Information and Computation 249 (2016) 76–109

Contents lists available at ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

A general SOS theory for the specification of probabilistic transition systems

Pedro R. D'Argenio [a,*], Daniel Gebler [b], Matias David Lee [a,1]

[a] FaMAF, Universidad Nacional de Córdoba – CONICET, Ciudad Universitaria, X5000HUA – Córdoba, Argentina
[b] Dept. of Computer Science, VU University Amsterdam, De Boelelaan 1081a, NL-1081 HV Amsterdam, The Netherlands

ARTICLE INFO

Article history:
Received 2 February 2015
Received in revised form 11 November 2015
Available online 17 March 2016

Keywords:
SOS
Probabilistic transition systems
Bisimulation
Congruence
Rule format
Full abstraction

ABSTRACT

This article focuses on the formalization of the structured operational semantics approach for languages with primitives that introduce probabilistic and non-deterministic behavior. We define a general theoretic framework and present the $nt\mu f\theta/nt\mu x\theta$ rule format that guarantees that bisimulation equivalence (in the probabilistic setting) is a congruence for any operator defined in this format. We show that the bisimulation is fully abstract w.r.t. the $nt\mu f\theta/nt\mu x\theta$ format and (possibilistic) trace equivalence in the sense that bisimulation is the coarsest congruence included in trace equivalence for any operator definable within the $nt\mu f\theta/nt\mu x\theta$ format (in other words, bisimulation is the smallest congruence relation guaranteed by the format). We also provide a conservative extension theorem and show that languages that include primitives for exponentially distributed time behavior (such as IMC and Markov automata based language) fit naturally within our framework.

1. Introduction

Structural operational semantics (SOS for short) [1] is a powerful tool to provide semantics to programming languages. In SOS, process behavior is described using transition systems and the behavior of a composite process is given in terms of the behavior of its components. SOS has been formalized using an algebraic framework as *Transition Systems Specifications (TSS)* [2–6, etc.]. Basically, a TSS contains a signature, a set of actions or labels, and a set of rules. The signature defines the terms in the language. The set of actions represents all possible activities that a process (i.e., a term over the signature) can perform. The rules define how a process should behave (i.e., perform certain activities) in terms of the behavior of its subprocesses, that is, the rules define compositionally the transition system associated to each term of the language. A particular focus of these formalizations was to provide a meta-theory that ensures a diversity of semantic properties by simple inspection on the form of the rules. Thus, there are results on congruences and full abstraction, conservative extension, security, etc. (See [7,6,8] for overviews and references therein.)

In this article we focus on congruence and full abstraction. A congruence theorem guarantees that whenever the rules of a TSS are in a particular format, then a designated equivalence relation is preserved by every context in the signature of such TSS. Thus, for instance, strong bisimulation equivalence [9] is a congruence on any TSS in the *ntyft/ntyxt* format [4]. Full abstraction is a somewhat dual result. An equivalence relation is fully abstract with respect to a language and a given equivalence relation $\equiv$ if it is the largest relation included in $\equiv$ that is a congruence for all operators in the language [10].

* Corresponding author.
E-mail addresses: dargenio@famaf.unc.edu.ar (P.R. D'Argenio), e.d.gebler@vu.nl (D. Gebler), lee@famaf.unc.edu.ar, matias-david.lee@ens-lyon.fr (M.D. Lee).
[1] Current address: LIP, Université de Lyon, CNRS, Ecole Normale Supérieure de Lyon, INRIA, Université Claude-Bernard Lyon 1, France.

http://dx.doi.org/10.1016/j.ic.2016.03.009
0890-5401/

This notion can be straightforwardly extended to a TSS format by considering *all* definable languages in such format: an equivalence relation is fully abstract with respect to a particular format and an equivalence relation $\equiv$ if it is the largest relation included in $\equiv$ that is a congruence for all operators whose semantics is defined by a TSS in that format [10]. For example, strong bisimilarity is fully abstract w.r.t. the *ntyft/ntyxt* format [4] but not w.r.t. the *tyft/tyxt* format [2] or the GSOS format [3].

The introduction of probabilistic process algebras [11–13, etc.] motivated the need for a theory of structural operational semantics to define *probabilistic* transition systems. Previous to the introduction of our format [14], few results have appeared in this direction [15–18] presenting congruence theorems for (probabilistic) bisimilarity [19,20], but no full abstraction result. All previously mentioned studies consider transitions in the form of a quadruple denoted by $t \xrightarrow{a,q} t'$, where t and t' are terms in the language, a is an action or label, and $q \in (0,1]$ is a probability value. A transition of that form denotes that term t can perform an action a and with probability q continue with the execution of t'. Moreover, it is required that $\pi_{t,a}$, defined by $\pi_{t,a}(t') = \sum_{t \xrightarrow{a,q} t'} q$, is a probability distribution. (This interpretation corresponds to the reactive view, it varies under the generative view [12].) This notation introduces several problems. The first one is that the transition relation cannot be treated as a set because two different derivations may yield the same quadruple. This requires artifacts like multisets or bookkeeping indexes. The second problem is that formats need to be defined jointly on a set of rules rather than a single rule to ensure that $\pi_{t,a}$ is a probability distribution. (Notice that $\pi_{t,a}$ depends on a *set* of transitions which are obtained using different rules.)

Rather than following this approach, we directly represent transitions as a triple $t \xrightarrow{a} \pi_{t,a}$. Thus, a single triple contains the complete information of the probabilistic jump. Moreover, this representation also allows for non-determinism in the sense that if $t \xrightarrow{a} \pi$ and $t \xrightarrow{a} \pi'$ not necessarily $\pi = \pi'$ as requested by reactive systems. Hence, our *probabilistic transition system specifications (PTSS)* define objects very much like Segala's probabilistic automata [21]. More precisely we represent transitions using two different sorts, one that represent states and the other distributions. Thus a labeled transition $t \xrightarrow{a} \theta$ goes from one *state term* t to a *distribution term* θ. If θ is a closed term, then its interpretations $[\![\theta]\!]$ is a probability distribution on state terms. By having a two-sorted signature, operations can be parameterized on distributions, and moreover, we can neatly express open terms in the rules of the PTSS. So, each (probabilistic) transition $t \xrightarrow{a} \theta$ is obtained as a consequence of a single derivation in our PTSSs, and hence formats focus on single rules (as it is the case for non-probabilistic TSSs). This significantly eases the inspection of the format. In addition, a byproduct of this choice is that the proof strategies for the majority of the lemmas and theorems of this article are much the same as those for their non-probabilistic relatives. We observe that this way of representing transitions in rules for process algebra has already appeared in [22], it is also used in the Segala-GSOS format [16] and it is pretty much related to bialgebraic approaches to SOS [16,23].

More precisely, the contributions on this article are:

1. We introduce PTSS with negative and quantitative premises and the possibility of lookahead (Section 3). It uses a two-sorted term algebra to represent the language, where the *distribution* sort is aimed to be interpreted as a probability distribution on the *state* sort. (Section 2.)
2. We use here the most general method to give meaning to PTSSs: we adapt the definition of least 3-valued stable models [5,24] to our setting and only limit to complete PTSSs when a 2-valued model is required. (Section 3.)
3. We introduce the *ntμfθ/ntμxθ* format in Section 4 and show through carefully crafted examples that each of the restrictions of the format is effectively needed to ensure that bisimulation is a congruence. Moreover, we present a shorthand notation that significantly simplifies the verification of the restrictions, making the format almost as easy to check as the *ntyft/ntyxt* format [4,5].
4. We give a detailed proof that bisimulation is a congruence for any operator defined within the *ntμfθ/ntμxθ* format as long as every rule is well-founded. (Section 5.)
5. We adapt the concept of *conservative extension* [2,8] to our probabilistic setting. Conservative extensions allow to modularly extend a language preserving all the behavioral properties of the original terms. We also provide a general theorem that guarantees that an extension is conservative. This is presented in Section 6.
6. We show that bisimulation equivalence is fully abstract with respect to the *ntμfθ/ntμxθ* format and trace equivalence, that is, it is the coarsest congruence w.r.t. any operator definable in (complete) *ntμfθ/ntμxθ* PTSSs (Section 7).
7. Finally, we discuss some expressiveness issues. Notably, we show that the theory extends immediately to IMCs [25] and Markov automata [26]. We also provide a format that guarantees that the model of the PTSS is indeed a Markov automaton. (Section 8.)

Besides reporting the full proofs, this article extends, improves and correct the work already presented in [14]. In fact, several mistakes were inadvertently introduced there. Some modifications have already been introduced in [27] but also there we have introduced some error. That is why we briefly report the differences and corrections in Appendix A.

2. Preliminaries

Let $S = \{s, d\}$ be a set denoting two sorts. Elements of sort $s \in S$ are intended to represent states in the transition system, while elements of sort $d \in S$ will represent distributions over states. We let σ range over S.

An *S-sorted signature* is a structure (F, ar), where (i) F is a set of *function names*, and (ii) $\mathsf{ar}\colon F \to ((S^* \cup S^\omega) \times S)$ is the *arity function*. The rank of $f \in F$ is the number of arguments of f, defined by $\mathsf{rk}(f) = n$ if $\mathsf{ar}(f) = \sigma_1 \dots \sigma_n \to \sigma$, and $\mathsf{rk}(f) = \omega$ if $\mathsf{ar}(f) \in (S^\omega \times S)$. (We write "$\sigma_1 \dots \sigma_n \to \sigma$" instead of "$(\sigma_1 \dots \sigma_n, \sigma)$" to highlight that function f maps to sort σ.) In particular, function f is a *constant* if $\mathsf{rk}(f) = 0$. Moreover, we denote with F_σ the subset of functions names in F that map into sort σ. To simplify the presentation we will write an S-sorted signature (F, ar) as a pair of disjoint signatures (Σ_s, Σ_d) where Σ_s is the set of operations that map to s and Σ_d is the set of operations that map to d.

Let $\mathcal{V}$ and $\mathcal{D}$ be two infinite sets of s-sorted and d-sorted variables, respectively, where $\mathcal{V}, \mathcal{D}, F$ are all mutually disjoint. We use x, y, z (with possible sub- or super-scripts) to range over $\mathcal{V}$, μ, ν to range over $\mathcal{D}$ and ζ to range over $\mathcal{V} \cup \mathcal{D}$.

Definition 1. Let Σ_s and Σ_d be two signatures as before and let $V \subseteq \mathcal{V}$ and $D \subseteq \mathcal{D}$. We simultaneously define the sets of *state terms* $T(\Sigma_s, V, D)$ and *distribution terms* $T(\Sigma_d, V, D)$ as the smallest sets satisfying:

(i) $V \subseteq T(\Sigma_s, V, D)$;
(ii) $D \subseteq T(\Sigma_d, V, D)$;
(iii) $f(\xi_1, \cdots, \xi_{\mathsf{rk}(f)}) \in T(\Sigma_\sigma, V, D)$, if $\mathsf{ar}(f) = \sigma_1 \dots \sigma_n \dots \to \sigma$ and $\xi_i \in T(\Sigma_{\sigma_i}, V, D)$.

We let $\mathbb{T}(\Sigma) = T(\Sigma_s, \mathcal{V}, \mathcal{D}) \cup T(\Sigma_d, \mathcal{V}, \mathcal{D})$ denote the set of all *open terms* and distinguish the sets $\mathbb{T}(\Sigma_s) = T(\Sigma_s, \mathcal{V}, \mathcal{D})$ of *open state terms* and $\mathbb{T}(\Sigma_d) = T(\Sigma_d, \mathcal{V}, \mathcal{D})$ of *open distribution terms*. Similarly, we let $T(\Sigma) = T(\Sigma_s, \emptyset, \emptyset) \cup T(\Sigma_d, \emptyset, \emptyset)$ denote the set of all *closed terms* and distinguish the sets $T(\Sigma_s) = T(\Sigma_s, \emptyset, \emptyset)$ of *closed state terms* and $T(\Sigma_d) = T(\Sigma_d, \emptyset, \emptyset)$ of *closed distribution terms*. We let $t, t', t_1, \dots$ range over state terms, $\theta, \theta', \theta_1, \dots$ range over distribution terms, and $\xi, \xi', \xi_1, \dots$ range over any kind of terms. With $Var(\xi) \subseteq \mathcal{V} \cup \mathcal{D}$ we denote the set of variables occurring in term ξ.

Let $\Delta(T(\Sigma_s))$ denote the set of all (discrete) probability distributions on $T(\Sigma_s)$. We let π range over $\Delta(T(\Sigma_s))$. For each $t \in T(\Sigma_s)$, let $\delta_t \in \Delta(T(\Sigma_s))$ denote the *Dirac distribution*, i.e., $\delta_t(t) = 1$ and $\delta_t(t') = 0$ if t and t' are not syntactically equal. For $X \subseteq T(\Sigma_s)$ we define $\pi(X) = \sum_{t \in X} \pi(t)$. The convex combination $\sum_{i \in I} p_i \pi_i$ of a family $\{\pi_i\}_{i \in I}$ of probability distributions with $p_i \in (0,1]$ and $\sum_{i \in I} p_i = 1$ is defined by $(\sum_{i \in I} p_i \pi_i)(t) = \sum_{i \in I}(p_i \pi_i(t))$.

The type of signatures we consider has a particular construction. We start from a signature Σ_s of finitary functions mapping into sort s and construct the signature Σ_d of functions mapping into d as follows. For each $f \in F_s$ we include a function symbol $\boldsymbol{f} \in F_d$ with $\mathsf{ar}(\boldsymbol{f}) = d \dots d \to d$ and $\mathsf{rk}(\boldsymbol{f}) = \mathsf{rk}(f)$. We call $\boldsymbol{f}$ the *probabilistic lifting* of f. (We use boldface fonts to indicate that a function in Σ_d is the probabilistic lifting of another in Σ_s.) Moreover Σ_d may include any of the following additional operators:

- δ with arity $\mathsf{ar}(\delta) = s \to d$ and
- $\bigoplus_{i \in I}[p_i]\_$ with I being a finite or countable infinite index set, $\sum_{i \in I} p_i = 1$, $p_i \in (0,1]$ for all $i \in I$, and $\mathsf{ar}\left(\bigoplus_{i \in I}[p_i]\_\right) = d^{|I|} \to d$.

Notice that if I is countably infinite, $\bigoplus_{i \in I}[p_i]\_$ is an infinitary operator. This is the only class of infinitary operators that we allow. We write $\theta_1 \oplus_{p_1} \theta_2$ instead of $\bigoplus_{i \in \{1,2\}}[p_i]\theta_i$ whenever the index set I has exactly two elements.

Operators δ and $\bigoplus_{i \in I}[p_i]\_$ are used to construct discrete probability functions of countable support: $\delta(t)$ is interpreted as a distribution that assigns probability 1 to the state term t and probability 0 to any other term t' (syntactically) different from t, and $\bigoplus_{i \in I}[p_i]\theta_i$ represents a distribution that weights with p_i the distribution represented by the term θ_i. Moreover, a probabilistically lifted operator $\boldsymbol{f}$ is interpreted by properly lifting the probabilities of the operands to terms composed with the operator f.

Formally, the algebra associated with a probabilistically lifted signature $\Sigma = (\Sigma_s, \Sigma_d)$ is defined as follows. For sort s, it is the freely generated algebraic structure $T(\Sigma_s)$. For sort d, it is defined by the carrier $\Delta(T(\Sigma_s))$ and the interpretation $[\![\ ]\!] : T(\Sigma_d) \to \Delta(T(\Sigma_s))$ defined by:

- $[\![\delta(t)]\!] = \delta_t$ for all $t \in T(\Sigma_s)$.
- $[\![\bigoplus_{i \in I}[p_i]\ \theta_i]\!] = \sum_{i \in I} p_i [\![\theta_i]\!]$ for $\{\theta_i \mid i \in I\} \subseteq T(\Sigma_d)$,
- $[\![\boldsymbol{f}(\theta_1, \dots, \theta_{\mathsf{rk}(f)})]\!](f(\xi_1, \dots, \xi_{\mathsf{rk}(f)})) = \begin{cases} \prod_{\sigma_i = s} [\![\theta_i]\!](\xi_i) & \text{if for all } \sigma_j = d, \theta_j = \xi_j \\ 0 & \text{otherwise} \end{cases}$

Here it is assumed that $\prod \emptyset = 1$. Notice that in the semantics of a lifted function $\boldsymbol{f}$, the big product only considers the distributions related to the s-sorted positions in f, while the distribution terms corresponding to the d-sorted positions in f should match exactly to the parameters of $\boldsymbol{f}$. We remark that if f were infinitary, then the semantics of $\boldsymbol{f}$ (through an appropriate definition) would introduce continuous distributions.

A *substitution* ρ is a map $\mathcal{V} \cup \mathcal{D} \to \mathbb{T}(\Sigma)$ such that $\rho(x) \in \mathbb{T}(\Sigma_s)$, for all $x \in \mathcal{V}$, and $\rho(\mu) \in \mathbb{T}(\Sigma_d)$, for all $\mu \in \mathcal{D}$. A substitution is closed if it maps each variable to a closed term. A substitution extends to a mapping from terms to terms as usual.

Finally, we remark a general property of distribution terms: let $f \in \Sigma_s$ with $\mathsf{ar}(f) = \sigma_1 \dots \sigma_n \to s$, and let $\sigma_j = s$; then $\boldsymbol{f} \in \Sigma_d$ is distributive w.r.t. $\oplus$ in the position j, i.e.

$$[\![\rho(\boldsymbol{f}(\ldots,\xi_{j-1},\textstyle\bigoplus_{i\in I}[p_i]\theta_i,\xi_{j+1},\ldots))]\!] = [\![\rho(\textstyle\bigoplus_{i\in I}[p_i]\boldsymbol{f}(\ldots,\xi_{j-1},\theta_i,\xi_{j+1},\ldots))]\!]$$

for any closed substitution ρ. The proof follows straightforwardly from the definition of $[\![\_]\!]$. However, notice that $\boldsymbol{f}$ *does not* distribute w.r.t. $\oplus$ in a position k such that $\sigma_k = d$.

Example 1. We define a comprehensive signature that sets the framework of our running example. We assume the existence of a set A of action labels. Let $\Sigma = (\Sigma_s, \Sigma_d)$ be a probabilistically lifted signature such that Σ_s is a signature that contains:

- constants 0 (stop process) and ε (skip process) of sort s, i.e., $\mathsf{ar}(0) = \mathsf{ar}(\varepsilon) = s$;
- a family of unary probabilistic prefix operators $a.\_$ with $a \in A$ and $\mathsf{ar}(a) = d \to s$,
- binary operators $+$ (alternative composition or sum), $;$ (sequential composition), and, for each $B \subseteq A$, $||_B$ (parallel composition) with $\mathsf{ar}(+) = \mathsf{ar}(;) = \mathsf{ar}(||_B) = ss \to s$; and
- a family of unary operators $\mathsf{fs}_F(\_)$ and $\mathsf{sc}_F(\_)$ for each $F \subseteq A$, with $\mathsf{ar}(\mathsf{fs}_F) = \mathsf{ar}(\mathsf{sc}_F) = s \to s$, that we call, respectively, *faulty state* and *safe controller*.

Moreover, Σ_d contains δ, all binary operators $\oplus_p$, and the lifted operators, which are as follows:

- constants, $\mathbf{0}$ and $\boldsymbol{\varepsilon}$ with $\mathsf{ar}(\mathbf{0}) = \mathsf{ar}(\boldsymbol{\varepsilon}) = d$;
- the family of unary operators $\boldsymbol{a}.\_$, with $a \in A$ and $\mathsf{ar}(\boldsymbol{a}) = d \to d$,
- binary operators $\boldsymbol{+}$, $\boldsymbol{;}$, and, for each $B \subseteq A$, $\boldsymbol{||_B}$ with $\mathsf{ar}(\boldsymbol{+}) = \mathsf{ar}(\boldsymbol{;}) = \mathsf{ar}(\boldsymbol{||_B}) = dd \to d$, and
- the unary operators $\mathbf{fs}_{\boldsymbol{F}}(\_)$ and $\mathbf{sc}_{\boldsymbol{F}}(\_)$ with $F \subseteq A$ and $\mathsf{ar}(\mathbf{fs}_{\boldsymbol{F}}) = \mathsf{ar}(\mathbf{sc}_{\boldsymbol{F}}) = d \to d$.

The intended meaning of the probabilistic prefix operator $a.\theta$ is that this term can perform action a and move to term t with probability $[\![\theta]\!](t)$. Operator $t\,||_B\,t'$ is a CSP-like parallel composition where actions in B are forced to synchronize and all other actions should be performed independently. The rest of the operators, with the exception of fs_F and sc_F, have the usual meaning.

The set $F \subseteq A$ in fs_F and sc_F contains the set of all actions that are consider a failure. $\mathsf{fs}_F(t)$ checks if t is a process that inevitably ends up executing a failure action in F with some positive probability. This is indicated by letting $\mathsf{fs}_F(t)$ successfully terminate. That is, $\mathsf{fs}_F(t)$ successfully terminates if for any possible resolution of the non-determinism, the probability that t eventually reaches a state that executes a failure action in F is greater than 0. Otherwise it behaves as the stop process. $\mathsf{sc}_F(t)$ controls the process t so that it never reaches a state in which it will inevitably end up executing a failure action in F. It preserves all other behavior. $\square$

Notice that the same Dirac distribution of a closed state term can be written in several ways using the operator δ or the probabilistically lifted signature. Thus the terms $\delta(a.\boldsymbol{\varepsilon}\,||_B(a.\boldsymbol{\varepsilon}+b.\boldsymbol{\varepsilon}))$, $\boldsymbol{a.\varepsilon}\boldsymbol{||_B}\delta(a.\boldsymbol{\varepsilon}+b.\boldsymbol{\varepsilon})$, and $\boldsymbol{a.\varepsilon}\boldsymbol{||_B}(\boldsymbol{a.\varepsilon}\boldsymbol{+}\boldsymbol{b.\varepsilon})$ represent the same distribution. Indeed, it is not difficult to show that $\delta_{a.\boldsymbol{\varepsilon}\,||_B(a.\boldsymbol{\varepsilon}+b.\boldsymbol{\varepsilon})} = [\![\delta(a.\boldsymbol{\varepsilon}\,||_B(a.\boldsymbol{\varepsilon}+b.\boldsymbol{\varepsilon}))]\!] = [\![\boldsymbol{a.\varepsilon}\boldsymbol{||_B}\delta(a.\boldsymbol{\varepsilon}+b.\boldsymbol{\varepsilon})]\!] = [\![\boldsymbol{a.\varepsilon}\boldsymbol{||_B}(\boldsymbol{a.\varepsilon}\boldsymbol{+}\boldsymbol{b.\varepsilon})]\!]$. However, the Dirac operator δ is necessary to construct *open* distribution terms. The term $\delta(x)$ cannot be written in another manner, since the instance of the state term variable x is not yet known.

3. Probabilistic transition system specifications

A (probabilistic) transition relation prescribes which possible activity can be performed by a term in a signature. Such activity is described by the label of the action and a probability distribution on terms that indicates the probability to reach a particular new term. We will follow the probabilistic automata style of probabilistic transitions [21] which are a generalization of the so-called reactive model [20].

Definition 2 *(PTS).* A *probabilistic labeled transition system* (PTS) is a triple $(T(\Sigma_s), A, \to)$, where $\Sigma = (\Sigma_s, \Sigma_d)$ is a probabilistically lifted signature, A is a countable set of actions, and $\to \subseteq T(\Sigma_s) \times A \times \Delta(T(\Sigma_s))$, is a transition relation.

We write $t \xrightarrow{a} \pi$ for $(t, a, \pi) \in \to$.

Transition relations are usually defined by means of structured operational semantics in Plotkin's style [1]. Algebraic characterizations of this style were provided in [2,4,5] where the term *transition system specification* was used and which we adopt in our paper. In fact, based on these works, we define *probabilistic transition system specifications*.

Definition 3 *(PTSS).* A *probabilistic transition system specification* (PTSS) is a triple $P = (\Sigma, A, R)$ where Σ is a probabilistically lifted signature, A is a set of labels, and R is a set of rules of the form:

$$\frac{\{t_k \xrightarrow{a_k} \theta_k \mid k \in K\} \cup \{t_l \stackrel{b_l}{\not\longrightarrow} \mid l \in L\} \cup \{\theta_j(T_j) \bowtie_j q_j \mid j \in J\}}{t \xrightarrow{a} \theta}$$

where K, L, J are index sets, $t, t_k, t_l \in \mathbb{T}(\Sigma_s)$, $a, a_k, b_l \in A$, $T_j \subseteq \mathbb{T}(\Sigma_s)$, $\bowtie_j \in \{>, \geq, <, \leq\}$, $q_j \in [0,1]$ and $\theta_j, \theta_k, \theta \in \mathbb{T}(\Sigma_d)$.

Table 1
Rules for the process algebra of Example 1 ($Y \subseteq \mathcal{V}$ is a countably infinite set, $x \notin Y$, and $\{\checkmark\} \cap A = \emptyset$).

$$\frac{}{\varepsilon \xrightarrow{\checkmark} \mathbf{0}} \qquad \frac{}{a.\mu \xrightarrow{a} \mu} \qquad \frac{x \xrightarrow{a} \mu}{x + y \xrightarrow{a} \mu} \qquad \frac{y \xrightarrow{a} \mu}{x + y \xrightarrow{a} \mu}$$

$$\frac{x \xrightarrow{a} \mu}{x;\, y \xrightarrow{a} \mu\mathbf{;}\delta(y)}\ a \neq \checkmark \qquad \frac{x \xrightarrow{\checkmark} \mu \quad y \xrightarrow{a} \mu'}{x;\, y \xrightarrow{a} \mu'}$$

$$\frac{x \xrightarrow{a} \mu}{x \,||_B\, y \xrightarrow{a} \mu \,\mathbf{||_B}\, \delta(y)}\ a \notin B \cup \{\checkmark\} \qquad \frac{y \xrightarrow{a} \mu}{x \,||_B\, y \xrightarrow{a} \delta(x) \,\mathbf{||_B}\, \mu}\ a \notin B \cup \{\checkmark\}$$

$$\frac{x \xrightarrow{a} \mu \quad y \xrightarrow{a} \mu'}{x \,||_B\, y \xrightarrow{a} \mu \,\mathbf{||_B}\, \mu'}\ a \in B \cup \{\checkmark\}$$

$$\frac{x \xrightarrow{a} \mu \quad \mu(Y) > 0 \quad \{\mathsf{fs}_F(y) \stackrel{\checkmark}{\not\longrightarrow} \mid y \in Y\}}{\mathsf{sc}_F(x) \xrightarrow{a} \mathbf{sc_F}(\mu)}\ a \notin F$$

$$\frac{x \xrightarrow{b} \mu \quad \{x \stackrel{a}{\not\longrightarrow} \mid a \notin F\}}{\mathsf{fs}_F(x) \xrightarrow{\checkmark} \mathbf{0}}\ b \in F \qquad \frac{x \xrightarrow{a} \mu \quad \{\mathsf{sc}_F(x) \stackrel{a'}{\not\longrightarrow} \mid a' \in A \cup \{\checkmark\}\}}{\mathsf{fs}_F(x) \xrightarrow{\checkmark} \mathbf{0}}$$

Expressions of the form $t \xrightarrow{a} \theta$, $t \stackrel{a}{\not\longrightarrow}$, and $\theta(T) \bowtie p$ are called *positive literal*, *negative literal*, and *quantitative literal*, respectively. For any rule $r \in R$, literals above the line are called *premises*, notation $\text{prem}(r)$; the literal below the line is called *conclusion*, notation $\text{conc}(r)$. We denote with $\text{pprem}(r)$, $\text{nprem}(r)$, and $\text{qprem}(r)$ the sets of positive, negative, and quantitative premises of the rule r, respectively. A rule r without premises is called an *axiom*. In general, we allow the sets of positive, negative, and quantitative premises to be infinite.

Substitutions provide instances to the rules of a PTSS that, together with some appropriate machinery, allow us to define probabilistic transition relations. Given a substitution ρ, it extends to literals as follows:

$$\rho(t \stackrel{a}{\not\longrightarrow}) = \rho(t) \stackrel{a}{\not\longrightarrow} \qquad \rho(\theta(T) \bowtie p) = \rho(\theta)(\rho(T)) \bowtie p \qquad \rho(t \xrightarrow{a} \theta) = \rho(t) \xrightarrow{a} \rho(\theta)$$

We say that r' is a (closed) instance of a rule r if there is a (closed) substitution ρ so that $r' = \rho(r)$. We say that ρ is a *proper substitution of* r if for all quantitative premises $\theta(T) \bowtie p$ of r and all $t \in T$, $[\![\rho(\theta)]\!](\rho(t)) > 0$ holds. Thus, if ρ is proper, all terms in $\rho(T)$ are in the support of $[\![\rho(\theta)]\!]$. Proper substitutions avoid the introduction of spurious terms, i.e. terms that after a transition are reached with probability 0. We use only this kind of substitution in the paper.

Example 2. The rules for the process algebra of Example 1 are defined in Table 1. We assume that $\checkmark \notin A$. We denote with P_{sc} the PTSS defined by these rules. We only explain the rules for sc_F and fs_F since the other rules resemble their counterparts in a traditional non-probabilistic setting.

The rule for sc_F states that $\mathsf{sc}_F(t)$ is allowed to perform a non-failing step that t can perform as long as this step does not lead to an inevitable failure with non-zero probability. The first rule for fs_F states that $\mathsf{fs}_F(t)$ inevitably fails if it can only perform a failure action. The second rule sates that if $\mathsf{sc}_F(t)$ is not able to perform any action while t is, then it must be because t will inevitably fail with non-zero probability. This rule uses the lookahead embedded in the rule for sc_F to assess that, in the long run, t will eventually execute a failure action with some non-zero probability. In the following, we show that the interaction between the second rule of fs_F and the rule of sc_F through negative premises is not a problem and that this PTSS has a clearly defined semantics. □

In the rest of the paper, we will deal with models as *symbolic* transition relations in the set $T(\Sigma_s) \times A \times T(\Sigma_d)$ rather than the *concrete* transition relations in $T(\Sigma_s) \times A \times \Delta(T(\Sigma_s))$ required by a PTS. Hence we will mostly refer with the term "transition relation" to the symbolic transition relation. In any case, a symbolic transition relation induces always a unique concrete transition relation by interpreting every target distribution term as the distribution it defines; that is, the symbolic transition $t \xrightarrow{a} \theta$ is interpreted as the concrete transition $t \xrightarrow{a} [\![\theta]\!]$. If the symbolic transition relation turns out to be a model of a PTSS P, we say that the induced concrete transition relation defines a PTS associated to P.

However, first we need to define an appropriate notion of model. As has already been argued many times (e.g. [4,5,24]), transition system specifications with negative premises do not uniquely define a transition relation and different reasonable techniques may lead to incomparable models. For instance, the PTSS with the single constant f, set of labels $\{a, b\}$ and the two rules

$$\frac{f \stackrel{b}{\not\longrightarrow}}{f \xrightarrow{a} \boldsymbol{f}} \quad \text{and} \quad \frac{f \stackrel{a}{\not\longrightarrow}}{f \xrightarrow{b} \boldsymbol{f}}, \tag{1}$$

has two models that are justifiably compatible with the rules (so-called supported models [3,5,24]): $\{f \xrightarrow{a} \boldsymbol{f}\}$ and $\{f \xrightarrow{b} \boldsymbol{f}\}$.

An alternative view is to consider *3-valued models*. A 3-valued model partitions the set $T(\Sigma_s) \times A \times T(\Sigma_d)$ in three sets containing, respectively, the transition that are known to hold, that are known not to hold, and those whose validity is unknown. Thus, a 3-valued model can be presented as a pair $\langle \mathsf{CT}, \mathsf{PT}\rangle$ of transition relations $\mathsf{CT}, \mathsf{PT} \subseteq T(\Sigma_s) \times A \times T(\Sigma_d)$, with $\mathsf{CT} \subseteq \mathsf{PT}$, where CT is the set of transitions that *certainly* hold and PT is the set of transitions that *possibly* hold. So, transitions in $\mathsf{PT} \setminus \mathsf{CT}$ are those whose validity is unknown and transitions in $(T(\Sigma_s) \times A \times T(\Sigma_d)) \setminus \mathsf{PT}$ are those that certainly do not hold.

A 3-valued model $\langle \mathsf{CT}, \mathsf{PT}\rangle$ that is justifiably compatible with the proof system defined by a PTSS P is said to be *stable* for P. We will make clear what we mean by "justifiably compatible" in Definition 5.

Before formally defining the notions of proof and 3-valued stable model we introduce some notation. Given a transition relation $\mathsf{Tr} \subseteq T(\Sigma_s) \times A \times T(\Sigma_d)$, $t \xrightarrow{a} \theta$ *holds in* Tr, notation $\mathsf{Tr} \models t \xrightarrow{a} \theta$, if $t \xrightarrow{a} \theta \in \mathsf{Tr}$; $t \stackrel{a}{\not\longrightarrow}$ *holds in* Tr, notation $\mathsf{Tr} \models t \stackrel{a}{\not\longrightarrow}$, if for all $\theta \in T(\Sigma_d)$, $t \xrightarrow{a} \theta \notin \mathsf{Tr}$. A closed quantitative constraint $\theta(T) \bowtie p$ *holds in* Tr, notation $\mathsf{Tr} \models \theta(T) \bowtie p$, if $[\![\theta]\!](T) \bowtie p$. Notice that the satisfaction of a quantitative constraint does not depend on the transition relation. We nonetheless use this last notation as it turns out to be convenient. Given a set of literals H, we write $\mathsf{Tr} \models H$ if for all $\phi \in H$, $\mathsf{Tr} \models \phi$.

Definition 4 *(Proof).* Let $P = (\Sigma, A, R)$ be a PTSS. Let ψ be a positive literal and let H be a set of literals. A *proof* of a transition rule $\frac{H}{\psi}$ from P is a well-founded, upwardly branching tree where each node is a literal such that:

1. the root is ψ; and
2. if χ is a node and K is the set of nodes directly above χ, then one of the following conditions holds:
   (a) $K = \emptyset$ and $\chi \in H$, or
   (b) $\chi = (\theta(T) \bowtie p)$ is a closed quantitative literal such that $[\![\theta]\!](T) \bowtie p$ holds, or
   (c) $\frac{K}{\chi}$ is a valid substitution instance of a rule from R.

$\frac{H}{\psi}$ *is provable from* P, notation $P \vdash \frac{H}{\psi}$, if there exists a proof of $\frac{H}{\psi}$ from P.

Before, we said that a 3-valued stable model $\langle \mathsf{CT}, \mathsf{PT}\rangle$ for a PTSS P has to be *justifiably compatible* with the proof system defined by P. By "compatible" we mean that $\langle \mathsf{CT}, \mathsf{PT}\rangle$ has to be consistent with every provable rule. With "justifiable" we require that for each transition in CT and PT there is actually a proof that justifies it. More precisely, we require that (a) for every certain transition in CT there is a proof in P such that all negative hypotheses of the proof are known to hold (i.e. there is no possible transition in PT denying a negative hypothesis), and (b) for every possible transition in PT there is a proof in P such that all negative hypotheses possibly hold (i.e. there is no certain transition in CT denying a negative hypothesis). This is formally stated in the next definition.

Definition 5 *(3-valued stable model).* Let $P = (\Sigma, A, R)$ be a PTSS. A tuple $\langle \mathsf{CT}, \mathsf{PT}\rangle$ with $\mathsf{CT} \subseteq \mathsf{PT} \subseteq T(\Sigma_s) \times A \times T(\Sigma_d)$ is a *3-valued stable model* for P if for every closed positive literal ψ,

(a) $\psi \in \mathsf{CT}$ iff there is a set N of closed negative literals such that $P \vdash \frac{N}{\psi}$ and $\mathsf{PT} \models N$
(b) $\psi \in \mathsf{PT}$ iff there is a set N of closed negative literals such that $P \vdash \frac{N}{\psi}$ and $\mathsf{CT} \models N$.

The example above, in equation (1), has three 3-valued stable models: $\langle\{f \xrightarrow{a} \boldsymbol{f}\}, \{f \xrightarrow{a} \boldsymbol{f}\}\rangle$, $\langle\{f \xrightarrow{b} \boldsymbol{f}\}, \{f \xrightarrow{b} \boldsymbol{f}\}\rangle$, and $\langle\emptyset, \{f \xrightarrow{a} \boldsymbol{f}, f \xrightarrow{b} \boldsymbol{f}\}\rangle$. Notice that the last one is the model that contains *least information* in the sense that it is the one with most unknown transitions. Formally, a model $\langle \mathsf{CT}, \mathsf{PT}\rangle$ has *at most as much information as* $\langle \mathsf{CT}', \mathsf{PT}'\rangle$, if $\mathsf{CT} \subseteq \mathsf{CT}'$ and $\mathsf{PT} \supseteq \mathsf{PT}'$. It turns out that every PTSS has an (information-)least 3-valued stable model [24].[2]

In fact, the least 3-valued stable model of a PTSS can be constructed using induction. (We borrow this construction from [28,29].)

Lemma 1. *Let P be a PTSS. For each ordinal α, define the pair $\langle \mathsf{CT}_\alpha, \mathsf{PT}_\alpha\rangle$ as follows:*

- $\mathsf{CT}_0 = \emptyset$ *and* $\mathsf{PT}_0 = T(\Sigma_s) \times A \times T(\Sigma_d)$.
- *For every non-limit ordinal $\alpha > 0$, define:*

$$\mathsf{CT}_\alpha = \left\{ t \xrightarrow{a} \theta \mid \textit{for some set } N \textit{ of negative literals, } P \vdash \frac{N}{t \xrightarrow{a} \theta} \textit{ and } \mathsf{PT}_{\alpha-1} \models N \right\}$$

[2] Since every non-trivial closed transition rule $\frac{H}{\psi}$ provable in a PTSS can be rewritten as a rule such that H does not contains quantitative literals, the results about meaning of TSS of [5,24] can be easily restated and proved in our setting mutatis mutandis. Therefore and without further ado, we will credit these articles in respect to the results about meaning of PTSS with negative premises.

$$\mathsf{PT}_\alpha = \left\{ t \xrightarrow{a} \theta \mid \textit{for some set } N \textit{ of negative literals, } P \vdash \frac{N}{t \xrightarrow{a} \theta} \textit{ and } \mathsf{CT}_{\alpha-1} \models N \right\}$$

- *For every limit ordinal* α, *define*

$$\mathsf{CT}_\alpha = \bigcup_{\beta<\alpha} \mathsf{CT}_\beta \quad \textit{and} \quad \mathsf{PT}_\alpha = \bigcap_{\beta<\alpha} \mathsf{PT}_\beta$$

Then:

1. *if* $\beta \leq \alpha$, $\mathsf{CT}_\beta \subseteq \mathsf{CT}_\alpha$ *and* $\mathsf{PT}_\beta \supseteq \mathsf{PT}_\alpha$, *that is,* $\langle \mathsf{CT}_\beta, \mathsf{PT}_\beta \rangle$ *has at most as much information as* $\langle \mathsf{CT}_\alpha, \mathsf{PT}_\alpha \rangle$, *and*
2. *there is an ordinal* λ *such that* $\mathsf{CT}_\lambda = \mathsf{CT}_{\lambda+1}$ *and* $\mathsf{PT}_\lambda = \mathsf{PT}_{\lambda+1}$. *Moreover,* $\langle \mathsf{CT}_\lambda, \mathsf{PT}_\lambda \rangle$ *is the least 3-valued stable model for* P.

This result is shown in [29,28] for a non-probabilistic setting and using a slightly different definition of 3-valued models. (With minor changes the same proofs appearing in [29,28] apply to our setting). We remark that the first item of the lemma can be proved using transfinite induction on the lexicographic order of (α, β), and the second item follows using the Knaster–Tarski theorem.[3]

PTSSs with least 3-valued stable model that are also a 2-valued model are particularly interesting, since this model is actually the only 3-valued stable model [5,24].

Definition 6. A PTSS P is said to be *complete* if its least 3-valued stable model $\langle \mathsf{CT}, \mathsf{PT} \rangle$ satisfies that $\mathsf{CT} = \mathsf{PT}$ (i.e., the model is also 2-valued).

PTSSs not containing rules with negative premises as well as stratifiable PTSSs [14,4] are complete [5,24].

We associate a probabilistic transition system to each complete PTSS.

Definition 7. Let P be a complete PTSS and let $\langle \mathsf{Tr}, \mathsf{Tr} \rangle$ be its unique 3-valued stable model. We say that Tr is the *transition relation associated to* P. We also define the *PTS associated to* P as the unique PTS $(T(\Sigma_s), A, \longrightarrow)$ such that $t \xrightarrow{a} \pi$ if and only if $t \xrightarrow{a} \theta \in \mathsf{Tr}$ and $[\![\theta]\!] = \pi$ for some $\theta \in T(\Sigma_d)$.

Two PTSSs P and P' are *equivalent* if they have the same associated transition relation. The next lemma states that to show that two PTSSs are equivalent, it is sufficient to show that they can prove the same set of rules with only negative premises.

Lemma 2. *Let* P *and* P' *be two PTSSs over the same signature such that* $P \vdash \frac{N}{c}$ *iff* $P' \vdash \frac{N}{c}$ *for all closed rule* $\frac{N}{c}$ *with* N *containing only negative premises. Then*

1. *a 3-valued model is stable for* P *iff it is stable for* P',
2. P *is complete iff* P' *is complete, and*
3. *if any of* P *or* P' *is complete, then they have associated the same transition relation and the same PTS.*

This lemma is an adapted variant of (part of) Proposition 29 in [24]. Its proof follows by observing that only closed rules with negative premises are needed in Definition 5.

Example 3. We show that the PTSS P_{sc} defined in Example 2 is complete. For this we will use Lemma 2 and the notion of stratification. A *stratification* for a given PTSS is a function $str : (T(\Sigma_s) \times A \times T(\Sigma_d)) \to \alpha$, for some ordinal α, such that for every rule r in the PTSS and closed (proper) substitution ρ, it holds that

1. for every $\psi \in \mathrm{pprem}(r)$, $str(\rho(\psi)) \leq str(\rho(\mathrm{conc}(r)))$, and
2. for every $t \overset{a}{\not\longrightarrow} \in \mathrm{nprem}(r)$ and closed term $\theta \in T(\Sigma_d)$, $str(\rho(t) \xrightarrow{a} \theta) < str(\rho(\mathrm{conc}(r)))$.

If such a stratification exists the PTSS is complete [5,24].

Unfortunately, our running example is not stratifiable as such. This can be seen from the two rules in which sc_F and fs_F interact. By taking a proper closed substitution ρ such that $\rho(x) = \rho(Y) = a.\mathbf{0}$ and $\rho(\mu) = \boldsymbol{a.0}$ we obtained the following closed instances of the rules:

$$\frac{a.\mathbf{0} \xrightarrow{a} \boldsymbol{a.0} \quad (\boldsymbol{a.0})(a.\mathbf{0}) > 0 \quad \mathsf{fs}_F(a.\mathbf{0}) \overset{\checkmark}{\not\longrightarrow}}{\mathsf{sc}_F(a.\mathbf{0}) \xrightarrow{a} \boldsymbol{\mathsf{sc}_F}(\boldsymbol{a.0})} \qquad \frac{a.\mathbf{0} \xrightarrow{a} \boldsymbol{a.0} \quad \{\mathsf{sc}_F(a.\mathbf{0}) \overset{b}{\not\longrightarrow} \mid b \in A \cup \{\checkmark\}\}}{\mathsf{fs}_F(a.\mathbf{0}) \xrightarrow{\checkmark} \mathbf{0}}$$

[3] To construct the actual complete lattice for the Knaster–Tarski theorem, [29] adopts a different construction of pairs to represent 3-valued models. These pairs have the form $\langle \mathsf{CT}, \mathsf{UT} \rangle$ where CT is as before and $\mathsf{UT} \subseteq T(\Sigma_s) \times A \times T(\Sigma_d)$ is the set of *unknown* transitions. In our setting, this corresponds to a pair $\langle \mathsf{CT}, \mathsf{CT} \cup \mathsf{UT} \rangle$. To see the treatment of this type of construction see [29,28].

provided $a \notin F$. Notice that any stratification function needs to satisfy that $str(\mathsf{fs}_F(a.\mathbf{0}) \xrightarrow{\checkmark} \mathbf{0}) < str(\mathsf{sc}_F(a.\mathbf{0}) \xrightarrow{a} \mathbf{sc_F}(\boldsymbol{a}.\mathbf{0})) < str(\mathsf{fs}_F(a.\mathbf{0}) \xrightarrow{\checkmark} \mathbf{0})$, which is a clear contradiction.

Obviously, we expect the first rule to be spurious since, hopefully, transition $a.\mathbf{0} \xrightarrow{a} \boldsymbol{a}.\mathbf{0}$ will be false in any 3-valued stable model. So, we construct an equivalent PTSS that precisely rules out any of these spurious rules and show that this other PTSS is indeed stratifiable and hence complete. Using Lemma 2 we conclude that our PTSS of Example 2 is also complete.

So, the new PTSS P'_{sc} contains exactly all closed rules provable in P_{sc} of the form $\frac{N}{\psi}$ with N being a *minimal* set of negative premises. By minimal we indicate that all literals in N should appear in some node of the proof of $P_{\mathsf{sc}} \vdash \frac{N}{\psi}$. Clearly P_{sc} and P'_{sc} are in the conditions of Lemma 2. Therefore we only have to prove that P'_{sc} is stratifiable.

Define the stratification function for P'_{sc} by $str(t \xrightarrow{a} \theta) = str(t)$ for all closed transition $t \xrightarrow{a} \theta$ where str is inductively defined on the structure of the terms as follows:

$$
\begin{array}{ll}
str(0) = str(\mathbf{0}) = 0 & str(\mathsf{sc}_F(t)) = str(t) \\
str(\varepsilon) = str(\boldsymbol{\varepsilon}) = 2 & str(\mathbf{sc_F}(\theta)) = str(\theta) \\
str(a.\theta) = str(\boldsymbol{a}.\theta) = str(\theta) + 2 & str(\mathsf{fs}_F(t)) = str(t) + 1 \\
str(t_1 + t_2) = \max\{str(t_1), str(t_2)\} & str(\mathbf{fs_F}(\theta)) = str(\theta) + 1 \\
str(\theta_1 \mathbin{\boldsymbol{+}} \theta_2) = \max\{str(\theta_1), str(\theta_2)\} & str(\delta(t)) = str(t) \\
str(t_1 ; t_2) = str(t_1 \,||_B\, t_2) = str(t_1) + str(t_2) & str(\theta_1 \oplus_p \theta_2) = \max\{str(\theta_1), str(\theta_2)\} \\
str(\theta_1 \boldsymbol{;} \theta_2) = str(\theta_1 \,\boldsymbol{||_B}\, \theta_2) = str(\theta_1) + str(\theta_2) &
\end{array}
$$

Using induction on the height of the proof of $P_{\mathsf{sc}} \vdash \frac{N}{t \xrightarrow{a} \theta}$, we show that for every rule $\frac{N}{t \xrightarrow{a} \theta}$ in P'_{sc}, str satisfies:

(a) $str(t) \geq str(\theta) + 2$, and
(b) for every $t' \xrightarrow{a}\!\!\!\!\!/\;\; \in N$, $str(t') < str(t)$.

From (b) it follows that str is a stratification in P'_{sc}. We first state two facts that can be proven by structural induction:

F1. For every $\xi \in T(\Sigma)$, $str(\xi) \in \mathbb{N}$.
F2. For every $\theta \in T(\Sigma_d)$ and $t \in T(\Sigma_s)$, if $[\![\theta]\!](t) > 0$ then $str(\theta) \geq str(t)$.

Fact F1 holds because Σ_d does not contain the infinitary version of $\bigoplus_{i \in I}[p_i]\_$. (In fact, it only contains the binary $\oplus_p$.) Besides, F1 ensures that the sum is commutative. This is important for the induction in the cases in which rules for ; and $||_B$ are applied.

We will only show the case in which the rule for sc_F is used at the root of the proof of $P_{\mathsf{sc}} \vdash \frac{N}{t \xrightarrow{a} \theta}$ since this is the most relevant case. Thus, there is a closed substitution ρ such that $\mathsf{sc}_F(\rho(x)) = t$, $\mathbf{sc_F}(\rho(\mu)) = \theta$, $P_{\mathsf{sc}} \vdash \frac{N'}{\rho(x) \xrightarrow{a} \rho(\mu)}$ with minimal $N' \subseteq N$, $[\![\rho(\mu)]\!](\rho(y)) > 0$ for all $y \in Y$, and $\{\mathsf{fs}_F(\rho(y)) \xrightarrow{\checkmark}\!\!\!\!\!/\;\; \mid y \in Y\} \subseteq N$.

Using case (a) of the induction hypothesis, we calculate $str(t) = str(\mathsf{sc}_F(\rho(x))) = str(\rho(x)) \geq str(\rho(\mu)) + 2 = str(\mathbf{sc_F}(\rho(\mu))) + 2 = str(\theta) + 2$, which proves (a).

Using case (b) of the induction hypothesis, we have that

$$
\text{for every } t' \xrightarrow{a}\!\!\!\!\!/\;\; \in N', str(t') < str(\rho(x)) = str(\mathsf{sc}_F(\rho(x))) = str(t) \tag{2}
$$

and, using Fact F2 and case (a) of the induction hypothesis, for all $y \in Y$,

$$
str(\mathsf{fs}_F(\rho(y))) = str(\rho(y)) + 1 < str(\rho(\mu)) + 2 \leq str(\rho(x)) = str(\mathsf{sc}_F(\rho(x))) = str(t). \tag{3}
$$

Hence, by (2) and (3) and the fact that $N = N' \cup \{\mathsf{fs}_F(\rho(y)) \xrightarrow{\checkmark}\!\!\!\!\!/\;\; \mid y \in Y\}$, case (b) is proven. □

4. The $nt\mu f\theta / nt\mu x\theta$ format

In this section we introduce our rule format. We motivate and discuss each of the choices that restrict the format by showing that if they are relaxed, we can construct an operator for which bisimulation is not a congruence. First, we define formally the notion of bisimulation on probabilistic transition systems [19,20]. The definition we adopt in this paper is a little less common since it does not require that the relation is an equivalence as in [19,20], nor deals with sets closed under the relation as in [30,31]. Nevertheless the largest bisimulation according to the definition here is indeed the usual bisimulation equivalence [22, Prop. 3.4.4].

Given a relation $\mathsf{R} \subseteq T(\Sigma_s) \times T(\Sigma_s)$, its lift to $\Delta(T(\Sigma_s)) \times \Delta(T(\Sigma_s))$ is defined as follows: $\pi \;\mathsf{R}\; \pi'$ if and only if there is a weight function $w : (T(\Sigma_s) \times T(\Sigma_s)) \to [0, 1]$ such that for all $t, t' \in T(\Sigma_s)$, (i) $w(t, T(\Sigma_s)) = \pi(t)$, (ii) $w(T(\Sigma_s), t') = \pi'(t')$, and (iii) $w(t,t') > 0$ implies $t \mathrel{\mathsf{R}} t'$. It is easy to check that the weight function is a probability distribution on $(T(\Sigma_s) \times T(\Sigma_s))$. Moreover, the lifting of R is reflexive, symmetric or transitive if R is. The overloading on the use of R should be harmless.

Definition 8. Let $P = (T(\Sigma_s), A, \rightarrow)$ be a PTS. A relation $\mathsf{R} \subseteq T(\Sigma_s) \times T(\Sigma_s)$ is a bisimulation if R is symmetric and for all $t, t' \in T(\Sigma_s)$, $\pi \in \Delta(T(\Sigma_s))$, $a \in A$,

$$t \mathrel{\mathsf{R}} t' \text{ and } t \xrightarrow{a} \pi \text{ imply that there exists } \pi' \in \Delta(T(\Sigma_s)) \text{ s.t. } t' \xrightarrow{a} \pi' \text{ and } \pi \mathrel{\mathsf{R}} \pi'.$$

We define the relation $\sim$, called *bisimilarity* or *bisimulation equivalence*, as the smallest relation that includes all bisimulation relations. It is well-known that $\sim$ is itself a bisimulation and an equivalence relation.

A congruence over an algebraic structure is an equivalence relation on the algebra elements that is compatible with its structure. Formally, a (sort-respecting) equivalence relation $\mathsf{R} \subseteq T(\Sigma) \times T(\Sigma)$ is a *congruence* if for all $f \in \Sigma$ and $\xi_i, \xi_i' \in T(\Sigma)$ with $\xi_i \mathrel{\mathsf{R}} \xi_i'$ for all $i \in \{1, \dots, \mathsf{rk}(f)\}$, $f(\xi_1, \dots, \xi_{\mathsf{rk}(f)}) \mathrel{\mathsf{R}} f(\xi_1', \dots, \xi_{\mathsf{rk}(f)}')$.

In our setting we interpret R on distribution terms as the lifting of R from their interpretation: for $\theta, \theta' \in T(\Sigma_d)$, we define $\theta \mathrel{\mathsf{R}} \theta'$ if and only if $[\![\theta]\!] \mathrel{\mathsf{R}} [\![\theta']\!]$.

An interesting result is that if Σ is a probabilistically lifted signature, then it suffices to prove that R is only preserved by the s-mapping function symbols.

Proposition 3. *Let $\Sigma = (\Sigma_s, \Sigma_d)$ be a probabilistically lifted signature. Let $\mathsf{R} \subseteq T(\Sigma) \times T(\Sigma)$ be a relation such that*

1. *for all $\theta, \theta' \in T(\Sigma_d)$, $\theta \mathrel{\mathsf{R}} \theta'$ iff $[\![\theta]\!] \mathrel{\mathsf{R}} [\![\theta']\!]$, and*
2. *for all $f \in \Sigma_s$ and $\xi_i, \xi_i' \in T(\Sigma)$ with $\xi_i \mathrel{\mathsf{R}} \xi_i'$, $i \in \{1, \dots, \mathsf{rk}(f)\}$, $f(\xi_1, \dots, \xi_{\mathsf{rk}(f)}) \mathrel{\mathsf{R}} f(\xi_1', \dots, \xi_{\mathsf{rk}(f)}')$.*

Then, for all $\boldsymbol{f} \in \Sigma_d$, if $\theta_i \mathrel{\mathsf{R}} \theta_i'$ for all $i \in \{1, \dots, \mathsf{rk}(\boldsymbol{f})\}$, $\boldsymbol{f}(\theta_1, \dots, \theta_{\mathsf{rk}\, f}) \mathrel{\mathsf{R}} \boldsymbol{f}(\theta_1', \dots, \theta_{\mathsf{rk}\, f}')$.

As a consequence, if R is an equivalence relation, then it is also a congruence on Σ.

Proof. The fact that R is a congruence whenever it is an equivalence relation, follows from item 2, for all s operators, and the first part of the proposition, for all d operators. Therefore, we only prove the first part. We proceed by induction doing a case analysis.

Case δ. Suppose $t \mathrel{\mathsf{R}} t'$. By defining the weight function $w(t,t') = 1$ we can conclude that $\delta(t) \mathrel{\mathsf{R}} \delta(t')$.

Case $\bigoplus$. Suppose $\theta_i \mathrel{\mathsf{R}} \theta_i'$ which is witnessed by the weight function w_i, for all $i \in I$. By straightforward calculations, we can conclude that w, defined by $w(t,t') = \sum_{i\in I} p_i w_i(t,t')$, for all $t, t' \in T(\Sigma_s)$, is a weight function witnessing $\bigoplus_{i\in I}[p_i]\theta_i \mathrel{\mathsf{R}} \bigoplus_{i\in I}[p_i]\theta_i'$.

Case $\boldsymbol{f}$. Let $\boldsymbol{f}$ be the probabilistic lifting of f with $\mathsf{ar}(f) = \sigma_1 \dots \sigma_{\mathsf{rk}(f)} \rightarrow s$. For simplicity, assume that the sets of indexes I and J are a partition of $\{1, \dots, \mathsf{rk}(f)\}$, where $\sigma_i = s$ for all $i \in I$ and $\sigma_j = d$ for all $j \in J$. Suppose that $\theta_i \mathrel{\mathsf{R}} \theta_i'$ is witnessed by the weight function w_i, for all $i \in I$. We define function w by

$$w(f(\xi_1, \dots, \xi_{\mathsf{rk}(f)}), f(\xi_1', \dots, \xi_{\mathsf{rk}(f)}')) = \prod_{i\in I} w_i(\xi_i, \xi_i') \cdot \prod_{j\in J} \mathbf{1}_{\theta_j}(\xi_j) \cdot \mathbf{1}_{\theta_j'}(\xi_j')$$

and $w(t,t') = 0$ in any other case. The characteristic function $\mathbf{1}_\theta$ used above, is defined as usual: $\mathbf{1}_\theta(\theta) = 1$ and $\mathbf{1}_\theta(\theta') = 0$ for all $\theta' \neq \theta$. We show that w satisfy (i)–(iii) and, as a consequence, it witnesses $\boldsymbol{f}(\theta_1, \dots, \theta_{\mathsf{rk}\, f}) \mathrel{\mathsf{R}} \boldsymbol{f}(\theta_1', \dots, \theta_{\mathsf{rk}\, f}')$. For (i), we calculate:

$$\begin{aligned}
w(f(\xi_1, \dots, \xi_{\mathsf{rk}(f)}), T(\Sigma_s)) &= \textstyle\sum_{(\xi_1,\dots,\xi_{\mathsf{rk}(f)})\in T(\Sigma)^{\mathsf{rk}(f)}} w(f(\xi_1, \dots, \xi_{\mathsf{rk}(f)}), f(\xi_1', \dots, \xi_{\mathsf{rk}(f)}')) \\
&= \textstyle\sum_{(\xi_1',\dots,\xi_{\mathsf{rk}(f)}')\in T(\Sigma)^{\mathsf{rk}(f)}} \prod_{i\in I} w_i(\xi_i, \xi_i') \cdot \prod_{j\in J} \mathbf{1}_{\theta_j}(\xi_j) \cdot \mathbf{1}_{\theta_j'}(\xi_j') \\
&= \textstyle\prod_{i\in I} \sum_{\xi_i'\in T(\Sigma_s)} w_i(\xi_i, \xi_i') \cdot \prod_{j\in J} \mathbf{1}_{\theta_j}(\xi_j) \cdot \sum_{\xi_j'\in T(\Sigma_d)} \mathbf{1}_{\theta_j'}(\xi_j') \\
&= \textstyle\prod_{i\in I} w_i(\xi_i, T(\Sigma_s)) \cdot \prod_{j\in J} \mathbf{1}_{\theta_j}(\xi_j) \cdot \mathbf{1}_{\theta_j'}(T(\Sigma_d)) \\
&= \textstyle\prod_{i\in I} [\![\theta_i]\!](\xi_i) \cdot \prod_{j\in J} \mathbf{1}_{\theta_j}(\xi_j) \\
&= [\![\boldsymbol{f}(\theta_1, \dots, \theta_{\mathsf{rk}\, f})]\!](f(\xi_1, \dots, \xi_{\mathsf{rk}(f)}))
\end{aligned}$$

The case of (ii) follows similarly. For (iii), suppose $w(f(\xi_1, \dots, \xi_{\mathsf{rk}(f)}), f(\xi_1', \dots, \xi_{\mathsf{rk}(f)}')) > 0$. Hence $\prod_{i\in I} w_i(\xi_i, \xi_i') \cdot \prod_{j\in J} \mathbf{1}_{\theta_j}(\xi_j) \cdot \mathbf{1}_{\theta_j'}(\xi_j') > 0$ and from here $w_i(\xi_i, \xi_i') > 0$, for all $i \in I$, and $\theta_j = \xi_j$ and $\theta_j' = \xi_j'$, for all $j \in J$. As a consequence $\xi_i \mathrel{\mathsf{R}} \xi_i'$, because w_i is a weight function, and $\xi_j = \theta_j \mathrel{\mathsf{R}} \theta_j' = \xi_j'$ by hypothesis. From here, $f(\xi_1, \dots, \xi_{\mathsf{rk}(f)}) \mathrel{\mathsf{R}} f(\xi_1', \dots, \xi_{\mathsf{rk}(f)}')$ by the hypothesis of the lemma. □

Before introducing the $nt\mu f\theta/nt\mu x\theta$ format, we give a first approach to extend the *ntyft/ntyxt* format with probabilities that considers a restrictive form of quantitative premise. It can also be seen as a generalization of Segala-GSOS format [16] with terms in the premises as well as full lookahead. This first approach considers rules of the form

$$\frac{\{t_m \xrightarrow{a_m} \mu_m \mid m \in M\} \cup \{t_n \stackrel{b_n}{\not\longrightarrow} \mid n \in N\} \cup \{\theta_l(z_l) > 0 \mid l \in L\}}{f(\zeta_1, \ldots, \zeta_{\mathsf{rk}(f)}) \xrightarrow{a} \theta} \tag{F}$$

where M, N, and L are index sets, z_l, ζ_k, and μ_m, with $1 \le k \le \mathsf{rk}(f)$ and $m \in M$, are all different variables, $\left(\bigcup_{l\in L} Var(\theta_l)\right) \cap \{\zeta_1, \ldots, \zeta_{\mathsf{rk}(f)}\} = \emptyset$, $f \in F_s$, $t_m, t_n \in \mathbb{T}(\Sigma_s)$, and $\theta_l, \theta \in \mathbb{T}(\Sigma_d)$.

It can be proved that bisimilarity is a congruence for any operator defined in format (F). Indeed, it follows as a corollary of Theorem 4 since format (F) can be seen as a particular case of a rule in $nt\mu f\theta$ format.

In the following we present several counterexamples justifying the restrictions imposed by format (F). These counterexamples also apply to the $nt\mu f\theta/nt\mu x\theta$ format.

We consider the probabilistic lifting of a signature containing unary operator f with $\mathsf{ar}(f) = s \to s$, and three constants b, c and d of sort s, together with a label $a \in A$. We will also consider the following axioms:

$$c \xrightarrow{a} \boldsymbol{c} \qquad\qquad d \xrightarrow{a} \theta_d \quad \text{where } \theta_d = \boldsymbol{c} \oplus_{0.5} \boldsymbol{d}$$

No rule is associated to constant b. Notice that $c \sim d$. In the following we concentrate on rules for f.

The need that the source of the conclusion of a rule has a particular format has already been shown by several counterexamples in [2,4] for the *tyft/tyxt* format. We adapt an example from [4] to motivate the need. Consider the axiom

$$f(b) \xrightarrow{a} \boldsymbol{f}(\boldsymbol{b}).$$

Then $f(f(b)) \sim b$ since none of them perform any action. However, $f(f(f(b)))$ and $f(b)$ are not bisimilar since $f(b)$ can perform an action but $f(f(f(b)))$ cannot.

Consider now the rule

$$\frac{x \xrightarrow{a} \boldsymbol{c}}{f(x) \xrightarrow{a} \boldsymbol{c}}.$$

Then, despite that $c \sim d$, $f(c)$ and $f(d)$ are not bisimilar since $d \xrightarrow{a} \boldsymbol{c}$ is *not* a valid transition in the (unique) supported model. This shows that the target of a positive premise cannot be a distribution on a particular (shape of) term.

The following rule has a similar problem:

$$\frac{x \xrightarrow{a} \mu \quad \mu(d) > 0}{f(x) \xrightarrow{a} \boldsymbol{c}}$$

This rule shows that quantitative literals cannot inquire over arbitrary terms: note that $f(c)$ and $f(d)$ are not bisimilar since $c \xrightarrow{a} \boldsymbol{c}$ and $[\![\boldsymbol{c}]\!](d) = 0$.

Moreover, the requirement that all variables z_l, μ_m, and ζ_k are different is inherited from the *tyft/tyxt* format. Examples from [2] are easily adaptable to our setting.

Allowing for a quantitative literal that compares with a value different from 0 is also problematic. Consider rule

$$\frac{x \xrightarrow{a} \mu \quad \mu(y) \ge 1 \quad y \xrightarrow{a} \mu'}{f(x) \xrightarrow{a} \boldsymbol{c}}$$

Again $f(c)$ and $f(d)$ are not bisimilar since $d \xrightarrow{a} \theta_d$, and there is no single term t in which $[\![\theta_d]\!](t) \ge 1$.

This example suggests that quantitative premises should have the form $\mu(Y) > p$ or $\mu(Y) \ge p$ where Y is a set of variables. So the previous rule could be recast as

$$\frac{x \xrightarrow{a} \mu \quad \mu(\{y, z\}) \ge 1 \quad y \xrightarrow{a} \mu'}{f(x) \xrightarrow{a} \boldsymbol{c}} \tag{4}$$

However, the same problem repeats if we introduce a new constant e and axiom $e \xrightarrow{a} ([0.4]\boldsymbol{c} \oplus [0.3]\boldsymbol{d} \oplus [0.3]\boldsymbol{e})$. In fact, it turns out that Y needs to be *infinite* (consider the case in which a new infinite set of constants $\{e_n\}_{n\in\mathbb{N}_0}$ is defined with $e_n \xrightarrow{a} (\bigoplus_{i\in\mathbb{N}_0} \left[\frac{1}{2^{i+1}}\right] \boldsymbol{e_i}))$. Moreover, it is necessary that all terms that substitute some variable in Y have some *symmetric behavior*, i.e, all variable in Y has to satisfy the same conditions. In rule 4 such symmetric behavior is not present, allowing for z to be substituted by any valid term, in particular one that not necessarily performs action a which was not the originally intended behavior. Moreover, symmetry is also necessary for the congruence result as we will see later.

In view of these considerations, we extend format (F) with quantitative premises of the form $\theta(Y) > p$ or $\theta(Y) \ge p$, with Y an infinite set of term variables. We call this format $nt\mu f\theta/nt\mu x\theta$ following the nomenclature of [2,4]. Later we will give an example justifying the symmetry restriction. The following definition is important to ensure symmetry.

Definition 9. Let $\{Y_l\}_{l\in L}$ be a family of sets of state term variables in $\mathcal{V}$ with the same cardinality. Let $W \subseteq \mathcal{V}$. The l-th element of a tuple $\vec{z}$ is denoted by $\vec{z}(l)$. For a set of tuples $T = \{\vec{z}_i \mid i \in I\}$ we denote the l-th projection by $\Pi_l(T) = \{\vec{z}_i(l) \mid i \in I\}$. We say that $\mathcal{Z} \subseteq \prod_{l\in L} Y_l \times \prod_{\zeta\in W}\{\zeta\}$ is a *diagonal in* $\prod_{l\in L} Y_l$, if

1. for all $l \in L$, $\Pi_l(\mathcal{Z}) = Y_l$; and
2. for all $\vec{z}, \vec{z}' \in \mathcal{Z}$, $(\exists l \in L : \vec{z}(l) = \vec{z}'(l)) \Rightarrow \vec{z} = \vec{z}'$.

Property (ii) ensures that different tuples $\vec{z}, \vec{z}' \in \mathcal{Z}$ differ in all L-positions, and by property (i) every variable of every Y_l is used in (exactly) one $\vec{z} \in \mathcal{Z}$. We call this property "diagonal" following the intuition that each L-prefix of $\vec{z}$ represents a coordinate in the space $\prod_{l\in L} Y_l$, so that the L-projection of $\mathcal{Z}$ can be seen as the line that traverses the main diagonal of the space $\prod_{l\in L} Y_l$. Therefore, notice that, for $Y_l = \{y_l^0, y_l^1, y_l^2, \ldots\}$ and $W = \{w_1, \ldots, w_n\}$, a possible definition for $\mathcal{Z}$ such that it is a diagonal in $\prod_{l\in L} Y_l$, is

$$\mathcal{Z} = \{(y_1^0, y_2^0, \ldots, y_L^0, w_1, \ldots, w_n), (y_1^1, y_2^1, \ldots, y_L^1, w_1, \ldots, w_n), (y_1^2, y_2^2, \ldots, y_L^2, w_1, \ldots, w_n), \ldots\}$$

In addition, we use the following notation: $t(\zeta_1, \ldots, \zeta_n)$ denotes a term that only has variables in the set $\{\zeta_1, \ldots, \zeta_n\}$, that is $Var(t(\zeta_1, \ldots, \zeta_n)) \subseteq \{\zeta_1, \ldots, \zeta_n\}$, and moreover, $t(\zeta_1', \ldots, \zeta_n')$ denotes the same term as $t(\zeta_1, \ldots, \zeta_n)$ in which each variable ζ_i has been replaced by ζ_i'.

Definition 10. Let $P = (\Sigma, A, R)$ be a PTSS. A rule $r \in R$ is in *ntμfθ format* if it has the following form

$$\frac{\bigcup_{m\in M}\{t_m(\vec{z}) \xrightarrow{a_m} \mu_m^{\vec{z}} \mid \vec{z} \in \mathcal{Z}\} \cup \bigcup_{n\in N}\{t_n(\vec{z}) \stackrel{b_n}{\not\longrightarrow} \mid \vec{z} \in \mathcal{Z}\} \cup \{\theta_l(Y_l) \trianglerighteq_{l,k} p_{l,k} \mid l \in L, k \in K_l\}}{f(\zeta_1, \ldots, \zeta_{\mathsf{rk}(f)}) \xrightarrow{a} \theta}$$

with $\trianglerighteq_{l,k} \in \{>, \geq\}$ for all $l \in L$ and $k \in K_l$, $Y_l \subseteq \mathcal{V}$ for all $l \in L$, $W \subseteq \mathcal{V} \cup \mathcal{D} \setminus \bigcup_{l\in L} Y_l$ and $\mathcal{Z} \in \prod_{l\in L} Y_l \times \prod_{\zeta\in W}\{\zeta\}$ is a diagonal in $\prod_{l\in L} Y_l$. In addition, it has to satisfy the following conditions:

1. Each set Y_l should be at least countably infinite, for all $l \in L$, and the cardinality of L should be strictly smaller than that of the Y_l's.
2. All variables $\zeta_1, \ldots, \zeta_{\mathsf{rk}(f)}$ are different.
3. All variables $\mu_m^{\vec{z}}$, with $m \in M$ and $\vec{z} \in \mathcal{Z}$, are different and $\{\zeta_1, \ldots, \zeta_{\mathsf{rk}(f)}\} \cap \{\mu_m^{\vec{z}} \mid \vec{z} \in \mathcal{Z}, m \in M\} = \emptyset$.
4. For all $l \in L$, $Y_l \cap \{\zeta_1, \ldots, \zeta_{\mathsf{rk}(f)}\} = \emptyset$, and $Y_l \cap Y_{l'} = \emptyset$ for all $l' \in L$, $l \neq l'$.
5. For all $m \in M$, the set $\{\mu_m^{\vec{z}} \mid \vec{z} \in \mathcal{Z}\} \cap \big(Var(\theta) \cup (\bigcup_{l\in L} Var(\theta_l)) \cup W\big)$ is finite.
6. For all $l \in L$, the set $Y_l \cap \big(Var(\theta) \cup \bigcup_{l'\in L} Var(\theta_{l'})\big)$ is finite.

A rule $r \in R$ is in *ntμxθ format* if its form is like above but has a conclusion of the form $x \xrightarrow{a} \theta$ and, in addition, it satisfies the same conditions as above, except that whenever we write $\{\zeta_1, \ldots, \zeta_{\mathsf{rk}(f)}\}$, we should write $\{x\}$. P is in *ntμfθ format* if all its rules are in ntμfθ format. P is in *ntμfθ/ntμxθ format* if all its rules are in either ntμfθ format or ntμxθ format.

Variables $\zeta_1, \ldots, \zeta_{\mathsf{rk}(f)}$ appearing in the source of the conclusion are binding. So are variables in $\bigcup_{l\in L} Y_l$ appearing in quantitative premises and variables in $\{\mu_m^{\vec{z}} \mid m \in M \wedge \vec{z} \in \mathcal{Z}\}$ appearing in the target of a positive premise. Therefore they all need to be different. This is stated in conditions 2, 3, and 4. Every set Y_l has to be infinite, which is stated in condition 1. By requiring that $\mathcal{Z}$ is diagonal in $\prod_{l\in L} Y_l$ and bundling the set of positive premises in $\{t_m(\vec{z}) \xrightarrow{a_m} \mu_m^{\vec{z}} : \vec{z} \in \mathcal{Z}\}$, we ensure a symmetric behavior of terms $t_m(\vec{z})$ for every possible substitution of variables $\vec{z}$. This is the same for the negative premises. In fact, notice that, since $\mathcal{Z}$ is diagonal in $\prod_{l\in L} Y_l$, a substitution ρ is always free to assign different terms to coordinates 1 to L in two different terms $t(y_1, \ldots, y_L, \ldots)$ and $t(y_1', \ldots, y_L', \ldots)$. Finally, condition 5 ensures that the symmetric behavior introduced in the positive premises $\{t_m(\vec{z}) \xrightarrow{a_m} \mu_m^{\vec{z}} : \vec{z} \in \mathcal{Z}\}$ is used consistently in a lookahead. This is guaranteed by requesting that a finite number of $\mu_m^{\vec{z}}$ (of all introduced in the family m of positive premises) may appear in a bound occurrence. Similarly, condition 6 ensures that the variables in the set Y_l are use consistently, also by requesting that only a finite subset of variables in Y_l may appear in a bound occurrence.

The following example shows that quantitative premises cannot check for upper bounds (or equality). Consider the rule

$$\frac{x \xrightarrow{a} \mu \quad \mu(Y) \leq 0.5}{f(x) \xrightarrow{a} \boldsymbol{c}}$$

with c and d defined as before. $f(c)$ and $f(d)$ are not bisimilar because $f(d) \xrightarrow{a} \boldsymbol{c}$ by taking the substitution ρ such that $\rho(y) = c$ for all $y \in Y$, but $f(c) \stackrel{a}{\not\longrightarrow}$ since there is no term t such that it can be *properly* substituted in y (i.e., such that $[\![\boldsymbol{c}]\!](t) > 0$) and $[\![\boldsymbol{c}]\!](t) \leq 0.5$.

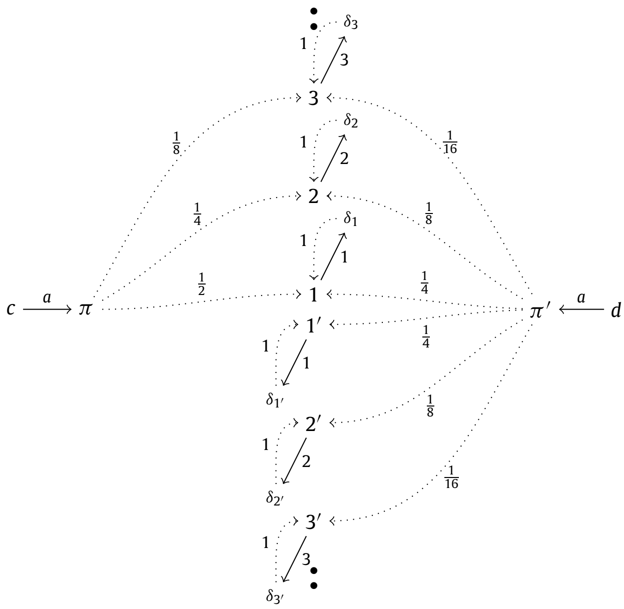


Fig. 1. Graphical representation of the axioms used to show why the symmetry requirement is needed.

Notice that if Y_l appears in two different quantitative premises they should appear in the context of the same θ_l, otherwise we can define an operator that distinguishes bisimilar process as shown in the following example. Consider the rule

$$\frac{x \xrightarrow{a} \mu \quad x' \xrightarrow{a} \mu' \quad \mu(Y) \geq 1 \quad \mu'(Y) \geq 1}{f(x,x') \xrightarrow{a} \boldsymbol{f}(\mu,\mu')}$$

with c and d defined as before. Notice that $f(c,c) \xrightarrow{a} \boldsymbol{f}(\boldsymbol{c},\boldsymbol{c})$ but $f(c,d) \stackrel{a}{\not\rightarrow}$. For the later case we would need to define a substitution ρ s.t. $\rho(\mu) = \boldsymbol{c}$, $\rho(\mu') = \theta_d$, and $[\![\boldsymbol{c}]\!](\rho(Y)) = [\![\theta_d]\!](\rho(Y)) = 1$. This implies that necessarily $\rho(Y) = \{c,d\}$ in which case ρ is not proper (since $[\![\rho(\mu)]\!](d) = [\![\boldsymbol{c}]\!](d) = 0$).

If symmetry of behavior on variables in Y_l were not enforced, it would also be possible to distinguish distributions that are equivalent. To show this, consider a signature with state constants c, d, and $\{n, n' \mid n \in \mathbb{N}_0\}$, unary operator f, $\mathsf{ar}(f) = s \to s$, and rules

$$n \xrightarrow{n} \boldsymbol{n} \qquad n' \xrightarrow{n} \boldsymbol{n'} \qquad c \xrightarrow{a} \theta \qquad d \xrightarrow{a} \theta'$$

$$\text{with} \quad \theta = \bigoplus\nolimits_{n\in\mathbb{N}_0} \left[\tfrac{1}{2^{n+1}}\right] \boldsymbol{n} \quad \text{and} \quad \theta' = \bigoplus\nolimits_{n\in\mathbb{N}_0} \left(\left[\tfrac{1}{2^{n+2}}\right] \boldsymbol{n} \oplus \left[\tfrac{1}{2^{n+2}}\right] \boldsymbol{n'}\right)$$

$$\frac{x \xrightarrow{a} \mu \quad \mu(\{y_k\}_{k\in\mathbb{N}_0}) \geq 1 \quad \{y_k \xrightarrow{k} \mu_k \mid k \in \mathbb{N}_0\}}{f(x) \xrightarrow{b} \mu}$$

Fig. 1 depicts the probabilistic transition system for the constants defined by the rules above. Notice that $c \sim d$; nonetheless, $f(c) \xrightarrow{b} \boldsymbol{c}$ but $f(d) \stackrel{b}{\not\rightarrow}$ since $d \xrightarrow{a} \theta'$ and there is no way to match both n and n' to two different variables y_{k_1} and y_{k_2} (for all $n \in \mathbb{N}_0$), hence $[\![\theta']\!](\rho(\{y_k\}_{k\in\mathbb{N}_0})) = 0.5$ for any substitution ρ satisfying the positive premises.

If all symmetric variables $\mu_m^{\vec{z}}$ are allowed to be used (contradicting condition 5), it would also be possible to distinguish distributions that are equivalent. To show this, consider the variation of the previous example where two rules for constants $\{n, n' \mid n \in \mathbb{N}_0\}$ are added and the rule of f is changed as follows:

$$n \xrightarrow{b} \boldsymbol{n} \qquad n' \xrightarrow{b} \boldsymbol{n'} \qquad \frac{x \xrightarrow{a} \mu \quad \mu(\{y_k\}_{k\in\mathbb{N}_0}) \geq 1 \quad \{y_k \xrightarrow{b} \mu_k \mid k \in \mathbb{N}_0\} \quad \{\mu_k(\{y_k^j\}_{j\in\mathbb{N}_0}) \geq 1 \mid k \in \mathbb{N}_0\} \quad \{\{y_k^j \xrightarrow{k} \mu_k^j \mid j \in \mathbb{N}_0\} \mid k \in \mathbb{N}_0\}}{f(x) \xrightarrow{b} \mu}$$

Again, notice that $c \sim d$; nonetheless, $f(c) \xrightarrow{b} \boldsymbol{c}$ but $f(d) \stackrel{b}{\not\rightarrow}$. The reason is similar as the previous example, except that it needs a more complex reasoning on the two steps of lookahead: Suppose we intend to prove $f(d) \xrightarrow{b} \theta''$ for some

θ''. Then we need to construct a substitution ρ such that $\rho(x) = d$, and hence only $\rho(\mu) = \theta'$ is possible. To achieve $\theta'(\{\rho(y_k)\}_{k\in\mathbb{N}_0}) \geq 1$, we need that $\rho(y_k) = n$ and $\rho(y_{k'}) = n'$ for two different $k, k' \in \mathbb{N}_0$. If $\rho(y_k) = n$ then $\rho(\mu_k) = \boldsymbol{n}$ and $\rho(y_k^j) = n$ for all $j \in \mathbb{N}_0$. Then, necessarily $k = n$ for $\rho(y_k^j) \xrightarrow{k} \rho(\mu_k^j)$ to hold. A similar reasoning yields that if $\rho(y_{k'}) = n'$ then $k' = n$, contradicting the fact that k and k' need to be different.

Finally, following a similar reasoning to the cases above, the following rule justifies the presence of condition 6:

$$\frac{x \xrightarrow{a} \mu \quad \mu(\{y_k\}_{k\in\mathbb{N}_0}) \geq 1 \quad \{\delta(y_k)(\{y_k^j\}_{j\in\mathbb{N}_0}) \geq 1 \mid k \in \mathbb{N}_0\} \quad \{\{y_k^j \xrightarrow{k} \mu_k^j \mid j \in \mathbb{N}_0\} \mid k \in \mathbb{N}_0\}}{f(x) \xrightarrow{b} \mu}$$

The rationale to show that $f(c) \xrightarrow{b} \boldsymbol{c}$ but $f(d) \xrightarrow{b}\!\!\!\!\!/\;$ is similar to the previous case.

If conditions 5 and 6 are strengthened so that the sets contain at most one variable, the burden introduced by the restrictions associated to symmetry can be significantly eased using some special notation. Therefore we require that

5′. for all $m \in M$ $\left|\{\mu_m^{\vec{z}} \mid \vec{z} \in \mathcal{Z}\} \cap \left(Var(\theta) \cup (\bigcup_{l\in L} Var(\theta_l)) \cup W\right)\right| \leq 1$, and
6′. for all $l \in L$, $\left|Y_l \cap \left(Var(\theta) \cup \bigcup_{l'\in L} Var(\theta_{l'})\right)\right| \leq 1$

Provided that conditions 5′ and 6′ are satisfied, and assuming that $\mathcal{Z} = \prod_{l\in L} Y_l \times \prod_{h=1}^{H}\{\zeta_h\}$, we can write $t_m(Y_1, \ldots, Y_L, \zeta_1, \ldots, \zeta_H) \xrightarrow{a_m} \mu_m$ as an abbreviation for $\{t_m(\vec{z}) \xrightarrow{a_m} \mu_m^{\vec{z}} : \vec{z} \in \mathcal{Z}\}$, where μ_m is the only $\mu_m^{\vec{z}}$ that may be used in an *ntμfθ/ntμxθ* rule outside its defining positive premise. Similarly, we write $t_n(Y_1, \ldots, Y_L, \zeta_1, \ldots, \zeta_H) \xrightarrow{b_n}\!\!\!\!\!/\;$ as an abbreviation for $\{t_n(\vec{z}) \xrightarrow{b_n}\!\!\!\!\!/\; : \vec{z} \in \mathcal{Z}\}$. Moreover, if $y_l \in Y_l \cap \left(Var(\theta) \cup \bigcup_{l'\in L} Var(\theta_{l'})\right)$ we replace each occurrence of y_l in θ and $\theta_{l'}$ by Y_l. For example, rule $\frac{x \xrightarrow{a} \mu \quad \mu(Y)>0 \quad \{\mathsf{fs}_F(y) \xrightarrow{\checkmark}\!\!\!\!\!/\; \mid y\in Y\}}{\mathsf{sc}_F(x) \xrightarrow{a} \mathbf{sc}_F(\mu)}$ can be rewritten to $\frac{x \xrightarrow{a} \mu \quad \mu(Y)>0 \quad \mathsf{fs}_F(Y) \xrightarrow{\checkmark}\!\!\!\!\!/}{\mathsf{sc}_F(x) \xrightarrow{a} \mathbf{sc}_F(\mu)}$.

The *ntμfθ/ntμxθ* format can then be restated in the setting of this notation as follows. A rule is in *abbreviated ntμfθ format* if it has the form:

$$\frac{\{t_m \xrightarrow{a_m} \mu_m : m \in M\} \;\cup\; \{t_n \xrightarrow{b_n}\!\!\!\!\!/\; : n \in N\} \;\cup\; \{\theta_l(Y_l) \trianglerighteq_{l,k} p_{l,k} : l \in L, k \in K_l\}}{f(\zeta_1, \ldots, \zeta_{\mathsf{rk}(f)}) \xrightarrow{a} \theta}$$

where $\trianglerighteq_{l,k} \in \{>, \geq\}$, each Y_l is a new variable name not belonging to $\mathcal{V} \cup \mathcal{D}$, $Var(t_m), Var(t_n), Var(\theta_l), Var(\theta) \subseteq \mathcal{V} \cup \mathcal{D} \cup \{Y_l \mid l \in L\}$, for all $l \in L$, $m \in M$ and $n \in N$, and variables Y_l, μ_m, ζ_i, with $l \in L$, $m \in M$ and $1 \leq i \leq \mathsf{rk}(f)$, are all different.

Notice that this notation hides all the restrictions associated to symmetry. Hence the definition of the format becomes remarkably simpler. Of course, it has the small caveat imposed by restrictions 5′ and 6′. Notice also that this new formulation of the *ntμfθ/ntμxθ* format makes it more evident that it is the natural probabilistic extension of the *ntyft/ntyxt* format.

We finally remark that all rules of our running example P_{sc} (see Table 1) are in *ntμfθ* format. Moreover, they all satisfy conditions 5′ and 6′ and hence can be rewritten in the abbreviated *ntμfθ* format. In particular, the rule for sc_F is rewritten as

$$\frac{x \xrightarrow{a} \mu \quad \mu(Y) > 0 \quad \mathsf{fs}_F(Y) \xrightarrow{\checkmark}\!\!\!\!\!/}{\mathsf{sc}_F(x) \xrightarrow{a} \mathbf{sc}_F(\mu)} \; a \notin F$$

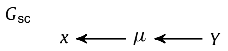
5. The congruence theorem

In this section we prove the following general theorem:

Theorem 4. *Let P be a complete well-founded PTSS in ntμfθ/ntμxθ format. Then $\sim$ is a congruence relation for all operators defined in P.*

Notice that the theorem does not apply to all PTSSs in *ntμfθ/ntμxθ* format but only to those whose rules are *well-founded*. Basically, a rule is well-founded if every bound variable (i.e. a variable that appears in the source of the conclusion, in the set Y of a quantitative premise, or in the target of a positive premise) does not depend on itself or on infinitely many bound variables. In Section 5.1 we formally introduce the notions of dependency graph, well-founded rule, and also free variable. It turns out that for any complete PTSS in *ntμfθ/ntμxθ* format there is an equivalent PTSS in *ntμfθ* format without free variables, which simplifies the proof of the theorem. We show this in Section 5.2. In Section 5.3, we introduce the *congruence closure* of a relation and some general properties about it. This concept is central to the proof of Theorem 4 —reported in Section 5.4— since its aim is to show that the congruence closure of the bisimulation equivalence is a bisimulation relation. As a consequence they coincide, since the congruence closure extends the original relation. Hence bisimulation equivalence is a congruence.

Fig. 2. Dependency graphs for two non-well-founded sets of premises.



$\text{degree}(x) = 1 \quad \text{degree}(\mu) = 2$
$\text{degree}(y) = 3 \quad \text{for all } y \in Y$

Fig. 3. Dependency graph of the rule of sc_F and dependency degree of its variables.

5.1. Well-founded premises and free variables

Given a rule r, the instantiation of a bound variable in r depends on the instantiation of all variables occurring in the term that appears on the same literal that the bound variable is defined. Thus, if $t \xrightarrow{a} \mu$ is a positive literal in r, we say that μ *depends* on all variables in $Var(t)$. Similarly, any variable in Y *depends* on all the variables in $Var(\theta)$ if $\theta(Y) \trianglerighteq p$ is a quantitative literal in r. Thus, we exclude rules in which there are circular dependencies or any infinite backward chain of dependencies since we will need to construct substitutions in an inductive manner. To define the proper partial order, we use the notion of dependency graph which was introduced in [2] together with the notion of well-founded rule. We adapt them to our setting.

Definition 11. Let W be a set of positive and quantitative premises. The *(variable) dependency directed graph* of W is given by $G_{\mathsf{W}} = (V, E)$ with

- $V = \cup_{\psi \in \mathsf{W}} Var(\psi)$ and
- $E = \{\langle \zeta, \mu \rangle \mid (t \xrightarrow{a} \mu) \in \mathsf{W}, \zeta \in Var(t)\} \cup \{\langle \zeta, y \rangle \mid (\theta(Y) \trianglerighteq p) \in \mathsf{W}, \zeta \in Var(\theta), y \in Y\}$.

We say that W is *well-founded* if any backward chain of edges in G_{W} is finite. For each $\zeta \in V$, define its *dependency degree* in W by $\text{degree}(\zeta) = \sup(\{\text{degree}(\zeta') + 1 \mid (\zeta', \zeta) \in E\})$, where $\sup(\emptyset) = 0$.

A rule is called *well-founded* if its set of positive and quantitative premises is well-founded. A PTSS is called *well-founded* if all its rules are well-founded.

Example 4. Let

$$\mathsf{W}_1 = \{f_1(x_1, Y_2) \xrightarrow{a} \mu_1, \mu_1(Y_1) > 0, f_2(x_2, Y_1) \xrightarrow{a} \mu_2, \mu_2(Y_2) > 0\}$$
$$\mathsf{W}_2 = \{Y_{n+1} \xrightarrow{a} \mu_n, \mu_n(Y_n) > 0 \mid n \in \mathbb{N}\}$$

Their respective dependency graphs G_{W_1} and G_{W_2} are depicted in Fig. 2 where we introduce an abuse of notation: for example, the edge $Y_2 \to \mu_1$ represents the infinite set of edges $\{y_2 \to \mu_1^{y_2} \mid y_2 \in Y_2\}$ introduced by the set of transitions $f_1(x_1, Y_2) \xrightarrow{a} \mu_1 = \{f_1(x_1, y_2) \xrightarrow{a} \mu_1^{y_2} \mid y_2 \in Y_2\}$.

The set W_1 is not well-founded because G_{W_1} has a cycle. W_2 is not well-founded because for every node in G_{W_2} there is an infinite backward chain starting on it.

The rule for sc_F is an example of a well-founded rule. Its dependency graph is reported in Fig. 3 as well as the dependency degree of its variables. □

Definition 12. A variable occurs *free* in a rule r if it occurs in r but not in the source of the conclusion, in the set Y of a quantitative premise $\theta(Y) \trianglerighteq q$, or in the target of a positive premise.

A rule is called *pure* if it is well-founded and does not contain free variables. A PTSS is called *pure* if all of its rules are pure.

5.2. From ntμfθ/ntμxθ format to pure ntμfθ format

In this section, we show that every complete well-founded PTSS in *ntμfθ*/*ntμxθ* can be translated into an equivalent PTSS that is pure and in *ntμfθ* format. We do this in several steps. We first show that for every PTSS in *ntμfθ*/*ntμxθ* there is another PTSS in *ntμfθ* that can prove exactly the same set of rules (Lemma 5). By using Lemma 2 it immediately follows that both PTSSs define exactly the same transition relation (Corollary 6). Next, we show that for every complete and well-founded PTSS in *ntμfθ* format there is a pure and complete PTSS in *ntμfθ* format that proves exactly the same rules (Lemma 7). Using Lemma 2 we can ensure that both PTSS define the same transition relation (Corollary 8).

Lemma 5. *Let $P = (\Sigma, A, R)$ be a PTSS in ntμfθ/ntμxθ format. Then there is a PTSS $P' = (\Sigma, A, R')$ in ntμfθ format such that, for all rule $\frac{H}{\phi}$, $P \vdash \frac{H}{\phi}$ iff $P' \vdash \frac{H}{\phi}$. Moreover, P' is well-founded whenever P is. Similarly, P' is complete whenever P is.*

Proof (Sketch). For each r and function symbol $f \in \Sigma$ we define the open substitution ρ_f by:

$$\rho_f(x) = f(\zeta_1, \dots, \zeta_{\mathsf{rk}(f)}) \quad \text{if } x \text{ is in the source of the conclusion of } r \text{ and } \zeta_1, \dots, \zeta_{\mathsf{rk}(f)} \text{ are variables that do not occur in } r \text{ and respect the arity of } f.$$
$$\rho_f(\zeta) = \zeta \quad \text{otherwise.}$$

We define the set of rules R' that contains all rules $r \in R$ that are in *ntμfθ* format, and all rules $\rho_f(r)$ for all $r \in R$ in *ntμxθ* format and $f \in \Sigma_s$. Notice that $\rho_f(r)$ is well-founded whenever r is well-founded. So, if P is well-founded, so is P'.

To prove that $P \vdash \frac{H}{\psi}$ implies $P' \vdash \frac{H}{\psi}$ we take a proof $\mathfrak{p}_\psi^H$ of $P \vdash \frac{H}{\psi}$ and construct a proof $\mathfrak{p}_\psi'^H$ by mimicking $\mathfrak{p}_\psi^H$ using the rule $\rho_f(r)$ in $\mathfrak{p}_\psi'^H$ whenever r in *ntμxθ* is used in $\mathfrak{p}_\psi^H$ and the target variable in $\mathrm{conc}(r)$ is substituted by a term of the form $f(\xi_1, \cdots, \xi_{\mathsf{rk}(f)})$. We also have to accommodate the current substitution according to ρ_f.

The reverse implication proceeds in the same way only that when rules ρ_f are used in $\mathfrak{p}_\psi'^H$ they are replaced by r in $\mathfrak{p}_\psi^H$ and again the current substitution is accommodated with ρ_f in the inverse manner.

Since both P and P' prove exactly the same set of rules, it immediately follows that P is complete iff P' is complete. □

Lemma 2 guarantees that two PTSSs that can prove exactly the same sets of rules $\frac{H}{\phi}$ with H containing only negative literals have also the same set of 3-valued stable models. Moreover, if one of them is complete, so is the other, in which case they are equivalent. Using this fact, the following result is a corollary of Lemma 5.

Corollary 6. *Let $P = (\Sigma, A, R)$ be a complete PTSS in ntμfθ/ntμxθ format. Then there is a complete PTSS $P' = (\Sigma, A, R')$ in ntμfθ format that is equivalent to P.*

The following lemma states that for every complete well-founded PTSS in *ntμfθ/ntμxθ* format there is another PTSS that is complete and pure in *ntμfθ/ntμxθ* format that proves exactly the same set of rules. Moreover, if the first PTSS is *ntμfθ*, so is the second one.

Lemma 7. *Let $P = (\Sigma, A, R)$ be a well-founded PTSS in ntμfθ/ntμxθ format. Then there is a pure PTSS $P' = (\Sigma, A, R')$ in ntμfθ/ntμxθ format such that for all rule $\frac{H}{\phi}$, $P \vdash \frac{H}{\phi}$ iff $P' \vdash \frac{H}{\phi}$. Moreover, if P is in ntμfθ format then P' is also in ntμfθ format. In addition, P is complete iff P' is complete.*

Proof (Sketch). For every rule $r \in R$, if r has no free variables then $r \in R'$. If $r \in R$ has free variables, then for all substitution $\hat{\rho}$ such that

$$\hat{\rho}(x) = t \quad \text{for all free variable } x \in \mathcal{V} \text{ in } r \text{ and } t \in T(\Sigma_s),$$
$$\hat{\rho}(\mu) = \theta \quad \text{for all free variable } \mu \in \mathcal{D} \text{ in } r \text{ and } \theta \in T(\Sigma_d); \text{ and}$$
$$\hat{\rho}(\zeta) = \zeta \quad \text{otherwise,}$$

we define $r' \in R'$ by $\hat{\rho}(r)$. Note that all rules in R' have no free variables and they are in *ntμfθ* or *ntμxθ* format if r is in *ntμfθ* or *ntμxθ* format, respectively. Therefore, if rules in P is in *ntμfθ* format then P' is also in *ntμfθ* format.

The proof that both PTSSs prove exactly the same set of rules follows in the same way as for Lemma 5. Moreover, since both P and P' prove exactly the same set of rules, it follows that P is complete iff P' is complete. □

Using Lemma 2, the following is a corollary of Lemma 7.

Corollary 8. *Let $P = (\Sigma, A, R)$ be a complete and well-founded PTSS in ntμfθ/ntμxθ format. Then there is a complete PTSS $P' = (\Sigma, A, R')$ in pure ntμfθ/ntμxθ format that is equivalent with P. Moreover, if P is in ntμfθ format then P' is in ntμfθ format.*

5.3. The congruence closure

The *congruence closure*, introduced in Definition 13, is central to the proof of Theorem 4. By construction, it defines a relation that is preserved by all contexts. The aim of the proof of Theorem 4 is to show that the congruence closure of $\sim$ is a bisimulation.

Notice that the congruence closure is defined on a relation over $T(\Sigma_s) \times T(\Sigma_s)$ but actually defines a relation over $T(\Sigma) \times T(\Sigma)$.

Definition 13 *(Congruence closure).* Let $P = (\Sigma, A, R)$ be a PTSS. The *congruence closure* of a relation $\mathsf{R} \subseteq T(\Sigma_s) \times T(\Sigma_s)$ is defined as the smallest relation $\mathsf{R}_P \subseteq T(\Sigma) \times T(\Sigma)$ such that:

1. $\mathsf{R} \subseteq \mathsf{R}_P$,
2. $\boldsymbol{c}\ \mathsf{R}_P\ \boldsymbol{c'}$ whenever $c, c' \in \Sigma_s$, $\mathsf{ar}(c) = \mathsf{ar}(c') = s$ and $c\ \mathsf{R}\ c'$ and
3. $f(\xi_1, \cdots, \xi_{\mathsf{rk}(f)})\ \mathsf{R}_P\ f(\xi'_1, \cdots, \xi'_{\mathsf{rk}(f)})$ whenever $\xi_i\ \mathsf{R}_P\ \xi'_i$ for all $i = 1, \ldots, \mathsf{rk}(f)$ and $f \in \Sigma_s \cup \Sigma_d$.

The proof of the following lemma is straightforward by structural induction.

Lemma 9. *Let ρ, ρ' be two closed substitutions such that $\rho(\zeta)\ \mathsf{R}_P\ \rho'(\zeta)$ for all $\zeta \in \mathcal{V} \cup \mathcal{D}$. Then $\rho(\vartheta)\ \mathsf{R}_P\ \rho'(\vartheta)$ for every term $\vartheta \in \mathbb{T}(\Sigma)$.*

For a bisimulation relation R, we have already defined that $\theta\ \mathsf{R}\ \theta'$ if and only if $[\![\theta]\!]\ \mathsf{R}\ [\![\theta']\!]$ for $\theta, \theta' \in T(\Sigma_d)$. This extends the definition of bisimulation relation to all closed distribution terms. We fix this notation from now on. In the following lemma we show that R_P lifts properly to distributions. This ensures that, though R_P is not yet proven to be a bisimulation relation, $[\![\theta]\!]\ \mathsf{R}_P\ [\![\theta']\!]$ whenever $\theta\ \mathsf{R}_P\ \theta'$.

Lemma 10. *Let $\mathsf{R} \subseteq T(\Sigma_s) \times T(\Sigma_s)$ be a bisimulation relation. Then, for all $\theta, \theta' \in T(\Sigma_d)$ such that $\theta\ \mathsf{R}_P\ \theta'$, $[\![\theta]\!]\ \mathsf{R}_P\ [\![\theta']\!]$.*

Proof. We proceed by induction on the definition of R_P. Case 1 does not apply since $\mathsf{R} \subseteq T(\Sigma_s) \times T(\Sigma_s)$. If it is due to case 2, by defining the weight function $w(c, c') = 1$ we can conclude that $[\![\boldsymbol{c}]\!]\ \mathsf{R}_P\ [\![\boldsymbol{c'}]\!]$.

For case 3 we proceed by case analysis in the three type of operations.

Case δ. Suppose $\delta(t)\ \mathsf{R}_P\ \delta(t')$. Then, necessarily, $t\ \mathsf{R}_P\ t'$. By defining the weight function $w(t, t') = 1$ we can conclude that $[\![\delta(t)]\!]\ \mathsf{R}_P\ [\![\delta(t')]\!]$.

Case $\oplus$. If $\bigoplus_{i \in I}[p_i]\theta_i\ \mathsf{R}_P\ \bigoplus_{i \in I}[p_i]\theta'_i$, $\theta_i\ \mathsf{R}_P\ \theta'_i$ for all $i \in I$. By the induction hypothesis $[\![\theta_i]\!]\ \mathsf{R}_P\ [\![\theta'_i]\!]$. Suppose that for each $i \in I$, this is witnessed by the weight function w_i. It is straightforward to conclude that w, defined by $w(t, t') = \sum_{i \in I} p_i w_i(t, t')$, for all $t, t' \in T(\Sigma_s)$, is a weight function witnessing $[\![\bigoplus_{i \in I}[p_i]\theta_i]\!]\ \mathsf{R}_P\ [\![\bigoplus_{i \in I}[p_i]\theta'_i]\!]$.

Case $\boldsymbol{f}$. Suppose $\boldsymbol{f}(\theta_1, \ldots, \theta_{\mathsf{rk}(f)})\ \mathsf{R}_P\ \boldsymbol{f}(\theta'_1, \ldots, \theta'_{\mathsf{rk}(f)})$. Then, $\theta_i\ \mathsf{R}_P\ \theta'_i$ and by the induction hypothesis $[\![\theta_i]\!]\ \mathsf{R}_P\ [\![\theta'_i]\!]$. Suppose that for each $i \in I$, this is witnessed by the weight function w_i. Suppose $\boldsymbol{f}$ is the probabilistic lifting of f with $\mathsf{ar}(f) = \sigma_1 \ldots \sigma_{\mathsf{rk}(f)} \to s$. Take the sets of indexes I and J that partition $\{1, \ldots, \mathsf{rk}(f)\}$ such that $\sigma_i = s$ for all $i \in I$ and $\sigma_j = d$ for all $j \in J$. Define function w by

$$w(f(\xi_1, \ldots, \xi_{\mathsf{rk}(f)}), f(\xi'_1, \ldots, \xi'_{\mathsf{rk}(f)})) = \prod_{i \in I} w_i(\xi_i, \xi'_i) \cdot \prod_{j \in J} \delta_{\theta_j}(\xi_j) \cdot \delta_{\theta'_j}(\xi'_j)$$

and $w(t, t') = 0$ in any other case. By calculating as in the proof of Proposition 3, we conclude that it is indeed a weight function witnessing $[\![\boldsymbol{f}(\theta_1, \ldots, \theta_{\mathsf{rk}(f)})]\!]\ \mathsf{R}_P\ [\![\boldsymbol{f}(\theta'_1, \ldots, \theta'_{\mathsf{rk}(f)})]\!]$. □

5.4. Proof of Theorem 4

Along the section we have set the basis for the proof of Theorem 4 whose core lies on Lemma 11. This lemma uses the inductive construction of Lemma 1 to show that R_P converges towards a bisimulation, provided that R is a bisimulation relation. The structure of its proof takes the ideas set in [5] with some stylized framework taken from [28,29]. However, the construction of the substitution on the simulating side requires particular ingenuity to adapt to probabilities and quantified premises.

Lemma 11. *Let P be a complete and pure PTSS in ntμfθ format. For all ordinal α, let $\langle \mathsf{CT}_\alpha, \mathsf{PT}_\alpha \rangle$ be the 3-valued models of P constructed inductively as in Lemma 1 with $\langle \mathsf{CT}_\lambda, \mathsf{PT}_\lambda \rangle$ being the 3-valued least stable model. (Hence $\mathsf{CT}_\lambda = \mathsf{PT}_\lambda$ is the transition relation associated to P.) Let R be a bisimulation relation (on the associated transition relation CT_λ). Then, for all $\alpha \leq \lambda$ and $t_1, t_2 \in T(\Sigma_s)$ such that $t_1\ \mathsf{R}_P\ t_2$,*

I_α. *$t_1 \xrightarrow{a} \theta_1 \in \mathsf{CT}_\alpha$ implies that $t_2 \xrightarrow{a} \theta_2 \in \mathsf{CT}_\lambda$ with $\theta_1\ \mathsf{R}_P\ \theta_2$, for some $\theta_2 \in T(\Sigma_d)$, and*
II_α. *$t_1 \xrightarrow{a} \theta_1 \in \mathsf{CT}_\lambda$ implies that $t_2 \xrightarrow{a} \theta_2 \in \mathsf{PT}_\alpha$ with $\theta_1\ \mathsf{R}_P\ \theta_2$, for some $\theta_2 \in T(\Sigma_d)$.*

Proof. We proceed by transfinite induction on α proving simultaneously both items. For case $\alpha = 0$, I_0 and II_0 hold immediately since $\mathsf{CT}_0 = \emptyset$ and $\mathsf{PT}_0 = T(\Sigma_s) \times A \times T(\Sigma_d)$. If α is a limit ordinal, I_α follows by transfinite induction from the fact that $\mathsf{CT}_\alpha = \bigcup_{\beta < \alpha} \mathsf{CT}_\beta$. II_α also follows from transfinite induction using the fact that $\mathsf{PT}_\alpha = \bigcap_{\beta < \alpha} \mathsf{PT}_\beta$ and considering that $\mathsf{PT}_\beta \supseteq \mathsf{PT}_{\beta'}$, whenever $\beta \leq \beta'$ (Lemma 1.1), to ensure that the existent θ_2 is the same for each $\beta < \alpha$.

We focus on the successor case and suppose, by induction hypothesis, that $\mathrm{I}_{\alpha-1}$ and $\mathrm{II}_{\alpha-1}$ hold.

If $t_1\ \mathsf{R}_P\ t_2$ because $t_1\ \mathsf{R}\ t_2$ (Definition 13, case 1), I_α and II_α follow from Lemma 1.1 which ensures that $\mathsf{CT}_\alpha \subseteq \mathsf{CT}_\lambda$ and $\mathsf{PT}_\alpha \supseteq \mathsf{PT}_\lambda = \mathsf{CT}_\lambda$.

We focus on the case in which $t_1 \mathrel{\mathsf{R}_P} t_2$ as a consequence of Definition 13.3. Then, $t_1 = f(\xi_1^1, \cdots, \xi_{\mathsf{rk}(f)}^1)$ and $t_2 = f(\xi_1^2, \cdots, \xi_{\mathsf{rk}(f)}^2)$ with $\xi_i^1 \mathrel{\mathsf{R}_P} \xi_i^2$, for all $i = 1, \ldots, \mathsf{rk}(f)$, and $f \in \Sigma_s$.

We proceed first with case I_α. Since $f(\xi_1^1, \cdots, \xi_{\mathsf{rk}(f)}^1) \xrightarrow{a} \theta_1 \in \mathsf{CT}_\alpha$, there is a set H of negative literals such that $P \vdash \frac{H}{f(\xi_1^1, \cdots, \xi_{\mathsf{rk}(f)}^1) \xrightarrow{a} \theta_1}$ and $\mathsf{PT}_{\alpha-1} \models H$. We use induction on the height γ of the proof of $P \vdash \frac{H}{f(\xi_1^1, \cdots, \xi_{\mathsf{rk}(f)}^1) \xrightarrow{a} \theta_1}$. So, by Definition 4, there must exist a rule r of the form

$$\frac{\{t_m(\vec{z}) \xrightarrow{a_m} \mu_m^{\vec{z}} \mid m \in M, \vec{z} \in \mathcal{Z}\} \cup \{t_n(\vec{z}) \stackrel{b_n}{\not\longrightarrow} \mid n \in N, \vec{z} \in \mathcal{Z}\} \cup \{\theta_l(Y_l) \trianglerighteq_{l,k} p_{l,k} \mid l \in L, k \in K_l\}}{f(\zeta_1, \ldots, \zeta_{\mathsf{rk}(f)}) \xrightarrow{a} \theta}$$

and a proper substitution ρ_1 such that

($\rho_1$1) $\rho_1(\zeta_i) = \xi_i^1$, for all $i \in \{1, \ldots, \mathsf{rk}(f)\}$,
($\rho_1$2) $\rho_1(\theta) = \theta_1$,
($\rho_1$3) for each $m \in M$ and $\vec{z} \in \mathcal{Z}$, there is a set $H_m^{\vec{z}} \subseteq H$ of negative literals such that $P \vdash \frac{H_m^{\vec{z}}}{\rho_1(t_m(\vec{z})) \xrightarrow{a_m} \rho_1(\mu_m^{\vec{z}})}$ is proved with a proof shorter than γ, and $\mathsf{PT}_{\alpha-1} \models H_m^{\vec{z}}$ (since $\mathsf{PT}_{\alpha-1} \models H$),
($\rho_1$4) for each $n \in N$ and $\vec{z} \in \mathcal{Z}$, $\rho_1(t_n(\vec{z})) \stackrel{b_n}{\not\longrightarrow} \in H$, hence $\mathsf{PT}_{\alpha-1} \models \rho_1(t_n(\vec{z})) \stackrel{b_n}{\not\longrightarrow}$, and
($\rho_1$5) for each $l \in L$ and $k \in K_l$, $[\![\rho_1(\theta_l)]\!](\rho_1(Y_l)) \trianglerighteq_{l,k} p_{l,k}$.

We construct a substitution ρ_2 such that, together with rule r, proves $f(\xi_1^2, \cdots, \xi_{\mathsf{rk}(f)}^2) \xrightarrow{a} \rho_2(\theta) \in \mathsf{CT}_\lambda$ and $\rho_1(\theta) \mathrel{\mathsf{R}_P} \rho_2(\theta)$. To construct ρ_2 we proceed by induction on the variable dependency graph of r.

Because of the quantitative premises, we need to collect in each set $\rho_2(Y_l)$ sufficient terms to let $[\![\rho_2(\theta_l)]\!](\rho_2(Y_l)) \trianglerighteq_{l,k} p_{l,k}$ hold. So, for each term in $t_1^* \in \rho_1(Y_l)$, we will let $\rho_2(Y_l)$ contains all terms t_2^* in the support set of $[\![\rho_2(\theta_l)]\!]$ such that $t_1^* \mathrel{\mathsf{R}_P} t_2^*$. For this we find a partition of the set of variables $\mathcal{Z}$ that makes room to allocate precisely all this terms for each $l \in L$.[4] The partition is constructed to keep the appropriate correspondence on the instances of vectors $\vec{z} \in \mathcal{Z}$, particularly if some $\mu_m^{\vec{z}}$ or $\vec{z}(l) \in Y_l$ is used in other place apart of its defining position.

Let $D = \{\rho_1(\vec{z}) \mid \vec{z} \in \mathcal{Z}\}$. Let $\Xi = \{Z_{\vec{d}} \subseteq \mathcal{Z} \mid \vec{d} \in D\}$ be a partition of $\mathcal{Z}$ such that for all $\vec{d} \in D$

(Ξ1) $|Z_{\vec{d}}| \geq \aleph_0$;
(Ξ2) there exists some $\vec{z} \in Z_{\vec{d}}$ such that $\rho_1(\vec{z}) = \vec{d}$;
(Ξ3) for all $\vec{z} \in \mathcal{Z}$ and $m \in M$, if $\mu_m^{\vec{z}} \in \mathit{Var}(\theta) \cup (\cup_{l \in L} \mathit{Var}(\theta_l)) \cup W$ and $\rho_1(\vec{z}) = \vec{d}$, then $\vec{z} \in Z_{\vec{d}}$ (here, W is as in Definition 10); and
(Ξ4) for all $\vec{z} \in \mathcal{Z}$, if, for some $l \in L$, $\vec{z}(l) \in Y_l \cap \left(\mathit{Var}(\theta) \cup \bigcup_{l' \in L} \mathit{Var}(\theta_{l'})\right)$ and $\rho_1(\vec{z}) = \vec{d}$, then $\vec{z} \in Z_{\vec{d}}$.

Condition (Ξ1) ensures that there are sufficient places for substitution ρ_2 to allocate all required terms to make the quantitative premises valid. Condition (Ξ2) associates the set of variable vectors $Z_{\vec{d}}$ with the vector $\vec{d}$. So, ρ_2 will be defined such that, for every $\vec{z} \in Z_{\vec{d}}$ and index k, $\vec{d}(k) \mathrel{\mathsf{R}_P} \rho_2(\vec{z}(k))$. Notice that ($\Xi$2) is only concerned with the existence of one $\vec{z} \in Z_{\vec{d}}$ such that $\rho_1(\vec{z}) = \vec{d}$ (by the definition of D such $\vec{z}$ can always exist). Any other $\vec{z}'$ satisfying the same condition is, in principle, ignored. This is so because $\rho_1(\vec{z}') = \rho_1(\vec{z})$ and for the construction of ρ_2 it is only important to know that the vector $\vec{d}$ is used by the proof of the transition. However, if any of the variables of $\vec{z}'$ is used in any of the bound terms, then we specially request that $\vec{z}'$ is also in $Z_{\vec{d}}$. This is required by (Ξ3) in the case that $\mu_m^{\vec{z}'}$ appears in θ, any θ_l, or W (and hence in some $t_m(\vec{z}')$ or $t_n(\vec{z}')$), and by (Ξ4) in the case that some $\vec{z}'(l)$ appears in θ or any θ_l. Conditions 1, 5, and 6 in Definition 10 ensure that the cardinality of $\mathcal{Z}$ is strictly larger than the set of vector variables under the conditions of (Ξ3) and (Ξ4). This, in turns, guarantees that each $Z_{\vec{d}}$ can be chosen to be infinitely large. Therefore, the partition Ξ indeed exists.

We define ρ_2 such that

---

[4] Contrarily to the non-probabilistic case (see, e.g., [2,4,5,28]), we cannot construct a substitution ρ_2 such that $\rho_1(\zeta) \mathrel{\mathsf{R}_P} \rho_2(\zeta)$ for every variable ζ. To understand why, consider a PTSS with constants c, d, and $\{n, n' \mid n \in \mathbb{N}\}$, a unary operator f, and rules

$$n \xrightarrow{a} \boldsymbol{n} \qquad c \xrightarrow{b} \theta \qquad \frac{x \xrightarrow{b} \mu \quad \mu(\{y_k \mid k \in \mathbb{N}_0\}) \geq 1 \quad \{y_k \stackrel{b}{\not\longrightarrow} \mu_k \mid k \in \mathbb{N}_0\}}{f(x) \xrightarrow{b} \mu}$$

$$n' \xrightarrow{a'} \boldsymbol{n'} \qquad d \xrightarrow{b} \theta'$$

with $\theta = \boldsymbol{1} \oplus_{\frac{1}{2}} \bigoplus_{n \in \mathbb{N}} \left[\frac{1}{2^{n+1}}\right] \boldsymbol{n'}$ and $\theta' = \boldsymbol{1'} \oplus_{\frac{1}{2}} \bigoplus_{n \in \mathbb{N}} \left[\frac{1}{2^{n+1}}\right] \boldsymbol{n}$.

Clearly $f(c) \sim f(d)$. Suppose that $f(c) \xrightarrow{a} \theta$ is proved using substitution ρ_1 such that $\rho_1(y_0) = 1$ and $\rho_1(y_n) = n'$ for $n \in \mathbb{N}$. Then any matching ρ_2 satisfying $\rho_1(\zeta) \mathrel{\mathsf{R}_P} \rho_2(\zeta)$ for every ζ will necessarily assign $\rho_2(y_n) = 1$ for every $n \geq 1$ and it only remains variable y_0 to fit one constant in $\{n \mid n \in \mathbb{N}\}$. Hence it is not possible to construct a substitution ρ_2 under the conditions above such that $\rho_2(\mu)(\rho_2(\{y_k \mid k \in \mathbb{N}_0\})) \geq 1$ holds.

Notice that, in principle, it is sufficient to find a ρ_2 such that $\forall k \in \mathbb{N}_0 : \exists k' \in \mathbb{N}_0 : \rho_1(y_k) \mathrel{\mathsf{R}_P} \rho_2(y_{k'})$, and $\forall k' \in \mathbb{N}_0 : \exists k \in \mathbb{N}_0 : \rho_1(y_k) \mathrel{\mathsf{R}_P} \rho_2(y_{k'})$, and, of course, meeting the conditions of the premises.

($\rho_2 1$) $\rho_1(\zeta)\ \mathsf{R}_P\ \rho_2(\zeta)$ for all $\zeta \in Var(\theta) \cup (\cup_{l \in L} Var(\theta_l)) \cup W \cup \{\zeta_1, \dots, \zeta_{\mathsf{rk}(f)}\}$,
($\rho_2 2$) $\rho_2(\Pi_l(Z_{\vec{d}})) = \left\{ t \in T(\Sigma_s) \mid \vec{d}(l)\ \mathsf{R}_P\ t \text{ and } [\![\rho_2(\theta_l)]\!](t) > 0 \right\}$,
($\rho_2 3$) $\rho_2(\zeta_i) = \xi_i^2$ for all $i \in \{1, \dots, \mathsf{rk}(f)\}$,
($\rho_2 4$) $\rho_2(t_m(\vec{z})) \xrightarrow{a_m} \rho_2(\mu_m^{\vec{z}}) \in \mathsf{CT}_\lambda$ for all $m \in M$ and $\vec{z} \in \mathcal{Z}$,
($\rho_2 5$) $[\![\rho_2(\theta_l)]\!](\rho_2(Y_l)) \trianglerighteq_{l,k} p_{l,k}$ for all $l \in L$ and $k \in K_l$, and
($\rho_2 6$) $\mathsf{CT}_\lambda \models \rho_2(t_n(\vec{z})) \stackrel{b_n}{\not\longrightarrow}$ for all $n \in N$ and $\vec{z} \in \mathcal{Z}$,

We prove ($\rho_2 1$)–($\rho_2 4$) by constructing ρ_2 inductively on the dependency degree of each variable (which we can do because r is well-founded). For $i \in \{1, \dots, \mathsf{rk}(f)\}$, define $\rho_2(\zeta_i) = \xi_i^2$, which immediately yields ($\rho_2 3$). Moreover, $\rho_1(\zeta_i) = \xi_i^1\ \mathsf{R}_P\ \xi_i^2 = \rho_2(\zeta_i)$ and hence ($\rho_2 1$) and ($\rho_2 2$) hold for this case. (($\rho_2 2$) holds trivially, since $\zeta_i \notin \bigcup_{l \in L} Y_l$).

For the inductive case, we assume that every variable ζ with degree$(\zeta) < k$ satisfy ($\rho_2 1$) and ($\rho_2 2$).

We analyze first the case of $\mu_m^{\vec{z}}$ with degree$(\mu_m^{\vec{z}}) = k$. Necessarily, $\vec{z} \in Z_{\vec{d}}$ for some $Z_{\vec{d}} \in \Xi$ since Ξ forms a partition of $\mathcal{Z}$. By ($\Xi 2$), there exists $\vec{z}' \in Z_{\vec{d}}$ such that $\rho_1(\vec{z}') = \vec{d}$. In particular, if $\mu_m^{\vec{z}} \in Var(\theta) \cup (\cup_{l \in L} Var(\theta_l)) \cup W$, we know by ($\Xi 3$) that $\rho_1(\vec{z}) = \vec{d}$, in which case we choose $\vec{z}' = \vec{z}$. Since all variables in $Var(t_m(\vec{z}))$ have a dependency degree smaller than k, using the induction hypothesis on ($\rho_2 1$) and ($\rho_2 2$) respectively, we have:

- If $\zeta \in Var(t_m(\vec{z})) \cap W$, $\rho_1(\vec{z}'(\zeta)) = \rho_1(\zeta)\ \mathsf{R}_P\ \rho_2(\zeta) = \rho_2(\vec{z}(\zeta))$. (Here $\vec{z}(\zeta)$ represents the variable in the coordinate ζ which is ζ itself.)
- For every $l \in L$, if $\zeta \in Var(t_m(\vec{z})) \cap Y_l$, then

$$\rho_2(\zeta) = \rho_2(\vec{z}(l)) \in \rho_2(\Pi_l(Z_{\vec{d}})) = \left\{ t \in T(\Sigma_s) \mid \vec{d}(l)\ \mathsf{R}_P\ t \text{ and } [\![\rho_2(\theta_l)]\!](t) > 0 \right\},$$

  and hence $\rho_1(\vec{z}'(l)) = \vec{d}(l)\ \mathsf{R}_P\ \rho_2(\vec{z}(l))$.

Therefore, by Lemma 9, $\rho_1(t_m(\vec{z}'))\ \mathsf{R}_P\ \rho_2(t_m(\vec{z}))$. Furthermore, by ($\rho_1 3$), there is a proof of $P \vdash \frac{H_m^{\vec{z}}}{\rho_1(t_m(\vec{z})) \xrightarrow{a_m} \rho_1(\mu_m^{\vec{z}})}$ with $\mathsf{PT}_{\alpha-1} \models H_m^{\vec{z}}$. Thus, $\rho_1(t_m(\vec{z}')) \xrightarrow{a_m} \rho_1(\mu_m^{\vec{z}'}) \in \mathsf{CT}_\alpha$. Since moreover, the proof is shorter than γ, by induction I_α, there exists $\theta' \in T(\Sigma_d)$ such that $\rho_2(t_m(\vec{z})) \xrightarrow{a_m} \theta' \in \mathsf{CT}_\lambda$ and $\rho_1(\mu_m^{\vec{z}'})\ \mathsf{R}_P\ \theta'$. Define $\rho_2(\mu_m^{\vec{z}}) = \theta'$. Then ($\rho_2 1$) holds since $\vec{z}'$ was chosen to be $\vec{z}$ in case $\mu_m^{\vec{z}} \in Var(\theta) \cup (\cup_{l \in L} Var(\theta_l)) \cup W$, and ($\rho_2 2$) holds trivially. Moreover, also ($\rho_2 4$) is satisfied.

It only remains to show the case of the term variables in $\bigcup_{l \in L} Y_l$. Recall that all variables in Y_l have the same dependency degree. So, we define ρ_2 simultaneously for all variables in Y_l with degree$(Y_l) = k$. We directly define ρ_2 such that

$$\rho_2(\Pi_l(Z_{\vec{d}})) = \left\{ t \in T(\Sigma_s) \mid \vec{d}(l)\ \mathsf{R}_P\ t \text{ and } [\![\rho_2(\theta_l)]\!](t) > 0 \right\} \tag{5}$$

for all $Z_{\vec{d}} \in \Xi$. For this to be a good definition, we need to show that

(i) $Y_l = \bigcup_{\vec{d} \in D} \Pi_l(Z_{\vec{d}})$,
(ii) $\Pi_l(Z_{\vec{d}}) \cap \Pi_l(Z_{\vec{d}'}) \neq \emptyset$ implies $Z_{\vec{d}} = Z_{\vec{d}'}$, and
(iii) there exists $t \in T(\Sigma_s)$ such that $\vec{d}(l)\ \mathsf{R}_P\ t$ and $[\![\rho_2(\theta_l)]\!](t) > 0$.

(i) is immediate since Ξ is a partition of $\mathcal{Z}$.

For (ii) suppose $y \in \Pi_l(Z_{\vec{d}}) \cap \Pi_l(Z_{\vec{d}'})$. Then, there is a $\vec{z} \in \mathcal{Z}$ such that $\vec{z}(l) = y$. By Definition 9, such $\vec{z}$ needs to be unique, from which (ii) follows.

For (iii) we proceed as follows. By induction on the dependency degree, we know that for all $\zeta \in Var(\theta_l)$, $\rho_1(\zeta)\ \mathsf{R}_P\ \rho_2(\zeta)$. Then, by Lemmas 9 and 10, $[\![\rho_1(\theta_l)]\!]\ \mathsf{R}_P\ [\![\rho_2(\theta_l)]\!]$. As a consequence, there is a weight function w such that

$$w(\vec{d}(l), T(\Sigma_s)) = [\![\rho_1(\theta_l)]\!](\vec{d}(l)) = [\![\rho_1(\theta_l)]\!](\rho_1(\vec{z}(l))) > 0$$

for some $\vec{z} \in Z_{\vec{d}}$. The existence of $\vec{z}$ is guaranteed by ($\Xi 2$) and the last inequality is a consequence of ρ_1 being proper. Then, there must exist some $t \in T(\Sigma_s)$ such that $w(\vec{d}(l), t) > 0$, and hence $\vec{d}(l)\ \mathsf{R}_P\ t$. Finally, we calculate

$$[\![\rho_2(\theta_l)]\!](t) = w(T(\Sigma_s), t) \geq w(\vec{d}(l), t) > 0$$

which proves (iii).

The definition in (5) not only ensures ($\rho_2 2$) but also ($\rho_2 1$) in case $y \in Var(\theta) \cup \bigcup_{l' \in L} Var(\theta_{l'})$. Indeed, if $\vec{z}$ is such that $\vec{z}(l) = y \in \Pi_l(Z_{\vec{d}})$, then $\vec{z} \in Z_{\vec{d}}$ and hence, necessarily $\rho_1(\vec{z}) = \vec{d}$ because of ($\Xi 4$). Therefore $\rho_1(y) = \vec{d}(l)\ \mathsf{R}_P\ \rho_2(y)$ since $y \in \Pi_l(Z_{\vec{d}})$.

It only remain to show cases ($\rho_2 5$) and ($\rho_2 6$). We focus first on ($\rho_2 5$). Because of ($\Xi 3$) and ($\rho_2 1$), $\rho_1(\zeta)\ \mathsf{R}_P\ \rho_2(\zeta)$ for all $\zeta \in Var(\theta_l)$, from which $[\![\rho_1(\theta_l)]\!]\ \mathsf{R}_P\ [\![\rho_2(\theta_l)]\!]$, because of Lemmas 9 and 10. Let w be the weight function that witness it. We can now calculate:

$$
\begin{aligned}
[\![\rho_2(\theta_l)]\!](\rho_2(Y_l)) &= \textstyle\sum_{t'\in\rho_2(Y_l)}[\![\rho_2(\theta_l)]\!](t') \\
&= \textstyle\sum_{t'\in\rho_2(Y_l)} w(T(\Sigma_s),t') && \text{(by property (ii) of weight functions)}\\
&= \textstyle\sum_{t\in T(\Sigma_s)}\sum_{t'\in\rho_2(Y_l)} w(t,t') \\
&\geq \textstyle\sum_{t\in\rho_1(Y_l)}\sum_{t'\in\rho_2(Y_l)} w(t,t') && \text{(because } \rho_1(Y_l)\subseteq T(\Sigma_s))\\
&= \textstyle\sum_{t\in\rho_1(Y_l)}\sum_{t'\in T(\Sigma_s)} w(t,t') && (*)\\
&= [\![\rho_1(\theta_l)]\!](\rho_1(Y_l)) && \text{(by property (i) of weight functions)}\\
&\trianglerighteq_{l,k} p_{l,k} && \text{(by } (\rho_1 5))
\end{aligned}
$$

Since $t\in\rho_1(Y_l)$ there must exist $\vec{d}\in D$ such that $\vec{d}(l)=t$. Then, by property (iii) of weight functions, $w(t,t')>0$ implies $t\,\mathsf{R}_P\,t'$ and hence $t'\in\rho_2(\Pi_l(Z_{\vec{d}}))\subseteq\rho_2(Y_l)$. From here, if $t'\notin\rho_2(Y_l)$, $w(t,t')=0$, which justifies (*).

Finally we prove $(\rho_2 6)$. $(\rho_2 1)$ and Lemma 9 imply that $\rho_1(t_n(\vec{z}))\,\mathsf{R}_P\,\rho_2(t_n(\vec{z}))$. By contradiction assume $\rho_2(t_n(\vec{z}))\xrightarrow{b_n}\theta'_2\in\mathsf{CT}_\lambda$ for some $\theta'_2\in T(\Sigma_d)$. By induction, $\mathrm{II}_{\alpha-1}$ implies $\rho_1(t_n(\vec{z}))\xrightarrow{b_n}\theta'_1\in\mathsf{PT}_{\alpha-1}$ for some $\theta'_1\in T(\Sigma_d)$. However, this contradicts $(\rho_1 4)$ which states that $\rho_1(t_n(\vec{z}))\xrightarrow{b_n}\!\!\!\!\!\!/\;\;\in H$ and $\mathsf{PT}_{\alpha-1}\models H$.

Properties $(\rho_2 1)$–$(\rho_2 6)$ imply that rule r together with substitution ρ_2 form the basis of the proof of a transition rule $\frac{H'}{f(\xi^2_1,\cdots,\xi^2_{\mathsf{rk}(f)})\xrightarrow{a}\rho_2(\theta)}$ with $\mathsf{CT}_\lambda\models H'$. Hence $f(\xi^2_1,\cdots,\xi^2_{\mathsf{rk}(f)})\xrightarrow{a}\rho_2(\theta)\in\mathsf{CT}_\lambda$. By $(\rho_2 1)$ and Lemma 9, $\rho_1(\theta)\,\mathsf{R}_P\,\rho_2(\theta)$, which concludes the proof of I_α.

The proof of case II_α follows symmetrically to the case I_α only that when it says CT_α and $\mathsf{PT}_{\alpha-1}$, it should be changed by CT_λ, and when it says CT_λ, it should be changed appropriately by PT_α or $\mathsf{CT}_{\alpha-1}$. For the sake of completeness, we spell this part of the proof out in Appendix B. □

Theorem 4 follows as a corollary of Lemma 11.

Proof of Theorem 4. By Corollaries 6 and 8 there is an equivalent complete and pure PTSS P' in $nt\mu f\theta$ format. Therefore P' is in the conditions of Lemma 11. By taking $R=\sim$ and $\alpha=\lambda$ in Lemma 11 we can conclude that $\sim_P$ is a bisimulation relation and, since $\sim\subseteq\sim_P$ by Definition 13, $\sim=\sim_P$. Also, by Definition 13, $\sim_P$ preserves all operators in P', and hence in P. As a consequence $\sim$ is a congruence for all operators in P. □

6. Modular properties

Often, one wants to extend a language with new operations and behaviors. This is naturally done by adding new functions and rules to the original PTSS. In other words, given two PTSSs $P^0=(\Sigma^0,A^0,R^0)$ and $P^1=(\Sigma^1,A^1,R^1)$, one wants to combine them in a new PTSS $P^0\uplus P^1$, where we generally assume that P^0 is the original PTSS and P^1 is the extension.[5] A desired property is that the extension does not alter the behavior of the terms in the original language. That is, one expects that for every old term $t\in T(\Sigma^0_s)$, the set of outgoing transitions defined by P^0 is exactly the same that those defined by $P^0\uplus P^1$. In this case we say that $P^0\uplus P^1$ is a *conservative extension* of P^0.

The property of conservative extension has been studied in the non-probabilistic setting (see [32,29,8] and references therein). In this section, we adapt the definition of conservative extension to the probabilistic setting and provide important results that connect the syntactic definition to the models of the original PTSS and its extension. We actually take the results from [29,8] which apply with fairly minor changes to the probabilistic setting.

In order to combine two PTSSs, the function names should provide the same functionality in both signatures. Provided this hold, the union or *sum* of the two PTSSs is definable.

Definition 14. Let $\Sigma^0=(F^0,\mathsf{ar}^0)$ and $\Sigma^1=(F^1,\mathsf{ar}^1)$ be two S-sorted signatures such that for all $f\in F^0\cap F^1$, $\mathsf{ar}^0(f)=\mathsf{ar}^1(f)$. In such case, the *sum* of Σ^0 and Σ^1, denoted by $\Sigma^0\uplus\Sigma^1$, is defined as the new signature $(F^0\cup F^1,\mathsf{ar}^0\cup\mathsf{ar}^1)$.

Definition 15. Let $P^0=(\Sigma^0,A^0,R^0)$ and $P^1=(\Sigma^1,A^1,R^1)$ be two PTSSs such that the sum $\Sigma^0\uplus\Sigma^1$ is defined. Then, the *sum* of P^0 and P^1, denoted by $P^0\uplus P^1$, is also defined, in which case $P^0\uplus P^1=(\Sigma^0\uplus\Sigma^1,A^0\cup A^1,R^0\cup R^1)$.

In early definitions (e.g. [2,4,32]) an extension $P^0\uplus P^1$ is conservative w.r.t. P^0 if the original semantics of a term t in P^0 is exactly the same in $P^0\uplus P^1$. In other words, $t\xrightarrow{a}\theta$ is a transition in the *unique* model of P^0 if and only if it is also a transition in the *unique* model of $P^0\uplus P^1$. However, to have such a requirement, we need that both P^0 and $P^0\uplus P^1$ are,

[5] Normally, the combinations of two TSSs is denoted with the symbol ⊕ instead of ⊎. We have chosen the second symbol to avoid confusion with our probabilistic summation operator which is usually also denoted with ⊕.

complete at the least. We will now give a general definition and show later that the particular case of complete PTSSs is as expected. Inspired by the fact that only rules with only negative premises play a role in the definition of 3-valued stable models (see Definition 5 and also Lemma 2), we have the following definition.

Definition 16. $P^0 \uplus P^1$ is a *conservative extension* of P^0 if for all $t \in T(\Sigma_s^0)$, $a \in A^0 \cup A^1$, $\theta \in T(\Sigma_d^0 \cup \Sigma_d^1)$ and set of closed negative premises N, $P^0 \uplus P^1 \vdash \frac{N}{t \xrightarrow{a} \theta}$ implies $P^0 \vdash \frac{N}{t \xrightarrow{a} \theta}$.

Notice that the implication in the other direction is an immediate consequence of all rules of P^0 being also rules of $P^0 \uplus P^1$.

Theorem 12 below gives a general syntactic characterization to ensure that $P^0 \uplus P^1$ is a conservative extension of P^0. First, some few concepts and shorthands need to be introduced.

Definition 17. A variable ζ is *source dependent* in a rule $\frac{H}{t \xrightarrow{a} \theta}$ if one of the following statements holds:

- $\zeta \in Var(t)$,
- there exists $t^* \xrightarrow{b} \theta^* \in H$ such that all variables in $Var(t^*)$ are source dependent and $\zeta \in Var(\theta^*)$, or
- there exists $\theta^*(T) \bowtie p \in H$ such that all variables in $Var(\theta^*)$ are source dependent and $\zeta \in Var(t^*)$ for some $t^* \in T$.

We say that a rule is *source dependent* if all its variables are. Similarly, we say that a PTSS is *source dependent* if all its rules are.

The term t in rule $\frac{H}{t \xrightarrow{a} \theta}$ is usually called the "source" of the rule, therefore the name of "source dependent". It is worth to notice that if a rule is pure, then it is source dependent.

Given two signatures Σ^0 and Σ^1, a term $\xi \in \mathbb{T}(\Sigma^0 \uplus \Sigma^1)$ is said to be *fresh* if $\xi \notin \mathbb{T}(\Sigma^0)$. That is, a term is fresh if it contains a function name of the new signature Σ^1.

Let r be a rule of $P^0 \uplus P^1$. We let $r\lfloor$ denote the same rules as r where all the premises whose leading terms are fresh have been removed. (By "leading terms" we mean the left-hand side terms in positive and negative premises, and the distribution term in the quantitative premises.) That is, if $r = \frac{H}{t \xrightarrow{a} \theta}$ then

$$r\lfloor = \frac{\{t^* \xrightarrow{b} \theta^* \in H \mid t^* \in \mathbb{T}(\Sigma^0)\} \cup \{t^* \xrightarrow{b}\!\!\!\!\!/ \;\in H \mid t^* \in \mathbb{T}(\Sigma^0)\} \cup \{\theta^*(T^*) \bowtie p \in H \mid \theta^* \in \mathbb{T}(\Sigma^0)\}}{t \xrightarrow{a} \theta}$$

Now we are in conditions to state the theorem.

Theorem 12. *Under the following conditions $P^0 \uplus P^1$ is a conservative extension of P^0:*

1. *for every rule $r \in R^0$, all its variables are source dependent, and*
2. *for every rule $r = \frac{H}{t \xrightarrow{a} \theta} \in R^1$, one of the following conditions hold:*
   (a) *t is fresh,*
   (b) *or there is a positive premise $t^* \xrightarrow{b} \theta^* \in H$ such that*
      (i) *$t^* \in \mathbb{T}(\Sigma^0)$,*
      (ii) *all variables in $Var(t^*)$ are source dependent in $r\lfloor$, and*
      (iii) *either $b \notin A^0$ or θ^* is fresh;*
   (c) *or there is a quantitative premise $\theta^*(T^*) \bowtie p \in H$ such that*
      (i) *$\theta^* \in \mathbb{T}(\Sigma^0)$,*
      (ii) *all variables in $Var(\theta^*)$ are source dependent in $r\lfloor$, and*
      (iii) *T^* contains a fresh term.*

The proof of Theorem 12 follows the same structure of the proof of Theorem 3.20 in [29]. However, we report a proof in Appendix C since the quantitative premises require some special treatment.

Definition 16 provides a *syntactic* notion of conservative extension in the sense that the extension preserves exactly all provable rules of the form $\frac{N}{t \xrightarrow{a} \theta}$ with N being a set of negative premises and t being an "old" term. Since rules with only negative premises are fundamental on the construction of the models (see Definition 5) we expect also that the models defined by the extended PTSS are also a "conservative extension" of the models of the original PTSS. In this case, we mean that each model of the extended PTSS is a model of the original PTSS when restricted to the original terms, and moreover, every model of the original PTSS can be extended to a model of the extended PTSS without changing the (certain or possible) transitions of the old terms. This is stated by Theorem 13.

We first introduce some short-hand notation. Let Tr be a set of transition relations with terms over the signature $\Sigma^0 \uplus \Sigma^1$. We let $\mathsf{Tr}\lfloor = \{t \xrightarrow{a} \theta \in \mathsf{Tr} \mid t \in T(\Sigma_0)\}$ be the subset of Tr where all transitions with fresh sources have been removed.

Theorem 13. *Let $P^0 \uplus P^1$ be a conservative extension of P^0. Then,*

1. *if $\langle \mathsf{CT}, \mathsf{PT}\rangle$ is a 3-valued stable model of $P^0 \uplus P^1$, $\langle \mathsf{CT}\lfloor, \mathsf{PT}\lfloor\rangle$ is a 3-valued stable model of P_0; and*
2. *if $\langle \mathsf{CT}, \mathsf{PT}\rangle$ is a 3-valued stable model of P_0, there is a 3-valued stable model $\langle \mathsf{CT}', \mathsf{PT}'\rangle$ of $P^0 \uplus P^1$ such that $\mathsf{CT} = \mathsf{CT}'\lfloor$ and $\mathsf{PT} = \mathsf{PT}'\lfloor$.*

The previous theorem refers to stable models in general. More importantly a conservative extension also preserves the *least* stable model.

Theorem 14. *Let $P^0 \uplus P^1$ be a conservative extension of P^0. If $\langle \mathsf{CT}, \mathsf{PT}\rangle$ is the least 3-valued stable model of $P^0 \uplus P^1$ then $\langle \mathsf{CT}\lfloor, \mathsf{PT}\lfloor\rangle$ is the least 3-valued stable model of P_0.*

The proofs of statements 1 and 2 in Theorem 13, and Theorem 14 are exactly the same as the proofs of Theorems 3.24, 3.25, and 3.26 of [29], respectively, with very minor adaptations to accommodate our setting. So we directly refer the reader to [29] for the proofs.

It is immediate from Theorem 14 that if $P^0 \uplus P^1$ is complete and a conservative extension of P^0, then P_0 is also complete. However, as shown in [29], it is not generally the case that if P_0 is complete, so is its conservative extension $P^0 \uplus P^1$. In fact, it is also not true that if P_0 and P_1 are complete, so is the conservative extension $P^0 \uplus P^1$. This is shown by taken P_0 to be a PTSS with only a constant a and the rules $\frac{}{a \xrightarrow{a} \delta(a)}$ and $\frac{x \stackrel{a}{\not\longrightarrow}}{x \xrightarrow{a} \delta(x)}$, and P_1 the PTSS with only constant b and no rules. Then $\langle \{a \xrightarrow{a} \delta(a)\}, \{a \xrightarrow{a} \delta(a)\}\rangle$ and $\langle \emptyset, \emptyset\rangle$ are the only stable models of P_0 and P_1, respectively —hence P_0 and P_1 are complete—, and $\langle \{a \xrightarrow{a} \delta(a)\}, \{a \xrightarrow{a} \delta(a), b \xrightarrow{a} \delta(b)\}\rangle$ is the only 3-stable model of $P^0 \uplus P^1$.

7. Tracing bisimulation

An equivalence relation is said to be *fully abstract* w.r.t. a set of operators Σ and another equivalence $\equiv$ if it is the coarsest congruence for all contexts constructed with operators in Σ that is included in $\equiv$. This concept can be lifted to a particular PTSS format as follows: an equivalence relation on PTSs is fully abstract w.r.t. a PTSS format and an equivalence $\equiv$ if it is the coarsest congruence for all context constructed with operators specifiable in a complete PTSS in such format and that is finer than $\equiv$ [10].

Two terms are *(possibilistic)* trace equivalent if they can perform the same sequences of actions with some positive probability (but not necessarily the same). In this section we show that a "finitary" version of the bisimulation equivalence —which we called *bounded bisimilarity*— is fully abstract with respect to the *ntμfθ/ntμxθ* format and trace equivalence. That is, we show that the trace congruence induced by the *ntμfθ/ntμxθ* format is exactly the bounded bisimulation equivalence. In particular, the bounded bisimulation equivalence agrees with $\sim$ on image finite probabilistic transition systems. (A transition relation $\longrightarrow$ is image-finite iff for all $t \in T(\Sigma)$ and $a \in A$, the set $\{\theta \mid t \xrightarrow{a} \theta\}$ is finite.)

Definition 18. Let $P = (\Sigma, A, R)$ be a complete PTSS and $\longrightarrow$ its associated transition relation. Given $t \in T(\Sigma_s)$, a sequence $a_1 \dots a_n \in A^*$ is a trace from t iff there are terms $t_0, \dots, t_n \in T(\Sigma_s)$ and $\theta_1, \dots, \theta_n \in T(\Sigma_d)$ s.t. $t_0 = t$, $t_i \xrightarrow{a_{i+1}} \theta_{i+1}$ and $[\![\theta_{i+1}]\!](t_{i+1}) > 0$ for $0 \le i < n$. Let *traces*(t) be the set of all traces from t. Terms $t, t' \in T(\Sigma_s)$ are *trace equivalent (with respect to P)*, notation $t \equiv^{\mathrm{t}}_P t'$, iff *traces*$(t) =$ *traces*(t').

Definition 19. Let P be a complete PTSS in *ntμfθ/ntμxθ* format. Terms $t, t' \in T(\Sigma_s)$ are *trace congruent with respect to ntμfθ/ntμxθ* if for every PTSS P' in *ntμfθ/ntμxθ* format such that $P \uplus P'$ is complete, well-founded and a conservative extension of P, $C[t] \equiv^{\mathrm{t}}_{P \uplus P'} C[t']$ for every context $C[\_]$ of $P \uplus P'$. In this case we write $t \equiv^{\mathrm{t}}_{nt\mu f\theta/nt\mu x\theta} t'$.

Then, it is our aim to show that $\equiv^{\mathrm{t}}_{nt\mu f\theta/nt\mu x\theta}$ agrees precisely with the bounded bisimulation equivalence which is formally defined as follows.

Definition 20. Let $P = (\Sigma, A, R)$ be a complete PTSS and let $\longrightarrow$ be its associated transition relation. For each $n \in \mathbb{N}$, we define $\simeq^n_P \subseteq T(\Sigma_s) \times T(\Sigma_s)$ inductively by:

$$\begin{aligned}
\simeq^0_P \; &= \; T(\Sigma_s) \times T(\Sigma_s) \\
\simeq^{n+1}_P \; &= \; \{(t, t') \mid (\forall \theta : t \xrightarrow{a} \theta \Rightarrow \exists \theta' : t' \xrightarrow{a} \theta' \wedge \theta \simeq^n_P \theta') \wedge \\
&\qquad\qquad (\forall \theta' : t' \xrightarrow{a} \theta' \Rightarrow \exists \theta : t \xrightarrow{a} \theta \wedge \theta \simeq^n_P \theta')\}
\end{aligned}$$

$$\mathsf{B}_0(x,y) \xrightarrow{yes} \bot \qquad T1$$

$$\frac{x \xrightarrow{a} \mu \quad \{\mu(Z_i) \geq q_i,\ \mathsf{B}_{n-1}(z_i, Z_i) \xrightarrow{yes} \mu_i\}_{i=1}^{k}}{\mathsf{Pr}_n^k(x, z_1, \dots, z_k) \xrightarrow{(a,q_1,\dots,q_k)} \bot} \qquad T2$$

$$\frac{\mathsf{Pr}_n^k(x, z_1, \dots, z_k) \xrightarrow{(a,q_1,\dots,q_k)} \mu \quad \mathsf{Pr}_n^k(y, z_1, \dots, z_k) \stackrel{(a,q_1,\dots,q_k)}{\not\longrightarrow}}{\mathsf{B}_n(x,y) \xrightarrow{no} \bot} \qquad T3$$

$$\frac{\mathsf{B}_n(x,y) \stackrel{no}{\not\longrightarrow} \quad \mathsf{B}_n(y,x) \stackrel{no}{\not\longrightarrow}}{\mathsf{B}_n(x,y) \xrightarrow{yes} \bot} \ (4) \qquad T4$$

Fig. 4. Rules for the bisimulation tester (for all $n, k > 0$, $a \in A$ and $q_1, \dots, q_k \in \mathbb{Q}$).

(We use $\theta \simeq_P^n \theta'$ as a shorthand for $[\![\theta]\!] \simeq_P^n [\![\theta']\!]$.) Whenever $t \simeq_P^n t'$ we say that t and t' are *n-bounded bisimilar* Moreover, we say that t and t' are *bounded bisimilar*, notation $t \simeq_P t'$, if $t \simeq_P^n t'$ for all $n \in \mathbb{N}$.

It is easy to see that each $\simeq_P^n$ is an equivalence relation and, as a consequence, so is $\simeq_P$. Bounded bisimilarity and bisimulation equivalence agree on image-finite probabilistic transition systems [22, Lemma 3.5.8]. That is, if $\to$ is image-finite, then $\sim = \simeq_P$.

We now define the *bisimulation tester*, that is, a PTSS P^T that can be added conservatively to another PTSS and that introduces contexts that are able to distinguish terms that are not bounded bisimilar. More precisely, P^T introduces a trivial constant $\bot$ and two family of functions: binary functions B_n and $(k+1)$-ary functions Pr_n^k, where $n, k \in \mathbb{N}$. Their intended meaning is as follows. $\mathsf{B}_n(t,u)$ can detect whether t and u are n-bounded bisimilar by showing transition $\mathsf{B}_n(t,u) \xrightarrow{yes} \bot$. Otherwise, $\mathsf{B}_n(t,u) \xrightarrow{no} \bot$. In this way, two non-bisimilar terms t and u can be distinguished by the context $\mathsf{B}_n(t,\_)$ for some appropriate n. Pr_n^k is used as an auxiliary operator to test the measures of k (not necessarily different) $(n-1)$-bounded bisimulation equivalence classes. More precisely, $\mathsf{Pr}_n^k(t, u_1, \cdots, u_k) \xrightarrow{(a,q_1,\dots,q_k)} \bot$ if there is a transition $t \xrightarrow{a} \theta$ such that $[\![\theta]\!]([u_1]_{\simeq^{n-1}}) \geq q_1, \dots, [\![\theta]\!]([u_k]_{\simeq^{n-1}}) \geq q_k$, where $[u_j]_{\simeq^{n-1}} = \{u \in T(\Sigma_s) \mid u_j \simeq^{n-1} u\}$ and $q_1, \dots, q_k \in \mathbb{Q}$. We write $\mathsf{B}_{n-1}(z_i, Z_i) \xrightarrow{yes} \mu_i$ to denote the set $\{\mathsf{B}_{n-1}(z_i, z) \xrightarrow{yes} \mu_i \mid z \in Z_i\}$ following the notation introduced at the end of Section 4.

Definition 21. Let $P = (\Sigma, A, R)$ be a PTSS. The *bisimulation tester of* P is the PTSS $P^T = (\Sigma^T, A \cup A^T, R^T)$ where

- $\Sigma_s \cap \Sigma_s^T = \emptyset$ and Σ_s^T contains binary functions B_n and $(k+1)$-ary functions Pr_n^k for all $n \in \mathbb{N}$, and the constant $\bot$;
- $A^T = (\bigcup_{i>0}(A \times \mathbb{Q}^i)) \cup \{yes, no\}$; and
- R^T contains the rules given in Fig. 4.

The idea behind functions Pr_n^k explained above becomes apparent in rule $T2$. Besides, notice that distinction between two non-n-bounded bisimilar terms is revealed by rule $T3$. There, the negative premise indicates that there is no a-transition from the instance of y that measures more than q_i in each equivalence class $[z_i]_{\simeq^{n-1}}$ (in the appropriate instance of z_i) while the positive premise indicates that the instance of x *has* an a transition of this kind.

Observe that P^T is well-founded and in *ntμfθ* format but is *not* pure. Though this is not necessary, it is quite convenient in our case: the non-pure rule $T3$ allows for instances of arbitrary terms (and hence arbitrary $(n-1)$-bounded bisimulation equivalence classes) which is in the core of the definition of the n-bisimulations. Nevertheless, the family of rules $T3$ can be replaced by an equivalent set of pure rules as stated in Lemma 7.

Finally, notice that if P is a source dependent PTSS then $P \uplus P^T$ satisfies the hypothesis of Theorem 12 (the conclusion of each rule in P^T contain only fresh terms) and, as a consequence, $P \uplus P^T$ is a conservative extension of P.

The following lemma is central to our main result presented in Theorem 16 below.

Lemma 15. *Let $P = (\Sigma, A, R)$ be a complete PTSS in ntμfθ/ntμxθ format such that $P \uplus P^T$ conservatively extends P and is also complete. If* Tr *is the associated transition relation of $P \uplus P^T$, then*

1. $t \simeq_P^n t'$ *implies* $\mathsf{B}_n(t,t') \xrightarrow{yes} \bot \in \mathsf{Tr}$, *for all* $t, t' \in T(\Sigma_s)$; *and*
2. *if in addition either* Tr *is image finite or* Σ_d *only contains finitary and rational instances of* $\oplus$, $\mathsf{B}_n(t,t') \xrightarrow{yes} \bot \in \mathsf{Tr}$ *implies* $t \simeq_P^n t'$, *for all* $t, t' \in T(\Sigma_s)$.

Proof. First notice that, as a consequence of Theorem 14, $\mathsf{Tr}\!\!\downharpoonright$ is the associated transition relation of P.

Case 1. We prove it by induction on n. Notice that for all $t, t' \in T(\Sigma_s)$, $\mathsf{B}_0(t,t') \xrightarrow{yes} \bot \in \mathsf{Tr}$ because of rule $T1$,[6] hence case $n = 0$ follows trivially. For the induction case, suppose item 1 is valid for n, we show it also holds for $n+1$.

By contradiction, let $\mathsf{B}_{n+1}(t,t') \xrightarrow{yes} \bot \notin \mathsf{Tr}$. Because of rule $T4$, suppose w.l.o.g., that $\mathsf{Tr} \not\models \mathsf{B}_{n+1}(t,t') \xrightarrow{no}\!\!\!\!\!\!/\ \ $. Hence $\mathsf{Tr} \models \mathsf{B}_{n+1}(t,t') \xrightarrow{no} \bot$. By rule $T3$,

$$\mathsf{Tr} \models \mathsf{Pr}^k_{n+1}(t, t_1, \ldots, t_k) \xrightarrow{(a,q_1,\ldots,q_k)} \bot \quad \text{and} \tag{6}$$

$$\mathsf{Tr} \models \mathsf{Pr}^k_{n+1}(t', t_1, \ldots, t_k) \xrightarrow{(a,q_1,\ldots,q_k)}\!\!\!\!\!\!\!\!\!\!/\ \ \ \ \ , \tag{7}$$

for some $k \in \mathbb{N}$, $t_1, \ldots, t_k \in T(\Sigma_s \uplus \Sigma_s^T)$, $q_1, \ldots, q_k \in \mathbb{Q}$, and $a \in A$.

From (6) and rule $T2$, there exist $\theta \in T(\Sigma_d)$ and $T_1, \ldots T_k \subseteq supp(\llbracket\theta\rrbracket)$ such that $\mathsf{Tr} \models t \xrightarrow{a} \theta$, $\mathsf{Tr} \models \mathsf{B}_n(t_i, T_i) \xrightarrow{yes} \bot$, and $\theta(T_i) \geq q_i$ for all $i \in \{1 \ldots k\}$. By induction hypothesis, $T_i \subseteq [t_i]_{\simeq^n}$ for all i.

Besides, since $t \in T(\Sigma_s)$, $t \xrightarrow{a} \theta \in \mathsf{Tr}\rfloor$. Because $t \simeq_P^{n+1} t'$ there is some $\theta' \in T(\Sigma_d)$ such that $t' \xrightarrow{a} \theta' \in \mathsf{Tr}\rfloor \subseteq \mathsf{Tr}$ and $\theta \simeq_P^n \theta'$. For each i, define $T_i' = [t_i]_{\simeq^n} \cap supp(\llbracket\theta'\rrbracket)$. By induction hypothesis, $\mathsf{B}_n(t_i, T_i') \xrightarrow{yes} \bot \in \mathsf{Tr}$. Moreover, we can calculate $\llbracket\theta'\rrbracket(T_i') = \llbracket\theta'\rrbracket([t_i]_{\simeq^n}) = \llbracket\theta\rrbracket([t_i]_{\simeq^n}) \geq \llbracket\theta\rrbracket(T_i) \geq q_i$. Instantiating rule $T2$ we obtain

$$\frac{t' \xrightarrow{a} \theta' \quad \{\theta'(T_i') \geq q_i,\ \mathsf{B}_n(t_i, T_i') \xrightarrow{yes} \bot\}_{i=1}^k}{\mathsf{Pr}^k_{n+1}(t', t_1, \ldots, t_k) \xrightarrow{(a,q_1,\ldots,q_k)} \bot}$$

Since we have just proved that all premises hold in Tr, $\mathsf{Tr} \models \mathsf{Pr}^k_{n+1}(t', t_1, \ldots, t_k) \xrightarrow{(a,q_1,\ldots,q_k)} \bot$. This contradicts (7), which proves this part of the lemma.

Case 2. We prove it by induction on n. Definition 20 states that for all $t, t' \in T(\Sigma_s)$, $t \simeq_P^0 t'$, hence case $n = 0$ follows trivially. For the induction case, suppose item 2 is valid for n, we show it also holds for $n+1$.

By contradiction suppose $t \not\simeq_P^{n+1} t'$. Then, w.l.o.g., assume that for some $a \in A$ and $\theta \in T(\Sigma_d)$,

$$t \xrightarrow{a} \theta \in \mathsf{Tr}\rfloor \text{ but there is no } \theta' \in T(\Sigma_d) \text{ such that } t' \xrightarrow{a} \theta' \in \mathsf{Tr}\rfloor \text{ and } \theta \simeq_P^n \theta'. \tag{8}$$

Let $\Theta = \{\theta' \mid t' \xrightarrow{a} \theta'\}$. Suppose first $\Theta \neq \emptyset$.

If Tr is image finite then Θ is finite. Hence there are $k \leq |\Theta|$ different equivalence classes, $C_1, \ldots, C_k \in T(\Sigma_s)/\simeq_P^n$, such that for each $\theta' \in \Theta$, $\llbracket\theta\rrbracket(C_i) \neq \llbracket\theta'\rrbracket(C_i)$ for some $i \in \{1, \ldots, k\}$. Moreover, we can safely assume that $\llbracket\theta\rrbracket(C_i) > \llbracket\theta'\rrbracket(C_i)$.[7] In addition, for all $i \in \{1, \ldots, k\}$, define $q_i \in \mathbb{Q}$ such that $\llbracket\theta\rrbracket(C_i) \geq q_i > \sup\{\llbracket\theta'\rrbracket(C_i) \mid \theta' \in \Theta, \llbracket\theta\rrbracket(C_i) > \llbracket\theta'\rrbracket(C_i)\}$. (Since Θ is finite and $\mathbb{Q}$ is dense, q_i always exists.)

If Σ_d only contains finitary and rational instances of $\oplus$ then, by straightforward induction, it can be proved that $\llbracket\theta\rrbracket$ has finite support. Then, let $C_1, \ldots, C_k \in T(\Sigma_s)/\simeq_P^n$ be all the different equivalence classes such that $\llbracket\theta\rrbracket(C_i) > 0$ for all $i \in \{1, \ldots, k\}$ and $\sum_{i=1}^k \llbracket\theta\rrbracket(C_i) = 1$. Again, for each $\theta' \in \Theta$, $\llbracket\theta\rrbracket(C_i) > \llbracket\theta'\rrbracket(C_i)$ for some $i \in \{1, \ldots, k\}$ as a consequence of (8). It can be shown by induction that $\llbracket\theta\rrbracket(C_i)$ is a rational number, using the fact that we can only use rational numbers p_i in terms of the form $\bigoplus_{i=1}^m [p_i] t_i$. So, in this case, we define $q_i = \llbracket\theta\rrbracket(C_i)$ for all $i \in \{1, \ldots, k\}$. (Since Θ may be infinite, $\sup\{\llbracket\theta'\rrbracket(C_i) \mid \theta' \in \Theta, \llbracket\theta\rrbracket(C_i) > \llbracket\theta'\rrbracket(C_i)\}$ could converge to q_i. That is why here we define q_i differently.)

By letting $T_i = C_i \cap supp(\llbracket\theta\rrbracket)$, in any case, we have that

$$\begin{aligned} &\text{for all } i \in \{1, \ldots, k\},\ \llbracket\theta\rrbracket(T_i) = \llbracket\theta\rrbracket(C_i) \geq q_i, \text{ and} \\ &\text{for all } \theta' \in \Theta, q_i > \llbracket\theta'\rrbracket(C_i), \text{ for some } i \in \{1, \ldots, k\}. \end{aligned} \tag{9}$$

Let $t_i \in C_i$. By induction hypothesis, $\mathsf{B}_n(t_i, T_i) \xrightarrow{yes} \bot \in \mathsf{Tr}$. Instantiating rule $T2$ we obtain

$$\frac{t \xrightarrow{a} \theta \quad \{\theta(T_i) \geq q_i,\ \mathsf{B}_n(t_i, T_i) \xrightarrow{yes} \bot\}_{i=1}^k}{\mathsf{Pr}^k_{n+1}(t, t_1, \ldots, t_k) \xrightarrow{(a,q_1,\ldots,q_k)} \bot}$$

Because all premises hold in Tr,

$$\mathsf{Tr} \models \mathsf{Pr}^k_{n+1}(t, t_1, \ldots, t_k) \xrightarrow{(a,q_1,\ldots,q_k)} \bot. \tag{10}$$

[6] Along this proof we omit making reference to the existence of an appropriate substitution together with the referred rule whenever it does not contribute to the significance of the proof.

[7] Otherwise $\llbracket\theta\rrbracket(C_i) < \llbracket\theta'\rrbracket(C_i)$ and $\llbracket\theta\rrbracket(C) \leq \llbracket\theta'\rrbracket(C)$ for all other $C \in T(\Sigma_s)/\simeq_P^n$, which leads to the absurdity $1 = \llbracket\theta\rrbracket(C_i) + \sum_{C \in T(\Sigma_s)/\simeq_P^n, C \neq C_i} \llbracket\theta\rrbracket(C) < \llbracket\theta'\rrbracket(C_i) + \sum_{C \in T(\Sigma_s)/\simeq_P^n, C \neq C_i} \llbracket\theta'\rrbracket(C) = 1$.

By assumption $\mathsf{B}_{n+1}(t,t') \xrightarrow{yes} \bot \in \mathsf{Tr}$. So, by rule *T4*, $\mathsf{Tr} \models \mathsf{B}_{n+1}(t,t') \stackrel{no}{\not\longrightarrow}$. Because of this and (10), rule *T3* yields that necessarily $\mathsf{Tr} \models \mathsf{Pr}^k_{n+1}(t,t_1,\dots,t_k) \xrightarrow{(a,q_1,\dots,q_k)} \bot$ which can only be proved using rule *T2* with an instance

$$\frac{t' \xrightarrow{a} \theta^* \quad \{\theta^*(T'_i) \geq q_i,\ \mathsf{B}_n(t_i,T'_i) \xrightarrow{yes} \bot\}_{i=1}^k}{\mathsf{Pr}^k_{n+1}(t',t_1,\dots,t_k) \xrightarrow{(a,q_1,\dots,q_k)} \bot}$$

for some $T'_1,\dots,T'_k \subseteq T(\Sigma_s \uplus \Sigma^T_s)$. Necessarily, all premises should hold in Tr. Therefore, by induction hypothesis $T'_i \subseteq C_i$ for all $i \in \{1,\dots,k\}$. Hence $\theta^* \in \Theta$ and $[\![\theta^*]\!](C_i) \geq [\![\theta^*]\!](T'_i) \geq q_i$ for all $i \in \{1,\dots,k\}$ which contradicts (9). This proves the induction case under the assumption that $\Theta \neq \emptyset$.

For the case $\Theta = \emptyset$, take any $t_1 \in T(\Sigma_s)$ and $q_1 \in \mathbb{Q}$ such that $[\![\theta]\!](t_1) \geq q_1 > 0$. Then, we take the following instance of rule *T2*:

$$\frac{t \xrightarrow{a} \theta \quad \theta(\{t_1\}) \geq q_1 \quad \mathsf{B}_n(t_1,t_1) \xrightarrow{yes} \bot}{\mathsf{Pr}^1_{n+1}(t,t_1) \xrightarrow{(a,q_1)} \bot}$$

Since $\mathsf{B}_n(t_1,t_1) \xrightarrow{yes} \bot \in \mathsf{Tr}$ by induction hypothesis and $t \xrightarrow{a} \theta \in \mathsf{Tr}\!\downharpoonright \subseteq \mathsf{Tr}$, all premises hold in Tr and hence $\mathsf{Pr}^1_{n+1}(t,t_1) \xrightarrow{(a,q_1)} \bot \in \mathsf{Tr}$.

On the other hand, since $\mathsf{Pr}^1_{n+1}(t',t_1) \xrightarrow{(a,q_1)} \bot \in \mathsf{Tr}$ can only be proved with some instance of *T2* in which $t' \xrightarrow{a} \theta'$ with $\theta' \in \Theta = \emptyset$, we conclude $\mathsf{Tr} \models \mathsf{Pr}^1_{n+1}(t',t_1) \stackrel{(a,q_1)}{\not\longrightarrow} \bot$.

Then, we have the following instance of *T2* in which its premises hold in Tr:

$$\frac{\mathsf{Pr}^1_{n+1}(t,t_1) \xrightarrow{(a,q_1)} \bot \quad \mathsf{Pr}^1_{n+1}(t',t_1) \stackrel{(a,q_1)}{\not\longrightarrow}}{\mathsf{B}_{n+1}(t,t') \xrightarrow{no} \bot}$$

and hence also $\mathsf{B}_{n+1}(t,t') \xrightarrow{no} \bot \in \mathsf{Tr}$. However, this contradicts the hypothesis $\mathsf{B}_{n+1}(t,t') \xrightarrow{yes} \bot \in \mathsf{Tr}$ which can only be proved using the instance of *T4* that requires that $\mathsf{Tr} \models \mathsf{B}_{n+1}(t,t') \stackrel{no}{\not\longrightarrow}$. This concludes the proof. □

The additional conditions in Lemma 15.2 are necessary as shown by the following examples.

Example 5. Consider a PTSS P_∞ with a signature containing the stop process, prefix and summation as in the running example and additional constant ∞. It also includes the infinitary version of $\oplus$. The rules for the new operator require the additional definition of a class of distribution terms as follows. For all $j \in \mathbb{N}$

$$\frac{}{\infty \xrightarrow{a} \theta^j}$$

where, for every $i, j \in \mathbb{N}$,

$$t_i = a.(\boldsymbol{b}.\mathbf{0} \oplus_{\frac{1}{i}} \boldsymbol{c}.\mathbf{0}), \qquad t^j_i = \textbf{if } (i \neq j) \textbf{ then } t_i \textbf{ else } 0, \qquad \text{and} \qquad \theta^j = \textstyle\bigoplus_{i\in\mathbb{N}} \left[\frac{1}{2^i}\right] \delta(t^j_i).$$

Since no rule in P_∞ has negative premises, P_∞ is complete. Take $\theta^* = \bigoplus_{i\in\mathbb{N}} \left[\frac{1}{2^i}\right] \delta(t_i)$, and notice that $\infty + a.\theta^* \not\simeq^3_{P_\infty} \infty$ since $\infty + a.\theta^* \xrightarrow{a} \theta^*$ and for all $i \in \mathbb{N}$, $\theta^*(t_i) > \theta^i([t_i]_{\simeq^3_{P_\infty}}) = 0$.

However, any operator Pr^k_3 (which is central to the distinction of transitions by means of rule *T2*) can distinguish the transition $\infty + a.\theta^* \xrightarrow{a} \theta^*$ from at most k transitions of ∞. To distinguish $\infty + a.\theta^* \xrightarrow{a} \theta^*$ from every transition $\infty \xrightarrow{a} \theta^j$ at the same time, we would need infinitary operators $\mathsf{Pr}^\infty_n(x, z_1, z_2, \dots)$ which we explicitly disallowed in the signature. (If infinitary operators are allowed in Σ_s it would be easy to construct continuous distributions, something that our definitions are not prepared to deal with.)

Example 6. Notice that the previous example uses an infinitary but rational instance of $\oplus$. We change the definition of ∞ to show that we also need that, though finitary, $\oplus$ cannot be instantiated with irrational numbers. Let $r \in [0,1]$ be an irrational number. For all $q \in [0,r] \cap \mathbb{Q}$, define

$$\frac{}{\infty \xrightarrow{a} \theta^q}$$

where, for every $p \in [0,1]$, $\theta^p = \boldsymbol{b}.\mathbf{0} \oplus_p \boldsymbol{c}.\mathbf{0}$.

Notice that $\infty + a.\theta^r \not\simeq^2_{P_\infty} \infty$ since $\infty + a.\theta^r \xrightarrow{a} \theta^r$ and $\theta^r(b.\mathbf{0}) > \theta^q([b.\mathbf{0}]_{\simeq^2_{P_\infty}}) = 0$ for all $q \in [0,r] \cap \mathbb{Q}$.

However, $\infty + a.\theta^r$ and ∞ cannot be distinguished by rule $T3$ since $\mathrm{Pr}_2^1(\infty, b.\mathbf{0}) \xrightarrow{(a,q)} \bot$ holds for any rational number $q < r$. The smallest number p such that $\theta^r(b.\mathbf{0}) = r \geq p > \theta^q([b.\mathbf{0}]_{\simeq^2_{P\infty}})$ for all q is actually r. So the tester would be able to distinguish $\infty + a.\theta^r$ and ∞ only if transition $\mathrm{Pr}_2^1(a, b.\mathbf{0}) \xrightarrow{(a,r)} \bot$ is allowed.

There is no technical restriction to construct a tester like this. We have only limited to rationals to show that it is sufficiently powerful to prove Theorem 16 below.

Theorem 16 states that bisimulation equivalence is *fully abstract* with respect to the $nt\mu f\theta/nt\mu x\theta$ format and trace equivalence. That is, bisimulation equivalence is the coarsest congruence with respect to any operator whose semantics is defined through $nt\mu f\theta/nt\mu x\theta$ rules and that is included in trace equivalence. Its proof is a direct consequence of Theorem 4, Lemma 15 and [22, Lemma 3.4.8].

Theorem 16. *Let P be a pure and complete PTSS in $nt\mu f\theta/nt\mu x\theta$ format such that its associated transition relation is image finite and $P \uplus P^T$ is complete. Then, for all $t, t' \in T(\Sigma_s)$,*

$$t \equiv^{\mathrm{t}}_{nt\mu f\theta/nt\mu x\theta} t' \quad \Leftrightarrow \quad t \simeq_P t' \quad \Leftrightarrow \quad t \sim_P t'$$

Proof. Suppose $t \sim_P t'$. Let P' be a PTSS in $nt\mu f\theta/nt\mu x\theta$ format such that $P \uplus P'$ is complete and a conservative extension of P. Then $t \sim_{P \uplus P'} t'$. By Theorem 4, for every context $C[\_]$ of $P \uplus P'$, $C[t] \sim_{P \uplus P'} C[t']$. Therefore $t \equiv^{\mathrm{t}}_{nt\mu f\theta/nt\mu x\theta} t'$ and hence $t \sim_P t' \Rightarrow t \equiv^{\mathrm{t}}_{nt\mu f\theta/nt\mu x\theta} t'$.

Suppose $t \not\simeq_P t'$. This implies that there is $n \in \mathbb{N}$ such that $t \not\simeq^n_P t'$. By Theorem 12 $P \uplus P^T$ is a conservative extension of P since P is pure, and hence source dependent, and the sources of all rules of P^T are fresh. Then we are in the conditions of Lemma 15, from which $\mathrm{Tr} \models B_n(t, t) \xrightarrow{yes} \bot$ and $\mathrm{Tr} \models B_n(t, t) \stackrel{yes}{\not\longrightarrow}$, where Tr is the transition associated to $P \uplus P^T$. Hence, the context $B_n(t, \_)$ distinguishes between t and t' and then $t \not\equiv^{\mathrm{t}}_{nt\mu f\theta/nt\mu x\theta} t'$. Therefore, $t \equiv^{\mathrm{t}}_{nt\mu f\theta/nt\mu x\theta} t' \Rightarrow t \simeq_P t'$.

Finally $t \simeq_P t' \Rightarrow t \sim t'$, by [22, Lemma 3.4.8]. □

In the case that the associated transition relation of P is not image finite but P only contains finitary and rational instances of $\oplus$, we cannot make use of [22, Lemma 3.4.8] but Lemma 15 still holds in full. Hence $t \sim_P t' \Rightarrow t \equiv^{\mathrm{t}}_{nt\mu f\theta/nt\mu x\theta} t' \Rightarrow t \simeq_P t'$.

Notice that Theorem 16 strangely requires that $P \uplus P^T$ is complete. This is necessary precisely because of the observation at the end of Section 6. If we take P to be the PTSS with only a constant a and the rules $\frac{}{a \xrightarrow{a} \delta(a)}$ and $\frac{x \stackrel{a}{\not\longrightarrow}}{x \xrightarrow{a} \delta(x)}$, then $P \uplus P^T$ will not be complete. (See the example in the last paragraph of Section 6.) This could be circumvented by translating P in an equivalent PTSS P' that is compatible with the tester P^T (or, more precisely with a variant of the tester). However, we omit this more general result for the complication and length of its proof which, in addition, does not add any substantial technical contribution.

8. Expressiveness issues

8.1. Limiting PTSSs to rational numbers

With the exception of the discussion of full abstraction and the bisimulation tester (see Section 7) the rest of the work does not make any particular assumption on the use of numbers in $[0, 1]$ on probabilistic sums or quantitative premises.

In the following we briefly discuss the fact that limiting to rationals do not yield limitations on PTSS in $nt\mu f\theta/nt\mu x\theta$ format. First notice that, since any real number can be expressed as a countable sum of rationals, any term $\bigoplus_{i \in I}[p_i]\theta_i$ can be equally written as $\bigoplus_{i \in I, j \in \mathbb{N}}[q_i^j]\theta_i$ where each $q_i^j \in [0, 1] \cap \mathbb{Q}$ and for every $i \in I$, $\sum_{j \in \mathbb{N}} q_i^j = p_i$.

Similarly, since any real number can be expressed as a converging sequence of rationals, it turns out that it is sufficient to consider quantitative premises of the form $\theta(Y) > q$ with $q \in \mathbb{Q}$ (or, alternatively, $\theta(Y) \geq q$). In effect, a rule r in a PTSS containing a quantitative premise of the form $\theta(Y) \geq p$, can be replaced by a rule that is just like r but contains the set of quantitative premises $\{\theta(Y) > q \mid q \in [0, p) \cap \mathbb{Q}\}$ instead of $\theta(Y) \geq p$. Such a change would yield an equivalent PTSS. If instead, a rule r contains a quantitative premise of the form $\theta(Y) > p$, for each $q \in (p, 1] \cap \mathbb{Q}$, define the rule r_q that is like r but contains the quantitative premise $\theta(Y) > q$ instead of a premise $\theta(Y) > p$. Replacing rule r by the set of rules $\{r_q \mid q \in (p, 1] \cap \mathbb{Q}\}$ in the original PTSS would also yield an equivalent PTSS. The rationale of the first replacement is that $p' \geq p$ if and only if $p' > q$ for *all* rational $q < p$. The second case is based on the fact that $p' > p$ if and only if $p' > q$ for *some* rational $q > p$.

8.2. The case of exponential distributions

A continuous time Markov chain can be seen as a transition system where each transition represents the (exponentially distributed) occurrence time of an event. Thus, a Markovian transition is a relation that goes from states to states and is labeled with a positive real number indicating the rate of the controlling exponential distribution: if $s \overset{\lambda}{\rightsquigarrow} s'$, the system will move from state s to state s' after a delay of τ time units that depends on an exponential distribution of rate $\lambda \in \mathbb{R}^+$.

Markov automata [26] is an extension of PTSs that includes also this other type of relation following the style introduced by interactive Markov chains (IMC) [25]. Thus, a Markov automaton is a tuple $(S, A, \rightarrow, \rightsquigarrow)$ where $(S, A, \rightarrow)$ is a PTS and $\rightsquigarrow \subseteq S \times \mathbb{R}^+ \times S$. Markov automata (and the particular case of IMCs) have been used as the underlying semantic model of different process algebras (e.g. [33,25]).

The Markovian behavior can be also modeled with a probabilistic transition as follows [26]: $s \xrightarrow{\mathsf{rate}(\gamma)} \pi$ where $\gamma = \sum_{s \overset{\lambda}{\rightsquigarrow} s'} \lambda$ is the rate of the (exponentially distributed) sojourn time in s, and the probability of jumping to state s' after such sojourn time is $\pi(s') = \frac{\lambda'}{\gamma}$ where $\lambda' = \sum_{s \overset{\lambda}{\rightsquigarrow} s'} \lambda$ (notice that in this second case s' is also fixed). Thus, a Markov automata can be also given as a PTS $(S, A, \rightarrow)$ (where A may contain labels in $\{\mathsf{rate}(\lambda) \mid \lambda \in \mathbb{R}^+\}$) provided that for each state s,

$$s \xrightarrow{\mathsf{rate}(\lambda)} \pi \text{ and } s \xrightarrow{\mathsf{rate}(\lambda')} \pi' \text{ implies } \lambda = \lambda' \text{ and } \pi = \pi'. \tag{11}$$

It turns out that bisimulation as given in Definition 8 corresponds to the usual definition on Markov automata [25,26]. Therefore, under this PTS view, all the theory introduced above lift immediately to Markov automata. The only problem remaining here is that the *ntμfθ/ntμxθ* format does not guarantee that rules preserve the property given in (11). Indeed, using our running example it is easy to see that the term $\mathsf{rate}(\lambda).\mathbf{0} \,||_\emptyset\, \mathsf{rate}(\lambda').\mathbf{0}$ violates the property.

The next theorem gives sufficient conditions to ensure that the associated transition of a complete PTSS is a Markov automata.

Theorem 17. *The associated transition of a complete PTSS $P = (\Sigma, A, R)$ is a Markov automata if every rule in R of the form $\frac{H}{t \xrightarrow{\mathsf{rate}(\lambda)} \theta}$ satisfies:*

1. $t = f(\zeta_1, \ldots, \zeta_{\mathsf{rk}(f)})$ *with* $\zeta_1, \ldots \zeta_{\mathsf{rk}(f)} \in \mathcal{V} \cup \mathcal{D}$,
2. $Var(\theta) \subseteq \{\zeta_1, \ldots \zeta_{\mathsf{rk}(f)}\} \cup \left\{\mu \mid \zeta_i \xrightarrow{\mathsf{rate}(\gamma)} \mu \in H \text{ for some } i \in \{1, \ldots, \mathsf{rk}(f)\} \text{ and } \gamma \in \mathbb{R}^+\right\}$
3. *if there is a different rule* $\frac{H'}{f(\zeta'_1, \ldots, \zeta'_{\mathsf{rk}(f)}) \xrightarrow{\mathsf{rate}(\lambda')} \theta'} \in R$, *then there are* $\hat{t}, \hat{t}' \in \mathbb{T}(\Sigma_s)$, $a \in A$ *and* $\mu' \in \mathcal{D}$ *such that*
   (a) $Var(\hat{t}) \subseteq \{\zeta_1, \ldots \zeta_{\mathsf{rk}(f)}\} \cup \left\{\mu \mid \zeta_i \xrightarrow{\mathsf{rate}(\gamma)} \mu \in H \text{ for some } i \in \{1, \ldots, \mathsf{rk}(f)\} \text{ and } \gamma \in \mathbb{R}^+\right\}$;
   (b) *there is a substitution* ρ *such that* $\hat{t}' = \rho(\hat{t})$, $\rho(\zeta_i) = \zeta'_i$ *for all* $i \in \{1, \ldots, \mathsf{rk}(f)\}$, *and, if* $\zeta_i \xrightarrow{\mathsf{rate}(\gamma)} \mu \in H$ *with* $\mu \in Var(t)$, *then* $\rho(\mu) \in \mathcal{D}$ *and* $\zeta'_i \xrightarrow{\mathsf{rate}(\gamma)} \rho(\mu) \in H'$; *and*
   (c) *either*
      - $\hat{t} \xrightarrow{a} \mu' \in H$ *and* $\hat{t}' \overset{a}{\not\rightarrow} \in H'$, *or*
      - $\hat{t} \overset{a}{\not\rightarrow} \in H$ *and* $\hat{t}' \xrightarrow{a} \mu' \in H'$.

If all these conditions are met, we say that P is in Markov automata format *(*MA format *for short).*

Before proving the theorem, we show some examples that motivate the conditions of the MA format. First notice that Markov automata require a strong form of determinism on rate labels. Then, the MA format aims to preserve such strong determinism in a given term provided its subterms also have this type of determinism. Nondeterminism is central in the interactive transitions of a Markov automata. Since the nondeterminism of transitions in the premises of a rule may be transferred to transitions in the conclusion of it, the role of interactive transitions in the construction of a Markovian transition should be limited. For instance, consider a PTSS with constants a, b and the unary operator f, and interactive label c with the following rules:

$$\frac{}{a \xrightarrow{c} \boldsymbol{a}} \qquad \frac{}{a \xrightarrow{c} \boldsymbol{b}} \qquad \frac{x \xrightarrow{c} \mu}{f(x) \xrightarrow{\mathsf{rate}(1)} \mu}$$

Then, both transitions $f(a) \xrightarrow{\mathsf{rate}(1)} \boldsymbol{a}$ and $f(a) \xrightarrow{\mathsf{rate}(1)} \boldsymbol{b}$ can be derived. Thus, condition 2 does not allow that the target of the conclusion depends on the targets of interactive premises.

Similarly, lookahead cannot be trusted since we cannot guarantee how the terms in support sets are substituted in a rule. Consider, a PTSS with the same signature but the following rules instead:

$$\frac{}{a \xrightarrow{\mathsf{rate}(1)} \boldsymbol{a} \oplus_{\frac{1}{2}} \boldsymbol{b}} \qquad \frac{x \xrightarrow{\mathsf{rate}(1)} \mu \quad \mu(Y) > 0}{f(x) \xrightarrow{\mathsf{rate}(1)} \delta(y)} \text{ with } y \in Y$$

Table 2
Extension of the process algebra of Example 1 with Markovian transitions.

$\dfrac{x \xrightarrow{\text{rate}(\lambda)} \mu \quad y \xrightarrow{\text{rate}(\lambda')} \mu'}{x + y \xrightarrow{\text{rate}(\lambda+\lambda')} \mu \oplus_{\frac{\lambda}{\lambda+\lambda'}} \mu'}$	$\dfrac{x \xrightarrow{\text{rate}(\lambda)} \mu \quad y \xrightarrow{\text{rate}(\lambda')} \mu'}{x \,\|_B\, y \xrightarrow{\text{rate}(\lambda+\lambda')} (\mu \,\|_B\, \delta(y)) \oplus_{\frac{\lambda}{\lambda+\lambda'}} (\delta(x) \,\|_B\, \mu')}$
$\dfrac{x \xrightarrow{\text{rate}(\lambda)} \mu \quad \{y \stackrel{\text{rate}(\lambda')}{\not\longrightarrow} \mid \lambda' \in \mathbb{R}+\}}{x + y \xrightarrow{\text{rate}(\lambda)} \mu}$	$\dfrac{x \xrightarrow{\text{rate}(\lambda)} \mu \quad \{y \stackrel{\text{rate}(\lambda')}{\not\longrightarrow} \mid \lambda' \in \mathbb{R}+\}}{x \,\|_B\, y \xrightarrow{\text{rate}(\lambda)} \mu \,\|_B\, \delta(y)}$
$\dfrac{\{x \stackrel{\text{rate}(\lambda)}{\not\longrightarrow} \mid \lambda \in \mathbb{R}+\} \quad y \xrightarrow{\text{rate}(\lambda')} \mu}{x + y \xrightarrow{\text{rate}(\lambda')} \mu}$	$\dfrac{\{x \stackrel{\text{rate}(\lambda)}{\not\longrightarrow} \mid \lambda \in \mathbb{R}+\} \quad y \xrightarrow{\text{rate}(\lambda')} \mu}{x \,\|_B\, y \xrightarrow{\text{rate}(\lambda')} \delta(x) \,\|_B\, \mu}$

Depending on how variables in Y are assigned, transitions $f(a) \xrightarrow{\text{rate}(1)} \delta(a)$ and $f(a) \xrightarrow{\text{rate}(1)} \delta(b)$ can be derived.

Condition 3 ensures that different rules do not have closed instances in such a way that the source of the conclusion is the same. Thus, it states that for any closed instance of both rules with equal source at the conclusion, there is a state term that appears as source of a positive premise in one rule and of a negative premise in the other such that the literals deny each other (condition 3c). Again, we need to ensure that such a common term is inevitably constructed as a consequence of the source of the conclusion. That is why the restriction on the set of variables in condition 3a and the correspondence through a properly constructed substitution (condition 3b).

Proof of Theorem 17. Let Tr be the transition relation associated to P. It suffices to show that if $t \xrightarrow{\text{rate}(\lambda^1)} \theta^1 \in \text{Tr}$ and $t \xrightarrow{\text{rate}(\lambda^2)} \theta^2 \in \text{Tr}$, then $\lambda^1 = \lambda^2$ and $\theta^1 = \theta^2$.

We proceed by structural induction on t. So let $t = f(\xi_1, \ldots, \xi_{\text{rk}(f)})$ with $\xi_1, \ldots, \xi_{\text{rk}(f)} \in T(\Sigma)$ and assume that the property is valid for each $\xi_i \in T(\Sigma_s)$.

Suppose by contradiction that either $\lambda^1 \neq \lambda^2$ or $\theta^1 \neq \theta^2$. Since the model is complete, by Definition 5 there are two sets of negative premises N^1 and N^2 such that $\text{Tr} \models N^1$, $\text{Tr} \models N^2$, $P \vdash \dfrac{N^1}{f(\xi_1,\ldots,\xi_{\text{rk}(f)}) \xrightarrow{\text{rate}(\lambda^1)} \theta^1}$, and $P \vdash \dfrac{N^2}{f(\xi_1,\ldots,\xi_{\text{rk}(f)}) \xrightarrow{\text{rate}(\lambda^2)} \theta^2}$. Let $\mathfrak{p}^1$ and $\mathfrak{p}^2$ be their respective proofs.

We consider two cases according the last rules used in each proof are the same or not.

Suppose the last rule used in both proofs is the same. Let $\dfrac{H}{f(\zeta_1,\ldots,\zeta_{\text{rk}(f)}) \xrightarrow{\text{rate}(\lambda)} \theta}$ be such rule. Then there are two substitution ρ^1 and ρ^2 for the proofs $\mathfrak{p}^1$ and $\mathfrak{p}^2$, respectively, such that $\rho^1(\zeta_i) = \rho^2(\zeta_i) = \xi_i$ for all $i \in \{1, \ldots, \text{rk}(f)\}$. In addition, by induction hypothesis $\rho^1(\zeta_i) \xrightarrow{\text{rate}(\gamma_i^1)} \rho^1(\mu)$ and $\rho^2(\zeta_i) \xrightarrow{\text{rate}(\gamma_i^2)} \rho^2(\mu)$ implies $\gamma_i^1 = \gamma_i^2$ and $\rho^1(\mu) = \rho^2(\mu)$. As a consequence of condition 2 $\theta^1 = \rho^1(\theta) = \rho^2(\theta) = \theta^2$. Moreover $\lambda^1 = \lambda^2 = \lambda$ because the last rules applied in both proofs are the same. Therefore we reach a contradiction for this case.

So it has to be the case that the last rules on $\mathfrak{p}^1$ and $\mathfrak{p}^2$ are different. Let $\dfrac{H}{f(\zeta_1,\ldots,\zeta_{\text{rk}(f)}) \xrightarrow{\text{rate}(\lambda)} \theta}$ and $\dfrac{H'}{f(\zeta'_1,\ldots,\zeta'_{\text{rk}(f)}) \xrightarrow{\text{rate}(\lambda')} \theta'}$ be the respective rules. Then there are two substitution ρ^1 and ρ^2 for the proofs $\mathfrak{p}^1$ and $\mathfrak{p}^2$, respectively, such that $\rho^1(\zeta_i) = \rho^2(\zeta'_i) = \xi_i$ for all $i \in \{1, \ldots, \text{rk}(f)\}$. Because of condition 3, there are $\hat{t}, \hat{t}' \in \mathbb{T}(\Sigma_s)$, $a \in A$ and $\mu' \in \mathcal{D}$ satisfying conditions 3a, 3b, and 3c.

Thus, if $\mu \in \mathit{Var}(\hat{t})$, $\zeta_i \xrightarrow{\text{rate}(\gamma)} \mu \in H$, for some $1 \leq i \leq \text{rk}(f)$. Moreover, $\zeta'_i \xrightarrow{\text{rate}(\gamma')} \rho(\mu) \in H'$. Then, by induction hypothesis, $\rho^1(\zeta_i) \xrightarrow{\text{rate}(\gamma)} \rho^1(\mu)$ and $\rho^2(\zeta'_i) \xrightarrow{\text{rate}(\gamma')} \rho^2(\rho(\mu))$ implies $\gamma = \gamma'$ and $\rho^1(\mu) = \rho^2(\rho(\mu))$. Moreover $\rho^1(\zeta_i) = \rho^2(\zeta'_i) = \rho^2(\rho(\zeta_1))$. Because of this and condition 3a, $\rho^2(\hat{t}') = \rho^2(\rho(\hat{t})) = \rho^1(\hat{t})$. W.l.o.g. suppose $\hat{t} \xrightarrow{a} \mu' \in H$ and $\hat{t}' \stackrel{a}{\not\longrightarrow} \in H'$ is the case in condition 3c. Then $\rho^1(\hat{t}) \xrightarrow{a} \rho^1(\mu') \in \text{Tr}$ and $\text{Tr} \models \rho^2(\hat{t}') \stackrel{a}{\not\longrightarrow}$, i.e., $\text{Tr} \models \rho^1(\hat{t}) \stackrel{a}{\not\longrightarrow}$ which is a clear contradiction, hence proving the theorem. □

Example 7. We can extend our running example to ensure that it is in MA format. We do so by extending all rules in Table 1 to run on labels $a \in A \cup \{\text{rate}(\lambda) \mid \lambda \in \mathbb{R}^+\}$ with the exceptions of the rules for $+$ and $\|_B$. For them, rules in Table 1 are only defined for the interactive labels $a \in A \setminus \{\text{rate}(\lambda) \mid \lambda \in \mathbb{R}^+\}$. For the rate labels, we define the new rules in Table 2.

9. Related work

We first remark that the $\mathit{nt}\mu\mathit{f}\theta/\mathit{nt}\mu\mathit{x}\theta$ format should be considered as a probabilistic extension of the *tyft/tyxt* and *ntyft/ntyxt* formats [2,4]. These formats can be encoded in $\mathit{nt}\mu\mathit{f}\theta/\mathit{nt}\mu\mathit{x}\theta$ format if non-probabilistic transitions $t \xrightarrow{a} t'$ are considered as a probabilistic transition in the usual way, i.e., as $t \xrightarrow{a} \delta(t')$. Provided this encoding, an *ntyft* rule of the form

$$\frac{\{t_m \xrightarrow{a_m} y_m \mid m \in M\} \cup \{t_n \stackrel{b_n}{\not\longrightarrow} \mid n \in N\}}{f(x_1, \dots, x_{\mathrm{rk}(f)}) \xrightarrow{a} t}$$

can be rewritten as the following *ntμfθ* rule (we are using the *abbreviated ntμfθ* format),

$$\frac{\{\hat{t}_m \xrightarrow{a_m} \mu_m \mid m \in M\} \cup \{\mu_m(Y_m) > 0 \mid m \in M\} \cup \{\hat{t}_n \stackrel{b_n}{\not\longrightarrow} \mid n \in N\}}{f(x_1, \dots, x_{\mathrm{rk}(f)}) \xrightarrow{a} \delta(\hat{t})}$$

with $\hat{t}$ being the same term as t where each occurrence of variable y_m has been replaced by Y_m.

SOS for probabilistic systems have received relatively little attention before our introduction of the predecessor *ntμfν/ntμxν* format in [14]. To our knowledge, only [15–18,34] study rule formats to specify probabilistic transition systems, and in [16,23] they are embedded in general bialgebraic frameworks.

Both RTSS format [18] and PGSOS format [15,16] consider transitions with the form $t \xrightarrow{a,q} t'$ as already explained in the introduction. They allow for the specification of only reactive probabilistic systems [12] (i.e. they should satisfy that if $t \xrightarrow{a} \pi$ and $t \xrightarrow{a} \pi'$, then $\pi = \pi'$). Moreover, these formats are very much like GSOS [3] in the sense that premises are of the form $x_i \xrightarrow{a_i,q_i} y_i$ or $x_i \stackrel{b_i}{\not\longrightarrow}$ where each x_i is a variable appearing on the term $f(x_1, \dots, x_{\mathrm{rk}(f)})$ at the source of the conclusion. Moreover, q_i needs to be a variable, so there is no possibility of testing for a particular probability value. In addition, RTSS allows for a restricted form of lookahead: only one step ahead from variable y_i can be tested and moreover probabilities should be appropriately combined in the conclusion of the rule. (RTSS can be generalized to arbitrary steps of lookahead but such generalization would render the format unreadable [18].) We remark that both RTSS and PGSOS formats can be encoded in the *ntμfθ/ntμxθ* format. Segala-GSOS format [16] allows for rules similar to that in equation (F), with the restriction that terms t_m and t_n can only be any of the variables x_k. Therefore, lookahead is not permitted beyond a quantitative testing. The target of the conclusion in the Segala-GSOS format has a particular form, which is similar to $\bigoplus_{i \in I}[p_i]\theta_i$ where each θ_i does not contain $\oplus$ and δ only appears applied to a variable. Since $\oplus$ distributes with the lifted operators, this expression is as expressive as any distribution term in which δ only appears applied to a variable. However, the Segala-GSOS format is here a little bit more expressive since it allows to express the copying of a sampled value (apart from the copying of the distribution). Provided this characteristic is not present, all other characteristics of the Segala-GSOS format can be encoded in the *ntμfθ/ntμxθ* format.

Bialgebras present an abstract categorical framework to study structured operational semantics and, in this setting, general congruence theorems have been presented [35,23]. They introduce the so-called *abstract GSOS* and *abstract safe ntree* [35,23]. In fact, Segala-GSOS is derived as an instance of abstract GSOS [16]. It is known that the non-probabilistic *ntyft/ntyxt* format cannot be instanced as an abstract safe ntree and hence cannot be introduced in a bialgebraic framework in the current state of the art. This also would apply to our format since it is a generalization of the *ntyft/ntyxt* format. However the *tyft/tyxt* format has been encoded in a categorical setting using topos [36], in particular the lookahead. Then it would be an open question whether this could also be done for the positive subset of *ntμfθ/ntμxθ*.

It is worth to mention that all previously mentioned formats only consider a single-sorted algebra. Moreover, we notice that none of these formats can encode the bisimulation tester of Definition 21 since it needs lookahead, negative premises of the form $f(\vec{x}) \stackrel{a}{\not\longrightarrow}$, and quantitative premises testing against any possible probability value. None of the previous formats allow for all these simultaneously. In fact, to the authors knowledge no full abstraction result for rule formats has been presented before for PTSS, nor for complete PTS. Nevertheless, related to this result, we should remark that testers for bisimulation of reactive (i.e. deterministic) probabilistic transition systems were already introduced in [20]. Also, the recent paper [37] has shown that an extension of the higher order π calculus that includes action refusal and passivation (called $\mathrm{HO}\pi_{\mathrm{pass,ref}}$) is powerful enough to distinguish bisimulation in reactive probabilistic transition systems. However, in these two cases, the achieved full abstraction is with respect to *probabilistic* trace equivalence rather than the weaker possibilistic trace equivalence used in Theorem 16.

Recently, there have been some few works on SOS and rule formats for quantitative variants of labeled transition systems that are worth to mention. [38] discuses a coalgebraic approach to produce a GSOS-like format (with some additional restriction) for reactive probabilistic transition system with *continuous* probabilities (namely, labeled Markov processes [30]). Based in the bialgebraic setting, [39–41] introduces another GSOS-like format for several classes of *weighted* transition systems. It includes a type of premise that allows to test for the total accumulated weight (i.e. the measure of the support set). This format still bears weights as labels. Based on this last work as well as [16,42] introduces yet another variant of GSOS, in this case oriented to the general setting of uniform labeled transition systems [43]. This format allows for quantitative premises that test for positive (like in Segala-GSOS [16]) and total accumulated weight (like in [40,41]). In all previous works, the corresponding bisimulation is shown to be a congruence for the operators defined in the said format, but for none of them bisimulation is fully abstract since they do not allow for lookahead and general quantitative premises.

There have been some additional work on PTSS that goes beyond bisimulation. [34] introduces a format to ensure non-expansiveness of ϵ-bisimulation using probability values on the labels. This work has been generalized an extended in [44] following the style set in this article. [45] characterizes a class of operators that ensures non-extensiveness of the bisimulation metric. [46,47] introduces different restrictions to the GSOS format following the style set in this article so that each format ensures non-extensiveness, non-expansiveness, and uniform continuity, respectively. [48] provides a decomposition theorem for a probabilistic variant of the Hennessy–Milner logic based on the RTSS format [18]. Starting from a GSOS-like PTSS, [49] introduces an algorithm to derive complete equational theories for bisimulation, convex bisimulation and the bisimulation metric.

Finally, we observe that all previous mentioned work, including ours, is mostly oriented to the reactive type of models (either deterministic [12] or non-deterministic [21]) with the exception of [17,18] which also provide a rule format for generative probabilistic systems [12].

10. Conclusions

In this article we have introduced a general theory for structured operational semantics for languages with probabilistic features. We focused on rule formats and introduced the *ntμfθ/ntμxθ* format, the most general (less restricting) of all formats available in the literature that preserves bisimilarity. We proved that bisimilarity is a congruence for all operators definable in this format and that it is also the least congruence relation preserved by all such operators included in possibilistic trace equivalence. While working towards that aim, we also defined the meaning of PTSSs with negative premises and studied the concept of conservative extensions on PTSSs. Finally, we discussed expressiveness issues adding the particular case of IMCs and Markov automata: we introduced the MA format on complete PTSS that guarantees that the model it defines is indeed a Markov automaton.

We highlight the introduction of our quantitative premises which, in combination with lookahead, permits the constructions of highly expressive operators such as the bisimulation tester of Definition 21 and the safe controller of the running example. The bisimulation tester, in particular, enables the definition of powerful operators that are able to measure precise probabilities. For instance, we can introduce the deadlock measuring operator dk where $\mathsf{dk}(t) \xrightarrow{q} \bot$ whenever t reaches a deadlock state with probability larger or equal to q in any possible resolution of non-determinism. The rules are as follows

$$\frac{\{x \stackrel{a}{\not\longrightarrow} \mid a \in A\}}{\mathsf{dk}(x) \xrightarrow{1} \bot} \qquad \frac{\{\mathsf{B}_n(x,y) \xrightarrow{yes} \mu_n \mid n \in \mathbb{N}_0\}}{\mathsf{B}(x,y) \xrightarrow{yes} \bot}$$

$$\frac{x \xrightarrow{a} \mu \quad \{\mathsf{dk}(z_i) \xrightarrow{p_i} \mu_i,\quad \mu(Z_i) \geq q_i,\quad \mathsf{B}(z_i, Z_i) \xrightarrow{yes} \mu_i',\quad \mathsf{B}(z_i, z_j) \stackrel{yes}{\not\longrightarrow}\}_{\substack{i,j \in I\\ i \neq j}}}{\mathsf{dk}(x) \xrightarrow{\sum_{i \in I} q_i p_i} \bot} \quad \begin{array}{l} I \text{ is a countable} \\ \text{index set and} \\ \sum_{i \in I} q_i \leq 1 \end{array}$$

The last rule appropriately collect the probabilities by looking ahead on disjoint (non-bisimilar) terms (notice the use of the bisimulation tester). Operation dk is somehow related to the zero process of [50] that allows for detection of inevitable deadlock.

We remark that the congruence theorem also holds for PTSs with subprobability distributions (i.e. distributions such that $\pi(T(\Sigma)) < 1$). However, we do not know whether the full abstraction result remains valid in this setting: our tester would fail to distinguish c from d where $c \xrightarrow{a} ([0.5]\boldsymbol{c} \oplus [0.5]\bot)$, $c \xrightarrow{a} ([0.5]\boldsymbol{c})$, and $d \xrightarrow{a} ([0.5]\boldsymbol{c} \oplus [0.5]\bot)$. (The term $([0.5]\boldsymbol{c})$ represents a subprobability distribution that only chooses c with probability 0.5.) We suspect that a test for the total measure of support sets like in [40,41] is actually needed.

There are two important issues that remain unsolved and which we wrongly claimed valid in [27]. The first one is whether the well-founded hypothesis of the congruence theorem (Theorem 4) is indeed necessary. The second one is whether the *ntμfθ/ntμxθ* format can be reduced to a probabilistic variant of the *ntree* format [51]. In [27], we made a mistake on the proof of Lemma 8 that we could not repair. Hence, Theorem 5 (which stated that every *ntμfθ/ntμxθ* PTSS can be reduced to *pntree*) and Corollary 1 (which dropped the well-founded hypothesis) in [27] remain unproved. We do know, however, that the claims hold for a restriction of the *ntμfθ/ntμxθ* format, in which quantitative premises can only be tested against 0, i.e. if the rules of the PTSS are in the format of equation (F).

Acknowledgments

Supported by ANPCyT PICT 2012-1823, SeCyT-UNC, Eramus Mundus Action 2 Lot 13A EU Mobility Programme 2010-2401/001-001-EMA2 and EU 7FP grant agreement 295261 (MEALS). We thank the reviewers for their careful reading. Their remarks and questions helped us to improve the article.

Appendix A. Comparison to [14] and [27]

The following list highlights the most important points in which the present paper improves over [14]. Moreover, we also compare to the related article [27].

1. PTSS in [14] are based on single-sorted algebras. There the target of a transition is a distribution on terms. Thus, in order to define the target of the conclusion we use arithmetic expressions of the form $\sum_{i \in I} p_i \cdot ((\prod_{j \in J} \nu_i^j) \circ g_i^{-1})$ where

$\sum_{i\in I} p_i = 1$, ν_i^j are variables over actual probability distributions on terms, and g_i are (measurable) functions on the set of terms. Carelessly, we did not require some necessary compositional properties on g_i, which falsifies the congruence theorem. The adoption of distribution terms as a second sort introduces naturally such a compositionality property and, in fact, it is part of Definition 13 and the associated properties proven in Lemmas 9 and 10.

The two-sorted signatures (which we have already used in [27,49]) also allow us to obtain a significantly neater definition of PTSSs.

2. In this article we addressed the most general way to give meaning to PTSS using 3-valued stable models, and considered complete PTSS when a 2-valued model is required. In [14] we limited to stratified models. In [27] we already presented the same meaning as here through well-supported proofs.
3. The format introduced in [14] contains two mistakes. The first one is the already mentioned problem behind the g_i functions. The second one is with regard to the quantitative premises. We requested that the set of quantitative premises has the form $\{\mu_l^{\vec{z}}(Y_l) \trianglerighteq_l q_l \mid l \in L, \vec{z} \in \mathcal{Z}\}$, while we should have actually requested the form $\{\mu_l^{\vec{z}}(Y_l) \trianglerighteq_l q_l \mid l \in L\}$, since allowing for *different* quantitative inquiries on the same set Y_l introduces a contradiction. This has been corrected here.
4. The $nt\mu f\theta/nt\mu x\theta$ format defined here allows for more complex quantitative premises than those in [14] since they may have the form $\theta(Y) \trianglerighteq q$ where θ is any distribution term rather than only a distribution variable. It is also more flexible with respect to the use of the variables $\mu_m^{\vec{z}}$ and those in the sets Y_l. This can be seen in restrictions 5 and 6 of Definition 10 which are also more general than the restrictions from [27].
5. The congruence theorem in our original paper [14, Theorem 12] is missing the well-founded rules hypothesis which is actually necessary. This has already been reported in [27]. Notice, besides that the congruence theorem there [27, Theorem 4] is limited to stratifiable PTSSs (the proof has not appeared in the published paper).
6. The results on conservative extensions in this paper are new. In [14] we introduced conservative extension using the usual (more restricted) semantic definition, which here is a consequence of Theorem 14. Besides Theorem 12 is more general than Theorem 14 in [14], adapting to the most general conditions in non-probabilistic TSS theory [29].
7. The results on full abstraction (Sec. 7) are now proved in the context of complete PTSSs (rather than its subset of stratified PTSSs as given in [14]) and the new results of conservative extension.
8. All the results on expressiveness, including that of Markov automata, are new (see Sec. 8).

Appendix B. Conclusion of the proof of Lemma 11: Successor subcase on II_α

By induction hypothesis suppose that $\mathrm{I}_{\alpha-1}$ and $\mathrm{II}_{\alpha-1}$ hold. We focus on the remaining case of II_α in which $t_1 \, \mathrm{R}_P \, t_2$ as a consequence of Definition 13.3 (other cases were proved in the main text).

Then, $t_1 = f(\xi_1^1, \cdots, \xi_{\mathrm{rk}(f)}^1)$ and $t_2 = f(\xi_1^2, \cdots, \xi_{\mathrm{rk}(f)}^2)$ with $\xi_i^1 \, \mathrm{R}_P \, \xi_i^2$, for all $i = 1, \ldots, \mathrm{rk}(f)$, and $f \in \Sigma_s$. Since $f(\xi_1^1, \cdots, \xi_{\mathrm{rk}(f)}^1) \xrightarrow{a} \theta_1 \in \mathrm{CT}_\lambda$, there is a set H of negative literals such that $P \vdash \frac{H}{f(\xi_1^1, \cdots, \xi_{\mathrm{rk}(f)}^1) \xrightarrow{a} \theta_1}$ and $\mathrm{CT}_\lambda \models H$. We use induction on the height γ of the proof of $P \vdash \frac{H}{f(\xi_1^1, \cdots, \xi_{\mathrm{rk}(f)}^1) \xrightarrow{a} \theta_1}$. So, by Definition 4, there must exist a rule r of the form

$$\frac{\{t_m(\vec{z}) \xrightarrow{a_m} \mu_m^{\vec{z}} \mid m \in M, \vec{z} \in \mathcal{Z}\} \cup \{t_n(\vec{z}) \stackrel{b_n}{\not\longrightarrow} \mid n \in N, \vec{z} \in \mathcal{Z}\} \cup \{\theta_l(Y_l) \trianglerighteq_{l,k} p_{l,k} \mid l \in L, k \in K_l\}}{f(\zeta_1, \ldots, \zeta_{\mathrm{rk}(f)}) \xrightarrow{a} \theta}$$

and a proper substitution ρ_1 such that

($\rho_1 1$) $\rho_1(\zeta_i) = \xi_i^1$, for all $i \in \{1, \ldots, \mathrm{rk}(f)\}$,
($\rho_1 2$) $\rho_1(\theta) = \theta_1$,
($\rho_1 3$) for each $m \in M$ and $\vec{z} \in \mathcal{Z}$, there is a set $H_m^{\vec{z}} \subseteq H$ of negative literals such that $P \vdash \frac{H_m^{\vec{z}}}{\rho_1(t_m(\vec{z})) \xrightarrow{a_m} \rho_1(\mu_m^{\vec{z}})}$ is proved with a proof shorter than γ, and $\mathrm{CT}_\lambda \models H_m^{\vec{z}}$ (since $\mathrm{CT}_\lambda \models H$),
($\rho_1 4$) for each $n \in N$ and $\vec{z} \in \mathcal{Z}$, $\rho_1(t_n(\vec{z})) \stackrel{b_n}{\not\longrightarrow} \in H$, hence $\mathrm{CT}_\lambda \models \rho_1(t_n(\vec{z})) \stackrel{b_n}{\not\longrightarrow}$, and
($\rho_1 5$) for each $l \in L$ and $k \in K_l$, $[\![\rho_1(\theta_l)]\!](\rho_1(Y_l)) \trianglerighteq_{l,k} p_{l,k}$.

We construct a substitution ρ_2 such that, together with rule r, proves $f(\xi_1^2, \cdots, \xi_{\mathrm{rk}(f)}^2) \xrightarrow{a} \rho_2(\theta) \in \mathrm{PT}_\alpha$ and $\rho_1(\theta) \, \mathrm{R}_P \, \rho_2(\theta)$. To construct ρ_2 we proceed by induction on the variable dependency graph of r as we did for the case of I_α.

Let $D = \{\rho_1(\vec{z}) \mid \vec{z} \in \mathcal{Z}\}$. Let $\Xi = \{Z_{\vec{d}} \subseteq \mathcal{Z} \mid \vec{d} \in D\}$ be a partition of $\mathcal{Z}$ such that for all $\vec{d} \in D$

($\Xi 1$) $|Z_{\vec{d}}| \geq \aleph_0$;
($\Xi 2$) there exists some $\vec{z} \in Z_{\vec{d}}$ such that $\rho_1(\vec{z}) = \vec{d}$;
($\Xi 3$) for all $\vec{z} \in \mathcal{Z}$ and $m \in M$, if $\mu_m^{\vec{z}} \in Var(\theta) \cup (\cup_{l \in L} Var(\theta_l)) \cup W$ and $\rho_1(\vec{z}) = \vec{d}$, then $\vec{z} \in Z_{\vec{d}}$ (here, W is as in Definition 10); and
($\Xi 4$) for all $\vec{z} \in \mathcal{Z}$, if, for some $l \in L$, $\vec{z}(l) \in Y_l \cap \left(Var(\theta) \cup \bigcup_{l' \in L} Var(\theta_{l'})\right)$ and $\rho_1(\vec{z}) = \vec{d}$, then $\vec{z} \in Z_{\vec{d}}$.

Just like for the successor subcase on I_α, the partition Ξ exists as a consequence of conditions 1, 5, and 6 in Definition 10.

In the following, we define ρ_2 such that

($\rho_2 1$) $\rho_1(\zeta)\ \mathsf{R}_P\ \rho_2(\zeta)$ for all $\zeta \in Var(\theta) \cup (\cup_{l\in L} Var(\theta_l)) \cup W \cup \{\zeta_1, \dots, \zeta_{\mathsf{rk}(f)}\}$,
($\rho_2 2$) $\rho_2(\Pi_l(Z_{\vec{d}})) = \left\{t \in T(\Sigma_s) \mid \vec{d}(l)\ \mathsf{R}_P\ t \text{ and } [\![\rho_2(\theta_l)]\!](t) > 0\right\}$,
($\rho_2 3$) $\rho_2(\zeta_i) = \xi_i^2$ for all $i \in \{1, \dots, \mathsf{rk}(f)\}$,
($\rho_2 4$) $\rho_2(t_m(\vec{z})) \xrightarrow{a_m} \rho_2(\mu_m^{\vec{z}}) \in \mathsf{PT}_\alpha$ for all $m \in M$ and $\vec{z} \in \mathcal{Z}$,
($\rho_2 5$) $[\![\rho_2(\theta_l)]\!](\rho_2(Y_l)) \trianglerighteq_{l,k} p_{l,k}$ for all $l \in L$ and $k \in K_l$, and
($\rho_2 6$) $\mathsf{CT}_{\alpha-1} \models \rho_2(t_n(\vec{z})) \stackrel{b_n}{\not\longrightarrow}$ for all $n \in N$ and $\vec{z} \in \mathcal{Z}$,

We prove ($\rho_2 1$)–($\rho_2 4$) by constructing ρ_2 inductively on the dependency degree of each variable (which we can do because r is well-founded). For $i \in \{1, \dots, \mathsf{rk}(f)\}$, define $\rho_2(\zeta_i) = \xi_i^2$, which immediately yields ($\rho_2 3$). Moreover, $\rho_1(\zeta_i) = \xi_i^1\ \mathsf{R}_P\ \xi_i^2 = \rho_2(\zeta_i)$ and hence ($\rho_2 1$) and ($\rho_2 2$) hold for this case. (($\rho_2 2$) holds trivially).

For the inductive case, we assume that every variable ζ with $\text{degree}(\zeta) < k$ satisfy ($\rho_2 1$) and ($\rho_2 2$).

We analyze first the case of $\mu_m^{\vec{z}}$ with $\text{degree}(\mu_m^{\vec{z}}) = k$. Necessarily, $\vec{z} \in Z_{\vec{d}}$ for some $Z_{\vec{d}} \in \Xi$ since Ξ forms a partition of $\mathcal{Z}$. By ($\Xi 2$), there exists $\vec{z}' \in Z_{\vec{d}}$ such that $\rho_1(\vec{z}') = \vec{d}$. In particular, if $\mu_m^{\vec{z}} \in Var(\theta) \cup (\cup_{l\in L} Var(\theta_l)) \cup W$, we know by ($\Xi 3$) that $\rho_1(\vec{z}) = \vec{d}$, in which case we choose $\vec{z}' = \vec{z}$. Since all variables in $Var(t_m(\vec{z}))$ have a dependency degree smaller than k, using the induction hypothesis on ($\rho_2 1$) and ($\rho_2 2$) respectively, we have:

- If $\zeta \in Var(t_m(\vec{z})) \cap W$, $\rho_1(\vec{z}'(\zeta)) = \rho_1(\zeta)\ \mathsf{R}_P\ \rho_2(\zeta) = \rho_2(\vec{z}(\zeta))$. (Here $\vec{z}(\zeta)$ represents the variable in the coordinate ζ which is ζ itself.)
- For every $l \in L$, if $\zeta \in Var(t_m(\vec{z})) \cap Y_l$, then
$$\rho_2(\zeta) = \rho_2(\vec{z}(l)) \in \rho_2(\Pi_l(Z_{\vec{d}})) = \left\{t \in T(\Sigma_s) \mid \vec{d}(l)\ \mathsf{R}_P\ t \text{ and } [\![\rho_2(\theta_l)]\!](t) > 0\right\},$$
and hence. $\rho_1(\vec{z}'(l)) = \vec{d}(l)\ \mathsf{R}_P\ \rho_2(\vec{z}(l))$.

Therefore, by Lemma 9, $\rho_1(t_m(\vec{z}'))\ \mathsf{R}_P\ \rho_2(t_m(\vec{z}))$. Furthermore, by ($\rho_1 3$), there is a proof of $P \vdash \dfrac{H_m^{\vec{z}}}{\rho_1(t_m(\vec{z})) \xrightarrow{a_m} \rho_1(\mu_m^{\vec{z}})}$ with $\mathsf{CT}_\lambda \models H_m^{\vec{z}}$. Thus, $\rho_1(t_m(\vec{z}')) \xrightarrow{a_m} \rho_1(\mu_m^{\vec{z}'}) \in \mathsf{CT}_\lambda$. Since moreover, the proof is shorter than γ, by induction II_α, there exists $\theta' \in T(\Sigma_d)$ such that $\rho_2(t_m(\vec{z})) \xrightarrow{a_m} \theta' \in \mathsf{PT}_\alpha$ and $\rho_1(\mu_m^{\vec{z}'})\ \mathsf{R}_P\ \theta'$. Define $\rho_2(\mu_m^{\vec{z}}) = \theta'$. Then ($\rho_2 1$) holds since $\vec{z}'$ was chosen to be $\vec{z}$ in case $\mu_m^{\vec{z}} \in Var(\theta) \cup (\cup_{l\in L} Var(\theta_l)) \cup W$, and ($\rho_2 2$) holds trivially. Moreover, also ($\rho_2 4$) is satisfied.

It only remains to show the case of the term variables in $\bigcup_{l\in L} Y_l$. Recall that all variables in Y_l have the same dependency degree. So, we define ρ_2 simultaneously for all variables in Y_l with $\text{degree}(Y_l) = k$. We directly define ρ_2 such that

$$\rho_2(\Pi_l(Z_{\vec{d}})) = \left\{t \in T(\Sigma_s) \mid \vec{d}(l)\ \mathsf{R}_P\ t \text{ and } [\![\rho_2(\theta_l)]\!](t) > 0\right\} \tag{B.1}$$

for all $Z_{\vec{d}} \in \Xi$. For this to be a good definition, we need to show that

(i) $Y_l = \bigcup_{\vec{d}\in D} \Pi_l(Z_{\{d_l\}_L})$,
(ii) $\Pi_l(Z_{\vec{d}}) \cap \Pi_l(Z_{\vec{d}'}) \neq \emptyset$ implies $Z_{\vec{d}} = Z_{\vec{d}'}$, and
(iii) there exists $t \in T(\Sigma_s)$ such that $\vec{d}(l)\ \mathsf{R}_P\ t$ and $[\![\rho_2(\theta)]\!](t) > 0$.

(i) is immediate since Ξ is a partition of $\mathcal{Z}$.

For (ii) suppose $y \in \Pi_l(Z_{\vec{d}}) \cap \Pi_l(Z_{\vec{d}'})$. Then, there is a $\vec{z} \in \mathcal{Z}$ such that $\vec{z}(l) = y$. By Definition 9, such $\vec{z}$ needs to be unique, from which (ii) follows.

For (iii) we proceed as follows. By induction on the dependency degree, we know that for all $\zeta \in Var(\theta_l)$, $\rho_1(\zeta)\ \mathsf{R}_P\ \rho_2(\zeta)$. Then, by Lemmas 9 and 10, $[\![\rho_1(\zeta)]\!]\ \mathsf{R}_P\ [\![\rho_2(\zeta)]\!]$. As a consequence, there is a weight function w such that

$$w(\vec{d}(l), T(\Sigma_s)) = [\![\rho_1(\zeta)]\!](\vec{d}(l)) = [\![\rho_1(\zeta)]\!](\rho_1(\vec{z}(l))) > 0$$

for some $\vec{z} \in Z_{\vec{d}}$. The existence of $\vec{z}$ is guaranteed by ($\Xi 2$) and the last inequality is a consequence of ρ_1 being proper. Then, there must exist some $t \in T(\Sigma_s)$ such that $w(\vec{d}(l), t) > 0$, and hence $\vec{d}(l)\ \mathsf{R}_P\ t$. Finally, we calculate

$$[\![\rho_2(\theta_l)]\!](t) = w(T(\Sigma_s), t) \geq w(\vec{d}(l), t) > 0$$

which proves (iii).

The definition of (B.1) not only ensures ($\rho_2 2$) but also ($\rho_2 1$) in case $y \in Var(\theta) \cup \bigcup_{l'\in L} Var(\theta_{l'})$. Indeed, if $\vec{z}$ is such that $\vec{z}(l) = y \in \Pi_l(Z_{\vec{d}})$, then $\vec{z} \in Z_{\vec{d}}$ and hence, necessarily $\rho_1(\vec{z}) = \vec{d}$ because of ($\Xi 4$). Therefore $\rho_1(y) = \vec{d}(l)\ \mathsf{R}_P\ \rho_2(y)$ since $y \in \Pi_l(Z_{\vec{d}})$.

It only remain to show cases $(\rho_2 5)$ and $(\rho_2 6)$. We focus first on $(\rho_2 5)$. Because of $(\Xi 3)$ and $(\rho_2 1)$, $\rho_1(\zeta)\ \mathsf{R}_P\ \rho_2(\zeta)$ for all $\zeta \in Var(\theta_l)$, from which $[\![\rho_1(\theta_l)]\!]\ \mathsf{R}_P\ [\![\rho_2(\theta_l)]\!]$, because of Lemmas 9 and 10. Let w be the weight function that witness it. We can now calculate:

$$
\begin{aligned}
[\![\rho_2(\theta_l)]\!](\rho_2(Y_l)) &= \textstyle\sum_{t'\in\rho_2(Y_l)} [\![\rho_2(\theta_l)]\!](t') \\
&= \textstyle\sum_{t'\in\rho_2(Y_l)} w(T(\Sigma_s), t') && \text{(by property (ii) of weight functions)} \\
&= \textstyle\sum_{t\in T(\Sigma_s)} \sum_{t'\in\rho_2(Y_l)} w(t,t') \\
&\geq \textstyle\sum_{t\in\rho_1(Y_l)} \sum_{t'\in\rho_2(Y_l)} w(t,t') && \text{(because } \rho_1(Y_l)\subseteq T(\Sigma_s)) \\
&= \textstyle\sum_{t\in\rho_1(Y_l)} \sum_{t'\in T(\Sigma_s)} w(t,t') && (*) \\
&= [\![\rho_1(\theta_l)]\!](\rho_1(Y_l)) && \text{(by property (i) of weight functions)} \\
&\trianglerighteq_{l,k} p_{l,k} && \text{(by } (\rho_1 5))
\end{aligned}
$$

Since $t \in \rho_1(Y_l)$ there must exist $\vec{d} \in D$ such that $\vec{d}(l) = t$. Then, by property (iii) of weight functions, $w(t,t') > 0$ implies $t\ \mathsf{R}_P\ t'$ and hence $t' \in \rho_2(\Pi_l(Z_{\vec{d}})) \subseteq \rho_2(Y_l)$. From here, if $t' \notin \rho_2(Y_l)$, $w(t,t') = 0$, which justifies (*).

Finally we prove $(\rho_2 6)$. $(\rho_2 1)$ and Lemma 9 imply that $\rho_1(t_n(\vec{z}))\ \mathsf{R}_P\ \rho_2(t_n(\vec{z}))$. By contradiction assume $\rho_2(t_n(\vec{z})) \xrightarrow{b_n} \theta_2' \in \mathsf{CT}_{\alpha-1}$ for some $\theta_2' \in T(\Sigma_d)$. By induction, $\mathrm{II}_{\alpha-1}$ implies $\rho_1(t_n(\vec{z})) \xrightarrow{b_n} \theta_1' \in \mathsf{CT}_\lambda$ for some $\theta_1' \in T(\Sigma_d)$. However, this contradicts $(\rho_1 4)$ which states that $\rho_1(t_n(\vec{z})) \stackrel{b_n}{\not\longrightarrow} \in H$ and $\mathsf{CT}_\lambda \models H$.

Properties $(\rho_2 1)$–$(\rho_2 6)$ imply that rule r together with substitution ρ_2 form the basis of the proof of a transition rule $\frac{H'}{f(\xi_1^2,\cdots,\xi_{\mathsf{rk}(f)}^2)\xrightarrow{a}\rho_2(\theta)}$ with $\mathsf{CT}_{\alpha-1} \models H'$. Hence $f(\xi_1^2,\cdots,\xi_{\mathsf{rk}(f)}^2) \xrightarrow{a} \rho_2(\theta) \in \mathsf{PT}_\alpha$. By $(\rho_2 1)$ and Lemma 9, $\rho_1(\theta)\ \mathsf{R}_P\ \rho_2(\theta)$, which concludes the proof of I_α.

This finishes this part of the proof.

Appendix C. Proof of Theorem 12

The proof of the theorem follows by double induction. The first induction is applied on the height of the proof of $P^0 \uplus P^1 \vdash \frac{N}{t\xrightarrow{a}\theta}$ following Definition 16. The second induction follows the inductive definition of source dependent variables. To facilitate this we introduce the idea of *source distance* of a variable ζ in a rule r, which is the minimal number of steps that takes to deduce that ζ is source dependent in r. Formally, if $r = \frac{H}{t\xrightarrow{a}\theta} \in R^1$, the source distance $\mathrm{sd}(r,\zeta)$ is defined as follows:

- if $\zeta \in Var(t)$, then $\mathrm{sd}(r,\zeta) \leq n$ for all $n \in \mathbb{N}_0$;
- if $t^* \xrightarrow{b} \theta^* \in H$ and $\mathrm{sd}(r,\zeta^*) \leq n$ for all $\zeta^* \in Var(t^*)$, then $\mathrm{sd}(r,\zeta) \leq n+1$ for all $\zeta \in Var(\theta^*)$;
- if $\theta^*(T^*) \bowtie p \in H$ and $\mathrm{sd}(r,\zeta^*) \leq n$ for all $\zeta^* \in Var(\theta^*)$, then $\mathrm{sd}(r,\zeta) \leq n+1$ for all $\zeta \in \bigcup_{t^*\in T^*} Var(t^*)$.

Finally, $\mathrm{sd}(r,\zeta) = \min\,\{n \mid \mathrm{sd}(r,\zeta) \leq n\}$.

For the proof we will also require the following lemma.

Lemma 18. *Let $t \in T(\Sigma^0 \uplus \Sigma^1)$ and $\theta \in T(\Sigma_d^0)$. If $[\![\theta]\!](t) > 0$ then $t \in T(\Sigma_s^0)$.*

The proof of the lemma follows by straightforward induction on the structure of θ.

Proof of Theorem 12. Let $\frac{N}{t\xrightarrow{a}\theta}$ be a closed rule with $t \in T(\Sigma^0)$ and N a set of negative premises and suppose that $P^0 \uplus P^1 \vdash \frac{N}{t\xrightarrow{a}\theta}$ with a proof $\mathfrak{p}$. We show that $\mathfrak{p}$ is also a proof of $P^0 \vdash \frac{N}{t\xrightarrow{a}\theta}$. We proceed by induction on the height of $\mathfrak{p}$. Call this induction (†).

So, suppose the induction hypothesis proved for all proofs strictly smaller than $\mathfrak{p}$. The last step of $\mathfrak{p}$ is defined by a rule $r = \frac{H}{t'\xrightarrow{a}\theta'} \in R^0 \cup R^1$ and a closed substitution $\rho : \mathcal{V} \cup \mathcal{D} \to T(\Sigma^0 \uplus \Sigma^1)$ such that $\rho(t') = t$.

We first show that

$$\rho(\zeta) \in T(\Sigma^0) \text{ for all variable } \zeta \text{ that is source dependent in } r{\downharpoonleft}. \qquad (\star)$$

We proceed by induction on the source distance $\mathrm{sd}(r{\downharpoonleft},\zeta)$. Call this induction (‡).

If $\mathrm{sd}(r{\downharpoonleft},\zeta) = 0$ then $\zeta \in Var(t')$. Since $\rho(t') = t \in T(\Sigma^0)$, necessarily $\rho(\zeta)T(\Sigma^0)$. For the inductive case, let $\mathrm{sd}(r{\downharpoonleft},\zeta) = n+1$. By definition, one of the following cases hold:

A. $t^* \xrightarrow{b} \theta^* \in H$ with $t^* \in \mathbb{T}(\Sigma^0)$ such that $\zeta \in Var(\theta^*)$ and $\mathrm{sd}(r, \zeta^*) \leq n$ for all $\zeta^* \in Var(t^*)$, or
B. $\theta^*(T^*) \bowtie p \in H$ with $\theta^* \in \mathbb{T}(\Sigma^0)$ such that $\zeta \in Var(t^*)$, for some $t^* \in T^*$, and $\mathrm{sd}(r, \zeta^*) \leq n$ for all $\zeta^* \in Var(\theta^*)$.

For case A, induction (‡) implies $\rho(\zeta^*) \in T(\Sigma^0)$ for all $\zeta^* \in Var(t^*)$ and, as a consequence, $\rho(t^*) \in T(\Sigma^0)$. The closed rule $\frac{N}{\rho(t^*) \xrightarrow{b} \rho(\theta^*)}$ is proved with a strict sub-proof of $\mathfrak{p}$ so, by induction (†), $P^0 \vdash \frac{N}{\rho(t^*) \xrightarrow{b} \rho(\theta^*)}$. In particular $\rho(\theta^*) \in T(\Sigma^0)$ and hence $\rho(\zeta) \in T(\Sigma^0)$.

For case B, induction (‡) implies $\rho(\zeta^*) \in T(\Sigma^0)$ for all $\zeta^* \in Var(\theta^*)$ and from here $\rho(\theta^*) \in T(\Sigma^0)$. By Lemma 18, $\rho(t^*) \in T(\Sigma^0)$ and hence $\rho(\zeta) \in T(\Sigma^0)$.

Next, we show that $r \in R^0$. We prove this by contradiction. So, suppose $r \in R^1$. Since $\rho(t') = t \in T(\Sigma^0)$, $t' \in \mathbb{T}(\Sigma^0)$. Then either hypothesis 2b or hypothesis 2c of the theorem applies.

If 2b applies, there exists $t^* \xrightarrow{b} \theta^* \in H$ such that $t^* \in \mathbb{T}(\Sigma^0)$, all variables in $Var(t^*)$ are source dependent in $r\lfloor$, and either $b \notin A^0$ or θ^* is fresh. In this last case $\rho(\theta^*) \notin \mathbb{T}(\Sigma^0)$ Since either $b \notin A^0$ or $\rho(\theta^*) \notin \mathbb{T}(\Sigma^0)$, the sub-proof of $\mathfrak{p}$ proving $\frac{N}{\rho(t^*) \xrightarrow{b} \rho(\theta^*)}$ cannot be a proof in P^0. So, according to induction (‡), $\rho(t^*) \notin T(\Sigma^0)$. Since $t^* \in \mathbb{T}(\Sigma^0)$, necessarily $\rho(\zeta^*) \notin T(\Sigma^0)$ for some $\zeta^* \in Var(t^*)$. Then, by $(\star)$, ζ^* is not source dependent in $r\lfloor$ which contradicts Hypothesis 2(b)ii of the theorem.

If 2c applies, there exists $\theta^*(T^*) \bowtie p \in H$ such that $\theta^* \in \mathbb{T}(\Sigma^0)$, all variables in $Var(\theta^*)$ are source dependent in $r\lfloor$, and T^* contains a fresh term t^*. Because ρ is proper, $[\![\rho(\theta^*)]\!](\rho(t^*)) > 0$, and by Lemma 18, $\rho(\theta^*) \notin T(\Sigma^0)$. Therefore, $\rho(\zeta^*) \notin T(\Sigma^0)$ for some $\zeta^* \in Var(\theta^*)$. Then, by $(\star)$, ζ^* is not source dependent in $r\lfloor$ which contradicts Hypothesis 2(c)ii of the theorem.

So $r \in R^0$ and hence $r = r\lfloor$, so $\rho(\zeta) \in T(\Sigma^0)$ for all variable ζ that is source dependent in r. Because of Hypothesis 1, $\rho(\zeta) \in T(\Sigma^0)$ for all variable ζ in r and hence $\rho(r)$ is a closed instance of r containing only terms in $T(\Sigma^0)$. In particular, for every $t^* \xrightarrow{b} \theta^* \in H$, $\rho(t^*) \in T(\Sigma^0)$. Then, by induction (†), there is a strict sub-proof of $\mathfrak{p}$ of $P^0 \vdash \frac{N}{\rho(t^*) \xrightarrow{b} \rho(\theta^*)}$. Since the last step of $\mathfrak{p}$ is given by $\rho(r)$ which is closed in P^0, then $\mathfrak{p}$ is also a proof in P^0. $\square$

References

[1] G. Plotkin, A structural approach to operational semantics, Report DAIMI FN-19, Aarhus University (1981), reprinted in J. Log. Algebraic Program. 60–61 (2004) 17–139, http://dx.doi.org/10.1016/j.jlap.2004.05.001.
[2] J.F. Groote, F. Vaandrager, Structured operational semantics and bisimulation as a congruence, Inf. Comput. 100 (1992) 202–260, http://dx.doi.org/10.1016/0890-5401(92)90013-6.
[3] B. Bloom, S. Istrail, A.R. Meyer, Bisimulation can't be traced, J. ACM 42 (1995) 232–268, http://dx.doi.org/10.1145/200836.200876.
[4] J.F. Groote, Transition system specifications with negative premises, Theor. Comput. Sci. 118 (2) (1993) 263–299, http://dx.doi.org/10.1016/0304-3975(93)90111-6.
[5] R. Bol, J.F. Groote, The meaning of negative premises in transition system specifications, J. ACM 43 (1996) 863–914, http://dx.doi.org/10.1145/234752.234756.
[6] M.R. Mousavi, M.A. Reniers, J.F. Groote, SOS formats and meta-theory: 20 years after, Theor. Comput. Sci. 373 (3) (2007) 238–272, http://dx.doi.org/10.1016/j.tcs.2006.12.019.
[7] L. Aceto, W. Fokkink, C. Verhoef, Structural operational semantics, in: Handbook of Process Algebra, Elsevier, 2001, pp. 197–292.
[8] L. Aceto, W. Fokkink, C. Verhoef, Conservative extension in structural operational semantics, in: Current Trends in Theoretical Computer Science, 2001, pp. 504–524.
[9] R. Milner, Communication and Concurrency, Prentice-Hall, 1989.
[10] R.J. van Glabbeek, Full abstraction in structural operational semantics, in: M. Nivat, C. Rattray, T. Rus, G. Scollo (Eds.), Algebraic Methodology and Software Technology (AMAST '93), Workshops in Computing, Springer, 1993, pp. 75–82.
[11] J.A. Bergstra, J.C.M. Baeten, S.A. Smolka, Axiomatizing probabilistic processes: ACP with generative probabilities, Inf. Comput. 121 (1995) 234–254, http://dx.doi.org/10.1006/inco.1995.1135.
[12] R.J. van Glabbeek, S.A. Smolka, B. Steffen, Reactive, generative, and stratified models of probabilistic processes, Inf. Comput. 121 (1995) 59–80, http://dx.doi.org/10.1006/inco.1995.1123.
[13] B. Jonsson, K.G. Larsen, W. Yi, Probabilistic extensions of process algebras, in: Handbook of Process Algebra, Elsevier, 2001, pp. 685–710.
[14] P.R. D'Argenio, M.D. Lee, Probabilistic transition system specification: congruence and full abstraction of bisimulation, in: L. Birkedal (Ed.), Foundations of Software Science and Computational Structures – 15th International Conference, Proceedings, FOSSACS 2012, in: LNCS, vol. 7213, Springer, 2012, pp. 452–466.
[15] F. Bartels, GSOS for probabilistic transition systems, in: Proc. CMCS'02, in: Electronic Notes in Theoretical Computer Science, vol. 65, Elsevier, 2002, pp. 29–53.
[16] F. Bartels, On generalised coinduction and probabilistic specification formats, Ph.D. thesis, VU University Amsterdam, 2004.
[17] R. Lanotte, S. Tini, Probabilistic congruence for semistochastic generative processes, in: V. Sassone (Ed.), Foundations of Software Science and Computational Structures, 8th International Conference, Proceedings, FOSSACS 2005, in: LNCS, vol. 3441, Springer, 2005, pp. 63–78.
[18] R. Lanotte, S. Tini, Probabilistic bisimulation as a congruence, ACM Trans. Comput. Log. 10 (2009) 1–48, http://dx.doi.org/10.1145/1462179.1462181.
[19] K.G. Larsen, A. Skou, Bisimulation through probabilistic testing, in: Conference Record of the Sixteenth Annual ACM Symposium on Principles of Programming Languages, ACM Press, 1989, pp. 344–352.
[20] K.G. Larsen, A. Skou, Bisimulation through probabilistic testing, Inf. Comput. 94 (1991) 1–28, http://dx.doi.org/10.1016/0890-5401(91)90030-6.
[21] R. Segala, Modeling and verification of randomized distributed real-time systems, Ph.D. thesis, MIT, 1995.
[22] C. Baier, On algorithmics verification methods for probabilistic systems, Habilitation thesis, Universität Mannheim, 1998.
[23] B. Klin, Bialgebras for structural operational semantics: an introduction, Theor. Comput. Sci. 412 (38) (2011) 5043–5069, http://dx.doi.org/10.1016/j.tcs.2011.03.023.
[24] R. van Glabbeek, The meaning of negative premises in transition system specifications II, J. Log. Algebraic Program. 60–61 (2004) 229–258, http://dx.doi.org/10.1016/j.jlap.2004.03.007.

[25] H. Hermanns, Interactive Markov Chains: The Quest for Quantified Quality, LNCS, vol. 2428, Springer, 2002.
[26] C. Eisentraut, H. Hermanns, L. Zhang, On probabilistic automata in continuous time, in: Proceedings of the 25th Annual IEEE Symposium on Logic in Computer Science, LICS 2010, IEEE Computer Society, 2010, pp. 342–351.
[27] M.D. Lee, D. Gebler, P.R. D'Argenio, Tree rules in probabilistic transition system specifications with negative and quantitative premises, in: Proc. EXPRESS/SOS'12, in: EPTCS, vol. 89, 2012, pp. 115–130.
[28] W. Fokkink, Rooted branching bisimulation as a congruence, J. Comput. Syst. Sci. 60 (2000) 13–37, http://dx.doi.org/10.1006/jcss.1999.1663.
[29] W. Fokkink, C. Verhoef, A conservative look at operational semantics with variable binding, Inf. Comput. 146 (1) (1998) 24–54, http://dx.doi.org/10.1006/inco.1998.2729.
[30] J. Desharnais, A. Edalat, P. Panangaden, Bisimulation for labelled Markov processes, Inf. Comput. 179 (2) (2002) 163–193, http://dx.doi.org/10.1006/inco.2001.2962.
[31] P.R. D'Argenio, P.S. Terraf, N. Wolovick, Bisimulations for non-deterministic labelled Markov processes, Math. Struct. Comput. Sci. 22 (1) (2012) 43–68.
[32] P.R. D'Argenio, C. Verhoef, A general conservative extension theorem in process algebras with inequalities, Theor. Comput. Sci. 177 (2) (1997) 351–380, http://dx.doi.org/10.1016/S0304-3975(96)00292-7.
[33] M. Timmer, J. Katoen, J. van de Pol, M. Stoelinga, Efficient modelling and generation of Markov automata, in: M. Koutny, I. Ulidowski (Eds.), CONCUR 2012 – Concurrency Theory – 23rd International Conference, Proceedings, CONCUR 2012, Newcastle upon Tyne, UK, September 4–7, 2012, in: LNCS, vol. 7454, Springer, 2012, pp. 364–379.
[34] S. Tini, Non-expansive ϵ-bisimulations for probabilistic processes, Theor. Comput. Sci. 411 (2010) 2202–2222, http://dx.doi.org/10.1016/j.tcs.2010.01.027.
[35] D. Turi, G.D. Plotkin, Towards a mathematical operational semantics, in: Proceedings, 12th Annual IEEE Symposium on Logic in Computer Science, IEEE Computer Society, 1997, pp. 280–291.
[36] S. Staton, General structural operational semantics through categorical logic, in: Proceedings of the Twenty-Third Annual IEEE Symposium on Logic in Computer Science, LICS 2008, IEEE Computer Society, 2008, pp. 166–177.
[37] M. Bernardo, D. Sangiorgi, V. Vignudelli, On the discriminating power of passivation and higher-order interaction, in: T.A. Henzinger, D. Miller (Eds.), Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), CSL-LICS'14, ACM, 2014, p. 14.
[38] G. Bacci, M. Miculan, Structural operational semantics for continuous state probabilistic processes, in: Proc. CMCS'12, in: LNCS, vol. 7399, Springer, 2012, pp. 71–89.
[39] B. Klin, V. Sassone, Structural operational semantics for stochastic process calculi, in: Proc. FoSSaCS'08, in: LNCS, vol. 4962, Springer, 2008, pp. 428–433.
[40] B. Klin, Structural operational semantics for weighted transition systems, in: J. Palsberg (Ed.), Semantics and Algebraic Specification, Essays Dedicated to Peter D. Mosses on the Occasion of His 60th Birthday, in: LNCS, vol. 5700, Springer, 2009, pp. 121–139.
[41] B. Klin, V. Sassone, Structural operational semantics for stochastic and weighted transition systems, Inf. Comput. 227 (2013) 58–83, http://dx.doi.org/10.1016/j.ic.2013.04.001.
[42] M. Miculan, M. Peressotti, GSOS for non-deterministic processes with quantitative aspects, in: N. Bertrand, L. Bortolussi (Eds.), Proceedings Twelfth International Workshop on Quantitative Aspects of Programming Languages and Systems, QAPL 2014, in: EPTCS, vol. 154, 2014, pp. 17–33.
[43] M. Bernardo, R. De Nicola, M. Loreti, A uniform framework for modeling nondeterministic, probabilistic, stochastic, or mixed processes and their behavioral equivalences, Inf. Comput. 225 (2013) 29–82, http://dx.doi.org/10.1016/j.ic.2013.02.004.
[44] D. Gebler, S. Tini, Compositionality of approximate bisimulation for probabilistic systems, in: Proc. EXPRESS/SOS'13, in: EPTCS, vol. 120, Open Publishing Association, 2013, pp. 32–46.
[45] G. Bacci, G. Bacci, K.G. Larsen, R. Mardare, Computing behavioral distances, compositionally, in: K. Chatterjee, J. Sgall (Eds.), Mathematical Foundations of Computer Science 2013 – 38th International Symposium, MFCS 2013, in: LNCS, vol. 8087, Springer, 2013, pp. 74–85.
[46] D. Gebler, S. Tini, SOS specifications of probabilistic systems by uniformly continuous operators, in: L. Aceto, D. de Frutos-Escrig (Eds.), 26th International Conference on Concurrency Theory, CONCUR 2015, in: LIPIcs, vol. 42, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2015, pp. 155–168.
[47] D. Gebler, Robust SOS specifications of probabilistic processes, Ph.D. thesis, Vrije Universiteit Amsterdam, 2015.
[48] D. Gebler, W. Fokkink, Compositionality of probabilistic Hennessy–Milner logic through structural operational semantics, in: M. Koutny, I. Ulidowski (Eds.), CONCUR 2012 – Concurrency Theory – 23rd International Conference, Proceedings, in: LNCS, vol. 7454, Springer, 2012, pp. 395–409.
[49] P.R. D'Argenio, D. Gebler, M.D. Lee, Axiomatizing bisimulation equivalences and metrics from probabilistic SOS rules, in: A. Muscholl (Ed.), Foundations of Software Science and Computation Structures – 17th International Conference, Proceedings, FOSSACS 2014, in: LNCS, vol. 8412, Springer, 2014, pp. 289–303.
[50] J.C.M. Baeten, J.A. Bergstra, Process algebra with a zero object, in: J.C.M. Baeten, J.W. Klop (Eds.), CONCUR '90, Theories of Concurrency: Unification and Extension, Proceedings, in: LNCS, vol. 458, Springer, 1990, pp. 83–98.
[51] W. Fokkink, R.J. van Glabbeek, Ntyft/ntyxt rules reduce to ntree rules, Inf. Comput. 126 (1) (1996) 1–10, http://dx.doi.org/10.1006/inco.1996.0030.