HAL open science

Symbolic protocol verification with dice: process equivalences in the presence of probabilities (extended version)

Vincent Cheval, Raphaëlle Crubillé, Steve Kremer

To cite this version:

Vincent Cheval, Raphaëlle Crubillé, Steve Kremer. Symbolic protocol verification with dice: process equivalences in the presence of probabilities (extended version). 2023. hal-03683907v2

HAL Id: hal-03683907

https://inria.hal.science/hal-03683907v2

Preprint submitted on 30 May 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Symbolic protocol verification with dice: process equivalences in the presence of probabilities* (extended version)

Vincent Cheval
Inria Paris

Raphaëlle Crubillé
Aix-Marseille Université
LIS, CNRS

Steve Kremer
Université de Lorraine
Inria Nancy Grand-Est & LORIA

Abstract

Symbolic protocol verification generally abstracts probabilities away, considering computations that succeed only with negligible probability, such as guessing random numbers or breaking an encryption scheme, as impossible. This abstraction, sometimes referred to as the perfect cryptography assumption, has shown very useful as it simplifies automation of the analysis. However, probabilities may also appear in the control flow where they are generally not negligible. In this paper we consider a framework for symbolic protocol analysis with a probabilistic choice operator: the probabilistic applied pi calculus. We define and explore the relationships between several behavioral equivalences. In particular we show the need to require randomized schedulers – indeed we exhibit a counter-example to one of the main results in a previous work that relied on non-randomized ones. As in other frameworks that mix both non-deterministic and probabilistic choices, schedulers may sometimes be unrealistically powerful. We therefore consider two subclasses of processes that avoid this problem. When considering purely non-deterministic protocols, as is done in classical symbolic verification, we show that a probabilistic adversary has—maybe surprisingly—a strictly superior distinguishing power for may testing, which, when the number of sessions is bounded, we show to coincide with purely possibilistic similarity. Finally, we consider fully probabilistic protocols and show that trace equivalence corresponds to a notion of may testing with purely probabilistic attackers. We also briefly discuss complexity and automation for these subclasses when the number of sessions is bounded.

*This work has been partly supported by the ANR Research and teaching chair in AI ASAP with support from the region Grand Est and by France 2030 program managed by ANR (ANR-22-PECY-0006).

Contents

1 Introduction **5**

I A Probabilistic Applied Pi Calculus **7**

2 Probabilistic Applied π-calculus **7**
2.1 Message as terms 7
2.2 Syntax of the process calculus 8
2.3 Operational semantics 9

3 May Testing Equivalences **11**
3.1 Resolving the internal non-determinism 11
3.2 Computing the probability of reaching a barbed state 16
3.3 Defining May Testing Equivalence 17

4 Trace equivalence **17**
4.1 Labelled semantics 18
4.2 Trace Preorder 19
4.3 On randomized or non-randomized resolutions 19

5 Simulation and observational preorders **21**
5.1 Simulation preorder 23
5.2 Observational preorder 25
5.3 Bisimilarity and observational equivalence do not coincide with non-randomized schedulers 26
5.3.1 Counter-example to coincidence of bisimulation and abservational congruence in [GLPT07] 30
5.3.2 The counter-example for a conservative variant of [GLPT07] bisimulation 35

II Well behaved subclasses of protocols **39**

6 Non-Probabilistic Processes **40**
6.1 May-testing with non-probabilistic adversary and trace equivalence coincide 40
6.2 May-testing and simulation coincide for bounded processes 41
6.2.1 Hennessy-Milner logical characterization of strong simulation 42
6.2.2 Complexity 44
6.3 May-testing and simulation do not coincide for unbounded processes 44

7 Fully Probabilistic Agents Communicating on Public Channels **46**
7.1 Removing residual non-determinism . . . 47
7.1.1 Determinizing may-testing for FP processes . . . 50
7.1.2 On trace equivalence for FP processes . . . 50
7.2 May testing equivalence of FP processes with unrestricted adversary. . . . 51
7.3 A fully probabilistic operational semantics for FP processes and determinate adversaries . . . 51

8 Deciding trace equivalence and tool support **53**
8.1 History . . . 54
8.2 Partition tree . . . 57

9 An example: dining cryptographers **61**
9.1 Dining cryptographers, in probabilistic pi-calculus. . . . 61
9.2 Labelled semantics for the dining cryptographers protocol . . . 63
9.3 N^{ℓ} and N_{DC} are bisimilar . . . 65
9.4 Security of the dining cryptographers protocol . . . 71

10 Conclusion and future work **74**

11 Conclusion and future work **74**

A Randomized and non-randomized resolutions coincide for may-testing **80**

B Appendix on trace equivalence **85**
B.1 Randomized and non-randomized resolutions coincide for trace equivalence 85

C Relations $\stackrel{\tau}{\Longrightarrow}_{\mathsf{r}}$ and $\Longrightarrow_{\mathcal{R}_{\mathsf{r}}}$ coincide **90**

D Observational equivalence with name restriction in context **96**

E τ-determinisation **98**

F Simulation and observational preorders coincide **101**
F.1 Some preliminary results . . . 101
F.1.1 Properties on $\mathrm{RProb}_{\mathcal{R}^o_{\mathsf{r}}}(\mathcal{P}, \downarrow c)$ . . . 106
F.2 Restricted characterization of observational relations . . . 109
F.3 Observational preorder implies simulation . . . 110
F.3.1 τ transitions . . . 111
F.3.2 Static equivalence transitions . . . 112
F.3.3 Input and output transitions . . . 113
F.4 Simulation implies observational preorder . . . 123
F.5 Main result . . . 129

G Non probabilistic processes **129**
G.1 Hennessy-Milner's Logical caracterisation 129
G.2 Proposition 6 133

H Fully probabilistic processes **136**

1 Introduction

Automated symbolic protocol verification, based on the seminal work of Dolev and Yao [DY83], has nowadays reached a level of maturity enabling successful use on complex real-world security protocols, including TLS [BBK17, CHH+17], Signal [CGCD+20], authentication protocols of the 5G standard [BDH+18], or EMV's secure payment protocols [BST21] to name only a few. In the symbolic model, a non-deterministic, computationally unbounded attacker is assumed to have complete control of the network, being able to intercept any messages, and forge new ones. As a counterpart, cryptography is *idealized* and the attacker can only use predefined rules to manipulate messages that are represented by terms, e.g. expressed by an equation $dec(enc(m, k), k) = m$ stating that a message m encrypted with k can be decrypted with the same key. This treatment of cryptography is in opposition to computational models where we assume a probabilistic polynomial time attacker, messages are represented by bitstrings and assumptions that an arbitrary such attacker has at most *negligible* probability of breaking a cryptographic primitive. Similarly, in the symbolic model, random values, such as keys or nonces, are chosen freshly from an infinite domain, rather than chosen randomly from a sufficiently large domain. These symbolic abstractions of cryptography and randomness have even been shown sound [CKW10] (under rather strong assumptions) and significantly ease the automation of proofs. Hence, symbolic modeling of messages is arguably useful for formally analyzing cryptographic protocols.

However, the above-described abstractions of randomness only apply to the *messages*, and not to the *control flow*. Typical examples which crucially rely on randomized control flow are mechanisms for providing anonymity, such as the dining cryptographers protocol [Cha88], Mix-nets [Cha81] or Crowds [RR98]. In this paper, we will investigate indistinguishability properties, expressed as equivalences in a cryptographic process calculus, the applied pi calculus [ABF17], extended with a probabilistic choice operator. Typically, the testing equivalence expresses that two processes are equivalent if they exhibit the same behaviour when put in parallel with an arbitrary attacker process. Our work presents foundations for a model that *(i)* extends the scope of symbolic protocol analysis to probabilistic protocols, and *(ii)* allows to consider non-probabilistic protocols in the presence of a probabilistic attacker. In particular, when we consider purely concurrent processes–without probabilistic behavior–the equivalence we obtain is strictly stronger than the standard testing equivalence on such purely concurrent processes; in other terms, probabilistic adversaries are–for good reasons, as we will argue–more powerful in order to distinguish such processes than the purely concurrent adversaries considered in existing works and tools.

Our contributions. In a first part we introduce a probabilistic applied pi calculus and its semantics, which has similarities to [GLPT07], with two major differences. *(i)* We express our semantics in terms of general non-deterministic probabilistic transition systems (NPLTS)–also called probabilistic automata in the literature–which allows us to benefit from a large body of existing results on these systems [SL95, PS07, Cas18, BSV19, DVGHM09, Sto02, Eis17]. *(ii)* More importantly, we differ in the way non-determinism is

resolved: unlike [GLPT07] we allow for *randomized* schedulers—rather than choosing one particular non-deterministic choice, we allow the scheduler to choose an arbitrary distribution on the available non-deterministic choices. Next we introduce testing equivalence, and show that unlike in the purely non-deterministic choice, may-testing is strictly stronger than trace equivalence. Finally, we introduce notions of (bi)simulation and observational preorder and equivalence and show that the simulation and observational pre-order, respectively bisimilarity and observational equivalence, coincide for randomized schedulers. We also show that for non-randomized schedulers, these equivalences do *not* coincide, which provides a counter-example to one of the main results in [GLPT07].

A well-known phenomenon [CP10, AAPvR10] in process calculi that are both probabilistic and non-deterministic is the existence of some *nonrealistic schedulers* that are able to use the internal probabilistic choices done by an agent in order to schedule another agent's non-deterministic choices, i.e., the scheduler leaks the probabilistic choices. Therefore, we study two important *subclasses* of processes that avoid this phenomenon. First, we consider the classical class of non-probabilistic processes, as in the original applied pi calculus, but in the presence of probabilistic adversaries. We show that, if we additionally bound the number of sessions, may-testing with probabilistic adversaries coincides with the classical, purely possibilistic notion of similarity. This provides a contextual characterization of the notion of similarity which is reminiscent of [DVGHM09] in the setting of CSP. Relying on results from [CKR18], this implies that testing equivalence with probabilistic adversaries is co-NEXPTIME complete for a large class of cryptographic primitives. Second, we consider a class of fully probabilistic processes, which is reminiscent of a probabilistic version of simple processes in [CCD13, CC08], and a slight generalization of the processes in [CSV17]. We next show that trace equivalence as considered in [CSV17], is weaker than may-testing, but coincides with a version of may-testing where attacker processes are restricted disallowing replication, parallel, and non-deterministic choice, but allowing probabilistic choices. Finally, we briefly discuss how the algorithm for deciding trace equivalence in the DeepSec verifier [CKR18] could be adapted to this fully probabilistic case, providing a more general setting than Bauer *et al.* [BCSV18] who additionally bound the size of input messages. A thorough treatment of this adaptation and implementation is left for future work. Most of our results are summarized in Figure 1 that depicts the relationship between the different preorders (with similar relations between corresponding equivalences).

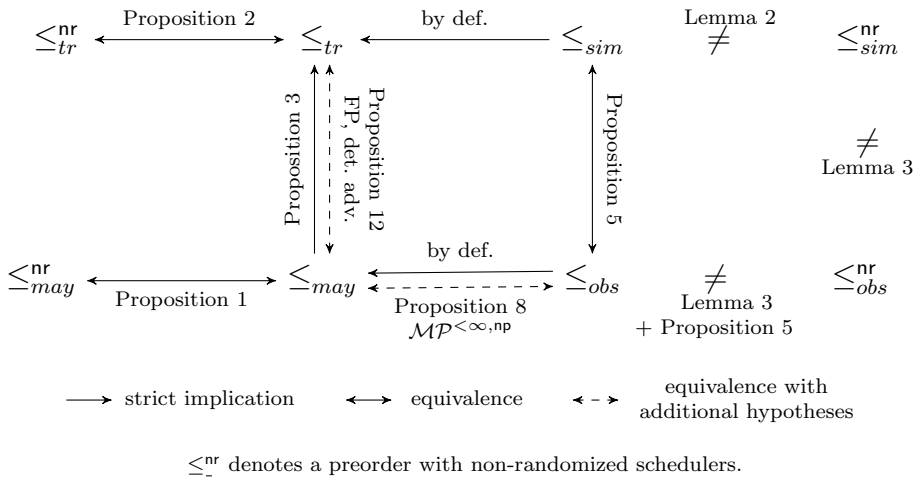


Figure 1: Summary of the relationship between preorders.

Part I
A Probabilistic Applied Pi Calculus

In this first part we present a probabilistic extension of the applied pi calculus. We first introduce its syntax and internal semantics. Then we introduce different equivalences and preorders, and study their relations. We start with the classical may-testing equivalence, which requires to be precise about how non-determinism is resolved. Then we introduce a labelled semantics and the notion of trace equivalence. Unlike in the purely non-deterministic case, trace equivalence is (strictly) weaker than may testing. Finally, we introduce other equivalences and preorders: similarity, bisimilarity and observational preorder/equivalence. We emphasize the need for randomized schedulers; indeed, the use of non-randomized schedulers results into a non-transitive simulation relation.

2 Probabilistic Applied π-calculus

In this paper, we will work with probabilistic applied π-calculus, the probabilistic variant of applied π-calculus introduced by Goubault-Larrecq et al. [GLPT07].

2.1 Message as terms

We assume an infinite set of names, denoted $\mathcal{N} = \{a, b, \ldots, \}$. We partition the set $\mathcal{N}$ into two disjoint infinite sets $\mathcal{N}_{pub}$ and $\mathcal{N}_{priv}$ to respectively represents *public* and *private* names. The distinction between public and private names is analogous to the distinction between free and bound names in the original applied pi calculus. We define an infinite set of variables $\mathcal{X}$. Finally we consider a finite set of *function symbols* with their arity

$\mathcal{F} = \{f/n, g/m, \ldots\}$, called *signature*. *Terms* are defined as names, variables, and function symbols applied to other terms. For any $\mathsf{F} \subseteq \mathcal{F}$, $\mathsf{N} \subseteq \mathcal{N}$ and $\mathsf{V} \subseteq \mathcal{X}$, the set of terms built from N and V by applying function symbols in F is denoted by $\mathcal{T}(\mathsf{F}, \mathsf{N} \cup \mathsf{V})$. We call *protocol terms* the terms from $\mathcal{T}(\mathcal{F}, \mathcal{N} \cup \mathcal{X})$.

We also suppose that terms are equipped with a binary relation $\doteq$ that expresses that two terms evaluate to the same result, and a predicate $Msg(\cdot)$ that is intended to hold when evaluation succeeds. We suppose that $\doteq$ is a symmetric and transitive relation that is closed under substitution of terms for names and variables, as well as application of function symbols and such that for all $a, b \in \mathcal{N}$, $a = b$ if and only if $a \doteq b$. $Msg(\cdot)$ is supposed to hold on any names, to be closed under renamings and $t_1 \doteq t_2$ implies that $Msg(t_1)$ and $Msg(t_2)$. Finally, we require that $Msg(t)$ implies $t \doteq t$.

For example, the $\doteq$ relation could capture that $dec(enc(m, k), k) \doteq m$ for any m, k modelling that decryption cancels out encryption when the same key k is used and one may define $Msg(dec(n, k))$ as false to express that decryption could fail if the ciphertext it is applied to is not an encryption with the matching key.

How $\doteq$ and $Msg(\cdot)$ are precisely defined is not relevant for the results of this paper and we wish to capture several formalisms. $\doteq$ can for instance be defined by an equational theory, as in the applied pi calculus [ABF17] (where $Msg(\cdot)$ would evaluate to true on any term), defined by a constructor-destructor rewrite system, allowing evaluation to fail when a destructor application does not reduce, as in the DeepSec tool [CKR18], or a combination of these as in the ProVerif tool [Bla16].

2.2 Syntax of the process calculus

The syntax for *processes* is defined as follows:

$P, Q ::=$	processes
0	nil
$\mathsf{in}(u, x); P$	output
$\mathsf{out}(u, v); P$	input
$P \mid Q$	parallel composition
$!P$	replication
$\mathsf{new}\ a; P$	restriction
$\mathsf{if}\ u = v\ \mathsf{then}\ P\ \mathsf{else}\ Q$	conditional
$P + Q$	non-deterministic choice
$P +_p Q$	probabilistic choice

where u, v are protocol terms, $x \in \mathcal{X}$, $a \in \mathcal{N}$ and $p \in]0; 1[$. A process P is closed when all variables in P are bound by an input.

Notation 1. We write $\mathcal{SP}$ for the set of all processes in probabilistic applied π-calculus, and $\mathcal{MP}$ for the set of all multisets over $\mathcal{SP}$. We sometimes consider syntactic subclasses of these processes. For finite processes, i.e., without replication, we denote these sets by

$\mathcal{SP}^{<\infty}$ and $\mathcal{MP}^{<\infty}$. For non probabilistic, i.e. purely non-determinisitic processes without $+_p$, we write $\mathcal{SP}^{\mathsf{np}}$ and $\mathcal{MP}^{\mathsf{np}}$ and when considering both restrictions we write $\mathcal{SP}^{<\infty,\mathsf{np}}$ and $\mathcal{MP}^{<\infty,\mathsf{np}}$.

2.3 Operational semantics

We will now define the semantics of the probabilistic applied π-calculus. We opt for a different presentation of the semantics than Goubault-Larrecq *et al.* [GLPT07] relying on existing formalisms for transition systems. Moreover, we allow for a more general class of schedulers.

Notation 2. Let $\mathcal{S}$ be any set. We denote by $\mathcal{D}(\mathcal{S})$ the set of all finitely supported probability distributions over $\mathcal{S}$. We denote by $\mathcal{D}^{\leq 1}(\mathcal{S})$ the set of all sub-probability distributions over $\mathcal{S}$ (observe that $\mathcal{D}(\mathcal{S}) \subseteq \mathcal{D}^{\leq 1}(\mathcal{S})$). For $p, q \geq 0$, and D, E two sub-distributions, we write $p \cdot D + q \cdot E$ for the measure defined as $(p \cdot D + q \cdot E)(x) = p \cdot D(x) + q \cdot E(x)$. In the particular case where $q = 0$, the resulting sub-distribution does not depend on E, and we simply write $p \cdot D$ instead of $p \cdot D + 0 \cdot E$.

If $D \in \mathcal{D}(\mathcal{S})$, we denote by $\mathrm{supp}(D)$ the support of D, i.e. the set of all elements $s \in \mathcal{S}$ such that $D(s) > 0$. If $\mathcal{S}' \subseteq \mathcal{S}$, we note $D(\mathcal{S}') = \sum_{s \in \mathcal{S}'} D(s)$. Finally, we denote by δ_x the Dirac distribution on x.

The operational semantics of processes is defined by a relation between multisets of processes and probability distributions on multisets of processes, denoted $\mathcal{P} \rightarrow_\tau \mu$. This relation is defined in Figure 2.

Remark 1. One may note that our calculus offers a non-deterministic choice operator that is resolved internally. This differs from the standard pi-calculus [MPW92] where the non-deterministic choice operator is resolved externally. Even though the original applied pi calculus [ABF17] does not contain non-deterministic choice the process $P + Q$ can be encoded as

$$\mathsf{new}\ c; ((\mathsf{out}(c, \mathsf{tok}); P) \mid (\mathsf{in}(c, \mathsf{tok}); Q))$$

where c and x do not occur in P nor in Q. Alternatively, we could have defined $+$ as syntactic sugar.

In the following, we will deal with the operational semantics of our calculus with tools designed for generic probabilistic systems. We choose the notion of *non-deterministic probabilistic labelled transition systems* (NPLTS) used for instance in [BSV19]. A NPLTS allows to represent states that have both *internal* and *external* non-deterministic behavior. It can be noted that it coincides with the notion of *simple probabilistic automata* of Segala et al [SL95].

Notation 3. Let $\mathcal{S}$ be any set. We denote $\mathcal{P}(\mathcal{S})$ for the set of all finite subsets of $\mathcal{S}$. Moreover, we can augment $\mathcal{S}$ with a special element $\star$ will be used to talk about deadlocks, i.e. $\mathcal{S} \cup \{\star\}$.

$$\mathcal{P} \cup \{\!\{0\}\!\} \to_\tau \delta_{\mathcal{P}} \qquad \text{(Null)}$$
$$\mathcal{P} \cup \{\!\{\mathsf{if}\ u = v\ \mathsf{then}\ P\ \mathsf{else}\ Q\}\!\} \to_\tau \delta_{\mathcal{P}\cup\{\!\{P\}\!\}} \qquad \text{if } u \doteq v \qquad \text{(Then)}$$
$$\mathcal{P} \cup \{\!\{\mathsf{if}\ u = v\ \mathsf{then}\ P\ \mathsf{else}\ Q\}\!\} \to_\tau \delta_{\mathcal{P}\cup\{\!\{Q\}\!\}} \qquad \text{if } u \not\doteq v \qquad \text{(Else)}$$
$$\mathcal{P} \cup \{\!\{\mathsf{out}(u,t).P, \mathsf{in}(v,x).Q\}\!\} \to_\tau \delta_{\mathcal{P}\cup\{\!\{P,Q\{x\mapsto t\}\}\!\}} \qquad \text{if } Msg(t) \wedge u \doteq v \qquad \text{(Comm)}$$
$$\mathcal{P} \cup \{\!\{P \mid Q\}\!\} \to_\tau \delta_{\mathcal{P}\cup\{\!\{P,Q\}\!\}} \qquad \text{(Par)}$$
$$\mathcal{P} \cup \{\!\{!P\}\!\} \to_\tau \delta_{\mathcal{P}\cup\{\!\{!P,P\}\!\}} \qquad \text{(Repl)}$$
$$\mathcal{P} \cup \{\!\{\mathsf{new}\ a; P\}\!\} \to_\tau \delta_{\mathcal{P}\cup\{\!\{P\{^{a'}/_{a}\}\}\!\}} \qquad \text{where } a' \in \mathcal{N}_{priv} \text{ is fresh} \qquad \text{(New)}$$
$$\mathcal{P} \cup \{\!\{P + Q\}\!\}) \to_\tau \delta_{\mathcal{P}\cup\{\!\{P\}\!\}} \qquad \text{(Choice-1)}$$
$$\mathcal{P} \cup \{\!\{P + Q\}\!\} \to_\tau \delta_{\mathcal{P}\cup\{\!\{Q\}\!\}} \qquad \text{(Choice-2)}$$
$$\mathcal{P} \cup \{\!\{P +_p Q\}\!\} \to_\tau p \cdot \delta_{\mathcal{P}\cup\{\!\{P\}\!\}} + (1-p) \cdot \delta_{\mathcal{P}\cup\{\!\{Q\}\!\}} \qquad \text{(PChoice)}$$

Figure 2: Semantics of the calculus

Definition 1 (NPLTS)**.** A NPLTS is a triple $(\mathcal{S}, \mathcal{A}, \mathsf{trans})$, where

- $\mathcal{S}$ is a set of states,
- $\mathcal{A} = \mathcal{A}_{int} \sqcup \mathcal{A}_{ext}$ is a set of labels, and
- $\mathsf{trans} : \mathcal{S} \to \mathcal{A} \to \mathcal{P}(\mathcal{D}(\mathcal{S}))$ is a transition function: for each state in $\mathcal{S}$, and each label in $\mathcal{A}$, $\mathsf{trans}(s)(a)$ is a set of (finitely supported) distributions.

The labels in $\mathcal{A}_{int}$, respectively $\mathcal{A}_{ext}$ are called *internal*, respectively *external* actions. For $s \in \mathcal{S}, a \in \mathcal{A}$, when $D \in \mathsf{trans}(s,a)$ we write $s \xrightarrow{a} D$ if $a \in \mathcal{A}_{ext}$ and $s \xrightarrow{\tau} D$ if $a \in \mathcal{A}_{int}$.

In the rest of this paper, we may define a NPLTS by only its transition function, i.e., we will say that $\mathsf{trans} : \mathcal{S} \to \mathcal{A} \to \mathcal{P}(\mathcal{D}(\mathcal{S}))$ is the NPLTS $(\mathcal{S}, \mathcal{A}, \mathsf{trans})$. When considering an NPLTS with only one internal action, this action will usually be noted τ, in such a way that $s \xrightarrow{\tau} D$ if and only if $D \in \mathsf{trans}(s, \tau)$.

We now express our operational semantics as a NPLTS, whose only action is the internal action $\{\tau\}$. The need for external actions will become clear in Section 4, when defining a labelled semantics as a NPLTS N^ℓ with an internal action τ, and several external actions that represent adversarial transitions. Moreover, in Section **??**, we consider a refinement of both labelled and non-labelled semantics, using *several* internal actions: an internal action will correspond to an internal action τ decorated with an annotation visible by the scheduler.

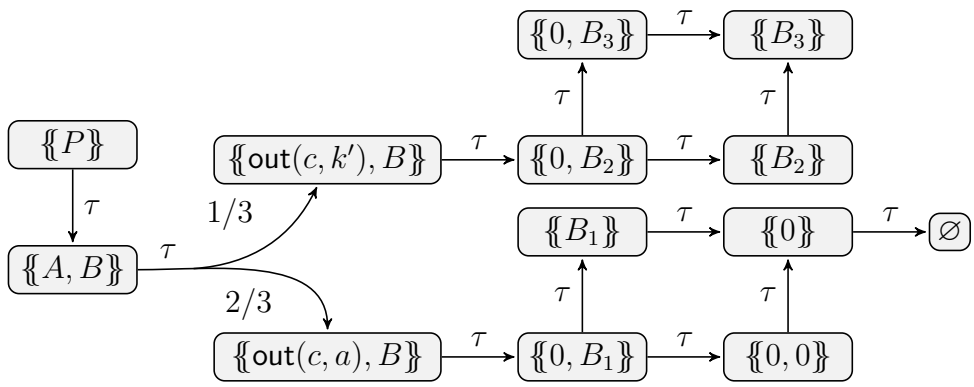
Definition 2. The *operational semantics* is the NPLTS $\mathsf{N}^o = (\mathcal{MP}, \{\tau\}, \mathsf{trans}^o)$ where for every $s \in \mathcal{MP}$, $\mathsf{trans}^o(s)(\tau) = \{D \mid s \to_\tau D\}$.

Note that the states of the NPLTS N^o contain *all* possible multisets of processes and how they are executed. Obviously, N^o is thus an infinite transition system. In examples

illustrating transitions of a multiset of processes $\mathcal{P}$, we only show the relevant fragment of N^o that contains $\mathcal{P}$.

Example 1. The complete execution of the following process P is given in Figure 3.

$$(\mathsf{out}(c,k) +_{1/3} \mathsf{out}(c,a)) \mid \mathsf{in}(c,x); \mathsf{if}\ x = k\ \mathsf{then}\ \mathsf{out}(c,ok)$$



$A = \mathsf{out}(c,k) +_{1/3} \mathsf{out}(c,a)$

$B = \mathsf{in}(c,x); \mathsf{if}\ x = k'\ \mathsf{then}\ \mathsf{out}(c,ok)$

$B_1 = \mathsf{if}\ a = k'\ \mathsf{then}\ \mathsf{out}(c,ok)$

$B_2 = \mathsf{if}\ k' = k'\ \mathsf{then}\ \mathsf{out}(c,ok)$

$B_3 = \mathsf{out}(c,ok)$

Figure 3: Semantics of the process P from Example 1

3 May Testing Equivalences

3.1 Resolving the internal non-determinism

We generically express the way to resolve the internal non-determinism of a NPLTS using the formalism of *resolutions*: resolving the non-determinism means choosing from the NPLTS, a particular transition system without internal non-determinism. The resulting transition system is called a *Reactive Probabilistic Labelled Model* and has still external, but no internal, non-determinism. It can be noted that this model is equivalent to Labelled Markov Chains when extended with internal actions.

Definition 3 (RPLTS)**.** A Reactive Probabilistic Labelled Transition System (RPLTS) is a triple $(\mathcal{S}, \mathcal{A}, \mathsf{trans})$, where

- $\mathcal{S}$ is a set of states,
- $\mathcal{A} = \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}$ a set of labels, and

- $\mathsf{trans} : \mathcal{S} \to (\mathcal{A}_{ext} \to (\mathcal{D}(\mathcal{S}) \cup \{\star\})) \sqcup (\mathcal{A}_{int} \times \mathcal{D}(\mathcal{S}))$ is a transition function that assigns to each state in $\mathcal{S}$
  - either a function mapping labels in $\mathcal{A}_{ext}$ to a failure or a distribution over $\mathcal{S}$ (the non deterministic external actions);
  - or one unique distribution with its internal label from $\mathcal{A}_{int}$ (the deterministic internal action).

The states $s \in \mathcal{S}$ such that $\mathsf{trans}(s) : \mathcal{A}_{ext} \to (\mathcal{D}(\mathcal{S}) \cup \{\star\})$ are called *external states*, while the ones such that $\mathsf{trans}(s) : (\mathcal{A}_{int} \times \mathcal{D}(\mathcal{S}))$ are called *internal states*. Given an RPLTS R, we will denote by $\mathcal{S}_{ext}(R)$ and $\mathcal{S}_{int}(R)$ the sets of external and internal states of R respectively.

In the particular case of a NPLTS with no external action, resolving the internal non-determinism results in a system with *no* non-determinism at all. This is for instance the case of the operational semantics N^o. Such a purely probabilistic system can be modelled as a *reactive probabilistic transition system* (that is equivalent to the notion of Markov Chain).

Definition 4 (RPTS)**.** A Reactive Probabilistic Transition System (RPTS) is a pair $(\mathcal{S}, \mathsf{trans})$, where

- $\mathcal{S}$ is a set of states, and
- $\mathsf{trans} : \mathcal{S} \to (\mathcal{D}(\mathcal{S}) \cup \{\star\})$ is a transition function that assigns to each state in $\mathcal{S}$ either a failure token $\star$, or a distribution over $\mathcal{S}$.

We now define *resolutions*–or schedulers–for a NPLTS that allow to solve the *internal*, but not external, non-determinism: a resolution describes *one* of the possible ways of turning an NPLTS into a RPLTS. It means that for each state s, a resolution should choose whether s is an internal state or external state; in the first case, a *unique* pair of an internal action and a post-transition distribution must be chosen; in the second case, for each external action a, the resolution must choose a *unique* distribution D (if it exists) such that $s \to_a D$. It is however slighly more complicated, since the possible existence of cycles in the execution–meaning that from the same state, the scheduler can do successively different choices–lead to the necessity of a *correspondance function*.

Example 2. There are indeed cycles in the NPLTS N^o, because of the replication operator !. For instance, we can consider the following process P:

$$P := !Q \qquad \text{with } Q := \mathsf{in}(u, x) \mid (\mathsf{out}(u, 0) + \mathsf{out}(u, 1)).$$

We represent in Figure 4 a fragment of N^o containing the state $\{\!\{P\}\!\}$. (Observe that this fragment is not self-contained, in the sense that there exist N^o-transitions from states in this fragment to states absent from this fragment).

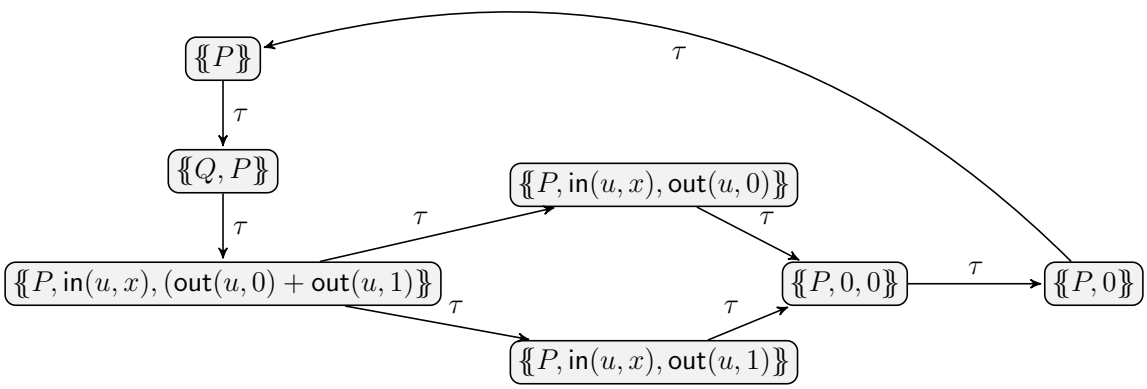


Figure 4: A cycle in N^o, from Example 2

Notation 4. Let $\mathcal{S}$ be a set of states and $\Delta \subseteq \mathcal{D}(\mathcal{S})$ be a finite set of probability distributions over $\mathcal{S}$. The *convex hull* of Δ is defined as:

$$\text{conv}(\Delta) := \{D \in \mathcal{D}(\mathcal{S}) \mid \exists \alpha_1, \ldots, \alpha_n \in \mathbb{R}. \exists D_1, \ldots, D_n \in \Delta. \sum_{i=1}^{n} \alpha_i = 1 \wedge D = \sum_{i=1}^{n} \alpha_i \cdot D_i\}$$

Notation 5. Let $\mathcal{S}, \mathcal{S}'$ be two sets of states and $f : \mathcal{S} \to \mathcal{S}'$. We define the function $\overline{f} : \mathcal{D}(\mathcal{S}) \to \mathcal{D}(\mathcal{S}')$ to be the *probabilistic lifting of* f, where $\overline{f}(D) = \sum_{s \in \mathcal{S}} D(s) \cdot \delta_{f(s)}$.

When obvious from context, we will overload the notation and write f instead of $\overline{f}$.

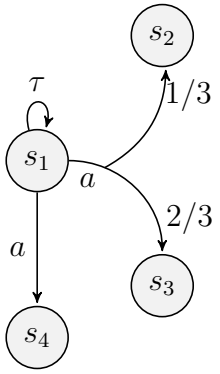
Definition 5 ([BSV19])**.** Let $\mathsf{trans} : \mathcal{S} \to \mathcal{A}_{int} \sqcup \mathcal{A}_{ext} \to \mathcal{P}(\mathcal{D}(\mathcal{S}))$ be a NPLTS.
A *randomized, respectively non-randomized, resolution* for trans is a triple $(\mathcal{S}', \mathsf{corr}, \mathsf{trans}')$, where $\mathcal{S}'$ is a set of states, $\mathsf{corr} : \mathcal{S}' \to \mathcal{S}$ is the *correspondence function*, and $\mathsf{trans}' : \mathcal{S}' \to (\mathcal{A}_{ext} \to (\mathcal{D}(\mathcal{S}') \cup \{\star\})) \sqcup (\mathcal{A}_{int} \times \mathcal{D}(\mathcal{S}'))$ is a RPLTS R such that:

if $s' \in \mathcal{S}_{ext}(R)$ and $\mathsf{trans}'(s')(a) = D$, or $s' \in \mathcal{S}_{int}(R)$ and $\mathsf{trans}'(s') = (a, D)$,

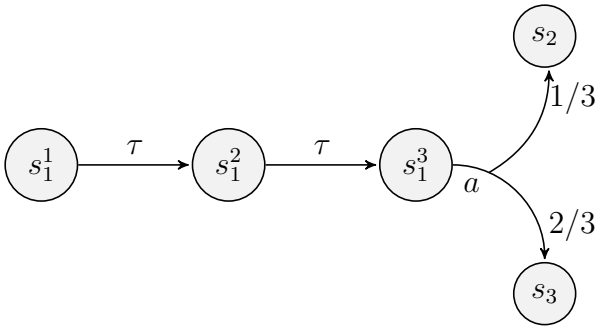
then $\mathsf{corr}(D) \in \text{conv}(\mathsf{trans}(\mathsf{corr}(s'))(a))$ (randomized), respectively
corr is injective on the support of D and $\mathsf{corr}(D) \in \mathsf{trans}(\mathsf{corr}(s'))(a)$ (non-randomized).

Given a NPLTS N we denote by $\mathcal{R}_{\mathsf{r}}(\mathsf{N})$, respectively $\mathcal{R}_{\mathsf{nr}}(\mathsf{N})$, the set of randomized, respectively non-randomized resolutions. Observe that any non-randomized resolution is also a randomized resolution, i.e., $\mathcal{R}_{\mathsf{nr}}(\mathsf{N}) \subset \mathcal{R}_{\mathsf{r}}(\mathsf{N})$.

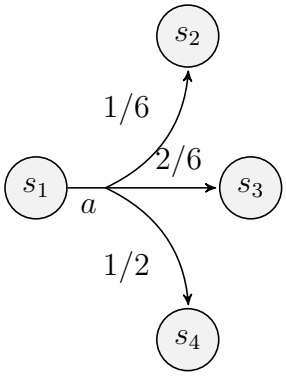
Remark 2. In the particular case of an NPLTS N that has only one internal action τ, and no external actions, as for instance N^o, a resolution is a triple $\mathsf{R} = (\mathcal{S}', \mathsf{corr}, \mathsf{trans}')$, where $\mathcal{S}'$ is a set of states, $\mathsf{corr} : \mathcal{S}' \to \mathcal{S}$ is the *correspondence function*, and $\mathsf{trans}' : \mathcal{S}' \to (\varnothing \to (\mathcal{D}(\mathcal{S}') \cup \{\star\})) \sqcup (\{\tau\} \times \mathcal{D}(\mathcal{S}'))$. Recall that for any set X, the cardinality of the set $(\varnothing \to X)$ is 1: by abuse of notation, we denote by $\star$ the unique element of the set



(a) A NPLTS N



(b) A non-randomized resolution for N
$\mathsf{corr}(s_1^i) = s_1$ $(1 \leq i \leq 3)$, $\mathsf{corr}(s_j) = s_j$ $(2 \leq j \leq 3)$.



(c) A randomized resolution for N
$\mathsf{corr}(s_i) = s_i$ $(1 \leq i \leq 3)$

$(\varnothing \to (\mathcal{D}(\mathcal{S}') \cup \{\star\}))$. With this notation–and by indentifying any set X to the isomorphic set $\{\tau\} \times X$–we can simply rewrite trans' as:

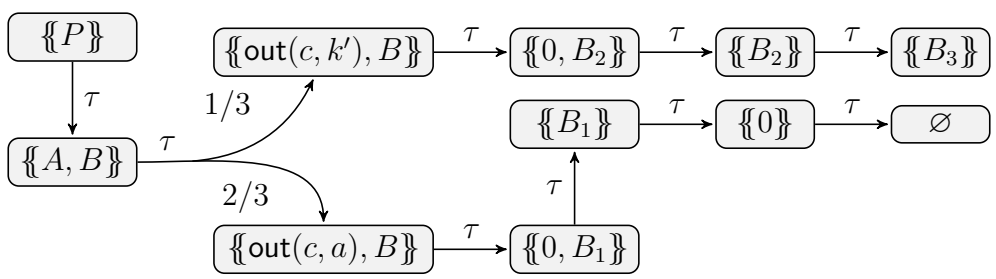
$$\mathsf{trans}' : \mathcal{S}' \to \{\star\} \sqcup \mathcal{D}(\mathcal{S}').$$

To sum up, there are two possibilities when we star from a R-state $s' \in \mathcal{S}'$: either the execution stops here (in this case, $\mathsf{trans}(s') = \star$, and thus s' is an external state), or the scheduler chooses the next step (in this case, $\mathsf{trans}(s') \in \mathcal{D}(\mathcal{S}')$, and thus s' is an internal state). Formally, it means that the N-resolutions are actually RPTSs–the purely probabilistic structure defined in Definition 4. Moreover, we can rewrite the simplified constraints on resolutions given in Definition 5 as follows:

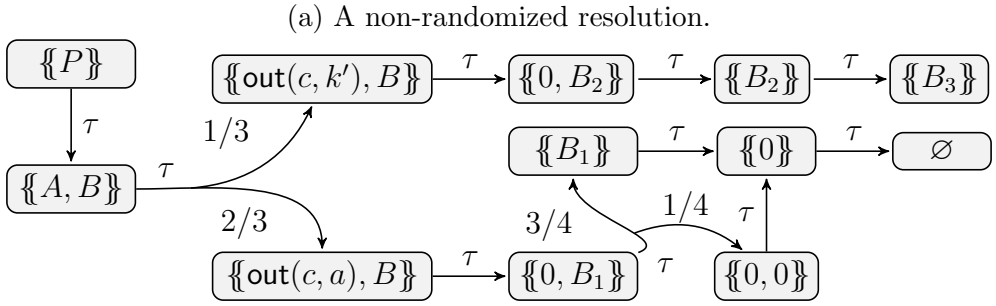
if $\mathsf{trans}'(s') = D$

then $\mathsf{corr}(D) \in \mathrm{conv}(\mathsf{trans}(\mathsf{corr}(s'))(\tau))$ (randomized), respectively
corr is injective on the support of D and $\mathsf{corr}(D) \in \mathsf{trans}(\mathsf{corr}(s'))(\tau)$ (non-randomized).

We show in Figure 6 examples of N^o-resolutions for the process P from Example 1 and its semantics in Figure 3.



(a) A non-randomized resolution.



(b) A randomized resolution.

Figure 6: Examples of resolutions for process P from Example 1 where the correspondence function corr is the identity. Resolutions in N^o correspond to a Markov Chain.

3.2 Computing the probability of reaching a barbed state

We first precise when a state of N^o, i.e., a multiset of processes, exhibits a barb c.

Definition 6. For any public name $c \in \mathcal{N}_{pub}$, and a multiset of processes $\mathcal{P} \in \mathcal{MP}$, we say that $\mathcal{P}$ *exhibits barb* c when there exists a process $\mathsf{out}(u,t).Q$ in $\mathcal{P}$ where $c \doteq u$ and $Msg(t)$. We denote by $\downarrow c$ the set of all multisets of processes that exhibit the barb c.

We formalize here the probability of reaching a state in some set of target states, in a *fully probabilistic* transition system, i.e., in a transition system where all non-determinism–internal or external–has already been resolved. We first define the probability of reaching such a state in at most n steps, and then we take the probability of reaching them eventually as the limit of the n-step reaching probabilities.

Definition 7. Let $R = (\mathcal{S}, \mathsf{trans})$ be a RPTS, $\mathcal{T} \subseteq \mathcal{S}$ a set of states, and s an initial state. For every $n \in \mathbb{N}$ we define the *probability of reaching* $\mathcal{T}$ *from* s *in at most* n *steps* as:

$$\mathrm{RProb}_R^{\leq 0}(s,\mathcal{T}) = \begin{cases} 1 & \text{if } s \in \mathcal{T} \\ 0 & \text{otherwise.} \end{cases}$$

$$\mathrm{RProb}_R^{\leq n+1}(s,\mathcal{T}) = \begin{cases} 1 & \text{if } s \in \mathcal{T} \\ 0 & \text{if } s \notin \mathcal{T} \wedge \mathsf{trans}(s) = \star \\ \sum_{u \in \mathrm{supp}(D)} D(u) \cdot \mathrm{RProb}_R^{\leq n}(u,\mathcal{T}) & \text{if } s \notin \mathcal{T} \wedge \mathsf{trans}(s) = D \end{cases}$$

We define the *probability of reaching* $\mathcal{T}$ *from* s as:

$$\mathrm{RProb}_R(s,\mathcal{T}) = \lim_{n \to +\infty} \mathrm{RProb}_R^{\leq n}(s,\mathcal{T}).$$

Note that, as $\mathrm{RProb}_R^{\leq n}(s,\mathcal{T})$ is an increasing function in n we can replace the limit by the supremum on $n \in \mathbb{N}$.

Notation 6. Let $\mathsf{N} = (\mathcal{S}_\mathsf{N}, \mathcal{A}, \mathsf{trans}_\mathsf{N})$ be a NPLTS, and $\mathsf{R} = (\mathcal{S}_\mathsf{R}, \mathsf{corr}_\mathsf{R}, \mathsf{trans}_\mathsf{R})$ be a resolution for N. Recall that $\widehat{\mathsf{R}} = (\mathcal{S}_\mathsf{R}, \mathcal{A}, \mathsf{trans}_\mathsf{R})$ is a RPLTS. From $\widehat{\mathsf{R}}$, we build a RPTS by removing the external actions: we define $\widetilde{\mathsf{R}} = (\mathcal{S}_\mathsf{R}, \mathsf{trans}_{\widetilde{\mathsf{R}}})$ where

$$\mathsf{trans}_{\widetilde{\mathsf{R}}}(s) = \begin{cases} \star & \text{when } s \in \mathcal{S}_{ext}(\widehat{\mathsf{R}}) \\ D & \text{when } s \in \mathcal{S}_{int}(\widehat{\mathsf{R}}) \text{ and } \mathsf{trans}_\mathsf{R}(s) = (a_{int}, D) \end{cases}$$

For $\mathcal{T} \subseteq \mathcal{S}_\mathsf{R}$, $s \in \mathcal{S}_\mathsf{R}$ and resolution R we write $\mathrm{RProb}_\mathsf{R}(s,\mathcal{T})$, respectively $\mathrm{RProb}_\mathsf{R}^{\leq n}(s,\mathcal{T})$, for the probability $\mathrm{RProb}_{\widetilde{\mathsf{R}}}(s,\mathcal{T})$, respectively $\mathrm{RProb}_{\widetilde{\mathsf{R}}}^{\leq n}(s,\mathcal{T})$.

For $\mathcal{T} \subseteq \mathcal{S}_\mathsf{N}$, $s \in \mathcal{S}_\mathsf{N}$, and $\mathcal{R} \subseteq \mathcal{R}_\mathsf{r}(\mathsf{N})$, we note $\mathrm{RProb}_\mathcal{R}(s,\mathcal{T})$, respectively $\mathrm{RProb}_\mathcal{R}^{\leq n}(s,\mathcal{T})$, for the probability $\sup\{\mathrm{RProb}_\mathsf{R}(s', \mathsf{corr}_\mathsf{R}^{-1}(\mathcal{T})) \mid \mathsf{R} = (\mathcal{S}_\mathsf{R}, \mathsf{corr}_\mathsf{R}, \mathsf{trans}_\mathsf{R}) \in \mathcal{R}, \mathsf{corr}_\mathsf{R}(s') = s\}$, respectively $\sup\{\mathrm{RProb}_\mathsf{R}^{\leq n}(s', \mathsf{corr}_\mathsf{R}^{-1}(\mathcal{T})) \mid \mathsf{R} = (\mathcal{S}_\mathsf{R}, \mathsf{corr}_\mathsf{R}, \mathsf{trans}_\mathsf{R}) \in \mathcal{R}, \mathsf{corr}_\mathsf{R}(s') = s\}$.

In the following we denote by $\mathcal{R}_\mathsf{r}^o$ (resp. $\mathcal{R}_\mathsf{nr}^o$) the set of all randomized (resp. non-randomized) resolutions for N^o, i.e., $\mathcal{R}_\mathsf{r}^o = \mathcal{R}_\mathsf{r}(\mathsf{N}^o)$ and $\mathcal{R}_\mathsf{nr}^o = \mathcal{R}_\mathsf{nr}(\mathsf{N}^o)$.

3.3 Defining May Testing Equivalence

Definition 8 (May testing equivalence)**.** Let $\mathcal{R}$ be a set of resolutions for N^o and $\mathcal{P}, \mathcal{Q} \in \mathcal{MP}$. We say that

$$\mathcal{P} \leq^{\mathcal{R}}_{may} \mathcal{Q} \quad \text{iff} \quad \begin{array}{l} \forall Adv \in \mathcal{MP} \text{ s.t. } fn(Adv) \subseteq \mathcal{N}_{pub}.\ \forall c \in \mathcal{N}_{pub}. \\ \mathrm{RProb}_{\mathcal{R}}(\mathcal{P} \cup Adv, \downarrow c) \leq \mathrm{RProb}_{\mathcal{R}}(\mathcal{Q} \cup Adv, \downarrow c) \end{array}$$

We say that $\mathcal{P}, \mathcal{Q}$ are may testing equivalent for $\mathcal{R}$, denoted $\mathcal{P} \approx^{\mathcal{R}}_{may} \mathcal{Q}$ when both $\mathcal{P} \leq^{\mathcal{R}}_{may} \mathcal{Q}$ and $\mathcal{Q} \leq^{\mathcal{R}}_{may} \mathcal{P}$.

We first show that for may-testing, it is sufficient to consider non-randomized resolutions.

Proposition 1. The may testing preorder coincides for randomized and non-randomized resolutions:

$$\leq^{\mathcal{R}^o_{\mathsf{r}}}_{may} = \leq^{\mathcal{R}^o_{\mathsf{nr}}}_{may}$$

The proof of this result is given in Appendix A.

Given that the may testing preorder coincides for randomized and non-randomized resolutions we will simply write $\leq_{may}$ in what follows.

Remark 3. One alternative definition of probabilistic may testing pre-orders studied in the literature is as follows: $\mathcal{P} \leq' \mathcal{Q}$ iff

for all $Adv \in \mathcal{MP}$ s.t. $fn(Adv) \subseteq \mathcal{N}_{pub}$, $c \in \mathcal{N}_{pub}$, resolution R and R-state s s.t. $\mathsf{corr}(s) = \mathcal{P} \mid Adv$,

there exists resolution R' and R'-state s' such that $\mathsf{corr}'(s') = \mathcal{Q} \mid Adv$ and

$$\mathrm{RProb}_{\mathsf{R}}(s, \mathsf{corr}^{-1}(\downarrow c)) = \mathrm{RProb}_{\mathsf{R}'}(s', \mathsf{corr}'^{-1}(\downarrow c))$$

However, the resulting pre-orders on processes are counter-intuitive: for instance, when we consider the processes $\mathcal{P} := \mathsf{out}(a, 0)$ and $\mathcal{Q} := \mathsf{out}(a, 0) +_{1/2} (\mathsf{out}(a, 0) +_{1/2} \mathsf{out}(a, 0))$, we can show that $(\mathcal{Q}, \mathcal{P}) \notin \leq'$, for both randomized or non-randomized schedulers. Indeed, when we take $Adv = 0$, and we see that there exists a resolution R such that $\mathrm{RProb}_{\mathsf{R}}(\mathcal{Q}, \downarrow a) = \frac{1}{2}$, but for every resolution R', it holds that $\mathrm{RProb}_{\mathsf{R}'}(\mathcal{P}, \downarrow a) = 1$.

4 Trace equivalence

As usual in pi calculi, and in the applied π-calculus in particular we define a *labelled* semantics. The intent of the labels is to capture adversarial actions and avoid the universal quantification over processes in equivalence definitions.

4.1 Labelled semantics

A state in this labeled semantics is defined by associating a multiset of processes with a *frame*, modeling the *knowledge* accumulated by the adversary. We also consider a new set of variables $\mathcal{AX} = \{\mathsf{ax}_1, \mathsf{ax}_2, \ldots\}$ distinct from $\mathcal{X}$ that will act as pointers to output messages.

Definition 9. An extended process is an ordered pair $(\mathcal{P}, \phi)$, where $\mathcal{P} \in \mathcal{MP}$ and ϕ is a ground substitution $\{\mathsf{ax}_1 \mapsto t_1; \ldots; \mathsf{ax}_n \mapsto t_n\}$ such that $\mathsf{ax}_i \in \mathcal{AX}$, $t_i \in \mathcal{T}(\mathcal{F}, \mathcal{N})$ and $Msg(t_i)$ for $1 \leq i \leq n$.

We denote by $\mathcal{SP}_\ell$ the set of all extended processes (and use $\mathcal{SP}_\ell^{<\infty}$, $\mathcal{SP}_\ell^{\mathsf{np}}$ and $\mathcal{SP}_\ell^{<\infty,\mathsf{np}}$ for subclasses as before).

A *recipe* is a term from $\mathcal{T}(\mathcal{F}, \mathcal{N}_{pub} \cup \mathcal{AX}\}$ representing how an attacker can deduce a message.

Notation 7. If D is a distribution over $\mathcal{MP}$, and ϕ a frame, we write (D, ϕ) for the distribution over extended processes defined as $(D, \phi) = \sum_{\mathcal{P} \in \mathrm{supp}(D)} D(\mathcal{P}) \cdot \delta_{(\mathcal{P},\phi)}$.

We now define the NPLTS N^ℓ for the labelled semantics. The only internal action is $\{\tau\}$, and we add *external actions*, that model the interactions with an external environment.

Definition 10. The *labelled semantics* is the NPLTS $\mathsf{N}^\ell = (\mathcal{SP}_\ell, \mathcal{A}^\ell_{ext} \sqcup \{\tau\}, \mathsf{trans}^\ell)$ where

- $\mathcal{A}^\ell_{ext} = \{in(\xi, \zeta), out(\xi, \mathsf{ax}), (\xi \stackrel{?}{=} \zeta), (\xi \stackrel{?}{\neq} \zeta) \mid \xi, \zeta \text{ recipes}, \ \mathsf{ax} \in \mathcal{AX}\}$
- $\mathsf{trans}^\ell((\mathcal{P}, \phi))(a) = \{D \mid (\mathcal{P}, \phi) \to_a D\}$ where $\to_a$ is defined by the following rules:
  - $(\mathcal{P}, \phi) \to_\tau (D, \phi)$ if $\mathcal{P} \to_\tau D$
  - $(\{\!\{\mathsf{in}(u, x); P\}\!\} \cup \mathcal{P}, \phi) \to_{in(\xi,\zeta)} \delta_{(\{\!\{P\{^{\zeta\phi}/_x\}\}\!\} \cup \mathcal{P}, \phi)}$ if $u \doteq \xi\phi$, $Msg(\zeta\phi)$ and $vars(\xi, \zeta) \subseteq dom(\phi)$
  - $(\{\!\{\mathsf{out}(u, t); P\}\!\} \cup \mathcal{P}, \phi) \to_{out(\xi,\mathsf{ax}_{n+1})} \delta_{(\{\!\{P\}\!\} \cup \mathcal{P}, \phi\{ax_{n+1} \mapsto t\})}$ if $u \doteq \xi\phi$, $Msg(t)$, $vars(\xi) \subseteq dom(\phi)$ and $|\phi| = n$
  - $(\mathcal{P}, \phi) \to_{(\xi \sim \zeta)} \delta_{(\mathcal{P},\phi)}$ if $vars(\xi, \zeta) \subseteq dom(\phi)$ and $\xi\phi \sim \zeta\phi$ where $\sim \in \{\doteq, \not\doteq\}$

Note that when we lift $\to_\tau$ to extended processes we suppose that the freshness requirement of a new name a' in the (New) rule of fig. 2 also applies to the frame ϕ, i.e., a' must not appear in ϕ. As for the operational semantics, we consider randomized and non-randomized resolutions for N^ℓ and denote the corresponding sets of resolutions by $\mathcal{R}^\ell_{\mathsf{r}}$, respectively $\mathcal{R}^\ell_{\mathsf{nr}}$.

Remark 4. It should be noted that we deal with static equivalence in a different way as done usually in the applied pi-calculus, or implicitly in the probabilistic applied pi-calculus in [GLPT07]: indeed, static equivalence is encoded into the NPLTS N^ℓ by a countable set of actions–all the tests $(\xi \stackrel{?}{=} \zeta)$ and their negations– instead of just one action testing static

equivalence. The motivation behind this choice is to be able to represent every *action* from the NPLTS by an *elementary push-button action* of the adversary. As shown later, this choice has no effect whatsoever on the definition of the simulation pre-orders (or on bisimulation)–see Remark 8 for more details, but it leads to a different notion of trace equivalence, that is closer to may testing equivalence–see Remark 5.

4.2 Trace Preorder

We first define the probability of executing a trace in a resolution. As we are interested in a *weak* trace preorder, traces are sequences of external actions only. In our definition we will use the previously introduced notation $\mathrm{RProb}_{\mathsf{R}}(s, \{t\})$: recall that this denotes the probability of reaching state t from state s under resolution R using only internal actions.

Definition 11. Let $\mathsf{N} = (\mathcal{S}_{\mathsf{N}}, \mathcal{A}_{int} \sqcup \mathcal{A}_{ext}, \mathsf{trans}_{\mathsf{N}})$ be a NPLTS. Let $\mathsf{R} = (\mathcal{S}_{\mathsf{R}}, \mathsf{corr}_{\mathsf{R}}, \mathsf{trans}_{\mathsf{R}})$ be a resolution for N^{ℓ}. Let $w \in {\mathcal{A}_{ext}}^*$ be a trace, i.e., a finite word on the alphabet $\mathcal{A}_{ext}$. For all states $s \in \mathcal{S}_{\mathsf{R}}$, we define the *probability of executing w starting from s in* R as:

$$\mathrm{Prob}_{\mathsf{R}}(s, \epsilon) = 1$$
$$\mathrm{Prob}_{\mathsf{R}}(s, a.w) = \sum_{\substack{t \in \mathcal{S}_{\mathsf{R}} \\ \text{s.t. } \exists D \in \mathcal{D}(\mathcal{S}_{\mathsf{R}}), \mathsf{trans}_{\mathsf{R}}(t)(a) = D}} \mathrm{RProb}_{\mathsf{R}}(s, \{t\}) \cdot \sum_{s' \in \mathrm{supp}(D)} D(s') \cdot \mathrm{Prob}_{\mathsf{R}}(s', w)$$

Given a set of resolutions $\mathcal{R} \subseteq \mathcal{R}_{\mathsf{r}}(\mathsf{N})$, a state $u \in \mathcal{S}_{\mathsf{N}}$, we denote by $\mathrm{Prob}_{\mathcal{R}}(s, w)$ the maximal probability of executing w from s in $\mathcal{R}$:

$$\mathrm{Prob}_{\mathcal{R}}(u, w) = \sup_{\substack{\mathsf{R} = (\mathcal{S}_{\mathsf{R}}, \mathsf{corr}_{\mathsf{R}}, \mathsf{trans}_{\mathsf{R}}) \in \mathcal{R} \\ s \in \mathcal{S}_{\mathsf{R}} \text{ s.t. } \mathsf{corr}(s) = u}} \mathrm{Prob}_{\mathsf{R}}(s, w)$$

In this work, we are interested mostly by the may paradigm for non-determinism. Observe that nonetheless, we could define must-trace equivalence where we would compute the infimum of probabilities rather than supremum of probabilities in Definition 11.

Definition 12. Let $\mathcal{R} \subseteq \mathcal{R}_{\mathsf{r}}^{\ell}$ be a set of resolutions for N^{ℓ} and $(\mathcal{P}, \phi)$, $(\mathcal{P}', \phi') \in \mathcal{SP}_{\ell}$.

$$(\mathcal{P}, \phi) \leq_{tr}^{\mathcal{R}} (\mathcal{P}', \phi') \quad \text{iff} \quad \forall w \in {\mathcal{A}_{ext}^{\ell}}^*. \ \mathrm{Prob}_{\mathcal{R}}((\mathcal{P}, \phi), w) \leq \mathrm{Prob}_{\mathcal{R}}((\mathcal{P}', \phi'), w)$$

$(\mathcal{P}, \phi)$ and $(\mathcal{P}', \phi')$ are trace equivalent for $\mathcal{R}$ if $(\mathcal{P}, \phi) \leq_{tr}^{\mathcal{R}} (\mathcal{P}', \phi')$ and $(\mathcal{P}', \phi') \leq_{tr}^{\mathcal{R}} (\mathcal{P}, \phi)$.

4.3 On randomized or non-randomized resolutions

Observe that Definition 12 depends on the class of admissible resolutions under consideration, i.e., whether we restrict ourselves to non-randomized resolutions, or we consider all randomized resolutions. In the following, we show–as we formally state in proposition 2–that these two notions of trace equivalence actually coincide. This result is not surprising: indeed it has for instance been shown in [Cas18] (in the restricted setting of strong

trace equivalence and NPLTS with an *image-finiteness* condition) that trace preorder–called there *supremal probability trace pre-order*–does not depend on whether we consider all randomized resolutions, or only non-randomized ones. Here, we show the same result for the notion of weak trace pre-order we gave in Definition 12.

Proposition 2. Let $(\mathcal{P}, \phi)$ and $(\mathcal{P}', \phi')$ be two extended processes.

$$(\mathcal{P}, \phi) \leq_{tr}^{\mathcal{R}_{\mathsf{r}}^{\ell}} (\mathcal{P}', \phi') \quad \text{iff} \quad (\mathcal{P}, \phi) \leq_{tr}^{\mathcal{R}_{\mathsf{nr}}^{\ell}} (\mathcal{P}', \phi')$$

The proof of this result is given in Appendix B.1. In the rest of this paper, as $\leq_{tr}^{\mathcal{R}_{\mathsf{nr}}^{\ell}} = \leq_{tr}^{\mathcal{R}_{\mathsf{r}}^{\ell}}$, we simply denote trace inclusion by $\leq_{tr}$.

Trace preorders is (strictly) weaker than the may testing preorder: it is the sense of Proposition 3 below.

Proposition 3. Let $\mathcal{P}, \mathcal{Q} \in \mathcal{MP}$ be two processes.

$$\mathcal{P} \leq_{may} \mathcal{Q} \quad \Rightarrow \quad (\mathcal{P}, \varnothing) \leq_{tr} (\mathcal{Q}, \varnothing)$$

Moreover, there exist processes $\mathcal{P}, \mathcal{Q} \in \mathcal{MP}$ such that

$$(\mathcal{P}, \varnothing) \leq_{tr} (\mathcal{Q}, \varnothing) \text{ and } \mathcal{P} \not\leq_{may} \mathcal{Q}$$

Proof sketch. We show both points separately.

- Our goal is to show that every trace w can be emulated by an adversary Adv. Observe that any trace w can be seen as a (linear) formula in $\mathcal{F}$, where $\mathcal{F}$ is the Henessy-Milner logic from Definition 25. It means that for every $ok \in \mathcal{N}_{pub}$ such that $ok \notin fn(w)$ and $n \in \mathbb{N}$, we can consider the adversary $Adv_{w,n}^{ok}$ from Definition 27. Recall that we cannot apply directly Lemma 12, because here there can be probabilistic choices inside $\mathcal{P}$. Nonetheless, as long as the formulas considered are *traces*, we are going to show a generalization of Lemma 12 to probabilistic processes. More precisely, we are going to show: for all trace w, for all $\mathcal{P} \in \mathcal{MP}$, $\phi \in \mathcal{F}$ with $ok \notin fn(\mathcal{P}, \phi, w)$:

$$\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell})}((\mathcal{P}, \phi), w) = \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{o})}(\mathcal{P} \cup \{\!\{Adv_{w,|\phi|}^{ok}\phi\}\!\}, \downarrow ok). \tag{1}$$

  We write $\mathcal{I}$ for the set

$$\mathcal{I} := \{(\mathcal{P} \cup \{\!\{Adv_{w,|\phi|}^{ok}\phi)\}\!\} \mid (\mathcal{P}, \phi) \in \mathcal{SP}_{\ell}, w \in \mathcal{A}_{ext}^{\star}, ok \notin fn(\mathcal{P}, \phi, w)\}$$

  Observe that we can write the restriction of N^{o} to $\mathcal{I}$ using the NPLTS $\mathsf{N}^{\ell tr}$ defined in Definition 44, in the sense where: $\forall s = \mathcal{P} \cup \{\!\{Adv_{w,|\phi|}^{ok}\phi\}\!\} \in \mathcal{I}$: $s \xrightarrow{\tau}_{\mathsf{N}^{o}} D$, if and only if there exists E such that $((\mathcal{P}, \phi), w) \xrightarrow{\tau}_{\mathsf{N}^{\ell tr}} E$, and $D = \overline{f}(E)$ where $f : ((\mathcal{P}', \phi'), w') \in \mathcal{S}_{\mathsf{N}^{\ell tr}} \mapsto \mathcal{P}' \cup \{\!\{Adv_{w',|\phi'|}^{ok}\phi'\}\!\}) \in \mathcal{I}$–see Notation 5 for the meaning of $\overline{f}$. Moreover, a

$$\begin{array}{rcl} \mathcal{P} & = & \{\!\{\mathsf{new}\ k;\ (P(0) \mid P(0) \mid P(1) \mid P_{dec})\}\!\} \\ \mathcal{Q} & = & \{\!\{\mathsf{new}\ k;\ (P(0) \mid P(1) \mid P(1) \mid P_{dec})\}\!\} \end{array} \quad \text{and} \quad \begin{array}{rcl} P(x) & = & \mathsf{new}\ r; \mathsf{out}(c, enc(x, r, k)) \\ P_{dec} & = & \mathsf{in}(d, x); \mathsf{out}(d, dec(x, k)) \end{array}$$

Figure 7: Processes $\mathcal{P}, \mathcal{Q}$ such that $(\mathcal{P}, \varnothing) \leq_{tr} (\mathcal{Q}, \varnothing)$ and $\mathcal{P} \not\leq_{may} \mathcal{Q}$

state $\mathcal{P} \cup \{\!\{Adv^{ok}_{w,|\phi|}\phi\}\!\} \in \mathcal{I}$ is in $\downarrow ok$ if and only if $w = \epsilon$. From this observation, we can deduce:

$$\begin{aligned} &\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P} \cup \{\!\{Adv^{ok}_{w,|\phi|}\phi\}\!\}, \downarrow ok) \\ &= \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell^{tr}})}((\mathcal{P}, \phi), w), \{(s, \epsilon) \mid s \in \mathcal{SP}_\ell\}) \\ &= \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell^{tr}})}((\mathcal{P}, \phi), w), \{success\}) \text{ since } \forall s \in \mathcal{SP}_\ell, (s, \epsilon) \xrightarrow{\tau}_{\mathsf{N}^{\ell^{tr}}} \delta_{success}. \end{aligned}$$

Since we know from Lemma 33 that

$$\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell^{tr}})}((\mathcal{P}, \phi), w), \{success\}) = \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell})}((\mathcal{P}, \phi), w)$$

we conclude that (1) holds. From there, we obtain the result directly by looking at the definition of the may-testing preorder and the trace preorder.

- The fact that may testing is *strictly* stronger is for instance witnessed by processes $\mathcal{P}, \mathcal{Q}$ in Figure 7.

□

Remark 5. Observe that–contrary to usual results in the literature, see for instance [CCD13]–Proposition 3 holds even for processes non image-finite. This discrepancy comes from our choice of labelled actions for static equivalence (see Remark 4): a trace cannot test *directly* static equivalence, but can only do a *finite* numbers of recipe tests.

5 Simulation and observational preorders

In this section, we define the *simulation* and *observational preorders* on probabilistic pi-calculus processes and corresponding equivalences. Our definition of simulation preorder is taken from the definition of *randomized weak simulation preorder* introduced by Segala and Lynch for probabilistic automata [SL95]. Both simulation and observational preorders relie on a weak relation for internal actions which we define as follows, one for randomized and one for non-randomized resolutions.

Definition 13. Let $\mathsf{N} = (\mathcal{S}_\mathsf{N}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_\mathsf{N})$ be a NPLTS, and $D, E \in \mathcal{D}^{\leq 1}(\mathcal{S}_\mathsf{N})$.

- We write $D \overset{\tau}{\Longrightarrow}_{\mathcal{R}_\mathsf{r}(\mathsf{N})} E$ when there exists $R = (\mathcal{S}_R, \mathsf{corr}_R, \mathsf{trans}_R) \in \mathcal{R}_\mathsf{r}(\mathsf{N})$, and $D', E' \in \mathcal{D}^{\leq 1}(\mathcal{S}_R)$ such that $\mathsf{corr}_R(D') = D$, $\mathsf{corr}_R(E') = E$, $\mathrm{supp}(E') \subseteq \mathcal{S}_{ext}(R)$ and for all $u \in \mathcal{S}_{ext}(R)$, $E'(u) = \sum_{s' \in \mathcal{S}_R} D'(s') \cdot \mathrm{RProb}_R(s', \{u\})$.

- We write $D \overset{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N})} E$ when there exists $R = (\mathcal{S}_R, \mathsf{corr}_R, \mathsf{trans}_R) \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N})$, and $D', E' \in \mathcal{D}^{\leq 1}(\mathcal{S}_R)$ such that corr_R is injective on the support of D', $\mathsf{corr}_R(D') = D$, $\mathsf{corr}(E') = E$, $\mathrm{supp}(E') \subseteq \mathcal{S}_{ext}(R)$ and for all $u \in \mathcal{S}_{ext}(R)$, $E'(u) = \sum_{s' \in \mathcal{S}_R} D'(s') \cdot \mathrm{RProb}_R(s', \{u\})$.

Moreover, for all $s \in \mathcal{S}_{\mathsf{N}}$, $D \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{N}})$, and $\mathcal{R} \in \{\mathcal{R}_{\mathsf{r}}(\mathsf{N}), \mathcal{R}_{\mathsf{nr}}(\mathsf{N})\}$, we write $s \overset{\tau}{\Longrightarrow}_{\mathcal{R}} D$ when $\delta_s \overset{\tau}{\Longrightarrow}_{\mathcal{R}} D$.

Observe that in the NPLTS N^{ℓ}, even though $s \overset{\tau}{\to} D$ implies that D has finite support, it is possible to have $s \overset{\tau}{\Longrightarrow}_{\mathcal{R}} E$, where the sub-distribution E has infinite support.

As we will see below, the non-randomized weak relation $\overset{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N})}$ does not allow to define a robust simulation preorder. However, before defining the simulation preorder, we give a more direct caracterisation of the weak relation $\overset{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{r}}(\mathsf{N})}$, without using the notion of resolutions. This caracterisation is more widely used in the literature on probabilistic bisimulation–see e.g. [DVGHM09]–and eases proofs. First, we lift a relation $\to \subseteq \mathcal{S} \times \mathcal{D}(\mathcal{S})$ to a relation in $\mathcal{D}(\mathcal{S}) \times \mathcal{D}(\mathcal{S})$.

Definition 14. Let $\mathcal{S}$ be a discrete set and $\to \subseteq \mathcal{S} \times \mathcal{D}(\mathcal{S})$ be a probabilistic reduction relation. We define its lifting $\to_{\mathsf{r}} \subseteq \mathcal{D}^{\leq 1}(\mathcal{S}) \times \mathcal{D}^{\leq 1}(\mathcal{S})$ as

$$D \to_{\mathsf{r}} \sum_{i \in I} \alpha_i \cdot E_i$$

when I is any countable set, $D = \sum_{i \in I} \alpha_i \cdot \delta_{x_i}$, and $x_i \to E_i$ for all $i \in I$ (observe that it can be that $x_i = x_j$ even when $i \neq j$).

Observe that we can apply Definition 14 above to any NPLTS by considering its probabilistic reduction relation $\overset{\tau}{\to}$. We will do this implicitely in the following.

We are now ready to give an alternative characterisation for the weak reduction relation $\Longrightarrow_{\mathcal{R}_{\mathsf{r}}}$, more in line with the tradition in the field of probabilistic simulation. There are a number of equivalent definitions in the literature: we chose here the one given in [DVGHM09].

Definition 15. Let $\to$ be a binary relation in $\mathcal{S} \times \mathcal{D}(\mathcal{S})$ for a discrete set $\mathcal{S}$. We define the relation $\Longrightarrow_{\mathsf{r}} \subseteq \mathcal{D}^{\leq 1}(\mathcal{S}) \times \mathcal{D}^{\leq 1}(\mathcal{S})$ as

$$D \Longrightarrow_{\mathsf{r}} D' \text{ if there is an infinite scheme: } \begin{array}{lcl} D & = & D_0^{\to} + D_0^{\top} \\ D_0^{\to} & \to_{\mathsf{r}} & D_1^{\to} + D_1^{\top} \\ & & \vdots \\ D_k^{\to} & \to_{\mathsf{r}} & D_{k+1}^{\to} + D_{k+1}^{\top} \\ & & \vdots \end{array}$$

where $D_k^{\to}, D_k^{\top}$ are sub-distributions over $\mathcal{S}$ and $D' = \sum_{k \in \mathbb{N}} D_k^{\top}$.

When starting from the transition relation $\overset{\tau}{\to}$ for a NPLTS N, we denote the resulting relations by $\overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}}$. When N is clear from the context, we may directly write $\overset{\tau}{\Longrightarrow}_{\mathsf{r}}$.

Remark 6. Whenever we have a *finite* scheme in a similar shape as the *infinite* scheme asked for in Definition 15, observe that we can always complete it into an infinite scheme, using the fact that $\varnothing \to \varnothing + \varnothing$–where $\varnothing$ stands for the sub-distribution with empty support, i.e. $\varnothing(x) = 0$ for every $x \in \mathcal{S}$. In particular, if we start from a state $(\mathcal{P}, \phi)$ in N^ℓ where $\mathcal{P}$ is a process *without replication*, then *every* infinite scheme $\delta_{(\mathcal{P},\phi)} \overset{\tau}{\Longrightarrow}_{\mathsf{r}} D$ is actually a finite scheme. A simple corollary to this remark is that $\overset{\tau}{\Longrightarrow}_{\mathsf{r}}$ is reflexive (by taking $D_0^\top = D$ and all other distributions being $\varnothing$).

We now show in the following statement that the two characterizations, i.e. $\overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}}$ and $\Longrightarrow_{\mathcal{R}_\mathsf{r}}$, are equal (proof in Appendix C).

Lemma 1. Let $\mathsf{N} = (\mathcal{S}_\mathsf{N}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_\mathsf{N})$ be a NPLTS and $D, E \in \mathcal{D}^{\leq 1}(\mathcal{S}_\mathsf{N})$.

$$D \overset{\tau}{\Longrightarrow}_{\mathsf{r}} E \text{ if and only if } D \Longrightarrow_{\mathcal{R}_\mathsf{r}} E$$

Remark 7. The weak reduction relation $\overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}^\ell}$ (and so equivalently $\overset{\tau}{\Longrightarrow}_{\mathcal{R}_\mathsf{r}(\mathsf{N}^\ell)}$) allows to *lose some probabilities* in the presence of a replication in our extended processes. Consider the extended process $A = (\{!P\} \cup \mathcal{P}, \phi)$. We have that $\delta_A \overset{\tau}{\Longrightarrow}_{\mathsf{r}} D$ where $\mathrm{supp}(D) = \{A\}$, $D(A) = p$ and p can be any value smaller than 1. To show this, we can build the following infinite scheme:

$$\delta_A = D_0 + D \qquad \text{and for all } k \in \mathbb{N}, D_k \overset{\tau}{\to} D_{k+1} + \varnothing$$

with for all $k \in \mathbb{N}$, $\mathrm{supp}(D_k) = \{A_k\}$, $A_k = (\{!P; \underbrace{P; \ldots; P}_{k \text{ times}}\} \cup \mathcal{P}, \phi)$ and $D_k(A_k) = 1 - p$.

On the other hand, as noted in Remark 6, when processes do not contain replication, $\delta_{(\mathcal{P},\phi)} \overset{\tau}{\Longrightarrow}_{\mathsf{r}} D$ actually corresponds to a finite scheme. Thus, we cannot lose probabilities, i.e. D is a distribution.

5.1 Simulation preorder

We are now going to define the notions of probabilistic simulation preorder, similarity and bisimilarity. However, in these definitions, we will only consider the relation $\overset{\tau}{\Longrightarrow}_{\mathsf{r}}$ (or equivalently $\Longrightarrow_{\mathcal{R}_\mathsf{r}}$) and not $\overset{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}}$. First, as highlighted for instance in [Eis17, Den05], when considering bisimilarity or similarity on NPLTSs in general, we are forced to consider randomized resolutions, otherwise the resulting relations are not *transitive*. Note that in [GLPT07], they do rely on non-randomized schedulers in their definition of bisimulation. It does not necessarily mean that their relation is not transitive as they focus directly on the semantics of processes. However, we will show in Section 5.3 that bisimulation and observational equivalence do *not* coincide when using the non-randomized relation $\overset{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}}$, hence disproving [GLPT07, Theorem 2]. This reenforces our belief that it is preferable to use randomized schedulers in our definition.

To define the simulation preorder, we need to introduce the lifting of a relation to sub-distributions as follows.

Definition 16 (Lifting of a relation)**.** Let R be a binary relation on a discrete set $\mathcal{S}$. We define the *lifting of R to sub-distributions* as the binary relation on $\mathcal{D}^{\leq 1}(\mathcal{S})$, denoted $\widehat{R}$, defined as:

$$D \ \widehat{R} \ E \text{ when } \forall \mathcal{S}' \subseteq \mathcal{S}, D(\mathcal{S}') \leq E(R(\mathcal{S}'))$$

where $R(\mathcal{S}') = \{s \in \mathcal{S} \mid s' \in \mathcal{S}' \wedge s' \ R \ s\}$.

We note that this lifting has the following properties:

- if R is reflexive, then $\widehat{R}$ is reflexive as well;
- if R is symmetric then for any $D_1, D_2 \in \mathcal{D}(\mathcal{S})$, i.e., D_1, D_2 are distributions rather than sub-distributions, if $D_1 \ \widehat{R} \ D_2$ then $D_2 \ \widehat{R} \ D_1$.

The second property is actually not obvious on the current definition. It is however a direct consequence of an alternative, *coupling-based* characterization of lifting, that can be found under the name of *Strassen's theorem* for instance in [ABB+18] (it is stated there for proper distributions, instead of sub-distributions, but the generalisation to sub-distributions can be easily done by lifting all sub-distributions D over X to proper distributions $D_\perp$ over $X \cup \{\perp\}$ where $\perp$ is an arbitrary new element added to represent divergence).

Notation 8. Let $\mathsf{N} = (\mathcal{S}_\mathsf{N}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_\mathsf{N})$ be a NPLTS. Let $a \in \mathcal{A}_{ext}$ and $D, D' \in \mathcal{D}^{\leq 1}(\mathcal{S}_\mathsf{N})$. We write $D \overset{a}{\Longrightarrow}_\mathsf{r} D'$ when $D \overset{\tau}{\Longrightarrow}_\mathsf{r} E_1$, $E_1 \overset{a}{\rightarrow} E_2$ and $E_2 \overset{\tau}{\Longrightarrow}_\mathsf{r} D'$ for some E_1, E_2.

Similarly, for $a_1, \ldots, a_n \in \mathcal{A}_{ext}$ then we write $D \overset{a_1 \ldots a_n}{\Longrightarrow}_\mathsf{r} D'$ when $D \overset{a_1}{\Longrightarrow}_\mathsf{r} E_1 \overset{a_2}{\Longrightarrow}_\mathsf{r} \ldots \overset{a_{n-1}}{\Longrightarrow}_\mathsf{r} E_{n-1} \overset{a_n}{\Longrightarrow}_\mathsf{r} D'$.

Definition 17. Let $\mathsf{N} = (\mathcal{S}_\mathsf{N}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_\mathsf{N})$ be a NPLTS. A relation $R \subseteq (\mathcal{S}_\mathsf{N} \times \mathcal{S}_\mathsf{N})$ is

- a *simulation* if $s_1 \ R \ s_2$ implies that for all $a \in \mathcal{A}_{ext} \cup \{\tau\}$, $D_1 \in \mathcal{D}(\mathcal{S}_\mathsf{N})$

$$\text{if} \quad s_1 \overset{a}{\rightarrow} D_1 \quad \text{then} \quad s_2 \overset{a}{\Longrightarrow}_\mathsf{r} D_2, \ D_2 \in \mathcal{D}(\mathcal{S}_\mathsf{N}) \text{ and } D_1 \ \widehat{R} \ D_2$$

- a *bisimulation* if R is a simulation and R is symmetric.

The *simulation preorder*, denoted $\leq^\mathsf{N}_{sim}$, is the largest simulation and *bisimilarity*, denoted $\approx^\mathsf{N}_{bi}$, is the largest bisimulation. We define *similarity*, denoted $\approx^\mathsf{N}_{sim}$, as $\leq^\mathsf{N}_{sim} \cap {\leq^\mathsf{N}_{sim}}^{-1}$.

As usual in the field of (bi)simulation, it can be shown that $\leq^\mathsf{N}_{sim}$, respectively $\approx^\mathsf{N}_{bi}$, exists [Eis17] and that it is a pre-order, i.e. a reflexive and transitive relation, respectively an equivalence, i.e., a reflexive, symmetric and transitive relation [Sto02].

The following proposition from [Sto02] states that, as usual in the non-probabilistic case, the weak arrow $\overset{a}{\Rightarrow}$ can replace the single arrow $\overset{a}{\rightarrow}$ in the definition of weak simulation. It is important to observe that this is not the case when we choose *non-randomized* schedulers (see Section 5.3).

Proposition 4. Let $\mathsf{N} = (\mathcal{S}_\mathsf{N}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_\mathsf{N})$ be a NPLTS, and R be the largest binary relation on $\mathcal{S}_\mathsf{N}$ such that $s_1 \; R \; s_2$ implies that for every $a \in \mathcal{A}_{ext} \cup \{\tau\}$, if $s_1 \overset{a}{\Longrightarrow}_\mathsf{r} D_1$ then $s_2 \overset{a}{\Longrightarrow}_\mathsf{r} D_2$ and $D_1 \; \widehat{R} \; D_2$. We have $R = \leq^{\mathsf{N}}_{sim}$.

Remark 8. Please observe that our choice of labelled actions for static equivalence (see Remark 4) has no impact on the resulting simulation and bisimulation. Indeed, if two N^ℓ-states $(\mathcal{P}, \phi)$ and $(\mathcal{Q}, \psi)$ are in the simulation pre-order or bisimulation, then ϕ is statically equivalent to ψ. Indeed, for all $a \in \{\xi \overset{?}{=} \zeta, \xi \overset{?}{\neq} \zeta, \mathsf{ax} \in, \mathsf{ax} \notin\}$, $\delta_{(\mathcal{P},\phi)} \xrightarrow{a} \delta_{(\mathcal{P},\phi)}$ implies that $\delta_{(\mathcal{Q},\psi)} \overset{a}{\Longrightarrow}_\mathsf{r} D$ and $\delta_{(\mathcal{P},\phi)} \; \widehat{\leq^{\mathsf{N}^\ell}_{sim}} \; D$. Since neither the a transition or τ transition modifies the frame, the former indicates that $\delta_{(\mathcal{Q},\psi)} \overset{\tau}{\Longrightarrow}_\mathsf{r} E_1$, $E_1 \xrightarrow{a} E_2$ and $E_2 \overset{\tau}{\Longrightarrow}_\mathsf{r} D$, with for all $(\mathcal{Q}', \psi') \in \mathrm{supp}(E_1)$, $\psi = \psi'$. The former ensures that $\mathrm{supp}(E_1) \neq \varnothing$. Therefore, for all ax, ξ, ζ, if $\xi \overset{?}{=} \zeta$, $\xi \overset{?}{\neq} \zeta$, $\mathsf{ax} \in$ or $\mathsf{ax} \notin$ holds on ϕ then it also holds on ψ respectively. It implies that ϕ and ψ are statically equivalent.

5.2 Observational preorder

Definition 18. The *observational preorder* $\leq^{\mathcal{R}}_{obs}$ is the largest relation R on $\mathcal{MP}$ such that $\mathcal{P} \; R \; \mathcal{Q}$ implies :

- for all $c \in \mathcal{N}_{pub}$, $\mathrm{RProb}_{\mathcal{R}}(\mathcal{P}, \downarrow c) \leq \mathrm{RProb}_{\mathcal{R}}(\mathcal{Q}, \downarrow c)$;
- if $\mathcal{P} \overset{\tau}{\Longrightarrow}_\mathsf{r} D$ then $\mathcal{Q} \overset{\tau}{\Longrightarrow}_\mathsf{r} E$ and $D \; \widehat{R} \; E$;
- for all closed $Adv \in \mathcal{MP}$ such that $fn(Adv) \subseteq \mathcal{N}_{pub}$, $\{Adv\} \cup \mathcal{P} \; R \; \{Adv\} \cup \mathcal{Q}$.

The *observational equivalence* $\approx^{\mathcal{R}}_{obs}$ is defined by additionally requesting R to be symmetric and in the second bullet point, by requesting both $D \; \widehat{R} \; E$ and $E \; \widehat{R} \; D$ to hold.

Remark 9. Note that we slightly diverge from the original definition of observational equivalence [ABF17] where an evaluation context $C[_]$ is of the form

$$\mathsf{new}\ n_1; \ldots; \mathsf{new}\ n_k; (_ \mid A)$$

In our definition we simply consider a parallel process, and no additional name restriction. However, we prove in Appendix D that these two definitions coincide. Intuitively, restricting names whose scope includes the adversarial process A corresponds to making previously public channels invisible to the attacker at later steps, hence it does not provide additional distinguishing power.

In the following, we show the asymetric counterpart to the result stated in [GLPT07] on the coincidence between bisimulation and observational equivalence. The proof can be found in Appendix F.

Proposition 5. Let $\mathcal{P}, \mathcal{Q}$ two processes in $\mathcal{MP}$.

$$\mathcal{P} \leq^{\mathcal{R}_\mathsf{r}}_{obs} \mathcal{Q} \quad \text{iff} \quad (\mathcal{P}, \varnothing) \leq^{\mathsf{N}^\ell}_{sim} (\mathcal{Q}, \varnothing) \qquad \text{and} \qquad \mathcal{P} \approx^{\mathcal{R}_\mathsf{r}}_{obs} \mathcal{Q} \quad \text{iff} \quad (\mathcal{P}, \varnothing) \approx^{\mathsf{N}^\ell}_{bi} (\mathcal{Q}, \varnothing)$$

5.3 Bisimilarity and observational equivalence do not coincide with non-randomized schedulers

Here, we give more details on the different behaviours of (bi)simulation and observational preorder and equivalence, depending on whether we consider randomized or non-randomized schedulers. In [GLPT07] for instance, *non-randomized* schedulers are considered in the definition of bisimulation and observational equivalence on the probabilistic applied π-calculus.

As said earlier, for general NPLTSs, simulation is not transitive when considering non randomized schedulers [Eis17]. We show here that even on our specific NPLTS N^ℓ, simulation is not transitive (Lemma 2. Furthermore, for non-randomized schedulers, bisimulation (resp. simulation) and observational equivalence (resp. preorder) do not coincide (Lemma 3). However, they do coincide for randomized schedulers (Proposition 5). This discrepancy would also arise when comparing observational preorder with a similar definition where we would only require that $\mathcal{P} \xrightarrow{\tau} D$ (rather $\mathcal{P} \overset{\tau}{\Longrightarrow}_{\mathsf{r}} D$) implies $\mathcal{Q} \overset{\tau}{\Longrightarrow}_{\mathsf{r}} E$ and $D \ \widehat{R} \ E$. This *one-step* observational preorder is equivalent to observational preorder for randomized scheduler but not for non-randomized scheduler.

We are going to compare processes with respect to the bisimilarity $\approx_{bi}^{\mathsf{N}^\ell}$ as well as the observational equivalence with *non-randomized schedulers*. The definition of these variants with non-randomized resolutions follows Definition 18 but we use $\overset{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}$ instead of $\overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}^o}$. We denote this non randomized bisimularity as $\approx_{bi}^{\mathsf{nr}}$ (and similar for $\leq_{sim}^{\mathsf{nr}}$, $\approx_{obs}^{\mathsf{nr}}$ and $\leq_{obs}^{\mathsf{nr}}$).

Lemma 2. $\leq_{sim}^{\mathsf{nr}}$ is not transitive.

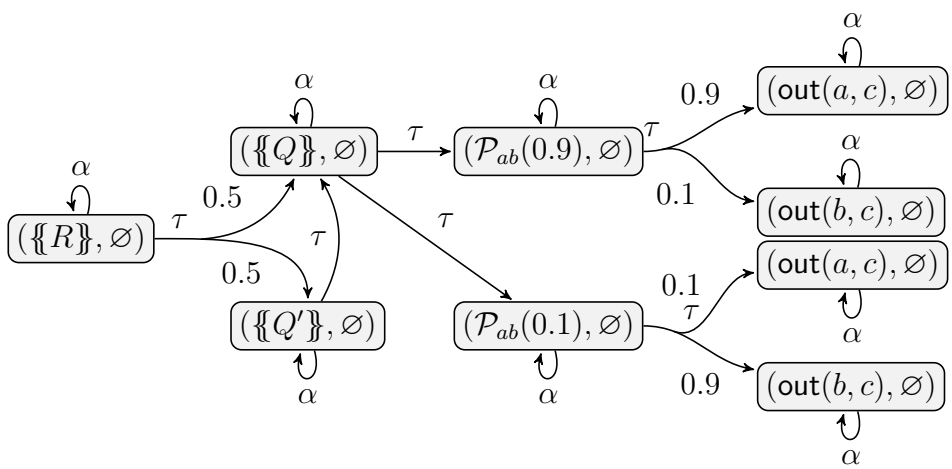
Proof. Consider processes P, Q and R defined in Figure 8. The corresponding fragment of N^ℓ is displayed in Figure 8a. We will show that

$$(\{\!\{P\}\!\}, \varnothing) \leq_{sim}^{\mathsf{nr}} (\{\!\{R\}\!\}, \varnothing) \text{ and } (\{\!\{R\}\!\}, \varnothing) \leq_{sim}^{\mathsf{nr}} (\{\!\{Q\}\!\}, \varnothing) \text{ but } (\{\!\{P\}\!\}, \varnothing) \not\leq_{sim}^{\mathsf{nr}} (\{\!\{R\}\!\}, \varnothing)$$

We first show that $(\{\!\{P\}\!\}, \varnothing) \leq_{sim}^{\mathsf{nr}} (\{\!\{R\}\!\}, \varnothing)$. Notice that any α transition can easily be matched, i.e. $(\{\!\{P\}\!\}, \varnothing) \xrightarrow{\alpha} (\{\!\{P\}\!\}, \varnothing)$ and $(\{\!\{R\}\!\}, \varnothing) \xrightarrow{\alpha} (\{\!\{R\}\!\}, \varnothing)$. Furthermore, we have $(\{\!\{P\}\!\}, \varnothing) \xrightarrow{\tau} 0.5 \cdot \delta_{(\{\!\{\mathsf{out}(a,c)\}\!\}, \varnothing)} + 0.5 \cdot \delta_{(\{\!\{\mathsf{out}(b,c)\}\!\}, \varnothing)}$ which can be matched in $(\{\!\{R\}\!\}, \varnothing)$ by using the scheduler displayed in Figure 8b, i.e. $(\{\!\{R\}\!\}, \varnothing) \overset{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}} 0.5 \cdot \delta_{(\{\!\{\mathsf{out}(a,c)\}\!\}, \varnothing)} + 0.5 \cdot \delta_{(\{\!\{\mathsf{out}(b,c)\}\!\}, \varnothing)}$. This concludes the proof of $(\{\!\{P\}\!\}, \varnothing) \leq_{sim}^{\mathsf{nr}} (\{\!\{R\}\!\}, \varnothing)$.

It is easy to see that $(\{\!\{Q\}\!\}, \varnothing) \approx_{bi}^{\mathsf{nr}} (\{\!\{Q'\}\!\}, \varnothing)$ and so $(\{\!\{R\}\!\}, \varnothing) \leq_{sim}^{\mathsf{nr}} (\{\!\{Q\}\!\}, \varnothing)$.

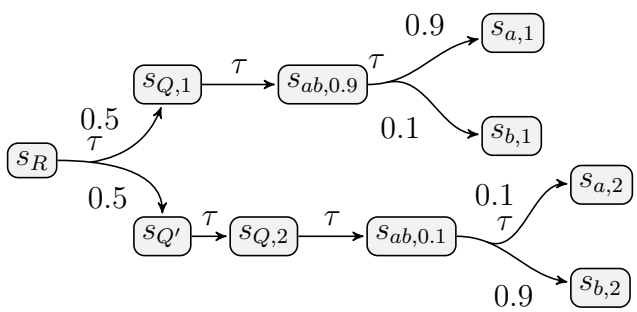
Finally, we need to prove that the transition $(\{\!\{P\}\!\}, \varnothing) \xrightarrow{\tau} 0.5 \cdot \delta_{(\{\!\{\mathsf{out}(a,c)\}\!\}, \varnothing)} + 0.5 \cdot \delta_{(\{\!\{\mathsf{out}(b,c)\}\!\}, \varnothing)}$ cannot be simulated in $(\{\!\{Q\}\!\}, \varnothing)$. First one can see for all $d \in \{a, b\}$, for all $\mathcal{P} \in \{\{\!\{Q\}\!\}, \mathcal{P}_{ab}(0.9), \mathcal{P}_{ab}(0.1)\}$, $(\mathsf{out}(d,c), \varnothing) \not\leq_{sim}^{\mathsf{nr}} (\mathcal{P}, \varnothing)$. Indeed, $(\mathsf{out}(d,c), \varnothing) \xrightarrow{out(d,\mathsf{ax}_1)} \delta_{(\{\!\{0\}\!\}, \phi)}$ with $\phi = \{\mathsf{ax}_1 \mapsto c\}$ but we can have at best $(\mathcal{P}, \varnothing) \overset{out(d,\mathsf{ax}_1)}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}} 0.9 \cdot \delta_{(\{\!\{0\}\!\}, \phi)}$. Thus, the only relevant extended process from $\leq_{sim}^{\mathsf{nr}} ((\{\!\{\mathsf{out}(d,c)\}\!\}, \varnothing))$ reachable from $(\{\!\{Q\}\!\}, \varnothing)$ is $(\{\!\{\mathsf{out}(d,c)\}\!\}, \varnothing)$ itself. However, we can only have $(\{\!\{Q\}\!\}, \varnothing) \overset{out(d,\mathsf{ax}_1)}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}} 0.1 \cdot \delta_{(\{\!\{\mathsf{out}(a,c)\}\!\}, \varnothing)} +$



For the sake of readability, α stands for all labels $\mathsf{ax}_i \notin$, for $i \in \mathbb{N}$ and all labels $\xi \sim \xi'$ for all closed recipes ξ, ξ' such that $\xi \sim \xi'$ ($\sim \in \{\doteq, \not\doteq\}$). Furthermore, let

$$
\begin{aligned}
Q &= (\mathsf{out}(a,c) +_{0.9} \mathsf{out}(b,c)) + (\mathsf{out}(a,c) +_{0.1} \mathsf{out}(b,c)) & R &= Q +_{0.5} Q' \\
Q' &= \mathsf{if}\ c = c\ \mathsf{then}\ Q\ \mathsf{else}\ 0 & P &= \mathsf{out}(a,c) +_{0.5} \mathsf{out}(b,c) \\
\mathcal{P}_{ab}(p) &= \{\!\{\mathsf{out}(a,c) +_p \mathsf{out}(b,c)\}\!\}
\end{aligned}
$$

(a) The fragment of N^ℓ corresponding to $(\{\!\{Q\}\!\}, \varnothing)$ and $(\{\!\{R\}\!\}, \varnothing)$.

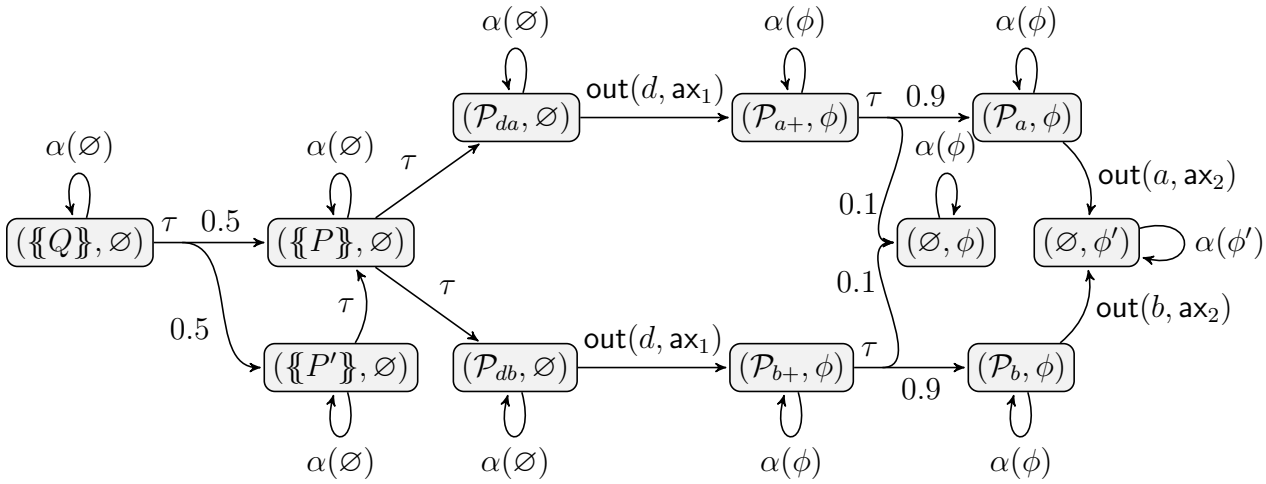


(b) The resolution for $(\{\!\{R\}\!\}, \varnothing) \overset{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}} 0.5 \cdot \delta_{\mathsf{out}(a,c)} + 0.5 \cdot \delta_{\mathsf{out}(b,c)}$.

Figure 8: Fragments of N^ℓ showing that $(\{\!\{P\}\!\}, \varnothing) \leq^{\mathsf{nr}}_{sim} (\{\!\{R\}\!\}, \varnothing)$, $(\{\!\{R\}\!\}, \varnothing) \leq^{\mathsf{nr}}_{sim} (\{\!\{Q\}\!\}, \varnothing)$ but $(\{\!\{P\}\!\}, \varnothing) \not\leq^{\mathsf{nr}}_{sim} (\{\!\{Q\}\!\}, \varnothing)$

$0.9 \cdot \delta_{(\{\!\{\mathsf{out}(b,c)\}\!\}, \varnothing)}$ or $(\{\!\{Q\}\!\}, \varnothing) \overset{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}} 0.9 \cdot \delta_{(\{\!\{\mathsf{out}(a,c)\}\!\}, \varnothing)} + 0.1 \cdot \delta_{(\{\!\{\mathsf{out}(b,c)\}\!\}, \varnothing)}$ and both distributions are incomparable with $0.5 \cdot \delta_{(\{\!\{\mathsf{out}(a,c)\}\!\}, \varnothing)} + 0.5 \cdot \delta_{(\{\!\{\mathsf{out}(b,c)\}\!\}, \varnothing)}$. Hence, $(\{\!\{P\}\!\}, \varnothing) \not\leq^{\mathsf{nr}}_{sim} (\{\!\{R\}\!\}, \varnothing)$. $\square$

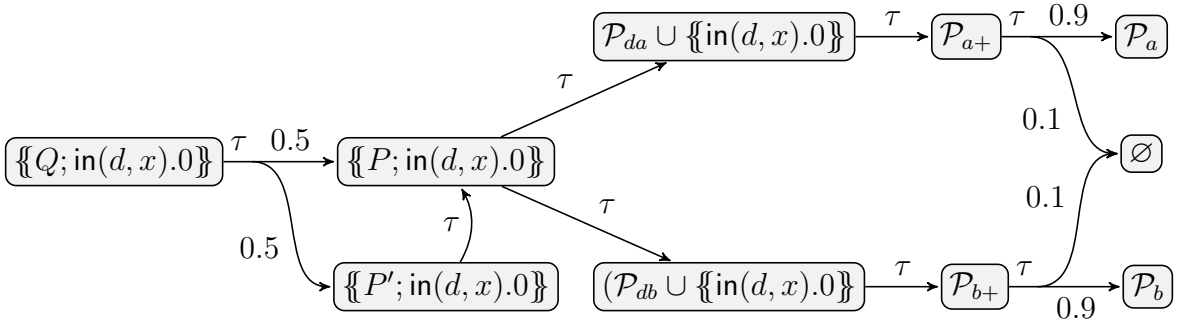
We now show that for non-randomized schedulers (bi)simularity and observational equivalence, respectively preorder, do not coincide. The processes witnessing this result are a direct counter-example to [GLPT07, Theorem 2].



For readability, given a closed frame ϕ, $\alpha(\phi)$ stands for all labels $\mathsf{ax}_i \notin$, for $i > |\phi|$ and $\mathsf{ax}_i \in$ for $i \leq |\phi|$, and all labels $\xi \sim \xi'$ for all closed recipes ξ, ξ' such that $\xi\phi \sim \xi'\phi$ ($\sim \in \{\doteq, \not\doteq\}$).

(a) The fragment of N^ℓ corresponding to $(\{\!\{Q\}\!\}, \varnothing)$ and $(\{\!\{P\}\!\}, \varnothing)$

$$\mathcal{P}_{da} = \mathsf{out}(d, c); (\mathsf{out}(a, c) +_{0.9} 0) \qquad \mathcal{P}_{a+} = \{\!\{\mathsf{out}(a, c) +_{0.9} 0\}\!\} \qquad \mathcal{P}_a = \{\!\{\mathsf{out}(a, c)\}\!\}$$
$$\mathcal{P}_{db} = \mathsf{out}(d, c); (\mathsf{out}(b, c) +_{0.9} 0) \qquad \mathcal{P}_{b+} = \{\!\{\mathsf{out}(b, c) +_{0.9} 0\}\!\} \qquad \mathcal{P}_b = \{\!\{\mathsf{out}(b, c)\}\!\}$$
$$\phi = \{\mathsf{ax}_1 \to c\} \qquad \phi' = \{\mathsf{ax}_1 \to c, \mathsf{ax}_2 \to c\}$$



(b) The fragment of N^o corresponding to $\{\!\{P; \mathsf{in}(d, x).0\}\!\}$ and $\{\!\{Q; \mathsf{in}(d, x).0\}\!\}$

Figure 9: Fragments of NPLTS showing $(\{\!\{Q\}\!\}, \varnothing) \approx^{\mathsf{nr}}_{bi} (\{\!\{P\}\!\}, \varnothing)$ and $\{\!\{Q\}\!\} \not\lesssim^{\mathsf{nr}}_{obs} \{\!\{P\}\!\}$.

Lemma 3. There exist processes $P, Q \in \mathcal{SP}$ such that

$$(\{\!\{Q\}\!\}, \varnothing) \approx_{bi} (\{\!\{P\}\!\}, \varnothing), \qquad (\{\!\{Q\}\!\}, \varnothing) \approx_{bi}^{\mathsf{nr}} (\{\!\{P\}\!\}, \varnothing) \quad \text{and} \quad \{\!\{Q\}\!\} \not\leq_{obs}^{\mathsf{nr}} \{\!\{P\}\!\}$$

Proof. We consider the following processes:

$$\begin{array}{rcl} P & = & \mathsf{out}(d,c); (\mathsf{out}(a,c) +_{0.9} 0) + \mathsf{out}(d,c); (\mathsf{out}(b,c) +_{0.9} 0) \\ P' & = & \mathsf{if}\ c = c\ \mathsf{then}\ P\ \mathsf{else}\ 0 \\ Q & = & P +_{1/2} P' \end{array}$$

We first show that $(\{\!\{Q\}\!\}, \varnothing) \approx_{bi}^{\mathsf{nr}} (\{\!\{P\}\!\}, \varnothing)$. For readability we ignore intermediate states of the form $\mathcal{P} \cup \{\!\{0\}\!\}$ as, for any $\mathcal{P}$ and ϕ, $(\mathcal{P} \cup \{\!\{0\}\!\}), \phi) \xrightarrow{\tau} (\mathcal{P}, \phi)$ and $(\mathcal{P} \cup \{\!\{0\}\!\}, \phi) \approx_{bi}^{\mathsf{nr}} (\mathcal{P}, \phi)$. Following the notations of Figure 9a, define the binary relation R as the reflexive, symmetric and transitive closure of

$$\{((\{\!\{Q\}\!\}, \varnothing), (\{\!\{P\}\!\}, \varnothing)), \quad ((\{\!\{P\}\!\}, \varnothing), (\{\!\{P'\}\!\}, \varnothing))\}$$

We show that R is a bisimulation. Let $s_1, s_2 \in \{(\{\!\{Q\}\!\}, \varnothing), (\{\!\{P\}\!\}, \varnothing), (\{\!\{P'\}\!\}, \varnothing)\}$. If $s_1 \xrightarrow{\alpha(\varnothing)} D$ then $D = \delta_{s_1}$ and $s_2 \xRightarrow{\alpha(\phi)}_{\mathcal{R}_{\mathsf{nr}}} \delta_{s_2}$. By definition of R, $\delta_{s_1} \mathrel{\widehat{R}} \delta_{s_2}$. If $s_1 \xrightarrow{\tau} D$ then we are in one of the following cases:

- $s_1 = (\{\!\{Q\}\!\}, \varnothing)$ and $D = 0.5 \cdot \delta_{(\{\!\{P\}\!\}, \varnothing)} + 0.5 \cdot \delta_{(\{\!\{P'\}\!\}, \varnothing)}$, or $s_1 = (\{\!\{P'\}\!\}, \varnothing)$ and $D = \delta_{(\{\!\{P\}\!\}, \varnothing)}$. In these cases, $s_2 \xRightarrow{\tau}_{\mathcal{R}_{\mathsf{nr}}} \delta_{s_2}$ and $D \mathrel{\widehat{R}} \delta_{s_2}$.
- $s_1 = (\{\!\{P\}\!\}, \varnothing)$ and either $D = \delta_{(\mathcal{P}_{da}, \varnothing)}$ or $D = \delta_{(\mathcal{P}_{db}, \varnothing)}$. As $s_2 \xRightarrow{\tau}_{\mathcal{R}_{\mathsf{nr}}} \delta_{s_1}$ we also have that $s_2 \xRightarrow{\tau}_{\mathcal{R}_{\mathsf{nr}}} D$ which allows us to conclude by reflexivity of R.

All remaining cases are trivial by reflexivity of R. The same relation can also be shown to be a witness that $(\{\!\{Q\}\!\}, \varnothing) \approx_{bi} (\{\!\{P\}\!\}, \varnothing)$.

Next, we need to show that $\{\!\{Q\}\!\} \not\leq_{obs}^{\mathsf{nr}} \{\!\{P\}\!\}$. For this we show that

$$\{\!\{Q;\ \mathsf{in}(d,x).0\}\!\} \not\leq_{obs}^{\mathsf{nr}} \{\!\{P;\ \mathsf{in}(d,x).0\}\!\}$$

(since $\leq_{obs}^{\mathsf{nr}}$ is closed under application of an attacker process). For readability we tacitly omit intermediate states of the form $\mathcal{P} \cup \{\!\{0\}\!\}$ as $\mathcal{P} \cup \{\!\{0\}\!\} \xrightarrow{\tau} \mathcal{P}$ and $\mathcal{P} \cup \{\!\{0\}\!\} \approx_{obs}^{\mathsf{nr}} \mathcal{P}$. Consider Figure 9b. We can build a non-randomized scheduler such that

$$\{\!\{Q;\ \mathsf{in}(d,x).0\}\!\} \xRightarrow{\tau}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)} D \quad \text{where} \quad D = 0.45 \cdot \delta_{\mathcal{P}_a} + 0.45 \cdot \delta_{\mathcal{P}_b} + 0.1 \cdot \delta_{\varnothing}$$

However, there is no distribution E such that $\{\!\{P;\ \mathsf{in}(d,x).0\}\!\} \xRightarrow{\tau}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)} E$, and $D \mathrel{\widehat{\leq_{obs}^{\mathsf{nr}}}} E$. Indeed, the set S of all E such that $\{\!\{P;\ \mathsf{in}(d,x).0\}\!\} \xRightarrow{\tau}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)} E$ is

$$S = \{\delta_s \mid s \in \{\{\!\{P;\ \mathsf{in}(d,x).0\}\!\}, \{\!\{\mathcal{P}_{da}; \mathsf{in}(d,x)\}\!\}, \{\!\{\mathcal{P}_{db}; \mathsf{in}(d,x)\}\!\}, \{\!\{\mathcal{P}_{a+}\}\!\}, \{\!\{\mathcal{P}_{b+}\}\!\}\} \cup \{F_a, F_b\}$$
$$\text{where } F_c = 0.9 \cdot \delta_{\{\!\{\mathcal{P}_c\}\!\}} + 0.1 \cdot \delta_{\{\!\{0\}\!\}} \quad \text{for } c \in \{a, b\}.$$

Observe–looking at Definition 18–that for any distribution E such that $D \widehat{\leq^{\mathsf{nr}}_{obs}} E$ it must hold that:

$$\sum_{s \in \mathrm{supp}(E)} E(s) \cdot \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(s, \downarrow c) \geq 0.45 \qquad \text{for } c \in \{a, b\}. \tag{2}$$

Indeed, we can see that $D \widehat{\leq^{\mathsf{nr}}_{obs}} E$ implies that:

$$\begin{aligned}
0.45 &= D(\{s \mid \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}}(s, \downarrow c) = 1\}) && \text{for } c \in \{a, b\} \\
&\leq E(\leq^{\mathsf{nr}}_{obs} (\{s \mid \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}}(s, \downarrow c) = 1\})) && \text{by definition of } \widehat{R} \\
&\leq E(\{s \mid \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}}(s, \downarrow c) = 1\}) && \text{by definition of } \leq^{\mathsf{nr}}_{obs} \\
&\leq \sum_{s \in \mathrm{supp}(E)} E(s) \cdot \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(s, \downarrow c)
\end{aligned}$$

We now use Equation (2) to show that there is no $E \in S$ such that $D \widehat{\leq^{\mathsf{nr}}_{obs}} E$.

- we see immediately that Equation (2) does not hold for F_a, F_b as

  $$\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}_{i+}, \downarrow j) = 0.9 \cdot \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}_i, \downarrow j) = 0 \qquad \text{for } (i, j) \in \{(a, b), (b, a)\};$$

- by the definition of $\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(,)$, we see that

  $$\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}_{i+}, \downarrow j) = \sum_{s \in \mathrm{supp}(F_c)} F_c(s) \cdot \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(s, \downarrow j)$$

  for $i \in \{a, b\}$ and every barb j. Hence, using the previous case, we conclude that Equation (2) does not hold for $\delta_{\mathcal{P}_{a+}}, \delta_{\mathcal{P}_{b+}}$;

- we have that $\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\{\!\{\mathcal{P}_{di}; \mathsf{in}(d, x)\}\!\}, \downarrow j) = \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}_{i+}, \downarrow j)$ for every barb j, and $i \in \{a, b\}$, and from there we can conclude using the previous case;

- finally, we have that

  $$\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\{\!\{P;\ \mathsf{in}(d, x).0\}\!\}, \downarrow j) = \max_{i \in \{a, b\}} \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\{\!\{\mathcal{P}_{di}; \mathsf{in}(d, x)\}\!\}, \downarrow j)$$

  for every barb j, and we conclude using the previous case.

Therefore, $\{\!\{Q\}\!\} \not\leq^{\mathsf{nr}}_{obs} \{\!\{P\}\!\}$.

□

5.3.1 Counter-example to coincidence of bisimulation and abservational congruence in [GLPT07]

Since we defined our operational semantics in a slightly different way as [GLPT07], we present below a proof that Lemma 3 also holds in their framework. Their semantics differs from ours in two distinct ways: the first one is simply a presentation issue, since they define

probabilistic executions and schedulers in a different but equivalent way; while the other one consists of minor difference in the semantics of the reduction. Here, we rewrite their definitions in our framework, while keeping their operational semantics, i.e., their one-step reduction relation. This paragraph is not entirely self-contained, but all definitions and notations used here can be found in [GLPT07].

Notation 9. We note $\mathcal{P}_\diamond$ for the set of extended processes (in the sense of [GLPT07]), up to static equivalence (again, in the sense of [GLPT07]). We note $\xrightarrow{a}_\diamond \subseteq \mathcal{P}_\diamond \times \mathcal{D}(\mathcal{P}_\diamond)$ for the one-step reduction relation there. For any name a, we write $\downarrow^\diamond a$ for the set of all extended processes (in the sense of [GLPT07]) of the form $C[\overline{a}\langle x\rangle.P]$, where C is an evaluation context (in the sense of [GLPT07]) that does not bind a. Whenever, processes are in $\mathcal{P}_\diamond$, we also use the syntax of [GLPT07] for outputs and inputs, i.e., $\overline{a}\langle x\rangle$ and $a(x)$ instead of $\mathsf{out}(a,x)$ and $\mathsf{in}(a,x)$.

From there, we define two NPLTS $\mathsf{N}^o_\diamond$ and $\mathsf{N}^\ell_\diamond$ that translate their operational semantics in our NPLTS based framework.

Definition 19. The set of states of both $\mathsf{N}^o_\diamond$ and $\mathsf{N}^\ell_\diamond$ is $\mathcal{P}_\diamond$. $\mathsf{N}^o_\diamond$'s set of actions is $\{\tau\}$, while $\mathsf{N}^\ell_\diamond$'s set of actions is:

$$\begin{aligned}&\{\tau\} \cup \{a \mid a \text{ labelled actions in [GLPT07]}\}\\ &\quad \cup \{? \in E \mid E \text{ equivalence class for static equivalence }\}.\end{aligned}$$

Observe that there is a direct correspondance between schedulers in the sense of [GLPT07], and non-randomized schedulers on $\mathsf{N}^\ell_\diamond$. We explicit this correspondance in Lemma 4 below.

Lemma 4. Let $P \in \mathcal{P}_\diamond$, A a subset of $\mathcal{P}_\diamond$, and $p \in [0,1]$.

- there exists a scheduler F (in the sense of [GLPT07]) such that $Prob^F_P(A) = p$ if and only if there exists $\mathsf{R} \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell_\diamond)$, and s' with $\mathsf{corr}_\mathsf{R}(s') = P$ such that

$$\mathrm{RProb}_\mathsf{R}(s', \mathsf{corr}_\mathsf{R}^{-1}(A)) = p;$$

- there exists a scheduler F (in the sense of [GLPT07]) such that $Prob^F_P(\alpha, A) = p$ if and only if there exists D such that

$$P \xrightarrow{\alpha}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell_\diamond)} D \quad \text{and} \quad D(A) = p;$$

- there exists a scheduler F–in the sense of [GLPT07] such that $Prob^F_P(\tau^\star\alpha\tau^\star, A) = p$ if and only if there exists $\mathsf{R} \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell_\diamond)$, and s with $\mathsf{corr}_\mathsf{R}(s) = P$ such that

$$\sum_{u \in \mathcal{S}_{ext}(\mathsf{R}) \mid \mathsf{trans}_\mathsf{R}(u)(a) \neq \star} \mathrm{RProb}_\mathsf{R}(s, \{u\}) \cdot \sum_v \mathsf{trans}_\mathsf{R}(u)(a)(v) \cdot \mathrm{RProb}_\mathsf{R}(v, \mathsf{corr}_\mathsf{R}^{-1}(A)) = p.$$

Using the correspondance in Lemma 4, the counter-example proof below can be followed using either original definitions in [GLPT07], or the NPLTS based view of the present paper.

Notation 10. Let R be an equivalence relation on $\mathcal{P}_\diamond$, and $P \in \mathcal{P}_\diamond$.

- For any scheduler F, we denote by $w_{F,P}$ the function that to any equivalence class E of R associates $Prob_P^F(E)$ and for any $T \in \mathcal{P}_\diamond$, we note $\mathcal{H}_T$ for the set of the different possible $w_{F,T}$ for any scheduler F.
- For any action α, scheduler F, we denote by $w_{F,P}^\alpha$ the function that to an any equivalence class E of R associates $Prob_P^F(\tau^\star\alpha\tau^\star, E)$. For any $T \in \mathcal{P}_\diamond$, we note $\mathcal{H}_T^\alpha$ for the set of the different possible $w_{\mathsf{R},s}^\alpha$ for $\mathsf{corr}_\mathsf{R}(s) = T$.

Using Notation 10, we can rewrite the definitions of both observational congruence and bisimulation in [GLPT07]:

Lemma 5. An observational congruence on $\mathcal{P}_\diamond$ in the sense of [GLPT07] is a symmetric relation R on $\mathcal{P}_\diamond$ such that $\mathcal{P}\ R\ \mathcal{Q}$ implies:

- $\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}_\diamond^o)}(\mathcal{P}, \downarrow^\diamond a) = \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}_\diamond^o)}(\mathcal{Q}, \downarrow^\diamond a)$;
- $\mathcal{H}_\mathcal{P} = \mathcal{H}_\mathcal{Q}$
- for all closing evaluation context C, $C[\mathcal{P}]\ R\ C[\mathcal{Q}]$.

We denote by $\approx_{obs}^\diamond$ the largest observational congruence on $\mathcal{P}_\diamond$.

Lemma 6. A bisimulation on $\mathcal{P}_\diamond$–in the sense of [GLPT07] is a symmetric relation R on $\mathcal{P}_\diamond$ such that $\mathcal{P}\ R\ \mathcal{Q}$ implies:

1. $\mathcal{H}_\mathcal{P} = \mathcal{H}_\mathcal{Q}$;
2. if $\mathcal{P} \xrightarrow{a}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}_\diamond^\ell)} D$ with $a \neq \tau$, then there exists $h \in \mathcal{H}_\mathcal{Q}^a$ such that for every equivalence class E of R, $h(E) = D(E)$

We denote by $\approx_{bi}^\diamond$ the largest bisimulation on $\mathcal{P}_\diamond$.

Lemma 7. There exist extended processes $Q_1, Q_2 \in \mathcal{P}_\diamond$ such that $Q_1 \approx_{bi}^\diamond Q_2$ and $Q_1 \not\approx_{obs}^\diamond Q_2$.

Proof. We slightly change the processes used in the proof of Lemma 3, to account for the change in the one-step reduction relation. We define $Q_1, Q_2 \in \mathcal{P}_\diamond$ as:

$$\begin{array}{rcl} P & = & \overline{a}\langle c\rangle.(\overline{d}\langle c\rangle.\overline{b_1}\langle c\rangle + \overline{d}\langle c\rangle.\overline{b_2}\langle c\rangle) \\ P' & = & \mathsf{if}\ c = c\ \mathsf{then}\ P\ \mathsf{else}\ 0 \\ Q_1 & = & \overline{a}\langle c\rangle.P \oplus_{1/2} \overline{a}\langle c\rangle.P' \\ Q_2 & = & \overline{a}\langle c\rangle.P \end{array}$$

We first show that $Q_1 \approx^{\diamond}_{bi} Q_2$, using the relevant fragment of $\mathsf{N}^{\ell}_{\diamond}$ represented in Figure 10a. We are going to show that the relation R defined as the reflexive, transitive and symmetric closure of $\{(Q_1, Q_2)\,,\,(Q_2, \overline{a}\langle c\rangle.P')\,,\,(P, P')\}$ is a bisimulation on $\mathcal{P}_{\diamond}$ in the sense of Lemma 6. What are the equivalence classes of R ? They consist of

$$C_0 := \{Q_1, Q_2, \overline{a}\langle c\rangle.P'\} \quad C_1 := \{P, P'\} \quad C_T = \{T\} \text{ for all other extended processes } T$$

We now show that R is a bisimulation by considering all (non-identical) pairs in R, and we show that the conditions of Lemma 6 hold. Let be $(U_1, U_2) \in R$, with $U_1 \neq U_2$ (if $U_1 = U_2$, it is obvious that both conditions in Lemma 6 hold).

- We first check Condition 1 in Lemma 6. We can see using Figure 10a that for every $U \in \{U_1, U_2\}$, $\mathcal{H}_U = \{(C_U \mapsto 1 \text{ with } U \in C_U,\, C_E \mapsto 0\ \forall E \text{ with } U \notin E\}$. (That's because $U \in \{(Q_1, Q_2, \overline{a}\langle c\rangle.P', P, P'\}$. Indeed no such process U can go out of its equivalence class with only τ-actions, thus we can conclude. From there, we can immediately conclude that Condition 1 in Lemma 6 holds.

- We now check Condition 2 in Lemma 6. First, if α is an action for static equivalence, we see immediately that the condition holds: indeed all the relevant processes are statically equivalent, since their frames are empty. (In the semantics of [GLPT07] channel names can be output without extending the frame.) Now, let us suppose that α is not an action for static equivalence. As a first step, we compute the $\mathcal{H}^a_U$ for $U \in \{(Q_1, Q_2, \overline{a}\langle c\rangle.P', P, P'\}$. Observe that $0_{\mathcal{H}} := E \mapsto 0$ is always in $\mathcal{H}^a_U$, because the scheduler can always decide not to do the a action. Moreover, we specify by $(E_1 \mapsto r_1, \ldots E_n \mapsto r_n)$ the function h and suppose it to be 0 on any class not in $E_1, \ldots E_n$.

  $\mathcal{H}^{\alpha}_{Q_1} = \{(C_1 \mapsto 1),\, (C_1 \mapsto \frac{1}{2}), 0_{\mathcal{H}}\}$ when $\alpha = \overline{a}\langle c\rangle$, $\{0_{\mathcal{H}}\}$ otherwise.
  $\mathcal{H}^{\alpha}_{Q_2} = \{(C_1 \mapsto 1),\, 0_{\mathcal{H}}\}$ when $\alpha = \overline{a}\langle c\rangle$, $\{0_{\mathcal{H}}\}$ otherwise.
  $\mathcal{H}^{\alpha}_{\overline{a}\langle c\rangle.P'} = \{(C_1 \mapsto 1),\, 0_{\mathcal{H}}\}$ when $\alpha = \overline{a}\langle c\rangle$, $\{0_{\mathcal{H}}\}$ otherwise.
  $\mathcal{H}^{\alpha}_{P} = \{(\{S\} \mapsto 1),\, 0_{\mathcal{H}}\} \cup \{(\{S\} \mapsto 1, \{P_{di}\} \mapsto 1) \mid i \in \{a, b\}\}$ when $\alpha = \overline{a}\langle c\rangle$, $\{0_{\mathcal{H}}\}$ otherwise.
  $\mathcal{H}^{\alpha}_{P'} = \{(\{S\} \mapsto 1),\, 0_{\mathcal{H}}\} \cup \{(\{S\} \mapsto 1, \{P_{di}\} \mapsto 1) \mid i \in \{a, b\}\}$ when $\alpha = \overline{a}\langle c\rangle$, $\{0_{\mathcal{H}}\}$ otherwise.

  We perform a case analysis depending on the first element in (U_1, U_2) (seen as an ordered pair).

  - $U_1 = Q_1$: Observe that there doesn't exist $\alpha \neq \tau$ such that $Q_1 \xrightarrow{\alpha}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} D$, thus we conclude.
  - $U_1 = Q_2$: Suppose that $Q_2 \xrightarrow{\alpha}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} D$ with $\alpha \neq \tau$: it means that $\alpha = \overline{a}\langle c\rangle$, and $D = \delta_P$. So we need to show that $(C_1 \mapsto 1) \in \mathcal{H}^{\alpha}_{U_2}$ for all U_2 such that $(U_1, U_2) \in R$. Then we conclude by seeing that indeed $h : (C_1 \mapsto 1) \in \mathcal{H}^{\alpha}_{Q_1}, \mathcal{H}^{\alpha}_{\overline{a}\langle c\rangle.P'}$ (for Q_1, for instance, it is simply the scheduling that does $Q_1 \xrightarrow{\tau}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} \frac{1}{2}\delta_{\overline{a}\langle c\rangle.P} + \frac{1}{2}\delta_{\overline{a}\langle c\rangle.P'} \xrightarrow{\alpha}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} \frac{1}{2}\delta_P + \frac{1}{2}\delta_{P'}$).

– $U_1 = \overline{a}\langle c\rangle.P'$ Whenever $\overline{a}\langle c\rangle.P' \xrightarrow{\alpha}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell_\diamond)} D$, it means that $\alpha = \overline{a}\langle c\rangle$, and $D = \delta_{P'}$. From there, we can see that the condition on Q_2 holds by observing that $(C_1 \mapsto 1) \in \mathcal{H}^\alpha_{Q_2}, \mathcal{H}^\alpha_{Q_1}$.

– $U_1 = P$: whenever $P \xrightarrow{\alpha}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell_\diamond)} D$, it means that $\alpha = \overline{a}\langle c\rangle$, and $D = \delta_S$. So we can conclude by seeing that $(\{S\} \mapsto 1) \in \mathcal{H}^\alpha_{P'}$.

– $U_2 = P'$: there is no non silent actions that P' can do in one step, so we conclude.

Now, we are going to show that $Q_1 \not\approx^\diamond_{obs} Q_2$. First, observe that by definition $\approx^\diamond_{obs}$ is closed by application of evaluation contexts, thus it is sufficient to show that $C[Q_1] \not\approx^\diamond_{obs} C[Q_2]$ for some evaluation context C. We take $C = [\,] \mid a(x).a(x).d(x)$. For any extended process $T \in \mathcal{P}_\diamond$, we write $cl(T)$ for its equivalence class under $\approx^\diamond_{obs}$. Since in particular elements connected by $\approx^\diamond_{obs}$ must have the same (supremum) sucess probability for each barb, we see that the equivalence classes $cl(\overline{b_1}\langle c\rangle)$, $cl(\overline{b_2}\langle c\rangle)$, and $cl(C[Q_1])$ are distinct. By considering the scheduler represented in Figure 10b, we see that there exists a $h \in \mathcal{H}_{C[Q_1]}$ such that $h(cl(\overline{b_1}\langle c\rangle)) = \frac{1}{2}$ and also $h(cl(\overline{b_2}\langle c\rangle)) = \frac{1}{2}$. Suppose now that $C[Q_1] \approx^\diamond_{obs} C[Q_2]$: it would mean that also $h \in \mathcal{H}_{C[Q_2]}$. But this is not possible, because of the following observation: since the schedulers are not randomized, and there is no probabilistic choice in the process $C[Q_2]$, $h(E) \in \{0, 1\}$ for every $h \in \mathcal{H}_{C[Q_2]}$, and E an equivalence class (this statement can also be checked directly by looking at all cases in the operational semantics). □

Another drawback of the definition of bisimulation given in [GLPT07] is that it is not conservative for processes without probabilities, as explicited in Lemma 8 below. We write $\approx^{\mathrm{det},\diamond}_{bi}$ for the bisimulation defined from non-probabilistic one-step rules: it means the weak bisimulation–in the LTS sense–on the LTS obtained as the restriction of $\mathsf{N}^\ell_\diamond$ to thoses processes in $\mathcal{P}_\diamond$ that do not contain probabilistic primitives.

Lemma 8. There exist extended processes $Q_1, Q_2 \in \mathcal{P}_\diamond$ such that no probabilistic primitives appear in Q_1, Q_2, and $Q_1 \not\approx^\diamond_{bi} Q_2$ and $Q_1 \approx^{\mathrm{det},\diamond}_{bi} Q_2$.

Proof. We consider the following pair of (non-probabilistic) programs:

$$Q_1 := \text{ if } (c = c) \text{ then } (a(x)|(\overline{a}\langle 0\rangle + \overline{a}\langle 1\rangle) \text{ else } 0;$$
$$Q_2 := Q_1 + 0$$

Observe that $Q_1 \approx^{\mathrm{det},\diamond}_{bi} Q_2$. Now, we are going to show that $Q_1 \not\approx^\diamond_{bi} Q_2$. Let R be a bisimulation on $\mathcal{P}_\diamond$. As previously, for any $P \in \mathcal{P}_\diamond$, we note $cl(P)$ for the equivalence class of P with respect to R. We do the proof by contradiction, so we suppose that $cl(Q_1) = cl(Q_2)$. Using the fact that R is a bisimulation, we can show that the following R-equivalence classes are distinct:

- C_0: the class containing the process 0;
- C_{Q_1,Q_2}: the class containing the processes Q_1 and Q_2;
- D_0: the class containing the process $a(x) \mid \overline{a}\langle 0\rangle$;

- D_1: the class containing the process $a(x) \mid \overline{a}\langle 1\rangle$;

We can see that there exists a (non-randomized) scheduler F such that $w_{F,Q_2}(C_0) = 1$, $w_{F,Q_2}(C_{Q_1,Q_2}) = 1$, and $w_{F,Q_2}(D_i) = 0$ for $i \in \{0,1\}$. (F is the scheduler that, starting from $Q_1 + 0$, does the non-deterministic choice towards 0). But, by looking at all possible scheduling from Q_1, we can see that there doesn't exists w_{F',Q_1} such that $w_{F',Q_1} = w_{F,Q_2}$: as a consequence $\mathcal{H}_{Q_1} \neq \mathcal{H}_{Q_2}$, thus we have a contradiction. □

5.3.2 The counter-example for a conservative variant of [GLPT07] bisimulation

We want to highlight here that the issue of non-conservativity is orthogonal to the issue of coincidence between bisimulation and observational equivalence: our claim is that the later is really based on the choice between randomized or non-randomized schedulers. In this section, we present a variant of the bisimulation defined in [GLPT07] on $\mathcal{P}_\diamond$, which is conservative but where schedulers are non-randomized, and we show that we still do not have the coincidence between bisimulation and observational equivalence.

Definition 20. An observational congruence on $\mathcal{P}_\diamond$ is a symmetric relation R on $\mathcal{P}_\diamond$ such that $\mathcal{P}\ R\ \mathcal{Q}$ implies:

- $\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o_\diamond)}(\mathcal{P}, \downarrow^\diamond a) = \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o_\diamond)}(\mathcal{Q}, \downarrow^\diamond a)$;
- if $\mathcal{P} \stackrel{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o_\diamond)} D$ then there exists E such that $\mathcal{Q} \stackrel{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o_\diamond)} E$ and $D\ \widehat{R}\ E$;
- for all closing evaluation context C, $C[\mathcal{P}]\ R\ C[\mathcal{Q}]$.

We note $\approx^\diamond_{obs}$ for the greatest observational congruence on $\mathcal{P}_\diamond$.

Definition 20 above can be seen as intermediate between our notion of observational congruence and the one in [GLPT07]: on the one hand, as in [GLPT07] only *non-randomized schedulers* are considered, the one step reduction relation is the same, and all evaluations contexts (and not only contexts of the form $[\,] \mid Adv$) are taken into account. On the other hand, we diverge from [GLPT07] on the following point when we look to replicate one step a by a succession $\tau^\star a \tau^\star$ of steps, we look only at the end point, and not at the path to go there. It is this divergence that allow us to get back conservativity.

Definition 21. A bisimulation on $\mathcal{P}_\diamond$ is a symmetric relation R on $\mathcal{P}_\diamond$ such that $\mathcal{P}\ R\ \mathcal{Q}$ implies:

- if $\mathcal{P} \stackrel{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell_\diamond)} D$ then there exists E such that $\mathcal{Q} \stackrel{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell_\diamond)} E$ and $D\ \widehat{R}\ E$;
- if $\mathcal{P} \stackrel{a}{\rightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell_\diamond)} D$ with $a \neq \tau$, then there exists E such that $\mathcal{Q} \stackrel{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell_\diamond)} E$ and $D\ \widehat{R}\ E$;

We note $\approx^\diamond_{bi}$ for the greatest bisimulation on $\mathcal{P}_\diamond$.

Observe that bisimilarity in the sense of Definition 21 above does not coincide with bisimilarity–in the sense of Definition 17–on the labelled NPLTS $\mathsf{N}^{\ell}_{\diamond}$. The important difference is that, as for observational congruence, in [GLPT07] only non-randomized schedulers are considered. Another technical difference is the use of $\stackrel{\tau}{\Rightarrow}$ instead of $\stackrel{\tau}{\rightarrow}$ on the left side in the first clause.

We are now going to show the counterpart of Lemma 3 for the observational congruence and weak bisimilarity in the sense of [GLPT07]. It actually disporoves [GLPT07, Theorem 2].

Lemma 9. There exist extended processes $Q_1, Q_2 \in \mathcal{P}_{\diamond}$ such that $Q_1 \approx^{\diamond}_{bi} Q_2$ and $Q_1 \not\approx^{\diamond}_{obs} Q_2$.

Proof. We need to change a little the processes used in the proof of Lemma 3, due to the change in the one-step reduction relation. We define $Q_1, Q_2 \in \mathcal{P}_{\diamond}$ as:

$$\begin{array}{rcl} P & = & \overline{a}\langle c\rangle.(\overline{d}\langle c\rangle.\overline{b_1}\langle c\rangle + \overline{d}\langle c\rangle.\overline{b_2}\langle c\rangle) \\ P' & = & \mathsf{if}\ c = c\ \mathsf{then}\ P\ \mathsf{else}\ 0 \\ Q_1 & = & \overline{a}\langle c\rangle.P \oplus_{1/2} \overline{a}\langle c\rangle.P' \\ Q_2 & = & \overline{a}\langle c\rangle.P \end{array}$$

We first show that $Q_1 \approx^{\diamond}_{bi} Q_2$, using the relevant fragment of $\mathsf{N}^{\ell}_{\diamond}$ represented in Figure 10a. We are going to show that the relation R defined as the reflexive and symmetric closure of $\{(Q_1, Q_2)\,,\,(Q_2, \overline{a}\langle c\rangle.P')\,,\,(P, P')\}$ is a bisimulation on $\mathcal{P}_{\diamond}$ in the sense of Definition 21. We do that by considering all (non-identical) pairs in R, and we show that the conditions of Definition 21 hold.

- (Q_1, Q_2): suppose that $Q_1 \stackrel{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} D$, then D is in $\{\delta_{Q_1}, (\frac{1}{2}\delta_{Q_2} + \frac{1}{2}\delta_{\overline{a}\langle c\rangle.P'})\}$. From there, we can conclude by observing that $Q_2 \stackrel{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} \delta_{Q_2}$, and both $\delta_{Q_1}\ \widehat{R}\ \delta_{Q_2}$ and $(\frac{1}{2}\delta_{Q_2} + \frac{1}{2}\delta_{\overline{a}\langle c\rangle.P'})\ \widehat{R}\ \delta_{Q_2}$ Now, suppose that $Q_1 \stackrel{\alpha}{\rightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} D$ with $\alpha \neq \tau$. First, if α is an action for static equivalence, we see immediately that the condition holds: indeed all the relevant processes are statically equivalent, since their frames are empty. (For this reason, we will not consider explicitly again actions for static equivalence in the following). Looking at $\mathsf{N}^{\ell}_{\diamond}$, we see that there is no other non-silent action that Q_1 can do.

- (Q_2, Q_1): suppose that $Q_2 \stackrel{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} D$, then $D = \delta_{Q_2}$, and we can immediately conclude. Suppose now that $Q_2 \stackrel{\alpha}{\rightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} D$ with $\alpha \neq \tau$: it means that $\alpha = \overline{a}\langle c\rangle$, and $D = \delta_P$. Then we conclude by seeing that $Q_1 \stackrel{\alpha}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} \delta_P$.

- $(Q_2, \overline{a}\langle c\rangle.P')$: suppose that $Q_2 \stackrel{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} D$, then as in the previous case $D = \delta_{Q_2}$, and we can immediately conclude. Suppose now that $Q_2 \stackrel{\alpha}{\rightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} D$ with $\alpha \neq \tau$: then $\alpha = \overline{a}\langle c\rangle$, and $D = \delta_P$. Then we can conclude by seeing that $\overline{a}\langle c\rangle.P' \stackrel{\alpha}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} \delta_P$.

- $(\overline{a}\langle c\rangle.P', Q_2)$. The only τ action that starts from $\overline{a}\langle c\rangle.P'$ is the loop τ action, thus we can immediately conclude for the τ clause. Whenever $\overline{a}\langle c\rangle.P' \xrightarrow{\alpha}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} D$, it means that $\alpha = \overline{a}\langle c\rangle$, and $D = \delta_{P'}$. From there, we can see that the condition on Q_2 holds by observing that $Q_2 \xrightarrow{\alpha}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} \delta_P$, and $\delta_{P'}\ \widehat{R}\ \delta_P$.

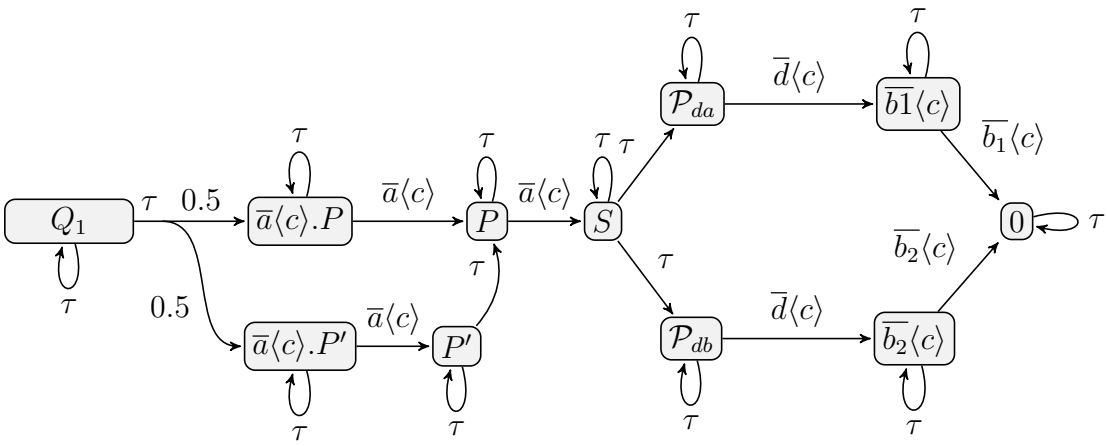
- (P, P'): the only τ action that starts from P is the loop action, thus we can pass immediately to the case of non-silent action. Whenever $P \xrightarrow{\alpha}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} D$, it means that $\alpha = \overline{a}\langle c\rangle$, and $D = \delta_S$. Now, observe that $P' \Longrightarrow_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} \delta_S$, and since R is reflexive (by definition), $\delta_S\ \widehat{R}\ \delta_S$.

- (P', P): suppose that $P' \overset{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} D$, then $D \in \{\delta_{P'}, \delta_P\}$. Since by the loop action $P \overset{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} \delta_P$, and moreover $P'\ R\ P$, we can conclude. We look now at non-silent actions: there are actually none to consider, since there is no non silent actions that P' can do in one step.

Now, we show that $Q_1 \not\approx^{\diamond}_{obs} Q_2$. First, observe that by definition $\approx^{\diamond}_{obs}$ is closed by application of evaluation context, thus it is enough to show that $C[Q_1] \not\approx^{\diamond}_{obs} C[Q_2]$ for some evaluation context C. We take $C = [\,] \mid a(x).a(x).d(x)$. Looking at the NPLTS $\mathsf{N}^{o}_{\diamond}$, we see that $C[Q_1] \overset{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} D := \frac{1}{2}\delta_{\overline{b_1}\langle c\rangle} + \frac{1}{2}\delta_{\overline{b_2}\langle c\rangle}$. Now, we claim that it is not possible to find E such that $C[Q_2] \overset{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} E$, and $D\ \widehat{\approx^{\diamond}_{obs}}\ E$. The argument is as follows: first, observe that all E such that $C[Q_2] \overset{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} E$ are dirac distributions: it is because the schedulers are not randomized, and there is no probilistic choice in the process $C[Q_2]$ (this statement can also be checked directly by looking at all cases in the operational semantics). It means that $D = \delta_A$, for some $A \in \mathcal{P}_{\diamond}$. But for having $(D, \delta_P) \in \widehat{\approx^{\diamond}_{obs}}$, A must be connected by $\approx^{\diamond}_{obs}$ to *all* elements in the support of D, i.e. both to $\overline{b_1}\langle c\rangle$ and $\delta_{\overline{b_2}\langle c\rangle}$. Since in particular elements connected by $\approx^{\diamond}_{obs}$ must have the same (supremum) sucess probability for each barb, we obtain a contradiction.

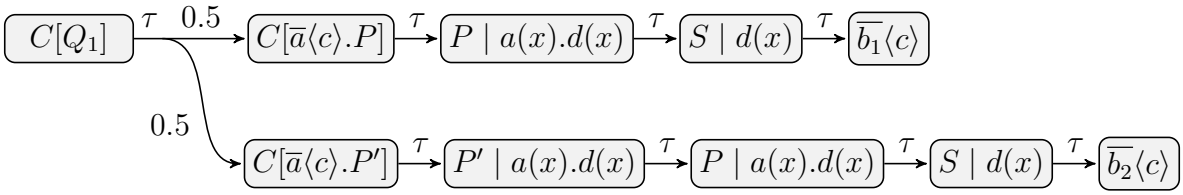
□

Remark 10. The processes Q_1, Q_2 used in the proof of Lemma 9 are not the simplest possible counter-example. However, they have the advantage to be robust to small changes in the defintion of bisimulation, in particular in the case where the double arrow $\Longrightarrow_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})}$ is used both left and right in all clauses of the bisimulation definition.



For readability, we ommit the actions ($? \in E$) for static equivalence. Observe that since none of these extended processes use active substitutions, in particular they are all in the same equivalence class for static equivalence. We used the following notations: $\mathcal{P}_{da} = \overline{d}\langle c\rangle.\overline{b_1}\langle c\rangle$ and $\mathcal{P}_{db} = \overline{d}\langle c\rangle.\overline{b_2}\langle c\rangle$.

(a) The fragment of $\mathsf{N}^{\ell}_{\diamond}$ corresponding to Q_1 and Q_2.



(b) A non-randomized resolution on $\mathsf{N}^{o}_{\diamond}$ witnessing $C[Q_1] \overset{\tau}{\Longrightarrow}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}_{\diamond})} \frac{1}{2}\delta_{\overline{b_1}\langle c\rangle} + \frac{1}{2}\delta_{\overline{b_2}\langle c\rangle}$.

Figure 10: Fragments of NPLTS showing $Q \approx^{\diamond}_{bi} P$, and $\mathbb{Q} \not\lesssim^{\diamond}_{obs} P$.

Part II
Well behaved subclasses of protocols

It is a well-known phenomenon that non-determinism and probabilistic choices do not interact well: a particular scheduler may for instance leak a secret probabilistic choice. Such schedulers are generally deemed unrealistic, and several papers aim at restricting schedulers [CP10, AAPvR10]. We illustrate this phenomenon on the following example.

Example 3. Consider the following two processes.

$$\begin{aligned} P :=& (\mathsf{in}(c,x).\ \text{if } x=0 \text{ then } \mathsf{out}(ok,1) \text{ else } \mathsf{out}(bad,1)) +_{1/2} \\ & (\mathsf{in}(c,x).\ \text{if } x=0 \text{ then } \mathsf{out}(bad,1) \text{ else } \mathsf{out}(ok,1)) \end{aligned}$$

$$Q := \mathsf{in}(c,x).(\mathsf{out}(ok,1) +_{1/2} \mathsf{out}(bad,1))$$

One may, intuitively, consider that these two processes exhibit the same behaviour. Q takes an input and then with probability 1/2 decides to either output on *ok* or on *bad*. P on the other hand first choses a branch with probability 1/2. Each branch performs an input and according to the input value outputs either on *ok* or on *bad*. However, as the two branches make opposite choices on the output depending on the input value, one might expect the probability to output on *ok* to be 1/2.

However, we now show that P and Q are not may testing equivalent and can be distinguished by the following adversary:

$$Adv = \mathsf{out}(c,0) \mid \mathsf{out}(c,1)$$

Indeed, we can show that:

$$\begin{aligned} & \exists \text{ resolution } R \text{ s.t. } \mathrm{RProb}_R(P \mid Adv, \downarrow ok) = 1 \\ \text{and} \quad & \forall \text{ resolution } R', \mathrm{RProb}_{R'}(P \mid Adv, \downarrow ok) \leq \frac{1}{2}. \end{aligned}$$

Intuitively, this results from the fact that the resolution may *leak* the probabilistic choice through the non-deterministic choice of the attacker to output 0 or 1. The resolution chooses the attacker to output 0 in the first probabilistic branch of P and 1 in the second.

In this part we identify two subclasses of processes that avoid this problem. The first such subclass is that of purely non-deterministic processes, i.e. without the $+_p$ operator. This is the class of the original applied pi calculus which also enjoys good tool support. Intuitively, the above problem is avoided as there are no secret probabilistic choices to leak. However, we show that even on purely non-deterministic processes *probabilistic* adversaries have a stronger distinguishing power for the may testing equivalence. We also show that when additionally restricting protocols to a bounded number of sessions, i.e.,

considering processes without replication, may-testing coincides with similarity. We therefore inherit from [CKR18] the fact that may-testing is coNEXP complete for a large class of cryptographic primitives.

The second subclass considers purely probabilistic processes with (nearly) no non-determinism. We show that trace equivalence in this class (as considered for instance in [CSV17]) corresponds to may-testing with a restricted adversary process which again avoids non-determinism. We also sketch how the algorithms of then DeepSec prover could be adapted to check trace equivalence in this probabilistic setting.

6 Non-Probabilistic Processes

In this section, we consider protocols that do not make probabilistic choices, but an *adversary* that can have a probabilistic behaviour. By Proposition 5, we already know that simulation preorder implies may-testing equivalence. We show in this section that for bounded non-probabilistic processes, may testing and simulation actually coincide. We also show that this is not the case in general for processes with an unbounded number of sessions, i.e., with replication.

6.1 May-testing with non-probabilistic adversary and trace equivalence coincide

We show in this section that our definitions of may testing and trace equivalence coincide with the classical definitions of the original, purely non-deterministic applied pi calculus when both regular and adversary processes are non probabilistic (up to the difference on static equivalence, discussed in Remark 4).

Indeed, when considering non-probabilistic processes, all distributions in the (labeled) operational semantics are Dirac distributions. Moreover, we already shown in Proposition 2 that trace equivalence with randomized or non-randomized resolutions are equivalent. Thus, when considering non-randomized resolutions, one can notice that the probability of executing a trace w from $(\mathcal{P}, \phi)$ will always be 0 or 1, and in fact is 1 if and only if $(\mathcal{P}, \phi) \to_{a_1} \ldots \to_{a_n} (\mathcal{P}', \phi')$ where $w = a_1 \ldots a_n$ when having removed τ actions and writing $(\mathcal{P}, \phi) \to_a (\mathcal{P}', \phi')$ instead of $(\mathcal{P}, \phi) \to_a \delta_{(\mathcal{P}', \phi')}$. Similarly, the probability of reaching a barb c from $\mathcal{P}$ is always 0 or 1, and in fact is 1 if and only if $\mathcal{P} \to^* \mathcal{P}' \in \downarrow c$ when writing $\mathcal{P} \to \mathcal{Q}$ instead of $\mathcal{P} \to_\tau \mathcal{Q}$.

We show in the following lemma that may testing and trace equivalence coincide in non-probabilistic settings. In particular, we recover the fact that for the classical definitions in non-probabilisitic settings, trace equivalence implies may-testing.

Proposition 6. Let $\mathcal{P}, \mathcal{Q} \in \mathcal{MP}^{\mathsf{np}}$.

$$(\mathcal{P}, \varnothing) \leq_{tr} (\mathcal{Q}, \varnothing) \quad \text{iff} \quad \begin{array}{l} \forall Adv \in \mathcal{MP}^{\mathsf{np}} \text{ s.t. } fn(Adv) \subseteq \mathcal{N}_{pub}.\ \forall c \in \mathcal{N}_{pub}. \\ \mathrm{RProb}_{\mathcal{R}}(\mathcal{P} \cup Adv, \downarrow c) \leq \mathrm{RProb}_{\mathcal{R}}(\mathcal{Q} \cup Adv, \downarrow c) \end{array}$$

The proof of this result can be found in Appendix G.2.

6.2 May-testing and simulation coincide for bounded processes

To show that may-testing (with probabilistic adversaries) and simulation coincide for bounded non-probabilistic processes, i.e. in $\mathcal{MP}^{<\infty,\mathsf{np}}$, we rely on a modal characterization of strong simulation on *image finite* LTS by a Hennessy-Milner logic. We can rely on simple LTS since we consider non-probabilistic processes (which implies that all distributions on the fragment of N^ℓ with states labeled by non-probabilistic processes are Dirac distributions).

Definition 22. A LTS $\mathsf{L} = (\mathcal{S}, \mathcal{A}, \rightarrow)$ is *image-finite* when for every $s \in \mathcal{S}, a \in \mathcal{A}$, the set $\{t \mid s \xrightarrow{a} t\}$ is finite.

Note that even the fragment of N^ℓ restricted to states in $\mathcal{SP}_\ell^{<\infty,\mathsf{np}}$ is technically *not* image finite. Indeed, the τ-action executing a restriction, i.e. $\mathsf{new}\ a; P$, may lead to infinitely many states (one for each *fresh* private name a' replacing a). However, as all these states (and subsequent states) are equal up to renaming, we can consider a fragment of N^ℓ where we only allow a single transition for the rule (New) per occurrence of name restriction in a state.

Definition 23. We say that a NPLTS N is a new-*determinization of* N^ℓ when $\mathsf{N} = (\mathcal{S}_{\mathsf{N}^\ell}, \mathcal{A}_{\mathsf{N}^\ell}, \mathsf{trans})$ with the following constraints on trans:

- either $\mathsf{trans}((\mathcal{P}, \phi))(a) = \varnothing$ for $a \in \mathcal{A}_{\mathsf{N}^\ell} \setminus \{\tau\}$, and $\mathsf{trans}((\mathcal{P}, \phi))(\tau)$ is the singleton $\{\delta_{(\mathcal{Q},\phi)}\}$ where $\mathcal{P} \rightarrow_\tau \delta_\mathcal{Q}$ by the rule (New)
- or $\mathsf{trans}((\mathcal{P}, \phi)) = \mathsf{trans}_{\mathsf{N}^\ell}((\mathcal{P}, \phi))$ and for all $D \in \mathsf{trans}((\mathcal{P}, \phi))(\tau)$, $(\mathcal{P}, \phi) \rightarrow_\tau D$ by any other rule than (New).

Though we use new-determinization primarily in this section for bounded processes to obtain the image-finite property, we can show that new-determinization preserves trace equivalence, simulation and bisimulation in general. The proof of the following lemma can be found in Appendix E.

Lemma 10. Let N be a new-determinization of N^ℓ.

$$\leq_{tr}^{\mathsf{N}} = \leq_{tr}^{\mathsf{N}^\ell} \quad \text{and} \quad \leq_{sim}^{\mathsf{N}} = \leq_{sim}^{\mathsf{N}^\ell} \quad \text{and} \quad \approx_{bi}^{\mathsf{N}} = \approx_{bi}^{\mathsf{N}^\ell}$$

It is a well-known fact ([Ama16]) that simulation for a LTS can be expressed as strong simulation on the corresponding *weak LTS*. Thus, when we only consider non-probabilistic processes, if we write $(\mathcal{P}, \phi) \xrightarrow{a} (\mathcal{P}, \phi')$ instead of $(\mathcal{P}, \phi) \rightarrow_a \delta_{(\mathcal{P},\phi')}$ then we can build from a new-determinization of N^ℓ a LTS where the transitions $(\mathcal{P}, \phi) \xrightarrow{\tau}^* \xrightarrow{a} \xrightarrow{\tau}^* (\mathcal{Q}, \psi)$ are merged into a single transition.

Definition 24. Given a new-determinization N of N^ℓ, we define the LTS L_N as follows: its states and actions set are the same as those of N, and its transition function is defined as: for all $a \in \mathcal{A}_{\mathsf{N}^\ell}$, $(\mathcal{P}, \phi) \xrightarrow{a}_{\mathsf{L}_\mathsf{N}} (\mathcal{Q}, \psi)$ when $(\mathcal{P}, \phi) \xrightarrow{\tau}^* \xrightarrow{a} \xrightarrow{\tau}^* (\mathcal{Q}, \psi)$ in N and $\mathcal{P}$ is non-probabilistic.

Notice that the fragment of $\mathsf{L_N}$ restricted to states in $\mathcal{SP}_\ell^{<\infty,\mathsf{np}}$ is image finite.

If we denote the strong simulation on the LTS L by $\leq_{ssim}^{\mathsf{L}}$, we obtain the following result.

Lemma 11. Let N be a new-determinization of N^ℓ. For all $\mathcal{P}, \mathcal{Q} \in \mathcal{MP}^{\mathsf{np}}$, we have:

$$(\mathcal{P}, \varnothing) \leq_{sim}^{\mathsf{N}} (\mathcal{Q}, \varnothing) \quad \text{iff} \quad (\mathcal{P}, \varnothing) \leq_{ssim}^{\mathsf{L_N}} (\mathcal{Q}, \varnothing)$$

Proof. The proof directly follows from the following two observations: for all $a \in \mathcal{A}_{\mathsf{N}^\ell}$,

- $(\mathcal{P}, \phi) \overset{a}{\Longrightarrow}_{\mathsf{r}} D$ implies that for all $(\mathcal{P}', \phi') \in \mathrm{supp}(D)$, $(\mathcal{P}, \phi) \overset{\tau}{\to}^* \overset{a}{\to} \overset{\tau}{\to}^* (\mathcal{P}', \phi')$, and
- $(\mathcal{P}, \phi) \overset{\tau}{\to}^* \overset{a}{\to} \overset{\tau}{\to}^* (\mathcal{P}', \phi')$ implies $(\mathcal{P}, \phi) \overset{a}{\Longrightarrow}_{\mathsf{r}} \delta_{(\mathcal{P}', \phi')}$. □

For the remaining of this section, we fix a new-determinization of N^ℓ and denote by L^ℓ its corresponding LTS. Moreover, we denote by $\mathsf{L}^\ell_{<\infty}$ the fragment of L^ℓ restricted to bounded processes.

6.2.1 Hennessy-Milner logical characterization of strong simulation

Our Hennessy-Milner logical characterization consists in expressing strong simulation preorder by the means of satisfaction of *logical formulas* by the LTS.

Definition 25. Let $\mathcal{A}$ be a countable set of actions. We define the set of *logical formulas* as:

$$F \in \mathcal{F} := \top \mid a.F \mid F_1 \wedge F_2, \qquad \text{where } a \in \mathcal{A}$$

In our case, the set of a actions will correspond to $\mathcal{A}^\ell_{ext}$ that is indeed countable. The satisfaction of such formulas by a LTS is defined as follows.

Definition 26. Let $\mathsf{L} = (\mathcal{S}, \mathcal{A}, \to)$ be a LTS. We say that L satisfies a formula F, written $s \models F$, if for all $s \in \mathcal{S}$,

- $s \models \top$;
- $s \models a.F$ when there exists t such that $s \overset{a}{\to} t$ and $t \models F$;
- $s \models F_1 \wedge F_2$ when $s \models F_1$ and $s \models F_2$.

The following proposition shows how to relate strong simulation with satisfiability of logical formulas.

Proposition 7 (HML caracterisation of simulation)**.** For an image-finite LTS L,

$$s \leq_{ssim}^{\mathsf{L}} t \quad \text{iff} \quad \forall F \in \mathcal{F}.\ s \models F \text{ implies } t \models F$$

Proof. In [Ama16], this caracterisation can be found with infinite disjunction. Using the fact that the bisimulation operator on relation is co-continuous for image-finite LTS, (as stated and shown in [Ama16]), we can show that the restriction to finite disjunction is sufficient. A generic proof of the finite-disjunction restriction for any modal caracterisation can be found in [GF12]. □

In order to prove that simulation coincides with may-testing for bounded non-probabilisitic processes, we show that we can *emulate* any logical formula by a probabilistic adversary: for all formulas F, we build a probabilistic adversary Adv such that for all extended processes $(\mathcal{P}, \phi)$, $\mathcal{P} \cup \{\!\!\{Adv\phi\}\!\!\}$ exhibits the adversarial barb ok with probability 1, if and only if the state $(\mathcal{P}, \phi)$ satisfies the formula F in L^{ℓ}.

Definition 27. Let F be a formula in $\mathcal{F}$, $ok \in \mathcal{N}_{pub}$ such that $ok \notin fn(F)$ and $n \in \mathbb{N}$. We define $Adv^{ok}_{F,n}$ by induction on the syntax of F:

- if $F = \top$ then $Adv^{ok}_{F,n} = \mathsf{out}(ok, ok)$.
- if $F = in(\xi, \zeta).F'$ then $Adv^{ok}_{F,n} = \mathsf{out}(\xi, \zeta); Adv^{ok}_{F',n}$ when $vars(\xi, \zeta) \subseteq \mathcal{AX}_n$ and $Adv^{ok}_{F,n} = 0$ otherwise.
- if $F = out(\xi, \mathsf{ax}).F'$ then $Adv^{ok}_{F,n} = \mathsf{in}(\xi, \mathsf{ax}); Adv^{ok}_{F',n+1}$ when $\mathsf{ax} = \mathsf{ax}_{n+1}$, $vars(\xi) \subseteq \mathcal{AX}_n$ and $Adv^{ok}_{F,n} = 0$ otherwise.
- if $F = (\xi \stackrel{?}{=} \zeta).F'$ then $Adv^{ok}_{F,n} = \mathsf{if}\ \xi = \zeta\ \mathsf{then}\ Adv^{ok}_{F',n}\ \mathsf{else}\ 0$ when $vars(\xi, \zeta) \subseteq \mathcal{AX}_n$ and $Adv^{ok}_{F,n} = 0$ otherwise.
- if $F = (\xi \stackrel{?}{\neq} \zeta).F'$ then $Adv^{ok}_{F,n} = \mathsf{if}\ \xi = \zeta\ \mathsf{then}\ 0\ \mathsf{else}\ Adv^{ok}_{F',n}$ when $vars(\xi, \zeta) \subseteq \mathcal{AX}_n$ and $Adv^{ok}_{F,n} = 0$ otherwise.
- if $F = F_1 \wedge F_2$, then $Adv^{ok}_{F,n} = Adv^{ok}_{F_1,n} +_{\frac{1}{2}} Adv^{ok}_{F_2,n}$.

In Definition 27, the integer n and the conditions on the variables of ξ, ζ ensure that the adversarial process $Adv^{ok}_{F,n}$ is closed (no free variables). This is not a restriction as $(\mathcal{P}, \varnothing) \models F$ implies that F satisfies these conditions.

Lemma 12. Let $\mathcal{P} \in \mathcal{MP}^{\mathsf{np}}$ and $ok \in \mathcal{N}_{pub}$ such that $ok \notin fn(\mathcal{P})$. For all formula $F \in \mathcal{F}$, we have

$$(\mathcal{P}, \varnothing) \models F \qquad \text{iff} \qquad \mathrm{RProb}_{\mathcal{R}_r}(\mathcal{P} \cup \{\!\!\{Adv^{ok}_{F,0}\}\!\!\}, \downarrow ok) = 1$$

The proof of Lemma 12 can be found in Appendix G.1. Notice that the lemma in fact also holds for processes with replication. The main result of this section follows almost directly.

Proposition 8. Let $\mathcal{P}, \mathcal{Q} \in \mathcal{MP}^{<\infty,\mathsf{np}}$.

$$(\mathcal{P}, \varnothing) \leq^{\mathsf{N}^{\ell}}_{sim} (\mathcal{Q}, \varnothing) \quad \text{iff} \quad \mathcal{P} \leq_{may} \mathcal{Q}$$

Proof. Suppose $(\mathcal{P}, \varnothing) \leq_{sim}^{\mathsf{N}^\ell} (\mathcal{Q}, \varnothing)$. By Proposition 5, $\mathcal{P} \leq_{obs}^{\mathcal{R}_\mathsf{r}} \mathcal{Q}$, which implies $\mathcal{P} \leq_{may} \mathcal{Q}$ by definition.

Let us now assume $\mathcal{P} \leq_{may} \mathcal{Q}$. From Lemmas 10 and 11, we know that $(\mathcal{P}, \varnothing) \leq_{sim}^{\mathsf{N}^\ell} (\mathcal{Q}, \varnothing)$ if and only if $(\mathcal{P}, \varnothing) \leq_{ssim}^{\mathsf{L}^\ell} (\mathcal{Q}, \varnothing)$. Moreover, since $\mathcal{P}$ and $\mathcal{Q}$ are bounded, we deduce that $(\mathcal{P}, \varnothing) \leq_{ssim}^{\mathsf{N}^\ell} (\mathcal{Q}, \varnothing)$ if and only if $(\mathcal{P}, \varnothing) \leq_{ssim}^{\mathsf{L}^\ell_{<\infty}} (\mathcal{Q}, \varnothing)$. As $\mathsf{L}^\ell_{<\infty}$ is image finite, we can rely on Proposition 7 to obtain that $(\mathcal{P}, \varnothing) \leq_{ssim}^{\mathsf{L}^\ell_{<\infty}} (\mathcal{Q}, \varnothing)$ if and only if for all $F \in \mathcal{F}$, $(\mathcal{P}, \varnothing) \models F$ implies $(\mathcal{Q}, \varnothing) \models F$. Therefore, let $F \in \mathcal{F}$ such that $(\mathcal{P}, \varnothing) \models F$. We take $ok \in \mathcal{N}_{pub}$ such that $ok \notin fn(F, \mathcal{P}, \mathcal{Q})$. By Lemma 12, we have $\mathrm{RProb}_{\mathcal{R}_\mathsf{r}}(\mathcal{P} \cup \{\!\{Adv^{ok}_{F,0}\}\!\}, \downarrow ok) = 1$. Since $\mathcal{P} \leq_{may} \mathcal{Q}$, we deduce that $\mathrm{RProb}_{\mathcal{R}_\mathsf{r}}(\mathcal{Q} \cup \{\!\{Adv^{ok}_{F,0}\}\!\}, \downarrow ok) = 1$ and so $(\mathcal{Q}, \varnothing) \models F$ once again by Lemma 12. □

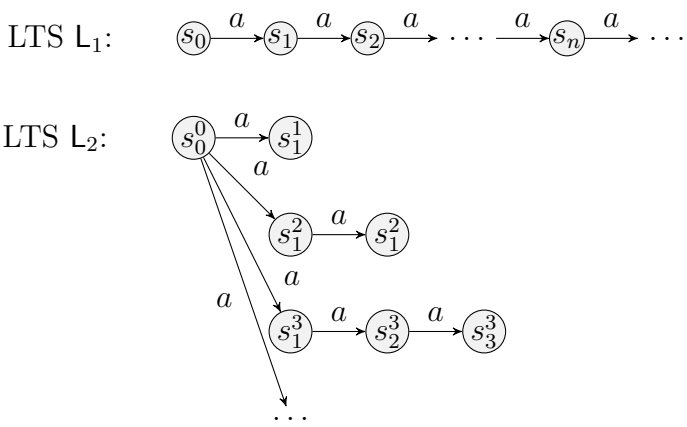
6.2.2 Complexity

Cheval *et al.* have shown [CKR18] that both deciding trace equivalence and bisimilarity is coNEXPTIME complete when cryptographic primitives are modelled by a subterm convergent destructor rewrite system and the number of sessions is bounded. (We refer the reader to [CKR18] for a precise definition of this class of rewrite systems.) The hardness proof reduces Succint 3Sat to both trace equivalence and bisimilarity using a same encoding which also proofs hardness of similarity. The coNEXPTIME decision procedure for bisimilarity can be directly adapted to the case of similarity, hence, by Proposition 8 we have the following result.

Corollary 1. Let $\mathcal{P}, \mathcal{Q} \in \mathcal{MP}^{<\infty,\mathsf{np}}$. Deciding $\mathcal{P} \approx_{may} \mathcal{Q}$ is coNEXPTIME complete when $\doteq$ is defined by a subterm convergent destructor rewrite system.

6.3 May-testing and simulation do not coincide for unbounded processes

To prove that may-testing and simulation do not coincide for processes with replication, we consider the following two LTS L_1 and L_2, that are an asymetric variant of the LTSs used in [vG87] to show that the finitary Hennessy-Milner logic from Definition 26 do not caracterise bisimulation.



Though both L_1 and L_2 may produce an unbounded number of a transitions, the initial transition in L_2 decides on an arbitrary, but fixed number of a transitions in the rest of the execution. This in particular shows that L_2 does not simulate L_1, i.e. $\mathsf{L}_1 \not\leq_{sim} \mathsf{L}_2$.

In the applied pi calculus, L_1 can be represented by the process $!\mathsf{out}(c, a)$. Modeling L_2 in the applied pi calculus is more complex as it requires to non-deterministically choose an integer $n \geq 0$, before outputting $n + 1$ times a. To non deterministically choose n, we rely on the following process that outputs n encoded in unary as $h^n(b)$:

$$Q_{count}(e) = \mathsf{new}\ d.\,(\mathsf{out}(d, b) \mid !\mathsf{in}(d, x).(\mathsf{out}(e, x) + \mathsf{out}(d, h(x))))$$

Intuitively, the channel d represents a memory cell initiated with a public name b (encoding 0). When reading on channel d the current value x, the process non deterministically chooses to increment x (updating the cell with $h(x)$) or to *select* the value x by outputting it on channel e.

It remains to model the process that given an integer x, produces $x + 1$ outputs of a:

$$Q_{out}(e) = \mathsf{new}\ d'.\mathsf{in}(e, x).(\mathsf{out}(d', b) \mid !\mathsf{in}(d', y).\mathsf{out}(c, a).\mathsf{if}\ x = y\ \mathsf{then}\ 0\ \mathsf{else}\ \mathsf{out}(d', h(y)))$$

Similarly to $Q_{count}(e)$, $Q_{out}(e)$ relies on a private d' to increament b until reaching the value x read on e. It is easy to see that the process outputs $x + 1$ times a .

Lemma 13. Let $Q = \mathsf{new}\ e.(Q_{count}(e) \mid Q_{out}(e))$. We have:

$$(!\mathsf{out}(c, a), \varnothing) \not\leq^{\mathsf{N}^\ell}_{sim} (Q, \varnothing) \quad \text{but} \quad !\mathsf{out}(c, a) \leq_{may} Q$$

Proof. To show that $(!\mathsf{out}(c, a), \varnothing) \not\leq^{\mathsf{N}^\ell}_{sim} (Q, \varnothing)$, we rely on the same idea used to show that $\mathsf{L}_1 \not\leq_{sim} \mathsf{L}_2$. Before the first output on c, the process Q must produce a communication on e, hence fixing the value of x used in $Q_{out}(e)$ which bounds the number of following outputs on c by $x + 1$. As $!\mathsf{out}(c, a)$ may output on c an unbounded number of times, we conclude.

To prove that $!\mathsf{out}(c, a) \leq_{may} Q$, we need to show that for all $Adv \in \mathcal{MP}$, for all $ch \in \mathcal{N}_{pub}$, if $fn(Adv) \subseteq \mathcal{N}_{pub}$ then $\mathrm{RProb}_{\mathcal{R}}(\{\!\{!\mathsf{out}(c, a)\}\!\} \cup Adv, \downarrow ch) \leq \mathrm{RProb}_{\mathcal{R}}(\{\!\{Q\}\!\} \cup$

$Adv, \downarrow ch)$. Let $\mathcal{P} = \{\!\{!\mathsf{out}(c,a)\}\!\}$. By unfolding the definition of $\mathrm{RProb}_{\mathcal{R}}(\mathcal{P} \cup Adv, \downarrow ch)$, we know that :

$$\begin{aligned}\mathrm{RProb}_{\mathcal{R}}(\mathcal{P} \cup Adv, \downarrow ch) &= \sup_{\substack{\mathsf{R}=(\mathcal{S}_{\mathsf{R}},\mathsf{corr}_{\mathsf{R}},\mathsf{trans}_{\mathsf{R}})\in\mathcal{R}\\ \mathsf{corr}_{\mathsf{R}}(s)=\mathcal{P}\cup Adv}} \mathrm{RProb}_{\mathsf{R}}(s, \mathsf{corr}_{\mathsf{R}}^{-1}(\downarrow ch)) \\ &= \sup_{\substack{\mathsf{R}=(\mathcal{S}_{\mathsf{R}},\mathsf{corr}_{\mathsf{R}},\mathsf{trans}_{\mathsf{R}})\in\mathcal{R}\\ \mathsf{corr}_{\mathsf{R}}(s)=\mathcal{P}\cup Adv}} \sup_{n\in\mathbb{N}} \mathrm{RProb}_{\mathsf{R}}^{\leq n}(s, \mathsf{corr}_{\mathsf{R}}^{-1}(\downarrow ch))\end{aligned}$$

Let $\mathsf{R} = (\mathcal{S}_{\mathsf{R}}, \mathsf{corr}_{\mathsf{R}}, \mathsf{trans}_{\mathsf{R}}) \in \mathcal{R}$, $s \in \mathcal{S}_{\mathsf{R}}$ such that $\mathsf{corr}_{\mathsf{R}}(s) = \mathcal{P} \cup Adv$ and let $n \in \mathbb{N}$. By definition, the number of transitions from s in the computation of $\mathrm{RProb}_{\mathsf{R}}^{\leq n}(s, \mathsf{corr}_{\mathsf{R}}^{-1}(\downarrow ch))$ is bounded by n. Thus, the resolution R may at most unfold n times the process $!\mathsf{out}(c,a)$. By denoting $P^n = \underbrace{\mathsf{out}(c,a); \ldots ; \mathsf{out}(c,a)}_{n \text{ times}}$, we can therefore easily build a resolution $\mathsf{R}' = (\mathcal{S}_{\mathsf{R}'}, \mathsf{corr}_{\mathsf{R}'}, \mathsf{trans}_{\mathsf{R}'}) \in \mathcal{R}$ and $s' \in \mathcal{S}_{\mathsf{R}'}$ such that $\mathsf{corr}_{\mathsf{R}}(s') = \{\!\{P^n\}\!\} \cup Adv$ and $\mathrm{RProb}_{\mathsf{R}}^{\leq n}(s, \mathsf{corr}_{\mathsf{R}}^{-1}(\downarrow ch)) = \mathrm{RProb}_{\mathsf{R}}^{\leq n}(s', \mathsf{corr}_{\mathsf{R}'}^{-1}(\downarrow ch))$.

However, one can easily show that $(P^n, \varnothing) \leq_{sim}^{\mathsf{N}^\ell} (Q, \varnothing)$ (Q only needs to choose integer $n-1$ to output exactly n times a). Since, by Proposition 5, simulation implies may-testing, we have:

$$\sup_{\substack{\mathsf{R}'=(\mathcal{S}_{\mathsf{R}'},\mathsf{corr}_{\mathsf{R}'},\mathsf{trans}_{\mathsf{R}'})\in\mathcal{R}\\ \mathsf{corr}_{\mathsf{R}}(s')=\{\!\{P^n\}\!\}\cup Adv}} \sup_{n'\in\mathbb{N}} \mathrm{RProb}_{\mathsf{R}'}^{\leq n'}(s', \mathsf{corr}_{\mathsf{R}'}^{-1}(\downarrow ch)) \leq \mathrm{RProb}_{\mathcal{R}}(\{\!\{Q\}\!\} \cup Adv, \downarrow ch)$$

By selecting $n' = n$, we deduce that $\mathrm{RProb}_{\mathsf{R}'}^{\leq n}(s', \mathsf{corr}_{\mathsf{R}'}^{-1}(\downarrow ch)) \leq \mathrm{RProb}_{\mathcal{R}}(\{\!\{Q\}\!\} \cup Adv, \downarrow ch)$ and so $\mathrm{RProb}_{\mathsf{R}}^{\leq n}(s, \mathsf{corr}_{\mathsf{R}}^{-1}(\downarrow ch)) \leq \mathrm{RProb}_{\mathcal{R}}(\{\!\{Q\}\!\} \cup Adv, \downarrow ch)$. It allows us to conclude that $\mathrm{RProb}_{\mathcal{R}}(\mathcal{P} \cup Adv, \downarrow ch) \leq \mathrm{RProb}_{\mathcal{R}}(\{\!\{Q\}\!\} \cup Adv, \downarrow ch)$. □

7 Fully Probabilistic Agents Communicating on Public Channels

We now do a formal comparaison with the probabilistic concurrent systems considered in [CSV17, BCSV18]. They consider systems that are build as the parallel compositions of independant agents, called *roles*, that are not able to communicate directly with each others: all communications are mediated by the adversary. Moreover, there is no non-determinism in the internal behavior of a role; the only non-determinism is controlled by the adversary–thus external–and consists in the adversary's choice for managing the communications.

Definition 28. We say that a process $\mathcal{P} = \{\mathcal{P}_1, \ldots, \mathcal{P}_n\} \in \mathcal{MP}$ is *fully probabilistic*(FP) when:

- there is no non-deterministic choice + in $\mathcal{P}_i$, and no parallel composition | and no !;

- there exists a list $u_1, \ldots, u_n$ of *public* channels such that all input and output actions in $\mathcal{P}_i$ are only done on u_i.

Notation 11. For a FP process $Q = Q_1 \mid \ldots \mid \ldots Q_m$, and $j \in \{1, \ldots, m\}$, we write $\mathsf{out}(c_j, t) \cdot Q$ and $\mathsf{in}(c_j, x) \cdot Q$ for $(Q_1 \mid \ldots \mid \mathsf{out}(c_j, t) \cdot Q_j \mid \ldots Q_m)$ and $(Q_1 \mid \ldots \mid \mathsf{in}(c_j, x) \cdot Q_j \mid \ldots Q_m)$ respectively.

Remark 11. Observe that when looking at the un-labelled semantics for a component $\mathcal{P}_i$ without the syntaxic constructs $+$ and $|$, the only source of non-determinism in $\xrightarrow{\tau}$ comes from new -redexes. To overcome this residual non-determinism, we replace as in Section 6 the NPLTS N^ℓ by a strict new -determinization of N^ℓ. In the present section, by abuse of notation, we will write N^ℓ for an (arbitrary) new -determinization of N^ℓ.

In [CSV17, BCSV18], the authors consider the trace equivalence for a restricted fragments of FP processes. More precisely, their processes have a constrained shape, used to suppress the necessity of scheduling decisions for inteleaving of honest τ-actions, and thus ensure that weak trace equivalence and strong trace equivalence coincide.

Remark 12. Observe that at this point, fully probabilistic processes have no replication. As a consequence, whenever $s \stackrel{\tau}{\Rightarrow} E$, it is actually a finite scheme, and the sub-distribution E is actually a proper distribution.

7.1 Removing residual non-determinism

In this section, we are interested in the fragment of N^ℓ whose states are of the form $(\mathcal{P}, \phi)$, with $\mathcal{P}$ a FP processes. Observe that this fragment has still *internal non-determinism*, since starting from a state $(P_1 \mid \ldots \mid P_n, \phi)$, it can be possible to do a τ action either in a component P_i, or in a component P_j. However, this internal non-determinism is much more *limited* that for general processes: indeed, intuitively, that we chose to reduce first P_i or first P_j will not have an effect on the resulting trace equivalence. In this section, we formalize this intuition by transfering known confluence results from (non-probabilistic) abstract rewriting systems to NPLTSs.

The first step consists in building, from any NPLTS N with only one action $\{\tau\}$, an abstract rewriting system $\overline{\mathsf{N}}$ by moving all information about probabilities from transition to states.

Definition 29. Let $\mathsf{N} = (\mathcal{S}, \{\tau\}, h_\tau)$ be a NPLTS. We define (non-probabilistic) abstract rewriting system $\overline{\mathsf{N}}$–i.e. a LTS with only one action τ–as follows:

- its set of states is $\{\mu = [(\alpha_1, s_1), ...(\alpha_n, s_n)] \in \mathcal{M}_{fin}([0,1] \times \mathcal{S}) \mid \sum \alpha_i = 1\}$.
- its only action is τ;
- the transition function $\xrightarrow{\tau}$ is defined as follows:

$$\frac{s \rightarrow_{\mathsf{N}} E \qquad (\alpha, s) \in Support(\mu)}{\mu \xrightarrow{\tau}_{\overline{\mathsf{N}}} \cup_{t \in Support(D)} \{\!\{(\alpha \cdot D(t), t)\}\!\} \cup \mu \setminus \{\!\{(\alpha, s)\}\!\}}.$$

We formalize in Lemma 14 below how we can recover informations about probabilistic executions in a NPLTS N by looking at (non-probabilistic) execution in the abstract rewriting system $\overline{\mathsf{N}}$. Here, it should be observed that this correspondance holds only when N has *no infinite sequence*.

Lemma 14. Let N be a NPLTS with only one τ action and no infinite sequence, s be a state in N, $A \subseteq \mathcal{S}_{ext}(\mathsf{N})$ a set of external states, and $\alpha \in [0,1]$. Then there exists a non-randomized (maximal) resolution $\mathsf{R} \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N})$ such that $\mathrm{RProb}_{\mathsf{R}}(s, \mathsf{corr}^{-1}(A)) = \alpha$ if and only if there is a finite (maximal) sequence $\sigma := \{\!\!\{(1,s)\}\!\!\} \xrightarrow{\tau}_{\overline{\mathsf{N}}} \mu_1 \xrightarrow{\tau}_{\overline{\mathsf{N}}} \dots \mu_n$, and $\alpha = \sum_{i, t_i \in A} \alpha_i$ with $\mu_n = \{\!\!\{(\alpha_1, t_1), \dots, (\alpha_m, t_m)\}\!\!\}$.

Proof. $\Rightarrow$: Let $\mathsf{R} \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N})$, $s_{\mathsf{R}} \in \mathcal{S}_{\mathsf{R}}$ with $\mathsf{corr}_{\mathsf{R}}(s_{\mathsf{R}}) = s$, and such that $\mathrm{RProb}_{\mathsf{R}}(s_{\mathsf{R}}, \mathsf{corr}^{-1}(A)) = \alpha$. Since N has no infinite sequence, there exists $n \in \mathbb{N}$ such that $\mathrm{RProb}^{\leq n}_{\mathsf{R}}(s_{\mathsf{R}}, \mathsf{corr}^{-1}(A)) = \alpha$, and when R is maximal, we can moreover require that $\{t \mid \mathrm{RProb}^{\leq n}_{\mathsf{R}}(s_{\mathsf{R}}, t) > 0\} \subseteq \{u \mid \mathsf{corr}_{\mathsf{R}}(u) \in \mathcal{S}_{ext}(\mathsf{N})\}$. We build a reduction sequence $\mu_0 = \{\!\!\{(1,s)\}\!\!\} \xrightarrow{\tau}_{\overline{\mathsf{N}}} \mu_1 \xrightarrow{\tau}_{\overline{\mathsf{N}}} \dots \mu_n$ in $\overline{\mathsf{N}}$ by first defining a family $(\rho_j)_{j \in \mathbb{N}}$ as $\rho_j := \{\!\!\{(D_j(u), \mathsf{corr}_{\mathsf{R}}(u)) \mid u \in \mathcal{S}_{\mathsf{R}}\}\!\!\}$, with D_j the distribution obtained after j steps from s' in R. Then we can observe that for every $j \in \mathbb{N}$, it holds that there exists a N such that $\rho_j \rightarrow^{N}_{\overline{\mathsf{N}}} \rho_{j+1}$, and from there we have the result. Moreover, if R is maximal, $Support(D_n) \subseteq \{u \mid \mathsf{corr}_{\mathsf{R}}(u) \in \mathcal{S}_{ext}(\mathsf{N})\}$, thus ρ_n is a normal form in $\overline{\mathsf{N}}$.

$\Leftarrow$: Let σ be a reduction sequence $\mu_0 = \{\!\!\{(1,s)\}\!\!\} \xrightarrow{\tau}_{\overline{\mathsf{N}}} \mu_1 \xrightarrow{\tau}_{\overline{\mathsf{N}}} \dots \mu_n$ in $\overline{\mathsf{N}}$. We build a resolution $\mathsf{R} \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N})$ by induction on n:

- if $n = 0$, the resolution has only one state s' with $\mathsf{corr}_{\mathsf{R}}(s') = s$. Moreover, if $\mu_n = \mu_0$ is a normal form in $\overline{\mathsf{N}}$, it means that s is an external state in N, thus R is a maximal resolution.
- Suppose that the result holds for $n \in \mathbb{N}$. Let $\sigma := \mu_0 = \{\!\!\{(1,s)\}\!\!\} \xrightarrow{\tau}_{\overline{\mathsf{N}}} \mu_1 \xrightarrow{\tau}_{\overline{\mathsf{N}}} \dots \mu_{n+1}$. We write $\mu_1 = \{\!\!\{(\alpha_1, s_1), \dots (\alpha_m, s_m)\}\!\!\}$. Looking at the definition of the ARS $\overline{\mathsf{N}}$, we see that we can split σ into m sequences $\{\!\!\{(1, s_i)\}\!\!\} \xrightarrow{\tau}_{\overline{\mathsf{N}}} \rho^i_1 \xrightarrow{\tau}_{\overline{\mathsf{N}}} \dots \rho^i_{N_i}$, with $N_i \leq n$, and $\mu_n = \{\!\!\{(\alpha_i \cdot \beta, s) \mid i \in \{1, ..., m\}, (\beta, s) \in \rho^i_{N_i}\}\!\!\}$. From there, we can apply the induction hypothesis, and we obtain a resolution R_i for $i \in \{1, \dots, m\}$, and a $s'_i \in \mathcal{S}_{\mathsf{R}_i}$ with $\mathsf{corr}_{\mathsf{R}_i}(s'_i) = s_i$. We can suppose that the $\mathcal{S}_{\mathsf{R}_i}$ are all disjoints. From there, we build a resolution R as the disjoint union of all R_i, plus a fresh state s'_0 with $\mathsf{corr}(s'_0) = s$, and $\mathsf{trans}_{\mathsf{R}}(s'_0) = \sum \alpha_i \cdot \delta_{s'_i}$. Moreover, if $\mu_n =$ is a normal form in $\overline{\mathsf{N}}$, then also the $\rho^i_{N_i}$ are normal from: it means that the induction hypothesis tolds us that each of the R_i is maximal, and from there we can conclude that R also is maximal.

□

In the next step, we show that confluence and termination properties are passed down from N to $\overline{\mathsf{N}}$. We are interested in these properties, because it is a well-known result of the literature on abstract rewriting system (Newmann's Lemma) that a ARS with no infinite

sequence and locally confluent is normalizing, i.e. each state has exactly one normal form.

Lemma 15. Let N a NPLTS with no infinite sequence (that is there is no $s_1, s_2, ...$ such that for all $i \in \mathbb{N}$, $s_i \to_{\mathsf{N}} D_i$, and $s_{i+1} \in \mathit{Support}(D_i)$), and which is locally confluent (i.e. for any $s \in \mathcal{S}_{\mathsf{N}}$, D_1, D_2 such that $s \xrightarrow{\tau}_{\mathsf{N}} D_1$, and $s \xrightarrow{\tau} D_2$, then there exists E such that $D_1 \to_{nr}^{\leq 1} E$ and $D_2 \Rightarrow_{nr}^{\leq 1} E$). Then the abstract rewriting system $\overline{\mathsf{N}}$ also has also infinite sequence and is locally confluent.

Proof.

- Let N be a NPLTS with no infinite sequence. We prove by contradiction that also $\overline{\mathsf{N}}$ has no infinite sequence: suppose that $\overline{\mathsf{N}}$ has an infinite sequence $\sigma := \mu_0 \xrightarrow{\tau} \mu_1 \xrightarrow{\tau} \mu_2 \ldots$. We write $\mu_0 = \{\!\{(\alpha_1, s_1), \ldots, (\alpha_n, s_n)\}\!\}$. Looking at the definition of $\overline{\mathsf{N}}$, we see that we can extract from σ a s_i, and an infinite reduction sequence $\delta_{(1,s_i)} \xrightarrow{\tau}_{\mathsf{N}^{tr}} \mu'_1 \xrightarrow{\tau} \mu'_2 \ldots$ in $\overline{\mathsf{N}}$. By iterating this reasonning, we obtain an infinite sequence on N, and it ends the proof.

- Let N be a locally confluent NPLTS. We prove that also $\overline{\mathsf{N}}$ is locally confluent. We suppose D, E_1, E_2 such that $D \xrightarrow{\tau} E_1$, and $D \xrightarrow{\tau} E_2$. Looking at Definition 29, it means that there exists (s_1, w_1), $(s_2, w_2) \in \mathit{Support}(D)$ such that $(s_i, w_i) \xrightarrow{\tau}_{\mathsf{N}^{tr}} F_i$, and $E_i = D(s_i, w_i) \cdot F_i + D_{|\mathcal{S}\setminus(s_i,w_i)}$ for $i \in \{1, 2\}$. There are two possible cases:
  - either $(s_1, w_1) \neq (s_2, w_2)$, and in this case $F_i \xrightarrow{\tau}_{\overline{\mathsf{N}^\ell}} \sum_{i\in\{1,2\}} D(s_i, w_i) \cdot F_i + D_{|\mathcal{S}\setminus\{(s_i,w_i)|i\in\{1,2\}\}}$ for every $i \in \{1, 2\}$, thus we can conclude.
  - or $(s_1, w_1) = (s_2, w_2)$. In this case, we can use the fact that by hypothesis N is confluent, thus there exists E_3 such that $D_1 \xrightarrow{\tau} D_3$ and $D_2 \xrightarrow{\tau} D_3$, and we can conclude from there.

□

Proposition 9. Let N be a NPLTS with only one τ action, that has no infinite sequence, and which is locally confluent. Let $A \subseteq \mathcal{S}_{ext}(\mathsf{N})$. Then for any maximal resolution R in $\mathcal{R}_{\mathsf{nr}}(\mathsf{N})$ it holds that:

$$\mathrm{RProb}_{\mathsf{R}}(s_{\mathsf{R}}, \mathsf{corr}_{\mathsf{R}}^{-1}(A)) = \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N})}(\mathsf{corr}_{\mathsf{R}}(s_{\mathsf{R}}), A).$$

Proof. Let $A \subseteq \mathcal{S}_{ext}(\mathsf{N})$. If $\rho = \{\!\{(\alpha_1, t_1), \ldots, (\alpha_m, t_m)\}\!\} \in \mathcal{S}_{\overline{\mathsf{N}}}$, we write $\rho(A) := \sum_{j \text{ s.t. } t_j \in A} \alpha_j$. Let R_1 in $\mathcal{R}_{\mathsf{nr}}(\mathsf{N})$ be a maximal resolution, and $\mathsf{R}_2 \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N})$ any resolution. Then we obtain by Lemma 14 two finite sequences $\sigma^i := \{\!\{(1, s^i)\}\!\} \xrightarrow{\tau}_{\overline{\mathsf{N}}} \mu^i_1 \xrightarrow{\tau}_{\overline{\mathsf{N}}} \ldots \mu^i_{n^i}$, and $\mathrm{RProb}_{\mathsf{R}_i}(s^i, \mathsf{corr}_{\mathsf{R}_i}^{-1}(A)) = \sum_{j \text{ s.t. } t^i_j \in A} \alpha^i_j$ with $\mu^i_{n^i} = \{\!\{(\alpha^i_1, t^i_1), \ldots, (\alpha^i_{m^i}, t^i_{m^i})\}\!\}$ for $i \in \{1, 2\}$. Moreover, since R_1 is maximal, $\mu^1_{n^1}$ is a normal form for $\overline{\mathsf{N}}$. Using Lemma 15 and Newmann's Lemma, we can see that $\overline{\mathsf{N}}$ is strongly normalizing, thus $\mu^2_{n^2} \overset{\tau}{\Rightarrow}_{\overline{\mathsf{N}}} \mu^1_{n^1}$. In order to conclude, it is enough to see that ince $A \subseteq \mathcal{S}_{ext}(\mathsf{N})$, $\rho \overset{\tau}{\Rightarrow}_{\overline{\mathsf{N}}} \rho'$ implies that $\rho(A) \leq \rho'(A)$. □

7.1.1 Determinizing may-testing for FP processes

Proposition 10. Let P be an FP process, ϕ a frame and Adv a fully determinate adversary. Let A be a target subset of states of the form $P' \cup Adv'$, with P' a FP process, and Adv' a fully deterministic adversary. Then for any maximal non-randomized resolution R on N^o:

$$\mathrm{RProb}_{\mathsf{R}}(P \cup Adv, A) = \mathrm{RProb}_{\mathcal{R}_{\mathsf{r}}(\mathsf{N}^o)}(P \cup Adv, A).$$

Proof. We first define a NPLTS $(\mathsf{N}^o)_A$ we obtain from N^o as follows:

- We remove all transitions starting from states $a \in A$;
- we add a state *success*, and from each state $a \in A$, we add the transition $a \to \delta_{success}$

We can see that to each resolution R, we can associate a resolution R_A on such that:

$$\mathrm{RProb}_{\mathsf{R}}(P \cup Adv, A) = \mathrm{RProb}_{\mathsf{R}_A}(P \cup Adv, success)$$

Since neither FP processes nor fully deterministic adversaries have !, the (smallest) fragment of N^o containing them has no infinite reduction sequence, and moreover using the fact that we have no meaningful non-determinism, we can show that N^o is locally confluent. As a consequence, it is also the case for $(\mathsf{N}^o)_A$. From there–and using the fact that A is a set of external states for $(\mathsf{N}^o)_A$, we can conclude as a direct consequence of Proposition 9. □

7.1.2 On trace equivalence for FP processes

It is possible to caracterise trace equivalence as the probility of reaching a particular external state *success* on a NPLTS $(\mathsf{N}^\ell)^{tr}$ with only one τ action, built from N^ℓ. The construction is done in Definition 44 in Section B.1, and the caracterisation is shown in Lemma 33. Since FP processes have no !, the FP fragment of N^ℓ has no infinite reduction sequences labelled by τ, and moreover is locally confluent. Looking at the way we defined $(\mathsf{N}^\ell)^{tr}$, we say that our construction preserves these properties.

As a corollary, and using Lemma 32, we obtain that we can caracterise the trace preorder using the ARS $\overline{(\mathsf{N}^\ell)^{tr}}$.

Proposition 11. For any non-randomized maximal resolution R on N^ℓ:

$$\forall s \in \mathcal{S}_{\mathsf{R}}, \forall w \in \mathcal{A}^\star_{ext}, \mathrm{Prob}_{\mathsf{R}}(s, w) = \mathrm{Prob}_{\mathcal{R}^\ell_{\mathsf{r}}}(\mathsf{corr}_{\mathsf{R}}(s), w).$$

Proof. First, observe that the FP fragment of N^ℓ has no infinite τ-reduction sequence, and is locally confluent. Then, we can see that those properties can be passed down to $(\mathsf{N}^\ell)^{tr}$. From there, we can conclude as a direct consequence of the caracterisation of the success probability of reaching a trace from Lemma 33, and Proposition 9. □

Remark 13. The proofs in the present section uses heavily the fact that there is no replication into FP-processes. Indeed, suppose that we consider instead processes of the form $\mathcal{P}_1 \mid \ldots \mid \mathcal{P}_n$, where the processes $\mathcal{P}_i$ have no non-determinism, but can implement

recursion, then Proposition 11 would fail. It is because maximal resolutions can then lead to *non-optimal* strategies, where non-essential part of the system can execute a loop infinitely often. Nonetheless, we believe that is possible–for a given trace w–to build *one* optimal resolution R_w that would maximise $\mathrm{Prob}_{\mathsf{R}}(s, w)$ for each process s, thus allowing us to remove non-determinism in computing the success probability for traces.

7.2 May testing equivalence of FP processes with unrestricted adversary.

As shown by the following example, even on [CSV17, BCSV18]'s fragment, trace equivalence do not coincide with may testing equivalence.

Example 4. Consider again the two processes of Example 3.

$$\begin{aligned} P :=& (\mathsf{in}(c, x).\ \text{if } x = 0 \text{ then } \mathsf{out}(c, ok) \text{ else } \mathsf{out}(c, bad)) +^{1/2} \\ & (\mathsf{in}(c, x).\ \text{if } x = 0 \text{ then } \mathsf{out}(c, bad) \text{ else } \mathsf{out}(c, ok)) \end{aligned}$$

$$Q := \mathsf{in}(c, x).(\mathsf{out}(c, ok) +^{1/2} \mathsf{out}(c, bad))$$

We have already shown in Example 3 that they are not testing equivalent (using a non-determinate adversary). We can however show easily that $(P, \varnothing)$ and $(Q, \varnothing)$ are trace equivalent. Indeed, the relevant traces are of the form $t_k := \mathsf{in}(c, k).\mathsf{out}(c, x_1).(x_1? = ok)$, for all the integers $k \in \mathbb{N}$. We can see that for every k, $\mathrm{Prob}_{\mathcal{R}_r^\ell}((P, \varnothing), t_k) = \mathrm{Prob}_{\mathcal{R}_r^\ell}((Q, \varnothing), t_k) = \frac{1}{2}$.

7.3 A fully probabilistic operational semantics for FP processes and determinate adversaries

However, if we restrict the set of possible adversary and that we consider only adversaries without non-determinism–i.e. written whitout using + or |–we obtain a (weaker) notion of may testing equivalence for FP processes. The main result of this section is that this weaker may testing *coincide* with trace equivalence.

Definition 30. We say that a process Adv is *fully determinate* if it is generated by the following grammar:

$$P, Q := 0 \mid \mathsf{in}(u, x) \cdot P \mid \mathsf{out}(u, v) \cdot P \mid \mathsf{new}\ a \cdot P \mid \mathsf{if}\ u = v\ \mathsf{then}\ P\ \mathsf{else}\ Q \mid P +_p Q$$

Moreover, we ask for a sucess token–formally a channel ok–that only the adversary can use. We say that two process P, Q are *determinate may testing equivalent* whenever they are indistinguishable by fully determinate adversaries.

Our goal is to show that two FP-processes are in the trace pre-ordered if and only if they are in the determinate may-testing preorder. Observe that one direction is immediate: it is

enough to show that any trace can be encoded by a determinate adversary Adv, thus two process that are in the determinate may-testing pre-order are also in the trace pre-order. In the remaining of this section, we show that the reverse implication also holds.

Definition 31. Given a fully determinate process Adv and an integer n, we define the set $Tr^{ok}(Adv, n)$ inductively on Adv as:

- $Tr^{ok}(0, n) = \varnothing$;
- $Tr^{ok}(\mathsf{in}(u, x); Adv, n) = \{\!\{(p_i, (u \stackrel{?}{\neq} ok).out(u, \mathsf{ax}_{n+1}).w_i)\}\!\}_{i=1}^{m}$ when $Tr^{ok}(Adv\{^{\mathsf{ax}_{n+1}}/_x\}, n+1) = \{\!\{(p_i, w_i)\}\!\}_{i=1}^{m}$
- $Tr^{ok}(\mathsf{out}(u, v); Adv', n) = \{\!\{(p_i, (u \stackrel{?}{\neq} ok).in(u, v).w_i)\}\!\}_{i=1}^{m} \cup \{\!\{(1, u \stackrel{?}{=} ok)\}\!\}$ when $Tr^{ok}(Adv, n) = \{\!\{(p_i, w_i)\}\!\}_{i=1}^{m}$
- $Tr^{ok}(Adv_1 +_p Adv_2, n) = \{\!\{(p \cdot p_k^1, w_k^1)\}\!\}_{k=1}^{n_1} \cup \{\!\{((1-p) \cdot p_k^2, w_k^2)\}\!\}_{k=1}^{n_2}$ when $Tr^{ok}(Adv_i, n) = \{\!\{(p_k^i, w_k^i)\}\!\}_{k=1}^{n_i}$ for $i = 1, 2$
- $Tr^{ok}(\mathsf{if}\ u = v\ \mathsf{then}\ Adv_1\ \mathsf{else}\ Adv_2, n) = \{\!\{(p_k^1, (u \stackrel{?}{=} v).w_k^1)\}\!\}_{k=1}^{n_1} \cup \{\!\{(p_k^2, (u \stackrel{?}{\neq} v).w_k^2)\}\!\}_{k=1}^{n_2}$
- $Tr^{ok}(\mathsf{new}\ a; Adv, n) = Tr^{ok}(Adv\{^b/_a\}, n)$ with $b \in \mathcal{N}_{pub}$ fresh.

The proof of the following lemma can be found in Appendix H.

Lemma 16. Let $ok \in \mathcal{N}_{pub}$. Let $(\mathcal{P}, \phi)$ be a purely probabilistic process. Let Adv be a fully determinate adversarial process such that $fv(Adv) \subseteq dom(\phi)$.

$$\begin{aligned}\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P} \cup Adv\phi, \downarrow ok) = \ & \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok) + (1 - \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok)) \times \\ & \textstyle\sum_{(\alpha, w) \in Tr^{ok}(Adv, |dom(\phi)|)} \alpha \cdot \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P}, \phi), w)\end{aligned}$$

We can now show the main proposition of this section.

Proposition 12. Let $\mathcal{P}, \mathcal{Q}$ be two FP processes. Then $(\mathcal{P}, \mathcal{Q})$ is in the may testing preorder for determinate adversaries if and only if $(\mathcal{P}, \varnothing)$ and $(\mathcal{Q}, \varnothing)$ are in the trace pre-order.

Proof. We focus on the non-straightforward implication: the trace preorder implies the may testing preorder for determinate adversaries. Let Adv be a fully determinate adversary process and let ok be a public name.

First, notice that as $\mathcal{P}$ and $\mathcal{Q}$ are both fully probabilisitic processes, we have

$$\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok) = \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P}, \varnothing), out(ok, \mathsf{ax}_1))$$

$$\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{Q}, \downarrow ok) = \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{Q}, \varnothing), out(ok, \mathsf{ax}_1))$$

Let $a_1 = \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P}, \varnothing), out(ok, \mathsf{ax}_1))$ and $a_2 = \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{Q}, \varnothing), out(ok, \mathsf{ax}_1))$. Since $(\mathcal{P}, \varnothing)$ and $(\mathcal{Q}, \varnothing)$ are in the trace pre-order, $a_1 \leq a_2$.

Similarly, for all $(\alpha, w) \in Tr^{ok}(Adv, |dom(\phi)|)$, as $(\mathcal{P}, \varnothing)$ and $(\mathcal{Q}, \varnothing)$ are in the trace pre-order we have that $\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P}, \varnothing), w) \leq \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{Q}, \varnothing), w)$. Defining

$$b_1 = \sum_{(\alpha,w) \in Tr^{ok}(Adv,|dom(\phi)|)} \alpha \cdot \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P}, \phi), w)$$

$$b_2 = \sum_{(\alpha,w) \in Tr^{ok}(Adv,|dom(\phi)|)} \alpha \cdot \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{Q}, \varnothing), w)$$

we obtain that $b_1 \leq b_2$.

Thus, by Lemma 16, $\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok) = a_1 + (1 - a_1) \times b_1$ and $\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{Q}, \downarrow ok) = a_2 + (1 - a_2) \times b_2$ with $0 \leq a_1 \leq a_2 \leq 1$ and $0 \leq b_1 \leq b_2 \leq 1$.

By considering the function $f(x, y) = x + y - xy$, we notice that showing $a_1 + (1 - a_1) \times b_1 \leq a_2 + (1 - a_2) \times b_2$ is equivalent to showing that $f(a_2, b_2) - f(a_1, b_1) \geq 0$. By computing the partial derivations, we can see that $f(a_2, b_2) \geq f(a_1, b_2) \geq f(a_1, b_1)$ which allows us to conclude. □

8 Deciding trace equivalence and tool support

As previous mentioned, Cheval *et al.* [CKR18] designed a decision procedure for trace equivalence when cryptographic primitives are modelled by a subterm convergent destructor rewrite system and a bounded number of sessions. This procedure is based on constraint solving techniques that represent the infinite set of all possible concrete executions of the processes and an arbitrary attacker as a finite symbolic tree, called the *partition tree*. Intuitively, each node of this symbolic tree represents the state of the two processes after executing a trace tr. Due to non-determinism, a node may contain several constraint systems corresponding to every possible interleaving allowing the execution of a given trace tr. Deciding trace equivalence between processes A and B, in the original, non-probabilistic setting, requires to check that each node of the symbolic tree contains at least one constraint system derived from process A and one from process B; or the node is empty.

We show how to extend this procedure in order to decide trace equivalence in a general setting where both probabilistic and non-determinism behavior may co-exist in the process. Obviously, we inherit the setting of a bounded number of sessions and cryptographic primitives modeled by a subterm convergent destructor rewrite system.

Following Proposition 2, proving $(\mathcal{P}, \phi) \leq_{tr} (\mathcal{P}', \phi')$ is equivalent to proving $(\mathcal{P}, \phi) \leq_{tr}^{\mathsf{nr}} (\mathcal{P}', \phi')$. Thus, by definition, we focus on the computation of $\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P}, \phi), w)$ for all $w \in {\mathcal{A}_{ext}^\ell}^*$. A main difficulty stems from the presence of universal quantification over resolutions. However, as $\mathcal{P}$ is bounded, we can completely ignore resolutions and focus on the labelled semantics, as shown by the following property.

Lemma 17. Let $(\mathcal{P}, \phi) \in \mathcal{SP}_\ell^{<\infty}$. Let $a \in \mathcal{A}_{ext}^\ell$. Let $w \in {\mathcal{A}_{ext}^\ell}^*$.

$$\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P}, \phi), \epsilon) = 1 \qquad \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P}, \phi), a.w) = \max(p_1, p_2)$$

where

$$p_1 = \max_{(\mathcal{P},\phi)\to_\tau D} \sum_{(\mathcal{P}',\phi')\in \mathrm{supp}(D)} D((\mathcal{P}',\phi')) \cdot \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P},\phi), a.w)$$

$$p_2 = \max_{(\mathcal{P},\phi)\to_a D} \sum_{(\mathcal{P}',\phi')\in \mathrm{supp}(D)} D((\mathcal{P}',\phi')) \cdot \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P},\phi), w)$$

Note that this inductive definition is well founded as the size of the processes strictly decreases at each semantics step since there is no replication.

8.1 History

As mentioned above, partition trees [CKR18] are a finite symbolic representation of the concrete executions of the two initial processes. Each node contains all reachable states of the two processes after executing some trace w. However, to compute the probability $\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P},\phi), w)$, Lemma 17 also requires to know the different semantics steps that led to the process states after executing w. In other words, it requires the *history* of each extended processes. Therefore, to simplify the probability computation, we extended the labelled semantics by adding the history of transitions leading to the extended process. To further simplify, we assume that each input, output, probabilistic choice and non-deterministic choice are decorated with a label $\ell \in \mathcal{L}$, denoted $\mathsf{in}^\ell(u,x);P$, $\mathsf{out}^\ell(u,v);P$ and $P +^\ell_p Q$, $P +^\ell Q$ respectively. Additionally, we assume that all labels are distinct in the initial processes.

Definition 32. We define *history entries* as elements from $\{\mathsf{h}_1(\ell), \mathsf{h}_2(\ell,\ell'), \mathsf{h}_+(\ell,p,i), \mathsf{h}_c(\ell,i) \mid i \in \{0,1\}, p \in]0,1[, \ell \text{ label}\}$. A *history*, usually denoted H, is a sequence of history entries.

Extended processes and the labelled semantics can naturally be extended to include history. In particular when $(\mathcal{P},\phi) \to_a D$ and $(\mathcal{P}',\phi') \in \mathrm{supp}(D)$, we define $(\mathcal{P},\phi,\mathsf{H}) \xrightarrow{a} (\mathcal{P}',\phi',\mathsf{H}')$ where:

- $\mathsf{H}' = \mathsf{H}\cdot\mathsf{h}_+(\ell,p,0)$ when $\mathcal{P} = \mathcal{Q} \cup \{\!\{P +^\ell_p Q\}\!\}$ and $\mathcal{P}' = \mathcal{Q} \cup \{\!\{P\}\!\}$;
- $\mathsf{H}' = \mathsf{H}\cdot\mathsf{h}_+(\ell,p,1)$ when $\mathcal{P} = \mathcal{Q} \cup \{\!\{P +^\ell_p Q\}\!\}$ and $\mathcal{P}' = \mathcal{Q} \cup \{\!\{Q\}\!\}$;
- $\mathsf{H}' = \mathsf{H}\cdot\mathsf{h}_c(\ell,0)$ when $\mathcal{P} = \mathcal{Q} \cup \{\!\{P +^\ell Q\}\!\}$ and $\mathcal{P}' = \mathcal{Q} \cup \{\!\{P\}\!\}$;
- $\mathsf{H}' = \mathsf{H}\cdot\mathsf{h}_c(\ell,1)$ when $\mathcal{P} = \mathcal{Q} \cup \{\!\{P +^\ell Q\}\!\}$ and $\mathcal{P}' = \mathcal{Q} \cup \{\!\{Q\}\!\}$;
- $\mathsf{H}' = \mathsf{H}\cdot\mathsf{h}_2(\ell,\ell')$ when $\mathcal{P} = \mathcal{Q} \cup \{\!\{\mathsf{out}^\ell(u,t).P, \mathsf{in}^{\ell'}(v,x).Q\}\!\}$, $\mathcal{P}' = \mathcal{Q} \cup \{\!\{P, Q\{x \mapsto t\}\}\!\}$;
- $\mathsf{H}' = \mathsf{H}\cdot\mathsf{h}_1(\ell)$ when $\mathcal{P} = \mathcal{Q} \cup \{\!\{\mathsf{out}^\ell(u,t).P\}\!\}$ and $a = out(\xi, \mathsf{ax}_n)$ and $\mathcal{P}' = \mathcal{Q} \cup \{\!\{P\}\!\}$;
- $\mathsf{H}' = \mathsf{H}\cdot\mathsf{h}_1(\ell)$ when $\mathcal{P} = \mathcal{Q} \cup \{\!\{\mathsf{in}^\ell(u,x).P\}\!\}$ and $a = in(\xi,\zeta)$ and $\mathcal{P}' = \mathcal{Q} \cup \{\!\{P\{x \mapsto \zeta\phi\}\}\!\}$;
- $\mathsf{H}' = \mathsf{H}$ otherwise.

Given $w \in {\mathcal{A}_{ext}^{\ell}}^*$, we write $(\mathcal{P}, \phi, \mathsf{H}) \overset{w}{\Rightarrow} (\mathcal{P}', \phi', \mathsf{H}')$ when $(\mathcal{P}, \phi, \mathsf{H}) \xrightarrow{a_1} \ldots \xrightarrow{a_n} (\mathcal{P}', \phi', \mathsf{H}')$ and w is $a_1 \ldots a_n$ with the τ labels removed.

Since labels occur at most once in the initial process, intuitively, two extended processes with a shared prefix executed the same semantics steps. In other words, if

$$(\mathcal{P}, \phi, \mathsf{H}) \overset{w}{\Rightarrow} (\mathcal{P}_1, \phi_1, \mathsf{H}_0 \cdot \mathsf{H}_1) \quad \text{and} \quad (\mathcal{P}, \phi, \mathsf{H}) \overset{w}{\Rightarrow} (\mathcal{P}_2, \phi_2, \mathsf{H}_0 \cdot \mathsf{H}_2)$$

then there exist w_0, w_1 and an extended process $(\mathcal{P}_0, \phi_0, \mathsf{H}_0)$ such that $w = w_0 w_1$ and

$$\begin{tikzcd}
 & & (\mathcal{P}_1, \phi_1, \mathsf{H}_0 \cdot \mathsf{H}_1) \\
(\mathcal{P}, \phi, \mathsf{H}) \arrow[r, Rightarrow, "w_0"] & (\mathcal{P}_0, \phi_0, \mathsf{H}_0) \arrow[ur, Rightarrow, "w_1"] \arrow[dr, Rightarrow, "w_1"'] & \\
 & & (\mathcal{P}_2, \phi_2, \mathsf{H}_0 \cdot \mathsf{H}_2)
\end{tikzcd}$$

We now describe how we can compute the probability that $(\mathcal{P}, \phi)$ executes a trace w from the set of histories obtained after executing w, i.e. $\{\mathsf{H}' \mid (\mathcal{P}, \phi, []) \overset{w}{\Rightarrow} (\mathcal{P}', \phi', \mathsf{H}')\}$ where $[]$ denotes the empty sequence.

Definition 33. Let S be a set of histories. We denote by $S_{|h} = \{\mathsf{H}' \mid (h \cdot \mathsf{H}') \in S\}$. We define $\mathsf{compute}(S)$ inductively as follows:

- $\mathsf{compute}(\varnothing) = 0$
- $\mathsf{compute}(\{[]\}) = 1$, i.e., if S is the singleton containing the empty sequence
- otherwise

$$\mathsf{compute}(S) = \max \begin{cases} \max\limits_{\ell} \mathsf{compute}(S_{|\mathsf{h}_1(\ell)}) \\ \max\limits_{\ell,\ell'} \mathsf{compute}(S_{|\mathsf{h}_2(\ell,\ell')}) \\ \max\limits_{\ell,i} \mathsf{compute}(S_{|\mathsf{h}_c(\ell,i)}) \\ \max\limits_{\ell,p} (p \cdot \mathsf{compute}(S_{|\mathsf{h}_+(\ell,p,0)}) + (1-p) \cdot \mathsf{compute}(S_{|\mathsf{h}_+(\ell,p,1)})) \end{cases}$$

The correspondence between $\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P}, \phi), w)$ and the function $\mathsf{compute}(\cdot)$ is given in the following lemma.

Lemma 18. Let (P, ϕ) be an extended process, $w \in {\mathcal{A}_{ext}^{\ell}}^*$ and $S = \{\mathsf{H}' \mid (\mathcal{P}, \phi, []) \overset{w}{\Rightarrow} (P', \phi', \mathsf{H}')\}$. We have that $\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P}, \phi), w) = \mathsf{compute}(S)$.

Proof. Let $A = (\mathcal{P}, \phi)$ be an extended process. Let $w \in {\mathcal{A}_{ext}^{\ell}}^*$. Let us define $S(A, w)$ the set $\{\mathsf{H} \mid (\mathcal{P}, \phi, []) \overset{w}{\Rightarrow} (P', \phi', \mathsf{H})\}$. Then, we show by induction on $(|A|, |w|)$ that $\mathsf{compute}(S(A)) = \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}(A, w)$.

Base case $(|A|, |w|) = (0, 0)$*, i.e.,* $P = 0$ *and* $w = \epsilon$*.* In such a case, by Lemma 17, we deduce that $\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}(A, w) = 1$. Moreover, by definition of $S(A, w)$, $S(A, w) = \{[]\}$ meaning that $\mathsf{compute}(S(A, w)) = 1$. This allows us to conclude.

Inductive step $(|A|, |w|) > (0, 0)$*.* We do a case analysis on w and the available semantics steps on A (see Definition 10):

- Case $(\mathcal{P}, \phi) \to_\tau \delta_(\mathcal{P}', \phi))$ with Nil, Par or Conditional rule: In such a case, as the rule are deterministic, two simple inductive proofs allow us to show that $\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}(A, w) = \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}(B, w)$ and $\mathsf{compute}(S(A, w)) = \mathsf{compute}(S(B, w))$. This typically indicates that the order on which deterministic actions are applied does not matter. Since $|B| < |A|$, we can conclude by applying our inductive hypothesis.

- Case $w = aw'$ with $a = (\xi \sim \zeta)$: In such a case, $A \not\to_a \delta_A$ iff $(\mathcal{P}, \phi, []) \xrightarrow{a} (\mathcal{P}, \phi, [])$. Similarly to the previous case, we can easily show by induction that either (i) $\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}(A, w) = 0$ and $A \not\to_a \delta_A$, meaning that $(\mathcal{P}, \phi, []) \not\xrightarrow{a}$, $S(A, w) = \varnothing$ and so $\mathsf{compute}(S(A, w)) = 0$; or (ii) $\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}(A, w) = \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}(A, w')$ and $A \to_a \delta_A$. In the latter case, we deduce by definition that $\mathsf{compute}(S(A, w')) = \mathsf{compute}(S(A, w))$. By inductive hypothesis, $\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}(A, w') = \mathsf{compute}(S(A, w'))$ which allows us to conclude.

- Otherwise, the remaining semantic steps give us that for all $B = (\mathcal{P}', \phi')$, $(\mathcal{P}, \phi) \to_b D$ and $B \in \mathrm{supp}(D)$ if and only if $(\mathcal{P}, \phi, []) \xrightarrow{b} (\mathcal{P}', \phi', [h])$. Moreover, due to distinct occurrences on our processes, we also deduce that two distinct transition steps cannot correspond to the same history. Therefore, $(\mathcal{P}, \phi, []) \xrightarrow{b} (\mathcal{P}', \phi', [h])$ implies that $S(A, w)_{|h} = S(B, w')$. Applying our inductive hypothesis on (B, w'), we deduce that $\mathsf{compute}(S(A, w)_{|h}) = \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}(B, w')$.

  Hence, when h does not correspond to a probabilistic choice, we have by definition that $D = \delta_B$ and so:

  $$D(B) \cdot \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}(B, w') = \mathsf{compute}(S(A, w)_{|h})$$

  When $h = \mathsf{h}_+(\ell, p, i)$ with $i \in \{0, 1\}$, we know that $b = \tau, \phi' = \phi$ and $(\mathcal{P}, \phi, []) \xrightarrow{\tau} (\mathcal{P}'', \phi, [\mathsf{h}_+(\ell, p, 1 - i)])$ such that $\mathrm{supp}(D) = \{B, B'\}$ with $B' = (\mathcal{P}'', \phi)$. Therefore,

  $$\begin{aligned}\sum_{s \in \mathrm{supp}(D)} D(s) \cdot \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}(s, w) &= p_i \cdot \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}(B, w) + p_{1-i} \cdot \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}(B', w) \\ &= p_i \cdot \mathsf{compute}(S(A, w)_{|h}) + \\ &\quad p_{1-i} \cdot \mathsf{compute}(S(A, w)_{|\mathsf{h}_+(\ell, p, 1-i)})\end{aligned}$$

  with $p_0 = p$ and $p_1 = 1 - p$.

  By definition of $\mathsf{compute}(S(A, w))$ and Lemma 17, we conclude. □

This lemma provides the core property that allows us to update the partition trees generated by the procedure in [CKR18] as well as the test performed on each node of this partition tree to conclude trace preorder.

8.2 Partition tree

The algorithm in [CKR18] relies on a symbolic semantics to finitely models the infinitely branching concrete semantics of the calculus. They consider *symbolic processes* $(\mathcal{P}, \mathcal{C})$ where $\mathcal{P}$ is a multiset of (non-necessarily ground) processes and $\mathcal{C}$ is a constraint system containing a frame (non-necessarily ground). The frame included in a constraint system $\mathcal{C}$ is denoted $\Phi(\mathcal{C})$. We naturally extend symbolic processes with histories: $(\mathcal{P}, \mathcal{C}, \mathsf{H})$.

In [CKR18], symbolic configurations are accompanied with a symbolic semantics as a labelled transition relation, denoted $\xrightarrow{\ell}_{\mathsf{s}}$. We naturally extend this semantics to our probabilistic settings. Intuitively, if $(\mathcal{P}, \mathcal{C}) \xrightarrow{\ell}_{\mathsf{s}} (\mathcal{P}', \mathcal{C}')$ in [CKR18] semantics then $(\mathcal{P}, \mathcal{C}, p, \mathsf{H}) \xrightarrow{\ell}_{\mathsf{s}} (\mathcal{P}', \mathcal{C}', p, \mathsf{H}')$ where H' is follows the construction described in Section 8.1. Additionally, we add a semantics rule for the probabilistic choice where we compute the new probability.

$$
\begin{array}{lcl}
(\{\!\{P +_r^\ell Q\}\!\} \cup \mathcal{P}, \mathcal{C}, \mathsf{H}) & \xrightarrow{\tau}_{\mathsf{s}} & (\{\!\{P\}\!\} \cup \mathcal{P}, \mathcal{C}, \mathsf{H} \cdot \mathsf{h}_+(\ell, p, 0)) \\
(\{\!\{P +_r^\ell Q\}\!\} \cup \mathcal{P}, \mathcal{C}, \mathsf{H}) & \xrightarrow{\tau}_{\mathsf{s}} & (\{\!\{Q\}\!\} \cup \mathcal{P}, \mathcal{C}, \mathsf{H} \cdot \mathsf{h}_+(\ell, p, 1))
\end{array}
$$

We do not detail how constraint systems are generated here as we do not alter their generation. We however recall that a *solution* of a constraint system is a pair of substitutions (Σ, σ) such that Σ is a substitution of recipes, hence representing how the attacker computes messages, and σ is the substitution instantiating the variables of the process. Σ and σ are called second-order and first-order substitutions respectively. Given a constraint system $\mathcal{C}$, the set of solutions is denoted $Sol(\mathcal{C})$. Note that later on, when talking about partition tree, we will restrict the solutions of constraint systems that satisfy some predicates π. These solutions will be denoted $Sol^\pi(\mathcal{C})$

The soundness and completeness of the semantics can be adapted from [CKR22, Proposition 3.2] as follows:

Lemma 19 (soundness and completeness of the symbolic semantics)**.** Let $(\mathcal{P}, \mathcal{C}, \mathsf{H})$ be a symbolic process.

1. *Soundness:* for all symbolic steps $(\mathcal{P}, \mathcal{C}, \mathsf{H}) \xrightarrow{a}_{\mathsf{s}} (\mathcal{Q}, \mathcal{C}', \mathsf{H}')$ and $(\Sigma, \sigma) \in Sol(\mathcal{C}')$, there exists a concrete labelled transition $(\mathcal{P}\sigma, \Phi(\mathcal{C})\sigma\!\downarrow, \mathsf{H}) \xrightarrow{a\Sigma} (\mathcal{Q}\sigma, \Phi(\mathcal{C}')\sigma\!\downarrow, \mathsf{H}')$

2. *Completeness:* for all symbolic processes $(\mathcal{P}, \mathcal{C}, \mathsf{H})$, $(\Sigma, \sigma) \in Sol(\mathcal{C})$ and concrete traces $(\mathcal{P}\sigma, \Phi(\mathcal{C})\sigma\!\downarrow, \mathsf{H}) \xrightarrow{a} (\mathcal{Q}, \Phi, \mathsf{H}')$, there exists a symbolic step $(\mathcal{P}, \mathcal{C}, \mathsf{H}) \xrightarrow{a'}_{\mathsf{s}} (\mathcal{Q}', \mathcal{C}', \mathsf{H}')$ and $(\Sigma', \sigma') \in Sol(\mathcal{C}')$ such that $\Sigma \subseteq \Sigma'$, $\mathcal{Q} = \mathcal{Q}'\sigma'$, $a = a'\Sigma'$ and $\Phi = \Phi(\mathcal{C}')\sigma'\!\downarrow$.

We can now describe the partition trees that can be generated thanks to the procedure described in [CKR22]. Each node of a partition tree is in fact labelled by a configuration defined as follows.

Definition 34 (configuration)**.** A *configuration* is a pair (Γ, π) where Γ is a set of symbolic processes and π a predicate on second-order substitutions. We also require that:

1. the predicate π is defined on $vars^2(\Gamma)$, that is, for all Σ, $\pi(\Sigma)$ *iff* $\pi(\Sigma_{|vars^2(\Gamma)})$;

2. for all $(\mathcal{P}_1, \mathcal{C}_1, \mathsf{H}_1), (\mathcal{P}_2, \mathcal{C}_2, \mathsf{H}_2) \in \Gamma$, if $(\Sigma, \sigma_1) \in Sol^{\pi}(\mathcal{C}_1)$ then there exists σ_2 such that $(\Sigma, \sigma_2) \in Sol^{\pi}(\mathcal{C})$ and $\Phi(\mathcal{C}_1)\sigma_1 \sim \Phi(\mathcal{C}_2)\sigma_2$.

We state the properties satisfied by the partition tree.

Definition 35 (partition tree)**.** A *partition tree* of two bounded processes P and Q is a tree T whose nodes are labelled by configurations and edges by visible symbolic actions, and that verifies the following properties. First of all $P, Q \in \Gamma(root(T))$ and $\pi(root(T)) = \top$, where $root(T)$ denotes the root node of the tree. Then for all nodes n of T, $(\mathcal{P}, \mathcal{C}) \in \Gamma(n)$ and visible symbolic actions α:

1. *Closure by τ-transition*: if $(\mathcal{P}, \mathcal{C}, \mathsf{H}) \overset{\tau}{\Rightarrow}_{\mathsf{s}} (\mathcal{P}', \mathcal{C}', \mathsf{H}')$ and $Sol^{\pi(n)}(\mathcal{C}') \neq \varnothing$ then $(\mathcal{P}', \mathcal{C}', \mathsf{H}') \in \Gamma(n)$.

2. for all $(\mathcal{P}, \mathcal{C}, p, \mathsf{H}) \in \Gamma$, $Sol^{\pi}(\mathcal{C}) \neq \varnothing$;

3. *All symbolic transitions are reflected in the tree:* if $(\mathcal{P}, \mathcal{C}, \mathsf{H}) \overset{\alpha}{\Rightarrow}_{\mathsf{s}} (\mathcal{P}', \mathcal{C}', \mathsf{H}')$ and $(\Sigma, \sigma) \in Sol^{\pi(n)}(\mathcal{C}')$ then there exists an edge $n \overset{\alpha}{\to} n'$ in T such that $(\mathcal{P}', \mathcal{C}', \mathsf{H}') \in \Gamma(n')$ and $(\Sigma', \sigma) \in Sol^{\pi(n')}(\mathcal{C}')$ for some Σ' that coincides with Σ on $vars^2(n)$.

Moreover for all edges $n \overset{\alpha}{\to} n_c$ of T and $(\mathcal{P}_c, \mathcal{C}_c, \mathsf{H}_c) \in \Gamma(n_c)$:

4. *Predicates are refined along branches:* for all Σ, if Σ verifies $\pi(n_c)$ then it verifies $\pi(n)$.

5. *Nodes are maximal:* if $(\Sigma, \sigma) \in Sol^{\pi(n)}(\mathcal{C})$, $(\Sigma_c, \sigma_c) \in Sol^{\pi(n_c)}(\mathcal{C}_c)$ and $\Sigma \subseteq \Sigma_c$, then $\Gamma(n_c)$ contains all symbolic processes $(\mathcal{P}', \mathcal{C}', \mathsf{H}')$ such that $(\mathcal{P}, \mathcal{C}, \mathsf{H}) \overset{\alpha}{\Rightarrow}_{\mathsf{s}} (\mathcal{P}', \mathcal{C}', \mathsf{H}')$ and, for some substitution σ', $(\Sigma_c, \sigma') \in Sol(\mathcal{C}')$ and $\Phi(\mathcal{C}_c)\sigma_c \sim \Phi(\mathcal{C}')\sigma'$.

The set of partition trees of P and Q is written $\mathsf{PTree}(P, Q)$.

The children of a node n represent all the symbolic processes that can be reached by one symbolic transition from the processes of n. This corresponds to Item 3 of the definition. Note that these children a grouped by symbolic processes that are statically equivalence following Definition 34 of a configuration. Note that Item 5 indicates that if there were other symbolic processes statically equivalent to one in a configuration, then they should appear in the same configuration. If we denote by $\mathcal{A}^{\ell}_{ext-}$ the set of actions $\mathcal{A}^{\ell}_{ext}$ minus the one of the form $\xi \sim \zeta$, we can generalize this property to trace in the following lemma.

Lemma 20 (Adapted from [CKR22, Lemma A.1])**.** Consider a partition tree $T \in \mathsf{PTree}(P, Q)$. Assume $(\mathcal{P}_1, \mathcal{C}_1, \mathsf{H}_1), \eta \overset{w}{\Rightarrow}_T (\mathcal{P}'_1, \mathcal{C}'_1, \mathsf{H}'_1), \eta'$ and $(\mathcal{P}_2, \mathcal{C}_2, \mathsf{H}_2) \overset{w}{\Rightarrow}_{\mathsf{s}} (\mathcal{P}'_2, \mathcal{C}'_2, \mathsf{H}'_2)$ with $(\mathcal{P}_2, \mathcal{C}_2, \mathsf{H}_2) \in \Gamma(\eta)$. For all solutions $(\Sigma', \sigma'_1) \in Sol^{\pi(\eta')}(\mathcal{C}'_1)$ and $(\Sigma', \sigma'_2) \in Sol^{\pi(\eta')}(\mathcal{C}'_2)$ such that $\Phi(\mathcal{C}'_1)\sigma'_1 \sim \Phi(\mathcal{C}'_2)\sigma'_2$, we have $(\mathcal{P}_2, \mathcal{C}_2, \mathsf{H}_2), \eta \overset{w}{\Rightarrow}_T (\mathcal{P}'_2, \mathcal{C}'_2, \mathsf{H}'_2), \eta'$.

Lemma 21 (Adapted from [CKR22, Lemma A.2])**.** Consider a partition tree $T \in \mathsf{PTree}(P, Q)$. Let η be a node of T and $(\mathcal{P}, \mathcal{C}, \mathsf{H}) \in \Gamma(\eta)$. If $(\mathcal{P}, \mathcal{C}, \mathsf{H}) \overset{w}{\Rightarrow}_{\mathsf{s}} (\mathcal{P}', \mathcal{C}', \mathsf{H}')$ and $(\Sigma, \sigma) \in Sol^{\pi(\eta)}(\mathcal{C}')$ then there exist a node η' and a substitution Σ' such that $(\mathcal{P}, \mathcal{C}, \mathsf{H}), \eta \overset{w}{\Rightarrow}_T (\mathcal{P}', \mathcal{C}', \mathsf{H}'), \eta'$ and $(\Sigma', \sigma) \in Sol^{\pi(\eta')}(\mathcal{C}')$.

These two lemmas allow us to prove our main theorem.

Theorem 1. Let $P, Q \in \mathcal{MP}^{<\infty}$ and $\doteq$ be defined by a subterm convergent destructor rewrite system. Trace preorder $(\{\!\{P\}\!\}, \varnothing) \leq_{tr} (\{\!\{Q\}\!\}, \varnothing)$ is decidable.

Proof. First, we show that we can restrict the set of traces we need to verify. In particular, it suffices to look at traces $w \in \mathcal{A}_{ext-}^{\ell\,*}$. In other words, we can *push* static equivalence tests towards the end of traces. Moreover, for all concrete traces w_1 not containing static equivalence tests, it suffices to check a finite number of concrete traces $w_2^1, \ldots, w_2^n$ built only on static equivalence tests. To do this, we use a proof technique similar to the proof in [CCD13] showing that trace equivalence and may testing coincide for processes with bounded number of sessions. Let us define the sets $S_P(w_1) = \{(\mathcal{P}', \phi', \mathsf{H}') \mid (\{\!\{P\}\!\}, \varnothing, []) \overset{w_1}{\Longrightarrow} (\mathcal{P}', \phi', \mathsf{H}')\}$ and $S_Q(w_1) = \{(\mathcal{P}', \phi', \mathsf{H}') \mid (\{\!\{Q\}\!\}, \varnothing, []) \overset{w_1}{\Longrightarrow} (\mathcal{P}', \phi', \mathsf{H}')\}$. Since P and Q are bounded processes, $S_P(w_1)$, $S_Q(w_1)$ and $(S_P(w_1) \cup S_Q(w_1))\backslash_\sim$ are finite (here $\sim$ refers to static equivalence of frames). Therefore, for all $(\mathcal{P}', \phi', \mathsf{H}') \in S_P(w_1) \cup S_Q(w_1)$, we can define a finite sequence of actions w_2 built only on actions of the form $\xi \doteq \zeta$ or $\xi \not\doteq \zeta$ that exactly defines the equivalence class of $(\mathcal{P}', \phi', \mathsf{H}')$ in $(S_P \cup S_Q)\backslash_\sim$, i.e., for all $(\mathcal{P}'', \phi'', \mathsf{H}'') \in S_P(w_1) \cup S_Q(w_1)$, $\phi' \sim \phi''$ if and only if $(\mathcal{P}'', \phi'', \mathsf{H}'') \overset{w_2}{\Longrightarrow} (\mathcal{P}'', \phi'', \mathsf{H}'')$. Thus, if we denote by W this set of traces sufficient for proving trace preorder, we have that $(\{\!\{P\}\!\}, \varnothing) \leq_{tr} (\{\!\{Q\}\!\}, \varnothing)$ if and only if for all $w \in W$, $\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\{\!\{P\}\!\}, \varnothing), w) \leq \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\{\!\{Q\}\!\}, \varnothing), w)$.

Second, thanks to procedure in [CKR18], we know that there exists a partition tree $T \in \mathsf{PTree}(P, Q)$. If we denote by $\mathsf{H}(S)$ the set of histories of the (symbolic) extended processes in S, we will show that

$$\forall w \in W, \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\{\!\{P\}\!\}, \varnothing), w) \leq \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\{\!\{Q\}\!\}, \varnothing), w)$$
$$\text{if and only if}$$
$$\forall \eta \in T, \mathsf{compute}(\mathsf{H}(\Gamma_P(\eta))) \leq \mathsf{compute}(\mathsf{H}(\Gamma_Q(\eta)))$$

To do so, it suffices to prove the following two properties and applying Lemma 18

- Soundness: $\forall \eta \in T$, $\exists w \in W$ s.t. $\mathsf{H}(S_P(w)) = \mathsf{H}(\Gamma_P(\eta))$ and $\mathsf{H}(S_Q(w)) = \mathsf{H}(\Gamma_Q(\eta))$
- Completeness: $\forall w \in W$, $\exists \eta \in T$ s.t. $\mathsf{H}(S_P(w)) = \mathsf{H}(\Gamma_P(\eta))$ and $\mathsf{H}(S_Q(w)) = \mathsf{H}(\Gamma_Q(\eta))$

Let us denote η_r the root of T. To prove the soundness, take $\eta \in T$ and $(\mathcal{P}, \mathcal{C}, \mathsf{H}) \in \Gamma(\eta)$. By definition, there exists w_s such that $(\{\!\{P\}\!\}, \mathcal{C}_\varnothing, []), \eta_r \overset{w_s}{\Longrightarrow}_T (\mathcal{P}, \mathcal{C}, \mathsf{H}), \eta$ or $(\{\!\{Q\}\!\}, \mathcal{C}_\varnothing, []), \eta_r \overset{w_s}{\Longrightarrow}_T (\mathcal{P}, \mathcal{C}, \mathsf{H}), \eta$. W.l.o.g., let us assume that $(\{\!\{P\}\!\}, \mathcal{C}_\varnothing, []), \eta_r \overset{w_s}{\Longrightarrow}_T (\mathcal{P}, \mathcal{C}, \mathsf{H}), \eta$.

1. By Item 2 of Definition 35, there exists $(\Sigma, \sigma) \in Sol^{\pi(\eta)}(\mathcal{C})$.

2. By Lemma 19, $(\{\!\{P\}\!\}, \varnothing, []) \xRightarrow{w_s\Sigma} (\mathcal{P}\sigma, \Phi(\mathcal{C})\sigma\!\downarrow, \mathsf{H})$.

3. By taking $w \in W$ such that $w_s\Sigma$ is a prefix of w, i.e. $w = w_s\Sigma{\cdot}w'$, and $(\mathcal{P}\sigma, \Phi(\mathcal{C})\sigma\!\downarrow, \mathsf{H}) \xRightarrow{w'} (\mathcal{P}\sigma, \Phi(\mathcal{C})\sigma\!\downarrow, \mathsf{H})$, i.e. w' is the witness for the static equivalence, we obtain that $\mathsf{H} \in \mathsf{H}(S_P(w))$.

4. By Item 2 of Definition 34, if $(\mathcal{P}_2, \mathcal{C}_2, \mathsf{H}_2) \in \Gamma(\eta)$ and $(\{\!\{P\}\!\}, \mathcal{C}_\varnothing, []), \eta_r \xRightarrow{w_s}_T (\mathcal{P}_2, \mathcal{C}_2, \mathsf{H}_2), \eta$ then there exists σ_2 such that $(\Sigma, \sigma_2) \in Sol^{\pi(\eta)}(\mathcal{C}_2)$ and $\Phi(\mathcal{C})\sigma \sim \Phi(\mathcal{C}_2)\sigma_2$. Therefore, by applying once again Lemma 19, we obtain that $\mathsf{H}_2 \in \mathsf{H}(S_P(w))$. Hence, $\mathsf{H}(\Gamma_P(\eta)) \subseteq \mathsf{H}(S_P(w))$.

It remains to show that $\mathsf{H}(S_P(w)) \subseteq \mathsf{H}(\Gamma_P(\eta))$: Take $(\{\!\{P\}\!\}, \varnothing, []) \xRightarrow{w} (Proc_2', \phi_2', \mathsf{H}_2)$.

1. By Lemma 19, there exists $(\{\!\{P\}\!\}, \mathcal{C}_\varnothing, []) \xRightarrow{w_s}_{\mathsf{s}} (\mathcal{P}_2, \mathcal{C}_2, \mathsf{H}_2)$ and $(\Sigma, \sigma_2) \in Sol^{\pi(\eta)}(\mathcal{C}_2)$ such that $\mathcal{P}_2\sigma_2 = \mathcal{P}_2'$ and $\Phi(\mathcal{C}_2)\sigma_2\!\downarrow = \phi_2'$.

2. By definition of w, $\Phi(\mathcal{C}_2)\sigma_2 \sim \Phi(\mathcal{C})\sigma$.

3. By Lemma 20, we deduce that $(Proc_2, \mathcal{C}_2, \mathsf{H}_2) \in \Gamma(\eta)$. Hence, $\mathsf{H}(S_P(w)) \subseteq \mathsf{H}(\Gamma_P(\eta))$.

Let us now prove the completeness property. Let $w \in W$. Thus, we can split $w = w_1w_2$ where $w_1 \in {\mathcal{A}^\ell_{ext-}}^*$ and w_2 only contain actions of the form $\xi \sim \zeta$. Thus, $(\{\!\{P\}\!\}, \varnothing, []) \xRightarrow{w_1} (\mathcal{P}', \phi', \mathsf{H})$.

1. By Lemma 19, there exists $(\{\!\{P\}\!\}, \mathcal{C}_\varnothing, []) \xRightarrow{w_s}_{\mathsf{s}} (\mathcal{P}, \mathcal{C}, \mathsf{H})$ and $(\Sigma, \sigma) \in Sol(\mathcal{C})$ such that $\mathcal{P}\sigma = \mathcal{P}'$ and $\Phi(\mathcal{C})\sigma\!\downarrow = \phi'$.

2. By Lemma 21, there exist a node η and a substitution Σ' such that $(\{\!\{P\}\!\}, \mathcal{C}_\varnothing, []), \eta_r \xRightarrow{w_s}_{\mathsf{s}} (\mathcal{P}, \mathcal{C}, \mathsf{H}), \eta$ and $(\Sigma', \sigma) \in Sol^{\pi(\eta)}(\mathcal{C})$. Thus, $\mathsf{H} \in \mathsf{H}(\Gamma_P(\eta))$. Moreover, we already shown that $\mathsf{H}(S_P(w_1\Sigma'w_2)) = \mathsf{H}(\Gamma_P(\eta))$.

3. Consider now $(\{\!\{P\}\!\}, \varnothing, []) \xRightarrow{w_1\Sigma w_2} (\mathcal{P}_2', \phi_2', \mathsf{H}_2)$. Once again by Lemma 19, there exists $(\{\!\{P\}\!\}, \mathcal{C}_\varnothing, []) \xRightarrow{w_s}_{\mathsf{s}} (\mathcal{P}_2, \mathcal{C}_2, \mathsf{H}_2)$ and σ_2 such that $\mathcal{P}_2\sigma_2 = \mathcal{P}'$ and $\Phi(\mathcal{C}_2)\sigma_2\!\downarrow = \phi_2'$. Moreover, by definition of w, $\phi_2' \sim \phi'$.

4. Notice that since $(\Sigma, \sigma) \in Sol(\mathcal{C})$ and $(\Sigma', \sigma) \in Sol(\mathcal{C})$, we deduce that for all $X \in dom(\Sigma)$, $X\Sigma\phi' = X\Sigma\phi'$. Hence $X\Sigma\phi_2' = X\Sigma\phi_2'$. This allows us to deduce that $(\{\!\{P\}\!\}, \varnothing, []) \xRightarrow{w_1\Sigma'w_2} (\mathcal{P}_2', \phi_2', \mathsf{H}_2)$ and so $\mathsf{H}(S_P(w_1\Sigma w_2)) \subseteq \mathsf{H}(S_P(w_1\Sigma' w_2))$. With similar arguments, we can show that $\mathsf{H}(S_P(w_1\Sigma' w_2)) \subseteq \mathsf{H}(S_P(w_1\Sigma w_2))$ and so $\mathsf{H}(S_P(w)) = \mathsf{H}(\Gamma_P(\eta))$. □

As a direct corollary we obtain that we can decide determinate may testing for purely probabilistic processes as it coincides with trace equivalence.

Corollary 2. Let $P, Q \in \mathcal{MP}^{\mathsf{pp}}$ and $\doteq$ be defined by a subterm convergent destructor rewrite system. Determinate may testing preorder $(\{\!\{P\}\!\}, \varnothing) \leq_{d\text{-}may} (\{\!\{Q\}\!\}, \varnothing)$ is decidable.

We have implemented the procedure described above in the DeepSec tool. The input language has been extended with a probabilistic choice operator $+_p$ where p is a real number in $]0,1[$. When trace equivalence between 2 processes is queried, the tool uses the above procedure for verification. The development is available on DeepSec's official github repository at [**?**].

As we will see in Section 9, we can use DeepSec to show that the dining cryptographers protocol does not provide anonymity when coins are *biased*.

9 An example: dining cryptographers

In this section, we look at how our formalism behave on a very standard of probabilistic protocol: dining cryptographers.

9.1 Dining cryptographers, in probabilistic pi-calculus.

Notation 12. For $b, b' \in \{0,1\}$, we note $b \oplus b'$ for b xor b'. (And similarly for the syntactic construction xor in the terms grammar).

We split the definition of the protocol in several component. The first step is to model the fact that two adjacent cryptographers can throw a dice, and obtain a probabilistic information bit that will be known only by them. We model this by the *oracle process* below (the two channels c_l and c_r model the pair of agents that throws the dice).

Definition 36 (Oracle process)**.** We define a process, which is indexed by two communication channels c_l and c_r, as follows:

$$O_{c_l,c_r} := (\mathsf{out}(c_l,0) \mid \mathsf{out}(c_r,0)) +_{1/2} (\mathsf{out}(c_l,1) \mid \mathsf{out}(c_r,1))$$

We now define the process that correspond to *one* agent: this process is indexed by three channels–a channel c_l for communicating with the oracle placed to his right, a channel c_r for communicating with the oracle placed to his right, and a (public) channel c for sending its final answer. It also depends on whether the agent has payed or not, which we model by a Boolean b.

Definition 37 (Agent process)**.** For every Boolean b, we define a process indexed by three communication channels c_l, c_r and c, as follows:

$$A_{c_l,c_r,c}(b) := \mathsf{in}(c_r,x_r);\mathsf{in}(c_l,x_l);\mathsf{out}(c, x_l \oplus x_r \oplus b).$$

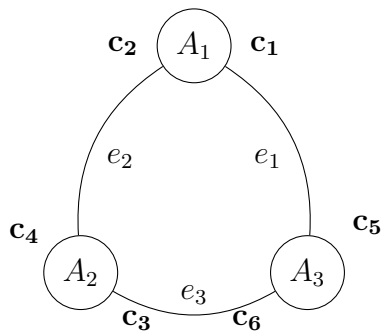
We are now ready to define the whole system: we put three agents, and their corresponding oracles, in parallel. Please notice that the channels used to communicate with the oracles are hidden from the adversary, thus binded by new , while the channels used by the agents to communicate their final results are free.

In order to be able to give a *compact* presentation of this system, we use a three-vertices graph. As represented in the graph below, we need to be able to talk about three families of elements:

- the set of agents (or *vertices*), that we note $\mathcal{A} = \{a_1, a_2, a_3\}$. (We take those to be public names, this way we can identify an agent with the (public) channel they use for returning their final result);
- the set of oracles (or *edges*), that we note $\mathcal{E} = \{e_1, e_2, e_3\}$;
- the set of (private) channels that allow the oracle to communicate their random bit to a pair of agent. We note this set $\mathcal{C} = \{\mathbf{c_1}, ..., \mathbf{c_n}\}$.

Notation 13. As represented on the figure below, we can associate at each vertex a pair of channel–the first element being the channel on its left, and the second the channel on its right; and similarly to each edge (i.e to each oracle). Reversely, we can associate to each channel both a vertex and an edge. We formalise this by two functions $c : \mathcal{A} \cup \mathcal{E} \to \mathcal{C} \times \mathcal{C}$, and $e : \mathcal{C} \to E$, $a : \mathcal{C} \to A$ (we note $c.l$ and $c.r$ for the first and second projection of c respectively).

Similarly, for any pair of distinct edges $e_1, e_2 \in \mathcal{E}$, we note $a(e_1 \& e_2)$ for their (unique) common vertex, and $a(e_1 \setminus e_2)$, for the (unique) vertex that belongs in e_1 but not in e_2.



We are now ready to define a process that represents the whole protocol.

Notation 14. If $P_1, \dots P_n$ is a family of processes, we note $||_{i \in \{1,\dots,n\}} P_i$ for the process $P_1 \mid \dots \mid P_n$.

Definition 38. Let $B : \mathcal{A} \to \{0, 1\}$ a Boolean-valued function giving the secret bit for each participant $a \in \mathcal{A}$.

$$DC_B := \mathsf{new}\ (c_1, \dots, c_n) \left(||_{e \in \mathcal{E}}\ O_{c_l(e), c_r(e)}\ \mid ||_{a \in \mathcal{A}}\ A_{c_l(a), c_r(a), a}(B(a)) \right)$$

Notation 15. We call 1-*weighted* those valuation functions $B : \mathcal{A} \to \{0, 1\}$ such that $\mathrm{card}(B^{-1}(\{1\})) = 1$. We write $\mathcal{W}_1$ for the set of all such functions.

Notation 16. In order to analyse the evolution of DC, we need a few notation for sub-processes:

1. First, we introduce a notation for the part of DC that has not changed: for $\mathcal{E}' \subseteq E$, and $\mathcal{A}' \subseteq \mathcal{A}$, we note:

$$P^B_{\mathcal{E}', \mathcal{A}'} = ||_{e \in \mathcal{E}'}\ O_{c_l(e), c_r(e)}\ \mid ||_{a \in \mathcal{A}'}\ A_{c_l(a), c_r(a), a}(B(a)).$$

2. the next notation is for the oracle sub-processes that have already done their probabilistic choice: for $\mathcal{E}' \subseteq \mathcal{E}$, an assignment function $f : \mathcal{E}' \to \{0,1\}$, and a set of *already fired* pairs $L \subseteq (\mathcal{E}' \times \{l, r\})$:

$$O^1_{\mathcal{E}',f,L} = ||_{(e,i)\notin L} \ (\mathsf{out}(c_i(e), f(e))).$$

3. We now look at how evolve the participants sub-processes. First, we introduce a notation for the participants that have done exactly one input: for $\mathcal{A}' \subseteq \mathcal{A}$, and $f : \mathcal{A}' \to \{0,1\}$, we note:

$$C^1_{\mathcal{A}',f} = ||_{a\in\mathcal{A}'} \ \mathsf{in}(c_l(a), x_l); \mathsf{out}(a, f(a) \oplus x_r \oplus B(a));$$

4. finally, we look at the participants that have already done two inputs, but that have still to communicate their final result. For $\mathcal{A}' \subseteq \mathcal{A}$, and $f_1, f_2 : \mathcal{A}' \to \{0,1\}$, we note:

$$C^2_{\mathcal{A}',f_1,f_2} = ||_{a\in\mathcal{A}'} \ \mathsf{out}(a, f_1(a) \oplus f_2(a) \oplus B(a))$$

By abuse of notation, we will note for example O^0_f instead of $O^0_{\mathcal{E}',f}$, since it is possible to recover the domain $\mathcal{E}'$ from the function f.

Observe that $DC_B = \mathsf{new}\ (c_1, \ldots, c_n) P^B_{\mathcal{E},\mathcal{A}}$.

9.2 Labelled semantics for the dining cryptographers protocol

Our goal is to show the following security property: for every two functions $B, B' : \mathcal{A} \to \{0,1\}$ such that $\mathrm{card}(i \mid C(i) = 1) = 1$ for $C = B, B'$, it holds that DC_B and $DC_{B'}$ are weakly bisimilar.

Unfortunately, the labelled semantics for DC is quite complicated: in particular, since we do not enforce a particular order for the communications between the oracles O_i and the participants A_i, we have both probabilistic and non-deterministic behaviour. As a consequence, it is difficult to prove equivalence directly in the LMP for the labelled semantics. To solve this problem, we define an auxiliary *simplified* LMP N_{DC}, and from there:

- We show that N_{DC} is weakly bisimilar to the LMP for the labelled semantics;
- We show that the states corresponding to DC_B and $DC_{B'}$ in N_{DC} are bisimilar in N_{DC}.

As a first step, we formalise an intuitive notion of *relevant steps* in the execution of the protocol, that we call *events*. The event $e[\leftarrow b]$ means that the oracle $e \in \mathcal{E}$ is *sampling* the Boolean $b \in \{0,1\}$. The event $a[\rightarrow b]$ means that the participant $a \in A$ is *outputting* the Boolean b. For technical reason, we separate internal events, that corresponds to probabilistic choice, to external events, that correspond to a participant outputting its result.

Definition 39. We define sets of *internal events* and *external events*, that we note Λ and Λ^{ext} respectively, as :

$$\Lambda := \{e[\leftarrow b] \mid e \in \mathcal{E}, b \in \{0,1\}\}$$
$$\Lambda^{ext} := \{a[\rightarrow b] \mid a \in \mathcal{A}, b \in \{0,1\}\}.$$

An *history* h is a pair (s,l), where s is a set of internal events in Λ such that no edge $e \in \mathcal{E}$ occurs two times in s, and l is a list of external events in Λ^{ext} such that no participant $a \in \mathcal{A}$ occurs two times in l.

Notation 17. To each history $h = (s,l)$, we associate a frame ϕ_h defined as: if $l = (a_1[\rightarrow b_1], \dots a_n[\rightarrow b_n])$, we take $\phi_h := \{\mathsf{ax}_1 = b_1, \dots \mathsf{ax}_n = b_n\}$.
For $e \in \mathcal{E}$, and $h = (s,l)$ an history, we note $e \in l$ when there exists a Boolean b such that $e[\leftarrow b] \in s$, and $e \notin h$ when there exists no such b. We define similarly $a \in h$ and $a \notin h$ for $a \in \mathcal{A}$. We will write $dom_{\mathcal{A}}(h) := \{a \in \mathcal{A} \mid a \in h\}$, and similarly $dom_{\mathcal{E}}(h) := \{e \in \mathcal{E} \mid e \in h\}$ Moreover, by abuse of notation, we will note s for $h = (s, \epsilon)$, and also l for $h = (\varnothing, l)$.

Definition 40. We define a NPLTS $\mathsf{N}_{DC} = (\mathcal{S}_{DC}, \mathcal{A}_{DC}, \mathsf{trans}_{DC})$ as follows:

- its sets are the pairs (h, B), where $B : \mathcal{A} \to \{0,1\}$, and h is an history.
- its set of action coincides with the one of N^{ℓ}, i.e.$\{\tau\} \cup \mathcal{A}^{\ell}_{ext}$
- its transition function trans_{DC} is defined as:

  $((s,l),B) \xrightarrow{\tau} \frac{1}{2} \cdot \delta_{(s \cup (e[\leftarrow 0],l),B)} + \frac{1}{2} \cdot \delta_{(s \cup (e[\leftarrow 1],l),B)}$ when $e \notin s$

  $((s,l),B) \xrightarrow{\mathsf{out}(b,a)} \delta_{(s,l::(a[\rightarrow b]),B)}$ when $a \notin l, \exists b_l, b_r \in \{0,1\}, e_l(a)[\leftarrow b_l] \in s \wedge e_r(a)[\leftarrow b_r] \in s$
  $\wedge\, b = b_r \oplus b_l \oplus B(a)$

  $(h,B) \xrightarrow{(\xi \stackrel{?}{=} \zeta)} \delta_{(h,B)}$ when $vars(\xi,\zeta) \subseteq dom(\phi_h) \wedge \xi(\phi_h) \sim \zeta(\phi_h)$

  $(h,B) \xrightarrow{(\xi \stackrel{?}{\neq} \zeta)} \delta_{(h,B)}$ when $vars(\xi,\zeta) \subseteq dom(\phi_h) \wedge \xi(\phi_h) \not\sim \zeta(\phi_h)$.

  where ϕ_0 is the initial empty frame.

Notation 18. In order to simplify the notations below, we introduce the following notation: if $\mathcal{A}'$ is a finite set, and list $= a_1, \dots, a_n$ is an enumeration of $\mathcal{A}'$, we define order(list) as the total order relation generated by $a_i \leq a_{i+1}$. Observe that, with the notation above, an *history* is entirely characterised by giving the data $(dom_{\mathcal{E}}(h), v_{\mathcal{E}}(h), dom_{\mathcal{A}}(h), \leq_h, v_{\mathcal{A}}(h))$, where $v_{\mathcal{E}}(h) : dom_{\mathcal{E}}(h) \to \{0,1\}$, $\leq_h$ a (total) order relation on $dom_{\mathcal{A}}(h)$, and $v_{\mathcal{A}}(h) : dom_{\mathcal{A}}(h) \to \{0,1\}$

Proposition 13. There exists an NPLTS bisimulation R on $\mathsf{N}_{DC} \cup \mathsf{N}^{\ell}$ such that for every $B : \mathcal{A} \to \{0,1\}$, it holds that $(\epsilon, B)\, R\, (DC_B, \varnothing)$.

The next subsection is devoted to the proof of Proposition 13 above. More precisely, Proposition 13 is a direct corollary of Proposition 14, that will be shown at the end of the next sub-section.

9.3 N^ℓ and N_{DC} are bisimilar

As a first step, we replace N^ℓ by a new -determinization of it.

Notation 19. We write $\rightarrow_{\text{det}} \subseteq \mathcal{SP}_\ell \times \mathcal{SP}_\ell$ for the *non-probabilistic* τ-reduction relation on N^ℓ. That is, $(P, \phi) \rightarrow_{\text{det}} (Q, \psi)$ when $(P, \phi) \xrightarrow{\tau} \delta_{(Q,\psi)}$ in N^ℓ. Observe that no $\rightarrow_{\text{det}}$ step can change the frame, thus it also implies that $\phi = \psi$.

In order to handle more easily all the processes that can be reached during the execution of the protocol, we introduce the techinical notions of *interaction pair*: intuitively it encodes the information about the internal communications between oracles and participants.

Definition 41. We call *oracle interaction* a set of the form $S \subseteq \{(e, s) \mid e \in \mathcal{E}, s \in \{l, r\}$. We write I_O for the set of all oracle interactions. We write $\text{dom}(S)$ for all e such that $\exists s$, $(e, s) \in S$.

We call *participant interaction* an element of the form $T \subseteq \{(a, s) \mid a \in \mathcal{A}, s \in \{l, r, \rightarrow\}\}$. We write $\text{dom}(T)$ for the set of all a such that $\exists s$, $(a, s) \in T$. We say that such a participant is *valid* when for every $a \in \mathcal{A}$, $(a, l) \in T$ implies that also $(a, r) \in T$, and $(a, \rightarrow) \in T$ implies that both $(a, l), (a, r) \in T$. We write I_P for the sets of all valid participants interactions. We say that a pair $(S, T) \in I_O \times I_P$ is *matching*, and we note $S \triangleleft T$ when: $\forall (e, s) \in S, (a.s(e), \neg s) \in T$, and $\forall (a, s) \in T$ with $s \in \{l, r\}, (e.s(a), \neg s) \in S$ (where $\neg l = r$, and $\neg r = l$).

Notation 20. To every matching pair $S \triangleleft T$, and every function $f : \mathcal{E}' \rightarrow \{0, 1\}$ where $\text{dom}(S) \subseteq \mathcal{E}'$, and $B \in \mathcal{W}_1$, we can define uniquely the corresponding process and frame:

$$\begin{aligned} P(B, f, S \triangleleft T) :=& P^B_{\mathcal{E}\setminus\mathcal{E}', \mathcal{A}\setminus\text{dom}(T)} \mid O^1_{f,S} \mid C^1_{\{a\in\text{dom}(T) \mid (a,l)\notin T\}, (a\mapsto f(e.r(a)))} \\ & \mid C^2_{\{a\in\text{dom}(T) \mid (a,l)\in T, (a,\rightarrow)\notin T\}, (a\mapsto (f(e.r(a)), f(e.l(a))))} \end{aligned}$$

Observe that $P(B, f, S \triangleleft T)$ is exactly the process obtained by doing all oracle probabilistic choice as specified by f, and then the interaction between oracles and participants specified by $S \triangleleft T$. We can also observe that it does not matter–i.e. the resulting process is the same–in which order the interactions and the probabilistic choices are done, as long as they happens as specified by f and $S \triangleleft T$.

We first prove a caracterisation of matchings interaction pairs.

Lemma 22. Let $\eta : (e, s) \in \mathcal{E} \times \{l, r\} \mapsto (a.s(e), \neg s) \in \mathcal{A} \times \{l, r, \rightarrow\}$, and ξ the partial function defined as $\xi : (a, s) \in \mathcal{A} \times \{l, r, \rightarrow\} \mapsto (e.s(a), \neg s) \in \mathcal{E} \times \{l, r\}$ when $s \in \{l, r\}$. Then if S is an oracle interaction, and T a valid participant interaction, $S \triangleleft T$ is a valid interaction pair if and only if $\eta(S) \subseteq T$ and $\xi(T) = S$.

Proof. First, we can see that $\eta \circ \xi = \text{id}_{\mathcal{E}\times\{l,r\}}$, and moreover we can rewrite immediately the definition of matching pairs as: if S is an oracle interaction, and T a valid participant interaction, $S \triangleleft T$ is a valid interaction pair iff $\eta(S) \subseteq T$, and $\xi(T) \subseteq S$. We now prove the intended result.

- Suppose that $S \triangleleft T$ is an interaction pair. Observe that, since $\xi \circ \eta = \mathrm{id}_{\mathcal{E} \times \{l,r\}}$, we can deduce from the first inequality: $S = \xi(\eta(S)) \subseteq \xi(T)$, which is enough to conclude.

- Suppose that S is an oracle interaction, and T a valid participant interaction, such that $\eta(S) \subseteq T$, and $S = \xi(T)$. Then the result is immediate.

□

Observe that a causal order can be defined on the notions of *matching pairs*: we will write $S \triangleleft T \leq S' \triangleleft T'$ when the interaction defined in $S' \triangleleft T'$ can be obtained by internal communications (between oracles and participants) from the interaction defined in $S \triangleleft T$. We formalize this idea in the notation below.

Notation 21. We define a partial order $\leq$ on matching interaction pairs by: $(S \triangleleft T) \leq (S' \triangleleft T')$ when both $(S \triangleleft T)$ and $(S' \triangleleft T')$ are matching pairs in $I_O \times I_P$, and moreover $S \subseteq S'$, $T \subseteq T'$. We define $\leq^\tau$ by $(S \triangleleft T) \leq^\tau (S' \triangleleft T')$ when $(S \triangleleft T) \leq (S' \triangleleft T')$ and moreover there is no element of the form $(a, \rightarrow)$ in $T' \setminus T$.

Lemma 23. Let $B \in \mathcal{W}_1$, $f : \mathcal{E}_0 \rightarrow \{0,1\}$. Let $S \triangleleft T$ such that $\mathrm{dom}(S) \subseteq \mathcal{E}_0$. Then for every $S' \triangleleft T'$ with $\mathrm{dom}(S') \subseteq \mathcal{E}_0$ and $(S \triangleleft T) \leq^\tau (S' \triangleleft T')$, it holds that for every frame ϕ, $P(B, f, S \triangleleft T), \phi \rightarrow^\star_{det} P(B, f, S' \triangleleft T'), \phi$.

Proof. Let $S \triangleleft T$ be a matching interaction pair such that $\mathrm{dom}(S) \subseteq \mathcal{E}_0$ and $(S' \triangleleft T') \leq (S \triangleleft T)$. By definition of the preorder $\leq$ on interaction pairs, it means that $S' \subseteq S$, $T' \subseteq T$. So we note $n_S = \mathrm{card}(S \setminus S')$, and $n_T = \mathrm{card}(T \setminus T')$ respectively. We're going to do the proof by induction on $n_S + n_T$. First, observe that if $n = 0$, then $S = S'$, $T = T'$, and we obtain immediately the result. We now consider the induction case. Suppose that $n > 0$. Observe that, by definition of $\leq^\tau$, we know that there is no element of the form $(a, \leftarrow) \in T \setminus T'$.

- Suppose that there is an element of the form $(a, l) \in T \setminus T'$. We take $T'' = T \setminus \{a, l\}$. Since $(a, \leftarrow)$ is not in $T \setminus T'$, it cannot be in T either (that's because, since (a, l) is in $T \setminus T'$, it is not in T', thus by definition of valid participant interaction, $(a, \rightarrow) \notin T'$). From there, we see that $(a, \leftarrow) \notin T'' \subseteq T$, and thus T'' is again a valid participant interaction. We note $S'' = S \setminus \xi(a, l)$–observe that ξ is well-defined on this element. Using Lemma 22, we can check that $S'' \triangleleft T''$ is again a valid interaction pair: indeed $\eta(S'') = \eta(S) \setminus \{\eta(\xi(a, l)\} = \eta(S) \setminus \{a, l\} \subseteq T \setminus \{a, l\} = T''$, and $\xi(T'') = \xi(T) \setminus \{\xi(a, l)\} = S \setminus \{\xi(a, l)\} = S''$. So we obtain $(S' \triangleleft T') \leq^\tau (S'' \triangleleft T'')$, and we can apply the induction hypothesis to $S'' \triangleleft T''$, thus it holds that: $P(B, f, S' \triangleleft T'), \phi \rightarrow^\star_{det} P(B, f, S'' \triangleleft T''), \phi$. In order to conclude, it is enough to see that passing from $S'' \triangleleft T''$ to $S \triangleleft T$ correspond to doing a communication on the left channel for the participant a, and thus $P(B, f, S'' \triangleleft T''), \phi \rightarrow_{det} P(B, f, S \triangleleft T), \phi$.

- Suppose that there is no element of the form $(a, l) \in T \setminus T'$, but an element of the form $(a, r) \in T \setminus T'$. We take $T'' = T \setminus \{a, r\}$. Again, we can see that T'' is again a valid participant interaction. We note $S'' = S \setminus \xi(a, l)$–observe that ξ is

well-defined on this element. Using Lemma 22, we can check that $S'' \triangleleft T''$ is again a valid interaction pair. So we obtain $(S' \triangleleft T') \leq^{\tau} (S'' \triangleleft T'')$, and we can apply the induction hypothesis to $S'' \triangleleft T''$, thus it holds that: $P(B, f, S' \triangleleft T'), \phi \rightarrow^{\star}_{det} P(B, f, S'' \triangleleft T''), \phi$. In order to conclude, it is enough to see that passing from $S'' \triangleleft T''$ to $S \triangleleft T$ correspond to doing a communication on the right channel for the participant a, and thus $P(B, f, S'' \triangleleft T''), \phi \rightarrow_{det} P(B, f, S \triangleleft T), \phi$.

- Actually, there is no other cases: indeed, when we are not in one of the previous case, it means that $T = T'$. But we can also use Lemma 22, that tells us that $\xi(T) = S$, and $\xi(T') = S'$. It means that $T = T'$, and $S = S'$, thus $n = 0$.

□

Lemma 24. Let $B \in \mathcal{W}_1$, $f : \mathcal{E}' \rightarrow \{0, 1\}$. Let $S \triangleleft T$ such that $\mathrm{dom}(S) \subseteq \mathcal{E}'$. Then for every frame ϕ, $(P(B, f, S \triangleleft T), \phi) \xrightarrow{\mathsf{out}(b',a)} D$ if and only if:

1. $\{(a, l), (a, r)\} \subseteq dom(T)$, and $(a, \rightarrow) \notin dom(T)$.
2. $b' = B(a) \oplus f(e.l(a)) \oplus f(e.r(a))$ (Observe that item 1 implies that $e.l(a), e.r(a) \in S$ because T is valid, and $S \triangleleft T$ is a matching pair. Thus also $e.l(a), e.r(a) \in \mathcal{E}'$, and b is well-defined.)
3. $D = (P(B, f, S \triangleleft T'), \phi \cup \{\mathsf{ax}_{n+1} = b'\}$, where n is the length of the ϕ, and $T' := T \cup \{(a, \rightarrow)\}$.

Proof. Recall that by definition:

$$\begin{aligned} P(B, f, S \triangleleft T) :=& P^{B}_{\mathcal{E}\setminus\mathcal{E}',\mathcal{A}\setminus\mathrm{dom}(T)} \mid O^{1}_{f,S} \mid C^{1}_{\{a\in\mathrm{dom}(T)\mid(a,l)\notin T\},(a\mapsto f(e.r(a)))} \\ & \mid C^{2}_{\{a\in\mathrm{dom}(T)\mid(a,l)\in T,(a,\rightarrow)\notin T\},(a\mapsto(f(e.r(a)),f(e.l(a))))} \end{aligned}$$

Looking at how we defined the components O^1, C^1, C^2... in Notation 16, we see that the only part of $P(B, f, S \triangleleft T)$ that can do an output action is the C^2-component, i.e. :

$$P :=||_{\{a\in\mathrm{dom}(T)\mid(a,l)\in T,(a,\rightarrow)\notin T\}} \mathsf{out}(a, f(e.l(a)) \oplus f(e.r(a)) \oplus B(a))$$

We write Q for the non C^2-part of $P(B, f, S \triangleleft T)$, that is for the process such that $P(B, f, S \triangleleft T) = P \mid Q$.

- Suppose that $(P(B, f, S \triangleleft T), \phi) \xrightarrow{\mathsf{out}(b',a)} D$. It means that $D = \delta_{(P'|Q,\phi')}$, with $(P, \phi) \xrightarrow{\mathsf{out}(b',a)} \delta_{(P',\phi')}$. Looking at the shape of P, we see immediately from there that we must have $a \in \{a \in \mathrm{dom}(T) \mid (a, l) \in T, (a, \rightarrow) \notin T\}$. Moreover, since T is a valid participant interaction (by hypothesis), we can deduce from there that $a \in \{a \in \mathrm{dom}(T) \mid (a, l) \in T, (a, r) \in T, (a, \rightarrow) \notin T\}$, which is exactly item 1. Moreover–and again by looking at the shape of P, we see that the output b' must

be: $f(e.l(a)) \oplus f(e.r(a)) \oplus B(a)$: it is exactly item 1. We now look at the resulting process P': we see that it must be:

$$\begin{aligned} P' =& ||_{\{a' \in \mathrm{dom}(T) | (a',l) \in T, (a',\rightarrow) \notin T\} \setminus \{a\}} \mathsf{out}(a', f(e.l(a')) \oplus f(e.r(a')) \oplus B(a')) \\ =& C^2_{\{a' \in \mathrm{dom}(T) | (a',l) \in T, (a',\rightarrow) \notin T\} \setminus \{a\}, (a' \mapsto (f(e.r(a')), f(e.l(a'))))} \end{aligned}$$

Thus we see that $Q \mid P' = P(B, f, S \triangleleft T')$, with $T' = T \cup \{[(a, \rightarrow)]\}$–and we can check easily that $S \triangleleft T'$ is indeed a valid matching pair. Similarly, when we look at the frame ψ, we see that it must be $\psi = \phi \cup \{\mathsf{ax}_n = f(e.l(a)) \oplus f(e.r(a)) \oplus B(a)\}$, and that concludes the proof of item 3.

- Suppose that the conditions item 1, item 2 item 3 hold. Let $T' := T \cup \{(a, \rightarrow)\}$. We're going to show that $(P, \phi) \xrightarrow{\mathsf{out}(b',a)} D$. First, observe that by item 1, the subprocess $\mathsf{out}(a', f(e.l(a')) \oplus f(e.r(a')) \oplus B(a'))$ is in P. Then, by item 2, we see that $b' = \mathsf{out}(a', f(e.l(a')) \oplus f(e.r(a')) \oplus B(a'))$, so we can indeed do the action $\mathsf{out}(b', a)$ from P'. Finally, by item 3, we see that the target of this action is indeed D.

□

Notation 22. An history h is *compatible* with an interaction pair $S \triangleleft T$ when: $\mathrm{dom}(S) \subseteq \{e \mid e \in h\}$, and $\{(a \mid (a, \rightarrow) \in T\} = \{a \mid a \in h\}$. We note $(S \triangleleft T) \amalg h$ when it is the case.

In order to show our simulation result, we will need the following auxilliary lemma:

Lemma 25. Let $h = (s, l) \in \mathcal{H}$, and $S \triangleleft T$ an interaction matching pair compatible with h. Suppose that $e \notin h$. Then $h_0 := (s \cup [e \leftarrow 0], l)$, $h_1 := (s \cup [e \leftarrow 1], l)$ are both compatible with $S \triangleleft T$, and moreover:

$$P(B, v_{\mathcal{E}}(h), S \triangleleft T) \xrightarrow{\tau} \frac{1}{2} \cdot \delta_{P(B, v_{\mathcal{E}}(h_0), S \triangleleft T)} + \frac{1}{2} \cdot \delta_{P(B, v_{\mathcal{E}}(h_1), S \triangleleft T}.$$

Proof. We first show that for $i \in \{0, 1\}$, h_i is compatible with $S \triangleleft T$. Observe that $\mathrm{dom}(S) \subseteq \mathrm{dom}(_)\mathcal{E}(h) \subseteq \mathrm{dom}(_)\mathcal{E}(h_i)$, and $\{(a \mid (a, \rightarrow) \in T\} = dom_{\mathcal{A}}(h) = dom_{\mathcal{A}}(h_i)$, so $(S \triangleleft T) \amalg h_i$. We now look at the shape of $P(B, v_{\mathcal{E}}(h), S \triangleleft T)$: recall that

$$\begin{aligned} P(B, v_{\mathcal{E}}(h), S \triangleleft T) :=& P^B_{\mathcal{E} \setminus dom_{\mathcal{E}}(h), \mathcal{A} \setminus \mathrm{dom}(T)} \mid O^1_{v_{\mathcal{E}}, S} \mid C^1_{\{a \in \mathrm{dom}(T) | (a,l) \notin T\}, (a \mapsto v_{\mathcal{E}}(e.r(a)))} \\ & \mid C^2_{\{a \in \mathrm{dom}(T) | (a,l) \in T, (a,\rightarrow) \notin T\}, (a \mapsto (v_{\mathcal{E}}(e.r(a)), v_{\mathcal{E}}(e.l(a))))} \end{aligned}$$

We look at the part of the system that remain unchanged since the beginning of the execution, i.e. $P^B_{\mathcal{E} \setminus dom_{\mathcal{E}}(h), \mathcal{A} \setminus \mathrm{dom}(T)}$. Recall that:

$$P^B_{\mathcal{E} \setminus dom_{\mathcal{E}}(h), \mathcal{A} \setminus \mathrm{dom}(T)} = ||_{e \in \mathcal{E} \setminus dom_{\mathcal{E}}(h)} O_{c_l(e), c_r(e)} \mid ||_{a \in \mathcal{A} \setminus \mathrm{dom}(T)} A_{c_l(a), c_r(a), a}(B(a)).$$

Observe that, for every $e_0 \in \mathcal{E}$, $O_{c_l(e_0), c_r(e_0)} \rightarrow \frac{1}{2} \cdot \delta_{\mathsf{out}(c_l(e_0),0) | \mathsf{out}(c_r(e_0),0)} + \frac{1}{2} \cdot \delta_{\mathsf{out}(c_l(e_0),1) | \mathsf{out}(c_r(e_0),1)}$. From there, we can deduce, for every $e_0 \in \mathcal{E} \setminus dom_{\mathcal{E}}(h)$: $P^B_{\mathcal{E} \setminus dom_{\mathcal{E}}(h), \mathcal{A} \setminus \mathrm{dom}(T)} \rightarrow \frac{1}{2} \cdot \delta_{Q_0(e_0)} + \frac{1}{2} \cdot \delta_{Q_1(e_0)}$, where $Q_i(e_0) := P^B_{\mathcal{E} \setminus (dom_{\mathcal{E}}(h) \cup \{e_0\}), \mathcal{A} \setminus \mathrm{dom}(T)} \mid \mathsf{out}(c_l(e_0), 0) \mid \mathsf{out}(c_r(e_0), 0)$. Now,

observe that, for $i \in \{0,1\}$, $O^1_{v_{\mathcal{E}}(h),S} \mid \mathsf{out}(c_l(e_0),i) \mid \mathsf{out}(c_r(e_0),i) = O^1_{v_{\mathcal{E}}(h)+(e_0\mapsto i)}$. Now, putting everything together, we obtain, for every $e_0 \in \mathcal{E} \setminus dom_{\mathcal{E}}(h)$:

$$P(B, v_{\mathcal{E}}(h), S \triangleleft T) \to \frac{1}{2} \cdot \delta_{P(B,v_{\mathcal{E}}(h)+(e_0\mapsto 0),S\triangleleft T)} + \frac{1}{2} \cdot \delta_{P(B,v_{\mathcal{E}}(h)+(e_0\mapsto 1),S\triangleleft T)}.$$

And we can conclude by observing that $v_{\mathcal{E}}(h) + (e_0 \mapsto i) = v_{\mathcal{E}}(h_i)$ for $i \in \{0,1\}$. □

Definition 42. We define a binary relation $R \subseteq \mathcal{S}_{DC} \times \mathcal{S}_{\mathsf{N}^\ell}$. We are going to define R as $R = \cup_{h,B}\{(h,B)\} \times R^B_h \times \{\phi_h\}$, Let be $h \in \mathcal{H}$, and $B \in \mathcal{W}_1$. We first look at the case where no result is outputted (i.e. the only non-empty part of the history $h = (s,l)$ is the set of internal actions s). Recall that a $h \in \mathcal{H}$ is characterised by the data of $(\mathcal{E}', \mathcal{A}', \leq, f : \mathcal{E}' \to \{0,1\}, g : \mathcal{A}' \to \{0,1\})$, where all these objects are as in Notation 18. To build the R^B_h, we do a case disjunction on the respective cardinality of $\mathcal{A}'$ and $\mathcal{E}'$.

- if $\mathrm{card}(\mathcal{A}') = \mathrm{card}(\mathcal{E}') = 0$–that is, $h = \epsilon_{\mathcal{H}}$–we take $R^B_h = \{(DC_B, \phi)\} \cup \{(\mathsf{new}\ (c_p, \ldots, c_n).P^B_{\mathcal{E},\mathcal{A}}, \phi) \mid 1 > p \geq n\}$;
- $R^B_h = \{P(B, v, S \triangleleft T) \mid (S \triangleleft T \amalg h) \wedge (\forall a \in \mathcal{A}', g(a) = B(a) \oplus f(e.l(a)) \oplus f(e.r(a))) \wedge v = f\}$.

Lemma 26. Let be $B \in \mathcal{W}_1$, $h \in \mathcal{H}$. Suppose that $P \in S^B_h$.

- if $(h,B) \xrightarrow{\tau} D$. Then there exists h_1, h_2 with $D = \frac{1}{2} \cdot \delta_{(h_1,B)} + \frac{1}{2}\delta_{(h_2,B)}$, and $(P, \phi_h) \overset{\tau}{\Rightarrow} \frac{1}{2} \cdot \delta_{(P_1,\phi_{h_1})} + \frac{1}{2} \cdot \delta_{(P_2,\phi_{h_2})}$, with $P_i \in S^B_{h_i}$ for $i \in \{1,2\}$.
- if $(h,B) \xrightarrow{a} (h',B)$. Then $(P, \phi_h) \overset{a}{\Rightarrow} (P', \phi_{h'})$, and $P' \in S^B_{h'}$.

Proof.
- Suppose that $(h,B) \xrightarrow{\tau} D$. Looking at the definition of N_{DC}, we see that the only possible case for a τ action when the rule applied is: $((s,l),B) \xrightarrow{\tau} \frac{1}{2} \cdot \delta_{(s\cup(e[\leftarrow 0],l),B)} + \frac{1}{2} \cdot \delta_{(s\cup(e[\leftarrow 1],l),B)}$ when $e \notin s$, and $h = (s,l)$. So we take $h_1 = (s \cup (e[\leftarrow 0],l),B)$, and $h_2 = (s \cup (e[\leftarrow 0],l),B)$. Then we can conclude using Lemma 25 (and the fact that we have again $(S \triangleleft T) \amalg h_i)$ for $i \in \{0,1\}$).
- Suppose that $(h,B) \xrightarrow{a} (h',B)$, where a is an action testing frame equivalence. Then we see that $h' = h$. By design of N_{DC}, we can see that those actions match the ones in N^ℓ, and thus $(P,\phi_h) \xrightarrow{a} (P,\phi_h)$ (observe that this action depends only on ϕ_h, thus no guarantee on P are necessary). Since by hypothesis $(h,B)R(P,\phi_h)$, we can conclude;
- Suppose that $(h,B) \xrightarrow{a} (h',B)$, and a is not a testing frame action. By looking at how we defined N_{DC}, it means that the rule used was (with $h = (s,l)$): $(h,B) \xrightarrow{\mathsf{out}(b,a)} \delta_{(s,l::(a[\to b]),B)}$ and moreover the following conditions hold: $a \notin h$, $\exists b_l, b_r \in \{0,1\}, e_l(a)[\leftarrow b_l] \in s \wedge e_r(a)[\leftarrow b_r] \in s$ and $b = b_r \oplus b_l \oplus B(a)$. We note $f : \mathcal{E}' \to \{0,1\}$ and $g : \mathcal{A}' \to \{0,1\}$ for the two partial valuations functions associated to h. By definition of R, we know that P is of the form $P(B, f, S \triangleleft T)$

and moreover $(S \triangleleft T \amalg h)$ and $\forall a' \in \mathcal{A}', g(a') = B(a') \oplus f(e.l(a')) \oplus f(e.r(a')))$. Since $(S \triangleleft T \amalg h)$, we can see that $(a, \rightarrow) \notin T$. As a first step, we build a new matching interaction pair $S' \triangleleft T'$ compatible with h. To do that, we ensure that the participant a has received both its left and its right input: We take $S' = S \cup \{(e.r(a), l), (e.l(a), r)\}$, and $T' = T \cup \{(a, r), (a, l)\}$. We can easily check that T' is indeed a valid participant interaction, that $S' \triangleleft T'$ is a matching interaction pair, and that $(S' \triangleleft T') \amalg h$. Moreover, it is immediate by construction that $S \triangleleft T \leq S' \triangleleft T'$, (and also, by compatibility with h, in particular $\mathrm{dom}(S), \mathrm{dom}(S)' \subseteq E'$) and thus by Lemma 23 $P(B, f, S \triangleleft T) \rightarrow^{\star}_{det} P(B, f, S' \triangleleft T')$. From there, we obtain using Lemma 24 that $(P(B, f, S \triangleleft T), \phi_h) \xrightarrow{\mathsf{out}(b,a)} (P(B, F, S' \triangleleft T''), \phi_{h'})$ with $T'' = T' \cup \{(a, \rightarrow)$. Now, we can check easily that $(S' \triangleleft T'') \amalg h'$. It means that $(h', B)\, R\, (P(B, F, S' \triangleleft T''), \phi_{h'})$, which conclude the proof.

□

Lemma 27. Let $(h, B) \in \mathcal{H} \times \mathcal{W}_1$. Suppose that $P \in S^B_h$.

1. if $(P, \phi_h) \xrightarrow{\tau}_{det} (P', \phi')$, then $\phi' = \phi_{h'}$ and $P' \in S^B_h$;

2. if $(P, \phi_h) \xrightarrow{\tau} D$, and D is not a dirac distribution. Then there exists h_1, h_2, and P_1, P_2 with $P_1 \in S^B_{h_1}$, $P_2 \in S^B_{h_2}$ with $D = \frac{1}{2} \cdot \delta_{(P_1, \phi_{h_1})} + \frac{1}{2} \cdot \delta_{(P_2, \phi_{h_2})}$, and moreover $(h, B) \xrightarrow{\tau} \frac{1}{2} \cdot \delta_{(h_1, B)} + \frac{1}{2} \cdot \delta_{(h_2, B)}$;

3. $(P, \phi_h) \xrightarrow{a} D$, then there exists P', h' with $D = \delta_{(P', \phi_{h'})}$, $(h, B) \xrightarrow{a} (h', B)$, and $P' \in S^B_{h'}$.

Proof. Let be $P \in S^B_h$. Recall that a $h \in \mathcal{H}$ is characterised by the data of $(dom_{\mathcal{E}}(h), v_{\mathcal{E}}(h), dom_{\mathcal{A}}(h), \leq_h, v_{\mathcal{A}}(h))$, where all these objects are as in Notation 18. $P \in S^b_h$ means that there exists a valid interaction pair $S \triangleleft T$, and such that $(S \triangleleft T \amalg h)$, and $(\forall a \in dom_{\mathcal{A}}(h), v_{\mathcal{A}}(h)(a) = B(a) \oplus v_{\mathcal{E}}(h)(e.l(a)) \oplus v_{\mathcal{E}}(h)(e.r(a)))$, and moreover $P = P(B, v_{\mathcal{E}}(h), S \triangleleft T)$.

1. We look at all the possible *deterministic* τ actions from $(P(B, v_{\mathcal{E}}(h), S \triangleleft T), \phi_h)$: intuitively, those are the τ-steps that correspond to a communication between a participant and an oracle. Observe that when an oracle process throws its dice, i.e. does a probabilistic choice, it is not a deterministic τ-step. From there, we can see that all these deterministic τ-step reach a state of the form $(P(B, v_{\mathcal{E}}(h), S' \triangleleft T'), \phi_h)$, where $S' \triangleleft T'$ is a valid interaction pair compatible with the history h. From there, we see that $P(B, v_{\mathcal{E}}(h), S' \triangleleft T') \in S^B_h$.

2. Suppose now that $(P(B, v_{\mathcal{E}}(h), S \triangleleft T), \phi_h) \xrightarrow{\tau} D$, and D is not a dirac distribution. Looking at the definition of $P(B, v_{\mathcal{E}}(h), S \triangleleft T)$, we see that the only possible τ-step here is when some oracle process $e \notin dom_{\mathcal{E}}(h)$ does a probabilistic choice– i.e. throws its dice. It means that neither the frame, nor the history of internal communication $S \triangleleft T$ is modified: the only difference is that the partial valuation function is more defined. So we end up in the distribution over processes: $D =$

$\frac{1}{2} \cdot \delta_{(P(B,f_0,S \lhd T),\phi_h)} + \frac{1}{2} \cdot \delta_{(P(B,f_1,S \lhd T),\phi_h)}$, where $f_i = v_{\mathcal{E}}(h) + (e \mapsto i)$, where here $+$ represents the union of partial functions with disjoint domains. We now want to find $h_i \in \mathcal{H}$ such that $\phi_{h_i} = \phi_h$, and moreover $P(B, f_i, S \lhd T) \in S^B_{h_i}$. We define $h_i = h :: [e \leftarrow i]$. We need to show two things: (a) that $S \lhd T \amalg h_i$; that (b) that $(\forall a \in dom(h_i)_{\mathcal{A}}, v_{\mathcal{A}}(h_i)(a) = B(a) \oplus v_{\mathcal{E}}(h_i)(e.l(a)) \oplus v_{\mathcal{E}}(h_i)(e.r(a)))$; and (c) the partial function $v_{\mathcal{E}}(h_i)$ coincides with f_i. We can see immediately that a) holds, since $S \lhd T \amalg h$, and h_i extends h. We can see that b) holds by observing that $dom_{\mathcal{A}}(h_i) = dom_{\mathcal{A}}(h)$, and $v_{\mathcal{A}}(h_i) = v_{\mathcal{A}}(h)$. To conclude, we see that also c) holds–by construction of h_i and f_i.

3. Suppose now that $(P(B, v_{\mathcal{E}}(h), S \lhd T), \phi_h) \xrightarrow{\alpha} D$. Then, looking at the shape of the process $(P(B, v_{\mathcal{E}}(h), S \lhd T), \phi_h)$, we see that there are two options:

   - either α is a testing frame action; in that case $D = \delta_{(P(B,v_{\mathcal{E}}(h),S \lhd T),\phi_h)}$, and moreover the test specified by α is successful on the frame ϕ_h. From there, we see immediately that $(B, h) \xrightarrow{\alpha} \delta_{(B,h)}$;
   - or α is of the form $\alpha = \mathsf{out}(b, a)$, with $b \in \{0, 1\}$ and $a \in \mathcal{A}$. In that case–by Lemma 24–it means that $a \in domT$, $(a, l) \in T$, $(a, \rightarrow) \notin T$, and $b = B(a) \oplus v_{\mathcal{E}}(h)(e.l(a)) \oplus v_{\mathcal{E}}(h)(e.r(a))$, and moreover $D = \delta_{P(B,v_{\mathcal{E}}(h),S \lhd (T::[(a,\rightarrow)]),\phi_h \cup \{\mathsf{ax}_{n+1}=b\}}$, with n the length of ϕ_h. From $S \lhd T \amalg h$, we deduce that: $dom(S) \subseteq dom_{\mathcal{E}}(h)$, and $\{a \mid (a, \rightarrow) \in T\}$=$dom_{\mathcal{A}}(h)$. We are now ready to show that $(B, h) \xrightarrow{\mathsf{out}(b,a)} (B, h :: [a \rightarrow b])$–with $h :: [a \rightarrow b]$ is a shortcut for $(s, l :: [a \rightarrow b])$ when $h = (s, l)$. To do that, we need to check three requirements–that come from the definition of N_{DC}. (a) First, from $\{a \mid (a, \rightarrow) \in T\}$=$dom_{\mathcal{A}}(h)$ we deduce that $a \notin dom_{\mathcal{A}}(h)$. (b) Second, since $S \lhd T$ is a valid matching interaction pair $(a, l) \in T$ implies that also $(a, r) \in T$, and from $\{(a, l), (a, r)\} \subseteq dom(T)$ we obtain $\{e.l(a), e.r(a)\} \subseteq dom(S) \subseteq dom_{\mathcal{E}}(h)$. (c) Finally, by hypothesis we already know that $b = B(a) \oplus v_{\mathcal{E}}(h)(e.l(a)) \oplus v_{\mathcal{E}}(h)(e.l(a))$.. Now, to conclude, we need to check that $P(B, v_{\mathcal{E}}(h), S \lhd (T :: [(a, \rightarrow)]) \in S^B_{h::[a \rightarrow b]}$, and $\phi_{h::[a \rightarrow b]} = \phi_h \cup \{\mathsf{ax}_{n+1} = b\}$. It is easy to see that it is indeed the case, which ends the proof.

□

Proposition 14. The relation R of Definition 42 is a bisimulation on $\mathsf{N}_{DC} \sqcup \mathsf{N}^{\ell}$

Proof. It is a direct consequence of Lemmas 26 and 27. □

9.4 Security of the dining cryptographers protocol

Proposition 13 allows us to study the simple system N_{DC} instead of working directly with N^{ℓ}.

Proposition 15. Let $B, B' \in \mathcal{W}_1$. Then the N_{DC}-states $(\epsilon_{\mathcal{H}}, B)$ and $(\epsilon_{\mathcal{H}}, B')$ are bisimilar.

Proof. We fix $B, B' \in \mathcal{W}_1$. We build a relation R on N_{DC}-states that contains the pair $((\epsilon_{\mathcal{H}}, B), (\epsilon_{\mathcal{H}}, B'))$, and we show that it is a bisimulation. We use again the history characterisation of Notation 18, which tells us that $h = (s_h, l_h) \in \mathcal{H}$ is uniquely defined by giving l_h, and a set $\mathcal{F}_h \subseteq \mathcal{E}$ equiped with a function $f_h : \mathcal{F} \to \{0, 1\}$.

Our construction is as follows: the states (h, B) and (h', B') are connected by R when all the three following conditions hold:

1. $l_h = l_{h'}$, $\mathcal{F}_h = \mathcal{F}_{h'}$ (we will simply note them $\mathcal{F}$ below);
2. $\forall e_1, e_2 \in \mathcal{F}_h$, $e_1 \neq e_2$, it holds that $B(a) \oplus f(e_1) \oplus f(e_2) = B'(a) \oplus f'(e_1) \oplus f'(e_2)$, where $a = a(e_1 \& e_2)$ as in Notation 13.
3. $\forall e_1, e_2 \in \mathcal{F}_h$, $e_1 \neq e_2$, $(f(e_1) \oplus B(a_1)) \oplus (f(e_2) \oplus B(a_2)) = (f'(e_1) \oplus B'(a_1)) \oplus (f'(e_2) \oplus B'(a_2))$, where $a_1 = a(e_1 \setminus e_2)$ and $a_2 = a(e_2 \setminus e_1)$ as defined in Notation 13.

First, observe that $(\epsilon_{\mathcal{H}}, B)\, R\, (\epsilon_{\mathcal{H}}, B')$. Thus to show Proposition 15, it is enough to show that R is a bisimulation. Let $(t, t') \in R$, and $\alpha \in \mathcal{A}_{DC}$ such that $t \xrightarrow{\alpha} D$. We need to show that $t' \overset{\alpha}{\Rightarrow} D'$, and $D(\widehat{R})D'$. First, observe that since $(t, t') \in R$, we know that there exists s, s' set of internal events such that $t = ((s, l), B)$ and $s' = ((s', l), B')$. Moreover, we can see that s, s' have the same underlying subset of edges, i.e. s, s' are characterised by $f_s, f_{s'} : \mathcal{F} \subseteq \mathcal{E} \to \{0, 1\}$.

We do a case disjunction on the form of α; the only relevant cases are the ones mentionned in Definition 40.

- if α is of the form $(\xi \overset{?}{=} \zeta)$, or $(\xi \overset{?}{\neq} \zeta)$ we have immediately the result, because $\phi_h = \phi_{h'} = \phi_l$;
- if $\alpha = \mathsf{out}(b, a)$, then $D = \delta_{(s, l::(a[\to b]), B)}$, and $\exists b_l, b_r \in \{0, 1\}, e_l(a)[\leftarrow b_l] \in s \wedge e_r(a)[\leftarrow b_r] \in s$ and $b = b_r \oplus b_l \oplus B(a)$. Actually, with our history characterisation–from Notation 18–we have $b_l = f_s(e_l(a))$, $b_r = f_s(a_r(a))$. By condition (1), $\exists b'_l, b'_r \in \{0, 1\}, e_l(a)[\leftarrow b'_l] \in s \wedge e_r(a)[\leftarrow b'_r] \in s'$, and actually $b'_l = f_{s'}(e_l(a))$ and $b'_r = e_r(a))$. By condition (2), we also have $b = b'_r \oplus b'_l \oplus B'(a)$. From there, we obtain that $t' \xrightarrow{\alpha} \delta_{(s', l::(a[\to b]), B')}$. To conclude, we need to show that $(s, l :: (a[\to b]), B)\, R\, (s', l :: (a[\to b]), B')$, i.e that the requirements (1), (2) and (3) hold. We can do this easily in that case: on the one hand, the internal part of the history hasn't been changed by the action α. On the other hand, the external parts of the histories coincide for these two states: it is $l :: (a[\to b])$, so all the requirements hold.
- if $\alpha = \tau$, then $\exists e \notin \mathcal{F}$ such that $D = \frac{1}{2} \cdot \delta_{(s \cup (e[\leftarrow 0], l), B)} + \frac{1}{2} \cdot \delta_{(s \cup (e[\leftarrow 1], l), B)}$. In that case, we see that we can *replicate* this τ action on t', in the sense that (since $e \notin \mathcal{F}$) $t' \xrightarrow{\tau} D' := \frac{1}{2} \cdot \delta_{(s' \cup (e[\leftarrow 0], l), B')} + \frac{1}{2} \cdot \delta_{(s' \cup (e[\leftarrow 1], l), B')}$. For $b \in \{0, 1\}$, we note $u(b) = (s \cup (e[\leftarrow b], l), B)$ and $u'(b) = (s' \cup (e[\leftarrow b], l), B')$. Observe that in order to show that $D\widehat{R}D'$, it is enough to show either $(u(0)Ru'(0) \wedge u(1)Ru'(1))$ or $(u(0)Ru'(1) \wedge u(1)Ru'(0))$. First, we can immediately check that Condition (1) holds for all these pair of states. So it is enough to look at Conditions (2) and (3). Here, we do a case disjunction on the cardinality of $\mathcal{F}$–that here, can be 0,1 or 2:

- if $\mathrm{card}(\mathcal{F}) = 0$ (i.e. $s = s' = \varnothing$), then we can show that $(u(0)Ru'(0) \wedge u(1)Ru'(1))$. We do the proof that $u(0)Ru'(0)$ (the proof of $u(1)Ru'(1)$ is similar. Since $\mathrm{card}(\mathcal{F}) = 0$, the cardinal of the internal part of the history in the states $u(0$ and $u'(0)$ is 1: that means that the requirements (2) and (3) are empty, and we can conclude.
- if $\mathrm{card}(\mathcal{F}) = 1$, we note $\mathcal{F} = \{e_0\}$. We note a for the (uniquely defined) participant that belong to both e and e_0. We now do a case disjunction on the boolean $b_0 := (B(a) \oplus f(e_0)) \oplus (B'(a) \oplus f'(e_0))$. If $b_0 = 0$, we are going to show that $(u(0)Ru'(0) \wedge u(1)Ru'(1))$, and if $b_0 = 1$, we will show that $(u(0)Ru'(1) \wedge u(1)Ru'(0))$. We can deal with these two cases at the same time, by stating our new goal as:
$$\forall b \in \{0,1\},\ u(b)\, R\, u'(b \oplus b_0).$$
We fix $b \in \{0,1\}$. It means that we need to show Conditions (2) and (3) for $u(b)$ and $u'(b \oplus b_0)$:

  Cond (2): When we rewrite (2) in that case, we see that it boils down to: $B(a) \oplus f(e_0) \oplus b = B'(a) \oplus f'(e_0) \oplus (b \oplus b_0)$. We can write this equality equivalently as:
$$(B(a) \oplus f(e_0) \oplus b) \oplus (B'(a) \oplus f'(e_0) \oplus (b \oplus b_0)) = 0.$$
  Now, we are able to conclude using comutativity and associativity of $\oplus$ and the definition of b_0.

  Cond (3): When we rewrite (3) in that case, we see that it boils down to: $f(e_0) \oplus B(a_{e_0}) \oplus b \oplus B(a_e) = f'(e_0) \oplus B'(a_{e_0}) \oplus (b \oplus b_0) \oplus B'(a_e)$, with $a_{e_0} = a(e_0 \setminus e)$ and $a_e = a(e \setminus e_0)$. Recall that both B and B' are 1-weighted, so we have: $B(a) \oplus B(a_e) \oplus B(a_{e_0}) = 1 = B'(a) \oplus B'(a_e) \oplus B'(a_{e_0})$. From there, we can conclude as above.
- if $\mathrm{card}(\mathcal{F}) = 2$, then we note $\mathcal{F} = \{e_1, e_2\}$, and $a = a(e_1 \& e_2)$. Observe that since tRt', we know that $f(e_1) \oplus B(a_1) \oplus f(e_2) \oplus B(a_2) = f'(e_1) \oplus B'(a_1) \oplus f'(e_2) \oplus B'(a_2)$, with $a_1 = a(e_1 \setminus e_2)$, and $a_2 = a(e_2 \setminus e_1)$. Observe that this equality can be rewritten equivalently as: $f(e_1) \oplus B(a_1) \oplus f(e_2) \oplus B(a_2) \oplus f'(e_1) \oplus B'(a_1) \oplus f'(e_2) \oplus B'(a_2) = 0$, and thus also as $f(e_1) \oplus B(a_1) \oplus f'(e_1) \oplus B'(a_1) = f(e_2) \oplus B(a_2) \oplus f'(e_2) \oplus B'(a_2) := b_0$. We note b_0 for the resulting boolean. We are going to show:
$$\forall b \in \{0,1\},\ u(b)\, R\, u'(b \oplus b_0).$$
Observe that it is enough to check Conditions (2) and (3) on the pair of edges $\{e_1, e\}$ and $\{e_2, e\}$. (We already know that it works for $\{e_1, e_2\}$, since tRt'.) We do the proof for $\{e_1, e\}$ (it is similar for the other pair).

  Cond (2): We need to show: $B(\bar{a}) \oplus f(e_1) \oplus b = B'(\bar{a}) \oplus f'(e_1) \oplus (b \oplus b_0)$, where $\bar{a} = a(e_1 \& e)$. Observe–looking at the geometrical disposition of the edges, that $\bar{a} = a(e_1 \& e) = a(e_1 \setminus e_2) = a_1$. Thus we can rewrite our goal as: $B(a_1) \oplus f(e_1) \oplus b \oplus B'(a_1) \oplus f'(e_1) \oplus (b \oplus b_0) = 0$. From there, we can conclude using the fact that $b_0 = f(e_1) \oplus B(a_1) \oplus f'(e_1) \oplus B'(a_1)$.

Cond (3): We need to show that $(f(e_1) \oplus B(\underline{a})) \oplus b \oplus B(\bar{a})) = (f'(e_1) \oplus B'(\underline{a})) \oplus (b \oplus b_0 \oplus B'(\bar{a}))$, where $\underline{a} = a(e_1 \setminus e)$ and $\bar{a} = a(e \setminus e_1)$. First, we can connect the $\underline{a}, \bar{a}$ to the a, a_1, a_2 already defined, by noting: $\underline{a} = a(e_1 \setminus e) = a(e_1 \& e_2) = a$, and $\bar{a} = a(e \setminus e_1) = a(e \& e_2) = a(e_2 \setminus e_1) = a_2$. So we can rewrite our goal as:

$$(f(e_1) \oplus B(a)) \oplus b \oplus B(a_2)) \oplus (f'(e_1) \oplus B'(a)) \oplus (b \oplus b_0 \oplus B'(a_2)) = 0.$$

By hypothesis (i.e. tRt'), we know that Condition (2) holds for $\{e_1, e_2\}$, so we have: $B(a) \oplus f(e_1) \oplus f(e_2) = B'(a) \oplus f'(e_1) \oplus f'(e_2)$. We can rewrite that as: $B(a) \oplus B'(a) = f(e_1) \oplus f'(e_1) \oplus f(e_2) \oplus f'(e_2)$. Using this, we can rewrite our goal as:

$$f(e_1) \oplus B(a_2) \oplus f'(e_1) \oplus b_0 \oplus B'(a_2) \oplus (f(e_1) \oplus f'(e_1) \oplus f(e_2) \oplus f'(e_2)) = 0.$$

We can now simplify the equation above as:

$$B(a_2) \oplus b_0 \oplus B'(a_2) \oplus f(e_2) \oplus f'(e_2) = 0,$$

and finally we can conclude since by definition of b_0 we have: $b_0 = f(e_2) \oplus B(a_2) \oplus f'(e_2) \oplus B'(a_2)$.

□

Corollary 3 (Security for the dining cryptographers protocol)**.** Let $B, B' : \mathcal{A} \to \{0, 1\}$ two functions such that $\text{card}(B^{-1}(\{1\})) = \text{card}(B'^{-1}(\{1\})) = 1$. Then the states $s_B := (DC_B, \phi)$ and $s_{B'} := (DC'_B, \phi)$, with $\phi_0 := \{\mathsf{ax}_1 = a_1, \mathsf{ax}_2 = a_2, \mathsf{ax}_3 = a_3\}$ are bisimilar in N^ℓ.

Proof. Since we know by Proposition 15 that $t_B := ((\varnothing, \epsilon), B)$ and $t_{B'} = ((\varnothing, \epsilon), B')$ are bisimilar in N_{DC}, we also have $(t_B, t_{B'}) \in (\sim_{\mathsf{N}_{DC} \cup \mathsf{N}^\ell})$ (because N^ℓ and N_{DC} have disjoint state spaces). By proposition13, we also have $t_B \sim_{\mathsf{N}_{DC} \cup \mathsf{N}^\ell} s_B$, and $t_{B'} \sim_{\mathsf{N}_{DC} \cup \mathsf{N}^\ell} s_{B'}$. Since $\sim_{\mathsf{N}_{DC} \cup \mathsf{N}^\ell}$ is an equivalence relation, we can combine all this to obtain that $s_B \sim_{\mathsf{N}_{DC} \cup \mathsf{N}^\ell} s_{B'}$. From here (again because N^ℓ and N_{DC} have disjoint state spaces), we can conclude that $s_B \sim_{\mathsf{N}^\ell}, s_{B'}$. □

10 Conclusion and future work

11 Conclusion and future work

In this paper we introduced a framework to reason about indistinguishability properties, modelled as process equivalences, in symbolic models enhanced with probabilities. Defining such a framework turns out to rely on subtle technicalities such as the need for randomized schedulers, overlooked in previous attempts. In addition to solving technical problems,

we believe that randomized schedulers capture more faithfully the idea that one cannot predict how non-determinism is resolved. Randomized schedulers generalize the idea that a schedulers chooses a particular distribution among the ones available by allowing an arbitrary combination (in the convex hull) of the available distributions.

We define different, classical behavioral and labelled equivalences and show their precise relations. As usual in models mixing non-determinism and probabilities, the resulting equivalences may be considered as too strong: indeed arbitrary schedulers may leak the (private) probabilistic choices of the processes and give the attacker an unrealistically strong distinguishing power. Defining more restricted schedulers that are only allowed partial knowledge of the current state, such as in [CP10], is orthogonal to our work. We however believe that our work provides a convenient framework for defining such more fine-grained notions of schedulers and consider this an interesting direction for future work.

We therefore study two classes of protocols where this problem is avoided. First, we study protocols that do not make probabilistic choices, but allow the adversary to do so. This class of non-probabilistic protocols corresponds to the classical setting and captures all major case studies performed in the context of symbolic models. Our results highlight that the classical notion of may-testing, considered rather intuitive as it models an arbitrary attacker running in parallel, does not take into account attackers that make probabilistic choices. Interestingly, when bounding the number of sessions, (non-probabilistic) similarity exactly captures such probabilistic attackers and offers an attractive target for automated analysis. Second, we study a class of fully probabilistic protocols, also considered in [CSV17], and show that trace equivalence on such protocols coincides with may testing in the presence of a (syntactic) class of determinate attackers. One may indeed argue that determinacy removes artificial non-deterministic choices that the attacker could exploit and that correspond to unrealistic behaviors. When protocols can be expressed in the class of purely probabilistic processes, from a formal analysis point, it seems appealing to do so as it also simplifies the analysis.

We also show how deciding trace equivalence can be automated in the presence of probabilities. We propose a decision procedure that extends previous work by Cheval *el al* [CKR18] and implement this procedure in the DeepSec tool. Hence, we provide tool support for proving determinate may-testing on the class of purely probabilistic processes when the number of sessions is bounded and cryptographic primitives are modeled as a subterm destructor rewrite system. On more general classes of processes, our tool can be used for attack finding: disproving trace equivalence implies that may testing (and all stronger equivalences) does not hold either, therefore violating security properties stated as an equivalence.

Finally, we illustrate our framework by studying the well-known Dining Cryptographers protocol. We model the protocol and its anonymity property in the probabilistic applied π-calculus. Then, we use our framework to prove that anonymity holds, and demonstrate DeepSec's attack finding ability on a variant of the protocol that uses a biased coin.

Our work paves the road towards several future works, in addition to exploring restricted schedulers mentioned above. The insight that (purely possibilistic) similarity takes into account probabilistic adversaries (as it coincides with may testing) when the number

of sessions is bounded and protocols are non-deterministic motivates adding support for (bi)similarity in a tool such as DeepSec (which currently only verifies trace equivalence). A different direction going beyond the subclasses considered in this paper is to investigate restrictions of the scheduler (building, *e.g.*, on ideas from [CP10, AAPvR10]) in our framework to limit the adversary's power without restricting the class of protocols. Finally, a more prospective direction is the use of more quantitative equivalences, *i.e.*, distances between processes, that might be interesting to compare different protocols that try to achieve a same property.

Acknowledgements. We thank Alwen Tiu and the anonymous reviewers for their helpful comments and suggestions.

References

[AAPvR10] Mário S. Alvim, Miguel E. Andrés, Catuscia Palamidessi, and Peter van Rossum. Safe equivalences for security properties. In Cristian S. Calude and Vladimiro Sassone, editors, *Theoretical Computer Science - 6th IFIP TC 1/WG 2.2 International Conference, TCS 2010, Held as Part of WCC 2010, Brisbane, Australia, September 20-23, 2010. Proceedings*, volume 323 of *IFIP Advances in Information and Communication Technology*, pages 55–70. Springer, 2010.

[ABB+18] Alejandro Aguirre, Gilles Barthe, Lars Birkedal, Aleš Bizjak, Marco Gaboardi, and Deepak Garg. Relational reasoning for markov chains in a probabilistic guarded lambda calculus. In *European Symposium on Programming*, pages 214–241. Springer, Cham, 2018.

[ABF17] Martín Abadi, Bruno Blanchet, and Cédric Fournet. The applied pi calculus: Mobile values, new names, and secure communication. *Journal of the ACM (JACM)*, 2017.

[Ama16] Roberto Amadio. Operational methods in semantics, 2016.

[BBK17] Karthikeyan Bhargavan, Bruno Blanchet, and Nadim Kobeissi. Verified models and reference implementations for the tls 1.3 standard candidate. In *IEEE Symposium on Security and Privacy (SP 2017)*, pages 483–502. IEEE, 2017.

[BCSV18] Matthew S Bauer, Rohit Chadha, A Prasad Sistla, and Mahesh Viswanathan. Model checking indistinguishability of randomized security protocols. In *International Conference on Computer Aided Verification*, pages 117–135. Springer, 2018.

[BDH+18] David A. Basin, Jannik Dreier, Lucca Hirschi, Sasa Radomirovic, Ralf Sasse, and Vincent Stettler. A formal analysis of 5g authentication. In David Lie,

Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS'18)*, pages 1383–1396. ACM, 2018.

[Bla16] Bruno Blanchet. Modeling and verifying security protocols with the applied pi calculus and proverif. *Foundations and Trends in Privacy and Security*, 2016.

[BST21] David A. Basin, Ralf Sasse, and Jorge Toro-Pozo. The EMV standard: Break, fix, verify. In *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*, pages 1766–1781. IEEE, 2021.

[BSV19] Filippo Bonchi, Ana Sokolova, and Valeria Vignudelli. The theory of traces for systems with nondeterminism and probability. In *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–14. IEEE, 2019.

[Cas18] Valentina Castiglioni. Trace and testing metrics on nondeterministic probabilistic processes. In *Proceedings Combined 25th International Workshop on Expressiveness in Concurrency and 15th Workshop on Structural Operational Semantics and 15th Workshop on Structural Operational Semantics,(EXPRESS/SOS) 2018*, volume 276, pages 19–36, 2018.

[CC08] Hubert Comon-Lundh and Véronique Cortier. Computational soundness of observational equivalence. In Peng Ning, Paul F. Syverson, and Somesh Jha, editors, *Proceedings of the 2008 ACM Conference on Computer and Communications Security, CCS 2008, Alexandria, Virginia, USA, October 27-31, 2008*, pages 109–118. ACM, 2008.

[CCD13] Vincent Cheval, Véronique Cortier, and Stéphanie Delaune. Deciding equivalence-based properties using constraint solving. *Theor. Comput. Sci.*, 492:1–39, 2013.

[CGCD+20] Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, and Douglas Stebila. A formal security analysis of the signal messaging protocol. *Journal of Cryptology*, 33(4):1914–1983, 2020.

[Cha81] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–88, 1981.

[Cha88] David Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *J. Cryptol.*, 1(1):65–75, 1988.

[CHH+17] Cas Cremers, Marko Horvat, Jonathan Hoyland, Sam Scott, and Thyla van der Merwe. A comprehensive symbolic analysis of TLS 1.3. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1773–1788. ACM, 2017.

[CKR18] Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina. Deepsec: Deciding equivalence properties in security protocols - theory and practice. In *Proceedings of the 39th IEEE Symposium on Security and Privacy (S&P'18)*, pages 525–542, San Francisco, CA, USA, May 2018. IEEE Computer Society Press.

[CKR22] Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina. Deepsec: Deciding equivalence properties for security protocols - improved theory and practice. *CoRR*, abs/2211.03225, 2022.

[CKW10] Véronique Cortier, Steve Kremer, and Bogdan Warinschi. A survey of symbolic methods in computational analysis of cryptographic systems. *Journal of Automated Reasoning*, 46(3-4):225–259, April 2010.

[CP10] Konstantinos Chatzikokolakis and Catuscia Palamidessi. Making random choices invisible to the scheduler. *Inf. Comput.*, 208(6):694–715, 2010.

[CSV17] Rohit Chadha, A Prasad Sistla, and Mahesh Viswanathan. Verification of randomized security protocols. In *2017 32nd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–12. IEEE, 2017.

[Den05] Yuxin Deng. Axiomatisations and types for probabilistic and mobile processes. *École des Mines de Paris*, 2005.

[DVGHM09] Yuxin Deng, Rob Van Glabbeek, Matthew Hennessy, and Carroll Morgan. Testing finitary probabilistic processes. In *International Conference on Concurrency Theory*, pages 274–288. Springer, 2009.

[DY83] Danny Dolev and Andrew Chi-Chih Yao. On the security of public key protocols. *IEEE Trans. Inf. Theory*, 29(2):198–207, 1983.

[Eis17] Christian Georg Eisentraut. *Principles of Markov automata*. PhD thesis, Saarländische Universitäts-und Landesbibliothek, 2017.

[GF12] Maciej Gazda and Wan Fokkink. Modal logic and the approximation induction principle. *Mathematical Structures in Computer Science*, 22(2):175, 2012.

[GLPT07] Jean Goubault-Larrecq, Catuscia Palamidessi, and Angelo Troina. A probabilistic applied pi–calculus. In *Asian Symposium on Programming Languages and Systems*, pages 175–190. Springer, 2007.

[LSA14] Ugo Dal Lago, Davide Sangiorgi, and Michele Alberti. On coinductive equivalences for higher-order probabilistic functional programs. In Suresh Jagannathan and Peter Sewell, editors, *The 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '14, San Diego, CA, USA, January 20-21, 2014*, pages 297–308. ACM, 2014.

[MPW92] Robin Milner, Joachim Parrow, and David Walker. A calculus of mobile processes, I. *Inf. Comput.*, 100(1):1–40, 1992.

[PS07] Augusto Parma and Roberto Segala. Logical characterizations of bisimulations for discrete probabilistic systems. In *International Conference on Foundations of Software Science and Computational Structures*, pages 287–301. Springer, 2007.

[RR98] Michael K. Reiter and Aviel D. Rubin. Crowds: Anonymity for web transactions. *ACM Trans. Inf. Syst. Secur.*, 1(1):66–92, 1998.

[SL95] Roberto Segala and Nancy Lynch. Probabilistic simulations for probabilistic processes. *Nordic Journal of Computing*, 2(2):250–273, 1995.

[Sto02] Mariëlle Stoelinga. *Alea jacta est: verification of probabilistic, real-time and parametric systems*. PhD thesis, University of Nijmegen, the Netherlands, April 2002. Available via `http://www.soe.ucsc.edu/~marielle`.

[vG87] Rob J van Glabbeek. Bounded nondeterminism and the approximation induction principle in process algebra. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 336–347. Springer, 1987.

A Randomized and non-randomized resolutions coincide for may-testing

Lemma 28 (One-step derandomization)**.** Let $\mathsf{N} = (\mathcal{S}_\mathsf{N}, \mathcal{A}, \mathsf{trans}_\mathsf{N})$ be a NPLTS, such that $\mathsf{trans}_\mathsf{N}(s, \tau) = D$ implies that D has finite support. Let $\mathsf{R} = (\mathcal{S}_\mathsf{R}, \mathsf{corr}_\mathsf{R}, \mathsf{trans}_\mathsf{R}) \in \mathcal{R}_\mathsf{r}(\mathsf{N})$, and $s \in \mathcal{S}_\mathsf{R}$ an internal state. Let $(\tau, D) \in \mathcal{A}_{int} \times \mathcal{D}(\mathcal{S}_\mathsf{R})$ the R-transition step from s, i.e. $\mathsf{trans}_\mathsf{R}(s) = (\tau, D)$. We define the set of *possible de-randomizations* of $\beta = (s, \tau, D)$ as.

$$\begin{aligned}\Delta(\beta) = \{F \in \mathcal{D}(\mathcal{S}_\mathsf{R}) \mid & (\tau, \mathsf{corr}_\mathsf{R}(F)) \in \mathsf{trans}_\mathsf{N}(\mathsf{corr}_\mathsf{R}(s)),\\ & \mathsf{corr}_\mathsf{R} \text{ injective on } \mathrm{supp}(F),\\ & \mathrm{supp}(F) \subseteq \mathrm{supp}(D)\}\end{aligned}$$

Then the randomized transition step β can be expressed as the convex sum of de-randomized step, or more formally:

$$\exists \eta \in \mathcal{D}(\Delta(\beta)) \text{ s.t. } \sum_{F \in \Delta(\beta)} \eta(F) \cdot F = D.$$

Proof. By hypothesis, $\mathsf{R} \in \mathcal{R}_\mathsf{r}(\mathsf{N})$, thus there exists a distribution γ over $\mathsf{trans}_\mathsf{N}(\mathsf{corr}_\mathsf{R}(s))(\tau)$ such that $\mathsf{corr}_\mathsf{R}(D) = \sum_{E \in \mathsf{trans}_\mathsf{N}(\mathsf{corr}_\mathsf{R}(s))(\tau)} \gamma(E) \cdot E$. Recall that, for any $F \in \Delta(\beta)$, since corr_R is *injective* on the support of F, we can define $(\mathsf{corr}_\mathsf{R})^{-1}_{|\mathrm{supp}(F)}(t) \in \mathcal{S}_\mathsf{R}$, for any $t \in \mathcal{S}_\mathsf{N}$. We define, for $F \in \Delta(\beta) \subseteq \mathcal{D}(\mathcal{S}_\mathsf{R})$:

$$\eta(F) = \gamma(\mathsf{corr}_\mathsf{R}(F)) \cdot \prod_{s \in \mathrm{supp}(\mathsf{corr}_\mathsf{R}(F))} \frac{D((\mathsf{corr}_\mathsf{R})^{-1}_{|\mathrm{supp}(F)}(s))}{\mathsf{corr}_\mathsf{R}(D)(s)}.$$

Notice that $\mathrm{supp}(F) \subseteq \mathrm{supp}(D)$ implies $\mathrm{supp}(\mathsf{corr}_\mathsf{R}(F)) \subseteq \mathrm{supp}(\mathsf{corr}_\mathsf{R}(D))$, and so for all $s \in \mathrm{supp}(\mathsf{corr}_\mathsf{R}(F))$, $\mathsf{corr}_\mathsf{R}(D)(s) \neq 0$ which ensures that $\eta(D)$ is correctly defined.

- First, we check that η is indeed a distribution.

$$\begin{aligned}\sum_{F \in \Delta(\beta)} \eta(F) &= \sum_{F \in \Delta(\beta)} \gamma(\mathsf{corr}_\mathsf{R}(F)) \cdot \prod_{s \in \mathrm{supp}(\mathsf{corr}_\mathsf{R}(F))} \frac{D((\mathsf{corr}_\mathsf{R})^{-1}_{|\mathrm{supp}(F)}(s))}{\mathsf{corr}_\mathsf{R}(D)(s)}\\ &= \sum_{E \in \mathsf{trans}_\mathsf{N}(s)(\tau)} \gamma(E) \cdot \sum_{F \in \Delta(\beta) \mid \mathsf{corr}_\mathsf{R}(F) = E} \prod_{s \in \mathrm{supp}(\mathsf{corr}_\mathsf{R}(F))} \frac{D((\mathsf{corr}_\mathsf{R})^{-1}_{|\mathrm{supp}(F)}(s))}{\mathsf{corr}_\mathsf{R}(D)(s)}.\end{aligned}$$

  Recall that γ is a distribution over $\mathsf{trans}_\mathsf{N}(\mathsf{corr}_\mathsf{R}(s))(\tau)$. Hence, for all $E \in \mathsf{trans}_\mathsf{N}(\mathsf{corr}_\mathsf{R}(s))(\tau)$, $\gamma(E) \neq 0$ if and only if $E \in \mathrm{supp}(\gamma)$. Hence:

$$\sum_{F \in \Delta(\beta)} \eta(F) = \sum_{\substack{E \in \mathsf{trans}_\mathsf{N}(s)(\tau)\\ \cap\ \mathrm{supp}(\gamma)}} \gamma(E) \cdot \sum_{F \in \Delta(\beta) \mid \mathsf{corr}_\mathsf{R}(F) = E} \prod_{s \in \mathrm{supp}(\mathsf{corr}_\mathsf{R}(F))} \frac{D((\mathsf{corr}_\mathsf{R})^{-1}_{|\mathrm{supp}(F)}(s))}{\mathsf{corr}_\mathsf{R}(D)(s)}.$$

Observe that, given some $E \in \mathsf{trans_N}(s)(\tau) \cap \mathrm{supp}(\gamma)$, choosing some $F \in \Delta(\beta)$ such that $\mathsf{corr_R}(F) = E$ is equivalent to choosing, for every $s \in \mathrm{supp}(E)$, a *unique* $\widetilde{s} \in \mathcal{S}_\mathsf{R}$ such that $\mathsf{corr_R}(\widetilde{s}) = s$, and then to define $F = \sum_{s \in \mathrm{supp}(E)} E(s) \cdot \delta_{\widetilde{s}}$. Notice that by construction, we have $\mathsf{corr_R}$ injective on $\mathrm{supp}(F)$. Moreover, for all $v \in \mathrm{supp}(F)$, $\mathsf{corr_R}(v) \in \mathrm{supp}(E)$. Since $E \in \mathrm{supp}(\gamma)$ and $\mathsf{corr_R}(D) = \sum_{E \in \mathsf{trans_N}(\mathsf{corr_R}(s))(\tau)} \gamma(E) \cdot E$, we deduce that $\mathsf{corr_R}(v) \in \mathrm{supp}(\mathsf{corr_R}(D))$ and so $v \in \mathrm{supp}(D)$. This ensure that $F \in \Delta(\beta)$.

As a consequence, for $E \in \mathsf{trans_N}(s)(\tau) \cap \mathrm{supp}(\gamma)$:

$$\sum_{\substack{F \in \Delta(\beta) \\ |\mathsf{corr_R}(F) = E}} \prod_{s \in \mathrm{supp}(\mathsf{corr_R}(F))} \frac{D((\mathsf{corr_R})^{-1}_{|\mathrm{supp}(F)}(s))}{\mathsf{corr_R}(D)(s)} = \sum_{\substack{\phi : \mathrm{supp}(E) \mapsto \mathcal{S}_\mathsf{R} \\ |\forall u,\, \mathsf{corr_R}(\phi(u)) = u}} \prod_{s \in \mathrm{supp}(E)} \frac{D(\phi(s))}{\mathsf{corr_R}(D)(s)} \tag{3}$$

Recall that for all $E \in \mathrm{supp}(\gamma)$, for all $s \in \mathrm{supp}(E)$, $\mathsf{corr_R}(D)(s) \neq 0$ and $\mathsf{corr_R}(D)(s) = \sum_{u \in \mathsf{corr_R}^{-1}(\{s\})} D(u)$, and thus $u \in \mathsf{corr_R}^{-1}(\{s\}) \mapsto \frac{D(u)}{\mathsf{corr_R}(D)(s)} \in [0,1]$ is a distribution. From there, we can consider the *product distribution* for any (finite) set $\mathcal{S}_I = \{s_i \mid i \in I \wedge \mathsf{corr_R}(D)(s_i) \neq 0\} \subseteq \mathcal{S}_\mathsf{N}$ given as: $(u_i)_{i \in I} \in \prod_{i \in I} \mathsf{corr_R}^{-1}(\{s_i\}) \mapsto \prod_{i \in I} \frac{D(u_i)}{\mathsf{corr_R}(D)(s_i)}$. In particular, since this product distribution is indeed a distribution, it holds that:

$$\sum_{\substack{\phi : \mathcal{S}_I \mapsto \mathcal{S}_\mathsf{R} \\ |\forall u,\, \mathsf{corr_R}(\phi(u)) = u}} \prod_{s \in \mathcal{S}_I} \frac{D(\phi(s))}{\mathsf{corr_R}(D)(s)} = 1. \tag{4}$$

By taking $\mathcal{S}_I = \mathrm{supp}(E)$, (4) tells us that: $\sum_{\substack{\phi : \mathrm{supp}(E) \mapsto \mathcal{S}_\mathsf{R} \\ |\forall u,\, \mathsf{corr_R}(\phi(u)) = u}} \prod_{s \in \mathrm{supp}(E)} \frac{D(\phi(s))}{\mathsf{corr_R}(D)(s)} = 1$, and we can conclude from there.

- we want now to show that $\sum_{F \in \Delta(\beta)} \eta(F) \cdot F = D$. Let $t \in \mathcal{S}_\mathsf{R}$. By unfolding the definition of $\eta(F)$ and using the same reasoning as in the previous bullet point, we obtain:

$$\begin{aligned}
&\sum_{F \in \Delta(\beta)} \eta(F) \cdot F(t) \\
&= \sum_{F \in \Delta(\beta)} \gamma(\mathsf{corr_R}(F)) \cdot \prod_{s \in \mathrm{supp}(\mathsf{corr_R}(F))} \frac{D((\mathsf{corr_R})^{-1}_{|\mathrm{supp}(F)}(s))}{\mathsf{corr_R}(D)(s)} \cdot F(t) \\
&= \sum_{E \in \mathsf{trans_N}(s)(\tau)} \gamma(E) \cdot \sum_{\substack{\phi : \mathrm{supp}(E) \to \mathcal{S}_\mathsf{R} \\ |\forall u,\, \mathsf{corr_R}(\phi(u)) = u,\, t \in Im(\phi)}} \prod_{s \in \mathrm{supp}(E)} \frac{D(\phi(s))}{\mathsf{corr_R}(D)(s)} \cdot E(\phi^{-1}(t))
\end{aligned}$$

The last equality is obtain using the same reasoning as in the previous bullet point. Additionally, we restrict the function ϕ we consider by only taking the one where $t \in Im(\phi)$ (as $t \notin Im(\phi)$ would imply $F(t) = 0$). Also notice that $F(t) = E(\phi^{-1}(t))$.

Finally, since $\phi^{-1}(t) = \mathsf{corr}_{\mathsf{R}}(t)$, we obtain the following:

$$
\begin{aligned}
&\sum_{F \in \Delta(\beta)} \eta(F) \cdot F(t) \\
&= \sum_{E \in \mathsf{trans}_{\mathsf{N}}(s)(\tau)} \gamma(E) \cdot \sum_{\substack{\phi : \mathrm{supp}(E) \to \mathcal{S}_{\mathsf{R}} \\ |\forall u,\, \mathsf{corr}_{\mathsf{R}}(\phi(u)) = u, \\ \phi(\mathsf{corr}_{\mathsf{R}}(t)) = t}} \prod_{s \in \mathrm{supp}(E)} \frac{D(\phi(s))}{\mathsf{corr}_{\mathsf{R}}(D)(s)} \cdot E(\mathsf{corr}_{\mathsf{R}}(t)) \\
&= \sum_{E \in \mathsf{trans}_{\mathsf{N}}(s)(\tau)} \gamma(E) \cdot \Big(\sum_{\substack{\phi : \mathrm{supp}(E) \setminus \{\mathsf{corr}_{\mathsf{R}}(t)\} \to \mathcal{S}_{\mathsf{R}} \\ |\forall u,\, \mathsf{corr}_{\mathsf{R}}(\phi(u)) = u}} \prod_{s \in \mathrm{supp}(E) \setminus \{\mathsf{corr}_{\mathsf{R}}(t)\}} \frac{D(\phi(s))}{\mathsf{corr}_{\mathsf{R}}(D)(s)} \Big) \\
&\qquad\qquad \cdot \frac{D(t)}{\mathsf{corr}_{\mathsf{R}}(D)(\mathsf{corr}_{\mathsf{R}}(t))} \cdot E(\mathsf{corr}_{\mathsf{R}}(t)) \\
&= \sum_{E \in \mathsf{trans}_{\mathsf{N}}(s)(\tau)} \gamma(E) \cdot \frac{D(t)}{\mathsf{corr}_{\mathsf{R}}(D)(\mathsf{corr}_{\mathsf{R}}(t))} \cdot E(\mathsf{corr}_{\mathsf{R}}(t)) \text{ by } (4) \\
&= \frac{D(t)}{\mathsf{corr}_{\mathsf{R}}(D)(\mathsf{corr}_{\mathsf{R}}(t))} \cdot \mathsf{corr}_{\mathsf{R}}(D)(\mathsf{corr}_{\mathsf{R}}(t)) \text{ by hypothesis on } \gamma \\
&= D(t).
\end{aligned}
$$

□

Lemma 29 (finite steps derandomization)**.** Let N be a NPLTS defined by its transition function $\mathsf{trans}_{\mathsf{N}} : \mathcal{S}_{\mathsf{N}} \to \mathcal{A}_{int} \sqcup \mathcal{A}_{ext} \to \mathcal{P}(\mathcal{D}(\mathcal{S}_{\mathsf{N}}))$. Moreover, we ask N to be such that $\mathsf{trans}_{\mathsf{N}}(s, \tau) = D$ implies that D has finite support. For every set $\mathcal{T} \subseteq \mathcal{S}_{\mathsf{N}}$, for every randomized resolution $\mathsf{R} = (\mathcal{S}_{\mathsf{R}}, \mathsf{corr}_{\mathsf{R}}, \mathsf{trans}_{\mathsf{R}}) \in \mathcal{R}_{\mathsf{r}}(\mathsf{N})$, for every state $s \in \mathcal{S}_{\mathsf{R}}$, it holds that for every $n \in \mathbb{N}$:

$$
\begin{aligned}
\mathrm{RProb}^{\leq n}_{\mathsf{R}}(s, \mathsf{corr}^{-1}_{\mathsf{R}}(\mathcal{T})) \in \mathrm{conv}(\{&\mathrm{RProb}_{\mathsf{R}'}(s', \mathsf{corr}^{-1}_{\mathsf{R}'}(\mathcal{T})) \\
&\mid \mathsf{R}' = (\mathcal{S}_{\mathsf{R}'}, \mathsf{corr}_{\mathsf{R}'}, \mathsf{trans}_{\mathsf{R}'}) \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N}),\ \mathsf{corr}_{\mathsf{R}}(s) = \mathsf{corr}_{\mathsf{R}'}(s')\})
\end{aligned}
$$

Proof of Lemma 29. Let $\mathcal{T} \subseteq \mathcal{S}_{\mathsf{N}}$, and $\mathsf{R} = (\mathcal{S}_{\mathsf{R}}, \mathsf{corr}_{\mathsf{R}}, \mathsf{trans}_{\mathsf{R}}) \in \mathcal{R}_{\mathsf{r}}(\mathsf{N})$. We do the proof by induction on n:

- Base case $n = 0$: We define $\mathsf{R}_0 := (\mathcal{S}_{\mathsf{N}}, id, \mathsf{trans}_{\mathsf{R}_0})$, where id stands for the identity function, and all states in $\mathcal{S}_{\mathsf{N}}$ are external states such that $\mathsf{trans}_{\mathsf{R}_0}(u)(a) = \star$ for every $u \in \mathcal{S}_{\mathsf{N}}, a \in A_{ext}$. We can see immediately that $\mathsf{R}_0 \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N})$. Observe that $\mathrm{RProb}_{\mathsf{R}_0}(u, \mathcal{T}) = 1$ when $u \in \mathcal{T}$, and 0 otherwise. As a consequence, for $s \in \mathcal{S}_{\mathsf{R}}$, $\mathrm{RProb}^{\leq 0}_{\mathsf{R}}(s, \mathsf{corr}^{-1}_{\mathsf{R}}(\mathcal{T})) = \mathrm{RProb}_{\mathsf{R}_0}(s, \mathcal{T})$.

- Inductive step: We suppose that the result holds for $n \geq 0$. Let $s \in \mathcal{S}_{\mathsf{R}}$. We do a case disjunction on the first R-transition from s:

– if s is an external state or $s \in \mathsf{corr}_{\mathsf{R}}^{-1}(\mathcal{T})$ then $\mathrm{RProb}_{\mathsf{R}}^{\leq n+1}(s, \mathsf{corr}_{\mathsf{R}}^{-1}(\mathcal{T})) = \mathrm{RProb}_{\mathsf{R}}^{\leq 0}(s, \mathsf{corr}_{\mathsf{R}}^{-1}(\mathcal{T}))$ by definition. By applying the same reasoning as in the base case, the result holds;

– otherwise there exists a distribution $E \in \mathcal{D}(\mathcal{S}_{\mathsf{R}})$ such that $\mathsf{trans}_{\mathsf{R}}(s) = (\tau, E)$, with τ an internal action, and $\mathsf{corr}_{\mathsf{R}}(E) \in \mathrm{conv}(\mathsf{trans}_{\mathsf{N}}(\mathsf{corr}_{\mathsf{R}}(s))(\tau))$. For each $v \in \mathcal{S}_{\mathsf{N}}$, we define the set of *resolutions starting from* v as: $\mathcal{R}_{\mathsf{nr}}(\mathsf{N}, v) = \{(\mathsf{R}', w) \mid \mathsf{R}' = (\mathcal{S}_{\mathsf{R}'}, \mathsf{corr}_{\mathsf{R}'}, \mathsf{trans}_{\mathsf{R}'}) \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N}), w \in \mathcal{S}_{\mathsf{R}'}, \mathsf{corr}_{\mathsf{R}'}(w) = v\}$. By applying the induction hypothesis to the states in the support of E, we obtain that for all $t \in \mathrm{supp}(E)$ there exists a distribution $\Theta_t \in \mathcal{D}(\mathcal{R}_{\mathsf{nr}}(\mathsf{N}, \mathsf{corr}_{\mathsf{R}}(t)))$ such that:

$$\mathrm{RProb}_{\mathsf{R}}^{\leq n}(t, \mathsf{corr}_{\mathsf{R}}^{-1}(\mathcal{T})) = \sum_{(\mathsf{R}', u) \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N}, \mathsf{corr}_{\mathsf{R}}(t))} \Theta_t(\mathsf{R}', u) \cdot \mathrm{RProb}_{\mathsf{R}'}(u, \mathsf{corr}_{\mathsf{R}'}^{-1}(\mathcal{T})). \tag{5}$$

Observe that choosing, for every $t \in \mathrm{supp}(E)$, one non-randomized resolution starting from $\mathsf{corr}(t)$, i.e a $(\mathsf{R}_t, u_t) \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N}, \mathsf{corr}_{\mathsf{R}}(t))$, means choosing a function $f : t \in \mathrm{supp}(E) \mapsto (\mathsf{R}_t, u_t) \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N}, \mathsf{corr}_{\mathsf{R}}(t))$. We write $\mathcal{F}$ for the set of all those functions. Using the distributions Θ_t, we can built the *product distribution*, that compute the probability of choosing some $f \in \mathcal{F}$, when choosing each $f(t)$ with the probabilities specified by the distribution Θ_t. This way, we obtain $\Theta \in \mathcal{D}(\mathcal{F})$ defined as $\Theta(f) = \prod_{t \in \mathrm{supp}(E)} \Theta_t(f(t))$. Observe that, for any $t \in \mathrm{supp}(E)$, and $(\mathsf{R}', u) \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N}, \mathsf{corr}_{\mathsf{R}}(t))$, it holds that:

$$\Theta_t(\mathsf{R}', u) = \sum_{f \mid f(t) = (\mathsf{R}', u)} \Theta(f). \tag{6}$$

Moreover, by defining $\beta = (s, \tau, E)$ and using Lemma 28, we obtain the existence of a distribution $\eta \in \mathcal{D}(\Delta(\beta))$, with Δ defined in Lemma 28, such that:

$$\sum_{D \in \Delta(\beta)} \eta(D) \cdot D = E. \tag{7}$$

For every element $D \in \Delta(\beta)$, and any function $f : t \in \mathrm{supp}(E) \mapsto (\mathsf{R}_t, u_t) \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N}, \mathsf{corr}_{\mathsf{R}}(t))\}$, we build a non-randomized resolution $\mathsf{R}_{D,f}$ as:

* $\mathcal{S}_{\mathsf{R}_{D,f}} = \{s\} \sqcup \{\mathcal{S}_{\mathsf{R}_t} \mid t \in \mathrm{supp}(E),\ f(t) = (\mathsf{R}_t, u_t)\}$;
* the correspondance function $\mathsf{corr}_{\mathsf{R}_{D,f}}$ is defined as: $\mathsf{corr}_{\mathsf{R}_{D,f}}(u) = \mathsf{corr}_{\mathsf{R}_t}$ if $z \in \mathcal{S}_{\mathsf{R}_t}$, and $\mathsf{corr}_{\mathsf{R}_{D,f}}(s) = \mathsf{corr}(s)$;
* the transition function $\mathsf{trans}_{\mathsf{R}_{D,f}}$ is defined as: if $u \in \mathcal{S}_{\mathsf{R}_t}$, then $\mathsf{trans}_{\mathsf{R}_{D,f}}(u) = \mathsf{trans}_{\mathsf{R}_t}(u)$, and for all $u \in \mathcal{S}_{\mathsf{R}_{D,f}}$, $\mathsf{trans}_{\mathsf{R}_{D,f}}(s)(u) = D(t)$ when $\exists t \in \mathrm{supp}(E)$ such that $f(t) = (\mathsf{R}_t, u)$ for some R_t; and 0 otherwise.

We can easily check that $\mathsf{R}_{D,f} \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N})$: to do so, we need to use the fact that, by induction hypothesis, all the R_t given by f are in $\mathcal{R}_{\mathsf{nr}}(\mathsf{N})$, and the definition

of $\Delta(\beta)$ given in Lemma 28. In order to conclude, we are going to show:

$$\mathrm{RProb}^{\leq n+1}_{\mathsf{R}}(s, \mathsf{corr}^{-1}_{\mathsf{R}}(\mathcal{T})) = \sum_{\substack{D\in\Delta(\beta)\\ f\in\mathcal{F}}} \eta(D)\cdot\Theta(f)\cdot \mathrm{RProb}_{\mathsf{R}_{D,f}}(s, \mathsf{corr}^{-1}_{\mathsf{R}_{D,f}}(\mathcal{T})).$$

$$\begin{aligned}
&\mathrm{RProb}^{\leq n+1}_{\mathsf{R}}(s, \mathsf{corr}^{-1}_{\mathsf{R}}(\mathcal{T}))\\
&= \sum_{t\in\mathrm{supp}(E)} E(t)\cdot \mathrm{RProb}^{\leq n}_{\mathsf{R}}(t, \mathsf{corr}^{-1}_{\mathsf{R}}(\mathcal{T})) \text{ by Definition 7}\\
&= \sum_{t\in\mathrm{supp}(E)} E(t)\cdot \sum_{(\mathsf{R}',u)\in\mathcal{R}_{\mathsf{nr}}(\mathsf{N},\mathsf{corr}_{\mathsf{R}}(t))} \Theta_t(\mathsf{R}',u)\cdot \mathrm{RProb}_{\mathsf{R}'}(u, \mathsf{corr}^{-1}_{\mathsf{R}'}(\mathcal{T})) \text{ by (5)}\\
&= \sum_{t\in\mathrm{supp}(E)} \Big(\sum_{D\in\Delta(\beta)} \eta(D)\cdot D(t)\Big)\\
&\qquad\cdot \sum_{(\mathsf{R}',u)\in\mathcal{R}_{\mathsf{nr}}(\mathsf{N},\mathsf{corr}_{\mathsf{R}}(t))} \Big(\sum_{f|f(t)=(\mathsf{R}',u)} \Theta(f)\Big)\cdot \mathrm{RProb}_{\mathsf{R}'}(u, \mathsf{corr}^{-1}_{\mathsf{R}'}(\mathcal{T})) \text{ by (7) and (6)}\\
&= \sum_{\substack{D\in\Delta(\beta)\\ f\in\mathcal{F}}} \eta(D)\cdot\Theta(f)\cdot \sum_{t\in\mathrm{supp}(E)} D(t)\cdot \sum_{\substack{(\mathsf{R}',u)\in\mathcal{R}_{\mathsf{nr}}(\mathsf{N},\mathsf{corr}_{\mathsf{R}}(t))\\ |f(t)=(\mathsf{R}',u)}} \mathrm{RProb}_{\mathsf{R}'}(u, \mathsf{corr}^{-1}_{\mathsf{R}'}(\mathcal{T}))\\
&= \sum_{\substack{D\in\Delta(\beta)\\ f\in\mathcal{F}}} \eta(D)\cdot\Theta(f)\cdot \sum_{\substack{t\in\mathrm{supp}(E)\\ (\mathsf{R}',u)\in\mathcal{R}_{\mathsf{nr}}(\mathsf{N},\mathsf{corr}_{\mathsf{R}}(t))\\ |f(t)=(\mathsf{R}',u)}} D(t)\cdot \mathrm{RProb}_{\mathsf{R}'}(u, \mathsf{corr}^{-1}_{\mathsf{R}'}(\mathcal{T}))
\end{aligned}$$

By definition of $\mathsf{R}_{D,f}$, for all $t\in\mathrm{supp}(E)$ with $f(t)=(\mathsf{R}',u)$, we know that $\mathsf{trans}_{\mathsf{R}_{D,f}}(s)(u)=D(t)$, and for all other states $u\in\mathcal{S}_{\mathsf{R}_{f,D}}$, $\mathsf{trans}_{\mathsf{R}_{D,f}}(s)(u)=0$. Hence:

$$\begin{aligned}
&\mathrm{RProb}^{\leq n+1}_{\mathsf{R}}(s, \mathsf{corr}^{-1}_{\mathsf{R}}(\mathcal{T}))\\
&= \sum_{\substack{D\in\Delta(s,\tau,E)\\ f\in\mathcal{F}}} \eta(D)\cdot\Theta(f)\cdot \sum_{u\in\mathcal{S}_{\mathsf{R}_{D,f}}} \mathsf{trans}_{\mathsf{R}_{D,f}}(s)(u)\cdot \mathrm{RProb}_{\mathsf{R}_{D,f}}(u, \mathsf{corr}^{-1}_{\mathsf{R}_{D,f}}(\mathcal{T}))
\end{aligned}$$

Finally, $\mathrm{RProb}_{\mathsf{R}_{f,D}}(u, \mathsf{corr}^{-1}_{\mathsf{R}_{f,D}}(\mathcal{T})) = \lim_{n\to+\infty} \mathrm{RProb}^{\leq n}_{\mathsf{R}_{f,D}}(u, \mathsf{corr}^{-1}_{\mathsf{R}_{f,D}}(\mathcal{T}))$. With $\mathrm{supp}(\mathsf{trans}_{\mathsf{R}_{f,D}}(s))$ being finite, we deduce that:

$$\begin{aligned}
&\sum_{u\in\mathcal{S}_{\mathsf{R}_{D,f}}} \mathsf{trans}_{\mathsf{R}_{D,f}}(s)(u)\cdot \mathrm{RProb}_{\mathsf{R}_{D,f}}(u, \mathsf{corr}^{-1}_{\mathsf{R}_{D,f}}(\mathcal{T}))\\
&= \sum_{u\in\mathcal{S}_{\mathsf{R}_{D,f}}} \mathsf{trans}_{\mathsf{R}_{D,f}}(s)(u)\cdot \lim_{n\to+\infty} \mathrm{RProb}^{\leq n}_{\mathsf{R}_{D,f}}(u, \mathsf{corr}^{-1}_{\mathsf{R}_{D,f}}(\mathcal{T}))\\
&= \lim_{n\to+\infty} \sum_{u\in\mathcal{S}_{\mathsf{R}_{D,f}}} \mathsf{trans}_{\mathsf{R}_{D,f}}(s)(u)\cdot \mathrm{RProb}^{\leq n}_{\mathsf{R}_{D,f}}(u, \mathsf{corr}^{-1}_{\mathsf{R}_{D,f}}(\mathcal{T}))\\
&= \mathrm{RProb}_{\mathsf{R}_{D,f}}(s, \mathsf{corr}^{-1}_{\mathsf{R}_{D,f}}(\mathcal{T}))
\end{aligned}$$

We conclude that:

$$\mathrm{RProb}_{\mathsf{R}}^{\leq n+1}(s, \mathsf{corr}_{\mathsf{R}}^{-1}(\mathcal{T})) = \sum_{\substack{D \in \Delta(\beta) \\ f \in \mathcal{F}}} \eta(D) \cdot \Theta(f) \cdot \mathrm{RProb}_{\mathsf{R}_{D,f}}(s, \mathsf{corr}_{\mathsf{R}_{D,f}}^{-1}(\mathcal{T}))$$

□

Lemma 30. For all $\mathcal{P} \in \mathcal{MP}$, for all $c \in \mathcal{N}_{pub}$, $\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}^o}(\mathcal{P}, \downarrow c) = \mathrm{RProb}_{\mathcal{R}_{\mathsf{r}}^o}(\mathcal{P}, \downarrow c)$.

Proof. Since $\mathcal{R}_{\mathsf{nr}}^o \subset \mathcal{R}_{\mathsf{r}}^o$, we immediately have that $\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}^o}(\mathcal{P}, \downarrow c) \leq \mathrm{RProb}_{\mathcal{R}_{\mathsf{r}}^o}(\mathcal{P}, \downarrow c)$.

The reverse inequality follows by Lemma 29 (observe that the NPLTS N^o is indeed such that $\mathsf{trans}_{\mathsf{N}^o}(s, \tau) = D$ implies that D has finite support): for any resolution $\mathsf{R} \in \mathcal{R}_{\mathsf{r}}^o$, it holds that for every $n \in \mathbb{N}$

$$\mathrm{RProb}_{\mathsf{R}}^{\leq n}(\mathcal{P}, \downarrow c) \leq \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}^o}(\mathcal{P}, \downarrow c)$$

As a consequence:

$$\mathrm{RProb}_{\mathcal{R}_{\mathsf{r}}^o}(\mathcal{P}, \downarrow c) = \sup_{\mathsf{R} \in \mathcal{R}_{\mathsf{r}}^o} (\sup_{n \in \mathbb{N}}(\mathrm{RProb}_{\mathsf{R}}^{\leq n}(\mathcal{P}, \downarrow c)) \leq \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}^o}(\mathcal{P}, \downarrow c).$$

□

Proposition 1. The may testing preorder coincides for randomized and non-randomized resolutions:

$$\leq_{may}^{\mathcal{R}_{\mathsf{r}}^o} = \leq_{may}^{\mathcal{R}_{\mathsf{nr}}^o}$$

Proof. Direct from Lemma 30. □

B Appendix on trace equivalence

B.1 Randomized and non-randomized resolutions coincide for trace equivalence

Lemma 31. Let $\mathsf{N} = (\mathcal{S}_{\mathsf{N}}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_{\mathsf{N}})$ be a NPLTS, and $\mathsf{R} = (\mathcal{S}_{\mathsf{R}}, \mathsf{corr}_{\mathsf{R}}, \mathsf{trans}_{\mathsf{R}}) \in \mathcal{R}_{\mathsf{r}}(\mathsf{N})$. For $n \in \mathbb{N}$, $w \in {\mathcal{A}_{ext}}^*$ and $s \in \mathcal{S}_{\mathsf{R}}$, we define $\mathrm{Prob}_{\mathsf{R}}^n(s, w)$ as:

$$\mathrm{Prob}_{\mathsf{R}}^0(s, a.w) = 0$$
$$\mathrm{Prob}_{\mathsf{R}}^n(s, \epsilon) = 1$$
$$\mathrm{Prob}_{\mathsf{R}}^n(s, a.w) = \sum_{\substack{t \in \mathcal{S}_{\mathsf{R}} \\ \text{s.t. } \exists D \in \mathcal{D}(\mathcal{S}_{\mathsf{R}}), \mathsf{trans}_{\mathsf{R}}(t)(a) = D}} \mathrm{RProb}_{\mathsf{R}}^{\leq n-1}(s, \{t\}) \cdot \sum_{s' \in \mathrm{supp}(D)} D(s') \cdot \mathrm{Prob}_{\mathsf{R}}^{n-1}(s', w)$$

Then, for any $u \in \mathcal{S}_{\mathsf{N}}$, it holds that:

$$\mathrm{Prob}_{\mathcal{R}}(u, w) = \sup_{n \in \mathbb{N}} \sup_{\substack{\mathsf{R} = (\mathcal{S}_{\mathsf{R}}, \mathsf{corr}_{\mathsf{R}}, \mathsf{trans}_{\mathsf{R}}) \in \mathcal{R} \\ s \in \mathcal{S}_{\mathsf{R}} \text{ s.t. } \mathsf{corr}(s) = u}} \mathrm{Prob}_{\mathsf{R}}^n(s, w)$$

Proof. The proof is by induction on the length of w. $\square$

Here, we develop the tools to compute the trace success probability as reachability pribabilities on a new auxilliary NPLTS: the traces NPLTS N^{tr}, that we build from any NPLTS N. We first define a particular kind of NPLTS: a*probabilistic abstract rewriting system*(PARS) is a NPLTS with no external actions, and a unique internal action τ.

Definition 43. We say that a NPLTS N is a *probabilistic abstract rewriting system* when N has exactly one internal action τ, and no external action. When it is the case, we say that a N state s is a *normal form* when $\mathsf{trans}(s, \tau) = \varnothing$, i.e. no transition starts from s.

Definition 44. Let $\mathsf{N} = (\mathcal{S}_\mathsf{N}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_\mathsf{N})$ be a NPLTS. We define the PARS N^{tr} as follows: its states are $\{(s, w) \mid s \in \mathcal{S}_\mathsf{N},\ w \in \mathcal{A}^\star_{ext}\} \sqcup \{success\}$. The transition function $\rightarrow$ is defined as:

- $(s, w) \rightarrow_{\mathsf{N}^{tr}} (D, w)$ when $s \xrightarrow{\tau}_\mathsf{N} D$;
- $(s, aw) \rightarrow_{\mathsf{N}^{tr}} (D, w)$ when $s \xrightarrow{a}_\mathsf{N} D$;
- $(s, \epsilon) \rightarrow \delta_{success}$.

Observe that the normal forms of this PARS are: either the state *success*, or states of the form $(s, a.w)$, with $s \not\xrightarrow{a}$ and $s \not\xrightarrow{\tau}$.

Our goal is to prove that the trace equivalence can be computed directly in the PARS P^{tr}, instead of the labelled NPLTS N^{ℓ}. As a first step, we build a correspondence between N resolutions and N^{tr} resolutions. This correspondance consists actually of *two* operators: $\mathbf{C} : \mathcal{R}_\mathsf{r}(\mathsf{N}) \rightarrow \mathcal{R}_\mathsf{r}(\mathsf{N}^{tr})$ and $\mathbf{D} : \mathcal{R}_\mathsf{nr}(\mathsf{N}^{tr}) \rightarrow \mathcal{R}_\mathsf{nr}(\mathsf{N})$. Observe that, for technical reasons, the operator $\mathbf{D}$ can only be applied to non-randomized resolutions.

Definition 45. We define an operator $\mathbf{C} : \mathcal{R}_\mathsf{r}(\mathsf{N}) \rightarrow \mathcal{R}_\mathsf{r}(\mathsf{N}^{tr})$ as follows: let $\mathsf{R} = (\mathcal{S}_\mathsf{R}, \mathsf{corr}_\mathsf{R}, \mathsf{trans}_\mathsf{R}) \in \mathcal{R}_\mathsf{r}(\mathsf{N})$. We take $\mathbf{C}\mathsf{R} = (\mathcal{S}_{\mathbf{C}\mathsf{R}}, \mathsf{corr}_{\mathbf{C}\mathsf{R}}, \mathsf{trans}_{\mathbf{C}\mathsf{R}})$ where:

- $\mathcal{S}_{\mathbf{C}\mathsf{R}} = \{(s, w) \mid s \in \mathcal{S}_\mathsf{R}, w \in \mathcal{A}^\star_{ext}\} \sqcup \{success\}$;
- $\mathsf{corr}_{\mathbf{C}\mathsf{R}}(s, w) = (\mathsf{corr}_\mathsf{R}(s), w)$, and $\mathsf{corr}_{\mathbf{C}\mathsf{R}}(success) = success$;
- $\mathsf{trans}_{\mathbf{C}\mathsf{R}}(s, w)(\tau) = \begin{cases} (\mathsf{trans}_\mathsf{R}(s), w) \text{ if } s \text{ is an internal state in } \mathsf{R} \\ \delta_{success} \text{ if } s \text{ external state and } w = \epsilon \\ (\mathsf{trans}_\mathsf{R}(s)(a), w') \text{ when } w = a.w' \text{ and } \mathsf{trans}_\mathsf{R}(s)(a) \text{ is defined} \\ \text{ undefined otherwise.} \end{cases}$

Observe moreover that whenever R is a non-randomized resolution over N, $\mathbf{C}\mathsf{R}$ is a non-randomized resolution over N^{tr}.

Definition 46. We define an operator $\mathbf{D} : \mathcal{R}_\mathsf{nr}(\mathsf{N}^{tr}) \rightarrow \mathcal{R}_\mathsf{nr}(\mathsf{N})$ as follows: let $\mathsf{R} = (\mathcal{S}_\mathsf{R}, \mathsf{corr}_\mathsf{R}, \mathsf{trans}_\mathsf{R}) \in \mathcal{R}_\mathsf{r}(\mathsf{N}^{tr})$. We take $\mathbf{D}\mathsf{R} = (\mathcal{S}_\mathsf{R}, \mathsf{corr}_\mathsf{R}, \mathsf{trans}_{\mathbf{D}\mathsf{R}})$ where: $\mathsf{trans}_{\mathbf{D}\mathsf{R}} : \mathcal{S}_\mathsf{R} \times \mathcal{A}_\mathsf{N} \rightarrow \mathcal{D}(\mathcal{S}_\mathsf{R})$ is defined as:

- if $u \in \mathcal{S}_{\mathsf{R}}$ is such that $\mathsf{trans}_{\mathsf{R}}(u)(\tau)$ is undefined, then $\mathsf{trans}_{\mathsf{R}}(u)(a)$ is undefined for every $a \in \mathcal{A}_{ext} \cup \{\tau\}$;
- suppose now that $\mathsf{trans}_{\mathsf{R}}(u)(\tau) = D$. Since R is a non-randomized resolution, we can do the following cases disjunction:
  - either $u \in \mathcal{S}_{\mathsf{R}}$ is such that $\mathsf{corr}_{\mathsf{R}}(u) = (s, \epsilon)$, and $\mathsf{corr}_{\mathsf{R}}(D) = \delta_{success}$. Then we take $\mathsf{trans}_{\mathbf{DR}}(u)(a)$ as undefined for every $a \in \mathcal{A}_{ext} \cup \{\tau\}$;
  - or $u \in \mathcal{S}_{\mathsf{R}}$ is such that $\mathsf{corr}_{\mathsf{R}}(u) = (s, w)$, and $\mathsf{corr}_{\mathsf{R}}(D) = (E, w)$. Then we take $\mathsf{trans}_{\mathbf{DR}}(u)(\tau) = D$, and $\mathsf{trans}_{\mathbf{DR}}(u)(a)$ as undefined for every $a \in \mathcal{A}_{ext}$;
  - or $u \in \mathcal{S}_{\mathsf{R}}$ is such that $\mathsf{corr}_{\mathsf{R}}(u) = (s, a_0.w)$, and $\mathsf{corr}_{\mathsf{R}}(D) = (E, w)$. Then we take $\mathsf{trans}_{\mathbf{DR}}(u)(a_0) = D$, and $\mathsf{trans}_{\mathbf{DR}}(u)(a)$ as undefined for every $a \in \{\tau\} \cup (\mathcal{A}_{ext} \setminus \{a_0\})$.

Lemma 32. Let N a NPLTS, and $w \in \mathcal{A}_{ext}^{\star}$, . Then:

1. For every $\mathsf{R} \in \mathcal{R}_{\mathsf{r}}(\mathsf{N})$, and $s \in \mathcal{S}_{\mathsf{R}}$, $\mathrm{Prob}_{\mathsf{R}}(s, w) \leq \mathrm{RProb}_{\mathbf{CR}}((s, w), \mathsf{corr}_{\mathbf{CR}}^{-1}(success))$.
2. For every $\mathsf{R} \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{tr})$, and $s \in \mathcal{S}_{\mathsf{R}}$ such that there exists u, $\mathsf{corr}(s) = (u, w)$, it holds that $\mathrm{Prob}_{\mathbf{DR}}(s, w) \geq \mathrm{RProb}_{\mathsf{R}}(s, \mathsf{corr}_{\mathsf{R}}^{-1}(success))$.

Proof of item 1 in Lemma 32. Let us suppose $\mathsf{R} \in \mathcal{R}_{\mathsf{r}}(\mathsf{N})$, and $s \in \mathcal{S}_{\mathsf{R}}$. First, we can show easily by induction on n, that for all non-empty trace ω, for all states $t \in \mathcal{S}_{\mathsf{R}}, z \in \mathcal{S}_{\mathbf{CR}}$, it holds that:

$$\mathrm{RProb}_{\mathbf{CR}}^{\leq n}((t, w), \{z\}) = \begin{cases} \mathrm{RProb}_{\mathsf{R}}^{\leq n}(t, u) \text{ if } z = (u, w); \\ 0 \text{ if } \nexists u \text{ with } z = (u, w). \end{cases} \tag{8}$$

Now, observe that $\mathsf{corr}_{\mathbf{CR}}^{-1}(success) = \{success\}$. We use the limit-based caracterisation of trace success probability (see Lemma 31), and we obtain a rewriting of our goal–i.e. item 1 in Lemma 32–as the Equation (9) below:

$$\forall n \in \mathbb{N}, \mathrm{Prob}_{\mathsf{R}}^{n}(s, w) \leq \mathrm{RProb}_{\mathbf{CR}}((s, w), \{success\}); \tag{9}$$

Th proof of Equation 9 is by induction on length(w). If $w = \epsilon$, then $\mathrm{Prob}_{\mathsf{R}}^{n}(s, w) = 1$. Moreover, $\mathrm{RProb}_{\mathbf{CR}}((s, \epsilon), \{success\}) = 1$ since $\mathsf{trans}_{\mathbf{CR}}(s, \epsilon)(\tau) = \delta_{success}$, thus the result

holds. Suppose now that $w = a.w'$, and that Equation 9 holds for w'. Then:

$$
\begin{aligned}
&\mathrm{Prob}^n_{\mathsf{R}}(s, a.w') \\
&= \sum_{\substack{t \in \mathcal{S}_{\mathsf{R}} \\ \text{s.t. } \exists D \in \mathcal{D}(\mathcal{S}_{\mathsf{R}}), \\ \mathsf{trans}_{\mathsf{R}}(t)(a) = D}} \mathrm{RProb}^{\leq n}_{\mathsf{R}}(s, \{t\}) \cdot \sum_{s' \in \mathrm{supp}(D)} D(s') \cdot \mathrm{Prob}^n_{\mathsf{R}}(s', w') \text{ by Lemma 31} \\
&= \sum_{\substack{t \in \mathcal{S}_{\mathsf{R}} \\ \text{s.t. } \exists D \in \mathcal{D}(\mathcal{S}_{\mathsf{R}}), \\ \mathsf{trans}_{\mathsf{R}}(t)(a) = D}} \mathrm{RProb}^{\leq n}_{\mathbf{CR}}((s, a.w'), \{(t, a.w')\}) \cdot \sum_{s' \in \mathrm{supp}(D)} D(s') \cdot \mathrm{Prob}^n_{\mathsf{R}}(s', w') \\
&\leq \sum_{\substack{t \in \mathcal{S}_{\mathsf{R}} \\ \text{s.t. } \exists D \in \mathcal{D}(\mathcal{S}_{\mathsf{R}}), \\ \mathsf{trans}_{\mathsf{R}}(t)(a) = D}} \mathrm{RProb}^{\leq n}_{\mathbf{CR}}((s, a.w'), \{(t, a.w')\}) \cdot \sum_{s' \in \mathrm{supp}(D)} D(s') \cdot \mathrm{RProb}_{\mathbf{CR}}((s', w'), \{\mathit{success}\}) \text{ by HI;} \\
&= \sum_{\substack{u = (t, a.w') \in \mathcal{S}_{\mathbf{CR}} \\ \text{s.t. } \exists D \in \mathcal{D}(\mathcal{S}_{\mathbf{CR}}), \\ \mathsf{trans}_{\mathbf{CR}}(u)(\tau) = D}} \mathrm{RProb}^{\leq n}_{\mathbf{CR}}((s, a.w'), \{u\}) \cdot \sum_{v = (s', w') \in \mathrm{supp}(D)} D(v) \cdot \mathrm{RProb}_{\mathbf{CR}}(v, \{\mathit{success}\}) \\
&\leq \sum_{\substack{u = (t, a.w') \in \mathcal{S}_{\mathbf{CR}} \\ \text{s.t. } \exists D \in \mathcal{D}(\mathcal{S}_{\mathbf{CR}}), \\ \mathsf{trans}_{\mathbf{CR}}(u)(\tau) = D}} \mathrm{RProb}_{\mathbf{CR}}((s, a.w'), \{u\}) \cdot \sum_{v = (s', w') \in \mathrm{supp}(D)} D(v) \cdot \mathrm{RProb}_{\mathbf{CR}}(v, \{\mathit{success}\}) \\
&= \mathrm{RProb}_{\mathbf{CR}}((s, a.w'), \{\mathit{success}\})
\end{aligned}
$$

□

Proof of item 2 in Lemma 32. Let be $\mathsf{R} \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{tr})$, and $s \in \mathcal{S}_{\mathsf{R}}$ such that there exists u, $\mathsf{corr}_{\mathsf{R}}(s) = (u, w)$. First, observe that we can restate our goal as:

$$\mathrm{Prob}_{\mathbf{DR}}(s, w) \geq \mathrm{RProb}^{\leq n}_{\mathsf{R}}(s, \mathsf{corr}^{-1}_{\mathsf{R}}(\mathit{success})).$$

We do the proof by induction on n:

- $n = 0$: since by hypothesis $\mathsf{corr}_{\mathsf{R}}(s) = (u, w) \neq \mathit{success}$, it holds that $\mathrm{RProb}^{\leq 0}_{\mathsf{R}}(s, \mathsf{corr}^{-1}_{\mathsf{R}}(\mathit{success})) = 0$, thus the result holds;
- $n = 1$: looking at the way we define N^{tr}, we see that $\mathrm{RProb}^{\leq 1}_{\mathsf{R}}(s, \mathsf{corr}^{-1}_{\mathsf{R}}(\mathit{success})) > 0$ implies that $w = \epsilon$. When it is the case, $\mathrm{Prob}_{\mathbf{DR}}(s, w) = 1$, thus we can conclude;
- $n \to n + 1$ with $n > 0$: if $\mathrm{RProb}^{\leq n+1}_{\mathsf{R}}(s, \mathsf{corr}^{-1}_{\mathsf{R}}(\mathit{success})) = 0$, we have immediately

the result. Otherwise, it means that there exists D such that $s \to_{\mathsf{R}} D$, and:

$$\mathrm{RProb}_{\mathsf{R}}^{\leq n+1}(s, \mathsf{corr}_{\mathsf{R}}^{-1}(success)) = \sum_{s'} D(t) \cdot \mathrm{RProb}_{\mathsf{R}}^{\leq n}(s', \mathsf{corr}_{\mathsf{R}}^{-1}(success)) \tag{10}$$

$$= \sum_{s' | \mathsf{corr}_{\mathsf{R}}(s') = success} D(s') + \sum_{t | \exists u', w' \text{ s.t. } \mathsf{corr}_{\mathsf{R}}(s') = (u', w')} D(s') \cdot \mathrm{RProb}_{\mathsf{R}}^{\leq n}(s', \mathsf{corr}_{\mathsf{R}}^{-1}(success)) \tag{11}$$

$$\leq \sum_{s' | \mathsf{corr}_{\mathsf{R}}(t) = success} D(s') + \sum_{s' | \exists u', w' \text{ s.t. } \mathsf{corr}_{\mathsf{R}}(s') = (u', w')} D(s') \cdot \mathrm{Prob}_{\mathbf{DR}}(s', w') \qquad \text{by induction hyp.} \tag{12}$$

Looking at the way N^{tr} is defined, we do the following case disjunction on $s \to_{\mathsf{R}} D$:

1. either $w = \epsilon$. In that case, we see that $\mathrm{Prob}_{\mathbf{DR}}(s, w) = \mathrm{Prob}_{\mathbf{DR}}(s, w) = 1$, and we can conclude.
2. or $w = a.w_1$. In that case, $\sum_{s' | \mathsf{corr}_{\mathsf{R}}(t) = success} D(s') = 0$, and using the fact that R is a non-randomized distrubution, it holds that:
   - either $D = (E, w)$ with $E \in \mathcal{D}(\mathcal{S}_{\mathsf{N}})$, and $u \xrightarrow{\tau}_{\mathsf{N}} E$; In that case, looking at the definition of the operator $\mathbf{D}$, we see that $s \xrightarrow{\tau}_{\mathbf{DR}} D$. From there, we can rewrite Equation (12) as: $\mathrm{RProb}_{\mathsf{R}}^{\leq n+1}(s, \mathsf{corr}_{\mathsf{R}}^{-1}(success)) \leq \sum_{s'} D(s') \cdot \mathrm{Prob}_{\mathbf{DR}}(s', w) = \sum_{s'} (\mathsf{trans}_{\mathbf{DR}}(s)(\tau))(s') \cdot \mathrm{Prob}_{\mathbf{DR}}(s', w)$, and we can conclude by looking at how we defined the probability of doing a trace.
   - or $D = (E, w_1)$ whith $u \xrightarrow{a}_{\mathsf{N}} E$; in that case, looking at the definition of the operator $\mathbf{D}$, we see that $s \xrightarrow{a}_{\mathbf{DR}} D$. From there, we can conclude as in the previous case.

□

Lemma 33. Let $\mathsf{N} = (\mathcal{S}_{\mathsf{N}}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_{\mathsf{N}})$ be a NPLTS. Let be $s \in \mathcal{S}_{\mathsf{N}}$, and $w \in \mathcal{A}_{ext}^{\star}$.

1. Randomized case:

   $$\mathrm{Prob}_{\mathcal{R}_{\mathsf{r}}(\mathsf{N})}(s, w) \leq \sup\{\mathrm{RProb}_{\mathsf{R}}(s', \mathsf{corr}_{\mathsf{R}}^{-1}(success)) \text{ s.t. } \mathsf{R} \in \mathcal{R}_{\mathsf{r}}(\mathsf{N}^{tr}), s' \in \mathcal{S}_{\mathsf{R}}\, \mathsf{corr}_{\mathsf{R}}(s') = (s, w)\}.$$

2. Non-randomized case:

   $$\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N})}(s, w) = \sup\{\mathrm{RProb}_{\mathsf{R}}(s', \mathsf{corr}_{\mathsf{R}}^{-1}(success)) \text{ s.t. } \mathsf{R} \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{tr}), s' \in \mathcal{S}_{\mathsf{R}}\, \mathsf{corr}_{\mathsf{R}}(s') = (s, w)\}$$

Proof. We do the proof using Lemma 32: let us fix $s \in \mathcal{S}_{\mathsf{N}}$.

- Using (the first part of) Lemma 32, we see that for every $\mathsf{R} \in \mathcal{R}_{\mathsf{r}}(\mathsf{N})$, and $s' \in \mathcal{S}_{\mathsf{R}}$ with $\mathsf{corr}_{\mathsf{R}}(s') = s$, it holds that $\mathrm{Prob}_{\mathsf{R}}(s', w) \leq \mathrm{RProb}_{\mathbf{CR}}((s', w), \mathsf{corr}_{\mathbf{CR}}^{-1}(success))$. From there, we can see that $\mathrm{Prob}_{\mathsf{R}}(s', w) \leq \sup_{\mathsf{R}' \in \mathcal{R}_{\mathsf{r}}(\mathsf{N}^{tr}), u \in \mathcal{S}_{\mathsf{R}'}, \mathsf{corr}_{\mathsf{R}'}(u) = (s, w)} \mathrm{RProb}_{\mathsf{R}'}(u, \mathsf{corr}_{\mathsf{R}'}^{-1}(success))$. As a consequence, we obtain the item 1 in Lemma (33). Since moreover $\mathbf{C}(\mathcal{R}_{\mathsf{nr}}(\mathsf{N})) \subseteq \mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{tr})$, we obtain also the $\leq$ inequality for the item 2 in Lemma (33).

- Using (the second part of) Lemma 32, we see that for every $\mathsf{R} \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{tr})$, and $s' \in \mathcal{S}_{\mathsf{R}}$, such that $\mathsf{corr}_{\mathsf{R}}(s') = (s, w)$, it holds that $\mathrm{RProb}_{\mathsf{R}}(s', \mathsf{corr}_{\mathsf{R}}^{-1}(\mathit{success})) \leq \mathrm{Prob}_{\mathbf{DR}}(s', w)$. From there, we obtain that $\mathrm{RProb}_{\mathsf{R}}(s', \mathsf{corr}_{\mathsf{R}}^{-1}(\mathit{success})) \leq \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N})}(s, w)$, thus we can conclude.

□

Proposition 2. Let $(\mathcal{P}, \phi)$ and $(\mathcal{P}', \phi')$ be two extended processes.

$$(\mathcal{P}, \phi) \leq_{tr}^{\mathcal{R}_{\mathsf{r}}^{\ell}} (\mathcal{P}', \phi') \quad \text{iff} \quad (\mathcal{P}, \phi) \leq_{tr}^{\mathcal{R}_{\mathsf{nr}}^{\ell}} (\mathcal{P}', \phi')$$

Proof. First, observe that it is enough to show that for every trace w, for every N^{ℓ}-state u: $\mathrm{Prob}_{\mathcal{R}_{\mathsf{r}}(\mathsf{N}^{\ell})}(u, w) = \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell})}(u, w)$.

- Since $\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell}) \subseteq \mathcal{R}_{\mathsf{r}}(\mathsf{N}^{\ell})$, we see immediately that $\mathrm{Prob}_{\mathcal{R}_{\mathsf{r}}(\mathsf{N}^{\ell})}(u, w) \geq \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell})}(u, w)$.
- We now show the reverse inequality.

$$\begin{aligned}
&\mathrm{Prob}_{\mathcal{R}_{\mathsf{r}}(\mathsf{N}^{\ell})}(u, w) \\
&= \sup\{\mathrm{RProb}_{\mathsf{R}}(s, \mathsf{corr}_{\mathsf{R}}^{-1}(\mathit{success})) \mid \mathsf{R} \in \mathcal{R}_{\mathsf{r}}(\mathsf{N}^{\ell^{tr}}), s' \in \mathcal{S}_{\mathsf{R}},\ \mathsf{corr}_{\mathsf{R}}(s') = s\} \text{ by Lemma 33;} \\
&= \sup\{\mathrm{RProb}_{\mathsf{R}}^{\leq n}(s, \mathsf{corr}_{\mathsf{R}}^{-1}(\mathit{success})) \mid \mathsf{R} \in \mathcal{R}_{\mathsf{r}}(\mathsf{N}^{\ell^{tr}}), s' \in \mathcal{S}_{\mathsf{R}},\ \mathsf{corr}_{\mathsf{R}}(s') = s,\ n \in \mathbb{N}\} \\
&\leq \sup\{\mathrm{RProb}_{\mathsf{R}}^{\leq n}(s, \mathsf{corr}_{\mathsf{R}}^{-1}(\mathit{success})) \mid \mathsf{R} \in \mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell^{tr}}), s' \in \mathcal{S}_{\mathsf{R}},\ \mathsf{corr}_{\mathsf{R}}(s') = s,\ n \in \mathbb{N}\} \text{ by Lemma 29} \\
&= \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^{\ell})}(u, w) \text{ by Lemma 33}
\end{aligned}$$

□

C Relations $\overset{\tau}{\Longrightarrow}_{\mathsf{r}}$ and $\Longrightarrow_{\mathcal{R}_{\mathsf{r}}}$ coincide

Lemma 34. Let $\mathsf{N} = \mathsf{N} = (\mathcal{S}_{\mathsf{N}}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_{\mathsf{N}})$ be an NPLTS and a resolution $\mathsf{R} = (\mathcal{S}_{\mathsf{R}}, \mathsf{corr}_{\mathsf{R}}, \mathsf{trans}_{\mathsf{R}})$ of N. For all subset $\mathcal{T} \subseteq \mathcal{S}_{\mathsf{R}}$, for all $s \in \mathcal{S}_{\mathsf{R}}$,

$$\mathrm{RProb}_{\mathsf{R}}(s, \mathcal{T}) = \begin{cases} 1 & \text{if } s \in \mathcal{T} \\ 0 & \text{otherwise.} \end{cases}$$

$$\mathrm{RProb}_{\mathsf{R}}(s, \mathcal{T}) = \begin{cases} 1 & \text{if } s \in \mathcal{T} \\ 0 & \text{if } s \notin \mathcal{T} \wedge \mathsf{trans}_{\mathsf{R}}(s) = \star \\ \sum_{u \in \mathrm{supp}(D)} D(u) \cdot \mathrm{RProb}_{\mathsf{R}}(u, \mathcal{T}) & \text{if } s \notin \mathcal{T} \wedge \mathsf{trans}_{\mathsf{R}}(s) = (a, D) \end{cases}$$

Proof. Direct from Definition 7 and the fact that $\mathrm{RProb}_{R}^{\leq n}(s, \mathcal{T})$ is increasing on n. □

We now state three technical lemmas–Lemmas 35, 36, 37, about basic properties of the reduction relation $\rightarrow$ on distributions. These lemmas are used later in the proof of Lemma 1.

Lemma 35. Let X be a discrete set, $\rightarrow \subset X \times \mathcal{D}(X)$ a binary relation, and $s \in X$.

$$\delta_s \rightarrow_{\mathsf{r}} D \quad \text{iff} \quad D \in \text{conv}(\{E \mid s \rightarrow E\})$$

Proof. Direct from Definition 14 and Notation 4. □

Lemma 36. Let $\mathsf{N} = (\mathcal{S}_{\mathsf{N}}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_{\mathsf{N}})$ be a NPLTS, $\mathsf{R} = (\mathcal{S}_{\mathsf{R}}, \mathsf{corr}_{\mathsf{R}}, \mathsf{trans}_{\mathsf{R}}) \in \mathcal{R}_{\mathsf{r}}(\mathsf{N})$ and $D \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{R}})$ such that $\text{supp}(D) \subseteq \mathcal{S}_{int}(\mathsf{R})$. We have $\mathsf{corr}_{\mathsf{R}}(D) \xrightarrow{\tau}_{\mathsf{r}} \mathsf{corr}_{\mathsf{R}}(\mathsf{trans}_{\mathsf{R}}(D))$.

Proof. By Definition 5, for all $s \in \text{supp}(D)$, $\mathsf{corr}_{\mathsf{R}}(\mathsf{trans}_{\mathsf{R}}(s)) \in \text{conv}(\mathsf{trans}_{\mathsf{N}}(\mathsf{corr}_{\mathsf{R}}(s)))$. Hence $\mathsf{corr}_{\mathsf{R}}(\mathsf{trans}_{\mathsf{R}}(s)) \in \text{conv}(\{E_s \mid \mathsf{corr}_{\mathsf{R}}(s) \rightarrow E_s\})$. Furthermore, $\mathsf{corr}_{\mathsf{R}}(\mathsf{trans}_{\mathsf{R}}(D)) = \sum_{s \in \text{supp}(D)} D(s) \cdot \mathsf{corr}_{\mathsf{R}}(\mathsf{trans}_{\mathsf{R}}(s)) = \sum_{s \in \text{supp}(D)} D(s) \cdot \sum_{i=1}^{n_s} \alpha_i^s \cdot E_i^s = \sum_{s \in \text{supp}(D)} \sum_{i=1}^{n_s} (D(s) \cdot \alpha_i^s) \cdot E_i^s$ with $\mathsf{corr}_{\mathsf{R}}(s) \rightarrow E_i^s$ for all $i \in \{1, \ldots, n_s\}$ and $\sum_{i=1}^{n_s} \alpha_i^s = 1$. Since $D = \sum_{s \in \text{supp}(D)} D(s) \cdot \sum_{i=1}^{n_s} \alpha_i^s \cdot \delta_s$, we conclude that $\mathsf{corr}_{\mathsf{R}}(D) = \sum_{s \in \text{supp}(D)} D(s) \cdot \sum_{i=1}^{n_s} \alpha_i^s \cdot \delta_{\mathsf{corr}_{\mathsf{R}}(s)}$ and so $\mathsf{corr}_{\mathsf{R}}(D) \xrightarrow{\tau}_{\mathsf{r}} \mathsf{corr}_{\mathsf{R}}(\mathsf{trans}_{\mathsf{R}}(D))$. □

Lemma 37. Let X be any discrete set, and let $\rightarrow$ be a binary relation in $X \times \mathcal{D}(X)$.

Suppose that $D \rightarrow_{\mathsf{r}} E$. There there exists a family of sub-distribution over X: $(E_s)_{s \in \text{supp}(D)}$ such that for all $s \in \text{supp}(D)$, $\delta_s \rightarrow_{\mathsf{r}} E_s$ and $E = \sum_{s \in \text{supp}(D)} D(s) \cdot E_s$.

Proof. Assume that $D \rightarrow_{\mathsf{r}} E$. By definition, there exists a countable set I and a multiset $\{x_i\}_{i \in I}$ with for all $i \in I$, $x_i \in X$ such that:

- $D = \sum_{i \in I} \alpha_i \cdot \delta_{x_i}$
- for all $i \in I$, $x_i \rightarrow D_i$
- $E = \sum_{i \in I} \alpha_i \cdot D_i$

Note that $E = \sum_{s \in \text{supp}(D)} \cdot \sum_{\substack{i \in I \\ s = x_i}} \alpha_i \cdot D_i$ and for all $s \in X$, $D(s) = \sum_{\substack{i \in I \\ s = x_i}} \alpha_i$. Hence, $E = \sum_{s \in \text{supp}(D)} D(s) \cdot \sum_{\substack{i \in I \\ s = x_i}} \frac{\alpha_i}{D(s)} \cdot D_i$. If we define for all $s \in \text{supp}(D)$, $E_s = \sum_{\substack{i \in I \\ s = x_i}} \frac{\alpha_i}{D(s)} \cdot D_i$, we obtain that $E = \sum_{s \in \text{supp}(D)} D(s) \cdot E_s$ and for all $s \in \text{supp}(D)$, $E_s \in \text{conv}(\{F \mid s \rightarrow F\})$ which implies $\delta_s \rightarrow_{\mathsf{r}} E_s$ by Lemma 35. □

Corollary 4. Let X be any discrete set, and let $\rightarrow$ be a binary relation in $X \times \mathcal{D}(X)$.

Suppose that $D \rightarrow_{\mathsf{r}} E + F$. Then there exists two families of sub-distribution over X: $(E_s)_{s \in \text{supp}(D)}, (F_s)_{s \in \text{supp}(D)}$ such that for all $s \in \text{supp}(D)$, $\delta_s \rightarrow_{\mathsf{r}} E_s + F_s$, $E = \sum_{s \in \text{supp}(D)} D(s) \cdot E_s$ and $F = \sum_{s \in \text{supp}(D)} D(s) \cdot F_s$.

Proof. By Lemma 37, we know that there exists $(D_s)_{s \in \text{supp}(D)}$ such that for all $s \in \text{supp}(D)$, $\delta_s \rightarrow_{\mathsf{r}} D_s$ and $E + F = \sum_{s \in \text{supp}(D)} D(s) \cdot D_s$.

We define the two families $(E_s)_{s \in \text{supp}(D)}$ and $(F_s)_{s \in \text{supp}(D)}$ as follows: for all $s \in \text{supp}(D)$, for all $x \in X$,

- $E_s(x) = \frac{D_s(x) \cdot E(x)}{E(x) + F(x)}$

- $F_s(x) = \frac{D_s(x) \cdot F(x)}{E(x)+F(x)}$

We trivially have $D_s = E_s + F_s$. $\square$

Lemma 1. Let $\mathsf{N} = (\mathcal{S}_\mathsf{N}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_\mathsf{N})$ be a NPLTS and $D, E \in \mathcal{D}^{\leq 1}(\mathcal{S}_\mathsf{N})$.

$$D \stackrel{\tau}{\Longrightarrow}_\mathsf{r} E \text{ if and only if } D \Longrightarrow_{\mathcal{R}_\mathsf{r}} E$$

Proof. We prove the two directions of the equivalences separately.

Left-to-right direction. Let us suppose that $D \stackrel{\tau}{\Longrightarrow}_\mathsf{r} E$. It means that there exists an infinite scheme of the form:

$$\begin{aligned}
&D = D_0^{\rightarrow} + D_0^{\top} \\
&D_0^{\rightarrow} \stackrel{\tau}{\rightarrow}_\mathsf{r} D_1^{\rightarrow} + D_1^{\top} \\
&\dots \\
&D_k^{\rightarrow} \stackrel{\tau}{\rightarrow}_\mathsf{r} D_{k+1}^{\rightarrow} + D_{k+1}^{\top} \\
&\dots
\end{aligned}$$

with $E = \sum_{k \in \mathbb{N}} D_k^{\top}$. The proof consists of two steps: we first define a resolution $\mathsf{R} \in \mathcal{R}_\mathsf{r}(\mathsf{N})$, and in a second step we use R to show that $D \Longrightarrow_{\mathcal{R}_\mathsf{r}} E$.

1. We define $\mathsf{R} = (\mathcal{S}_\mathsf{R}, \mathsf{corr}_\mathsf{R}, \mathsf{trans}_\mathsf{R})$, where $\mathcal{S}_\mathsf{R} = \{(s, n, \alpha) \mid n \in \mathbb{N}, \alpha \in \{\rightarrow, \top\}, s \in \mathrm{supp}(D_n^{\alpha})\}$ and $\mathsf{corr}(s, n, \alpha) = s$ for every $n \in \mathbb{N}$ and every $\alpha \in \{\rightarrow, \top\}$, and

$$\mathsf{trans}_\mathsf{R}(s, n, \alpha) = \begin{cases} \star_{\mathcal{A}} & \text{if } \alpha = \top; \\ (\tau, \sum_{s' \in \mathcal{S}} \Delta(s, n, \top)(s') \cdot \delta_{(s', n+1, \top)} + \Delta(s, n, \rightarrow)(s') \cdot \delta_{(s', n+1, \rightarrow)}) & \\ \qquad \text{if } \alpha = \rightarrow . & \end{cases}$$

where $\star_{\mathcal{A}}$ stands for the function $(a \in \mathcal{A}_{ext} \mapsto \star)$, $\mathcal{S} = \{s \mid (s, n, \alpha) \in \mathcal{S}_\mathsf{R}\}$ and for all $s \in \mathrm{supp}(D_n^{\rightarrow}), n \in \mathbb{N}, \alpha \in \{\rightarrow, \top\}$, the sub-distributions $\Delta(s, n, \alpha)$ are obtained from Corollary 4 such that:

$$\delta_s \stackrel{\tau}{\rightarrow}_\mathsf{r} \Delta(s, n, \rightarrow) + \Delta(s, n, \top), \qquad \forall s \in \mathrm{supp}(D_n^{\rightarrow}); \tag{13}$$

$$D_{n+1}^{\rightarrow} = \sum_{s \in \mathrm{supp}(D_n^{\rightarrow})} D_n^{\rightarrow}(s) \cdot \Delta(s, n, \rightarrow); \tag{14}$$

$$D_{n+1}^{\top} = \sum_{s \in \mathrm{supp}(D_n^{\rightarrow})} D_n^{\rightarrow}(s) \cdot \Delta(s, n, \top). \tag{15}$$

We first check that R is indeed a N-resolution: first observe that for all external states $s' \in \mathcal{S}_{ext}(\mathsf{R})$, for all $a \in \mathcal{A}_{ext}$, $\mathsf{trans}_\mathsf{R}(s') = \star$. Secondly, for all internal states $s' \in \mathcal{S}_{int}(\mathsf{R})$ with $\mathsf{trans}_\mathsf{R}(s') = (\tau, F)$, it means that $s' = (s, n, \rightarrow)$, $s \in \mathrm{supp}(D_n^{\rightarrow})$ and

$$F = \sum_{s' \in \mathcal{S}} \Delta(s, n, \top)(s') \cdot \delta_{(s', n+1, \top)} + \sum_{s' \in \mathcal{S}} \Delta(s, n, \rightarrow)(s') \cdot \delta_{(s', n+1, \rightarrow)}$$

Note that for all $s \in \mathcal{S}, n \in \mathbb{N}$, $\mathrm{supp}(\Delta(s,n,\top)) \subseteq \mathcal{S}$ and $\mathrm{supp}(\Delta(s,n,\to)) \subseteq \mathcal{S}$. Hence $\mathsf{corr}_{\mathsf{R}}(F) = \Delta(s,n,\to) + \Delta(s,n,\top)$. From (13) and Lemma 35, we obtain that $\mathsf{corr}_{\mathsf{R}}(F) \in \mathrm{conv}(\mathsf{trans}_{\mathsf{N}}(s)(\tau))$, thus we can conclude that $\mathsf{R} \in \mathcal{R}_{\mathsf{r}}(\mathsf{N})$.

2. We define a distribution over R-states: $D' = \sum_{s\in\mathcal{S}} D_0^{\to}(s)\cdot\delta_{s,0,\to} + \sum_{s\in\mathcal{S}} D_0^{\top}(s)\cdot\delta_{s,0,\top}$. We see immediately that $\mathsf{corr}_{\mathsf{R}}(D') = D$.

   Looking at Definition 13, we see that we need now to compute the sub-distribution $\mathsf{corr}(E')$, with E' defined as $\mathrm{supp}(E') \subseteq \mathcal{S}_{ext}(\mathsf{R})$ and for all $u' \in \mathcal{S}_{ext}(\mathsf{R})$, $E'(u') = \sum_{s'\in\mathcal{S}_{\mathsf{R}}} D'(s') \cdot \mathrm{RProb}_{\mathsf{R}}(s', \{u'\})$. First, recall that for all $u' \in \mathcal{S}_{ext}(\mathsf{R})$, u' is of the form $(u,p,\top)$ with $p \in \mathbb{N}$ and $u \in \mathcal{S}$. Additionally, note that both $\mathrm{supp}(D_0^{\to})$ and $\mathrm{supp}(D_0^{\top})$ are included in $\mathcal{S} \subseteq \mathcal{S}_{\mathsf{N}}$.

$$\begin{aligned} E'(u,p,\top) = &\sum_{s\in\mathcal{S}_{\mathsf{N}}} D_0^{\to}(s)\cdot \mathrm{RProb}_{\mathsf{R}}((s,0,\to),\{(u,p,\top)\}) \\ &+ \sum_{s\in\mathcal{S}_{\mathsf{N}}} D_0^{\top}(s)\cdot \mathrm{RProb}_{\mathsf{R}}((s,0,\top),\{(u,p,\top)\}) \end{aligned}$$

   Observe that for every $(s,0,\top) \in \mathcal{S}_{ext}(\mathsf{R})$, $\mathrm{RProb}_{\mathsf{R}}((s,0,\top),\{(u,p,\top)\}) = 1$ if $u = s$, $p = 0$ and 0 otherwise.

   Furthermore, by definition of $\mathsf{trans}_{\mathsf{R}}$, if $\mathsf{trans}_{\mathsf{R}}(s,n,\to) = (\tau, F)$ then $(s',n',\alpha') \in \mathrm{supp}(F)$ implies $n' = n+1$. Thus, we can easily prove by induction that for all $(s,n,\to),(t,m,\top) \in \mathcal{S}_{\mathsf{R}}$, $\mathrm{RProb}_{\mathsf{R}}((s,n,\to),\{(t,m,\top)\}) > 0$ implies that $m > n$. Using these two facts, we obtain that:

$$E'(u,0,\top) = D_0^{\top}(u) \tag{16}$$

$$E'(u,p,\top) = \sum_{s\in\mathcal{S}_{\mathsf{N}}} D_0^{\to}(s)\cdot \mathrm{RProb}_{\mathsf{R}}((s,0,\to),\{(u,p,\top)\}) \quad \text{for } p \geq 1. \tag{17}$$

   To go forward from here, we are going to show the following auxiliary statement: for all $p \in \mathbb{N}$, for all $m < p \in \mathbb{N}$, for all $u \in \mathcal{S}$,

$$\sum_{s\in\mathcal{S}_{\mathsf{N}}} D_m^{\to}(s)\cdot \mathrm{RProb}_{\mathsf{R}}((s,m,\to),\{(u,p,\top)\}) = D_p^{\top}(u). \tag{18}$$

   We do the proof by induction on $p - m$. For all $(s,n,\to) \in \mathcal{S}_{int}(\mathsf{R})$, let us denote $F_{s,n}$ the distribution such that $\mathsf{trans}_{\mathsf{R}}(s,n,\to) = (\tau, F_{s,n})$.

$$\begin{aligned} &\sum_{s\in\mathcal{S}_{\mathsf{N}}} D_m^{\to}(s)\cdot \mathrm{RProb}_{\mathsf{R}}((s,m,\to),\{(u,p,\top)\}) \\ &= \sum_{s\in\mathcal{S}_{\mathsf{N}}} D_m^{\to}(s)\cdot \sum_{t\in\mathrm{supp}(F_{s,m})} F_{s,m}(t)\cdot \mathrm{RProb}_{\mathsf{R}}(t,\{(u,p,\top)\}) \text{ by Lemma 34} \end{aligned}$$

By definition of $F_{s,n}$, $t \in \text{supp}(F_{s,n})$ implies that $t = (t', m+1, \alpha)$ with $t' \in \mathcal{S}$ and $\alpha \in \{\top, \rightarrow\}$ and $F_{s,n}(t) = \Delta(s, m, \top)(t') + \Delta(s, m, \rightarrow)(t')$. Hence:

$$\begin{aligned}
&\sum_{s \in \mathcal{S}_\mathsf{N}} D^{\rightarrow}_m(s) \cdot \text{RProb}_\mathsf{R}((s, m, \rightarrow), \{(u, p, \top)\}) \\
&= \sum_{s \in \mathcal{S}_\mathsf{N}} D^{\rightarrow}_m(s) \cdot (\sum_{t \in \mathcal{S}_\mathsf{N}} (\Delta(s, m, \top)(t) \cdot \text{RProb}_\mathsf{R}((t, m+1, \top), \{(u, p, \top)\}) \\
&\qquad + \sum_{t \in \mathcal{S}_\mathsf{N}} \Delta(s, m, \rightarrow)(t) \cdot \text{RProb}_\mathsf{R}((t, m+1, \rightarrow), \{(u, p, \top)\}))
\end{aligned}$$

- if $p = m+1$ then for all $t \in \mathcal{S}_\mathsf{N}$, $\text{RProb}_\mathsf{R}((t, m+1, \top), \{(u, m+1, \top)\}) = 1$ if $t = u$ and 0 otherwise. Moreover, as we previously shown, $\text{RProb}_\mathsf{R}((t, m+1, \rightarrow), \{(u, m+1, \top)\}) = 0$. Therefore:

$$\begin{aligned}
\sum_{s \in \mathcal{S}_\mathsf{N}} D^{\rightarrow}_m(s) \cdot \text{RProb}_\mathsf{R}((s, m, \rightarrow), \{(u, p, \top)\}) &= \sum_{s \in \mathcal{S}_\mathsf{N}} D^{\rightarrow}_m(s) \cdot \Delta(s, m, \top)(u) \\
&= D^{\top}_p(u) \quad \text{by (15).}
\end{aligned}$$

- if $p > m+1$ then for all $t \in \mathcal{S}_\mathsf{N}$, $\text{RProb}_\mathsf{R}((t, m+1, \top), \{(u, p, \top)\}) = 0$. Hence:

$$\begin{aligned}
&\sum_{s \in \mathcal{S}_\mathsf{N}} D^{\rightarrow}_m(s) \cdot \text{RProb}_\mathsf{R}((s, m, \rightarrow), \{(u, p, \top)\}) \\
&= \sum_{s \in \mathcal{S}_\mathsf{N}} D^{\rightarrow}_m(s) \cdot \sum_{t \in \mathcal{S}_\mathsf{N}} \Delta(s, m, \rightarrow)(t) \cdot \text{RProb}_\mathsf{R}((t, m+1, \rightarrow), \{(u, p, \top)\}) \\
&= \sum_{t \in \mathcal{S}_\mathsf{N}} \left(\sum_{s \in \mathcal{S}_\mathsf{N}} D^{\rightarrow}_m(s) \cdot \Delta(s, m, \rightarrow)(t) \right) \cdot \text{RProb}_\mathsf{R}((t, m+1, \rightarrow), \{(u, p, \top)\}) \\
&= \sum_{t \in \mathcal{S}_\mathsf{N}} D^{\rightarrow}_{m+1}(t) \cdot \text{RProb}_\mathsf{R}((t, m+1, \rightarrow), \{(u, p, \top)\})) \qquad \text{by (14)} \\
&= D^{\top}_p(u) \quad \text{by induction hypothesis}
\end{aligned}$$

This concludes the proof of Equation 18. Combining (16), (17) and (18), we have shown:

$$E'(u, p, \top) = D^{\top}_p(u) \quad \forall p \in \mathbb{N}.$$

We conclude the proof by noticing that $\mathsf{corr}(E')(u) = \sum_{p \in \mathbb{N}} D^{\top}_p(u) = E(u)$.

Right-to-left direction. We suppose that $D \Longrightarrow_{\mathcal{R}_\mathsf{r}} E$. It means that there exists a resolution $\mathsf{R} = (\mathcal{S}_\mathsf{R}, \mathsf{corr}_\mathsf{R}, \mathsf{trans}_\mathsf{R}) \in \mathcal{R}_\mathsf{r}(\mathsf{N})$ and $D', E' \in \mathcal{D}^{\leq 1}(\mathcal{S}_\mathsf{R})$ such that $\mathsf{corr}_\mathsf{R}(D') = D$, $\mathsf{corr}_\mathsf{R}(E') = E$, $\text{supp}(E') \subseteq \mathcal{S}_{ext}(\mathsf{R})$ and for every $u \in \mathcal{S}_{ext}(\mathsf{R})$, $E'(u) = \sum_{s' \in \mathcal{S}_\mathsf{R}} D'(s') \cdot \text{RProb}_\mathsf{R}(s', \{u\})$. From there, we are going to build an infinite scheme, in the spirit of Definition 15. We

define by induction on n two families of sub-distributions on $\mathcal{S}_{\mathsf{R}}$, $({D'}_n^{\rightarrow})_{n\in\mathbb{N}}$ and $({D'}_n^{\top})_{n\in\mathbb{N}}$, as follows:

$$
\begin{aligned}
{D'}_0^{\rightarrow} &= D'_{|\mathcal{S}_{int}(\mathsf{R})} & {D'}_0^{\top} &= D'_{|\mathcal{S}_{ext}(\mathsf{R})} \\
{D'}_{n+1}^{\rightarrow} &= \mathsf{trans}_{\mathsf{R}}({D'}_n^{\rightarrow})_{|\mathcal{S}_{int}(\mathsf{R})} & {D'}_{n+1}^{\top} &= \mathsf{trans}_{\mathsf{R}}({D'}_n^{\rightarrow})_{|\mathcal{S}_{ext}(\mathsf{R})}.
\end{aligned}
$$

We denote for all $n \in \mathbb{N}$, ${D'}_n = {D'}_n^{\rightarrow} + {D'}_n^{\top}$. Hence, $D' = D'_0$. Using Lemma 36, we can check that for all $n \in \mathbb{N}$, $\mathsf{corr}_{\mathsf{R}}({D'}_n^{\rightarrow}) \xrightarrow{\tau}_{\mathsf{r}} \mathsf{corr}_{\mathsf{R}}({D'}_{n+1})$. Then we define, for every $n \in \mathbb{N}$, $\alpha \in \{\rightarrow, \top\}$, $D_n^{\alpha} = \mathsf{corr}_{\mathsf{R}}({D'}_n^{\alpha}) \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{N}})$.

We now show that for all $n \in \mathbb{N}$, for all $j \leq n$, for all $u \in \mathcal{S}_{ext}(\mathsf{R})$,

$$
\sum_{s' \in \mathcal{S}_{\mathsf{R}}} {D'}_j(s') \cdot \mathrm{RProb}_R^{\leq n-j}(s', \{u\}) = \sum_{j \leq k \leq n} {D'}_k^{\top}(u). \tag{19}
$$

We prove this property by induction on $n - j$:

- if $n = j$, then we can first see that $\sum_{s' \in \mathcal{S}_{\mathsf{R}}} {D'}_j(s') \cdot \mathrm{RProb}_R^{\leq 0}(s', \{u\}) = {D'}_j(u)$. Since u is an external state, and by definition of ${D'}_j$, it holds that ${D'}_j(u) = {D'}_j^{\top}(u)$, so the result holds.

- case $n - j > 0$:

$$
\begin{aligned}
&\sum_{s' \in \mathcal{S}_{\mathsf{R}}} {D_j}'(s') \cdot \mathrm{RProb}_R^{\leq n-j}(s', \{u\}) \\
&= \sum_{s' \in \mathcal{S}_{\mathsf{R}}} {D'}_j^{\rightarrow}(s') \cdot \mathrm{RProb}_R^{\leq n-j}(s', \{u\}) + \sum_{s' \in \mathcal{S}_{\mathsf{R}}} {D'}_j^{\top}(s') \cdot \mathrm{RProb}_R^{\leq n-j}(s', \{u\}) \\
&= \sum_{s' \in \mathcal{S}_{\mathsf{R}}} {D'}_j^{\rightarrow}(s') \cdot \mathrm{RProb}_R^{\leq n-j}(s', \{u\}) + {D'}_j^{\top}(u) \quad \text{since } s' \in \mathrm{supp}({D'}_j^{\top}) \Rightarrow s' \in \mathcal{S}_{ext}(\mathsf{R}) \\
&= \sum_{s' \in \mathcal{S}_{\mathsf{R}}, \mathsf{trans}_{\mathsf{R}}(s') = (\tau, F_{s'})} {D'}_j^{\rightarrow}(s') \cdot \sum_{v' \in \mathcal{S}_{\mathsf{R}}} F_{s'}(v') \cdot \mathrm{RProb}_R^{\leq n-j-1}(v', \{u\}) + {D'}_j^{\top}(u) \\
&= \sum_{v' \in \mathcal{S}_{\mathsf{R}}} D'_{j+1}(v') \cdot \mathrm{RProb}_R^{\leq n-(j+1)}(v', \{u\}) + {D'}_j^{\top}(u) \quad \text{since } \mathsf{trans}_{\mathsf{R}}({D'}_j^{\rightarrow}) = D'_{j+1} \\
&= \sum_{j+1 \leq k \leq n} {D'}_k^{\top}(u) + {D'}_j^{\top}(u) \quad \text{by induction hypothesis,}
\end{aligned}
$$

  and that concludes the proof of (19).

We are now able to end the proof, by seeing that for all $w \in \mathcal{S}_{\mathsf{N}}$,

$$\begin{aligned}
E(w) &= \sum_{u \in \mathsf{corr_R}^{-1}(w)} E'(u) \qquad \text{since by hypothesis } \mathsf{corr_R}(E') = E \\
&= \sum_{u \in \mathsf{corr_R}^{-1}(w)} \sum_{s' \in \mathcal{S}_{\mathsf{R}}} D'_0(s') \cdot \mathrm{RProb}_R(s', \{u\}) \qquad \text{by hypothesis, and since } D' = D'_0 \\
&= \sup_{n \in \mathbb{N}} \sum_{u \in \mathsf{corr_R}^{-1}(w)} \sum_{s' \in \mathcal{S}_{\mathsf{R}}} D'_0(s') \cdot \mathrm{RProb}_R^{\leq n}(s', \{u\}) \\
&= \sup_{n \in \mathbb{N}} \sum_{u \in \mathsf{corr_R}^{-1}(w)} \sum_{0 \leq k \leq n} {D'}_k^{\top}(u) \qquad \text{by (19) instantiated with } j = 0 \\
&= \sup_{n \in \mathbb{N}} \sum_{0 \leq k \leq n} D_k^{\top}(w) \qquad \text{since } \mathsf{corr_R}({D'}_k^{\top}) = D_k^{\top} \\
&= \sum_{k \in \mathbb{N}} D_k^{\top}(w),
\end{aligned}$$

which ends the proof. □

D Observational equivalence with name restriction in context

In the original applied pi calculus, observational equivalence is closed by application of an *adversarial context*, i.e., if $P \approx Q$ then $C[P] \approx C[Q]$ where $C[_]$ is a context of the form $\mathsf{new}\ a_1; \ldots; \mathsf{new}\ a_n; (_ \mid Adv)$ where Adv is a process. Intuitively, previously public names $a_1, \ldots, a_n$ in P and Q may becomes restricted, i.e. private, by the application of the adversarial context.

In our definition of observational equivalence (Definition 18), we only require that the adversarial process Adv is put in parellel of P and Q without allowing for additional name restrictions. In our formalism, this corresponds to the third bullet point of Definition 18, i.e.:

$$\text{for all closed } Adv \in \mathcal{MP} \text{ such that } fn(Adv) \subseteq \mathcal{N}_{pub},\ \{Adv\} \cup \mathcal{P}\ R\ \{Adv\} \cup \mathcal{Q}.$$

We show in this section that in fact adding these restrictions in the definition of observational equivalence does not add any power to the attacker by showing that the classical definition and our definition coincide. Note that the original formalism of the applied pi calculus is slightly different from ours as they do not separate names in public and private names as we do. Furthermore, they do not have a rule that executes the name restriction as our rule (New). Instead, they consider a structural equivalence $\equiv$ that manages name restrictions. For instance,

$$\mathsf{new}\ a; 0 \equiv 0 \qquad \mathsf{new}\ a; \mathsf{new}\ b; P \equiv \mathsf{new}\ b; \mathsf{new}\ a; P$$
$$P \mid \mathsf{new}\ a; Q \equiv \mathsf{new}\ a; (P \mid Q) \text{ when } a \notin fv(P) \cup fn(P)$$

Similarly, by the fact that our calculus relies on multisets of processes, the rules (Null), (Par) and (Repl) capture the following equations in the structural equivalence:

$$P \equiv P \mid 0 \qquad P_1 \mid (P_2 \mid P_3) \equiv (P_1 \mid P_2) \mid P_3 \qquad P \mid Q \equiv Q \mid P \qquad !P \equiv P \mid !P$$

Thus, as mentioned in [ABF17, Section 2.3], any process P in the original applied pi calculus is structurally equivalent as a process of the form $\mathsf{new}\ a_1; \ldots; \mathsf{new}\ a_n; (P_1 \mid \ldots \mid P_n)$ where name restrictions have been pushed to the top, which can be expressed by a configuration $(\{a_1, \ldots, a_n\}, \{\!\{P_1, \ldots, P_n\}\!\})$. In our calculus, the distinction between private and public names enforces that all names $a_1, \ldots, a_n$ are in $\mathcal{N}_{priv}$ which allows us to only keep the multiset $\{\!\{P_1, \ldots, P_n\}\!\}$ (see Figure 2).

Therefore, applying an adversarial context with restriction is equivalent in our formalism to applying a renaming from public names of our process to fresh privates names. This leads to the following definition of the original observational equivalence:

Definition 47. The *original observational preorder* $\leq^{\mathcal{R}}_{ori}$ is the largest relation R on $\mathcal{MP}$ such that $\mathcal{P}\ R\ \mathcal{Q}$ implies :

- for all $c \in \mathcal{N}_{pub}$, $\mathrm{RProb}_{\mathcal{R}}(\mathcal{P}, \downarrow c) \leq \mathrm{RProb}_{\mathcal{R}}(\mathcal{Q}, \downarrow c)$;
- if $\mathcal{P} \xRightarrow{\tau}_{\mathsf{r}} D$ then $\mathcal{Q} \xRightarrow{\tau}_{\mathsf{r}} E$ and $D\ \widehat{R}\ E$;
- for all closed $Adv \in \mathcal{MP}$, for all renaming ρ, if $fn(Adv) \subseteq \mathcal{N}_{pub}$, $dom(\rho) \subseteq \mathcal{N}_{pub}$, $img(\rho) \subseteq \mathcal{N}_{priv}$ and $img(\rho) \cap \mathrm{names}(\mathcal{P}, \mathcal{Q}, Adv) = \varnothing$ then $\{Adv\rho\} \cup \mathcal{P}\rho\ R\ \{Adv\rho\} \cup \mathcal{Q}\rho$.

The *original observational equivalence* $\approx^{\mathcal{R}}_{ori}$ is defined by additionally requesting R to be symmetric and in the second bullet point, by requesting both $D\ \widehat{R}\ E$ and $E\ \widehat{R}\ D$ to hold.

Let us now show that the two notions coincide.

Lemma 38. $\leq^{\mathcal{R}}_{ori} = \leq^{\mathcal{R}}_{obs}$ and $\approx^{\mathcal{R}}_{ori} = \approx^{\mathcal{R}}_{obs}$.

Proof. Trivially, we have that $\leq^{\mathcal{R}}_{ori} \subseteq \leq^{\mathcal{R}}_{obs}$ and $\approx^{\mathcal{R}}_{ori} \subseteq \approx^{\mathcal{R}}_{obs}$ since we can always take ρ being the empty renaming.

Consider the relation $\mathcal{R}$ defined as $\mathcal{P}\,\mathcal{R}\,\mathcal{Q}$ iff there exists $\mathcal{P}', \mathcal{Q}'$ and a renaming such that ρ such that $\mathcal{P} = \mathcal{P}'\rho$, $\mathcal{Q} = \mathcal{Q}'\rho$, $\mathcal{P}' \leq^{\mathcal{R}}_{obs} \mathcal{Q}'$, $dom(\rho) \subseteq \mathcal{N}_{pub}$, $img(\rho) \subseteq \mathcal{N}_{priv}$ and $img(\rho) \cap \mathrm{names}(\mathcal{P}', \mathcal{Q}', Adv) = \varnothing$.

Recall that $\doteq$ is closed under substitution of names by terms. Therefore, for all u, v such that $img(\rho) \cap names(u, v) = \varnothing$, $u \doteq v$ if and only if $u\rho \doteq v\rho$. Thus, $\mathcal{P}\rho \to_\tau D'$ implies $\mathcal{P} \to_\tau D$ where $dom(D') = dom(D)\rho$ and $D'(x\rho) = D(x\rho)$. Furthermore, if $\mathcal{P} \to_\tau D$ then $\mathcal{P}\rho \to_\tau D\rho$ where $D\rho$ is the distribution such that $dom(D\rho) = dom(D)$ and $D\rho(x\rho) = D(x\rho)$. Notice that for the rule (New), we consider w.l.o.g. that a' is fresh also with respect to the private names in ρ. In other words, we have that $\mathcal{P}\rho \to_\tau D\rho$ iff $\mathcal{P} \to_\tau D$.

This can be propagate to schedulers, i.e. $(\mathsf{corr}, R) \in \mathcal{R}^o_{\mathsf{r}}$ if and only if $(\mathsf{corr}\rho, R) \in \mathcal{R}^o_{\mathsf{r}}$. Hence, we derive that

- $\mathrm{RProb}_{\mathcal{R}_r^o}(\mathcal{P}, \mathcal{T}) = \mathrm{RProb}_{\mathcal{R}_r^o}(\mathcal{P}\rho, \mathcal{T}\rho)$
- $D \stackrel{\tau}{\Longrightarrow}_{\mathcal{R}_r^o} E$ if and only if $D\rho \stackrel{\tau}{\Longrightarrow}_{\mathcal{R}_r^o} E\rho$

We now show that $\mathcal{R}$ satisfies the three items in Definition 47:

- Let $c \in \mathcal{N}_{pub}$. If $c \in dom(\rho)$ then c does neither occur in $\mathcal{P}'\rho$ nor in $\mathcal{Q}'\rho$. Hence, $\mathrm{RProb}_{\mathcal{R}_r^o}(\mathcal{P}', \downarrow c) = 0 = \mathrm{RProb}_{\mathcal{R}_r^o}(\mathcal{Q}', \downarrow c)$. Otherwise, $\downarrow c = \downarrow c\rho \cup \mathcal{T}$ where for all $\mathcal{P}' \in \mathcal{T}$, $fn(\mathcal{P}') \cap dom(\rho) \neq \varnothing$. Since, $\mathcal{P}'\rho$ and $\mathcal{Q}'\rho$ do not contain public names from $dom(\rho)$, they can never reach states from $\mathcal{T}$. Hence, $\mathrm{RProb}_{\mathcal{R}_r^o}(\mathcal{P}'\rho, \downarrow c) = \mathrm{RProb}_{\mathcal{R}_r^o}(\mathcal{P}'\rho, \downarrow c\rho) = \mathrm{RProb}_{\mathcal{R}_r^o}(\mathcal{P}', \downarrow c)$. Since $\mathcal{P}' \leq_{obs}^{\mathcal{R}} \mathcal{Q}'$, we deduce that $\mathrm{RProb}_{\mathcal{R}_r^o}(\mathcal{P}', \downarrow c) \leq \mathrm{RProb}_{\mathcal{R}_r^o}(\mathcal{Q}', \downarrow c) \leq \mathrm{RProb}_{\mathcal{R}_r^o}(\mathcal{Q}'\rho, \downarrow c\rho) \leq \mathrm{RProb}_{\mathcal{R}_r^o}(\mathcal{Q}', \downarrow c)$.
- If $\mathcal{P}\rho \stackrel{\tau}{\Longrightarrow}_{\mathcal{R}_r^o} D\rho$ then $\mathcal{P}' \stackrel{\tau}{\Longrightarrow}_{\mathcal{R}_r^o} D$. By $\mathcal{P}' \leq_{obs}^{\mathcal{R}} \mathcal{Q}'$, we have $\mathcal{Q}' \stackrel{\tau}{\Longrightarrow}_{\mathcal{R}_r^o} E$ and $D \widehat{\leq_{obs}^{\mathcal{R}}} E$. This implies that $D\rho \,\widehat{\mathcal{R}}\, E\rho$ with $\mathcal{Q}'\rho \stackrel{\tau}{\Longrightarrow}_{\mathcal{R}_r^o} E\rho$.
- Let $Adv \in \mathcal{MP}$ and ρ' be a renaming such that $fn(Adv) \subseteq \mathcal{N}_{pub}$, $dom(\rho') \subseteq \mathcal{N}_{pub}$, $img(\rho') \subseteq \mathcal{N}_{priv}$ and $img(\rho') \cap \mathrm{names}(\mathcal{P}'\rho, \mathcal{Q}'\rho) = \varnothing$. Note that the domains of ρ and ρ' may not be disjoint. Similarly, the process Adv may contain public names from $dom(\rho)$.

  Hence, let ρ_{pub} be a renaming such that $dom(\rho_{pub}) = dom(\rho) \cap (dom(\rho') \cup fn(Adv))$, $img(\rho_{pub}) \subseteq \mathcal{N}_{pub} \setminus fn(\mathcal{P}', \mathcal{Q}', Adv)$. Hence, we define $\rho_1 = \rho\rho_{pub}^{-1}\rho'$.

  We have $\mathcal{P}'\rho_1 = (\mathcal{P}'\rho)\rho'$ since $img(\rho_{pub}) \subseteq \mathcal{N}_{pub} \setminus fn(\mathcal{P}', \mathcal{Q}', Adv)$. Moreover, as $dom(\rho_{pub}) = dom(\rho) \cap (dom(\rho') \cup fn(Adv))$, we have that

  $$(Adv\rho_{pub})\rho = Adv\rho_{pub}\rho|_{dom(\rho)\setminus dom(\rho_{pub})} = Adv\rho|_{dom(\rho)\setminus dom(\rho_{pub})}\rho_{pub} = Adv\rho_{pub}$$

  Therefore, $Adv\rho_{pub}\rho_1 = Adv\rho_{pub}\rho_{pub}^{-1}\rho' = Adv\rho'$. This allows us to deduce that $\{Adv\rho'\} \cup \mathcal{P}'\rho' = (\{Adv\rho_{pub}\} \cup \mathcal{P}')\rho_1$. Similarly, we have $\{Adv\rho'\} \cup \mathcal{Q}'\rho' = (\{Adv\rho_{pub}\} \cup \mathcal{Q}')\rho_1$.

  We know that $\mathcal{P}' \leq_{obs}^{\mathcal{R}} \mathcal{Q}'$. Hence $\{Adv\rho_{pub}\} \cup \mathcal{P}' \leq_{obs}^{\mathcal{R}} \{Adv\rho_{pub}\} \cup \mathcal{Q}'$ which allows us to conclude that $\{Adv\rho_{pub}\rho_1\} \cup \mathcal{P}'\rho_1 \,\mathcal{R}\, \{Adv\rho_{pub}\rho_1\} \cup \mathcal{Q}'\rho_1$ and so $\{Adv\rho'\} \cup \mathcal{P}\rho' \,\mathcal{R}\, \{Adv\rho'\} \cup \mathcal{Q}\rho'$. □

E τ-determinisation

Notation 23. We says that a NPLTS N is *a* new *-determinization of* N^ℓ when $\mathsf{N} = (\mathcal{S}_{\mathsf{N}^\ell}, \mathcal{A}_{\mathsf{N}^\ell}, \mathsf{trans})$ with the following constraints on its transition function trans:

- for $a \in \mathcal{A}_{\mathsf{N}^\ell} \setminus \{\tau\}$, $\mathsf{trans}(s)(a) = \mathsf{trans}_{\mathsf{N}^\ell}(s)(a)$, and $\mathsf{trans}(s)(\tau) \subseteq \mathsf{trans}_{\mathsf{N}^\ell}(s)(\tau)$;
- for every $D \in \mathsf{trans}_{\mathsf{N}^\ell}(s)(\tau)$ not obtained by a new reduction, $D \in \mathsf{trans}(s)(a)$;

- for $s = (\{\!\{\mathsf{new}\ a.\mathcal{Q}\}\!\} \cup \mathcal{P}, \phi)$, there exists at least one $E \in \mathsf{trans}(s)(\tau)$ with E of the form $\delta_{(\{\!\{\mathcal{Q}\{b/a\}\}\!\} \cup \mathcal{P}, \phi)}$ with $b \in \mathcal{N}_{priv}$ fresh in s. We say that the new -determinisation is *strict* when there is exactly one such $E \in \mathsf{trans}(s)(\tau)$.

Observe that we can easily build a particular strict new -determinization by ordering the private names, and choosing for each new -reduction the first available fresh private name.

Notation 24. We define an equivalence relation on $\mathcal{SP}_\ell$, that we call *equivalence with respect to private names substitution*, and that we note $\equiv_{\mathcal{N}_{priv}}$: $(\mathcal{P}, \phi) \equiv_{\mathcal{N}_{priv}} (\mathcal{Q}, \psi)$ when there exists private names $a_1, \ldots, a_n$, $b_1, \ldots, b_n$ with $b_1, \ldots, b_n$ fresh in $(\mathcal{P}, \phi)$ such that

$$(\mathcal{Q}, \psi) = (\mathcal{P}\{a_1/b_1\} \ldots \{a_n/b_n\}, \phi\{a_1/b_1\} \ldots \{a_n/b_n\}).$$

Lemma 39. Let N be a new -determinization of N^ℓ, and $s, t \in \mathcal{SP}_\ell$ such that $s \equiv_{\mathcal{N}_{priv}} t$. Then $s \leq^{\mathsf{N}}_{sim} t$.

Observe that in particular N^ℓ is a (non strict) new -determinization of itself, thus Lemma 39 also holds for $\mathsf{N} = \mathsf{N}^\ell$.

Lemma 40. Let N be a new -determinization of N^ℓ. Let $s \in \mathcal{SP}_\ell$, and $a \in \mathcal{A}_{\mathsf{N}^\ell}$ such that $s \xrightarrow{a}_{\mathsf{N}^\ell} D$. Then there exists E such that $s \xrightarrow{a}_{\mathsf{N}} E$, and $D(\widehat{\equiv_{\mathcal{N}_{priv}}})E$

Lemma 41. Let N be a new -determinization of N^ℓ. Let $s \in \mathcal{SP}_\ell$, and $a \in \mathcal{A}_{\mathsf{N}^\ell}$ such that $s \overset{a}{\Rightarrow}_{\mathsf{N}^\ell} D$. Then there exists E, such that $s \overset{a}{\Rightarrow}_{\mathsf{N}} E$, and $D(\widehat{\equiv_{\mathcal{N}_{priv}}})E$.

Notation 25. Let $\mathsf{N}_1 = (\mathcal{S}_{\mathsf{N}_1}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_{\mathsf{N}_1})$ and $\mathsf{N}_2 = (\mathcal{S}_{\mathsf{N}_2}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_{\mathsf{N}_2})$ be two NPLTSs, with the same set of actions. We define the *disjoint union of* N_1 *and* N_2 as the NPLTS $\mathsf{N}_1 \dot{+} \mathsf{N}_2 := (\mathcal{S}_{\mathsf{N}_1} \sqcup \mathcal{S}_{\mathsf{N}_2}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_{\mathsf{N}_1 \dot{+} \mathsf{N}_2})$ where the transition function $\mathsf{trans}_{\mathsf{N}_1 \dot{+} \mathsf{N}_2}$ defined as:

$$\mathsf{trans}_{\mathsf{N}_1 \dot{+} \mathsf{N}_2}(s) = \begin{cases} \mathsf{trans}_{\mathsf{N}_1}(s) \text{ when } s \in \mathcal{S}_{\mathsf{N}_1} \\ \mathsf{trans}_{\mathsf{N}_2}(s) \text{ when } s \in \mathcal{S}_{\mathsf{N}_2}. \end{cases}$$

In the following, when considering $\mathsf{N}_1 \dot{+} \mathsf{N}_2$, where N_1 and N_2 have non disjoint states spaces, we will write $s^{\mathsf{N}_1}, s^{\mathsf{N}_2}$ to design the copies of s in $\mathcal{S}_{\mathsf{N}_1}$ and $\mathcal{S}_{\mathsf{N}_2}$ respectively. Similarly, if D is a distribution over $\mathcal{S}_{\mathsf{N}_1} \cup \mathcal{S}_{\mathsf{N}_2}$, we will write D^{N_1} and D^{N_2} to mean the distributions over $\mathcal{S}_{\mathsf{N}_1} \sqcup \mathcal{S}_{\mathsf{N}_2}$ where all states s in the support of the distribution are taken in $\mathcal{S}_{\mathsf{N}_1}$ and $\mathcal{S}_{\mathsf{N}_2}$ respectively.

Lemma 42. Let N be a new -determinization of N^ℓ. Then the binary relation $R \subseteq \mathcal{S}_{\mathsf{N}^\ell \dot{+} \mathsf{N}} \times \mathcal{S}_{\mathsf{N}^\ell \dot{+} \mathsf{N}}$ defined as $R = \{(s^{\mathsf{N}^\ell}, t^{\mathsf{N}}) \mid s \equiv_{\mathcal{N}_{priv}} t\} \cup \{(s^{\mathsf{N}}, t^{\mathsf{N}^\ell}) \mid s \equiv_{\mathcal{N}_{priv}} t\}$, is a (strong) bisimulation on the NPLTS $\mathsf{N}_1 \dot{+} \mathsf{N}_2$.

Proof. First, we can easily check that it is an equivalence relation (reflexive, transitive and symmetric).

- Let $(s^{\mathsf{N}^\ell}, t^{\mathsf{N}})$ such that $s \equiv_{\mathcal{N}_{priv}} t$, and let be a such that $s^{\mathsf{N}^\ell} \xrightarrow{a}_{\mathsf{N}^\ell \dot{+} \mathsf{N}} D^{\mathsf{N}^\ell}$. Then by definition of the transition function $\mathsf{trans}_{\mathsf{N}^\ell \dot{+} \mathsf{N}}$, it means that $s \xrightarrow{a}_{\mathsf{N}^\ell} D$. Using Lemma 40, we see that there exists E such that $s \xrightarrow{a}_{\mathsf{N}} E$, and $D(\widehat{\equiv_{\mathcal{N}_{priv}}})E$. Since we know from Lemma 39 that $\equiv_{\mathcal{N}_{priv}}$ is a bisimulation on N, and since by hypothesis $s \equiv_{\mathcal{N}_{priv}} t$, we obtain the existence of a third distribution F such that $t \xrightarrow{a}_{\mathsf{N}} F$, and $E\widehat{\equiv_{\mathcal{N}_{priv}}}F$. Recall that by definition of $\mathsf{N}^\ell \dot{+} \mathsf{N}$, $t \xrightarrow{a}_{\mathsf{N}} F$ implies that $t^{\mathsf{N}} \xrightarrow{a}_{\mathsf{N}^\ell \dot{+} \mathsf{N}} F^{\mathsf{N}}$. Moreover, since $\equiv_{\mathcal{N}_{priv}}$ is transitive, and since $\widehat{\cdot}$ preserves transitivity–from **??**–, we can conclude that $D\widehat{\equiv_{\mathcal{N}_{priv}}}F$.

- Let $(s^{\mathsf{N}}, t^{\mathsf{N}^\ell})$ such that $s \equiv_{\mathcal{N}_{priv}} t$, and let be a such that $s^{\mathsf{N}} \xrightarrow{a}_{\mathsf{N}^\ell \dot{+} \mathsf{N}} D^{\mathsf{N}}$. Then it is also true that $s^{\mathsf{N}^\ell} \xrightarrow{a}_{\mathsf{N}^\ell \dot{+} \mathsf{N}} D^{\mathsf{N}^\ell}$. Since by Lemma 39 $\equiv_{\mathcal{N}_{priv}}$ is a bisimulation on N^ℓ, we obtain directly a distribution F such that $t \xrightarrow{a}_{\mathsf{N}^\ell} F$, and $D\widehat{\equiv_{\mathcal{N}_{priv}}}F$, and we conclude from there.

□

Corollary 5. Let N be a new -determinization of N^ℓ. Then $\leq_{tr}^{\mathsf{N}}$ coincides with $\leq_{tr}^{\mathsf{N}^\ell}$.

Proof. It is known–and easy to prove–that any pair (s, t) of bisimular states in a NPLTS N have also the same supremum probability of doing a trace. Using that fact, and Lemma 42, we see that for any state in N^ℓ, and for any $w \in ((\mathcal{A}_{ext})_{\mathsf{N}^\ell})^\star$:

$$\begin{aligned}
\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}(s, w) &= \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell \dot{+} \mathsf{N})}(s^{\mathsf{N}^\ell}, w) \text{ by definition of NPLTSs dijoint union} \\
&= \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell \dot{+} \mathsf{N})}(s^{\mathsf{N}}, w) \text{ since } s^{\mathsf{N}^\ell}, s^{\mathsf{N}} \text{ are bisimilar by Lemma 42} \\
&= \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N})}(s, w),
\end{aligned}$$

and we can conclude from there. □

Corollary 6. Let N be a new -determinization of N^ℓ. Then $\leq_{sim}^{\mathsf{N}}$ coincides with $\leq_{sim}^{\mathsf{N}^\ell}$.

Proof.
- Let us first show that $\leq_{sim}^{\mathsf{N}}$ is a simulation on N^ℓ: let $s, t \in \mathcal{SP}_\ell$ such that $s \leq_{sim}^{\mathsf{N}} t$. We suppose that for some $a \in \mathcal{A}_{\mathsf{N}^\ell}$, $s \xrightarrow{a}_{\mathsf{N}^\ell} D$. From there, we can write that $s^{\mathsf{N}^\ell} \xrightarrow{a}_{\mathsf{N}^\ell \dot{+} \mathsf{N}} D^{\mathsf{N}^\ell}$. By Lemma 42, there exists E such that $D\widehat{\equiv_{\mathcal{N}_{priv}}}E$, and $s^{\mathsf{N}} \xrightarrow{a}_{\mathsf{N}^\ell \dot{+} \mathsf{N}} E^{\mathsf{N}}$. From there, we are able to use the fact that $s \leq_{sim}^{\mathsf{N}} t$, to obtain a third distribution F such that $t^{\mathsf{N}} \overset{a}{\Rightarrow}_{\mathsf{N}^\ell \dot{+} \mathsf{N}} F^{\mathsf{N}}$, and $E\widehat{\leq_{sim}^{\mathsf{N}}}F$. Since a strong bisimulation is also a weak bisimulation for any NPLTS–and Proposition 4–we can again use Lemma 42 to get a distribution H such that $F\widehat{\equiv_{\mathcal{N}_{priv}}}H$ and $t^{\mathsf{N}^\ell} \overset{a}{\Rightarrow}_{\mathsf{N}^\ell \dot{+} \mathsf{N}} H^{\mathsf{N}^\ell}$. To recap, it means that we have $t \overset{a}{\Rightarrow}_{\mathsf{N}^\ell} H$, and $D\,(\widehat{\equiv_{\mathcal{N}_{priv}}}; \widehat{\leq_{sim}^{\mathsf{N}}}; \widehat{\equiv_{\mathcal{N}_{priv}}})\,H$. By Lemma 39, $\equiv_{\mathcal{N}_{priv}} \subseteq \leq_{sim}^{\mathsf{N}}$, and we can conclude by transitivity of $\leq_{sim}^{\mathsf{N}}$ and Lemma **??**.

- We show similarly that $\leq_{sim}^{\mathsf{N}^\ell}$ is a simulation on N.

□

As a consequence from Corollary 5 and **??**, it is enough to consider N, a strict new -determinization of N^ℓ.

F Simulation and observational preorders coincide

This section is dedicated to the proof of Proposition 5.

F.1 Some preliminary results

Lemma 43. For all $a \in \mathcal{N}$, for all ground terms t, if $a \notin st(t)$ then $a \neq t$.

Proof. Recall that $\doteq$ is closed under substitution of names by other terms. Let $b \in \mathcal{N} \setminus \{a, st(t)\}$ and $\sigma = \{^b/_a\}$. Thus, if $a \doteq t$ then $a\sigma \doteq t\sigma$ and $b \doteq t$ which would imply $a \doteq b$ which contradicts our hypothesis. □

Lemma 44. Let $(\mathcal{P}, \phi) \in \mathcal{SP}_\ell$. For all $\mathcal{P} \xrightarrow{\tau} \delta_{\mathcal{P}'}$ by application of the rules (Par) or (Nil), $\mathcal{P} \approx_{obs}^{\mathcal{R}_r} \mathcal{P}'$ and $(\mathcal{P}, \phi) \approx_{bi}^{\mathsf{N}^\ell} (\mathcal{P}', \phi)$.

Proof. Trivial. □

Lemma 45. Let $\mathcal{P}, \mathcal{P}' \in \mathcal{SP}$, ϕ, ϕ' be two frames and ρ be a renaming of names.

If one of the two following properties holds

- $img(\rho) \cap names(\mathcal{P}, \mathcal{P}', \phi, \phi') = \varnothing$ and $dom(\rho) \cap img(\rho) = \varnothing$
- $(fn(\mathcal{P}, \mathcal{P}', \phi, \phi') \cap \mathcal{N}_{priv}) = dom(\rho)$ and $img(\rho) \subseteq \mathcal{N}_{priv}$

then

- For all $R \in \{\leq_{obs}^{\mathcal{R}_r}, \approx_{obs}^{\mathcal{R}_r}\}$, $\mathcal{P}\ R\ \mathcal{P}'$ if and only if $\mathcal{P}\rho\ R\ \mathcal{P}'\rho$
- For all $R \in \{\leq_{sim}^{\mathsf{N}^\ell}, \approx_{bi}^{\mathsf{N}^\ell}\}$, $(\mathcal{P}, \phi)\ R\ (\mathcal{P}', \phi')$ if and only if $(\mathcal{P}, \phi)\rho\ R\ (\mathcal{P}', \phi')\rho$.

Proof. Direct by noticing that $\doteq$ is closed by under substitution of names by other terms, i.e. for all u, v such that $img(\rho) \cap names(u, v)$, $u \doteq v$ if and only if $u\rho \doteq v\rho$. □

Lemma 46. Let $\mathsf{N} = (\mathcal{S}_\mathsf{N}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_\mathsf{N})$ be a NPLTS, $D, E \in \mathcal{D}^{\leq 1}(\mathcal{S}_\mathsf{N})$ and R be a relation over $\mathcal{S}_\mathsf{N}$. If D has a finite support and $D\ \widehat{R}\ E$ then there exists a family of sub-distributions $\{E_x\}_{x \in \mathrm{supp}(D)}$ such that:

- for all $y \in \mathcal{S}_\mathsf{N}$, $\sum_{x \in \mathrm{supp}(D)} E_x(y) \leq E(y)$
- for all $x \in \mathrm{supp}(D)$, $D(x) \cdot \delta_x\ \widehat{R}\ E_x$ and $\mathrm{supp}(E_x) = R(\{x\})$

Proof. For this proof, we rely on [LSA14, Lemma 3.9] that states the following: Assume $p_1, \ldots, p_n \leq 1$ and a family $\{r_I \leq 1\}_{I \subseteq \{1,\ldots,n\}}$. If for all $I \subseteq \{1, \ldots, n\}$, $\sum_{i \in I} p_i \leq \sum_{\substack{J \subseteq \{1,\ldots,n\} \\ J \cap I \neq \varnothing}} r_J \leq 1$ then for all nonempty $I \subseteq \{1, \ldots, n\}$, for all $k \in I$, there exists $s_{k,I} \leq 1$ such that:

- for all $I \subseteq \{1, \ldots, n\}$, $\sum_{k \in I} s_{k,I} \leq 1$

- for all $k \in \{1, \dots, n\}$, $p_k \leq \sum_{\substack{I \subseteq \{1,\dots,n\} \\ k \in I}} s_{k,I} \cdot r_I$.

We know that D has finite support. Hence, we can consider $\mathrm{supp}(D) = \{x_1, \dots, x_n\}$ and so we define for all $i \in \{1, \dots, n\}$, $p_i = D(x_i)$. For all $I \subseteq \{1, \dots, n\}$, let us define the sets $X_I = \{x_i\}_{i \in I}$ and S_I such that:

$$S_I = \{y \in \mathcal{S}_{\mathsf{N}} \mid \forall i \in \{1, \dots, n\}, x_i \ R \ y \Leftrightarrow i \in I\}$$

First, notice that $S_I \cap S_J \neq \varnothing$ implies $I = J$. Second, let us show that $R(X_I) = \bigcup_{\substack{J \subseteq \{1,\dots,n\} \\ J \cap I \neq \varnothing}} S_J$. Let $y \in R(X_I)$. There exists $i \in I$ such that $x_i \ R \ y$. By taking the largest set $J \subseteq \{1, \dots, n\}$ such that for all $j \in J$, $x_j \ R \ y$, we deduce that $y \in S_J$. Notice that $i \in J$ and so $J \cap I \neq \varnothing$. On the other hand, for all $J \subseteq \{1, \dots, n\}$, for all $y \in J$, if $J \cap I \neq \varnothing$ then there exists $i \in I$ such that $x_i \ R \ y$ an so $y \in R(X_I)$.

Thus, for all $I \subseteq \{1, \dots, n\}$, we define $r_I = E(S_I)$. Recall that $D \ \widehat{R} \ E$ and $S_I \cap S_J \neq \varnothing$ implies $I = J$. Therefore we obtain that for all $I \subseteq \{1, \dots, n\}$, $\sum_{i \in I} p_i = D(X_I) \leq E(R(X_I)) = \sum_{\substack{J \subseteq \{1,\dots,n\} \\ J \cap I \neq \varnothing}} E(S_J)$. Hence, for all nonempty $I \subseteq \{1, \dots, n\}$, for all $k \in I$, there exists $s_{k,I} \leq 1$ such that:

- for all $I \subseteq \{1, \dots, n\}$, $\sum_{k \in I} s_{k,I} \leq 1$
- for all $k \in \{1, \dots, n\}$, $D(x_k) \leq \sum_{\substack{I \subseteq \{1,\dots,n\} \\ k \in I}} s_{k,I} \cdot E(S_I)$.

For all $k \in \{1, \dots, k\}$, we define the sub-distribution $E_{x_k} = \sum_{\substack{I \subseteq \{1,\dots,n\} \\ k \in I}} s_{k,I} \cdot \sum_{y \in S_I} E(y) \cdot \delta_y$. Let us show the two desired properties:

- Let $y \in \mathcal{S}_{\mathsf{N}}$. Since $S_I \cap S_J \neq \varnothing$ implies $I = J$, there is a most one $I \subseteq \{1, \dots, n\}$ such that $y \in S_I$. Hence $\sum_{k=1}^{n} E_{x_k}(y) = \sum_{k=1, k \in I}^{n} s_{k,I} \cdot E(y) = E(y) \cdot \sum_{k=1, k \in I}^{n} s_{k,I} \leq E(y)$.
- for all $k \in \{1, \dots, n\}$, $D(x_k) \leq \sum_{\substack{I \subseteq \{1,\dots,n\} \\ k \in I}} s_{k,I} \cdot E(S_I)$. By taking $X_{\{k\}}$, we already showed that $R(\{x_k\}) = \bigcup_{\substack{I \subseteq \{1,\dots,n\} \\ I \cap \{k\} \neq \varnothing}} S_I$. Hence $E_{x_k}(R(\{x_k\}) = \sum_{\substack{I \subseteq \{1,\dots,n\} \\ k \in I}} E_{x_k}(S_I)$. Since $E_{x_k}(S_I) = s_{k,I} \cdot E(S_I)$, we conclude that $D(x_k) \cdot \delta_{x_k} \ \widehat{R} \ E_{x_k}$. □

The following lemma is similar to the previous one but for equivalence relation.

Lemma 47. Let $\mathsf{N} = (\mathcal{S}_{\mathsf{N}}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_{\mathsf{N}})$ be a NPLTS, $D, E \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{N}})$ and R be an equivalence relation over $\mathcal{S}_{\mathsf{N}}$. If $D \ \widehat{R} \ E$ and $E \ \widehat{R} \ D$ then there exists a family of sub-distributions $\{E_x\}_{x \in \mathrm{supp}(D)}$ such that:

- $\sum_{x \in \mathrm{supp}(D)} E_x = E$
- for all $x \in \mathrm{supp}(D)$, $D(x) \cdot \delta_x \ \widehat{R} \ E_x$, $E_x \ \widehat{R} \ D(x) \cdot \delta_x$ and $\mathrm{supp}(E_x) = R(\{x\})$

Proof. Since R is an equivalence relation, $D \ \widehat{R} \ E$ and $E \ \widehat{R} \ D$ imply that for all $x \in \mathrm{supp}(D)$, $D(R(\{x\})) = E(R(\{x\}))$. Hence, we define $E_x = \sum_{y \in R(x)} \frac{E(y) \cdot D(x)}{E(R\{x\})} \delta_y$. For all $y \in \mathcal{S}_{\mathsf{N}}$,

$$\sum_{x \in \mathrm{supp}(D)} E_x(y) = \sum_{x \in \mathrm{supp}(D) \cap R(\{y\})} \frac{E(y) \cdot D(x)}{E(R(\{x\}))} = E(y)$$

Moreover, for all $x \in \mathrm{supp}(D)$, $E_x(R(\{x\})) = \sum_{y \in R(\{x\})} \frac{E(y) \cdot D(x)}{E(R\{x\})} = D(x)$ which allows us to conclude. $\square$

In the following, we say that $D \xrightarrow{\tau}_{\mathsf{r}} E$ *has finite support* if both D and E have finite support. Similarly, $D \xRightarrow{\tau}_{\mathsf{r}} E$ has finite support if all $D_k^{\rightarrow} \xrightarrow{\tau}_{\mathsf{r}} D_{k+1}^{\rightarrow} + D_{k+1}^{\top}$ composing the infinite scheme of $D \xRightarrow{\tau}_{\mathsf{r}} E$ have also finite support. Note that it implies that D has finite support but E may still have infinite support.

Lemma 48. Let $\mathsf{N} \in \{\mathsf{N}^{\ell}, \mathsf{N}^{o}\}$. Let $D_1, D_2, E_1, E_2 \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{N}})$. Let R be a relation on $\mathcal{S}_{\mathsf{N}}$. We have the following properties:

1. $D_1 \ \widehat{R} \ D_2$, $E_1 \ \widehat{R} \ E_2$ and $(D_2 + E_2) \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{N}})$ imply $D_1 + E_1 \ \widehat{R} \ D_2 + E_2$.
2. $\forall \alpha$, $D_1 \ \widehat{R} \ D_2$ and $\alpha \cdot D_2 \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{N}})$ imply $\alpha \cdot D_1 \ \widehat{R} \ \alpha \cdot D_2$
3. if $D_1 + D_2 \ \widehat{R} \ E$ and D_1, D_2 have finite support (resp. $D_1 + D_2 \ \widehat{R} \ E$, $E \ \widehat{R} \ D_1 + D_2$ and R is an equivalence relation) then there exist E_1, E_2 such that $E_1 + E_2 = E$ and $D_i \ \widehat{R} \ E_i$ (resp. $D_i \ \widehat{R} \ E_i$ and $E_i \ \widehat{R} \ D_i$) for $i = 1, 2$
4. if $D_1 \ \widehat{R} \ E_1$ and $\forall x \in \mathrm{supp}(D_1)$, $\forall y \in R(x)$, $x \to F_1$ implies $\delta_y \xRightarrow{\tau}_{\mathsf{r}} F_2$ and $F_1 \ \widehat{R} \ F_2$ then
   (a) $D_1 \xrightarrow{\tau}_{\mathsf{r}} D_2$ with finite support implies $E_1 \xRightarrow{\tau}_{\mathsf{r}} E_2$ and $D_2 \ \widehat{R} \ E_2$
   (b) $D_1 \xRightarrow{\tau}_{\mathsf{r}} D_2$ with finite support implies $E_1 \xRightarrow{\tau}_{\mathsf{r}} E_2$ and $D_2 \ \widehat{R} \ E_2$
5. if R is an equivalence relation, $D_1 \ \widehat{R} \ E_1$, $E_1 \ \widehat{R} \ D_1$ and $\forall x \in \mathrm{supp}(D_1)$, $\forall y \in R(x)$, $x \to F_1$ implies $\delta_y \xRightarrow{\tau}_{\mathsf{r}} F_2$, $F_1 \ \widehat{R} \ F_2$ and $F_2 \ \widehat{R} \ F_1$ then
   (a) $D_1 \xrightarrow{\tau}_{\mathsf{r}} D_2$ implies $E_1 \xRightarrow{\tau}_{\mathsf{r}} E_2$, $D_2 \ \widehat{R} \ E_2$ and $E_2 \ \widehat{R} \ D_2$
   (b) $D_1 \xRightarrow{\tau}_{\mathsf{r}} D_2$ and $D_2 \in \mathcal{D}(\mathcal{S}_{\mathsf{N}})$ imply $E_1 \xRightarrow{\tau}_{\mathsf{r}} E_2$, $D_2 \ \widehat{R} \ E_2$ and $E_2 \ \widehat{R} \ D_2$

Proof. Properties 1 and 2 are immediate, by definition of $\widehat{R}$.

For Property 3, let $D = D_1 + D_2$. If D has finite support, we can apply Lemma 46 to obtain the family sub-distributions $\{E_x\}_{x \in \mathrm{supp}(D)}$ such that

- for all $y \in \mathcal{S}_{\mathsf{N}}$, $\sum_{x \in \mathrm{supp}(D)} E_x(y) \leq E(y)$
- for all $x \in \mathrm{supp}(D)$, $D(x) \cdot \delta_x \ \widehat{R} \ E_x$ and $\mathrm{supp}(E_x) = R(\{x\})$

Let us define

$$E'_1 = \sum_{x \in \mathrm{supp}(D)} \frac{D_1(x)}{D(x)} \cdot E_x \quad \text{and} \quad E'_2 = \sum_{x \in \mathrm{supp}(D)} \frac{D_2(x)}{D(x)} \cdot E_x$$

We first prove that $D_i \ \widehat{R} \ E'_i$ for $i \in \{1, 2\}$. We know that for all $x \in \mathrm{supp}(D)$, $D(x) \cdot \delta_x \ \widehat{R} \ E_x$. Hence, $D_i(x) \cdot \delta_x \ \widehat{R} \ \frac{D_i(x) \cdot E_x}{D(x)}$ and so $D_i \ \widehat{R} \ E'_i$. Finally, since for all $y \in \mathcal{S}_{\mathsf{N}}$, $\sum_{x \in \mathrm{supp}(D)} E_x(y) \leq E(y)$ and $\sum_{x \in \mathrm{supp}(D)} E_x = E'_1 + E'_2$, there exists H such that $E'_1 + E'_2 + H = E$, meaning that we can arbitrarily define $E_1 = E'_1 + H_1$ and $E_2 = E'_2 + H_2$ with $H_1 + H_2 = H$ in order to conclude.

If R is an equivalence relation, $D_1 + D_2 \ \widehat{R} \ E$ and $E \ \widehat{R} \ D_1 + D_2$, then we can instead apply Lemma 47. Hence, for $i \in \{1, 2\}$, for all $x \in \mathrm{supp}(D)$, $D_i(x) \cdot \delta_x \ \widehat{R} \ \frac{D_i(x) \cdot E_x}{D(x)}$ and $\frac{D_i(x) \cdot E_x}{D(x)} \ \widehat{R} \ D_i(x) \cdot \delta_x$. Defining E'_1 and E'_2 as above we obtain that $D_i \ \widehat{R} \ E'_i$ and $E'_i \ \widehat{R} \ D_i$. Moreover, by Lemma 47, for all $y \in \mathcal{S}_{\mathsf{N}}$, $\sum_{x \in \mathrm{supp}(D)} E_x(y) = E(y)$ and so $E'_1 + E'_2 = E$ which allows us to conclude.

We now prove Property 4a. Assume that D_1 has finite support, $D_1 \ \widehat{R} \ E_1$ and $\forall x \in \mathrm{supp}(D_1)$, $\forall y \in R(x)$, $x \to F_1$ implies $\delta_y \overset{\tau}{\Longrightarrow}_{\mathsf{r}} F_2$ and $F_1 \ \widehat{R} \ F_2$.

Let us assume that $D_1 \overset{\tau}{\to}_{\mathsf{r}} D_2$ and D_2 has finite support. Thus there exists a countable set I and a multiset $\{x_i\}_{i \in I}$ with for all $i \in I$, $x_i \in \mathcal{S}_{\mathsf{N}}$ such that $D_1 = \sum_{i \in I} \alpha_i \cdot \delta_{x_i}$, $D_2 = \sum_{i \in I} \alpha_i \cdot F_i$ and for all $i \in I$, $x_i \to F_i$. Note that by hypothesis, $x_i \to F_i$ implies that F_i has finite support. Thus, D_2 having finite support allows us to consider w.l.o.g that I is finite.

By applying Lemma 46, $D_1 \ \widehat{R} \ E_1$ implies that there exists $\{E_x\}_{x \in D_1}$ such that

- for all $y \in \mathcal{S}_{\mathsf{N}}$, $\sum_{x \in \mathrm{supp}(D_1)} E_x(y) \leq E_1(y)$
- for all $x \in \mathrm{supp}(D_1)$, $D_1(x) \cdot \delta_x \ \widehat{R} \ E_x$ and $\mathrm{supp}(E_x) = R(\{x\})$

Let $i \in I$. Let $y \in \mathrm{supp}(E_{x_i})$. As $y \in R(\{x_i\})$, by hypothesis, $\delta_y \overset{\tau}{\Longrightarrow}_{\mathsf{r}} F'_{i,y}$ and $F_i \ \widehat{R} \ F'_{i,y}$. Thus by properties 1 and 2, $\sum_{y \in \mathrm{supp}(E_{x_i})} E_{x_i}(y) \cdot F_i \ \widehat{R} \ \sum_{y \in \mathrm{supp}(E_{x_i})} E_{x_i}(y) \cdot F'_{i,y}$ and hence $F_i \ \widehat{R} \ \sum_{y \in \mathrm{supp}(E_{x_i})} \frac{E_{x_i}(y)}{E_{x_i}(R(\{x_i\})} \cdot F'_{i,y}$. Since $E_2 = \sum_{i \in I} \alpha_i \cdot F_i$, if we denote $H_2 = \sum_{i \in I} \sum_{y \in \mathrm{supp}(E_{x_i})} \frac{\alpha_i \cdot E_{x_i}(y)}{E_{x_i}(R(\{x_i\}))} \cdot F'_{i,y}$ then $D_2 \ \widehat{R} \ H_2$. Notice that:

$$\begin{aligned}
H_2 &= \sum_{x \in \mathrm{supp}(D_1)} \sum_{\substack{i \in I \\ x = x_i}} \sum_{y \in \mathrm{supp}(E_{x_i})} \frac{\alpha_i \cdot E_{x_i}(y)}{E_{x_i}(R(\{x_i\}))} \cdot F'_{i,y} \\
&= \sum_{x \in \mathrm{supp}(D_1)} \sum_{\substack{i \in I \\ x = x_i}} \sum_{y \in \mathrm{supp}(E_{x_i})} \frac{\alpha_i \cdot E_{x_i}(y)}{E_x(R(\{x\}))} \cdot F'_{i,y} \\
&= \sum_{x \in \mathrm{supp}(D_1)} \sum_{\substack{i \in I \\ x = x_i}} \frac{\alpha_i}{E_x(R(\{x\}))} \cdot \sum_{y \in \mathrm{supp}(E_{x_i})} E_{x_i}(y) \cdot F'_{i,y}
\end{aligned}$$

Furthermore, we know that for all $i \in I$, for all $y \in R(\{x_i\})$, $\delta_y \overset{\tau}{\Longrightarrow}_{\mathsf{r}} F'_{i,y}$. Therefore, $E_{x_i} \overset{\tau}{\Longrightarrow}_{\mathsf{r}} \sum_{y \in \mathrm{supp}(E_{x_i})} E_{x_i}(y) \cdot F'_{i,y}$, which implies that:

$$\sum_{x \in \mathrm{supp}(D_1)} \sum_{\substack{i \in I \\ x = x_i}} \frac{\alpha_i}{E_x(R(\{x\}))} \cdot E_x \overset{\tau}{\Longrightarrow}_{\mathsf{r}} H_2$$

Note that the following holds:

$$\begin{aligned}
\sum_{x \in \mathrm{supp}(D_1)} \sum_{\substack{i \in I \\ x = x_i}} \frac{\alpha_i}{E_x(R(\{x\})} \cdot E_x &= \sum_{x \in \mathrm{supp}(D_1)} \frac{\sum_{\substack{i \in I \\ x = x_i}} \alpha_i}{E_x(R(\{x\}))} \cdot E_x \\
&= \sum_{x \in \mathrm{supp}(D_1)} \frac{D_1(x)}{E_x(R(\{x\}))} \cdot E_x
\end{aligned}$$

Hence, if we denote $H_1 = \sum_{x \in \mathrm{supp}(D_1)} \frac{D_1(x)}{E_x(R(\{x\}))} \cdot E_x$, we obtain $H_1 \overset{\tau}{\Longrightarrow}_{\mathsf{r}} H_2$. Finally, we know that for all $x \in \mathrm{supp}(D_1)$, $D_1(x) \leq E_x(R(\{x\}))$ and for all $y \in \mathcal{S}_{\mathsf{N}}$, $\sum_{x \in \mathrm{supp}(D_1)} E_x(y) \leq E_1(y)$. Thus, there exists H'_1 such that $E_1 = H_1 + H'_1$. This allows us to deduce that $E_1 \overset{\tau}{\Longrightarrow}_{\mathsf{r}} H_2 + H'_1$ and $D_2 \ \widehat{R} \ (H_2 + H'_1)$. This completes the proof of property 4a.

The proof for property 5a follows very closely. Instead of using Lemma 46, we rely on Lemma 47. Note in this case, $D_1(x) = E_x(R(\{x\}))$ implying that $H_1 = \sum_{x \in \mathrm{supp}(D_1)} E_x = E_1$. This allows us to conclude the proof of property 5a.

Let us now prove property 4b. Assume $D_1 \overset{\tau}{\Longrightarrow}_{\mathsf{r}} D_2$ with internal finite support. By definition, there exists the following infinite scheme:

$$\begin{aligned}
&D_1 = D_0^{\rightarrow} + D_0^{\top} \\
&D_0^{\rightarrow} \overset{\tau}{\rightarrow}_{\mathsf{r}} D_1^{\rightarrow} + D_1^{\top} \\
&\dots \\
&D_k^{\rightarrow} \overset{\tau}{\rightarrow}_{\mathsf{r}} D_{k+1}^{\rightarrow} + D_{k+1}^{\top} \\
&\dots
\end{aligned}$$

such that $D_2 = \sum_{k \in \mathbb{N}} D_k^{\top}$ and for all $k \in \mathbb{N}$, $D_k^{\rightarrow}$ and $D_k^{\top}$ have finite support. We can easily show by induction that for all $k \in \mathbb{N}$,

- $E_1 \overset{\tau}{\Longrightarrow}_{\mathsf{r}} E_k^{\rightarrow} + \sum_{i=0}^{k} E_i^{\top}$
- $D_k^{\rightarrow} \ \widehat{R} \ E_k^{\rightarrow}$
- $\sum_{i=0}^{k} D_i^{\top} \ \widehat{R} \ \sum_{i=0}^{k} E_i^{\top}$

In the base case $k = 0$, we can apply Property 3 to deduce that there exists $E_0^{\rightarrow}$ and $E_0^{\top}$ such that $E = E_0^{\rightarrow} + E_0^{\top}$ and for all $\alpha \in \{\rightarrow, \top\}$, $D_0^{\alpha} \ \widehat{R} \ E_0^{\alpha}$.

In the inductive step $k > 0$, we know that $D_{k-1}^{\rightarrow} \xrightarrow{\tau}_{\mathsf{r}} D_k^{\rightarrow} + D_k^{\top}$. By induction hypothesis, we know that there exist $E_1 \Longrightarrow_{\mathsf{r}} E_{k-1}^{\rightarrow} + \sum_{i=0}^{k-1} E_i^{\top}$ such that $E_{k-1}^{\rightarrow} \ \widehat{R} \ E_{k-1}^{\rightarrow}$ and $\sum_{i=0}^{k-1} D_i^{\top} \ \widehat{R} \ \sum_{i=0}^{k-1} E_i^{\top}$. By applying Property 4a, we obtain that $E_{k-1}^{\rightarrow} \Longrightarrow_{\mathsf{r}} E'$ such that $D_k^{\rightarrow} + D_k^{\top} \ \widehat{R} \ E'$. By applying Property 3, we deduce that there exists $E_k^{\rightarrow}, E''$ such that $E' = E_k^{\rightarrow} + E_k^{\top}$, $D_k^{\rightarrow} \ \widehat{R} \ E_k^{\rightarrow}$ and $D_k^{\top} \ \widehat{R} \ E_k^{\top}$. Therefore, $\sum_{i=0}^{k} D_i^{\top} \ \widehat{R} \ \sum_{i=0}^{k} E_i^{\top}$. Note that $E_{k-1}^{\rightarrow} \Longrightarrow_{\mathsf{r}} E_k^{\rightarrow} + E_k^{\top}$ implies $E_{k-1}^{\rightarrow} + \sum_{i=0}^{k-1} E_i^{\top} \Longrightarrow_{\mathsf{r}} E_k^{\rightarrow} + \sum_{i=0}^{k} E_i^{\top}$. This concludes the inductive proof.

In the case where $\lim_{k\to\infty} E_k^{\rightarrow}$ exists, we obtain that $E_1 \Longrightarrow_{\mathsf{r}} \lim_{k\to\infty} E_k^{\rightarrow} + \sum_{k\in\mathbb{N}} E_k^{\top}$ with $\sum_{k\in\mathbb{N}} D_i^{\top} \ \widehat{R} \ \sum_{k\in\mathbb{N}} E_k^{\top}$. Hence, we conclude by defining $E_2 = \lim_{k\to\infty} E_k^{\rightarrow} + \sum_{k\in\mathbb{N}} E_k^{\top}$ and so $D_2 \ \widehat{R} \ E_2$. In the case $\lim_{k\to\infty} E_k^{\rightarrow}$ does not exist, the semantics in Figures 2 and 10 imply that there exists $k_! \in \mathbb{N}$ and a set S such that for all $k > k_!$, $\mathrm{supp}(E_k^{\rightarrow}) \cap \{\{!P\} \cup \mathcal{P} \in \mathcal{SP}\} = S$ (resp. $\{(\{!P\}, \phi) \cup \mathcal{P} \in \mathcal{SP}\}$ when $\mathsf{N} = \mathsf{N}^{\ell}$). Note that if we define $E_k^S = \sum_{x\in S} E_k^{\rightarrow}(x) \cdot \delta_x$ then $\lim_{k\to\infty} E_k^S$ exists. Moreover, thanks to Remark 7, we have that $E_k^{\rightarrow} \xrightarrow{\tau}_{\mathsf{r}} E_k^S$. Thus, $E_1 \Longrightarrow_{\mathsf{r}} E_k^S + \sum_{i=0}^{k} E_i^{\top}$. We can therefore conclude by defining $E_2 = \lim_{k\to\infty} E_k^S + \sum_{k\in\mathbb{N}} E_k^{\top}$.

Finally, the proof of property 5b follows the same reasoning as property 4b: We prove by induction that for all $k \in \mathbb{N}$,

- $E_1 \Longrightarrow_{\mathsf{r}} E_k^{\rightarrow} + \sum_{i=0}^{k} E_i^{\top}$
- $D_k^{\rightarrow} \ \widehat{R} \ E_k^{\rightarrow}$ and $E_k^{\rightarrow} \ \widehat{R} \ D_k^{\rightarrow}$
- $\sum_{i=0}^{k} E_i^{\top} \ \widehat{R} \ \sum_{i=0}^{k} D_i^{\top}$

The base case once again uses property 3 but the inductive step relies on property 5a rather than property 4a. To conclude the final proof, we know that $E_2 \in \mathcal{D}(\mathcal{S}_{\mathsf{N}})$. Thus, $\lim_{k\to\infty} E_k^{\rightarrow} = \varnothing$. This allows us to conclude by defining $E = \sum_{k\in\mathbb{N}} E_k^{\top}$. □

F.1.1 Properties on $\mathbf{RProb}_{\mathcal{R}_{\mathsf{r}}^o}(\mathcal{P}, \downarrow c)$

We define $\mathcal{R}_{\mathsf{r}}^{of} = \{(\mathcal{S}, \mathsf{corr}, \mathsf{trans}) \in \mathcal{R}_{\mathsf{r}}^o \mid \forall s \in \mathcal{S}, \mathsf{trans}(s) = D \text{ implies } D \text{ has finite support}\}$.

Let us define $\mathcal{P} \equiv \mathcal{P}'$ when there exists a renaming of names ρ such that $fn(\mathcal{P}) \cap \mathcal{N}_{priv} = dom(\rho)$, $img(\rho) \subseteq \mathcal{N}_{priv}$ and $\mathcal{P}\rho = \mathcal{P}'$. Note that $\mathcal{P} \equiv \mathcal{P}'$ implies $\mathcal{P} \approx_{obs} \mathcal{P}'$ thanks to Lemma 45. Given a distribution F, we denote $F/_{\equiv} = \sum_{x\in\mathrm{supp}(F)/_{\equiv}} \sum_{y\equiv x} F(y) \cdot \delta_x$. Given two distributions F and F', we say that $F \equiv F'$ when $F/_{\equiv} = F'/_{\equiv}$.

Lemma 49. For all $F, H \in \mathcal{D}^{\leq 1}(\mathsf{N}^o)$, $F \xrightarrow{\tau}_{\mathsf{r}} H$ with F having finite support implies that $F \xrightarrow{\tau}_{\mathsf{r}} H'$ with $H \equiv H'$ and H' having finite support.

Proof. $F \xrightarrow{\tau}_{\mathsf{r}} H$ implies that there exists $F = \sum_{i\in I} \alpha_i \cdot \delta_{x_i}$ and $H = \sum_{i\in I} \alpha_i \cdot D_i$ with

$x_i \to D_i$.

$$\begin{aligned} F &= \sum_{i \in I} \alpha_i \cdot \delta_{x_i} \\ &= \sum_{x \in \mathrm{supp}(F)} \sum_{\substack{i \in I \\ x = x_i}} \alpha_i \cdot \delta_x \\ &= \sum_{x \in \mathrm{supp}(F)} \sum_{\substack{D \in \mathcal{D}(\mathsf{N}^o)/_\equiv \\ |x \to D}} \Big(\sum_{\substack{i \in I \\ |x = x_i \\ \wedge D \equiv D_i}} \alpha_i \Big) \cdot \delta_x \end{aligned}$$

Notice that by Figure 2, given x the set $\{D \in \mathcal{D}(\mathsf{N}^o)/_\equiv\}$ is finite. Indeed we only consider finite multisets of processes and the only rule that can generate an infinite number of successor is the rule (NEW) but they are all equivalent under $\equiv$. Thus, by defining $H' = \sum_{x \in \mathrm{supp}(F)/_\equiv} \sum_{\substack{D \in \mathcal{D}^{\leq 1}(\mathsf{N}^o)/_\equiv \\ |x \to D}} (\sum_{\substack{i \in I \\ |x = x_i \\ \wedge D \equiv D_i}} \alpha_i) \cdot D$, the result holds. □

Lemma 50. Let $\mathsf{R} = (\mathcal{S}, \mathsf{corr}, \mathsf{trans}) \in \mathcal{R}^o_{\mathsf{r}}$ (resp. $\mathcal{R}^{of}_{\mathsf{r}}$) . For all $n \in \mathcal{N}_{pub}$, for all $c \in \mathcal{N}_{pub}$, for all $\mathcal{P} \in \mathcal{MP}$, for all $s \in \mathcal{S}$, if $\mathsf{corr}(s) = \mathcal{P}$ then there exists $D \in \mathcal{D}(\mathcal{S}^o_{\mathsf{N}})$ such that:

- $\mathcal{P} \overset{\tau}{\Longrightarrow}_{\mathsf{r}} D$ (resp. with finite support)
- $\mathrm{RProb}^{\leq n}_{\mathsf{R}}(s, \mathsf{corr}^{-1}(\downarrow c)) \leq D(\downarrow c)$

Proof. We prove this property by induction on n.

Base case $n = 0$: In such a case, $\mathrm{RProb}^{\leq n}_{\mathsf{R}}(s, \mathsf{corr}^{-1}(\downarrow c)) = 1$ if $\mathcal{P} \in \downarrow c$ and 0 otherwise. Thus, we can define $D = \delta_{\mathcal{P}}$ to directly obtain that $\mathcal{P} \overset{\tau}{\Longrightarrow}_{\mathsf{r}} D$ and $\mathrm{RProb}^{\leq n}_{\mathsf{R}}(\mathcal{P}, \downarrow c) \leq D(\downarrow c)$.

Inductive step $n > 0$: If $s \in \mathsf{corr}^{-1}(\downarrow c)$ or if $\mathsf{trans}(s) = \star$ then we can again define $D = \delta_{\mathcal{P}}$ to conclude. Let us now assume that $s \notin \mathsf{corr}^{-1}(\downarrow c)$ and $\mathsf{trans}(s) = E$. In such a case,

$$\mathrm{RProb}^{\leq n}_{\mathsf{R}}(s, \mathsf{corr}^{-1}(\downarrow c)) = \sum_{u \in \mathrm{supp}(E)} E(u) \cdot \mathrm{RProb}^{\leq n-1}_{\mathsf{R}}(u, \mathsf{corr}^{-1}(\downarrow c))$$

By definition of a resolution, $\mathsf{corr}(E) \in \mathrm{conv}(\mathsf{trans}_{\mathsf{N}^o}(\mathsf{corr}(s)))$ and so $\delta_{\mathcal{P}} \overset{\tau}{\to}_{\mathsf{r}} \mathsf{corr}(E)$. Note that when $\mathsf{R} \in \mathcal{R}^{of}_{\mathsf{r}}$, we know that $\mathsf{corr}(E)$ has finite support.

By inductive hypothesis, we know that for all $u \in \mathrm{supp}(E)$, there exists $D_u \in \mathcal{D}(\mathcal{S}^o_{\mathsf{N}})$ such that:

- $\mathsf{corr}(u) \overset{\tau}{\Longrightarrow}_{\mathsf{r}} D_u$ (with finite support when $\mathsf{R} \in \mathcal{R}^{of}_{\mathsf{r}}$)
- $\mathrm{RProb}^{\leq n-1}_{\mathsf{R}}(\mathsf{corr}(u), \mathsf{corr}^{-1}(\downarrow c)) \leq D_u(\downarrow c)$

Let us define $D = \sum_{u \in \mathrm{supp}(E)} E(u) \cdot D_u$. Furthermore,

$$\sum_{\mathcal{Q} \in \downarrow c} D(Q) = \sum_{\mathcal{Q} \in \downarrow c} \sum_{u \in \mathrm{supp}(E)} E(u) \cdot D_u(\mathcal{Q}) = \sum_{u \in \mathrm{supp}(E)} E(u) \cdot \sum_{\mathcal{Q} \in \downarrow c} D_u(\mathcal{Q})$$

Thus, $\mathrm{RProb}^{\leq n}_{\mathsf{R}}(s, \mathsf{corr}^{-1}(\downarrow c)) \leq D(\downarrow c)$. Note that since for all $u \in \mathrm{supp}(E)$, $\mathsf{corr}(u) \overset{\tau}{\Longrightarrow}_{\mathsf{r}} D_u$, we conclude that $\delta(\mathcal{P}) \overset{\tau}{\Longrightarrow}_{\mathsf{r}} D$. Furthermore when $\mathsf{R} \in \mathcal{R}^{of}_{\mathsf{r}}$, we know that $\mathsf{corr}(E)$ has finite support and $\mathsf{corr}(u) \overset{\tau}{\Longrightarrow}_{\mathsf{r}} D_u$ has finite support. Hence so does $\delta(\mathcal{P}) \overset{\tau}{\Longrightarrow}_{\mathsf{r}} D$. □

Lemma 51. For all $\mathcal{P} \in \mathcal{MP}$, for all $c \in \mathcal{N}_{pub}$,

- $\delta_{\mathcal{P}} \overset{\tau}{\Longrightarrow}_{\mathsf{r}} E$ implies $E(\downarrow c) \leq \mathrm{RProb}_{\mathcal{R}^o_{\mathsf{r}}}(\mathcal{P}, \downarrow c)$
- $\delta_{\mathcal{P}} \overset{\tau}{\Longrightarrow}_{\mathsf{r}} E$ with finite support implies $E(\downarrow c) \leq \mathrm{RProb}_{\mathcal{R}^{of}_{\mathsf{r}}}(\mathcal{P}, \downarrow c)$

Proof. Thanks to Lemma 1, we know that $\delta_{\mathcal{P}} \overset{\tau}{\Longrightarrow}_{\mathsf{r}} E$ implies that there exists $R = (\mathcal{S}, \mathsf{corr}, \mathsf{trans}) \in \mathcal{R}^o_{\mathsf{r}}$, and $D', E' \in \mathcal{D}^{\leq 1}(\mathcal{S})$ such that $\mathsf{corr}(D') = \delta_{\mathcal{P}}$, $\mathsf{corr}(E') = E$, $\mathrm{supp}(E') \subseteq \mathcal{S}_{ext}(R)$ and for all $u \in \mathcal{S}_{ext}(R)$, $E'(u) = \sum_{s' \in \mathcal{S}} D'(s') \cdot \mathrm{RProb}_R(s', \{u\})$. Therefore,

$$\begin{aligned}
E(\downarrow c) &= \sum_{\substack{u \in \mathcal{S}_{ext}(R) \\ |\mathsf{corr}(u) \in \downarrow c}} E'(u) \\
&= \sum_{\substack{u \in \mathcal{S}_{ext}(R) \\ |\mathsf{corr}(u) \in \downarrow c}} \sum_{s' \in \mathcal{S}} D'(s') \cdot \mathrm{RProb}_R(s', \{u\}) \\
&= \sum_{s' \in \mathcal{S}} D'(s') \cdot \sum_{\substack{u \in \mathcal{S}_{ext}(R) \\ |\mathsf{corr}(u) \in \downarrow c}} \mathrm{RProb}_R(s', \{u\}) \\
&\leq \sum_{s' \in \mathcal{S}} D'(s') \cdot \mathrm{RProb}_R(s', \mathsf{corr}^{-1}(\downarrow c)) \\
&\leq \sup_{\substack{s' \in \mathcal{S} \\ \mathsf{corr}(s') = \mathcal{P}}} \mathrm{RProb}_R(s', \mathsf{corr}^{-1}(\downarrow c)) \\
&\leq \mathrm{RProb}_{\mathcal{R}^o_{\mathsf{r}}}(\mathcal{P}, \downarrow c)
\end{aligned}$$

Note that one can easily check from the proof of Lemma 1 that the results carries over to $\delta_{\mathcal{P}} \overset{\tau}{\Longrightarrow}_{\mathsf{r}} D$ with finite support, i.e. in that case, the resolution R is in $\mathcal{R}^{of}_{\mathsf{r}}$, and so the rest of the proof follows. □

Lemma 52. For all $\mathcal{P} \in \mathcal{MP}$, for all $c \in \mathcal{N}_{pub}$,

$$\begin{aligned}
\mathrm{RProb}_{\mathcal{R}^o_{\mathsf{r}}}(\mathcal{P}, \downarrow c) &= \sup\{\ D(\downarrow c) \mid \delta_{\mathcal{P}} \overset{\tau}{\Longrightarrow}_{\mathsf{r}} D\} \\
&= \sup\{\ D(\downarrow c) \mid \delta_{\mathcal{P}} \overset{\tau}{\Longrightarrow}_{\mathsf{r}} D \text{ with finite support}\} \\
&= \mathrm{RProb}_{\mathcal{R}^{of}_{\mathsf{r}}}(\mathcal{P}, \downarrow c)
\end{aligned}$$

Proof. Consider the set $S = \{ D(\downarrow c) \mid \delta_{\mathcal{P}} \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} D\}$. By Lemma 50, we know that $\mathrm{RProb}_{\mathcal{R}^o_{\mathsf{r}}}(\mathcal{P}, \downarrow c) \leq \sup S$ and by Lemma 51, we have that $\sup S \leq \mathrm{RProb}_{\mathcal{R}^o_{\mathsf{r}}}(\mathcal{P}, \downarrow c)$. Similarly, if we denote $S_f = \{ D(\downarrow c) \mid \delta_{\mathcal{P}} \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} D$ with finite support$\}$, we have $\sup S_f = \mathrm{RProb}_{\mathcal{R}^{of}_{\mathsf{r}}}(\mathcal{P}, \downarrow c)$.

However, by Lemma 49, a simple induction on the infinite scheme building $\delta_{\mathcal{P}} \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} D$ allows us to deduce that there exists D' such that $\delta_{\mathcal{P}} \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} D'$ having finite support and such that $D \equiv D'$. Since the equivalence $\equiv$ only affects private names, we conclude that $D(\downarrow c) = D'(\downarrow c)$ and so $S = S_f$. □

F.2 Restricted characterization of observational relations

Let us define the following equivalences:

Definition 48. The restricted observational preorders $\leq^{r_0}_{obs}, \leq^{r_1}_{obs}, \leq^{r_2}_{obs}$ are the largest relation R on $\mathcal{MP}$ such that $\mathcal{P}\ R\ \mathcal{Q}$ implies :

- for all $c \in \mathcal{N}_{pub}$, $\mathrm{RProb}_{\mathcal{R}_{\mathsf{r}}}(\mathcal{P}, \downarrow c) \leq \mathrm{RProb}_{\mathcal{R}_{\mathsf{r}}}(\mathcal{Q}, \downarrow c)$;
- Case $\leq^{r_0}_{obs}$: if $\mathcal{P} \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} D$ then $\mathcal{Q} \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} E$ and $D\ \widehat{R}\ E$;

  Case $\leq^{r_1}_{obs}$: if $\mathcal{P} \stackrel{\tau}{\rightarrow} D$ then $\mathcal{Q} \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} E$ and $D\ \widehat{R}\ E$;

  Case $\leq^{r_2}_{obs}$: if $\mathcal{P} \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} D$ with finite support then $\mathcal{Q} \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} E$ and $D\ \widehat{R}\ E$;
- for all closed $Adv \in \mathcal{MP}$ such that $fn(Adv) \subseteq \mathcal{N}_{pub}$, $\{Adv\} \cup \mathcal{P}\ R\ \{Adv\} \cup \mathcal{Q}$.

The restricted observational equivalences $\approx^{r_0}_{obs}$, $\approx^{r_1}_{obs}$ and $\approx^{r_2}_{obs}$ are defined by additionally requesting R to be symmetric respectively in the cases of $\leq^{r_0}_{obs}$, $\leq^{r_1}_{obs}$ and $\leq^{r_2}_{obs}$. The restricted observational equivalence $\approx'^{r_0}_{obs}$, $\approx'^{r_1}_{obs}$ and $\approx'^{r_2}_{obs}$ are defined respectively in the cases $\leq^{r_0}_{obs}$, $\leq^{r_1}_{obs}$, $\leq^{r_2}_{obs}$ by additionally requesting that R to be symmetric and in the second bullet point, by requesting D to be a distribution and both $D\ \widehat{R}\ E$ and $E\ \widehat{R}\ D$ to hold.

Lemma 53. $\leq_{obs}$, $\leq^{r_0}_{obs}$, $\leq^{r_1}_{obs}$ and $\leq^{r_2}_{obs}$ coincide. $\approx^{r_0}_{obs}$, $\approx^{r_1}_{obs}$, $\approx^{r_2}_{obs}$, $\approx'^{r_0}_{obs}$, $\approx'^{r_1}_{obs}$ and $\approx'^{r_2}_{obs}$ coincide.

Proof. Let us start with the simple results: Notice that $\leq^{r_0}_{obs}$ is in fact the same definition as $\leq_{obs}$. In the definition of $\approx^{r_1}_{obs}$, if $\mathcal{P} \stackrel{\tau}{\rightarrow} D$ then $\mathcal{Q} \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} E$ and $D\ \widehat{\approx^{r_1}_{obs}}\ E$. However, D is a distribution by Figure 2. Hence, $D\ \widehat{\approx^{r_1}_{obs}}\ E$ also implies that E is a distribution. Since $\approx^{r_1}_{obs}$ is symmetric, we deduce that $E\ \widehat{\approx^{r_1}_{obs}}\ D$ and so $\approx^{r_1}_{obs}$ and $\approx'^{r_1}_{obs}$ coincide.

We show that $\leq^{r_0}_{obs}$ coincide with $\leq^{r_2}_{obs}$. We trivially have $\leq^{r_0}_{obs}$ implies $\leq^{r_2}_{obs}$. Let us thus focus on the other implication. Assume that $\mathcal{P} \leq^{r_2}_{obs} \mathcal{Q}$. Take $\mathcal{P} \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} D$. By definition,

there exists the following infinite scheme:

$$\begin{array}{l}
\delta_{\mathcal{P}} = D_0^{\rightarrow} + D_0^{\top} \\
D_0^{\rightarrow} \xrightarrow{\tau}_{\mathsf{r}} D_1^{\rightarrow} + D_1^{\top} \\
\dots \\
D_k^{\rightarrow} \xrightarrow{\tau}_{\mathsf{r}} D_{k+1}^{\rightarrow} + D_{k+1}^{\top} \\
\dots
\end{array}$$

such that $D = \sum_{k \in \mathbb{N}} D_k^{\top}$.

Thanks to Lemma 49, a simple induction allows us to deduce that there exists $\mathcal{P} \xRightarrow{\tau}_{\mathsf{r}} D'$ with finite support (D' may have infinite support) such that $D \equiv D'$. By $\mathcal{P} \leq_{obs}^{r_2} \mathcal{Q}$, we deduce that there exists $\mathcal{Q} \xRightarrow{\tau}_{\mathsf{r}} E$ such that $D' \widehat{\leq_{obs}^{r_2}} E$. But $D \equiv D'$ implies $D \widehat{\leq_{obs}^{r_2}} E$ which allows us to conclude.

The same proof allows us to show that $\approx_{obs}^{r_0}$ and $\approx_{obs}^{r_2}$ coincide. A minor modification of the proof also allows us to show that $\approx_{obs}^{'r_0}$ and $\approx_{obs}^{'r_2}$. Indeed, only the last sentence would change as we would obtain that there exists $\mathcal{Q} \xRightarrow{\tau}_{\mathsf{r}} E$ such that $D' \widehat{\approx_{obs}^{'r_2}} E$ and $E \widehat{\approx_{obs}^{'r_2}} D'$. But once again $D \equiv D'$ and $E \widehat{\approx_{obs}^{'r_2}} D'$ also imply $E \widehat{\approx_{obs}^{'r_2}} D$.

Let us now show that $\leq_{obs}^{r_1}$ and $\leq_{obs}^{r_2}$ coincide. We trivially have $\leq_{obs}^{r_2}$ implies $\leq_{obs}^{r_1}$ thus let us focus on the other implication. Assume that $\mathcal{P} \leq_{obs}^{r_1} \mathcal{Q}$. Hence $\delta_{\mathcal{P}} \widehat{\leq_{obs}^{r_1}} \delta_{\mathcal{Q}}$. Let $\mathcal{P} \xRightarrow{\tau}_{\mathsf{r}} D$ with finite support. By Property 4b of Lemma 48, we have that there exists E such that $\mathcal{Q} \xRightarrow{\tau}_{\mathsf{r}} E$ such that $D \widehat{\leq_{obs}^{r_1}} E$. Hence we conclude the proof. Note that the same proof allows us to prove that $\approx_{obs}^{r_1}$ and $\approx_{obs}^{r_2}$ coincide.

The same proof where we apply Property 5b of Lemma 48 allows us to prove that $\approx_{obs}^{'r_1}$ and $\approx_{obs}^{'r_2}$ coincide. □

F.3 Observational preorder implies simulation

For this direction of the equivalence, we need to represent as a process the frame of an extended process $(\mathcal{P}, \phi)$. Intuitively, for all $\mathsf{ax}_i \in dom(\phi)$, we will output on a public name c_{ax_i} the term $\mathsf{ax}_i\phi$. Formally, consider a frame $\phi = \{\mathsf{ax}_1 \rightarrow t_1, \dots \mathsf{ax}_n \rightarrow t_n\}$ and a sequence of public names $\mathcal{N}_{ch} = [c_{\mathsf{ax}_i} \in \mathcal{N}_{pub}]_{i=1}^n$, we define $\mathcal{F}(\phi, \mathcal{N}_{ch}) = \{\!\!\{\mathsf{out}(c_{\mathsf{ax}_i}, t_i).0\}\!\!\}_{i=1}^n$.

Given a frame ϕ and a sequence $\mathcal{N}_{ch}$, we define the following sets and functions:

- $\mathcal{SP}_\ell(\phi, \mathcal{N}_{ch}) = \{(\mathcal{P}, \phi) \in \mathcal{SP}_\ell \mid fn(\phi, \mathcal{P}) \cap \mathcal{N}_{ch} = \varnothing \wedge |\phi| = |\mathcal{N}_{ch}|\}$.
- $\mathcal{SP}(\phi, \mathcal{N}_{ch}) = \{\mathcal{P} \cup \mathcal{F}(\phi, \mathcal{N}_{ch}) \in \mathcal{SP} \mid fn(\phi, \mathcal{P}) \cap \mathcal{N}_{ch} = \varnothing \wedge |\phi| = |\mathcal{N}_{ch}|\}$
- $\pi_{\phi, \mathcal{N}_{ch}}^{e \rightarrow p} : \mathcal{SP}_\ell(\phi, \mathcal{N}_{ch}) \rightarrow \mathcal{SP}(\phi, \mathcal{N}_{ch})$ such that $\pi_{\phi, \mathcal{N}_{ch}}^{e \rightarrow p}((\mathcal{P}, \phi)) = \mathcal{P} \cup \mathcal{F}(\phi, \mathcal{N}_{ch})$
- $\pi_{\phi, \mathcal{N}_{ch}}^{p \rightarrow e} : \mathcal{SP}(\phi, \mathcal{N}_{ch}) \rightarrow \mathcal{SP}_\ell(\phi, \mathcal{N}_{ch})$ such that $\pi_{\phi, \mathcal{N}_{ch}}^{p \rightarrow e}(\mathcal{P} \cup \mathcal{F}(\phi, \mathcal{N}_{ch})) = (\mathcal{P}, \phi)$

To prove that observational preorder and equivalence imply simulation and bisimulation respectively, we define the relation R_{op} with $op \in \{\leq, \approx\}$ on extended processes as follows: For all $(\mathcal{P}, \phi), (\mathcal{P}', \phi') \in \mathcal{SP}_\ell$, $(\mathcal{P}, \phi)\ R_{op}\ (\mathcal{P}', \phi')$ if and only if $(\mathcal{P}, \phi) \in \mathcal{SP}_\ell(\phi, \mathcal{N}_{ch})$, $(\mathcal{P}', \phi') \in \mathcal{SP}_\ell(\phi', \mathcal{N}_{ch})$ and $\pi^{e\to p}_{\phi,\mathcal{N}_{ch}}((\mathcal{P}, \phi))\ op^{\mathcal{R}_\mathsf{r}}_{obs}\ \pi^{e\to p}_{\phi',\mathcal{N}_{ch}}((\mathcal{P}', \phi'))$ for some $\mathcal{N}_{ch}$.

Our definition of R_{op} parametrized by op will allow us to prove intermediate results that will holds both for the proof of observational preorder implying simulation and the proof of observational equivalence implying bisimulation.

Lemma 54. Let $\mathcal{N}_{ch}$ be a sequence of public names and ϕ, ϕ' two frames. Let $D, E \in \mathcal{D}^{\leq 1}(\bigcup_\phi \mathcal{SP}(\phi, \mathcal{N}_{ch}))$. For all $op \in \{\leq, \approx\}$, $D\ \widehat{op^{\mathcal{R}_\mathsf{r}}_{obs}}\ E$ implies $\sum_\phi \sum_{Q\in\mathcal{SP}(\phi,\mathcal{N}_{ch})} D(Q) \cdot \delta_{\pi^{p\to e}_{\phi,\mathcal{N}_{ch}}(Q)}\ \widehat{R_{op}}\ \sum_\phi \sum_{Q\in\mathcal{SP}(\phi,\mathcal{N}_{ch})} E(Q) \cdot \delta_{\pi^{p\to e}_{\phi,\mathcal{N}_{ch}}(Q)}$.

Proof. Let $\mathcal{S} \subseteq \mathcal{SP}_\ell$. Let $[\mathcal{S}] = \{(\mathcal{P}'', \phi'') \in \mathcal{SP}_\ell \mid (\mathcal{P}, \phi) \in \mathcal{S} \wedge (\mathcal{P}, \phi)\ R_{op}\ (\mathcal{P}'', \phi'')\}$. Let $\mathcal{S}_1 = \bigcup_\phi \pi^{e\to p}_{\phi,\mathcal{N}_{ch}}(\mathcal{SP}_\ell(\phi, \mathcal{N}_{ch}) \cap \mathcal{S})$ and $[\mathcal{S}_1] = \{\mathcal{Q}' \in \mathcal{SP} \mid \mathcal{Q} \in \mathcal{S}_1 \wedge \mathcal{Q}\ op^{\mathcal{R}_\mathsf{r}}_{obs}\ \mathcal{Q}'\}$.

Since $D\ \widehat{op^{\mathcal{R}_\mathsf{r}}_{obs}}\ E$, we know that $D(\mathcal{S}_1) \leq E([\mathcal{S}_1])$. By definition of $\mathcal{S}_1$ and since D is a sub-distribution of $\cup_\phi \mathcal{SP}(\phi, \mathcal{N}_{ch})$, we have $D(\mathcal{S}_1) = \sum_\phi \sum_{(Q,\phi)\in\mathcal{SP}_\ell(\phi,\mathcal{N}_{ch})\cap\mathcal{S}} D(\pi^{e\to p}_{\phi,\mathcal{N}_{ch}}(Q))$.

Moreover, we know by hypothesis that $E \in \bigcup_\phi \mathcal{D}^{\leq 1}(\mathcal{SP}(\phi, \mathcal{N}_{ch}))$. Hence, if we define $[\mathcal{S}_2] = \{\mathcal{Q}' \in \mathcal{SP}(\phi, \mathcal{N}_{ch}) \mid \mathcal{Q} \in \mathcal{S}_1 \wedge \mathcal{Q}\ op^{\mathcal{R}_\mathsf{r}}_{obs}\ \mathcal{Q}' \wedge \text{frame } \phi\}$ then $E([\mathcal{S}_1]) = E([\mathcal{S}_2])$. Therefore, by definition of R_{op} and $[\mathcal{S}_2]$, we deduce that $\mathcal{S}_3 = \{\pi^{p\to e}_{\phi,\mathcal{N}_{ch}}(Q) \mid Q \in [\mathcal{S}_2]\} \subseteq [\mathcal{S}]$. This allows us to deduce that $\sum_\phi \sum_{Q\in\mathcal{SP}(\phi,\mathcal{N}_{ch})} D(Q) \cdot \delta_{\pi^{p\to e}_{\phi,\mathcal{N}_{ch}}(Q)}(\mathcal{S}_1) = D(\mathcal{S}_1) \leq E([\mathcal{S}_1]) \leq E([\mathcal{S}_2]) = \sum_\phi \sum_{Q\in\mathcal{SP}(\phi,\mathcal{N}_{ch})} E(Q) \cdot \delta_{\pi^{p\to e}_{\phi,\mathcal{N}_{ch}}(Q)}(\mathcal{S}_3) \leq \sum_\phi \sum_{Q\in\mathcal{SP}(\phi,\mathcal{N}_{ch})} E(Q) \cdot \delta_{\pi^{p\to e}_{\phi,\mathcal{N}_{ch}}(Q)}([\mathcal{S}])$. □

Corollary 7. Let $\mathcal{N}_{ch}$ be a sequence of public names and ϕ, ϕ' two frames. Let $D \in \mathcal{D}^{\leq 1}(\mathcal{SP}(\phi, \mathcal{N}_{ch}))$, $E \in \mathcal{D}^{\leq 1}(\mathcal{SP}(\phi', \mathcal{N}_{ch}))$. For all $op \in \{\leq, \approx\}$, $D\ \widehat{op^{\mathcal{R}_\mathsf{r}}_{obs}}\ E$ implies $\pi^{p\to e}_{\phi,\mathcal{N}_{ch}}(D)\ \widehat{R_{op}}\ \pi^{p\to e}_{\phi',\mathcal{N}_{ch}}(E)$.

F.3.1 τ transitions

Lemma 55. For all $op \in \{\leq, \approx\}$, for all $(\mathcal{P}, \phi), (\mathcal{P}', \phi') \in \mathcal{SP}_\ell$, if $(\mathcal{P}, \phi)\ R_{op}\ (\mathcal{P}', \phi')$ and $(\mathcal{P}, \phi) \xrightarrow{\tau}_{\mathsf{N}^\ell} D$ then $(\mathcal{P}', \phi') \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^\ell} E$ and $D\ \widehat{R_{op}}\ E$ (and $E\ \widehat{R_\approx}\ D$ when $op = \approx$).

Proof. By Definition 10, $D = (D', \phi)$ with $\mathcal{P} \xrightarrow{\tau}_{\mathsf{N}^o} D'$. Since $(\mathcal{P}, \phi)\ R_{op}\ (\mathcal{P}', \phi')$, we know that $(\mathcal{P}, \phi) \in \mathcal{SP}_\ell(\phi, \mathcal{N}_{ch})$, $(\mathcal{P}', \phi') \in \mathcal{SP}_\ell(\phi', \mathcal{N}_{ch})$ and $\mathcal{P} \cup \mathcal{F}(\phi, \mathcal{N}_{ch})\ op^{\mathcal{R}_\mathsf{r}}_{obs}\ \mathcal{P}' \cup \mathcal{F}(\phi', \mathcal{N}_{ch})$ for some $\mathcal{N}_{ch}$.

By Figure 2, we deduce that $\mathcal{P} \cup \mathcal{F}(\phi, \mathcal{N}_{ch}) \xrightarrow{\tau}_{\mathsf{N}^o} D_1 = \sum_{\mathcal{Q}\in\text{supp}(D')} D'(\mathcal{Q}) \cdot \delta_{\mathcal{Q}\cup\mathcal{F}(\phi,\mathcal{N}_{ch})}$ and so $\mathcal{P} \cup \mathcal{F}(\phi, \mathcal{N}_{ch}) \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} D_1$. By Definition 18, $\mathcal{P}' \cup \mathcal{F}(\phi', \mathcal{N}_{ch}) \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} E_1$ for some E_1 such that $D_1\ \widehat{op^{\mathcal{R}_\mathsf{r}}_{obs}}\ E_1$ (and $E_1\ \widehat{R_\approx}\ D_1$ when $op = \approx$).

Let us analyse the support of E_1. For all $\mathcal{Q} \cup \mathcal{F}(\phi', \mathcal{N}_{ch}) \xrightarrow{\tau}_{\mathsf{N}^o} F$ with $\mathcal{N}_{ch} \cap fn(\mathcal{Q}) = \varnothing$, the only transition from Figure 2 that may reduce an output from $\mathcal{F}(\phi', \mathcal{N}_{ch})$ is the rule (Comm). However that would imply that $\mathcal{Q} = \{\!\!\{\mathsf{in}(u, x).Q\}\!\!\} \cup \mathcal{Q}'$ with $c_{\mathsf{ax}_i} \doteq u$ for some $i \in$

$\{1, \ldots, |\phi'|\}$. But, we know that $c_{\mathsf{ax}_i} \notin st(u)$ and so by Lemma 43, $c_{\mathsf{ax}_i} \not\doteq u$, hence a contradiction. This allows us to deduce that $\mathrm{supp}(F) \subseteq \mathcal{SP}(\phi', \mathcal{N}_{ch})$ and $(\mathcal{Q}, \phi') \xrightarrow{\tau}_{\mathsf{N}^\ell} \pi^{p\to e}_{\phi',\mathcal{N}_{ch}}(F)$. Lemma 35 and a simple induction on the infinite scheme defining $\mathcal{P}' \cup \mathcal{F}(\phi', \mathcal{N}_{ch}) \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} E_1$ allow us to conclude that $\mathrm{supp}(E_1) \subseteq \mathcal{SP}(\phi', \mathcal{N}_{ch})$ and $(\mathcal{P}', \phi') \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^\ell} \pi^{p\to e}_{\phi',\mathcal{N}_{ch}}(E_1)$. Since $\pi^{p\to e}_{\phi,\mathcal{N}_{ch}}(D_1) = D$, we conclude by Lemma 54. $\square$

F.3.2 Static equivalence transitions

Lemma 56. For all $op \in \{\leq, \approx\}$, for all $(\mathcal{P}, \phi), (\mathcal{P}', \phi') \in \mathcal{SP}_\ell$, if $(\mathcal{P}, \phi)\ R_{op}\ (\mathcal{P}', \phi')$ and $(\mathcal{P}, \phi) \xrightarrow{a}_{\mathsf{N}^\ell} D$ with $a \in \{\xi \doteq \zeta, \xi \not\doteq, \mathsf{ax} \in, \mathsf{ax} \notin\}$ then $(\mathcal{P}', \phi') \xRightarrow{a}_{\mathsf{r},\mathsf{N}^\ell} E$ and $D\ \widehat{R_{op}}\ E$ (and $E\ \widehat{R_\approx}\ D$ when $op = \approx$).

Proof. By definition of R_{op}, we know that $(\mathcal{P}, \phi)\ R_{op}\ (\mathcal{P}', \phi')$ implies $(\mathcal{P}, \phi) \in \mathcal{SP}_\ell(\phi, \mathcal{N}_{ch})$, $(\mathcal{P}', \phi') \in \mathcal{SP}_\ell(\phi', \mathcal{N}_{ch})$ and $\pi^{e\to p}_{\phi,\mathcal{N}_{ch}}((\mathcal{P}, \phi))\ op^{\mathcal{R}_\mathsf{r}}_{obs}\ \pi^{e\to p}_{\phi',\mathcal{N}_{ch}}((\mathcal{P}', \phi'))$ for some $\mathcal{N}_{ch}$. Hence, $|\phi| = |\phi'|$. Hence, for all $a \in \{\mathsf{ax} \in, \mathsf{ax} \notin\}$, $(\mathcal{P}, \phi) \xrightarrow{a}_{\mathsf{N}^\ell} \delta_{(\mathcal{P},\phi)}$ implies $(\mathcal{P}', \phi') \xrightarrow{a}_{\mathsf{N}^\ell} \delta_{(\mathcal{P}',\phi')}$ which implies $(\mathcal{P}', \phi') \xRightarrow{a}_{\mathsf{r},\mathsf{N}^\ell} \delta_{(\mathcal{P}',\phi')}$. Since $(\mathcal{P}, \phi)\ R_{op}\ (\mathcal{P}', \phi')$, we directly have that $\delta_{(\mathcal{P},\phi)}\ \widehat{R_{op}}\ \delta_{(\mathcal{P}',\phi')}$. When $op = \approx$, $R_\approx$ is symmetric hence $(\mathcal{P}', \phi')\ R_\approx\ (\mathcal{P}, \phi)$ also implying $\delta_{(\mathcal{P}',\phi')}\ \widehat{R_\approx}\ \delta_{(\mathcal{P},\phi)}$. Thus the result holds.

Let us now focus on the case where $a = \xi\ o\ \zeta$ with $o \in \{\doteq, \not\doteq\}$. Let $n = |\phi|$ and assume that $\mathcal{N}_{ch} = [c_{\mathsf{ax}_i}]_{i=1}^n$. We consider a public name ok such that $ok \notin fn(\mathcal{P}, \mathcal{P}', \phi, \phi')$, some variables $x_1, \ldots, x_n$ and the renaming $\rho = \{^{x_i}/_{\mathsf{ax}_i}\}_{i=1}^n$. We build the following processes $Test^{\doteq}$ and $Test^{\not\doteq}$.

$$
\begin{aligned}
Test^{\doteq} &:= \mathsf{in}(c_{\mathsf{ax}_1}, x_1).\ldots.\mathsf{in}(c_{\mathsf{ax}_n}, x_n).Test^{\doteq}_{if}\\
Test^{\doteq}_{if} &:= \mathsf{if}\ \xi\rho = \zeta\rho\ \mathsf{then}\ \mathsf{out}(ok, ok).0\ \mathsf{else}\ 0\\
Test^{\not\doteq} &:= \mathsf{in}(c_{\mathsf{ax}_1}, x_1).\ldots.\mathsf{in}(c_{\mathsf{ax}_n}, x_n).Test^{\not\doteq}_{if}\\
Test^{\not\doteq}_{if} &:= \mathsf{if}\ \xi\rho = \zeta\rho\ \mathsf{then}\ 0\ \mathsf{else}\ \mathsf{out}(ok, ok).0
\end{aligned}
$$

Since ξ, ζ are recipes we know that $fn(\xi, \zeta) \subseteq \mathcal{N}_{pub}$ and so $fn(Test^{\doteq}, Test^{\not\doteq}) \subseteq \mathcal{N}_{pub}$. Hence, by Definition 18, for all $o \in \{\doteq, \not\doteq\}$, $\{\!\{Test^o\}\!\} \cup \pi^{e\to p}_{\phi,\mathcal{N}_{ch}}((\mathcal{P}, \phi))\ op^{\mathcal{R}_\mathsf{r}}_{obs}\ \{\!\{Test^o\}\!\} \cup \pi^{e\to p}_{\phi',\mathcal{N}_{ch}}((\mathcal{P}', \phi'))$.

Let us denote $\mathcal{P}_T = \{\!\{Test^o\}\!\} \cup \pi^{e\to p}_{\phi,\mathcal{N}_{ch}}((\mathcal{P}, \phi))$ and $\mathcal{P}'_T = \{\!\{Test^o\}\!\} \cup \pi^{e\to p}_{\phi',\mathcal{N}_{ch}}((\mathcal{P}', \phi'))$. Notice that $(\mathcal{P}, \phi) \xrightarrow{a}_{\mathsf{N}^\ell} \delta_{(\mathcal{P},\phi)}$ implies that $\xi\phi\ o\ \zeta\phi$. Furthermore, $\pi^{e\to p}_{\phi,\mathcal{N}_{ch}}((\mathcal{P}, \phi)) = \mathcal{P} \cup \{\!\{\mathsf{out}(c_{\mathsf{ax}_i}, \mathsf{ax}_i\phi).0\}\!\}_{i=1}^n$. Hence, by successively applying the rule (Comm) on $c_{\mathsf{ax}_1}, \ldots, c_{\mathsf{ax}_n}$, we deduce that $\mathcal{P}_T \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} \delta_{\mathcal{P}\cup\{\!\{Test^o_{if}\sigma\}\!\}}$ with $\sigma = \rho^{-1}\phi$. Since $\xi\phi\ o\ \zeta\phi$ implies $(\xi\rho)\rho^{-1}\phi\ o\ (\zeta\rho)\rho^{-1}\phi$, we can apply the rule (Then) when o is $\doteq$ and (Else) otherwise to obtain that $\mathcal{P}_T \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} \delta_{\mathcal{P}\cup\{\!\{\mathsf{out}(ok,ok).0\}\!\}}$. Thus, $\mathrm{RProb}_{\mathcal{R}_\mathsf{r}}(\mathcal{P}_T, \downarrow ok) = 1$.

Since $\mathcal{P}_T\ op^{\mathcal{R}_\mathsf{r}}_{obs}\ \mathcal{P}'_T$, we deduce that $\mathrm{RProb}_{\mathcal{R}_\mathsf{r}}(\mathcal{P}'_T, \downarrow ok) = 1$. Hence, there exists a resolution $\mathsf{R} = (\mathcal{S}_\mathsf{R}, \mathsf{corr}_\mathsf{R}, \mathsf{trans}_\mathsf{R}) \in \mathcal{R}_\mathsf{r}$ and $s \in \mathcal{S}_\mathsf{R}$ such that $\mathsf{corr}_\mathsf{R}(s) = \mathcal{P}'_T$ and $\mathrm{RProb}_\mathsf{R}(s, \mathsf{corr}_\mathsf{R}^{-1}(\downarrow ok)) > 0$, meaning that there exists $p \in \mathbb{N}$ such that $\mathrm{RProb}^{\leq p}_\mathsf{R}(s, \mathsf{corr}_\mathsf{R}^{-1}(\downarrow ok)) > 0$.

Let us define $A = \{\mathcal{Q} \cup \{\mathsf{out}(c_{\mathsf{ax}_i}, \mathsf{ax}_i\phi').0\}_{i=j}^{n} \cup \{\!\{\mathsf{in}(c_{\mathsf{ax}_j}, x_j).\ldots\mathsf{in}(c_{\mathsf{ax}_n}, x_n).Test^o_{if}\sigma_j\}\!\} \mid j = 1\ldots n+1, (\mathcal{Q}, \phi') \in \mathcal{SP}_\ell(\phi', \mathcal{N}_{ch})\}$ where $\sigma_j = \{^{\mathsf{ax}_i\phi'}/_{x_i}\}_{i=1}^{j-1}$. We first notice that $\mathcal{P}'_T \in A$. Moreover, thanks to the fact that $(\mathcal{Q}, \phi') \in \mathcal{SP}_\ell(\phi', \mathcal{N}_{ch})\}$ implies $c_{\mathsf{ax}_i} \notin fn(\mathcal{Q})$ and thanks to Lemma 43, we can show that for all $\mathcal{Q}' \in A$, $\mathcal{Q}' \xrightarrow{\tau}_{\mathsf{N}^o} F$ implies $\mathrm{supp}(F) \subseteq A \cup \downarrow ok$.

This allows us to prove by induction on $p \in \mathbb{N}$ that for all $s \in \mathcal{S}_\mathsf{R}$, $\mathrm{RProb}^{\leq p}_\mathsf{R}(s, \mathsf{corr}^{-1}_\mathsf{R}(\downarrow ok)) > 0$ and $\mathsf{corr}_\mathsf{R}(s) \in A$ imply there exist $s_1, s_2 \in \mathcal{S}_\mathsf{R}$ such that $\mathsf{corr}_\mathsf{R}(s_1) = \mathcal{Q}' \cup \{\!\{Test^o_{if}\sigma_n\}\!\} \in A$, $\mathsf{corr}_\mathsf{R}(s_2) = \mathcal{Q}' \cup \{\!\{\mathsf{out}(ok, ok).0\}\!\}$ and $s_2 \in \mathrm{supp}(\mathsf{trans}_\mathsf{R}(s_1))$. For s_2 to be in $\mathrm{supp}(\mathsf{trans}_\mathsf{R}(s_1))$, it implies that $\mathcal{Q}' \cup \{\!\{\mathsf{out}(ok, ok).0\}\!\} \xrightarrow{\tau}_{\mathsf{N}^o} \delta_{\mathcal{Q}' \cup \{\!\{\mathsf{out}(ok,ok).0\}\!\}}$ by application of the rule (Then) when o is $\doteq$ and the rule (Else) otherwise. Thus, $\xi\rho\sigma_n \; o \; \zeta\rho\sigma_n$ holds and so $\xi\phi' \; o \; \zeta\phi'$ holds.

We can therefore conclude that $(\mathcal{P}', \phi') \xrightarrow{a}_{\mathsf{N}^\ell} \delta_{(\mathcal{P}', \phi')}$ and once again noticing that $(\mathcal{P}, \phi) \; R_{op} \; (\mathcal{P}', \phi')$ implies $\delta_{(\mathcal{P},\phi)} \; \widehat{R_{op}} \; \delta_{(\mathcal{P}',\phi')}$; and that when $op = \approx$, $R_\approx$ is symmetric hence $(\mathcal{P}', \phi') \; R_\approx \; (\mathcal{P}, \phi)$ also implying $\delta_{(\mathcal{P}',\phi')} \; \widehat{R_\approx} \; \delta_{(\mathcal{P},\phi)}$. □

F.3.3 Input and output transitions

For input and output transitions, we will need to consider predicates on the relation $\rightarrow$ of a NPLTS. Given a predicate π, we will write $\pi(x \rightarrow D)$ when π holds on $x \rightarrow D$. Given a logic formula ϕ with predicates as atoms, we denote by $(x \rightarrow D) \models \phi$ the natural satisfiability of ϕ by $x \rightarrow D$. Given $D \xrightarrow{\tau}_\mathsf{r} E$ with $D = \sum_{i \in I} \alpha_i \cdot \delta_{x_i}$, $E = \sum_{i \in I} \alpha_i \cdot D_i$ and $x_i \rightarrow D_i$, we will write $(D \xrightarrow{\tau}_\mathsf{r} E) \models \phi$ when for all $i \in I$, $\pi(x_i \rightarrow D_i) \models \phi$. Finally, given $D \xRightarrow{\tau}_\mathsf{r} E$ with the infinite scheme $D = D_0^{\rightarrow} + D_0^{\top}$ and $D_k^{\rightarrow} \xrightarrow{\tau}_\mathsf{r} D_{k+1}^{\rightarrow} + D_{k+1}^{\top}$ for $k \in \mathbb{N}$, we write $(D \xRightarrow{\tau}_\mathsf{r} E) \models \phi$ when for all $k \in \mathbb{N}$, $(D_k^{\rightarrow} \xrightarrow{\tau}_\mathsf{r} D_{k+1}^{\rightarrow} + D_{k+1}^{\top}) \models \phi$.

For some of our proof, we will consider a measure function on states of our NPLTS associated with a total order. Formally, a measure for a NPLTS $\mathsf{N} = (\mathcal{S}_\mathsf{N}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_\mathsf{N})$ is a function $\mathsf{m} : \mathcal{S}_\mathsf{N} \mapsto I$ for some set I associated with a total order $<_\mathsf{m}$ on I that includes a minimal element for $<_\mathsf{m}$. Given a sub-distribution $D \in \mathcal{D}^{\leq 1}(\mathcal{S}_\mathsf{N})$, we denote $\mathsf{m}(D) = \max\{\mathsf{m}(x) \mid x \in \mathrm{supp}(D)\}$.

Lemma 57. Let $\mathsf{N} = (\mathcal{S}_\mathsf{N}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_\mathsf{N})$ be a NPLTS with $\mathcal{A}_{int} = \{\tau\}$. Let $\pi_1, \ldots, \pi_n$ be predicates on $\rightarrow$. For all $(\sum_{i=1}^{m_A} A_i \xrightarrow{\tau}_\mathsf{r} \sum_{i=1}^{m_B} B_i) \models \pi_1 \vee \ldots \vee \pi_n$, there exist $\{A_k^p \mid p = 1\ldots n, k = 1\ldots m_A\}$ and $\{B_{k,i}^p \mid p = 1\ldots n, k = 1\ldots m_A, i = 1\ldots m_B\}$ such that:

- for all $p \in \{1, \ldots, n\}$, for all $k \in \{1, \ldots, m_A\}$, $(A_k^p \xrightarrow{\tau}_\mathsf{r} \sum_{i=1}^{m_B} B_{k,i}^p) \models \pi_p$
- for all $k \in \{1, \ldots, m_A\}$, $A_k = \sum_{p=1}^{n} A_k^p$
- for all $i \in \{1, \ldots, m_B\}$, $B_i = \sum_{p=1}^{n} \sum_{k=1}^{m_A} B_{k,i}^p$

Proof. By definition of $(\sum_{i=1}^{m_A} A_i \xrightarrow{\tau}_\mathsf{r} \sum_{i=1}^{m_B} B_i) \models \pi_1 \vee \ldots \vee \pi_n$, we know there exists a countable set I and a multiset $\{x_i\}_{i \in I}$ with for all $i \in I$, $x_i \in \mathcal{S}_\mathsf{N}$ such that $\sum_{i=1}^{m_A} A_i = \sum_{i \in I} \alpha_i \cdot \delta_{x_i}$, $\sum_{i=1}^{m_B} B_i = \sum_{i \in I} \alpha_i \cdot D_i$ and for all $i \in I$, $x_i \rightarrow D_i$ with $\pi_p(x_i \rightarrow D_i)$ for some $p \in \{1, \ldots, n\}$.

With partition I into $I_1 \cup \ldots \cup I_n$ such that for all $p \in \{1, \ldots, n\}$, for all $i \in I_p$, $\pi_p(x_i \to D_i)$. We define for all $k \in \{1 \ldots m_A\}$, $p \in \{1 \ldots n\}$, the sub-distribution $A_k^p = \sum_{i \in I_p} \frac{\alpha_i \cdot A_k(x_i)}{\sum_{j=1}^{m_A} A_k(x_i)} \cdot \delta_{x_i}$. Hence, $(A_k^p \xrightarrow{\tau}_{\mathsf{r}} \sum_{i \in I_p} \frac{\alpha_i \cdot A_k(x_i)}{\sum_{j=1}^{m_A} A_j(x_i)} \cdot D_i) \models \pi_p$. Therefore, for all $\ell \in \{1, \ldots, m_B\}$, we define $B_{k,\ell}^p$ such that for all $x \in \mathrm{supp}(B_\ell)$, $B_{k,\ell}^p(x) = \frac{B_\ell(x)}{\sum_{j=1}^{m_B} B_j(x)} \cdot \sum_{i \in I_p} \frac{\alpha_i \cdot A_k(x_i)}{\sum_{j=1}^{m_A} A_j(x_i)} \cdot D_i(x)$. We directly have $\sum_{\ell=1}^{m_B} B_{k,\ell}^p = \sum_{i \in I_p} \frac{\alpha_i \cdot A_k(x_i)}{\sum_{j=1}^{m_A} A_j(x_i)} \cdot D_i$ and so $(A_k^p \xrightarrow{\tau}_{\mathsf{r}} \sum_{\ell=1}^{m_B} B_{k,\ell}^p) \models \pi_p$.

Let us show that for all $k \in \{1, \ldots, m_A\}$, $A_k = \sum_{p=1}^n A_k^p$. Let $k \in \{1, \ldots, m_A\}$ and $x \in \mathcal{S}_{\mathsf{N}}$. We have $\sum_{p=1}^n A_k^p(x) = \sum_{p=1}^n A_k^p(x) = \sum_{p=1}^n \sum_{i \in I_p} \frac{\alpha_i \cdot A_k(x_i)}{\sum_{j=1}^{m_A} A_j(x_i)} \cdot \delta_{x_i}(x) = \sum_{p=1}^n \sum_{i \in I_p} \frac{\alpha_i \cdot A_k(x)}{\sum_{j=1}^{m_A} A_j(x)} \cdot \delta_{x_i}(x) = \frac{\cdot A_k(x)}{\sum_{j=1}^{m_A} A_j(x)} \sum_{p=1}^n \sum_{i \in I_p} \alpha_i \cdot \delta_{x_i}(x) = \frac{\cdot A_k(x)}{\sum_{j=1}^{m_A} A_j(x)} \cdot \sum_{i=1}^{m_A} A_i(x) = A_k(x)$.

Finally, let us show that for all $\ell \in \{1, \ldots, m_B\}$, $B_\ell = \sum_{p=1}^n \sum_{k=1}^{m_A} B_{k,\ell}^p$. By definition, for all $x \in \mathcal{S}_{\mathsf{N}}$,

$$\begin{aligned}
\sum_{p=1}^n \sum_{k=1}^{m_A} B_{k,i}^p(x) &= \sum_{p=1}^n \sum_{k=1}^{m_A} \sum_{i \in I_p} \frac{\alpha_i \cdot A_k(x_i)}{\sum_{j=1}^{m_A} A_j(x_i)} \cdot D_i(x) \\
&= \frac{B_\ell(x)}{\sum_{j=1}^{m_B} B_j(x)} \cdot \sum_{p=1}^n \sum_{k=1}^{m_A} \sum_{i \in I_p} \frac{\alpha_i \cdot A_k(x_i)}{\sum_{j=1}^{m_A} A_j(x_i)} \cdot D_i(x) \\
&= \frac{B_\ell(x)}{\sum_{j=1}^{m_B} B_j(x)} \cdot \sum_{p=1}^n \sum_{i \in I_p} \frac{\alpha_i \cdot \sum_{k=1}^{m_A} A_k(x_i)}{\sum_{j=1}^{m_A} A_j(x_i)} \cdot D_i(x) \\
&= \frac{B_\ell(x)}{\sum_{j=1}^{m_B} B_j(x)} \cdot \sum_{p=1}^n \sum_{i \in I} \alpha_i \cdot D_i(x) \\
&= \frac{B_\ell(x)}{\sum_{j=1}^{m_B} B_j(x)} \cdot \sum_{i=1}^{m_B} B_i(x) \\
&= B_\ell(x)
\end{aligned}$$

□

Lemma 58. Let $\mathsf{N} = (\mathcal{S}_{\mathsf{N}}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_{\mathsf{N}})$ be a NPLTS with $\mathcal{A}_{int} = \{\tau\}$. Let $\pi_c^{\to}$, $\pi_s^{\to}$, π_{all} be three predicates on $\to$. Let $\pi^{\mathcal{S}}$ be a predicate on $\mathcal{S}_{\mathsf{N}}$ such that for all $x \in \mathcal{S}_{\mathsf{N}}$, for all $D \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{N}})$,

- if $\pi^{\mathcal{S}}(x)$ then $\pi_c^{\to}(x \to D)$ or $\pi_s^{\to}(x \to D)$
- if $\pi_c^{\to}(x \to D)$ then $\pi^{\mathcal{S}}(D)$

For all $D, E \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{N}})$, if $D \xRightarrow{\tau}_{\mathsf{r}} E$ with the following infinite scheme

$$D = D_0^{\to} + D_0^{\top} \qquad \forall k \in \mathbb{N}.\ D_k^{\to} \to_{\mathsf{r}} D_{k+1}^{\to} + D_{k+1}^{\top}$$

and $\pi^{\mathcal{S}}(D_0^{\to})$ then there exists $A, A^{\top}, B, B^{\top}, C \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{N}})$ such that

$$(D \xRightarrow{\tau}_{\mathsf{r}} A + A^{\top}) \models \pi_c^{\to} \qquad (A \xrightarrow{\tau}_{\mathsf{r}} B + B^{\top}) \models \pi_s^{\to} \qquad B \xRightarrow{\tau}_{\mathsf{r}} C \qquad E = C + B^{\top} + A^{\top}$$

Moreover, if we assume the existence of measure function m on N such that for all $x \in \mathcal{S}_{\mathsf{N}}$, for all $D' \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{N}})$, $\pi_s^{\rightarrow}(x \rightarrow D')$ implies $\mathsf{m}(x) >_{\mathsf{m}} \mathsf{m}(D')$ and if $\mathsf{m}(A) \leq_{\mathsf{m}} \mathsf{m}(B + B^{\top})$ then $(D \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} E) \models \pi_c^{\rightarrow}$.

Finally, if $(D \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} E) \models \pi_{all}$ then $(D \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} A + A^{\top}) \models \pi_{all}$, $(A \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} B + B^{\top}) \models \pi_{all}$ and $(B \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} C) \models \pi_{all}$.

Proof. Consider the following property $P(n)$ defined as: there exist $((Save_{i,k}^{\rightarrow})_{k=0}^{n-i})_{i=0}^{n-1}$, $((Save_{i,k}^{\top})_{k=0}^{n-i})_{i=0}^{n-1}$, $k \in \{0, \ldots, n-i\}$, $(\overline{F}_k^{\rightarrow})_{k=0}^{n}$, $(F_k^{\top})_{k=0}^{n}$, and $(F_k^{\rightarrow})_{k=0}^{n-1}$ such that

1. for all $k \in \{0, \ldots, n\}$, $\pi^{\mathcal{S}}(\overline{F}_k^{\rightarrow})$
2. for all $k \in \{0, \ldots, n\}$, $D_k^{\rightarrow} = \overline{F}_k^{\rightarrow} + \sum_{i=0}^{k-1} Save_{i,k-i}^{\rightarrow}$
3. for all $k \in \{0, \ldots, n\}$, $D_k^{\top} = F_k^{\top} + \sum_{i=0}^{k-1} Save_{i,k-i}^{\top}$
4. for all $i \in \{0, \ldots, n-1\}$, for all $k \in \{0, \ldots, n-i-1\}$, $Save_{i,k}^{\rightarrow} \rightarrow_{\mathsf{r}} Save_{i,k+1}^{\rightarrow} + Save_{i,k+1}^{\top}$
5. for all $i \in \{0, \ldots, n-1\}$, $(Save_{i,0}^{\rightarrow} \rightarrow_{\mathsf{r}} Save_{i,1}^{\rightarrow} + Save_{i,1}^{\top}) \models \pi_s^{\rightarrow}$
6. for all $k \in \{0, \ldots, n-1\}$, $(F_k^{\rightarrow} \stackrel{\tau}{\rightarrow}_{\mathsf{r}} \overline{F}_{k+1}^{\rightarrow} + F_{k+1}^{\top}) \models \pi_c^{\rightarrow}$
7. for all $k \in \{0, \ldots, n-1\}$, $\overline{F}_k^{\rightarrow} = F_k^{\rightarrow} + Save_{k,0}^{\rightarrow}$

We show that for all $n \in \mathbb{N}$, $P(n)$ holds by induction on n.

Base case $n = 0$: By choosing $\overline{F}_0^{\rightarrow} = D_0^{\rightarrow}$ and $F_0^{\top} = D_0^{\top}$, the result directly holds since by hypothesis $\pi^{\mathcal{S}}(D_0^{\rightarrow})$ holds.

Inductive step $n > 0$: We have that by hypothesis that $D_n^{\rightarrow} \rightarrow_{\mathsf{r}} D_{n+1}^{\rightarrow} + D_{n+1}^{\top}$. Furthermore by inductive hypothesis, $D_n^{\rightarrow} = \overline{F}_n^{\rightarrow} + \sum_{i=0}^{n-1} Save_{i,n-i}^{\rightarrow}$.

By Lemma 57, we know that there exist some sub-distributions $Save_{i,n-i+1}^{\rightarrow}$ and $Save_{i,n-i+1}^{\top}$ for all $i \in \{0, \ldots, n-1\}$ and $H^{\rightarrow}$ and $H^{\top}$ such that:

- $\overline{F}_n^{\rightarrow} \rightarrow_{\mathsf{r}} H^{\rightarrow} + H^{\top}$
- for all $i \in \{0, \ldots, n-1\}$, $Save_{i,n-i}^{\rightarrow} \rightarrow_{\mathsf{r}} Save_{i,n-i+1}^{\rightarrow} + Save_{i,n-i+1}^{\top}$
- for all $\alpha \in \{\rightarrow, \top\}$, $D_{n+1}^{\alpha} = H^{\alpha} + \sum_{i=0}^{n-1} Save_{i,n-i+1}^{\alpha}$

By hypothesis, $\pi^{\mathcal{S}}(\overline{F}_n^{\rightarrow})$ hence $(\overline{F}_n^{\rightarrow} \rightarrow_{\mathsf{r}} H^{\rightarrow} + H^{\top}) \models \pi_c^{\rightarrow} \vee \pi_s^{\rightarrow}$. By Lemma 57, we deduce that there exists $\overline{F}_n^{c}$, $\overline{F}_n^{s}$, $H^{c,\rightarrow}$, $H^{s,\rightarrow}$, $H^{c,\top}$, $H^{s,\top}$ such that:

- $\overline{F}_n^{\rightarrow} = \overline{F}_n^{c} + \overline{F}_n^{s}$
- for all $a \in \{s, c\}$, $(\overline{F}_n^{a} \rightarrow_{\mathsf{r}} H^{a,\rightarrow} + H^{a,\top}) \models \pi_a^{\rightarrow}$
- for all $\alpha \in \{\rightarrow, \top\}$, $H^{\alpha} = H^{c,\alpha} + H^{s,\alpha}$

We define the sub-distributions $F_n^{\rightarrow} = \overline{F}_n^c$, $\overline{F}_{n+1}^{\rightarrow} = H^{c,\rightarrow}$, $F_{n+1}^{\top} = H^{c,\top}$, $Save_{n,0}^{\rightarrow} = \overline{F}_n^s$, $Save_{n,0}^{\top} = \varnothing$, $Save_{n,1}^{\rightarrow} = H^{s,\rightarrow}$ and $Save_{n,1}^{\top} = H^{s,\top}$.

We prove the different properties of $P(n+1)$ by applying the inductive hypothesis on $P(n)$ and the following reasoning: Since $(\overline{F}_n^c \rightarrow_{\mathsf{r}} H^{c,\rightarrow} + H^{c,\top}) \models \pi_c^{\rightarrow}$, we know from our hypotheses on $\pi_c^{\rightarrow}$ and $\pi^{\mathcal{S}}$ that $\pi^{\mathcal{S}}(\overline{F}_{n+1}^{\rightarrow})$ holds, hence property 1 holds. Moreover, $D_{n+1}^{\rightarrow} = H^{\rightarrow} + \sum_{i=0}^{n-1} Save_{i,n-i+1}^{\rightarrow}$ and so $D_{n+1}^{\rightarrow} = \overline{F}_{n+1}^{\rightarrow} + Save_{n,1}^{\rightarrow} + \sum_{i=0}^{n-1} Save_{i,n-i+1}^{\rightarrow} = \overline{F}_{n+1}^{\rightarrow} + \sum_{i=0}^{n} Save_{i,(n+1)-i}^{\rightarrow}$, hence hence property 2 holds. Similarly, $D_{n+1}^{\top} = H^{\top} + \sum_{i=0}^{n-1} Save_{i,n-i+1}^{\top}$ and so $D_{n+1}^{\top} = F_{n+1}^{\top} + Save_{n,1}^{\top} + \sum_{i=0}^{n-1} Save_{i,n-i+1}^{\top} = F_{n+1}^{\top} + \sum_{i=0}^{n} Save_{i,(n+1)-i}^{\top}$, hence hence property 3 holds. Notice that we showed $(\overline{F}_n^s \rightarrow_{\mathsf{r}} H^{s,\rightarrow} + H^{s,\top}) \models \pi_s^{\rightarrow}$. Thus, $(Save_{n,0}^{\rightarrow} \rightarrow_{\mathsf{r}} Save_{n,1}^{\rightarrow} + Save_{n,1}^{\top}) \models \pi_s^{\rightarrow}$ and so property 5 holds. We already proved that for all $i \in \{0, \ldots, n-1\}$, $Save_{i,n-i}^{\rightarrow} \rightarrow_{\mathsf{r}} Save_{i,n-i+1}^{\rightarrow} + Save_{i,n-i+1}^{\top}$. Since $(Save_{n,0}^{\rightarrow} \rightarrow_{\mathsf{r}} Save_{n,1}^{\rightarrow} + Save_{n,1}^{\top}) \models \pi_s^{\rightarrow}$, we directly deduce that for all $i \in \{0, \ldots, n\}$, $Save_{i,n-i}^{\rightarrow} \rightarrow_{\mathsf{r}} Save_{i,(n+1)-i}^{\rightarrow} + Save_{i,(n+1)-i}^{\top}$ and so property 4 holds. Similarly, we proved that $(\overline{F}_n^c \rightarrow_{\mathsf{r}} H^{c,\rightarrow} + H^{c,\top}) \models \pi_c^{\rightarrow}$ meaning that $(F_n^{\rightarrow} \rightarrow_{\mathsf{r}} \overline{F}_{n+1}^{\rightarrow} + F_{n+1}^{\top}) \models \pi_c^{\rightarrow}$, thus property 6 holds. Finally, we know that $\overline{F}_n^{\rightarrow} = \overline{F}_n^c + \overline{F}_n^s$ implying $\overline{F}_n^{\rightarrow} = F_n^{\rightarrow} + Save_{n,0}^{\rightarrow}$. Therefore, property 7 holds. This conclude the proof of $P(n)$ for all $n \in \mathbb{N}$.

To complete the main proof, notice that $F_0^{\rightarrow} + Save_{0,0}^{\rightarrow} = D_0^{\rightarrow}$, $F_0^{\top} = D_0^{\top}$ and for all $k \in \mathbb{N}$, $F_k^{\rightarrow} \xrightarrow{\tau}_{\mathsf{r}} F_{k+1}^{\rightarrow} + (Save_{k+1,0}^{\rightarrow} + F_{k+1}^{\top})$ imply that $D \Longrightarrow_{\mathsf{r}} \sum_{k\in\mathbb{N}} Save_{k,0}^{\rightarrow} + F_k^{\top}$. Notice that for all $k \in \mathbb{N}$, we already proved that $(F_k^{\rightarrow} \xrightarrow{\tau}_{\mathsf{r}} F_{k+1}^{\rightarrow} + (Save_{k+1,0}^{\rightarrow} + F_{k+1}^{\top})) \models \pi_c^{\rightarrow}$. By denoting $A = \sum_{k\in\mathbb{N}} Save_{k,0}^{\rightarrow}$ and $A^{\top} = \sum_{k\in\mathbb{N}} F_k^{\top}$, we deduce that $(D \Longrightarrow_{\mathsf{r}} A + A^{\top}) \models \pi_c^{\rightarrow}$.

Now notice that for all $i \in \mathbb{N}$, we know from the property 5 of $\forall n \in \mathbb{N}.P(n)$ that $(Save_{i,0}^{\rightarrow} \rightarrow_{\mathsf{r}} Save_{i,1}^{\rightarrow} + Save_{i,1}^{\top}) \models \pi_s^{\rightarrow}$. Thus $(\sum_{i\in\mathbb{N}} Save_{i,0}^{\rightarrow} \rightarrow_{\mathsf{r}} \sum_{i\in\mathbb{N}} Save_{i,1}^{\rightarrow} + Save_{i,1}^{\top}) \models \pi_s^{\rightarrow}$. By denoting $B = \sum_{i\in\mathbb{N}} Save_{i,1}^{\rightarrow}$ and $B^{\top} = \sum_{i\in\mathbb{N}} Save_{i,1}^{\top}$, we deduce that $(A \rightarrow_{\mathsf{r}} B + B^{\top}) \models \pi_s^{\rightarrow}$.

Finally let us build $B_0^{\rightarrow} = \sum_{i\in\mathbb{N}} Save_{i,1}^{\rightarrow}$ and $B_0^{\top} = \varnothing$. We know from the property $\forall n \in \mathbb{N}.P(n)$ that for all $i \in \mathbb{N}$, for all $k > 0$, $Save_{i,k}^{\rightarrow} \rightarrow_{\mathsf{r}} Save_{i,k+1}^{\rightarrow} + Save_{i,k+1}^{\top}$. Hence for all $k > 0$, $\sum_{i\in\mathbb{N}} Save_{i,k}^{\rightarrow} \rightarrow_{\mathsf{r}} \sum_{i\in\mathbb{N}} Save_{i,k+1}^{\rightarrow} + \sum_{i\in\mathbb{N}} Save_{i,k+1}^{\top}$. Hence, if we define for all $k > 0$, for all $\alpha \in \{\rightarrow, \top\}$, $B_k^{\alpha} = \sum_{i\in\mathbb{N}} Save_{i,k+1}^{\alpha}$, we deduce that for all $k \in \mathbb{N}$, $B_k^{\rightarrow} \rightarrow_{\mathsf{r}} B_{k+1}^{\rightarrow} + B_{k+1}^{\top}$. Therefore, by denoting $C = \sum_{k>0} \sum_{i\in\mathbb{N}} Save_{i,k+1}^{\top}$, we obtain $B \Longrightarrow_{\mathsf{r}} C$. It remains to prove that $E = A^{\top} + B^{\top} + C$: $A^{\top} + B^{\top} + C = \sum_{k\in\mathbb{N}} F_k^{\top} + \sum_{i\in\mathbb{N}} Save_{i,1}^{\top} + \sum_{k>0} \sum_{i\in\mathbb{N}} Save_{i,k+1}^{\top} = \sum_{i\in\mathbb{N}} F_i^{\top} + \sum_{k\in\mathbb{N}} \sum_{i\in\mathbb{N}} Save_{i,k+1}^{\top} = \sum_{k\in\mathbb{N}} D_k^{\top} = E$ (see property 3 of the property P) . This allows us to conclude that $E = A^{\top} + B^{\top} + C$.

Let us now assume that $\mathsf{m}(A) \leq_{\mathsf{m}} \mathsf{m}(B + B^{\top})$. We proved that $(A \xrightarrow{\tau}_{\mathsf{r}} B + B^{\top}) \models \pi_s^{\rightarrow}$. Thus, $\mathsf{m}(A) >_{\mathsf{m}} \mathsf{m}(B + B^{\top})$ and so $A = B = B^{\top} = \varnothing$. Since $B \overset{\tau}{\Longrightarrow}_{\mathsf{r}} C$, we deduce that $C = \varnothing$. With $E = C + B^{\top} + A^{\top}$ and $(D \overset{\tau}{\Longrightarrow}_{\mathsf{r}} A + A^{\top}) \models \pi_c^{\rightarrow}$, we conclude that $(D \overset{\tau}{\Longrightarrow}_{\mathsf{r}} E) \models \pi_c^{\rightarrow}$. □

Lemma 59. Let $\mathsf{N} = (\mathcal{S}_{\mathsf{N}}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_{\mathsf{N}})$ be a NPLTS with $\mathcal{A}_{int} = \{\tau\}$. Let π_1, π_2 be two predicates on $\rightarrow$ and $\pi_1^{\mathcal{S}}, \pi_2^{\mathcal{S}}$ be two predicates on $\mathcal{S}_{\mathsf{N}}$ such that for all $x \in \mathcal{S}_{\mathsf{N}}$, for all $D \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{N}})$

- $\pi_1^{\mathcal{S}}(x) \wedge \pi_2^{\mathcal{S}}(x)$ does not hold;
- for all $i \in \{1,2\}$, $\pi_i^{\mathcal{S}}(x)$ iff $\pi_i(x \to D)$
- for all $i \in \{1,2\}$,$\pi_i(x \to D)$ implies $\pi_i^{\mathcal{S}}(D)$.

For all $A_1, A_2, B \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{N}})$, if

$$A_1 + A_2 \overset{\tau}{\Longrightarrow}_{\mathsf{r}} B \qquad \pi_1^{\mathcal{S}}(A_1) \qquad \pi_2^{\mathcal{S}}(A_2)$$

then there exist $B_1, B_2 \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{N}})$ such that $B = B_1 + B_2$ and for all $i \in \{1,2\}$, $\pi^{\mathcal{S}}(B_i)$ and $(A_i \overset{\tau}{\Longrightarrow}_{\mathsf{r}} B_i) \models \pi_i$

Proof. By definition of $A_1 + A_2 \overset{\tau}{\Longrightarrow}_{\mathsf{r}} B$, we know there exists an infinite scheme $A_1 + A_2 = C_0^{\to} + C_0^{\top}$ and for all $k \in \mathbb{N}$, $C_k^{\to} \overset{\tau}{\to}_{\mathsf{r}} C_{k+1}^{\to} + C_{k+1}^{\top}$ and $B = \sum_{k \in \mathbb{N}} C_k^{\top}$.

Let us consider the property $P(n)$ defined as: there exist $\{C_{k,i}^{\alpha} \mid \alpha \in \{\to, \top\}, i \in \{1,2\}, k \in \{0, \ldots, n\}\}$ such that

1. for all $\alpha \in \{\to, \top\}$, for all $k \in \{0, \ldots, n\}$, $C_{k,1}^{\alpha} + C_{k,2}^{\alpha} = C_k^{\alpha}$
2. for all $\alpha \in \{\to, \top\}$, for all $k \in \{0, \ldots, n\}$, for all $i \in \{1,2\}$, $\pi_i^{\mathcal{S}}(C_{k,i}^{\alpha})$ holds.
3. for all $k \in \{0, \ldots, n-1\}$, for all $i \in \{1,2\}$, $(C_{k,i}^{\to} \overset{\tau}{\to}_{\mathsf{r}} C_{k+1,i}^{\to} + C_{k+1,i}^{\top}) \models \pi_i$.

We prove $P(n)$ for all $n \in \mathbb{N}$ by induction on n.

Base case $n = 0$: Since for all $x \in \mathcal{S}_{\mathsf{N}}$, $\pi_1^{\mathcal{S}}(x) \wedge \pi_2^{\mathcal{S}}(x)$ and $\pi_i(A_i)$ for $i = 1,2$, we deduce that there exists $C_{0,1}^{\to}, C_{0,2}^{\to}, C_{0,1}^{\top}, C_{0,2}^{\top}$ such that for all $\alpha \in \{\to, \top\}$, $C_{0,1}^{\alpha} + C_{0,2}^{\alpha} = C_0^{\alpha}$, and $\pi_i^{\mathcal{S}}(C_{0,i}^{\alpha})$ for $i = 1,2$.

Inductive step $n > 0$: By our inductive hypothesis, we know that $C_n^{\to} = C_{n,1}^{\to} + C_{n,2}^{\to}$ with $\pi_1^{\mathcal{S}}(C_{n,1}^{\to})$ and $\pi_2^{\mathcal{S}}(C_{n,2}^{\to})$. Furthermore, $C_k^{\to} \overset{\tau}{\to}_{\mathsf{r}} C_{k+1}^{\to} + C_{k+1}^{\top}$.

By hypothesis on π_1 and π_2 and the fact that both $\pi_1^{\mathcal{S}}(C_{n,1}^{\to})$ and $\pi_2^{\mathcal{S}}(C_{n,2}^{\to})$ hold, we deduce that $(C_n^{\to} \overset{\tau}{\to}_{\mathsf{r}} C_{n+1}^{\to} + C_{n+1}^{\top}) \models \pi_1 \vee \pi_2$. By Lemma 57, we deduce that there exists $\{C_{n,k}^{\to,p} \mid p = 1,2 \wedge k = 1,2\}$ and $\{C_{n+1,k}^{\alpha,p} \mid \alpha \in \{\to, \top\}, k \in \{1,2\}, p \in \{1,2\}\}$ such that:

- for all $p = 1,2$, for all $k = 1,2$, $(C_{n,k}^{\to,p} \overset{\tau}{\to}_{\mathsf{r}} C_{n+1,k}^{\to,p} + C_{n+1,k}^{\top,p}) \models \pi_p$
- for all $k = 1,2$, $C_{n,k}^{\to} = C_{n,k}^{\to,1} + C_{n,k}^{\to,2}$
- for all $\alpha \in \{\to, \top\}$, $C_{n+1}^{\alpha} = \sum_{p=1}^{2} \sum_{k=1}^{2} C_{n+1,k}^{\alpha,p}$

By hypothesis on π_1 and π_2, for all $p = 1,2$, for all $k = 1,2$, $(C_{n,k}^{\to,p} \overset{\tau}{\to}_{\mathsf{r}} C_{n+1,k}^{\to,p} + C_{n+1,k}^{\top,p}) \models \pi_p$ implies $\pi_p^{\mathcal{S}}(C_{n,k}^{\to,p})$ holds. However, $\pi_1^{\mathcal{S}}(C_{n,1}^{\to})$ implies that for all $x \in \mathrm{supp}(C_{n,1}^{\to})$, $\neg\pi_2^{\mathcal{S}}(x)$. Hence $\neg\pi_2^{\mathcal{S}}(C_{n,1}^{\to,2})$ and so $C_{n,1}^{\to,2} = \varnothing$. Similarly, we deduce that $C_{n,2}^{\to,1} = \varnothing$. Both of them imply that $C_{n+1,2}^{\to,1} = C_{n+1,2}^{\top,1} = C_{n+1,1}^{\to,2} = C_{n+1,1}^{\top,2} = \varnothing$. To summarize, we have that for all $p \in \{1,2\}$,

- $(C^{\rightarrow,p}_{n,p} \xrightarrow{\tau}_{\mathsf{r}} C^{\rightarrow,p}_{n+1,p} + C^{\top,p}_{n+1,p}) \models \pi_p$
- $C^{\rightarrow}_{n,p} = C^{\rightarrow,p}_{n,p}$
- for all $\alpha \in \{\bot, \rightarrow\}$, $C^{\alpha}_{n+1} = C^{\alpha,1}_{n+1,1} + C^{\alpha,2}_{n+1,2}$.

We conclude by defining $C^{\alpha}_{n+1,i} = C^{\alpha,i}_{n+1,i}$ for $i \in \{1,2\}$ and $\alpha \in \{\rightarrow, \top\}$.

Since $P(n)$ holds for all $n \in \mathbb{N}$, we directly obtain that for all $i \in \{1,2\}$, $(C^{\rightarrow}_{0,i} + C^{\top}_{0,i} \overset{\tau}{\Longrightarrow}_{\mathsf{r}} \sum_{k\in\mathbb{N}} C\top_{k,i}) \models \pi_i$ with $\pi^{\mathcal{S}}_i(\sum_{k\in\mathbb{N}} C\top_{k,i})$. With $B = \sum_{k\in\mathbb{N}} C^{\top}_k = \sum_{k\in\mathbb{N}} C^{\top}_{k,1} + \sum_{k\in\mathbb{N}} C^{\top}_{k,2}$, we conclude by taking $B_i = \sum_{k\in\mathbb{N}} C^{\top}_{k,i}$ for $i = 1,2$. □

Lemma 60. Let $\mathsf{N} = (\mathcal{S}_{\mathsf{N}}, \mathcal{A}_{ext} \sqcup \mathcal{A}_{int}, \mathsf{trans}_{\mathsf{N}})$ and $\mathsf{N}' = (\mathcal{S}_{\mathsf{N}'}, \mathcal{A}'_{ext} \sqcup \mathcal{A}'_{int}, \mathsf{trans}_{\mathsf{N}'})$ be two NPLTS with $\mathcal{A}_{int} = \mathcal{A}'_{int} = \{\tau\}$. Let $f : \mathcal{S}_{\mathsf{N}} \rightarrow \mathcal{S}_{\mathsf{N}'}$. Let π_{all} and π_c two predicates on $\rightarrow_{\mathsf{N}}$. Let $\pi^{\mathcal{S}}$ be a predicate.

If for all $A, B \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{N}})$, for all $D \in \mathcal{D}(\mathcal{S}_{\mathsf{N}})$, for all $x \in \mathcal{S}_{\mathsf{N}}$,

- if $\pi^{\rightarrow}_c(x \rightarrow_{\mathsf{N}} D)$ then $\pi^{\mathcal{S}}(D)$
- $(A \xrightarrow{\tau}_{\mathsf{r},\mathsf{N}} B) \models \neg\pi_c \wedge \pi_{all}$ implies $f(A) = f(B)$ and either $A = \varnothing$ or $\mathsf{m}(A) > \mathsf{m}(B)$
- $(A \xrightarrow{\tau}_{\mathsf{r},\mathsf{N}} B) \models \pi_c \wedge \pi_{all}$ implies $f(A) \xrightarrow{\tau}_{\mathsf{r},\mathsf{N}'} f(B)$ and $\mathsf{m}(A) = \mathsf{m}(B)$

then for all $(D \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}} E) \models \pi_{all}$, we have $f(D) \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}'} f(E)$

Proof. Consider three sub-distributions $A, A^{\top}_1, A^{\top}_2$ such that $(D \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}} A + A^{\top}_1) \models \pi_{all}$, $E = A^{\top}_1 + A^{\top}_2$, $(A \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}} A^{\top}_2) \models \pi_{all}$ and $f(D) \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}'} f(A + A^{\top}_1)$. Such sub-distributions exist since we can take $A = D$, $A^{\top}_1 = \varnothing$ and $A^{\top}_2 = E$. Let us take $A, A^{\top}_1, A^{\top}_2$ a maximal for the following order $(A, A^{\top}_1, A^{\top}_2) < (B, B^{\top}_1, B^{\top}_2)$ when $A^{\top}_1 <_{\mathcal{D}} B^{\top}_1$ or $A^{\top}_1 = B^{\top}_1$ and $\mathsf{m}(A) >_{\mathsf{m}} \mathsf{m}(B)$ (where $<_{\mathcal{D}}$ stands for the inclusion of distribution, i.e. $D <_{\mathcal{D}} D'$ if for all x, $D(x) < D'(x)$).

By applying Lemma 58 on $(A \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}} A^{\top}_2) \models \pi_{all}$ (with $\pi^{\rightarrow}_c = \pi_c$ and $\pi^{\rightarrow}_s = \neg\pi_c$), we deduce that there exist $\overline{A}^{\rightarrow}, \overline{A}^{\top}, \overline{B}^{\rightarrow}, \overline{B}^{\top}, \overline{C}$ such that:

$$(A \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}} \overline{A}^{\rightarrow} + \overline{A}^{\top}) \models \pi_c \wedge \pi_{all} \quad (\overline{A}^{\rightarrow} \xrightarrow{\tau}_{\mathsf{r},\mathsf{N}} \overline{B}^{\rightarrow} + \overline{B}^{\top}) \models \neg\pi_c \wedge \pi_{all} \quad (\overline{B}^{\rightarrow} \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}} \overline{C}) \models \pi_{all}$$

with $A^{\top}_2 = \overline{C} + \overline{B}^{\top} + \overline{A}^{\top}$. Let us define $\overline{A} = \overline{B}^{\rightarrow}$, $\overline{A}^{\top}_1 = \overline{A}^{\top} + \overline{B}^{\top} + A^{\top}_1$ and $\overline{A}^{\top}_2 = \overline{C}$. We show the following properties:

- $f(D) \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}'} f(\overline{A}) + f(\overline{A}^{\top}_1)$: We know that $(A \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}} \overline{A}^{\rightarrow} + \overline{A}^{\top}) \models \pi_c \wedge \pi_{all}$. By hypothesis on $\pi_c \wedge \pi_{all}$, we deduce that $f(A) \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}'} f(\overline{A}^{\rightarrow}) + f(\overline{A}^{\top})$. Hence $f(A) + f(A^{\top}_1) \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}'} f(\overline{A}^{\rightarrow}) + f(\overline{A}^{\top}) + f(A^{\top}_1)$. By hypothesis on $\neg\pi_c \wedge \pi_{all}$, we deduce from $(\overline{A}^{\rightarrow} \xrightarrow{\tau}_{\mathsf{r},\mathsf{N}} \overline{B}^{\rightarrow} + \overline{B}^{\top}) \models \neg\pi_c \wedge \pi_{all}$ that $f(\overline{A}^{\rightarrow}) = f(\overline{B}^{\rightarrow}) + f(\overline{B}^{\top})$. Hence $f(A) + f(A^{\top}_1) \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}'} f(\overline{A}) + f(\overline{A}^{\top}_1)$ and so $f(D) \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}'} f(\overline{A}) + f(\overline{A}^{\top}_1)$.

- $(D \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}} \overline{A}+\overline{A}_1^\top) \models \pi_{all}$: $(A \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}} \overrightarrow{\overline{A}}+\overline{A}^\top) \models \pi_c \wedge \pi_{all}$ implies that $(A+A_1^\top \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}} \overrightarrow{\overline{A}}+\overline{A}^\top+A_1^\top) \models \wedge\pi_{all}$. Furthermore $(\overrightarrow{\overline{A}} \xrightarrow{\tau}_{\mathsf{r},\mathsf{N}} \overrightarrow{\overline{B}}+\overline{B}^\top) \models \neg\pi_c \wedge \pi_{all}$ implies that $(\overrightarrow{\overline{A}}+\overline{A}^\top+A_1^\top \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}} \overrightarrow{\overline{B}}+\overline{B}^\top+\overline{A}^\top+A_1^\top) \models \pi_{all}$. With $\overrightarrow{\overline{B}}+\overline{B}^\top+\overline{A}^\top+A_1^\top = \overline{A}+\overline{A}_1^\top$ and the fact that $(D \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}} A+A_1^\top) \models \pi_{all}$, we conclude that $(D \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}} \overline{A}+\overline{A}_1^\top) \models \pi_{all}$.
- $(\overline{A} \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}} \overline{A}_2^\top) \models \pi_c \vee \pi_s$: Notice that $\overline{A}_2^\top = \overline{C}$ and $\overline{A} = \overrightarrow{\overline{B}}$ hence the result holds.
- $\overline{A}_1^\top + \overline{A}_2^\top = \overline{A}^\top + \overline{B}^\top + A_1^\top + \overline{C} = A_2^\top + A_1^\top = E$.

Since we selected $A, A_1^\top, A_2^\top$ as a maximal, then $(A, A_1^\top, A_2^\top) \not< (\overline{A}, \overline{A}_1^\top, \overline{A}_2^\top)$. Since $\overline{A}_1^\top = \overline{A}^\top+\overline{B}^\top+A_1^\top \geq A_1^\top$, we deduce that $\overline{A}^\top = \overline{B}^\top = \varnothing$. Therefore, $(A, A_1^\top, A_2^\top) \not< (\overline{A}, \overline{A}_1^\top, \overline{A}_2^\top)$ implies $\mathsf{m}(A) \leq_{\mathsf{m}} \mathsf{m}(\overline{A})$.

Note that by hypothesis on $\pi_c \wedge \pi_{all}$, $(A \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}} \overrightarrow{\overline{A}} + \overline{A}^\top) \models \pi_c \wedge \pi_{all}$ implies that $\mathsf{m}(A) = \mathsf{m}(\overrightarrow{\overline{A}})$ and so $\mathsf{m}(\overrightarrow{\overline{A}}) \leq_{\mathsf{m}} \mathsf{m}(\overline{A}) = \mathsf{m}(\overrightarrow{\overline{B}})$. By Lemma 58, we obtain that $(A \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}} A_2^\top) \models \pi_c \wedge \pi_{all}$ and so $(A + A_1^\top \xRightarrow{\tau}_{\mathsf{r}} E) \models \pi_c \wedge \pi_{all}$. By hypothesis on $\pi_c \wedge \pi_{all}$, we conclude that $f(A) + f(A_1^\top) \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}'} f(E)$ and so $f(D) \xRightarrow{\tau}_{\mathsf{r}} f(E)$. □

Lemma 61. For all $op \in \{\leq, \approx\}$, for all $a \in \{in(\xi,\zeta), out(\xi,\mathsf{ax}) \mid \xi,\zeta \text{ recipes}, \mathsf{ax} \in \mathcal{AX}\}$, for all $(\mathcal{P},\phi), (\mathcal{P}',\phi') \in \mathcal{SP}_\ell$, if $(\mathcal{P},\phi)\ R_{op}\ (\mathcal{P}',\phi')$ and $(\mathcal{P},\phi) \xrightarrow{a}_{\mathsf{N}^\ell} D$ then $(\mathcal{P}',\phi') \xRightarrow{a}_{\mathsf{r},\mathsf{N}^\ell} E$ and $D\ \widehat{R_{op}}\ E$ (and $E\ \widehat{R_\approx}\ D$ when $op = \approx$).

Proof. The proof for both input actions and output actions follows the same structure. We will start by considering the case when $a = in(\xi,\zeta)$ and only illustrate the part that change for the case $a = out(\xi,\mathsf{ax})$.

By definition, $(\mathcal{P},\phi) \xrightarrow{in(\xi,\zeta)}_{\mathsf{N}^\ell} D$ implies that $\mathcal{P} = \mathcal{P}_1 \cup \{\!\!\{\mathsf{in}(u,x).P\}\!\!\}$, $u \doteq \xi\phi$, $Msg(\zeta\phi)$, $vars(\xi,\zeta) \subseteq dom(\phi)$ and $D = \delta_{(\{\!\!\{P\{\zeta\phi/x\}\}\!\!\} \cup \mathcal{P}_1,\phi)}$. By definition of R_{op}, we know that $(\mathcal{P},\phi)\ R_{op}\ (\mathcal{P}',\phi')$ implies $(\mathcal{P},\phi) \in \mathcal{SP}_\ell(\phi,\mathcal{N}_{ch})$, $(\mathcal{P}',\phi') \in \mathcal{SP}_\ell(\phi',\mathcal{N}_{ch})$ and $\pi^{e\to p}_{\phi,\mathcal{N}_{ch}}((\mathcal{P},\phi))\ op^{\mathcal{R}_\mathsf{r}}_{obs}\ \pi^{e\to p}_{\phi',\mathcal{N}_{ch}}((\mathcal{P}',\phi'))$ for some $\mathcal{N}_{ch}$. Hence, $|\phi| = |\phi'|$ and let us denote $n = |\phi|$. Thanks to Lemma 45, we can assume that $\mathcal{N}_{ch} \cap fn(\xi,\zeta) = \varnothing$.

Let us consider a fresh sequence $\mathcal{N}'_{ch} = [c'_{\mathsf{ax}_i}]_{i=1}^n$ of public name, i.e. $fn(\mathcal{N}'_{ch}) \cap fn(\mathcal{P},\phi,\mathcal{P}',\phi',\mathcal{N}_{ch}) = \varnothing$. Let us define $\rho = \{^{x_i}/_{\mathsf{ax}_i}\}_{i=1}^n$. Finally, consider a fresh public name $ok \in \mathcal{N}_{pub}$. We build the following process Out:

$$\begin{aligned} Out &:= \mathsf{in}(c_{\mathsf{ax}_1},x_1).\ldots.\mathsf{in}(c_{\mathsf{ax}_n},x_n).\mathsf{out}(\xi\rho,\zeta\rho).(Frame +_{0.5} \mathsf{out}(ok,ok).0) \\ Frame &:= \mathsf{out}(c'_{\mathsf{ax}_1},x_1).0 \mid \ldots \mid \mathsf{out}(c'_{\mathsf{ax}_n},x_n).0 \end{aligned}$$

First notice that Out is closed and $fn(Out) \subseteq \mathcal{N}_{pub}$ since ξ and ζ are recipes such that $vars(\xi,\zeta) \subseteq dom(\phi)$. If we denote $\mathcal{P}_O = \{\!\!\{Out\}\!\!\} \cup \pi^{e\to p}_{\phi,\mathcal{N}_{ch}}((\mathcal{P},\phi))$ and $\mathcal{P}'_O = \{\!\!\{Out\}\!\!\} \cup \pi^{e\to p}_{\phi',\mathcal{N}_{ch}}((\mathcal{P}',\phi'))$, we have $\mathcal{P}_O\ op^{\mathcal{R}_\mathsf{r}}_{obs}\ \mathcal{P}'_O$.

Since $\pi^{e\to p}_{\phi,\mathcal{N}_{ch}}((\mathcal{P},\phi)) = \mathcal{P} \cup \{\!\!\{\mathsf{out}(c_{\mathsf{ax}_i},\mathsf{ax}_i\phi).0\}\!\!\}_{i=1}^n$, we can successively apply the rule (Comm) on $c_{\mathsf{ax}_1},\ldots,c_{\mathsf{ax}_n}$ to obtain that $\mathcal{P}_O \xRightarrow{\tau}_{\mathsf{r}} \delta_{\mathcal{P}\cup\{\!\!\{\mathsf{out}(\xi\rho\sigma,\zeta\rho\sigma).(Frame+_{0.5}0)\}\!\!\}}$ with $\sigma = \rho^{-1}\phi$. By hypothesis, $\xi\phi \doteq u$ and $Msg(\zeta\phi)$. Hence we can apply the rule (Comm) on u to obtain

$\mathcal{P}_O \xRightarrow{\tau}_{\mathsf{r}} \delta_{\mathcal{P}_1 \cup \{\!\{P\{\zeta\phi/_x\}\}\!\} \cup \{\!\{(Frame +_{0.5} 0)\}\!\}}$. Finally, we apply the rules (PChoice) and (Par), we have the following:

$$\mathcal{P}_O \xRightarrow{\tau}_{\mathsf{r}} 0.5 \cdot \delta_{\mathcal{P}_1 \cup \{\!\{P\{\zeta\phi/_x\}, \mathsf{out}(ok,ok).0\}\!\}} + 0.5 \cdot \delta_{\mathcal{P}_1 \cup \{\!\{P\{\zeta\phi/_x\}\}\!\} \cup \mathcal{F}(\phi, \mathcal{N}'_{ch})}$$

By denoting $D_1 = 0.5 \cdot \delta_{\mathcal{P}_1 \cup \{\!\{P\{\zeta\phi/_x\}; \mathsf{out}(ok,ok).0\}\!\}} + 0.5 \cdot \delta_{\mathcal{P}_1 \cup \{\!\{P\{\zeta\phi/_x\}\}\!\} \cup \mathcal{F}(\phi, \mathcal{N}'_{ch})}$, we deduce from $\mathcal{P}_O \; op^{\mathcal{R}_\mathsf{r}}_{obs} \; \mathcal{P}'_O$ that there exists E_1 such that $\mathcal{P}'_O \xRightarrow{\tau}_{\mathsf{r}} E_1$ and $D_1 \; \widehat{op^{\mathcal{R}_\mathsf{r}}_{obs}} \; E_1$. Thanks to Lemma 44, we can assume w.l.o.g. that no rule (Par) or (Nil) is applicable on E_1.

Let us analyse E_1. We consider the following processes:

- $A^{j,k}_f(\mathcal{Q}') = \{\!\{\mathsf{in}(c_{\mathsf{ax}_j}, x_j).\ldots.\mathsf{in}(c_{\mathsf{ax}_n}, x_n).\mathsf{out}(\xi\rho\sigma_j, \zeta\rho\sigma_j).(Frame\sigma_{j-1} +_{0.5} \mathsf{out}(ok, ok))\}\!\} \cup \mathcal{Q}' \cup \{\!\{\mathsf{out}(c_{\mathsf{ax}_i}, \mathsf{ax}_i\phi').0\}\!\}^n_{i=j+1} \cup \{\!\{0\}\!\}^k_{i=1}$
- $A^k_{out}(\mathcal{Q}') = \{\!\{\mathsf{out}(\xi\rho, \zeta\rho\sigma_j).(Frame\sigma_n +_{0.5} \mathsf{out}(ok, ok).0)\}\!\} \cup \mathcal{Q}' \cup \{\!\{0\}\!\}^k_{i=1}$
- $A^k_+(\mathcal{Q}') = \{\!\{Frame\sigma_n +_{0.5} \mathsf{out}(ok, ok).0\}\!\} \cup \mathcal{Q}' \cup \{\!\{0\}\!\}^k_{i=1}$
- $A^{j,k}_{ch'}(\mathcal{Q}') = \{\!\{\mathsf{out}(c'_{\mathsf{ax}_j}, \mathsf{ax}_j\phi').0\}\!\}^j_{i=1} \cup \{\!\{\mathsf{out}(c'_{\mathsf{ax}_{j+1}}, \mathsf{ax}_{j+1}\phi').0 \mid \ldots \mid \mathsf{out}(c'_{\mathsf{ax}_n}, \mathsf{ax}_n\phi').0\}\!\} \cup \mathcal{Q}' \cup \{\!\{0\}\!\}^n_{i=1}$
- $A^k_{ok}(\mathcal{Q}') = \{\!\{\mathsf{out}(ok, ok).0\}\!\} \cup \mathcal{Q}' \cup \{\!\{0\}\!\}^k_{i=1}$

where $\sigma_j = \{^{\mathsf{ax}_i\phi'}/_{x_i}\}^j_{i=1}$.

Let us denote $\mathcal{A}^{j,k}_f = \{A^{i,k}_f(\mathcal{Q}) \mid \mathcal{Q} \in \mathcal{SP}_\ell(\phi', \mathcal{N}_{ch}) \wedge fn(\mathcal{Q}) \cap \mathcal{N}'_{ch} = \varnothing\}$. Similarly, we define $\mathcal{A}^k_{out}$, $\mathcal{A}^k_+$, $\mathcal{A}^{j,k}_{ch'}$ and $\mathcal{A}^k_{ok}$. We define a measure function m on processes from $\mathcal{A}^{j,k}_f$, $\mathcal{A}^k_{out}$, $\mathcal{A}^k_+$, $\mathcal{A}^{j,k}_{ch'}$ and $\mathcal{A}^k_{ok}$ as follows: For all $\mathcal{Q}$,

$$\begin{array}{lll} \mathcal{Q} \in \mathcal{A}^{j,k}_f \Rightarrow \mathsf{m}(\mathcal{Q}) = (5, j, k) & \mathcal{Q} \in \mathcal{A}^k_{out} \Rightarrow \mathsf{m}(\mathcal{Q}) = (4, k, 0) & \mathcal{Q} \in \mathcal{A}^k_+ \Rightarrow \mathsf{m}(\mathcal{Q}) = (3, k, 0) \\ \mathcal{Q} \in \mathcal{A}^{j,k}_{ch'} \Rightarrow \mathsf{m}(\mathcal{Q}) = (2, n-j, k) & \mathcal{Q} \in \mathcal{A}^k_{ok} \Rightarrow \mathsf{m}(\mathcal{Q}) = (1, k, 0) & \end{array}$$

Moreover, we consider a function $\mathsf{corr} : \mathcal{SP} \mapsto \mathcal{SP}_\ell$ such that for all $(\mathcal{Q}, \phi') \in \mathcal{SP}_\ell(\phi', \mathcal{N}_{ch})$ with $fn(\mathcal{Q}) \cap \mathcal{N}'_{ch} = \varnothing$, $\mathsf{corr}(A^{j,k}_f(\mathcal{Q})) = \mathsf{corr}(A^k_{out}(\mathcal{Q})) = \mathsf{corr}(A^k_+(\mathcal{Q})) = \mathsf{corr}(A^{j,k}_{ch'}(\mathcal{Q})) = \mathsf{corr}(A^k_{ok}(\mathcal{Q})) = (\mathcal{Q}, \phi')$.

Since $\mathcal{P}'_O \xRightarrow{\tau}_{\mathsf{r}} E_1$, we know that there exists an infinite scheme

$$\begin{array}{l} \delta_{\mathcal{P}'_0} = E^{\rightarrow}_0 + E^{\top}_0 \\ E^{\rightarrow}_0 \xrightarrow{\tau}_{\mathsf{r}} E^{\rightarrow}_1 + E^{\top}_1 \\ \ldots \\ E^{\rightarrow}_k \xrightarrow{\tau}_{\mathsf{r}} E^{\rightarrow}_{k+1} + E^{\top}_{k+1} \\ \ldots \end{array}$$

such that $E_1 = \sum_{k \in \mathbb{N}} E^{\top}_k$.

First notice that $\mathcal{P}'_O = A^{n,0}_{frame}(\mathcal{P}')$ and $\mathsf{corr}(\mathcal{P}'_O) = (\mathcal{P}', \phi')$. Second, by a simple case analysis, we deduce the following statements for all $\mathcal{Q} \rightarrow D$

- $\mathcal{Q} \in \mathcal{A}_f^{j,k}$ implies either $\mathrm{supp}(D) \subseteq \mathcal{A}_f^{j-1,k+1} \cup \mathcal{A}_f^{j,k-1} \cup \mathcal{A}_{out}^{k+1}$ and $\mathsf{corr}(D) = \mathsf{corr}(\delta_{\mathcal{Q}})$; or $\mathrm{supp}(D) \subseteq \mathcal{A}_f^{j,k}$ and $\mathsf{corr}(\mathcal{Q}) \xrightarrow{\tau} \mathsf{corr}(D)$.
- $\mathcal{Q} \in \mathcal{A}_{out}^{k}$ implies either $\mathrm{supp}(D) \subseteq \mathcal{A}_{out}^{k-1}$ and $\mathsf{corr}(D) = \mathsf{corr}(\delta_{\mathcal{Q}})$; or $\mathrm{supp}(D) \subseteq \mathcal{A}_{+}^{k}$ and $\mathsf{corr}(\mathcal{Q}) \xrightarrow{in(\xi,\zeta)} \mathsf{corr}(D)$; or $\mathrm{supp}(D) \subseteq \mathcal{A}_{out}^{k}$ and $\mathsf{corr}(\mathcal{Q}) \xrightarrow{\tau} \mathsf{corr}(D)$
- $\mathcal{Q} \in \mathcal{A}_{+}^{k}$ implies either $\mathrm{supp}(D) \subseteq \mathcal{A}_{+}^{k-1} \cup \mathcal{A}_{ch'}^{0,k} \cup \mathcal{A}_{ok}^{k}$ and $\mathsf{corr}(D) = \mathsf{corr}(\delta_{\mathcal{Q}})$; or $\mathrm{supp}(D) \subseteq \mathcal{A}_{+}^{k}$ and $\mathsf{corr}(\mathcal{Q}) \xrightarrow{\tau} \mathsf{corr}(D)$
- $\mathcal{Q} \in \mathcal{A}_{ch'}^{j,k}$ implies either $\mathrm{supp}(D) \subseteq \mathcal{A}_{ch'}^{j+1,k} \cup \mathcal{A}_{ch'}^{j,k-1}$ and $\mathsf{corr}(D) = \mathsf{corr}(\delta_{\mathcal{Q}})$; or $\mathrm{supp}(D) \subseteq \mathcal{A}_{ch'}^{j,k}$ and $\mathsf{corr}(\mathcal{Q}) \xrightarrow{\tau} \mathsf{corr}(D)$
- $\mathcal{Q} \in \mathcal{A}_{ok}^{k}$ implies either $\mathrm{supp}(D) \subseteq \mathcal{A}_{ok}^{k-1}$ and $\mathsf{corr}(D) = \mathsf{corr}(\delta_{\mathcal{Q}})$; or $\mathrm{supp}(D) \subseteq \mathcal{A}_{ok}^{k}$ and $\mathsf{corr}(\mathcal{Q}) \xrightarrow{\tau} \mathsf{corr}(D)$

One of the direct property we deduce from these is that for all $k \in \mathbb{N}$, for all $\alpha \in \{\rightarrow, \top\}$, $\mathrm{supp}(E_k^{\alpha}) \subseteq \bigcup_{k=0}^{n} \bigcup_{j=0}^{n} \mathcal{A}_f^{j,k} \cup \mathcal{A}_{out}^{k} \cup \mathcal{A}_{+}^{k} \cup \mathcal{A}_{ch'}^{j,k} \cup \mathcal{A}_{ok}^{k}$.

We proved that $D_1 \ \widehat{op_{obs}^{\mathcal{R}_r}} \ E_1$. Consider E_{ok} the largest sub-distribution of E_1 such that for all $\mathcal{P}'' \in \mathrm{supp}(E_{ok})$, $\mathcal{P}_1 \cup \{\!\{P\{^{\zeta\phi}/_x\}, \mathsf{out}(ok, ok).0\}\!\} \ op_{obs}^{\mathcal{R}_r} \ \mathcal{P}''$. Notice that $\mathrm{RProb}_{\mathcal{R}_r}(\mathcal{P}_1 \cup \{\!\{P\{^{\zeta\phi}/_x\}, \mathsf{out}(ok, ok).0\}\!\}, \downarrow ok) = 1$. Hence, $\mathrm{supp}(E_{ok}) \subseteq \{A_{ok}^{k}(\mathcal{Q}'') \mid (\mathcal{Q}'', \phi') \in \mathcal{SP}_{\ell}(\phi', \mathcal{N}_{ch})\}$. Similarly, if we denote $E_{ch'}$ the largest sub-distribution of E_1 such that for all $\mathcal{P}'' \in \mathrm{supp}(E_{ch'})$, $\mathcal{P}_1 \cup \{\!\{P\{\zeta\phi/_x\}\}\!\} \cup \mathcal{F}(\phi, \mathcal{N}'_{ch}) \ op_{obs}^{\mathcal{R}_r} \ \mathcal{P}''$, we obtain that $\mathrm{supp}(E_{ch'}) \subseteq \{A_{ch'}^{j,k}(\mathcal{Q}'') \mid (\mathcal{Q}'', \phi') \in \mathcal{SP}_{\ell}(\phi', \mathcal{N}_{ch})\}$. However, $D_1 \ \widehat{op_{obs}^{\mathcal{R}_r}} \ E_1$ implies that $D_1(\mathcal{P}_1 \cup \{\!\{P\{^{\zeta\phi}/_x\}, \mathsf{out}(ok, ok).0\}\!\}) = 0.5 \leq \sum_{\mathcal{P}''} E_{ok}(\mathcal{P}'')$ and $D_1(\mathcal{P}_1 \cup \{\!\{P\{\zeta\phi/_x\}\}\!\} \cup \mathcal{F}(\phi, \mathcal{N}'_{ch})) = 0.5 \leq \sum_{\mathcal{P}''} E_{ch'}(\mathcal{P}'')$. Since $\mathrm{supp}(E_{ch'}) \cap \mathrm{supp}(E_{ok}) = \varnothing$, we conclude that $E_1 = E_{ch'} \dotplus E_{ok}$ with $\sum_{\mathcal{P}''} E_{ch'}(\mathcal{P}'') = \sum_{\mathcal{P}''} E_{ok}(\mathcal{P}'') = 0.5$. Finally, since no rule (Nil) or (Par) is applicable on E_1, we deduce that $\mathrm{supp}(E_{ch'}) \subseteq \mathcal{A}_{ch'}^{n,0}$ and so $\mathrm{supp}(E_{ch'}) \subseteq \mathcal{SP}(\phi', \mathcal{N}'_{ch})$.

Note that by construction of $E_{ch'}$, $\delta_{\mathcal{P}_1 \cup \{\!\{P\{\zeta\phi/_x\}\}\!\} \cup \mathcal{F}(\phi, \mathcal{N}'_{ch})} \ \widehat{op_{obs}^{\mathcal{R}_r}} \ 2 \cdot E$. Thus, by denoting $E = 2 \cdot E_{ch'}$ and by Lemma 54, we obtain that $D = \pi_{\phi', \mathcal{N}'_{ch}}^{p \rightarrow e}(\delta_{\mathcal{P}_1 \cup \{\!\{P\{\zeta\phi/_x\}\}\!\} \cup \mathcal{F}(\phi, \mathcal{N}'_{ch})}) \ \widehat{R_{op}} \ \pi_{\phi', \mathcal{N}'_{ch}}^{p \rightarrow e}(E)$.

It remains to show that $(\mathcal{P}', \phi') \xRightarrow{in(\xi,\zeta)}_{\mathsf{r},\mathsf{N}^{\ell}} \pi_{\phi', \mathcal{N}'_{ch}}^{p \rightarrow e}(E)$: Consider the predicate $\pi^{\mathcal{S}}$ such that $\pi^{\mathcal{S}}(\mathcal{Q})$ holds iff $\mathcal{Q} \subseteq \bigcup_{k=0}^{n} \mathcal{A}_{out}^{k} \cup \bigcup_{j=1}^{n} \mathcal{A}_f^{j,k}$. We also consider the predicates $\pi_s^{\rightarrow}$ and $\pi_c^{\rightarrow}$ on $\xrightarrow{\tau}$ such that $\pi_s^{\rightarrow}(\mathcal{Q} \rightarrow D)$ holds iff $\mathcal{Q} \in \mathcal{A}_{out}^{k}$ for some k and $\mathrm{supp}(D) \subseteq \mathcal{A}_{+}^{k}$; and $\pi_c^{\rightarrow}(\mathcal{Q} \rightarrow D)$ holds iff $\pi^{\mathcal{S}}(\mathcal{Q})$ and either $\mathsf{corr}(\delta_{\mathcal{Q}}) = \mathsf{corr}(D)$ or $\mathsf{corr}(\mathcal{Q}) \xrightarrow{\tau} \mathsf{corr}(D)$. Notice that $\pi^{\mathcal{S}}$, $\pi_c^{\rightarrow}$ and $\pi_s^{\rightarrow}$ satisfy the conditions of Lemma 57. Therefore, $A, A^{\top}, B, B^{\top}, C \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{N}})$ such that

$$(\delta_{\mathcal{P}'_0} \xRightarrow{\tau}_{\mathsf{r}} A + A^{\top}) \models \pi_c^{\rightarrow} \qquad (A \xrightarrow{\tau}_{\mathsf{r}} B + B^{\top}) \models \pi_s^{\rightarrow} \qquad B \xRightarrow{\tau}_{\mathsf{r}} C$$

with $E_1 = C + B^{\top} + A^{\top}$. Note that we already proved that $E_1 = E_{ch'} \dotplus E_{ok}$ and so we deduce that $A^{\top} = B^{\top} = \varnothing$.

Notice that by definition of $\pi_s^{\rightarrow}$, $A \xrightarrow{\tau}_{\mathsf{r}} B$ implies $A \xrightarrow{\tau} B$. Moreover, $\pi_s^{\rightarrow}(\mathcal{Q} \xrightarrow{\tau} D)$ also implies $\mathsf{corr}(\mathcal{Q}) \xrightarrow{in(\xi,\zeta)} \mathsf{corr}(D)$. Therefore, $\mathsf{corr}(A) \xrightarrow{in(\xi,\zeta)} \mathsf{corr}(B)$.

Let us focus on $(\delta_{\mathcal{P}'_0} \xRightarrow{\tau}_{\mathsf{r}} A) \models \pi_c^{\rightarrow}$. We define the predicate π'_c such that $\pi'_c(\mathcal{Q} \rightarrow D)$ holds iff $\mathsf{corr}(\mathcal{Q}) \xrightarrow{\tau}_{\mathsf{N}^\ell} \mathsf{corr}(D)$. By construction, notice that $(A \xrightarrow{\tau}_{\mathsf{r},\mathsf{N}} B) \models \neg\pi'_c \wedge \pi_c^{\rightarrow}$ implies $\mathsf{corr}(A) = \mathsf{corr}(B)$ and either $A = \varnothing$ or $\mathsf{m}(A) > \mathsf{m}(B)$. Similarly, by construction, $(A \xrightarrow{\tau}_{\mathsf{r},\mathsf{N}} B) \models \pi'_c \wedge \pi_c^{\rightarrow}$ implies $\mathsf{corr}(A) \xrightarrow{\tau}_{\mathsf{N}^\ell} \mathsf{corr}(B)$ and $\mathsf{m}(A) = \mathsf{m}(B)$. This allows us to apply Lemma 60 on $(\delta_{\mathcal{P}'_0} \xRightarrow{\tau}_{\mathsf{r}} A) \models \pi_c^{\rightarrow}$. Therefore, $\mathsf{corr}(\delta_{\mathcal{P}'_0}) \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^\ell} \mathsf{corr}(A)$.

Let us summarize what we have proved so far: $\mathsf{corr}(\delta_{\mathcal{P}'_O}) \xRightarrow{\tau}_{\mathsf{r}} \mathsf{corr}(A) \xrightarrow{in(\xi,\zeta)} \mathsf{corr}(B)$ with $B \xRightarrow{\tau}_{\mathsf{r}} E_1$ with $\mathrm{supp}(B) \subseteq \bigcup_{k=1}^{n} \mathcal{A}_+^k$. Let us redefine the predicate $\pi^{\mathcal{S}}$ such that $\pi^{\mathcal{S}}(x)$ holds iff $x \in \bigcup_{k=1}^{n} \mathcal{A}_+^k$. We redefine π_c and π_s such that $\pi_c(x \rightarrow D)$ holds when $\pi^{\mathcal{S}}(D)$ and $\mathsf{corr}(x) \xrightarrow{\tau} \mathsf{corr}(D)$; and $\pi_s(x \rightarrow D)$ holds when $\mathsf{corr}(D) = \mathsf{corr}(\delta_x)$ and $\mathsf{m}(x) > \mathsf{m}(D)$. By applying Lemma 58 on $B \xRightarrow{\tau}_{\mathsf{r}} E_1$, we deduce that there exists $(B \xRightarrow{\tau}_{\mathsf{r}} B_1 + B_1^{\top}) \models \pi_c$, $(B_1 \xrightarrow{\tau}_{\mathsf{r}} B_2 + B_2^{\top}) \models \pi_s$, $B_2 \xRightarrow{\tau}_{\mathsf{r}} B_3$ with $E_1 = B_3 + B_1^{\top} + B_2^{\top}$. Once again we know that $E_1 = E_{ch'} \dot{+} E_{ok}$ and so we deduce that $B_1^{\top} = \varnothing$.

By definition of π_c, we deduce that $\mathsf{corr}(B) \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^\ell} \mathsf{corr}(B_1)$. Moreover, by definition of π_s, the transition $B_1 \xrightarrow{\tau}_{\mathsf{r}} B_2 + B_2^{\top}$ correspond to the execution of the probabilistic choice in the process $Frame +_{0.5} \mathsf{out}(ok, ok).0$. Thus, there exist two sub distributions $B_{ok}, B_{ch'}$ such that $B_2 + B_2^{\top} = 0.5 \cdot B_{ok} + 0.5 \cdot B_{ch'}$, $\mathrm{supp}(B_{ok}) \subseteq \cup_{k=0}^{n} \mathcal{A}_{ok}^k$, $\mathrm{supp}(B_{ch'}) \subseteq \cup_{k=0}^{n} \mathcal{A}_{ch'}^{0,k}$ and $\mathsf{corr}(B_1) = \mathsf{corr}(B_{ok}) = \mathsf{corr}(B_{ch'})$. By applying Lemma 59, we deduce that $0.5 \cdot B_{ok} \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} E_{ok}$ and $0.5 \cdot B_{ch'} \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} E_{ch'}$, implying that $B_{ok} \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} 2 \cdot E_{ok}$ and $B_{ch'} \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} 2 \cdot E_{ch'}$

We will finally show that $\mathsf{corr}(B_{ch'}) \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^\ell} \mathsf{corr}(2 \cdot E_{ch'})$ by applying Lemma 60 with predicate $\pi^{\mathcal{S}}$ on $\mathcal{S}_{\mathsf{N}^o}$ and predicates π_{all}, π_c on $\rightarrow_{\mathsf{N}^o}$ defined as:

- $\pi^{\mathcal{S}}(x)$ holds iff $x \in \cup_{k=0}^{n} \cup_{j=0}^{n} \mathcal{A}_{ch'}^{j,k}$
- $\pi_c(x \rightarrow_{\mathsf{N}^o} D)$ holds iff $\mathsf{m}(x) = \mathsf{m}(D)$ and $\mathsf{corr}(x) \rightarrow_{\mathsf{N}^\ell} \mathsf{corr}(D)$.
- π_{all} is always true.

This complete the proof of $\delta_{(\mathcal{P}',\phi')} \xRightarrow{in(\xi,\zeta)}_{\mathsf{r},\mathsf{N}^\ell} \mathsf{corr}(2 \cdot E_{ch'}) = \pi_{\phi',\mathcal{N}'_{ch}}^{p \rightarrow e}(E)$.

Let us now consider the case of the output action $a = out(\xi, \mathsf{ax})$. By definition, $(\mathcal{P}, \phi) \xrightarrow{out(\xi,\mathsf{ax})}_{\mathsf{N}^\ell} D$ implies that $\mathcal{P} = \mathcal{P}_1 \cup \{\!\!\{\mathsf{out}(u,t).P\}\!\!\}$, $u \doteq \xi\phi$, $\mathsf{ax} = \mathsf{ax}_{n+1}$, $Msg(t)$, $vars(\xi) \subseteq dom(\phi)$ and $D = \delta_{(\{\!\!\{P\}\!\!\} \cup \mathcal{P}_1, \phi\{\mathsf{ax} \mapsto t\})}$. Compare to the input case, we consider a sequence of public name $\mathcal{N}'_{ch}$ with one additional channel, i.e. $\mathcal{N}'_{ch} = [c'_{\mathsf{ax}_i}]_{i=1}^{n+1}$. Moreover, we consider the following process In instead of the process Out:

$$
\begin{aligned}
In &:= \mathsf{in}(c_{\mathsf{ax}_1}, x_1).\ldots.\mathsf{in}(c_{\mathsf{ax}_n}, x_n).\mathsf{in}(\xi\rho, x_{n+1}).(Frame +_{0.5} \mathsf{out}(ok, ok).0) \\
Frame &:= \mathsf{out}(c'_{\mathsf{ax}_1}, x_1).0 \mid \ldots \mid \mathsf{out}(c'_{\mathsf{ax}_{n+1}}, x_{n+1}).0
\end{aligned}
$$

Thus the initial processes $\mathcal{P}_O$ and $\mathcal{P}'_O$ used in the proof are defined as $\mathcal{P}_O = \{\!\!\{In\}\!\!\} \cup \pi_{\phi,\mathcal{N}_{ch}}^{e \rightarrow p}((\mathcal{P}, \phi))$ and $\mathcal{P}'_O = \{\!\!\{In\}\!\!\} \cup \pi_{\phi',\mathcal{N}_{ch}}^{e \rightarrow p}((\mathcal{P}', \phi'))$. Executing the process $\mathcal{P}_O$ allows us to

obtain:

$$\mathcal{P}_O \stackrel{\tau}{\Longrightarrow}_{\mathsf{r}} 0.5 \cdot \delta_{\mathcal{P}_1 \cup \{\!\!\{P, \mathsf{out}(ok,ok).0\}\!\!\}} + 0.5 \cdot \delta_{\mathcal{P}_1 \cup \{\!\!\{P\}\!\!\} \cup \mathcal{F}(\phi\{\mathsf{ax}_{n+1} \mapsto t\}, \mathcal{N}'_{ch})}$$

Then when we analyse the support of E_1, we consider the following processes:

- $A_f^{j,k}(\mathcal{Q}', \phi') = \{\!\!\{\mathsf{in}(c_{\mathsf{ax}_j}, x_j).\ldots.\mathsf{in}(c_{\mathsf{ax}_n}, x_n).\mathsf{out}(\xi\rho\sigma_j, x_{n+1}).(Frame\sigma_{j-1} +_{0.5} \mathsf{out}(ok, ok))\}\!\!\} \cup \mathcal{Q}' \cup \{\!\!\{\mathsf{out}(c_{\mathsf{ax}_i}, \mathsf{ax}_i\phi').0\}\!\!\}_{i=j+1}^{n} \cup \{\!\!\{0\}\!\!\}_{i=1}^{k}$
- $A_{in}^{k}(\mathcal{Q}', \phi') = \{\!\!\{\mathsf{in}(\xi\rho, x_{n+1}).(Frame\sigma_n +_{0.5} \mathsf{out}(ok, ok).0)\}\!\!\} \cup \mathcal{Q}' \cup \{\!\!\{0\}\!\!\}_{i=1}^{k}$
- $A_{+}^{k}(\mathcal{Q}', \phi') = \{\!\!\{Frame\sigma_{n+1} +_{0.5} \mathsf{out}(ok, ok).0\}\!\!\} \cup \mathcal{Q}' \cup \{\!\!\{0\}\!\!\}_{i=1}^{k}$
- $A_{ch'}^{j,k}(\mathcal{Q}', \phi') = \{\!\!\{\mathsf{out}(c'_{\mathsf{ax}_j}, \mathsf{ax}_j\phi').0\}\!\!\}_{i=1}^{j} \cup \{\!\!\{\mathsf{out}(c'_{\mathsf{ax}_{j+1}}, \mathsf{ax}_{j+1}\phi').0 \mid \ldots \mid \mathsf{out}(c'_{\mathsf{ax}_{n+1}}, \mathsf{ax}_n\phi').0\}\!\!\} \cup \mathcal{Q}' \cup \{\!\!\{0\}\!\!\}_{i=1}^{n}$
- $A_{ok}^{k}(\mathcal{Q}', \phi') = \{\!\!\{\mathsf{out}(ok, ok).0\}\!\!\} \cup \mathcal{Q}' \cup \{\!\!\{0\}\!\!\}_{i=1}^{k}$

where $\sigma_j = \{^{\mathsf{ax}_i\phi'}/_{x_i}\}_{i=1}^{j}$. Notice here that a frame is given as argument since it will be augment once the process $\mathsf{in}(\xi\rho, x_{n+1})$ is executed. As such, the set $\mathcal{A}_f^{j,k}$ is defined as $\{A_f^{i,k}(\mathcal{Q}', \phi') \mid (\mathcal{Q}', \phi') \in \mathcal{SP}_\ell(\phi', \mathcal{N}_{ch}) \wedge fn(\mathcal{Q}) \cap \mathcal{N}'_{ch} = \varnothing\}$. Similarly, the correspondence function $\mathsf{corr} : \mathcal{SP} \mapsto \mathcal{SP}_\ell$ is defined as for all $(\mathcal{Q}', \phi') \in \mathcal{SP}_\ell(\phi', \mathcal{N}_{ch})$ with $fn(\mathcal{Q}) \cap \mathcal{N}'_{ch} = \varnothing$, $\mathsf{corr}(A_f^{j,k}(\mathcal{Q}', \phi')) = \mathsf{corr}(A_{out}^{k}(\mathcal{Q}', \phi')) = \mathsf{corr}(A_{+}^{k}(\mathcal{Q}', \phi')) = \mathsf{corr}(A_{ch'}^{j,k}(\mathcal{Q}', \phi')) = \mathsf{corr}(A_{ok}^{k}(\mathcal{Q}', \phi')) = (\mathcal{Q}', \phi')$. The measure function m only differ on $\mathcal{A}_{ch'}^{j,k}$ as follows: if $\mathcal{Q} \in \mathcal{A}_{ch'}^{j,k}$ then $\mathsf{m}(\mathcal{Q}) = (2, n+1-j, k)$. The rest of the proof follows by using the same reasoning. . □

F.4 Simulation implies observational preorder

For this direction of the equivalence, we define the relation R_{op} with $op \in \{\leq, \approx\}$ on multisets of processes as follows: For all $\mathcal{P}, \mathcal{P}' \in \mathcal{SP}$, $\mathcal{P}\ R_{op}\ \mathcal{P}'$ if and only if there exist a multiset of processes $\mathcal{P}_{Att}$, a renaming of variables ρ, two extended processes $(\mathcal{Q}, \phi), (\mathcal{Q}', \phi') \in \mathcal{SP}_\ell$ such that:

- $|\phi| = |\phi'| = n$
- $dom(\rho) \subseteq \mathcal{N}_{pub}$, $img(\rho) \subseteq \mathcal{N}_{priv}$, $img(\rho) \cap names(\mathcal{Q}, \mathcal{Q}', \phi, \phi') = \varnothing$
- $fv(\mathcal{P}_{Att}) \subseteq \{x_1, \ldots, x_n\}$ and $fn(\mathcal{P}_{Att}) \subseteq \mathcal{N}_{pub}$
- $\mathcal{P} = \mathcal{Q}\rho \cup \mathcal{P}_{Att}\{^{\mathsf{ax}_i\phi}/_{x_i}\}_{i=1}^{n}\rho$
- $\mathcal{P}' = \mathcal{Q}'\rho \cup \mathcal{P}_{Att}\{^{\mathsf{ax}_i\phi'}/_{x_i}\}_{i=1}^{n}\rho$
- $(\mathcal{Q}, \phi)\ op^{\mathsf{N}^\ell}\ (\mathcal{Q}', \phi')$

Lemma 62. For all $op \in \{\leq, \approx\}$, for all $\mathcal{P}, \mathcal{P}' \in \mathcal{SP}$, if $\mathcal{P}\ R_{op}\ \mathcal{P}'$ then for all closed $\mathcal{P}_{Att} \in \mathcal{SP}$ such that $fn(\mathcal{P}_{Att}) \subseteq \mathcal{N}_{pub}$ then $\mathcal{P}_{Att} \cup \mathcal{P}\ R_{op}\ \mathcal{P}_{Att} \cup \mathcal{P}'$.

Proof. Trivial by definition of R_{op}. $\square$

Lemma 63. Let $op \in \{\leq, \approx\}$. Let $D, D' \in \mathcal{D}^{\leq 1}(\mathcal{S}_{\mathsf{N}^\ell})$. Let $n \in \mathbb{N}$. Let ρ be a renaming such that $dom(\rho) \subseteq \mathcal{N}_{pub}$, $img(\rho) \subseteq \mathcal{N}_{priv}$ and for all $(\mathcal{P}, \phi) \in \text{supp}(D) \cup \text{supp}(D')$, $img(\rho) \cap names(\mathcal{P}, \phi) = \varnothing$ and $|\phi| = n$. Let $\mathcal{P}_{Att} \in \mathcal{SP}$ such that $fv(\mathcal{P}_{Att}) \subseteq \{x_1, \ldots, x_n\}$ and $fn(\mathcal{P}_{Att}) \subseteq \mathcal{N}_{pub}$.

If $D \ \widehat{op^{\mathsf{N}^\ell}} \ D'$ then

$$\sum_{(\mathcal{Q},\phi)\in\text{supp}(D)} D((\mathcal{Q},\phi)) \cdot \delta_{\mathcal{Q}\rho\cup\mathcal{P}_{Att}\{^{\mathsf{ax}_i\phi}/_{x_i}\}_{i=1}^n\rho} \ \widehat{R_{op}} \sum_{(\mathcal{Q},\phi)\in\text{supp}(D')} D'((\mathcal{Q},\phi)) \cdot \delta_{\mathcal{Q}\rho\cup\mathcal{P}_{Att}\{^{\mathsf{ax}_i\phi}/_{x_i}\}_{i=1}^n\rho}$$

Proof. Given a frame ϕ of size n, we denote by σ_ϕ the substitution $\{^{\mathsf{ax}_1\phi}/_{x_i}\}_{i=1}^n$. We denote by E and E' the sub-distributions $\sum_{(\mathcal{Q},\phi)\in\text{supp}(D)} D((\mathcal{Q},\phi)) \cdot \delta_{\mathcal{Q}\rho\cup\mathcal{P}_{Att}\sigma_\phi\rho}$ and $\sum_{(\mathcal{Q},\phi)\in\text{supp}(D')} D'((\mathcal{Q},\phi)) \cdot \delta_{\mathcal{Q}\rho\cup\mathcal{P}_{Att}\sigma_\phi\rho}$ respectively. Let $S \subseteq \mathcal{SP}$. Let us denote $S_1 = \{(\mathcal{Q},\phi) \in \text{supp}(D) \mid (\mathcal{Q}\rho \cup \mathcal{P}_{Att}\sigma_\phi\rho) \in S\}$.

Let $S' = \{(\mathcal{Q}',\phi') \in \text{supp}(D') \mid (\mathcal{Q}\rho\cup\mathcal{P}_{Att}\sigma_\phi\rho) \in S \cap \text{supp}(D) \text{ and } (\mathcal{Q},\phi) \ op^{\mathsf{N}^\ell} \ (\mathcal{Q}',\phi')\}$. By definition of E, we have:

$$\begin{aligned}
E(S) &= \sum_{\substack{(\mathcal{Q},\phi)\in\text{supp}(D)\\ |\mathcal{Q}\rho\cup\mathcal{P}_{Att}\sigma_\phi\rho\in S}} D((\mathcal{Q},\phi)) \\
&= D(S_1) && \text{by definition of } S_1 \\
&\leq D'(op^{\mathsf{N}^\ell}\ (S_1)) && \text{by } D \ \widehat{op^{\mathsf{N}^\ell}} \ D' \\
&\leq \sum_{\substack{(\mathcal{Q}',\phi')\in\text{supp}(D')\\ |(\mathcal{Q},\phi)\in S_1\wedge(\mathcal{Q},\phi)op^{\mathsf{N}^\ell}(\mathcal{Q}',\phi')}} D'((\mathcal{Q}',\phi')) \\
&\leq \sum_{\substack{(\mathcal{Q}',\phi')\in\text{supp}(D')\\ |(\mathcal{Q}\rho\cup\mathcal{P}_{Att}\sigma_\phi\rho)\in S\\ \wedge(\mathcal{Q}\rho\cup\mathcal{P}_{Att}\sigma_\phi\rho)R_{op}(\mathcal{Q}'\rho\cup\mathcal{P}_{Att}\sigma_{\phi'}\rho)}} D'((\mathcal{Q}',\phi')) && \text{by definition of } R_{op} \\
&\leq E'(R_{op}\ (S))
\end{aligned}$$

This allows us to conclude that $E \ \widehat{R_{op}} \ E'$. $\square$

Lemma 64. For all $op \in \{\leq, \approx\}$, for all $\mathcal{P}, \mathcal{P}' \in \mathcal{SP}$, if $\mathcal{P} \ R_{op} \ \mathcal{P}'$ and $\mathcal{P} \xrightarrow{\tau}_{\mathsf{N}^o} D$ then $\mathcal{P} \Longrightarrow^{\tau}_{\mathsf{r},\mathsf{N}^o} D'$ and $D \ \widehat{R_{op}} \ D'$ (and $D' \ \widehat{R_{op}} \ D$ when $op = \approx$).

Proof. By definition of $\mathcal{P} \ R_{op} \ \mathcal{P}'$, we know that there exist $(\mathcal{Q},\phi), (\mathcal{Q}',\phi') \in \mathcal{SP}_\ell$, $\mathcal{P}_{Att} \in \mathcal{SP}$, a renaming of variables ρ and two substitutions σ, σ' such that $(\mathcal{Q},\phi) \ op^{\mathsf{N}^\ell} \ (\mathcal{Q}',\phi')$, $\mathcal{P} = \mathcal{Q}\rho\cup\mathcal{P}_{Att}\sigma\rho$, $\mathcal{P}' = \mathcal{Q}'\rho\cup\mathcal{P}_{att}\sigma'\rho$, $|\phi| = |\phi'|$, $fv(\mathcal{P}_{Att}) \subseteq \{x_1, \ldots, x_n\}$, $\sigma = \{^{\mathsf{ax}_i\phi}/_{x_i}\}_{i=1}^n\rho$, $\sigma' = \{^{\mathsf{ax}_i\phi'}/_{x_i}\}_{i=1}^n\rho$, $dom(\rho) \subseteq \mathcal{N}_{pub}$, $img(\rho) \subseteq \mathcal{N}_{priv}$ and $img(\rho) \cap names(\mathcal{Q},\mathcal{Q}') = \varnothing$

Let us do a case analysis on the rule applied in $\mathcal{P} \xrightarrow{\tau}_{\mathsf{N}^o} D$.

Case of a rule solely applied on $\mathcal{Q}\rho$: In such a case, $\mathcal{Q}\rho \xrightarrow{\tau}_{\mathsf{N}^o} D_1$ such that $D = \sum_{\mathcal{Q}'' \in \mathcal{SP}} D_1(\mathcal{Q}'') \cdot \delta_{\mathcal{Q}'' \cup \mathcal{P}_{Att}\sigma}$. Notice that $\mathcal{Q}\rho \xrightarrow{\tau}_{\mathsf{N}^o} D_1$ implies that $(\mathcal{Q}, \phi) \xrightarrow{\tau}_{\mathsf{N}^\ell} \sum_{\mathcal{Q}'' \in \mathcal{SP}} D_1(\mathcal{Q}''\rho) \cdot \delta_{(\mathcal{Q}'', \phi)} = D_2$ and for all $(\mathcal{Q}'', \phi) \in \mathrm{supp}(D_2)$, $img(\rho) \cap names(\mathcal{Q}'') = \varnothing$. By hypothesis, $(\mathcal{Q}, \phi)\ op^{\mathsf{N}^\ell}\ (\mathcal{Q}', \phi')$. Hence there exists $(\mathcal{Q}', \phi') \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^\ell} D_2'$ and $D_2\ \widehat{op^{\mathsf{N}^\ell}}\ D_2'$ (and $D_2'\ \widehat{op^{\mathsf{N}^\ell}}\ D_2$ when $op = \approx$). By the semantics of $\xrightarrow{\tau}_{\mathsf{N}^\ell}$ in Figure 10 and by Lemma 45, we obtain that for all $(\mathcal{Q}'', \phi'') \in \mathrm{supp}(D_2')$, $\phi' = \phi''$ and we can assume w.l.o.g. that $img(\rho) \cap names(\mathcal{Q}'') = \varnothing$ (i.e. when the rule (New) generates a new private names, we can always pick one that is not in $img(\rho)$).

Hence, we also deduce that $\mathcal{Q}'\rho \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} \sum_{(\mathcal{Q}'', \phi') \in \mathrm{supp}(D_2')} D_2'(\mathcal{Q}'', \phi') \cdot \delta_{\mathcal{Q}''\rho}$. Therefore $\mathcal{Q}'\rho \cup \mathcal{P}_{Att}\sigma' \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} \sum_{(\mathcal{Q}'', \phi') \in \mathrm{supp}(D_2')} D_2'(\mathcal{Q}'', \phi') \cdot \delta_{\mathcal{Q}''\rho \cup \mathcal{P}_{Att}\sigma'}$. Let us denote $D' = \sum_{(\mathcal{Q}'', \phi') \in \mathrm{supp}(D_2')} D_2'(\mathcal{Q}'', \phi') \cdot \delta_{\mathcal{Q}''\rho \cup \mathcal{P}_{Att}\sigma'}$. We conclude by applying Lemma 63 that $D\ \widehat{R_{op}}\ D'$ (and $D'\ \widehat{R_{op}}\ D$ when $op = \approx$).

Case of a rule solely applied on $\mathcal{P}_{Att}\sigma$: In such a case $\mathcal{P}_{Att}\sigma \xrightarrow{\tau}_{\mathsf{N}^o} D_1$ such that $D = \sum_{\mathcal{P}'_{Att} \in \mathcal{SP}} D_1(\mathcal{P}'_{Att}) \cdot \delta_{\mathcal{Q}'\rho \cup \mathcal{P}'_{Att}}$. We first show that there exists a renaming ρ' with $dom(\rho') \subseteq \mathcal{N}_{pub}$, $img(\rho') \subseteq \mathcal{N}_{priv}$ and $img(\rho') \cap names(\mathcal{Q}, \mathcal{Q}') = \varnothing$ such that :

- for all $\mathcal{P}'_{Att} \in \mathrm{supp}(D_1)$, there exists a multiset of process $\overline{\mathcal{P}'_{Att}}$ such that $\mathcal{P}'_{Att} = \overline{\mathcal{P}'_{Att}}\{^{\mathsf{ax}_i\phi}/_{x_i}\}_{i=1}^n\rho'$, $fn(\mathcal{P}''_{Att}) \subseteq \mathcal{N}_{pub}$ and $fv(\mathcal{P}''_{Att}) \subseteq \{x_1, \ldots, x_n\}$
- $\mathcal{P}_{Att}\sigma' \xrightarrow{\tau}_{\mathsf{N}^o} \sum_{\mathcal{P}'_{Att} \in \mathrm{supp}(D_1)} D_1(\mathcal{P}'_{Att}) \cdot \delta_{\overline{\mathcal{P}'_{Att}}\{^{\mathsf{ax}_i\phi'}/_{x_i}\}_{i=1}^n\rho'}$

We do a case analysis on the rule applied in $\mathcal{P}_{Att}\sigma \xrightarrow{\tau}_{\mathsf{N}^o} D_1$. The cases of the rules (Null), (Par), (Repl), (Choice-1), (Choice-2) and (PChoice) are trivial by taking $\rho' = \rho$. Note that in all these cases but (PChoice), D_1 is in fact a dirac.

Let us now look at the rule (Comm): In such a case, $\mathcal{P}_{Att} = \{\!\!\{\mathsf{out}(u, t).P, \mathsf{in}(v, x).Q\}\!\!\} \cup \mathcal{P}_{Att,1}$, $\mathcal{P}'_{Att} = \{\!\!\{P\sigma, Q\sigma\{^{t\sigma}/_x\}\}\!\!\} \cup \mathcal{P}'_{Att}\sigma$, $D_1 = \delta_{\mathcal{P}'_{Att}}$, $Msg(t\sigma)$ and $u\sigma \doteq v\sigma$. Note that $t\sigma = t\phi\rho$, $u\sigma = u\phi\rho$ and $v\sigma = v\phi\rho$. Since both $\doteq$ and $Msg(\cdot)$ are closed under renaming, we deduce that $u\phi \doteq v\phi$ and $Msg(t\phi)$. Furthermore, $fn(t, u, v) \subseteq \mathcal{N}_{pub}$ meaning that t, u, v are recipes. Since we know by hypothesis that $(\mathcal{Q}, \phi)\ op^{\mathsf{N}^\ell}\ (\mathcal{Q}', \phi')$, we deduce that $u\phi \doteq v\phi$ implies $u\phi' \doteq v\phi'$, and $Msg(t\phi)$ implies $Msg(t\phi')$. Once again, by the closure under renaming argument, we obtain that $u\phi'\rho \doteq v\phi'\rho$ and $Msg(t\phi'\rho)$. This allows us to deduce that $\mathcal{P}_{Att}\sigma' \xrightarrow{\tau}_{\mathsf{N}^o} \delta_{\{\!\!\{P\sigma', Q\sigma'\{^{t\sigma'}/_x\}\}\!\!\} \cup \mathcal{P}'_{Att}\sigma'}$, and so we conclude by taking $\rho' = \rho$ and $\overline{\mathcal{P}'_{Att}} = \{\!\!\{P, Q\{^t/_x\}\}\!\!\} \cup \mathcal{P}_{Att,1}$.

The cases of the rules (Then) and (Else) are done similarly since the condition to apply the rule only depend on the success or not of an equality $\doteq$.

Finally, let us consider the rule (New): In such a case, $\mathcal{P}_{Att} = \{\!\!\{\mathsf{new}\ a.P\}\!\!\} \cup \mathcal{P}_{Att,1}$, $\mathcal{P}'_{Att} = \{\!\!\{P\sigma\{^{a'}/_a\}\}\!\!\} \cup \mathcal{P}_{Att,1}\sigma$ and $D_1 = \delta_{\mathcal{P}'_{Att}}$ where a' is fresh. W.l.o.g., we can take a' such that $a' \notin names(\mathcal{Q}, \mathcal{Q}', \phi, \phi')$. We take a new fresh name $a_{pub} \in \mathcal{N}_{pub}$ and we conclude by defining $\rho' = \rho\{a_{pub} \mapsto a'\}$ and $\overline{\mathcal{P}'_{Att}} = \{\!\!\{P\{^{a_{pub}}/_a\}\}\!\!\} \cup \mathcal{P}_{Att,1}$.

We have therefore proved that:

- $\mathcal{P}_{Att}\sigma \xrightarrow{\tau}_{\mathsf{N}^o} \sum_{\mathcal{P}'_{Att} \in \mathrm{supp}(D_1)} D_1(\mathcal{P}'_{Att}) \cdot \delta_{\overline{\mathcal{P}'_{Att}}\{^{\mathsf{ax}_i\phi}/_{x_i}\}_{i=1}^n\rho'}$

- $\mathcal{P}_{Att}\sigma' \xrightarrow{\tau}_{\mathsf{N}^o} \sum_{\mathcal{P}'_{Att}\in \mathrm{supp}(D_1)} D_1(\mathcal{P}'_{Att}) \cdot \delta_{\overline{\mathcal{P}'_{Att}}\{^{\mathsf{ax}_i\phi'}/_{x_i}\}_{i=1}^n\rho'}$

Since $\mathcal{Q}\rho = \mathcal{Q}\rho'$ and $\mathcal{Q}'\rho = \mathcal{Q}'\rho'$, we obtain:

- $\mathcal{P}_{Att}\sigma \cup \mathcal{Q}\rho \xrightarrow{\tau}_{\mathsf{N}^o} \sum_{\mathcal{P}'_{Att}\in \mathrm{supp}(D_1)} D_1(\mathcal{P}'_{Att}) \cdot \delta_{\mathcal{Q}\rho'\cup\overline{\mathcal{P}'_{Att}}\{^{\mathsf{ax}_i\phi}/_{x_i}\}_{i=1}^n\rho'} = D$
- $\mathcal{P}_{Att}\sigma' \cup \mathcal{Q}'\rho \xrightarrow{\tau}_{\mathsf{N}^o} \sum_{\mathcal{P}'_{Att}\in \mathrm{supp}(D_1)} D_1(\mathcal{P}'_{Att}) \cdot \delta_{\mathcal{Q}'\rho'\cup\overline{\mathcal{P}'_{Att}}\{^{\mathsf{ax}_i\phi'}/_{x_i}\}_{i=1}^n\rho'}$

Note that for all $\mathcal{P}'_{Att} \in \mathrm{supp}(D_1)$, by $(\mathcal{Q},\phi)\ op^{\mathsf{N}^\ell}\ (\mathcal{Q}',\phi')$ and by construction of ρ' and $\overline{\mathcal{P}'_{Att}}$, we have that:

$$\mathcal{Q}\rho' \cup \overline{\mathcal{P}'_{Att}}\{^{\mathsf{ax}_i\phi}/_{x_i}\}_{i=1}^n\rho'\ R_{op}\ \mathcal{Q}'\rho' \cup \overline{\mathcal{P}'_{Att}}\{^{\mathsf{ax}_i\phi'}/_{x_i}\}_{i=1}^n\rho'$$

Note that when $op = \approx$, $(\mathcal{Q},\phi)\ op^{\mathsf{N}^\ell}\ (\mathcal{Q}',\phi')$ implies $(\mathcal{Q}',\phi')\ op^{\mathsf{N}^\ell}\ (\mathcal{Q},\phi)$ and so we also have:

$$\mathcal{Q}'\rho' \cup \overline{\mathcal{P}'_{Att}}\{^{\mathsf{ax}_i\phi'}/_{x_i}\}_{i=1}^n\rho'\ R_{\approx}\ \mathcal{Q}\rho' \cup \overline{\mathcal{P}'_{Att}}\{^{\mathsf{ax}_i\phi}/_{x_i}\}_{i=1}^n\rho'$$

By denoting $D' = \sum_{\mathcal{P}'_{Att}\in \mathrm{supp}(D_1)} D_1(\mathcal{P}'_{Att})\cdot\delta_{\mathcal{Q}'\rho'\cup\overline{\mathcal{P}'_{Att}}\{^{\mathsf{ax}_i\phi'}/_{x_i}\}_{i=1}^n\rho'}$, we conclude that $D\ \widehat{R_{op}}\ D'$ and $\mathcal{P}_{Att}\sigma' \cup \mathcal{Q}'\rho \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}^o} D'$ (and $D'\ \widehat{R_{op}}\ D$ when $op = \approx$)

*Case of rule (*Comm*) between an output on $\mathcal{Q}\rho$ and an input on $\mathcal{P}_{Att}\sigma$:* In such a case $\mathcal{Q} = \{\!\{\mathsf{out}(u,t).P\}\!\} \cup \mathcal{Q}_1$, $\mathcal{P}_{Att} = \{\!\{\mathsf{in}(v,x).Q\}\!\} \cup \mathcal{P}_{Att,1}$, $D = \delta_{\{\!\{P\rho, Q\sigma\{^{t\rho}/_x\}\}\!\}\cup\mathcal{P}_{Att,1}\sigma\cup\mathcal{Q}_1\rho}$, $Msg(t\rho)$ and $v\sigma \doteq u\rho$. Note that $fn(v) \subseteq \mathcal{N}_{pub}$ and $fv(v) \subseteq \{x_1,\ldots,x_n\}$. If we denote $\rho_{\mathcal{AX}} = \{x_i \mapsto \mathsf{ax}_i\}_{i=1}^n$, we obtain that $v\rho_{\mathcal{AX}}$ is a recipe with $fv(v\rho_{\mathcal{AX}}) \subseteq dom(\phi)$. Note that since $Msg(\cdot)$ and $\doteq$ are closed by renaming, we deduce from $Msg(t\rho)$ and $v\sigma \doteq u\rho$ that $Msg(t)$ and $v\rho_{\mathcal{AX}}\phi \doteq u$. Thus, $(\mathcal{Q},\phi) \xrightarrow{out(v\rho_{\mathcal{AX}},\mathsf{ax}_{n+1})}_{\mathsf{N}^\ell} \delta_{(\{\!\{P\}\!\}\cup\mathcal{Q}_1,\phi\{\mathsf{ax}_{n+1}\mapsto t\})} = D_1$.

Let x_{n+1} be a fresh variable. If we define $\phi_1 = \phi\{\mathsf{ax}_{n+1} \mapsto t\}$, $\mathcal{P}_{Att,2} = \{\!\{Q\{^{x_{n+1}}/_x\}\}\!\} \cup \mathcal{P}_{Att,1}$ and $\sigma_1 = \{^{\mathsf{ax}_i\phi_1}/_{x_i}\}_{i=1}^{n+1}\rho$ then we obtain that $D = \delta_{(\{\!\{P\}\!\}\cup\mathcal{Q}_1)\rho\cup\mathcal{P}_{Att,2}\sigma_1}$. Notice that $fv(\mathcal{P}_{Att,2}) \subseteq \{x_1,\ldots,x_{n+1}\}$ and $fn(\mathcal{P}_{Att,2}) \subseteq \mathcal{N}_{pub}$.

By hypothesis, we have $(\mathcal{Q},\phi)\ op^{\mathsf{N}^\ell}\ (\mathcal{Q}',\phi')$. Thus, there exists D'_1 such that $(\mathcal{Q}',\phi') \xrightarrow{\xrightarrow{out(v\rho_{\mathcal{AX}},\mathsf{ax}_{n+1})}}_{\mathsf{r},\mathsf{N}^\ell} D'_1$ and $D_1\ \widehat{op^{\mathsf{N}^\ell}}\ D'_1$ (and $D'_1\ \widehat{op^{\mathsf{N}^\ell}}\ D_1$ when $op = \approx$). By definition, there exists E and F such that $(\mathcal{Q}',\phi') \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}^\ell} E$, $E \xrightarrow{out(v\rho_{\mathcal{AX}},\mathsf{ax}_{n+1})}_{\mathsf{N}^\ell} F$ and $F \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}^\ell} D'_1$.

By the semantics of $\xrightarrow{\tau}_{\mathsf{N}^\ell}$ in Figure 10 and by Lemma 45, we obtain that for all $(\mathcal{Q}'',\phi'') \in \mathrm{supp}(E)$, $\phi' = \phi''$ and we can assume w.l.o.g. that $img(\rho)\cap names(\mathcal{Q}'') = \varnothing$ (i.e. when the rule (New) generates a new private name, we can always pick one that is not in $img(\rho)$). Hence, we also deduce that $\mathcal{Q}'\rho \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}^o} \sum_{(\mathcal{Q}'',\phi')\in\mathrm{supp}(E)} E((\mathcal{Q}'',\phi'))\cdot\delta_{\mathcal{Q}''\rho}$. Therefore $\mathcal{Q}'\rho \cup \mathcal{P}_{Att}\sigma' \overset{\tau}{\Longrightarrow}_{\mathsf{r},\mathsf{N}^o} \sum_{(\mathcal{Q}'',\phi')\in\mathrm{supp}(E)} E(\mathcal{Q}'',\phi')\cdot\delta_{\mathcal{Q}''\rho\cup\mathcal{P}_{Att}\sigma'}$.

Note that $D_1\ \widehat{op^{\mathsf{N}^\ell}}\ D'_1$ and D_1 being a distribution imply that E, F and D'_1 are also distributions. Thus for all $(\mathcal{Q}'',\phi') \in \mathrm{supp}(E)$, there exist $u', t', P', \mathcal{Q}'''$ such that $\mathcal{Q}'' = \{\!\{\mathsf{out}(u',t').P'\}\!\} \cup \mathcal{Q}'''$ such that $u' \doteq v\rho_{\mathcal{AX}}\phi'$, $Msg(t')$ and $(\mathcal{Q}'',\phi') \xrightarrow{out(v\rho_{\mathcal{AX}},\mathsf{ax}_{n+1})}_{\mathsf{N}^\ell} \delta_{(\{\!\{P'\}\!\}\cup\mathcal{Q}''',\phi'\{\mathsf{ax}_{n+1}\mapsto t'\})}$ with $(\{\!\{P'\}\!\}\cup\mathcal{Q}''',\phi'\{\mathsf{ax}_{n+1}\mapsto t'\}) \in \mathrm{supp}(F)$. Since $u' \doteq v\rho_{\mathcal{AX}}\phi'$ and $Msg(t')$ imply $u'\rho \doteq v\sigma'$ and $Msg(t'\rho)$, we deduce that $\mathcal{Q}''\rho\cup\{\!\{\mathsf{in}(v\sigma',x).Q\sigma'\}\!\}\cup\mathcal{P}_{Att,1}\sigma' \xrightarrow{\tau}_{\mathsf{N}^o}$

$\delta_{\{\!\{P'\rho, Q\sigma'\{^{t'\rho}/_{x'}\}\}\!\}\cup\mathcal{Q}'''\rho\cup\mathcal{P}_{Att,1}\sigma'}$. If we denote $\phi'_1 = \phi'\{\mathsf{ax}_{n+1} \mapsto t'\}$ and $\sigma'_1 = \{^{\mathsf{ax}_i\phi'_1}/_{x_i}\}_{i=1}^{n+1}\rho$ then we obtain $\mathcal{Q}''\rho \cup \{\!\{\mathsf{in}(v\sigma', x).Q\sigma'\}\!\} \cup \mathcal{P}_{Att,1}\sigma' \xrightarrow{\tau}_{\mathsf{N}^o} \delta_{(\{\!\{P'\}\!\}\cup\mathcal{Q}''')\rho\cup\mathcal{P}_{Att,2}\sigma'_1}$.

We have therefore proved that:

$$\sum_{(\mathcal{Q}'',\phi')\in\mathrm{supp}(E)} E((\mathcal{Q}'',\phi'))\cdot\delta_{\mathcal{Q}''\rho\cup\mathcal{P}_{Att}\sigma'} \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} \sum_{(\mathcal{Q}'',\phi'')\in\mathrm{supp}(F)} F((\mathcal{Q}'',\phi''))\cdot\delta_{\mathcal{Q}''\rho\cup\mathcal{P}_{Att,2}\{^{\mathsf{ax}_i\phi''}/_{x_i}\}_{i=1}^{n+1}\rho}$$

Note that $F \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^\ell} D'_1$. Once again by the semantics of $\xrightarrow{\tau}_{\mathsf{N}^\ell}$ in Figure 10 and by Lemma 45, we can easily show that:

$$\sum_{(\mathcal{Q}'',\phi'')\in\mathrm{supp}(F)} F((\mathcal{Q}'',\phi'))\cdot\delta_{\mathcal{Q}''\rho\cup\mathcal{P}_{Att,2}\{^{\mathsf{ax}_i\phi''}/_{x_i}\}_{i=1}^{n+1}\rho} \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} \sum_{(\mathcal{Q}'',\phi'')\in\mathrm{supp}(D'_1)} D'_1((\mathcal{Q}'',\phi''))\cdot\delta_{\mathcal{Q}''\rho\cup\mathcal{P}_{Att,2}\{^{\mathsf{ax}_i\phi''}/_{x_i}\}_{i=1}^{n+1}\rho}$$

Let us denote $D' = \sum_{(\mathcal{Q}'',\phi'')\in\mathrm{supp}(D'_1)} D'_1((\mathcal{Q}'',\phi''))\cdot\delta_{\mathcal{Q}''\rho\cup\mathcal{P}_{Att,2}\{^{\mathsf{ax}_i\phi''}/_{x_i}\}_{i=1}^{n+1}\rho}$. We conclude by applying Lemma 63 that $D\ \widehat{R_{op}}\ D'$ (and $D'\ \widehat{R_{op}}\ D$ when $op = \approx$).

*Case of rule (*Comm*) between an input on $\mathcal{Q}\rho$ and an output on $\mathcal{P}_{Att}\sigma$:* In such a case $\mathcal{Q} = \{\!\{\mathsf{in}(v,x).Q\}\!\} \cup \mathcal{Q}_1$, $\mathcal{P}_{Att} = \{\!\{\mathsf{out}(u,t).P\}\!\} \cup \mathcal{P}_{Att,1}$, $D = \delta_{\{\!\{P\sigma, Q\rho\{^{t\sigma}/_x\}\}\!\}\cup\mathcal{P}_{Att,1}\sigma\cup\mathcal{Q}_1\rho}$, $Msg(t\sigma)$ and $v\rho \doteq u\sigma$. Note that $fn(u,t) \subseteq \mathcal{N}_{pub}$ and $fv(u,t) \subseteq \{x_1,\ldots,x_n\}$. If we denote $\rho_{\mathcal{AX}} = \{x_i \mapsto \mathsf{ax}_i\}_{i=1}^n$, we obtain that $u\rho_{\mathcal{AX}}$ and $t\rho_{\mathcal{AX}}$ are recipes with $fv(u\rho_{\mathcal{AX}}, t\rho_{\mathcal{AX}}) \subseteq dom(\phi)$. Note that since $Msg(\cdot)$ and $\doteq$ are closed by renaming, we deduce from $Msg(t\sigma)$ and $v\rho \doteq u\sigma$ that $Msg(t\rho_{\mathcal{AX}}\phi)$ and $v \doteq u\rho_{\mathcal{AX}}\phi$. Thus, $(\mathcal{Q},\phi) \xrightarrow{in(u\rho_{\mathcal{AX}}, t\rho_{\mathcal{AX}})}_{\mathsf{N}^\ell} \delta_{(\{\!\{Q\{^{t\rho_{\mathcal{AX}}\phi}/_x\}\}\!\}\cup\mathcal{Q}_1,\phi)} = D_1$.

If we define $\mathcal{P}_{Att,2} = \{\!\{P\}\!\} \cup \mathcal{P}_{Att,1}$ then we obtain that $D = \delta_{(\{\!\{Q\{^{t\rho_{\mathcal{AX}}\phi}/_x\}\}\!\}\cup\mathcal{Q}_1)\rho\cup\mathcal{P}_{Att,2}\sigma}$. Notice that $fv(\mathcal{P}_{Att,2}) \subseteq \{x_1,\ldots,x_n\}$ and $fn(\mathcal{P}_{Att,2}) \subseteq \mathcal{N}_{pub}$.

By hypothesis, we have $(\mathcal{Q},\phi)\ op^{\mathsf{N}^\ell}\ (\mathcal{Q}',\phi')$. Thus, there exists D'_1 such that $(\mathcal{Q}',\phi') \xRightarrow{in(u\rho_{\mathcal{AX}}, t\rho_{\mathcal{AX}})}_{\mathsf{r},\mathsf{N}^\ell} D'_1$ and $D_1\ \widehat{op^{\mathsf{N}^\ell}}\ D'_1$ (and $D'_1\ \widehat{op^{\mathsf{N}^\ell}}\ D_1$ when $op = \approx$). By definition, there exists E and F such that $(\mathcal{Q}',\phi') \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^\ell} E$, $E \xrightarrow{in(u\rho_{\mathcal{AX}}, t\rho_{\mathcal{AX}})}_{\mathsf{N}^\ell} F$ and $F \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^\ell} D'_1$.

By the semantics of $\xrightarrow{\tau}_{\mathsf{N}^\ell}$ in Figure 10 and by Lemma 45, we obtain that for all $(\mathcal{Q}'',\phi'') \in \mathrm{supp}(E)$, $\phi' = \phi''$ and we can assume w.l.o.g. that $img(\rho) \cap names(\mathcal{Q}'') = \varnothing$ (i.e. when the rule (New) generates a new private name, we can always pick one that is not in $img(\rho)$). Hence, we also deduce that $\mathcal{Q}'\rho \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} \sum_{(\mathcal{Q}'',\phi')\in\mathrm{supp}(E)} E((\mathcal{Q}'',\phi'))\cdot\delta_{\mathcal{Q}''\rho}$. Therefore $\mathcal{Q}'\rho \cup \mathcal{P}_{Att}\sigma' \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} \sum_{(\mathcal{Q}'',\phi')\in\mathrm{supp}(E)} E(\mathcal{Q}'',\phi')\cdot\delta_{\mathcal{Q}''\rho\cup\mathcal{P}_{Att}\sigma'}$.

Note that $D_1\ \widehat{op^{\mathsf{N}^\ell}}\ D'_1$ and D_1 being a distribution imply that E, F and D'_1 are also distributions. Thus for all $(\mathcal{Q}'',\phi') \in \mathrm{supp}(E)$, there exist $v', x', Q', \mathcal{Q}'''$ such that $\mathcal{Q}'' = \{\!\{\mathsf{in}(v',x').Q'\}\!\} \cup \mathcal{Q}'''$ such that $v' \doteq u\rho_{\mathcal{AX}}\phi'$, $Msg(t\rho_{\mathcal{AX}}\phi')$ and $(\mathcal{Q}'',\phi') \xrightarrow{in(u\rho_{\mathcal{AX}}, t\rho_{\mathcal{AX}})}_{\mathsf{N}^\ell} \delta_{(\{\!\{Q'\{^{t\rho_{\mathcal{AX}}\phi'}/_{x'}\}\}\!\}\cup\mathcal{Q}''',\phi')}$ with $(\{\!\{Q'\{^{t\rho_{\mathcal{AX}}\phi'}/_{x'}\}\}\!\} \cup \mathcal{Q}''',\phi') \in \mathrm{supp}(F)$. Since $v' \doteq u\rho_{\mathcal{AX}}\phi'$ and $Msg(t\rho_{\mathcal{AX}}\phi')$ imply $v'\rho \doteq u\sigma'$ and $Msg(t\sigma')$, we deduce that $\mathcal{Q}''\rho \cup \{\!\{\mathsf{out}(u\sigma', t\sigma').P\sigma'\}\!\} \cup \mathcal{P}_{Att,1}\sigma' \xrightarrow{\tau}_{\mathsf{N}^o} \delta_{\{\!\{P\sigma', Q'\rho\{^{t\sigma'}/_{x'}\}\}\!\}\cup\mathcal{Q}'''\rho\cup\mathcal{P}_{Att,1}\sigma'}$. Therefore $\mathcal{Q}''\rho \cup \{\!\{\mathsf{out}(u\sigma', t\sigma').P\sigma'\}\!\} \cup \mathcal{P}_{Att,1}\sigma' \xrightarrow{\tau}_{\mathsf{N}^o} \delta_{(\{\!\{Q'\{^{t\rho_{\mathcal{AX}}\phi'}/_{x'}\}\}\!\}\cup\mathcal{Q}''')\rho\cup\mathcal{P}_{Att,2}\sigma'}$.

We have therefore proved that:

$$\sum_{(\mathcal{Q}'',\phi')\in\mathrm{supp}(E)} E((\mathcal{Q}'',\phi'))\cdot\delta_{\mathcal{Q}''\rho\cup\mathcal{P}_{Att}\sigma'} \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} \sum_{(\mathcal{Q}'',\phi')\in\mathrm{supp}(F)} F((\mathcal{Q}'',\phi'))\cdot\delta_{\mathcal{Q}''\rho\cup\mathcal{P}_{Att,2}\sigma'}$$

Note that $F \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^\ell} D'_1$. Once again by the semantics of $\xrightarrow{\tau}_{\mathsf{N}^\ell}$ in Figure 10 and by Lemma 45, we can easily show that:

$$\sum_{(\mathcal{Q}'',\phi')\in\mathrm{supp}(F)} F((\mathcal{Q}'',\phi'))\cdot\delta_{\mathcal{Q}''\rho\cup\mathcal{P}_{Att,2}\sigma'} \xRightarrow{\tau}_{\mathsf{r},\mathsf{N}^o} \sum_{(\mathcal{Q}'',\phi')\in\mathrm{supp}(D'_1)} D'_1((\mathcal{Q}'',\phi'))\cdot\delta_{\mathcal{Q}''\rho\cup\mathcal{P}_{Att,2}\sigma'}$$

Let us denote $D' = \sum_{(\mathcal{Q}'',\phi')\in\mathrm{supp}(D'_1)} D'_1((\mathcal{Q}'',\phi'))\cdot\delta_{\mathcal{Q}''\rho\cup\mathcal{P}_{Att,2}\sigma'}$. We conclude by applying Lemma 63 that $D\ \widehat{R_{op}}\ D'$ (and $D'\ \widehat{R_{op}}\ D$ when $op = \approx$). □

Lemma 65. For all $op \in \{\leq, \approx\}$, for all $\mathcal{P}, \mathcal{P}' \in \mathcal{SP}$, if $\mathcal{P}\ R_{op}\ \mathcal{P}'$ then for all $c \in \mathcal{N}_{pub}$, $\mathrm{RProb}_{\mathcal{R}^o_{\mathsf{r}}}(\mathcal{P}, \downarrow c) \leq \mathrm{RProb}_{\mathcal{R}^o_{\mathsf{r}}}(\mathcal{P}', \downarrow c)$.

Proof. By Lemma 52, $\mathrm{RProb}_{\mathcal{R}^o_{\mathsf{r}}}(\mathcal{P}, \downarrow c) = \sup\{\ D(\downarrow c) \mid \delta_{\mathcal{P}} \xRightarrow{\tau}_{\mathsf{r}} D$ with finite support$\}$.

Let $\mathcal{P} \xRightarrow{\tau}_{\mathsf{r}} D$ with finite support. By Lemma 64 and Property 4a of Lemma 48, we deduce that there exists $\mathcal{P}' \xRightarrow{\tau}_{\mathsf{r}} D'$ such that $D\ \widehat{R_{op}}\ D'$.

By definition of $D\ \widehat{R_{op}}\ D'$, we know that for all $\mathcal{P}_1 \in \mathrm{supp}(D)$, $\mathcal{P}'_1 \in \mathrm{supp}(D')$, there exist $\mathcal{P}_{Att}$, a renaming of variables ρ and two extended processes $(\mathcal{Q}, \phi)$ and $(\mathcal{Q}', \phi')$ such that:

- $|\phi| = |\phi'| = n$
- $(\mathcal{Q}, \phi)\ op^{\mathsf{N}^\ell}\ (\mathcal{Q}', \phi')$
- $\mathcal{P}_1 = \mathcal{Q}\rho \cup \mathcal{P}_{Att}\{^{\mathsf{ax}_i\phi}/_{x_i}\}_{i=1}^n\rho$
- $\mathcal{P}'_1 = \mathcal{Q}'\rho \cup \mathcal{P}_{Att}\{^{\mathsf{ax}_i\phi'}/_{x_i}\}_{i=1}^n\rho$

By construction, if $\mathcal{P}_{Att} \in \downarrow c$ then $\mathcal{P}_1, \mathcal{P}'_1 \in \downarrow c$. Otherwise, if $(\mathcal{Q}, \phi) \xrightarrow{out(c,\mathsf{ax}_{n+1})} E$ then by Figure 10, we know that E is a dirac. But $(\mathcal{Q}, \phi)\ op^{\mathsf{N}^\ell}\ (\mathcal{Q}', \phi')$ implies that there exist $(\mathcal{Q}', \phi') \xRightarrow{\tau}_{\mathsf{r}} F_1$ and $F_1 \xrightarrow{out(c,\mathsf{ax}_{n+1})} F_2$ and $F_2 \xRightarrow{\tau}_{\mathsf{r}} E'$ such that $E\ \widehat{op^{\mathsf{N}^\ell}}\ E'$. By definition of $\widehat{op^{\mathsf{N}^\ell}}$ and since E is a dirac, we deduce that E' is a distribution, which implies that both F_1 and F_2 are distributions. In particular, $F_1 \xrightarrow{out(c,\mathsf{ax}_{n+1})} F_2$ tells us that $\sum_{\mathcal{Q}''\in\downarrow c} F_1(\mathcal{Q}'') = 1$. Note that the τ on $(\mathcal{Q}', \phi')$ carries over $\mathcal{P}'_1$. Thus, there exists H such that $\mathcal{P}'_1 \xRightarrow{\tau}_{\mathsf{r}} H$ and $H(\downarrow c) = 1$.

Finally, let $S = \mathrm{supp}(D) \cap \downarrow c$. Since, $D\ \widehat{R_{op}}\ D'$, we deduce that $D(S) \leq D'(R_{op}\ (S))$. As we have just show that for all $\mathcal{P}'_1 \in R_{op}\ (S)$, there exists H such that $\mathcal{P}'_1 \xRightarrow{\tau}_{\mathsf{r}} H$ with $H(\downarrow c) = 1$, we deduce that there exists D'' such that $D' \xRightarrow{\tau}_{\mathsf{r}} D''$ such that $D(S) \leq D'(R_{op}\ (S)) \leq D''(\downarrow c)$.

To summarize, we have show that for all $\mathcal{P} \xRightarrow{\tau}_{\mathsf{r}} D$ with finite support, there exists $\mathcal{P}' \xRightarrow{\tau}_{\mathsf{r}} D''$ such that $D(\downarrow c) \leq D''(\downarrow c)$. Hence $\sup\{\ D(\downarrow c) \mid \delta_{\mathcal{P}} \xRightarrow{\tau}_{\mathsf{r}} D$ with finite support$\} \leq \sup\{\ D(\downarrow c) \mid \delta_{\mathcal{P}'} \xRightarrow{\tau}_{\mathsf{r}} D\}$. We conclude by applying again Lemma 52. □

F.5 Main result

Proposition 5. Let $\mathcal{P}, \mathcal{Q}$ two processes in $\mathcal{MP}$.

$$\mathcal{P} \leq_{obs}^{\mathcal{R}_r} \mathcal{Q} \quad \text{iff} \quad (\mathcal{P}, \varnothing) \leq_{sim}^{\mathsf{N}^\ell} (\mathcal{Q}, \varnothing) \qquad \text{and} \qquad \mathcal{P} \approx_{obs}^{\mathcal{R}_r} \mathcal{Q} \quad \text{iff} \quad (\mathcal{P}, \varnothing) \approx_{bi}^{\mathsf{N}^\ell} (\mathcal{Q}, \varnothing)$$

Proof. The proof of observational preorder (resp. equivalence) implying simulation (resp. bisimulation) is directly given by application of Lemmas 55, 56 and 61.

Lemmas 62, 64 and 65 directly gives that simulation (resp. bisimulation) implies $\leq_{obs}^{r_1}$ (resp. $\approx_{obs}^{'r_1}$). We conclude by Lemma 53.

□

G Non probabilistic processes

G.1 Hennessy-Milner's Logical caracterisation

We split the proof of Lemma 12 in two lemmas: Lemmas 66 and 68 below.

Lemma 66. Let $\mathcal{P}$ a non-probabilistic process, ϕ a frame. Let $F \in \mathcal{F}$. Let $ok \in \mathcal{N}_{pub}$ such that $ok \notin fn(\mathcal{P}, \phi, F)$. If $(\mathcal{P}, \phi) \models F$ then there exists a resolution $R = (Y, corr, r)$, and $s \in Y$ such that $corr(s) = (\mathcal{P} \cup \{\!\{Adv_{F,|\phi|}^{ok}\phi\}\!\})$ and $\mathrm{RProb}_R(s, corr^{-1}(\downarrow ok)) = 1$.

Proof. Let $n = |\phi|$. We do the proof by induction on the structure of the logical formula F.

Case $F = \top$: $Adv_{\top,n}^{ok} \in \downarrow ok$ hence the result directly holds.

Case $F = a.F'$: we suppose that $(\mathcal{P}, \phi) \models F$. Then by definition of formula validity, we know that there exists a state $(\mathcal{Q}, \psi)$ such that $(\mathcal{P}, \phi) \xrightarrow{\tau}^* \xrightarrow{a} \xrightarrow{\tau}^* (\mathcal{Q}, \psi)$, and $(\mathcal{Q}, \psi) \models F'$. Using the induction hypothesis, we can deduce from $(\mathcal{Q}, \psi) \models F'$ that there exists a pair (R_1, s_1), where $R_1 = (Y_1, corr_1, r_1)$ is a resolution on the NPLTS N^o, $s_1 \in Y_1$ such that $corr(s_1) = \mathcal{Q} \mid Adv_{F',n'}^{ok}\psi$ and $\mathrm{RProb}_{R_1}(s_1, corr_1^{-1}(\downarrow ok)) = 1$ (where $n' = n + 1$ when a is an output and $n' = n$ otherwise).

Moreover, we can deduce from $(\mathcal{P}, \phi) \xrightarrow{\tau}^* \xrightarrow{a} \xrightarrow{\tau}^* (\mathcal{Q}, \psi)$ that $Adv_{F,n}^{ok} \neq 0$ and there exists a sequence of steps:

$$(\mathcal{P}, \phi) \xrightarrow{\tau} (\mathcal{P}'_1, \phi) \ldots \xrightarrow{\tau} (\mathcal{P}'_n, \phi) \xrightarrow{a} (\mathcal{P}''_1, \psi) \ldots \xrightarrow{\tau} (\mathcal{P}''_m, \psi) \xrightarrow{\tau} (\mathcal{Q}, \psi)$$

Looking at the way we define the adversary $Adv_{F,n}^{ok}$ in Definition 27, we see that we can deduce:

$$\begin{aligned}(\mathcal{P} \cup \{\!\{Adv_{F,n}^{ok}\phi\}\!\}) &\xrightarrow{\tau} (\mathcal{P}'_1 \cup \{\!\{Adv_{F,n}^{ok}\phi\}\!\}) \xrightarrow{\tau} \ldots \xrightarrow{\tau} (\mathcal{P}'_k \cup \{\!\{Adv_{F,n}^{ok}\phi\}\!\}) \xrightarrow{\tau} \\ &(\mathcal{P}''_1 \cup \{\!\{Adv_{F',n'}^{ok}\psi\}\!\}) \xrightarrow{\tau} \ldots \xrightarrow{\tau} (\mathcal{P}''_m \cup \{\!\{Adv_{F',n'}^{ok}\psi\}\!\}) \xrightarrow{\tau} (\mathcal{Q} \cup \{\!\{Adv_{F',n'}^{ok}\psi\}\!\})\end{aligned}$$

We build a resolution $R = (Y, corr, r)$ on the NPLTS N^o as follows (our construction is graphically represented in Figure 11):

- $Y = Y_1 \sqcup \{l(0), \ldots, l(k)\} \sqcup \{q(1), \ldots, q(m)\}$, where $\sqcup$ models *disjoint* union, and the $l(.)$, $q(.)$ are simply two disjoint copies of natural numbers;
- $corr : Y \to \mathcal{MP}$ is defined as $corr(y) = corr_1(y)$ when $y \in Y_1$, $corr(l(0)) = (\mathcal{P} \cup \{\!\{Adv^{ok}_{F,n}\phi\}\!\})$, $corr(l(i)) = (\mathcal{P}'_k \cup \{\!\{Adv^{ok}_{F,n}\phi\}\!\})$ for $0 < i \leq k$; $corr(q(j)) = (\mathcal{P}''_j \cup \{\!\{Adv^{ok}_{F',n'}\psi\}\!\})$ for $1 \leq j \leq m$.
- $r : Y \to \mathcal{D}(Y)$ is defined as $r(y) = r_1(y)$ when $y \in Y_1$, $r(l(i)) = \delta_{l(i+1)}$ for $0 \leq i \leq k-1$, $r(l(k)) = \delta_{q(1)}$, $r(q(j)) = \delta_{q(j+1)}$ for $1 \leq j \leq m-1$, $r(q(k)) = \delta_{s_1}$.

We can check that R is indeed a resolution in the sense of Definition 5, and that moreover:

$$\begin{aligned}\mathrm{RProb}_R(l(0), corr^{-1}(\downarrow ok)) &= \mathrm{RProb}_R(s_1, corr_1^{-1}(\downarrow ok)) \\ &= \mathrm{RProb}_{R_1}(s_1, corr_1^{-1}(\downarrow ok)) = 1\end{aligned}$$

Case $F = F_1 \wedge F_2$: we suppose that $(\mathcal{P}, \phi) \models F$. Then by definition of formula validity, we know that $(\mathcal{P}, \phi) \models F_1$ and $(\mathcal{P}, \phi) \models F_2$. By applying the induction hypothesis on F_1 and F_2, we obtain two resolution $R_1 = (Y_1, corr_1, r_1)$, $R_2 = (Y_2, corr_2, r_2)$, and $s_1 \in Y_1$, $s_2 \in Y_2$ with $corr_1(s_1) = (\mathcal{P} \cup \{\!\{Adv^{ok}_{F_1,n}\phi\}\!\})$ and $corr_2(s_2) = (\mathcal{P} \cup \{\!\{Adv^{ok}_{F_2,n}\phi\}\!\})$ such that moreover:

$$\begin{aligned}&\mathrm{RProb}_{R_1}(s_1, corr_1^{-1}(\downarrow ok)) = 1 \\ &\mathrm{RProb}_{R_2}(s_2, corr_2^{-1}(\downarrow ok)) = 1\end{aligned}$$

We now build, using the resolution R_1 and R_2, a resolution R as represented in Figure 12.

- $Y = Y_1 \sqcup Y_2 \sqcup \{l(0)\}$;
- $corr : Y \to \mathcal{MP}$ is defined as $corr(y) = corr_1(y)$ when $y \in Y_1$, $corr(y) = corr_2(y)$ when $y \in Y_2$, $corr(l(0)) = (\mathcal{P} \cup \{\!\{Adv^{ok}_{F,n}\phi\}\!\})$,
- $r : Y \to \mathcal{D}(Y)$ is defined as $r(y) = r_1(y)$ when $y \in Y_1$, $r(y) = r_2(y)$ when $y \in Y_2$, $r(l(0)) = \frac{1}{2}\delta_{s_1} + \frac{1}{2}\delta_{s_2}$.

We can check that R is indeed a resolution in the sense of Definition 5, and that moreover:

$$\begin{aligned}\mathrm{RProb}_R(l(0), corr^{-1}(\downarrow ok)) &= \frac{1}{2} \cdot \mathrm{RProb}_R(s_1, corr^{-1}(\downarrow ok)) + \frac{1}{2} \cdot \mathrm{RProb}_R(s_2, corr^{-1}(\downarrow ok)) \\ &= \frac{1}{2} \cdot \mathrm{RProb}_R(s_1, corr_1^{-1}(\downarrow ok)) + \frac{1}{2} \cdot \mathrm{RProb}_R(s_2, corr_2^{-1}(\downarrow ok)) \\ &= 1\end{aligned}$$

This allows us to conclude. □

Lemma 67. Let $(\mathcal{P}, \phi)$ be a non-probabilistic extended process. Let $F \in \mathcal{F}$. If $(\mathcal{P}, \phi) \xrightarrow{\tau}^* (\mathcal{P}', \phi)$ and $(\mathcal{P}', \phi) \models F$ then $(\mathcal{P}, \phi) \models F'$.

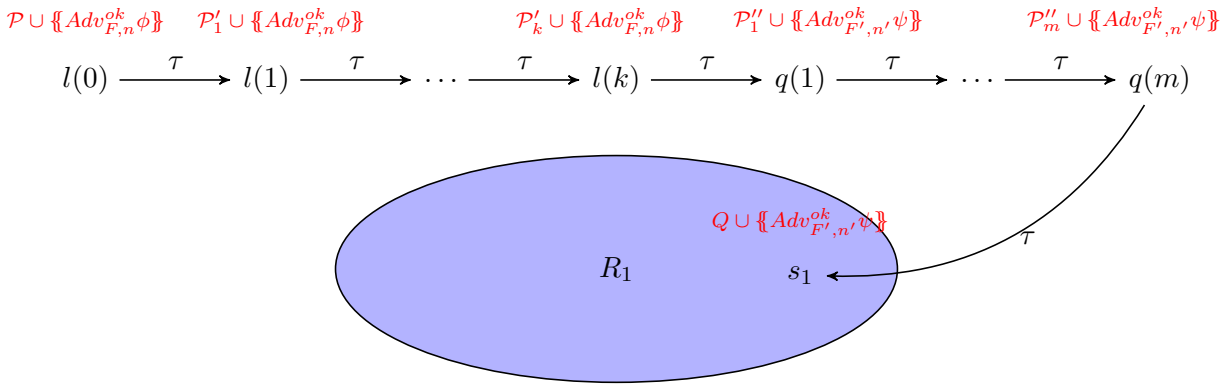


Figure 11: The resolution R for the formula $a.F'$.

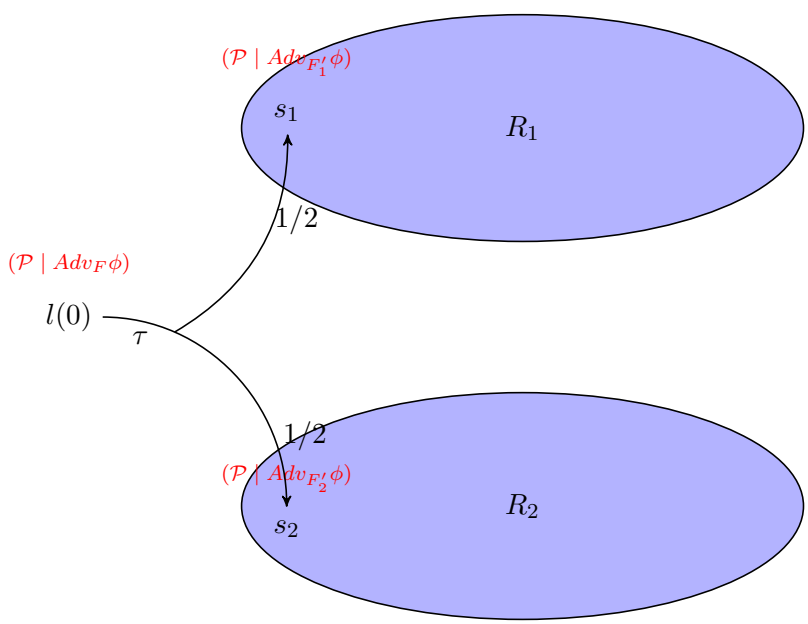


Figure 12: The resolution R for the formula $F'_1 \wedge F'_2$.

Proof. By induction on the structure of F and by noticing that if $(\mathcal{P}', \phi) \xrightarrow{a} (\mathcal{Q}, \phi')$ in the LTS L^ℓ then we also have $(\mathcal{P}, \phi) \xrightarrow{a} (\mathcal{Q}, \phi')$ in the LTS L^ℓ. $\square$

Lemma 68. Let $\mathcal{P}$ a non-probabilistic process, ϕ a frame. Let $F \in \mathcal{F}$. Let $ok \in \mathcal{N}_{pub}$ such that $ok \notin fn(\mathcal{P}, \phi, F)$. If there exists a pair (R, s) with $R = (Y, corr, r) \in \mathcal{R}^o_{\mathsf{nr}}$, such that $corr(s) = (\mathcal{P} \cup \{\!\{Adv^{ok}_{F,|\phi|}\phi\}\!\})$ and $\mathrm{RProb}_R(s, corr^{-1}(\downarrow ok)) = 1$ then $(\mathcal{P}, \phi) \models F$.

Proof. Let $n = |\phi|$. We do the proof by induction on the structure of F.

Case $F = \top$: we can see immediately that the result holds as the formula $\top$ holds for all extended processes.

Case $F = a.F'$: Since $\mathrm{RProb}_R(s, corr^{-1}(\downarrow ok)) = 1$ and $ok \notin fn(\mathcal{P}, \phi, F)$, we deduce that $Adv^{ok}_{F,n} \neq 0$ and $Adv^{ok}_{F,n} \notin \downarrow ok$. Thus, using Lemma 34 and the fact that $\mathcal{P}$ is a non-probabilistic process and the fact that R is a non-randomized resolution, we deduce that there exist $\mathcal{P}_1, \ldots, \mathcal{P}_k$, $\mathcal{Q}$, ϕ' and the following sequence

$$s \xrightarrow{\tau} \delta_{s_1} \quad s_1 \xrightarrow{\tau} \delta_{s_2} \quad \ldots s_{k-1} \xrightarrow{\tau} \delta_{s_k} \quad s_k \xrightarrow{\tau} \delta_{s_a}$$

such that

- for all $i \in \{1, \ldots k\}$, $corr(s_i) = \mathcal{P}_i \cup \{\!\{Adv^{ok}_{F,n}\phi\}\!\}$
- $\mathcal{P} \xrightarrow{\tau} \delta_{\mathcal{P}_1}$
- for all $i \in \{1, \ldots, k-1\}$, $\mathcal{P}_i \xrightarrow{\tau} \delta_{\mathcal{P}_{i+1}}$
- $corr(s_a) = \mathcal{Q} \cup \{\!\{Adv^{ok}_{F',|\phi'|}\phi'\}\!\}$
- $(\mathcal{P}_k, \phi) \xrightarrow{a} \delta_{(\mathcal{Q},\phi')}$
- $\mathrm{RProb}_R(s_a, corr^{-1}(\downarrow ok)) = 1$

Note that here, k can be equal to 0 and in that case $s \xrightarrow{\tau} \delta_{s_a}$. We deduce that $(\mathcal{P}, \phi) \xrightarrow{a} (\mathcal{Q}, \phi')$ in the LTS L^ℓ. Using our inductive hypothesis on F' and the pair (R, s_a), we deduce obtain that $(\mathcal{Q}, \phi') \models F'$. By definition of the validity of a formula, we conclude that $(\mathcal{P}, \phi) \models a.F'$.

Case $F = F_1 \wedge F_2$: Since $Adv^{ok}_{F,n} = Adv^{ok}_{F_1,n} +_{\frac{1}{2}} Adv^{ok}_{F_2,n}$, $Adv^{ok}_{F,n} \notin \downarrow ok$. Hence, using Lemma 34 and the fact that $\mathcal{P}$ is a non-probabilistic process and the fact that R is a non-randomized resolution, we deduce from $\mathrm{RProb}_R(s, corr^{-1}(\downarrow ok)) = 1$ that there exist $\mathcal{P}_1, \ldots, \mathcal{P}_k$, $\mathcal{Q}$, ϕ' and the following sequence

$$s \xrightarrow{\tau} \delta_{s_1} \quad s_1 \xrightarrow{\tau} \delta_{s_2} \quad \ldots s_{k-1} \xrightarrow{\tau} \delta_{s_k} \quad s_k \xrightarrow{\tau} \frac{1}{2}\delta_{s_{a_1}} + \frac{1}{2}\delta_{s_{a_2}}$$

such that

- for all $i \in \{1, \ldots k\}$, $corr(s_i) = \mathcal{P}_i \cup \{\!\{Adv^{ok}_{F,n}\phi\}\!\}$

- $\mathcal{P} \xrightarrow{\tau} \delta_{\mathcal{P}_1}$
- for all $i \in \{1, \ldots, k-1\}$, $\mathcal{P}_i \xrightarrow{\tau} \delta_{\mathcal{P}_{i+1}}$
- $corr(s_{a_1}) = \mathcal{P}_k \cup \{\!\{Adv^{ok}_{F_1,n}\phi\}\!\}$
- $corr(s_{a_2}) = \mathcal{P}_k \cup \{\!\{Adv^{ok}_{F_2,n}\phi\}\!\}$
- $\mathrm{RProb}_R(s_{a_1}, corr^{-1}(\downarrow ok)) = 1$
- $\mathrm{RProb}_R(s_{a_2}, corr^{-1}(\downarrow ok)) = 1$

By applying our inductive hypothesis on F_1 and the pair (R, s_{a_1}), we obtain $(\mathcal{P}_k, \phi) \models F_1$. Similarly, we also obtain $(\mathcal{P}_k, \phi) \models F_2$. As $(\mathcal{P}, \phi) \xrightarrow{\tau}^* (\mathcal{P}_k, \phi)$, we conclude by applying Lemma 67 that $(\mathcal{P}, \phi) \models F_1 \wedge F_2$. □

Lemma 12. Let $\mathcal{P} \in \mathcal{MP}^{\mathsf{np}}$ and $ok \in \mathcal{N}_{pub}$ such that $ok \notin fn(\mathcal{P})$. For all formula $F \in \mathcal{F}$, we have

$$(\mathcal{P}, \varnothing) \models F \qquad \text{iff} \qquad \mathrm{RProb}_{\mathcal{R}_r}(\mathcal{P} \cup \{\!\{Adv^{ok}_{F,0}\}\!\}, \downarrow ok) = 1$$

Proof. Direct from Lemmas 30, 66 and 68. □

G.2 Proposition 6

Lemma 69. Let $(\mathcal{P}, \phi)$ and $(\mathcal{P}', \phi')$ be two extended processes such that $dom(\phi) = dom(\phi')$. Let $A \in \mathcal{MP}$ such that $fn(A) \subseteq \mathcal{N}_{pub}$ and $fv(A) \subseteq dom(\phi)$. If $\mathcal{P} \cup A\phi \rightarrow^* \mathcal{Q}$ then there exists $(\mathcal{P}_1, \phi_1) \in \mathcal{SP}_\ell$, an adversarial process A_1 for $dom(\phi_1)$ and a trace w such that $\mathcal{Q} = \mathcal{P}_1 \cup A_1\phi_1$, $(\mathcal{P}, \phi) \xrightarrow{w} (\mathcal{P}_1, \phi_1)$ and for all recipes ξ, ζ, if $vars(\xi, \zeta) \subseteq dom(\phi_1)$ and $\xi\phi_1 \doteq \zeta\phi_1$ then

$$(\mathcal{P}', \phi') \xrightarrow{w} (\mathcal{P}'_1, \phi'_1) \rightarrow_{\xi \stackrel{?}{=} \zeta} (\mathcal{P}'_1, \phi'_1) \text{ implies } \mathcal{P}' \cup A\phi' \rightarrow^* \mathcal{P}'_1 \cup A_1\phi'_1$$

Proof. We prove this lemma by induction on the length of the derivation $\mathcal{P} \cup A\phi \rightarrow^* \mathcal{Q}$.

Base case $\ell = 0$: In such a case, $\mathcal{Q} = \mathcal{P} \cup A\phi$. We take $w = \varepsilon$ and $A_1 = A$. Let ξ, ζ be recipes such that $vars(\xi, \zeta) \subseteq dom(\phi')$ and $\xi\phi \doteq \zeta\phi$. We conclude by noticing that $(\mathcal{P}', \phi') \xrightarrow{\varepsilon} (\mathcal{P}'_1, \phi'_1) \rightarrow_{\xi \stackrel{?}{=} \zeta} (\mathcal{P}'_1, \phi'_1)$ implies $\phi' = \phi'_1$ and $\mathcal{P}' \rightarrow^* \mathcal{P}'_1$. Therefore, $\mathcal{P}' \cup A\phi \rightarrow^* \mathcal{P}'_1 \cup A_1\phi'_1$.

Inductive step $\ell > 0$: In such a case, we have $\mathcal{P} \cup A\phi \rightarrow^* \mathcal{Q}_2 \rightarrow \mathcal{Q}$ where the length of the derivation $\mathcal{P} \cup A\phi \rightarrow^* \mathcal{Q}_2$ is strictly smaller than ℓ. We can apply our inductive hypothesis to obtain that there exist $(\mathcal{P}_2, \phi_2) \in \mathcal{SP}_\ell$, an adversarial process A_2 for $dom(\phi_2)$ and a trace w_2 such that $\mathcal{Q}_2 = \mathcal{P}_2 \cup A_2\phi_2$, $(\mathcal{P}, \phi) \xrightarrow{w_2} (\mathcal{P}_2, \phi_2)$ and for all recipes ξ', ζ', if $vars(\xi', \zeta') \subseteq dom(\phi_2)$ and $\xi'\phi_2 \doteq \zeta'\phi_2$ then

$$(\mathcal{P}', \phi') \xRightarrow{w_2} (\mathcal{P}'_2, \phi'_2) \rightarrow_{\xi' \stackrel{?}{=} \zeta'} (\mathcal{P}'_2, \phi'_2) \text{ implies } \mathcal{P}' \cup A\phi' \rightarrow^* \mathcal{P}'_2 \cup A_2\phi'_2$$

By taking $\xi' = \zeta' \in \mathcal{N}_{pub}$, we have that $(\mathcal{P}', \phi') \overset{w_2}{\Longrightarrow} (\mathcal{P}'_2, \phi'_2)$ implies $\mathcal{P}' \cup A\phi' \to^* \mathcal{P}'_2 \cup A_2\phi'_2$.

We do a case analysis on the rule applied in $\mathcal{P}_2 \cup A_2\phi_2 \to \mathcal{Q}$.

Case of an internal reduction on $\mathcal{P}_2$: In such a case $\mathcal{P}_2 \to \mathcal{P}_1$ and $\mathcal{P}_Q = \mathcal{P}_1 \cup A_2\phi_2$. Let $A_1 = A_2$, $\phi_1 = \phi_2$ and $w = w_2$. Note that $\mathcal{P}_2 \to \mathcal{P}_1$ implies $(\mathcal{P}_2, \phi_2) \to_\tau (\mathcal{P}_1, \phi_1)$ hence $(\mathcal{P}, \phi) \overset{w}{\to} (\mathcal{P}_1, \phi_1)$.

Let ξ, ζ be recipes such that $vars(\xi, \zeta) \subseteq dom(\phi_1)$. If $(\mathcal{P}', \phi') \overset{w}{\to} (\mathcal{P}'_1, \phi'_1) \to_{\xi \overset{?}{=} \zeta} (\mathcal{P}'_1, \phi'_1)$ then we can directly rely on our inductive hypothesis to conclude.

Case of an internal reduction on $A_2\phi_2$: In such a case, there exists an adversarial process A_1 such that $A_2\phi_2 \to A_1\phi_2$ and $\mathcal{P}_Q = \mathcal{P}_1 \cup A_1\phi_2$. To define the trace we need to consider, let us look at the rule $A_2\phi_2 \to A_1\phi_2$.

- Rule Then: In such a case, $A_2 = A' \cup \{\!\!\{\mathsf{if}\ u = v\ \mathsf{then}\ P\ \mathsf{else}\ Q\}\!\!\}$ and $A_1 = A' \cup \{\!\!\{P\}\!\!\}$. We define $w = w_2.(u \overset{?}{=} v)$.
- Rule Else: In such a case, $A_1 = A' \cup \{\!\!\{\mathsf{if}\ u = v\ \mathsf{then}\ P\ \mathsf{else}\ Q\}\!\!\}$ and $A_1 = A' \cup \{\!\!\{Q\}\!\!\}$. We define $w = w_2.(u \overset{?}{\neq} v)$.
- Otherwise, we define $w = w_2$

Let $\phi_1 = \phi_2$ and $\mathcal{P}_1 = \mathcal{P}_2$. In the case of the rule Then (resp. Else), $A_2\phi_2 \to A_1\phi_2$ implies that $u\phi_2 \doteq v\phi_2$ (resp. $u\phi_2 \not\doteq v\phi_2$). Hence $(\mathcal{P}_2, \phi_2) \to_{(u \overset{?}{=} v)} (\mathcal{P}_1, \phi_1)$ (resp. $(\mathcal{P}_2, \phi_2) \to_{(u \overset{?}{\neq} v)} (\mathcal{P}_1, \phi_1)$) and so $(\mathcal{P}, \phi) \overset{w}{\to} (\mathcal{P}_1, \phi_1)$.

Let us now take ξ, ζ recipes such that $vars(\xi, \zeta) \subseteq dom(\phi_1)$ and $(\mathcal{P}', \phi') \overset{w_2}{\longrightarrow} (\mathcal{P}'_2, \phi'_2) \to_a (\mathcal{P}'_1, \phi'_1) \to_{\xi \overset{?}{=} \zeta} (\mathcal{P}'_1, \phi'_1)$ with a being either $(u \overset{?}{=} v)$ or $(u \overset{?}{\neq} v)$ or τ following the rule applied on $A_2\phi_2 \to A_1\phi_2$. If $a = \tau$ then we trivially have that $(\mathcal{P}'_2, \phi'_2) = (\mathcal{P}'_1, \phi'_1)$ and $A_2\phi'_2 \to A_1\phi'_1$. Hence, $\mathcal{P}'_2 \cup A_2\phi'_2 \to \mathcal{P}'_2 \cup A_1\phi'_1$ and so the result holds.

If $a = (u \overset{?}{=} v)$ (resp. $(u \overset{?}{\neq} v)$) then $(\mathcal{P}'_2, \phi'_2) \to_a (\mathcal{P}'_1, \phi'_1)$ implies that $(\mathcal{P}'_2, \phi'_2) = (\mathcal{P}'_1, \phi'_1)$ and $u\phi'_1 \doteq v\phi'_1$ (resp. $u\phi'_1 \not\doteq v\phi'_1$). Hence, $A_2\phi'_2 \to A_1\phi'_1$ which allows us to conclude.

*Case of the rule (*Comm*) between $\mathcal{P}_2$ (input) and $A_2\phi_2$ (output):* In such a case, we have $\mathcal{P}_2 = \mathcal{P}_3 \cup \{\!\!\{\mathsf{in}(c, x).P\}\!\!\}$ and $A_2 = A_3 \cup \{\!\!\{\mathsf{out}(u, v).Q\}\!\!\}$ with $Msg(v\phi_2)$, $u\phi_2 \doteq c$, $\mathcal{P}_1 = \mathcal{P}_3 \cup \{\!\!\{P\{x \to v\phi_2\}\}\!\!\}$ and $A_1 = A_3 \cup \{\!\!\{Q\}\!\!\}$. Therefore by denoting $\phi_1 = \phi_2$, we have $(\mathcal{P}_2, \phi_2) \to_{in(u,v)} (\mathcal{P}_1, \phi_1)$. We define $w = w_2.in(u, v)$.

Let us now take ξ, ζ recipes such that $vars(\xi, \zeta) \subseteq dom(\phi_1)$ and $(\mathcal{P}', \phi') \overset{w_2}{\longrightarrow} (\mathcal{P}'_2, \phi'_2) \to_{in(u,v)} (\mathcal{P}'_1, \phi'_1) \to_{\xi \overset{?}{=} \zeta} (\mathcal{P}'_1, \phi'_1)$. By definition, we deduce that $\phi'_1 = \phi'_2$, $\mathcal{P}'_2 = \mathcal{P}'_3 \cup \{\!\!\{\mathsf{in}(c', x).P'\}\!\!\}$, $\mathcal{P}'_1 = \mathcal{P}'_3 \cup \{\!\!\{P'\{x \to v\phi'_1\}\}\!\!\}$, $c' \doteq u\phi'_1$ and $Msg(v\phi'_1)$. This allows us to conclude that $\mathcal{P}'_2 \cup A_2\phi'_2 \to \mathcal{P}'_1 \cup A_1\phi'_1$.

*Case of the rule (*Comm*) between $\mathcal{P}_2$ (output) and $A_2\phi_2$ (input):* In such a case, we have $\mathcal{P}_2 = \mathcal{P}_3 \cup \{\!\!\{\mathsf{out}(c, t).P\}\!\!\}$ and $A_2 = A_3 \cup \{\!\!\{\mathsf{in}(u, \mathsf{ax}_{n+1}).Q\}\!\!\}$ (w.l.o.g. we rename the variable to ax_{n+1} if $|dom(\phi_1)| = n$) with $Msg(t)$, $c \doteq u\phi_1$, $\mathcal{P}_1 = \mathcal{P}_3 \cup \{\!\!\{P\}\!\!\}$ and $A_1 = A_3 \cup \{\!\!\{Q\{x \to t\}\}\!\!\}$.

As $Msg(t)$ and $c \doteq u\phi_1$, we can notice that $(\mathcal{P}_2, \phi_2) \rightarrow_{out(u,\mathsf{ax}_{n+1})} (\mathcal{P}_3 \cup \{\!\{P\}\!\}, \phi_2\{\mathsf{ax}_{n+1} \mapsto t\})$. By defining $w = w_2.out(u, \mathsf{ax}_{n+1})$, $\phi_1 = \phi_2\{\mathsf{ax}_{n+1} \mapsto t\}$, we have $(\mathcal{P}, \phi) \xrightarrow{w} (\mathcal{P}_1, \phi_1)$.

Let us now take ξ, ζ recipes such that $vars(\xi, \zeta) \subseteq dom(\phi_1)$ and $(\mathcal{P}', \phi') \xrightarrow{w_2} (\mathcal{P}'_2, \phi'_2) \rightarrow_{out(u,\mathsf{ax}_{n+1})} (\mathcal{P}'_1, \phi'_1) \rightarrow_{\xi \stackrel{?}{=} \zeta} (\mathcal{P}'_1, \phi'_1)$. By definition, $\mathcal{P}' = \mathcal{P}'_3 \cup \{\!\{\mathsf{out}(c', t').P'\}\!\}$, $Msg(t')$, $c' \doteq u\phi'_1$, $\mathcal{P}'_1 = \mathcal{P}'_3 \cup \{\!\{P'\}\!\}$ and $\phi'_1 = \phi'_2\{\mathsf{ax}_{n+1} \mapsto t'\}$. This allows us to obtain $\mathcal{P}'_2 \cup A_2\phi'_2 \rightarrow \mathcal{P}'_1 \cup A_1\phi'_1$. □

Proposition 6. Let $\mathcal{P}, \mathcal{Q} \in \mathcal{MP}^{\mathsf{np}}$.

$$(\mathcal{P}, \varnothing) \leq_{tr} (\mathcal{Q}, \varnothing) \quad \text{iff} \quad \begin{array}{l} \forall Adv \in \mathcal{MP}^{\mathsf{np}} \text{ s.t. } fn(Adv) \subseteq \mathcal{N}_{pub}.\ \forall c \in \mathcal{N}_{pub}. \\ \mathrm{RProb}_{\mathcal{R}}(\mathcal{P} \cup Adv, \downarrow c) \leq \mathrm{RProb}_{\mathcal{R}}(\mathcal{Q} \cup Adv, \downarrow c) \end{array}$$

Proof. To show that may-testing implies trace equivalence, we rely on Lemma 12. Indeed, a trace $w = a_1 \ldots a_n$ can be seen as a formula $F = a_1.a_2. \ldots a_n.\top$. In particular, $(\mathcal{P}, \varnothing) \xrightarrow{w} (\mathcal{P}_1, \phi_1)$ if and only if $(\mathcal{P}, \varnothing) \models F$. Hence, by taking $ok \in \mathcal{N}_{pub}$ such that $ok \notin fn(w, \mathcal{P}, \mathcal{Q})$, we can apply Lemma 12 to obtain that $\mathrm{RProb}_{\mathcal{R}_\mathsf{r}}(\mathcal{P} \cup Adv^{ok}_{F,0}, \downarrow ok) = 1$. By hypothesis, we deduce that $\mathrm{RProb}_{\mathcal{R}_\mathsf{r}}(\mathcal{Q} \cup Adv^{ok}_{F,0}, \downarrow ok) = 1$ and so $(\mathcal{Q}, \varnothing) \models F$ once again by Lemma 12. This allows us to conclude that $(\mathcal{Q}, \varnothing) \xrightarrow{w} (\mathcal{Q}_1, \phi'_1)$.

To show that trace equivalence implies may-testing. Let us consider a non-probabilisitic $A \in \mathcal{MP}$ such that $fn(A) \subseteq \mathcal{N}_{pub}$. Let $c \in \mathcal{N}_{pub}$.

Assume that $\mathrm{RProb}_{\mathcal{R}^o_{\mathsf{nr}}}(\mathcal{P} \cup A, \downarrow c) \neq 0$ (otherwise the result trivially holds). Thus $\mathrm{RProb}_{\mathcal{R}^o_{\mathsf{nr}}}(\mathcal{P} \cup A, \downarrow c) = 1$ and so $\mathcal{P} \cup Adv \rightarrow \mathcal{P}' \in \downarrow c$. By Lemma 69, there exists $(\mathcal{P}_1, \phi_1) \in \mathcal{SP}_\ell$, and adversarial process Adv_1 for $dom(\phi_1)$ and a trace w such that $\mathcal{P}' = \mathcal{P}_1 \cup Adv_1\phi_1$, $(\mathcal{P}, \varnothing) \xrightarrow{w} (\mathcal{P}_1, \phi_1)$ and for all recipes ξ, ζ, if $vars(\xi, \zeta) \subseteq dom(\phi_1)$ and $\xi\phi_1 \doteq \zeta\phi_1$ then

$$(\mathcal{Q}, \varnothing) \xrightarrow{w} (\mathcal{Q}_1, \phi'_1) \rightarrow_{\xi \stackrel{?}{=} \zeta} (\mathcal{Q}_1, \phi'_1) \text{ implies } \mathcal{Q} \cup Adv \rightarrow^* \mathcal{Q}_1 \cup Adv_1\phi'_1 \tag{20}$$

If $Adv_1\phi_1 \in \downarrow c$ then $Adv_1 = Adv_2 \cup \{\!\{\mathsf{out}(u, t).P\}\!\}$ with $u\phi_1 \doteq c$. Consider the trace $w' = w.(u \stackrel{?}{=} c)$. We thus have $(\mathcal{P}, \varnothing) \xrightarrow{w'} (\mathcal{P}_1, \phi_1)$. Since $(\mathcal{P}, \varnothing) \leq_{tr} (\mathcal{Q}, \varnothing)$ then there exists $(\mathcal{Q}, \varnothing) \xrightarrow{w.(u \stackrel{?}{=} c)} (\mathcal{Q}_2, \phi'_2)$. Therefore, we have $(\mathcal{Q}, \varnothing) \xrightarrow{w} (\mathcal{Q}_1, \phi'_1) \rightarrow_{u \stackrel{?}{=} c} (\mathcal{Q}_1, \phi'_1) \xrightarrow{\varepsilon} (\mathcal{Q}_2, \phi'_2)$. We deduce that $\mathcal{Q} \cup A \rightarrow^* \mathcal{Q}_1 \cup A_1\phi'_1$ and $u\phi'_1 \doteq c$. Therefore, $A_1\phi'_1 \in \downarrow c$ and so $\mathcal{Q}_1 \cup A_1\phi'_1 \in \downarrow c$. This allows us to conclude that $\mathrm{RProb}_{\mathcal{R}^o_{\mathsf{nr}}}(\mathcal{Q} \cup A, \downarrow c) = 1$.
If $\mathcal{P}_1 \in \downarrow c$ then $\mathcal{P}_1 = \mathcal{P}_2 \cup \{\!\{\mathsf{out}(u, t).P\}\!\}$ with $u \doteq c$ and $Msg(t)$. Hence $(\mathcal{P}_1, \phi_1) \rightarrow_{out(c,\mathsf{ax}_{n+1})} (\mathcal{P}_2 \cup \{\!\{P\}\!\}, \phi_1\{\mathsf{ax}_{n+1} \mapsto t\})$. Since $(\mathcal{P}, \varnothing) \leq_{tr} (\mathcal{Q}, \varnothing)$ then there exists $(\mathcal{Q}, \varnothing) \xrightarrow{w.out(c,\mathsf{ax}_{n+1})} (\mathcal{Q}_3, \phi'_3)$. Therefore, $(\mathcal{Q}, \varnothing) \xrightarrow{w} (\mathcal{Q}_1, \phi'_1) \rightarrow_{out(c,\mathsf{ax}_{n+1})} (\mathcal{Q}_2, \phi'_2) \xrightarrow{\varepsilon} (\mathcal{Q}_3, \phi'_3)$. But $(\mathcal{Q}_1, \phi'_1) \rightarrow_{out(c,\mathsf{ax}_{n+1})} (\mathcal{Q}_2, \phi'_2)$ implies that $\mathcal{Q}_1 = \mathcal{Q}' \cup \{\!\{\mathsf{out}(u', t').P'\}\!\}$ with $c \doteq u'$ and $Msg(t')$. Hence $\mathcal{Q}_1 \in \downarrow c$. By applying Equation (20) with $\xi = \zeta = c$, we deduce that $\mathcal{Q} \cup Adv \rightarrow^* \mathcal{Q}_1 \cup Adv_1\phi'_1$ which allows us to conclude that $\mathrm{RProb}_{\mathcal{R}^o_{\mathsf{nr}}}(\mathcal{Q} \cup A, \downarrow c) = 1$. □

H Fully probabilistic processes

Lemma 16. Let $ok \in \mathcal{N}_{pub}$. Let $(\mathcal{P}, \phi)$ be a purely probabilistic process. Let Adv be a fully determinate adversarial process such that $fv(Adv) \subseteq dom(\phi)$.

$$\begin{aligned}\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P} \cup Adv\phi, \downarrow ok) = \; & \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok) + (1 - \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok)) \times \\ & \textstyle\sum_{(\alpha,w) \in Tr^{ok}(Adv, |dom(\phi)|)} \alpha \cdot \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P}, \phi), w)\end{aligned}$$

Proof. Using the property of maximal schedulers of Proposition 10, we know that there exists a maximal scheduler (corr, R) in $\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)$ such that $\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P} \cup Adv\phi, \downarrow ok) = \mathrm{RProb}_R(s, \mathsf{corr}^{-1}(\downarrow ok))$ where $\mathsf{corr}(s) = \mathcal{P} \cup Adv\phi$.

Moreover we can suppose that $\mathsf{corr}_{\mathsf{R}}$ is simply the identity. It is because, we can see that there always exists a maximal resolution where $\mathsf{corr}_{\mathsf{R}}$ is the identity. Hence, we obtain:

$$\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P} \cup Adv\phi, \downarrow ok) = \mathrm{RProb}_R(\mathcal{P} \cup Adv\phi, \downarrow ok)$$

We will show in fact that from R, we can build a maximal resolution in $\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)$, that we denote $\mathsf{B}_\ell(R)$ such that:

$$\begin{aligned}\mathrm{RProb}_R(\mathcal{P} \cup Adv\phi, \downarrow ok) = \; & \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok) + (1 - \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok)) \times \\ & \textstyle\sum_{(\alpha,w) \in Tr^{ok}(Adv, |dom(\phi)|)} \alpha \cdot \mathrm{Prob}_{\mathsf{B}_\ell(R)}((\mathcal{P}, \phi), w)\end{aligned}$$

Finally, as we only consider finite processes without replication, if we restrict the sets of R to the processes reachabable from $\mathcal{P} \cup Adv\phi$, i.e. $\mathcal{P} \cup Adv\phi \to^* \mathcal{P}'$ then R is finite. Thus:

$$\mathrm{RProb}_R(s, \mathcal{T}) = \begin{cases} 1 & \text{if } s \in \mathcal{T} \\ 0 & \text{if } s \notin \mathcal{T} \wedge \mathsf{trans}(s) = \star \\ \sum_{u \in \mathrm{supp}(D)} D(u) \cdot \mathrm{RProb}_R(u, \mathcal{T}) & \text{if } s \notin \mathcal{T} \wedge \mathsf{trans}(s) = D \end{cases}$$

We do a proof by induction on the sub-scheduler starting from $\mathcal{P} \cup Adv\phi$.

Case $\mathcal{P} \cup Adv\phi \in \downarrow ok$: In such a case, either there exists $\mathsf{out}(u, v); P \in \mathcal{P}$ such that $u \doteq ok$ or $Adv = \mathsf{out}(u', v'); Adv'$ with $u'\phi \doteq ok$. In the former case, we deduce that for any maximal scheduler R' starting from $\mathcal{P}$, $\mathrm{RProb}_{R'}(\mathcal{P}, \downarrow ok) = 1$. By taking $\mathsf{B}_o(R) = R'$ and $\mathsf{B}_\ell(R)$ any maximal scheduler starting from $(\mathcal{P}, \phi)$, we conclude. In the latter case, we have by construction that $Tr^{ok}(Adv\phi, |dom(\phi)|) = \{\!\{(p_i, (u' \stackrel{?}{\neq} ok).in(u', \mathsf{ax}_{n+1}).w_i)\}\!\}_{i=1}^m \cup \{\!\{(1, u' \stackrel{?}{=} ok)\}\!\}$ when $Tr^{ok}(Adv, n) = \{\!\{(p_i, w_i)\}\!\}_{i=1}^m$. As $u'\phi \doteq ok$, we deduce that for all $i \in \{1, \ldots, m\}$, $\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P}, \phi), (u' \stackrel{?}{\neq} ok).in(u, \mathsf{ax}_{n+1}).w_i) = 0$. Hence, by taking any maximal scheduler $\mathsf{B}_\ell(R)$, we have:

$$\sum_{(\alpha,w) \in Tr^{ok}(Adv, |dom(\phi)|)} \alpha \cdot \mathrm{Prob}_{\mathsf{B}_\ell(R)}((\mathcal{P}, \phi), w) = \mathrm{Prob}_{\mathsf{B}_\ell(R)}((\mathcal{P}, \phi), (u' \stackrel{?}{=} ok)) = 1$$

By taking any maximal scheduler $\mathsf{B}_o(R)$ and by denoting $\beta = \mathrm{RProb}_{\mathsf{B}_o(R)}(\mathcal{P}, \downarrow ok)$, we have:

$$\begin{aligned}\mathrm{RProb}_R(\mathcal{P} \cup Adv\phi, \downarrow ok) \; & = \beta + (1 - \beta) * \textstyle\sum_{(\alpha,w) \in Tr^{ok}(Adv, |dom(\phi)|)} \alpha \cdot \mathrm{Prob}_{\mathsf{B}_\ell(R)}((\mathcal{P}, \phi), w) \\ & = \beta + (1 - \beta) = 1\end{aligned}$$

Case $\mathcal{P}\cup Adv\phi \notin\downarrow ok$ *and* $\mathsf{trans}(\mathcal{P}\cup Adv\phi) = \star$*:* As R is maximal, we deduce that there is no possible transition on $\mathcal{P}\cup Adv\phi$. Hence, all processes in $\mathcal{P}$ starts by an input or an output (no τ transition) and either $Adv = 0$ or $Adv = \mathsf{in}(c,x); Adv'$ or $Adv = \mathsf{out}(c,u); Adv'$ with $c\phi \neq c_i$ for all $i \in \{1,\ldots,n\}$. Moreover, when $Adv = \mathsf{out}(c,u); Adv'$, $c\phi \neq ok$. By construction, we deduce that for all $(\alpha, w) \in Tr^{ok}(Adv, |dom(\phi)|)$, $\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P},\phi), w) = 0$. Hence by taking any maximal scheduler as $\mathsf{B}_\ell(R)$, we deduce that:

$$\sum_{(\alpha,w)\in Tr^{ok}(Adv,|dom(\phi)|)} \alpha \cdot \mathrm{Prob}_{\mathsf{B}_\ell(R)}((\mathcal{P},\phi), w) = 0$$

Moreover, since all processes in $\mathcal{P}$ starts by an input or an output (no τ transition) and they have distinct channels, we deduce that for any maximal scheduler $\mathsf{B}_o(R)$ from $\mathcal{P}$ with transition function trans', we have $\mathsf{trans}'(\mathcal{P}) = \star$. Hence, $\mathrm{RProb}_{\mathsf{B}_o(R)}(\mathcal{P}, \downarrow ok) = 0$ which allows us to conclude.

Case $\mathcal{P} \cup \{\!\{Adv\phi\}\!\} \notin\downarrow ok$ *and* $\mathsf{trans}(\mathcal{P} \cup \{\!\{Adv\phi\}\!\}) = D$*:* In such a case, we have four possibilities with respect to the transition $\mathsf{trans}(\mathcal{P} \cup \{\!\{Adv\phi\}\!\}) = D$:

- τ transition on $\mathcal{P}$: In such a case, we have either $D = \delta_{\mathcal{Q}\cup\{\!\{Adv\phi\}\!\}}$ where $\mathcal{P} \xrightarrow{\tau} \mathcal{Q}$ is either conditional or a name restriction; or $\mathcal{P} = \{\!\{P_1 +_p P_2\}\!\} \cup \mathcal{P}'$ and $D = p \cdot \delta_{\mathcal{Q}_1\cup\{\!\{Adv\phi\}\!\}} + (1-p)\cdot\delta_{\mathcal{Q}_2\cup\{\!\{Adv\phi\}\!\}}$ with $\mathcal{Q}_1 = \{\!\{P_1\}\!\} \cup \mathcal{P}'$ and $\mathcal{Q}_2 = \{\!\{P_2\}\!\} \cup \mathcal{P}'$.

  In the first case, by definition, $\mathrm{RProb}_R(\mathcal{Q}\cup\{\!\{Adv\phi\}\!\}, \downarrow ok) = \mathrm{RProb}_R(\mathcal{P}\cup\{\!\{Adv\phi\}\!\}, \downarrow ok)$. Moreover, by applying our inductive hypothesis, we deduce that there exist a scheduler R_ℓ such that

  $$\begin{aligned}\mathrm{RProb}_R(\mathcal{Q}\cup\{\!\{Adv\phi\}\!\}, \downarrow ok) = \;& \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{Q}, \downarrow ok) + (1 - \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{Q}, \downarrow ok))\times \\ & \textstyle\sum_{(\alpha,w)\in Tr^{ok}(Adv,|dom(\phi)|)} \alpha \cdot \mathrm{Prob}_{R_\ell}((\mathcal{Q},\phi), w)\end{aligned}$$

  By taking the maximal scheduler $\mathsf{B}_\ell(R)$ that connects $(\mathcal{P},\phi)$ to $(\mathcal{Q},\phi)$ by the transition $(\mathcal{P},\phi) \xrightarrow{\tau} \delta_{(\mathcal{Q},\phi)}$ (and behaves as R_ℓ everywhere else), we deduce that for all $(\alpha, w) \in Tr^{ok}(Adv, |dom(\phi)|)$, $\mathrm{Prob}_{R_\ell}((\mathcal{Q},\phi), w) = \mathrm{Prob}_{\mathsf{B}_\ell(R)}((\mathcal{P},\phi), w)$. Similarly, by Proposition 10, $\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{Q}, \downarrow ok) = \mathrm{RProb}_{R'}(\mathcal{Q}, \downarrow ok)$ for some R' maximal. By taking the maximal scheduler R'' that connects $\mathcal{P}$ to $\mathcal{Q}$ by the transition $\mathcal{P} \xrightarrow{\tau} \delta_{\mathcal{Q}}$ (and behaves as R' everywhere else), we deduce that $\mathrm{RProb}_{R'}(\mathcal{Q}, \downarrow ok) = \mathrm{RProb}_{R''}(\mathcal{P}, \downarrow ok) = \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok)$. This allows us to conclude that.

  Consider the second case i.e., $\mathcal{P} = \{\!\{P_1 +_p P_2\}\!\} \cup \mathcal{P}'$ and $D = p\cdot\delta_{\mathcal{Q}_1\cup\{\!\{Adv\phi\}\!\}} + (1-p)\cdot\delta_{\mathcal{Q}_2\cup\{\!\{Adv\phi\}\!\}}$. In that case, $\mathrm{RProb}_R(\mathcal{P}\cup\{\!\{Adv\phi\}\!\}, \downarrow ok) = p\cdot\mathrm{RProb}_R(\mathcal{Q}_1\cup\{\!\{Adv\phi\}\!\}, \downarrow ok) + (1-p)\cdot\mathrm{RProb}_R(\mathcal{Q}_2\cup\{\!\{Adv\phi\}\!\}, \downarrow ok)$. Moreover, $(\mathcal{P},\phi) \xrightarrow{\tau} p\cdot\delta_{(\mathcal{Q}_1,\phi)} + (1-p)\cdot\delta_{(\mathcal{Q}_2,\phi)}$.

  By inductive hypothesis, for all $i \in \{1,2\}$, there exist schedulers R_1, R_2 such that:

  $$\begin{aligned}\mathrm{RProb}_R(\mathcal{Q}_i\cup\{\!\{Adv\phi\}\!\}, \downarrow ok) = \;& \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{Q}_i, \downarrow ok) + (1 - \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{Q}_i, \downarrow ok))\times \\ & \textstyle\sum_{(\alpha,w)\in Tr^{ok}(Adv,|dom(\phi)|)} \alpha \cdot \mathrm{Prob}_{R_i}((\mathcal{Q}_i,\phi), w)\end{aligned}$$

Actually, since by Proposition 11, all maximal resolutions on N^ℓ lead to the same probability of reaching a trace, we can suppose $R_1 = R_2$. By taking the scheduler $\mathsf{B}_\ell(R)$ that connects $(\mathcal{P}, \phi)$ to $(\mathcal{Q}_1, \phi)$ with probability p and $(\mathcal{P}, \phi)$ to $(\mathcal{Q}_2, \phi)$ with probability $1 - p$, (and behaves as $R_1 = R_2$ elsewhere) we deduce that for all $(\alpha, w) \in Tr^{ok}(Adv, |dom(\phi)|)$, $\mathrm{Prob}_{\mathsf{B}_\ell(R)}((\mathcal{P}, \phi), w) = p \cdot \mathrm{Prob}_{\mathsf{B}_\ell(R)}((\mathcal{Q}_1, \phi), w) + (1-p) \cdot \mathrm{Prob}_{\mathsf{B}_\ell(R)}((\mathcal{Q}_2, \phi), w) = p \cdot \mathrm{Prob}_{R_1}((\mathcal{Q}_1, \phi), w) + (1-p) \cdot \mathrm{Prob}_{R_2}((\mathcal{Q}_2, \phi), w)$. Similarly, we have that $\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok) = p \cdot \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{Q}_1, \downarrow ok) + (1-p) \cdot \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{Q}_2, \downarrow ok)$.

To summarize, we have

- $\sum_{(\alpha,w) \in Tr^{ok}(Adv, |dom(\phi)|)} \alpha \cdot \mathrm{Prob}_{\mathsf{B}_\ell(R)}((\mathcal{P}, \phi), w) = p \cdot \beta_1 + (1-p) \cdot \beta_2$
- $\beta_i = \sum_{(\alpha,w) \in Tr^{ok}(Adv, |dom(\phi)|)} \alpha \cdot \mathrm{Prob}_{R_i}((\mathcal{Q}_i, \phi), w)$ for $i = 1, 2$
- $\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok) = p \cdot \gamma_1 + (1-p) \cdot \gamma_2$
- $\gamma_i = \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{Q}_i, \downarrow ok)$ for $i = 1, 2$

As $\mathrm{RProb}_R(\mathcal{P} \cup \{\!\{Adv\phi\}\!\}, \downarrow ok) = p \cdot \mathrm{RProb}_R(\mathcal{Q}_1 \cup \{\!\{Adv\phi\}\!\}, \downarrow ok) + (1-p) \cdot \mathrm{RProb}_R(\mathcal{Q}_2 \cup \{\!\{Adv\phi\}\!\}, \downarrow ok) = p \cdot (\beta_1 + \gamma_1) + (1-p) \cdot (\beta_2 + \gamma_2) = (p \cdot \beta_1 + (1-p) \cdot \beta_2) + (p \cdot \gamma_1 + (1-p) \cdot \gamma_2)$, we conclude.

- Probabilistic choice on $Adv\phi$: In such a case, $Adv = Adv_1 +_p Adv_2$ and $Tr^{ok}(Adv_1 +_p Adv_2, n) = \{\!\{(p \cdot p_k^1, w_k^1)\}\!\}_{k=1}^{n_1} \cup \{\!\{((1-p) \cdot p_k^2, w_k^2)\}\!\}_{k=1}^{n_2}$ when $Tr^{ok}(Adv_i, n) = \{\!\{(p_k^i, w_k^i)\}\!\}_{k=1}^{n_i}$ for $i = 1, 2$. Moreover, by definition:

$$\mathrm{RProb}_R(\mathcal{P} \cup \{\!\{Adv\phi\}\!\}, \downarrow ok) = p \cdot \mathrm{RProb}_R(\mathcal{P} \cup \{\!\{Adv_1\phi\}\!\}, \downarrow ok) + (1-p) \cdot \mathrm{RProb}_R(\mathcal{P} \cup \{\!\{Adv_2\phi\}\!\}, \downarrow ok)$$

By inductive hypothesis, for all $i \in \{1, 2\}$, there exist two maximal schedulers R_1, R_2 such that:

$$\begin{aligned} \mathrm{RProb}_R(\mathcal{P} \cup \{\!\{Adv_i\phi\}\!\}, \downarrow ok) = \; & \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok) + (1 - \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok)) \times \\ & \textstyle\sum_{k=1}^{n_i} p_k^i \cdot \mathrm{Prob}_{R_i}((\mathcal{P}, \phi), w_k^i) \end{aligned}$$

Note that thanks to our lemma on maximal resolutions, we can in fact suppose that $R_1 = R_2$ since $\mathrm{Prob}_{R_1}((\mathcal{P}, \phi), w') = \mathrm{Prob}_{R_2}((\mathcal{P}, \phi), w')$ for all w'. Let us take $\mathsf{B}_\ell(R) = R_1$. Thus, we obtain that:

$$\begin{aligned} \mathrm{RProb}_R(\mathcal{P} \cup \{\!\{Adv\phi\}\!\}, \downarrow ok) = \; & \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok) + (1 - \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok)) \times \\ & (p \cdot \textstyle\sum_{k=1}^{n_1} p_k^1 \cdot \mathrm{Prob}_{\mathsf{B}_\ell(R)}((\mathcal{P}, \phi), w_k^1) + \\ & (1-p) \cdot \textstyle\sum_{k=1}^{n_2} p_k^2 \cdot \mathrm{Prob}_{\mathsf{B}_\ell(R)}((\mathcal{P}, \phi), w_k^2)) \end{aligned}$$

Since $Tr^{ok}(Adv_1 +_p Adv_2, n) = \{\!\{(p \cdot p_k^1, w_k^1)\}\!\}_{k=1}^{n_1} \cup \{\!\{((1-p) \cdot p_k^2, w_k^2)\}\!\}_{k=1}^{n_2}$, we conclude.

- Name restriction on $Adv\phi$: In such a case, $Adv = \mathsf{new}\ a; Adv'$ with $Tr^{ok}(Adv, n) = Tr^{ok}(Adv'\{^b/_a\}, n)$ and $b \in \mathcal{N}_{pub}$ fresh. Moreover, by definition:

$$\mathrm{RProb}_R(\mathcal{P} \cup \{\!\!\{Adv\phi\}\!\!\}, \downarrow ok) = \mathrm{RProb}_R(\mathcal{P} \cup \{\!\!\{Adv'\{^b/_a\}\phi\}\!\!\}, \downarrow ok)$$

  By applying the inductive hypothesis on $\mathcal{P} \cup \{\!\!\{Adv'\{^b/_a\}\phi\}\!\!\}$, we directly conclude.

- Conditional branching on $Adv\phi$. We focus on the case where the transition corresponds to the rule Then (the case of the rule Else is similar). Thus $Adv = \mathsf{if}\ u = v\ \mathsf{then}\ Adv_1\ \mathsf{else}\ Adv_2$ and $Tr^{ok}(\mathsf{if}\ u = v\ \mathsf{then}\ Adv_1\ \mathsf{else}\ Adv_2, n) = \{\!\!\{(p_k^1, (u \stackrel{?}{=} v).w_k^1)\}\!\!\}_{k=1}^{n_1} \cup \{\!\!\{(p_k^2, (u \stackrel{?}{\neq} v).w_k^2)\}\!\!\}_{k=1}^{n_2}$. Since the rule Then was applied, we have that $u\phi \doteq v\phi$. Hence, for all $k \in \{1, \ldots, n_2\}$, $\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P}, \phi), (u \stackrel{?}{\neq} v).w_k^2) = 0$ and for all $k \in \{1, \ldots, n_1\}$, $\mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P}, \phi), w_k^1) = \mathrm{Prob}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^\ell)}((\mathcal{P}, \phi), (u \stackrel{?}{=} v).w_k^1)$. By applying our inductive hypothesis on $\mathcal{P} \cup \{\!\!\{Adv_1\phi\}\!\!\}$, we directly conclude.

- Internal communication with output on $Adv\phi$ and input on $\mathcal{P}$: In such a case, $Adv = \mathsf{out}(u, v); Adv'$ and $Tr^{ok}(Adv, n) = \{\!\!\{(p_i, (u \stackrel{?}{\neq} ok).in(u, v).w_i)\}\!\!\}_{i=1}^m \cup \{\!\!\{(1, u \stackrel{?}{=} ok)\}\!\!\}$ when $Tr^{ok}(Adv', n) = \{\!\!\{(p_i, w_i)\}\!\!\}_{i=1}^m$. Moreover, $\mathcal{P} = \mathcal{P}' \cup \{\!\!\{\mathsf{in}(c, x); P\}\!\!\}$ with $u\phi \doteq c$. Finally, we deduce that $D = \delta_{\mathcal{Q} \cup \{\!\!\{Adv'\phi\}\!\!\}}$ where $\mathcal{Q} = \mathcal{P}' \cup \{\!\!\{P\{^{v\phi}/_x\}\}\!\!\}$. Hence, by definition, we deduce that:

$$\mathrm{RProb}_R(\mathcal{P} \cup \{\!\!\{Adv\phi\}\!\!\}, \downarrow ok) = \mathrm{RProb}_R(\mathcal{Q} \cup \{\!\!\{Adv'\phi\}\!\!\}, \downarrow ok)$$

  Note that since $\mathcal{P} \cup Adv\phi \notin \downarrow ok$, we know that $ok \not\stackrel{?}{\neq} c$ and so $ok \neq c$. Thus, by definition of the labeled semantics, we have $(\mathcal{P}, \phi) \xrightarrow{(ok \stackrel{?}{\neq} u).in(u,v)} (Q, \phi)$. By applying our inductive hypothesis, we deduce that there exist a scheduler R_ℓ such that

$$\begin{aligned}\mathrm{RProb}_R(\mathcal{Q} \cup \{\!\!\{Adv'\phi\}\!\!\}, \downarrow ok) = \ & \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{Q}, \downarrow ok) + (1 - \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{Q}, \downarrow ok)) \times \\ & \textstyle\sum_{(\alpha, w) \in Tr^{ok}(Adv', |dom(\phi)|)} \alpha \cdot \mathrm{Prob}_{R_\ell}((\mathcal{Q}, \phi), w)\end{aligned}$$

  Recall that $ok \neq c$. Hence, by definition of purely probabilisitic processes, $\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{Q}, \downarrow ok) = \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok)$.

  By taking the scheduler $\mathsf{B}_\ell(R)$ that connect $(\mathcal{P}, \phi)$ to $(\mathcal{Q}, \phi)$ by the transitions $(\mathcal{P}, \phi) \xrightarrow{in(u,v)} (\mathcal{Q}, \phi)$ and then executes R_ℓ, we deduce that for all $i \in \{1, \ldots, m\}$, $\mathrm{Prob}_{R_\ell}((\mathcal{Q}, \phi), w_i) = \mathrm{Prob}_{\mathsf{B}_\ell(R)}((\mathcal{P}, \phi), (ok \stackrel{?}{\neq} u).in(u, v).w)$ which allows us to conclude.

- Internal communication with input on $Adv\phi$ and output on $\mathcal{P}$: In such a case, $Adv = \mathsf{in}(u, x); Adv'$ and $Tr^{ok}(Adv, n) = \{\!\!\{(p_i, (u \stackrel{?}{\neq} ok).out(u, \mathsf{ax}_{n+1}).w_i)\}\!\!\}_{i=1}^m$ when $Tr^{ok}(Adv', n{+}1) = \{\!\!\{(p_i, w_i)\}\!\!\}_{i=1}^m$. Moreover, $\mathcal{P} = \mathcal{P}' \cup \{\!\!\{\mathsf{out}(c, v); P\}\!\!\}$ with $u\phi \doteq c$. Finally, we deduce that $D = \delta_{\mathcal{Q} \cup \{\!\!\{Adv'\phi'\}\!\!\}}$ where $\mathcal{Q} = \mathcal{P}' \cup \{\!\!\{P\}\!\!\}$ and $\phi' = \phi\{\mathsf{ax}_{n+1} \mapsto v\}$. Hence, by definition, we deduce that:

$$\mathrm{RProb}_R(\mathcal{P} \cup \{\!\!\{Adv\phi\}\!\!\}, \downarrow ok) = \mathrm{RProb}_R(\mathcal{Q} \cup \{\!\!\{Adv'\phi'\}\!\!\}, \downarrow ok)$$

Note that since $\mathcal{P} \cup Adv\phi \notin \downarrow ok$, we know that $ok \not\doteq c$ and so $ok \neq c$. Thus, by definition of the labeled semantics, we have $(\mathcal{P}, \phi) \xrightarrow{(ok \overset{?}{\neq} u).out(u, \mathsf{ax}_n+1)} \delta_{(Q,\phi')}$. By applying our inductive hypothesis, we deduce that there exists a scheduler R_ℓ such that

$$\begin{array}{rl} \mathrm{RProb}_R(\mathcal{Q} \cup \{\!\{Adv'\phi'\}\!\}, \downarrow ok) = & \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{Q}, \downarrow ok) + (1 - \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{Q}, \downarrow ok)) \times \\ & \sum_{(\alpha,w) \in Tr^{ok}(Adv', |dom(\phi')|)} \alpha \cdot \mathrm{Prob}_{R_\ell}((\mathcal{Q}, \phi'), w) \end{array}$$

Recall that $ok \neq c$. Hence, by definition of purely probabilisitic processes, $\mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{Q}, \downarrow ok) = \mathrm{RProb}_{\mathcal{R}_{\mathsf{nr}}(\mathsf{N}^o)}(\mathcal{P}, \downarrow ok)$.

By taking the scheduler $\mathsf{B}_\ell(R)$ that connect $(\mathcal{P}, \phi)$ to $(\mathcal{Q}, \phi')$ by the transition $(\mathcal{P}, \phi) \xrightarrow{out(u, \mathsf{ax}_{n+1})} (\mathcal{Q}, \phi')$ and then executes R_ℓ, we deduce that for all $i \in \{1, \ldots, m\}$, $\mathrm{Prob}_{R_\ell}((\mathcal{Q}, \phi'), w_i) = \mathrm{Prob}_{\mathsf{B}_\ell(R)}((\mathcal{P}, \phi), (ok \overset{?}{\neq} u).out(u, \mathsf{ax}_{n+1}).w_i)$ which allows us to conclude.

$\square$