(id_p)(''sm'') \tag{A.3}$$

$$\sum_{t \in Fired(s)} pre(p,t) = \sigma(id_p)(''sots'') \tag{A.4}$$

$$\sum_{t \in Fired(s)} post(t,p) = \sigma(id_p)(''sits'') \tag{A.5}$$

Rewriting the goal with A.1, A.2, A.3, A.4 and A.5, tautology . ∎

A.3.2 Rising edge and condition combination

Lemma 15 (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. 3, then*
$\forall t \in T, id_t \in Comps(\Delta)$ *s.t.* $\gamma(t) = id_t$,

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

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 construction and 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
$\texttt{comp}(id_t, ''transition'', gm_t, ipm_t, opm_t) \in d.cs$:

$$\sigma'(id_t)(''scc'') = \prod_{i=0}^{\Delta(id_t)(''conditions\_number'')-1} \sigma'(id_t)(''input\_conditions'')[i] \tag{A.6}$$

Rewriting the goal with A.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** $conds(t) = \emptyset$:

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

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

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

  $$\Delta(id_t)(''cn'') = 1 \tag{A.7}$$
  $$\sigma'(id_t)(''ic'')[0] = \texttt{true} \tag{A.8}$$

  Rewriting the goal with A.7 and A.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:

  $$\Delta(id_t)(''cn'') = |conds(t)| \tag{A.9}$$

  Rewriting the goal with (A.9),

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

  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.
$\forall i \in [0, |conds(t)| - 1],\ \sigma'(id_t)(''ic'')[i] = \begin{cases} E_c(\tau, \iota(i)) & if\ \mathbb{C}(t, \iota(i)) = 1 \\ \mathtt{not}(E_c(\tau, \iota(i))) & if\ \mathbb{C}(t, \iota(i)) = -1 \end{cases}$

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

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

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

$$\mathbb{C}(t, \beta(i)) = 1 \lor \mathbb{C}(t, \beta(i)) = -1 \tag{A.10}$$

Case analysis on (A.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 $<\mathtt{input\_conditions(i)} \Rightarrow \mathtt{id_c}> \in ipm_t$.
  By property of the stabilize relation and $<\mathtt{input\_conditions(i)} \Rightarrow \mathtt{id_c}> \in ipm_t$:

  $$\sigma'(id_t)(''ic'')[i] = \sigma'(id_c) \tag{A.11}$$

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

  $$\sigma'(id_c) = \sigma_i(id_c) \tag{A.12}$$

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

  $$\sigma_i(id_c) = E_p(\tau, \uparrow)(id_c) \tag{A.13}$$

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

  $$E_p(\tau, \uparrow)(id_c) = E_c(\tau, c) \tag{A.14}$$

  Rewriting the goal with (A.11), (A.12), (A.13), (A.14), tautology.

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

  $$\sigma'(id_t)(''ic'')[i] = \mathtt{not}\ \sigma'(id_c) \tag{A.15}$$

Then, equations (A.12), (A.13) and (A.14) also hold this case.

Rewriting the goal with (A.15), (A.12), (A.13) and (A.14), tautology.

□

A.3.3 Rising edge and time counters

Lemma 16 (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. 3, then*
$\forall t \in T_i, id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$,
$(upper(I_s(t)) = \infty \wedge s'.I(t) \leq lower(I_s(t)) \Rightarrow s'.I(t) = \sigma'(id_t)("s\_time\_counter"))$
$\wedge (upper(I_s(t)) = \infty \wedge s'.I(t) > lower(I_s(t)) \Rightarrow \sigma'(id_t)("s\_time\_counter") = lower(I_s(t)))$
$\wedge (upper(I_s(t)) \neq \infty \wedge s'.I(t) > upper(I_s(t)) \Rightarrow \sigma'(id_t)("s\_time\_counter") = upper(I_s(t)))$
$\wedge (upper(I_s(t)) \neq \infty \wedge s'.I(t) \leq upper(I_s(t)) \Rightarrow s'.I(t) = \sigma'(id_t)("s\_time\_counter"))$.

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

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

By construction and 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, 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 $\boxed{s'.I(t) = \sigma'(id_t)("s\_time\_counter").}$

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

   $$\sigma'(id_t)("s\_time\_counter") = \sigma(id_t)("s\_time\_counter") \tag{A.16}$$

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

   $$s.I(t) = \sigma(id_t)("s\_time\_counter") \tag{A.17}$$

   Rewriting the goal with (A.16) and (A.17), tautology.

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

   Proved in the same fashion as 1.

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

   Proved in the same fashion as 1.

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

   Proved in the same fashion as 1.

$\square$

A.3.4 Rising edge and reset orders

Lemma 17 (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. 3, 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
$\boxed{s'.reset_t(t) = \sigma'(id_t)("s\_reinit\_time\_counter").}$
By construction and 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 $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$:

$$\sigma'(id_t)("srtc") = \sum_{i=0}^{\Delta(id_t)("input\_arcs\_number")-1} \sigma'(id_t)("reinit\_time")[i] \tag{A.18}$$

Rewriting the goal with (A.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:
  $$\Delta(id_t)("ian") = 1 \tag{A.19}$$

  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 $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$:

  $$\sigma'(id_t)("rt")[0] = \sigma'(id_{ft}) \tag{A.20}$$
  $$\sigma'(id_{ft}) = \sigma'(id_t)("fired") \tag{A.21}$$
  $$\sigma'(id_t)("fired") = \sigma'(id_t)("s\_fired") \tag{A.22}$$
  $$\sigma'(id_t)("s\_fired") = \sigma'(id_t)("s\_firable").\sigma'(id_t)("s\_priority\_combination") \tag{A.23}$$

  Rewriting the goal with (A.20), (A.35), (A.22) and (A.23),
  $\boxed{s'.reset_t(t) = \sigma'(id_t)("s\_firable").\sigma'(id_t)("s\_priority\_combination").}$

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

  $$\sigma'(id_t)("spc") = \prod_{i=0}^{\Delta(id_t)("ian")-1} \sigma'(id_t)("priority\_authorizations")[i] \tag{A.24}$$

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

$$\sigma'(id_t)(\text{"}priority\_authorizations\text{"})[0] = true \tag{A.25}$$

Rewriting the goal with (A.19), (A.24) and (A.25), and simplifying the equation, $\boxed{s'.reset_t(t) = \sigma'(id_t)(\text{"}s\_firable\text{"}).}$

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

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

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

  $$s'.reset_t(t) = \texttt{true} \tag{A.26}$$

  Rewriting the goal with (A.26), $\boxed{\sigma'(id_t)(\text{"}s\_firable\text{"}) = \texttt{true}.}$

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

  $$\sigma(id_t)(\text{"}s\_firable\text{"}) = \sigma'(id_t)(\text{"}s\_firable\text{"}) \tag{A.27}$$

  Rewriting the goal with (A.27), $\boxed{\sigma(id_t)(\text{"}s\_firable\text{"}) = \texttt{true}.}$

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

  $$t \in Firable(s) \Leftrightarrow \sigma(id_t)(\text{"}sfa\text{"}) = \texttt{true} \tag{A.28}$$

  Rewriting the goal with (A.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 $E_c, \tau \vdash s \xrightarrow{\uparrow} s'$:

  $$s'.reset_t(t) = \texttt{false} \tag{A.29}$$

  Rewriting the goal with (A.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 (A.27) holds.

  Rewriting the goal with (A.27), $\boxed{\sigma(id_t)(\text{"}s\_firable\text{"}) = false.}$

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

  $$t \notin Firable(s) \Leftrightarrow \sigma(id_t)(\text{"}sfa\text{"}) = \texttt{false} \tag{A.30}$$

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

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

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

  $$\Delta(id_t)("ian") = |input(t)| \tag{A.31}$$

  Rewriting the goal with (A.31), $\boxed{s'.reset_t(t) = \sum_{i=0}^{|input(t)|-1} \sigma'(id_t)("rt")[i].}$

  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 (A.26) holds.

    Rewriting the goal with (A.26), $\boxed{\sum_{i=0}^{|input(t)|-1} \sigma'(id_t)("rt")[i] = \texttt{true}.}$

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

    By construction and 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. <`reinit_transition_time(j)` $\Rightarrow$ $\texttt{id}_{\texttt{ji}}$> $\in opm_p$ and <`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, <`reinit_transition_time(j)` $\Rightarrow$ $\texttt{id}_{\texttt{ji}}$> $\in opm_p$ and <`reinit_time(i)` $\Rightarrow$ $\texttt{id}_{\texttt{ji}}$> $\in ipm_t$:

    $$\sigma'(id_t)("rt")[i] = \sigma'(id_{ji}) = \sigma'(id_p)("rtt")[j] \tag{A.32}$$

    Rewriting the goal with (A.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:

    $$\begin{aligned} \sigma'(id_p)("rtt")[j] = &((\sigma(id_p)("oat")[j] = \texttt{BASIC} + \sigma(id_p)("oat")[j] = \texttt{TEST}) \\ &.(\sigma(id_p)("sm") - \sigma(id_p)("sots") < \sigma(id_p)("oaw")[j]) \\ &.(\sigma(id_p)("sots") > 0)) \\ &+ \sigma(id_p)("otf")[j] \end{aligned} \tag{A.33}$$

    Rewriting the goal with (A.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:

$$\sigma(id_t)(''fired'') = \sigma(id_{ft}) = \sigma(id_p)(''otf'')[j] \tag{A.34}$$

Rewriting the goal with (A.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 $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$:

$$t \in Fired(s) \Leftrightarrow \sigma(id_t)(''fired'') = \texttt{true} \tag{A.35}$$

Knowing that $t \in Fired(s)$, we can rewrite the goal with the right side of (A.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 $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$:

    $$s'.reset_t(t) = \texttt{true} \tag{A.36}$$

    Rewriting the goal with (A.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 construction and 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

$<\mathtt{reinit\_time(i)} \Rightarrow \mathtt{id_{ji}}> \in ipm_t$. Let us take such an i, j and id_{ji}, and let us use i to prove the goal: $\boxed{\sigma'(id_t)("rt")[i] = \mathtt{true}.}$
By property of the stabilize relation, $<\mathtt{reinit\_transition\_time(j)} \Rightarrow \mathtt{id_{ji}}> \in opm_p$ and $<\mathtt{reinit\_time(i)} \Rightarrow \mathtt{id_{ji}}> \in ipm_t$:

$$\sigma'(id_t)("rt")[i] = \sigma'(id_{ji}) = \sigma'(id_p)("rtt")[j] \tag{A.37}$$

Rewriting the goal with (A.37), $\boxed{\sigma'(id_p)("rtt")[j] = \mathtt{true}.}$
By property of the $\mathtt{Inject}_{\uparrow}$, the $\mathcal{H}$-VHDL rising edge and the stabilize relations:

$$\begin{aligned}\sigma'(id_p)("rtt")[j] =&((\sigma(id_p)("oat")[j] = \mathtt{BASIC} + \sigma(id_p)("oat")[j] = \mathtt{TEST})\\ &.(\sigma(id_p)("sm") - \sigma(id_p)("sots") < \sigma(id_p)("oaw")[j])\\ &.(\sigma(id_p)("sots") > 0))\\ &+\sigma(id_p)("otf")[j]\end{aligned} \tag{A.38}$$

Rewriting the goal with (A.38),

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

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

$$\sigma'(id_p)("oat")[j] = \mathtt{BASIC} \tag{A.39}$$

$$\sigma'(id_p)("oaw")[j] = \omega \tag{A.40}$$

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

$$\sigma(id_p)("sm") = s.M(p) \tag{A.41}$$

$$\sigma(id_p)("sots") = \sum_{t_i \in Fired(s)} pre(p, t_i) \tag{A.42}$$

Rewriting the goal with (A.39), (A.40), (A.41) and (A.42), and simplifying the goal:

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

Thanks to the hypotheses 1 and 3:

$$s.M(p) - \sum_{t_i \in Fired(s)} pre(p, t_i) < \omega \quad = \quad \texttt{true} \tag{A.43}$$

$$\sum_{t_i \in Fired(s)} pre(p, t_i) > 0 \quad = \quad \texttt{true} \tag{A.44}$$

$$\tag{A.45}$$

Rewriting the goal with (A.43) and (A.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 $\forall \omega \in \mathbb{N}^*$, $pre(p, t) = (\omega, \texttt{basic}) \lor pre(p, t) = (\omega, \texttt{test}) \Rightarrow s.M(p) - \sum_{t_i \in Fired(s)} pre(p, t_i) \geq \omega$.

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

$$s'.reset_t(t) = \texttt{false} \tag{A.46}$$

Rewriting the goal with (A.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 $<\texttt{reinit\_transition\_time}(\texttt{j}) \Rightarrow \texttt{id}_{\texttt{ji}}> \in opm_p$ and $<\texttt{reinit\_time}(\texttt{i}) \Rightarrow \texttt{id}_{\texttt{ji}}> \in ipm_t$. Let us take such a p, id_p, gm_p, ipm_p, opm_p, j and id_{ji}.
By property of the stabilize relation, $<\texttt{reinit\_transition\_time}(\texttt{j}) \Rightarrow \texttt{id}_{\texttt{ji}}> \in opm_p$ and $<\texttt{reinit\_time}(\texttt{i}) \Rightarrow \texttt{id}_{\texttt{ji}}> \in ipm_t$:

$$\sigma'(id_t)(''rt'')[i] = \sigma'(id_{ji}) = \sigma'(id_p)(''rtt'')[j] \tag{A.47}$$

Rewriting the goal with (A.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:

$$\begin{aligned}\sigma'(id_p)(''rtt'')[j] = &((\sigma(id_p)(''oat'')[j] = \texttt{BASIC} + \sigma(id_p)(''oat'')[j] = \texttt{TEST})\\ &.(\sigma(id_p)(''sm'') - \sigma(id_p)(''sots'') < \sigma(id_p)(''oaw'')[j])\\ &.(\sigma(id_p)(''sots'') > 0))\\ &+ \sigma(id_p)(''otf'')[j]\end{aligned} \tag{A.48}$$

Rewriting the goal with (A.48),

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

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:

$$\sigma(id_t)(\text{"}fired\text{"}) = \sigma(id_{ft}) = \sigma(id_p)(\text{"}otf\text{"})[j] \tag{A.49}$$

Rewriting the goal with (A.49),

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

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

$$t \notin Fired(s) \Leftrightarrow \sigma(id_t)(\text{"}fired\text{"}) = \texttt{false} \tag{A.50}$$

Knowing that $t \notin Fired(s)$, we can rewrite the goal with the right side of (A.50) and simplify the goal (i.e, $\forall b \in \mathbb{B},\ b + \texttt{false} = b$):

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

Then, there are two cases:

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

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

   $$\sum_{t_i \in Fired(s)} pre(p, t_i) = \sigma(id_p)(\text{"}sots\text{"}) \tag{A.51}$$

   Rewriting the goal with (A.51) and $\sum\limits_{t_i \in Fired(s)} pre(p, t_i) = 0$, simplifying the goal: tautology.

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

   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 $\texttt{comp}(id_p, \text{"}place\text{"}, gm_p, ipm_p, opm_p) \in d.cs$:

$$\sigma(id_p)(\text{"}oaw\text{"})[j] \quad = \quad \omega \tag{A.52}$$

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

$$\sigma(id_p)(\text{"}sm\text{"}) \quad = \quad s.M(p) \tag{A.53}$$
$$\sigma(id_p)(\text{"}sots\text{"}) \quad = \quad \sum_{t_i \in Fired(s)} pre(p, t_i) \tag{A.54}$$

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:

$$s.M(p) - \sum_{t_i \in Fired(s)} pre(p, t_i) < \omega = \texttt{false} \tag{A.55}$$

Rewriting the goal with (A.52), (A.53), (A.54), and (A.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 $\texttt{comp}(id_p, \text{"}place\text{"}, gm_p, ipm_p, opm_p) \in d.cs$:

$$\sigma(id_p)(\text{"}oat\text{"})[j] = \texttt{INHIB} \tag{A.56}$$

Rewriting the goal with (A.56), and simplifying the goal, tautology.

□

A.3.5 Rising edge and action executions

Lemma 18 (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. 3, 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 $E_c, \tau \vdash s \xrightarrow{\uparrow} s'$:

$$s.ex(a) = s'.ex(a) \tag{A.57}$$

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:

$$\sigma(id_a) = \sigma'(id_a) \tag{A.58}$$

Rewriting the goal with (A.57) and (A.58), $\boxed{s.ex(a) = \sigma(id_a).}$

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

A.3.6 Rising edge and function executions

Lemma 19 (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. 3, 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 $E_c, \tau \vdash s \xrightarrow{\uparrow} s'$:

$$s'.ex(f) = \sum_{t \in Fired(s)} \mathbb{F}(t, f) \tag{A.59}$$

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 $\texttt{ps}("function", \emptyset, sl, ss) \in d.cs$:

  $$\sigma'(id_f) = false \tag{A.60}$$

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

  $$\sum_{t \in Fired(s)} \mathbb{F}(t, f) = \texttt{false} \tag{A.61}$$

  Rewriting the goal with (A.59), (A.60) and (A.61), tautology.

- **CASE** $trs(f) \neq \emptyset$:
  By construction, $\texttt{id}_\texttt{f} \Leftarrow \texttt{id}_{\texttt{ft}_0} + \cdots + \texttt{id}_{\texttt{ft}_\texttt{n}} \in ss_\uparrow$, 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 $\texttt{ps}("function", \emptyset, sl, ss) \in d.cs$:

  $$\sigma'(id_f) = \sigma(id_{ft_0}) + \cdots + \sigma(id_{ft_n}) \tag{A.62}$$

  Rewriting the goal with (A.59) and (A.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 $\boxed{\exists t \in Fired(s) \text{ s.t. } \mathbb{F}(t,f) = \texttt{true}.}$

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 $\texttt{comp}(id_{t_i}, \text{"}transition\text{"}, gm_{t_i}, ipm_{t_i}, opm_{t_i}) \in d.cs$ 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 $\texttt{comp}(id_{t_i}, \text{"}transition\text{"}, gm_{t_i}, ipm_{t_i}, opm_{t_i}) \in d.cs$:

$$\sigma(id_{t_i})(\text{"}fired\text{"}) = \sigma(id_{ft_i}) \tag{A.63}$$

Thanks to (A.63) and $\sigma(id_{ft_i}) = \texttt{true}$, we can deduce that $\sigma(id_{t_i})(\text{"}fired\text{"}) = \texttt{true}$.

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

$$t_i \in Fired(s) \Leftrightarrow \sigma(id_{t_i})(\text{"}fired\text{"}) = \texttt{true} \tag{A.64}$$

Thanks to (A.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 $\boxed{\forall t \in Fired(s) \text{ s.t. } \mathbb{F}(t,f) = \texttt{false}.}$

  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 $\texttt{comp}(id_t, \text{"}transition\text{"}, gm_t, ipm_t, opm_t) \in d.cs$ 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 $\texttt{comp}(id_t, \text{"}transition\text{"}, gm_t, ipm_t, opm_t) \in d.cs$, equation (A.63) holds.
    By property of $\gamma \vdash s \overset{\downarrow}{\sim} \sigma$, equation (A.64) holds.
    Thanks to (A.63) and (A.64), we can deduce that $\sigma(id_{ft_i}) = \texttt{true}$.
    Then, $\sigma(id_{ft_i}) = \texttt{true}$ contradicts $\sigma(id_{ft_0}) + \cdots + \sigma(id_{ft_n}) = \texttt{false}$.

□

A.3.7 Rising edge and sensitization

Lemma 20 (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. 3, then*
$\forall t \in T, id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t, t \in Sens(s'.M) \Leftrightarrow \sigma'(id_t)(\text{"}s\_enabled\text{"}) = \texttt{true}$.

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

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

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

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

$$\sigma'(id_t)(\text{"}se\text{"}) = \prod_{i=0}^{\Delta(id_t)(\text{"}ian\text{"})-1} \sigma'(id_t)(\text{"}input\_arcs\_valid\text{"})[i] \tag{A.65}$$

   Rewriting the goal with (A.65), $\boxed{\prod_{i=0}^{\Delta(id_t)(\text{"}ian\text{"})-1} \sigma'(id_t)(\text{"}iav\text{"})[i] = \mathtt{true}.}$

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

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

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

   - **CASE** $input(t) = \emptyset$:
     By construction, $<\mathtt{input\_arcs\_number} \Rightarrow \mathtt{1}> \in gm_t$ and $<\mathtt{input\_arcs\_valid(0)} \Rightarrow \mathtt{true}> \in ipm_t$.
     By property of the elaboration and stabilize relations and $\mathtt{comp}(id_t, \text{"}transition\text{"}, gm_t, ipm_t, opm_t) \in d.cs$:

$$\Delta(id_t)(\text{"}ian\text{"}) = 1 \tag{A.66}$$
$$\sigma'(id_t)(\text{"}iav\text{"})[0] = \mathtt{true} \tag{A.67}$$

     Thanks to (A.66), we can deduce that $i = 0$. Rewriting the goal with (A.67), tautology.

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

$$\Delta(id_t)(\text{"}ian\text{"}) = |input(t)| \tag{A.68}$$

     Thanks to (A.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 $\mathtt{comp}(id_p, \text{"}place\text{"}, gm_p, ipm_p, opm_p) \in d.cs$ and $<\mathtt{output\_arcs\_valid(j)} \Rightarrow \mathtt{id_{ji}}> \in opm_p$ and $<\mathtt{input\_arcs\_valid(i)} \Rightarrow \mathtt{id_{ji}}> \in ipm_t$.
     By property of the stabilize relation, $\mathtt{comp}(id_t, \text{"}transition\text{"}, gm_t, ipm_t, opm_t) \in d.cs$ and $\mathtt{comp}(id_p, \text{"}place\text{"}, gm_p, ipm_p, opm_p) \in d.cs$:

$$\sigma'(id_t)(\text{"}iav\text{"})[i] = \sigma'(id_{ji}) = \sigma'(id_p)(\text{"}oav\text{"})[j] \tag{A.69}$$

Rewriting the goal with (A.69), $\boxed{\sigma'(id_p)(''oav'')[j] = \texttt{true}.}$

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

$$\begin{aligned}\sigma'(id_p)(''oav'')[j] = &((\sigma'(id_p)(''oat'')[j] = \texttt{BASIC} + \sigma'(id_p)(''oat'')[j] = \texttt{TEST}) \\ &. \sigma'(id_p)(''sm'') \geq \sigma'(id_p)(''oaw'')[j]) \\ &+ (\sigma'(id_p)(''oat'')[j] = \texttt{INHIB} . \sigma'(id_p)(''sm'') < \sigma'(id_p)(''oaw'')[j])\end{aligned} \tag{A.70}$$

Rewriting the goal with (A.70),

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

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 $\texttt{comp}(id_p, ''place'', gm_p, ipm_p, opm_p) \in d.cs$:

  $$\sigma'(id_p)(''oat'')[j] = \texttt{BASIC} \tag{A.71}$$
  $$\sigma'(id_p)(''oaw'')[j] = \omega \tag{A.72}$$

  Rewriting the goal with (A.71) and (A.72), and simplifying the goal:
  $\boxed{\sigma'(id_p)(''sm'') \geq \omega = \texttt{true}.}$
  Appealing to Lemma Rising Edge Equal Marking:

  $$s'.M(p) = \sigma'(id_p)(''sm'') \tag{A.73}$$

  Rewriting the goal with (A.73): $\boxed{s'.M(p) \geq \omega = \texttt{true}.}$
  By definition of $t \in Sens(s'.M)$, $s'.M(p) \geq \omega = \texttt{true}.$
- **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 $\texttt{comp}(id_p, ''place'', gm_p, ipm_p, opm_p) \in d.cs$:

  $$\sigma'(id_p)(''oat'')[j] = \texttt{INHIB} \tag{A.74}$$
  $$\sigma'(id_p)(''oaw'')[j] = \omega \tag{A.75}$$

  Rewriting the goal with (A.74) and (A.75), and simplifying the goal:
  $\boxed{\sigma'(id_p)(''sm'') < \omega = \texttt{true}.}$
  Appealing to Lemma Rising Edge Equal Marking, equation (A.73) holds.

Rewriting the goal with (A.73): $\boxed{s'.M(p) < \omega = \mathtt{true}.}$

By definition of $t \in Sens(s'.M)$, $s'.M(p) < \omega = \mathtt{true}.$

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

   By definition of $t \in Sens(s'.M)$, let us show

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

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

   (a) Assuming $pre(p,t) = (\omega, \mathtt{basic}) \lor pre(p,t) = (\omega, \mathtt{test})$, let us show $\boxed{s'.M(p) \geq \omega.}$

   The proceeding is the same for $pre(p,t) = (\omega, \mathtt{basic})$ and $pre(p,t) = (\omega, \mathtt{test})$. Therefore, we will only cover the case where $pre(p,t) = (\omega, \mathtt{basic})$.

   By property of the stabilize relation and $\mathtt{comp}(id_t, ''transition'', gm_t, ipm_t, opm_t) \in d.cs$, equation (A.65) holds.

   Rewriting $\sigma'(id_t)(''se'') = \mathtt{true}$ with (A.65), $\prod_{i=0}^{\Delta(id_t)(''ian'')-1} \sigma'(id_t)(''input\_arcs\_valid'')[i] = \mathtt{true}$.

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

   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 $\mathtt{comp}(id_p, ''place'', gm_p, ipm_p, opm_p) \in d.cs$ and $<\mathtt{output\_arcs\_valid(j)} \Rightarrow \mathtt{id_{ji}}> \in opm_p$ and $<\mathtt{input\_arcs\_valid(i)} \Rightarrow \mathtt{id_{ji}}> \in ipm_t$. 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, $<\mathtt{input\_arcs\_number} \Rightarrow |input(t)|> \in gm_t$.

   By property of the elaboration relation and $\mathtt{comp}(id_t, ''transition'', gm_t, ipm_t, opm_t) \in d.cs$, equation (A.68) holds.

   Thanks to (A.68), we can deduce that $\forall i \in [0, |input(t)| - 1]$, $\sigma'(id_t)(''iav'')[i] = \mathtt{true}$.

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

   By property of the stabilize relation, $\mathtt{comp}(id_t, ''transition'', gm_t, ipm_t, opm_t) \in d.cs$ and $\mathtt{comp}(id_p, ''place'', gm_p, ipm_p, opm_p) \in d.cs$, equation (A.69) holds.

   Thanks to (A.69), we can deduce that $\sigma'(id_p)(''oav'')[j] = \mathtt{true}$.

   By property of the stabilize relation and $\mathtt{comp}(id_p, ''place'', gm_p, ipm_p, opm_p) \in d.cs$, equation (A.70) holds. Thanks to (A.70), we can deduce that:

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

By construction, $<$`output_arcs_types(j)` $\Rightarrow$ `BASIC`$>$ $\in ipm_p$ and
$<$`output_arcs_weights(j)` $\Rightarrow \omega> \in ipm_p$.
By property of the stabilize relation and $\texttt{comp}(id_p, \text{"}place\text{"}, gm_p, ipm_p, opm_p) \in d.cs$, equations (A.71) and (A.72) hold.
Thanks to (A.71) and (A.72), we can deduce that $\sigma'(id_p)(\text{"}sm\text{"}) \geq \omega = \texttt{true}$.
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, $<$`output_arcs_types(j)` $\Rightarrow$ `INHIB`$>$ $\in ipm_p$ and
$<$`output_arcs_weights(j)` $\Rightarrow \omega> \in ipm_p$.
By property of the stabilize relation and $\texttt{comp}(id_p, \text{"}place\text{"}, gm_p, ipm_p, opm_p) \in d.cs$, equations (A.74) and (A.72) hold.
Thanks to (A.74) and (A.72), we can deduce that $\sigma'(id_p)(\text{"}sm\text{"}) < \omega = \texttt{true}$.
Appealing to Lemma Rising Edge Equal Marking, $s'.M(p) < \omega$.

□

Lemma 21 (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. 3, 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. Proving the above lemma is trivial by appealing to Lemma Rising Edge Equal Sensitized and by reasoning on contrapositives. □

A.4 Falling Edge

A.4.1 Falling Edge and marking

Lemma 22 (Falling Edge Equal Marking). *then* $\forall p \in P, id_p \in Comps(\Delta)$ *s.t.* $\gamma(p) = id_p,\ s'.M(p) = \sigma'(id_p)(\text{"}s\_marking\text{"})$.

Proof. Given a $p \in P$ and an $id \in Comps(\Delta)$ s.t. $\gamma(p) = id_p$, let us show
$\boxed{s'.M(p) = \sigma'(id_p)(\text{"}s\_marking\text{"}).}$

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

$$s.M(p) = s'.M(p) \tag{A.76}$$

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

$$\sigma'(id_p)(\text{"}s\_marking\text{"}) = \sigma(id_p)(\text{"}s\_marking\text{"}) \tag{A.77}$$

Rewriting the goal with (A.76) and (A.77): $\boxed{s.M(p) = \sigma(id_p)(\text{"}s\_marking\text{"}).}$

By definition of $\gamma, E_c, \tau \vdash s \overset{\downarrow}{\sim} \sigma$: $s.M(p) = \sigma(id_p)(\text{"}s\_marking\text{"})$.

□

Lemma 23 (Falling Edge Equal Output Token Sum). *then* $\forall p, id_p$ *s.t.* $\gamma(p) = id_p$, $\sum\limits_{t \in Fired(s')} pre(p,t) = \sigma'(id_p)(\text{"}s\_output\_token\_sum\text{"})$.

Proof. Given a $p \in P$ and an $id_p \in Comps(\Delta)$, let us show
$\boxed{\sum\limits_{t \in Fired(s')} pre(p,t) = \sigma'(id_p)(\text{"}s\_output\_token\_sum\text{"}).}$

By construction and by definition of id_p, there exist gm_p, ipm_p, opm_p s.t. $\texttt{comp}(id_p, \text{"}place\text{"}, gm_p, ipm_p, opm_p) \in d.cs$.

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

$$\sigma'(id_p)(\text{"}sots\text{"}) = \sum_{i=0}^{\Delta(id_p)(\text{"}oan\text{"})-1} \begin{cases} \sigma'(id_p)(\text{"}oaw\text{"})[i] \texttt{ if } (\sigma'(id_p)(\text{"}otf\text{"})[i] \\ \qquad . \, \sigma'(id_p)(\text{"}oat\text{"})[i] = \texttt{BASIC}) \\ 0 \ otherwise \end{cases} \tag{A.78}$$

Rewriting the goal with (A.78):

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

Let us unfold the definition of the left sum term:

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

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.

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

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

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

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

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

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

$$\Delta(id_p)(\text{"}oan\text{"}) = 1 \tag{A.79}$$

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

$$\sigma'(id_p)("oat")[0] = \texttt{BASIC} \tag{A.80}$$
$$\sigma'(id_p)("otf")[0] = \texttt{true} \tag{A.81}$$
$$\sigma'(id_p)("oaw")[0] = 0 \tag{A.82}$$

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

$$\sum_{t \in Fired(s')} \begin{cases} \omega \texttt{ if } pre(p,t) = (\omega, \texttt{basic}) \\ 0 \textit{ otherwise} \end{cases} = 0 \tag{A.83}$$

Rewriting the goal with (A.79), (A.80), (A.81), (A.82) and (A.83), 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:

$$\Delta(id_p)("oan") = |output(p)| \tag{A.84}$$

Rewriting the goal with (A.84): $\boxed{\sum_{t \in Fired(s')} f(t) = \sum_{i=0}^{|output(p)|-1} g(i).}$

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:

$$g(0) = \begin{cases} \sigma'(id_p)("oaw")[0] \texttt{ if } (\sigma'(id_p)("otf")[0] \\ \qquad . \ \sigma'(id_p)("oat")[0] = \texttt{BASIC}) \\ 0 \textit{ otherwise} \end{cases} \tag{A.85}$$

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

(a) $(\sigma'(id_p)(\text{"}otf\text{"})[0]\ .\ \sigma'(id_p)(\text{"}oat\text{"})[0] = \texttt{BASIC}) = \texttt{false}$:
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) $(\sigma'(id_p)(\text{"}otf\text{"})[0]\ .\ \sigma'(id_p)(\text{"}oat\text{"})[0] = \texttt{BASIC}) = \texttt{true}$:
In that case, $g(0) = \sigma'(id_p)(\text{"}oaw\text{"})[0]$, $\sigma'(id_p)(\text{"}otf\text{"})[0] = \texttt{true}$ and $\sigma'(id_p)(\text{"}oat\text{"})[0] = \texttt{BASIC}$.
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 construction and by definition of id_t, there exist gm_t, ipm_t, opm_t s.t. $\texttt{comp}(id_t, \text{"}transition\text{"}, gm_t, ipm_t, opm_t) \in d.cs$.
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, $\sigma'(id_p)(\text{"}oat\text{"})[0] = \texttt{BASIC}$ and $<\texttt{output\_arcs\_types}(0) \Rightarrow \texttt{a}> \in ipm_p$:

$$pre(p,t) = (\omega, \texttt{basic}) \tag{A.86}$$

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 $\sigma'(id_p)(\text{"}otf\text{"})[0] = \texttt{true}$:

$$\sigma'(id_t)(\text{"}fired\text{"}) = \texttt{true} \tag{A.87}$$

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

$$\sigma'(id_p)(\text{"}oaw\text{"})[0] = \omega \tag{A.88}$$

Rewriting the goal with (A.88):

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

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 24 (Falling Edge Equal Input Token Sum). *then* $\forall p, id_p$ *s.t.* $\gamma(p) = id_p$, $\sum_{t \in Fired(s')} post(t, p) = \sigma'_p(\text{"}s\_input\_token\_sum\text{"})$.

Proof. Given a $p \in P$ and an $id_p \in Comps(\Delta)$, let us show $\boxed{\sum_{t \in Fired(s')} post(t, p) = \sigma'(id_p)(\text{"}s\_input\_token\_sum\text{"})}$.

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

$$\sigma'(id_p)(\text{"}sits\text{"}) = \sum_{i=0}^{\Delta(id_p)(\text{"}ian\text{"})-1} \begin{cases} \sigma'(id_p)(\text{"}iaw\text{"})[i] \texttt{ if } \sigma'(id_p)(\text{"}itf\text{"})[i] \\ 0 \; otherwise \end{cases} \tag{A.89}$$

Rewriting the goal with (A.89):

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

Let us unfold the definition of the left sum term:

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

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

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

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

$$\Delta(id_p)(\text{"}ian\text{"}) = 1 \tag{A.90}$$

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

$$\sigma'(id_p)(\text{"}itf\text{"})[0] = \texttt{true} \tag{A.91}$$
$$\sigma'(id_p)(\text{"}iaw\text{"})[0] = 0 \tag{A.92}$$

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

$$\sum_{t \in Fired(s')} \begin{cases} \omega \texttt{ if } post(t,p) = \omega \\ 0 \; otherwise \end{cases} = 0 \tag{A.93}$$

Rewriting the goal with (A.90), (A.91), (A.92), and (A.93), 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:

$$\Delta(id_p)(''ian'') = |input(p)| \tag{A.94}$$

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 (A.94): $\boxed{\sum_{t \in Fired(s')} f(t) = \sum_{i=0}^{|input(p)|-1} g(i).}$

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:

$$g(0) = \begin{cases} \sigma'(id_p)(''iaw'')[0] \texttt{ if } \sigma'(id_p)(''itf'')[0] \\ 0 \; otherwise \end{cases} \tag{A.95}$$

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 construction and 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 $<\texttt{input\_arcs\_types}(0) \Rightarrow \texttt{a}> \in ipm_p$:

$$post(t, p) = \omega \tag{A.96}$$

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 $\sigma'(id_p)("itf")[0] = \texttt{true}$:

$$\sigma'(id_t)("fired") = \texttt{true} \tag{A.97}$$

Appealing to Lemma **??** and (A.97), 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 $<\texttt{input\_arcs\_weights}(0) \Rightarrow \omega> \in ipm_p$:

$$\sigma'(id_p)("iaw")[0] = \omega \tag{A.98}$$

Rewriting the goal with (A.98):

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

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

$\square$

A.4.2 Falling edge and time counters

Lemma 25 (Falling Edge Equal Time Counters). *then* $\forall t \in T_i, id_t \in Comps(\Delta)$ *s.t.* $\gamma(t) = id_t$,
$(upper(I_s(t)) = \infty \wedge s'.I(t) \leq lower(I_s(t)) \Rightarrow s'.I(t) = \sigma'(id_t)(''s\_time\_counter''))$
$\wedge(upper(I_s(t)) = \infty \wedge s'.I(t) > lower(I_s(t)) \Rightarrow \sigma'(id_t)(''s\_time\_counter'') = lower(I_s(t)))$
$\wedge(upper(I_s(t)) \neq \infty \wedge s'.I(t) > upper(I_s(t)) \Rightarrow \sigma'(id_t)(''s\_time\_counter'') = upper(I_s(t)))$
$\wedge(upper(I_s(t)) \neq \infty \wedge s'.I(t) \leq upper(I_s(t)) \Rightarrow s'.I(t) = \sigma'(id_t)(''s\_time\_counter''))$.

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

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

By construction and 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 $\texttt{comp}(id_t, ''transition'', gm_t, ipm_t, opm_t) \in d.cs$:

$$\begin{aligned}\sigma(id_t)(''se'') = \texttt{true} \wedge \Delta(id_t)(''tt'') \neq \texttt{NOT\_TEMPORAL} \wedge \sigma(id_t)(''srtc'') = \texttt{false}\\ \wedge\sigma(id_t)(''stc'') < \Delta(id_t)(''mtc'') \Rightarrow \sigma'(id_t)(''stc'') = \sigma(id_t)(''stc'') + 1\end{aligned} \tag{A.99}$$

$$\begin{aligned}\sigma(id_t)(''se'') = \texttt{true} \wedge \Delta(id_t)(''tt'') \neq \texttt{NOT\_TEMPORAL} \wedge \sigma(id_t)(''srtc'') = \texttt{false}\\ \wedge\sigma(id_t)(''stc'') \geq \Delta(id_t)(''mtc'') \Rightarrow \sigma'(id_t)(''stc'') = \sigma(id_t)(''stc'')\end{aligned} \tag{A.100}$$

$$\begin{aligned}\sigma(id_t)(''se'') = \texttt{true} \wedge \Delta(id_t)(''tt'') \neq \texttt{NOT\_TEMPORAL}\\ \wedge\sigma(id_t)(''srtc'') = \texttt{true} \Rightarrow \sigma'(id_t)(''stc'') = 1\end{aligned} \tag{A.101}$$

$$\sigma(id_t)(''se'') = \texttt{false} \vee \Delta(id_t)(''tt'') = \texttt{NOT\_TEMPORAL} \Rightarrow \sigma'(id_t)(''stc'') = 0 \tag{A.102}$$

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 $\sigma(id_t)(''se'') = \texttt{false}$ (A.103).
   Appealing to (A.102) and (A.103), we have $\sigma'(id_t)(''stc'') = 0$ (A.104).
   By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.I(t) = 0$ (A.105).

Rewriting the goal with (A.104) and (A.105): tautology.

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

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $\sigma(id_t)("se") = \texttt{true}$ (A.106).
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 $\Delta(id_t)("tt") = \texttt{TEMP\_A\_INF}$ (A.107).
Case analysis on $s.reset_t(t)$; there are two cases:

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

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, $\sigma(id_t)("srtc") = \texttt{true}$ (A.108).
Appealing to (A.101), (A.106), (A.107) and (A.108), we have $\sigma'(id_t)("stc") = 1$ (A.109).
By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.I(t) = 1$ (A.110).
Rewriting the goal with (A.109) and (A.110): tautology.

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

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $\sigma(id_t)("srtc") = \texttt{false}$ (A.111).
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 $\Delta(id_t)("mtc") = a$ (A.112).
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 $upper(I_s(t)) = \infty$:

$$s'.I(t) = s.I(t) + 1 \tag{A.113}$$

Rewriting the goal with (A.113): $\boxed{s.I(t) + 1 = \sigma'(id_t)("stc").}$
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 $upper(I_s(t)) = \infty$:

$$s.I(t) = \sigma(id_t)("stc") \tag{A.114}$$

Appealing to (A.112), (A.114) and $s.I(t) < a$:

$$\sigma(id_t)("stc") < \Delta(id_t)("mtc") \tag{A.115}$$

Appealing to (A.99), (A.115), (A.111) and (A.106):

$$\sigma'(id_t)("stc") = \sigma(id_t)("stc") + 1 \tag{A.116}$$

Rewriting the goal with (A.116) and (A.114): 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:

$$\Delta(id_t)(\text{"}mtc\text{"}) = a \quad (A.117)$$
$$\Delta(id_t)(\text{"}tt\text{"}) = \texttt{TEMP\_A\_INF} \quad (A.118)$$

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

$$\sigma(id_t)(\text{"}se\text{"}) = \texttt{true} \quad (A.119)$$

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

$$\sigma(id_t)(\text{"}srtc\text{"}) = \texttt{false} \quad (A.120)$$

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

$$\begin{aligned} s'.I(t) = s.I(t) + 1 &\Rightarrow s.I(t) + 1 > lower(I_s(t)) \\ &\Rightarrow s.I(t) \geq lower(I_s(t)) \end{aligned} \quad (A.121)$$

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

$$\sigma(id_t)(\text{"}stc\text{"}) = lower(I_s(t)) \quad (A.122)$$

Appealing to (A.100):

$$\sigma'(id_t)(\text{"}stc\text{"}) = \sigma(id_t)(\text{"}stc\text{"}) \quad (A.123)$$

Rewriting the goal with (A.122) and (A.123): tautology.

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

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

$$s.I(t) = \sigma(id_t)(''stc'') \tag{A.124}$$

Appealing to (A.100):

$$\sigma'(id_t)(''stc'') = \sigma(id_t)(''stc'') \tag{A.125}$$

Rewriting the goal with (A.125), (A.124) and $s.I(t) = lower(I_s(t))$: tautology.

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

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

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:

$$\Delta(id_t)(''mtc'') = b = upper(I_s(t)) \tag{A.126}$$
$$\Delta(id_t)(''tt'') \neq \texttt{NOT\_TEMP} \tag{A.127}$$

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

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

By definition of $E_c, \tau \vdash s \overset{\downarrow}{\rightarrow} s'$, 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 $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$ and $t \in Sens(s.M)$:

$$\sigma(id_t)(''se'') = \texttt{true} \tag{A.128}$$

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

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

By definition of $E_c, \tau \vdash s \overset{\downarrow}{\rightarrow} s'$: $s'.I(t) = 1$.
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 $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$ and $s.reset_t(t) = \texttt{false}$:

$$\sigma(id_t)(''srtc'') = \texttt{false} \tag{A.129}$$

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

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

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

$$s'.I(t) = s.I(t) \tag{A.130}$$

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

$$\sigma(id_t)(''stc'') = upper(I_s(t)) \tag{A.131}$$

Appealing to (A.100), we have $\sigma'(id_t)(''stc'') = \sigma(id_t)(''stc'')$.
Rewriting the goal with $\sigma'(id_t)(''stc'') = \sigma(id_t)(''stc'')$ and (A.131): tautology.

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

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

$$s.I(t) = \sigma(id_t)(''stc'') \tag{A.132}$$

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

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

  Appealing to (A.126), (A.132) and $s.I(t) = upper(I_s(t))$:

  $$\Delta(id_t)(''mtc'') \leq \sigma(id_t)(''stc'') \tag{A.133}$$

  Appealing to (A.133) and (A.100):

  $$\sigma'(id_t)(''stc'') = \sigma(id_t)(''stc'') \tag{A.134}$$

  Rewriting the goal with (A.134), (A.132) and $s.I(t) = upper(I_s(t))$: tautology.

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

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

  $$s'.I(t) = s.I(t) + 1 \tag{A.135}$$

  From (A.135) 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. $\boxed{upper(I_s(t)) \neq \infty \wedge s'.I(t) \leq upper(I_s(t)) \Rightarrow s'.I(t) = \sigma'(id_t)(''s\_time\_counter'').}$

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

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:

$$\Delta(id_t)(''mtc'') = b = upper(I_s(t)) \tag{A.136}$$
$$\Delta(id_t)(''tt'') \neq \texttt{NOT\_TEMP} \tag{A.137}$$

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 $\sigma(id_t)(''se'') = \texttt{false}$ (A.138).
Appealing (A.102) and (A.138), we have $\sigma'(id_t)(''stc'') = 0$ (A.139).

By definition of $E_c, \tau \vdash s \overset{\downarrow}{\to} s'$, we have $s'.I(t) = 0$ (A.140).

Rewriting the goal with (A.139) and (A.140): tautology.

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

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $\sigma(id_t)(''se'') = \texttt{true}$ (A.141).
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 $\sigma(id_t)(''srtc'') = \texttt{true}$ (A.142).
Appealing to (A.101), (A.137), (A.141) and (A.142), we have $\sigma'(id_t)(''stc'') = 1$ (A.143).

By definition of $E_c, \tau \vdash s \overset{\downarrow}{\to} s'$, we have $s'.I(t) = 1$ (A.144).
Rewriting the goal with (A.143) and (A.144), tautology.

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

By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $\sigma(id_t)(''srtc'') = \texttt{false}$ (A.145).
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 $E_c, \tau \vdash s \overset{\downarrow}{\to} s'$, 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 $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $s.I(t) = \sigma(id_t)(''stc'')$ (A.146).

- $s.I(t) < upper(I_s(t))$:
From $s.I(t) < upper(I_s(t))$, (A.146) and (A.136), we can deduce $\sigma(id_t)(''stc'') < \Delta(id_t)(''mtc'')$ (A.147).
From (A.99), (A.141), (A.137), (A.145) and (A.147), we can deduce:

$$\sigma'(id_t)(''stc'') = \sigma(id_t)(''stc'') + 1 \tag{A.148}$$

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

$$s'.I(t) = s.I(t) + 1 \tag{A.149}$$

Rewriting the goal with (A.148) and (A.149), 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 $s.I(t) = upper(I_s(t))$.

□

A.4.3 Falling edge and condition values

Lemma 26 (Falling Edge Equal Condition Values). *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 $\boxed{s'.cond(c) = \sigma'(id_c).}$

By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, we have $s'.cond(c) = E_c(\tau, c)$ (A.150).
By property of the $\texttt{Inject}_{\downarrow}$, the $\mathcal{H}$-VHDL falling edge, the stabilize relations and $id_c \in Ins(\Delta)$, we have $\sigma'(id_c) = E_p(\tau, \downarrow)(id_c)$ (A.151).
Rewriting the goal with (A.150) and (A.151): $\boxed{E_c(\tau, c) = E_p(\tau, \downarrow)(id_c)}$
By definition of $\gamma \vdash E_p \overset{env}{=} E_c$: $E_c(\tau, c) = E_p(\tau, \downarrow)(id_c)$.

□

A.4.4 Falling and action executions

Lemma 27 (Falling Edge Equal Action Executions). *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 $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$:

$$s'.ex(a) = \sum_{p \in marked(s.M)} \mathbb{A}(p, a) \tag{A.152}$$

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

  $$\sigma'(id_a) = false \tag{A.153}$$

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

  $$\sum_{p \in marked(s.M)} \mathbb{A}(p, a) = \texttt{false} \tag{A.154}$$

Rewriting the goal with (A.152), (A.153) and (A.154), tautology.

- **CASE** $pls(a) \neq \emptyset$:
By construction, $\mathtt{id_a} \Leftarrow \mathtt{id_{mp_0}} + \cdots + \mathtt{id_{mp_n}} \in ss_{a\downarrow}$, 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 $\mathtt{Inject}_{\downarrow}$, the $\mathcal{H}$-VHDL falling edge, the stabilize relations, and $\mathtt{ps}(''action'', \emptyset, sl, ss) \in d.cs$:

$$\sigma'(id_a) = \sigma(id_{mp_0}) + \cdots + \sigma(id_{mp_n}) \quad \text{(A.155)}$$

Rewriting the goal with (A.152) and (A.155), $\boxed{\sum\limits_{p \in marked(s.M)} \mathbb{A}(p,a) = \sigma(id_{mp_0}) + \cdots + \sigma(id_{mp_n}).}$

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

  - **CASE** $\sigma(id_{mp_0}) + \cdots + \sigma(id_{mp_n}) = \mathtt{true}$:
  Then, we can rewrite the goal as follows: $\boxed{\sum\limits_{p \in marked(s.M)} \mathbb{A}(p,a) = \mathtt{true}.}$

  To prove the above goal, let us show $\boxed{\exists p \in marked(s.M)\ s.t.\ \mathbb{A}(p,a) = \mathtt{true}.}$
  From $\sigma(id_{mp_0}) + \cdots + \sigma(id_{mp_n}) = \mathtt{true}$, we can deduce that $\exists id_{mp_i}\ s.t.\ \sigma(id_{mp_i}) = \mathtt{true}$. Let us take an id_{mp_i} s.t. $\sigma(id_{mp_i}) = \mathtt{true}$.
  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 $\mathtt{comp}(id_{p_i}, ''place'', gm_{p_i}, ipm_{p_i}, opm_{p_i}) \in d.cs$ and $<\mathtt{marked} \Rightarrow \mathtt{id_{mp_i}}> \in opm_{p_i}$. 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 $\mathtt{comp}(id_{p_i}, ''place'', gm_{p_i}, ipm_{p_i}, opm_{p_i}) \in d.cs$:

$$\sigma(id_{mp_i}) = \sigma(id_{p_i})(''marked'') \quad \text{(A.156)}$$
$$\sigma(id_{p_i})(''marked'') = \sigma(id_{p_i})(''sm'') > 0 \quad \text{(A.157)}$$

  From (A.156), (A.157) and $\sigma(id_{mp_i}) = \mathtt{true}$, we can deduce that $\sigma(id_{p_i})(''marked'') = \mathtt{true}$ and $(\sigma(id_{p_i})(''sm'') > 0) = \mathtt{true}$.

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

$$s.M(p_i) = \sigma(id_{p_i})(''sm'') \quad \text{(A.158)}$$

  From (A.158) and $(\sigma(id_{p_i})(''sm'') > 0) = \mathtt{true}$, 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: $\boxed{\mathbb{A}(p,a) = \mathtt{true}.}$

  By definition of $p_i \in pls(a)$, $\mathbb{A}(p,a) = \mathtt{true}$.

  - **CASE** $\sigma(id_{mp_0}) + \cdots + \sigma(id_{mp_n}) = \mathtt{false}$:
  Then, we can rewrite the goal as follows: $\boxed{\sum\limits_{p \in marked(s.M)} \mathbb{A}(p,a) = \mathtt{false}.}$

  To prove the above goal, let us show $\boxed{\forall p \in marked(s.M)\ s.t.\ \mathbb{A}(p,a) = \mathtt{false}.}$

  Given a $p \in marked(s.M)$, let us show $\boxed{\mathbb{A}(p,a) = \mathtt{false}.}$

  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 $\texttt{comp}(id_p, \text{"}place\text{"}, gm_p, ipm_p, opm_p) \in d.cs$ 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 $\texttt{comp}(id_p, \text{"}place\text{"}, gm_p, ipm_p, opm_p) \in d.cs$:

$$\sigma(id_{mp_i}) = \sigma(id_p)(\text{"}marked\text{"}) \tag{A.159}$$

$$\sigma(id_p)(\text{"}marked\text{"}) = \sigma(id_p)(\text{"}sm\text{"}) > 0 \tag{A.160}$$

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

  By definition of $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $s.M(p) = \sigma(id_p)(\text{"}sm\text{"})$, 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, $s.M(p) > 0$).

$\square$

A.4.5 Falling edge and function executions

Lemma 28 (Falling Edge Equal Function Executions). *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 $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$:

$$s.ex(f) = s'.ex(f) \tag{A.161}$$

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:

$$\sigma(id_f) = \sigma'(id_f) \tag{A.162}$$

Rewriting the goal with (A.161) and (A.162), $\boxed{s.ex(f) = \sigma(id_f).}$

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

A.4.6 Falling edge and firable transitions

Lemma 29 (Falling Edge Equal Firable). *then* $\forall t \in T, id_t \in Comps(\Delta)$ *s.t.* $\gamma(t) = id_t, t \in Firable(s') \Leftrightarrow \sigma'(id_t)(\text{"}s\_firable\text{"}) = \texttt{true}$.

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

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.

$\square$

Lemma 30 (Falling Edge Equal Firable 1). *then* $\forall t \in T, id_t \in Comps(\Delta)$ *s.t.* $\gamma(t) = id_t$, $t \in Firable(s') \Rightarrow \sigma'(id_t)(''s\_firable'') = \texttt{true}$.

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 $\boxed{\sigma'(id_t)(''s\_firable'') = \texttt{true}.}$

By construction and 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 $\texttt{comp}(id_t, ''transition'', gm_t, ipm_t, opm_t) \in d.cs$:

$$\sigma'(id_t)(''sfa'') = \sigma(id_t)(''se'') \mathbin{.} \sigma(id_t)(''scc'') \mathbin{.} \texttt{checktc}(\Delta(id_t), \sigma(id_t)) \tag{A.163}$$

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

$$\begin{aligned}
\texttt{checktc}(\Delta(id_t), \sigma(id_t)) = \Big(& \texttt{not}\ \sigma(id_t)(''srtc'') \mathbin{.} \\
& \big[(\Delta(id_t)(''tt'') = \texttt{TEMP_A_B} \mathbin{.} (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1) \\
& \qquad\qquad \mathbin{.} (\sigma(id_t)(''stc'') \leq \sigma(id_t)(''B'') - 1)) \\
& + (\Delta(id_t)(''tt'') = \texttt{TEMP_A_A} \mathbin{.} (\sigma(id_t)(''stc'') = \sigma(id_t)(''A'') - 1)) \\
& + (\Delta(id_t)(''tt'') = \texttt{TEMP_A_INF} \mathbin{.} (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1))\big]\Big) \\
& + \big(\sigma(id_t)(''srtc'') \mathbin{.} \Delta(id_t)(''tt'') \neq \texttt{NOT_TEMP} \mathbin{.} \sigma(id_t)(''A'') = 1\big) \\
& + \Delta(id_t)(''tt'') = \texttt{NOT_TEMP}
\end{aligned} \tag{A.164}$$

Rewriting the goal with (A.163): $\boxed{\sigma(id_t)(''se'') \mathbin{.} \sigma(id_t)(''scc'') \mathbin{.} \texttt{checktc}(\Delta(id_t), \sigma(id_t)) = \texttt{true}.}$
Then, there are three points to prove:

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

   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 $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we know that $t \in Sens(s.M)$ implies $\sigma(id_t)(''se'') = \texttt{true}$.

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

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

$$\sigma(id_t)(\text{"}scc\text{"}) = \prod_{c \in conds(t)} \begin{cases} E_c(\tau, c) & if\ \mathbb{C}(t,c) = 1 \\ \texttt{not}(E_c(\tau, c)) & if\ \mathbb{C}(t,c) = -1 \end{cases} \tag{A.165}$$

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

Rewriting the goal with (A.165): $\boxed{\prod_{c \in conds(t)} \begin{cases} E_c(\tau, c) & if\ \mathbb{C}(t,c) = 1 \\ \texttt{not}(E_c(\tau, c)) & if\ \mathbb{C}(t,c) = -1 \end{cases} = \texttt{true}.}$

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**:

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

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

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 $\mathbb{C}(t,c) = 1 \lor \mathbb{C}(t,c) = -1$:

(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 $t \notin T_i \lor s'.I(t) \in I_s(t)$. Let us perform case analysis on $t \notin T_i \lor s'.I(t) \in I_s(t)$:

(a) $t \notin T_i$:

By construction, <`transition_type` $\Rightarrow$ `NOT_TEMP`> $\in gm_t$, and by property of the elaboration relation, we have $\Delta(id_t)(''tt'') = \texttt{NOT\_TEMP}$.
From $\Delta(id_t)(''tt'') = \texttt{NOT\_TEMP}$, 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. <`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:

$$\begin{aligned}
\texttt{checktc}(\Delta(id_t), \sigma(id_t)) = \Big(&\texttt{not}\ \sigma(id_t)(''srtc'') \,.\\
&\big[(\Delta(id_t)(''tt'') = \texttt{TEMP_A_B} \,.\, (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1)\\
&\qquad .\, (\sigma(id_t)(''stc'') \leq \sigma(id_t)(''B'') - 1))\\
&+(\Delta(id_t)(''tt'') = \texttt{TEMP_A_A} \,.\\
&\quad (\sigma(id_t)(''stc'') = \sigma(id_t)(''A'') - 1))\\
&+(\Delta(id_t)(''tt'') = \texttt{TEMP_A_INF} \,.\\
&\quad (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1))\big]\Big)\\
&+ \big(\sigma(id_t)(''srtc'') \,.\, \sigma(id_t)(''A'') = 1\big)
\end{aligned} \tag{A.166}$$

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:

$$\texttt{checktc}(\Delta(id_t), \sigma(id_t)) = \big(\sigma(id_t)(''A'') = 1\big) \tag{A.167}$$

Rewriting the goal with (A.167), and simplifying the goal: $\boxed{\sigma(id_t)(''A'') = 1.}$

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

$$\begin{array}{c} \texttt{checktc}(\Delta(id_t), \sigma(id_t)) \\ = \\ \begin{array}{l} (\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_B} \;\; . \; (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1) \\ \qquad\qquad\qquad\qquad\qquad\; . \; (\sigma(id_t)(''stc'') \leq \sigma(id_t)(''B'') - 1)) \\ +(\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_A} \; . \; (\sigma(id_t)(''stc'') = \sigma(id_t)(''A'') - 1)) \\ +(\Delta(id_t)(''tt'') = \texttt{TEMP\_A\_INF} \; . \; (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1)) \end{array} \end{array} \tag{A.168}$$

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 $\texttt{checktc}$ as follows:

    $$\texttt{checktc}(\Delta(id_t), \sigma(id_t)) = (\sigma(id_t)(''stc'') = \sigma(id_t)(''A'') - 1) \tag{A.169}$$

    Rewriting the goal with (A.169), 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 $\texttt{checktc}$ as follows:

    $$\begin{array}{c} \texttt{checktc}(\Delta(id_t), \sigma(id_t)) \\ = \\ (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1) \; . \; (\sigma(id_t)(''stc'') \leq \sigma(id_t)(''B'') - 1) \end{array} \tag{A.170}$$

Rewriting the goal with (A.170), 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, <`time_A_value` $\Rightarrow a$> $\in ipm_t$ and <`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 <`transition_type` $\Rightarrow$ `TEMP_A_INF`> $\in gm_t$. By property of the elaboration relation, we have $\Delta(id_t)(''tt'') =$ `TEMP_A_INF`; thus we can simplify the term `checktc` as follows:

$$\texttt{checktc}(\Delta(id_t), \sigma(id_t)) = (\sigma(id_t)(''stc'') \geq \sigma(id_t)(''A'') - 1) \tag{A.171}$$

  Rewriting the goal with (A.171), 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, $<\texttt{time\_A\_value} \Rightarrow a> \in ipm_t$, and by property of stable σ, we have $\sigma(id_t)("A") = a$.
  Rewriting the goal with $\sigma(id_t)("stc") = a$ and $\sigma(id_t)("A") = a$: $a - 1 \leq a$.

$\square$

Lemma 31 (Falling Edge Equal Firable 2). *then* $\forall t \in T, id_t \in Comps(\Delta)$ *s.t.* $\gamma(t) = id_t, \sigma'(id_t)("s\_firable") = \texttt{true} \Rightarrow t \in Firable(s')$.

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

By construction and 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 $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$:

$$\sigma'(id_t)("sfa") = \sigma(id_t)("se") \,.\, \sigma(id_t)("scc") \,.\, \texttt{checktc}(\Delta(id_t), \sigma(id_t)) = \texttt{true} \tag{A.172}$$

From (A.172), we can deduce:

$$\sigma(id_t)("se") = \texttt{true} \tag{A.173}$$
$$\sigma(id_t)("scc") = \texttt{true} \tag{A.174}$$
$$\texttt{checktc}(\Delta(id_t), \sigma(id_t)) = \texttt{true} \tag{A.175}$$

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. $\boxed{t \notin T_i \lor s'.I(t) \in I_s(t)}$
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 $\sigma(id_t)("se") = \texttt{true} \Leftrightarrow t \in Sens(s.M)$.

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

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

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

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

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

   Let us prove these two points:

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

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

$$\sigma(id_t)(''scc'') = \prod_{c \in conds(t)} \begin{cases} E_c(\tau,c) & \textit{if } \mathbb{C}(t,c) = 1 \\ \mathtt{not}(E_c(\tau,c)) & \textit{if } \mathbb{C}(t,c) = -1 \end{cases} = \mathtt{true} \tag{A.176}$$

   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:

$$E_c(\tau,c)\ .\prod_{c' \in conds(t) \setminus \{c\}} \begin{cases} E_c(\tau,c') & \textit{if } \mathbb{C}(t,c') = 1 \\ \mathtt{not}(E_c(\tau,c')) & \textit{if } \mathbb{C}(t,c') = -1 \end{cases} = \mathtt{true} \tag{A.177}$$

   From (A.177), we can deduce that $E_c(\tau,c) = \mathtt{true}$.

   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 $E_c(\tau,c) = \mathtt{true}$: tautology.

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

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

$$\sigma(id_t)(''scc'') = \prod_{c \in conds(t)} \begin{cases} E_c(\tau,c) & \textit{if } \mathbb{C}(t,c) = 1 \\ \mathtt{not}(E_c(\tau,c)) & \textit{if } \mathbb{C}(t,c) = -1 \end{cases} = \mathtt{true} \tag{A.178}$$

   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:

$$\mathtt{not}\ E_c(\tau,c)\ .\prod_{c' \in conds(t) \setminus \{c\}} \begin{cases} E_c(\tau,c') & \textit{if } \mathbb{C}(t,c') = 1 \\ \mathtt{not}(E_c(\tau,c')) & \textit{if } \mathbb{C}(t,c') = -1 \end{cases} = \mathtt{true} \tag{A.179}$$

   From (A.179), we can deduce that $E_c(\tau,c) = \mathtt{false}$.

   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 $E_c(\tau,c) = \mathtt{false}$: tautology.

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

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

(a) $\left(\texttt{not}\ \sigma(id_t)(''srtc'')\ .\ [\ldots]\right) = \texttt{true}$[1]

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

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

(a) $\left(\texttt{not}\ \sigma(id_t)(''srtc'')\ .\ [\ldots]\right) = \texttt{true}$:

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

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

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

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 $s'.I(t) = s.I(t) + 1$.

  $\Rightarrow \boxed{\sigma(id_t)(''A'') \leq s.I(t) + 1 \leq \sigma(id_t)(''B'')}$ (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 $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, we have $\sigma(id_t)(''stc'') = upper(I_s(t)) = b$.

[1] See equation (A.164) for the full definition

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. $(\Delta(id_t)("tt") = \texttt{TEMP\_A\_A} \mathbin{.} (\sigma(id_t)("stc") = \sigma(id_t)("A") - 1)) = \texttt{true}$:
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, <`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 $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, 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 $E_c, \tau \vdash s \overset{\downarrow}{\rightarrow} s'$, 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 $\gamma, E_c, \tau \vdash s \overset{\uparrow}{\sim} \sigma$, 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. $(\Delta(id_t)("tt") = \texttt{TEMP\_A\_INF} \mathbin{.} (\sigma(id_t)("stc") \geq \sigma(id_t)("A") - 1)) = \texttt{true}$:
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 $\sigma(id_t)(''se'') = \texttt{true}$, 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 $s'.I(t) = s.I(t) + 1$.
$\Rightarrow \boxed{\sigma(id_t)(''A'') \leq s.I(t) + 1}$ (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 $\sigma(id_t)(''se'') = \texttt{true}$, 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 $s'.I(t) = s.I(t) + 1$.
  $\Rightarrow \boxed{\sigma(id_t)(''A'') \leq s.I(t) + 1}$ (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) $\big(\sigma(id_t)(''srtc'') \,.\, \Delta(id_t)(''tt'') \neq \texttt{NOT\_TEMP} \,.\, \sigma(id_t)(''A'') = 1\big) = \texttt{true}$
Then, converting boolean equalities into intuitionistic predicates, we have:

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

By property of the elaboration relation, and $\Delta(id_t)(''tt'') \neq \texttt{NOT\_TEMP}$, 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 $\sigma(id_t)(''se'') = \texttt{true}$, we can deduce $t \in Sens(s.M)$, and from $\sigma(id_t)(''srtc'') = \texttt{true}$, we can deduce $s.reset_t(t) = \texttt{true}$.
By definition of $E_c, \tau \vdash s \xrightarrow{\downarrow} s'$, $t \in Sens(s.M)$ and $s.reset_t(t) = \texttt{true}$, 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) $\big(\Delta(id_t)(''tt'') = \texttt{NOT\_TEMP}\big) = \texttt{true}$
Let us show $\boxed{t \notin T_i}$.
By property of the elaboration relation and $\Delta(id_t)(''tt'') = \texttt{NOT\_TEMP}$, we have $t \notin T_i$.

□

Lemma 32 (Falling Edge Equal Not Firable). *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. Proving the above lemma is trivial by appealing to Lemma Falling Edge Equal Firable and by reasoning on contrapositives. □

A.4.7 Falling edge and fired transitions

Lemma 33 (Falling Edge Equal Fired Set). *then* $\forall t \in T$, $id_t \in Comps(\Delta)$ *s.t.* $\gamma(t) = id_t$, $\forall fset \subseteq T$, *s.t.* $IsFiredSet(s', fset)$, $t \in fset \Leftrightarrow \sigma'(id_t)(''fired'') = true$.

Proof. Given a $t \in T$, and $id_t \in Comps(\Delta)$, and a $fset \subseteq T$ s.t. $IsFiredSet(s', fset)$, let us show $\boxed{t \in fset \Leftrightarrow \sigma'(id_t)(''fired'') = true.}$

By definition of $IsFiredSet(s', fset)$, we have $IsFiredSetAux(s', \emptyset, T, fset)$.
Then, we can appeal to Lemma Falling Edge Equal Fired Set Aux to solve the goal, but first we must prove the following *extra hypothesis* (i.e, one of the premise of Lemma Falling Edge Equal Fired Set Aux):

$$\boxed{\begin{array}{l}\forall t' \in T, id_{t'} \in Comps(\Delta) \text{ s.t. } \gamma(t') = id_{t'},\\ (t' \in \emptyset \Rightarrow \sigma'(id_{t'})(''fired'') = \texttt{true}) \wedge (\sigma'(id_{t'})(''fired'') = \texttt{true} \Rightarrow t' \in \emptyset \vee t' \in T).\end{array}}$$

Given a $t' \in T$ and an $id_{t'} \in Comps(\Delta)$ s.t. $\gamma(t') = id_{t'}$, there are two points to prove:

1. $\boxed{t' \in \emptyset \Rightarrow \sigma'(id_{t'})(''fired'') = \texttt{true}}$
2. $\boxed{\sigma'(id_{t'})(''fired'') = \texttt{true} \Rightarrow t' \in \emptyset \vee t' \in T}$

Let us show these two points:

1. Assuming $t' \in \emptyset$, let us show $\boxed{\sigma'(id_{t'})(''fired'') = \texttt{true}.}$

   $t' \in \emptyset$ is a contradiction.

2. Assuming $\sigma'(id_{t'})(''fired'') = \texttt{true}$, let us show $\boxed{t' \in \emptyset \vee t' \in T.}$

   By definition, $t' \in T$.

□

Lemma 34 (Falling Edge Equal Fired Set Aux). *then* $\forall t \in T, id_t \in Comps(\Delta)$ *s.t.* $\gamma(t) = id_t$, $\forall fired \subseteq T$, $T_s \subseteq T$, $fset \subseteq T$, *assume that:*

- $IsFiredSetAux(s', fired, T_s, fset)$
- *EH (Extra. Hypothesis):*
  $\forall t' \in T$, $id_{t'} \in Comps(\Delta)$ s.t. $\gamma(t') = id_{t'}$,
  $(t' \in fired \Rightarrow \sigma'(id_{t'})(''fired'') = \texttt{true}) \wedge (\sigma'(id_{t'})(''fired'') = \texttt{true} \Rightarrow t' \in fired \vee t' \in T_s)$.

then $t \in fset \Leftrightarrow \sigma'(id_t)(''fired'') = \texttt{true}$.

Proof. Given a $t \in T$, an $id_t \in Comps(\Delta)$, a $fired, T_s, fset \subseteq T$, and assuming $IsFiredSetAux(s', fired, T_s, fset)$ and EH, let us show $\boxed{t \in fset \Leftrightarrow \sigma'(id_t)(''fired'') = \texttt{true}.}$
Let us reason by induction on $IsFiredSetAux(s', fired, T_s, fset)$.

- **BASE CASE**: $\boxed{t \in fired \Leftrightarrow \sigma'(id_t)(''fired'') = \texttt{true}.}$

  In that case, $fired = fset$ and $T_s = \emptyset$, EH looks like this:

  $\forall t' \in T$, $id_{t'} \in Comps(\Delta)$ s.t. $\gamma(t') = id_{t'}$,
  $(t' \in fired \Rightarrow \sigma'(id_{t'})(''fired'') = \texttt{true}) \wedge (\sigma'(id_{t'})(''fired'') = \texttt{true} \Rightarrow t' \in fired \vee t' \in \emptyset)$.

  From EH, we can deduce $t \in fired \Leftrightarrow \sigma'(id_t)(''fired'') = \texttt{true}.$

- **INDUCTION CASE**: $\boxed{t \in fset \Leftrightarrow \sigma'(id_t)(''fired'') = \texttt{true}.}$

  In that case, we have:

  - $IsTopPrioritySet(T_s, tp)$
  - $ElectFired(s', fired, tp, fired')$
  - $FiredAux(s', fired', T_s \setminus tp, fset)$

  $(\forall t' \in T, id_{t'} \in Comps(\Delta)$ *s.t.* $\gamma(t') = id_{t'}$,
  $(t' \in fired' \Rightarrow \sigma'(id_{t'})(''fired'') = \texttt{true}) \wedge (\sigma'(id_{t'})(''fired'') = \texttt{true} \Rightarrow t' \in fired' \vee t' \in T_s \setminus tp)) \Rightarrow$
  $t \in fset \Leftrightarrow \sigma'_t(''fired'') = true.$

  Applying the induction hypothesis, then, the new goal is:

  $\forall t' \in T, id_{t'} \in Comps(\Delta)$ *s.t.* $\gamma(t') = id_{t'}$,
  $(t' \in fired' \Rightarrow \sigma'(id_{t'})(''fired'') = \texttt{true})$
  $\wedge(\sigma'(id_{t'})(''fired'') = \texttt{true} \Rightarrow t' \in fired' \vee t' \in T_s \setminus tp)$

  Apply Lemma Elect Fired Equal Fired to solve the goal.

□

Lemma 35 (Elect Fired Equal Fired). *then* $\forall fired, fired', T_s, tp, fset \subseteq T$, *assume that:*

- $IsTopPrioritySet(T_s, tp)$
- $ElectFired(s', fired, tp, fired')$
- $FiredAux(s', fired', T_s \setminus tp, fset)$
- *EH (Extra. Hypothesis):*
  $\forall t' \in T, id_{t'} \in Comps(\Delta)$ *s.t.* $\gamma(t') = id_{t'}$,
  $(t' \in fired \Rightarrow \sigma'(id_{t'})(''fired'') = \texttt{true}) \wedge (\sigma'(id_{t'})(''fired'') = \texttt{true} \Rightarrow t' \in fired \vee t' \in T_s)$

then $\forall t \in T, id_t \in Comps(\Delta)$ *s.t.* $\gamma(t) = id_t$,
$(t \in fired' \Rightarrow \sigma'(id_t)(''fired'') = \texttt{true}) \wedge (\sigma'(id_t)(''fired'') = \texttt{true} \Rightarrow t \in fired' \vee t \in T_s \setminus tp)$.

Proof. Given a $t \in T$ and an $id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$, let us show
$\boxed{(t \in fired' \Rightarrow \sigma'(id_t)(''fired'') = \texttt{true}) \wedge (\sigma'(id_t)(''fired'') = \texttt{true} \Rightarrow t \in fired' \vee t \in T_s \setminus tp).}$

Let us reason by induction on $ElectFired(s', fired, tp, fired')$; there are three cases:

1. **BASE CASE**: $tp = \emptyset$ and $fired = fired'$.
2. **INDUCTIVE CASE**: $tp = \{t_0\} \cup tp_0$ and t_0 is elected to be fired.
3. **INDUCTIVE CASE**: $tp = \{t_0\} \cup tp_0$ and t_0 is not elected to be fired.

Let us prove the goal in these three contexts:

1. **BASE CASE**:

$$\boxed{(t \in fired \Rightarrow \sigma'(id_t)(''fired'') = \mathtt{true}) \wedge (\sigma'(id_t)(''fired'') = \mathtt{true} \Rightarrow t \in fired \vee t \in T_s).}$$

Apply EH to solve the goal.

2. **INDUCTIVE CASE**: $tp = \{t_0\} \cup tp_0$ and t_0 is elected to be fired.

In that case, we have:

- $IsTopPrioritySet(T_s, \{t_0\} \cup tp_0)$
- $ElectFired(s', fired \cup \{t_0\}, tp_0, fired')$
- $IsFiredSetAux(s', fired', T_s \setminus \{t_0\} \cup tp_0, fset)$
- $t_0 \in Firable(s')$
- $t_0 \in Sens(s'.M - \sum_{t_i \in Pr(t, fired)} pre(t_i))$ where $Pr(t, fired) = \{t' \mid t' \succ t \wedge t' \in fired\}$
- EH: $\forall t' \in T,\ id_{t'} \in Comps(\Delta)$ s.t. $\gamma(t') = id_{t'}$,
  $(t' \in fired \Rightarrow \sigma'(id_{t'})(''f'') = \mathtt{true}) \wedge (\sigma'(id_{t'})(''f'') = \mathtt{true} \Rightarrow t' \in fired\ \vee\ t' \in T_s)$

$\forall T_s' \subseteq T,$
$IsTopPrioritySet(T_s', tp_0) \Rightarrow$
$IsFiredSetAux(s', fired', T_s' \setminus tp_0, fset) \Rightarrow$
$(\forall t' \in T, id_{t'} \in Comps(\Delta)$ s.t. $\gamma(t') = id_{t'},$
$(t' \in fired \cup \{t_0\} \Rightarrow \sigma_{t'}'(''f'') = \mathtt{true}) \wedge (\sigma'(id_{t'})(''f'') = \mathtt{true} \Rightarrow t' \in fired \cup \{t_0\}\ \vee\ t' \in T_s')) \Rightarrow$
$\forall t \in T,\ id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t,$
$(t \in fired' \Rightarrow \sigma'(id_t)(''f'') = \mathtt{true}) \wedge (\sigma'(id_t)(''f'') = \mathtt{true} \Rightarrow t \in fired' \vee t \in T_s' \setminus tp_0)$

$\forall t \in T,\ id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t,$
$(t \in fired' \Rightarrow \sigma_t'(''f'') = \mathtt{true}) \wedge (\sigma_t'(''f'') = \mathtt{true} \Rightarrow t \in fired' \vee t \in T_s \setminus \{t_0\} \cup tp_0)$

To solve the goal, we can apply the induction hypothesis with $T_s' = T_s \setminus \{t_0\}$; then, there are three points to prove:

(a) $\boxed{IsTopPrioritySet(T_s \setminus \{t_0\}, tp_0)}$

(b) $\boxed{IsFiredSetAux(s', fired', (T_s \setminus \{t_0\}) \setminus tp_0, fset)}$

(c) $\forall t' \in T, id_{t'} \in Comps(\Delta)$ s.t. $\gamma(t') = id_{t'},$
$(t' \in fired \cup \{t_0\} \Rightarrow \sigma_{t'}'(''f'') = \mathtt{true}) \wedge (\sigma'(id_{t'})(''f'') = \mathtt{true} \Rightarrow t' \in fired \cup \{t_0\}\ \vee\ t' \in T_s \setminus \{t_0\})$

Let us prove these three points:

(a) $\boxed{IsTopPrioritySet(T_s \setminus \{t_0\}, tp_0)}$

Not provable yet.

(b) $\boxed{IsFiredSetAux(s', fired', (T_s \setminus \{t_0\}) \setminus tp_0, fset)}$.
We know that $(T_s \setminus \{t_0\}) \setminus tp_0 = T_s \setminus (\{t_0\} \cup tp_0)$, and thus
$IsFiredSetAux(s', fired', T_s \setminus (\{t_0\} \cup tp_0), fset)$ is an assumption.

(c) $\boxed{\begin{array}{l}\forall t' \in T, id_{t'} \in Comps(\Delta) \text{ s.t. } \gamma(t') = id_{t'}, \\ (t' \in fired \cup \{t_0\} \Rightarrow \sigma'(id_{t'})(''f'') = \mathtt{true}) \wedge (\sigma'(id_{t'})(''f'') = \mathtt{true} \Rightarrow t' \in fired \cup \\ \{t_0\} \ \vee \ t' \in T_s \setminus \{t_0\})\end{array}}$

Given a $t' \in T$ and an $id_{t'} \in Comps(\Delta)$ s.t. $\gamma(t') = id_{t'}$, let us show
$\boxed{\begin{array}{l}(t' \in fired \cup \{t_0\} \Rightarrow \sigma'(id_{t'})(''f'') = \mathtt{true}) \\ \wedge (\sigma'(id_{t'})(''f'') = \mathtt{true} \Rightarrow t' \in fired \cup \{t_0\} \ \vee \ t' \in T_s \setminus \{t_0\}).\end{array}}$
The proof is in two parts.

i. Assuming that $t' \in fired \cup \{t_0\}$, let us show $\boxed{\sigma'(id_{t'})(''f'') = \mathtt{true}.}$
Case analysis on $t' \in fired \cup \{t_0\}$; there are two cases:
- $t' \in fired$
- $t' = t_0$

Let us prove the goal in these two contexts.
- **CASE** $t' \in fired$: Thanks to EH, we can deduce $\sigma'_{t'}(''f'') = \mathtt{true}$.
- **CASE** $t' = t_0$:
By definition of $id_{t'}$, there exist a $gm_{t'}$, $ipm_{t'}$, $opm_{t'}$ s.t. $\mathtt{comp}(id_{t'}, ''transition'', gm_{t'}, ipm_{t'}, opm_{t'}) \in d.cs$.
By property of the stabilize relation and $\mathtt{comp}(id_{t'}, ''transition'', gm_{t'}, ipm_{t'}, opm_{t'}) \in d.cs$:
$$\sigma(id_{t'})(''f'') = \sigma(id_{t'})(''sfa'') \,.\, \sigma(id_{t'})(''spc'') \tag{A.180}$$
Rewriting the goal with (A.180): $\boxed{\sigma(id_{t'})(''sfa'') \,.\, \sigma(id_{t'})(''spc'') = \mathtt{true}.}$
Then, we can show that:
  - $\sigma(id_{t'})(''sfa'') = \mathtt{true}$ by applying Lemma Falling Edge Equal Firable
  - $\sigma(id_{t'})(''spc'') = \mathtt{true}$ by applying Lemma Stabilize Compute Priority Combination After Falling Edge.

ii. Assuming that $\sigma'(id_{t'})(''f'') = \mathtt{true}$, let us show $\boxed{t' \in fired \cup \{t_0\} \ \vee \ t' \in T_s \setminus \{t_0\}.}$
From $\sigma'(id_{t'})(''f'') = \mathtt{true}$ and EH, we can deduce that $t' \in fired \vee t' \in T_s$.
Case analysis on $t' \in fired \vee t' \in T_s$.
- **CASE** $t' \in fired$: then, it is trivial to show $t' \in fired \cup \{t_0\}$.
- **CASE** $t' \in T_s$: We know that $t_0 \in T_s$. Therefore, either $t' \in T_s \setminus \{t_0\}$, or $t' = t_0$, and then, $t' \in fired \cup \{t_0\}$.

3. **INDUCTIVE CASE**: $tp = \{t_0\} \cup tp_0$ and t_0 is not elected to be fired.

- $IsTopPrioritySet(T_s, \{t_0\} \cup tp_0)$
- $ElectFired(s', fired, tp_0, fired')$

- $IsFiredSetAux(s', fired', T_s \setminus \{t_0\} \cup tp_0, fset)$
- $\neg\big(t_0 \in Firable(s') \wedge t_0 \in Sens(s'.M - \sum_{t_i \in Pr(t, fired)} pre(t_i))\big)$
- EH:
  $\forall t' \in T, id_{t'} \in Comps(\Delta)$ s.t. $\gamma(t') = id_{t'}$,
  $(t' \in fired \Rightarrow \sigma'(id_{t'})(''f'') = \texttt{true}) \wedge (\sigma'(id_{t'})(''f'') = \texttt{true} \Rightarrow t' \in fired \ \vee \ t' \in T_s)$

$\forall T'_s \subseteq T$,
$IsTopPrioritySet(T'_s, tp_0) \Rightarrow$
$IsFiredSetAux(s', fired', T'_s \setminus tp_0, fset) \Rightarrow$
$\big(\forall t' \in T, id_{t'} \in Comps(\Delta)$ s.t. $\gamma(t') = id_{t'}$,
$(t' \in fired \Rightarrow \sigma'(id_{t'})(''f'') = \texttt{true}) \wedge (\sigma'(id_{t'})(''f'') = \texttt{true} \Rightarrow t' \in fired \ \vee \ t' \in T'_s)\big) \Rightarrow$
$\forall t \in T, id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$,
$\big(t \in fired' \Rightarrow \sigma'(id_t)(''f'') = \texttt{true}\big) \wedge \big(\sigma'(id_t)(''f'') = \texttt{true} \Rightarrow t \in fired' \vee t \in T'_s \setminus tp_0\big)$

$\forall t \in T, id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$,
$\big(t \in fired' \Rightarrow \sigma'(id_t)(''f'') = \texttt{true}\big) \wedge \big(\sigma'(id_t)(''f'') = \texttt{true} \Rightarrow t \in fired' \vee t \in T_s \setminus \{t_0\} \cup tp_0\big)$.

Then, we can apply the induction hypothesis with $T'_s = T_s \setminus \{t_0\}$, then, there are three points to prove:

(a) $\boxed{IsTopPrioritySet(T_s \setminus \{t_0\}, tp_0)}$

(b) $\boxed{IsFiredSetAux(s', fired', (T_s \setminus \{t_0\}) \setminus tp_0, fset)}$

(c) $\forall t' \in T, id_{t'} \in Comps(\Delta)$ s.t. $\gamma(t') = id_{t'}$,
$(t' \in fired \Rightarrow \sigma'(id_{t'})(''f'') = \texttt{true}) \wedge (\sigma'(id_{t'})(''f'') = \texttt{true} \Rightarrow t' \in fired \ \vee \ t' \in T_s \setminus \{t_0\})$

Let us prove these three points:

(a) $\boxed{IsTopPrioritySet(T_s \setminus \{t_0\}, tp_0)}$

Not provable yet.

(b) $\boxed{IsFiredSetAux(s', fired', (T_s \setminus \{t_0\}) \setminus tp_0, fset)}$
We know that $(T_s \setminus \{t_0\}) \setminus tp_0 = T_s \setminus (\{t_0\} \cup tp_0)$, and thus
$IsFiredSetAux(s', fired', T_s \setminus (\{t_0\} \cup tp_0), fset)$ is an assumption.

(c) $\forall t' \in T, id_{t'} \in Comps(\Delta)$ s.t. $\gamma(t') = id_{t'}$,
$(t' \in fired \Rightarrow \sigma'(id_{t'})(''f'') = \texttt{true}) \wedge (\sigma'(id_{t'})(''f'') = \texttt{true} \Rightarrow t' \in fired \ \vee \ t' \in T_s \setminus \{t_0\})$
Given a $t' \in T$ and an $id_{t'} \in Comps(\Delta)$ s.t. $\gamma(t') = id_{t'}$, let us show

$(t' \in fired \Rightarrow \sigma'(id_{t'})(''f'') = \texttt{true}) \wedge (\sigma'(id_{t'})(''f'') = \texttt{true} \Rightarrow t' \in fired \ \vee \ t' \in T_s \setminus \{t_0\})$

The proof is in two parts:

i. Assuming that $t' \in fired$, let us show $\boxed{\sigma'(id_{t'})("f") = \texttt{true}.}$
   From $t' \in fired$ and EH, $\sigma'(id_{t'})("f") = \texttt{true}.$

ii. Assuming that $\sigma'(id_{t'})("f") = \texttt{true}$, let us show $\boxed{t' \in fired \ \lor \ t' \in T_s \setminus \{t_0\}.}$
   Thanks to $\sigma'(id_{t'})("f") = \texttt{true}$ and EH, we know that: $t' \in fired \lor t' \in T_s$.
   Case analysis on $t' \in fired \lor t' \in T_s$; there are two cases:

   - **CASE** $t' \in fired.$
   - **CASE** $t' \in T_s$:
     From $IsTopPrioritySet(T_s, \{t_0\} \cup tp_0)$, we can deduce that $t_0 \in T_s$. Therefore, either $t' \in T_s \setminus \{t_0\}$ or $t' = t_0$.
     In the case where $t' = t_0$, we need to show a contradiction by proving $t' \in Firable(s')$ and $t' \in Sens(s'.M - \sum_{t_i \in Pr(t, fired)} pre(t_i))$ based on $\sigma'(id_{t'})("f") = \texttt{true}$.
     By definition of $id_{t'}$, there exist a $gm_{t'}$, $ipm_{t'}$, $opm_{t'}$ s.t. $\texttt{comp}(id_{t'}, "transition", gm_{t'}, ipm_{t'}, opm_{t'}) \in d.cs$.
     By property of the stabilize relation and $\texttt{comp}(id_{t'}, "transition", gm_{t'}, ipm_{t'}, opm_{t'}) \in d.cs$:
     $$\sigma(id_{t'})("f") = \sigma(id_{t'})("sfa") \,.\, \sigma(id_{t'})("spc") = \texttt{true} \tag{A.181}$$
     From $\sigma(id_{t'})("sfa") = \texttt{true}$, and appealing to Lemma Falling Edge Equal Firable, we can deduce $t' \in Firable(s')$.
     From $\sigma(id_{t'})("spc") = \texttt{true}$, and appealing to Lemma Stabilize Compute Priority Combination After Falling Edge, we can deduce $t' \in Sens(s'.M - \sum_{t_i \in Pr(t, fired)} pre(t_i))$.
     Then, as $t' = t_0$, $\neg(t_0 \in Firable(s') \land t_0 \in Sens(s'.M - \sum_{t_i \in Pr(t, fired)} pre(t_i)))$ is a contradiction.

□

Lemma 36 (Stabilize Compute Priority Combination After Falling Edge). *then* $\forall t \in T, id_t \in Comps(\Delta)$ *s.t.* $\gamma(t) = id_t$,
$\forall fired, fired', T_s, tp, fset \subseteq T$ *assume that:*

- $IsTopPrioritySet(T_s, \{t\} \cup tp)$
- $ElectFired(s', fired, tp, fired')$
- $FiredAux(s', fired', T_s \setminus \{t\} \cup tp, fset)$
- *EH:* $\forall t' \in T, id_{t'} \in Comps(\Delta)$ *s.t.* $\gamma(t') = id_{t'}$,
  $(t' \in fired \Rightarrow \sigma'(id_{t'})("f") = \texttt{true}) \land (\sigma'(id_{t'})("f") = \texttt{true} \Rightarrow t' \in fired \ \lor \ t' \in T_s)$.
- $t \in Firable(s')$

then $t \in Sens(s'.M - \sum_{t_i \in Pr(t, fired)} pre(t_i)) \Leftrightarrow \sigma'(id_t)("spc") = \texttt{true}$

Proof. Given a $t \in T$ and an $id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$, a $fired$, $fired'$, T_s, tp, $fset \subseteq T$ and assuming all the above hypotheses, let us show

$\boxed{t \in Sens(s'.M - \sum_{t_i \in Pr(t,fired)} pre(t_i)) \Leftrightarrow \sigma'(id_t)(''spc'') = \mathtt{true}.}$

By construction and by definition of id_t, there exist gm_t, ipm_t, opm_t s.t. $\mathtt{comp}(id_t, ''transition'', gm_t, ipm_t, opm_t) \in d.cs$.

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

$$\sigma'(id_t)(''spc'') = \prod_{i=0}^{\Delta(id_t)(''ian'')-1} \sigma'(id_t)(''pauths'')[i] \tag{A.182}$$

Rewriting the goal with (A.182):

$\boxed{t \in Sens(s'.M - \sum_{t_i \in Pr(t,fired)} pre(t_i)) \Leftrightarrow \prod_{i=0}^{\Delta(id_t)(''ian'')-1} \sigma'(id_t)(''pauths'')[i] = \mathtt{true}.}$

Then, the proof is in two parts:

1. $t \in Sens(s'.M - \sum_{t_i \in Pr(t,fired)} pre(t_i)) \Rightarrow \prod_{i=0}^{\Delta(id_t)(''ian'')-1} \sigma'(id_t)(''pauths'')[i] = \mathtt{true}$
2. $\prod_{i=0}^{\Delta(id_t)(''ian'')-1} \sigma'(id_t)(''pauths'')[i] = \mathtt{true} \Rightarrow t \in Sens(s'.M - \sum_{t_i \in Pr(t,fired)} pre(t_i))$

Let us prove both sides of the equivalence:

1. Assuming that $t \in Sens(s'.M - \sum_{t_i \in Pr(t,fired)} pre(t_i))$, let us show

   $\boxed{\prod_{i=0}^{\Delta(id_t)(''ian'')-1} \sigma'(id_t)(''pauths'')[i] = \mathtt{true}.}$

   Let us perform case analysis on $input(t)$; there are 2 cases:

   - **CASE** $input(t) = \emptyset$:
     By construction, $<\mathtt{input\_arcs\_number} \Rightarrow 1> \in gm_t$ and $<\mathtt{priority\_authorizations}(0) \Rightarrow \mathtt{true}> \in ipm_t$.
     By property of the elaboration relation, we have $\Delta(id_t)(''ian'') = 1$, and by property of the stabilize relation, we have $\sigma'(id_t)(''pauths'')[0] = \mathtt{true}$.
     Rewriting the goal with $\Delta(id_t)(''ian'') = 1$ and $\sigma'(id_t)(''pauths'')[0] = \mathtt{true}$, and simplifying the goal: tautology.
   - **CASE** $input(t) \neq \emptyset$:
     Then, let us show an equivalent goal:
     $\boxed{\forall i \in [0, \Delta(id_t)(''ian'') - 1],\ \sigma'(id_t)(''pauths'')[i] = \mathtt{true}.}$
     Given an $i \in [0, \Delta(id_t)(''ian'') - 1]$, let us show $\boxed{\sigma'(id_t)(''pauths'')[i] = \mathtt{true}.}$
     By construction, $<\mathtt{input\_arcs\_number} \Rightarrow |input(t)|> \in gm_t$.
     By property of the elaboration relation, we have $\Delta(id_t)(''ian'') = |input(t)|$. Then, we can deduce $i \in [0, |input(t)| - 1]$.

By construction, for all $i \in [0, |input(t)| - 1]$, there exist a $p \in input(t)$ and an $id_p \in Comps(\Delta)$ s.t. $\gamma(p) = id_p$, there exist a gm_p, ipm_p, opm_p s.t. $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$, and there exist a $j \in [0, |output(p)|]$ and an $id_{ji} \in Sigs(\Delta)$ s.t. $<\texttt{input\_arcs\_valid(i)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in ipm_t$ and $<\texttt{output\_arcs\_valid(j)} \Rightarrow \texttt{id}_{\texttt{ji}}> \in opm_t$.
Let us take such a $p \in input(t)$, $id_p \in Comps(\Delta)$, gm_p, ipm_p, opm_p, $j \in [0, |output(p)|]$ and $id_{ji} \in Sigs(\Delta)$.
Now, let us perform case analysis on the nature of the arc connecting p and t; there are 2 cases:

– **CASE** $pre(p,t) = (\omega, \texttt{test})$ or $pre(p,t) = (\omega, \texttt{inhib})$:
  By construction, $<\texttt{priority\_authorizations(i)} \Rightarrow \texttt{true}> \in ipm_t$, and by property of the stabilize relation: $\sigma'(id_t)("pauths")[i] = \texttt{true}$.
– **CASE** $pre(p,t) = (\omega, \texttt{basic})$:
  Let us define $output_c(p) = \{t \in T \mid \exists \omega,\ pre(p,t) = (\omega, \texttt{basic})\}$, the set of output transitions of p that are in conflict. Then, there are two cases, one for each way to solve the conflicts between the output transitions of p:
  * **CASE** For all pair of transitions in $output_c(p)$, all conflicts are solved by mutual exclusion:
    By construction, $<\texttt{priority\_authorizations(i)} \Rightarrow \texttt{true}> \in ipm_t$, and by property of the stabilize relation: $\sigma'(id_t)("pauths")[i] = \texttt{true}$.
  * **CASE** The priority relation is a strict total order over the set $output_c(p)$:
    By construction, there exists an $id'_{ji} \in Sigs(\Delta)$ s.t.
    $<\texttt{priority\_authorizations(i)} \Rightarrow \texttt{id}'_{\texttt{ji}}> \in ipm_t$ and
    $<\texttt{priority\_authorizations(j)} \Rightarrow \texttt{id}'_{\texttt{ji}}> \in opm_p$.
    By property of the stabilize relation, $\texttt{comp}(id_t, "transition", gm_t, ipm_t, opm_t) \in d.cs$ and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$:

$$\sigma'(id_t)("pauths")[i] = \sigma'(id'_{ji}) = \sigma'(id_p)("pauths")[j] \tag{A.183}$$

    Rewriting the goal with (A.183): $\boxed{\sigma'(id_p)("pauths")[j] = \texttt{true}.}$
    By property of the stabilize relation and $\texttt{comp}(id_p, "place", gm_p, ipm_p, opm_p) \in d.cs$:

$$\sigma'(id_p)("pauths")[j] = (\sigma'(id_p)("sm") \geq \texttt{vsots} + \sigma'(id_p)("oaw")[j]) \tag{A.184}$$

    Let us define the $\texttt{vsots}$ term as follows:

$$\texttt{vsots} = \sum_{i=0}^{j-1} \begin{cases} \sigma'(id_p)("oaw")[i] \ \texttt{if} \ \sigma'(id_p)("otf")[i]. \\ \qquad\qquad\qquad\qquad \sigma'(id_p)("oat")[i] = \texttt{basic} \\ 0 \ otherwise \end{cases} \tag{A.185}$$

    Rewriting the goal with (A.184): $\boxed{\sigma'(id_p)("sm") \geq \texttt{vsots} + \sigma'(id_p)("oaw")[j]}$
    By definition of $t \in Sens(s'.M - \sum_{t_i \in Pr(t, fired)} pre(t_i))$, we have $s'.M(p) \geq \sum_{t_i \in Pr(t, fired)} pre(p, t_i) + \omega$.
    Then, there are three points to prove:
    (a) $\boxed{s'.M(p) = \sigma'(id_p)("sm")}$

(b) $\boxed{\omega = \sigma'(id_p)(''oaw'')[j]}$

(c) $\boxed{\sum_{t_i \in Pr(t,fired)} pre(p,t_i) = \texttt{vsots}}$

Let us prove these three points:

(a) $\boxed{s'.M(p) = \sigma'(id_p)(''sm'')}$

Appealing to Lemma Falling Edge Equal Marking: $s'.M(p) = \sigma'(id_p)(''sm'')$.

(b) $\boxed{\omega = \sigma'(id_p)(''oaw'')[j]}$

By construction, and as $pre(p,t) = (\omega, \texttt{basic})$, we have $<\texttt{output\_arcs\_weights(j)} \Rightarrow \omega> \in ipm_p$.

By property of the stabilize relation and $\texttt{comp}(id_p, ''place'', gm_p, ipm_p, opm_p) \in d.cs$: $\omega = \sigma'(id_p)(''oaw'')[j]$.

(c) $\boxed{\sum_{t_i \in Pr(t,fired)} pre(p,t_i) = \texttt{vsots}}$

Let us replace the left and right term of the equality by their full definition:

$$\boxed{\begin{gathered}\sum_{t_i \in Pr(t,fired)} \begin{cases} \omega \texttt{ if } pre(p,t_i) = (\omega, \texttt{basic}) \\ 0 \textit{ otherwise} \end{cases} \\ = \\ \sum_{i=0}^{j-1} \begin{cases} \sigma'(id_p)(''oaw'')[i] \texttt{ if } \sigma'(id_p)(''otf'')[i]. \\ \qquad \sigma'(id_p)(''oat'')[i] = \texttt{basic} \\ 0 \textit{ otherwise} \end{cases}\end{gathered}}$$

Let us define $f(t_i) = \begin{cases} \omega \texttt{ if } pre(p,t_i) = (\omega, \texttt{basic}) \\ 0 \textit{ otherwise} \end{cases}$ and

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

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

BASE CASE: then, we have $i > j - 1$, and then $j = 0$.

$$\boxed{\sum_{t_i \in Pr(t,fired)} \begin{cases} \omega \texttt{ if } pre(p,t_i) = (\omega, \texttt{basic}) \\ 0 \textit{ otherwise} \end{cases} = 0}$$

We know that the priority relation is a strict total order over the transitions of set $output_c(p)$. This ordering is reflected in the ordering of the indexes of output port `priority_authorizations` of place component instances. Thus, in the `priority_-authorizations` output port of a place component instance, the element of index 0 is connected to the transition of $output_c(t)$ with the highest firing priority. We know that component id_t is connected to `priority_authorizations(0)` in the output port map of component id_p. By construction, transition t is the transition of $output_c(p)$ with the highest firing priority, i.e, $\nexists t' \in output_c(p)$ s.t. $t' \succ t$.

For all transition $t_i \in Pr(t, fired)$, either t_i is not in $output_c(p)$, and thus t_i has no effect in the value of the sum term $\sum\limits_{t_i \in Pr(t,fired)} f(t_i)$; or, $t_i \in output_c(p)$. Then, by definition of $t_i \in Pr(t, fired)$, $t_i \succ t$, which is contradiction with $\nexists t' \in output_c(p)$ s.t. $t' \succ t$.

INDUCTIVE CASE: then, $0 \leq j - 1$, and thus $j > 0$.

For all $Pr' \subseteq T$, $g(0) + \sum\limits_{t_i \in Pr'} f(t_i) = g(0) + \sum\limits_{i=1}^{j-1} g(i)$

$$\sum_{t_i \in Pr(t,fired)} f(t_i) = g(0) + \sum_{i=1}^{j-1} g(i).$$

By definition of $g(0)$:

$$\sum_{t_i \in Pr(t,fired)} f(t_i) = \begin{cases} \sigma'(id_p)(\text{"}oaw\text{"})[0] \texttt{ if } \sigma'(id_p)(\text{"}otf\text{"})[0]. \\ \qquad\qquad \sigma'(id_p)(\text{"}oat\text{"})[0] = \texttt{basic} \\ 0 \ otherwise \end{cases} + \sum_{i=1}^{j-1} g(i).$$

Case analysis on the value of $\sigma'(id_p)(\text{"}otf\text{"})[0] \ . \ \sigma'(id_p)(\text{"}oat\text{"})[0] = \texttt{basic}$:

In the case where $\big(\sigma'(id_p)(\text{"}otf\text{"})[0] \ . \ \sigma'(id_p)(\text{"}oat\text{"})[0] = \texttt{basic}\big) = \texttt{false}$, then $g(0) = 0$, and we can use the induction hypothesis with $Pr' = Pr(t, fired)$ to prove the goal.

In the case where $\big(\sigma'(id_p)(\text{"}otf\text{"})[0] \ . \ \sigma'(id_p)(\text{"}oat\text{"})[0] = \texttt{basic}\big) = \texttt{true}$, then $g(0) = \sigma'(id_p)(\text{"}oaw\text{"})[0]$:

$$\sum_{t_i \in Pr(t,fired)} f(t_i) = \sigma'(id_p)(\text{"}oaw\text{"})[0] + \sum_{i=1}^{j-1} g(i).$$

By construction, and knowing that $j > 0$ and that the priority relation is a strict total order over the set $output_c(p)$, there exist a $t_0 \in output_c(p)$ s.t. $t_0 \succ t$. Moreover, there exist an $id_{t_0} \in Comps(\Delta)$ s.t. $\gamma(t_0) = id_{t_0}$, and by definition of id_{t_0}, there exist gm_{t_0}, ipm_{t_0} and opm_{t_0} s.t. $\texttt{comp}(id_{t_0}, \text{"}transition\text{"}, gm_{t_0}, ipm_{t_0}, opm_{t_0}) \in d.cs$. Finally, there exist an $id_{ft_0} \in Sigs(\Delta)$ s.t. $<\texttt{fired} \Rightarrow \texttt{id}_{\texttt{ft}_0}> \in opm_{t_0}$ and $<\texttt{output\_transitions\_fired}(0) \Rightarrow \texttt{id}_{\texttt{ft}_0}> \in ipm_p$.
By property of the stabilize relation, $\texttt{comp}(id_p, \text{"}place\text{"}, gm_p, ipm_p, opm_p) \in d.cs$ and $\texttt{comp}(id_{t_0}, \text{"}transition\text{"}, gm_{t_0}, ipm_{t_0}, opm_{t_0}) \in d.cs$:

$$\sigma'(id_{t_0})(\text{"}f\text{"}) = \sigma'(id_{ft_0}) = \sigma'(id_p)(\text{"}otf\text{"})[0] = \texttt{true} \tag{A.186}$$

From EH and $\sigma'(id_{t_0})(''f'') = \mathtt{true}$, we have either $t_0 \in fired$ or $t_0 \in T_s$.

❑ In the case where $t_0 \in fired$, then, by definition of $\sum$:

$$\boxed{f(t_0) + \sum_{t_i \in Pr(t,fired)\setminus\{t_0\}} f(t_i) = \sigma'(id_p)(''oaw'')[0] + \sum_{i=1}^{j-1} g(i).}$$

By definition of $t_0 \in output_c(p)$, there exists $\omega \in \mathbb{N}^*$ s.t. $pre(p, t_0) = (\omega, \mathtt{basic})$. Thus, we have $f(t_0) = \omega$
By construction, $<\mathtt{output\_arcs\_weights}(0) \Rightarrow \omega>$, and by property of the stabilize relation, we have $\sigma'(id_p)(''oaw'')[0] = \omega$. Thus, we can deduce that $g(0) = \omega$, and then we can rewrite the goal in order to apply the induction hypothesis with $Pr' = Pr(t, fired) \setminus \{t_0\}$.

❑ In the case where $t_0 \in T_s$:
As t is a top-priority transition in set T_s, there exists no transition $t' \in T_s$ s.t. $t' \succ t$.
Contradicts $t_0 \succ t$.

2. Assuming that $\prod_{i=0}^{\Delta(id_t)(''ian'')-1} \sigma'(id_t)(''pauths'')[i] = \mathtt{true}$, let us show $\boxed{t \in Sens(s'.M - \sum_{t_i \in Pr(t,fired)} pre(t_i)).}$

   By definition of $t \in Sens(s'.M - \sum_{t_i \in Pr(t,fired)} pre(t_i))$:

$$\boxed{\begin{array}{l}\forall p \in P, \omega \in \mathbb{N}^*,\\ \big((pre(p,t) = (\omega, \mathtt{basic}) \vee pre(p,t) = (\omega, \mathtt{test})) \Rightarrow s'.M(p) - \sum_{t_i \in Pr(t,fired)} pre(p,t_i) \geq \omega\big)\\ \wedge\ \big(pre(p,t) = (\omega, \mathtt{inhib}) \Rightarrow s'.M(p) - \sum_{t_i \in Pr(t,fired)} pre(p,t_i) < \omega\big)\end{array}}$$

   Given a $p \in P$ and an $\omega \in \mathbb{N}^*$, let us show

$$\boxed{\begin{array}{l}\big((pre(p,t) = (\omega, \mathtt{basic}) \vee pre(p,t) = (\omega, \mathtt{test})) \Rightarrow s'.M(p) - \sum_{t_i \in Pr(t,fired)} pre(p,t_i) \geq \omega\big)\\ \wedge\ \big(pre(p,t) = (\omega, \mathtt{inhib}) \Rightarrow s'.M(p) - \sum_{t_i \in Pr(t,fired)} pre(p,t_i) < \omega\big)\end{array}}$$

   By construction, there exists an $id_p \in Comps(\Delta)$ s.t. $\gamma(p) = id_p$. By construction and by definition of id_p, there exist gm_p, ipm_p, opm_p s.t. $\mathtt{comp}(id_p, ''place'', gm_p, ipm_p, opm_p) \in d.cs$.

   There are three different cases:

   (a) Assuming that $pre(p,t) = (\omega, \mathtt{test})$, let us show $\boxed{s'.M(p) - \sum_{t_i \in Pr(t,fired)} pre(p,t_i) \geq \omega.}$

   Then, assuming that the priority relation is well-defined, there exists no transition t_i connected by a `basic` arc to p that verified $t_i \succ t$. This is because t is connected to p by a `test`

arc; thus, t is not in conflict with the other output transitions of p; thus, there is no relation of priority between t and the output of p.
Then, we can deduce that $\sum_{t_i \in Pr(t,fired)} pre(p, t_i) = 0$.
Then, the new goal is $s'.M(p) \geq \omega$.
Knowing that $t \in Firable(s')$, thus, $t \in Sens(s'.M)$, thus, we have $s'.M(p) \geq \omega$.

(b) Assuming that $pre(p,t) = (\omega, \texttt{inhib})$, let us show $\boxed{s'.M(p) - \sum_{t_i \in Pr(t,fired)} pre(p, t_i) < \omega.}$

Use the same strategy as above.

(c) Assuming that $pre(p,t) = (\omega, \texttt{basic})$, let us show $\boxed{s'.M(p) - \sum_{t_i \in Pr(t,fired)} pre(p, t_i) \geq \omega.}$

Then, there are two cases:

i. **CASE** For all pair of transitions in $output_c(p)$, all conflicts are solved by mutual exclusion.
Then, assuming that the priority relation is well-defined, it must not be defined over the set $output_c(t)$, and we know that $t \in output_c(p)$ since $pre(p,t) = (\omega, \texttt{basic})$.
Then, there exists no transition t_i connected to p by a `basic` arc that verifies $t_i \succ t$.
Then, we can deduce $\sum_{t_i \in Pr(t,fired)} pre(p, t_i) = 0$.
Then, the new goal is $s'.M(p) \geq \omega$.
We know $t \in Firable(s')$, thus, $t \in Sens(s'.M)$, thus, $s'.M(p) \geq \omega$.

ii. **CASE** The priority relation is a strict total order over the set $output_c(p)$.
By construction, there exists $id_t \in Comps(\Delta)$ s.t. $\gamma(t) = id_t$. By construction and 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 construction, there exist $j \in [0, |input(t)| - 1]$, $k \in [0, |output(t)| - 1]$, and $id_{kj} \in Sigs(\Delta)$ s.t. $<\texttt{priority\_authorizations(j)} \Rightarrow \texttt{id}_{\texttt{kj}}> \in ipm_t$ and $<\texttt{priority\_authorizations(k)} \Rightarrow \texttt{id}_{\texttt{kj}}> \in opm_p$. Let us take such an j, k and id_{kj}.
From $\prod_{i=0}^{\Delta(id_t)(\text{"}ian\text{"})-1} \sigma'(id_t)(\text{"}pauths\text{"})[i] = \texttt{true}$, we can deduce that for all $i \in [0, \Delta(id_t)(\text{"}ian\text{"}) - 1]$, $\sigma'(id_t)(\text{"}pauths\text{"})[i] = \texttt{true}$.
By construction, $<\texttt{input\_arcs\_number} \Rightarrow |input(t)|> \in gm_t$, and by property of the elaboration relation, we have $\Delta(id_t)(\text{"}ian\text{"}) = |input(t)|$. Then, from $j \in [0, |input(t)| - 1]$, we can deduce $j \in [0, \Delta(id_t)(\text{"}ian\text{"}) - 1]$. And, from $\forall i \in [0, \Delta(id_t)(\text{"}ian\text{"}) - 1]$, $\sigma'(id_t)(\text{"}pauths\text{"})[i] = \texttt{true}$, we can deduce $\sigma'(id_t)(\text{"}pauths\text{"})[j] = \texttt{true}$.
By property of the stabilize relation, $\texttt{comp}(id_p, \text{"}place\text{"}, gm_p, ipm_p, opm_p) \in d.cs$ and $\texttt{comp}(id_t, \text{"}transition\text{"}, gm_t, ipm_t, opm_t) \in d.cs$:

$$\sigma'(id_p)(\text{"}pauths\text{"})[k] = \sigma'(id_{kj})\sigma'(id_t)(\text{"}pauths\text{"})[j] = \texttt{true} \tag{A.187}$$

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

$$\sigma'(id_p)(\text{"}pauths\text{"})[k] = (\sigma'(id_p)(\text{"}sm\text{"}) \geq \texttt{vsots} + \sigma'(id_p)(\text{"}oaw\text{"})[k]) \tag{A.188}$$

Let us define the `vsots` term as follows:

$$\texttt{vsots} = \sum_{i=0}^{k-1} \begin{cases} \sigma'(id_p)(''oaw'')[i] \texttt{ if } \sigma'(id_p)(''otf'')[i]. \\ \qquad\qquad\qquad\qquad \sigma'(id_p)(''oat'')[i] = \texttt{basic} \\ 0 \; otherwise \end{cases} \tag{A.189}$$

From (A.187) and (A.188), we can deduce that $\sigma'(id_p)(''sm'') \geq \texttt{vsots} + \sigma'(id_p)(''oaw'')[k]$. Then, there are three points to prove:

A. $\boxed{s'.M(p) = \sigma'(id_p)(''sm'')}$

B. $\boxed{\omega = \sigma'(id_p)(''oaw'')[k]}$

C. $\boxed{\sum_{t_i \in Pr(t,fired)} pre(p, t_i) = \texttt{vsots}}$

See 1 for the remainder of the proof.

□

Lemma 37 (Falling Edge Equal Not Fired)**.** *then* $\forall t, id_t \; s.t. \; \gamma(t) = id_t, \; t \notin Fired(s') \Leftrightarrow \sigma'_t(''fired'') =$ `false`.

Proof. Proving the above lemma is trivial by appealing to Lemma **??** and by reasoning on contra-positives. □