

Rooted branching bisimulation as a congruence for probabilistic transition systems

Matias D. Lee*

FaMAF, UNC-CONICET
Córdoba, Argentina
lee@famaf.unc.edu.ar

Erik P. de Vink

TU/e, Eindhoven, The Netherlands
CWI, Amsterdam, The Netherlands
evink@win.tue.nl

We propose a probabilistic transition system specification format, referred to as *probabilistic RBB safe*, for which rooted branching bisimulation is a congruence. The congruence theorem is based on the approach of Fokkink for the qualitative case. For this to work, the theory of transition system specifications in the setting of labeled transition systems needs to be extended to deal with probability distributions, both syntactically and semantically. We provide a scheduler-free characterization of probabilistic branching bisimulation as adapted from work of Andova et al. for the alternating model. Counter examples are given to justify the various conditions required by the format.

1 Introduction

Structural operational semantics is a standard methodology to provide a semantics to programming languages and process algebras [2]. In this setting, a signature Σ , a set of actions \mathcal{A} and a set of rules \mathcal{R} define a transition system specification (TSS). The signature is used to define the terms of the language $T(\Sigma)$. The interpretation of each term is given by a labeled transition system where the states range over $T(\Sigma)$, the labels over \mathcal{A} and the transitions are governed by the set of rules \mathcal{R} . This technique has been widely studied in the context of qualitative process algebras, see [27] for an overview. A particular topic of interest is the study of rule formats for which a behavioral equivalence is guaranteed to be a congruence. This property, crucial for a compositional analysis, ensures that pairwise equivalent terms t_1, \dots, t_n and t'_1, \dots, t'_n give rise to the equivalence of the terms $f(t_1, \dots, t_n)$ and $f(t'_1, \dots, t'_n)$,

Much work has been done on formats for labeled transition systems, i.e. in a qualitative setting. Although the main focus is on strong bisimulation [19, 13, 2], weaker notions that support abstraction from internal behavior has been studied as well. In [6], Bloom introduced formats covering weak bisimulation, rooted weak bisimulation, branching bisimulation and rooted branching bisimulation. In [17] these results are extended for η -bisimulation and delay bisimulations. In addition, in [14], a more liberal format is introduced for rooted branching bisimulation, called RBB safe.

Going into the other direction, addition of quantitative information, e.g. the inclusion of probabilities, allows to model systems in more detail. The aim to include these features motivated further extension of the theory of structured operational semantics. In the context of probabilistic process algebras previous results in the qualitative setting have been extended to deal with quantitative decorations. Based on the category-theoretical framework of Turi and Plotkin [5] proposes *probabilistic GSOS*. In turn, this has been generalized in [22, 23] yielding *weighted GSOS*. For generative systems [24] introduces *GTTS*, a format allowing features like look-ahead. The format *ntyft/ntyxt* is translated to the probabilistic setting in [11], while generation of axiomatizations [1, 4] for probabilistic GSOS is reported in [10]. In [26] so-called *weight-function SOS* is proposed for *ULTraS*, a generalization of probabilistic transition systems.

*Supported by 2010–2401/001–001–EMA2 and EU 7FP grant agreement 295261 (MEALS) and SECyT–UNC.

The bottom line for all these works is that strong bisimulation is a congruence for probabilistic transition systems.

So far, no congruence format is given dealing with both additional aspects, i.e. taking quantitative information into account, and, at the same time, catering for a weak notion of bisimulation. To the best of our knowledge, this paper presents the first specification format for the quantitative setting that respects a weak equivalence, viz. branching bisimulation. Our work follows the approach initiated in [11, 25] to define probabilistic transition systems specifications (*PTSS*). A *PTSS* is composed of a two-sorted signature (Σ_s, Σ_d) , a set of actions \mathcal{A} that contains the internal action τ , and a set of rules \mathcal{R} . The signature Σ_s is used to represent states, while Σ_d is used to represent distributions over states. Transitions have the shape $t \xrightarrow{a} \theta$ with the following intended meaning: state t can execute an action a and the next state is selected using the state distribution $\llbracket \theta \rrbracket$. Thus, the interpretation of the distribution term θ is a probability distribution over states. Note, this framework allows for non-determinism: if $t \xrightarrow{a} \theta$ and $t \xrightarrow{a} \theta'$ we do not require $\theta = \theta'$. Hence, a *PTSS* defines systems similar to Segala's probabilistic automata [28]. In order to prove that branching bisimulation is a congruence, we follow the ideas presented in [14]. For that reason, we call our specification format the *probabilistic RBB safe* format, referring to the RBB safe format proposed by Fokkink. Often, working with probabilistic automata where non-determinism and probabilities coexist, requires the introduction of schedulers to determine the probability of a particular execution [29, 12]. A key point for our proof of the main result is a characterization of branching bisimulation without schedulers. This characterization was introduced for the alternating model in [3], and we have adapted it to our context.

In Section 2, two-sorted signatures and distributions over states are introduced. Section 3 introduces probabilistic transition system specifications. Section 4 discusses schedulers, weak transitions, probabilistic branching bisimulation and branching bisimulation. The second relation is a restricted version of the former. The format that we present deals with branching bisimulation. In Section 5, the probabilistic RBB safe specification format is presented. We furthermore touch upon some intricacies of it and give the congruence theorem. In Section 6 some conclusions are drawn and future lines of research are indicated.

2 Preliminaries

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

An S -sorted signature is a structure (Σ, ar) , where (i) Σ is a set of function names, and (ii) $ar: \Sigma \rightarrow S^* \times S$ is the arity function. The rank of $f \in \Sigma$ is the number of arguments of f , i.e. $rk(f) = n$ if $ar(f) = \sigma_1 \cdots \sigma_n \rightarrow \sigma$. We write $\sigma_1 \cdots \sigma_n \rightarrow \sigma$ instead of $(\sigma_1 \cdots \sigma_n, \sigma)$ to highlight that function f maps to sort σ . Function f is a constant if $rk(f) = 0$. To simplify the presentation we will write an S -sorted signature Σ as a pair of disjoint signatures (Σ_s, Σ_d) where Σ_s is the set of operations that map to sort s , and Σ_d is the set of operations that map to sort d .

Let \mathcal{V} and \mathcal{D} be two infinite sets of S -sorted variables, for states and distributions, respectively, where \mathcal{V} , \mathcal{D} , and Σ are all mutually disjoint. We use x, y, z (with possible decorations, subscripts or superscripts) 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 $V \subseteq \mathcal{V}$ and $D \subseteq \mathcal{D}$. We define the sets of state terms $T(\Sigma_s, V, D)$ and distribution terms $T(\Sigma_d, V, D)$ as the smallest sets of terms satisfying

- (i) $V \subseteq T(\Sigma_s, V, D)$, and $D \subseteq T(\Sigma_d, V, D)$;

(ii) $f(\xi_1, \dots, \xi_{rk(f)}) \in T(\Sigma_\sigma, \mathcal{V}, \mathcal{D})$ if $ar(f) = \sigma_1 \cdots \sigma_n \rightarrow \sigma$ and $\xi_i \in T(\Sigma_{\sigma_i}, \mathcal{V}, \mathcal{D})$.

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 ξ, ξ', ξ_1, \dots range over any kind of terms. We use $var(\xi) \subseteq \mathcal{V} \cup \mathcal{D}$ to denote the set of variables occurring in term ξ .

Let $\Delta(T(\Sigma_s))$ denote the set of all (discrete) probability distributions over $T(\Sigma_s)$. 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 (finite) 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 are of a particular form, to which we refer to as ‘‘probabilistic lifted signature’’. We start from a signature Σ_s of functions mapping into sort s and construct the signature Σ_d of functions mapping into d as follows. For each $f \in \Sigma_s$ we include a function symbol $\mathbf{f} \in \Sigma_d$ with $ar(\mathbf{f}) = d \cdots d \rightarrow d$ and $rk(\mathbf{f}) = rk(f)$. We call \mathbf{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 $ar(\delta) = s \rightarrow d$ and
- $\bigoplus_{i \in I} [p_i]_{_}$ of arity $ar(\bigoplus_{i \in I} [p_i]_{_}) = d^{|I|} \rightarrow d$ for index set I , $p_i \in (0, 1]$ for $i \in I$, $\sum_{i \in I} p_i = 1$.

In particular, we write $\theta_1 \oplus_{p_1} \theta_2$ instead of $\bigoplus_{i \in \{1, 2\}} [p_i] \theta_i$ when the index set I has exactly two elements.

The operators δ and $\bigoplus_{i \in I} [p_i]_{_}$ are used to construct discrete probability functions of finite support: $\delta(t)$ is interpreted as the Dirac distribution for 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 \mathbf{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 following interpretation:

- $\llbracket \delta(t) \rrbracket = \delta_t$ for all $t \in T(\Sigma_d)$
- $\llbracket \bigoplus_{i \in I} [p_i] \theta_i \rrbracket = \sum_{i \in I} p_i \llbracket \theta_i \rrbracket$ for $\{\theta_i \mid i \in I\} \subseteq T(\Sigma_d)$
- $\llbracket \mathbf{f}(\theta_1, \dots, \theta_{rk(f)}) \rrbracket (g(\xi_1, \dots, \xi_{rk(g)})) = \begin{cases} \prod_{\sigma_j = s} \llbracket \theta_j \rrbracket (\xi_j) & \text{if } f \equiv g \text{ and for all } j: \sigma_j = d \Rightarrow \xi_j = \theta_j \\ 0 & \text{otherwise} \end{cases}$

In the above definition we assume that $\prod \emptyset = 1$. Notice that in the semantics of a lifted function \mathbf{f} , the product at the right-hand side 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 the parameters of \mathbf{f} .

A substitution ρ is a map $\mathcal{V} \cup \mathcal{D} \rightarrow \mathbb{T}(\Sigma)$ 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.

Example 2. To set the context of our running example we introduce the following signature. We assume a set \mathcal{A} of action labels, and distinguish $\tau \in \mathcal{A}$. Let $\Sigma = (\Sigma_s, \Sigma_d)$ be a probabilistically lifted signature where Σ_s contains: (i) constants 0 (inaction or the stop process) of sort s , i.e., $ar(0) = s$; (ii) a family

of unary probabilistic prefix operators $a._$ for $a \in \mathcal{A}$ with $\text{ar}(a) = d \rightarrow s$; (iii) and a binary operator $+$ (alternative composition or sum) with $\text{ar}(+) = ss \rightarrow s$. Moreover, Σ_d contains δ , all binary operators \oplus_p , and the lifted operators, which are as follows: (iv) the constant $\mathbf{0}$ with $\text{ar}(\mathbf{0}) = d$; (v) the family of unary operators $\mathbf{a}._$ for $a \in \mathcal{A}$ with $\text{ar}(\mathbf{a}) = d \rightarrow d$; (vi) the binary operator $\mathbf{+}$ with $\text{ar}(\mathbf{+}) = dd \rightarrow d$.

The intended meaning of the probabilistic prefix operator $a.\theta$ is that this term can perform action a and move to a term t with probability $\llbracket \theta \rrbracket(t)$. The stop process $\mathbf{0}$ and alternative composition $+$ have their usual meaning.

3 Probabilistic Transition System Specifications

In our setting, a probabilistic transition relation prescribes what possible activity can be performed by a term in a signature. Such activity is described by an action and a probability distribution on terms that indicates the probability to reach a particular new term. Our definition is along the lines of probabilistic automata [28].

Definition 3 (PTS). A probabilistic labeled transition system (PTS) is a triple $A = (T(\Sigma_s), \mathcal{A}, \rightarrow)$, where $\Sigma = (\Sigma_s, \Sigma_d)$ is a probabilistically lifted signature, \mathcal{A} is a set of actions, and $\rightarrow \subseteq T(\Sigma_s) \times \mathcal{A} \times \Delta(T(\Sigma_s))$ is a transition relation.

We build on [19, 18, 8] for our definition of a probabilistic transition system specification.

Definition 4 (PTSS). A probabilistic transition system specification (PTSS) is a triple $P = (\Sigma, \mathcal{A}, \mathcal{R})$ where Σ is a probabilistically lifted signature, \mathcal{A} is a set of labels, and \mathcal{R} is a set of rules of the form:

$$\frac{\{ t_k \xrightarrow{a_k} \theta_k \mid k \in K \} \cup \{ t_\ell \xrightarrow{b_\ell} \theta_\ell \mid \ell \in L \}}{t \xrightarrow{a} \theta}$$

where K, L are index sets, $t, t_k, t_\ell \in \mathbb{T}(\Sigma_s)$, $a, a_k, b_\ell \in \mathcal{A}$, and $\theta_k, \theta_\ell \in \mathbb{T}(\Sigma_d)$.

Expressions of the form $t \xrightarrow{a} \theta$ and $t \xrightarrow{a}$ are called *positive literals* and *negative literals*, respectively. For any rule $r \in \mathcal{R}$, literals above the line are called *premises*, notation $\text{prem}(r)$; the literal below the line is called the *conclusion*, notation $\text{conc}(r)$. 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: $\rho(t \xrightarrow{a} \theta) = \rho(t) \xrightarrow{a} \rho(\theta)$ and $\rho(t \xrightarrow{a}) = \rho(t) \xrightarrow{a}$. We say that r' is a (closed) instance of a rule r if there is a (closed) substitution ρ such that $r' = \rho(r)$.

For the sake of clarity, in the rest of the paper, we will deal with models as *symbolic* transition relations, i.e. subsets of $T(\Sigma_s) \times \mathcal{A} \times T(\Sigma_d)$ rather than *concrete* transition relations in $T(\Sigma_s) \times \mathcal{A} \times \Delta(T(\Sigma_s))$ required by a PTS. We will mostly refer with the term “transition relation” to a symbolic transition relation. In any case, a symbolic transition relation induces 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 $t \xrightarrow{a} \llbracket \theta \rrbracket$. 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 a model. As has been argued elsewhere (e.g. [18, 8, 16]), 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 $\frac{f \xrightarrow{b}}{f \xrightarrow{a} f}$ and $\frac{f \xrightarrow{a}}{f \xrightarrow{b} f}$, has two models that are justifiably compatible with the rules (so called supported models [7, 8, 16]), viz. $\{f \xrightarrow{a} \mathbf{f}\}$ and $\{f \xrightarrow{b} \mathbf{f}\}$.

An alternative view is to consider so-called *3-valued models*. A 3-valued model partitions the set $T(\Sigma_s) \times \mathcal{A} \times T(\Sigma_d)$ in three sets containing, respectively, the transitions 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 $\langle CT, PT \rangle$ of transition relations $CT, PT \subseteq T(\Sigma_s) \times \mathcal{A} \times T(\Sigma_d)$, with $CT \subseteq PT$, where CT is the set of transitions that *certainly* hold, and PT is the set of transitions that *possibly* hold. So, transitions in $PT \setminus CT$ are those whose validity is unknown and transitions in $(T(\Sigma_s) \times \mathcal{A} \times T(\Sigma_d)) \setminus PT$ are those that certainly do not hold. In view of the above, a 2-valued model satisfies $CT = PT$.

A 3-value model $\langle CT, PT \rangle$ 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 6. Before formally defining the notions of a proof and 3-valued stable model we introduce some notation. Given a transition relation $Tr \subseteq T(\Sigma_s) \times \mathcal{A} \times T(\Sigma_d)$, $t \xrightarrow{a} \theta$ holds in Tr , notation $Tr \models t \xrightarrow{a} \theta$, if $t \xrightarrow{a} \theta \in Tr$; $t \not\xrightarrow{a}$ holds in Tr , notation $Tr \models t \not\xrightarrow{a}$, if for all $\theta \in T(\Sigma_d)$, $t \xrightarrow{a} \theta \notin Tr$. Given a set of literals H , we write $Tr \models H$ if for all $\psi \in H$, $Tr \models \psi$.

Definition 5 (Proof). Let $P = (\Sigma, \mathcal{A}, \mathcal{R})$ 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) $\frac{K}{\chi}$ is a valid substitution instance of a rule from \mathcal{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 .

Above we stated that a 3-value stable model $\langle CT, PT \rangle$ for a PTSS P has to be *justifiably compatible* with the proof system defined by P . By ‘compatible’ we mean that $\langle CT, PT \rangle$ 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 6 (3-valued stable model). Let $P = (\Sigma, \mathcal{A}, \mathcal{R})$ be a PTSS. A tuple $\langle CT, PT \rangle$ with $CT \subseteq PT \subseteq T(\Sigma_s) \times \mathcal{A} \times T(\Sigma_d)$ is a 3-valued stable model for P if for every closed positive literal ψ it holds that

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

In fact, the least 3-valued stable model of a PTSS can be constructed using induction. We borrow this construction from [14, 15].

Lemma 7. Let P be a PTSS. For each ordinal α define the pair $\langle CT_\alpha, PT_\alpha \rangle$ as follows:

- $CT_0 = \emptyset$ and $PT_0 = T(\Sigma_s) \times \mathcal{A} \times T(\Sigma_d)$.
- For every non-limit ordinal $\alpha > 0$, define
$$CT_\alpha = \{ t \xrightarrow{a} \theta \mid \text{for some set } N \text{ of negative literals, } P \vdash \frac{N}{t \xrightarrow{a} \theta} \text{ and } PT_{\alpha-1} \models N \}$$

$$PT_\alpha = \{ t \xrightarrow{a} \theta \mid \text{for some set } N \text{ of negative literals, } P \vdash \frac{N}{t \xrightarrow{a} \theta} \text{ and } CT_{\alpha-1} \models N \}$$

- For every limit ordinal α , define $CT_\alpha = \bigcup_{\beta < \alpha} CT_\beta$ and $PT_\alpha = \bigcap_{\beta < \alpha} PT_\beta$.

Then it holds that

- If $\beta \leq \alpha$, $CT_\beta \subseteq CT_\alpha$ and $PT_\beta \supseteq PT_\alpha$, that is, $\langle CT_\beta, PT_\beta \rangle$ has at most as much information as $\langle CT_\alpha, PT_\alpha \rangle$.
- There is an ordinal λ such that $CT_\lambda = CT_{\lambda+1}$ and $PT_\lambda = PT_{\lambda+1}$. Moreover, $\langle CT_\lambda, PT_\lambda \rangle$ is the least 3-valued stable model for P .

This result is shown in [15, 14] for a non-probabilistic setting using a slightly different definition of 3-valued models. However, with minor changes the same proof applies to our setting as well. We note that the first item of the lemma can be proved using transfinite induction on the lexicographic order of the pair (α, β) . the second item follows from the Knaster-Tarski theorem. PTSS with a least 3-valued stable model that are also a 2-valued model are of particular interest, since such a model is actually the only 3-valued stable model [8, 16].

Definition 8. A PTSS P is said to be complete if its least 3-valued stable model $\langle CT, PT \rangle$ satisfies that $CT = PT$ i.e., the model is also 2-valued.

Now, we can associate a probabilistic transition system to a complete PTSS.

Definition 9. Let P be a complete PTSS and let $\langle Tr, Tr \rangle$ 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 $(T(\Sigma_s), \mathcal{A}, \rightarrow)$ such that $t \xrightarrow{a} \pi$ iff $t \xrightarrow{a} \theta \in Tr$ and $\llbracket \theta \rrbracket = \pi$ for some $\theta \in T(\Sigma_d)$.

Example 10. The rules for the process algebra of Example 2 are defined by

$$\frac{}{a.\mu \xrightarrow{a} \mu} \qquad \frac{x \xrightarrow{a} \mu}{x+y \xrightarrow{a} \mu} \qquad \frac{y \xrightarrow{a} \mu}{x+y \xrightarrow{a} \mu}$$

We use \tilde{P} for the PTSS defined by these rules.

4 Branching bisimulations for probabilistic transition systems

For a set X , we denote by $\Delta_{sub}(X)$ the set of discrete sub-probability distributions over X . Given $\pi \in \Delta_{sub}(X)$, we denote by $spt(\pi)$ its support $\{x \in X \mid \pi(x) > 0\}$, and by $\pi(\perp)$ the value $1 - \pi(X)$, for a distinguished symbol $\perp \notin X$. We use δ_\perp to represent the empty distribution, i.e. $\delta_\perp(X) = 0$.

An *execution fragment* of a PTS A is a finite or infinite alternating sequence of states and actions $\alpha = s_0 a_1 s_1 a_2 s_2 \dots$ such that $s_{i-1} \xrightarrow{a_i} \pi_i$ and $s_i \in spt(\pi_i)$, for each $i > 0$. We say, α is starting from $fst(\alpha) = s_0$, and in case the sequence is finite, ending in $lst(\alpha)$. Put $length(\alpha) = n$ if $\alpha = s_0 a_1 s_1 \dots a_n s_n$, and $length(\alpha) = \infty$ if α is infinite. We write $frags(A)$ for the set of execution fragments of A , and by $frags^*(A)$ the set of finite execution fragments of A . An execution fragment α is a prefix of an execution fragment α' , denoted by $\alpha \preceq \alpha'$, if the sequence α is a prefix of the sequence α' . The trace $trace(\alpha)$ of α is the subsequence of external actions of α . We use ε to denote the empty trace. Similarly, we define $trace(a) = a$, for $a \in \mathcal{A}$, and $trace(\tau) = \varepsilon$.

Given a state s , we write \vec{s} to denote the set of outgoing transitions of the state s . A *scheduler* for a PTS A is a function $\zeta : frags^*(A) \rightarrow \Delta_{sub}(\rightarrow)$ with $\zeta(\alpha) \in \Delta_{sub}(\overrightarrow{lst(\alpha)})$. A scheduler ζ is *deterministic* if for all $\alpha \in frags^*(A)$ $\zeta(\alpha)$ is either a Dirac distribution or the empty distribution. Note that by using sub-probability distributions, it is possible that with non-zero probability no transition is chosen after α ,

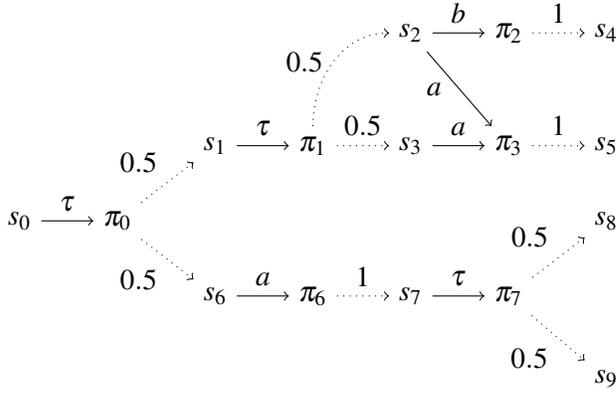
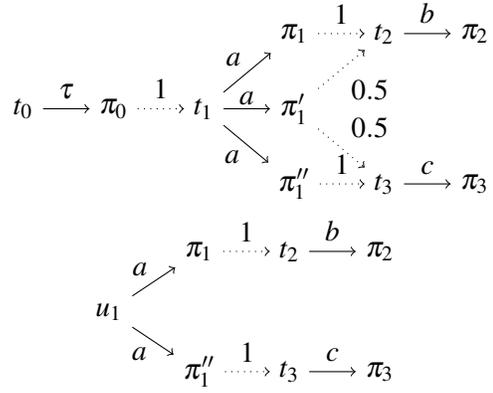


Figure 1: PTS of Example 12

Figure 2: $t_0 \approx_{pb} u_1$ but $t_0 \not\approx_b u_1$

that is, the computation stops with probability $\zeta(\alpha)(\perp)$. Given a scheduler ζ and a finite execution fragment α , the distribution $\zeta(\alpha)$ describes how transitions are chosen to move on from $lst(\alpha)$. A scheduler ζ and a state s induce a probability distribution $\pi_{\zeta,s}$ over execution fragments on measurable sets as generated by the cones of finite execution fragments. The cone C_α of a finite fragment α is the set $\{\alpha' \in frags(A) \mid \alpha \preceq \alpha'\}$. With respect to ζ and s , the probability $\pi_{\zeta,s}$ of the cone C_α is recursively defined by

$$\begin{aligned} \pi_{\zeta,s}(C_t) &= \delta_s(t) \\ \pi_{\zeta,s}(C_{\alpha a t}) &= \pi_{\zeta,s}(C_\alpha) \cdot \sum_{lst(\alpha) \xrightarrow{a} \pi} \zeta(\alpha)(lst(\alpha) \xrightarrow{a} \pi) \cdot \pi(t) \end{aligned}$$

Given a scheduler ζ , a state s and a finite execution fragment α , the *probability of executing α* based on ζ and s , notation $\pi_{\zeta,s}(\alpha)$, is defined as $\pi_{\zeta,s}(\alpha) = \pi_{\zeta,s}(C_\alpha) \cdot \zeta(\alpha)(\perp)$. We define the length of a scheduler ζ with respect to a state s by $length_s(\zeta) = \max\{length(\alpha) \mid fst(\alpha) = s, \zeta(\alpha) \neq \delta_\perp\}$. Given a scheduler ζ , we may define a truncation ζ_n by $\zeta_n(\alpha) = \zeta(\alpha)$ if $length(\alpha) \leq n$, otherwise $\zeta_n(\alpha) = \delta_\perp$.

We say that a state s can execute a weak transition for action $a \in \mathcal{A}$ if there is a scheduler ζ such that the action a is executed with probability 1. After a is executed, with probability $\pi_{\zeta,s}(\{\alpha \in frags^*(A) \mid lst(\alpha) = t\})$ the state t will be reached. If $a = \tau$, we have a similar definition but with probability 1 no visible action is executed.

Definition 11. Let A be a PTS with $s \in S$ and $a \in \Sigma \cup \{\varepsilon\}$. A transition $s \xrightarrow{a}_c \pi$ is called a weak combined transition if there exists a scheduler ζ such that the following holds for $\pi_{\zeta,s}$:

1. $\pi_{\zeta,s}(frags^*(A)) = 1$.
2. For each $\alpha \in frags^*(A)$, if $\pi_{\zeta,s}(\alpha) > 0$ then $trace(\alpha) = trace(a)$.
3. For each state t , $\pi_{\zeta,s}(\{\alpha \in frags^*(A) \mid lst(\alpha) = t\}) = \pi(t)$.

Occasionally we want to make reference to the scheduler ζ underlying a weak combined transition $s \xrightarrow{a}_c \pi$. We do so by writing $s \xrightarrow{a}_\zeta \pi$. If the scheduler is deterministic, we may write $s \xrightarrow{a} \pi$.

Example 12. The state s_0 in Figure 1, has the following weak combined transitions: (i) $s_0 \xrightarrow{\varepsilon} \delta_{s_0}$ (ii) $s_0 \xrightarrow{\varepsilon}_c \pi_{s_0}$ with $\pi_{s_0}(s_0) = \pi_{s_0}(s_2) = \pi_{s_0}(s_3) = 0.2$ and $\pi_{s_0}(s_6) = 0.4$ (iii) $s_0 \xrightarrow{a} \pi_a$ with $\pi_a(s_5) = \pi_a(s_7) = 0.5$ (iv) $s_0 \xrightarrow{a}_c \pi'_a$ with $\pi'_a(s_5) = 0.5$, $\pi'_a(s_7) = 0.2$ and $\pi'_a(s_8) = \pi_a(s_9) = 0.15$. Notice combined transitions in (i) and (iii) are defined using deterministic schedulers. There is no weak combined transition from s_0 with action b , since there is no scheduler that allows to execute b with probability 1.

Next, we generalize the notion of a weak combined transition to allow for a distribution of source states.

Definition 13. Let $A = (T(\Sigma_s), \mathcal{A}, \rightarrow)$ be a PTS, $\pi, \pi' \in \Delta_{sub}(S)$ sub-probability distributions, and $a \in \mathcal{A}$ an action. We say that $\pi \xrightarrow{a}_c \pi'$ is a weak combined hyper transition if there exists a family of weak combined transitions $\{s \xrightarrow{a}_c \pi_s\}_{s \in spt(\pi')}$ such that $\pi' = \sum_{s \in spt(\pi)} \pi(s) \cdot \pi_s$.

In the sequel we will consider weak combined transitions and weak combined hyper transitions consisting of transitions taken from a specific subset, the so-called *allowed* transitions. This leads to the notion of allowed transitions.

Definition 14. Choose, for a PTS $A = (T(\Sigma_s), \Sigma, \rightarrow)$, a subset of transitions $P \subseteq \rightarrow$. We say that $s \xrightarrow{a,P}_c \pi$ is an allowed weak combined transition from s to π respecting P , if there exists a scheduler ζ inducing a weak combined transition $s \xrightarrow{a}_c \mu$ such that, for each $\alpha \in frags^*(A)$, $spt(\zeta(\alpha)) \subseteq P$. Similarly, we say that $\pi \xrightarrow{a,P}_c \pi'$ is an allowed weak combined hyper transition from π to π' respecting P , if there exists a family of allowed weak combined transitions $\{s \xrightarrow{a,P}_c \pi_s\}_{s \in spt(\pi)}$ such that $\pi' = \sum_{s \in spt(\pi)} \pi(s) \cdot \pi_s$.

We write $s \xrightarrow{a}_c \pi$ if there is a scheduler ζ such that $length(\zeta) = 1$ and $s \xrightarrow{a}_\zeta \pi$. We write $\pi \xrightarrow{a}_c \pi'$ if $\pi \xrightarrow{a}_c \pi'$ with an associated family of transitions $\{s \xrightarrow{a}_c \pi_s\}_{s \in spt(\pi)}$. We employ similar notation for combined transitions with deterministic schedulers and allowed transitions.

The paper [12] proposes to consider in their study of weak probabilistic bisimulation the notion of an allowed transition (see Definition 14). The key idea is to consider transitions taken from a specific part of the transition system. We use the essence of this to distill the notions of *probabilistic branching bisimulation* and *branching bisimulation*.

Given a relation $\mathcal{B} \subseteq T(\Sigma_s) \times T(\Sigma_s)$, its lifting to $\Delta(T(\Sigma_s)) \times \Delta(T(\Sigma_s))$ is defined as follows: $\pi \mathcal{B} \pi'$ iff there is a weight function $w : (T(\Sigma_s) \times T(\Sigma_s)) \rightarrow [0, 1]$ 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 $t \mathcal{B} t'$. 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 \mathcal{B} is reflexive, symmetric and/or transitive if \mathcal{B} is. The overloading of \mathcal{B} should not raise confusion.

Definition 15. Let $A = (T(\Sigma_s), \mathcal{A}, \rightarrow)$ be a PTS, and let $\mathcal{B} \subseteq T(\Sigma_s) \times T(\Sigma_s)$ be a symmetric relation. A transition $s \xrightarrow{\tau} \pi$ is called branching preserving for \mathcal{B} if $\delta(s) \mathcal{B} \pi$. The relation \mathcal{B} on $T(\Sigma_s)$ is called a probabilistic branching bisimulation (resp. branching bisimulation) for A if, for a branching preserving set of transitions $P \subseteq \xrightarrow{\tau}$, it holds that $s \mathcal{B} t$ and $s \xrightarrow{a}_c \pi_s$ imply either

(i) $a = \tau$ and $s \xrightarrow{\tau} \pi_s \in P$, or

(ii) $t \xrightarrow{\tau,P}_c \tilde{\pi}_t$ with $\tilde{\pi}_t \xrightarrow{a}_c \pi_t$ (resp. $\tilde{\pi}_t \xrightarrow{a} \pi_t$) and $\pi_s \mathcal{B} \pi_t$, for all states $s, t \in T(\Sigma_s)$.

We write $s \approx_{pb} t$ (resp. $s \approx_b t$) if there exists a probabilistic branching bisimulation (resp. branching bisimulation) for A relating states s and t .

Example 16. In Figure 2 we can see the subtle difference between the relations \approx_{pb} and \approx_b . Comparing the transitions of t_1 with the transitions of u_1 , we have that the transition $t_1 \xrightarrow{a} [0.5]t_2 \oplus [0.5]t_3$ can be mimicked by u_1 with the transitions $u_1 \xrightarrow{\tau} \delta_{u_1}$ and $\delta_{u_1} \xrightarrow{a}_c [0.5]t_2 \oplus [0.5]t_3$. Therefore it is clear that $t_1 \approx_{pb} u_1$ and $t_0 \approx_{pb} u_1$. In this case, $t_0 \xrightarrow{\tau} \delta_{t_1}$ is branching preserving. On the other hand there is no transition $\delta_{u_1} \xrightarrow{a} [0.5]t_2 \oplus [0.5]t_3$, therefore $t_1 \not\approx_b u_1$ and $t_0 \not\approx_b u_1$.

In [3], a definition for branching bisimulation for the alternating model [20] is presented. Contrary to our definition above, it does not use the notion of schedulers. We explain the underlying intuition considering the PTS depicted in Figure 3. It is clear that states $T = \{t_1, \dots, t_4\}$ are branching bisimilar

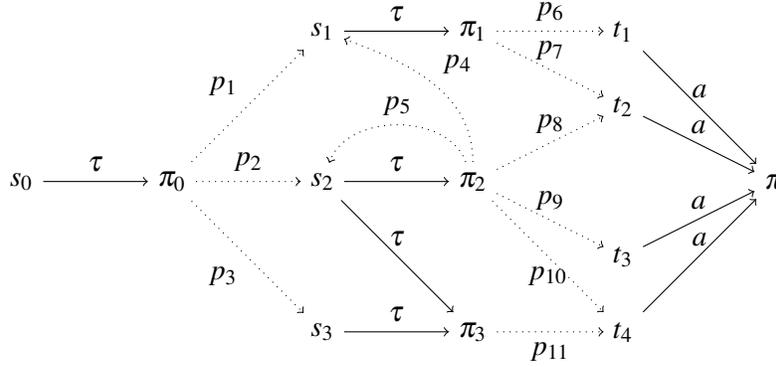


Figure 3: Schedulers are not needed to define branching bisimulation

and that all transitions labeled τ are branching preserving. Notice that for every scheduler ζ such that $s \xrightarrow{a}_{\zeta} \pi_{\zeta}$ we have $\pi_{\zeta} = \pi$. Thus, in this particular example, schedulers do not make any difference for the definition of a combined transition executing a . In general, it does not make any change choosing, with different probabilities, between branching preserving transitions until a visible action is executed, because the targets of two branching preserving transitions are, by definition, the same modulo branching bisimulation.

We adapt the definition of [3] for branching bisimulation without scheduler for alternating systems to the present setting. This new definition coincides with Definition 15. A *concrete* execution of a PTS A is a sequence $s_0 a_0 \pi_0 s_1 \dots \pi_{n-1} s_n a_n \pi_n$ such that $s_i \xrightarrow{a_i} \pi_i$ for $0 \leq i \leq n$ and $s_{j+1} \in \text{spt}(\pi_j)$ for $0 \leq j < n$.

Definition 17. A symmetric relation $\mathcal{B} \subseteq T(\Sigma_s) \times T(\Sigma_s)$ is called a branching bisimulation without scheduler for a PTS $A = (T(\Sigma_s), \mathcal{A}, \rightarrow)$ iff $s \mathcal{B} s'$ and $s \xrightarrow{a} \pi$ imply (i) $a = \tau$ and $\delta_s \mathcal{B} \pi$, or (ii) $a \in \Sigma$ and there is a concrete execution $s_0 \tau \pi_1 s_1 \tau \pi_2 s_2 \dots \pi_n s_n a \pi'$ such that $s' = s_0$, $s \mathcal{B} s_i$ for $0 \leq i \leq n$, $\delta_s \mathcal{B} \pi_j$ for $1 \leq j \leq n$ and $\pi \mathcal{B} \pi'$. We write $s \sim_b s'$ if a branching bisimulation without scheduler for A relates s and s' .

Thus, while the scheduler-based definition requires preservation of branching by the transitions that are combined, the scheduler-less definition requires branching bisimilarity of the intermediate states and distribution with the source state. In view of this, the next result does not come as a surprise.

Theorem 18. Let $A = (T(\Sigma_s), \mathcal{A}, \rightarrow)$ be a PTS. Then $s \approx_b t$ iff $s \sim_b t$, for all $s, t \in T(\Sigma_s)$. \square

It is well-known that typically branching bisimulation per se is not preserved by most process algebras [14, 9]. This is solved strengthening the requirements by means of the *rootedness condition*. In this way, we obtain a stronger notion, in our setting that of a rooted branching bisimulation.

Definition 19. A symmetric relation $R \subseteq T(\Sigma_s) \times T(\Sigma_s)$ is a rooted branching bisimulation with respect to a PTS $A = (T(\Sigma_s), \mathcal{A}, \rightarrow)$ if, for all $s, t \in T(\Sigma_s)$, $s R t$ and $s \xrightarrow{a} \theta_s$ imply $t \xrightarrow{a} \theta_t$ for some θ_t s.t. $\theta_s \approx_b \theta_t$.

5 The probabilistic RBB format

A congruence over an algebraic structure is an equivalence relation on the elements of the algebra compatible with its structure. Formally, a (sort-respecting) equivalence relation $\mathcal{C} \subseteq T(\Sigma) \times T(\Sigma)$ is a *congruence* if for all $f \in \Sigma$ and $\xi_i, \xi'_i \in T(\Sigma)$ with $\xi_i \mathcal{C} \xi'_i$ for all i , $1 \leq i \leq \text{rk}(f)$, it holds that $f(\xi_1, \dots, \xi_{\text{rk}(f)}) \mathcal{C} f(\xi'_1, \dots, \xi'_{\text{rk}(f)})$.

We next explain the restrictions needed by the format. Then we present the probabilistic RBB safe specification format. If a PTSS P satisfies this specification format then rooted branching bisimulation

is a congruence for all operator defined by P . Finally, we present the definitions and lemmas needed to prove the main result. Basically, we have extended the ideas from [14] to our setting.

Restrictions over the format. Consider, in the context of our running example, the terms $s = a.(b.0)$ and $t = a.(c.b.0)$. Note $s \approx_{rb} t$. The restrictions on the format discussed below are justified by the following examples.

Look-ahead is not allowed. The format presented in [11, 25] allows *quantitative premises*. These premises have the shape $\theta(Y) \triangleright p$ with $\theta \in \mathbb{T}(\Sigma_d)$, $Y \subseteq \mathcal{V}$, $\triangleright \in \{>, \geq\}$ and $p \in [0, 1]$. Given a closed substitution ρ , the closed premise $\rho(\theta(Y) \triangleright p)$ holds iff $\llbracket \rho(\theta) \rrbracket(\rho(Y)) \triangleright p$ holds. Without quantitative premises it is not possible to have look-ahead. Suppose that our rules (Definition 4) support this kind of premises, then we can add to \tilde{P} the operator f , $ar(f) = s \rightarrow s$, defined by

$$\frac{x \xrightarrow{a} \mu \quad \mu(\{y\}) > 0 \quad y \xrightarrow{b} v}{f(x) \xrightarrow{a} 0} \quad (1)$$

Then $f(s) \xrightarrow{a}$ and $f(t) \not\xrightarrow{a}$, therefore $f(s) \not\approx_{rb} f(t)$. The problem with look-ahead is the possibility for testing after an action is executed. The processes reached (with probability greater than zero) after the execution of the action may not be rooted branching bisimilar. To avoid this problem and simplify the presentation, the kind of rules that we are using does not support quantitative premises.

The following examples follow in essence the same idea: by combining operators with particular rules, it is possible to test, in some way, the target of a positive premise. In addition, we use the examples to motivate other ingredients of our format below.

Arbitrary testing of a positive premise target using other rules is not allowed. Add to \tilde{P} the operator f with $ar(f) = s \rightarrow s$, and operator g with $ar(g) = ss \rightarrow s$ defined by

$$\frac{x \xrightarrow{a} \mu}{f(x) \xrightarrow{a} g(\delta(x), \mu)} \quad \frac{x_2 \xrightarrow{b} \mu}{g(x_1, x_2) \xrightarrow{b} 0} \quad (2)$$

then $f(s) \not\approx_{rb} f(t)$. Notice, $f(s) \xrightarrow{a} g(\delta(s), b.0)$ and $g(s, b.0) \xrightarrow{b} 0$, while $f(t) \xrightarrow{a} g(\delta(t), c.b.0)$ and $g(t, c.b.0) \not\xrightarrow{b}$. Here, the target of the premise $x \xrightarrow{a} \mu$ of the first rule is tested, via instantiation of x_2 , in the second rule. When the target of a positive premise is used as an argument of the function in the target of the conclusion, we say that the position of the argument is *wild*. If the position is not wild, then it is *tame*. Here, the second argument of g is wild. To ‘control’ wild arguments, following [14], *patience rules* are introduced, see Definition 21. In this case, a patience rule for the second argument of g is defined by

$$\frac{x_2 \xrightarrow{\tau} \mu}{g(x_1, x_2) \xrightarrow{\tau} g(\delta(x_1), \mu)} \quad (3)$$

Taking into account this new rule we have that $f(s) \approx_b f(t)$.

However, the problem we have presented is more general. Add to \tilde{P} operator f with $ar(f) = s \rightarrow s$, operator g with $ar(g) = ss \rightarrow s$ and operator h with $ar(h) = s \rightarrow s$ defined by

$$\frac{x \xrightarrow{a} \mu}{f(x) \xrightarrow{a} h(g(\delta(x), \mu))} \quad \frac{x_2 \xrightarrow{b} \mu}{g(x_1, x_2) \xrightarrow{b} 0} \quad \frac{x_1 \xrightarrow{b} \mu}{h(x_1) \xrightarrow{b} 0} \quad (4)$$

Then $f(s) \not\approx_{rb} f(t)$. In the target of the conclusion of the first rule, the second argument of g is the target of a positive premise. In addition, this term is the argument of h . In this case, we have that the second argument of g and the argument of h are wild. Also here, terms $f(s)$ and $f(t)$ can become rooted branching bisimilar adding patience rules for the wild arguments. In the next section, Definition 20

formalizes the notion of a wild argument and Definition 22 is introduced to deal with their nesting.

Finally, we point out that the condition of being wild can be ‘*inherited*’. For example, take into account rules from (2) and (3). Recall, the second argument of g is wild and its patience rule is defined. Add a new operator h with $ar(h) = ss \rightarrow s$ and the following rules

$$\frac{}{g(x_1, x_2) \xrightarrow{a} \delta(h(x_2, x_1))} \quad \frac{x_1 \xrightarrow{b} \mu}{h(x_1, x_2) \xrightarrow{c} \mathbf{0}} \quad (5)$$

the first argument of h is wild because variable x_2 appears in that position and it also appears in a wild position of g . If we do not add a patience rule for the first argument of h we have $f(s) \not\approx_{rb} f(t)$.

Wild arguments cannot be used in the source of a premise unrestrictedly. Again, take into account rules from (2) and (3) and add either one of the following rules

$$\frac{x_2 \xrightarrow{b} \mu}{g(x_1, x_2) \xrightarrow{a} \mathbf{0}} \quad \frac{x_2 \xrightarrow{\tau} \mu}{g(x_1, x_2) \xrightarrow{a} \mathbf{0}} \quad (6)$$

In both cases we get $f(s) \not\approx_{rb} f(t)$. The first rule is an example that shows that a wild argument cannot appear as the source of a negative premise. The second rule shows that a wild argument cannot be used as the source of a positive premise with label τ . Both kind of restrictions will be present in the format.

The RBB format. Definition 20 introduces the *nesting graph*: an edge from $\langle f, i \rangle$ to $\langle g, j \rangle$ in the graph encodes that a variable appearing in the i -th argument of f , also appears in a term that is used as the j -th argument of g in the conclusion of a rule. This graph is used to define when a variable is wild.

Definition 20. (a) Let $P = (\Sigma, \mathcal{A}, \mathcal{R})$ be a PTSS. The nesting graph of the PTSS P is the directed graph $\mathcal{G}_P = (V, E)$ with

$$\begin{aligned} V &= \{ \langle f, i \rangle \mid f \in \Sigma_s, 1 \leq i \leq rk(f) \} \\ E &= \{ (\langle f, i \rangle, \langle g, j \rangle) \mid r \in \mathcal{R}, \text{conc}(r) = f(\dots, \zeta_i, \dots) \xrightarrow{a} C[g(\dots, \xi_{j-1}, C'[\zeta_i, \xi_{j+1}, \dots])] \} \cup \\ &\quad \{ (\langle f, i \rangle, \langle g, j \rangle) \mid r \in \mathcal{R}, \text{conc}(r) = f(\dots, \zeta_i, \dots) \xrightarrow{a} C[\mathbf{g}(\dots, \xi_{j-1}, C'[\zeta_i, \xi_{j+1}, \dots])] \} \end{aligned}$$

(b) Let P be a PTSS and $\mathcal{G}_P = (V, E)$ be its nesting graph. A node $\langle g, j \rangle \in V$ is called wild if

1. $t \xrightarrow{a} \mu \in \text{prem}(r)$ and $\text{tgt}(\text{conc}(r)) = C[g(\dots, \xi_{j-1}, C'[\mu, \xi_{j+1}, \dots])]$ for some $r \in \mathcal{R}$, or
2. $t \xrightarrow{a} \mu \in \text{prem}(r)$ and $\text{tgt}(\text{conc}(r)) = C[\mathbf{g}(\dots, \xi_{j-1}, C'[\mu, \xi_{j+1}, \dots])]$ for some $r \in \mathcal{R}$, or
3. $(\langle f, i \rangle, \langle g, j \rangle) \in E$ and $\langle f, i \rangle$ is wild.

The i -th argument of an operator f or \mathbf{f} is wild if $\langle f, i \rangle$ is wild, otherwise it is tame.

In the definition of a wild argument, items (b.1) and (b.2) deal with the case where the target of a positive premise μ is used in the target of the conclusion. Two cases are needed to deal with $g \in \Sigma_s$ and its lifting $\mathbf{g} \in \Sigma_d$. Notice that $g \in \Sigma_s$ can appear in a distribution term, particularly in the target of the conclusion, using the operator δ . The nesting of context allows to take into account all possible cases. Item (b.3) deals with the ‘inheritance’ mentioned above. Below, the definitions of *patience rules*, *w-nested contexts* and the *RBB safe specification format* are given. Later we explain how these are used to ensure that rooted branching bisimulation is a congruence.

Definition 21. Let $\zeta \in \mathcal{V} \cup \mathcal{D}$, define $\bar{\zeta} = \delta(\zeta)$ whenever ζ has sort s and $\bar{\zeta} = \zeta$, otherwise. The patience rule for the i -th argument (of sort s) of a function symbol $f \in \Sigma_s$ is the rule

$$\frac{x_i \xrightarrow{\tau} \mu}{f(\dots, \zeta_{i-1}, x_i, \zeta_{i+1}, \dots) \xrightarrow{\tau} \mathbf{f}(\dots, \bar{\zeta}_{i-1}, \mu, \bar{\zeta}_{i+1}, \dots)}$$

Definition 22. The set of w -nested contexts is defined inductively by

1. The empty context $[\]$ is w -nested.
2. The term $f(\dots, \xi_{i-1}, C[\], \xi_{i+1}, \dots)$ is w -nested if $C[\]$ is w -nested and the i -th argument of the function symbol f is wild.
3. The term $\delta(C[\])$ is w -nested if $C[\]$ is w -nested.
4. The term $\bigoplus_{i \in I} [p_i] \xi_i$ is w -nested if $\xi_j = C[\]$ for some $j \in I$, and $C[\]$ is w -nested.
5. The term $\mathbf{f}(\dots, \xi_{i-1}, C[\], \xi_{i+1}, \dots)$ is w -nested if $C[\]$ is w -nested and the i -th argument of the function symbol \mathbf{f} is wild.

The variable ζ appears in a w -nested position in $\xi \in \mathbb{T}(\Sigma)$ if there is a w -nested context $C[\]$ with $C[\zeta] = \xi$.

Definition 23. Let $P = (\Sigma, \mathcal{A}, \mathcal{R})$ be a PTSS where each argument of $f \in \Sigma$ is defined as wild or tame with respect to \mathcal{G}_P . The PTSS P is in the probabilistic RBB safe specification format if for all $r \in \mathcal{R}$ one of the following conditions holds.

1. r is a patience rule for a wild argument of a function symbol in Σ .
2. r is a RBB safe rule, i.e. r has the following shape

$$\frac{\{t_m \xrightarrow{a_m} \mu_m \mid m \in M\} \quad \{t_n \xrightarrow{b_n} \nu_n \mid n \in N\}}{f(\zeta_1, \dots, \zeta_{\text{rk}(f)}) \xrightarrow{a} \theta}$$

where M and N are index sets, ζ_k , and μ_m , with $1 \leq k \leq \text{rk}(f)$ and $m \in M$, are all different variables, $f \in \Sigma_s$, $t_m, t_n \in \mathbb{T}(\Sigma_s)$ and $\theta \in \mathbb{T}(\Sigma_d)$, and the following conditions are met.

- (a) If the i -th argument of f is wild and has a patience rule in \mathcal{R} , then for all $\psi \in \text{prem}(r)$ such that $\zeta_i = x_i \in \text{var}(\psi)$, $\psi = x_i \xrightarrow{a_i} \mu_i$ with $a_i \neq \tau$.
- (b) If the i -th argument of f is wild and does not have a patience rule in \mathcal{R} , then ζ_i does not occur in the source of a premise of r .
- (c) Variables μ_m , for $m \in M$, and variables ζ_i , where i -th argument of f is wild, only occur at w -nested positions in θ .
- (d) $\mu_m \notin \text{var}(t_{m'})$ for all $m, m' \in M$.

Patience rules for wild arguments allow to progress along the i -th parameter using the transition $x_i \xrightarrow{\tau} \mu$. Because of the patience rules and the restriction to test a wild argument (Definition 23.2a), τ -transitions will not be detected by the premises of the rules of a PTSS satisfying the format. If an argument of some f is wild and it has no patience rule, then it cannot be tested (Definition 23.2b). Notice that the patience rules lift the τ -transition that can be executed by the i -th parameter of f to f , i.e. if the i -th parameter of f can execute a τ -transition then f can execute a τ -transition affecting only the this parameter. Then, the lifting of a τ -transition has to be also ‘controlled’. This is done requiring Definition 23.2c. Finally, restriction Definition 23.2d is added to avoid dealing with non-well-founded set of premises (see [18]). Because rules do not support quantitative premises, see Definition 4, this is not a significant restriction.

For the probabilistic RBB safe specification format we have the following congruence result.

Theorem 24. Let P be a complete PTSS in RBB safe specification format. Then \approx_{rb} is a congruence relation for all operators defined in P .

In the rest of this section we present the key elements needed to prove Theorem 24. For the sake of clarity, we fix $P = (\Sigma, \mathcal{A}, \mathcal{R})$, a complete PTSS. For any ordinal α , let $\langle \text{CT}_\alpha, \text{PT}_\alpha \rangle$ be the 3-valued model of P

constructed inductively as in Lemma 7 with $\langle CT_\lambda, PT_\lambda \rangle$ being the 3-valued least stable model. Thus, $CT_\lambda = PT_\lambda$ is the transition relation associated to P .

First we introduce the relations \mathcal{C} and \mathcal{B} . \mathcal{C} is the congruence closure of rooted branching bisimulation, and \mathcal{B} is a kind of congruence closure of the branching bisimulation based on wild and tame arguments and relation \mathcal{C} . Notice the correlation between \mathcal{B} and the restrictions imposed to the target of the conclusion of a rule in RBB safe format.

Definition 25. (a) The relation $\mathcal{C} \subseteq T(\Sigma) \times T(\Sigma)$ is the smallest relation such that

1. $\approx_{rb} \subseteq \mathcal{C}$,
2. $c \mathcal{C} c'$ whenever $c, c' \in \Sigma_s$, $ar(c), ar(c') = s$ and $c \mathcal{C} c'$, and
3. $f(\xi_1, \dots, \xi_{rk(f)}) \mathcal{C} f(\xi'_1, \dots, \xi'_{rk(f)})$ whenever $\xi_i \mathcal{C} \xi'_i$ for all i , $1 \leq i \leq rk(f)$ and $f \in \Sigma_s \cup \Sigma_d$.

(b) The relation $\mathcal{B} \subseteq T(\Sigma) \times T(\Sigma)$ is the smallest relation such that

1. $\approx_b \subseteq \mathcal{B}$,
2. $c \mathcal{B} c'$ whenever $c, c' \in \Sigma_s$, $ar(c), ar(c') = s$ and $c \mathcal{B} c'$, and
3. $f(\xi_1, \dots, \xi_{rk(f)}) \mathcal{C} f(\xi'_1, \dots, \xi'_{rk(f)})$ whenever $f \in \Sigma_s \cup \Sigma_d$,
 - $\xi_i \mathcal{C} \xi'_i$ for the i -th tame arguments of f , and
 - $\xi_i \mathcal{B} \xi'_i$ for the i -th wild arguments of f .

The two cases of the following lemma can be proved using structural induction with respect to $\vartheta \in \mathbb{T}(\Sigma)$ and the definitions of \mathcal{C} and \mathcal{B} .

Lemma 26. Let ρ, ρ' be two closed substitutions and $\vartheta \in \mathbb{T}(\Sigma)$.

- If $\rho(\zeta) \mathcal{C} \rho'(\zeta)$ for all $\zeta \in \mathcal{V} \cup \mathcal{D}$, then $\rho(\vartheta) \mathcal{C} \rho'(\vartheta)$.
- If, for each variable $\zeta \in \text{var}(\vartheta)$, either
 - $\rho(\zeta) \mathcal{C} \rho'(\zeta)$, or
 - $\rho(\zeta) \mathcal{B} \rho'(\zeta)$ and x only occurs at w -nested positions in ϑ ,
 then $\sigma(\vartheta) \mathcal{B} \sigma'(\vartheta)$.

The relations \mathcal{C} and \mathcal{B} lift properly to distributions. This ensures that $[\![\theta]\!] \mathcal{C} [\![\theta']]\!]$ and $[\![\theta]\!] \mathcal{B} [\![\theta']]\!]$ whenever $\theta \mathcal{C} \theta'$ and $\theta \mathcal{B} \theta'$, respectively. Therefore we can work at the symbolic level.

Lemma 27. Let $\theta, \theta' \in T(\Sigma_d)$. If $\theta \mathcal{C} \theta'$ then $[\![\theta]\!] \mathcal{C} [\![\theta']]\!]$. If $\theta \mathcal{B} \theta'$ then $[\![\theta]\!] \mathcal{B} [\![\theta']]\!]$.

Theorem 24 is a straight consequence of Lemma 28. Notice that clause (III $_\alpha$) uses the characterization of branching bisimulation without schedulers.

Lemma 28. If P is in probabilistic RBB safe format and $s, t \in T(\Sigma_s)$, then

- (I $_\alpha$) If $s \mathcal{C} t$ and $s \xrightarrow{a} \theta_s \in CT_\lambda$, then $t \xrightarrow{a} \theta_t \in PT_\alpha$ for some $\theta_t \in T(\Sigma_d)$.
- (II $_\alpha$) If $s \mathcal{C} t$ and $s \xrightarrow{a} \theta_s \in CT_\alpha$, then $t \xrightarrow{a} \theta_t \in CT_\lambda$ for some $\theta_t \in T(\Sigma_d)$ with $\theta_s \mathcal{B} \theta_t$.
- (III $_\alpha$) If $s \mathcal{B} t$ and $s \xrightarrow{a} \theta_s \in CT_\alpha$ then either:
 - $a = \tau$ and $\delta(s) \mathcal{B} \theta_s$ or
 - there is a concrete execution $t_0 \tau \theta_1 t_1 \tau \theta_2 t_2 \dots \theta_n t_n a \theta_t$ in CT_λ such that $t = t_0$, $s \mathcal{B} t_i$ for $0 \leq i \leq n$, $\delta(s) \mathcal{B} \theta_j$ for $1 \leq j \leq n$ and $\theta_s \mathcal{B} \theta_t$.

Proof of Theorem 24. Clause (III_α) of Lemma 28 yields that \mathcal{B} is a branching bisimulation. Together with clause (II_α) this implies that \mathcal{C} is a rooted branching bisimulation. By definition of \approx_{rb} , $\mathcal{C} \subseteq \approx_{rb}$ and by definition of \mathcal{C} , $\mathcal{C} \supseteq \approx_{rb}$, therefore $\mathcal{C} = \approx_{rb}$. Finally, by Definition 25.a.3, rooted branching bisimulation is a congruence. \square

Example 29. *The following example shows that the format does not preserve probabilistic branching bisimulation. Let $t_1 = a.\mathbf{b} + a.\mathbf{c}$ and $t_2 = t_1 + a.([0.5]\mathbf{b} \oplus [0.5]\mathbf{c})$ then $t_1 \approx_{pb} t_2$ (we omit the distribution $\mathbf{0}$). Consider the following rules:*

$$\frac{x \xrightarrow{a} \mu}{f(x) \xrightarrow{a} \mathbf{g}(\mu, \mu)} \quad \frac{x_1 \xrightarrow{b} \mu_1 \quad x_2 \xrightarrow{c} \mu_2}{g(x_1, x_2) \xrightarrow{a} \mathbf{0}} \quad \frac{x \xrightarrow{\tau} \mu}{g(x, y) \xrightarrow{\tau} \mathbf{g}(\mu, \delta(y))} \quad \frac{y \xrightarrow{\tau} \mu}{g(x, y) \xrightarrow{\tau} \mathbf{g}(\delta(x), \mu)}$$

then $f(t_1) = a.(\mathbf{g}(\mathbf{b}, \mathbf{b})) + a.(\mathbf{g}(\mathbf{c}, \mathbf{c}))$, $f(t_2) = f(t_1) + a.(\mathbf{g}([0.5]\mathbf{b} \oplus [0.5]\mathbf{c}, [0.5]\mathbf{b} \oplus [0.5]\mathbf{c}))$. Notice it is not possible to combine distributions $\mathbf{g}(\mathbf{b}, \mathbf{b})$ and $\mathbf{g}(\mathbf{c}, \mathbf{c})$ to get the distribution $\mathbf{g}([0.5]\mathbf{b} \oplus [0.5]\mathbf{c}, [0.5]\mathbf{b} \oplus [0.5]\mathbf{c})$. In addition $\mathbf{g}(\mathbf{b}, \mathbf{b}) \approx_{pb} \mathbf{g}(\mathbf{c}, \mathbf{c}) \approx_{pb} \mathbf{0} \not\approx_{pb} \mathbf{g}([0.5]\mathbf{b} \oplus [0.5]\mathbf{c}, [0.5]\mathbf{b} \oplus [0.5]\mathbf{c})$.

6 Concluding remarks

In this paper we have presented the RBB safe specification format, to the best of our knowledge, the first transition system specification format in the quantitative setting that respects a weak equivalence.

Two main ideas underlie our approach. First, the qualitative RBB safe specification format [14] occurs to translate smoothly to the way of specifying probabilistic transitions systems as proposed in [11, 25]. The representation of distributions over states via the algebraic of distribution terms, is crucial to adapt the result. With syntactic grip on distributions in place we are able to incorporate the definitions of a nesting graph and a wild argument, patience rules, w-nested context and w-nested position, and finally the format specification itself. In addition, Lemma 27 ensures that relations at the syntactic level lift well to the semantical level.

Second, the characterization of branching bisimulation without schedulers of [3] reduced the complexity of our proofs. In general, frameworks combining internal transitions and probabilities, exploit schedulers to define weak combined transitions. This gives extra overhead in the technical treatment. Witnessing that working with these notions is not that easy, decision algorithms for e.g. weak probabilistic bisimulation [21] and weak distribution bisimulation [12] are from recent years.

Future work includes an extension of the format, or a new one, to ensure that probabilistic branching bisimulation is a congruence. It also includes an extension to support quantitative premises. As explained in Section 5, quantitative premises cannot be used to include look-ahead in the format directly. However, the two-sorted approach allows rules of the shape

$$\frac{\mu_1 \oplus_{p_1} \delta(\{y_2\})(\{y_1\}) \supseteq p_1 \quad \mu_2 \oplus_{p_2} \delta(\{y_1\})(\{y_2\}) \supseteq p_2}{f(\mu_1, \mu_2) \xrightarrow{a} \theta}$$

In order to achieve this goal, techniques introduced for the $\text{nt}\mu f\theta/\text{nt}\mu \times \theta$ format [11] can be used. Other research investigates the characterization of branching bisimulation without schedulers to obtain new results in the probabilistic context. Currently we are working on a logic to characterize this relation, focusing on completeness.

Acknowledgment. The authors would like to thank Pedro R. D'Argenio for helpful discussions.

References

- [1] L. Aceto, B. Bloom & F.W. Vaandrager (1994): *Turning SOS Rules into Equations*. *Information and Computation* 111, pp. 1–52, doi:10.1006/inco.1994.1040.
- [2] L. Aceto, W. Fokkink & C. Verhoef (1999): *Handbook of Process Algebra*, chapter Chapter 3: Structural Operational Semantics, pp. 197–292. Elsevier.
- [3] S. Andova, S. Georgievska & N. Trčka (2012): *Branching bisimulation congruence for probabilistic systems*. *Theoretical Computer Science* 413, pp. 58–72, doi:10.1016/j.tcs.2011.07.020.
- [4] J.C.M. Baeten & E.P. de Vink (2004): *Axiomatizing GSOS with Termination*. *Journal of Logic and Algebraic Programming* 60–61, pp. 323–351, doi:10.1016/j.jlap.2004.03.001.
- [5] F. Bartels (2004): *On Generalised Coinduction and Probabilistic Specification Formats*. Ph.D. thesis, Vrije Universiteit Amsterdam.
- [6] B. Bloom (1995): *Structural operational semantics for weak bisimulations*. *Theoretical Computer Science* 146, pp. 25–68, doi:10.1016/0304-3975(94)00152-9.
- [7] B. Bloom, S. Istrail & A.R. Meyer (1995): *Bisimulation can't be traced*. *Journal of the ACM* 42, pp. 232–268, doi:10.1145/200836.200876.
- [8] R. Bol & J.F. Groote (1996): *The meaning of negative premises in transition system specifications*. *Journal of the ACM* 43, pp. 863–914, doi:10.1145/234752.234756.
- [9] V. Castiglioni, R. Lanotte & S. Tini (2014): *A Specification Format for Rooted Branching Bisimulation*. *Fundamenta Informaticae* 135, pp. 355–369, doi:10.3233/FI-2014-1128.
- [10] P.R. D'Argenio, D. Gebler & M.D. Lee (2014): *Axiomatizing bisimulation equivalences and metrics from probabilistic SOS rules*. In A. Muscholl, editor: *Proc. FoSSACS, LNCS 8412*, pp. 289–303, doi:10.1007/978-3-642-54830-7_19.
- [11] P.R. D'Argenio & M.D. Lee (2012): *Probabilistic transition system specification: Congruence and full abstraction of bisimulation*. In L. Birkedal, editor: *Proc. FOSSACS, LNCS 7213*, pp. 452–466, doi:10.1007/978-3-642-28729-9_30.
- [12] C. Eisentraut, H. Hermanns, J. Krämer, A. Turrini & Lijun Zhang (2013): *Deciding Bisimilarities on Distributions*. In K. Joshi, M. Siegle, M. Stoelinga & P.R. D'Argenio, editors: *Proc. QEST, LNCS 8054*, pp. 72–88, doi:10.1007/978-3-642-40196-1_6.
- [13] W. Fokkink (1994): *The tyft/tyxt Format Reduces to Tree Rules*. In M. Hagiya & J.C. Mitchell, editors: *Proc. TACS 1994, LNCS 789*, pp. 440–453, doi:10.1007/3-540-57887-0_109.
- [14] W. Fokkink (2000): *Rooted Branching Bisimulation as a Congruence*. *Journal of Computer and System Sciences* 60, pp. 13–37, doi:10.1006/jcss.1999.1663.
- [15] W. Fokkink & C. Verhoef (1998): *A Conservative Look at Operational Semantics with Variable Binding*. *Information and Computation* 146, pp. 24–54, doi:10.1006/inco.1998.2729.
- [16] R.J. van Glabbeek (2004): *The Meaning of Negative Premises in Transition System Specifications II*. *Journal of Logic and Algebraic Programming* 60–61, pp. 229–258, doi:10.1016/j.jlap.2004.03.007.
- [17] R.J. van Glabbeek (2005): *On cool congruence formats for weak bisimulations*. In Dang Van Hung & M. Wirsing, editors: *Proc. ICTAC 2005, LNCS 3722*, pp. 318–333, doi:10.1007/11560647_21.
- [18] J.F. Groote (1993): *Transition system specifications with negative premises*. *Theoretical Computer Science* 118, pp. 263–299, doi:10.1016/0304-3975(93)90111-6.
- [19] J.F. Groote & F. Vaandrager (1992): *Structured Operational Semantics and Bisimulation as a Congruence*. *Information and Computation* 100, pp. 202–260, doi:10.1016/0890-5401(92)90013-6.
- [20] H. Hansson (1991): *Time and probability in formal design of distributed systems*. Ph.D. thesis, University of Uppsala.
- [21] H. Hermanns & A. Turrini (2012): *Deciding Probabilistic Automata Weak Bisimulation in Polynomial Time*. In D. D'Souza, T. Kavitha & J. Radhakrishnan, editors: *FSTTCS 2012, 18, Dagstuhl*, pp. 435–447.

- [22] B. Klin (2009): *Structural Operational Semantics for Weighted Transition Systems*. In J. Palsberg, editor: *Semantics and Algebraic Specification*, LNCS 5700, pp. 121–139, doi:10.1007/978-3-642-04164-8_7.
- [23] B. Klin & V. Sassone (2013): *Structural operational semantics for stochastic and weighted transition systems*. *Information and Computation* 227, pp. 58–83, doi:10.1016/j.ic.2013.04.001.
- [24] R. Lanotte & S. Tini (2009): *Probabilistic bisimulation as a congruence*. *ACM Transactions on Computational Logic* 10, pp. 1–48, doi:10.1145/1462179.1462181.
- [25] M.D. Lee, D. Gebler & P.R. D’Argenio (2012): *Tree rules in probabilistic transition system specifications with negative and quantitative premises*. In B. Luttik & M.A. Reniers, editors: *Proc. EXPRESS/SOS, EPTCS 89*, pp. 115–130, doi:10.4204/EPTCS.89.9.
- [26] M. Miculan & M. Peressotti (2014): *GSOS for non-deterministic processes with quantitative aspects*. In N. Bertrand & L. Bortolussi, editors: *Proc. QAPL 2014, EPTCS 154*, pp. 17–33, doi:10.4204/EPTCS.154.2.
- [27] M.R. Mousavi, M.A. Reniers & J.F. Groote (2007): *SOS formats and meta-theory: 20 years after*. *Theoretical Computer Science* 373, pp. 238–272, doi:10.1016/j.tcs.2006.12.019.
- [28] R. Segala (1995): *Modeling and Verification of Randomized Distributed Real-Time Systems*. Ph.D. thesis, MIT.
- [29] R. Segala & N.A. Lynch (1995): *Probabilistic simulations for probabilistic processes*. *Nordic Journal of Computing* 2, pp. 250–273.