Safe Reasoning with Logic LTS

Gerald Lüttgen[1] and Walter Vogler[2]

[1] Department of Computer Science, University of York, York YO10 5DD, U.K.
luettgen@cs.york.ac.uk
[2] Institut für Informatik, Universität Augsburg, D–86135 Augsburg, Germany
vogler@informatik.uni-augsburg.de

Abstract. Previous work has introduced the setting of Logic LTS, together with a variant of ready simulation as fully-abstract refinement preorder, which allows one to compose operational specifications using a CSP-style parallel operator as well as the propositional connectives conjunction and disjunction. In this paper, we show how a temporal logic for specifying safety properties may be embedded into Logic LTS so that (a) the temporal operators are compositional for ready simulation and (b) ready simulation, when restricted to pairs of processes and formulas, coincides with the logic's satisfaction relation. The utility of this setting as a semantic foundation for mixed operational and temporal-logic specification languages is demonstrated via a simple example.

1 Introduction

Recently, the setting of Logic LTS has been introduced which combines operational and logic styles of specification [13, 14] in one unified framework. It includes operational operators, such as parallel composition, and the propositional-logic operators conjunction and disjunction. Logic LTS extends labelled transition systems by an *inconsistency* predicate on states, where an inconsistent state, or process, denotes empty behaviour that cannot be implemented (cf. Sec. 2). Inconsistencies may arise when conjunctively composing processes with different ready sets, i.e., initial action sets [13]. The refinement preorder $\sqsubseteq_{\mathrm{RS}}$ adapted for Logic LTS is a variant of ready simulation [2, 6, 17]. It is fully abstract wrt. a reference preorder that relates consistent implementations only to consistent specifications [14], i.e., it is the coarsest compositional preorder wrt. parallel composition, conjunction and disjunction when taking consistency into account. Most notably, the setting justifies a simulation-type preorder when starting from the binary basic observable 'consistency'.

This paper extends Logic LTS by temporal-logic operators, thereby fulfilling our ultimate goal of combining process algebraic and temporal logic operators in a uniform compositional refinement setting in which logical satisfaction and process refinement can be used interchangeably. The temporal logic of interest is a branching-time logic, allowing one to specify the most important class of temporal properties in practice, viz. *safety properties*, over atomic propositions that refer to the enabledness of actions; in particular, we consider the standard temporal operators *always* and *unless* (*weak until*). These operators will be embedded into Logic LTS such that the logic satisfaction relation $\models$ is compatible with $\sqsubseteq_{\mathrm{RS}}$ (cf. Sec. 3). This means that, firstly, $p \models \phi$ if and only if $p \sqsubseteq_{\mathrm{RS}} \phi$, for any process p and temporal-logic formula ϕ; secondly, ready simulation is compositional for the temporal operators. Obviously, the logic's propositional operators will exactly match the ones that are already included in Logic LTS.

This setting is unique in the literature in that it allows one to *freely* mix operational operators, propositional logic operators and temporal logic operators, while still permitting *compositional* reasoning, as discussed in the related work section below (cf. Sec. 5). Our work is strongly inspired by current research into novel notations and methodologies for developing software, where requirements and designs of behaviourally complex systems are regularly specified using a mixture of declarative and operational languages, allowing for the traceable transitioning from software requirements to designs. At the requirements level, popular languages include restricted forms of English or simple spreadsheets (*declarative, also temporal*) and block diagrams or state machines (*operational*). At design level, UML class diagrams combined with the Object Constraint Language (*declarative, partly temporal*) and Statecharts (*operational*) are frequently used. The setting presented in this paper serves as the semantic backbone for a related, industry-supported research project[3] that extends Statecharts with temporal-logic-style contracts and employs ready simulation $\sqsubseteq_{\mathrm{RS}}$ for compositional model checking. Indeed, our main theorem proving the compatibility of $\models$ with $\sqsubseteq_{\mathrm{RS}}$ (Thm. 12) provides a formal basis for compositional verification.

2 The Setting of Logic LTS

We begin with briefly recalling the setting of Logic LTS as introduced in [13, 14], together with several results and notations that are relevant to this paper.

Inconsistency. Logic LTS considers *inconsistencies* that may arise under conjunctive composition as first-class observables. A conjunctively composed state between two processes is marked as inconsistent, if one offers an action that the other cannot perform, i.e., if the processes have different *ready sets.* Consider the processes p, q and r in Fig. 1(a). Process p and q specify that exactly action a and resp. b is offered initially, i.e., their ready sets are $\{a\}$ and resp. $\{b\}$. Similarly, r specifies that a and b are offered initially and thus has ready set $\{a, b\}$. Hence, $p \wedge q$ and $p \wedge r$ are *inconsistent* (or *false*), and should be tagged as such. Formally, our variant of LTS will be augmented by an *inconsistency predicate* F, so that $p \wedge q,\ p \wedge r \in F$ in our example. Observe also that, e.g., according to failures semantics [3], p and q (resp. p and r) do not have a common implementation.

Most notably, inconsistencies may propagate backwards along transitions. For example, in the conjunction $p' \wedge q'$ shown in Fig. 1(b), both conjuncts require action a to be performed, whence $p' \wedge q'$ should have an a-transition. But

[3] "*Refinement Patterns for Contractual Statecharts*"; funded by the EPSRC under grant no. EP/E034853/1.

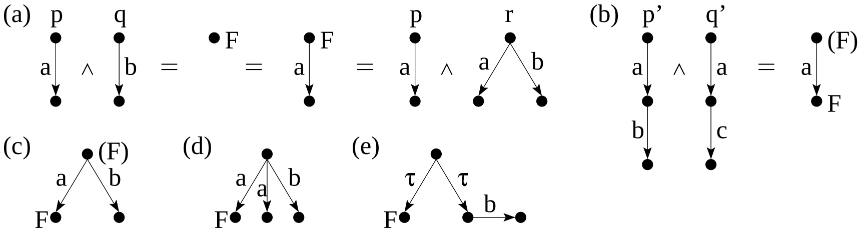

Fig. 1. (a)–(b): Conjunctive composition; (c)–(e): Backward propagation.

this transition does lead to an inconsistent state and, in the absence of any alternative a-transition leading to a consistent state, $p' \wedge q'$ must itself be considered inconsistent. In this spirit, inconsistency propagates backwards for the process in Fig. 1(c), whereas it does not for the processes in Figs. 1(d) and 1(e). Note that in Fig. 1(e), actions τ are used to specify the disjunction between alternatives.

Formal definitions. Let $\mathcal{A}$ be a non-empty alphabet of visible actions with representatives a and b. With τ being a distinguished, internal action, let $\mathcal{A}_\tau$ denote $\mathcal{A} \cup \{\tau\}$ with representatives α and β. An LTS is a triple $\langle P, \longrightarrow, F\rangle$, where P is the set of *processes* (states), $\longrightarrow \subseteq P \times \mathcal{A}_\tau \times P$ is the *transition relation*, and $F \subseteq P$ is the *inconsistency predicate*. We write $p \xrightarrow{\alpha} p'$ instead of $\langle p, \alpha, p'\rangle \in \longrightarrow$, and $\mathcal{I}(p)$ stands for the ready set $\{\alpha \in \mathcal{A}_\tau \,|\, p \xrightarrow{\alpha}\}$ of p. A process p that cannot engage in a τ-transition, i.e., $p \not\xrightarrow{\tau}$, is called *stable*.

We introduce weak transitions by writing (i) $p \overset{\epsilon}{\Longrightarrow} p'$ if $p \xrightarrow{\tau}{}^{*} p'$; and (ii) $p \overset{a}{\Longrightarrow} p'$ if $\exists \overline{p}, \overline{p}'.\, p \overset{\epsilon}{\Longrightarrow} \overline{p} \xrightarrow{a} \overline{p}' \overset{\epsilon}{\Longrightarrow} p'$. If all processes along a computation $p \overset{\epsilon}{\Longrightarrow} p'$ or $p \overset{a}{\Longrightarrow} p'$, including p and p', are consistent, we write $p \overset{\epsilon}{\Longrightarrow}_{\mathrm{F}} p'$ and resp. $p \overset{a}{\Longrightarrow}_{\mathrm{F}} p'$. If in addition p' is stable, we write $p \overset{\epsilon}{\Longrightarrow}\!| \, p'$ and resp. $p \overset{a}{\Longrightarrow}\!| \, p'$. With this, we introduce a notion to deal with *divergence*, i.e., infinite sequences of τ-transitions, where divergence is viewed as catastrophic if a process cannot stabilise: process p *cannot stabilise* if $\nexists p'.\, p \overset{\epsilon}{\Longrightarrow}\!| \, p'$.

Moreover, we require an LTS to satisfy the following *τ-purity* condition: $p \xrightarrow{\tau}$ implies $\nexists a \in \mathcal{A}.\, p \xrightarrow{a}$, for all $p \in P$. Hence, each process represents either an external or internal (disjunctive) choice between its outgoing transitions. This restriction reflects the fact that ready sets can only be observed at stable states, and is justified in [13]. Logic LTSs must satisfy two further properties, of which the first one formalises our backward propagation of inconsistencies:

Definition 1 (Logic LTS [13]). An LTS $\langle P, \longrightarrow, F\rangle$ is a *Logic LTS* if

(LTS1) $F \subseteq P$ such that $p \in F$ if $\exists \alpha \in \mathcal{I}(p)\, \forall p' \in P.\, p \xrightarrow{\alpha} p' \implies p' \in F$;
(LTS2) p cannot stabilise $\implies p \in F$.

Operators. Logic LTSs are equipped with various propositional-logic and process-algebraic operators; we can only give a brief account here and refer the reader to [13, 14] for details. The *parallel operator* $\|_A$, for some synchronisation alphabet $A \subseteq \mathcal{A}$, is essentially the one of CSP [3], but favours τ-transitions over visible transitions so as to preserve τ-purity. Naturally, $p \;\|_A\; q$ is inconsistent if p or q is inconsistent. The *conjunction operator* $\wedge$ is a synchronous product (or parallel composition) for visible transitions and an asynchronous product for τ-transitions, and thus also favours τ-transitions. Process $p \wedge q$ is inconsistent if p or q is inconsistent; or if p and q are stable but have different ready sets; or if it becomes inconsistent by backward propagation.

The *disjunction operator* $\vee$ is an internal choice operator, where $p \vee q$ is inconsistent if both p and q are. Fig. 1(e) depicts a disjunction of an inconsistent process with a consistent process that can engage in action b; hence, the disjunctive process is consistent. Thus, $p \vee q$ essentially is a process with two τ-transitions to p and resp. q; correspondingly, τ is not so much seen as an internal action in our setting but primarily indicates a logical disjunct.

Refinement. Our refinement preorder is a variant of ready simulation [2, 6, 17]:

Definition 2 (Ready simulation on Logic LTS [14]). Let $\langle P, \longrightarrow_P, F_P \rangle$ and $\langle Q, \longrightarrow_Q, F_Q \rangle$ be two Logic LTSs. Relation $\mathcal{R} \subseteq P \times Q$ is a *stable ready simulation relation*, if the following conditions hold, for any $\langle p, q \rangle \in \mathcal{R}$, $a \in \mathcal{A}$:

(RS1) p, q stable; **(RS3)** $p \overset{a}{\Longrightarrow}\!|\, p' \implies \exists q'.\, q \overset{a}{\Longrightarrow}\!|\, q'$ and $\langle p', q' \rangle \in \mathcal{R}$;
(RS2) $p \notin F_P \implies q \notin F_Q$; **(RS4)** $p \notin F_P \implies \mathcal{I}(p) = \mathcal{I}(q)$.

We write $p \underset{\sim}{\sqsubset}_{\mathrm{RS}} q$ if there exists a stable ready simulation relation $\mathcal{R}$ such that $\langle p, q \rangle \in \mathcal{R}$. Further, p is *ready simulated* by q, in symbols $p \sqsubseteq_{\mathrm{RS}} q$, if $\forall p'.\, p \overset{\epsilon}{\Longrightarrow}\!|\, p' \implies \exists q'.\, q \overset{\epsilon}{\Longrightarrow}\!|\, q'$ and $p' \underset{\sim}{\sqsubset}_{\mathrm{RS}} q'$. Finally, we let $=_{\mathrm{RS}}$ stand for the kernel of $\sqsubseteq_{\mathrm{RS}}$.

While we allow transitions leaving inconsistent states, they are ignored in the above definition. Thus, one may remove such transitions without changing the relevant behaviour of processes; for technical convenience, we do not include this additional normalisation when defining our operators. Our operators satisfy the following properties wrt. $\sqsubseteq_{\mathrm{RS}}$:

Proposition 3 ([14]). *Let p, q, r be processes, $p' \sqsubseteq_{RS} q'$ and $A \subseteq \mathcal{A}$.*

- Compositionality: $p' \wedge r \sqsubseteq_{RS} q' \wedge r$, $p' \vee r \sqsubseteq_{RS} q' \vee r$, $p' \|_A r \sqsubseteq_{RS} q' \|_A r$;
- $\wedge$ is conjunction: $r \sqsubseteq_{RS} p \wedge q \iff r \sqsubseteq_{RS} p$ *and* $r \sqsubseteq_{RS} q$;
- $\vee$ is disjunction: $p \vee q \sqsubseteq_{RS} r \iff p \sqsubseteq_{RS} r$ *and* $q \sqsubseteq_{RS} r$.

The second item above demonstrates that $\wedge$ is indeed conjunction: clearly, a process should implement a conjunction if and only if it implements both conjuncts.

In addition, we have shown in [14] that relation $\sqsubseteq_{\mathrm{RS}}$ is fully abstract for the preorder $\sqsubseteq_F$, which is defined by $p \sqsubseteq_F q$ iff $q \in F_Q \implies p \in F_P$ (i.e., an inconsistent specification q cannot have a consistent implementation p as refinement). This means that our simulation-type preorder is justified simply by starting from a binary basic observable, namely consistency.

3 Temporal Logic & Logic LTS

The temporal properties we embed in Logic LTS are essentially the safety properties of the universal fragment of *action-based CTL* [4], adapted to our setting.

This is the largest fragment we can hope for since, firstly, Logic LTS is based on standard LTS, without Büchi annotations or similar acceptance conditions. Hence, finite-state Logic LTS is not expressive enough for encoding liveness (or fairness) properties. Secondly, we wish for the logic satisfaction relation $\models$ to be compatible with $\sqsubseteq_{\mathrm{RS}}$, i.e., $p \models \phi \iff p \sqsubseteq_{\mathrm{RS}} \phi$, for any process p and formula ϕ. Hence, by transitivity of $\sqsubseteq_{\mathrm{RS}}$, we have that $p \sqsubseteq_{\mathrm{RS}} q$ and $q \models \phi$ implies $p \models \phi$, i.e., the implementation p with the 'smaller' behaviour has to satisfy more formulas than the specification q. This justifies our focus on the *universal* fragment. Therefore, we consider the following set $\mathcal{F}$ of temporal formulas ϕ:

$$\phi ::= \mathit{tt} \mid \mathit{ff} \mid \mathit{en}(a) \mid \mathit{dis}(a) \mid \phi \vee \phi \mid \phi \wedge \phi \mid [a]\phi \mid \Box\phi \mid \phi \mathsf{W} \phi$$

Here, the atomic propositions $\mathit{en}(a)$ and $\mathit{dis}(a)$ denote the enabledness and resp. disabledness of action a, and $[a]$, $\Box$ and W are the usual *next*, *always* (*generally*) and *unless* (*weak until*) operators. Note that formula tt (resp. ff) may be derived as $\mathit{en}(a) \vee \mathit{dis}(a)$ (resp. $\mathit{en}(a) \wedge \mathit{dis}(a)$); moreover, $\Box\phi$ is equivalent to $\phi \mathsf{W} \mathit{ff}$.

Satisfaction relation. Recall that, in our setting, action τ is not so much seen as an internal action, but an instable process p is a 'disjunction'; hence, $p \models \phi$ should mean that $p_0 \models \phi$ for all 'disjuncts' p_0 of p, i.e., for each p_0 with $p \overset{\epsilon}{\Longrightarrow}| \, p_0$. Thus, we define $\models$ as follows, where $\overset{\mathcal{A}}{\Longrightarrow}|$ stands for $\bigcup_{a \in \mathcal{A}} \overset{a}{\Longrightarrow}|$:

Definition 4 (Satisfaction relation). Given a Logic LTS with state set P, the satisfaction relation $\models \subseteq P \times \mathcal{F}$ is defined by the following rules:

$$\begin{array}{llll}
p \models \mathit{tt} & \text{always} & p \models \mathit{en}(a) & \text{if } \forall p_0 .\, p \overset{\epsilon}{\Longrightarrow}| \, p_0 \implies p_0 \overset{a}{\longrightarrow} \\
p \models \mathit{ff} & \text{if } p \in F & p \models \mathit{dis}(a) & \text{if } \forall p_0 .\, p \overset{\epsilon}{\Longrightarrow}| \, p_0 \implies p_0 \overset{a}{\not\longrightarrow}
\end{array}$$

$$\begin{array}{ll}
p \models \phi \vee \psi & \text{if } \forall p_0 .\, p \overset{\epsilon}{\Longrightarrow}| \, p_0 \implies (p_0 \models \phi \text{ or } p_0 \models \psi) \\
p \models \phi \wedge \psi & \text{if } \forall p_0 .\, p \overset{\epsilon}{\Longrightarrow}| \, p_0 \implies (p_0 \models \phi \text{ and } p_0 \models \psi) \\
 & \\
p \models [a]\phi & \text{if } \forall p_0, p_1 .\ p \overset{\epsilon}{\Longrightarrow}| \, p_0 \overset{a}{\Longrightarrow}| \, p_1 \implies p_1 \models \phi \\
p \models \Box\phi & \text{if } (p_n \models \phi \text{ whenever } p \overset{\epsilon}{\Longrightarrow}| \, p_0 \overset{\mathcal{A}}{\Longrightarrow}| \, p_1 \ldots \overset{\mathcal{A}}{\Longrightarrow}| \, p_n) \\
p \models \phi \mathsf{W} \psi & \text{if } (p_n \models \phi \text{ or } \exists i \leq n .\, p_i \models \psi, \text{ whenever } p \overset{\epsilon}{\Longrightarrow}| \, p_0 \overset{\mathcal{A}}{\Longrightarrow}| \, p_1 \ldots \overset{\mathcal{A}}{\Longrightarrow}| \, p_n)
\end{array}$$

This definition coincides for τ-less p with the standard one but, in contrast to processes within LTS, ff is satisfiable, namely by inconsistent processes.

To motivate the quantification "$\forall p_0 .\, p \overset{\epsilon}{\Longrightarrow}| \, p_0$" for the $\vee$-case further, consider that $\models$ must be defined such that the process p that has one initial a-transition followed by a b-transition, satisfies formula $[a]\mathit{en}(b)$. Similarly, the process q that has one initial a-transition followed by a c-transition, should satisfy $[a]\mathit{en}(c)$. Since we aim for a setting in which $\models$ may be freely replaced by $\sqsubseteq_{\mathrm{RS}}$ and since $\sqsubseteq_{\mathrm{RS}}$ is a precongruence, we must have $p \vee q \models [a]\mathit{en}(b) \vee [a]\mathit{en}(c)$. In a classic definition of satisfiability, this would mean $p \vee q \models [a]\mathit{en}(b)$ or $p \vee q \models [a]\mathit{en}(c)$, which are both clearly false. In addition and as claimed above, each process p indeed satisfies $\mathit{en}(a) \vee \mathit{dis}(a)$ since each 'disjunct' p_0 of p is stable and hence either can engage in a (i.e., satisfies $\mathit{en}(a)$) or cannot (i.e., satisfies $\mathit{dis}(a)$).

As an aside and provided that p and q belong to Logic LTSs that are *finitely branching*, we get the following Hennessy-Milner-style characterisation of $\sqsubseteq_{\text{RS}}$, where $\mathcal{F}_{\text{RS}}$ are the *essential formulas*, namely the formulas in $\mathcal{F}$ that do neither contain operators $\wedge$, $\Box$ and W, nor sub-formulas tt and $dis(a)$:

Theorem 5 (Characterisation). *$p \sqsubseteq_{RS} q \iff \forall \phi \in \mathcal{F}_{RS}.\, q \models \phi \implies p \models \phi$.*

This characterisation is more or less a corollary to an analogous result of Bloom [2]. In his thesis, Bloom considered a characterisation based on the opposite implication than the one we require. Correspondingly, he used the dual fragment of formulas, e.g., employing $\langle a \rangle$-modalities instead of $[a]$-modalities.

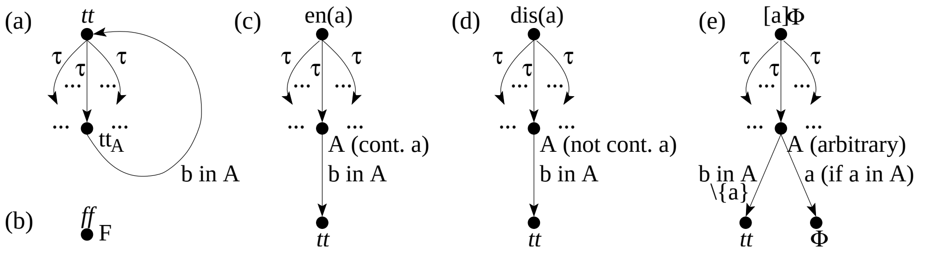

Fig. 2. Embedding of temporal-logic formulas into Logic LTS.

Embedding in Logic LTS. Next, we embed our temporal formulas into Logic LTS and present the desired compatibility result between $\models$ and $\sqsubseteq_{\text{RS}}$. The embedding is conducted along the structure of formulas. Formula tt corresponds to the initial state of the Logic LTS sketched in Fig. 2(a), which can nondeterministically select an arbitrary ready set $A \subseteq \mathcal{A}$ via a τ-transition to process tt_A. From there, it can engage in any transition labelled with an action $b \in A$ and return to tt. Hence, tt is a process that can simulate any other process, and is thus indeed the desired 'universal' process. Formula ff is trivially mapped to the inconsistent process depicted in Fig. 2(b), which can only ready simulate an inconsistent process. Formula $en(a)$ corresponds to the initial state of the Logic LTS in Fig. 2(c). This can select any ready set A containing a by silently moving to process A, from where it can engage in a b-transition, for any $b \in A$, to process tt. We embed formula $dis(a)$ analogously, where we require $a \notin A$ instead of $a \in A$; see Fig. 2(d).

Formula $\phi \wedge \psi$ (resp. $\phi \vee \psi$) is embedded by conjunctively (resp. disjunctively) composing the Logic LTSs of the embeddings of ϕ and ψ, using operator $\wedge$ (resp. $\vee$) on Logic LTS. The embedding of a formula $[a]\phi$ is sketched in Fig. 2(e). Again, the initial process may choose an arbitrary ready set A. The corresponding process A can engage in a b-step, for any $b \in A \setminus \{a\}$, to tt. In addition, if $a \in A$, there is an a-step to the initial state of ϕ's embedding. Hence, any a-derivative of $[a]\phi$ behaves as ϕ, whereas arbitrary behaviour is permitted for differently labelled derivatives. We now define $\Box$- and W-operators on Logic LTS, which facilitate the straightforward embedding of formulas $\Box\phi$ and $\phi \mathsf{W} \psi$:

Definition 6 ($\Box$-operator, "always"). Let $\langle P, \longrightarrow_P, F_P \rangle$ be a Logic LTS. Then, $\Box p$, for $p \in P$, is process (p) in Logic LTS $\langle \Box P, \longrightarrow_{\Box P}, F_{\Box P} \rangle$, where:

- $\Box P =_{\mathrm{df}} \{\vec{p} = (p_1, p_2, \dots, p_n) \,|\, n{\geq}1,\ \forall 1{\leq}i{\leq}n.\, p_i{\in}P\}$ is the set of finite vectors over P.
- $\longrightarrow_{\Box P}$ is defined by the following operational rules:

$$\begin{array}{rcl} p_i \xrightarrow{\tau}_P p_i' & \Longrightarrow & (p_1, \dots, p_i, \dots, p_n) \xrightarrow{\tau}_{\Box P} (p_1, \dots, p_i', \dots, p_n) \\ \forall i.\, p_i \xrightarrow{a}_P p_i' & \Longrightarrow & (p_1, \dots, p_n) \xrightarrow{a}_{\Box P} (p_1', \dots, p_n', p)\,. \end{array}$$

- $F_{\Box P}$ is the least set of finite vectors such that $\vec{p} = (p_1, \dots, p_n) \in F_{\Box P}$ if any one of the following conditions holds:

  (BF1) $\exists i.\, p_i \in F_P$;
  (BF2) $\vec{p}$ stable but $\exists i, j.\, \mathcal{I}_P(p_i) \neq \mathcal{I}_P(p_j)$;
  (BF3) $\exists \alpha \in \mathcal{I}_{\Box P}(\vec{p})\, \forall \vec{p}'.\, \vec{p} \xrightarrow{\alpha}_{\Box P} \vec{p}' \implies \vec{p}' \in F_{\Box P}$;
  (BF4) $\vec{p}$ cannot stabilise outside $F_{\Box P}$.

In the sequel, we use the convention that $\vec{p} \in \Box P$ has components $p_1, p_2, \dots, p_n$. Observe that $\langle \Box P, \longrightarrow_{\Box P}, F_{\Box P} \rangle$ is indeed a Logic LTS and that $\vec{p}$ behaves as the conjunction $\bigwedge_i p_i$. Intuitively, the above construction adds p to the process vector after every visible step, so that any stable process along a computation must respect p.

The vector notation that is employed in the above definition is convenient for proving compositionality, but it immediately leads to an infinite state space. However, we could have used process *sets* instead of process vectors, which would result in an $=_{\mathrm{RS}}$-equivalent definition. Most importantly, this would make the process sets of $\Box P$ finite if P is finite, and would thus permit a straightforward implementation of the $\Box$-operator.

Definition 7 (W-operator, "unless"). Let $\langle P, \longrightarrow_P, F_P \rangle$ and $\langle Q, \longrightarrow_Q, F_Q \rangle$ be Logic LTSs. Then, $p\mathsf{W}q$, for $p \in P$ and $q \in Q$, is a process within the Logic LTS $\langle P\mathsf{W}Q, \longrightarrow_{P\mathsf{W}Q}, F_{P\mathsf{W}Q} \rangle$, where:

- $P\mathsf{W}Q =_{\mathrm{df}} \{p\mathsf{W}q\} \cup \Box P \cup (\Box P \times Q)$ with $\Box P = \{\vec{p} \,|\, n{\geq}1,\ \forall 1{\leq}i{\leq}n.\, p_i \in P\}$.
- $\longrightarrow_{P\mathsf{W}Q}$ is defined by the following operational rules:

$$\begin{array}{rcl} \multicolumn{3}{l}{\text{always } p\mathsf{W}q \xrightarrow{\tau}_{P\mathsf{W}Q} \langle (), q \rangle} \\ \multicolumn{3}{l}{\text{always } p\mathsf{W}q \xrightarrow{\tau}_{P\mathsf{W}Q} (p)} \\ p_i \xrightarrow{\tau}_P p_i' & \Longrightarrow & (p_1, \dots, p_i, \dots, p_n) \xrightarrow{\tau}_{P\mathsf{W}Q} (p_1, \dots, p_i', \dots, p_n) \\ \forall i.\, p_i \xrightarrow{a}_P p_i' & \Longrightarrow & (p_1, \dots, p_n) \xrightarrow{a}_{P\mathsf{W}Q} \langle (p_1', \dots, p_n'), q \rangle \\ \forall i.\, p_i \xrightarrow{a}_P p_i' & \Longrightarrow & (p_1, \dots, p_n) \xrightarrow{a}_{P\mathsf{W}Q} (p_1', \dots, p_n', p) \\ q' \xrightarrow{\tau}_Q q'' & \Longrightarrow & \langle (p_1, \dots, p_n), q' \rangle \xrightarrow{\tau}_{P\mathsf{W}Q} \langle (p_1, \dots, p_n), q'' \rangle \\ p_i \xrightarrow{\tau}_P p_i' & \Longrightarrow & \langle (p_1, \dots, p_n), q' \rangle \xrightarrow{\tau}_{P\mathsf{W}Q} \langle (p_1, \dots, p_i', \dots, p_n), q' \rangle \\ q' \xrightarrow{a}_Q q'' & \text{and} & \\ \forall i.\, p_i \xrightarrow{a}_P p_i' & \Longrightarrow & \langle (p_1, \dots, p_n), q' \rangle \xrightarrow{a}_{P\mathsf{W}Q} \langle (p_1', \dots, p_n'), q'' \rangle\,. \end{array}$$

- $F_{P\mathsf{W}Q}$ is the least set such that $r \in F_{P\mathsf{W}Q}$ if any one of these conditions holds:
  (RF1) r equals $\vec{p}$ or $\langle \vec{p}, q' \rangle$ so that $\exists i.\, p_i \in F_P$, or $r = \langle \vec{p}, q' \rangle$ and $q' \in F_Q$;
  (RF2) r is stable, equals $\vec{p}$ or $\langle \vec{p}, q' \rangle$ and $\exists i, j.\, \mathcal{I}_P(p_i) \neq \mathcal{I}_P(p_j)$,
  or $r = \langle \vec{p}, q' \rangle$ stable and $\exists i.\, \mathcal{I}_P(p_i) \neq \mathcal{I}_Q(q')$;
  (RF3) $\exists \alpha \in \mathcal{I}(r)\, \forall r'.\, r \xrightarrow{\alpha}_{P\mathsf{W}Q} r' \implies r' \in F_{P\mathsf{W}Q}$;
  (RF4) r cannot stabilise outside $F_{P\mathsf{W}Q}$.

Again, the resulting Logic LTS is well-defined; processes $\langle \vec{p}, q \rangle$ should be thought of as $\bigwedge_i p_i \wedge q$. Intuitively, $p\mathsf{W}q$ behaves similarly to $\Box p$; however, initially and at any stable state along a computation, it may recede in conjoining p in favour of a one-off conjunction of q.

Theorem 8 (Compositionality). *Let $p \sqsubseteq_{RS} q$, $r \sqsubseteq_{RS} s$ and $a \in \mathcal{A}$. Then, $[a]p \sqsubseteq_{RS} [a]q$, $\Box p \sqsubseteq_{RS} \Box q$ and $p\mathsf{W}r \sqsubseteq_{RS} q\mathsf{W}s$.*

See the appendix for the proof. An essential point is the reasoning about inconsistencies; e.g., for a $\Box P$ Logic LTS, we adapt the concept of witness of [13] as follows:

Definition 9 ($\Box$-witness). A $\Box$-*witness* for $\Box P$ is a set $W \subseteq \Box P$ such that, for all $\vec{p} \in W$, the following conditions hold:
(W1) $\forall i.\, p_i \notin F_P$;
(W2) $\vec{p}$ stable $\implies \forall i, j.\, \mathcal{I}_P(p_i) = \mathcal{I}_P(p_j)$;
(W3) $\forall \alpha \in \mathcal{I}_{\Box P}(\vec{p}) \exists \vec{p}'.\, \vec{p} \xrightarrow{\alpha}_{\Box P} \vec{p}'$ and $\vec{p}' \in W$;
(W4) $\vec{p}$ can stabilise in W, i.e., $\exists \vec{p}', \vec{p}_1, \ldots \vec{p}_m.\, \vec{p} \xrightarrow{\tau}_{\Box P} \vec{p}_1 \xrightarrow{\tau}_{\Box P} \ldots$
$\ldots \xrightarrow{\tau}_{\Box P} \vec{p}_m = \vec{p}' \not\xrightarrow{\tau}_{\Box P}$ and $\forall i.\, \vec{p}_i \in W$.

The following straightforward property of $\Box$-witnesses gives us a useful tool for proving that *always* processes are consistent:

Proposition 10. *$\vec{p} \notin F_{\Box P}$ if and only if $\exists\, \Box$-witness $W.\, \vec{p} \in W$.*

The concrete witness needed in the $\Box$-compositionality proof is the following:

Lemma 11 (Concrete witness). *Given stable $p \notin F_P$ and $q \in Q$ with $p \underset{\sim}{\sqsubset}_{RS} q$, the set $W =_{df} W_1 \cup W_2 \subseteq \Box Q$ is a $\Box$-witness, where*

$$W_1 =_{df} \{\vec{q} = (q_1, \ldots, q_n) \mid \exists \vec{p} = (p_1, \ldots, p_n).\, \vec{p} \notin F_{\Box P} \text{ and } \forall i.\, p_i \underset{\sim}{\sqsubset}_{RS} q_i\};$$
$$W_2 =_{df} \{\vec{q} = (q_1, \ldots, q_n) \mid \exists \vec{q}' = (q'_1, \ldots, q'_n)).\, \vec{q}' \in W_1 \text{ and } \forall i.\, q_i \overset{\epsilon}{\Longrightarrow}\!| \, q'_i\}\,.$$

A similar witness concept and construction is needed for proving the W-operator compositional. We may now prove the desired compatibility result:

Theorem 12 (Compatibility). *Let p be a process and ϕ a temporal-logic formula in $\mathcal{F}$. Then, $p \models \phi \iff p \sqsubseteq_{RS} \phi$.*

Corollary 13. $\phi \sqsubseteq_{\mathrm{RS}} \psi \iff \forall p.\ p \models \phi \implies p \models \psi$.

Duality. We conclude this section by briefly discussing negation. Since our setting of Logic LTS is not expressive enough to encode liveness properties, such as the formula $\neg\Box\phi$, we do not have negation. Furthermore, Thm. 12 implies for the stable process *ff* that $\mathit{ff} \models \mathit{tt}$ and $\mathit{ff} \models \mathit{ff}$. Hence, we cannot define "$p \models \neg\mathit{tt}$ if not $p \models \mathit{tt}$" for inconsistent p, since $\neg\mathit{tt}$ should be equivalent to *ff*. However, for *consistent* processes and propositional formulas, we can express negation in our $\neg$-less logic. To show this, we define for consistent p and propositional ϕ: $p \models \neg\phi$ if $\forall p_0.\ p \overset{\epsilon}{\Longrightarrow}| \, p_0 \implies$ not $p_0 \models \phi$; as well as for formulas ϕ and ψ: $\phi \dashv\models \psi$ if $\forall p \notin F.\ p \models \phi \iff p \models \psi$.

Proposition 14 (Dualities).

$$\begin{array}{lll} \neg\mathit{tt} \dashv\models \mathit{ff} & \neg\mathit{en}(a) \dashv\models \mathit{dis}(a) & \neg(\phi \wedge \psi) \dashv\models \neg\phi \vee \neg\psi \\ \neg\mathit{ff} \dashv\models \mathit{tt} & \neg\mathit{dis}(a) \dashv\models \mathit{en}(a) & \neg(\phi \vee \psi) \dashv\models \neg\phi \wedge \neg\psi \end{array}$$

As a consequence, we can specify implications for consistent processes, e.g., $\mathit{en}(a) \longrightarrow \mathit{dis}(b)$ can be expressed as $\mathit{dis}(a) \vee \mathit{dis}(b)$. Finally, note that one cannot replace $\dashv\models$ by $=_{\mathrm{RS}}$ in Prop. 14 since $=_{\mathrm{RS}}$ also relates inconsistent processes.

4 Example

Consider the specification of a very simple networking component. Sender S (cf. Fig. 3) receives messages from a user process on port `send` and passes them on, via port `in`, to channel C. The specification of C employs an off-the-shelf design P (cf. Fig. 3), a generic channel that may loose messages; additionally, the behaviour of P is restricted by a constraint $\psi =_{\mathrm{df}} \Box[\texttt{in}][\texttt{in}](\mathit{en}(\texttt{out}) \wedge \mathit{dis}(\texttt{in}))$. Intuitively, ψ ensures that at most one message may be lost in a row.

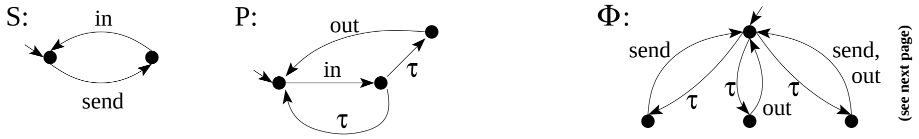

Fig. 3. Some Logic LTSs that occur in the example.

As an aside and assuming the availability of the standard process-algebraic prefix operator, ψ could equivalently be specified as $\Box[\texttt{in}][\texttt{in}]\texttt{out}.\mathit{tt}$, where $\texttt{out}.\mathit{tt}$ denotes the Logic LTS consisting of an `out`-transition from an initial state to process *tt*. Here, prefixing is employed as a compact notation for specifying that only a single action is allowed, which is especially useful (or even necessary) if the underlying alphabet is large (or infinite). This demonstrates one of the advantages of mixing operators from process algebras and temporal logics.

The overall specification of our example is now $\texttt{Spec} =_{\mathrm{df}} ((P \wedge \psi) \parallel_{\{\texttt{in}\}} S)/\texttt{in}$, where `/in` is a *hiding operator* on action `in`, similar to the identically named operator in CSP [9], which restricts the scope of `in` to `Spec` (cf. App. B for details). `Spec` is a truly *mixed* specification that conjunctively composes an operational component with a temporal-logic formula, and puts the result in

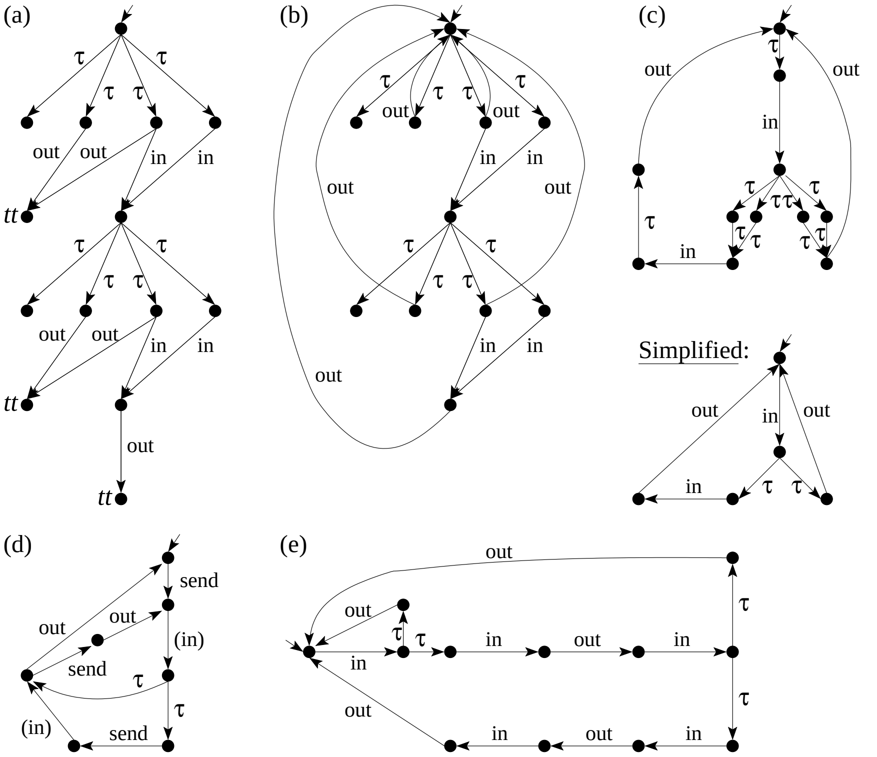

Fig. 4. Developing the Logic LTS of `Spec`.

parallel with another operational component while synchronising on the internal channel `in`. The Logic LTS semantics of `Spec` is successively developed along `Spec`'s structure in Fig. 4: (a) depicts the Logic LTS of $[\texttt{in}][\texttt{in}]\texttt{out}.tt$; (b) depicts the Logic LTS of ψ when reduced wrt. $=_{\text{RS}}$ (recall that there is a standard finite-state definition of the $\Box$-operator); (c) depicts the Logic LTS of $C =_{\text{df}} P \wedge \psi$ as well as a simplified, $=_{\text{RS}}$-equivalent version; and (d) depicts the simplified Logic LTS (omitting inconsistent states) of `Spec`, where label (`in`) stands for a τ that results from hiding `in`.[4]

Let us now assume that the designer wishes to verify that `Spec` does not deadlock: $\phi =_{\text{df}} \Box(en(\texttt{send}) \vee en(\texttt{out}))$, i.e., always `send` or `out` is enabled. To demonstrate $\texttt{Spec} \models \phi$, it is by Thm. 12 sufficient to prove $\texttt{Spec} \sqsubseteq_{\text{RS}} \phi$. Doing so is straightforward when considering the Logic LTSs of `Spec` and ϕ, which are depicted in Figs. 4(d) and 3, respectively. In addition, we know that, whenever we implement the channel design $C = P \wedge \psi$ by some C_i so that $C_i \sqsubseteq_{\text{RS}} C$, the implementation $\texttt{Impl} =_{\text{df}} (C_i \parallel_{\{\texttt{in}\}} S)/\texttt{in}$ satisfies ϕ, too. This is because $\texttt{Impl} \sqsubseteq_{\text{RS}} \texttt{Spec}$ by compositionality (cf. Prop. 3 and Thm. 17) and thus, by transitivity, $\texttt{Impl} \sqsubseteq_{\text{RS}} \phi$. Hence, $\texttt{Impl} \models \phi$ by Thm. 12.

[4] Note that applying the hiding operator is straightforward in our example, since processes with an outgoing `in`-transition do not have any other outgoing transition.

Possible implementations C_i of C include the LTS C_1 that engages in an `in-out`-loop, C_2 that behaves as an `in-in-out`-loop, or C_3 depicted in Fig. 4(e); the latter requires that at most one of each two messages and at most two of five messages are lost. Rather than proving $C_3 \sqsubseteq_{\mathrm{RS}} C$, one could establish $C_3 \sqsubseteq_{\mathrm{RS}} P$ and $C_3 \sqsubseteq_{\mathrm{RS}} \psi$ separately and then infer $C_3 \sqsubseteq_{\mathrm{RS}} P \wedge \psi = C$ by Prop. 3.

5 Related Work

Related work has often avoided mixing operational and logic styles of specification by translating one style into the other. Logic content may be translated into operational content, such as in Kurshan's work on *ω-automata* [11] which includes synchronous and asynchronous composition operators and employs trace inclusion for refinement. However, trace inclusion is insensitive to deadlock and is thus inadequate in the presence of concurrency.

Dually, operational content may be translated into logic formulas, as is implicitly done by Lamport in [12] where logic implication serves as refinement relation [1]. A similar approach is followed in UTP [10], the *Unifying Theories of Programming*, where a translation of the process algebra CSP [9] into logic formulas is indicated. Thus, conjunction is, e.g., applicable to processes a and $a+b$ (i.e., the p and r in Fig. 1(a)), which yields a process that can neither refuse b in the sense of failure semantics, nor can it perform b. Hence, $a \wedge (a+b)$ is an inconsistent process, but it is not treated as logically false as in our work. It seems that this inconsistency can be repaired in [10] by adding further choices (e.g., as in $(a \wedge (a+b)) + b = a + b$), which we regard as undesirable.

A seminal step towards a mixed setting was taken by Olderog in [15], where process-algebraic constructs are combined with *trace formulas*, and where failure semantics underlies refinement. In this approach, trace formulas can serve as processes, but not vice versa. Thus, and in contrast to our present work, [15] does not support the unrestricted mixing of operational and logic specification styles, which can be very useful as, e.g., demonstrated with our example in Sec. 4. In [7], a mixing of process algebraic and temporal logic operators is advocated, too: a simple process algebra is extended with an operator to express that eventually some action occurs (see also [16]). Again, the semantics is based on traces and is thus not deadlock-sensitive. However, the ideas of Guerra and Costa [7] may help to extend our approach to liveness properties, as may those in [8].

Finally, we mention the work of Fecher and Grabe [5], where ready simulation is used as implementation relation and where a specific satisfaction for temporal logic formulas is defined similar to our approach. Also in [5], whenever a process satisfies a formula, each implementation of the process satisfies the formula. However, [5] does not allow the free mixing of operators.

6 Conclusions & Future Work

This paper embedded a temporal logic for specifying safety properties into the ready-simulation-equipped setting of Logic LTS [14]. The chosen logic was a branching-time logic that allows one to specify properties regarding the enabledness of actions, using standard temporal operators such as *always* and *unless* (*weak until*), which were shown to be compositional for ready simulation. The embedding is conservative in that ready simulation, when restricted to pairs of processes and temporal formulas, coincides with the logic's satisfaction relation. The extended setting of Logic LTS is unique in the literature in that it lends itself to *freely* mixing operational and temporal-logic styles of specification, with ready simulation facilitating *compositional* refinement and model checking.

Regarding future work, Logic LTS should be extended so as to be able to express liveness and fairness properties, too; this is a non-trivial task since full abstraction should be preserved. We also wish to re-phrase our setting in the traditional process-algebraic fashion and to study axiomatisations of ready simulation. The challenge here will be to integrate both least and greatest fixpoint operators in a compositional way.

References

[1] M. Abadi and G. Plotkin. A logical view of composition. *TCS*, 114(1):3–30, 1993.

[2] B. Bloom. *Ready Simulation, Bisimulation, and the Semantics of CCS-like Languages.* PhD thesis, MIT, 1990.

[3] S.D. Brookes, C.A.R. Hoare, and A.W. Roscoe. A theory of communicating sequential processes. *J. ACM*, 31(3):560–599, 1984.

[4] R. De Nicola and F. Vaandrager. Action versus state based logics for transition systems. In *Semantics of Systems of Concurrent Processes*, vol. 469 of *LNCS*, pp. 407–419. Springer, 1990.

[5] H. Fecher and I. Grabe. Finite abstract models for deterministic transition systems. In *FSEN 2007*, vol. 4767 of *LNCS*, pp. 1–16. Springer, 2007.

[6] R. van Glabbeek. The linear time – branching time spectrum II, 1993. Available at http://theory.stanford.edu/˜rvg/abstracts.html#26.

[7] H. Guerra and J. F. Costa. Processes with local and global liveness requirements. *J. of Logic and Algebraic Programming*, 2008. To appear.

[8] T. A. Henzinger and R. Majumdar. Fair bisimulation. In *TACAS 2000*, vol. 1785 of *LNCS*, pp. 299–314. Springer, 2000.

[9] C.A.R. Hoare. *Communicating Sequential Processes.* Prentice Hall, 1985.

[10] C.A.R. Hoare and H. Jifeng. *Unified Theories of Programming.* Prentice Hall, 1998.

[11] R.P. Kurshan. *Computer-Aided Verification of Coordinating Processes: The Automata-Theoretic Approach.* Princeton Univ. Press, 1994.

[12] L. Lamport. The temporal logic of actions. *TOPLAS*, 16(3):872–923, 1994.

[13] G. Lüttgen and W. Vogler. Conjunction on processes: Full-abstraction via ready-tree semantics. *TCS*, 373(1–2):19–40, 2007.

[14] G. Lüttgen and W. Vogler. Ready simulation for concurrency: It's logical! In *ICALP 2007*, vol. 4596 of *LNCS*, pp. 752–763. Springer, 2007.

[15] E.-R. Olderog. *Nets, Terms and Formulas.* Cambridge Tracts in Theoretical Computer Science 23. Cambridge Univ. Press, 1991.

[16] A. Puhakka and A. Valmari. Liveness and fairness in process-algebraic verification. In *CONCUR 2001*, vol. 2154 of *LNCS*, pp. 202–217. Springer, 2001.

[17] I. Ulidowski. Refusal simulation and interactive games. In *AMAST 2002*, vol. 2422 of *LNCS*, pp. 208–222. Springer, 2002.

A Omitted Proofs

(Not to be published in the conference proceedings.)

This appendix contains those proofs of our statements, for which there is insufficient space in the main part of the paper. The proofs are not intended for publication in the conference proceedings, but are included here solely for the convenience of the reviewers; they will be published as a technical report, if the paper should be accepted.

In the following, we denote a transition $p \xrightarrow{\alpha} p'$ with $p, p' \notin F$ by $p \xrightarrow{\alpha}_{\mathrm{F}} p'$.

A.1 Proof of Theorem 8

Proof. Recall that the compositionality results for parallel composition, conjunction and disjunction were stated and proved in [14].

We start off with sketching the compositionality proof for $[a]$. Firstly, stable process A in the encoding $[a]P$ of $[a]p$ is matched by stable process A in the encoding $[a]Q$ of $[a]q$, showing (RS1) and (RS4). For (RS2), we observe: if $A \in F_{[a]Q}$, then we must have $a \in A$ and $q \in F_Q$, thus $p \in F_P$ and $A \in F_{[a]P}$. Now we assume $A \notin F_{[a]P}$; if $A \xrightarrow{a}_{\mathrm{F}} p \overset{\epsilon}{\Longrightarrow}| p_0$ then, since $p \sqsubseteq_{\mathrm{RS}} q$ by assumption, there is some q_0 with $q \overset{\epsilon}{\Longrightarrow}| q_0$ and $p_0 \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} q_0$; furthermore, $A \xrightarrow{a}_{\mathrm{F}} q \overset{\epsilon}{\Longrightarrow}| q_0$ in $[a]Q$. For $b \in \mathcal{A} \setminus \{a\}$, we have $A \xrightarrow{b}_{\mathrm{F}} tt$ in both $[a]P$ and $[a]Q$. Thus, (RS3) holds as well.

We now turn to proving compositionality regarding the operator $\Box$. If $p \in F_P$, then $\Box p \sqsubseteq_{\mathrm{RS}} \Box q$ is trivial. Now consider $p \notin F_P$ (and hence $q \notin F_Q$). Since the processes on which $\Box p$ can stabilise are exactly those $(\hat{p})$ with $p \overset{\epsilon}{\Longrightarrow}| \hat{p}$ (and similarly for q), we only have to establish the following statement:

Let $p \sqsubseteq_{\mathrm{RS}} q$ be given, i.e., for all $\hat{p}$ with $p \overset{\epsilon}{\Longrightarrow}| \hat{p}$, there exists some $\hat{q}$ such that $q \overset{\epsilon}{\Longrightarrow}| \hat{q}$ and $\hat{p} \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} \hat{q}$. We show that $(\hat{p}) \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} (\hat{q})$ in $\Box P$ and resp. $\Box Q$. To do so, it is sufficient to prove that

$$\mathcal{R} =_{\mathrm{df}} \{\langle \vec{p}, \vec{q} \rangle \,|\, \vec{p} = (p_1, \dots, p_n),\ \vec{q} = (q_1, \dots, q_n),\ \forall 1 \leq i \leq n.\, p_i \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} q_i\}$$

is a stable ready simulation relation. Obviously, $\langle (\hat{p}), (\hat{q}) \rangle \in \mathcal{R}$. We verify Conds. (RS1)–(RS4) of Def. 2, using the $\Box$-witness $W_1 \cup W_2$ of Lemma 11:

(RS1) Here, $\vec{p}$ and $\vec{q}$ are stable since all p_i and q_i are stable due to $p_i \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} q_i$.

(RS2) If $\vec{p} \notin F_{\Box P}$, then $\vec{q} \in W_1$ since $p_i \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} q_i$ for all i. Hence, $\vec{q} \notin F_{\Box Q}$ by Prop. 10.

(RS3) Let $\vec{p} \overset{a}{\Longrightarrow}| \vec{p}'$, i.e., $(p_1, \dots, p_n) \xrightarrow{a}_{\mathrm{F}} (\overline{p}_1, \dots, \overline{p}_n, p) \overset{\epsilon}{\Longrightarrow}| (p'_1, \dots, p'_n, \hat{p}) = \vec{p}'$ for some suitably chosen $\overline{p}_i$. Hence, $\overline{p}_i \overset{\epsilon}{\Longrightarrow}| p'_i$ and resp. $p \overset{\epsilon}{\Longrightarrow}| \hat{p}$, as well as $p_i \xrightarrow{a}_{\mathrm{F}} \overline{p}_i$, for all $1 \leq i \leq n$. Therefore, by $p_i \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} q_i$ and (RS3), there exist $\overline{q}_i$ and q'_i such that $q_i \xrightarrow{a}_{\mathrm{F}} \overline{q}_i \overset{\epsilon}{\Longrightarrow}| q'_i$ and $p'_i \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} q'_i$, and also $\hat{p} \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} \hat{q}$

by assumption. Thus, $\vec{q} \xrightarrow{a} (\overline{q}_1, \ldots, \overline{q}_n, q) \overset{\epsilon}{\Longrightarrow} \vec{q}' =_{\mathrm{df}} (q'_1, \ldots, q'_n, \hat{q}) \not\xrightarrow{\tau}$. Since $\vec{p}' \notin F_{\Box P}$, we have $\vec{q}' \in W_1$, whence all processes along the computation $(\overline{q}_1, \ldots, \overline{q}_n, q) \overset{\epsilon}{\Longrightarrow} \vec{q}'$ are in W_2. Finally, $\vec{q} \notin F_{\Box Q}$ by (RS2) above. Summarising and referring to Prop. 10, we have $\vec{q} \overset{a}{\Longrightarrow}\!| \, \vec{q}'$ and, obviously, $\langle \vec{p}', \vec{q}' \rangle \in \mathcal{R}$.

(RS4) The premise $\vec{p} \notin F_{\Box P}$ and the stability of $\vec{p}$ by (RS1) imply $\mathcal{I}_{\Box P}(\vec{p}) = \mathcal{I}_P(p_1) = \ldots = \mathcal{I}_P(p_n)$. Thus, by $p_i \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_i$ according to the definition of $\mathcal{R}$, we have $\mathcal{I}_P(p_i) = \mathcal{I}_Q(q_i)$ for all i. Therefore, $\mathcal{I}_{\Box P}(\vec{p}) = \mathcal{I}_Q(q_1) = \ldots = \mathcal{I}_Q(q_n) = \mathcal{I}_{\Box Q}(\vec{q})$ by our operational rules.

This completes the compositionality proof wrt. the $\Box$-operator. The proof for the W-operator follows along similar lines; it is omitted here since it does not require any new concept but only additional notation and case distinctions. □

A.2 Proof of Proposition 10

Proof. Direction "$\Longrightarrow$" follows from the fact that $\overline{F_{\Box P}}$, i.e., the complement of $F_{\Box P}$, is an $\wedge$-witness. For direction "$\Longleftarrow$" we note that $\overline{W}$ satisfies the conditions of $F_{\Box P}$, whence $F_{\Box P} \subseteq \overline{W}$. □

A.3 Proof of Lemma 11

Proof. We need to check Conds. (W1)–(W4) of $\Box$-witness.

(W1) If $\vec{q} \in W_1$, then $\vec{p} \notin F_{\Box P}$, which implies $p_i \notin F_P$ for all i. Hence, $q_i \notin F_Q$ by $p_i \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_i$, for all i.
If $\vec{q} \in W_2$, then $q_i \overset{\epsilon}{\Longrightarrow}\!|$, for all i, and thus $q_i \notin F_Q$.

(W2) If $\vec{q} \in W_1$ stable, then q_i, q_j are stable for any i, j and, by the above, $q_i, q_j \notin F_Q$. By $p_i \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_i$ and $p_j \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_j$, we obtain $\mathcal{I}_Q(q_i) = \mathcal{I}_P(p_i) = \mathcal{I}_P(p_j) = \mathcal{I}_Q(q_j)$, where the second equality holds due to $\vec{p} \notin F_{\Box P}$.
If $\vec{q} \in W_2$ stable, then $\vec{q} \in W_1$ and we are in the case above.

(W3) We first consider the case $\alpha = \tau$. Then, $\vec{q} \xrightarrow{\tau}$ implies $\exists i.\, q_i \xrightarrow{\tau} \overline{q}_i$ for some $\overline{q}_i$. Moreover, $\vec{q}$ can only be in W_2 and not in W_1 since W_1 requires $\vec{q}$ to be stable. Thus, w.l.o.g., $\overline{q}_i$ is chosen such that $\overline{q}_i \overset{\epsilon}{\Longrightarrow}\!|$. By definition of W_2, we have $\vec{q} \xrightarrow{\tau} (q_1, \ldots, \overline{q}_i, \ldots, q_n) \in W_2$.
If $\alpha \neq \tau$, then $\vec{q} \xrightarrow{\alpha}$ means $\vec{q} \in W_1$. Moreover, $q_i \xrightarrow{\alpha}$ for all i. Thus, due to $\vec{p} \notin F_{\Box P}$ and $p_i \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_i$, we have $\forall i.\, p_i \xrightarrow{\alpha}$ by (RS4). Thus, $\vec{p} \xrightarrow{\alpha}$, and hence $\exists \vec{p}'.\, \vec{p} \overset{\alpha}{\Longrightarrow}\!| \, (\vec{p}', p)$ and $\forall i.\, p_i \overset{\alpha}{\Longrightarrow}\!| \, p'_i$. By (RS3), there exist q'_i and $\hat{q}_i$ such that $q_i \xrightarrow{\alpha}_{\mathrm{F}} \hat{q}_i \overset{\epsilon}{\Longrightarrow}\!| \, q'_i$ and $p'_i \underset{\sim}{\sqsubset}_{\mathrm{RS}} q'_i$. Moreover, we know $p \underset{\sim}{\sqsubset}_{\mathrm{RS}} q$ and $p \notin F_P$, whence $(q'_1, \ldots, q'_n, q) \in W_1$. Now, $\vec{q} \xrightarrow{\alpha} (\hat{q}_1, \ldots, \hat{q}_n, q) \in W_2$.

(W4) If $\vec{q} \in W_1$, then q_i is stable for all i, which implies that $\vec{q}$ is stable, too. Therefore, $\vec{q}$ can stabilise trivially in W.
If $\vec{q} \in W_2$, then $\vec{q}$ can stabilise since every q_i can stabilise by the definition of W_2. This stabilisation is in W_2 by construction. □

A.4 Proof of Thm. 12

The proof of Thm. 12 uses the following lemma for dealing with process vectors in the case that $\phi = \Box\psi$:

Lemma 15. *Let $\vec{q} = (q_1, \ldots, q_n) \in \Box\Psi$ and $p \sqsubseteq_{RS} \vec{q}$. Then, $p \sqsubseteq_{RS} q_i$ for all i.*

Proof. We first show the lemma for $\underset{\sim}{\sqsubset}_{\mathrm{RS}}$ in place of $\sqsubseteq_{\mathrm{RS}}$, before concluding by establishing the root condition. In order to prove $p \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_i$ from $p \underset{\sim}{\sqsubset}_{\mathrm{RS}} \vec{q}$ for all $p \in P$ and $\vec{q} \in \Box\Psi$, it is sufficient to establish that

$$\mathcal{R} =_{\mathrm{df}} \{\langle p, q_i\rangle \mid \exists n, q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_n.\, p \underset{\sim}{\sqsubset}_{\mathrm{RS}} \vec{q}\}$$

is a stable ready simulation relation. We verify Conds. (RS1)–(RS4) of Def. 2:

(RS1) Process p is stable, and all q_i are stable since $\vec{q}$ is stable.
(RS2) If $p \notin F$, then $\vec{q} \notin F$ since $p \underset{\sim}{\sqsubset}_{\mathrm{RS}} \vec{q}$. Hence, $q_i \notin F$.
(RS3) Let $p \stackrel{a}{\Longrightarrow}\!| \, p'$. By $p \underset{\sim}{\sqsubset}_{\mathrm{RS}} \vec{q}$, there exists some $\vec{q}' = (q'_1, \ldots, q'_{n+1})$ such that $\vec{q} \stackrel{a}{\Longrightarrow}\!| \, \vec{q}'$ and $p' \underset{\sim}{\sqsubset}_{\mathrm{RS}} \vec{q}'$. Therefore, $q_i \stackrel{a}{\Longrightarrow}\!| \, q'_i$ and $\langle p', q'_i\rangle \in \mathcal{R}$.
(RS4) Let $p \notin F$. Then, $\mathcal{I}(p) = \mathcal{I}(\vec{q})$ due to $p \underset{\sim}{\sqsubset}_{\mathrm{RS}} \vec{q}$. By construction, $\mathcal{I}(\vec{q}) = \mathcal{I}(q_1) = \ldots = \mathcal{I}(q_n)$ since $\vec{q} \notin F$ by the above. Hence, $\mathcal{I}(p) = \mathcal{I}(q_i)$.

We can now complete the proof of the lemma by establishing the root condition. Let $p \stackrel{\epsilon}{\Longrightarrow}\!| \, p'$ for some p'. Hence, by $p \sqsubseteq_{\mathrm{RS}} \vec{q}$, there exists some $\vec{q}' = (q'_1, \ldots, q'_m)$ such that $\vec{q} \stackrel{\epsilon}{\Longrightarrow}\!| \, \vec{q}'$ and $p' \underset{\sim}{\sqsubset}_{\mathrm{RS}} \vec{q}'$. This implies $q_i \stackrel{\epsilon}{\Longrightarrow}\!| \, q'_i$ and, by the above, $p' \underset{\sim}{\sqsubset}_{\mathrm{RS}} q'_i$. □

We can now prove the compatibility theorem:

Proof. [of Thm. 12] The proof is by induction on the structure of ϕ. Note that the cases $\phi = tt$ and $\phi = ff$ are trivial, the case $\phi = dis(a)$ is analogous to the one for $\phi = en(a)$, and the case for $\phi = \psi_1 \mathsf{W} \psi_2$ follows along similar lines to the one for $\phi = \Box\psi$. Therefore, we focus only on the remaining cases:

- $\underline{\phi = en(a)}$*:* ("$\Longrightarrow$") Let $p \models en(a)$, i.e., $p \stackrel{\epsilon}{\Longrightarrow}\!| \, p_0$ implies $p_0 \stackrel{a}{\longrightarrow}$, for any p_0. Then, $p \sqsubseteq_{\mathrm{RS}} en(a)$ since $p_0 \underset{\sim}{\sqsubset}_{\mathrm{RS}} \mathcal{I}(p_0)$.

  ("$\Longleftarrow$") For all p_0 such that $p \stackrel{\epsilon}{\Longrightarrow}\!| \, p_0$ we must have some action set A containing a with $p_0 \underset{\sim}{\sqsubset}_{\mathrm{RS}} A$. Since $p_0 \notin F$, this means by (RS4) that $a \in \mathcal{I}(p_0)$, and by (LTS1) that $p_0 \stackrel{a}{\longrightarrow}_{\mathrm{F}}$. Hence, $p \models en(a)$.
- $\underline{\phi = [a]\psi}$*:* ("$\Longrightarrow$") Let $p \models [a]\psi$ and consider some process p_0 with $p \stackrel{\epsilon}{\Longrightarrow}\!| \, p_0$. By the definition of $\models$ we know that $p_1 \models \psi$ for all p_1 such that $p_0 \stackrel{a}{\Longrightarrow}\!| \, p_1$. Hence, $p_1 \sqsubseteq_{\mathrm{RS}} \psi$ by induction hypothesis, which implies $\psi \stackrel{\epsilon}{\Longrightarrow}\!| \, q_1$ for some q_1 with $p_1 \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_1$. We argue $p_0 \underset{\sim}{\sqsubset}_{\mathrm{RS}} \mathcal{I}(p_0)$ by showing that $\{\langle p_0, \mathcal{I}(p_0)\rangle\} \cup \underset{\sim}{\sqsubset}_{\mathrm{RS}}$ is a stable ready simulation relation. Obviously, the pair $\langle p_0, \mathcal{I}(p_0)\rangle$ satisfies Conds. (RS1), (RS2) and (RS4) of Def. 2. Regarding (RS3), we have for all $p_0 \stackrel{b}{\Longrightarrow}\!| \, p_1$ with $b \neq a$ (and $b \in \mathcal{I}(p_0)$) that $\mathcal{I}(p_0) \stackrel{b}{\Longrightarrow}\!| \, tt$ and $p_1 \underset{\sim}{\sqsubset}_{\mathrm{RS}} tt$.

Furthermore, for all $p_0 \overset{a}{\Longrightarrow|} p_1$, we have $\mathcal{I}(p_0) \xrightarrow{a}_{\mathrm{F}} \psi \overset{\epsilon}{\Longrightarrow|} q_1$ with $p_1 \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_1$, as noted above. Altogether, we thus have $p \sqsubseteq_{\mathrm{RS}} [a]\psi$.

("$\Longleftarrow$") Let $p \sqsubseteq_{\mathrm{RS}} [a]\psi$. Therefore, whenever $p \overset{\epsilon}{\Longrightarrow|} p_0$, we have $[a]\psi \overset{\epsilon}{\Longrightarrow|} A$ for some A with $p_0 \underset{\sim}{\sqsubset}_{\mathrm{RS}} A$. Obviously, $A = \mathcal{I}(p_0)$. By our Logic LTS encoding of $[a]\psi$ and (RS3), $p_0 \overset{a}{\Longrightarrow|} p_1$ for any such p_1 implies $\psi \overset{\epsilon}{\Longrightarrow|} q_1$ for some q_1 with $\mathcal{I}(p_0) \overset{a}{\Longrightarrow|} q_1$ and $p_1 \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_1$. Hence, $p_1 \sqsubseteq_{\mathrm{RS}} \psi$ and, by induction hypothesis, $p_1 \models \psi$. Therefore, $p \models [a]\psi$.

- $\underline{\phi = \psi_1 \vee \psi_2}$*:* ("$\Longrightarrow$") Let $p \models \psi_1 \vee \psi_2$. Whenever $p \overset{\epsilon}{\Longrightarrow|} p_0$, then $p_0 \models \psi_1$ or $p_0 \models \psi_2$, i.e., $p_0 \sqsubseteq_{\mathrm{RS}} \psi_1$ or $p_0 \sqsubseteq_{\mathrm{RS}} \psi_2$ by induction hypothesis. Assume w.l.o.g. that $p_0 \sqsubseteq_{\mathrm{RS}} \psi_1$, whence $\psi_1 \overset{\epsilon}{\Longrightarrow|} q_0$ for some q_0 with $p_0 \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_0$. By $\psi_1 \vee \psi_2 \overset{\epsilon}{\Longrightarrow|} q_0$, we conclude $p \sqsubseteq_{\mathrm{RS}} \psi_1 \vee \psi_2$.

  ("$\Longleftarrow$") Let $p \sqsubseteq_{\mathrm{RS}} \psi_1 \vee \psi_2$ and $p \overset{\epsilon}{\Longrightarrow|} p_0$. Therefore, w.l.o.g., $\psi_1 \vee \psi_2 \overset{\epsilon}{\Longrightarrow|} q_0$ due to $\psi_1 \overset{\epsilon}{\Longrightarrow|} q_0$ with $p_0 \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_0$. Hence, $p_0 \sqsubseteq_{\mathrm{RS}} \psi_1$ and, by induction hypothesis, $p_0 \models \psi_1$. This implies $p \models \psi_1 \vee \psi_2$.
- $\underline{\phi = \psi_1 \wedge \psi_2}$*:* ("$\Longrightarrow$") Let $p \models \psi_1 \wedge \psi_2$. Whenever $p \overset{\epsilon}{\Longrightarrow|} p_0$, then $p_0 \models \psi_1$ and $p_0 \models \psi_2$, i.e., $p_0 \sqsubseteq_{\mathrm{RS}} \psi_1$ and $p_0 \sqsubseteq_{\mathrm{RS}} \psi_2$ by induction hypothesis. By Prop. 3, we get $p_0 \sqsubseteq_{\mathrm{RS}} \psi_1 \wedge \psi_2$. Hence, $p \sqsubseteq_{\mathrm{RS}} \psi_1 \wedge \psi_2$.

  ("$\Longleftarrow$") Let $p \sqsubseteq_{\mathrm{RS}} \psi_1 \wedge \psi_2$ and $p \overset{\epsilon}{\Longrightarrow|} p_0$. Thus, $p_0 \sqsubseteq_{\mathrm{RS}} \psi_1 \wedge \psi_2$ and, by Prop. 3, we can now conclude that $p_0 \sqsubseteq_{\mathrm{RS}} \psi_1$ and $p_0 \sqsubseteq_{\mathrm{RS}} \psi_2$. Hence, by induction hypothesis, $p_0 \models \psi_1$ and $p_0 \models \psi_2$ and thus $p \models \psi_1 \wedge \psi_2$.
- $\underline{\phi = \Box\psi}$*:* Recall that $\overset{\mathcal{A}}{\Longrightarrow|}$ stands for $\bigcup_{a \in \mathcal{A}} \overset{a}{\Longrightarrow|}$. In this part of the proof, we write $p \overset{\mathcal{A}^*}{\Longrightarrow|} p'$ whenever $p \overset{\epsilon}{\Longrightarrow|} p_0 \overset{\mathcal{A}}{\Longrightarrow|} p_1 \dots \overset{\mathcal{A}}{\Longrightarrow|} p_n = p'$ with $n \geq 0$.

  ("$\Longrightarrow$") We first prove that

$$\mathcal{R} =_{\mathrm{df}} \{\langle p'', \vec{q}\rangle \mid p \overset{\mathcal{A}^*}{\Longrightarrow|} p'',\ \vec{q} \in \Box\Psi,\ \forall i.\, p'' \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_i\}$$

  is a stable ready simulation relation. We verify Conds. (RS1)–(RS4) of Def. 2:

  (RS1) p'' and all q_i are stable, whence $\vec{q}$ is stable, too.

  (RS2) Here, it is sufficient to show that $W'_1 \cup W'_2$ is a witness, where

$$\begin{aligned} W'_1 &=_{\mathrm{df}} \{\vec{q} \in \Box\Psi \mid \exists p''.\, p \overset{\mathcal{A}^*}{\Longrightarrow|} p'' \text{ and } \forall i.\, p'' \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_i\} \\ W'_2 &=_{\mathrm{df}} \{\vec{q} \in \Box\Psi \mid \exists \vec{q}\,' \in W'_1\, \forall i.\, q_i \overset{\epsilon}{\Longrightarrow|} q'_i\}\,. \end{aligned}$$

  The proof is similar to the one of Lemma 11, except for the proof of (W3) in case $\alpha \neq \tau$. Here, $\vec{q} \xrightarrow{\alpha}$ means $\vec{q} \in W'_1$ and $q_i \xrightarrow{\alpha}$ for all i. Since $p'' \notin F$, we get $p'' \xrightarrow{\alpha}$, by (RS4), and $p'' \overset{\alpha}{\Longrightarrow|} p'''$. By (RS3), there exist q''_i and q'_i such that $q_i \xrightarrow{\alpha}_{\mathrm{F}} q''_i \overset{\epsilon}{\Longrightarrow|} q'_i$ and $p''' \underset{\sim}{\sqsubset}_{\mathrm{RS}} q'_i$. Moreover, $p''' \models \psi$, whence $p''' \sqsubseteq_{\mathrm{RS}} \psi$ by induction hypothesis and thus $p''' \underset{\sim}{\sqsubset}_{\mathrm{RS}} \psi_0$ for some $\psi \overset{\epsilon}{\Longrightarrow|} \psi_0$. Thus, $(q'_1, \dots, q'_n, \psi_0) \in W'_1$ and $\vec{q} \xrightarrow{\alpha} (q''_1, \dots, q''_n, \psi) \in W'_2$.

  (RS3) Let $p'' \overset{a}{\Longrightarrow|} p'''$. Then, for some q'_i, $q_i \overset{a}{\Longrightarrow|} q'_i$ and $p''' \underset{\sim}{\sqsubset}_{\mathrm{RS}} q'_i$ by (RS3) for $p'' \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_i$. Furthermore, $p \overset{\mathcal{A}^*}{\Longrightarrow|} p'''$ implies $p''' \models \psi$, i.e., by induction hypothesis, $p''' \sqsubseteq_{\mathrm{RS}} \psi$ and $p''' \underset{\sim}{\sqsubset}_{\mathrm{RS}} \psi_0$ for some $\psi \overset{\epsilon}{\Longrightarrow|} \psi_0$. Thus, $\vec{q} \xrightarrow{a}$

$(q''_1, \ldots, q''_n, \psi) \overset{\epsilon}{\Longrightarrow} (q'_1, \ldots, q'_n, \psi_0) \not\longrightarrow$, for suitably chosen $q''_1, \ldots, q''_n$, and $\langle p''', (q'_1, \ldots, q'_n, \psi_0)\rangle \in \mathcal{R}$. Therefore, we have $(q'_1, \ldots, q'_n, \psi_0) \in W'_1$, and all processes along the computation are in W'_2. By Prop. 10, this proves $\vec{q} \overset{a}{\Longrightarrow}\!| \, (q'_1, \ldots, q'_n, \psi_0)$.

(RS4) Let $p'' \notin F$. Then, (RS4) for $p'' \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} q_i$ yields $\mathcal{I}(p'') = \mathcal{I}(q_i)$ for all i, i.e., $\mathcal{I}(p'') = \mathcal{I}(\vec{q})$ by the definition of $\Box\Psi$.

Now, $p \sqsubseteq_{\mathrm{RS}} \Box\psi$ by the following reasoning: Firstly, $p \models \psi$ implies $p \sqsubseteq_{\mathrm{RS}} \psi$ by induction hypothesis. Together with $p \overset{\epsilon}{\Longrightarrow}\!| \, p_0$, this guarantees the existence of some ψ_0 such that $\psi \overset{\epsilon}{\Longrightarrow}\!| \, \psi_0$ and $p_0 \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} \psi_0$. Then, $(\psi) \overset{\epsilon}{\Longrightarrow}\!| \, (\psi_0)$ in $\Box\Psi$ and $\langle p_0, (\psi_0)\rangle \in \mathcal{R}$. Thus, $p \sqsubseteq_{\mathrm{RS}} (\psi) = \Box\psi$.

("$\Longleftarrow$") Let $p \overset{\mathcal{A}^*}{\Longrightarrow}\!| \, p'$. Then, by $p \sqsubseteq_{\mathrm{RS}} \Box\psi$, there exists some $\vec{\psi}'$ such that $(\psi) \overset{\mathcal{A}^*}{\Longrightarrow}\!| \, \vec{\psi}'$ (performing the same sequence of visible actions) and $p' \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} \vec{\psi}'$. By Lemma 15, we have $p' \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} \psi'_i$ for all i. By our operational rules, the last component ψ' of $\vec{\psi}'$ is such that $\psi \overset{\epsilon}{\Longrightarrow}\!| \, \psi'$. Hence, $p' \sqsubseteq_{\mathrm{RS}} \psi$ and, by induction hypothesis, $p' \models \psi$. Thus, $p \overset{\mathcal{A}^*}{\Longrightarrow}\!| \, p'$ implies $p' \models \psi$, i.e., $p \models \Box\psi$. □

A.5 Proof of Corollary 13

Proof. Let $\phi \sqsubseteq_{\mathrm{RS}} \psi$ and $p \models \phi$. Then, $p \sqsubseteq_{\mathrm{RS}} \phi \sqsubseteq_{\mathrm{RS}} \psi$ by Thm. 12, and we are done by transitivity of $\sqsubseteq_{\mathrm{RS}}$. Conversely, if $p \models \phi$ implies $p \models \psi$, then $p \sqsubseteq_{\mathrm{RS}} \phi$ implies $p \sqsubseteq_{\mathrm{RS}} \psi$, again by Thm. 12, for all p. Hence, $\phi \sqsubseteq_{\mathrm{RS}} \psi$ when setting $p = \phi$. □

B Hiding in Logic LTS

(Not to be published in the conference proceedings.)

This appendix contains the development of the hiding operator for Logic LTS. As for the previous section, this section is included here solely for the convenience of the reviewers and will be published as a technical report, if the paper should be accepted.

Adding the process-algebraic operator $/h$ of hiding to our setting, where h denotes a visible action, is a necessity to be able to model systems that involve internal communication across parallel components. However, doing so is nontrivial since relabelling a visible action by the internal action τ typically destroys the τ-purity property required of Logic LTS. Hence, for the hiding operator to be well-defined, it must not only hide but also re-establish τ-purity. We start off by discussing some examples.

Firstly, consider the LTS shown in Fig. 5(a) on the left, but think of the τ-transition as the result of hiding action h; the idea should be that b must be offered, while a might be offered as an alternative. This can equivalently be expressed as the τ-pure LTS in Fig. 5(a) on the right. Operationally, this transformation can be understood as collecting all moves that are possible when 'looking

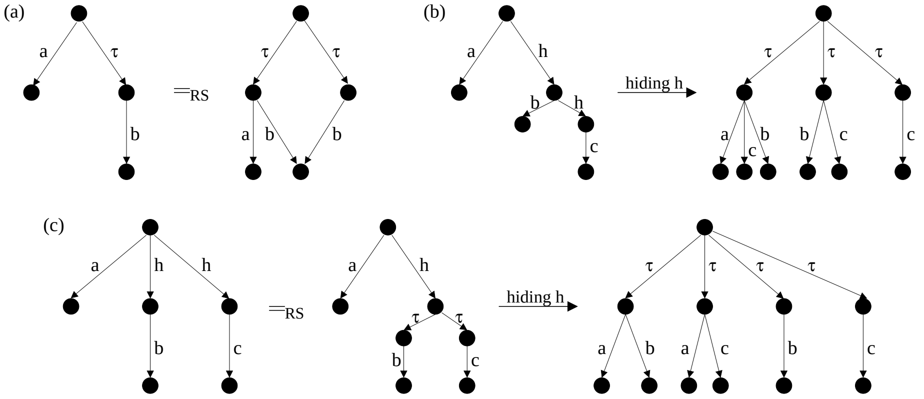

Fig. 5. Three examples regarding hiding.

through' the hidden action h or pre-empting action a by performing h. The second example, depicted in Fig. 5(b), requires us to iterate this idea when hiding action h. Note that, in the LTS on the right, the target states of the b-transitions are actually the same state, as are the target states of the c-transitions; we have drawn the LTS as a tree to improve the layout, which is also the case for the rightmost LTS in Fig. 5(c). In the final example, depicted in Fig. 5(c), we first observe the indicated equality, which translates the internal choice on action h to an h-step followed by disjunction. This rewriting makes it clear that actions b and c are exclusive alternatives, and each of these may be combined with action a when hiding h as shown.

We briefly indicate the 'equational' rationale behind these examples. The transformation in Ex. (a) is based on the following law of failures semantics [3]: $(p + h.q)/h = (p + q)/h \vee q/h$, where + denotes external choice. This law has been applied three times in Ex. (b), together with some other, obvious laws.

Note that the above law does not hold for ready simulation in case p can engage in an initial h-transition since, e.g.,

$$\begin{array}{rclcl} (h.a + h.b)/h & =_{\mathrm{RS}} & (h.a + b)/h \vee b & =_{\mathrm{RS}} & (a + b) \vee a \vee b \\ \neq_{\mathrm{RS}} \quad a \vee b & =_{\mathrm{RS}} & (h.(a \vee b)/h & =_{\mathrm{RS}} & (h.a + h.b)/h \end{array}$$

However, this issue is not a problem since several h-transitions can be merged into one via internal choice (disjunction), as shown in Ex. (c).

To formalise our intuition of 'looking through' h, we employ again some vector notation: given a Logic LTS $\langle P, \longrightarrow_P, F_P \rangle$, we augment P to $\hat{P} = P \cup \vec{P}$ by adding all finite vectors of stable, consistent processes: $\vec{P} =_{\mathrm{df}} \{\vec{p} = (p_1, p_2, \ldots, p_n) \,|\, n{\geq}1,\, \forall 1{\leq}i{\leq}n.\, p_i \in P \text{ stable and } p_i \notin F_P\}$. In the sequel, we use the convention that $\hat{p}$ is a generic process in $\hat{P}$, $p \in \hat{P}$ is a process from P, and $\vec{p} \in \hat{P}$ is a process from $\vec{P}$ with components $p_1, p_2, \ldots, p_n$.

Definition 16 (Hiding operator). The hiding of visible action $h \in \mathcal{A}$ in a Logic LTS $\langle P, \longrightarrow_P, F_P \rangle$ results in the Logic LTS $\langle P/h, \longrightarrow_{P/h}, F_{P/h} \rangle$, where

- $P/h =_{\mathrm{df}} \{\hat{p}/h \,|\, \hat{p} \in \hat{P}\}$

- $\longrightarrow_{P/h}$ is determined by the following operational rules:

  (H1) $p \xrightarrow{\tau}_P p' \implies p/h \xrightarrow{\tau}_{P/h} p'/h$

  (H2) $p \xrightarrow{a}_P p',\ p \not\xrightarrow{h}_P \implies p/h \xrightarrow{a}_{P/h} p'/h$

  (H3) $p \xrightarrow{h}_P,\ p(\overset{h}{\Longrightarrow}\!|_P)^* p_1 \overset{h}{\Longrightarrow}\!|_P\, p_2 \cdots \overset{h}{\Longrightarrow}\!|_P\, p_n \not\xrightarrow{h}_P \implies$
  $p/h \xrightarrow{\tau}_{P/h} (p_1, p_2, \ldots, p_n)/h$

  (H4) $p_j \xrightarrow{a}_P p',\ a \neq h,\ (p_1, p_2, \ldots, p_n) \in P/h \implies$
  $(p_1, p_2, \ldots, p_n)/h \xrightarrow{a}_{P/h} p'/h$

- $F_{P/h}$ is the least set satisfying the following conditions:

  (HF1) $p/h \in F_{P/h}$ if $p \in F_P$;

  (HF2) $p/h \in F_{P/h}$ if $\nexists p'.\, p \overset{\epsilon}{\Longrightarrow}\!|_P(\overset{h}{\Longrightarrow}\!|_P)^* p' \not\xrightarrow{h}_P$;

  (HF3) $\hat{p}/h \in F_{P/h}$ if $\exists \alpha {\in} \mathcal{I}(\hat{p}/h)\, \forall \hat{p}'/h.\, \hat{p}/h \xrightarrow{\alpha}_{P/h} \hat{p}'/h \implies \hat{p}'/h \in F_{P/h}$;

  (HF4) $\hat{p}/h \in F_{P/h}$ if $\hat{p}/h$ cannot stabilise outside $F_{P/h}$.

Now, hiding a visible action in a Logic LTS results again in a Logic LTS. Conds. (HF1) and (HF2) show that inconsistencies may be inherited from P, or may result from an inescapable divergence that arises by hiding h. Conds. (HF3) and (HF4) enforce Conds. (LTS1) and (LTS2) of Logic LTS.

Theorem 17 (Compositionality). *If $p \sqsubseteq_{RS} q$, $h \in \mathcal{A}$, then $p/h \sqsubseteq_{RS} q/h$.*

In the proof, we employ again a notion of *witness* for reasoning about the inconsistencies that may arise under hiding. For this, it will be convenient to consider every vector process $\vec{p} \in \vec{P}$ as consistent and augment the transition relation by transitions such that $p_i \xrightarrow{a}_P p \implies \vec{p} \xrightarrow{a}_{\hat{P}} p$, i.e., a process vector inherits all transitions of its component processes. Similarly, we extend $\stackrel{\sqsubset}{\sim}_{\mathrm{RS}} \subseteq P \times Q$ to obtain a new relation $\widehat{\stackrel{\sqsubset}{\sim}}_{\mathrm{RS}} \subseteq \hat{P} \times \hat{Q}$, by adding all pairs $\langle \vec{p}, \vec{q} \rangle \in \vec{P} \times \vec{Q}$ of vectors of equal length such that $\forall i.\, p_i \stackrel{\sqsubset}{\sim}_{\mathrm{RS}} q_i$. Our extensions are well-defined:

Lemma 18. *If $\langle P, \longrightarrow_P, F_P \rangle$ is a Logic LTS, then so is $\langle \hat{P}, \longrightarrow_{\hat{P}}, F_P \rangle$. Moreover, $\widehat{\stackrel{\sqsubset}{\sim}}_{RS}$ is a stable ready simulation relation, whence $\widehat{\stackrel{\sqsubset}{\sim}}_{RS} \subseteq \stackrel{\sqsubset}{\sim}_{RS}$.*

Proof. The first statement is quite straightforward. Firstly, τ-purity and (LTS2) are not violated since all $\vec{p} \in \vec{P}$ are stable. Secondly, let $\vec{p} \xrightarrow{a}$, i.e., there exists some i such that $p_i \xrightarrow{a}$. By (LTS1) for $p_i \in P$, we have the existence of some $p \notin F_P$ such that $p_i \xrightarrow{a} p$. Hence, also $\vec{p} \xrightarrow{a} p \notin F$, which establishes (LTS1) for our extension.

To prove the second statement, we verify Conds. (RS1)–(RS4) of Def. 2:

(RS1) Straightforward by the added operational rule.

(RS2) If $\vec{p}\, \widehat{\stackrel{\sqsubset}{\sim}}_{\mathrm{RS}}\, \vec{q}$, then both $\vec{p}, \vec{q} \notin F$.

(RS3) If $\vec{p}\, \widehat{\stackrel{\sqsubset}{\sim}}_{\mathrm{RS}}\, \vec{q}$, then $\vec{p} \overset{a}{\Longrightarrow}\!| p'$, i.e., $\vec{p} \xrightarrow{a} p \overset{\epsilon}{\Longrightarrow}\!| p'$ for some $p \notin F$, implies $p_i \xrightarrow{a}_{\mathrm{F}} p \overset{\epsilon}{\Longrightarrow}\!| p'$ by the added operational rule, i.e., $p_i \overset{a}{\Longrightarrow}\!| p'$. Since $p_i \stackrel{\sqsubset}{\sim}_{\mathrm{RS}} q_i$, we have $q_i \overset{a}{\Longrightarrow}\!| q'$ for some q' with $p' \stackrel{\sqsubset}{\sim}_{\mathrm{RS}} q'$. Hence, also $\vec{q} \overset{a}{\Longrightarrow}\!| q'$, as well as $p'\, \widehat{\stackrel{\sqsubset}{\sim}}_{\mathrm{RS}}\, q'$ by the definition of $\widehat{\stackrel{\sqsubset}{\sim}}_{\mathrm{RS}}$.

(RS4) If $\vec{p}\,\widehat{\underset{\sim}{\sqsubset}}_{\text{RS}}\,\vec{q}$, then $p_i \underset{\sim}{\sqsubset}_{\text{RS}} q_i$ and $p_i \notin F$ for all i; hence, $\mathcal{I}(p_i) = \mathcal{I}(q_i)$ by (RS4) for $p_i \underset{\sim}{\sqsubset}_{\text{RS}} q_i$. Thus, $\mathcal{I}(\vec{p}) = \bigcup_i \mathcal{I}(p_i) = \bigcup_i \mathcal{I}(q_i) = \mathcal{I}(\vec{q})$. □

Now we are in a position to formally define the concept of witness needed in the proof of Thm. 17:

Definition 19 (Hiding-witness). A *hiding-witness* is a set $W \subseteq P/h$ such that the following conditions hold:

(HW1) $\forall p/h \in W.\ \ p \notin F_P$ and $\exists p'.\, p \overset{\epsilon}{\Longrightarrow\!\!|}_P (\overset{h}{\Longrightarrow\!\!|}_P)^* p' \overset{h}{\not\longrightarrow}_P$;
(HW2) $\forall \hat{p}/h \in W.$ (a) $\forall \alpha \in \mathcal{I}_{P/h}(\hat{p}/h)\, \exists \hat{p}'/h \in W.\ \ \hat{p}/h \overset{\alpha}{\longrightarrow}_{P/h} \hat{p}'/h$;
(b) $\hat{p}/h$ can stabilise in W.

The statement and proof of the following proposition is analogous to the one for $\Box$-witnesses:

Proposition 20. *$\hat{p}/h \notin F_{P/h}$ if and only if $\exists$hiding-witness$\,W.\ \hat{p}/h \in W$.*

The particular hiding-witness that we will need is the following:

Lemma 21. *Let $\langle P, \longrightarrow_P, F_P\rangle$ and $\langle Q, \longrightarrow_Q, F_Q\rangle$ be Logic LTS and $h \in \mathcal{A}$. Then, the set $W =_{df} W_1'' \cup W_2''$ is a hiding-witness for $\langle Q/h, \longrightarrow_{Q/h}, F\rangle$, where*

$$W_1'' =_{df} \{\hat{q}/h \in Q/h \mid \exists \hat{p} \in \hat{P}.\ \hat{p}\,\widehat{\underset{\sim}{\sqsubset}}_{RS}\,\hat{q} \text{ and } \hat{p}/h \notin F\};$$
$$W_2'' =_{df} \{\hat{q}/h \in Q/h \mid \exists \hat{q}''.\ \hat{q} \overset{\tau}{\Longrightarrow\!\!|}\, \hat{q}'' \text{ and } \hat{q}''/h \in W_1''\}\,.$$

Note that $\hat{q}$ in W_2'' must necessarily be of the form q and cannot be the vector $\vec{q}$.

Proof. To establish Cond. (HW1) of Def. 19, let us first consider $q/h \in W_1''$ due to p. Note that $p/h \notin F$ implies $p \notin F_P$ and $q \notin F_Q$ by $p \underset{\sim}{\sqsubset}_{\text{RS}} q$ and (RS2). Then, since $p/h \notin F$ implies $\exists p'.\, p(\overset{h}{\Longrightarrow\!\!|}\,)^* p' \overset{h}{\not\longrightarrow}$ we find, by $p \underset{\sim}{\sqsubset}_{\text{RS}} q$ and (RS3), some q' such that $q(\overset{h}{\Longrightarrow\!\!|}\,)^* q'$ and $p' \underset{\sim}{\sqsubset}_{\text{RS}} q'$. Since $p' \notin F_P$, we obtain $q' \overset{h}{\not\longrightarrow}$ by (RS4).

Now, let us consider the case $q/h \in W_2''$ due to $q \overset{\tau}{\Longrightarrow\!\!|}\, \hat{q}''$ with $\hat{q}''/h \in W_1''$. Obviously, $q \notin F_Q$. Furthermore, $\hat{q}''$ has the form q'', and we have just shown that $\exists q'.\, q''(\overset{h}{\Longrightarrow\!\!|}\,)^* q' \overset{h}{\not\longrightarrow}$. Hence, $q \overset{\epsilon}{\Longrightarrow\!\!|}\, q''(\overset{h}{\Longrightarrow\!\!|}\,)^* q' \overset{h}{\not\longrightarrow}$.

To verify Cond. (HW2a), consider some $\alpha \in \mathcal{I}(\hat{q}/h)$ and distinguish the following cases:

$\underline{\alpha \neq \tau}$**:** Then $\hat{q}/h \in W_1''$ due to some $\hat{p}$. Note that it cannot be the case that $\hat{q}/h \in W_2''$; assume otherwise, $\hat{q} \overset{\tau}{\longrightarrow}$ and thus also $\hat{q}/h \overset{\tau}{\longrightarrow}$ by (H1), contradicting $\hat{q}/h \overset{\alpha}{\longrightarrow}$ with $\alpha \neq \tau$.
Again, we distinguish two cases, for both of which we establish $\hat{p}/h \overset{\alpha}{\longrightarrow}$. The first case is $\hat{q}/h \overset{\alpha}{\longrightarrow}$ due to (H2). Then, $\hat{q} \overset{\alpha}{\longrightarrow}$ and $\hat{q} \overset{h}{\not\longrightarrow}$. By $\hat{p}\,\widehat{\underset{\sim}{\sqsubset}}_{\text{RS}}\,\hat{q}$ and $\hat{p} \notin F_P$, we have $\hat{p} \overset{\alpha}{\longrightarrow}$ and $\hat{p} \overset{h}{\not\longrightarrow}$ by (RS4). Hence, $\hat{p}/h \overset{\alpha}{\longrightarrow}$.

The second case is $\hat{q}/h \xrightarrow{\alpha}$ due to (H4). Take some i with $q_i \xrightarrow{\alpha}$. Since $p_i \notin F_P$ by $\hat{p} \in \hat{P}$ and since $p_i \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_i$ by $\hat{p} \, \widehat{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} \, \hat{q}$, we have $p_i \xrightarrow{\alpha}$ and $\hat{p}/h \xrightarrow{\alpha}$.

Now we may conclude the proof for both cases. By (LTS1) and (LTS2), $\hat{p}/h \overset{\alpha}{\Longrightarrow}\!|$. Let $\hat{p}''/h \notin F$ be the first state on this computation with $\hat{p}''$ stable, whence $\hat{p} \overset{\alpha}{\Longrightarrow}\!| \, \hat{p}''$. By $\hat{p} \, \widehat{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} \, \hat{q}$, we also have some $\hat{q}''$ and q' with $\hat{q} \xrightarrow{\alpha}_{\mathrm{F}} q' \overset{\epsilon}{\Longrightarrow}\!| \, \hat{q}''$ and $\hat{p}'' \, \widehat{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} \, \hat{q}''$. Since $\hat{p}''/h \notin F$, we have $\hat{q}''/h \in W_1''$. Thus, $\hat{q}/h \xrightarrow{\alpha} q'/h \in W$.

<u>$\alpha = \tau$:</u> If $\hat{q}/h \in W_1''$ due to $\hat{p}$, then $\hat{q}$, being stable, must be q with $q \xrightarrow{h}$ and $\hat{p} = p$. Since $p/h \notin F$, we have $p \notin F_P$ and, by (RS4), $p \xrightarrow{h}$; furthermore, $p(\overset{h}{\Longrightarrow}\!|\,)^* p' \stackrel{h}{\not\longrightarrow}$ for some p'. Thus, $p/h \xrightarrow{\tau}$ by (H3) and $p/h \xrightarrow{\tau} \vec{p}/h \notin F$ for some suitable $\vec{p}/h$ by (LTS1), with $p(\overset{h}{\Longrightarrow}\!|\,)^* p_1 \overset{h}{\Longrightarrow}\!| \, p_2 \cdots \overset{h}{\Longrightarrow}\!| \, p_n \stackrel{h}{\not\longrightarrow}$ and $\vec{p} = (p_1, p_2, \ldots, p_n)$. From the assumption $p \underset{\sim}{\sqsubset}_{\mathrm{RS}} q$ we conclude by (RS3) that $q(\overset{h}{\Longrightarrow}\!|\,)^* q_1 \overset{h}{\Longrightarrow}\!| \, q_2 \cdots \overset{h}{\Longrightarrow}\!|$, $p_i \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_i$ for all $1 \leq i \leq n$, and $q_n \stackrel{h}{\not\longrightarrow}$ by (RS4). Thus, by (H3), $q/h \xrightarrow{\tau} \vec{q}/h$ and $\vec{p} \, \widehat{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} \, \vec{q}$, i.e., $\vec{q}/h \in W_1'' \subseteq W$.

If $\hat{q}/h \in W_2''$, then the state $\hat{q}'$ succeeding $\hat{q}$ on the respective computation $\hat{q} \overset{\tau}{\Longrightarrow}\!| \, \hat{q}''$ satisfies $\hat{q} \xrightarrow{\tau} \hat{q}'$ and $\hat{q}'/h \in W_2''$, or $\hat{q}'/h = \hat{q}''/h \in W_1''$.

To establish Cond. (HW2b) we can assume that we are in the case $\alpha = \tau$ above. Thus, either $\hat{q}/h \xrightarrow{\tau} \vec{q}/h \in W$ and $\vec{q}/h$ is stable; or $\hat{q}/h \overset{\epsilon}{\Longrightarrow} \hat{q}''/h$ with all states in W and $\hat{q}''$ stable. If $\hat{q}''/h$ is not stable, it can stabilise in W with some $\hat{q}''/h \xrightarrow{\tau} \vec{q}/h$ as in the 'either' case. □

We can now prove the compositionality result for ready simulation wrt. hiding.

Proof. [of Thm. 17] We first proof the compositionality statement wrt. stable ready simulation, i.e., the statement:

Let $p \underset{\sim}{\sqsubset}_{\mathrm{RS}} q$ and $h \in \mathcal{A}$ with $p \stackrel{h}{\not\longrightarrow}$ and $q \stackrel{h}{\not\longrightarrow}$. Then, $p/h \underset{\sim}{\sqsubset}_{\mathrm{RS}} q/h$.

To do so, it is sufficient to establish that $\mathcal{R} =_{\mathrm{df}} \mathcal{R}_1 \cup \mathcal{R}_2$ with

$$\begin{aligned}
\mathcal{R}_1 &=_{\mathrm{df}} \{\langle p/h, q/h \rangle \,|\, p \underset{\sim}{\sqsubset}_{\mathrm{RS}} q, \; p \stackrel{h}{\not\longrightarrow} \text{ and } q \stackrel{h}{\not\longrightarrow} \} \\
\mathcal{R}_2 &=_{\mathrm{df}} \{\langle \vec{p}/h, \vec{q}/h \rangle \,|\, \vec{p} = (p_1, p_2, \ldots, p_n) \in \vec{P}, \; \vec{q} = (q_1, q_2, \ldots, q_n) \in \vec{Q}, \text{ and} \\
&\qquad\qquad \vec{p} \, \widehat{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} \, \vec{q} \}
\end{aligned}$$

is a stable ready simulation relation. We check the four conditions of Def. 2:

(RS1) This condition is straightforward for all pairs in $\mathcal{R}_1$ and $\mathcal{R}_2$.

(RS2) Let $\langle \hat{p}/h, \hat{q}/h \rangle \in \mathcal{R}$. Then, $\hat{p}/h \notin F$ and $\hat{p} \, \widehat{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} \, \hat{q}$ implies $\hat{q}/h \in W_1'' \subseteq W$. Hence, $\hat{q}/h \notin F$ by Lemma 21.

(RS3) Let $\langle p/h, q/h \rangle \in \mathcal{R}_1$. We distinguish the following two cases: $p/h \overset{a}{\Longrightarrow}\!| \, p'/h$ and $p/h \overset{a}{\Longrightarrow}\!| \, \vec{p}/h$.

If $p/h \overset{a}{\Longrightarrow}\!| \, p'/h$, then this computation does not contain a state $\vec{p}/h$ since such states are stable, i.e., $\vec{p}/h \overset{\epsilon}{\Longrightarrow}\!| \, p'/h$ is not possible. Hence, the first step of $p/h \overset{a}{\Longrightarrow}\!| \, p'/h$ arises from (H2) and the others from (H1), i.e., $p/h \overset{a}{\Longrightarrow}\!| \, p'/h$ due to $p \xrightarrow{a}_{\mathrm{F}} p_1 \xrightarrow{\tau}_{\mathrm{F}} p_2 \cdots \xrightarrow{\tau}_{\mathrm{F}} p_n = p'$. We have that p' is stable since $p' \xrightarrow{\tau}$ would imply $p'/h \xrightarrow{\tau}$ by (H1). Furthermore, $p' \overset{h}{\not\longrightarrow}$; otherwise, $p'/h \notin F$ would imply $\exists p''. \, p' \overset{\epsilon}{\Longrightarrow}\!| \, (\overset{h}{\Longrightarrow}\!| \,)^* p'' \overset{h}{\not\longrightarrow}$, whence $p' (\overset{h}{\Longrightarrow}\!| \,)^* p'' \overset{h}{\not\longrightarrow}$ by the stability of p' and thus $p'/h \xrightarrow{\tau}$ by (H3).

Since $p \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} q$ and $p \overset{a}{\Longrightarrow}\!| \, p'$, we have $q \overset{a}{\Longrightarrow}\!| \, q'$ for some q' with $p' \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} q'$. Assume $q \overset{a}{\Longrightarrow}\!| \, q'$ arises from $q \xrightarrow{a}_{\mathrm{F}} q_1 \xrightarrow{\tau}_{\mathrm{F}} q_2 \cdots \xrightarrow{\tau}_{\mathrm{F}} q_m = q'$. By (RS4), we get $q \overset{h}{\not\longrightarrow}$ from $p \overset{h}{\not\longrightarrow}$ and $q' \overset{h}{\not\longrightarrow}$ from $p' \overset{h}{\not\longrightarrow}$.

Further, $q \overset{h}{\not\longrightarrow}$ implies $q/h \xrightarrow{a} q_1/h \xrightarrow{\tau} q_2/h \cdots \xrightarrow{\tau} q_m/h = q'/h$. Since $p/h, p'/h \notin F$ by assumption, we have $q/h, q'/h \in W_1''$. In addition, $q_i/h \in W_2''$, for all $1 \leq i \leq m-1$. This gives $q/h \overset{a}{\Longrightarrow}_{\mathrm{F}} q'/h$.

Since q' is stable and $q' \overset{h}{\not\longrightarrow}$, Rules (H1) and (H3) are not applicable to q'/h, i.e., $q/h \overset{a}{\Longrightarrow}\!| \, q'/h$. This finishes the first case.

We now consider $p/h \overset{a}{\Longrightarrow}\!| \, \vec{p}/h$. This computation has the form $p/h \overset{a}{\Longrightarrow}_{\mathrm{F}} p'/h \xrightarrow{\tau}_{\mathrm{F}} \vec{p}/h$ for some p'. Since $p'/h \xrightarrow{\tau}_{\mathrm{F}} \vec{p}/h$ implies $p' \xrightarrow{h}$ and thus p' stable, we can repeat some of the argument of the first case to obtain some q' with $p' \mathrel{\widehat{\underset{\sim}{\sqsubset}}}_{\mathrm{RS}} q'$, $q \overset{a}{\Longrightarrow}\!| \, q'$ due to $q \xrightarrow{a}_{\mathrm{F}} q_1 \xrightarrow{\tau}_{\mathrm{F}} q_2 \cdots \xrightarrow{\tau}_{\mathrm{F}} q_m = q'$, $q/h \xrightarrow{a} q_1/h \xrightarrow{\tau} q_2/h \cdots \xrightarrow{\tau} q_m/h = q'/h$ and $q/h \notin F$.

Now, $p'/h \xrightarrow{\tau}_{\mathrm{F}} \vec{p}/h$ due to $p' (\overset{h}{\Longrightarrow}\!| \,)^* p_1' \overset{h}{\Longrightarrow}\!| \, p_2' \cdots \overset{h}{\Longrightarrow}\!| \, p_n' \overset{h}{\not\longrightarrow}$. This implies, by (RS3), that $q' (\overset{h}{\Longrightarrow}\!| \,)^* q_1' \overset{h}{\Longrightarrow}\!| \, q_2' \cdots \overset{h}{\Longrightarrow}\!| \, q_n'$, for some q_i' with $p_i' \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} q_i'$, for $1 \leq i \leq n$, and $q_n' \overset{h}{\not\longrightarrow}$ due to (RS4). Since $p' \xrightarrow{h}$, we have $q' \xrightarrow{h}$ due to (RS4), i.e., $q'/h \xrightarrow{\tau} (q_1', q_2', \ldots, q_n')/h = \vec{q}/h \overset{\tau}{\not\longrightarrow}$ with $\langle \vec{p}/h, \vec{q}/h \rangle \in \mathcal{R}_2$.

It remains for us to argue that $q_i/h \notin F$, for all $1 \leq i \leq m$, and $\vec{q}/h \notin F$. The latter follows from $\vec{q}/h \in W_1''$ due to $\vec{p} \mathrel{\widehat{\underset{\sim}{\sqsubset}}}_{\mathrm{RS}} \vec{q}$ and $\vec{p}/h \notin F$. Further, $q'/h \notin F$ is a consequence of $q'/h \in W_1''$ due to $p' \mathrel{\widehat{\underset{\sim}{\sqsubset}}}_{\mathrm{RS}} q'$ and $p'/h \notin F$. Finally, $q_i/h \in W_2''$, for all $1 \leq i < m$.

Next, we establish (RS3) for some pair $\langle \vec{p}/h, \vec{q}/h \rangle \in \mathcal{R}_2$ and distinguish again two cases: $\vec{p}/h \overset{a}{\Longrightarrow}\!| \, p'/h$ and $\vec{p}/h \overset{a}{\Longrightarrow}\!| \, \vec{p}'/h$.

In the former case, $\vec{p}/h \xrightarrow{a}_{\mathrm{F}} p/h \overset{\epsilon}{\Longrightarrow}\!| \, p'/h$ due to $p_j \xrightarrow{a}_{\mathrm{F}} p = p_1' \xrightarrow{\tau}_{\mathrm{F}} p_2' \cdots \xrightarrow{\tau}_{\mathrm{F}} p_k' = p'$ with $p' \overset{\tau}{\not\longrightarrow}$ and $p' \overset{h}{\not\longrightarrow}$. Since $p_j \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} q_j$ by assumption and since $p_j \overset{a}{\Longrightarrow}\!| \, p'$, we have $q_j \overset{a}{\Longrightarrow}\!| \, q'$ for some q' with $p' \mathrel{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} q'$. Assume $q_j \overset{a}{\Longrightarrow}\!| \, q'$ due to $q_j \xrightarrow{a}_{\mathrm{F}} q_1' \xrightarrow{\tau}_{\mathrm{F}} q_2' \cdots \xrightarrow{\tau}_{\mathrm{F}} q_m' = q'$. Hence, we obtain, by (H4) and (H1), $\vec{q}/h \xrightarrow{a}_{\mathrm{F}} q_1'/h \overset{\epsilon}{\Longrightarrow}\!| \, q'/h$. To see this, observe that $q' \overset{\tau}{\not\longrightarrow}$ and $q' \overset{h}{\not\longrightarrow}$ by $p' \overset{h}{\not\longrightarrow}$ and (RS4), i.e., q'/h is stable. Furthermore, $q'/h \in W_1''$ due to p', and thus $q_i'/h \in W_2''$, for all $1 \leq i < m$; similarly, $\vec{q}/h \in W_1''$ due to $\vec{p} \mathrel{\widehat{\underset{\sim}{\sqsubset}}}_{\mathrm{RS}} \vec{q}$ by assumption.

Additionally, $p' \not\xrightarrow{h}$, $q' \not\xrightarrow{h}$ and $p' \underset{\sim}{\sqsubset}_{\mathrm{RS}} q'$ imply $\langle p'/h, q'/h \rangle \in \mathcal{R}_1$. This completes the reasoning for the former case.

In the latter case, we have $\vec{p}/h \overset{a}{\Longrightarrow}_{\mathrm{F}} p'/h \xrightarrow{\tau}_{\mathrm{F}} \vec{p}\,'/h$, again due to $p_j \xrightarrow{a}_{\mathrm{F}} p'_1 \xrightarrow{\tau}_{\mathrm{F}} p'_2 \cdots \xrightarrow{\tau}_{\mathrm{F}} p'_k = p'$ and $p'(\overset{h}{\Longrightarrow}|\,)^* p'_1 \overset{h}{\Longrightarrow}| \, p'_2 \cdots \overset{h}{\Longrightarrow}| \, p'_l \not\xrightarrow{h}$ with $\vec{p}\,' = (p'_1, p'_2, \ldots, p'_l)$ and $p' \not\xrightarrow{\tau}$ (due to $p' \xrightarrow{h}$). Since $p_j \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_j$ and $p_j \overset{a}{\Longrightarrow}| \, p'$, we have some q' with $q_j \overset{a}{\Longrightarrow}| \, q'$ and $p' \underset{\sim}{\sqsubset}_{\mathrm{RS}} q'$. Exploiting the latter we get $q'(\overset{h}{\Longrightarrow}|\,)^* q'_1 \overset{h}{\Longrightarrow}| \, q'_2 \cdots \overset{h}{\Longrightarrow}| \, q'_l \not\xrightarrow{h}$, with $p'_i \underset{\sim}{\sqsubset}_{\mathrm{RS}} q'_i$ for all $1 \leq i \leq l$, and $q' \xrightarrow{h}$. Now, $q'/h \in W''_1$ due to p', as well as $\vec{q}/h \in W''_1$ due to $\vec{p}$. The other processes on the computation $\vec{q}/h \overset{a}{\Longrightarrow} q'/h$ are in W''_2. Finally, $q'/h \xrightarrow{\tau}_{\mathrm{F}} (q'_1, q'_2, \ldots, q'_l)/h$ since $(q'_1, q'_2, \ldots, q'_l) \in W''_1$ due to $\vec{p}\,'$. We can now conclude $\vec{q}/h \overset{a}{\Longrightarrow}| \, (q'_1, q'_2, \ldots, q'_l)/h$ and $\langle \vec{p}\,'/h, (q'_1, q'_2, \ldots, q'_l)/h \rangle \in \mathcal{R}_2$.

(RS4) Let $\langle p/h, q/h \rangle \in \mathcal{R}_1$. Because of (RS4) and $p/h \notin F$, whence $p \notin F_P$, we have $\mathcal{I}(p) = \mathcal{I}(q)$. Hence, $\mathcal{I}(p/h) = \mathcal{I}(p) = \mathcal{I}(q) = \mathcal{I}(q/h)$ by the operational rules for hiding. Next, let $\langle \vec{p}/h, \vec{q}/h \rangle \in \mathcal{R}_2$. Then, $\mathcal{I}(\vec{p}/h) = (\bigcup_{1 \leq i \leq n} \mathcal{I}(p_i)) \setminus \{h\} = (\bigcup_{1 \leq i \leq n} \mathcal{I}(q_i)) \setminus \{h\} = \mathcal{I}(\vec{q}/h)$. To verify the second equality, observe that $p_i \notin F_P$ (by the definition of $\vec{p}/h$), $p_i \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_i$ and (RS4).

Now we turn to proving the statement of Thm. 17 itself. Firstly, consider a computation $p/h \overset{\epsilon}{\Longrightarrow}| \, p'/h$; this is due to $p \overset{\epsilon}{\Longrightarrow}| \, p'$ with (H1) as above. By the assumption $p \sqsubseteq_{\mathrm{RS}} q$, we know of the existence of some q' with $q \overset{\epsilon}{\Longrightarrow}| \, q'$ and $p' \underset{\sim}{\sqsubset}_{\mathrm{RS}} q'$. Additionally, $p' \not\xrightarrow{h}$ must hold; otherwise, by $p'/h \notin F$, (H3) would be applicable, contradicting that p'/h is stable. Since $p' \notin F_P$ and by (RS4) we get $q' \not\xrightarrow{h}$, which implies that q'/h is stable. Furthermore, $q'/h \in W''_1$ and, for all other processes $\overline{q}$ along the computation $q \overset{\epsilon}{\Longrightarrow}| \, q'$, we have $\overline{q}/h \in W''_2$. Hence, $q/h \overset{\epsilon}{\Longrightarrow}| \, q'/h$ and $\langle p'/h, q'/h \rangle \in \mathcal{R}_1$, whence $p'/h \underset{\sim}{\sqsubset}_{\mathrm{RS}} q'/h$.

Secondly, we consider a computation $p/h \overset{\epsilon}{\Longrightarrow}| \, \vec{p}/h$, i.e., $p/h \overset{\epsilon}{\Longrightarrow}_{\mathrm{F}} p'/h \xrightarrow{\tau}_{\mathrm{F}} \vec{p}/h$ for some suitable p'. Hence, $p \overset{\epsilon}{\Longrightarrow}| \, p'(\overset{h}{\Longrightarrow}|\,)^* p_1 \overset{h}{\Longrightarrow}| \, p_2 \cdots \overset{h}{\Longrightarrow}| \, p_n \not\xrightarrow{h}$ and $p' \xrightarrow{h}$. Again, we have $q \overset{\epsilon}{\Longrightarrow}| \, q'$ for some q' with $p' \underset{\sim}{\sqsubset}_{\mathrm{RS}} q'$ and, by (RS4), $q' \xrightarrow{h}$. By (RS3), $q'(\overset{h}{\Longrightarrow}|\,)^* q_1 \overset{h}{\Longrightarrow}| \, q_2 \cdots \overset{h}{\Longrightarrow}| \, q_n$ with $p_i \underset{\sim}{\sqsubset}_{\mathrm{RS}} q_i$ for all $1 \leq i \leq n$ and, by (RS4), $q_n \not\xrightarrow{h}$. Similarly as above, we conclude $q/h \overset{\epsilon}{\Longrightarrow}_{\mathrm{F}} q'/h$; note that $\vec{q}/h \in W''_1$ since $\vec{p} \, \widehat{\underset{\sim}{\sqsubset}}_{\mathrm{RS}} \, \vec{q}$ and $\vec{p}/h \notin F$. Thus, $q/h \overset{\epsilon}{\Longrightarrow}| \, \vec{q}/h$ and $\langle \vec{p}/h, \vec{q}/h \rangle \in \mathcal{R}_2$, whence also $\vec{p}/h \underset{\sim}{\sqsubset}_{\mathrm{RS}} \vec{q}/h$. □