Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science 175 (2007) 77–88
Electronic Notes in Theoretical Computer Science
www.elsevier.com/locate/entcs

Notes on Generative Probabilistic Bisimulation

Simone Tini [1,2]

Dipartimento di Scienze della Cultura, Politiche e dell'Informazione
Università dell'Insubria
Via Carloni 78, 22100, Como, Italy

Abstract

In this notes we consider the model of Generative Probabilistic Transition Systems, and Baier and Hermanns' notion of weak bisimulation defined over them. We prove that, if we consider any process algebra giving rise to a Probabilistic Transition System satisfying the condition of regularity and offering prefixing, interleaving, and guarded recursion, then the coarsest congruence that is contained in weak bisimulation is strong bisimulation.

Keywords: Process Algebras, Generative Probability, Behavioral Equivalences, Bisimulation, Weak Bisimulation, Congruence

1 Introduction

Probabilistic process algebras have been introduced in the literature (see, among the others, [1,2,3,7,10,11,12,16,18,21,31]) to develop techniques dealing with both functional and non-functional aspects of system behavior, such as performance and reliability. Models of probabilistic processes are classified in [18] into *generative*, *reactive*, and *stratified*. In the generative model, a single probability distribution is ascribed to all moves of a given process, independently of their action label. In the reactive model, the kind of action performed by a given process in chosen in a nondeterministic way, and a probability distribution is ascribed to all moves of that process labeled with that action. In the stratified model a given process has either *probability moves*, to which a single probability distribution is ascribed and that are associated with no action label, or a single *action move*, having an action label, thus implying a clear separation of action and probability. The model of *Probabilistic*

[1] Author partially supported by PRIN Project "Analisi di sistemi di Riduzione mediante sistemi di Transizione" (ART)

[2] Email: simone.tini@uninsubria.it

1571-0661
doi:10.1016/j.entcs.2006.09.016

Automata [29] was introduced to capture both probability and the classical process algebraic notion of nondeterminism. Here, a state of an automaton can have several *transitions* that are chosen in a nondeterministic way, and each transition leads to a probabilistic distribution over action labeled moves. Usually, the model of [29] is known as the *non-alternating model*, in contraposition with the *alternating model* of [19], where there is a clear distinction between *nondeterministic* states, enabling transitions leading to a unique state and that are chosen in a nondeterministic way, and *probabilistic states*, enabling a unique transition leading to a probabilistic distribution over states.

Probabilistic transition systems (PTSs, for short), which extend classic labeled transition systems by some mechanism to represent probability, have been employed as a basic semantic model of probabilistic processes. Of course, several definitions of PTS have been introduced, taking into account of the probabilistic model considered. In order to abstract away from irrelevant information on the way that probabilistic processes compute, several notions of probabilistic *equivalence* and *preorder* have been defined over the PTS models [2,8,9,11,12,19,20,22,23,25,30,32]. In order to fit a given equivalence into an axiomatic framework, it is required that it is a *congruence* with respect to all process algebra operations. *Probabilistic bisimulation*, which relates two processes iff their PTSs have the same probabilistic branching structure, and that was originally defined in [25] for the reactive model, enjoys the congruence property in the process algebras proposed in the papers mentioned above, and is one of the equivalence definitions most frequently employed.

In the nonprobabilistic case, *weak bisimulation* has been successfully proposed by Milner [26] as an equivalence relation that abstracts away from *internal* computation steps. A notion of weak bisimulation for the non-alternating model has been considered in [2,11,12,30]. Baier and Hermanns [5] formulated a notion of weak bisimulation inspired by [26] for the generative model. We refer to [5] for interesting motivations and results on probabilistic weak bisimulation.

In the nonprobabilistic setting, it is well known that weak bisimulation is not a congruence with respect to the operation of nondeterministic choice, which is offered by most of known process algebras. Due to the importance of having the congruence property, the coarsest congruence with respect to nondeterministic choice that is finer than weak bisimulation has been characterized, and called *observational congruence* by Milner [26]. Such a congruence is known also with the names of *rooted τ-bisimulation* [4] and *rooted weak bisimulation* [6]. Also in the non-alternating model, the coarsest congruence with respect to nondeterministic choice that is finer than weak bisimulation has been characterized [2,11,12].

Process algebras respecting the generative model do not offer any operation of nondeterministic choice. More precisely, these process algebras do not offer any operation introducing nondeterminism. However, in general, also in the generative model weak bisimulation is not a congruence. In fact, many process algebras offer a parametric version of interleaving operation, where the parameter determines the probability to move of each of the two composed processes, and we show by means of a simple example that weak bisimulation is not a congruence with respect to this interleaving operation. Also the CCS-like parallel composition operation of [10,7] and the CSP-like parallel composition operation of [10] do not preserve weak bisimulation.

Our aim is then to study in the generative model the problem to give a characterization of the coarsest equivalence notion being finer than probabilistic weak bisimulation and being a congruence with respect to any reasonable kernel of operations. To this purpose, we assume prefixing, interleaving, and guarded recursion as such a kernel of operations, since they are widely employed. We prove that, if we only consider process algebras giving rise to PTSs satisfying the regularity condition, then the congruence we aim to characterize is probabilistic bisimulation. In some sense, this result has negative consequences. In fact, in the nonprobabilistic case a lot of work has been done on congruences weaker than bisimulation and stronger than weak bisimulation [6,13,14,15,17], whereas in the generative case such a work cannot be repeated, since our result implies that there is no congruence strictly lying between bisimulation and weak bisimulation. Note that our result emphasizes also a difference between the generative and the non-alternating model, where the coarsest congruence contained in weak bisimulation is strictly coarsest than strong bisimulation. This difference depends on the fact that the parallel composition operation of the non-alternating model has no parameter, introduces nondeterminism, and can be treated as the classical interleaving operation of [26].

2 Probabilistic Bisimulations

Given any set S, let $\mathcal{M}(S)$ denote the set of all multisets over S. Let us employ "$\{\!|$" and "$|\!\}$" as brackets for multisets.

The following definition originates from [3,5,7].

Definition 2.1 A *generative probabilistic transition system* (GPTS, for short) is a triple $(\mathcal{S}, Act, T)$, where $\mathcal{S}$ is a set of *states*, Act is a countable set of *actions*, and $T \in \mathcal{M}(\mathcal{S} \times Act \times (0,1] \times \mathcal{S})$ is a multiset of *transitions* such that, for all states $s \in \mathcal{S}$:

$$\sum \{\!|\, p \mid \exists \alpha \in Act, s' \in S : (s, \alpha, p, s') \in T \,|\!\} \in \{0,1\}$$ [3]

Def. 2.1 requires that each state $s \in \mathcal{S}$ is *semistochastic*, namely, the probabilities of its outgoing transitions, if there are any, sum up to 1. Let us recall that GPTSs considered in [18,31] have a weaker requirement, since they admit that, for each state s, the sum of the probabilities of its outgoing transitions, if there are any, is a value $0 \leq q \leq 1$, the interpretation being that s deadlocks with probability $1 - q$. Results proved in the present paper hold also for the model of GPTS of [18,31], since they do not depend on any constraint on the probability of the transitions leaving from s.

Let $s \xrightarrow{\alpha,p} s'$ denote that $(s, \alpha, p, s') \in T$, $s \rightarrow$ denote that $s \xrightarrow{\alpha,p} s'$ holds for some α, p and s', and $s \not\rightarrow$ denote that $s \xrightarrow{\alpha,p} s'$ holds for no α, p and s'.

[3] Note that multisets are needed to handle the case where from a state s several transitions with the same label α and probability p lead to a state s'.

Let $s \Longrightarrow s'$ denote that s' is *reachable* from s, namely there exists a sequence of transitions $s_0 \xrightarrow{\alpha_0,p_0} s_1 \ldots s_{n-1} \xrightarrow{\alpha_{n-1},p_{n-1}} s_n$ such that $s_0 = s$ and $s_n = s'$.

In the following we assume the "regularity" condition, namely, for each state $s \in \mathcal{S}$ there are only finitely many outgoing transitions $s \xrightarrow{\alpha,p} s'$, and from s only finitely many other states can be reached through any (possibly infinite) sequence of transitions.

Let us recall the *cumulative probability distribution function* μ_G [18], which computes the total probability by which from a state s a state s' can be reached through transitions labeled with an action α. Adopting the convention that the empty sum of probability is 0, μ_G is defined as follows.

Definition 2.2 $\mu_G : \mathcal{S} \times Act \times \mathcal{S} \to [0,1]$ is the function given by: $\forall s \in \mathcal{S}$, $\forall \alpha \in Act$, $\forall s' \in \mathcal{S}$:

$$\mu_G(s,\alpha,s') = \sum \{\!| p \mid s \xrightarrow{\alpha,p} s' \in T |\!\}$$

Function μ_G can be extended to sets of target states. $\forall s \in \mathcal{S}$, $\forall \alpha \in Act$, $\forall S \subseteq \mathcal{S}$:

$$\mu_G(s,\alpha,S) = \sum_{s' \in S} \mu_G(s,\alpha,s')$$

Following [5], function μ_G can be extended to sequences of actions in Act^*. Let ϵ denote the empty sequence of actions. For each $\alpha \in Act$ and $\lambda \in Act^*$, let $\alpha\lambda$ denote the sequence in Act^* obtained by prefixing λ with α.

Then, $\forall s \in \mathcal{S}$, $\forall \alpha \in Act$, $\forall \lambda \in Act^*$, $\forall S \subseteq \mathcal{S}$:

$$\begin{aligned} \mu_G(s,\epsilon,S) &= 1 \text{ if } s \in S \\ \mu_G(s,\epsilon,S) &= 0 \text{ if } s \notin S \\ \mu_G(s,\alpha\lambda,S) &= \sum_{s' \in \mathcal{S}} \mu_G(s,\alpha,s') \cdot \mu_G(s',\lambda,S) \end{aligned}$$

Finally, following [5] function μ_G can be extended to sets of sequences of actions in Act^*. Let Λ denote any subset of Act^*, and Λ/α denote the set $\{\lambda \in Act^* \mid \alpha\lambda \in \Lambda\}$.

Then, $\forall s \in \mathcal{S}$, $\forall \Lambda \subseteq Act^*$, $\forall S \subseteq \mathcal{S}$:

$$\begin{aligned} \mu_G(s,\Lambda,S) &= 1 \text{ if } \epsilon \in \Lambda \text{ and } s \in S \\ \mu_G(s,\Lambda,S) &= \sum_{(\alpha,s') \in Act \times \mathcal{S}} \mu_G(s,\alpha,s') \cdot \mu_G(s',\Lambda/\alpha,S) \text{ otherwise} \end{aligned}$$

We can recall now the notion of bisimulation for GPTSs [18]. For any equivalence relation $\mathcal{R}$ over the set of states $\mathcal{S}$, let $\mathcal{S}/\mathcal{R}$ denote the set of equivalence classes induced by $\mathcal{R}$.

Definition 2.3 An equivalence relation $\mathcal{R} \subseteq \mathcal{S} \times \mathcal{S}$ is a *(strong) bisimulation* if $(s_1,s_2) \in \mathcal{R}$ implies: $\forall C \in \mathcal{S}/\mathcal{R}$, $\forall \alpha \in Act$:

$$\mu_G(s_1,\alpha,C) = \mu_G(s_2,\alpha,C)$$

The union of all bisimulations is, in turn, a bisimulation, denoted by $\sim$. Relation $\sim$ equates states having the same probabilistic branching structure.

Let us assume that *Act* contains the special *silent* action τ. We can recall now Baier and Hermanns' notion of weak bisimulation for GPTSs [5]. Let us denote sets of sequences of actions in Act^* with regular expressions.

Definition 2.4 An equivalence relation $\mathcal{R} \subseteq \mathcal{S} \times \mathcal{S}$ is a *weak bisimulation* if $(s_1, s_2) \in \mathcal{R}$ implies: $\forall C \in \mathcal{S}/\mathcal{R}$, $\forall a \in Act \setminus \{\tau\}$:

$$\mu_G(s_1, \tau^* a \tau^*, C) = \mu_G(s_2, \tau^* a \tau^*, C)$$

$$\mu_G(s_1, \tau^*, C) = \mu_G(s_2, \tau^*, C)$$

The union of all weak bisimulations is, in turn, a weak bisimulation, denoted by $\approx$. Relation $\approx$ is coarser than $\sim$, since it abstracts from silent computation steps.

3 Weak Bisimulation is not a Congruence

As usual, let us assume a process description language whose abstract syntax is given by a *signature*, consisting of a set of *operation symbols* Σ together with an *arity* mapping that assigns a natural $ar(f)$ to every $f \in \Sigma$.

For a set of *variables* `Var` ranged over by $x, y, \ldots$, the set of (*open*) *terms* over Σ and `Var` is the least set such that:

- each variable $x \in$ `Var` is a term;
- $f(t_1, \ldots, t_{ar(f)})$ is a term whenever $f \in \Sigma$ and $t_1, \ldots, t_{ar(f)}$ are terms.

Terms that do not contain variables in `Var` are called closed terms, or processes.

The semantics of the language is given by a GPTS, whose states are processes, and whose transitions are inferred by a set of SOS rules [27,28]. As usual, let us assume that Σ contains the operation symbol 0 (sometimes denoted **nil**) with $ar(0) = 0$, where 0 represents the idling process having no move.

Let us recall the notion of congruence.

Definition 3.1 An equivalence relation $\mathcal{R}$ over processes is called a *congruence* iff, for each $f \in \Sigma$, if relation $(t_i, t'_i) \in \mathcal{R}$ holds for all $1 \leq i \leq ar(f)$, then $(f(t_1, \ldots, t_{ar(f)}), f(t'_1, \ldots, t'_{ar(f)})) \in \mathcal{R}$.

Now, bisimulation $\sim$ is a congruence with respect to operations of well known process algebras used in the literature [1,3,7,10,16,18,21,24,31].

Let us consider the operation of probabilistic interleaving $\|^p$ of [3], whose semantics in SOS style is presented in Table 1. Intuitively, if both processes t_1 and t_2 can move, then the process $t_1 \|^p t_2$ moves as t_1 with probability p and as t_2 with probability $1-p$. If only t_1 (resp. t_2) can move, then $t_1 \|^p t_2$ moves as t_1 (resp. t_2) with probability 1.

By an example, we can show that weak bisimulation is not a congruence with respect to operation $\|^p$.

$$\frac{}{\alpha \cdot x \xrightarrow{\alpha,1} x} \qquad\qquad \frac{x[\mathbf{rec}X.\, x/X] \xrightarrow{\alpha,p} y}{\mathbf{rec}X.\, x \xrightarrow{\alpha,p} y}$$

$$\frac{x_1 \xrightarrow{\alpha_1,p_1} y_1 \quad x_2 \not\rightarrow}{x_1 \;\|^p\; x_2 \xrightarrow{\alpha_1,p_1} y_1 \;\|^p\; x_2} \qquad\qquad \frac{x_1 \not\rightarrow \quad x_2 \xrightarrow{\alpha_2,p_2} y_2}{x_1 \;\|^p\; x_2 \xrightarrow{\alpha_2,p_2} x_1 \;\|^p\; y_2}$$

$$\frac{x_1 \xrightarrow{\alpha_1,p_1} y_1 \quad x_2 \rightarrow}{x_1 \;\|^p\; x_2 \xrightarrow{\alpha_1,p_1 \cdot p} y_1 \;\|^p\; x_2} \qquad\qquad \frac{x_1 \rightarrow \quad x_2 \xrightarrow{\alpha_2,p_2} y_2}{x_1 \;\|^p\; x_2 \xrightarrow{\alpha_2,p_2\cdot(1-p)} x_1 \;\|^p\; y_2}$$

Table 1
Some probabilistic operations; x, x_1, x_2, y_1, y_2 are process variables, $\alpha, \alpha_1, \alpha_2$ range over *Act*, p, p_1, p_2 are variables over the interval $[0, 1]$, and X is a *recursion variable*.

Example 3.2 Let $a \in \mathit{Act} \setminus \{\tau\}$, and t_1 and t_2 be the processes $t_1 \equiv \tau \cdot a \cdot 0$ and $t_2 \equiv \tau \cdot \tau \cdot a \cdot 0$, where $\cdot$ is the prefixing operation described in Table 1. It is immediate that $t_1 \approx t_2$, but, for each $0 < p < 1$ and $b \in \mathit{Act} \setminus \{a, \tau\}$, $t_1 \;\|^p\; b \cdot 0 \not\approx t_2 \;\|^p\; b \cdot 0$. In fact, $\mu_G(t_1 \;\|^p\; b \cdot 0, \tau^* a \tau^*, 0 \;\|^p\; b \cdot 0) = p^2$, whereas $\mu_G(t_2 \;\|^p\; b \cdot 0, \tau^* a \tau^*, 0 \;\|^p\; b \cdot 0) = p^3$, and no other state weak bisimilar to $0 \;\|^p\; b \cdot 0$ is reachable from $t_1 \;\|^p\; b \cdot 0$ and $t_2 \;\|^p\; b \cdot 0$. Intuitively, to perform the a move before the b move by $b \cdot 0$, t_1 has to win two competitions versus $b \cdot 0$, whereas t_2 has to win three competitions, and the probability to win each of these competitions is p.

Notice that the arguments of Example 3.2 hold also if we replace the interleaving operation $\|^p$ with the CCS-like parallel composition operation $\|^p_q$ of [10,7], provided that $b \neq \overline{a}$, or with the CSP-like parallel composition operation $\|^p_A$ of [10], provided that the set of actions A contains neither a nor b.

4 Bisimulation is the Coarsest Congruence Contained in Weak Bisimulation

Let **rec** be the recursion operation defined in Table 1. We assume that the recursion variables always appear as *guarded*, according to the usual definition. In this section we prove that, if we consider any process algebra offering the operations of prefixing, recursion, and interleaving as in Table 1, then the coarsest congruence contained in weak bisimulation is bisimulation.

Let us introduce the notion of p-bisimulation. It can be viewed as a relation weaker than a bisimulation, in the sense that the probabilistic branching structure of processes is considered modulo the probability value p.

Definition 4.1 Given any $0 \leq p \leq 1$, an equivalence relation $\mathcal{R}_p \subseteq \mathcal{S} \times \mathcal{S}$ is a *p-bisimulation* if $(s_1, s_2) \in \mathcal{R}_p$ implies: $\forall C \in \mathcal{S}/\mathcal{R}_p$, $\forall \alpha \in \mathit{Act}$:

$$|\mu_G(s_1, \alpha, C) - \mu_G(s_2, \alpha, C)| \leq p$$

$$\mu_G(s_1, \alpha, C) = 0 \text{ iff } \mu_G(s_2, \alpha, C) = 0$$

On one side, it is not guaranteed that the union of all p-bisimulations is a p-bisimulation, and, therefore, p-bisimulations are less elegant than bisimulations and weak bisimulations. On the other side, p-bisimulations permit to relate two processes when they differ only for probabilities smaller than a given bound p. However, we are not interested here in studying their theory, we simply use p-bisimulations in our proofs.

The following result is immediate.

Proposition 4.2 *A p-bisimulation is also a q-bisimulation, for each $q > p$. A 0-bisimulation is a bisimulation.*

Given a process t, let $actions(t)$ denote the set of the actions appearing in the transition labels in the portion of GPTS rooted in t. The regularity condition over the GPTS ensures that $actions(t)$ is a finite set.

Let us assume two processes t and t'. Since $actions(t)$ and $actions(t')$ are finite sets, and since Act is a countable set, we can take two actions $b, c \in Act \setminus (actions(t) \cup actions(t') \cup \{\tau\})$. We can prove that, given arbitrary values $0 < p, q < 1$, then, if relation $(t \parallel^q \mathbf{rec}X\,.\,c \cdot X) \parallel^p \mathbf{rec}X\,.\,b \cdot X \approx (t' \parallel^q \mathbf{rec}X\,.\,c \cdot X) \parallel^p \mathbf{rec}X\,.\,b \cdot X$ holds, then there exists some $(p \cdot q)$-bisimulation relating t and t'.

Lemma 4.3 *Given arbitrary processes t, t', arbitrary values $0 < p, q < 1$, and any pair of actions $b, c \in Act \setminus (\{\tau\} \cup actions(t) \cup actions(t'))$, it holds that:*

$$(t \parallel^q \mathbf{rec}\,X.\,c \cdot X) \parallel^p \mathbf{rec}\,X.\,b \cdot X \approx (t' \parallel^q \mathbf{rec}\,X.\,c \cdot X) \parallel^p \mathbf{rec}\,X.\,b \cdot X$$

implies

$$t \sim_{p \cdot q} t' \textit{ for some } (p \cdot q)\textit{-bisimulation } \sim_{p \cdot q}$$

Proof.

First of all let us prove the following lemma.

Lemma 4.4 *For each pair of processes $s \approx s'$ such that s is reachable from $(t \parallel^q \mathbf{rec}\,X.\,c{\cdot}X) \parallel^p \mathbf{rec}\,X.\,b{\cdot}X$ and s' is reachable from $(t' \parallel^q \mathbf{rec}\,X.\,c{\cdot}X) \parallel^p \mathbf{rec}\,X.\,b{\cdot}X$, for each action $\alpha \in Act$, and for each equivalence class $C \in \mathcal{S}/\approx$, it holds that $|\mu_G(s, \alpha, C) - \mu_G(s', \alpha, C)| \leq p^2 \cdot q^2$.*

Proof. Let us note that s has the form $(t_1 \parallel^q \mathbf{rec}\,X.\,c{\cdot}X) \parallel^p \mathbf{rec}\,X.\,b{\cdot}X$ and s' has the form $(t_2 \parallel^q \mathbf{rec}\,X.\,c \cdot X) \parallel^p \mathbf{rec}\,X.\,b \cdot X$, for some t_1 and t_2. We can distinguish four cases:

(i) $\alpha = a$, with $a \in Act \setminus \{b, c, \tau\}$.

Let p_1 and p_2 be the values such that $p_1 = \mu_G(s, a, C)$ and $p_2 = \mu_G(s', a, C)$. We have to prove that $|p_1 - p_2| \leq p^2 \cdot q^2$. The thesis is immediate if $p_1 = p_2$. If $p_1 \neq p_2$, then w.l.o.g. we can assume that $p_1 > p_2$. Now, $p_1 = \mu_G(s, a, C)$ implies $\mu_G(s, \tau^* a \tau^*, C) \geq p_1$. Since $s \approx s'$ we infer that $\mu_G(s', \tau^* a \tau^*, C) \geq p_1$. Since $p_1 > p_2 = \mu_G(s', a, C)$, we infer that $\mu_G(s', \tau^+ a \tau^*, C) + \mu_G(s', a\tau^+, C)$ $\geq (p_1 - p_2)$, where τ^+ denotes the set of all the sequences of $n \geq 1$ τ-actions. Since $a \neq b$ and $a \neq c$, processes in C can be reached from s' by sequences $\tau^+ a \tau^*$ and $a \tau^+$ only through at least two moves by t_2. This implies that

$\mu_G(s', \tau^+ a \tau^*, C) + \mu_G(s', a\tau^+, C) \leq p^2 \cdot q^2$. Summarizing, $p^2 \cdot q^2 \geq p_1 - p_2$, and the thesis is proved.

(ii) $\alpha = b$.

Since $b \notin \mathit{actions}(t) \cup \mathit{actions}(t')$, the only b move by s is due to $\mathbf{rec}\, X.\, b \cdot X$ and leads to s itself, and, analogously, the only b move by s' is due to $\mathbf{rec}\, X.\, b \cdot X$ and leads to s' itself. Hence, either C contains neither s nor s', and the thesis is immediate since $\mu_G(s, b, C) = 0 = \mu_G(s', b, C)$, or C contains both s and s'. Let us concentrate on the second case. Since $t_1 \parallel^q \mathbf{rec} X.\ c \cdot X$ moves, it cannot happen that the probability of the b-move by $\mathbf{rec}\, X.\, b \cdot X$ is 1, we are sure that this b move has probability $1 - p$, and, therefore, $\mu_G(s, b, C) = 1 - p$. For the same reason we infer that $\mu_G(s', b, C) = 1 - p$. Summarizing, $\mu_G(s, b, C) = \mu_G(s', b, C)$, and the thesis is proved.

(iii) $\alpha = c$.

Let p_1 and p_2 be the values such that $p_1 = \mu_G(s, c, C)$ and $p_2 = \mu_G(s', c, C)$. Since $c \notin \mathit{actions}(t) \cup \mathit{actions}(t')$, the only c move by s is due to $\mathbf{rec}\, X.\, c \cdot X$ and leads to s itself, and, analogously, the only c move by s' is due to $\mathbf{rec}\, X.\, c \cdot X$ and leads to s' itself. Hence, either C contains neither s nor s', and the thesis is immediate since $\mu_G(s, c, C) = 0 = \mu_G(s', c, C)$, or C contains both s and s'. Let us concentrate on the second case. It holds that either $p_1 = p \cdot (1 - q)$, if t_1 has some move, or $p_1 = p$, if t_1 has no move. Moreover, either $p_2 = p \cdot (1 - q)$, if t_2 has some move, or $p_2 = p$, if t_2 has no move. Therefore, it suffices to prove that it cannot happen that t_1 moves and t_2 does not to infer that either $p_1 = p \cdot (1 - q) = p_2$ or $p_1 = p = p_2$, which implies the thesis.

By contradiction, let us assume that t_1 moves and t_2 does not. Since t_2 does not move, s' has only one b move with probability $1 - p$ and only one c move with probability p. Since $s \approx s'$, we infer that s has only moves in $\{b, c, \tau\}$, thus implying that t_1 has τ moves. This implies that the overall probability of sequences $\tau^* b \tau^*$ by s is strictly greater than $1 - p$, which contradicts that $s \approx s'$.

(iv) $\alpha = \tau$.

First of all let us note that, since $s \approx s'$, either C contains both s and s', or C contains neither s nor s'. If C contains neither s nor s', we can reason as in case (i).

Let us assume that C contains both s and s'. In this case, let p_1 and p_2 be the values such that $p_1 = \mu_G(s, \tau, C)$ and $p_2 = \mu_G(s', \tau, C)$. We have to prove that $|p_1 - p_2| \leq p^2 \cdot q^2$. The thesis is immediate if $p_1 = p_2$. If $p_1 \neq p_2$, then w.l.o.g. we can assume that $p_1 > p_2$. First of all let us note that, since each state $\hat{s}$ reachable from s or s' can perform the c move, it cannot happen that $\hat{s} \xrightarrow{b,1} \hat{s}$, and, therefore, we are sure that $\hat{s} \xrightarrow{b,1-p} \hat{s}$. Since both s and the processes in C reachable through one τ move from s (with total probability p_1) can perform b with probability $1 - p$ while remaining in C, it holds that $\mu_G(s, \tau^* b \tau^*, C) \geq (1 - p) + p_1 \cdot (1 - p)$. Since $s \approx s'$, it holds that $\mu_G(s', \tau^* b \tau^*, C) \geq (1 - p) + p_1 \cdot (1 - p)$. Since states in C cannot perform b with probability 1, we know that $\mu_G(s', b, C) = (1-p)$ and $\sum_{m+n=1} \mu_G(s', \tau^m b \tau^n, C) = p_2 \cdot (1-p)$. Hence, $\sum_{m+n\geq 2} \mu_G(s', \tau^m b \tau^n, C) \geq (p_1 - p_2)(1-p)$. Moreover, we know that $\sum_{m+n\geq 2} \mu_G(s', \tau^m b \tau^n, C) \leq p^2 \cdot q^2 \cdot (1-p)$, since $\tau^m b \tau^n$ with $m+n \geq 2$ requires at least two moves by t_2 and one move from $\mathbf{rec}\, X.\, b \cdot X$. Summarizing, $p^2 \cdot q^2 \cdot (1-p) \geq (p_1 - p_2) \cdot (1-p)$, which implies $p^2 \cdot q^2 \geq p_1 - p_2$, and the thesis is proved.

□

Lemma 4.4 implies that there is a $(p^2 \cdot q^2)$-bisimulation relating processes reachable from $(t \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X$ and $(t' \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X$ and that contains the pair formed by $(t \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X$ and $(t' \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X$. Let $\sim_{p^2 \cdot q^2}$ denote such a $(p^2 \cdot q^2)$-bisimulation.

Let us take any equivalence class $C \in \mathcal{S} / \sim_{p^2 \cdot q^2}$. We prove below that the set of processes $\hat{C} = \{s \text{ such that } (s \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X \in C\}$ are an equivalence class of a $(p \cdot q)$-bisimulation relating processes reachable from t and t'. Let $\sim_{p \cdot q}$ denote such a $(p \cdot q)$-bisimulation. Relations $\sim_{p \cdot q}$ equates t and t', since $(t \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X$ and $(t' \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X$ are equated by $\sim_{p^2 \cdot q^2}$. The thesis follows from $t \sim_{p \cdot q} t'$.

Hence, it remains to prove that $\hat{C} \in \mathcal{S} / \sim_{p \cdot q}$ for some $(p \cdot q)$-bisimulation $\sim_{p \cdot q}$. Given arbitrary processes $t_1, t_2 \in \hat{C}$, any equivalence class $\hat{D}$, and any action $\alpha \in \mathit{actions}(t_1) \cup \mathit{actions}(t_2)$, the semantics of $\parallel^p$ and $\parallel^q$ implies that:
$\mu_G(t_1, \alpha, \hat{D}) = \frac{1}{p \cdot q} \cdot \mu_G((t_1 \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X, \alpha, D)$,
$\mu_G(t_2, \alpha, \hat{D}) = \frac{1}{p \cdot q} \cdot \mu_G((t_2 \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^q \mathbf{rec}\, X.\, b \cdot X, \alpha, D)$.
Since $(t_1 \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X \sim_{p^2 \cdot q^2} (t_2 \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X$, we are sure that $|\mu_G((t_1 \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X, \alpha, D) - \mu_G((t_2 \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X), \alpha, D)| \leq p^2 \cdot q^2$. Therefore, $|\mu_G(t_1, \alpha, \hat{D}) - \mu_G(t_2, \alpha, \hat{D})| \leq p \cdot q$, as required. □

At first glance, our choice of using a context with two occurrences of the interleaving operator in Lemma 4.3 could be surprising. One could expect that a context with only one of these occurrences suffices. The point is that the proof of Lemma 4.4 does not work if we consider the context $\_ \parallel^p \mathbf{rec} X\, .\, b \cdot X$ instead of $(\_ \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X$. In fact, both in the proof of case $\alpha = b$, and in the proof of the case $\alpha = \tau$, we exploit the fact that the probability of the b move by $\mathbf{rec}\, X.\, b \cdot X$ cannot be 1. This is implied by the fact that $\mathbf{rec}\, X.\, c \cdot X$ can perform the c move. Without process $\mathbf{rec}\, X.\, c \cdot X$, the process on the left side of $\parallel^p$ could be a process without any move, and the b move by $\mathbf{rec}\, X.\, b \cdot X$ could have probability 1.

Notice that Lemma 4.3 above holds also if we replace the interleaving operations $\parallel^p$ and $\parallel^q$ with the CCS-like parallel composition operations $\parallel^p_{p'}$ and $\parallel^q_{q'}$ of [7,10], provided that t and t', besides performing neither b nor c, perform neither $\overline{b}$ nor $\overline{c}$. Moreover, Lemma 4.3 holds also if we replace $\parallel^p$ and $\parallel^q$ with the CSP-like parallel composition operations $\parallel^p_A$ and $\parallel^q_A$ of [10], with $A = \emptyset$.

Let us prove now that processes related by p-bisimulations for all $0 < p < 1$ are strong bisimilar.

Lemma 4.5 *Given processes t and t', if for each $0 < p < 1$ there exists a p-bisimulation $\sim_p$ such that $t \sim_p t'$, then it holds that $t \sim t'$.*

Proof. Since the regularity condition ensures that the number of states reachable from t and t' is finite, there exists an equivalence relation $\mathcal{R}$ over the states reachable from t and t' such that $(t, t') \in \mathcal{R}$ and such that, given any $\delta > 0$, $\mathcal{R}$ is an ϵ-bisimulation for infinite many $\delta > \epsilon > 0$. We can prove that $\mathcal{R}$ is a strong bisimulation. By contradiction, let us assume that $\mathcal{R}$ is not a strong bisimulation. Then, there exists a pair of states $(s, s') \in \mathcal{R}$, an action $\alpha \in Act$, and an equivalence class C over $\mathcal{R}$ such that $\mu_G(s, \alpha, C) \neq \mu_G(s', \alpha, C)$. Let d be the value $|\mu_G(s, \alpha, C) - \mu_G(s', \alpha, C)|$. It follows that $\mathcal{R}$ is not an ϵ-bisimulation for any $\epsilon < d$, which contradicts that $\mathcal{R}$ is an ϵ-bisimulation for infinite many $d > \epsilon > 0$. Now, since $\mathcal{R}$ is a bisimulation and $(t, t') \in \mathcal{R}$, the thesis holds. □

We can give now our main result.

Theorem 4.6 *Given arbitrary processes t and t', if for all $0 < p, q < 1$ and actions $b, c \in Act \backslash (\{\tau\} \cup actions(t) \cup actions(t'))$ it holds that $(t \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X \approx (t' \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X$ then it follows that $t \sim t'$.*

Proof. By Lemma 4.3, for each $0 < p, q < 1$, it holds that $t \sim_{p \cdot q} t'$ for some $(p \cdot q)$-bisimulation $\sim_{p \cdot q}$. Given any $0 < d < 1$, we can choose $p = q = \sqrt{d}$, to infer that $t \sim_d t'$. Since $t \sim_d t'$ for all $0 < d < 1$, we can apply Lemma 4.5 to infer $t \sim t'$, and the proof is complete. □

Let us assume that $\mathcal{R}$ is an equivalence relation over processes being a congruence w.r.t interleaving, prefixing and recursion, and being finer than weak bisimulation (i.e. $\mathcal{R} \subset \approx$). Given processes t and t' such that $(t, t') \in \mathcal{R}$, since $\mathcal{R}$ is a congruence, we infer that, for all $0 < p, q < 1$, $((t \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X, (t' \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X) \in \mathcal{R}$. Since $\mathcal{R} \subset \approx$, we infer $(t \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X \approx (t' \parallel^q \mathbf{rec}\, X.\, c \cdot X) \parallel^p \mathbf{rec}\, X.\, b \cdot X$. Thm. 4.6 implies that $t \sim t'$. Hence, $\mathcal{R} \subseteq \sim$. Since $\sim$ is a congruence w.r.t. interleaving, prefixing and recursion, we infer that $\sim$ is the coarsest congruence contained in $\approx$ that is a congruence w.r.t. these operations.

5 Conclusions

We have proved that, if one considers process algebras giving rise to GPTSs satisfying the regularity condition and offering recursion, interleaving and prefixing, then strong bisimulation is the coarsest congruence contained in weak bisimulation. This differentiates the generative probabilistic model not only with respect to the non-probabilistic case, where interesting congruences strictly lying between strong and weak bisimulation have been studied [6,13,14,15,17], but also with respect to the non-alternating model, where the coarsest congruence being finer than weak bisimulation has been characterized and proved to be coarser than strong bisimulation [2,11,12].

Analogies between the nonprobabilistic and the non-alternating model arise since in the non-alternating model process algebras offer parallel composition operations and a nondeterministic choice operation having the same nature of those of non-probabilistic process algebras. To support this observation the fact that the axiomatization of the coarsest congruence being finer than weak bisimulation requires rules similar to Milner's "expansion law" to manage parallel composition [12] and rules similar to Milner's "τ-law" to manage τ prefixing [2,11,12].

In the generative model, no operation introducing nondeterminism is allowed. Therefore one cannot hope to treat parallel composition operations as in the non-probabilistic case. Asynchronous parallel composition operations require parameters specifying the probability to move of each of the processes running in parallel. These parametric operations do not preserve weak bisimulation, since they distinguish $\tau^m \cdot t_1$ and $\tau^n \cdot t_1$, when $m \neq n$. In fact, when we compose in parallel $\tau^m \cdot t_1$ with another process t_2, the τ actions of $\tau^m \cdot t_1$ imply that actions of t_1 can be performed only after $\tau^m \cdot t_1$ has won m competitions versus t_2 to perform the m occurrences of τ, and each of these competitions is not for free, meaning that the probability of winning it is not 1 but depend on the parameter of the operation. The ability of discriminating $\tau^m \cdot t_1$ and $\tau^n \cdot t_1$ has as a consequence that there is no congruence strictly lying between strong and weak bisimulation.

Checking whether our result holds also for GPTSs that do not satisfy the regularity condition, and for transition systems respecting the reactive and stratified models of probabilistic processes could be interesting developments of the present notes.

References

[1] A. Aldini, M. Bravetti, and R. Gorrieri: A Process-algebraic Approach for the Analysis of Probabilistic Non-interference. J. Comput. Secur. 12(2), 2004, 191–245.

[2] E. Bandini and R. Segala: Axiomatizations for Probabilistic Bisimulation. Proc. Int. Coll. on Automata, Languages and Programming, Lecture Notes in Computer Science 2076, Springer, Berlin, 2001, 370–381.

[3] J. C. M. Baeten, J. A. Bergstra, and S. A. Smolka: Axiomatizing Probabilistic Processes: ACP with Generative Probabilities. Inf. Comput. 121(2), 1995, 234–255.

[4] J. C. M. Baeten and W. P. Weijland: Process Algebra. Cambridge Tracts in Theoretical Computer Science 18, Cambridge University Press, 1990.

[5] C. Baier and H. Hermanns: Weak Bisimulation for Fully Probabilistic Processes. Proc. Int. Conf. on Computer Aided Verification, Lecture Notes in Computer Science 1254, Springer, Berlin, 1997, 119–130.

[6] B. Bloom: Structural Operational Semantics for Weak Bisimulation. Theor. Comput. Sci. 146(1–2), 1995, 25–68.

[7] M. Bravetti and A. Aldini: Discrete Time Generative-reactive Probabilistic Processes with Different Advancing Speeds. Theor. Comput. Sci. 290(1), 2003, 355–406.

[8] I. Christoff: Testing Equivalences and Fully Abstract Models for Probabilistic Processes. Proc. Int. Conf. on Concurrency Theory, Lecture Notes in Computer Science 458, Springer, Berlin, 1990, 126–140.

[9] R. Cleaveland, S. A. Smolka, and A. Zwarico: Testing Preorders for Probabilistic Processes. Proc. Int. Colloquium on Automata, Languages and Programming, Lecture Notes in Computer Science 623, Springer, Berlin, 1992, 708–719.

[10] P. R. D'Argenio, H. Hermanns, and J. P. Katoen: On Generative Parallel Composition. Proc. Int. Work. on Probabilistic Methods in Verification, Electr. Notes Theor. Comput. Sci. 22, Elsevier, Amsterdam, 1999.

[11] Y. Deng and C. Palamidessi: Axiomatizations for Probabilistic Finite-State Behaviors. Proc. Int. Conf. on Foundations of Software Science and Computational Structures, Lecture Notes in Computer Science 3441, Springer, Berlin, 2005, 110–124.

[12] Y. Deng, C. Palamidessi, and J. Pang: Compositional Reasoning for Probabilistic Finite-State Behaviors. In Processes, Terms and Cycles: Steps on the Road to Infinity, Essays Dedicated to Jan Willem Klop, on the Occasion of His 60th Birthday, Lecture Notes in Computer Science 3838, Springer, Berlin, 2005, 309–337.

[13] W. J. Fokkink: Rooted Branching Bisimulation as a Congruence. J. Comput. Syst. Sci. 60(1), 2000, 13–37.

[14] W. J. Fokkink, R. J. van Glabbeek, and P. de Wind: Divide and Congruence Applied to Eta-bisimulation. Proc. Workshop on Structural Operational Semantics, Electr. Notes Theor. Comput. Sci. 156(1), Elsevier, Amsterdam, 2005, 97–113.

[15] W. J. Fokkink, R. J. van Glabbeek, and P. de Wind: Divide and Congruence: From Decomposition of Modalities to Preservation of Branching Bisimulation. Proc. Int. Symp. on Formal Methods for Components and Objects, Lecture Notes in Computer Science 4111, Springer, Berlin, 2005.

[16] A. Giacalone, C. C. Jou, and S. A. Smolka: Algebraic Reasoning for Probabilistic Concurrent Systems. Proc. IFIP Work. Conf. on Programming, Concepts and Methods, 1990, 443–458.

[17] R. J. van Glabbeek: On Cool Congruence Formats for Weak Bisimulations. Proc. Int. Colloquium on Theoretical Aspects of Computing, Lecture Notes in Computer Science 3722, Springer, Berlin, 2005, 331–346.

[18] R. J. van Glabbeek, S. A. Smolka, and B. Steffen: Reactive, Generative and Stratified Models of Probabilistic Processes. Inf. Comput. 121(1), 1995, 59–80.

[19] H. Hansson and B. Jonsson: A Framework for Reasoning about Time and Reliability. Proc. IEEE Real-Time Systems Symposium, IEEE Press, 1989, 102-111.

[20] B. Jonsson and K. G. Larsen: Specification and Refinement of Probabilistic Processes. Proc. IEEE Symp. on Logic in Computer Science, IEEE Press, 1991, 266–277.

[21] B. Jonsson, K. G. Larsen, and W. Yi: Probabilistic Extensions of Process Algebras. Handbook of Process Algebra, Elsevier, Amsterdam, 2001.

[22] B. Jonsson and W. Yi: Compositional Testing Preorders for Probabilistic Processes. Proc. IEEE Symp. on Logic in Computer Science, IEEE Press, 1995, 431–443.

[23] C. C. Jou and S. A. Smolka: Equivalences, Congruences and Complete Axiomatizations for Probabilistic Processes. Proc. Int. Conf. on Concurrency Theory, Lecture Notes in Computer Science 458, Springer, Berlin, 1990, 367–383.

[24] R. Lanotte and S. Tini: Probabilistic Congruence for Semistochastic Generative Processes. Proc. Int. Conf. on Foundations of Software Science and Computational Structures, Lecture Notes in Computer Science 3441, Springer, Berlin, 2005, 63–78.

[25] K. G. Larsen and A. Skou: Bisimulation Trough Probabilistic Testing. Inf. Comput. 94(1), 1991, 1–28.

[26] R. Milner: Communication and Concurrency. Prentice Hall, London, 1989.

[27] G. Plotkin: A Structural Approach to Operational Semantics. Tech. Rep. DAIMI FN-19, University of Aarhus, 1981.

[28] G. Plotkin: A Structural Approach to Operational Semantics. J. Log. Algebr. Program. 60–61, 2004, 17–139.

[29] R. Segala: Modeling and Verification of Randomized Distributed Real-Time Systems. PhD Thesis, MIT, Technical Report MIT/LCS/TR-676, 1995.

[30] R. Segala and N. Lynch: Probabilistic Simulations for Probabilistic Processes. Proc. Int. Conf. on Concurrency Theory, Lecture Notes in Computer Science 836, Springer, Berlin, 1994, 481–496.

[31] E. W. Stark and S. A. Smolka: A Complete Axiom System for Finite-State Probabilistic Processes. In Proof, Language and Interaction: Essays in Honor of Robin Milner, G. Plotkin, C.P. Stirling, and M. Tofte, Eds., MIT Press, 1999.

[32] S. Yuen, R. Cleaveland, Z. Dayar, and S. A. Smolka: Fully Abstract Characterizations of Testing Preorders for Probabilistic Processes. Proc. Int. Conf. on Concurrency Theory, Lecture Notes in Computer Science 863, Springer, Berlin, 1994, 497–512.