A Symbolic Characterisation of Open Bisimulation for the Spi Calculus

Sébastien Briais

École Polytechnique Fédérale de Lausanne, Switzerland
sebastien.briais@epfl.ch

Abstract. Open hedged bisimulation was proposed as a generalisation to the spi calculus of the pi calculus'open bisimulation. In this paper, we extend previous work on open hedged bisimulation. We show that open hedged bisimilarity is closed under *respectful substitutions* and give a symbolic characterisation of open hedged bisimulation. The latter result is an important step towards mechanisation of open hedged bisimilarity.

Introduction

The spi calculus was designed to formalise and study cryptographic protocols. It is an extension of the pi calculus that permits the transmission of *cryptographic messages* [2, 10].

Open bisimulation, introduced by Sangiorgi [16], is an attractive notion of equivalence for the pi calculus [13–15] for the following reasons. Firstly, it constitutes a reasonably full congruence, i.e., it is preserved by all operators including input prefix. Secondly, it allows for simple axiomatizations for finite terms. Thirdly, it is rather straightforward to build tools that symbolically check for open bisimilarity ([17] and [6] for example).

In [8] and [7] we defined open hedged bisimulation, which generalises open bisimulation to the spi calculus. We showed that it is a conservative extension of Sangiorgi's open bisimulation (under some conditions) and we proved that it is a sound approximation of late hedged bisimilarity (see [5] for an overview of bisimulation for the spi calculus).

In this paper, we extend the study of open hedged bisimulation and give two important results. We show that open hedged bisimilarity is preserved under *respectful substitutions* and we provide a *symbolic characterisation* of open hedged bisimulation. This symbolic characterisation is an important step towards the mechanisation of open hedged bisimilarity (for finite spi calculus processes). We also generalise our definitions to a spi calculus with a rich and realistic message language that includes *shared-key cryptography*, *public key cryptography*, *pairing* and *hashing*.

1 The Spi Calculus

Syntax We assume readers to have a basic knowledge of the notions and terminology of the pi calculus. The spi calculus is an extension of the pi calculus

that permits the transmission of cryptographic (compound) messages. We follow these [5, 4, 8, 7] presentations of the spi calculus. We also assume that the underlying cryptographic system is perfect as usually done [2, 3, 5].

We assume to have a countably infinite set of names $\boldsymbol{N}$. Names are used for channels, variables and clear text messages. Processes P are either the inactive process, inputs, outputs, guard prefixes, parallel compositions, restrictions, choices or replications. Formulae —or guards— ϕ include matching, conjunction and $[E\!:\!\boldsymbol{N}]$, which tests whether an expression E evaluates to a name. Indeed, contrary to [11], we assume as in [2, 3] that communication channels must be names; this allows the attacker to verify that a message is a name by attempting to transmit on it. Messages M are constructed from names by using primitive constructors for symmetric (shared-key) $\mathsf{Enc}^{\mathrm{s}}_K M$ and asymmetric (public/private key) cryptography $\mathsf{Enc}^{\mathrm{a}}_K M$ (where M is the content of the *cyphertext* and K is the key which may be an arbitrary message), pairing $(M\,.\,N)$, hashing $\mathsf{H}(M)$ or public/private key $\mathsf{pub}(M)$ and $\mathsf{priv}(M)$ (we denote by op an operator in $\{\mathsf{H}, \mathsf{pub}, \mathsf{priv}\}$). Expressions E extend messages with deconstructors for shared key decryption $\mathsf{Dec}^{\mathrm{s}}_F E$, public/private key decryption $\mathsf{Dec}^{\mathrm{a}}_F E$ and pair splitting $\pi_1\,(E)\,, \pi_2\,(E)$.

$$
\begin{array}{lll}
a, b, c, \ldots, k, l, m, n, \ldots, x, y, z, \ldots & & \text{names } \boldsymbol{N} \\
M, N := a \mid \mathsf{Enc}^{\mathrm{s}}_N M \mid \mathsf{Enc}^{\mathrm{a}}_N M \mid (M\,.\,N) & & \text{messages } \boldsymbol{M} \\
\quad \mid \mathsf{H}(M) \mid \mathsf{pub}(M) \mid \mathsf{priv}(M) & & \\
E, F := a \mid \mathsf{Enc}^{\mathrm{s}}_F E \mid \mathsf{Enc}^{\mathrm{a}}_F E \mid (E\,.\,F) & & \text{expressions } \boldsymbol{E} \\
\quad \mid \mathsf{H}(E) \mid \mathsf{pub}(E) \mid \mathsf{priv}(E) & & \\
\quad \mid \mathsf{Dec}^{\mathrm{s}}_F E \mid \mathsf{Dec}^{\mathrm{a}}_F E \mid \pi_1\,(E) \mid \pi_2\,(E) & & \\
\phi, \psi := tt \mid [E{=}F] \mid \phi \wedge \psi \mid [E\!:\!\boldsymbol{N}] & & \text{guards } \boldsymbol{F} \\
P, Q := \mathbf{0} \mid E(x).P \mid \overline{E}\langle F\rangle.P \mid \phi P & & \text{processes } \boldsymbol{P} \\
\quad \mid P + Q \mid P \,|\, Q \mid (\nu z)\, P \mid\, !\, P & &
\end{array}
$$

Free and bound names are defined as usual: x is a binding occurrence in $E(x).P$ and $(\nu x)\, P$. α-equivalence $\equiv_\alpha$ relates any two processes that only differ w.r.t. the clash-free renaming of their bound names. We write $\mathrm{fn}(P)$ the free names of P and $\mathrm{bn}(P)$ its bound names. We write $\mathrm{n}(M)$, $\mathrm{n}(E)$ and $\mathrm{n}(\phi)$ the set of all names of M, E and ϕ and extend this notation to sets of messages, expressions and formulae.

To treat asymmetric cryptography, we need a way to express the inverse key of a message; if $M = \mathsf{pub}(N)$ (resp. $\mathsf{priv}(N)$) we define $\mathsf{inv}(M)$ to be $\mathsf{priv}(N)$ (resp. $\mathsf{pub}(N)$) and otherwise we let $\mathsf{inv}(M) := \bot$. The language of messages chosen here is slightly more realistic than the one introduced in [4] particularly with respect to the treatment of asymmetric cryptography.

Substitutions σ are total functions from names x to messages M whose *support* $\mathrm{supp}(\sigma) = \{x \mid \sigma(x) \neq x\}$ is finite. The co-support of σ is $\mathrm{cosupp}(\sigma) = \{\sigma(x) \mid x \in \mathrm{supp}(\sigma)\}$. Substitutions are applied to processes, expressions, messages, formulae and actions (see below) in the common way, assuming the usual notion of capture avoiding substitutions. They are written in the postfix notation, e.g. $M\sigma$. We use the notation $\left[{}^{M_1}\!/_{x_1}, \ldots, {}^{M_n}\!/_{x_n}\right]$ when we enumerate a

substitution. The names $\mathrm{n}(\sigma)$ of a substitution σ are the names of its co-support and its support.

Labelled (late) Semantics Since arbitrary expressions may appear in input or output positions, we make sure that these expressions evaluate to a message or a channel name before performing the transition. The *concrete evaluation* $\mathbf{e}_{\mathrm{c}}(E)$ of an expression allows to check this, it is either a message M or $\bot$:

$$
\begin{array}{rcll}
\mathbf{e}_{\mathrm{c}}(a) & := & a & \text{if } a \in \boldsymbol{N} \\
\mathbf{e}_{\mathrm{c}}(\mathsf{Enc}^{\mathrm{s}}_F E) & := & \mathsf{Enc}^{\mathrm{s}}_N M & \text{if } \mathbf{e}_{\mathrm{c}}(E) = M \in \boldsymbol{M} \text{ and } \mathbf{e}_{\mathrm{c}}(F) = N \in \boldsymbol{M} \\
 & & \bot & \text{otherwise} \\
\mathbf{e}_{\mathrm{c}}(\mathsf{Enc}^{\mathrm{a}}_F E) & := & \mathsf{Enc}^{\mathrm{a}}_N M & \text{if } \mathbf{e}_{\mathrm{c}}(E) = M \in \boldsymbol{M} \text{ and } \mathbf{e}_{\mathrm{c}}(F) = N \in \boldsymbol{M} \\
 & & \bot & \text{otherwise} \\
\mathbf{e}_{\mathrm{c}}((E\,.\,F)) & := & (M\,.\,N) & \text{if } \mathbf{e}_{\mathrm{c}}(E) = M \in \boldsymbol{M} \text{ and } \mathbf{e}_{\mathrm{c}}(F) = N \in \boldsymbol{M} \\
 & & \bot & \text{otherwise} \\
\mathbf{e}_{\mathrm{c}}(\mathsf{op}(E)) & := & \mathsf{op}(M) & \text{if } \mathbf{e}_{\mathrm{c}}(E) = M \in \boldsymbol{M} \\
 & & \bot & \text{otherwise} \\
\mathbf{e}_{\mathrm{c}}(\mathsf{Dec}^{\mathrm{s}}_F E) & := & M & \text{if } \mathbf{e}_{\mathrm{c}}(E) = \mathsf{Enc}^{\mathrm{s}}_N M \in \boldsymbol{M} \text{ and } \mathbf{e}_{\mathrm{c}}(F) = N \in \boldsymbol{M} \\
 & & \bot & \text{otherwise} \\
\mathbf{e}_{\mathrm{c}}(\mathsf{Dec}^{\mathrm{a}}_F E) & := & M & \text{if } \mathbf{e}_{\mathrm{c}}(E) = \mathsf{Enc}^{\mathrm{s}}_N M \in \boldsymbol{M} \text{ and } \mathbf{e}_{\mathrm{c}}(F) = \mathsf{inv}(N) \in \boldsymbol{M} \\
 & & \bot & \text{otherwise} \\
\mathbf{e}_{\mathrm{c}}(\pi_1\,(E)) & := & M & \text{if } \mathbf{e}_{\mathrm{c}}(E) = (M\,.\,N) \in \boldsymbol{M} \\
 & & \bot & \text{otherwise} \\
\mathbf{e}_{\mathrm{c}}(\pi_2\,(E)) & := & N & \text{if } \mathbf{e}_{\mathrm{c}}(E) = (M\,.\,N) \in \boldsymbol{M} \\
 & & \bot & \text{otherwise}
\end{array}
$$

For guards, we have a predicate $\mathbf{e}(\phi)$ defined in the obvious way for true (tt) and conjunction. We define $\mathbf{e}([E{=}F])$ to be true iff $\mathbf{e}_{\mathrm{c}}(E) = \mathbf{e}_{\mathrm{c}}(F) = M \in \boldsymbol{M}$ and $\mathbf{e}([E{:}\boldsymbol{N}])$ to be true iff $\mathbf{e}_{\mathrm{c}}(E) = a \in \boldsymbol{N}$. It is convenient to define a shortcut for the guard $[E{=}E]$ —written $[E{:}\boldsymbol{M}]$— whose evaluation is true iff the concrete evaluation of E is a message.

To collect the concrete evaluation of expressions E tested to be names in a formula ϕ, we define the set $\mathbf{nc}(\phi)$ as $\mathbf{nc}(tt) = \mathbf{nc}([E{=}F]) = \emptyset$, $\mathbf{nc}(\phi \wedge \psi) = \mathbf{nc}(\phi) \cup \mathbf{nc}(\psi)$ and $\mathbf{nc}([E{:}\boldsymbol{N}]) = \{\mathbf{e}_{\mathrm{c}}(E)\}$. Obviously, if $\mathbf{e}(\phi)$ then $\mathbf{nc}(\phi) \subseteq \boldsymbol{N}$.

The set of actions $\mu \in \boldsymbol{A}$ is defined by $\mu := \tau \mid a(x) \mid (\nu \tilde{z})\,\overline{a}\,M$ where $a \in \boldsymbol{N}$, $M \in \boldsymbol{M}$ and $\tilde{z}$ is a tuple of pairwise distinct names. By abuse of notation, we write $\overline{a}\,M$ when $\tilde{z}$ is empty. We let $\mathrm{bn}(a(x)) := \{x\}$ and $\mathrm{bn}((\nu \tilde{z})\,\overline{a}\,M) = \{\tilde{z}\}$. We also define $\mathrm{ch}(a(x)) := a$ and $\mathrm{ch}((\nu \tilde{z})\,\overline{a}\,M) := a$.

The labelled transition $P \xrightarrow[S]{\mu} Q$ is defined by the derivation rules given in Table 1 (extended by the symmetric variants of NC-Close-l, NC-Par-l and NC-Sum-l). The set S collects the names used to apply rules NC-Input, NC-Output and NC-Guard. The set S puts no constraints on the transition relation. Indeed, the labelled semantics $P \xrightarrow{\mu} Q$ of the spi calculus is equivalent to the existence of an S such that $P \xrightarrow[S]{\mu} Q$. Note that as usual the bound names of μ are binding occurrences in Q.

$$\text{NC-Input}\ \frac{\mathbf{e}_{\mathrm{c}}(E) = a \in \boldsymbol{N}}{E(x).P \xrightarrow[\{a\}]{a(x)} P} \qquad \text{NC-Output}\ \frac{\mathbf{e}_{\mathrm{c}}(E) = a \in \boldsymbol{N} \qquad \mathbf{e}_{\mathrm{c}}(F) = M \in \boldsymbol{M}}{\overline{E}\langle F\rangle.P \xrightarrow[\{a\}]{\overline{a}\,M} P}$$

$$\text{NC-Close-L}\ \frac{P \xrightarrow[S]{a(x)} P' \qquad Q \xrightarrow[S']{(\nu\tilde{z})\,\overline{a}\,M} Q'}{P \mid Q \xrightarrow[S\cup S']{\tau} (\nu\tilde{z})\,(P'\{^{M}/_{x}\} \mid Q')}\ \{\tilde{z}\} \cap \mathrm{fn}(P) = \emptyset$$

$$\text{NC-Open}\ \frac{P \xrightarrow[S]{(\nu\tilde{z})\,\overline{a}\,M} P'}{(\nu z')\,P \xrightarrow[S\setminus\{z'\}]{(\nu z'\tilde{z})\,\overline{a}\,M} P'}\ z' \in \mathrm{n}(M) \setminus \{a, \tilde{z}\}$$

$$\text{NC-Res}\ \frac{P \xrightarrow[S]{\mu} P'}{(\nu z)\,P \xrightarrow[S\setminus\{z\}]{\mu} (\nu z)\,P'}\ z \notin \mathrm{n}(\mu) \qquad \text{NC-Guard}\ \frac{P \xrightarrow[S]{\mu} P' \qquad \mathbf{e}(\phi)}{\phi P \xrightarrow[S\cup\mathbf{nc}(\phi)]{\mu} P'}$$

$$\text{NC-Par-L}\ \frac{P \xrightarrow[S]{\mu} P'}{P \mid Q \xrightarrow[S]{\mu} P' \mid Q}\ \mathrm{bn}(\mu) \cap \mathrm{fn}(Q) = \emptyset \qquad \text{NC-Sum-L}\ \frac{P \xrightarrow[S]{\mu} P'}{P + Q \xrightarrow[S]{\mu} P'}$$

$$\text{NC-Rep-act}\ \frac{P \xrightarrow[S]{\mu} P'}{!\,P \xrightarrow[S]{\mu} P' \mid !\,P}\ \mathrm{bn}(\mu) \cap \mathrm{fn}(P) = \emptyset$$

$$\text{NC-Rep-close}\ \frac{P \xrightarrow[S]{a(x)} P' \qquad P \xrightarrow[S']{(\nu\tilde{z})\,\overline{a}\,M} P''}{!\,P \xrightarrow[S\cup S']{\tau} (\nu\tilde{z})\,(P'\{^{M}/_{x}\} \mid P'') \mid !\,P}\ \{\tilde{z}\} \cap \mathrm{fn}(P) = \emptyset$$

$$\text{NC-Alpha}\ \frac{P \equiv_{\alpha} P' \qquad P' \xrightarrow[S]{\mu} P''}{P \xrightarrow[S]{\mu} P''}$$

Table 1. The late semantics of the spi calculus

The following lemma states that applying a substitution σ to a process does not diminish its capabilities for action if σ does not replace names in S by compound messages.

Lemma 1. *If* $P \xrightarrow[S]{\mu} Q$ *then* $P\sigma \xrightarrow[S\sigma]{\mu\sigma} Q\sigma$ *provided that* $\mathrm{n}(\mathrm{cosupp}(\sigma)) \cap \mathrm{bn}(\mu) = \emptyset$ *and* $\forall x \in S : x\sigma \in \boldsymbol{N}$.

Notations on pairs If $C \subseteq A \times B$, we define $\pi_1(C) := \{a \mid (a,b) \in C\}$, $\pi_2(C) := \{b \mid (a,b) \in C\}$ and $C^{-1} = \{(b,a) \mid (a,b) \in C\}$.

If σ and ρ are substitutions, we define $C(\sigma,\rho) := \{(a\sigma, b\rho) \mid (a,b) \in C\}$.

2 Open Hedged Bisimulation

The classical notion of bisimulation used in the pi calculus is not adequate for the spi calculus. The reason is that requiring an exact match between observable actions is too strong in a cryptographic context where, for example, $\mathsf{Enc}^{\mathrm{s}}_k M$ and $\mathsf{Enc}^{\mathrm{s}}_k N$ need to be identified as long as k is unknown to the observer (attacker). To be able to have a cryptographic aware equivalence between actions, bisimulations are extended with structures (e.g. hedges, frame-theory pairs, S-environments) that explicitly keep track of the identities between messages. These identities can be seen as the attacker's knowledge about processes.

Hedges as Attacker Knowledge Abadi and Gordon proposed in [1] an "environment-sensitive" notion of bisimulation called *framed bisimulation*. *Hedged bisimulation* is a variant of framed bisimulation that has been shown in [5] to coincide with barbed equivalence (contrary to framed bisimulation). In hedged bisimulation, the environment consists of a *hedge* which is a finite set of pairs of messages that are supposed to be indistinguishable to the attacker.

We write $\boldsymbol{H}$ the set of hedges (i.e. the finite sets of pairs of messages). The *synthesis* $\mathcal{S}(h)$ of a hedge h is the (infinite) set of message pairs that can be constructed from the knowledge represented by h.

Definition 1 (synthesis). *If* h *is hedge, the* synthesis $\mathcal{S}(h)$ *of* h *is the smallest set satisfying:*

1. *if* $(M,N) \in h$ *then* $(M,N) \in \mathcal{S}(h)$
2. *if* $(M_1,N_1) \in \mathcal{S}(h)$ *and* $(M_2,N_2) \in \mathcal{S}(h)$ *then* $((M_1 \,.\, M_2),(N_1 \,.\, N_2)) \in \mathcal{S}(h)$
3. *if* $(M_1,N_1) \in \mathcal{S}(h)$ *and* $(M_2,N_2) \in \mathcal{S}(h)$ *then* $(\mathsf{Enc}^{\mathrm{s}}_{M_2} M_1, \mathsf{Enc}^{\mathrm{s}}_{N_2} N_1) \in \mathcal{S}(h)$
4. *if* $(M_1,N_1) \in \mathcal{S}(h)$ *and* $(M_2,N_2) \in \mathcal{S}(h)$ *then* $(\mathsf{Enc}^{\mathrm{a}}_{M_2} M_1, \mathsf{Enc}^{\mathrm{a}}_{N_2} N_1) \in \mathcal{S}(h)$
5. *if* $(M,N) \in \mathcal{S}(h)$ *then* $(\mathsf{op}(M), \mathsf{op}(N)) \in \mathcal{S}(h)$

The *analysis* $\mathcal{A}(h)$ of h is the set of message pairs obtained by deconstructing the knowledge represented by h.

Definition 2 (analysis). *If h is a hedge,* $\mathrm{analz}(h)$ *is the smallest hedge satisfying*

1. *if* $(M,N) \in h$ *then* $(M,N) \in \mathrm{analz}(h)$
2. *if* $((M_1 \,.\, M_2),(N_1 \,.\, N_2)) \in \mathrm{analz}(h)$ *then* $(M_1,N_1) \in \mathrm{analz}(h)$
3. *if* $((M_1 \,.\, M_2),(N_1 \,.\, N_2)) \in \mathrm{analz}(h)$ *then* $(M_2,N_2) \in \mathrm{analz}(h)$
4. *if* $(\mathsf{Enc}^{\mathrm{s}}_{M_2} M_1, \mathsf{Enc}^{\mathrm{s}}_{N_2} N_1) \in \mathrm{analz}(h)$ *and* $(M_2,N_2) \in \mathcal{S}(h)$ *then* $(M_1,N_1) \in \mathrm{analz}(h)$
5. *if* $(\mathsf{Enc}^{\mathrm{a}}_{M_2} M_1, \mathsf{Enc}^{\mathrm{a}}_{N_2} N_1) \in \mathrm{analz}(h)$ *and* $(\mathsf{inv}(M_2), \mathsf{inv}(N_2)) \in \mathcal{S}(h)$ *then* $(M_1,N_1) \in \mathrm{analz}(h)$

The analysis $\mathcal{A}(h)$ *of h is the smallest hedge such that* $h \subseteq \mathcal{A}(h)$ *and* $\mathrm{analz}(\mathcal{A}(h)) \subseteq \mathcal{A}(h)$.

Theorem 1. *$\mathcal{A}(h)$ is well-defined.*

Given a hedge h, an interesting derived hedge is its irreducible part $\mathcal{I}(h)$ which is the smallest hedge whose synthesis $\mathcal{S}(\mathcal{I}(h))$ is equal to the synthesis $\mathcal{S}(\mathcal{A}(h))$.

Definition 3 (irreducible part). *If h is a hedge, we define* $\mathit{reduce}(h) := \{(M,N) \in h \mid h \nvdash (M,N)\}$ *where* $h \vdash (M,N)$ *is the smallest predicate satisfying*

1. *if* $(M,N) \in \mathcal{S}(h)$ *then* $h \vdash (\mathsf{op}(M), \mathsf{op}(N))$
2. *if* $(M_1,N_1) \in \mathcal{S}(h)$ *and* $(M_2,N_2) \in \mathcal{S}(h)$ *then* $h \vdash ((M_1 \,.\, M_2),(N_1 \,.\, N_2))$
3. *if* $(M_1,N_1) \in \mathcal{S}(h)$ *and* $(M_2,N_2) \in \mathcal{S}(h)$ *then* $h \vdash (\mathsf{Enc}^{\mathrm{s}}_{M_2} M_1, \mathsf{Enc}^{\mathrm{s}}_{N_2} N_1)$
4. *if* $(M_1,N_1) \in \mathcal{S}(h)$ *and* $(M_2,N_2) \in \mathcal{S}(h)$ *then* $h \vdash (\mathsf{Enc}^{\mathrm{a}}_{M_2} M_1, \mathsf{Enc}^{\mathrm{a}}_{N_2} N_1)$

We define the irreducible part of h to be $\mathcal{I}(h) := \mathit{reduce}(\mathcal{A}(h))$.
A hedge is irreducible *iff* $\mathcal{I}(h) = h$.

Hedges are used to relate indistinguishable messages. However, it can happen that the attacker finds a contradiction in its knowledge. For example, if both (M,N_1) and (M,N_2) are in h and $N_1 \neq N_2$. The notion of *consistency* guarantees the absence of such contradictions.

Definition 4 (consistency). *A hedge h is* left consistent *iff*

1. *if* $(M,N) \in h$ *and* $M \in \boldsymbol{N}$ *then* $N \in \boldsymbol{N}$
2. *if* $(M,N) \in h$ *and* $(M,N') \in h$ *then* $N = N'$
3. *if* $(M,N) \in h$ *and* $(\mathsf{inv}(M),N') \in h$ *then* $N' = \mathsf{inv}(N)$
4. *if* $(\mathsf{op}(M'),N) \in h$ *then* $(M',N') \notin \mathcal{S}(h)$ *for any* N
5. $((M_1 \,.\, M_2),N) \notin h$ *for any* M_1, M_2 *and* N
6. *if* $(\mathsf{Enc}^{\mathrm{s}}_{M_2} M_1, N) \in h$ *then* $(M_2,N_2) \notin \mathcal{S}(h)$ *for any* N_2
7. *if* $(\mathsf{Enc}^{\mathrm{a}}_{M_2} M_1, N) \in h$ *then* $(M_1,N_1) \notin \mathcal{S}(h)$ *or* $(M_2,N_2) \notin \mathcal{S}(h)$ *for any* N_1 *and* N_2
8. *if* $(\mathsf{Enc}^{\mathrm{a}}_{M_2} M_1, N) \in h$ *and* $(\mathsf{inv}(M_2), N_2') \in \mathcal{S}(h)$ *then* $N_2' = \mathsf{inv}(N_2)$, $N = \mathsf{Enc}^{\mathrm{a}}_{N_2} N_1$ *and* $(M_1,N_1) \in \mathcal{S}(h)$

It is consistent *if both h and h^{-1} are left consistent.*

Consistent hedges are irreducibles.

Late hedged bisimulation A hedged relation $\mathcal{R}$ is a subset of $\boldsymbol{H} \times \boldsymbol{P} \times \boldsymbol{P}$ such that for $(h, P, Q) \in \mathcal{R}$ we have $\mathrm{fn}(P) \subseteq \mathrm{n}(\pi_1(h))$ and $\mathrm{fn}(Q) \subseteq \mathrm{n}(\pi_2(h))$. It is consistent if whenever $(h, P, Q) \in \mathcal{R}$, h is consistent. It is symmetric if whenever $(h, P, Q) \in \mathcal{R}$ we have $(h^{-1}, Q, P) \in \mathcal{R}$.

Definition 5 (late hedged bisimulation). *A symmetric consistent hedged relation $\mathcal{R}$ is a* late hedged bisimulation *if for all $(h, P, Q) \in \mathcal{R}$, if $P \xrightarrow{\mu_1} P'$ with, if $\mu_1 \neq \tau$, $\mathrm{bn}(\mu_1) \cap \mathrm{n}(\pi_1(h)) = \emptyset$ and $\mathrm{ch}(\mu_1) \in \pi_1(h)$ then there exists μ_2 and Q' such that $Q \xrightarrow{\mu_2} Q'$ with $\mathrm{bn}(\mu_2) \cap \mathrm{n}(\pi_2(h)) = \emptyset$ and*

1. *if $\mu_1 = \tau$ then $\mu_2 = \tau$ and $(h, P', Q') \in \mathcal{R}$*
2. *if $\mu_1 = a_1(x_1)$ then $\mu_2 = a_2(x_2)$ where $(a_1, a_2) \in h$ and for all $B \subseteq \boldsymbol{N} \times \boldsymbol{N}$ and $(M_1, M_2) \in \boldsymbol{M} \times \boldsymbol{M}$ such that*
   - *B is a consistent hedge*
   - *$\pi_1(B) \setminus \mathrm{n}(M_1) = \emptyset$*
   - *$\pi_1(B) \cap \mathrm{n}(\pi_1(h)) = \pi_2(B) \cap \mathrm{n}(\pi_2(h)) = \emptyset$*
   - *$(M_1, M_2) \in \mathcal{S}(h \cup B)$*

   we have $(h \cup B, P'\{^{M_1}/_{x_1}\}, Q'\{^{M_2}/_{x_2}\}) \in \mathcal{R}$
3. *if $\mu_1 = (\nu \tilde{c})\,\overline{a_1}\,M_1$ then $\mu_2 = (\nu d)\,\overline{a_2}\,M_2$ where $(a_1, a_2) \in h$ and $(\mathcal{I}(h \cup \{(M_1, M_2)\}), P', Q') \in \mathcal{R}$*

In the above definition, the condition $\mathrm{ch}(\mu_1) \in \pi_1(h)$ says that the transition is observable by the attacker. The second clause requires that the bisimulation game can be continued with any pair the attacker can synthesise from its knowledge possibly by adding fresh names (B). In the third clause, the emitted messages are added to the current knowledge of the attacker who immediately computes the irreducible part of h. The hedge h is required to be consistent to ensure that the emitted messages do not allow to distinguish the two processes.

Let $h \in \boldsymbol{H}$ and $P, Q \in \boldsymbol{P}$. We say that P and Q are *late hedged bisimilar under h* —written $P \sim^{h}_{\mathrm{LH}} Q$— if there exists a late hedged bisimulation $\mathcal{R}$ such that $(h, P, Q) \in \mathcal{R}$.

Environments for Open Bisimulation The idea of open bisimulation is to defer the substitution of input names until they are really needed in the bisimulation game.

For defining open bisimulation in the spi calculus [8, 7], we have to record on each input, during the bisimulation game, every messages the attacker can substitute to the input variable given its current knowledge. This information is represented by S-environments which consist of a hedge h representing the attacker's current knowledge, v which are names used as input names so far and $\prec$ which allows to recover the hedge the attacker had when a given input name was input. Moreover, since we require that communications can only occur on channel names, S-environments also need to remember which input names can be substituted by names only, this is stored in γ_l, γ_r.

Definition 6. *A* S-environment *is a quadruple $\mathsf{se} = (h, v, \prec, (\gamma_l, \gamma_r))$ where $h \in \boldsymbol{H}$, $v \subseteq \boldsymbol{N} \times \boldsymbol{N}$ is a consistent hedge, $\prec \subseteq h \times v$, $\gamma_l \subseteq \pi_1(v)$ and $\gamma_r \subseteq \pi_2(v)$. The set of all S-environments is written $\mathcal{S}_{\mathrm{H}}$.*

The hedge available *to* $(x, y) \in v$ *according to* $\prec$ *is defined by* $\mathsf{se}|_{(x,y)} := \{(M, N) \in h \mid (M, N) \prec (x, y)\}$.

The concrete hedge *of* se *is* $\mathfrak{H}(\mathsf{se}) := h \cup v$. *The inverse of* se *is* $\mathsf{se}^{-1} := (h^{-1}, v^{-1}, \prec^{-1}, (\gamma_r, \gamma_l))$ *where* $(N, M) \prec^{-1} (y, x)$ *iff* $(M, N) \prec (x, y)$.

The intuition behind $\prec$ is that if $(M, N) \prec (x, y)$, the attacker knew about (M, N) whenever (x, y) was used for input in the bisimulation game. In that case, we need to require that $x \notin \mathrm{n}(M)$ and $y \notin \mathrm{n}(N)$ to avoid circularities, which is included in the following definition.

Definition 7 (well-formed S-environments).
A S-environment $\mathsf{se} = (h, v, \prec, (\gamma_l, \gamma_r))$ *is* well-formed *if* $\pi_1(v) \cap \pi_1(h) = \pi_2(v) \cap \pi_2(h) = \emptyset$ *and for all* $(M, N) \in h$ *and* $(x, y) \in v$ *with* $(M, N) \prec (x, y)$ *we have* $x \notin \mathrm{n}(M)$ *and* $y \notin \mathrm{n}(N)$.

There are three relevant ways to add information to a S-environment se. We can add a pair of indistinguishable messages (M, N) to the hedge h (on process outputs) —note that whenever (M, N) was produced by the attacker, we don't put it in h since it adds no information to the attacker's knowledge. We can add a fresh pair (x, y) of input variables to v and update $\prec$ so that the hedge $\mathsf{se}|_{(x,y)}$ corresponds to the current hedge h (on process inputs). And finally, we can add new constraints in γ_l and γ_r to reflect that some input names were used as channels (on process transitions).

Definition 8. *Let* $\mathsf{se} = (h, v, \prec, (\gamma_l, \gamma_r))$ *be a S-environment.*

If $(M, N) \in \boldsymbol{M} \times \boldsymbol{M}$, *we define* $\mathsf{se} \oplus_{\mathrm{o}} (M, N) := (h', v, \prec, (\gamma_l, \gamma_r))$ *where* $h' = h$ *if* $(M, N) \in v$ *and* $h' = h \cup \{(M, N)\}$ *otherwise.*

If $(x, y) \in \boldsymbol{N} \times \boldsymbol{N}$, *we define* $\mathsf{se} \oplus_{\mathrm{i}} (x, y) := (h, v \cup \{(x, y)\}, \prec', (\gamma_l, \gamma_r))$ *where* $\prec' := \prec \cup (h \times \{(x, y)\})$.

If $S_1, S_2 \subseteq \boldsymbol{N}$, *we define* $\mathsf{se} \oplus_{\mathrm{c}} (S_1, S_2) := (h, v, \prec, (\gamma_l', \gamma_r'))$ *where* $\gamma_l' := \gamma_l \cup (S_1 \cap \pi_1(v))$ *and* $\gamma_r' := \gamma_r \cup (S_2 \cap \pi_2(v))$.

By adding information to particular S-environments as shown above, hedges available to variables in v can be ordered in an increasing sequence of hedges. This property is captured by the following definition.

Definition 9 (growing S-environments).
A S-environment $\mathsf{se} = (h, v, \prec, (\gamma_l, \gamma_r))$ *is* growing *iff there exists an injective mapping* $\theta : [\![1, n]\!] \to v$ *(where* $n := \mathrm{card}(v)$*) such that if* $h_i := \mathsf{se}|_{\theta(i)}$ *then* $h_i \subseteq h_{i+1}$ *for* $1 \leq i < n$.

The part $(h, v, \prec)$ of a growing S-environment can be seen as a sequence of hedges $h_1 \cdot h_2 \cdot \ldots \cdot h_n$ and a sequence of pairs of input names $(x_1, y_1) \cdot (x_2, y_2) \cdot \ldots \cdot (x_{n-1}, y_{n-1})$ with $h_i \subseteq h_{i+1}$ for $1 \leq i < n$, $h = h_n$, $v = \{(x_1, y_1), \ldots, (x_{n-1}, y_{n-1})\}$ and $(M, N) \prec (x_i, y_i)$ iff $(M, N) \in h_i$ for $1 \leq i < n$.

Conceptually, a S-environment se is a concise representation of every pair of substitutions resulting from plays performed by the attacker in the bisimulation game. These pairs are said to *respect* se and are given by the following definition.

Definition 10 (respectful substitutions). *Given a pair (σ, ρ) of substitutions, $B \subseteq \boldsymbol{N} \times \boldsymbol{N}$ a consistent hedge and $\mathsf{se} = (h, v, \prec, (\gamma_l, \gamma_r))$ a S-environment,* (σ, ρ) respects se with B *—written $(\sigma, \rho) \triangleright_B \mathsf{se}$— if*

1. $\mathrm{supp}(\sigma) \subseteq \pi_1(v)$
2. $\mathrm{supp}(\rho) \subseteq \pi_2(v)$
3. $\forall (b_1, b_2) \in B : b_1 \in \mathrm{n}(\sigma(\pi_1(v))) \vee b_2 \in \mathrm{n}(\rho(\pi_2(v)))$
4. $\pi_1(B) \cap (\mathrm{n}(\pi_1(h)) \setminus \pi_1(v)) = \emptyset$
5. $\pi_2(B) \cap (\mathrm{n}(\pi_2(h)) \setminus \pi_2(v)) = \emptyset$
6. $\forall (x, y) \in v : (x\sigma, y\rho) \in \mathcal{S}(\mathcal{I}(\mathsf{se}|_{(x,y)}(\sigma, \rho) \cup B))$
7. $\forall x \in \gamma_l : x\sigma \in \boldsymbol{N}$
8. $\forall y \in \gamma_r : y\rho \in \boldsymbol{N}$

In this definition, substitutions affect only names in v (input names). Given $(x, y) \in v$, these names can be replaced by any pair of messages the attacker could have synthesised from $\mathsf{se}|_{(x,y)}$ possibly adding fresh names (B) and taking into account previous choices made by the attacker for other input names. Moreover, input names used as communication channels (mentioned in γ_l or γ_r) are prevented from being substituted by something else than a name.

In a given S-environment se, choices made by the attacker during the bisimulation game correspond to pairs (σ, ρ) of respectful substitutions. These choices lead to an updated S-environment $\mathsf{se}_B^{(\sigma,\rho)}$.

Definition 11 (S-environment updating). *Given (σ, ρ) a pair of substitutions, $B \subseteq \boldsymbol{N} \times \boldsymbol{N}$ a consistent hedge and $\mathsf{se} = (h, v, \prec, (\gamma_l, \gamma_r))$ a S-environment such that $(\sigma, \rho) \triangleright_B \mathsf{se}$, the* update *of se by (σ, ρ) is $\mathsf{se}_B^{(\sigma,\rho)} := (h(\sigma, \rho), B, \prec'$ $, (\gamma_l', \gamma_r'))$ where $\gamma_l' := \sigma(\gamma_l) \cap \pi_1(B)$, $\gamma_r' := \rho(\gamma_r) \cap \pi_2(B)$ and for $(M, N) \in h$ and $(x', y') \in B$, $(M\sigma, N\rho) \prec' (x', y')$ iff for all $(x, y) \in v$ such that $x' \in \mathrm{n}(x\sigma)$ or $y' \in \mathrm{n}(y\rho)$ we have $(M, N) \prec (x, y)$.*

Well-formedness and growth of S-environments are preserved by updates.

Lemma 2. *Let (σ, ρ) be a pair of substitutions, $B \subseteq \boldsymbol{N} \times \boldsymbol{N}$ a consistent hedge and $\mathsf{se} = (h, v, \prec, (\gamma_l, \gamma_r))$ a S-environment such that $(\sigma, \rho) \triangleright_B \mathsf{se}$.*

If se is well-formed then $\mathsf{se}_B^{(\sigma,\rho)}$ is well-formed.

If se is growing then $\mathsf{se}_B^{(\sigma,\rho)}$ is growing.

For well-formed and growing S-environments, respectfulness composes.

Lemma 3. *Let $\mathsf{se} = (h, v, \prec, (\gamma_l, \gamma_r))$ a S-environment. Assume that se is well-formed and growing.*

Let (σ_1, ρ_1) be a pair of substitutions and $B_1 \subseteq \boldsymbol{N} \times \boldsymbol{N}$ a consistent hedge such that $(\sigma_1, \rho_1) \triangleright_{B_1} \mathsf{se}$. We write $\mathsf{se}_1 := \mathsf{se}_{B_1}^{(\sigma_1,\rho_1)}$.

Let (σ_2, ρ_2) be a pair of substitutions and $B_2 \subseteq \boldsymbol{N} \times \boldsymbol{N}$ a consistent hedge such that $(\sigma_2, \rho_2) \triangleright_{B_2} \mathsf{se}_1$. We write $\mathsf{se}_2 := \mathsf{se}_1{}_{B_2}^{(\sigma_2,\rho_2)}$.

Then $(\sigma, \rho) \triangleright_{B_2} \mathsf{se}$ and $\mathsf{se}_{B_2}^{(\sigma,\rho)} = \mathsf{se}_2$ where σ and ρ are defined such that $x\sigma := x\sigma_1\sigma_2$ if $x \in \pi_1(v)$ and $x\sigma := x$ otherwise and $y\rho := y\rho_1\rho_2$ if $y \in \pi_2(v)$ and $y\rho := y$ otherwise.

Finally, as for hedges, a notion of consistency for S-environments is needed: under every possible substitution, the attacker is unable to get a contradiction from its updated knowledge.

Definition 12 (consistency). *A S-environment* $\mathsf{se} = (h, v, \prec, (\gamma_l, \gamma_r))$ *is* consistent *if it is well-formed, growing, for every* $(x, y) \in v$*, we have* $x \in \gamma_l$ *iff* $y \in \gamma_r$ *and if for every* σ, ρ *and* B *such that* $(\sigma, \rho) \triangleright_B \mathsf{se}$*, we have* $\mathcal{I}(h(\sigma, \rho) \cup B)$ *is a consistent hedge.*

Open Bisimulation An *open hedged relation* $\mathcal{R}$ is a subset of $\mathcal{S}_{\text{H}} \times \boldsymbol{P} \times \boldsymbol{P}$ such that for $(\mathsf{se}, P, Q) \in \mathcal{R}$, we have $\text{fn}(P) \subseteq \text{n}(\pi_1(\mathfrak{H}(\mathsf{se})))$ and $\text{fn}(Q) \subseteq \text{n}(\pi_2(\mathfrak{H}(\mathsf{se})))$. It is *consistent* if, for every $(\mathsf{se}, P, Q) \in \mathcal{R}$, se is consistent. It is symmetric if for every $(\mathsf{se}, P, Q) \in \mathcal{R}$ we have $(\mathsf{se}^{-1}, Q, P) \in \mathcal{R}$.

Definition 13 (open hedged bisimulation). *A symmetric consistent open hedged relation* $\mathcal{R}$ *is an* open hedged bisimulation *if for all* $(\mathsf{se}, P, Q) \in \mathcal{R}$*, for all* σ, ρ *and* B *such that* $(\sigma, \rho) \triangleright_B \mathsf{se}$*, if* $P\sigma \xrightarrow[S_1]{\mu_1} P'$ *with, if* $\mu_1 \neq \tau$*,* $\text{bn}(\mu_1) \cap \text{n}(\pi_1(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))) = \emptyset$ *and* $\text{ch}(\mu_1) \in \pi_1(\mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)})))$ *there exists* Q'*,* μ_2 *and* S_2 *such that* $Q\rho \xrightarrow[S_2]{\mu_2} Q'$ *with* $\text{bn}(\mu_2) \cap \text{n}(\pi_2(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))) = \emptyset$ *and*

1. *if* $\mu_1 = \tau$ *then* $\mu_2 = \tau$ *and* $(\mathsf{se}_B^{(\sigma,\rho)} \oplus_{\text{c}} (S_1, S_2), P', Q') \in \mathcal{R}$
2. *if* $\mu_1 = a_1(x_1)$ *then* $\mu_2 = a_2(x_2)$ *where* $(a_1, a_2) \in \mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))$ *and* $(\mathsf{se}_B^{(\sigma,\rho)} \oplus_{\text{i}} (x_1, x_2) \oplus_{\text{c}} (S_1, S_2), P', Q') \in \mathcal{R}$
3. *if* $\mu_1 = (\nu \tilde{z_1})\, \overline{a_1}\, M_1$ *then* $\mu_2 = (\nu \tilde{z_2})\, \overline{a_2}\, M_2$ *where* $(a_1, a_2) \in \mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))$ *and* $(\mathsf{se}_B^{(\sigma,\rho)} \oplus_{\text{o}} (M_1, M_2) \oplus_{\text{c}} (S_1, S_2), P', Q') \in \mathcal{R}$

In any case, names used as channels (collected in S_1, S_2) are added to the environment's γ_l and γ_r. On inputs (clause 2), input names are added to the environment's v. On outputs (clause 3), messages are added to the environment's h.

Let $\mathsf{se} \in \mathcal{S}_{\text{H}}$ and $P, Q \in \boldsymbol{P}$. We say that P and Q are *open hedged bisimilar under* se —written $P \sim_{\text{OH}}^{\mathsf{se}} Q$— if there exists an open hedged bisimulation $\mathcal{R}$ such that $(\mathsf{se}, P, Q) \in \mathcal{R}$.

We proved in [8, 7] that open hedged bisimilarity is sound w.r.t. to late hedged bisimilarity, i.e.

Theorem 2. *If* $P \sim_{\text{OH}}^{\mathsf{se}} Q$ *then for every* σ, ρ *and* B *such that* $(\sigma, \rho) \triangleright_B \mathsf{se}$ *we have* $P\sigma \sim_{\text{LH}}^{\mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))} Q\rho$.

Open hedged bisimilarity is closed under respectful substitutions.

Theorem 3. *If* $P \sim_{\text{OH}}^{\mathsf{se}} Q$ *then for every* σ, ρ *and* B *such that* $(\sigma, \rho) \triangleright_B \mathsf{se}$ *we have* $P\sigma \sim_{\text{OH}}^{\mathsf{se}_B^{(\sigma,\rho)}} Q\rho$.

Proof. By Lemma 3 and since $\text{fn}(P) \subseteq \text{n}(\pi_1(\mathfrak{H}(\mathsf{se})))$*,* $\text{fn}(Q) \subseteq \text{n}(\pi_2(\mathfrak{H}(\mathsf{se})))$ *whenever* $P \sim_{\text{OH}}^{\mathsf{se}} Q$.

3 A Symbolic Characterisation

Symbolic Semantics The symbolic characterisation of open hedged bisimulation relies on a symbolic transition system inspired by [4].

The idea behind the symbolic semantics is to record —without checking— conditions needed to derive a transition. Restrictions are still handled by side conditions in derivation rules. Every other constraint is simply collected in *transition constraints*. A symbolic transition is written $P \xrightarrow[(\nu\tilde{c})\,\phi]{\mu} P'$ where μ is a *symbolic action* and $(\nu\tilde{c})\,\phi$ is a transition constraint.

The set of symbolic actions $\mu \in \boldsymbol{A}_{\mathrm{s}}$ is defined by $\mu := \tau \mid E(x) \mid (\nu\tilde{z})\,\overline{E}\,F$ where $E, F \in \boldsymbol{E}$ and $\tilde{z}$ is a tuple of pairwise distinct names. By abuse of notation, we write $\overline{E}\,F$ when $\tilde{z}$ is empty. We define $\mathrm{bn}(E(x)) = \{x\}$ and $\mathrm{bn}((\nu\tilde{z})\,\overline{E}\,F) = \{\tilde{z}\}$. We extend the notion of concrete evaluation to symbolic actions with $\mathbf{e}_{\mathrm{c}}(\tau) := \tau$, $\mathbf{e}_{\mathrm{c}}(E(x)) := \mathbf{e}_{\mathrm{c}}(E)(x)$ provided that $\mathbf{e}_{\mathrm{c}}(E) \neq \bot$, $\mathbf{e}_{\mathrm{c}}((\nu\tilde{z})\,\overline{E}\,F) := (\nu\tilde{z})\,\overline{\mathbf{e}_{\mathrm{c}}(E)}\;\mathbf{e}_{\mathrm{c}}(F)$ provided that $\mathbf{e}_{\mathrm{c}}(E) \neq \bot$ and $\mathbf{e}_{\mathrm{c}}(F) \neq \bot$. Otherwise it is undefined. We implicitly assume that $\mathbf{e}_{\mathrm{c}}(\mu)$ is defined on μ when we write this expression.

A transition constraint has the form $(\nu\tilde{c})\,\phi$ where $\phi \in \boldsymbol{F}$ and $\tilde{c}$ is a tuple of pairwise distinct names. Names $\tilde{c}$ are binding occurrences in ϕ. We extend α-equivalence to transition constraints. Again, when $\tilde{c}$ is empty, we write ϕ by abuse of notation.

The *abstract evaluation* $\mathbf{e}_{\mathrm{a}}(E)$ of an expression is the symbolic counterpart of concrete evaluation. Intuitively, it can be seen as the reduction of E without checking that encryption and decryption keys correspond. It is defined by:

$$
\begin{array}{rll}
\mathbf{e}_{\mathrm{a}}(a) := a & & \text{if } a \in \boldsymbol{N} \\
\mathbf{e}_{\mathrm{a}}(\mathsf{Enc}^{\mathrm{s}}_{F} E) := \mathsf{Enc}^{\mathrm{s}}_{\mathbf{e}_{\mathrm{a}}(F)} \mathbf{e}_{\mathrm{a}}(E) & & \\
\mathbf{e}_{\mathrm{a}}(\mathsf{Enc}^{\mathrm{a}}_{F} E) := \mathsf{Enc}^{\mathrm{a}}_{\mathbf{e}_{\mathrm{a}}(F)} \mathbf{e}_{\mathrm{a}}(E) & & \\
\mathbf{e}_{\mathrm{a}}((E\,.\,F)) := (\mathbf{e}_{\mathrm{a}}(E)\,.\,\mathbf{e}_{\mathrm{a}}(F)) & & \\
\mathbf{e}_{\mathrm{a}}(\mathsf{op}(E)) := \mathsf{op}(\mathbf{e}_{\mathrm{a}}(E)) & & \mathsf{op} \in \{\mathsf{pub}, \mathsf{priv}, \mathsf{H}\} \\
\mathbf{e}_{\mathrm{a}}(\mathsf{Dec}^{\mathrm{s}}_{F} E) := E_1 & & \text{if } \mathbf{e}_{\mathrm{a}}(E) = \mathsf{Enc}^{\mathrm{s}}_{E_2} E_1 \\
\qquad\qquad \mathsf{Dec}^{\mathrm{s}}_{\mathbf{e}_{\mathrm{a}}(F)} \mathbf{e}_{\mathrm{a}}(E) & & \text{otherwise} \\
\mathbf{e}_{\mathrm{a}}(\mathsf{Dec}^{\mathrm{a}}_{F} E) := E_1 & & \text{if } \mathbf{e}_{\mathrm{a}}(E) = \mathsf{Enc}^{\mathrm{a}}_{E_2} E_1 \\
\qquad\qquad \mathsf{Dec}^{\mathrm{a}}_{\mathbf{e}_{\mathrm{a}}(F)} \mathbf{e}_{\mathrm{a}}(E) & & \text{otherwise} \\
\mathbf{e}_{\mathrm{a}}(\pi_1\,(E)) := E_1 & & \text{if } \mathbf{e}_{\mathrm{a}}(E) = (E_1\,.\,E_2) \\
\qquad\qquad \pi_1\,(\mathbf{e}_{\mathrm{a}}(E)) & & \text{otherwise} \\
\mathbf{e}_{\mathrm{a}}(\pi_2\,(E)) := E_2 & & \text{if } \mathbf{e}_{\mathrm{a}}(E) = (E_1\,.\,E_2) \\
\qquad\qquad \pi_2\,(\mathbf{e}_{\mathrm{a}}(E)) & & \text{otherwise}
\end{array}
$$

The symbolic transition $P \xrightarrow[(\nu\tilde{c})\,\phi]{\mu} Q$ is defined by the derivation rules given in Table 2 (extended by the symmetric variants of S-Close-l, S-Par-l and S-Sum-l). Contrary to the symbolic semantics in [4], restricted names of μ are not binding transition constraints: we really have two kinds of bound names on symbolic transitions. Only the bound names of μ are binding occurrences in Q.

Before showing the relation between symbolic transitions and concrete transitions, an auxiliary definition is needed.

$$\text{S-Input}\ \frac{}{E(x).P \xrightarrow[[\,E:\boldsymbol{N}\,]]{\mathbf{e}_{\mathrm{a}}(E)(x)} P} \qquad \text{S-Output}\ \frac{}{\overline{E}\langle F\rangle.P \xrightarrow[[\,E:\boldsymbol{N}\,]\wedge[\,F:\boldsymbol{M}\,]]{\overline{\mathbf{e}_{\mathrm{a}}(E)}\ \mathbf{e}_{\mathrm{a}}(F)} P}$$

$$\text{S-Close-L}\ \frac{P \xrightarrow[(\nu\tilde{c})\ \phi]{E(x)} P' \qquad Q \xrightarrow[(\nu\tilde{d})\ \psi]{(\nu\tilde{z})\ \overline{F}\ G} Q'}{P \mid Q \xrightarrow[(\nu\tilde{c}\tilde{d})\ ([\,E=F\,]\wedge\phi\wedge\psi)]{\tau} (\nu\tilde{z})\,(P'\{^{G}/_{x}\} \mid Q')}\ \begin{array}{l}\{\tilde{z}\}\cap \mathrm{fn}(P)=\emptyset\\ \{\tilde{c}\}\cap \mathrm{n}(\psi,E,F)=\emptyset\\ \{\tilde{d}\}\cap \mathrm{n}(\phi,E,F)=\emptyset\end{array}$$

$$\text{S-Open}\ \frac{P \xrightarrow[(\nu\tilde{c})\ \phi]{(\nu\tilde{z})\ \overline{E}\ F} P'}{(\nu z')\,P \xrightarrow[(\nu z'\tilde{c})\ \phi]{(\nu z'\tilde{z})\ \overline{E}\ F} P'}\ \begin{array}{l} z'\in \mathrm{n}(F)\\ z'\notin \mathrm{n}(E)\\ z'\notin\{\tilde{z},\tilde{c}\}\end{array} \qquad \text{S-Res}\ \frac{P \xrightarrow[(\nu\tilde{c})\ \phi]{\mu} P'}{(\nu z)\,P \xrightarrow[(\nu\tilde{c})\ \phi]{\mu} (\nu z)\,P'}\ \begin{array}{l} z\notin \mathrm{n}(\mu)\\ z\notin \mathrm{n}(\phi)\end{array}$$

$$\text{S-RO-Guard}\ \frac{P \xrightarrow[(\nu\tilde{c})\ \phi]{\mu} P'}{(\nu z)\,P \xrightarrow[(\nu z\tilde{c})\ \phi]{\mu} (\nu z)\,P'}\ \begin{array}{l} z\notin \mathrm{n}(\mu)\\ z\in \mathrm{n}(\phi)\\ z\notin\{\tilde{c}\}\end{array}$$

$$\text{S-Guard}\ \frac{P \xrightarrow[(\nu\tilde{c})\ \psi]{\mu} P'}{\phi P \xrightarrow[(\nu\tilde{c})\ (\phi\wedge\psi)]{\mu} P'}\ \{\tilde{c}\}\cap \mathrm{n}(\phi)=\emptyset$$

$$\text{S-Par-L}\ \frac{P \xrightarrow[(\nu\tilde{c})\ \phi]{\mu} P'}{P \mid Q \xrightarrow[(\nu\tilde{c})\ \phi]{\mu} P' \mid Q}\ \mathrm{bn}(\mu)\cap \mathrm{fn}(Q)=\emptyset \qquad \text{S-Sum-L}\ \frac{P \xrightarrow[(\nu\tilde{c})\ \phi]{\mu} P'}{P+Q \xrightarrow[(\nu\tilde{c})\ \phi]{\mu} P'}$$

$$\text{S-Rep-act}\ \frac{P \xrightarrow[(\nu\tilde{c})\ \phi]{\mu} P'}{!\,P \xrightarrow[(\nu\tilde{c})\ \phi]{\mu} P' \mid !\,P}\ \mathrm{bn}(\mu)\cap \mathrm{fn}(P)=\emptyset$$

$$\text{S-Rep-Close}\ \frac{P \xrightarrow[(\nu\tilde{c})\ \phi]{E(x)} P' \qquad P \xrightarrow[(\nu\tilde{d})\ \psi]{(\nu\tilde{z})\ \overline{F}\ G} P''}{!\,P \xrightarrow[(\nu\tilde{c}\tilde{d})\ ([\,E=F\,]\wedge\phi\wedge\psi)]{\tau} (\nu\tilde{z})\,(P'\{^{G}/_{x}\} \mid P'') \mid !\,P}\ \begin{array}{l}\{\tilde{z}\}\cap \mathrm{fn}(P)=\emptyset\\ \{\tilde{c}\}\cap \mathrm{n}(\psi,E,F)=\emptyset\\ \{\tilde{d}\}\cap \mathrm{n}(\phi,E,F)=\emptyset\end{array}$$

$$\text{S-Alpha}\ \frac{P \equiv_{\alpha} P' \qquad (\nu\tilde{c})\,\phi \equiv_{\alpha} (\nu\tilde{c'})\,\phi' \qquad P' \xrightarrow[(\nu\tilde{c'})\ \phi']{\mu} P''}{P \xrightarrow[(\nu\tilde{c})\ \phi]{\mu} P''}$$

Table 2. The symbolic semantics of the spi calculus

Definition 14 ($>_{\mathrm{o}}$). *We let $>_{\mathrm{o}}$ be the least precongruence on expressions, guards and processes (modulo $\equiv_\alpha$ for processes) such that*

1. $\pi_1\left((E_1 \,.\, E_2)\right) >_{\mathrm{o}} E_1$ *provided that* $\mathbf{e}_{\mathrm{c}}(E_1) \neq \bot$
2. $\pi_2\left((E_1 \,.\, E_2)\right) >_{\mathrm{o}} E_2$ *provided that* $\mathbf{e}_{\mathrm{c}}(E_2) \neq \bot$
3. $\mathsf{Dec}^{\mathrm{s}}_{E_2}\mathsf{Enc}^{\mathrm{s}}_{E_2}E_1 >_{\mathrm{o}} E_1$ *provided that* $\mathbf{e}_{\mathrm{c}}(E_2) \neq \bot$
4. $\mathsf{Dec}^{\mathrm{a}}_{\mathsf{priv}(E_2)}\mathsf{Enc}^{\mathrm{a}}_{\mathsf{pub}(E_2)}E_1 >_{\mathrm{o}} E_1$ *provided that* $\mathbf{e}_{\mathrm{c}}(E_2) \neq \bot$
5. $\mathsf{Dec}^{\mathrm{a}}_{\mathsf{pub}(E_2)}\mathsf{Enc}^{\mathrm{a}}_{\mathsf{priv}(E_2)}E_1 >_{\mathrm{o}} E_1$ *provided that* $\mathbf{e}_{\mathrm{c}}(E_2) \neq \bot$

Processes related by $>_{\mathrm{o}}$ have the same (concrete) semantics.

Lemma 4. *Let $P, Q \in \boldsymbol{P}$ and assume that $P >_{\mathrm{o}} Q$.*

1. *if $P \xrightarrow[S]{\mu} P'$ then $Q \xrightarrow[S]{\mu} Q'$ and $P' >_{\mathrm{o}} Q'$.*
2. *if $Q \xrightarrow[S]{\mu} Q'$ and $\mathrm{bn}(\mu) \cap \mathrm{fn}(P) = \emptyset$ then $P \xrightarrow[S]{\mu} P'$ and $P' >_{\mathrm{o}} Q'$.*

Proof (sketch). By rule induction on the transitions and since

- *if $E >_{\mathrm{o}} F$ then $\mathbf{e}_{\mathrm{c}}(E) = M$ iff $\mathbf{e}_{\mathrm{c}}(F) = M$*
- *if $\phi >_{\mathrm{o}} \psi$ then $\mathbf{e}(\phi)$ iff $\mathbf{e}(\psi)$ and if $\mathbf{e}(\phi)$ then $\mathbf{nc}(\phi) = \mathbf{nc}(\psi)$*

Lemma 5. *Let $P \in \boldsymbol{P}$.*

1. *If $P \xrightarrow[(\nu\tilde{c})\,\phi]{\mu} P'$ and σ is such that $\mathrm{n}(\mathrm{cosupp}(\sigma)) \cap \mathrm{bn}(\mu) = \mathrm{n}(\sigma) \cap \{\tilde{c}\} = \emptyset$ and $\mathbf{e}(\phi\sigma)$ then $P\sigma \xrightarrow[\mathbf{nc}(\phi\sigma)\setminus\{\tilde{c}\}]{\mathbf{e}_{\mathrm{c}}(\mu\sigma)} Q'$ with $P'\sigma >_{\mathrm{o}} Q'$.*
2. *If $P\sigma \xrightarrow[S]{\mu} R$ and $\mathrm{n}(\mathrm{cosupp}(\sigma)) \cap \mathrm{bn}(\mu) = \emptyset$ then there exists μ', $\tilde{c}$, ϕ and Q such that $P \xrightarrow[(\nu\tilde{c})\,\phi]{\mu'} Q$, $\{\tilde{c}\} \cap \mathrm{n}(\sigma) = \emptyset$, $\mathbf{e}(\phi\sigma)$, $\mathbf{e}_{\mathrm{c}}(\mu'\sigma) = \mu$, $S = \mathbf{nc}(\phi\sigma) \setminus \{\tilde{c}\}$ and $Q\sigma >_{\mathrm{o}} R$.*

Proof (sketch). By rule induction on the transitions.

Symbolic Open Bisimulation Lemma 5 suggests the following definition:

Definition 15 (symbolic open hedged bisimulation). *A symmetric consistent open hedged relation $\mathcal{R}$ is a* symbolic open hedged bisimulation *if for all $(\mathsf{se}, P, Q) \in \mathcal{R}$, for all σ, ρ and B such that $(\sigma, \rho) \triangleright_B \mathsf{se}$, if $P \xrightarrow[(\nu\tilde{c})\,\phi_1]{\mu_1} P'$ with $\mathrm{n}(\sigma) \cap \{\tilde{c}\} = \emptyset$, $\mathbf{e}(\phi_1\sigma)$ and, if $\mu_1 \neq \tau$, $\mathrm{bn}(\mu_1) \cap \mathrm{n}(\pi_1(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))) = \emptyset$ and $\mathrm{ch}(\mathbf{e}_{\mathrm{c}}(\mu_1\sigma)) \in \pi_1(\mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)})))$ there exists Q', μ_2, $\tilde{d}$ and ϕ_2 such that $Q \xrightarrow[(\nu\tilde{d})\,\phi_2]{\mu_2} Q'$ with $\mathrm{n}(\rho) \cap \{\tilde{d}\} = \emptyset$, $\mathbf{e}(\phi_2\rho)$, $\mathrm{bn}(\mu_2) \cap \mathrm{n}(\pi_2(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))) = \emptyset$ and*

1. *if $\mu_1 = \tau$ then $\mu_2 = \tau$ and $(\mathsf{se}_B^{(\sigma,\rho)} \oplus_{\mathrm{c}} (S_1, S_2), P'\sigma, Q'\rho) \in \mathcal{R}$*
2. *if $\mu_1 = E_1(x_1)$ then $\mu_2 = E_2(x_2)$ where $(\mathbf{e}_{\mathrm{c}}(E_1\sigma), \mathbf{e}_{\mathrm{c}}(E_2\rho)) \in \mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))$ and $(\mathsf{se}_B^{(\sigma,\rho)} \oplus_{\mathrm{i}} (x_1, x_2) \oplus_{\mathrm{c}} (S_1, S_2), P'\sigma, Q'\rho) \in \mathcal{R}$*

3. *if* $\mu_1 = (\nu \tilde{z_1})\,\overline{E_1}\,F_1$ *then* $\mu_2 = (\nu \tilde{z_2})\,\overline{E_2}\,F_2$ *where* $(\mathbf{e}_{\mathrm{c}}(E_1\sigma), \mathbf{e}_{\mathrm{c}}(E_2\rho)) \in \mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))$ *and* $(\mathsf{se}_B^{(\sigma,\rho)} \oplus_{\mathrm{o}} (\mathbf{e}_{\mathrm{c}}(F_1\sigma), \mathbf{e}_{\mathrm{c}}(F_2\rho)) \oplus_{\mathrm{c}} (S_1, S_2), P'\sigma, Q'\rho) \in \mathcal{R}$

where $S_1 = \mathbf{nc}(\phi_1\sigma) \setminus \{\tilde{c}\}$ *and* $S_2 = \mathbf{nc}(\phi_2\rho) \setminus \{\tilde{d}\}$

Let $\mathsf{se} \in \mathcal{S}_{\mathrm{H}}$ and $P, Q \in \boldsymbol{P}$. We say that P and Q are *symbolic open hedged bisimilar under* se —written $P \sim^{\mathsf{se}}_{\mathrm{SO}} Q$— if there exists a symbolic open hedged bisimulation $\mathcal{R}$ such that $(\mathsf{se}, P, Q) \in \mathcal{R}$.

Theorem 4 (symbolic characterisation theorem). *Let* $\mathsf{se} \in \mathcal{S}_{\mathrm{H}}$ *and* $P, Q \in \boldsymbol{P}$. *Then* $P \sim^{\mathsf{se}}_{\mathrm{OH}} Q \iff P \sim^{\mathsf{se}}_{\mathrm{SO}} Q$.

Proof (sketch). We prove both implications:

$\Rightarrow$ *We show that* $\mathcal{R} = \{(\mathsf{se}, P, Q) \mid P' \sim^{\mathsf{se}}_{\mathrm{OH}} Q' \wedge P >_{\mathrm{o}} P' \wedge Q >_{\mathrm{o}} Q' \wedge \mathrm{fn}(P) \subseteq \mathrm{n}(\pi_1(\mathfrak{H}(\mathsf{se}))) \wedge \mathrm{fn}(Q) \subseteq \mathrm{n}(\pi_2(\mathfrak{H}(\mathsf{se})))\}$ *is a symbolic open hedged bisimulation.*

$\Leftarrow$ *We show that* $\mathcal{R} = \{(\mathsf{se}, P, Q) \mid P' \sim^{\mathsf{se}}_{\mathrm{SO}} Q' \wedge P' >_{\mathrm{o}} P \wedge Q' >_{\mathrm{o}} Q\}$ *is an open hedged bisimulation.*

Towards Mechanisation of Open Hedged Bisimulation Definition 15 clarifies which pairs of respectful substitutions have to be considered to enable transitions. Indeed, for (se, P, Q) and a symbolic transition $P \xrightarrow[(\nu \tilde{c})\ \phi]{\mu} P'$, we have to consider the pairs (σ, ρ) such that $(\sigma, \rho) \rhd_B \mathsf{se}$ and $\mathbf{e}(\phi\sigma)$ (with $\mathrm{n}(\sigma) \cap \{\tilde{c}\} = \emptyset$). Using a unification-like algorithm, we can show that every substitution σ that satisfies ϕ (i.e. $\mathbf{e}(\phi\sigma)$) and $\mathrm{supp}(\sigma) \subseteq V$ can be written $\sigma = \sigma_\phi\sigma'$ where σ_ϕ belongs to a finite set S_ϕ of the most general solutions of ϕ. We are then interested in instances $\sigma = \sigma_\phi\sigma'$ (with $\sigma_\phi \in S_\phi$) such that there exists ρ and B such that $(\sigma, \rho) \rhd_B \mathsf{se}$. By using similar ideas as developed in [9] to solve the so-called "problem of simultaneous construction" we work towards proving that there exists a finite set of *most general solutions* to this problem and that it is sufficient to inspect this finite set rather than the infinite set of Definition 15. The problem of checking consistency of a S-environment can be solved using similar ideas. This finally suggests that open hedged bisimulation is decidable for *finite* spi calculus terms. Note that it was shown in [12] that *finite control* spi calculus is Turing complete.

Conclusion and Future Work

We presented a revised (w.r.t. [8, 7]) version of open hedged bisimulation. We have shown a first congruence result: open hedged bisimilarity is preserved under every pair of respectful substitutions. We have given an alternative definition of open hedged bisimulation called symbolic open hedged bisimulation. It is built upon a symbolic transition system similar to [4]. The symbolic characterisation theorem suggests that open hedged bisimilarity is decidable for finite spi calculus processes.

In future work, we expect to settle this by formalising and proving algorithms we have quickly sketched. We would also like to clarify the precise link between open hedged bisimulation and symbolic bisimulation as presented in [4]. Finally, the study of congruence properties is another field of investigation we are considering: the non-symbolic definition of open hedged bisimulation is probably more suited to study such theoretical results.

References

1. Martín Abadi and Andrew D. Gordon. A bisimulation method for cryptographic protocols. *Nordic Journal of Computing*, 5(4):267–303, Winter.
2. Martín Abadi and Andrew D. Gordon. A calculus for cryptographic protocols: The Spi calculus. *Journal of Information and Computation*, 148(1):1–70, 1999.
3. Michele Boreale, Rocco De Nicola, and Rosario Pugliese. Proof techniques for cryptographic processes. *SIAM Journal on Computing*, 31(3):947–986, 2002.
4. Johannes Borgström, Sébastien Briais, and Uwe Nestmann. Symbolic bisimulation in the spi calculus. In Philippa Gardner and Nobuko Yoshida, editors, *CONCUR*, volume 3170 of *Lecture Notes in Computer Science*, pages 161–176. Springer, 2004.
5. Johannes Borgström and Uwe Nestmann. On bisimulations for the spi-calculus. In *Proceedings of AMAST 2002*, September 2002.
6. Sébastien Briais. *ABC Bisimulation Checker*. EPFL, 2003.
7. Sébastien Briais and Uwe Nestmann. Open bisimulation, revisited. *Special Issue of TCS*. To Appear.
8. Sébastien Briais and Uwe Nestmann. Open bisimulation, revisited. In Jos Baeten and Iain Phillips, editors, *Proceedings of EXPRESS 2005: Expressiveness in Concurrency*, volume 154 of *Electronic Notes in Theoretical Computer Science*, pages 93–105, 2005.
9. Yannick Chevalier. *Résolution de problèmes d'accessibilité pour la compilation et la validation de protocoles cryptographiques*. PhD thesis, Université Henri Poincaré – Nancy 1, 2003.
10. Véronique Cortier. *Vérification automatique des protocoles cryptographiques*. PhD thesis, École Normale Supérieure de Cachan, 2003.
11. Luca Durante, Riccardo Sisto, and Adriano Valenzano. Automatic testing equivalence verification of spi-calculus specifications. *ACM Transactions on Software Engineering and Methodology*, 12(2):222–284, April 2003.
12. Hans Hüttel. Deciding framed bisimilarity. In Antonín Kučera and Richard Mayr, editors, *Proceedings of INFINITY 2002*, volume 68 of *Electronic Notes in Theoretical Computer Science*, page 20, 2002.
13. Robin Milner, Joachim Parrow, and David Walker. A calculus of mobile processes, part I/II. *Information and Computation*, 100:1–77, September 1992.
14. Joachim Parrow. An introduction to the pi-calculus. In Jan Bergstra, Alban Ponse, and Scott Smolka, editors, *Handbook of Process Algebra*, pages 479–543. Elsevier Science, 2001.
15. D. Sangiorgi and D. Walker. *The π-calculus: a Theory of Mobile Processes*. Cambridge University Press, 2001.
16. Davide Sangiorgi. A theory of bisimulation for the π-calculus. *Acta Informatica*, 33:69–97, 1996.
17. Björn Victor. *A Verification Tool for the Polyadic π-Calculus*. Licentiate thesis, Department of Computer Systems, Uppsala University, Sweden, May © 1994. Available as report DoCS 94/50.

A Proofs

This appendix will not be part of the final paper. The following proofs will be released in a technical report to appear later.

The author has formalised in the proof assistant Coq several results that will be used in the following. In particular, most of the results concerning hedge theory have been already spread as an official Coq contribution and have been revised to take into account the new message language we use in this paper.

Concrete evaluation, abstract evaluation and $>_{\mathrm{o}}$

Lemma 6. *Let $M \in \boldsymbol{M}$. Then $\mathbf{e}_{\mathrm{c}}(M) = M$.*

Proof. *By induction on M.*

Lemma 7. *Let $E \in \boldsymbol{E}$ and $\sigma : \boldsymbol{N} \to \boldsymbol{M}$. If $\mathbf{e}_{\mathrm{c}}(E) = M \in \boldsymbol{M}$ then $\mathbf{e}_{\mathrm{c}}(E\sigma) = \mathbf{e}_{\mathrm{c}}(E)\sigma = M\sigma$.*

Proof. *By induction on E and by Lemma 6.*

Lemma 8. *Let $\phi \in \boldsymbol{F}$ and $\sigma : \boldsymbol{N} \to \boldsymbol{M}$. If $\mathbf{e}_{\mathrm{c}}(\phi) = \mathbf{true}$ then*

$$\mathbf{e}_{\mathrm{c}}(\phi\sigma) = \mathbf{true} \iff \forall x \in \mathbf{nc}(\phi) : x\sigma \in \boldsymbol{N}$$

Moreover, if $\mathbf{e}_{\mathrm{c}}(\phi\sigma) = \mathbf{true}$ then $\mathbf{nc}(\phi\sigma) = \mathbf{nc}(\phi)\sigma$.

Proof. *By induction on ϕ and thanks to Lemma 7.*

Lemma 9. *Let $E \in \boldsymbol{E}$. If $\mathbf{e}_{\mathrm{c}}(E) = M \in \boldsymbol{M}$, then $E >_{\mathrm{o}} M$.*

Proof. *By induction on E. We give the proof for the inductive case $E = \pi_1(F)$.*
Assume that $E = \pi_1(F)$ and the result holds for F.
Since $\mathbf{e}_{\mathrm{c}}(E) = M \in \boldsymbol{M}$, necessarily $\mathbf{e}_{\mathrm{c}}(F) = (M \,.\, N) \in \boldsymbol{M}$ for some N.
By induction, we have $F >_{\mathrm{o}} (M \,.\, N)$.
By $>_{\mathrm{o}}$-FST, we have $\pi_1(F) >_{\mathrm{o}} \pi_1((M \,.\, N))$, i.e. $E >_{\mathrm{o}} \pi_1((M \,.\, N))$.
By $>_{\mathrm{o}}$-FST-PAIR, we have $\pi_1((M \,.\, N)) >_{\mathrm{o}} M$, because $\mathbf{e}_{\mathrm{c}}(N) \neq \bot$ by Lemma 6 since $N \in \boldsymbol{M}$.
So, by $>_{\mathrm{o}}$-TRANS, we conclude that $E >_{\mathrm{o}} M$.

Lemma 10. *Let $E, F \in \boldsymbol{E}$ and assume that $E >_{\mathrm{o}} F$. Let $M \in \boldsymbol{M}$. Then*

$$\mathbf{e}_{\mathrm{c}}(E) = M \iff \mathbf{e}_{\mathrm{c}}(F) = M$$

Proof. $\Rightarrow$ *By rule induction on $E >_{\mathrm{o}} F$.*
$\Leftarrow$ *By rule induction on $E >_{\mathrm{o}} F$. We give below the proof for the case $>_{\mathrm{o}}$-FST-PAIR.*
Assume $E >_{\mathrm{o}} F$ by $>_{\mathrm{o}}$-FST-PAIR.
Then $E = \pi_1((F \,.\, G))$ with $\mathbf{e}_{\mathrm{c}}(G) \neq \bot$.
By hypothesis, $\mathbf{e}_{\mathrm{c}}(F) = M$. Since $\mathbf{e}_{\mathrm{c}}(G) \neq \bot$, there exists $N \in \boldsymbol{M}$ such that $\mathbf{e}_{\mathrm{c}}(G) = N$.
We have thus $\mathbf{e}_{\mathrm{c}}((F \,.\, G)) = (M \,.\, N)$.
So $\mathbf{e}_{\mathrm{c}}(E) = M$

Corollary 1. *Let $\phi, \psi \in \boldsymbol{F}$ and assume that $\phi >_{\mathrm{o}} \psi$. Then*

$$\mathbf{e}(\phi) \iff \mathbf{e}(\psi)$$

Moreover, if $\mathbf{e}(\phi)$, then $\mathbf{nc}(\phi) = \mathbf{nc}(\psi)$.

Lemma 11. *Let $E, F \in \boldsymbol{E}$ and $\sigma : \boldsymbol{N} \to \boldsymbol{M}$ a substitution. Assume that $E >_{\mathrm{o}} F$. Then $E\sigma >_{\mathrm{o}} F\sigma$.*

Proof. *By rule induction on $E >_{\mathrm{o}} F$ and thanks to Lemma 7.*

Lemma 12. *Let $E \in \boldsymbol{E}$. If $\mathbf{e}_{\mathrm{c}}(E) = M \in \boldsymbol{M}$ then $\mathbf{e}_{\mathrm{a}}(E) = \mathbf{e}_{\mathrm{c}}(E)$.*

Proof. *By induction on E.*

Lemma 13. *Let $E \in \boldsymbol{E}$ and $\sigma : \boldsymbol{N} \to \boldsymbol{M}$ a substitution. Then $\mathbf{e}_{\mathrm{a}}(\mathbf{e}_{\mathrm{a}}(E)\sigma) = \mathbf{e}_{\mathrm{a}}(E\sigma)$.*

Proof. *By induction on E. We give the proof for the inductive case $E = \pi_1\,(F)$.*
Assume $E = \pi_1\,(F)$ and the result holds for F.
By induction, we have (*) $\mathbf{e}_{\mathrm{a}}(\mathbf{e}_{\mathrm{a}}(F)\sigma) = \mathbf{e}_{\mathrm{a}}(F\sigma)$.
We have two cases:

1. *if $\mathbf{e}_{\mathrm{a}}(F) = (F_1\,.\,F_2)$ for some F_1, F_2.*
   Then $\mathbf{e}_{\mathrm{a}}(E) = F_1$.
   So $\mathbf{e}_{\mathrm{a}}(\mathbf{e}_{\mathrm{a}}(E)\sigma) = \mathbf{e}_{\mathrm{a}}(F_1\sigma)$.
   Rewriting (*) gives $\mathbf{e}_{\mathrm{a}}((F_1\,.\,F_2)\sigma) = \mathbf{e}_{\mathrm{a}}(F\sigma)$, i.e. $\mathbf{e}_{\mathrm{a}}((F_1\sigma\,.\,F_2\sigma)) = \mathbf{e}_{\mathrm{a}}(F\sigma)$.
   By definition, $\mathbf{e}_{\mathrm{a}}((F_1\sigma\,.\,F_2\sigma)) = (\mathbf{e}_{\mathrm{a}}(F_1\sigma)\,.\,\mathbf{e}_{\mathrm{a}}(F_2\sigma))$.
   So $\mathbf{e}_{\mathrm{a}}(F\sigma) = (\mathbf{e}_{\mathrm{a}}(F_1\sigma)\,.\,\mathbf{e}_{\mathrm{a}}(F_2\sigma))$.
   So $\mathbf{e}_{\mathrm{a}}(E\sigma) = \mathbf{e}_{\mathrm{a}}(\pi_1\,(F)\,\sigma) = \mathbf{e}_{\mathrm{a}}(\pi_1\,(F\sigma)) = \mathbf{e}_{\mathrm{a}}(F_1\sigma)$ by definition.
   Hence $\mathbf{e}_{\mathrm{a}}(\mathbf{e}_{\mathrm{a}}(E)\sigma) = \mathbf{e}_{\mathrm{a}}(E\sigma)$.
2. *otherwise*
   Then by definition, $\mathbf{e}_{\mathrm{a}}(E) = \pi_1\,(\mathbf{e}_{\mathrm{a}}(F))$.
   Thus, $\mathbf{e}_{\mathrm{a}}(E)\sigma = \pi_1\,(\mathbf{e}_{\mathrm{a}}(F)\sigma)$.
   So $\mathbf{e}_{\mathrm{a}}(\mathbf{e}_{\mathrm{a}}(E)\sigma) = \mathbf{e}_{\mathrm{a}}(\pi_1\,(\mathbf{e}_{\mathrm{a}}(F)\sigma))$.
   We have then two subcases:
   (a) if $\mathbf{e}_{\mathrm{a}}(\mathbf{e}_{\mathrm{a}}(F)\sigma) = (F_1\,.\,F_2)$
   By (*), we have then $\mathbf{e}_{\mathrm{a}}(F\sigma) = (F_1\,.\,F_2)$.
   By definition, we have $\mathbf{e}_{\mathrm{a}}(\mathbf{e}_{\mathrm{a}}(E)\sigma) = F_1$.
   And by definition, we have $\mathbf{e}_{\mathrm{a}}(\pi_1\,(F\sigma)) = F_1$.
   But $\mathbf{e}_{\mathrm{a}}(\pi_1\,(F\sigma)) = \mathbf{e}_{\mathrm{a}}(\pi_1\,(F)\,\sigma) = \mathbf{e}_{\mathrm{a}}(E\sigma)$.
   So $\mathbf{e}_{\mathrm{a}}(\mathbf{e}_{\mathrm{a}}(E)\sigma) = \mathbf{e}_{\mathrm{a}}(E\sigma)$.
   (b) otherwise
   So by definition, we have $\mathbf{e}_{\mathrm{a}}(\mathbf{e}_{\mathrm{a}}(E)\sigma) = \pi_1\,(\mathbf{e}_{\mathrm{a}}(\mathbf{e}_{\mathrm{a}}(F)\sigma))$ which is equal to $\pi_1\,(\mathbf{e}_{\mathrm{a}}(F\sigma))$ by (*).
   By (*), we know that $\mathbf{e}_{\mathrm{a}}(F\sigma)$ is not a pair so $\mathbf{e}_{\mathrm{a}}(\pi_1\,(F\sigma)) = \pi_1\,(\mathbf{e}_{\mathrm{a}}(F\sigma))$.
   But $\mathbf{e}_{\mathrm{a}}(\pi_1\,(F\sigma)) = \mathbf{e}_{\mathrm{a}}(E\sigma)$.
   So $\mathbf{e}_{\mathrm{a}}(\mathbf{e}_{\mathrm{a}}(E)\sigma) = \mathbf{e}_{\mathrm{a}}(E\sigma)$.

Corollary 2. *Let $E \in \boldsymbol{E}$. Then $\mathbf{e}_{\mathrm{a}}(\mathbf{e}_{\mathrm{a}}(E)) = \mathbf{e}_{\mathrm{a}}(E)$.*

Lemma 14. *Let $E \in \boldsymbol{E}$ and $\sigma : \boldsymbol{N} \to \boldsymbol{M}$ a substitution. Assume that $\mathbf{e}_{\mathrm{c}}(E\sigma) = M \in \boldsymbol{M}$. Then $\mathbf{e}_{\mathrm{c}}(\mathbf{e}_{\mathrm{a}}(E)\sigma) = M$.*

Proof. *By induction on E. We give the proof for the inductive case $E = \pi_1(F)$.*
Assume $E = \pi_1(F)$ and the result holds for F
We have $\mathbf{e}_{\mathrm{c}}(E\sigma) = \mathbf{e}_{\mathrm{c}}(\pi_1(F\sigma)) = M \in \boldsymbol{M}$.
Necessarily, $\mathbf{e}_{\mathrm{c}}(F\sigma) = (M \,.\, N)$ for some $N \in \boldsymbol{M}$.
By induction, we have thus $\mathbf{e}_{\mathrm{c}}(\mathbf{e}_{\mathrm{a}}(F)\sigma) = (M \,.\, N)$.
We have two cases:

1. *if $\mathbf{e}_{\mathrm{a}}(F) = (F_1 \,.\, F_2)$*
   Then $\mathbf{e}_{\mathrm{a}}(E) = F_1$.
   We have $\mathbf{e}_{\mathrm{c}}(\mathbf{e}_{\mathrm{a}}(F)\sigma) = \mathbf{e}_{\mathrm{c}}((F_1\sigma \,.\, F_2\sigma)) = (M \,.\, N)$.
   So necessarily, $\mathbf{e}_{\mathrm{c}}(F_1\sigma) = M$ and $\mathbf{e}_{\mathrm{c}}(F_2\sigma) = N$.
   Hence the result, since $\mathbf{e}_{\mathrm{c}}(E\sigma) = M = \mathbf{e}_{\mathrm{c}}(F_1\sigma) = \mathbf{e}_{\mathrm{c}}(\mathbf{e}_{\mathrm{a}}(E)\sigma)$.
2. *otherwise*
   We have $\mathbf{e}_{\mathrm{a}}(E) = \pi_1(\mathbf{e}_{\mathrm{a}}(F))$.
   So $\mathbf{e}_{\mathrm{c}}(\mathbf{e}_{\mathrm{a}}(E)\sigma) = \mathbf{e}_{\mathrm{c}}(\pi_1(\mathbf{e}_{\mathrm{a}}(F)\sigma))$.
   Since $\mathbf{e}_{\mathrm{c}}(\mathbf{e}_{\mathrm{a}}(F)\sigma) = (M \,.\, N)$, we have $\mathbf{e}_{\mathrm{c}}(\pi_1(\mathbf{e}_{\mathrm{a}}(F)\sigma)) = M$ by definition.
   Hence $\mathbf{e}_{\mathrm{c}}(\mathbf{e}_{\mathrm{a}}(E)\sigma) = \mathbf{e}_{\mathrm{c}}(E\sigma)$.

Lemma 15. *Let $E \in \boldsymbol{E}$ and $\sigma : \boldsymbol{N} \to \boldsymbol{M}$ a substitution. Assume that $\mathbf{e}_{\mathrm{c}}(E\sigma) \neq \bot$. Let $z \in \boldsymbol{N}$ such that $z \notin \mathrm{n}(\sigma)$. If $z \in \mathrm{n}(\mathbf{e}_{\mathrm{a}}(E))$, then $z \in \mathrm{n}(\mathbf{e}_{\mathrm{c}}(E\sigma))$.*

Proof. *Let $\sigma : \boldsymbol{N} \to \boldsymbol{M}$ a substitution and $z \in \boldsymbol{N}$ such that $z \notin \mathrm{n}(\sigma)$.*
For $x \in \boldsymbol{N}$, we define the inductive predicate $x \lhd E$ on expressions:

$$\frac{}{x \lhd x} \qquad \frac{x \lhd E_1}{x \lhd (E_1 \,.\, E_2)} \qquad \frac{x \lhd E_2}{x \lhd (E_1 \,.\, E_2)} \qquad \frac{x \lhd E_1}{x \lhd \mathsf{Enc}^{\mathrm{s}}_{E_2} E_1} \qquad \frac{x \lhd E_2}{x \lhd \mathsf{Enc}^{\mathrm{s}}_{E_2} E_1}$$

$$\frac{x \lhd E_1}{x \lhd \mathsf{Enc}^{\mathrm{a}}_{E_2} E_1} \qquad \frac{x \lhd E_2}{x \lhd \mathsf{Enc}^{\mathrm{a}}_{E_2} E_1} \qquad \frac{x \lhd E}{x \lhd \mathsf{op}(E)}\ \mathsf{op} \in \{\mathsf{pub}, \mathsf{priv}, \mathsf{H}\}$$

It is obvious that if $z \lhd E$ then $z \lhd E\sigma$.
We define also a measure $\sharp(E)$ on expressions:

$$\begin{array}{rll}
\sharp(a) := 0 & & \text{if } a \in \boldsymbol{N} \\
\sharp((E_1 \,.\, E_2)) := \sharp(E_1) + \sharp(E_2) & & \\
\sharp(\mathsf{Enc}^{\mathrm{s}}_{E_2} E_1) := \sharp(E_1) + \sharp(E_2) & & \\
\sharp(\mathsf{Enc}^{\mathrm{a}}_{E_2} E_1) := \sharp(E_1) + \sharp(E_2) & & \\
\sharp(\mathsf{op}(E)) := \sharp(E) & & \mathsf{op} \in \{\mathsf{pub}, \mathsf{priv}, \mathsf{H}\} \\
\sharp(\pi_1(E)) := 1 + \sharp(E) & & \text{if } E = (E_1 \,.\, E_2) \\
\qquad := \sharp(E) & & \text{otherwise} \\
\sharp(\pi_2(E)) := 1 + \sharp(E) & & \text{if } E = (E_1 \,.\, E_2) \\
\qquad := \sharp(E) & & \text{otherwise} \\
\sharp(\mathsf{Dec}^{\mathrm{s}}_F E) := 1 + \sharp(E) + \sharp(F) & & \text{if } E = \mathsf{Enc}^{\mathrm{s}}_{E_2} E_1 \\
\qquad := \sharp(E) + \sharp(F) & & \text{otherwise} \\
\sharp(\mathsf{Dec}^{\mathrm{a}}_F E) := 1 + \sharp(E) + \sharp(F) & & \text{if } E = \mathsf{Enc}^{\mathrm{a}}_{E_2} E_1 \\
\qquad := \sharp(E) + \sharp(F) & & \text{otherwise}
\end{array}$$

It is possible to show by a simple induction on E that

$$\forall E \in \boldsymbol{E} : \mathbf{e}_{\mathrm{a}}(E) = E \iff \sharp(E) = 0$$

Before showing the main result, we state and show several auxiliary results:

1. *If $\mathbf{e}_{\mathrm{c}}(E\sigma) \neq \bot$ and $z \lhd E$ then $z \in \mathrm{n}(\mathbf{e}_{\mathrm{c}}(E\sigma))$.*
   Proof. By a simple rule induction on $z \lhd E$.
2. *If $\mathbf{e}_{\mathrm{c}}(E\sigma) \neq \bot$, $z \in \mathrm{n}(E)$ and $\sharp(E) = 0$ then $z \lhd E$.*
   Proof. By induction on E
   - *$E = a \in \boldsymbol{N}$*
     Necessarily, $a = z$ thus $z \lhd E$.
   - *$E = (E_1 \,.\, E_2)$ and the result holds for E_1 and E_2*
     Clearly we have $\sharp(E_1) = \sharp(E_2) = 0$.
     Since $\mathrm{n}(E) = \mathrm{n}(E_1) \cup \mathrm{n}(E_2)$, we have $z \in \mathrm{n}(E_1)$ or $z \in \mathrm{n}(E_2)$.
     Moreover, since $\mathbf{e}_{\mathrm{c}}(E\sigma) \neq \bot$, we have necessarily $\mathbf{e}_{\mathrm{c}}(E_1\sigma) \neq \bot$ and $\mathbf{e}_{\mathrm{c}}(E_2\sigma) \neq \bot$.
     If $z \in \mathrm{n}(E_1)$ then by induction $z \lhd E_1$. Hence $z \lhd E$.
     If $z \in \mathrm{n}(E_2)$ then by induction $z \lhd E_2$. Hence $z \lhd E$.
     In both cases, we have $z \lhd E$.
   - *$E = \mathsf{Enc}^{\mathrm{s}}_{E_2} E_1$ or $E = \mathsf{Enc}^{\mathrm{a}}_{E_2} E_1$ and the result holds for E_1 and E_2*
     Similar to the case $E = (E_1 \,.\, E_2)$.
   - *$E = \mathsf{op}(F)$ (with $\mathsf{op} \in \{\mathsf{pub}, \mathsf{priv}, \mathsf{H}\}$) and the result holds for F*
     Trivial.
   - *$E = \pi_1\,(F)$ and the result holds for F*
     Since $\sharp(E) = 0$, we have $F \neq (F_1 \,.\, F_2)$ and $\sharp(F) = 0$.
     Since $\mathbf{e}_{\mathrm{c}}(E\sigma) \neq \bot$, we necessarily have $\mathbf{e}_{\mathrm{c}}(F\sigma) = (M_1 \,.\, M_2)$ for some $M_1, M_2 \in \boldsymbol{M}$ so $\mathbf{e}_{\mathrm{c}}(F\sigma) \neq \bot$.
     We have $\mathrm{n}(E) = \mathrm{n}(F)$ so $z \in \mathrm{n}(F)$.
     By induction, we have $z \lhd F$.
     By case analysis on $z \lhd F$ and since $\mathbf{e}_{\mathrm{c}}(F\sigma) = (M_1 \,.\, M_2)$ and $z \notin \mathrm{n}(\sigma)$, we have necessarily that $F = (F_1 \,.\, F_2)$ for some $F_1, F_2 \in \boldsymbol{E}$. This is a contradiction.
     This case is thus impossible.
   - *$E = \pi_2\,(F)$ and the result holds for F*
     Similar to the case $E = \pi_1\,(F)$
   - *$E = \mathsf{Dec}^{\mathrm{s}}_{G} F$ and the result holds for F and G*
     Since $\sharp(E) = 0$, we have $F \neq \mathsf{Enc}^{\mathrm{s}}_{F_2} F_1$, $\sharp(F) = 0$ and $\sharp(G) = 0$.
     Since $\mathbf{e}_{\mathrm{c}}(E\sigma) \neq \bot$, we have $\mathbf{e}_{\mathrm{c}}(F\sigma) = \mathsf{Enc}^{\mathrm{s}}_{M_2} M_1$ and $\mathbf{e}_{\mathrm{c}}(G\sigma) = M_2$ for some $M_1, M_2 \in \boldsymbol{M}$. Thus $\mathbf{e}_{\mathrm{c}}(F\sigma) \neq \bot$ and $\mathbf{e}_{\mathrm{c}}(G\sigma) \neq \bot$.
     Since $\mathrm{n}(E) = \mathrm{n}(F) \cup \mathrm{n}(G)$ we have $z \in \mathrm{n}(F)$ or $z \in \mathrm{n}(G)$.
     If $z \in \mathrm{n}(F)$, then by induction $z \lhd F$. By case analysis on $z \lhd F$ and since $\mathbf{e}_{\mathrm{c}}(F\sigma) = \mathsf{Enc}^{\mathrm{s}}_{M_2} M_1$ and $z \notin \mathrm{n}(\sigma)$, we necessarily have that $F = \mathsf{Enc}^{\mathrm{s}}_{F_2} F_1$ for some $F_1, F_2 \in \boldsymbol{E}$. This is a contradiction.
     So necessarily $z \in \mathrm{n}(G)$. By induction we have $z \lhd G$. Since $\mathbf{e}_{\mathrm{c}}(G\sigma) \neq \bot$ and $z \lhd G$ we have by (1) that $z \in \mathrm{n}(\mathbf{e}_{\mathrm{c}}(G\sigma)) = \mathrm{n}(M_2)$. So, since $\mathbf{e}_{\mathrm{c}}(F\sigma) = \mathsf{Enc}^{\mathrm{s}}_{M_2} M_1$, we have $z \in \mathrm{n}(\mathbf{e}_{\mathrm{c}}(F\sigma))$. Since $z \notin \mathrm{n}(\sigma)$, we necessarily have that $z \in \mathrm{n}(F)$. This leads to a contradiction.
     This case is thus impossible.

– $E = \mathsf{Dec}^{\mathrm{a}}_G F$ *and the result holds for* F *and* G
Similar to the case $E = \mathsf{Dec}^{\mathrm{s}}_G F$.

We can now show the main result.
Since $\mathbf{e}_{\mathrm{c}}(E\sigma) \neq \bot$, *there is* $M \in \boldsymbol{M}$ *such that* $\mathbf{e}_{\mathrm{c}}(E\sigma) = M$.
By Lemma 14, we have $\mathbf{e}_{\mathrm{c}}(\mathbf{e}_{\mathrm{a}}(E)\sigma) = M$. *Moreover by Corollary 2, we have* $\mathbf{e}_{\mathrm{a}}(\mathbf{e}_{\mathrm{a}}(E)) = \mathbf{e}_{\mathrm{a}}(E)$. *Thus* $\sharp(\mathbf{e}_{\mathrm{a}}(E)) = 0$.
So, since $z \in \mathrm{n}(\mathbf{e}_{\mathrm{a}}(E))$, *by (2) we get* $z \triangleleft \mathbf{e}_{\mathrm{a}}(E)$.
Then by (1) we get $z \in \mathrm{n}(\mathbf{e}_{\mathrm{c}}(\mathbf{e}_{\mathrm{a}}(E)\sigma)) = \mathrm{n}(M) = \mathrm{n}(\mathbf{e}_{\mathrm{c}}(E\sigma))$.

Concrete transitions

Lemma 16. *Let* $P \in \boldsymbol{P}$. *Assume that* $P \xrightarrow[S]{\mu} Q$ *and let* $\sigma : \boldsymbol{N} \to \boldsymbol{M}$ *a substitution such that* $\mathrm{n}(\mathrm{cosupp}(\sigma)) \cap \mathrm{bn}(\mu) = \emptyset$. *Then*

$$\forall x \in S : x\sigma \in \boldsymbol{N} \implies P\sigma \xrightarrow[S\sigma]{\mu\sigma} Q\sigma$$

Proof. By induction on $P \xrightarrow[S]{\mu} P'$.

If we are going to α*-rename* P, *we might as well consider that no names of* $\mathrm{n}(\sigma)$ *are bound in* P.

NC-Input *Assume that* $P = E(x).P' \xrightarrow[\{a\}]{a(x)} P'$ *with* $\mathbf{e}_{\mathrm{c}}(E) = a \in \boldsymbol{N}$.
By Lemma 7, we have $\mathbf{e}_{\mathrm{c}}(E\sigma) = a\sigma$. *Since* $a \in \{a\}$, *we have* $a\sigma \in \boldsymbol{N}$.
Thus by NC-Input, $P\sigma = E\sigma(x).P'\sigma \xrightarrow[\{a\sigma\}]{a\sigma(x)} P'\sigma$.

NC-Output *Assume that* $P = \overline{E}\langle F\rangle.P' \xrightarrow[\{a\}]{\overline{a}\,M} P'$ *with* $\mathbf{e}_{\mathrm{c}}(E) = a \in \boldsymbol{N}$ *and* $\mathbf{e}_{\mathrm{c}}(F) = M \in \boldsymbol{M}$.
By Lemma 7, we have $\mathbf{e}_{\mathrm{c}}(E\sigma) = a\sigma$ *and* $\mathbf{e}_{\mathrm{c}}(F\sigma) = M\sigma \in \boldsymbol{M}$. *By hypothesis,* $a\sigma \in \boldsymbol{N}$.
By NC-Output, $P\sigma = \overline{E\sigma}\langle F\sigma\rangle.P'\sigma \xrightarrow[\{a\sigma\}]{\overline{a\sigma}\,M\sigma} P'\sigma$.

NC-Guard *Assume that* $P = \phi P' \xrightarrow[\mathbf{nc}(\phi)\cup S]{\mu} P''$ *with* $P' \xrightarrow[S]{\mu} P''$ *and* $\mathbf{e}(\phi)$.
By induction, since $S \subseteq \mathbf{nc}(\phi) \cup S$, *we have* $P'\sigma \xrightarrow[S\sigma]{\mu\sigma} P''\sigma$.
By Lemma 8, we have $\mathbf{e}(\phi\sigma)$.
Thus by NC-Guard, $P\sigma = \phi\sigma P'\sigma \xrightarrow[\mathbf{nc}(\phi\sigma)\cup S\sigma]{\mu\sigma} P''\sigma$.
Still by Lemma 8, we have $\mathbf{nc}(\phi\sigma) = \mathbf{nc}(\phi)\sigma$ *so* $\mathbf{nc}(\phi\sigma)\cup S\sigma = (\mathbf{nc}(\phi)\cup S)\sigma$.

NC-Close-l *Assume that* $P = P_1 \mid P_2 \xrightarrow[S_1\cup S_2]{\tau} (\nu\tilde{z})\,(P_1'\{^{M}/_{x}\} \mid P_2') = Q$ *with* $P_1 \xrightarrow[S_1]{a(x)} P_1'$, $P_2 \xrightarrow[S_2]{(\nu\tilde{z})\,\overline{a}\,M} P_2'$ *and* $\{\tilde{z}\} \cap \mathrm{fn}(P_1) = \emptyset$. *We may assume that* $\{x, \tilde{z}\} \cap \mathrm{n}(\sigma) = \emptyset$.
By induction since $S_1 \subseteq S_1 \cup S_2$, *we have* $P_1\sigma \xrightarrow[S_1\sigma]{a\sigma(x)} P_1'\sigma$ *and since* $S_2 \subseteq S_1 \cup S_2$ *we have* $P_2\sigma \xrightarrow[S_2\sigma]{(\nu\tilde{z})\,\overline{a\sigma}\,M\sigma} P_2'\sigma$.

Since $\{\tilde{z}\} \cap \mathrm{fn}(P_1) = \emptyset$ *and* $\{\tilde{z}\} \cap \mathrm{n}(\sigma) = \emptyset$*, we have clearly that* $\{\tilde{z}\} \cap \mathrm{fn}(P_1\sigma) = \emptyset$.
Thus $P\sigma = P_1\sigma \mid P_2\sigma \xrightarrow[S_1\sigma \cup S_2\sigma]{\tau} (\nu\tilde{z})\,(P_1'\sigma\{^{M\sigma}/_x\} \mid P_2'\sigma) = Q'$ *by* NC-Close-L.
Since $x \notin \mathrm{n}(\sigma)$*, we have* $P_1'\sigma\{^{M\sigma}/_x\} = P_1'\{^{M}/_x\}\sigma$*. So* $Q' = Q\sigma$.

NC-Open *Assume that* $P = (\nu z')\,P' \xrightarrow[S\setminus\{z'\}]{(\nu z'\tilde{z})\,\overline{a}\,M} P''$ *with* $P' \xrightarrow[S]{(\nu\tilde{z})\,\overline{a}\,M} P''$ *and* $z' \in \mathrm{n}(M) \setminus \{a, \tilde{z}\}$.
Since $z' \notin \mathrm{n}(\sigma)$*, we have* $z'\sigma = z'$*. So if* $x \in S$*, then* $x\sigma \in \boldsymbol{N}$.
By induction, we thus have $P'\sigma \xrightarrow[S\sigma]{(\nu\tilde{z})\,\overline{a\sigma}\,M\sigma} P''\sigma$.
Since $z' \in \mathrm{n}(M)$ *and* $z' \notin \mathrm{n}(\sigma)$*, we have* $z' \in \mathrm{n}(M\sigma)$*. Since* $z' \neq a$*, we have* $z' \neq a\sigma$*. And we still have* $z' \notin \{\tilde{z}\}$.
So by NC-Open*, we have* $P\sigma \xrightarrow[S\sigma\setminus\{z'\}]{(\nu z'\tilde{z})\,\overline{a\sigma}\,M\sigma} P''\sigma$.
But $S\sigma \setminus \{z'\} = (S \setminus \{z'\})\sigma$ *since* $z' \notin \mathrm{n}(\sigma)$.

NC-Res *Assume that* $P = (\nu z)\,P' \xrightarrow[S\setminus\{z\}]{\mu} (\nu z)\,P'' = Q$ *with* $P' \xrightarrow[S]{\mu} P''$ *and* $z \notin \mathrm{n}(\mu)$.
Since $z \notin \mathrm{n}(\sigma)$*, it is obvious that if* $x \in S$ *then* $x\sigma \in \boldsymbol{N}$.
By induction, we thus have $P'\sigma \xrightarrow[S\sigma]{\mu\sigma} P''\sigma$.
Since $z \notin \mathrm{n}(\mu)$ *and* $z \notin \mathrm{n}(\sigma)$*, we have* $z \notin \mathrm{n}(\mu\sigma)$.
By NC-Res*, we thus have* $P\sigma = (\nu z)\,P'\sigma \xrightarrow[S\sigma\setminus\{z\}]{\mu\sigma} (\nu z)\,P''\sigma = Q\sigma$.
Since $z \notin \mathrm{n}(\sigma)$*, we have* $S\sigma \setminus \{z\} = (S \setminus \{z\})\sigma$.

Lemma 17. *Let* $P, Q \in \boldsymbol{P}$ *and assume that* $P >_{\mathrm{o}} Q$.

1. *if* $P \xrightarrow[S]{\mu} P'$ *then* $Q \xrightarrow[S]{\mu} Q'$ *and* $P' >_{\mathrm{o}} Q'$
2. *if* $Q \xrightarrow[S]{\mu} Q'$ *and* $\mathrm{bn}(\mu) \cap \mathrm{fn}(P) = \emptyset$ *then* $P \xrightarrow[S]{\mu} P'$ *and* $P' >_{\mathrm{o}} Q'$

Proof.

1. *By rule induction on* $P \xrightarrow[S]{\mu} P'$*. We give the proof for the following cases:*

NC-Input *Assume that* $P = E(x).P' \xrightarrow[\{a\}]{a(x)} P'$ *where* $\mathbf{e}_{\mathrm{c}}(E) = a \in \boldsymbol{N}$.
Since $P >_{\mathrm{o}} Q$*, we have* $Q \equiv_\alpha F(x).Q'$ *with* $E >_{\mathrm{o}} F$ *and* $P' >_{\mathrm{o}} Q'$.
By Lemma 10, we have $\mathbf{e}_{\mathrm{c}}(F) = a$.
Thus, by NC-Alpha *and* NC-Input*,* $Q \equiv_\alpha F(x).Q' \xrightarrow[\{a\}]{a(x)} Q'$ *and* $P' >_{\mathrm{o}} Q'$.

NC-Output *Assume that* $P = \overline{E_1}\langle E_2\rangle.P' \xrightarrow[\{a\}]{\overline{a}\,M} P'$ *with* $\mathbf{e}_{\mathrm{c}}(E_1) = a \in \boldsymbol{N}$ *and* $\mathbf{e}_{\mathrm{c}}(E_2) = M \in \boldsymbol{M}$.
Since $P >_{\mathrm{o}} Q$*, we have* $Q = \overline{F_1}\langle F_2\rangle.Q'$ *with* $E_1 >_{\mathrm{o}} F_1$*,* $E_2 >_{\mathrm{o}} F_2$ *and* $P' >_{\mathrm{o}} Q'$.
By Lemma 10, we have $\mathbf{e}_{\mathrm{c}}(F_1) = a$ *and* $\mathbf{e}_{\mathrm{c}}(F_2) = M$.
Thus, by NC-Output*,* $Q = \overline{F_1}\langle F_2\rangle.Q' \xrightarrow[\{a\}]{\overline{a}\,M} Q'$ *and* $P' >_{\mathrm{o}} Q'$.

NC-Close-L *Assume that* $P = P_1 \mid P_2$ *with* $P_1 \xrightarrow[S]{a(x)} P_1'$, $P_2 \xrightarrow[S']{(\nu\tilde{z})\,\overline{a}\,M} P_2'$, $\{\tilde{z}\}\cap\mathrm{fn}(P_1) = \emptyset$ *and* $P \xrightarrow[S\cup S']{\tau} (\nu\tilde{z})\,(P_1'\{^M/_x\} \mid P_2') = P'$.
Since $P >_\mathrm{o} Q$, *we have* $Q = Q_1 \mid Q_2$ *with* $P_1 >_\mathrm{o} Q_1$ *and* $P_2 >_\mathrm{o} Q_2$.
By induction, we have $Q_1 \xrightarrow[S]{a(x)} Q_1'$ *and* $Q_2 \xrightarrow[Q]{(\nu\tilde{z})\,\overline{a}\,M}{}'_2$ *with* $P_1' >_\mathrm{o} Q_1'$ *and* $P_2' >_\mathrm{o} Q_2'$.
Since $P_1 >_\mathrm{o} Q_1$ *we have* $\mathrm{fn}(Q_1) \subseteq \mathrm{fn}(P_1)$ *so* $\{\tilde{z}\} \cap \mathrm{fn}(Q_1) = \emptyset$.
Thus, by NC-Close-L, *we have*
$$Q = Q_1 \mid Q_2 \xrightarrow[S\cup S']{\tau} (\nu\tilde{z})\,(Q_1'\{^M/_x\} \mid Q_2') = Q'.$$
Since $P_1' >_\mathrm{o} Q_1'$ *and* $M \in \boldsymbol{M}$, *we have* $P_1'\{^M/_x\} >_\mathrm{o} Q_1'\{^M/_x\}$.
So $P' >_\mathrm{o} Q'$.

NC-Guard *Assume that* $P = \phi P_1$ *with* $P_1 \xrightarrow[S]{\mu} P'$, $\mathbf{e}(\phi)$ *and* $P = \phi P_1 \xrightarrow[S\cup\mathbf{nc}(\phi)]{\mu} P'$.
Since $P >_\mathrm{o} Q$, *we have* $Q = \psi Q_1$ *with* $\phi >_\mathrm{o} \psi$ *and* $P_1 >_\mathrm{o} Q_1$.
By induction, $Q_1 \xrightarrow[S]{\mu} Q'$.
By Corollary 1, we have $\mathbf{e}(\psi)$.
Thus, by NC-Guard, *we have* $Q = \psi Q_1 \xrightarrow[S\cup\mathbf{nc}(\psi)]{\mu} Q'$.
Again by Corollary 1, we have $\mathbf{nc}(\psi) = \mathbf{nc}(\phi)$ *so* $Q \xrightarrow[S\cup\mathbf{nc}(\phi)]{\mu} Q'$ *and* $P' >_\mathrm{o} Q'$.

NC-Par-L *Assume that* $P = P_1 \mid P_2$ *with* $P_1 \xrightarrow[S]{\mu} P_1'$, $\mathrm{bn}(\mu) \cap \mathrm{fn}(P_2) = \emptyset$ *and* $P \xrightarrow[S]{\mu} P' = P_1' \mid P_2$.
Since $P >_\mathrm{o} Q$, *we have* $Q = Q_1 \mid Q_2$ *with* $P_1 >_\mathrm{o} Q_1$ *and* $P_2 >_\mathrm{o} Q_2$.
By induction, we have $Q_1 \xrightarrow[S]{\mu} Q_1'$ *with* $P_1' >_\mathrm{o} Q_1'$.
Since $P_2 >_\mathrm{o} Q_2$, *we have* $\mathrm{fn}(Q_2) \subseteq \mathrm{fn}(P_2)$. *Hence* $\mathrm{bn}(\mu) \cap \mathrm{fn}(Q_2) = \emptyset$.
Thus, by NC-Par-L, *we have* $Q = Q_1 \mid Q_2 \xrightarrow[S]{\mu} Q_1' \mid Q_2 = Q'$.
Since $P_1' >_\mathrm{o} Q_1'$ *and* $P_2 >_\mathrm{o} Q_2$, *we have* $P' >_\mathrm{o} Q'$.

2. By rule induction on $P \xrightarrow[S]{\mu} P'$. *We give the proof for the following cases:*

NC-Input *Assume that* $Q = F(x).Q' \xrightarrow[\{a\}]{a(x)} Q'$ *with* $\mathbf{e}_\mathrm{c}(F) = a \in \boldsymbol{N}$.
Since $P >_\mathrm{o} Q$, *we have* $P \equiv_\alpha E(x).P'$ *with* $E >_\mathrm{o} F$ *and* $P' >_\mathrm{o} Q'$.
By Lemma 10, we have $\mathbf{e}_\mathrm{c}(E) = a$.
So, by NC-Alpha *and* NC-Input, *we have* $P \equiv_\alpha E(x).P' \xrightarrow[\{a\}]{a(x)} P'$ *and* $P' >_\mathrm{o} Q'$.

NC-Close-L *Assume that* $Q = Q_1 \mid Q_2$ *with* $Q_1 \xrightarrow[S]{a(x)} Q_1'$, $Q_2 \xrightarrow[S']{(\nu\tilde{z})\,\overline{a}\,M} Q_2'$, $\{\tilde{z}\} \cap \mathrm{fn}(Q_1) = \emptyset$ *and* $Q \xrightarrow[S\cup S']{\tau} (\nu\tilde{z})\,(Q_1'\{^M/_x\} \mid Q_2') = Q'$. *We may assume that* $\{x, \tilde{z}\} \cap \mathrm{fn}(P) = \emptyset$.
Since $P >_\mathrm{o} Q$, *we have* $P = P_1 \mid P_2$ *with* $P_1 >_\mathrm{o} Q_1$ *and* $P_2 >_\mathrm{o} Q_2$.
By induction, we have $P_1 \xrightarrow[S]{a(x)} P_1'$ *and* $P_2 \xrightarrow[S']{(\nu\tilde{z})\,\overline{a}\,M} P_2'$ *with* $P_1' >_\mathrm{o} Q_1'$ *and* $P_2' >_\mathrm{o} Q_2'$.

So by NC-Close-L, *we have*
$$P = P_1 \mid P_2 \xrightarrow[S \cup S']{\tau} (\nu \tilde{z})\,(P_1'\{^M/_x\} \mid P_2') = P'.$$
Since $P_1' >_{\mathrm{o}} Q_1'$ *and* $M \in \boldsymbol{M}$, *we have* $P_1'\{^M/_x\} >_{\mathrm{o}} Q_1'\{^M/_x\}$ *so* $P' >_{\mathrm{o}} Q'$.

NC-Par-L *Assume that* $Q = Q_1 \mid Q_2$ *with* $Q_1 \xrightarrow[S]{\mu} Q_1'$, $\mathrm{bn}(\mu) \cap \mathrm{fn}(Q_2) = \emptyset$ *and* $Q \xrightarrow[S]{\mu} Q' = Q_1' \mid Q_2$.
Since $P >_{\mathrm{o}} Q$, *we have* $P = P_1 \mid P_2$ *with* $P_1 >_{\mathrm{o}} Q_1$ *and* $P_2 >_{\mathrm{o}} Q_2$.
Since $\mathrm{bn}(\mu) \cap \mathrm{fn}(P) = \emptyset$, *we have* $\mathrm{bn}(\mu) \cap \mathrm{fn}(P_1) = \mathrm{bn}(\mu) \cap \mathrm{fn}(P_2) = \emptyset$.
By induction, $P_1 \xrightarrow[S]{\mu} P_1'$ *with* $P_1' >_{\mathrm{o}} Q_1'$.
Thus by NC-Par-L, $P = P_1 \mid P_2 \xrightarrow[S]{\mu} P_1' \mid P_2 = P'$.
Since $P_1' >_{\mathrm{o}} Q_1'$ *and* $P_2 >_{\mathrm{o}} Q_2$, *we have* $P' >_{\mathrm{o}} Q'$.

S-environments

Lemma 18. *Let* (σ, ρ) *be a pair of substitutions,* $B \subseteq \boldsymbol{N} \times \boldsymbol{N}$ *a consistent hedge and* $\mathsf{se} = (h, v, \prec, (\gamma_l, \gamma_r))$ *a S-environment such that* $(\sigma, \rho) \triangleright_B \mathsf{se}$. *If* se *is well-formed then* $\mathsf{se}_B^{(\sigma,\rho)}$ *is well-formed.*

Proof. *We note* $\mathsf{se}_B^{(\sigma,\rho)} = (h', v', \prec', (\gamma_l', \gamma_r'))$.

1. *By contradiction, assume that* $x \in \pi_1(h') \cap \pi_1(v')$.
   By definition of h', *there is* $M \in \pi_1(h)$ *such that* $x = M\sigma$. *Since* $x \in \boldsymbol{N}$, *necessarily* $M = a \in \boldsymbol{N}$.
   Since $\pi_1(h) \cap \pi_1(v) = \emptyset$ *and* $\mathrm{supp}(\sigma) \subseteq \pi_1(v)$, *we have* $x = M\sigma = a\sigma = a$ *because* $a \notin \mathrm{supp}(\sigma)$.
   We have thus $a \in \mathrm{n}(\pi_1(h))$, $a \notin \pi_1(v)$ *and* $a \in \pi_1(B)$. *This is a contradiction.*
   So $\pi_1(h') \cap \pi_1(v') = \emptyset$.
2. *Similarly* $\pi_2(h') \cap \pi_2(v') = \emptyset$.
3. *Assume that* $(M\sigma, N\rho) \prec' (x', y')$ *with* $(M, N) \in h$ *and* $(x', y') \in v'$.
   By contradiction, assume that $x' \in \mathrm{n}(M\sigma)$. *Necessarily, there exists* $(x, y) \in v$ *such that* $x \in \mathrm{n}(M)$ *and* $x' \in \mathrm{n}(x\sigma)$. *So we have* $(M, N) \prec (x, y)$. *This is a contradiction with* $x \notin \mathrm{n}(M)$. *So* $x' \notin \mathrm{n}(M\sigma)$.
   Similarly, $y' \notin \mathrm{n}(N\rho)$.

Lemma 19. *Let* (σ, ρ) *be a pair of substitutions,* $B \subseteq \boldsymbol{N} \times \boldsymbol{N}$ *a consistent hedge and* $\mathsf{se} = (h, v, \prec, (\gamma_l, \gamma_r))$ *a S-environment such that* $(\sigma, \rho) \triangleright_B \mathsf{se}$. *If* se *is growing then* $\mathsf{se}_B^{(\sigma,\rho)}$ *is growing.*

Proof. *We write* $v = \{(x_1, y_1), \ldots, (x_n, y_n)\}$ *and* $h_i = \mathsf{se}|_{(x_i, y_i)}$ *and assume that for all* $1 \leq i < n$, *we have* $h_i \subseteq h_{i+1}$.

We note $\mathsf{se}_B^{(\sigma,\rho)} = (h', v', \prec', (\gamma_l', \gamma_r'))$.

By definition, we have $(M, N) \prec (x_i, y_i) \iff (M, N) \in h_i$ *for* $(M, N) \in h$ *and* $1 \leq i \leq n$.

Let $(x', y') \in v'$ *and* $(M', N') \in h'$. *We have* $M' = M\sigma$ *and* $N' = N\rho$ *for* $(M, N) \in h$.

By definition, we have

$$\begin{aligned}(M',N') \prec' (x',y') &\iff \bigwedge_{\substack{(x,y)\in v\\ x'\in \mathrm{n}(x\sigma)\vee y'\in \mathrm{n}(y\rho)}} (M,N)\prec (x,y)\\ &\iff \bigwedge_{\substack{1\le i\le n\\ x'\in \mathrm{n}(x_i\sigma)\vee y'\in \mathrm{n}(y_i\rho)}} (M,N)\prec (x_i,y_i)\\ &\iff \bigwedge_{\substack{1\le i\le n\\ x'\in \mathrm{n}(x_i\sigma)\vee y'\in \mathrm{n}(y_i\rho)}} (M,N)\in h_i\end{aligned}$$

Moreover, we know that if $(x',y') \in v' = B$, *we have* $x' \in \mathrm{n}(\sigma(\pi_1(v)))$ *or* $y' \in \mathrm{n}(\sigma(\pi_2(v)))$, *so* $A_{(x',y')} := \{1 \le i \le n \mid x' \in \mathrm{n}(x_i\sigma) \vee y' \in \mathrm{n}(y_i\rho)\} \neq \emptyset$. *Since* $A_{(x',y')}$ *is a non empty subset of* $\mathbb{N}$, *its minimum element exists. We thus define* $idx((x',y')) := \min A_{(x',y')}$.

Since we have $h_1 \subseteq h_2 \subseteq \cdots \subseteq h_n$, *we have*

$$(M',N') \prec' (x',y') \iff (M,N) \in h_{idx((x',y'))}$$

for every $(M,N) \in h$, $(x',y') \in v'$, $M' = M\sigma$ *and* $N' = N\rho$.

We sort the elements $(x',y') \in v'$ *according to the value of* $idx((x',y'))$, *i.e. let* $z : [\![1,k]\!] \to v'$ *injective where* $k := \mathrm{card}(v')$ *such that if* $i \le j$ *then* $idx(z(i)) \le idx(z(j))$.

For $1 \le i \le k$, *we define*

$$\begin{aligned}h'_i := \mathsf{se}_B^{(\sigma,\rho)}|_{z(i)} &= \{(M',N') \in h' \mid (M',N') \prec' z(i)\}\\ &= \{(M\sigma,N\rho) \mid (M,N) \in h \wedge (M,N) \in h_{idx(z(i))}\}\\ &= h_{idx(z(i))}(\sigma,\rho)\end{aligned}$$

Thus since $h_1 \subseteq h_2 \subseteq \cdots \subseteq h_n$, *we have for* $1 \le i < k$ *that* $h'_i \subseteq h'_{i+1}$.

Hence $\mathsf{se}_B^{(\sigma,\rho)}$ *is growing.*

Lemma 20. *Let* (σ,ρ) *be a pair of substitutions,* $B \subseteq \boldsymbol{N}\times\boldsymbol{N}$ *a consistent hedge and* $\mathsf{se} = (h, v, \prec, (\gamma_l,\gamma_r))$ *a S-environment such that* $(\sigma,\rho) \triangleright_B \mathsf{se}$. *Then if* se *is well-formed and growing we have*

$$\forall (b1,b2) \in B : b_1 \in \mathrm{n}(\sigma(\pi_1(v))) \wedge b_2 \in \mathrm{n}(\rho(\pi_2(v)))$$

.

Proof. We write $v = \{(x_1,y_1),\ldots,(x_n,y_n)\}$ *such that if* $h_i := \mathsf{se}|_{(x_i,y_i)}$ *then* $h_i \subseteq h_{i+1}$ *for* $1 \le i < n$.

By contradiction, assume that there is $(b_1,b_2) \in B$ *such that* $b_1 \notin \mathrm{n}(\sigma(\pi_1(v)))$ *or* $b_2 \notin \mathrm{n}(\rho(\pi_2(v)))$.

By symmetry, assume for example that $b_2 \notin \mathrm{n}(\rho(\pi_2(v)))$. *By hypothesis, we have then that* $b_1 \in \mathrm{n}(\sigma(\pi_1(v)))$.

Let i_0 *minimal such that* $b_1 \in \mathrm{n}(x_{i_0}\sigma)$. *We have* $b_2 \notin \mathrm{n}(y_{i_0}\rho)$.

By hypothesis, we have $(x_{i_0}\sigma, y_{i_0}\rho) \in \mathcal{S}(\mathcal{I}(h_{i_0}(\sigma,\rho) \cup B))$.

Since $b_2 \notin \mathrm{n}(y_{i_0}\rho)$, Syn-Inc *have not been applied with* (b_1, b_2) *as premise. So necessarily, there is* $(M, N) \in h_{i_0}$ *such that* $b_1 \in \mathrm{n}(M\sigma)$. *Since* $\pi_1(B) \cap (\mathrm{n}(\pi_1(h)) \setminus \pi_1(v)) = \emptyset$, *there exists* j *such that* $x_j \in \mathrm{n}(M)$ *and* $b_1 \in \mathrm{n}(x_j\sigma)$. *By choice of* i_0, *we have* $i_0 \leq j$ *so* $h_{i_0} \subseteq h_j$.

Since $(M, N) \in h_{i_0} \subseteq h_j$, *we have* $(M, N) \prec (x_j, y_j)$.

Since se *is well-formed, we have* $x_j \notin \mathrm{n}(M)$. *This is a contradiction.*

This even proves that if $(b_1, b_2) \in B$ *and* i *is minimal such that* $b_1 \in \mathrm{n}(x_i\sigma)$ *then necessarily* $b_2 \in \mathrm{n}(y_i\sigma)$ *(this result will be used afterwards).*

Lemma 21. *Let* $h \in \boldsymbol{H}$ *and* $\{(x_1, y_1), \ldots, (x_n, y_n)\} \subseteq \boldsymbol{N} \times \boldsymbol{N}$.

Let also $(M_1, N_1), \ldots, (M_n, N_n) \in \boldsymbol{M} \times \boldsymbol{M}$ *and* $B \subseteq \boldsymbol{N} \times \boldsymbol{N}$ *such that*

$$\forall 1 \leq i \leq n : (M_i, N_i) \in \mathcal{S}(\mathcal{A}(h(\sigma,\rho) \cup B))$$

where σ *and* ρ *are defined such that*

$$x\sigma := \begin{cases} M_i & \text{if } x = x_i \\ x & \text{otherwise} \end{cases} \qquad y\rho := \begin{cases} N_i & \text{if } y = y_i \\ y & \text{otherwise} \end{cases}$$

Then

$$\forall (M, N) \in \mathcal{S}(\mathcal{A}(h \cup \{(x_1, y_1), \ldots, (x_n, y_n)\})) : \\ (M\sigma, N\rho) \in \mathcal{S}(\mathcal{A}(h(\sigma,\rho) \cup B))$$

Proof. *We use a characterisation of analysis and actually show that*

$$\forall i \in \mathbb{N} : \forall (M, N) \in \mathcal{S}(\mathrm{analz}^i(h \cup \{(x_1, y_1), \ldots, (x_n, y_n)\})) : \\ (M\sigma, N\rho) \in \mathcal{S}(\mathcal{A}(h(\sigma,\rho) \cup B))$$

Before showing this result, we show some auxiliary results.

1. *Let* $h' \in \boldsymbol{H}$ *such that*

   $$\forall (M, N) \in h' : (M\sigma, N\rho) \in \mathcal{S}(\mathcal{A}(h(\sigma,\rho) \cup B))$$

   Then

   $$\forall (M, N) \in \mathcal{S}(h') : (M\sigma, N\rho) \in \mathcal{S}(\mathcal{A}(h(\sigma,\rho) \cup B))$$

   Proof. *We show this result by rule induction on* $(M, N) \in \mathcal{S}(h')$. *The hypothesis gives the base case and the inductive cases are then obvious.*

2. *Let* $h' \in \boldsymbol{H}$ *such that*

   $$\forall (M, N) \in h' : (M\sigma, N\rho) \in \mathcal{S}(\mathcal{A}(h(\sigma,\rho) \cup B))$$

   then

   $$\forall (M, N) \in \mathrm{analz}(h') : (M\sigma, N\rho) \in \mathcal{S}(\mathcal{A}(h(\sigma,\rho) \cup B))$$

Proof. Again, we show this result by rule induction on $(M, N) \in \text{analz}(h')$.

- *If* $(M, N) \in \text{analz}(h')$ *by* Ana-Inc. *Then* $(M, N) \in h'$ *and the hypothesis gives the result.*
- *Assume that* $(M, N) \in \text{analz}(h')$ *by* Ana-Dec-a. *That means that* $(\mathsf{Enc}^{\mathrm{a}}_K M, \mathsf{Enc}^{\mathrm{a}}_L N) \in \text{analz}(h')$ *with* $K' = \mathsf{inv}(K) \in \boldsymbol{M}$, $L' = \mathsf{inv}(L) \in \boldsymbol{M}$ *and* $(K', L') \in \mathcal{S}(h')$.
  By induction, $(\mathsf{Enc}^{\mathrm{a}}_{K\sigma} M\sigma, \mathsf{Enc}^{\mathrm{a}}_{L\rho} N\rho) \in \mathcal{S}(\mathcal{A}(h(\sigma, \rho) \cup B))$.
  Either it was deduced by Syn-Inc *or by* Syn-Enc-a.
  - *(a) If it was by* Syn-Inc*:*
    Then $(\mathsf{Enc}^{\mathrm{a}}_{K\sigma} M\sigma, \mathsf{Enc}^{\mathrm{a}}_{L\rho} N\rho) \in \mathcal{A}(h(\sigma, \rho) \cup B)$.
    Trivially, $\mathsf{inv}(K\sigma) = K'\sigma \in \boldsymbol{M}$, $\mathsf{inv}(L\sigma) = L'\sigma \in \boldsymbol{M}$.
    According to the previous auxiliary result and since h' *satisfies the premise, we have* $(K'\sigma, L'\rho) \in \mathcal{S}(\mathcal{A}(h(\sigma, \rho) \cup B))$.
    By definition of analysis, we have $\text{analz}(\mathcal{A}(h(\sigma, \rho) \cup B)) = \mathcal{A}(h(\sigma, \rho) \cup B)$.
    So by Ana-Dec-a $(M\sigma, N\rho) \in \mathcal{A}(h(\sigma, \rho) \cup B)$.
    Thus by Syn-Inc*, we have* $(M\sigma, N\rho) \in \mathcal{S}(\mathcal{A}(h(\sigma, \rho) \cup B))$.
  - *(b) Otherwise, it was by* Syn-Enc-a *and then immediately, we have* $(M\sigma, N\rho) \in \mathcal{S}(\mathcal{A}(h(\sigma, \rho) \cup B))$.

We show now that

$$\forall i \in \mathbb{N} : \forall (M, N) \in \text{analz}^i(h \cup \{(x_1, y_1), \ldots, (x_n, y_n)\}) : \\ (M\sigma, N\rho) \in \mathcal{S}(\mathcal{A}(h(\sigma, \rho) \cup B))$$

By induction on i.

- $i = 0$
  We have by definition

$$\text{analz}^0(h \cup \{(x_1, y_1), \ldots, (x_n, y_n)\}) = h \cup \{(x_1, y_1), \ldots, (x_n, y_n)\}$$

  If $(M, N) \in h$, *then by definition,* $(M\sigma, N\rho) \in h(\sigma, \rho)$. *So by definition of the synthesis,* $(M\sigma, N\rho) \in \mathcal{S}(\mathcal{A}(h(\sigma, \rho) \cup B))$.
  If $(M, N) = (x_i, y_i)$ *for some* $1 \leq i \leq n$. *Then* $(M\sigma, N\rho) = (M_i, N_i) \in \mathcal{S}(\mathcal{A}(h(\sigma, \rho) \cup B))$ *by hypothesis.*
- *Assume the result holds for some* $i \in \mathbb{N}$.
  Then the second auxiliary lemma gives the result for $i{+}1$ *because* $\text{analz}(\text{analz}^i(h)) = \text{analz}^{i+1}(h)$.

Then by the first auxiliary result, we obtain

$$\forall i \in \mathbb{N} : \forall (M, N) \in \mathcal{S}(\text{analz}^i(h \cup \{(x_1, y_1), \ldots, (x_n, y_n)\})) : \\ (M\sigma, N\rho) \in \mathcal{S}(\mathcal{A}(h(\sigma, \rho) \cup B))$$

This completes the proof.

Theorem 5 (respectful substitutions composition). *Let $\mathsf{se} = (h, v, \prec, (\gamma_l, \gamma_r))$ a S-environment. We assume that se is well-formed and growing.*

Let (σ_1, ρ_1) be a pair of substitutions and $B_1 \subseteq \boldsymbol{N} \times \boldsymbol{N}$ a consistent hedge such that $(\sigma_1, \rho_1) \triangleright_{B_1} \mathsf{se}$. We note $\mathsf{se}_1 := \mathsf{se}_{B_1}^{(\sigma_1,\rho_1)}$.

Let (σ_2, ρ_2) be a pair of substitutions and $B_2 \subseteq \boldsymbol{N} \times \boldsymbol{N}$ a consistent hedge such that $(\sigma_2, \rho_2) \triangleright_{B_2} \mathsf{se}_1$. We note $\mathsf{se}_2 := \mathsf{se}_1{}_{B_2}^{(\sigma_2,\rho_2)}$.

Then $(\sigma, \rho) \triangleright_{B_2} \mathsf{se}$ and $\mathsf{se}_{B_2}^{(\sigma,\rho)} = \mathsf{se}_2$ where σ and ρ are defined such that

$$x\sigma := \begin{cases} x\sigma_1\sigma_2 & \text{if } x \in \pi_1(v) \\ x & \text{otherwise} \end{cases} \qquad y\rho := \begin{cases} y\rho_1\rho_2 & \text{if } y \in \pi_2(v) \\ y & \text{otherwise} \end{cases}$$

Proof. First, by Lemma 18 and by Lemma 19, we know that both se_1 and se_2 are well-formed and growing.

1. *By definition, we have* $\mathrm{supp}(\sigma) \subseteq \pi_1(v)$.
2. *Similarly,* $\mathrm{supp}(\rho) \subseteq \pi_2(v)$.
3. *Let $(b_1, b_2) \in B_2$. By Lemma 20, we have $b_1 \in \mathrm{n}(\sigma_2(\pi_1(B_1)))$. So, there exists $(a_1, a_2) \in B_1$ such that $b_1 \in \mathrm{n}(a_1\sigma_2)$.*
   By Lemma 20, we have $a_1 \in \mathrm{n}(\sigma_1(\pi_1(v)))$. So, there exists $(x, y) \in v$ such that $a_1 \in \mathrm{n}(x\sigma_1)$.
   Then $b_1 \in \mathrm{n}(x\sigma_1\sigma_2) = \mathrm{n}(x\sigma)$.
4. *By contradiction, assume that there exists $b_1 \in \pi_1(B_2) \cap (\mathrm{n}(\pi_1(h)) \setminus \pi_1(v))$.*
   By hypothesis, we have $b_1 \notin \mathrm{n}(\pi_1(h(\sigma_1, \rho_1)))$ or $b_1 \in \pi_1(B_1)$.
   If $b_1 \in \pi_1(B_1)$ then $b_1 \notin (\mathrm{n}(\pi_1(h)) \setminus \pi_1(v))$.
   So necessarily, $b_1 \notin \mathrm{n}(\pi_1(h(\sigma_1, \rho_1)))$. But since $b_1 \in \mathrm{n}(\pi_1(h))$ and $b_1 \notin \pi_1(v)$ and $\mathrm{supp}(\sigma_1) \subseteq \pi_1(v)$, we have $b_1 \in \mathrm{n}(\pi_1(h(\sigma_1, \rho_1)))$. This is a contradiction.
   So $\pi_1(B_2) \cap (\mathrm{n}(\pi_1(h)) \setminus \pi_1(v)) = \emptyset$.
5. *Similarly $\pi_2(B_2) \cap (\mathrm{n}(\pi_2(h)) \setminus \pi_2(v)) = \emptyset$.*
6. *We first prove that $h(\sigma_1, \rho_1)(\sigma_2, \rho_2) = h(\sigma, \rho)$, i.e. we show that for every $(M, N) \in h$, $(M\sigma_1\sigma_2, N\rho_1\rho_2) = (M\sigma, N\rho)$.*
   Let $(M, N) \in h$. We show that $M\sigma_1\sigma_2 = M\sigma$.
   Let $x \in \mathrm{n}(M)$. We have $x \in \pi_1(h)$. If $x \in \pi_1(v)$, then $x\sigma_1\sigma_2 = x\sigma$. Otherwise, if $x \notin \pi_1(v)$, then we have by hypothesis that $x \notin \pi_1(B_1)$. Moreover, since $\mathrm{supp}(\sigma_1) \subseteq \pi_1(v)$, we have $x\sigma_1 = x$. And since $\mathrm{supp}(\sigma_2) \subseteq \pi_1(B_1)$, we have $x\sigma_2 = x$. Thus $x\sigma_1\sigma_2 = x = x\sigma$. So for every name x of M, we have $x\sigma_1\sigma_2 = x\sigma$. So a simple induction on M shows that $M\sigma_1\sigma_2 = M\sigma$.
   Thus $h(\sigma_1, \rho_1)(\sigma_2, \rho_2) = h(\sigma, \rho)$.
   We write $v = \{(x_1, y_1), \ldots, (x_n, y_n)\}$ such that if $h_i = \mathsf{se}|_{(x_i,y_i)}$, then for $1 \leq i < n$, we have $h_i \subseteq h_{i+1}$.
   Let $1 \leq i \leq n$.
   We have by hypothesis $(x_i\sigma_1, y_i\rho_1) \in \mathcal{S}(\mathcal{I}(h_i(\sigma_1, \rho_1) \cup B_1))$.
   Let $B_1^i := \{(b_1, b_2) \in B_1 \mid \exists j \leq i : b_1 \in \mathrm{n}(x_j\sigma_1) \vee b_2 \in \mathrm{n}(y_j\rho_1)\}$. We have $B_1 = B_1^i \cup (B_1 \setminus B_1^i)$.
   Let $(b_1, b_2) \in B_1$ such that $b_1 \in \mathrm{n}(\pi_1(h_i(\sigma_1, \rho_1)))$. By definition, there exists $(M, N) \in h_i$ such that $b_1 \in \mathrm{n}(M\sigma_1)$. This implies that there exists j such that $x_j \in \mathrm{n}(M)$ and $b_1 \in \mathrm{n}(x_j\sigma_1)$. If $j \geq i$, then since se is growing, we have

$(M,N) \prec (x_j,y_j)$. *But since* se *is well-formed, we have* $x_j \notin \mathrm{n}(M)$. *This is a contradiction. Thus* $j < i$ *and* $(b_1,b_2) \in B_1^i$.
Similarly if $(b_1,b_2) \in B_1$ *is such that* $b_2 \in \mathrm{n}(\pi_2(h_i(\sigma_1,\rho_1)))$ *then* $(b_1,b_2) \in B_1^i$.
This proves that the useful names of B_1 *to compute the analysis* $\mathcal{A}(h_i(\sigma_1,\rho_1) \cup B_1)$ *are included in* B_1^i.
In other words, we have just proven that $\mathcal{S}(\mathcal{I}(h_i(\sigma_1,\rho_1) \cup B_1)) = \mathcal{S}(\mathcal{I}(h_i(\sigma_1,\rho_1) \cup B_1^i) \cup (B_1 \setminus B_1^i))$.
And by definition of B_1^i, *we have* $(x_i\sigma_1, y_i\rho_1) \in \mathcal{S}(\mathcal{I}(h_i(\sigma_1,\rho_1) \cup B_1^i))$ *(i.e. the names of* $B_1 \setminus B_1^i$ *are irrelevant to synthesise* $(x\sigma_1, y\rho_1)$*).*
Let $(b_1,b_2) \in B_1^i$. *We have that* $(b_1\sigma_2, b_2\sigma_2) \in \mathcal{S}(\mathcal{I}(\mathsf{se}_1|_{(b_1,b_2)}(\sigma_2,\rho_2) \cup B_2))$.
Let $(M\sigma_1, N\rho_1) \in \mathsf{se}_1|_{(b_1,b_2)}$ *where* $(M,N) \in h$. *We have* $b_1 \in \mathrm{n}(x_j\sigma)$ *or* $b_2 \in \mathrm{n}(y_j\sigma)$ *for some* $j \leq i$. *So by definition, we have* $(M,N) \prec (x_j,y_j)$. *Since* se *is growing, we have also* $(M,N) \prec (x_i,y_i)$. *So* $(M,N) \in \mathsf{se}|_{(x_i,y_i)} = h_i$.
Thus $(b_1\sigma_2, b_2\sigma_2) \in \mathcal{S}(\mathcal{A}(h_i(\sigma_1,\rho_1)(\sigma_2,\rho_2) \cup B_2))$ *for every* $(b_1,b_2) \in B_1^i$.
So by Lemma 21, we get $(M\sigma_1\sigma_2, N\sigma_1\sigma_2) \in \mathcal{S}(\mathcal{A}(h_i(\sigma_1,\rho_1)(\sigma_2,\rho_2) \cup B_2))$, *i.e.* $(M\sigma, N\rho) \in \mathcal{S}(\mathcal{A}(h_i(\sigma,\rho) \cup B_2))$.

7. *Let* $x \in \gamma_l$. *We have* $x\sigma_1 \in \boldsymbol{N}$. *If* $x\sigma_1 \in \pi_1(B_1)$, *then we have* $x\sigma_1\sigma_2 = x\sigma \in \boldsymbol{N}$. *If* $x\sigma_1 \notin \pi_1(B_1)$, *then* $x\sigma_1\sigma_2 = x\sigma_1 \in \boldsymbol{N}$.
8. *Similarly, if* $y \in \gamma_r$, *then* $y\rho \in \boldsymbol{N}$.
9. *We note* $(h_1, B_1, \prec_1, (\gamma_l^1, \gamma_r^1)) = \mathsf{se}_1$, $(h_2, B_2, \prec_2, (\gamma_l^2, \gamma_r^2)) = \mathsf{se}_2$ *and* $(h', B_2, \prec', (\gamma_l', \gamma_r')) = \mathsf{se}_{B_2}^{\sigma,\rho} = \mathsf{se}'$.
We have $h_1 = h(\sigma_1,\rho_1)$, $h_2 = h_1(\sigma_2,\rho_2) = h(\sigma_1,\rho_1)(\sigma_2,\rho_2)$ *and* $h' = h(\sigma,\rho)$. *According to the previous results, we have* $h_2 = h'$.
If $x_2 \in \gamma_l^2$ *then* $x_2 = x_1\sigma_2$ *for some* $x_1 \in \gamma_l^1$. *Since* $x_1 \in \gamma_l^1$, *there exists* $x \in \gamma_l$ *such that* $x_1 = x\sigma_1$. *We have* $x_2 = x\sigma_1\sigma_2 = x\sigma \in \sigma(\gamma_l)$. *Moreover* $x_2 \in \pi_1(B_2)$ *so* $x_2 \in \gamma_l'$.
Conversely, if $x_2 \in \gamma_l'$, *there is* $x \in \gamma_l$ *such that* $x_2 = x\sigma = x\sigma_1\sigma_2$. *Since* $x\sigma_1\sigma_2 = x \in \boldsymbol{N}$, *we have* $x\sigma_1 \in \boldsymbol{N}$. *Necessarily,* $x\sigma_1 \in \pi_1(B_1)$ *otherwise* $x\sigma_1\sigma_2 \notin \pi_1(B_2)$ *which would be a contradiction. So* $x_2 \in \gamma_l^2$.
Hence $\gamma_l' = \gamma_l^2$ *and* $\gamma_r' = \gamma_r^2$.
It remains to show that $\prec' = \prec_2$.
Since se *is growing, we write* $v = \{(x_1,y_1), \ldots, (x_n,y_n)\}$ *such that if* $h_i := \mathsf{se}|_{(x_i,y_i)}$ *we have* $h_i \subseteq h_{i+1}$ *for* $1 \leq i < n$.
Since se_1 *is growing, we write* $B_1 = \{(x_1',y_1'), \ldots, (x_p',y_p')\}$ *such that if* $h_i' := \mathsf{se}_1|_{(x_i',y_i')}$ *we have* $h_i' \subseteq h_{i+1}'$ *for* $1 \leq i < p$.
According to proof of Lemma 19, $(M\sigma_1\sigma_2, N\rho_1\rho_2) \prec_2 (x'',y'')$ *if and only if* $(M\sigma_1, N\rho_1) \prec_1 (x_i',y_i')$ *where* i *is the minimal index such that* $x'' \in \mathrm{n}(x_i'\sigma_2)$ *or* $y'' \in \mathrm{n}(y_i'\rho_2)$ *(where* $(M,N) \in h$ *and* $(x'',y'') \in B_2$.
Similarly, $(M\sigma, N\rho) \prec' (x'',y'')$ *if and only if* $(M,N) \prec (x_i,y_i)$ *where* i *is the minimal index such that* $x'' \in \mathrm{n}(x_i\sigma)$ *or* $y'' \in \mathrm{n}(y_i\rho)$ *(where* $(M,N) \in h$ *and* $(x'',y'') \in B_2$.
Assume that $(M\sigma, N\rho) \prec' (x'',y'')$. *Let* i *minimal such that* $x'' \in \mathrm{n}(x_i'\sigma_2)$ *or* $y'' \in \mathrm{n}(y_i'\rho_2)$. *According to proof of Lemma 20, we have that* $x'' \in \mathrm{n}(x_i'\sigma_2)$ *and* $y'' \in \mathrm{n}(y_i'\rho_2)$ *(because the S-environments are well-formed and growing). Now let* j *minimal such that* $x_i' \in \mathrm{n}(x_j\sigma_1)$ *or* $y_i' \in \mathrm{n}(y_j\rho_1)$. *Similarly, we*

have that $x'_i \in \mathrm{n}(x_j\sigma_1)$ *and* $y'_i \in \mathrm{n}(y_j\rho_1)$. *So* $x'' \in \mathrm{n}(x_j\sigma)$ *and* $y'' \in \mathrm{n}(y_j\rho)$. *So we have* $(M,N) \prec (x_j,y_j)$. *Thus* $(M\sigma_1, N\rho_1) \prec_1 (x'_i,y'_i)$ *and finally* $(M\sigma_1\sigma_2, N\rho_1\rho_2) \prec_2 (x'',y'')$, *i.e.* $(M\sigma,N\rho) \prec_2 (x'',y'')$. *We conclude that* $\prec' \subseteq \prec_2$.

Assume now that $(M\sigma_1\sigma_2, N\rho_1\rho_2) \prec_2 (x'',y'')$. *Let* i *minimal such that* $x'' \in \mathrm{n}(x_i\sigma)$ *or* $y'' \in \mathrm{n}(y_i\rho)$. *We have* $x'' \in \mathrm{n}(x_i\sigma)$ *and* $y'' \in \mathrm{n}(y_i\rho)$. *Necessarily, there is* j *such that* $x'_j \in \mathrm{n}(x_i\sigma_1)$ *and* $x'' \in \mathrm{n}(x'_j\sigma_2)$. *We then have* $(M\sigma_1, N\rho_1) \prec_1 (x'_j,y'_j)$. *Hence* $(M,N) \prec (x_i,y_i)$. *So* $(M\sigma,N\rho) \prec' (x'',y'')$. *We conclude that* $\prec_2 \subseteq \prec'$.

Finally, we have shown that $\mathsf{se}' = \mathsf{se}_2$.

Symbolic transitions

Lemma 22. *If* $P \xrightarrow[(\nu\tilde{c})\,\phi]{\mu} P'$ *and* σ *is such that* $\mathrm{n}(\mathrm{cosupp}(\sigma)) \cap \mathrm{bn}(\mu) = \mathrm{n}(\sigma) \cap \{\tilde{c}\} = \emptyset$ *and* $\mathbf{e}(\phi\sigma)$ *then* $P\sigma \xrightarrow[\mathbf{nc}(\phi\sigma)\setminus\{\tilde{c}\}]{\mathbf{e}_\mathrm{c}(\mu\sigma)} Q'$ *with* $P'\sigma >_\mathrm{o} Q'$.

Proof. *By rule induction on* $P \xrightarrow[(\nu\tilde{c})\,\phi]{\mu} P'$.

If we are going to α*-rename* P, *we might as well consider that no names of* $\mathrm{n}(\sigma)$ *are bound in* P.

We give the proof for the following cases:

S-Input *Assume that* $E(x).P' \xrightarrow[[E:\boldsymbol{N}]]{\mathbf{e}_\mathrm{a}(E)(x)} P'$ *and* $\mathbf{e}([E:\boldsymbol{N}]\sigma)$.
Then there exists $a \in \boldsymbol{N}$ *such that* $\mathbf{e}_\mathrm{c}(E\sigma) = a$.
By NC-Input, *we have* $P\sigma = E\sigma(x).P'\sigma \xrightarrow[\{a\}]{a(x)} P'\sigma$.
This gives the result since we also have $\mathbf{nc}([E:\boldsymbol{N}]\sigma) = \{\mathbf{e}_\mathrm{c}(E\sigma)\} = \{a\}$ *and* $P'\sigma >_\mathrm{o} P'\sigma$ *and* $\mathbf{e}_\mathrm{c}(\mathbf{e}_\mathrm{a}(E)\sigma) = \mathbf{e}_\mathrm{c}(E\sigma) = a$ *by Lemma 14.*

S-Output *Assume that* $\overline{E}\langle F\rangle.P' \xrightarrow[[E:\boldsymbol{N}]\wedge[F:\boldsymbol{M}]]{\overline{\mathbf{e}_\mathrm{a}(E)}\;\mathbf{e}_\mathrm{a}(F)} P'$ *and* $\mathbf{e}([E:\boldsymbol{N}]\sigma \wedge [F:\boldsymbol{M}]\sigma)$.
There exists $a \in \boldsymbol{N}$ *such that* $\mathbf{e}_\mathrm{c}(E\sigma) = a$ *and* $M \in \boldsymbol{M}$ *such that* $\mathbf{e}_\mathrm{c}(F\sigma) = M$.
So, by NC-Output, *we have* $P\sigma = \overline{E\sigma}\langle F\sigma\rangle.P'\sigma \xrightarrow[\{a\}]{\overline{a}\,M} P'\sigma$.
By Lemma 14, we have $\mathbf{e}_\mathrm{c}(\mathbf{e}_\mathrm{a}(E)\sigma) = \mathbf{e}_\mathrm{c}(E\sigma) = a$ *and* $\mathbf{e}_\mathrm{c}(\mathbf{e}_\mathrm{a}(F)\sigma) = \mathbf{e}_\mathrm{c}(F\sigma) = M$. *Moreover* $P'\sigma >_\mathrm{o} P'\sigma$ *and* $\mathbf{nc}(\phi\sigma) = \{\mathbf{e}_\mathrm{c}(E\sigma)\} = \{a\}$.

S-Close-l *Assume that* $P = P_1 \mid P_2 \xrightarrow[(\nu\tilde{z})\,([E=F]\wedge\phi_1\wedge\phi_2)]{\tau} (\nu\tilde{z})\,(P'_1\{^G/_x\} \mid P'_2) = P'$ *with* $P_1 \xrightarrow[(\nu\tilde{c_1})\,\phi_1]{E(x)} P'_1$, $P_2 \xrightarrow[(\nu\tilde{c_2})\,\phi_2]{(\nu\tilde{z})\,\overline{F}\,G} P'_2$, $\tilde{z} \cap \mathrm{fn}(P_1) = \emptyset$, $\tilde{c_1} \cap \mathrm{n}(\phi_1,E,F) = \emptyset$ *and* $\tilde{c_2} \cap \mathrm{n}(\phi_2,E,F) = \emptyset$. *We may assume that* $\{x,\tilde{z}\} \cap \mathrm{n}(\sigma) = \emptyset$.
Since $\mathbf{e}([E=F]\sigma \wedge \phi_1\sigma \wedge \phi_2\sigma)$, *we have* $\mathbf{e}(\phi_1\sigma)$ *and* $\mathbf{e}(\phi_2\sigma)$.
By induction, we have $P_1\sigma \xrightarrow[\mathbf{nc}(\phi_1\sigma)\setminus\{\tilde{c_1}\}]{\mathbf{e}_\mathrm{c}(E\sigma)(x)} Q'_1$, $P_2\sigma \xrightarrow[\mathbf{nc}(\phi_2\sigma)\setminus\{\tilde{c_2}\}]{(\nu\tilde{z})\,\overline{\mathbf{e}_\mathrm{c}(F\sigma)}\;\mathbf{e}_\mathrm{c}(G\sigma)} Q'_2$, $P'_1\sigma >_\mathrm{o} Q'_1$ *and* $P'_2\sigma >_\mathrm{o} Q'_2$.

Since $\mathbf{e}([E{=}F]\sigma)$*, there exists* $a \in \boldsymbol{M}$ *such that* $\mathbf{e}_{\mathrm{c}}(E\sigma) = \mathbf{e}_{\mathrm{c}}(F\sigma) = a$*. Moreover we have that* $\mathbf{e}_{\mathrm{c}}(E\sigma) \in \boldsymbol{N}$ *(according the induction hypothesis), so* $a \in \boldsymbol{N}$*. There exists also* $M \in \boldsymbol{M}$ *such that* $\mathbf{e}_{\mathrm{c}}(G\sigma) = M$*.*
So, by NC-Close-L*, we have* $P_1\sigma \mid P_2\sigma \xrightarrow[S_1 \cup S_2]{\tau} (\nu\tilde{z})\,(Q_1'\{{}^{M}/_{x}\} \mid Q_2') = Q'$ *because* $\{\tilde{z}\} \cap \mathrm{fn}(P_1\sigma) = \{\tilde{z}\} \cap \mathrm{fn}(P_1) = \emptyset$ *(since* $\{\tilde{z}\} \cap \mathrm{n}(\sigma) = \emptyset$*) where* $S_1 = \mathbf{nc}(\phi_1\sigma) \setminus \{\tilde{c_1}\}$ *and* $S_2 = \mathbf{nc}(\phi_2\sigma) \setminus \{\tilde{c_2}\}$*.*
Since $\mathbf{e}_{\mathrm{c}}(G\sigma) = M$*, by Lemma 9 we have* $G\sigma >_{\mathrm{o}} M$ *so* $P'\sigma >_{\mathrm{o}} Q'$*.*
Moreover, $\mathbf{nc}([E{=}F]\sigma \wedge \phi_1\sigma \wedge \phi_2\sigma) = \mathbf{nc}(\phi_1\sigma) \cup \mathbf{nc}(\phi_2\sigma)$ *by definition. Since* $\mathrm{n}(\sigma) \cap \{\tilde{c_1}\tilde{c_2}\} = \emptyset$ *and* $\{\tilde{c_2}\} \cap \mathrm{n}(\phi_1) = \emptyset$*, we have* $\mathbf{nc}(\phi_1\sigma) \setminus \{\tilde{c_1}\tilde{c_2}\} = \mathbf{nc}(\phi_1\sigma) \setminus \{\tilde{c_1}\} = S_1$*. Similarly, we have that* $\mathbf{nc}(\phi_2\sigma) \setminus \{\tilde{c_1}\tilde{c_2}\} = S_2$*. So* $\mathbf{nc}([E{=}F]\sigma \wedge \phi_1\sigma \wedge \phi_2\sigma) \setminus \{\tilde{c_1}\tilde{c_2}\} = S_1 \cup S_2$*.*

S-Guard *Assume that* $\psi P_1 \xrightarrow[(\nu\tilde{c})\,(\phi_1 \wedge \psi)]{\mu} P'$ *with* $P_1 \xrightarrow[(\nu\tilde{c})\,\phi_1]{\mu} P'$ *and* $\{\tilde{c}\} \cap \mathrm{n}(\psi) = \emptyset$*.*
Since $\mathbf{e}(\phi_1\sigma \wedge \psi\sigma)$*, we have* $\mathbf{e}(\phi_1\sigma)$ *and* $\mathbf{e}(\psi\sigma)$*.*
So by induction, $P_1\sigma \xrightarrow[\mathbf{nc}(\phi_1)\setminus\{\tilde{c}\}]{\mathbf{e}_{\mathrm{c}}(\mu\sigma)} Q'$ *with* $P'\sigma >_{\mathrm{o}} Q'$*.*
Since $\mathbf{e}(\psi\sigma)$*, by* NC-Guard*, we have* $P\sigma = \psi\sigma P_1\sigma \xrightarrow[S_1 \cup \mathbf{nc}(\psi\sigma)]{\mathbf{e}_{\mathrm{c}}(\mu\sigma)} Q'$ *where* $S_1 = \mathbf{nc}(\phi_1) \setminus \{\tilde{c}\}$*.*
Since $\{\tilde{c}\} \cap \mathrm{n}(\psi) = \emptyset$ *and* $\{\tilde{c}\} \cap \mathrm{n}(\sigma) = \emptyset$*, we have* $\mathbf{nc}(\psi\sigma) \setminus \{\tilde{c}\} = \mathbf{nc}(\psi\sigma)$*.*
Thus $\mathbf{nc}(\phi_1\sigma \wedge \psi\sigma) \setminus \{\tilde{c}\} = S_1 \cup \mathbf{nc}(\psi\sigma)$*.*

S-Open *Assume that* $P = (\nu z')\,P_1 \xrightarrow[(\nu z'\tilde{c})\,\phi]{(\nu z'\tilde{z})\,\overline{E}\,F} P'$ *with* $P_1 \xrightarrow[(\nu\tilde{c})\,\phi]{(\nu\tilde{z})\,\overline{E}\,F} P'$*,* $z' \in \mathrm{n}(F)$*,* $z' \notin \mathrm{n}(E)$ *and* $z' \notin \{\tilde{z}, \tilde{c}\}$*.*
By induction, we have $P_1\sigma \xrightarrow[\mathbf{nc}(\phi\sigma)\setminus\{\tilde{c}\}]{(\nu\tilde{z})\,\overline{\mathbf{e}_{\mathrm{c}}(E\sigma)}\,\mathbf{e}_{\mathrm{c}}(F\sigma)} Q'$ *with* $P'\sigma >_{\mathrm{o}} Q'$*.*
Clearly, $\mathbf{e}_{\mathrm{a}}(F) = F$*. So, since* $z' \in \mathrm{n}(F) = \mathrm{n}(\mathbf{e}_{\mathrm{a}}(F))$ *and* $z' \notin \mathrm{n}(\sigma)$*, we have* $z' \in \mathrm{n}(\mathbf{e}_{\mathrm{c}}(F\sigma))$ *by Lemma 15.*
Since $z' \notin \mathrm{n}(E)$*, we have* $z' \notin \mathrm{n}(\mathbf{e}_{\mathrm{c}}(E)\sigma)$*. Moreover* $z' \notin \{\tilde{z}\}$*.*
So, by NC-Open*, we have* $P\sigma = (\nu z')\,P_1\sigma \xrightarrow[S\setminus\{z'\}]{(\nu z'\tilde{z})\,\overline{\mathbf{e}_{\mathrm{c}}(E\sigma)}\,\mathbf{e}_{\mathrm{c}}(F\sigma)} Q'$ *with* $S = \mathbf{nc}(\phi\sigma) \setminus \{\tilde{c}\}$*.*
We have $\mathbf{nc}(\phi\sigma) \setminus \{z'\tilde{c}\} = S \setminus \{z'\}$*.*

S-Res *Assume that* $P = (\nu z)\,P_1 \xrightarrow[(\nu\tilde{c})\,\phi]{\mu} (\nu z)\,P_1' = P'$ *with* $P_1 \xrightarrow[(\nu\tilde{c})\,\phi]{\mu} P_1'$*,* $z \notin \mathrm{n}(\mu)$ *and* $z \notin \mathrm{n}(\phi)$*.*
By induction, we have $P_1\sigma \xrightarrow[\mathbf{nc}(\phi\sigma)\setminus\{\tilde{c}\}]{\mathbf{e}_{\mathrm{c}}(\mu\sigma)} Q_1'$ *with* $P_1'\sigma >_{\mathrm{o}} Q_1'$*.*
Since $z \notin \mathrm{n}(\sigma)$ *and* $z \notin \mathrm{n}(\mu)$*, we have* $z \notin \mathrm{n}(\mathbf{e}_{\mathrm{c}}(\mu\sigma))$*.*
So, by NC-Res*,* $P\sigma(\nu z)\,P_1\sigma \xrightarrow[S\setminus\{z\}]{\mathbf{e}_{\mathrm{c}}(\mu\sigma)} (\nu z)\,Q_1' = Q'$ *where* $S = \mathbf{nc}(\phi\sigma) \setminus \{\tilde{c}\}$*.*
We have $P'\sigma >_{\mathrm{o}} Q'$ *since* $P_1'\sigma >_{\mathrm{o}} Q_1'$*.*
Since $z \notin \mathrm{n}(\phi)$ *and* $z \notin \mathrm{n}(\sigma)$*, we have* $z \notin \mathrm{n}(\mathbf{nc}(\phi\sigma))$*. Thus* $S \setminus \{z\} = \mathbf{nc}(\phi\sigma) \setminus \{z\tilde{c}\} = \mathbf{nc}(\phi\sigma) \setminus \{\tilde{c}\} = S$*.*

S-RO-Guard *Assume that* $P = (\nu z)\,P_1 \xrightarrow[(\nu z\tilde{c})\,\phi]{\mu} (\nu z)\,P_1' = P'$ *with* $P_1 \xrightarrow[(\nu\tilde{c})\,\phi]{\mu} P_1'$*,* $z \notin \mathrm{n}(\mu)$*,* $z \notin \{\tilde{c}\}$ *and* $z \in \mathrm{n}(\phi)$*.*

By induction, we have $P_1\sigma \xrightarrow[\mathbf{nc}(\phi\sigma)\setminus\{\tilde{c}\}]{\mathbf{e}_c(\mu\sigma)} Q_1'$ *with* $P_1'\sigma >_o Q_1'$.
Since $z \notin n(\sigma)$ *and* $z \notin n(\mu)$, *we have* $z \notin n(\mathbf{e}_c(\mu\sigma))$.
So, by NC-Res, $P\sigma(\nu z)\, P_1\sigma \xrightarrow[S\setminus\{z\}]{\mathbf{e}_c(\mu\sigma)} (\nu z)\, Q_1' = Q'$ *where* $S = \mathbf{nc}(\phi\sigma) \setminus \{\tilde{c}\}$.
We have $P'\sigma >_o Q'$ *since* $P_1'\sigma >_o Q_1'$ *and* $\mathbf{nc}(\phi\sigma) \setminus \{z\tilde{c}\} = S \setminus \{z\}$.

Lemma 23. *If* $P\sigma \xrightarrow[S]{\mu} R$ *and* $n(\mathrm{cosupp}(\sigma)) \cap bn(\mu) = \emptyset$ *then there exists* μ', $\tilde{c}$, ϕ *and* Q *such that* $P \xrightarrow[(\nu\tilde{c})\,\phi]{\mu'} Q$, $\{\tilde{c}\} \cap n(\sigma) = \emptyset$, $\mathbf{e}(\phi\sigma)$, $\mathbf{e}_c(\mu'\sigma) = \mu$, $S = \mathbf{nc}(\phi\sigma)\setminus\{\tilde{c}\}$ *and* $Q\sigma >_o R$.

Proof. By rule induction on $P\sigma \xrightarrow[S]{\mu} R$.

If we are going to α*-rename* P, *we might as well consider that no names of* $n(\sigma)$ *are bound in* P.

We give the proof for the following cases:

NC-Input *Assume that* $P\sigma = E\sigma(x).P'\sigma \xrightarrow[\{a\}]{a(x)} P'\sigma = R$ *with* $\mathbf{e}_c(E\sigma) = a \in \boldsymbol{N}$.
We have $P = E(x).P'$, $R = P'\sigma$, $\mu = a(x)$ *and* $S = \{a\}$.
By S-Input, *we have* $P = E(x).P' \xrightarrow[[E:\boldsymbol{N}]]{\mathbf{e}_a(E)(x)} P'$.
We define $\mu' := \mathbf{e}_a(E)(x)$, $\tilde{c} := \emptyset$, $\phi := [E:\boldsymbol{N}]$ *and* $Q := P'$.
By Lemma 14, since $\mathbf{e}_c(E\sigma) = a \in \boldsymbol{N} \subseteq \boldsymbol{M}$, *we have* $\mathbf{e}_c(\mathbf{e}_a(E)\sigma) = a$, *so* $\mathbf{e}_c(\mu'\sigma) = \mu$.
Since $\mathbf{e}_c(E\sigma) = a \in \boldsymbol{N}$, *we have* $\mathbf{e}([E:\boldsymbol{N}]\sigma)$ *and* $\mathbf{e}(\phi\sigma)$. *Moreover* $\mathbf{nc}(\phi\sigma) = \{\mathbf{e}_c(E\sigma)\} = \{a\} = S$.
Finally $Q\sigma = P'\sigma >_o P'\sigma = R$.

NC-Output *Assume that* $P\sigma = \overline{E\sigma}\langle F\sigma\rangle.P'\sigma \xrightarrow[\{a\}]{\overline{a}\,M} P'\sigma = R$ *with* $\mathbf{e}_c(E\sigma) = a \in \boldsymbol{N}$ *and* $\mathbf{e}_c(F\sigma) = M \in \boldsymbol{M}$.
We have $P = \overline{E}\langle F\rangle.P'$, $R = P'\sigma$, $\mu = \overline{a}\,M$ *and* $S = \{a\}$.
By S-Output, *we have* $P = \overline{E}\langle F\rangle.P' \xrightarrow[[E:\boldsymbol{N}]\wedge[F:\boldsymbol{M}]]{\overline{\mathbf{e}_a(E)}\ \mathbf{e}_a(F)} P'$.
We define $\mu' := \overline{\mathbf{e}_a(E)}\ \mathbf{e}_a(F)$, $\tilde{c} := \emptyset$, $\phi := [E:\boldsymbol{N}] \wedge [F:\boldsymbol{M}]$ *and* $Q := P'$.
By Lemma 14, since $\mathbf{e}_c(E\sigma) = a \in \boldsymbol{N} \subseteq \boldsymbol{M}$, *we have* $\mathbf{e}_c(\mathbf{e}_a(E)\sigma) = a$. *Similarly,* $\mathbf{e}_c(\mathbf{e}_a(F)\sigma) = M$. *So* $\mathbf{e}_c(\mu'\sigma) = \mu$.
Since $\mathbf{e}_c(E\sigma) = a \in \boldsymbol{N}$ *and* $\mathbf{e}_c(F\sigma) = M \in \boldsymbol{M}$, *we have* $\mathbf{e}(\phi\sigma)$.
Moreover, $\mathbf{nc}(\phi\sigma) = \{\mathbf{e}_c(E\sigma)\} = \{a\} = S$.
Finally $Q\sigma = P'\sigma >_o P'\sigma = R$.

NC-Close-l *Assume that* $P\sigma = P_1\sigma \,|\, P_2\sigma \xrightarrow[S_1\cup S_2]{\tau} R$ *with* $P = P_1 \,|\, P_2$, $P_1\sigma \xrightarrow[S_1]{a(x)} R_1$, $P_2\sigma \xrightarrow[S_2]{(\nu\tilde{z})\,\overline{a}\,M} R_2$, $\{\tilde{z}\} \cap fn(P_1\sigma) = \emptyset$ *and* $R = (\nu\tilde{z})\,(R_1\{{}^{M}/_{x}\} \,|\, R_2)$. *We may assume that* $\{x, \tilde{z}\} \cap n(\sigma) = \emptyset$.
We have $\mu = \tau$ *and* $S = S_1 \cup S_2$.
By induction, there exists μ_1', μ_2', $\tilde{c_1}$, $\tilde{c_2}$, ϕ_1, ϕ_2, Q_1 *and* Q_2 *such that* $\tilde{c_1} \cap n(\sigma) = \tilde{c_2} \cap n(\sigma) = \emptyset$, $\mathbf{e}(\phi_1\sigma)$, $\mathbf{e}(\phi_2\sigma)$, $S_1 = \mathbf{nc}(\phi_1\sigma) \setminus \{\tilde{c_1}\}$, $S_2 = \mathbf{nc}(\phi_2\sigma) \setminus$

$\{\tilde{c_2}\}$, $P_1 \xrightarrow[(\nu\tilde{c_1})\,\phi_1]{\mu_1'} Q_1$, $P_2 \xrightarrow[(\nu\tilde{c_2})\,\phi_2]{\mu_2'} Q_2$, $\mathbf{e}_{\mathrm{c}}(\mu_1'\sigma) = a(x)$, $\mathbf{e}_{\mathrm{c}}(\mu_2'\sigma) = (\nu\tilde{z})\,\overline{a}\,M$, $Q_1\sigma >_{\mathrm{o}} R_1$ *and* $Q_2\sigma >_{\mathrm{o}} R_2$.
Necessarily, we have $\mu_1' = E(x)$ *for some* E *and* $\mu_2' = (\nu\tilde{z})\,\overline{F}\,G$ *for some* F *and* G *with* $\mathbf{e}_{\mathrm{c}}(E\sigma) = \mathbf{e}_{\mathrm{c}}(F\sigma) = a$ *and* $\mathbf{e}_{\mathrm{c}}(G\sigma) = M \in \boldsymbol{M}$.
By S-Alpha, *we may* α*-rename so that* $\{\tilde{c_1}\} \cap \mathrm{n}(\phi_2, E, F) = \emptyset$ *and* $\{\tilde{c_2}\} \cap \mathrm{n}(\phi_1, E, F) = \emptyset$ *and* $\{\tilde{c_1}\}$ *and* $\{\tilde{c_2}\}$ *are disjoints.*
We have $\{\tilde{z}\} \cap \mathrm{fn}(P_1\sigma) = \emptyset$. *Since* $\mathrm{n}(\sigma) \cap \{\tilde{z}\} = \emptyset$, *we have* $\{\tilde{z}\} \cap \mathrm{fn}(P_1) = \emptyset$.
So $P \xrightarrow[(\nu\tilde{c_1}\tilde{c_2})\,([E=F]\wedge\phi_1\wedge\phi_2)]{\tau} (\nu\tilde{z})\,(Q_1\{{}^{G}/_{x}\} \mid Q_2)$ *by* S-Close-l.
Define $Q = (\nu\tilde{z})\,(Q_1\{{}^{G}/_{x}\} \mid Q_2)$, $\phi = [E=F] \wedge \phi_1 \wedge \phi_2$, $\mu' := \tau$ *and* $\tilde{c} = \tilde{c_1}\tilde{c_2}$.
We have $\mathbf{e}_{\mathrm{c}}(\mu'\sigma) = \tau = \mu$, $\mathrm{n}(\sigma) \cap \{\tilde{c}\} = \emptyset$, $S = S_1 \cup S_2 = \mathbf{nc}(\phi)\sigma \setminus \{\tilde{c}\}$, *and* $\mathbf{e}(\phi\sigma)$.
Since $\mathbf{e}_{\mathrm{c}}(G\sigma) = M \in \boldsymbol{M}$ *we have* $G\sigma >_{\mathrm{o}} M$ *by Lemma 9. Thus, since we also have* $Q_1\sigma >_{\mathrm{o}} R_1$ *and* $Q_2\sigma >_{\mathrm{o}} R_2$, *we have* $Q\sigma >_{\mathrm{o}} R$.

NC-Guard *Assume that* $\psi\sigma P'\sigma \xrightarrow[S\cup\mathbf{nc}(\psi\sigma)]{\mu} R$ *with* $P'\sigma \xrightarrow[S]{\mu} R$ *and* $\mathbf{e}(\psi\sigma)$.
We have $P = \psi P'$. *By induction, there exists* $\tilde{c}, \mu', \phi'$ *and* Q *such that* $P \xrightarrow[(\nu\tilde{c})\,\phi']{\mu'} Q$, $\{\tilde{c}\} \cap \mathrm{n}(\sigma) = \emptyset$, $\mathbf{e}_{\mathrm{c}}(\mu'\sigma) = \mu$, $\mathbf{e}(\phi'\sigma)$, $S = \mathbf{nc}(\phi'\sigma) \setminus \{\tilde{c}\}$ *and* $Q\sigma >_{\mathrm{o}} R$.
By S-Alpha, *we may* α*-rename such that* $\{\tilde{c}\} \cap \mathrm{n}(\psi) = \emptyset$.
So $P \xrightarrow[(\nu\tilde{c})\,(\psi\wedge\phi')]{\mu'} Q$ *by* S-Guard.
We define $\phi := \psi \wedge \phi'$ *and we keep* μ', Q *and* $\tilde{c}$.
We have $\mathbf{e}(\phi\sigma)$ *since* $\mathbf{e}_{\mathrm{c}}(\psi\sigma) = \mathbf{e}(\phi'\sigma)$ *and* $\mathbf{nc}(\phi\sigma) \setminus \{\tilde{c}\} = \mathbf{nc}(\psi\sigma) \setminus \tilde{c} \cup \mathbf{nc}(\phi'\sigma) \setminus \tilde{c} = \mathbf{nc}(\psi\sigma) \cup S$ *because* $\{\tilde{c}\} \cap (\mathrm{n}(\psi) \cup \mathrm{n}(\sigma)) = \emptyset$. *This gives the result.*

NC-Open *Assume that* $(\nu z')\,P'\sigma \xrightarrow[S'\setminus\{z'\}]{(\nu z'\tilde{z})\,\overline{a}\,M} R$ *with* $P'\sigma \xrightarrow[S']{(\nu\tilde{z})\,\overline{a}\,M} R$ *and* $z' \in \mathrm{n}(M) \setminus \{a, \tilde{z}\}$.
We have $P = (\nu z')\,P'$, $\mu = (\nu z'\tilde{z})\,\overline{a}\,M$ *and* $S = S' \setminus \{z'\}$.
By induction, since $\mathrm{n}(\mathrm{cosupp}(\sigma)) \cap \{z', \tilde{z}\} = \emptyset$, *there exists* Q, μ', $\tilde{c'}$ *and* ϕ' *such that* $P' \xrightarrow[(\nu\tilde{c'})\,\phi']{\mu'} Q$, $\{\tilde{c'}\} \cap \mathrm{n}(\sigma) = \emptyset$, $\mathbf{e}(\phi'\sigma)$, $\mathbf{e}_{\mathrm{c}}(\mu'\sigma) = (\nu\tilde{z})\,\overline{a}\,M$, $S' = \mathbf{nc}(\phi'\sigma) \setminus \{\tilde{c'}\}$ *and* $Q\sigma >_{\mathrm{o}} R$.
Since $\mathbf{e}_{\mathrm{c}}(\mu'\sigma) = (\nu\tilde{z})\,\overline{a}\,M$, *necessarily,* $\mu' = (\nu\tilde{z})\,\overline{E}\,F$ *for some* E *and* F *with* $\mathbf{e}_{\mathrm{c}}(E\sigma) = a$ *and* $\mathbf{e}_{\mathrm{c}}(F\sigma) = M$.
By S-Alpha, *we may* α*-rename such that* $z' \notin \{\tilde{c}\}$.
Since $z' \in \mathrm{n}(M) \setminus \{\tilde{z}\}$, $\mathbf{e}_{\mathrm{c}}(F\sigma) = M$ *and* $z' \notin \mathrm{n}(\mathrm{cosupp}(\sigma))$, *we have* $z' \in \mathrm{n}(F)$.
Since $z' \neq a$, $\mathbf{e}_{\mathrm{c}}(E\sigma) = a$ *and* $z' \notin \mathrm{n}(\sigma)$, *then* $z' \notin \mathrm{n}(E)$.
So, by S-Open, *we have* $(\nu z')\,P' \xrightarrow[(\nu z'\tilde{c})\,\phi']{(\nu z'\tilde{z})\,\overline{E}\,F} Q$. *Clearly, this gives the result.*

NC-Res *Assume that* $(\nu z)\,P'\sigma \xrightarrow[S'\setminus\{z\}]{\mu} (\nu z)\,R' = R$ *with* $P'\sigma \xrightarrow[S']{\mu} R'$ *and* $z \notin \mathrm{n}(\mu)$.
By induction, there exists μ', $\{\tilde{c}\}$, ϕ' *and* Q' *such that* $P' \xrightarrow[(\nu\tilde{c})\,\phi']{\mu'} Q'$, $\{\tilde{c}\} \cap \mathrm{n}(\sigma) = \emptyset$, $\mathbf{e}(\phi'\sigma)$, $\mathbf{e}_{\mathrm{c}}(\mu'\sigma) = \mu$, $S' = \mathbf{nc}(\phi'\sigma) \setminus \{\tilde{c}\}$ *and* $Q'\sigma >_{\mathrm{o}} R'$.

By S-Alpha*, we may α-rename such that $z \notin \{\tilde{c}\}$.*
Since $z \notin \mathrm{n}(\mu)$, $\mathbf{e}_{\mathrm{c}}(\mu'\sigma) = \mu$ and $z \notin \mathrm{n}(\sigma)$, we have $z \notin \mathrm{n}(\mu')$.
There are two cases: either $z \in \mathrm{n}(\phi')$ or $z \notin \mathrm{n}(\phi')$.

1. *if $z \in \mathrm{n}(\phi')$*

   Then by S-RO-Guard*, we have $(\nu z)\, P' \xrightarrow[(\nu z\tilde{c})\ \phi']{\mu'} (\nu z)\, Q'$.*

   Clearly, $Q := (\nu z)\, Q'\sigma >_{\mathrm{o}} (\nu z)\, R' = R$ and $\{z\tilde{c}\} \cap \mathrm{n}(\sigma) = \emptyset$. So this gives the result.
2. *if $z \notin \mathrm{n}(\phi')$*

   Then by S-Res*, we have $(\nu z)\, P' \xrightarrow[(\nu \tilde{c})\ \phi']{\mu'} (\nu z)\, Q'$.*

   Clearly, $Q := (\nu z)\, Q'\sigma >_{\mathrm{o}} (\nu z)\, R' = R$.
   Moreover, since $z \notin \mathrm{n}(\phi')$, then $z \notin \mathrm{n}(\mathbf{nc}(\phi'\sigma))$ (because $z \notin \mathrm{n}(\sigma)$) so $z \notin S'$ and $S' \setminus \{z\} = S' = \mathbf{nc}(\phi'\sigma) \setminus \{\tilde{c}\}$. This gives the result.

Symbolic characterisation

Lemma 24. *$\mathcal{R} = \{(\mathsf{se}, P, Q) \mid P' \sim^{\mathsf{se}}_{\mathrm{OH}} Q' \wedge P >_{\mathrm{o}} P' \wedge Q >_{\mathrm{o}} Q' \wedge \mathrm{fn}(P) \subseteq \mathrm{n}(\pi_1(\mathfrak{H}(\mathsf{se}))) \wedge \mathrm{fn}(Q) \subseteq \mathrm{n}(\pi_2(\mathfrak{H}(\mathsf{se})))\}$ is a symbolic open hedged bisimulation.*

Proof. *Let $(\mathsf{se}, P, Q) \in \mathcal{R}$. There exists P_0 and Q_0 such that $P_0 \sim^{\mathsf{se}}_{\mathrm{OH}} Q_0$ and $P >_{\mathrm{o}} P_0$ and $Q >_{\mathrm{o}} Q_0$.*

Let σ, ρ and B such that $(\sigma, \rho) \triangleright_B \mathsf{se}$.

It is clear that $\mathrm{n}(\mathrm{cosupp}(\sigma)) \subseteq \mathrm{n}(\pi_1(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)})))$ and $\mathrm{n}(\mathrm{cosupp}(\rho)) \subseteq \mathrm{n}(\pi_2(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)})))$.

Also it is clear that since $\mathrm{fn}(P) \subseteq \mathrm{n}(\pi_1(\mathfrak{H}(\mathsf{se})))$ and $\mathrm{fn}(Q) \subseteq \mathrm{n}(\pi_2(\mathfrak{H}(\mathsf{se})))$ we have $\mathrm{fn}(P\sigma) \subseteq \mathrm{n}(\pi_1(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)})))$ and $\mathrm{fn}(Q\rho) \subseteq \mathrm{n}(\pi_2(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)})))$.

Assume that $P \xrightarrow[(\nu\tilde{c})\ \phi_1]{\mu_1} P'$ with $\mathrm{bn}(\mu_1) \cap \mathrm{n}(\pi_1(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))) = \emptyset$, $\mathrm{n}(\sigma) \cap \{\tilde{c}\} = \emptyset$, $\mathbf{e}(\phi_1\sigma)$ and $\mathrm{ch}(\mathbf{e}_{\mathrm{c}}(\mu_1\sigma)) \in \pi_1(\mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)})))$ (if $\mu_1 \neq \tau$).

By Lemma 5, since $\mathrm{bn}(\mu_1) \cap \mathrm{n}(\mathrm{cosupp}(\sigma)) = \emptyset$, we have $P\sigma \xrightarrow[\mathbf{nc}(\phi_1\sigma)\setminus\{\tilde{c}\}]{\mathbf{e}_{\mathrm{c}}(\mu_1\sigma)} P_1$ with $P'\sigma >_{\mathrm{o}} P_1$.

Since $P >_{\mathrm{o}} P_0$, we have $P\sigma >_{\mathrm{o}} P_0\sigma$.

So by Lemma 4, we have $P_0\sigma \xrightarrow[\mathbf{nc}(\phi_1\sigma)\setminus\{\tilde{c}\}]{\mathbf{e}_{\mathrm{c}}(\mu_1\sigma)} P_0'$ with $P_1 >_{\mathrm{o}} P_0'$.

Since $P_0 \sim^{\mathsf{se}}_{\mathrm{OH}} Q_0$, there exists Q_0' such that $Q_0\rho \xrightarrow[S]{\mu'} Q_0'$ with $\mathrm{bn}(\mu') \cap \mathrm{n}(\pi_2(\mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)})))) = \emptyset$ and $P_0' \sim^{\mathsf{se}'}_{\mathrm{OH}} Q_0'$ with se' depending on $\mathbf{e}_{\mathrm{c}}(\mu_1\sigma)$.

Since $Q\rho >_{\mathrm{o}} Q_0\rho$ and $\mathrm{bn}(\mu') \cap \mathrm{fn}(Q\rho) = \emptyset$, by Lemma 4 $Q\rho \xrightarrow[S]{\mu'} Q_1$ with $Q_1 >_{\mathrm{o}} Q_0'$.

And by Lemma 5, since $\mathrm{n}(\mathrm{cosupp}(\rho)) \cap \mathrm{bn}(\mu') = \emptyset$, we have $Q \xrightarrow[(\nu\tilde{d})\ \phi_2]{\mu_2} Q'$ with $Q'\rho >_{\mathrm{o}} Q_1$, $\mathbf{e}(\phi_2\rho)$, $\mathbf{e}_{\mathrm{c}}(\mu_2\rho) = \mu'$, $\mathrm{n}(\rho) \cap \{\tilde{d}\} = \emptyset$ and $S_2 = \mathbf{nc}(\phi_2\rho) \setminus \{\tilde{d}\}$. So $Q'\rho >_{\mathrm{o}} Q_0'$ and $\mathrm{bn}(\mu_2) \cap \mathrm{n}(\pi_2(\mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)})))) = \emptyset$ (because $\mathrm{bn}(\mu_2) = \mathrm{bn}(mu')$).

We then do a case analysis on μ_1.

– *if* $\mu_1 = \tau$, *then* $\mathbf{e}_{\mathrm{c}}(\mu_1\sigma) = \tau$. *Thus* $\mu' = \tau$ *and necessarily* $\mu_2 = \tau$.
Thus $\mathsf{se}' = \mathsf{se}_B^{(\sigma,\rho)} \oplus_{\mathrm{c}} (S_1, S_2)$ *where* $S_1 = \mathbf{nc}(\phi_1\sigma) \setminus \{\tilde{c}\}$.
Since $P'\sigma >_{\mathrm{o}} P'_0$, $Q'\rho >_{\mathrm{o}} Q'_0$, $\mathrm{fn}(P'\sigma) \subseteq \mathrm{fn}(P\sigma)$ *thus* $\mathrm{fn}(P'\sigma) \subseteq \mathrm{n}(\pi_1(\mathfrak{H}(\mathsf{se}')))$ *and similarly* $\mathrm{fn}(Q'\rho) \subseteq \mathrm{n}(\pi_2(\mathfrak{H}(\mathsf{se}')))$.
Thus $(\mathsf{se}', P'\sigma, Q'\rho) \in \mathcal{R}$.
– *if* $\mu_1 = E_1(x_1)$ *then* $\mathbf{e}_{\mathrm{c}}(\mu_1\sigma) = a_1(x_1)$. *Thus* $\mu' = a_2(x_2)$ *with* $(a_1, a_2) \in \mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))$.
Necessarily, $\mu_2 = E_2(x_2)$ *for some* E_2 *and we have* $\mathbf{e}_{\mathrm{c}}(E_2\rho) = a_2$.
And $\mathsf{se}' = \mathsf{se}_B^{(\sigma,\rho)} \oplus_{\mathrm{i}} (x_1, x_2) \oplus_{\mathrm{c}} (S_1, S_2)$ *where* $S_1 = \mathbf{nc}(\phi_1\sigma) \setminus \{\tilde{c}\}$.
We have $\mathrm{fn}(P'\sigma) \subseteq \mathrm{fn}(P\sigma) \cup \{x_1\}$ *so* $\mathrm{fn}(P'\sigma) \subseteq \mathrm{n}(\pi_1(\mathfrak{H}(\mathsf{se}')))$ *and similarly* $\mathrm{fn}(Q'\rho) \subseteq \mathrm{n}(\pi_2(\mathfrak{H}(\mathsf{se}')))$.
As above, we conclude that $(\mathsf{se}', P'\sigma, Q'\rho) \in \mathcal{R}$.
– *if* $\mu_1 = (\nu\tilde{z_1})\,\overline{E_1}\,F_1$, *then* $\mathbf{e}_{\mathrm{c}}(\mu_1\sigma) = (\nu\tilde{z_1})\,\overline{a_1}\,M_1$. *Thus* $\mu' = (\nu\tilde{z_2})\,\overline{a_2}\,M_2$ *with* $(a_1, a_2) \in \mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))$.
Necessarily, $\mu_2 = (\nu\tilde{z_2})\,\overline{E_2}\,F_2$ *with* $\mathbf{e}_{\mathrm{c}}(E_2\rho) = a_2$ *and* $\mathbf{e}_{\mathrm{c}}(F_2\rho) = M_2$.
And $\mathsf{se}' = \mathsf{se}_B^{(\sigma,\rho)} \oplus_{\mathrm{o}} (M_1, M_2) \oplus_{\mathrm{c}} (S_1, S_2)$ *where* $S_1 = \mathbf{nc}(\phi_1\sigma) \setminus \{\tilde{c}\}$.
As above, we conclude that $(\mathsf{se}', P'\sigma, Q'\rho) \in \mathcal{R}$.

Lemma 25. $\mathcal{R} = \{(\mathsf{se}, P, Q) \mid P' \sim_{\mathrm{SO}}^{\mathsf{se}} Q' \wedge P' >_{\mathrm{o}} P \wedge Q' >_{\mathrm{o}} Q\}$ *is an open hedged bisimulation.*

Proof. *Let* $(\mathsf{se}, P, Q) \in \mathcal{R}$. *There exists* P_0 *and* Q_0 *such that* $P_0 >_{\mathrm{o}} P$, $Q_0 >_{\mathrm{o}} Q$ *and* $P_0 \sim_{\mathrm{SO}}^{\mathsf{se}} Q_0$.

Let σ, ρ *and* B *such that* $(\sigma, \rho) \triangleright_B \mathsf{se}$.

It is clear that $\mathrm{n}(\mathrm{cosupp}(\sigma)) \subseteq \mathrm{n}(\pi_1(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)})))$ *and* $\mathrm{n}(\mathrm{cosupp}(\rho)) \subseteq \mathrm{n}(\pi_2(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)})))$.

Since $P_0 >_{\mathrm{o}} P$, *we have* $\mathrm{fn}(P) \subseteq \mathrm{fn}(P_0)$. *Similarly* $\mathrm{fn}(Q) \subseteq \mathrm{fn}(Q_0)$. *So* $\mathrm{fn}(P) \subseteq \mathrm{n}(\pi_1(\mathfrak{H}(\mathsf{se})))$ *and* $\mathrm{fn}(Q) \subseteq \mathrm{n}(\pi_2(\mathfrak{H}(\mathsf{se})))$. *Hence* $\mathrm{fn}(P\sigma) \subseteq \mathrm{n}(\pi_1(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)})))$ *and* $\mathrm{fn}(Q\rho) \subseteq \mathrm{n}(\pi_2(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)})))$.

Assume that $P\sigma \xrightarrow[S_1]{\mu_1} P'$ *with* $\mathrm{bn}(\mu_1) \cap \mathrm{n}(\pi_1(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))) = \emptyset$ *and* $\mathrm{ch}(\mu_1) \in \pi_1(\mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)})))$ *(if* $\mu_1 \neq \tau$*).*

Since $P_0 >_{\mathrm{o}} P$, *we have* $P_0\sigma >_{\mathrm{o}} P\sigma$. *So by Lemma 4, we have* $P_0\sigma \xrightarrow[S_1]{\mu_1} P'_0$ *with* $P'_0 >_{\mathrm{o}} P'$ *because* $\mathrm{bn}(\mu_1) \cap \mathrm{fn}(P_0\sigma) = \emptyset$.

Then by Lemma 5, since $\mathrm{n}(\mathrm{cosupp}(\sigma)) \cap \mathrm{bn}(\mu_1) = \emptyset$, *we have* $P_0 \xrightarrow[(\nu\tilde{c})\,\phi_1]{\mu'_1} P_1$ *with* $P_1\sigma >_{\mathrm{o}} P'_0$, $\mathbf{e}(\phi_1\sigma)$, $\mathrm{n}(\sigma) \cap \{\tilde{c}\} = \emptyset$, $\mathbf{e}_{\mathrm{c}}(\mu'_1\sigma) = \mu_1$ *and* $S_1 = \mathbf{nc}(\phi_1\sigma) \setminus \{\tilde{c}\}$.

Since $P_0 \sim_{\mathrm{SO}}^{\mathsf{se}} Q_0$, *we have* $Q_0 \xrightarrow[(\nu\tilde{d})\,\phi_2]{\mu'} Q_1$ *with* $\mathrm{n}(\rho) \cap \{\tilde{d}\} = \emptyset$, $\mathbf{e}(\phi_2\rho)$, $\mathrm{bn}(\mu') \cap \mathrm{n}(\pi_2(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))) = \emptyset$ *and* $P_1\sigma \sim_{\mathrm{SO}}^{\mathsf{se}'} Q_1\rho$ *with* se' *depending on* μ'_1.

So by Lemma 5, since $\mathrm{n}(\mathrm{cosupp}(\rho)) \cap \mathrm{bn}(\mu') = \emptyset$, *we have* $Q_0\rho \xrightarrow[\mathbf{nc}(\phi_2\rho)\setminus\{\tilde{d}\}]{\mathbf{e}_{\mathrm{c}}(\mu'\rho)} Q'_0$ *with* $Q_1\rho >_{\mathrm{o}} Q'_0$.

Since $Q_0 >_{\mathrm{o}} Q$, *we have* $Q_0\rho >_{\mathrm{o}} Q\rho$ *so by Lemma 4, since* $\mathrm{bn}(\mathbf{e}_{\mathrm{c}}(\mu'\rho)) = \mathrm{bn}(\mu')$ *and* $\mathrm{bn}(\mu') \cap \mathrm{fn}(Q_0\rho) = \emptyset$, $Q\rho \xrightarrow[\mathbf{nc}(\phi_2\rho)\setminus\{\tilde{d}\}]{\mathbf{e}_{\mathrm{c}}(\mu'\rho)} Q'$ *with* $Q'_0 >_{\mathrm{o}} Q'$. *We thus*

have $Q_1\rho >_{\mathrm{o}} Q'$ *and* $P_1\sigma >_{\mathrm{o}} Q'$. *Moreover* $\mathrm{bn}(\mathbf{e}_{\mathrm{c}}(\mu'\rho)) = \mathrm{bn}(\mu')$ *so* $\mathrm{bn}(\mathbf{e}_{\mathrm{c}}(\mu'\rho)) \cap \mathrm{n}(\pi_2(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))) = \emptyset$.

We then do a case analysis on μ_1

- *if* $\mu_1 = \tau$ *then* $\mu_1' = \tau$ *thus* $\mu' = \tau$ *and* $\mu_2 := \mathbf{e}_{\mathrm{c}}(\mu'\rho) = \tau$.
  We have $\mathsf{se}' = \mathsf{se}_B^{(\sigma,\rho)} \oplus_{\mathrm{c}} (S_1, S_2)$ *where* $S_2 = \mathbf{nc}(\phi_2\rho) \setminus \{\tilde{d}\}$.
  Since $P_1\sigma \sim_{\mathrm{SO}}^{\mathsf{se}'} Q_1$, $P_1\sigma >_{\mathrm{o}} Q'$ *and* $Q_1\rho >_{\mathrm{o}} Q'$, *we have* $(\mathsf{se}', P', Q') \in \mathcal{R}$.
- *if* $\mu_1 = a_1(x_1)$ *then* $\mu_1' = E_1(x_1)$ *with* $\mathbf{e}_{\mathrm{c}}(E_1\sigma) = a_1$. *Thus* $\mu' = E_2(x_2)$ *and* $\mu_2 := \mathbf{e}_{\mathrm{c}}(\mu'\rho) = a_2(x_2)$.
  We also have $(\mathbf{e}_{\mathrm{c}}(E_1), \mathbf{e}_{\mathrm{c}}(E_2)) \in \mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))$ *i.e.* $(a_1, a_2) \in \mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))$.
  And $\mathsf{se}' = \mathsf{se}_B^{(\sigma,\rho)} \oplus_{\mathrm{i}} (x_1, x_2) \oplus_{\mathrm{c}} (S_1, S_2)$ *where* $S_2 = \mathbf{nc}(\phi_2\rho) \setminus \{\tilde{d}\}$.
  As above, we conclude that $(\mathsf{se}', P', Q') \in \mathcal{R}$.
- *if* $\mu_1 = (\nu \tilde{z_1})\,\overline{a_1}\,M_1$ *then* $\mu_1' = (\nu \tilde{z_1})\,\overline{E_1}\,F_1$ *with* $\mathbf{e}_{\mathrm{c}}(E_1\sigma) = a_1$ *and* $\mathbf{e}_{\mathrm{c}}(F_1\sigma) = M_1$. *Thus* $\mu' = (\nu \tilde{z_2})\,\overline{E_2}\,F_2$ *and* $\mu_2 := \mathbf{e}_{\mathrm{c}}(\mu'\rho) = (\nu \tilde{z_2})\,\overline{a_2}\,M_2$ *where* $a_2 = \mathbf{e}_{\mathrm{c}}(E_2\rho)$ *and* $M_2 = \mathbf{e}_{\mathrm{c}}(F_2\rho)$.
  We also have $(\mathbf{e}_{\mathrm{c}}(E_1), \mathbf{e}_{\mathrm{c}}(E_2)) \in \mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))$ *i.e.* $(a_1, a_2) \in \mathcal{I}(\mathfrak{H}(\mathsf{se}_B^{(\sigma,\rho)}))$.
  And $\mathsf{se}' = \mathsf{se}_B^{(\sigma,\rho)} \oplus_{\mathrm{o}} (\mathbf{e}_{\mathrm{c}}(F_1\sigma), \mathbf{e}_{\mathrm{c}}(F_2\sigma)) \oplus_{\mathrm{c}} (S_1, S_2)$ *where* $S_2 = \mathbf{nc}(\phi_2\rho) \setminus \{\tilde{d}\}$.
  As above, we conclude that $(\mathsf{se}', P', Q') \in \mathcal{R}$.