Probabilistic Transition System Specification: Congruence and Full Abstraction of Bisimulation*

Pedro R. D'Argenio and Matias Lee

FaMAF, Universidad Nacional de Córdoba – CONICET
{dargenio,lee}@famaf.unc.edu.ar

Abstract. We present a format for the specification of probabilistic transition systems that guarantees that bisimulation equivalence is a congruence for any operator defined in this format. In this sense, the format is somehow comparable to the *ntyft/ntyxt* format in a non-probabilistic setting. We also study the modular construction of probabilistic transition systems specifications and prove that some standard conservative extension theorems also hold in our setting. Finally, we show that the trace congruence for image-finite processes induced by our format is precisely bisimulation on probabilistic systems.

1 Introduction

Plotkin's approach to operational semantics [21] is the standard way to give semantics to specification and programming language in terms of transition systems. It has been formalized with an algebraic flavor as *Transition Systems Specifications (TSS)* [8, 9, 12, 13, 20, 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, e.g., [1, 2, 20] for overviews).

In this paper 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 [19] is a congruence on any TSS in the *ntyft/ntyxt* format [12]. Full abstraction is somewhat a dual result: an equivalence relation is fully abstract with respect to a particular format if it is the largest relation s.t. no context definable in the format can exhibit different behavior when applied to two equivalent processes. For example, strong bisimilarity is fully abstract w.r.t. the *ntyft/ntyxt* format [12] but not w.r.t. the *tyft/tyxt* format [13] or the GSOS format [8].

The introduction of probabilistic process algebras [4, 14, 25, etc.] motivated the need for a theory of structural operational semantics to define *probabilistic* transition systems. A few results have appeared in this direction [6, 7, 16, 17] and, to our knowledge,

* Partially supported by Project ANPCYT PAE-PICT 02272 and SeCyT-UNC.

L. Birkedal (Ed.): FOSSACS 2012, LNCS 7213, pp. 452–466, 2012.
© Springer-Verlag Berlin Heidelberg 2012

only these works present congruence theorems for (probabilistic) bisimilarity [18], 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 [25].) 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 one 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 [22]. So, each probabilistic transition $t \xrightarrow{a} \pi$ is obtained by 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 paper 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 [5], it is also used in the Segala-GSOS format [7] and it is pretty much related to bialgebraic approaches to SOS [7, 15].

In this paper we introduce PTSS with negative and quantitative premises which also allow for lookahead. We use stratification [9, 12] as means to define probabilistic transition systems and prove the existence and uniqueness of models for stratifiable PTSSs (Sec. 3). We also propose a format, which we call *ntμfv/ntμxv*, that is very much like the *ntyft/ntyxt* format in non-probabilistic TSS and show that bisimilarity is a congruence for any operation defined under this format (Sec. 4). Besides, we give a definition for the modular construction of PTSSs and give sufficient conditions to ensure that one PTSS conservatively extends another (Sec. 5). We finally show that bisimilarity is fully abstract with respect to the *ntμfv/ntμxv* format, that is, it is the coarsest congruence w.r.t. any operator defined in *ntμfv/ntμxv* PTSSs that is included in trace equivalence (Sec. 6).

2 Preliminaries

We assume the presence of an infinite set of (term) variables $\mathcal{V}$ and we let x, y, z, x', $x_0, x_1, \ldots$ range over $\mathcal{V}$. A *signature* is a structure $\Sigma = (F, \mathsf{r})$, where (i) F is a set of *function names* disjoint with $\mathcal{V}$, and (ii) $\mathsf{r} : F \to \mathbb{N}_0$ is a *rank function* which gives the arity of a function name; if $f \in F$ and $\mathsf{r}(f) = 0$ then f is called a *constant name*. Let $W \subseteq \mathcal{V}$ be a set of variables. The set of Σ-terms over W, notation $T(\Sigma, W)$ is the

least set satisfying: (i) $W \subseteq T(\Sigma, W)$, and (ii) if $f \in F$ and $t_1, \cdots, t_{\mathrm{r}(f)} \in T(\Sigma, W)$, then $f(t_1, \cdots, t_{\mathrm{r}(f)}) \in T(\Sigma, W)$. $T(\Sigma, \emptyset)$ is abbreviated as $T(\Sigma)$; the elements of $T(\Sigma)$ are called *closed terms*. $T(\Sigma, \mathcal{V})$ is abbreviated as $\mathbb{T}(\Sigma)$; the elements of $\mathbb{T}(\Sigma)$ are called *open terms*. $Var(t) \subseteq \mathcal{V}$ is the set of variables in the open term t.

Since our aim is to deal with languages that describe probabilistic behavior, apart from signatures, variables, and terms, we also need to introduce probability distributions on terms and variables to run on these distributions. Let $\Delta(T(\Sigma))$ denote the set of all (discrete) probability distributions on $T(\Sigma)$. We let $\pi, \pi', \pi_0, \pi_1, \ldots$ range over $\Delta(T(\Sigma))$. As usual, for $\pi \in \Delta(T(\Sigma))$ and $T \subseteq T(\Sigma)$, we define $\pi(T) = \sum_{t \in T} \pi(t)$. For $t \in T(\Sigma)$, let δ_t denote the Dirac distribution, that is, $\delta_t(t') =$ if $(t{=}t')$ then 1 else 0. Moreover, the product measure $\prod_{i=1}^n \pi_i$ is defined by $(\prod_{i=1}^n \pi_i)(t_1, \ldots, t_n) = \prod_{i=1}^n \pi_i(t_i)$. In particular, if $n = 0$, $(\prod_{j \in \emptyset} \pi_j) = \delta_{()}$ is the distribution that assigns probability 1 to the 0-ary tuple. Let $g : T(\Sigma)^n \to T(\Sigma)$ and recall that $g^{-1}(t') = \{\vec{t} \in T(\Sigma)^n \mid g(\vec{t}) = t'\}$. Then $(\prod_{i=1}^n \pi_i) \circ g^{-1}$ is a well defined probability distribution on closed terms. In particular, if $g : T(\Sigma)^0 \to T(\Sigma)$ and $g(()) = t$, then $(\prod_{j \in \emptyset} \pi_j) \circ g^{-1} = \delta_{()} \circ g^{-1} = \delta_t$.

A *distribution variable* is a variable that takes values on $\Delta(T(\Sigma))$. Let $\mathcal{M}$ be an infinite set of distribution variables and let $\mu, \mu', \mu_0, \mu_1, \ldots$ range over $\mathcal{M}$. For a term variable $x \in \mathcal{V}$ we let δ_x be an *instantiable Dirac distribution*. That is, δ_x is a symbol that takes value δ_t whenever variable x takes value t. Let $\mathcal{D} = \{\delta_x : x \in \mathcal{V}\}$ be the set of instantiable Dirac distributions according to the variable set $\mathcal{V}$.

A substitution is a mapping that assigns terms to variables. In our case we need to extend this notion to probabilistic variables and instantiable Dirac distributions. A *(closed) substitution* ρ is a mapping in $(\mathcal{V} \cup \mathcal{M}) \to (T(\Sigma) \cup \Delta(T(\Sigma)))$ such that $\rho(x) \in T(\Sigma)$ whenever $x \in \mathcal{V}$, and $\rho(\mu) \in \Delta(T(\Sigma))$ whenever $\mu \in \mathcal{M}$. A substitution ρ extends to open terms and sets as usual and to instantiable Dirac distributions by $\rho(\delta_x) = \delta_{\rho(x)}$.

Example 1. We introduce the signature of a probabilistic process algebra that includes many of the most representative operators. We assume the existence of a set $\mathcal{L}$ of action labels. Then, our signature (which is the base of our running example) contains: two constants, $\mathbf{0}$ (stop process) and ε (skip process); a family of n-ary probabilistic prefix operators $a.([p_1]\_ \oplus \cdots \oplus [p_n]\_)$ with $a \in \mathcal{L}$, $n \geq 1$, $p_1, \ldots, p_n \in (0, 1]$ s.t. $\sum_{i=1}^n p_i = 1$ (we usually write $a.\sum_{i=1}^n [p_i]t_i$ for given terms $t_1, \ldots, t_n$); binary operators $\_ + \_$ (alternative composition or sum), $\_ ; \_$ (sequential composition), and, for each $B \subseteq \mathcal{L}$, $\_ \|_B \_$ (parallel composition); and a unary operator $\mathsf{U}(\_)$ that we call *unreach*. The intended meaning of $a.\sum_{i=1}^n [p_i]t_i$ is that this term can perform action a and move to term t_i with probability p_i. The unreach operation $\mathsf{U}(t)$ can perform an action a and stop if there is a probabilistic execution (or *scheduler*) from t in which action a is never performed (or properly speaking, it is not performed with probability 1). Finally, $t \|_B t'$ 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 have the usual meaning. □

3 Probabilistic Transition System Specifications

A (probabilistic) transition relation prescribes what 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 [22] which are a generalization of the so called reactive model [18]. So, let Σ be a signature and A be a set of labels. A *transition relation* is a set $\rightarrow \subseteq PTr(\Sigma, A)$, where $PTr(\Sigma, A) = T(\Sigma) \times A \times \Delta(T(\Sigma))$. We denote $(t, a, \pi) \in \rightarrow$ by $t \xrightarrow{a} \pi$.

Transition relations are usually defined by means of structured operational semantics in Plotkin's style [21]. Algebraic characterizations of this style were provided in [9, 12, 13] 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 2. *A* probabilistic transition system specification *(PTSS) is a triple* $P = (\Sigma, A, R)$ *where* $\Sigma = (F, r)$ *is a signature,* A *is a set of labels, and* R *is a set of rules of the form:*

$$\frac{\{t_k \xrightarrow{a_k} \mu_k : k \in K\} \cup \{t_l \xrightarrow{b_l} \not\rightarrow : l \in L\} \cup \{\mu_j(W_j) \gtrless_j q_j : j \in J\}}{t \xrightarrow{a} \sum_{i \in I} p_i(\prod_{n_i \in N_i} \nu_{n_i}) \circ g_i^{-1}}$$

where K, L, J *are index sets,* I *is a denumerable index set, each* N_i *is a finite index set,* $t, t_k, t_l \in \mathbb{T}(\Sigma)$, $a, a_k, b_l \in A$, $\mu_k, \mu_j \in \mathcal{M}$, $W_j \subseteq \mathcal{V}$, $\gtrless_j \in \{>, \geq, <, \leq\}$, $p_i, q_j \in [0, 1]$ *with* $\sum_{i \in I} p_i = 1$, *each* g_i *is a function s.t.* $g_i : T(\Sigma)^{N_i} \rightarrow T(\Sigma)$, *and* $\nu_{n_i} \in \mathcal{M} \cup \mathcal{D}$.

An expression of the form $t \xrightarrow{a} \pi$, $(t \xrightarrow{a} \not\rightarrow, \pi(T) \gtrless p)$ is a *positive literal* (*negative literal, quantitative literal*, resp.). For any rule $r \in R$, literals above the line are called *premises*, notation prem(r); the literal below the line is called *conclusion*, notation conc(r). We denote with pprem(r) (nprem(r), qprem(r)) the set of positive (negative, quantitative, resp.) literals of the rule r. A rule r is called *positive* if there are no negative premises, i.e., nprem(r) $= \emptyset$. A PTSS is called positive if it has only positive rules. A rule r without premises is called *axiom*. In general, we allow that the sets of positive, negative, and quantitative premises are 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: $\rho(t \xrightarrow{a} \mu) = \rho(t) \xrightarrow{a} \rho(\mu)$, $\rho(t \xrightarrow{a} \not\rightarrow) = \rho(t) \xrightarrow{a} \not\rightarrow$, $\rho(\mu(W) \gtrless p) = \rho(\mu)(\rho(W)) \gtrless p$, and $\rho(t \xrightarrow{a} \sum_{i \in I} p_i(\prod_{n_i \in N_i} \nu_{n_i}) \circ g_i^{-1}) = \rho(t) \xrightarrow{a} \sum_{i \in I} p_i(\prod_{n_i \in N_i} \rho(\nu_{n_i})) \circ g_i^{-1}$. Then, the notion of substitution extends to rules as expected. 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 premise $\rho(\mu(W)) \gtrless p$ of r it holds that $\rho(\mu(w)) > 0$ for all $w \in W$. Thus, if ρ is proper, all terms in $\rho(W)$ are in the support set of $\rho(\mu)$. Proper substitutions avoid the introduction of spurious terms. This is of particular importance for the conservative extension theorem (Theorem 14).

Example 3. The rules for the process algebra of Example 1 are defined in Table 1. We consider the set of actions $A = \mathcal{L} \cup \{\surd\}$ where $\surd \notin \mathcal{L}$. In the table we use the following shorthand notations for the target of the conclusion which we also adopt along the paper. We omit the summation if I is a singleton and, if $g(()) = t$, we write

Table 1. Rules for our probabilistic process algebra ($Y \subseteq \mathcal{V}$ is a countably infinite set)

$$\varepsilon \xrightarrow{\surd} \delta_{\mathbf{0}} \qquad a.\textstyle\sum_{i=1}^{n}[p_i]x_i \xrightarrow{a} \sum_{i=1}^{n} p_i\delta_{x_i} \qquad \frac{x \xrightarrow{a} \mu}{x+y \xrightarrow{a} \mu} \qquad \frac{y \xrightarrow{a} \mu}{x+y \xrightarrow{a} \mu}$$

$$\frac{x \xrightarrow{a} \mu}{x;y \xrightarrow{a} \mu;\delta_y}\ a \neq \surd \qquad \frac{x \xrightarrow{\surd} \mu \quad y \xrightarrow{a} \mu'}{x;y \xrightarrow{a} \mu'} \qquad \frac{x \xrightarrow{a} \mu \quad y \xrightarrow{a} \mu'}{x \parallel_B y \xrightarrow{a} \mu \parallel_B \mu'}\ a \in B\backslash\{\surd\}$$

$$\frac{x \xrightarrow{a} \mu}{x \parallel_B y \xrightarrow{a} \mu \parallel_B \delta_y}\ a \notin B \cup \{\surd\} \qquad \frac{y \xrightarrow{a} \mu}{x \parallel_B y \xrightarrow{a} \delta_x \parallel_B \mu}\ a \notin B \cup \{\surd\} \qquad \frac{x \xrightarrow{\surd} \mu \quad y \xrightarrow{\surd} \mu'}{x \parallel_B y \xrightarrow{\surd} \delta_{\mathbf{0}}}$$

$$\frac{x \not\xrightarrow{a}}{\mathsf{U}(x) \xrightarrow{a} \delta_{\mathbf{0}}} \qquad \frac{x \xrightarrow{b} \mu \quad \mu(Y) \geq 1 \quad \{\mathsf{U}(y) \xrightarrow{a} \mu'_y \mid y \in Y\}}{\mathsf{U}(x) \xrightarrow{a} \delta_{\mathbf{0}}}\ b \neq a, x \notin Y$$

δ_t instead of $(\prod_{n_i \in \emptyset} \nu_{n_i}) \circ g^{-1}$. Thus, in the rules of ε and $\mathsf{U}(x)$, we write $\delta_{\mathbf{0}}$ instead of $\sum_{i\in\{1\}} 1(\prod_{n_i\in\emptyset} \nu_{n_i}) \circ g_{\mathbf{0}}^{-1}$ with $g_{\mathbf{0}}(()) = \mathbf{0}$. If $g = id$ is the identity function, we only write μ instead of $\mu \circ id^{-1}$ as it is the case in the conclusion of rules for $+$. Finally, for an n-ary operator f, we write $f(\nu_1, \ldots, \nu_n)$ instead of $(\nu_1 \times \cdots \times \nu_n) \circ f^{-1}$. For instance, in the first rule of the sequential composition, we write $\mu;\delta_y$ instead of $(\mu \times \delta_y) \circ (;)^{-1}$.

We give some examples of closed instances of rules to understand the notation in the target of the conclusion. Take the closed instance $a.\sum_{i=1}^{3}[p_i]t_i \xrightarrow{a} \sum_{i=1}^{3} p_i\delta_{t_i}$ of the rule of the probabilistic prefix operator and assume that $t_1 \neq t_2 = t_3$. Then, $(\sum_{i=1}^{3} p_i\delta_{t_i})(t_1) = p_1$ which is what we expect. Moreover $(\sum_{i=1}^{3} p_i\delta_{t_i})(t_2) = (p_2 + p_3)$ which is also what we expect, since we need $(\sum_{i=1}^{3} p_i\delta_{t_i})(\{t_1, t_2, t_3\}) = 1$ (and $\{t_1, t_2, t_3\} = \{t_1, t_2\}$!).

Now, take the same term $a.\sum_{i=1}^{3}[p_i]t_i$ and the closed instance of the first rule of sequential composition $\frac{a.\sum_{i=1}^{3}[p_i]t_i \xrightarrow{a} \pi}{(a.\sum_{i=1}^{3}[p_i]t_i);\varepsilon \xrightarrow{a} \pi;\delta_\varepsilon}$ with $\pi = \sum_{i=1}^{3} p_i\delta_{t_i}$. Notice that $(\pi;\delta_\varepsilon)(t_2;\varepsilon) = (\pi \times \delta_\varepsilon)(\{(t_2, \varepsilon)\}) = (p_2 + p_3)$. Instead, for example, $(\pi;\delta_\varepsilon)(t_2;\mathbf{0}) = (\pi \times \delta_\varepsilon)(\{(t_2, \mathbf{0})\}) = \pi(t_2)\delta_\varepsilon(\mathbf{0}) = 0$, and $(\pi;\delta_\varepsilon)(t_2 + \varepsilon) = (\pi \times \delta_\varepsilon)((;)^{-1}(\{t_2 + \varepsilon\})) = (\pi \times \delta_\varepsilon)(\emptyset) = 0$. □

As has already been argued many times (see, e.g., [9, 12, 24]), transition system specifications with negative premises do not uniquely define a transition relation and different reasonable techniques may lead to incomparable choices. In any case, we expect that a transition relation associated to a PTSS P (i) respects the rules of P, that is, whenever the premises of a closed instance of a rule of P belong to the transition relation, so does its conclusion; and (ii) it does not include more transitions than those explicitly justified, i.e., a transition is defined only whenever there is a closed rule whose premises are in the transition relation. The first notion corresponds to that of model, and the second one to that of supported transition.

Before formally defining these notions we introduce some notation. Given a transition relation $\rightarrow \subseteq PTr(\Sigma, A)$, a positive literal $t \xrightarrow{a} \pi$ *holds in* $\rightarrow$, notation $\rightarrow \models t \xrightarrow{a} \pi$, if $(t, a, \pi) \in \rightarrow$. A negative literal $t \not\xrightarrow{a}$ *holds in* $\rightarrow$, notation $\rightarrow \models t \not\xrightarrow{a}$, if there is no $\pi \in \Delta(T(\Sigma))$ s.t. $(t, a, \pi) \in \rightarrow$. A quantitative literal $\pi(T) \gtrless p$ *holds in* $\rightarrow$, notation

$\rightarrow \models \pi(T) \gtrless p$ precisely when $\pi(T) \gtrless p$. Notice that the satisfaction of a quantitative literal 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 $\rightarrow \models H$ if $\forall \phi \in H : \rightarrow \models \phi$.

Definition 4. *Let $P = (\Sigma, A, R)$ be a PTSS. Let $\rightarrow \subseteq PTr(\Sigma, A)$ be a probabilistic transition system. Then $\rightarrow$ is* a supported model of *P if it satisfies that: $\psi \in \rightarrow$ iff there is a rule $\frac{H}{\chi} \in R$ and a proper substitution ρ s.t. $\rho(\chi) = \psi$ and $\rightarrow \models \rho(H)$.*

Notice that the form of the target of the conclusion of a rule guarantees that if $\psi = t \xrightarrow{a} \pi$ then π is indeed a probability distribution (and hence, $\pi(T(\Sigma)) = 1$).

We have already pointed out that PTSSs with negative premises do not uniquely define a transition relation. In fact, a PTSS may have more than one supported model. For instance, the PTSS with the single constant f, set of labels $\{a, b\}$ and the two rules $\frac{f \xrightarrow{a} \mu}{f \xrightarrow{a} \delta_f}$ and $\frac{f \not\xrightarrow{a}}{f \xrightarrow{b} \delta_f}$, has two supported models: $\{f \xrightarrow{a} \delta_f\}$ and $\{f \xrightarrow{b} \delta_f\}$. We will not dwell on this problem which has been studied at length in [9] and [24] in a non-probabilistic setting. We will only focus on the stratification method [12] which has been widely used to give meaning to TSS with negative premises. A stratification defines an order on closed positive literals that ensures that, in the stratified PTSS, the validity of a transition does not depend on the negation of the same transition.

Definition 5. *Let $P = (\Sigma, A, R)$ be a PTSS. A function $S : PTr(\Sigma, A) \rightarrow \alpha$, where α is an ordinal, is called* stratification *of P (and P is said to be* stratified*) if for every rule*

$$r = \frac{\{t_k \xrightarrow{a_k} \mu_k : k \in K\} \cup \{t_l \not\xrightarrow{b_l} : l \in L\} \cup \{\mu_j(W_j) \gtrless q_j : j \in J\}}{t \xrightarrow{a} \sum_i p_i(\prod_{n_i \in N_i} \nu_{n_i}) \circ g_i^{-1}}$$

and substitution $\rho : (\mathcal{V} \cup \mathcal{M}) \rightarrow (T(\Sigma) \cup \Delta(T(\Sigma)))$ it holds that: (i) for all $k \in K$, $S(\rho(t_k \xrightarrow{a_k} \mu_k)) \leq S(conc(r))$, and (ii) for all $l \in L$ and $\mu \in \mathcal{M}$, $S(\rho(t_l \xrightarrow{b_l} \mu)) < S(conc(r))$. Each set $S_\beta = \{\phi \mid S(\phi) = \beta\}$, with $\beta < \alpha$, is called stratum*. If for all $k \in K$, $S(\rho(t_k \xrightarrow{a_k} \mu_k)) < S(conc(r))$, then the stratification is said to be* strict*.*

A transition relation is constructed stratum by stratum in an increasing manner by transfinite recursion. If it has been decided whether a transition in a stratum $S_{\beta'}$, with $\beta' < \beta$, is valid or not, we already know the validity of the negative premise occurring in the premises of a transition φ in stratum S_β (since all positive instances of the negative premises are in strictly lesser stratums) and hence we can determine the validity of φ.

Definition 6. *Let $P = (\Sigma, A, R)$ be a PTSS with stratification $S : PTr(\Sigma, A) \rightarrow \alpha$ for some ordinal α. For all rule r, let $\mathsf{D}(r)$ be the smallest regular cardinal greater than $|pprem(r)|$, and let $\mathsf{D}(P)$ be the smallest regular cardinal such that $\mathsf{D}(P) \geq \mathsf{D}(r)$ for all $r \in R$. The transition relation $\rightarrow_{P,S}$* associated with *P (and based on S) is defined by $\rightarrow_{P,S} = \bigcup_{\beta<\alpha} \rightarrow_{P_\beta}$, where each $\rightarrow_{P_\beta} = \bigcup_{j \leq \mathsf{D}(P)} \rightarrow_{P_{\beta,j}}$ and each $\rightarrow_{P_{\beta,j}}$ is defined by*

$$\rightarrow_{P_{\beta,j}} = \Big\{ \psi \;\Big|\; S(\psi) = \beta \text{ and } \exists r \in R \text{ and proper substitution } \rho \text{ s.t. } \psi = conc(\rho(r)),\ (\textstyle\bigcup_{\gamma<\beta} \rightarrow_{P_\gamma}) \cup (\bigcup_{j'<j} \rightarrow_{P_{\beta,j'}}) \models qprem(\rho(r)) \cup pprem(\rho(r)) \text{ and } (\textstyle\bigcup_{\gamma<\beta} \rightarrow_{P_\gamma}) \models nprem(\rho(r)) \Big\}$$

The PTSS with the only two rules $\frac{f \xrightarrow{a} \mu}{f \xrightarrow{a} \delta_f}$ and $\frac{f \xrightarrow{a} \!\!\!\!/}{f \xrightarrow{b} \delta_f}$ (given before) can be stratified by a function S such that $S(f \xrightarrow{a} \delta_f) = 0$ and $S(f \xrightarrow{b} \delta_f) = 1$. Using S, the model associated with the PTSS is $\{f \xrightarrow{b} \delta_f\}$. More interestingly, a stratification for our running example is given by $S(t \xrightarrow{a} \mu) = \zeta(t)$ where $\zeta(\mathbf{0}) = \zeta(\varepsilon) = \zeta(a.\sum_{i=1}^{n}[p_i]t_i) = 0$, $\zeta(t_1 + t_2) = \zeta(t_1; t_2) = \zeta(t_1 \parallel_B t_2) = \max\{\zeta(t_1), \zeta(t_2)\}$, and $\zeta(\mathsf{U}(t)) = \zeta(t) + 1$. Notice that this stratification is *not* strict.

The existence of a stratification guarantees the existence of a supported model. In fact, such model is the one in Def. 6 (Theorem 7) and it is the only possible one defined via stratification (Theorem 8). Moreover, if it is defined using a strict stratification, the supported model is unique (Theorem 9).

The proofs of the following theorems follow closely the proofs of their non-probabilistic counterparts in [12] (Theorem 2.15, Lemma 2.16 and Theorem 2.18, respectively). The only actual difference lies on the quantitative premises, which do not pose any particular problem since their validity only depends on the substitution. For the next theorems, let $P = (\Sigma, A, R)$ be a PTSS with stratification S.

Theorem 7. *The transition relation $\rightarrow_{P,S}$ is a supported model of P.*

Theorem 8. *If S' is another stratification for P, $\rightarrow_{P,S} = \rightarrow_{P,S'}$.*

Theorem 9. *If S is strict, then, $\rightarrow_{P,S}$ is the only supported model of P.*

4 The *ntμfv/ntμxv* Format and the Congruence Theorem

In this section we present one of the main results of our paper: we introduce a general format that ensures that bisimulation equivalence is a congruence for any operator defined in this format. The importance of the theorem is that congruence of bisimilarity is guaranteed by mere inspection of the rules. We first define the notion of bisimulation on probabilistic transition system [18]. We use a more modern (but equivalent) definition.

Given a relation $\mathsf{R} \subseteq T(\Sigma) \times T(\Sigma)$, a set $Q \subseteq T(\Sigma)$ is R-closed if for all $t \in Q$ and $t' \in T(\Sigma)$, $t \mathsf{R} t'$ implies $t' \in Q$ (i.e. $\mathsf{R}(Q) \subseteq Q$). If a set Q is R-closed we write R-closed(Q). It is easy to verify that if two relation $\mathsf{R}, \mathsf{R}' \subseteq T(\Sigma) \times T(\Sigma)$ are such that $\mathsf{R}' \subseteq \mathsf{R}$, then for all set $Q \subseteq T(\Sigma)$, R-closed(Q) implies R'-closed(Q).

Definition 10. *A relation $\mathsf{R} \subseteq T(\Sigma) \times T(\Sigma)$ is a bisimulation if R is symmetric and for all $t, t' \in T(\Sigma)$, $\pi \in \Delta(T(\Sigma))$, $a \in A$,*

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

where $\pi \mathsf{R} \pi'$ if and only if $\forall Q \subseteq T(\Sigma) : \mathsf{R}\text{-closed}(Q) \Rightarrow \pi(Q) = \pi'(Q)$. We define the relation $\sim$ as the smallest relation that includes all other bisimulation. It is known that $\sim$ is itself a bisimulation relation and an equivalence relation.

Before introducing the *ntμfv/ntμxv* format, we give a first approach to extend the *ntyft/ntyxt* format with probabilities that considers a very restrictive form of quantitative premise. It can also be seen as a generalization of Segala-GSOS format [7] with

terms in the premises as well as lookahead. This first approach considers rules of the form

$$\frac{\{t_m \xrightarrow{a_m} \mu_m : m \in M\} \cup \{t_n \xrightarrow{b_n} \not\to : n \in N\} \cup \{\mu_l(z_l) > 0 : l \in L\}}{f(x_1, \ldots, x_{\mathsf{r}(f)}) \xrightarrow{a} \sum_{i \in I} p_i(\prod_{n_i \in N_i} \nu_{n_i}) \circ g_i^{-1}} \tag{F}$$

where M, N, and L are index sets, μ_m, z_l, x_k ($1 \leq k \leq \mathsf{r}(f)$) are all different variables, $f \in F$, $t_m, t_n \in \mathbb{T}(\Sigma)$, and p_i and g_i are like in Def. 2. Notice that all rules in Table 1 respond to this format except for the last one which has a quantitative premise comparing to a number different from 0. (It can be proved that bisimilarity is a congruence for any operator defined in format (F).)

In the following we present several counterexamples justifying the restrictions imposed by format in eq. (F). We consider a signature with a unary operator f and three constants b, c and d, together with a label a. We will also consider axioms $c \xrightarrow{a} \delta_c$ and $d \xrightarrow{a} (0.5 \cdot \delta_c + 0.5 \cdot \delta_d)$, and no rule associated to constant b. (We write π_d for $(0.5 \cdot \delta_c + 0.5 \cdot \delta_d)$). Notice that $c \sim d$. In the following we concentrate in 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 [12, 13] for the *tyft/tyxt* format. We adapt an example form [12] to motivate the need. Consider the axiom $f(b) \xrightarrow{a} \delta_{f(b)}$. Then $f(f(b)) \sim b$ since none of them perform any action. But $f(f(f(b)))$ and $f(b)$ are not bisimilar since $f(b)$ can perform an action but $f(f(f(b)))$ cannot. Similarly, the requirement that all variables μ_m, z_l, x_k are different is inherited from the *tyft/tyxt* format. Examples from [13] should be easily adaptable to our setting.

The next example shows that the target of a positive premise cannot be a distribution on a particular (shape of) term. Consider rule $\frac{x \xrightarrow{a} \delta_c}{f(x) \xrightarrow{a} \delta_c}$. Then, despite that $c \sim d$, $f(c)$ and $f(d)$ are not bisimilar since $d \xrightarrow{a} \delta_c$ is *not* a valid transition in the (unique) supported model. A similar effect has rule $\frac{x \xrightarrow{a} \mu \quad \mu(d) > 0}{f(x) \xrightarrow{a} \delta_c}$, which shows that quantitative literals cannot enquire over arbitrary terms: note that $f(c)$ and $f(d)$ are not bisimilar since $c \xrightarrow{a} \delta_c$ and $\delta_c(d) = 0$.

Allowing for a quantitative literal that compares with a value different from 0 is also problematic. Consider rule $\frac{x \xrightarrow{a} \mu \quad y \xrightarrow{a} \mu' \quad \mu(y) \geq 1}{f(x) \xrightarrow{a} \delta_c}$. Again $f(c)$ and $f(d)$ are not bisimilar since $d \xrightarrow{a} \pi_d$, and there is no single term t in which $\pi_d(t) \geq 1$.

This example suggest that quantitative premises should have the form $\mu(Y) > p$ or $\mu(Y) \geq p$ where Y is a set of variables. So the previous rule could be recast as $\frac{x \xrightarrow{a} \mu \quad y \xrightarrow{a} \mu' \quad \mu(\{y,z\}) \geq 1}{f(x) \xrightarrow{a} \delta_c}$. However, the same problem repeats if we introduce a new constant e with $e \xrightarrow{a} (0.4 \cdot \delta_c + 0.3 \cdot \delta_d + 0.3 \cdot \delta_e)$. 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 $e_n \xrightarrow{a} (\sum_{i \in \mathbb{N}_0} \frac{1}{2^{i+1}} \cdot \delta_{e_i})$). Moreover, it is necessary that all terms that substitutes some variable in Y have symmetric behavior. Notice that the term substituting z is not required to perform action a, which was not the originally intended behavior. Moreover, symmetry is also necessary for the congruence result as we will see later.

After the previous considerations, we extend format (F) with quantitative premises of the form $\mu(Y) > p$ or $\mu(Y) \geq p$. We call this format *ntμfv/ntμxv* following the nomenclature of [12, 13]. Later we give more examples justifying our restrictions.

Let $\{Y_l\}_L$ be a family of sets of variables with the same cardinality. Given a tuple $\vec{y}$, the l-th element of $\vec{y}$ is denoted by $\vec{y}(l)$. Fix a set $\mathsf{Diag}\{Y_l\}_L \subseteq \prod_{l\in L} Y_l$ so that:

(i) for all $l \in L$, $\pi_l(\mathsf{Diag}\{Y_l\}_L) = Y_l$ (here, π_l indicates the l-th projection); and
(ii) for all $\vec{y}, \vec{y'} \in \mathsf{Diag}\{Y_l\}_L$, $(\exists l \in L : \vec{y}(l) = \vec{y'}(l)) \Rightarrow \vec{y} = \vec{y'}$.

Notice that if each set $Y_l = \{y_l^0, y_l^1, y_l^2, \ldots\}$, a possible definition for $\mathsf{Diag}\{Y_l\}_L$ may be $\mathsf{Diag}\{Y_l\}_L = \{(y_0^0, y_1^0, \ldots, y_L^0), (y_0^1, y_1^1, \ldots, y_L^1), (y_0^2, y_1^2, \ldots, y_L^2), \ldots\}$.

Definition 11 (*ntμfv/ntμxv*). *Let $P = (\Sigma, A, R)$ be a stratifiable PTSS. A rule $r \in R$ is in ntμfv* format *if it has the form*

$$\frac{\bigcup_{m\in M}\{t_m(\vec{z}) \xrightarrow{a_m} \mu_m^{\vec{z}} : \vec{z} \in \mathcal{Z}\} \cup \bigcup_{n\in N}\{t_n(\vec{z}) \xrightarrow{b_n} \not\to : \vec{z} \in \mathcal{Z}\} \cup \{\mu_l^{\vec{z}}(Y_l) \trianglerighteq_l q_l : l \in L, \vec{z} \in \mathcal{Z}\}}{f(x_1, \ldots, x_{\mathrm{r}(f)}) \xrightarrow{a} \sum_{i\in I} p_i(\prod_{n_i\in N_i} \nu_{n_i}) \circ g_i^{-1}}$$

with $\trianglerighteq_l \in \{>, \geq\}$, for all $l \in L$, satisfying 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. *$\mathcal{Z} = \mathsf{Diag}\{Y_l\}_L \times \prod_{w\in W}\{w\}$, with $W \subseteq \mathcal{V} \setminus \bigcup_{l\in L} Y_l$.*
3. *All variables $\mu_m^{\vec{z}}$, with $m \in M$ and $\vec{z} \in \mathcal{Z}$, are different.*
4. *For all $\vec{z}, \vec{z'} \in \mathcal{Z}$, $m \in M$, if $\mu_m^{\vec{z}} = \nu_{n_i}$ and $\mu_m^{\vec{z'}} = \nu_{n_h}$ for some $n_i \in N_i$, $n_h \in N_h$, $i, h \in I$, then $\vec{z} = \vec{z'}$.*
5. *For all $l \in L$, $Y_l \cap \{x_1, \ldots, x_{\mathrm{r}(f)}\} = \emptyset$, and $Y_l \cap Y_{l'} = \emptyset$ for all $l' \in L$, $l \neq l'$.*
6. *All variables $x_1, \ldots, x_{\mathrm{r}(f)}$ are different.*
7. *$f \in F$ and for all $m \in M$ and $n \in N$, $t_m, t_n \in \mathbb{T}(\Sigma)$. In all cases, if $t \in \mathbb{T}(\Sigma)$ and $Var(t) \subseteq \{w_1, \ldots, w_H\}$, $t(w'_1, \ldots, w'_H)$ is the same term as t where each occurrence of variable w_h (if it appears in t) has been replaced by variable w'_h, for $1 \leq h \leq H$.*

A rule $r \in R$ is in ntμxv format *if its form is like before but with the conclusion having instead the form $x \xrightarrow{a} \sum_{i\in I} p_i(\prod_{n_i\in N_i} \nu_{n_i}) \circ g_i^{-1}$. It satisfies the same conditions as above only that $x \notin Y_l$ for all $l \in L$ instead of $Y_l \cap \{x_1, \ldots, x_{\mathrm{r}(f)}\} = \emptyset$ in item 5.*

P is in ntμfv (resp. ntμxv) format *if all its rules are in ntμfv (resp. ntμxv) format. P is in ntμfv/ntμxv* format *if all its rules are either in ntμfv format or ntμxv format.*

We define notation $t_m(\vec{Z}_m) \xrightarrow{a_m} \mu_m$ as an abbreviation for $\{t_m(\vec{z}) \xrightarrow{a_m} \mu_m^{\vec{z}} : \vec{z} \in \mathcal{Z}\}$ where $\vec{Z}_m = \mathsf{Diag}\{Y_l\}_{L'} \times \prod_{w\in W'}\{w\}$ with $L' \subseteq L$ and $W' \subseteq W$, where the number of variables of t_m is exactly the dimension of $\vec{Z}_m$ (i.e. $|Var(t_m)| = |L'| + |W'|$). Similarly, we define $t_n(\vec{Z}_n) \xrightarrow{b_n} \not\to$ as an abbreviation for $\{t_n(\vec{z}) \xrightarrow{b_n} \not\to : \vec{z} \in \mathcal{Z}\}$, and $\mu_l(Y_l) \trianglerighteq_l q_l$ for the set $\{\mu_l^{\vec{z}}(Y_l) \trianglerighteq_l q_l : \vec{z} \in \mathcal{Z}\}$. Thus, rule $\frac{y \xrightarrow{a} \mu}{x+y \xrightarrow{a} \mu}$ is the notational rewriting of rule $\frac{\{y \xrightarrow{a} \mu_i \mid i \geq 0\}}{x+y \xrightarrow{a} \mu_0}$ and rule $\frac{x \xrightarrow{b} \mu \quad \mu(Y) \geq 1 \quad \{\mathsf{U}(y) \xrightarrow{a} \mu'_y \mid y \in Y\}}{\mathsf{U}(x) \xrightarrow{a} \delta_{\mathbf{0}}} b \neq a$ can be rewritten to $\frac{x \xrightarrow{b} \mu \quad \mu(Y) \geq 1 \quad \mathsf{U}(Y) \xrightarrow{a} \mu'}{\mathsf{U}(x) \xrightarrow{a} \delta_{\mathbf{0}}} b \neq a$. In fact, notice that all rules of our running example (see Table 1) are in *ntμfv* format.

Restrictions 3, 5, 6 and 7 are basically the same requirements present in the format of eq. (F). Hence, all examples given before also apply to the *ntμfv/ntμxv* format. Besides, notice that rule $\frac{x \xrightarrow{a} \mu \quad y \xrightarrow{a} \mu' \quad \mu(y) \geq 1}{f(x) \xrightarrow{a} \delta_c}$ given before is not in *ntμfv/ntμxv* format, but the intended behavior can be encoded as the *ntμfv* rule $\frac{x \xrightarrow{a} \mu \quad Y \xrightarrow{a} \mu' \quad \mu(Y) \geq 1}{f(x) \xrightarrow{a} \delta_c}$.

The next example shows that quantitative literals cannot check for upper bounds (or equality). Consider the rule $\frac{x \xrightarrow{a} \mu \quad Y \xrightarrow{a} \mu' \quad \mu(Y) \leq 0.5}{f(x) \xrightarrow{a} \delta_c}$ with c and d defined as before. $f(c)$ and $f(d)$ are not bisimilar because $f(d) \xrightarrow{a} \delta_c$ by taking the substitution ρ such that $\rho(y) = c$ for all $y \in Y$, but $f(c) \not\xrightarrow{a}$ since there is no set of terms T such that *properly* substituted in Y (i.e., such that $\delta_c(t) > 0$ for all $t \in T$), $\delta_c(T) \leq 0.5$.

Finally, if symmetry of behavior on variables in Y_l were not enforced, it would also be possible to distinguish distributions that are equivalent. Consider now a signature with constants c, d, and $\{n, n' \mid n \in \mathbb{N}_0\}$, unary operator f and rules $n \xrightarrow{n} \delta_n$, $n' \xrightarrow{n} \delta_n$, $c \xrightarrow{a} \pi$, and $d \xrightarrow{a} \pi'$with $\pi = \sum_{i \in \mathbb{N}_0} \frac{1}{2^{i+1}} \cdot \delta_n$ and $\pi' = \sum_{i \in \mathbb{N}_0} (\frac{1}{2^{i+2}} \cdot \delta_n + \frac{1}{2^{i+2}} \cdot \delta_{n'})$, and $\frac{x \xrightarrow{a} \mu \quad \{y_k \xrightarrow{k} \mu_k \mid k \in \mathbb{N}_0\} \quad \mu(\{y_k\}_{k \in \mathbb{N}_0}) \geq 1}{f(x) \xrightarrow{b} \mu}$. Notice that $c \sim d$; nonetheless, $f(c) \xrightarrow{b} \delta_c$ but $f(d) \not\xrightarrow{b}$ since $d \xrightarrow{a} \pi'$ but there is no way to match both n and n' to two different variables y_{k_1} and y_{k_2} (for all $n \in \mathbb{N}_0$), and hence $\pi'(\rho(\{y_k\}_{k \in \mathbb{N}_0})) = 0.5$ for any substitution ρ satisfying the positive premises. We finally mention that conditions 1 and 4 in Def. 11 are more technical and their justification only becomes apparent in the proof of Theorem 12.

The strategy of proof for the congruence theorem follows the lines of the proof of Theorem 4.14 in [12] though some considerable rework is needed to manipulate quantitative premises. Notice, however that we do not require well-foundedness.

Theorem 12. *Let P be a stratifiable PTSS in ntμfv/ntμxv format. Then $\sim$ is a congruence relation.*

5 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 and P^1, one wants to combine them in a new PTSS $P^0 \oplus P^1$, where we generally assume that P^0 is the original PTSS and P^1 is the extension. 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 $t \in T(\Sigma^0)$, the set of outgoing transitions defined by P^0 is exactly the same that those defined by $P^0 \oplus P^1$. In this case we say that $P^0 \oplus P^1$ is a *conservative extension* of P^0.

Definition 13. *Let $\Sigma^0 = (F^0, \mathsf{r}^0)$ and $\Sigma^1 = (F^1, \mathsf{r}^1)$ be two signatures s.t. $f \in F^0 \cap F^1 \Rightarrow \mathsf{r}^0(f) = \mathsf{r}^1(f)$. The* sum *of Σ^0 and Σ^1, notation $\Sigma^0 \oplus \Sigma^1$, is the new signature $(F^0 \cup F^1, \mathsf{r})$ where $\mathsf{r}(f) =$ if $f \in F^0$ then $\mathsf{r}^0(f)$ else $\mathsf{r}^1(f)$ for all $f \in F^0 \cup F^1$.*

Given two PTSS $P^0 = (\Sigma^0, A^0, R^0)$ and $P^1 = (\Sigma^1, A^1, R^1)$ s.t. $\Sigma = \Sigma^0 \oplus \Sigma^1$ is defined, the sum *of P^0 and P^1, notation $P^0 \oplus P^1$, is the PTSS $P^0 \oplus P^1 = (\Sigma^0 \oplus \Sigma^1, A^0 \cup A^1, R^0 \cup R^1)$. We say that $P^0 \oplus P^1$ is a* conservative extension *of P^0 and that P^1* can be added

conservatively *to* P^0 *if* $P^0 \oplus P^1$ *is stratifiable and for all* $t \in T(\Sigma^0)$, $a \in A^0 \cup A^1$ *and* $\mu \in \Delta(T(\Sigma^0 \cup \Sigma^1))$ *it holds* $t \xrightarrow{a} \mu \in \rightarrow_{P^0 \oplus P^1} \Leftrightarrow t \xrightarrow{a} \mu \in \rightarrow_{P^0}$

Basically, a rule is well-founded if there is no circular dependency of variables in its set of premises. We adapt the definition of well-founded from [13] to our setting. Besides, we also require that distribution variables in the premises appear always bound.

Let W be a set containing positive and quantitative literals. The *variable dependency graph* of W is a directed graph with (i) set of nodes $\bigcup\{Var(\psi) : \psi \in W\}$, and (ii) edges $\{\langle x, \mu\rangle : x \in Var(t), (t \xrightarrow{a} \mu) \in W\} \cup \{\langle \mu, x\rangle : x \in X, (\mu(X) \trianglerighteq p) \in W\}$. W is *well-founded* if any backward chain of edges in the variable dependency graph is finite and every distribution variable has a predecessor. A rule is *well-founded* if the set of all its premises is well-founded. A PTSS is *well-founded* if all its rules are well-founded. A rule r is called *pure* if it is well-founded and does not contain free variables. A PTSS P is called *pure* if all of its rules are pure.

Theorem 14 gives sufficient conditions to ensure that a PTSS can be extended conservatively and its similar to Theorem 4.8 in [10]. Theorem 15 gives sufficient conditions to ensure that the sum PTSS $P^0 \oplus P^1$ is stratifiable, knowing that the original PTSSs P^0 and P^1 are also stratifiable. Its proof follows closely that of Theorem 5.8 in [12].

Theorem 14. *Let* $P^0 = (\Sigma^0, A^0, R^0)$ *be a PTSS in pure nt*μ*fv/nt*μ*xv format and let* $P^1 = (\Sigma^1, A^1, R^1)$ *be a PTSS such that for all rule* $r \in R^1$ *with* $conc(r) = t \xrightarrow{a} \mu$, $t \notin \mathbb{T}(\Sigma_0)$. *Let* $P = P^0 \oplus P^1$ *be defined and stratifiable. Then* P^1 *can be added conservatively to* P^0.

Theorem 15. *Let* $\Sigma^0 = (F^0, \mathsf{r}^0)$ *and* $\Sigma^1 = (F^0, \mathsf{r}^1)$ *be two signatures with constants* $a^0 \in F^0$ *and* $a^1 \in F^1$, *such that* $\Sigma^0 \oplus \Sigma^1$ *is defined. Let* $P^0 = (\Sigma^0, A^0, R^0)$ *and* $P^1 = (\Sigma^1, A^1, R^1)$ *be two stratifiable PTSS. If for all substitutions* ρ_0 *and* ρ_1 *and rules* $r_0 \in R^0$ *and* $r_1 \in R^1$, *it holds that* $\rho_0(\psi) \neq \rho_1(\phi)$ *with* $\phi = conc(r_1)$ *and* $\psi \in pprem(r_0)$ *or* $\psi = t \xrightarrow{a} \mu$ *with* $t \xrightarrow{a} \not\rightarrow \in nprem(r_0)$, *then* $P^0 \oplus P^1$ *is also stratifiable.*

6 Tracing Bisimulation

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 the trace congruence induced by the *nt*μ*fv/nt*μ*xv* format is exactly a "finitary" version of the bisimulation equivalence. This relation, which we called *bounded bisimilarity*, agrees with $\sim$ on image finite probabilistic transition systems. ($\rightarrow_P$ is image-finite iff for all $t \in T(\Sigma)$ and $a \in A$, the set $\{\mu \mid t \xrightarrow{a}_P \mu\}$ is finite.)

Definition 16. *Let* $P = (\Sigma, A, R)$ *be a stratifiable PTSS with associated relation* $\rightarrow_P$. *Given* $t \in T(\Sigma)$, *a sequence* $a_1 \dots a_n \in A^*$ *is a trace from t iff there are terms* $t_0, \dots, t_n \in T(\Sigma)$ *and distributions* $\pi_1, \dots, \pi_n$ *s.t.* $t_0 = t$, $t_i \xrightarrow{a_{i+1}} \pi_{i+1}$ *and* $\pi_{i+1}(t_{i+1}) > 0$ *for* $0 \leq i < n$. *Let* $\mathsf{Tr}(t)$ *be the set of all traces from t. Two terms* $t, t' \in T(\Sigma)$ *are* trace equivalent with respect to P, *notation* $t \equiv_P^T t'$, *iff* $\mathsf{Tr}(t) = \mathsf{Tr}(t')$.

We say that $C[x_1, \dots, x_n]$ is a *context* if $C[x_1, \dots, x_n]$ is an open term in which at most the distinct variables $x_1, \dots, x_n$ appear. As usual, $C[t_1, \dots, t_n]$ denotes the term obtained by replacing all occurrences of variables x_i by t_i.

Definition 17. *Let $P = (\Sigma, A, R)$ be a stratifiable PTSS in ntμfv/ntμxv format. Two terms $t, t' \in T(\Sigma)$ are* trace congruent with respect to *ntμfv/ntμxv, notation $t \equiv^{T}_{ntμfv/ntμxv} t'$, iff for all PTSS $P' = (\Sigma', A', R')$ in ntμfv/ntμxv format which can be added conservatively to P and for every context $C[x]$ it holds that $C[t] \equiv^{T}_{P \oplus P'} C[t']$.*

Let $P = (\Sigma, A, R)$ be a stratifiable PTSS with associated relation $\rightarrow_P$. The relations $\simeq^n_P \subseteq T(\Sigma) \times T(\Sigma)$ for $n \in \mathbb{N}$ are inductively defined by:

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

Given $t, t' \in T(\Sigma)$, t and t' are *n-bounded bisimilar* iff $t \simeq^n_P t'$. We say that t and t' are *bounded bisimilar*, notation $t \simeq_P t'$, if $t \simeq^n_P t'$ for all $n \in \mathbb{N}$.

Bounded bisimilarity and bisimulation equivalence agree on image-finite probabilistic transition systems [5, Lemma 3.5.8]. That is, if $\rightarrow_P$ 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 introduce contexts that are able to distinguish non-bisimilar terms. More precisely, P_T introduces two family of functions, binary functions B_n, $(k+1)$-ary functions Pr^k_n $(n, k \in \mathbb{N})$, and a trivial constant $\perp$. Their intended meaning is as follows. $\mathsf{B}_n(t,u)$ can detect whether t and u are n-bounded bisimilar by showing transition $\mathsf{B}_n(t,u) \xrightarrow{yes} \delta_\perp$. Otherwise, $\mathsf{B}_n(t,u) \xrightarrow{no} \delta_\perp$. 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^k_n is used as an auxiliary operator to test the measures of k (not necessarily different) $(n-1)$-bounded bisimulation equivalence classes. More precisely, $\mathsf{Pr}^k_n(t, u_1, \cdots, u_k) \xrightarrow{(a,q_1,\ldots,q_k)} \delta_\perp$ if there is a transition $t \xrightarrow{a} \pi$ such that $\pi([u_1]_{\simeq^{n-1}}) \geq q_1, \ldots, \pi([u_k]_{\simeq^{n-1}}) \geq q_k$, where $q_1, \ldots, q_k$ are some rational numbers.

Definition 18. *Let $P = (\Sigma, A, R)$ be a PTSS. The* bisimulation tester of *P is a PTSS $P_T = (\Sigma_T, A_T, R_T)$ where $\Sigma \subseteq \Sigma_T$ and Σ_T contains binary functions B_n and functions Pr^k_n with arity $k+1$, $n \in \mathbb{N}$ and a constant $\perp$, $A_T = A \cup (\bigcup_{i>0}(A \times \mathbb{Q}^i)) \cup \{yes, no\}$, and R contains the following rules (for all $n, k > 0$, $a \in A$ and $q \in \mathbb{Q}$):*

$$(1)\ \mathsf{B}_0(x,y) \xrightarrow{yes} \delta_\perp \qquad \frac{\mathsf{Pr}^k_n(x, z_1, \ldots, z_k) \xrightarrow{(a,q_1,\ldots,q_k)} \mu \quad \mathsf{Pr}^k_n(y, z_1, \ldots, z_k) \xrightarrow{(a,q_1,\ldots,q_k)} \not\rightarrow}{\mathsf{B}_n(x,y) \xrightarrow{no} \delta_\perp} \quad (3)$$

$$(2)\ \frac{x \xrightarrow{a} \mu \quad \{\mathsf{B}_{n-1}(z_i, Z_i) \xrightarrow{yes} \mu_i,\ \mu(Z_i) \geq q_i\}^k_{i=1}}{\mathsf{Pr}^k_n(x, z_1, \ldots, z_k) \xrightarrow{(a,q_1,\ldots,q_k)} \delta_\perp} \qquad \frac{\mathsf{B}_n(x,y) \xrightarrow{no} \not\rightarrow \quad \mathsf{B}_n(y,x) \xrightarrow{no} \not\rightarrow}{\mathsf{B}_n(x,y) \xrightarrow{yes} \delta_\perp} \quad (4)$$

The idea behind functions Pr^k_n explained above becomes apparent in rule (2). Besides, notice that distinction between two non n-bounded bisimilar terms is revealed by rule (3) where the negative premise indicates that it is is not able to find an a-transition for 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 is able to do it for x.

Observe that P_T is in *ntμfv* format but is *not* pure. Though this is not necessary, it is quite convenient in our case: the non-pure rule (3) 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 fact that P_T is not pure is not a problem to ensure that it extends conservatively a given PTSS in a well behaved manner using Theorems 14 and 15.

It is not too difficult to find a stratification for P_T (it can be obtained in a similar manner to [12, Lemma 6.8]). The following lemma is the core of Theorem 20 below.

Lemma 19. *Let $P = (\Sigma, A, R)$ be a stratifiable PTSS in pure ntμfv/ntμxv format containing at least one constant in its signature. Moreover, yes, no $\notin A$ and Σ does not contain function names B_n and Pr^k_n for all $n, k \in \mathbb{N}$. Then, $\mathsf{B}_n(t,t') \xrightarrow{yes} \delta_\perp \in \rightarrow_{P \oplus P_T} \Leftrightarrow t \simeq^n_P t'$, for all $t, t' \in T(\Sigma)$.*

Theorem 20 states that bisimulation equivalence is *fully abstract* with respect to the *ntμfv/ntμxv* format and trace equivalence. That is, it states that bisimulation equivalence is the coarsest congruence with respect to any operator whose semantics is defined through *ntμfv/ntμxv* rules and that is included in trace equivalence. Its proof is a direct consequence of Theorem 12, Lemma 19 and [5, Lemma 3.5.8].

Theorem 20. *Let $P = (\Sigma, A, R)$ be a stratifiable PTSS in pure ntμfv/ntμxv format containing at least one constant in Σ. Moreover, $\rightarrow_P$ is image-finite, yes, no $\notin A$ and Σ does not contain function names B_n and Pr^k_n for all $n, k \in \mathbb{N}$. Then, for all $t, t' \in T(\Sigma)$, $t \equiv^T_{ntμfv/ntμxv} t' \Leftrightarrow t \simeq_P t' \Leftrightarrow t \sim t'$*

7 Concluding Remarks

Related Work. SOS for probabilistic systems have received relatively little attention. To our knowledge, only [6, 7, 16, 17] study rule formats to specify probabilistic transition systems, and in [7, 15] they are embedded in general bialgebraic frameworks.

Both RTSS format [17] and PGSOS format [6, 7] 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 (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 [8] in the sense that premises are of the form $x_i \xrightarrow{a_i,q_i} y_i$ or $x_i \xrightarrow{b_i} \not\rightarrow$ where each x_i is a variable appearing on the term $f(\vec{x})$ 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. We remark that both RTSS and PGSOS formats can be encoded in the *ntμfv/ntμxv* format. Segala-GSOS format [7] allows for rules like in eq. (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. Clearly this format can also be encoded in the *ntμfv/ntμxv* format.

Bialgebras present an abstract categorical framework to study structured operational semantics and, in this setting, general congruence theorems have been presented [15, 23]. They introduce the so called *abstract GSOS* and *abstract safe ntree* [15, 23]. In fact, Segala-GSOS is derived as an instance of abstract GSOS [7]. In a recent and yet unpublished work, we showed that the *ntμfv/ntμxv* format reduces to a form of *probabilistic ntree* format, just like the *ntyft/ntyxt* format reduces to *ntree* format [11]. As in the

non-probabilistic case, negative premises are not reducible to the form $x \stackrel{a}{\not\rightarrow}$ and retain the form $t \stackrel{a}{\not\rightarrow}$ with t being an arbitrary term. Precisely because of this, our format (like the *ntyft/ntyxt* format) cannot be instanced as an abstract safe ntree. Moreover, it is also not fully clear to us how to encode quantitative premises in the bialgebraic framework.

Notice that none of the previously mentioned formats can encode the bisimulation tester of Def. 18 since it needs lookahead, negative premises of the form $f(\vec{x}) \stackrel{a}{\not\rightarrow}$, and quantitative premises testing against any possible probability value and 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. However, related to this result, we should remark that testers for bisimulation of *deterministic* probabilistic transition systems were already introduced in [18].

We also remark that the *ntμfv/ntμxv* format should be considered as a probabilistic extension of the *tyft/tyxt* and *ntyft/ntyxt* formats [12, 13]. These formats can be encoded in *ntμfv/ntμxv* format if non-probabilistic transitions $t \stackrel{a}{\longrightarrow} t'$ are considered as a probabilistic transition in the usual way, i.e., as $t \stackrel{a}{\longrightarrow} \delta_{t'}$. Finally, we observe that there is a rule format for generative probabilistic systems [16, 17] which is not covered by our format since it is very different in nature to the model we use.

Conclusion. In this article we have introduced PTSSs and the *ntμfv/ntμxv* format for rules that specify probabilistic transition systems. 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. We have also presented several standard theorems that ensure definability and uniqueness of models and conservative extensions, among others.

We highlight the introduction of our quantitative premises which, in combination with lookahead, permits the constructions of powerful operators. An example is the tester of Def. 18. Another one, more interesting, is a deadlock measuring operator dk where $\mathsf{dk}(t) \stackrel{q}{\longrightarrow} \nu$ iff t reaches a deadlock state with probability larger or equal to q in any possible resolution of nondeterminism. The rules are as follows

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

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

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 [3] 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 $c \stackrel{a}{\longrightarrow} (0.5 \cdot \delta_c + 0.5 \cdot \delta_{\perp})$, $c \stackrel{a}{\longrightarrow} (0.5 \cdot \delta_c)$, and $d \stackrel{a}{\longrightarrow} (0.5 \cdot \delta_c + 0.5 \cdot \delta_{\perp})$.

Acknowledgement. We would like to thank the anonymous referees whose suggestions let us improve the presentation of our paper.

References

1. Aceto, L., Fokkink, W., Verhoef, C.: Conservative extension in structural operational semantics. In: Current Trends in Theor. Comput. Sci., pp. 504–524. World Scientific (2001)
2. Aceto, L., Fokkink, W., Verhoef, C.: Structural operational semantics. In: Handbook of Process Algebra, pp. 197–292. Elsevier (2001)
3. Baeten, J.C.M., Bergstra, J.A.: Process Algebra with a Zero Object. In: Baeten, J.C.M., Klop, J.W. (eds.) CONCUR 1990. LNCS, vol. 458, pp. 83–98. Springer, Heidelberg (1990)
4. Baeten, J.C.M., Bergstra, J.A., Smolka, S.A.: Axiomatizing probabilistic processes: ACP with generative probabilities. Inf. Comput. 121(2), 234–255 (1995)
5. Baier, C.: On Algorithmics Verification Methods for Probabilistic Systems. Habilitation thesis, University of Mannheim (1999)
6. Bartels, F.: GSOS for probabilistic transition systems. Electr. Notes Theor. Comput. Sci. 65(1) (2002)
7. Bartels, F.: On Generalised Coinduction and Probabilistic Specification Formats. PhD thesis, Vrije Universiteit (2004)
8. Bloom, B., Istrail, S., Meyer, A.R.: Bisimulation can't be traced. J. ACM 42(1), 232–268 (1995)
9. Bol, R., Groote, J.F.: The meaning of negative premises in transition system specifications. J. ACM 43(5), 863–914 (1996)
10. D'Argenio, P.R., Verhoef, C.: A general conservative extension theorem in process algebras with inequalities. Theor. Comput. Sci. 177(2), 351–380 (1997)
11. Fokkink, W., van Glabbeek, R.J.: Ntyft/ntyxt rules reduce to ntree rules. Inf. Comput. 126(1) (1996)
12. Groote, J.F.: Transition system specifications with negative premises. Theor. Comput. Sci. 118(2), 263–299 (1993)
13. Groote, J.F., Vaandrager, F.: Structured operational semantics and bisimulation as a congruence. Inf. Comput. 100(2), 202–260 (1992)
14. Jonsson, B., Larsen, K.G., Yi, W.: Probabilistic extensions of process algebras. In: Handbook of Process Algebra, pp. 685–710. Elsevier (2001)
15. Klin, B.: Bialgebras for structural operational semantics: An introduction. Theor. Comput. Sci. 412(38), 5043–5069 (2011)
16. Lanotte, R., Tini, S.: Probabilistic Congruence for Semistochastic Generative Processes. In: Sassone, V. (ed.) FOSSACS 2005. LNCS, vol. 3441, pp. 63–78. Springer, Heidelberg (2005)
17. Lanotte, R., Tini, S.: Probabilistic bisimulation as a congruence. ACM Trans. Comput. Log. 10(2) (2009)
18. Larsen, K.G., Skou, A.: Bisimulation through probabilistic testing. Inf. Comput. 94(1), 1–28 (1991)
19. Milner, R.: Communication and Concurrency. Prentice-Hall, Inc. (1989)
20. Mousavi, M.R., Reniers, M.A., Groote, J.F.: SOS formats and meta-theory: 20 years after. Theor. Comput. Sci. 373(3), 238–272 (2007)
21. Plotkin, G.: A structural approach to operational semantics. Report DAIMI FN-19, Aarhus University (1981); reprinted in J. Log. Algebr. Program. 60-61, 17–139 (2004)
22. Segala, R.: Modeling and Verification of Randomized Distributed Real-Time Systems. PhD thesis. MIT (1995)
23. Turi, D., Plotkin, G.D.: Towards a mathematical operational semantics. In: LICS, pp. 280–291 (1997)
24. van Glabbeek, R.J.: The meaning of negative premises in transition system specifications II. J. Log. Algebr. Program. 60-61, 229–258 (2004)
25. van Glabbeek, R.J., Smolka, S.A., Steffen, B.: Reactive, generative and stratified models of probabilistic processes. Inf. Comput. 121(1), 59–80 (1995)