Acta Informatica manuscript No.
(will be inserted by the editor)

Tomáš Brázdil · Antonín Kučera · Oldřich Stražovský

Deciding Probabilistic Bisimilarity over Infinite-State Probabilistic Systems

Received: date / Revised: date

Abstract We prove that probabilistic bisimilarity is decidable over probabilistic extensions of BPA and BPP processes. For normed subclasses of probabilistic BPA and BPP processes we obtain polynomial-time algorithms. Further, we show that probabilistic bisimilarity between probabilistic pushdown automata and finite-state systems is decidable in exponential time. If the number of control states in PDA is bounded by a fixed constant, then the algorithm needs only polynomial time.

1 Introduction

Theory of probabilistic systems is a formal basis for modeling and verification of systems that exhibit some kind of uncertainty [29,27]. For example, this uncertainty can be caused by unpredictable errors (such as message loss in unreliable channels), randomization (as in randomized algorithms), or simply underspecification in some of the system components. The semantics of probabilistic systems is usually defined in terms of homogeneous Markov chains or Markov decision processes. The former model allows to specify just probabilistic behavioural aspects, while the latter one combines the paradigms of nondeterministic and probabilistic choice. The underlying semantic model used in this paper are *probabilistic transition systems (pTS)* [33] which subsume both of the aforementioned formalisms and also "ordinary" non-probabilistic transition systems. A simple pTS is shown in Fig. 1. It has three states s,t,u, two actions a,b, and four transitions $s \to \mu$, $s \to \nu$, $t \to \theta$, and $u \to \kappa$. At each state, one of the outgoing transitions is chosen non-deterministically (in Fig. 1, there is a non-deterministic choice only

The work has been supported by the research centre Institute for Theoretical Computer Science (ITI), project No. 1M0545.

T. Brázdil · A. Kučera · O. Stražovský
Faculty of Informatics, Masaryk University, Botanická 68a, 60200 Brno, Czech Republic
E-mail: {brazdil,kucera,strazovsky}@fi.muni.cz

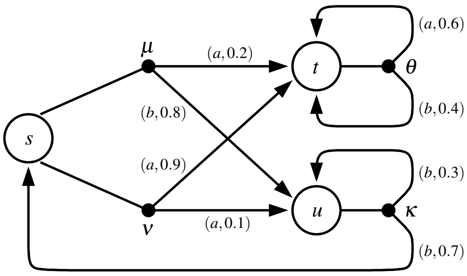

Fig. 1 A simple probabilistic transition system.

between $s \longrightarrow \mu$ and $s \longrightarrow \nu$). A given transition is then "performed" in a probabilistic fashion. For example, if the transition $s \longrightarrow \mu$ is chosen, then the states t and u are entered with the probability 0.2 and 0.8, and the actions a and b are emitted, respectively. Generally, a pTS can have finitely or countably many states, and each state can have zero or more (but at most countably many) outgoing transitions.

Methods for formal verification of probabilistic systems follow the two standard approaches of *model-checking* and *equivalence-checking*. In the model-checking approach, desired properties of the system are specified as a formula of a suitable probabilistic temporal logic (such as PCTL or PCTL* [11]), and then it is shown that the system satisfies the formula. In the equivalence-checking approach, one proves that the verified system is semantically equivalent to its *specification*, which is another probabilistic system. Here the notion of semantic equivalence can be formally captured in many ways. Most of the existing equivalences are probabilistic extensions of their non-probabilistic counterparts. One consequence of this is that various variants of *probabilistic bisimilarity* [30] play a very important role in this setting.

The state of the art: Algorithmic support for formal verification of probabilistic systems has so far been limited to finite-state systems [16,23,6,17,25, 10,29,5,15]. Only recently, model-checking algorithms for infinite-state models of fully probabilistic lossy channel systems [26,9,1,4,31,2,3,8,13], fully probabilistic pushdown automata [18,19,12], and recursive Markov chains [22,20,21] appeared. However, the authors are not aware of any results about equivalence-checking with probabilistic infinite-state systems.

Our Contribution: In the first part of our work we consider probabilistic extensions of the well-known families of BPA and BPP processes, which are denoted pBPA and pBPP, respectively. We have chosen a general extension based on the idea that process constants have finitely many basic transitions of the form $X \longrightarrow \mu$ where μ is a probability distribution over pairs of the form (a, α), where a is an action and α a sequence of BPA/BPP constants (in the case of BPP, sequences of constants are considered modulo commutativity and thus the concatenation operator models a simple form of parallel composition without synchronization). Basic transitions then define transitions performable from sequences of constants by adjusting the target distributions accordingly. Hence, our model subsumes the original (non-probabilistic) BPA and BPP, which can be understood as those subclasses of pBPA and pBPP where all distributions used in basic transitions are Dirac. Moreover, pBPA also subsumes a fully probabilistic extension of BPA. We prove that probabilistic bisimilarity (both in its combined and non-combined variant) is decidable for pBPA and pBPP processes. Moreover, for normed subclasses of pBPA and pBPP we have polynomial-time algorithms. Our results generalize the ones for non-probabilistic BPA and BPP by extending and adapting the original notions and proofs. Intuitively, such an extension is possible because probabilistic bisimilarity has similar algebraic and transfer properties as "ordinary" non-probabilistic bisimilarity. These properties can be reformulated and reproved in the probabilistic setting by incorporating some ideas for finite-state systems (e.g., the use of geometrical algorithms for finitely-generated convex spaces in the style of [15]), and there are also new techniques for handling problems which are specific to infinite-state probabilistic systems. After reestablishing these crucial properties, we can basically follow the original proofs because they mostly rely just on algebraic arguments. This can be seen as a nice evidence of the robustness of the original ideas.

In Section 5 we concentrate on checking probabilistic bisimilarity between processes of probabilistic pushdown automata (pPDA) and probabilistic finite-state automata. Our results are based on a generic method for checking semantic equivalences between PDA and finite-state processes proposed in [28]. This method clearly separates generic arguments (applicable to every behavioral equivalence which is a right PDA congruence in the sense of Definition 8) from the equivalence-specific parts that must be supplied for each behavioral equivalence individually. This method works also in the probabilistic setting, but the application part would be unnecessarily long and complicated if we used the original scheme of [28]. Therefore, the generic part of the method is first adjusted into a more "algebraic" form which simplifies some of the crucial steps. The method is then used to prove that probabilistic bisimilarity is decidable between pPDA and finite-state processes in exponential time. Actually, this algorithm is *polynomial* if the number of pPDA control states is bounded by a fixed constant (in particular, this holds for pBPA).

For the sake of completeness, we also included proofs which are the same (or similar) as in the non-probabilistic setting. These parts are always clearly marked in text. Thus, the paper becomes self-contained and should be understandable even for a reader who is not familiar with the results on BPA, BPP, and PDA presented in [14,28]. The only exception is Section 4.3 where we just indicate how to modify the polynomial-time algorithms for checking non-probabilistic bisimilarity over normed BPA and normed BPP so that they work also for normed pBPA and normed pBPP. The reason is that the functionality of the required modifications is in fact explained in Section 4 and hence one can easily follow the original presentation in [14].

The results presented in this paper generate many questions. Some of them are summarized in Section 6.

2 Basic Definitions

In the rest of this paper we use the symbols $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{R}$, and $\mathbb{R}^{\geq 0}$ to denote the sets of positive integers, non-negative integers, real numbers, and non-negative real numbers, respectively. If $R \subseteq A \times A$ is a binary relation on A, then $\equiv_R$ denotes the least equivalence on A that includes R.

A *discrete probability measure* (or *distribution*) over a finite or countably infinite set X is a function $\mu : X \to \mathbb{R}^{\geq 0}$ such that $\sum_{x \in X} \mu(x) = 1$. The set of all distributions over X is denoted $Disc(X)$. A *Dirac* distribution is a distribution which assigns 1 to exactly one object. A *rational* distribution is a distribution which assigns a rational number to each object. For every $\mu \in Disc(X)$ we define its *support*, denoted $supp(\mu)$, as the set $\{x \in X \mid \mu(x) > 0\}$. A *discrete probability space* is a pair (X, μ) where X is a set called *sample space* and μ a distribution over X.

2.1 Probabilistic Transition Systems

The underlying semantics of probabilistic systems is usually defined in terms of labelled Markov chains or labelled Markov decision processes, depending mainly on whether the considered system is sequential or parallel. Since some of our results are applicable to both sequential and parallel probabilistic systems, we use a more general formalism of [33] which subsumes the aforementioned models.

Definition 1 A *probabilistic transition system (pTS)* is a triple $\mathscr{S} = (S, Act, D)$ where S is a finite or countably infinite set of *states*, $Act \neq \emptyset$ is a set of *actions*, and $D \subseteq S \times Disc(Act \times S)$ is a finite or countably infinite *transition relation*. An element $(s, \mu) \in D$ is called a *transition* and alternatively denoted by $s \to \mu$.

We say that $t \in S$ is *reachable from $s \in S$ under a word $w = a_1 \cdots a_k \in Act^*$*, written $s \xrightarrow{w} t$ (or simply $s \to^* t$ if w is irrelevant), if there is a finite sequence $s = s_0, \cdots, s_k = t$ of states such that for every $0 \leq i < k$ there is $(s_i, \mu_i) \in D$ such that $\mu_i(a_{i+1}, s_{i+1}) > 0$.

A state s is *finitely-branching* if the set $\{\mu \mid s \to \mu\}$ is finite. A state s is *totally finitely-branching (tfb)* iff each state reachable from s is finitely-branching. The subset of all $s \in S$ that are tfb is denoted *tfb*(S).

For the rest of this section, let us fix a pTS $\mathscr{S} = (S, Act, D)$.

For each transition $s \to \mu$ we define the set of μ-successors of s by $succ(s, \mu) = \{t \in S \mid \mu(a, t) > 0 \text{ for some } a \in Act\}$. For each state s we define the set of its successors by $succ(s) = \bigcup_{s \to \mu} succ(s, \mu)$. For every $s \in S$, let $D(s) = \{(s, \mu) \in D\}$ be the set of its outgoing transitions. Every distribution $\sigma \in Disc(D(s))$ determines a unique distribution $\mu_\sigma \in Disc(Act \times S)$ defined for each $(a, t) \in Act \times S$ as $\mu_\sigma(a, t) = \sum_{(s,\mu) \in D(s)} \sigma(s, \mu)\mu(a, t)$. Note that the sum $\sum_{(s,\mu) \in D(s)} \sigma(s, \mu)\mu(a, t)$ exists because the set $D(s)$ is finite or countably infinite. A *combined transition relation* $D_C \subseteq S \times Disc(Act \times S)$ is defined by $D_C = \{(s, \mu_\sigma) \mid s \in S, \sigma \in Disc(D(s))\}$. We write $s \to_C \mu$ instead of $(s, \mu) \in D_C$. Obviously, introducing combined transitions does not influence the reachability relation. However, a single state can have uncountably many outgoing combined transitions. Therefore, the triple (S, Act, D_C) cannot be generally seen as a pTS in the sense of Definition 1.

2.2 Probabilistic Bisimilarity

Semantic equivalence of probabilistic processes can be formally captured in many ways. Existing approaches extend the ideas originally developed for non-probabilistic processes, and the resulting notions have similar properties as their

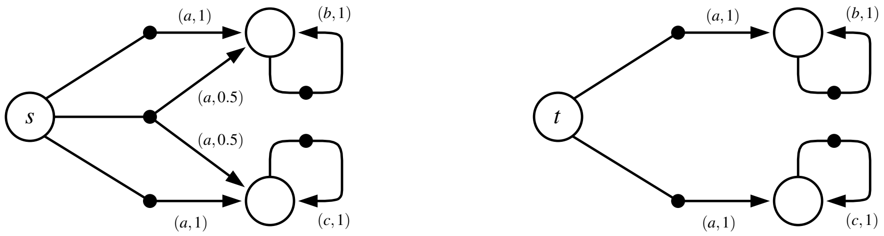

Fig. 2 A counterexample demonstrating that $\approx \not\subseteq \sim$. Note that $s \approx t$ but $s \not\sim t$.

non-probabilistic counterparts. One consequence of this is that probabilistic extensions of *bisimulation-like equivalences* play a very important role in this setting.

First we introduce some useful notions and notation. For the rest of this section, let us fix a pTS $\mathscr{S} = (S,Act,D)$. Let $E \subseteq S \times S$ be an equivalence relation. We say that two distributions $\mu, \nu \in Disc(Act{\times}S)$ are *equivalent according to* E, denoted $\mu E \nu$, iff for each $a \in Act$ and each equivalence class $C \in S/E$ we have that $\mu(a,C) = \nu(a,C)$, where $\mu(a,C) = \sum_{s \in C} \mu(a,s)$. In other words, the equivalence E (defined on states) determines a unique equivalence on distributions that is also denoted by E (sometimes we write $(\mu,\nu) \in E$ instead of $\mu E \nu$).

Definition 2 Let E be an equivalence on S, and let $(s,t) \in S \times S$. We say that the pair (s,t) *expands* in E iff

- for each $s \to \mu$ there is $t \to \nu$ such that $\mu E \nu$;
- for each $t \to \mu$ there is $s \to \nu$ such that $\mu E \nu$.

A relation $R \subseteq S \times S$ expands in E iff each $(s,t) \in R$ expands in E. An equivalence E on S is a *probabilistic bisimulation* iff E expands in E. We say that $s,t \in S$ are *bisimilar*, written $s \sim t$, iff they are related by some probabilistic bisimulation.

The notions of *combined expansion*, *combined bisimulation*, and *combined bisimilarity* (denoted $\approx$), are defined in the same way as above, using $\to_C$ instead of $\to$.

In general, probabilistic bisimilarity is a proper refinement of combined probabilistic bisimilarity (a simple example is given in Fig. 2). We refer to [33] for a more detailed comparison of these two equivalences. Since most of our results are valid for both of these equivalences, we usually refer just to “bisimilarity” and use the $\twoheadrightarrow$ and $\simeq$ symbols to indicate that a given construction works both for $\to$ and $\sim$, and for $\to_C$ and $\approx$, respectively. The word “expansion” is also overloaded in the rest of this paper.

Lemma 1 $\simeq$ *is a bisimulation.*

Proof Let $s,t \in S$ such that $s \simeq t$. We show that (s,t) expands in $\simeq$. Let $s \twoheadrightarrow \mu$. Since $s \simeq t$, there is a bisimulation E such that $(s,t) \in E$ and hence there is $t \twoheadrightarrow \nu$ such that $\mu E \nu$. We prove that $\mu \simeq \nu$, i.e., $\mu(a,C) = \nu(a,C)$ for every $a \in Act$ and $C \in S/{\simeq}$. Since $E \subseteq \simeq$, for every $C \in S/{\simeq}$ there is finite or countably infinite index set I such that $C_i \in S/E$ for every $i \in I$ and $C = \biguplus_{i \in I} C_i$. As $\mu E \nu$, we have that $\mu(a,C_i) = \nu(a,C_i)$ for every $i \in I$, and hence also $\mu(a,C) = \nu(a,C)$ as needed. □

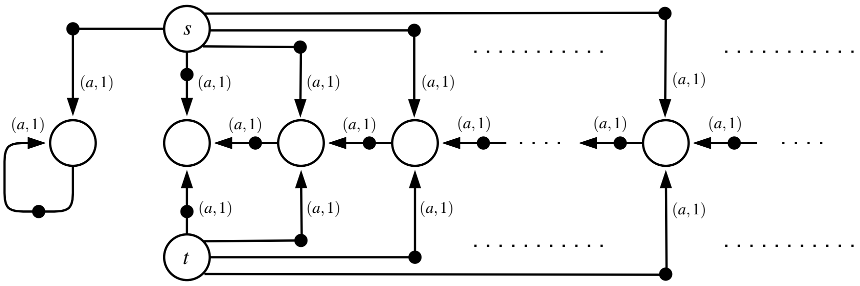

Fig. 3 A counterexample demonstrating $\simeq_\omega \not\subseteq \simeq$. Note that $s \simeq_\omega t$ but $s \not\simeq t$.

3 The Semidecidability of Non-Bisimilarity

The aim of this section is to establish a generic semidecidability result for non-bisimilarity over probabilistic processes. The basic idea is the same as in the non-probabilistic setting. Let us fix a pTS $\mathscr{S} = (S, Act, D)$. We show that bisimilarity can be approximated by an infinite family of equivalences $\simeq_i \subseteq S \times S$, $i \in \mathbb{N}_0$ so that for all $(s,t) \in S \times \mathit{tfb}(S)$ we have that $s \simeq t$ iff $s \simeq_i t$ for all $i \in \mathbb{N}_0$ (note that s does not have to be finitely-branching). This is a generalization of a similar result for non-probabilistic strong bisimilarity presented in [7], but new proof techniques are required to overcome the problem that even a finitely-branching process can have uncountably many outgoing combined transitions. From this we immediately obtain the semidecidability of $\not\simeq$ over $S \times \mathit{tfb}(S)$, assuming that each $\not\simeq_i$ is semidecidable over $S \times \mathit{tfb}(S)$ (see Corollary 1).

Definition 3 For every $i \in \mathbb{N}_0$ we define an equivalence $\simeq_i \subseteq S \times S$ inductively as follows:

- $\simeq_0 = S \times S$;
- $\simeq_{i+1}$ consists of those $(s,t) \in \simeq_i$ which expand in $\simeq_i$.

We also put $\simeq_\omega = \bigcap_{i=0}^{\infty} \simeq_i$.

It is easy to verify that for every $i \in \mathbb{N}_0$ we have that

- $\simeq_i$ is indeed an equivalence;
- $\simeq_{i+1} \subseteq \simeq_i$;
- $\simeq \subseteq \simeq_i$.

This means that $\simeq \subseteq \simeq_\omega$, but the other inclusion does *not* hold in general (the standard counterexample is recalled in Fig. 3).

Before proving the main result of this section, we need to examine the properties of $\simeq_i$ equivalences over *distributions* (see Section 2.2).

Lemma 2 *Let $\mu, \nu \in \mathit{Disc}(Act \times S)$.*

(a) For every $i \in \mathbb{N}_0$ we have that if $\mu \simeq_i \nu$, then also $\mu \simeq_j \nu$ for all $0 \leq j \leq i$.
(b) $\mu \simeq_\omega \nu$ iff $\mu \simeq_i \nu$ for all $i \in \mathbb{N}_0$.

Proof (a) We need to show that $\mu(a,C) = \nu(a,C)$ for all $a \in Act$ and $C \in S/{\simeq_j}$, assuming that this equality holds for all $a \in Act$ and $C \in S/{\simeq_i}$. However, it suffices to realize that each $C \in S/{\simeq_j}$ is a disjoint union of equivalence classes of $S/{\simeq_i}$, i.e., $C = \biguplus_{k \in I} C_k$ where $C_k \in S/{\simeq_i}$ for every $k \in I$ (this is because $\simeq_i$ is a refinement of $\simeq_j$ where $\simeq_i$ and $\simeq_j$ are treated as equivalences on *states*).

(b) The "⇒" direction is proven similarly as (a). For the other direction, let us fix some $\mu, \nu \in Disc(Act \times S)$ such that $\mu \simeq_i \nu$ for all $i \in \mathbb{N}_0$. We need to show that $\mu \simeq_\omega \nu$, which means to verify that $\mu(a,C) = \nu(a,C)$ for all $a \in Act$ and $C \in S/{\simeq_\omega}$. It follows directly from the definition of $\simeq_\omega$ that for every $i \in \mathbb{N}_0$ there is some $C_i \in S/{\simeq_i}$ such that $C = \bigcap_{i \in \mathbb{N}_0} C_i$. Since $\mu \simeq_i \nu$, we have that $\mu(a,C_i) = \nu(a,C_i)$ for every $i \in \mathbb{N}_0$. This means that also $\lim_{i\to\infty} \mu(a,C_i) = \lim_{i\to\infty} \nu(a,C_i)$. Since $C = \bigcap_{i \in \mathbb{N}_0} C_i$, we obtain that $\lim_{i\to\infty} \mu(a,C_i) = \mu(a,C)$ and $\lim_{i\to\infty} \nu(a,C_i) = \nu(a,C)$, and we are done. □

Now we present the main result of this section.

Theorem 1 *For all $(s,t) \in S \times tfb(S)$ we have that $s \simeq t$ iff $s \simeq_\omega t$.*

Proof Let $R = \{(s,t) \in S \times tfb(S) \mid s \simeq_\omega t\}$. We show that $\equiv_R$ is a bisimulation (remember that $\equiv_R$ is the least equivalence that includes R). To achieve that, we use a simple observation that $\equiv_R$ is a bisimulation iff R expands in $\equiv_R$ (the "only if" part is obvious; for the other direction, realize that $(s,t) \in {\equiv_R}$ iff $s = t$ or there is a finite sequence $s{=}u_0, \ldots, u_n{=}t$ of states such that (u_i, u_{i+1}) or (u_{i+1}, u_i) belongs to R for every $0 \leq i < n$. In the first case we are done immediately, and in the second case we use a straightforward induction on n to show that (s,t) expands in $\equiv_R$). Also observe that ${\equiv_R} \subseteq {\simeq_\omega}$ and that each equivalence class of $S/{\equiv_R}$ which contains at least one tfb state is also an equivalence class of $S/{\simeq_\omega}$.

Let $(s,t) \in R$. We show that (s,t) expands in $\equiv_R$. First, we consider the non-combined case:

A1. Let $s \to \mu$. Since $s \sim_\omega t$, there exists a sequence $\nu_0, \nu_1, \ldots$ such that for all $i \in \mathbb{N}_0$ we have that $t \to \nu_i$ and $\mu \sim_i \nu_i$. Since t is finitely branching, there is ν_k such that $\mu \sim_j \nu_k$ for infinitely many indices j. It follows from Lemma 2 (a) that $\mu \sim_i \nu_k$ for *all* $i \in \mathbb{N}_0$ and thus $\mu \sim_\omega \nu_k$ by Lemma 2 (b). We show that $\mu \equiv_R \nu_k$. Since all successors of t are tfb, we have that ν_k assigns a non-zero probability only to those equivalence classes of $S/{\equiv_R}$ which contain at least one tfb state. However, each such equivalence class is also a equivalence class of $S/{\sim_\omega}$ (see above). Therefore, $\mu \equiv_R \nu_k$.

A2. Let $t \to \mu$. Since $s \sim_\omega t$, there exists a sequence $\nu_0, \nu_1, \nu_2, \ldots$ such that for all $i \in \mathbb{N}_0$ we have that $s \to \nu_i$ and $\mu \sim_i \nu_i$. Since t is finitely-branching, for each ν_i there exists $t \to \mu'_i$ such that $\mu'_i \sim_\omega \nu_i$ (see the previous paragraph). The state t is finitely-branching which implies that there is $k \in \mathbb{N}_0$ and an infinite set of indices $M \subseteq \mathbb{N}_0$ such that $\nu_j \sim_\omega \mu'_k$ for all $j \in M$. It follows that $\mu \sim_j \nu_k$ for all $j \in M$ because $\mu \sim_j \nu_j \sim_\omega \mu'_k \sim_\omega \nu_k$. Since M is infinite, it follows from Lemma 2 (a) that $\mu \sim_i \nu_k$ for all $i \in \mathbb{N}_0$ and thus $\mu \sim_\omega \nu_k$ by Lemma 2 (b) which implies $\mu \equiv_R \nu_k$ in the same way as in A1.

Now we consider the combined case:

B1. Let $s \to_C \mu$. The main difference is that now there may be infinitely many different distributions $\nu_0, \nu_1, \ldots$ such that for all $i \in \mathbb{N}_0$ we have that $t \to_C \nu_i$ and $\mu \approx_i \nu_i$. Let k be the branching degree of t, i.e., there are exactly k

different non-combined transitions $t \rightarrow \xi_1, \cdots, t \rightarrow \xi_k$. Then each ν_i is a linear combination of $\xi_1, \cdots, \xi_k$. Suppose that

$$\nu_i = x_1^i \xi_1 + \cdots + x_k^i \xi_k$$

Since $\mu \approx_i \nu_i$, for all $a \in Act$ and $C \in S/{\approx_i}$ we have that $\mu(a,C) = \nu_i(a,C)$. By Lemma 2 (a) we obtain that $\mu \approx_j \nu_i$ for all $0 \leq j \leq i$. This means that for all $a \in Act$, $0 \leq j \leq i$, and $C \in S/{\approx_j}$ we have $\mu(a,C) = \nu_i(a,C)$. Since $\nu_i = x_1^i \xi_1 + \cdots + x_k^i \xi_k$, we further get

$$\mu(a,C) = x_1^i \xi_1(a,C) + \cdots + x_k^i \xi_k(a,C)$$

for all $a \in Act$ and $C \in S/{\approx_j}$, where $0 \leq j \leq i$.
It follows that $(x_1^i, \cdots, x_k^i)$ is a solution of the family F_i of linear equations

$$\mu(a,C) = x_1 \xi_1(a,C) + \cdots + x_k \xi_k(a,C)$$

constructed for all $a \in Act$ and $C \in S/{\approx_j}$ where $0 \leq j \leq i$. Let us note that this family can also have solutions in $\mathbb{R}^k$ which do not correspond to probability distributions, but this does not influence our arguments.
Since $F_i \subseteq F_{i+1}$ and there can be at most k+1 linearly independent linear equations with k variables, there must be some $n \in \mathbb{N}_0$ such that the set of all solutions of F_n is the same as the set of all solutions of $\bigcup_{i \in \mathbb{N}_0} F_i$. Let $\nu_n = y_1 \xi_1 + \cdots + y_k \xi_k$. Then $(y_1, \cdots, y_k)$ is a solution of F_n and hence also a solution of $\bigcup_{i \in \mathbb{N}_0} F_i$, which means that $\mu \approx_\omega \nu_n$ by Lemma 2 (b). From this we get $\mu \equiv_R \nu_n$ as in A1.

B2. Let $t \rightarrow_C \mu$. Since $s \approx_\omega t$, there exists a sequence $\nu_0, \nu_1, \nu_2, \ldots$ such that for all $i \in \mathbb{N}_0$ we have that $s \rightarrow_C \nu_i$ and $\nu_i \approx_i \mu$. Since t is finitely branching, for each ν_i there exists $t \rightarrow_C \mu_i'$ such that $\nu_i \approx_\omega \mu_i'$ (see B1). Now we use a similar argument as in B1. Let k be the branching degree of t, i.e., there are exactly k different non-combined transitions $t \rightarrow \xi_1, \cdots, t \rightarrow \xi_k$. Each μ_i' is a linear combination of $\xi_1, \cdots, \xi_k$. Suppose that

$$\mu_i' = x_1^i \xi_1 + \cdots + x_k^i \xi_k$$

Since $\nu_i \approx_i \mu_i'$, for all $a \in Act$ and $C \in S/{\approx_i}$ we have that $\nu_i(a,C) = \mu_i'(a,C)$. By Lemma 2 we have that $\nu_j \approx_j \mu_i'$ for all $0 \leq j \leq i$, because $\nu_j \approx_j \mu \approx_i \nu_i \approx_\omega \mu_i'$. This means that for all $a \in Act$, $0 \leq j \leq i$, and $C \in S/{\approx_j}$ we have $\nu_j(a,C) = \mu_i'(a,C)$. Since $\mu_i' = x_1^i \xi_1 + \cdots + x_k^i \xi_k$, we further get

$$\nu_j(a,C) = x_1^i \xi_1(a,C) + \cdots + x_k^i \xi_k(a,C)$$

for all $a \in Act$ and $C \in S/{\approx_j}$, where $0 \leq j \leq i$.
It follows that $(x_1^i, \cdots, x_k^i)$ is a solution of the family F_i of linear equations

$$\nu_j(a,C) = x_1 \xi_1(a,C) + \cdots + x_k \xi_k(a,C)$$

constructed for all $a \in Act$ and $C \in S/{\approx_j}$ where $0 \leq j \leq i$.
Since $F_i \subseteq F_{i+1}$ and there can be at most k+1 linearly independent linear equations with k variables, there must be some $n \in \mathbb{N}_0$ such that the set of all solutions of F_n is the same as the set of all solutions of $\bigcup_{i \in \mathbb{N}_0} F_i$. Let

$\mu'_n = y_1\xi_1 + \cdots + y_k\xi_k$. Then $(y_1, \cdots, y_k)$ is a solution of F_n and hence also a solution of $\bigcup_{i\in\mathbb{N}_0} F_i$, which means that $\nu_i \approx_i \mu'_n$ for all $i \in \mathbb{N}_0$. Moreover, $\mu \approx_i \nu_i \approx_i \mu'_n \approx_\omega \nu_n$ for all $i \in \mathbb{N}_0$, hence $\mu \approx_i \nu_n$ for all $i \in \mathbb{N}_0$, and thus we get $\mu \approx_\omega \nu_n$ by Lemma 2. Therefore, $\mu \equiv_R \nu_n$ by using the arguments of A1. □

Theorem 1 can be seen as a generalization of a similar result for non-probabilistic processes and strong bisimilarity presented in [7]. Also note that Theorem 1 does not impose any restrictions on distributions (which can possibly have an infinite support). A direct corollary to Theorem 1 is the following generic semidecidability result for non-bisimilarity:

Corollary 1 *If $\not\simeq_i$ is semidecidable over $S \times tfb(S)$ for each $i \in \mathbb{N}_0$, then $\not\simeq$ is semidecidable over $S \times tfb(S)$.*

Proof Let $(s,t) \in S \times tfb(S)$. According to Theorem 1, $s \not\simeq t$ iff there is some $i \in \mathbb{N}_0$ such that $s \not\simeq_i t$. Hence, we can construct a non-deterministic Turing machine $\mathscr{M}$ which first "guesses" an appropriate $i \in \mathbb{N}_0$ and then tries to verify that $s \not\simeq_i t$ by running the corresponding semidecision procedure. Obviously, $s \not\simeq t$ iff $\mathscr{M}$ has an accepting run. □

In the following sections we consider classes of pBPA, pBPP, and pPDA processes where *all* states in the associated pTS are finitely branching and for each transition $s \to \mu$ we have that μ is a rational distribution with a finite support. In this case, each $\simeq_i$ is effectively computable, as stated in the following lemma:

Lemma 3 *Let $\mathscr{S} = (S, Act, D)$ be a pTS such that each $s \in S$ is finitely branching and for each transition $s \to \mu$ we have that μ is a rational distribution with a finite support. For every $s \in S$ we define the size of $D(s)$, denoted $|D(s)|$, as follows:*

$$|D(s)| \;=\; \sum_{s\to\mu} \sum_{\substack{(a,u)\in Act\times S\\ \mu(a,u)>0}} |(\mu(a,u),a,u)|$$

where $|(\mu(a,u),a,u)|$ is the length of the corresponding binary encoding of the triple $(\mu(a,u),a,u)$. Note that $|D(s)|$ is finite for each $s \in S$.

Let $E \subseteq S \times S$ be an equivalence such that, for all $s,t \in S$, the problem whether $(p,q) \in E$ for given $p,q \in succ(s) \cup succ(t)$ is decidable in time polynomial in $|D(s)| + |D(t)|$. Then the problem whether (s,t) expands in E for given $s,t \in S$ is also decidable in time polynomial in $|D(s)| + |D(t)|$.

In particular, for every fixed $i \in \mathbb{N}_0$, the problem whether $s \simeq_i t$ for given $s,t \in S$ is decidable in time polynomial in $|D^i(s)| + |D^i(t)|$, where $D^i(s)$ is the set of all $u \in S$ such that $s \xrightarrow{w} u$ for some $w \in Act^*$ of length at most i.

Proof Let $\mathscr{S} = (S, Act, D)$ be a pTS and $E \subseteq S \times S$ an equivalence with the required properties. We show that the problem whether a given pair $(s,t) \in S \times S$ expands in E is decidable in time polynomial in $|D(s)| + |D(t)|$. Since E over $succ(s) \cup succ(t)$ is computable in time polynomial in $|D(s)| + |D(t)|$, the partition $(succ(s) \cup succ(t))/E$ is also computable in time polynomial in $|D(s)| + |D(t)|$ (where each $C \in (succ(s) \cup succ(t))/E$ is given explicitly by the set of its elements). Let $\mathscr{A} \subseteq Act$ be the set of all actions that are used in the outgoing transitions of s and t, i.e., $a \in \mathscr{A}$ iff there is a transition $s \to \mu$ or $t \to \mu$ and a state

$u \in S$ such that $\mu(a,u) > 0$. By definition of expansion, we need to check that for each $s \twoheadrightarrow \mu$ there is a matching $t \twoheadrightarrow \nu$ such that $\mu(a,C) = \nu(a,C)$ for all $a \in \mathscr{A}$ and $C \in (succ(s) \cup succ(t))/E$, and vice versa. In the non-combined case, this can obviously be done in time polynomial in $|D(s)|+|D(t)|$ (for each $s \to \mu$ we try out all $t \to \nu$ one-by-one, and vice versa). In the combined case, the procedure slightly more complicated (see also [15]). For every $\xi \in Disc(\mathscr{A} \times (succ(s) \cup succ(t)))$, let $\hat{\xi}$ be the associted distribution over $\mathscr{A} \times (succ(s) \cup succ(t))/E$ (that is, $\hat{\xi}(a,C) = \xi(a,C)$). Observe that when we interpret $\hat{\xi}$ as a vector of real numbers, then the sets $\{\hat{\mu} \mid s \to_C \mu\}$ and $\{\hat{\nu} \mid t \to_C \nu\}$ are *convex*. By definition of combined expansion, (s,t) expands in E iff the two convex sets are *equal*. This equality can be checked by verifying that $Gen(s) = Gen(t)$, where $Gen(s)$ and $Gen(t)$ are the sets of *generators* of the two convex sets defined as follows: Let us assume that $D(s) = \{(s,\mu_1), \cdots, (s,\mu_n)\}$ and $D(t) = \{(t,\nu_1), \cdots, (t,\nu_m)\}$. We say that $\hat{\mu}_i$, where $1 \leq i \leq n$, is *redundant* iff there are $x_1, \cdots, x_n \in \mathbb{R}^{\geq 0}$ such that $x_i = 0$, $\sum_{j=1}^{n} x_j = 1$, and $\hat{\mu} = \sum_{j=1}^{n} x_j \cdot \hat{\mu}_j$. The redundancy of a given $\hat{\nu}_i$, where $1 \leq i \leq m$, is defined analogously. The sets $Gen(s)$ and $Gen(t)$ consist of all $\hat{\mu}_i$ and $\hat{\nu}_i$ that are not redundant, respectively. Note that $Gen(s)$ and $Gen(t)$ are computable in time polynomial in $|D(s)|+|D(t)|$ by solving the associated instances of the linear programming problem.

It remains to show that for every fixed $i \in \mathbb{N}_0$, the problem whether $s \sim_i t$ for given $s,t \in S$ is decidable in time polynomial in $|D^i(s)|+|D^i(t)|$. This can be proved by a simple induction on i. The base case ($i = 0$) is immediate, and in the inductive step we use induction hypothesis together with the observation above (where $\simeq_i$ plays the role of E). □

4 Deciding Bisimilarity over pBPA and pBPP Processes

In this section we show that bisimilarity is decidable over configurations of pBPA and pBPP systems, which are probabilistic extensions of the well-known classes of BPA and BPP systems [14]. Moreover, we also show that bisimilarity over normed subclasses of pBPA and pBPP is decidable in polynomial time.

For a given finite set M, we use $(M^*,\cdot)$ and $(M^{\oplus},\cdot)$ to denote the free monoid over M and the free commutative monoid over M, respectively. That is, $(M^*,\cdot)$ is the set of all finite words over M with binary concatenation, and $(M^{\oplus},\cdot)$ is the set of all finite multisets over M with multiset union. The unit element is denoted ε.

Definition 4 A pBPA/pBPP system is a triple $\Delta = (N, \mathscr{A}, \mapsto)$ where N is a finite set of *constants*, $\mathscr{A}$ is a finite set of *actions*, and $\mapsto$ is a finite set of *rules* of the form $X \mapsto \mu$ where $X \in N$ and $\mu \in Disc(\mathscr{A} \times N^{\circ})$ is a rational distribution with a finite support. Here N° denotes either N^* or $N^{\oplus}$, depending on whether Δ is a pBPA or pBPP system, respectively. We require that for every $X \in N$ there is at least one rule of the form $X \mapsto \mu$.

For every $\mu \in Disc(\mathscr{A} \times N^{\circ})$ and all $\alpha, \beta \in N^{\circ}$, let $\mu[\alpha,\beta] \in Disc(\mathscr{A} \times N^{\circ})$ be the (unique) distribution satisfying $\mu[\alpha,\beta](a, \alpha\gamma\beta) = \mu(a,\gamma)$ for all $a \in \mathscr{A}$ and $\gamma \in N^{\circ}$.

To Δ we associate a pTS $\mathscr{S}_{\Delta} = (N^{\circ}, \mathscr{A}, D)$ where D is the least set of transitions such that whenever $X \mapsto \mu$, then $X\beta \to \mu[\varepsilon,\beta]$ for every $\beta \in N^{\circ}$ (note that we slightly abuse our notation by considering N as a subset of N°).

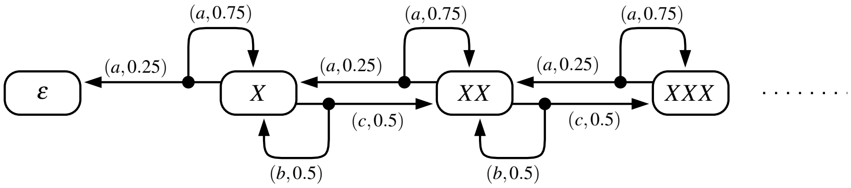

Fig. 4 The structure of $\mathscr{S}_\Delta$.

As an example, consider a pBPA system $\Delta = (\{X\},\{a,b,c\},\mapsto)$ with two rules $X \mapsto \mu$ and $X \mapsto \nu$, where $\mu(a,\varepsilon) = 0.25$, $\mu(a,X) = 0.75$, $\nu(b,X) = 0.5$, and $\nu(c,XX) = 0.5$. The structure of $\mathscr{S}_\Delta$ is shown in Fig. 4. If we interpret Δ as a pBPP system, then $\mathscr{S}_\Delta$ stays the same although the states now formally correspond to finite multisets over $\{X\}$.

Let us note that "ordinary", i.e., non-probabilistic BPA and BPP systems can be understood as those pBPA and pBPP where all distributions used in rules are Dirac [14].

For the rest of this section, let us fix a pBPA/pBPP system $\Delta = (N,\mathscr{A},\mapsto)$. Our aim is to show that $\simeq$ over $N^\circ \times N^\circ$ is decidable. By applying the results of Section 3 (Corollary 1 and Lemma 3), we can conclude that $\not\simeq$ over $N^\circ \times N^\circ$ is semidecidable. Hence, it suffices to show that $\simeq$ is semidecidable over $N^\circ \times N^\circ$. For every $R \subseteq N^\circ \times N^\circ$, let

- $Precon(R) = \{(\gamma\alpha\delta,\gamma\beta\delta) \mid (\alpha,\beta) \in R \text{ and } \gamma,\delta \in N^\circ\}$ be the least precongruence over $N^\circ \times N^\circ$ (with respect to the corresponding binary operation on N°) that includes R.
- $Con(R)$ be the least congruence over $N^\circ \times N^\circ$ that includes R.

The (generic) relationship between $Precon(R)$ and $Con(R)$ is clarified in our next lemma:

Lemma 4 *Let $R \subseteq N^\circ \times N^\circ$. Then $Con(R)$ is the least equivalence over $N^\circ \times N^\circ$ that includes $Precon(R)$. Moreover, if the membership to R is semidecidable, then the membership to $Con(R)$ is also semidecidable.*

Proof Clearly $\equiv_{Precon(R)} \subseteq Con(R)$, and one can easily check that $\equiv_{Precon(R)}$ is a congruence, which proves the other inclusion. Hence, for all $\alpha,\beta \in N^\circ$ we have that $(\alpha,\beta) \in Con(R)$ iff $\alpha = \beta$ or there is a finite sequence $\alpha = \gamma_1,\cdots,\gamma_n = \beta$ such that $(\gamma_i,\gamma_{i+1}) \in Precon(R)$ or $(\gamma_{i+1},\gamma_i) \in Precon(R)$ for every $1 \leq i < n$. If the membership to R is semidecidable, then the existence of such a finite sequence is obviously semidecidable as well. □

The semidecidability of $\simeq$ over $N^\circ \times N^\circ$ is obtained as a consequence of two observations, which are proven in the subsequent subsections.

Lemma 5 *For every $R \subseteq N^\circ \times N^\circ$ we have that R expands in $Con(R)$ iff $Con(R)$ expands in $Con(R)$.*

Lemma 6 *There is a finite relation $\mathscr{B} \subseteq N^\circ \times N^\circ$ such that $\simeq\, = Con(\mathscr{B})$ over $N^\circ \times N^\circ$.*

A direct corollary to Lemma 5 and Lemma 6 is the following:

Theorem 2 *For a given pair $(\alpha,\beta) \in N^\circ \times N^\circ$, it is decidable whether $\alpha \simeq \beta$.*

Proof Due to the results of Section 3, it suffices to show that the problem whether $\alpha \simeq \beta$ is semidecidable. We construct a non-deterministic Turing machine $\mathscr{M}$ which for a given pair $(\alpha,\beta) \in N^\circ \times N^\circ$ on input first "guesses" a finite relation $R \subseteq N^\circ \times N^\circ$ and then verifies that R expands in $Con(R)$ and $(\alpha,\beta) \in Con(R)$. Since R is finite, the membership to $Con(R)$ is semidecidable (see Lemma 4) and hence both of these conditions are semidecidable. If $\mathscr{M}$ succeeds, it halts in an accepting state. The correctness of this procedure follows from Lemma 5, and the existence of an accepting computation of $\mathscr{M}$ for a pair of bisimilar states on input follows from Lemma 6. □

4.1 A Proof of Lemma 5

We start by observing that *every* congruence on N°, when interpreted as an equivalence on *distributions* (see Section 2.2), is "compatible" with the $[\alpha,\beta]$-operator introduced in Definition 4. In particular, this lemma applies to $Con(R)$.

Lemma 7 *For every congruence $E \subseteq N^\circ \times N^\circ$ and all $\mu,\nu \in Disc(\mathscr{A} \times N^\circ)$ we have that if $(\mu,\nu) \in E$, then $(\mu[\alpha,\beta],\nu[\gamma,\delta]) \in E$ for all $\alpha,\beta,\gamma,\delta \in N^\circ$ such that $(\alpha,\gamma),(\beta,\delta) \in E$.*

Proof Let $E \subseteq N^\circ \times N^\circ$ be a congruence and $\mu,\nu \in Disc(\mathscr{A} \times N^\circ)$ distributions such that $(\mu,\nu) \in E$. Further, let $\alpha,\beta,\gamma,\delta \in N^\circ$ such that $(\alpha,\gamma),(\beta,\delta) \in E$. We show that $(\mu[\alpha,\beta],\nu[\gamma,\delta]) \in E$, i.e., $\mu[\alpha,\beta](a,C) = \nu[\gamma,\delta](a,C)$ for every $a \in A$ and $C \in N^\circ/E$.

Let us fix some $a \in \mathscr{A}$ and $C \in N^\circ/E$. For all $\rho,\sigma \in N^\circ$ and every $D \in N^\circ/E$, let $\rho D\sigma = \{\rho\xi\sigma \mid \xi \in D\}$. Note that each such $\rho D\sigma$ is either included in C or disjoint with C, because E is a congruence. Further, observe that for every $D \in N^\circ/E$ we have that $\alpha D\beta \subseteq C$ iff $\gamma D\delta \subseteq C$, because $(\alpha,\gamma),(\beta,\delta) \in E$ and E is a congruence. Now

$$\begin{aligned}
\mu[\alpha,\beta](a,C) &= \sum_{\substack{D\in N^\circ/E\\ \alpha D\beta\subseteq C}} \sum_{\xi\in D} \mu[\alpha,\beta](a,\alpha\xi\beta) = \sum_{\substack{D\in N^\circ/E\\ \alpha D\beta\subseteq C}} \sum_{\xi\in D} \mu(a,\xi)\\
&= \sum_{\substack{D\in N^\circ/E\\ \alpha D\beta\subseteq C}} \sum_{\xi\in D} \nu(a,\xi) = \sum_{\substack{D\in N^\circ/E\\ \gamma D\delta\subseteq C}} \sum_{\xi\in D} \nu[\gamma,\delta](a,\gamma\xi\delta)\\
&= \nu[\gamma,\delta](a,C)
\end{aligned}$$

□

Now we can present the promised proof of Lemma 5.

Lemma 5 *For every $R \subseteq N^\circ \times N^\circ$ we have that R expands in $Con(R)$ iff $Con(R)$ expands in $Con(R)$.*

Proof The "$\Leftarrow$" direction is obvious. For the other direction, let us first formulate a simple observation which will be used at the end of this proof:

> Let $E \subseteq N^\circ \times N^\circ$ be an equivalence. For all $\mu_1, \cdots, \mu_n, \nu_1, \cdots, \nu_n \in Disc(\mathscr{A} \times N^\circ)$ and all $x_1, \cdots, x_n \in \mathbb{R}^{\geq 0}$ such that $(\mu_i, \nu_i) \in E$ for all $1 \leq i \leq n$ and $\sum_{i=1}^n x_i = 1$ we have that $(\sum_{i=1}^n x_i \cdot \mu_i, \sum_{i=1}^n x_i \cdot \nu_i) \in E$.

A proof of this observation is trivial.

The key part our argument is to show that $Precon(R)$ expands in $Con(R)$. So, let $(\gamma\alpha\delta, \gamma\beta\delta) \in Precon(R)$, where $(\alpha, \beta) \in R$ and $\gamma, \delta \in N^\circ$. It follows directly from Definition 4 that for each transition $\gamma\alpha\delta \twoheadrightarrow \mu$ there are distributions μ_γ, μ_α, μ_δ, and coefficients $x_\gamma, x_\alpha, x_\delta \in \mathbb{R}^{\geq 0}$ such that the following conditions are satisfied:

- $x_\gamma + x_\alpha + x_\delta = 1$.
- For every $\rho \in \{\gamma, \alpha, \delta\}$ we have that if $x_\rho > 0$, then $\rho \twoheadrightarrow \mu_\rho$.
- $\mu = x_\gamma \cdot \mu_\gamma[\varepsilon, \alpha\delta] + x_\alpha \cdot \mu_\alpha[\gamma, \delta] + x_\delta \cdot \mu_\delta[\gamma\alpha, \varepsilon]$.

Note that this holds both for the combined and non-combined case and both for pBPA and pBPP systems. Let us define a distribution π as follows: If $x_\alpha = 0$, then π is chosen arbitrarily. Otherwise, there is a transition $\alpha \twoheadrightarrow \mu_\alpha$ and since $(\alpha, \beta) \in R$, there is a matching transition $\beta \twoheadrightarrow \pi$ such that $(\mu_\alpha, \pi) \in Con(R)$ (and thus we obtain the π). Now consider the transition $\gamma\beta\delta \twoheadrightarrow \nu$, where $\nu = x_\gamma \cdot \mu_\gamma[\varepsilon, \beta\delta] + x_\alpha \cdot \pi[\gamma, \delta] + x_\delta \cdot \mu_\delta[\gamma\beta, \varepsilon]$. Due to Lemma 7 we have that $(\mu_\gamma[\varepsilon, \alpha\delta], \mu_\gamma[\varepsilon, \beta\delta]), (\mu_\alpha[\gamma, \delta], \pi[\gamma, \delta]), (\mu_\delta[\gamma\alpha, \varepsilon], \mu_\delta[\gamma\beta, \varepsilon]) \in Con(R)$, and by applying the above observation we obtain $(\mu, \nu) \in Con(R)$ as needed.

Similarly, for every transition of $\gamma\beta\delta$ there is a matching transition of $\gamma\alpha\delta$ (the argument is fully symmetric).

Now we show that $Con(R)$ expands in $Con(R)$. Let $(\alpha, \beta) \in Con(R)$. Due to Lemma 4 we know that $(\alpha, \beta) \in Con(R)$ iff either $\alpha = \beta$ or there is a finite sequence $\alpha = \gamma_1, \cdots, \gamma_n = \beta$ such that $(\gamma_i, \gamma_{i+1}) \in Precon(R)$ or $(\gamma_{i+1}, \gamma_i) \in Precon(R)$ for every $1 \leq i < n$. In the first case we are done immediately, and in the second case we use a straightforward induction on n to show that (α, β) expands in $Con(R)$ (here we use the fact that $Precon(R)$ expands in $Con(R)$). □

4.2 A Proof of Lemma 6

In this section we show that there is finite relation $\mathscr{B} \subseteq N^\circ \times N^\circ$ such that $Con(\mathscr{B}) = \simeq$. Here we generalize the arguments developed for non-probabilistic BPA and BPP [14]. Since these constructions are to a large extent "algebraic", they still work in the (more general) probabilistic setting after reestablishing several simple properties of bisimilarity. To make this paper self-contained, we present full proofs both for pBPA and pBPP.

Definition 5 We say that $\alpha \in N^\circ$ is *normed* if there is $w \in \mathscr{A}^*$ such that $\alpha \xrightarrow{w} \varepsilon$ (remember that ε is the unit of N°). The *norm* of α, denoted $n(\alpha)$, is the length of the shortest such w. If $\beta \in N^\circ$ is not normed, we put $n(\beta) = \infty$. The subset of all normed $X \in N$ is denoted N_n, and the set $N \setminus N_n$ is denoted N_u. We say that Δ is normed if $N = N_n$.

Note that $n(X) \geq 1$, $n(\alpha\beta) = n(\alpha) + n(\beta)$, and that bisimilar states must have the same norm. Consequently, there are only finitely many states with a given finite norm.

Lemma 8 *$\simeq$ is a congruence on N°.*

Proof Since $\simeq$ expands in $\simeq$ (see Lemma 1), it also expands in $Con(\simeq)$. Hence, $Con(\simeq)$ expands in $Con(\simeq)$ by Lemma 5, which means that $Con(\simeq) \subseteq \simeq$. The other inclusion is trivial and thus we obtain $Con(\simeq) = \simeq$. □

Now we can prove Lemma 6 for pBPP.

Lemma 9 (pBPP variant of Lemma 6) *Let $\Delta = (N, \mathscr{A}, \mapsto)$ be a pBPP system. Then there is a finite relation $\mathscr{B} \subseteq N^{\oplus} \times N^{\oplus}$ such that $Con(\mathscr{B}) = \simeq$.*

Proof It was shown by Rédei [32] that every congruence on a finitely generated commutative semigroup is finitely generated. This implies the existence of $\mathscr{B}$ (see Lemma 8). A simple proof of Redei's theorem can be found, e.g., in [24]. □

A proof of Lemma 6 for pBPA is more complicated. We start with auxiliary observations which generalize the analogous results for non-probabilistic BPA presented in [14].

Lemma 10 *Let $\Delta = (N, \mathscr{A}, \mapsto)$ be a pBPA system.*

(1) For all $X \in N_u$ and $\alpha \in N^*$ we have that $X \simeq X\alpha$.
(2) For all $\alpha, \beta \in N^*$ such that $\alpha\gamma \simeq \beta\gamma$ for some $\gamma \in N_n^*$ we have that $\alpha \simeq \beta$.
(3) Let $\alpha, \beta \in N^*$. If there is some $\gamma \in N^*$, $\gamma \neq \varepsilon$ such that $\alpha \simeq \gamma\alpha$ and $\beta \simeq \gamma\beta$, then $\alpha \simeq \beta$.
(4) Let $\alpha, \beta \in N^*$. If there are infinitely many pairwise non-bisimilar $\gamma \in N^*$ such that $\alpha\gamma \simeq \beta\gamma$, then $\alpha \simeq \beta$.

Proof (1) Let $R = \{(\beta, \beta\alpha) \mid X \rightarrow^* \beta\}$. It is easy to verify that R expands in $\equiv_R$ (and hence also in $Con(R)$). Hence, $Con(R)$ is a bisimulation by Lemma 5. Since $(X, X\alpha) \in R \subseteq Con(R)$, we are done.

(2) Let $R = \{(\alpha, \beta) \mid \alpha, \beta \in N^*$ such that $\alpha\gamma \simeq \beta\gamma$ for some $\gamma \in N_n^*\}$. We show that R expands in $\equiv_R$ (and hence also in $Con(R)$), which means that $R \subseteq \simeq$ by Lemma 5. If $\alpha = \varepsilon$ or $\beta = \varepsilon$, then $\alpha = \beta = \varepsilon$ and we are done immediately. Now assume $\alpha \neq \varepsilon \neq \beta$ and $\alpha\gamma \simeq \beta\gamma$ for some fixed $\gamma \in N_n^*$. Let $\alpha \twoheadrightarrow \mu$. Then $\alpha\gamma \twoheadrightarrow \mu[\varepsilon, \gamma]$ and since $\alpha\gamma \simeq \beta\gamma$ and $\beta \neq \varepsilon$, there is $\beta \twoheadrightarrow \nu$ such that $\mu[\varepsilon, \gamma] \simeq \nu[\varepsilon, \gamma]$. Let E be an equivalence over $succ(\alpha) \cup succ(\beta)$ defined as follows: $E = \{(\sigma, \delta) \mid \sigma, \delta \in succ(\alpha) \cup succ(\beta), \sigma\gamma \simeq \delta\gamma\}$. Observe that $E \subseteq R \subseteq \equiv_R$. It follows directly from the definition of E that $(\mu, \nu) \in E$, and hence also $(\mu, \nu) \in \equiv_R$ as needed. Similarly, we can show that for every $\beta \twoheadrightarrow \nu$ there is a matching $\alpha \twoheadrightarrow \mu$ such that $(\mu, \nu) \in \equiv_R$ (the argument is symmetric).

(3) Let $R = \{(\alpha, \beta) \mid \alpha, \beta \in N^*, \alpha \simeq \gamma\alpha, \beta \simeq \gamma\beta$ for some $\gamma \neq \varepsilon\}$. We prove that $R \cup \simeq$ expands in $Con(R \cup \simeq)$, which means that $Con(R \cup \simeq)$ is a bisimulation by Lemma 5. Since the pairs of $\simeq$ expand in $\simeq$, it suffices to show that R expands in $Con(R \cup \simeq)$. So, let $(\alpha, \beta) \in R$, and let $\alpha \twoheadrightarrow \mu$. Since $\alpha \simeq \gamma\alpha$ and $\gamma \neq \varepsilon$, there is $\gamma \twoheadrightarrow \xi$ such that $\gamma\alpha \twoheadrightarrow \xi[\varepsilon, \alpha]$ and $\mu \simeq \xi[\varepsilon, \alpha]$. As $\gamma\beta \twoheadrightarrow \xi[\varepsilon, \beta]$ and $\beta \simeq \gamma\beta$, there is $\beta \twoheadrightarrow \nu$ such that $\xi[\varepsilon, \beta] \simeq \nu$. Since $(\alpha, \beta) \in R$, we also have $(\alpha, \beta) \in Con(R \cup \simeq)$ and hence $(\xi[\varepsilon, \alpha], \xi[\varepsilon, \beta]) \in Con(R \cup \simeq)$ by Lemma 7. Thus, $(\mu, \nu) \in Con(R \cup \simeq)$ by transitivity and hence $\beta \twoheadrightarrow \nu$ can be used as a response to $\alpha \twoheadrightarrow \mu$. Similarly, we show that for every $\beta \twoheadrightarrow \nu$ there is a matching $\alpha \twoheadrightarrow \mu$ such that $(\mu, \nu) \in Con(R \cup \simeq)$ (the argument is symmetric).

(4) Let $R = \{(\alpha,\beta) \mid \alpha\gamma \simeq \beta\gamma$ for infinitely many pairwise non-bisimilar $\gamma\}$. We prove that R expands in $\equiv_R$ (and hence also in $Con(R)$), which means that $R \subseteq \simeq$ by Lemma 5.

Let $(\alpha,\beta) \in R$. The case when $\alpha = \beta = \varepsilon$ is trivial. If $\alpha = \varepsilon$ and $\beta \neq \varepsilon$, then $\gamma \simeq \beta\gamma$ for infinitely many pairwise non-bisimilar γ's which contradicts (3). If $\alpha \neq \varepsilon$ and $\beta = \varepsilon$, we argue in the same way. Now suppose that $\alpha \neq \varepsilon \neq \beta$. Let us fix an infinite family of pairwise non-bisimilar $\gamma_i \in N^*$, $i \in \mathbb{N}$, such that $\alpha\gamma_i \simeq \beta\gamma_i$ for every $i \in \mathbb{N}$. Further, for every $i \in \mathbb{N}$ we define an equivalence E_i over $succ(\alpha) \cup succ(\beta)$ as follows: $E_i = \{(\sigma,\delta) \mid \sigma,\delta \in succ(\alpha) \cup succ(\beta), \sigma\gamma_i \simeq \delta\gamma_i\}$. Since the set $succ(\alpha) \cup succ(\beta)$ is finite, there is an infinite index set $I \subseteq \mathbb{N}$ such that all E_i, $i \in I$, are equal to some fixed equivalence E. Observe that $E \subseteq R$, hence also $E \subseteq \equiv_R$. Now let $\alpha \twoheadrightarrow \mu$. Then, for every $i \in I$, $\alpha\gamma_i \twoheadrightarrow \mu[\varepsilon,\gamma_i]$ and as $\alpha\gamma_i \simeq \beta\gamma_i$, there is $\beta \twoheadrightarrow \nu_i$ such that $\mu[\varepsilon,\gamma_i] \simeq \nu_i[\varepsilon,\gamma_i]$. It follows directly from the definition of E that $(\mu,\nu_i) \in E$ for every $i \in I$. Since $E \subseteq \equiv_R$, we obtain $(\mu,\nu_i) \in \equiv_R$. Hence, each $\beta \twoheadrightarrow \nu_i$, where $i \in I$, can be used as a response to $\alpha \twoheadrightarrow \mu$. Similarly, we show that for every $\beta \twoheadrightarrow \nu$ there is a matching $\alpha \twoheadrightarrow \mu$ such that $(\mu,\nu) \in \equiv_R$ (the argument is symmetric). □

Lemma 11 (pBPA variant of Lemma 6) *Let $\Delta = (N,\mathscr{A},\mapsto)$ be a pBPA system. Then there is a finite relation $\mathscr{B} \subseteq N^* \times N^*$ such that $Con(\mathscr{B}) = \simeq$.*

Proof For every $\alpha \in N^*$ we define its *finite prefix norm*, denoted $n_f(\alpha)$, as $\max\{n(\beta) \mid \alpha = \beta\gamma$ for some $\gamma \in N^*$ and $n(\beta) < \infty\}$. We also define a preorder $\preccurlyeq$ on $N^* \times N^*$ as follows: $(\alpha,\beta) \preccurlyeq (\alpha',\beta')$ iff $\max\{n_f(\alpha),n_f(\beta)\} \leq \max\{n_f(\alpha'),n_f(\beta')\}$.

Let $X\alpha, Y\beta \in NN^*$. The pair $(X\alpha,Y\beta)$ is *decomposable* if $X,Y \in N_n$ and there is some $\gamma \in N^*$ such that one of the following conditions holds:

- $X \simeq Y\gamma$ and $\gamma\alpha \simeq \beta$;
- $Y \simeq X\gamma$ and $\gamma\beta \simeq \alpha$.

Let $X,Y \in N$ and $\alpha,\beta \in N^*$. We say that (α,β) is an (X,Y)-*equalizer* if $X\alpha, Y\beta \in N_n^* N_u$, $X\alpha \simeq Y\beta$, and $(X\alpha,Y\beta)$ is not decomposable. Two (X,Y)-equalizers (α,β) and (α',β') are *similar* if $\alpha \simeq \alpha'$ and $\beta \simeq \beta'$, otherwise they are *distinct*. An (X,Y)-equalizer (α,β) is *minimal* if for every similar (X,Y)-equalizer (α',β') we have that $(\alpha,\beta) \preccurlyeq (\alpha',\beta')$.

We put $\mathscr{B} = \mathscr{B}_0 \cup \mathscr{B}_1 \cup \mathscr{B}_2$, where

- $\mathscr{B}_0 = \{(X,\alpha) \mid X \in N_n, \alpha \in N^*, X \simeq \alpha\}$
- $\mathscr{B}_1 = \{(X,XY) \mid X \in N_u, Y \in N\}$
- $\mathscr{B}_2 = \{(X\alpha,Y\beta) \mid X,Y \in N, (\alpha,\beta)$ is a minimal (X,Y)-equalizer$\}$

Observe that $\mathscr{B}_1$ is finite. $\mathscr{B}_0$ is also finite, because bisimilar states must have the same norm and there are only finitely many states with a given finite norm. It remains to show that $\mathscr{B}_2$ is finite and $Con(\mathscr{B}) = \simeq$.

Assume that $\mathscr{B}_2$ is infinite. Then there is a pair (X,Y) with infinitely many minimal (X,Y)-equalizers. Observe that for every minimal (X,Y)-equalizer (α,β) there are only finitely many minimal (X,Y)-equalizers that are similar to (α,β), because there are only finitely many states with a given finite norm. Hence, there are infinitely many minimal and pairwise distinct (X,Y)-equalizers (α_i,β_i), $i \in \mathbb{N}$. We distinguish three possibilities:

- $X,Y \in N_u$. Then the only (X,Y)-equalizer is $(\varepsilon,\varepsilon)$, which contradicts the existence of infinitely many pairwise distinct (X,Y)-equalizers.
- $X \in N_u$ and $Y \in N_n$. Then $\alpha_i = \varepsilon$ for all $i \in \mathbb{N}$, and hence all β_i are pairwise non-bisimilar. Since $Y \in N_n$, there is $w \in \mathscr{A}^*$ such that $Y \xrightarrow{w} \varepsilon$ and hence also $Y\beta_i \xrightarrow{w} \beta_i$ for all $i \in \mathbb{N}$. As $X \simeq Y\beta_i$, for every $i \in \mathbb{N}$ there must be a matching $X \xrightarrow{w} \gamma_i$ such that $\gamma_i \simeq \beta_i$. Since the rules of Δ involve only distributions with finite support, there are only finitely many states reachable from X via w. This means that infinitely many γ_i are equal to some fixed γ, which makes infinitely many β_i pairwise bisimilar. Thus, we obtain a contradiction. Similarly, we can exclude the case when $X \in N_n$ and $Y \in N_u$ (the argument is symmetric).
- $X,Y \in N_n$. Let us assume that $n(Y) \leq n(X)$ (the other case is symmetric). Then $Y \xrightarrow{w} \varepsilon$ for some $w \in \mathscr{A}^*$ whose length is $n(Y)$. Since $Y\beta_i \xrightarrow{w} \beta_i$, $X\alpha_i \simeq Y\beta_i$, and $n(Y) \leq n(X)$, there is $X \xrightarrow{w} \gamma_i$ such that $\gamma_i\alpha_i \simeq \beta_i$ for every $i \in \mathbb{N}$. As the rules of Δ involve only distributions with finite support, the number of all γ_i reachable from X via w is finite. Hence, there is an infinite index set $I \subseteq \mathbb{N}$ and a fixed state γ such that $\gamma_i = \gamma$ for every $i \in I$. This means that $\gamma\alpha_i \simeq \beta_i$ for all $i \in I$. Further, for all $i,j \in I$ we have that $\alpha_i \not\simeq \alpha_j$ (otherwise, the equalizers (α_i,β_i) and (α_j,β_j) would be similar). Hence, $X\alpha_i \simeq Y\gamma\alpha_i$ for infinitely many pairwise non-bisimilar α_i, which means that $X \simeq Y\gamma$ by applying Lemma 10 (4). Thus, we obtain that $(X\alpha_i, Y\beta_i)$ is decomposable for every $i \in I$, which is a contradiction.

The last step in our proof is to show that $Con(\mathscr{B}) = \simeq$. Since $\mathscr{B}$ contains only bisimilar pairs and $\simeq$ is a congruence, the inclusion $Con(\mathscr{B}) \subseteq \simeq$ is immediate. For the other inclusion, let us first realize that $(\varepsilon,\varepsilon) \in Con(\mathscr{B})$ and the only state bisimilar to ε is ε. Hence, we can concentrate just on bisimilar pairs of the form $(X\alpha, Y\beta)$ where $X\alpha, Y\beta \in NN^*$. By induction on $\preccurlyeq$, we show that $(X\alpha,Y\beta) \in Con(\mathscr{B})$. We distinguish two cases.

- $(X\alpha,Y\beta)$ is decomposable. Then $X,Y \in N_n$ and there is $\gamma \in N^*$ such that $X \simeq Y\gamma$ and $\gamma\alpha \simeq \beta$ (the other case is symmetric). Since $X \simeq Y\gamma$ and $X \in N_n$, we have that $(X,Y\gamma) \in \mathscr{B}_0$. Further, $(\gamma\alpha,\beta) \prec (X\alpha,Y\beta)$ because $n(\gamma) < n(Y\gamma) = n(X) < \infty$ and $n_f(\beta) < n_f(Y\beta)$. Hence, $(\gamma\alpha,\beta) \in Con(\mathscr{B})$ by induction hypothesis. From this we obtain $(X\alpha,Y\beta) \in Con(\mathscr{B})$ by applying congruence rules.
- $(X\alpha,Y\beta)$ is not decomposable. Let $X\alpha'$ and $Y\beta'$ be the maximal prefixes of $X\alpha$ and $Y\beta$ which belong to $N_n^* \cup N_n^* N_u$, respectively (that is, $X\alpha'$ is obtained from $X\alpha$ by deleting all constants following the first occurrence of an unnormed constant in $X\alpha$; similarly for $Y\beta'$ and $Y\beta$). Note that $X\alpha' \simeq Y\beta'$ by Lemma 10 (1). It suffices to show that $(X\alpha',Y\beta') \in Con(\mathscr{B})$, because then the pair $(X\alpha,Y\beta)$ also belongs to $Con(\mathscr{B})$ by applying congruence rules to $(X\alpha',Y\beta')$ and the pairs in $\mathscr{B}_1$.
  If (α',β') is a minimal (X,Y)-equalizer, we are done immediately because then $(X\alpha',Y\beta') \in \mathscr{B}_2$. Otherwise, there must be a minimal (X,Y)-equalizer (α'',β'') which is similar to (α',β'), i.e., $\alpha' \simeq \alpha''$ and $\beta' \simeq \beta''$. Since $(X\alpha'',Y\beta'') \in \mathscr{B}_2$, it remains to show that $(\alpha',\alpha''),(\beta',\beta'') \in Con(\mathscr{B})$. We consider three cases:
  - $X,Y \in N_u$. Then $\alpha'' = \alpha' = \beta'' = \beta' = \varepsilon$. Since $(\varepsilon,\varepsilon) \in Con(\mathscr{B})$, we are done.

- $X \in N_u$ and $Y \in N_n$. Then $\alpha'' = \alpha' = \varepsilon$, and hence we only need to show that $(\beta', \beta'') \in Con(\mathscr{B})$. From the minimality of (α'', β'') we obtain $n_f(\beta'') \leq n_f(\beta')$, and as $Y \in N_n$, we also have $n_f(\beta') < n_f(Y\beta') = n_f(Y\beta)$. Hence, $(\beta', \beta'') \prec (X\alpha, Y\beta)$ and thus $(\beta', \beta'') \in Con(\mathscr{B})$ by induction hypothesis. Symmetric arguments are used in the case when $X \in N_n$ and $Y \in N_u$.
- $X, Y \in N_n$. From the minimality of (α'', β'') we obtain $(\alpha', \alpha'') \preccurlyeq (\alpha', \beta')$ and $(\beta', \beta'') \preccurlyeq (\alpha', \beta')$. Since $X, Y \in N_n$, we further obtain $n_f(\alpha') < n_f(X\alpha') = n_f(X\alpha)$ and $n_f(\beta') < n_f(Y\beta') = n_f(Y\beta)$. This means that $(\alpha', \alpha'') \preccurlyeq (\alpha', \beta') \prec (X\alpha, Y\beta)$ and $(\beta', \beta'') \preccurlyeq (\alpha', \beta') \prec (X\alpha, Y\beta)$, hence $(\alpha', \alpha''), (\beta', \beta'') \in Con(\mathscr{B})$ by induction hypothesis. □

4.3 Polynomial-time algorithms for normed pBPA and normed pBPP

In this subsection we indicate how to modify the existing polynomial-time algorithms for non-probabilistic bisimilarity and normed BPA (or normed BPP) processes [14] so that they work also for normed pBPA and normed pBPP. The functionality of these algorithms is based on several algebraic properties of BPA and BPP which were generalized to pBPA and pBPP in previous sections. The claims and proofs of [14] which lead to the mentioned polynomial-time algorithms can now be extended to the probabilistic case almost by copying them word-by-word. The only remarkable difference is that the non-probabilistic notion of expansion must always be replaced with the probabilistic expansion introduced in Definition 2. To see that the modified algorithms are again polynomial, we need the following observation which is a simple consequence of Lemma 3:

Lemma 12 *Let $\Delta = (N, \mathscr{A}, \mapsto)$ be a pBPA/pBPP system. Let $E \subseteq N^\circ \times N^\circ$ be an equivalence such that the problem whether $(\alpha, \beta) \in E$ for given $\alpha, \beta \in N^\circ$ is decidable in time polynomial in the size of (Δ, α, β). Then the problem whether a given pair $(\alpha, \beta) \in N^\circ \times N^\circ$ expands in E is also decidable in time polynomial in the size of (Δ, α, β).*

Now we can state the main theorem. Since the constructions presented in [14] are somewhat lengthy, we do not repeat them in here.

Theorem 3 *Let $\Delta = (N, \mathscr{A}, \mapsto)$ be a normed pBPA or a normed pBPP system. The problem whether $\alpha \simeq \beta$ for given $\alpha, \beta \in N^\circ$ is decidable in time polynomial in the size of (Δ, α, β).*

5 Deciding Bisimilarity between pPDA and pFS Processes

Our aim is to show that bisimilarity between configurations of a given probabilistic pushdown system and states of a given finite-state pTS is decidable in exponential time. For this purpose we adapt the results of [28], where a generic framework for deciding various behavioral equivalences between pushdown configurations and states of a given finite-state system is developed. In this framework, the generic part of the problem (applicable to every behavioral equivalence which is a right PDA congruence in the sense of Definition 8) is clearly separated from the equivalence-specific part that must be supplied for each behavioral equivalence individually. The method works also in the probabilistic setting, but the application part would be unnecessarily complicated if we used the original scheme proposed in [28]. Therefore, we first develop the generic part of the method into a more "algebraic" form, and then apply the new variant to probabilistic bisimilarity. The introduced modification is generic and works also for other (non-probabilistic) behavioral equivalences.

Definition 6 A *probabilistic pushdown automaton (pPDA)* is a tuple $\Delta = (Q,\Gamma,\mathscr{A},\delta)$ where Q is a finite set of control states, Γ is a finite stack alphabet, $\mathscr{A}$ is a finite set of actions, and δ is a finite set of *rules* of the form $pX \hookrightarrow \mu$ where $pX \in Q{\times}\Gamma$ and $\mu \in \mathit{Disc}(\mathscr{A} \times (Q{\times}\Gamma^*))$ is a rational distribution with a finite support. We require that for every $pX \in Q{\times}\Gamma$ there is at least one rule of the form $pX \hookrightarrow \mu$.

For every $\mu \in \mathit{Disc}(\mathscr{A} \times (Q{\times}\Gamma^*))$ and every $\beta \in \Gamma^*$, let $\mu[\beta] \in \mathit{Disc}(\mathscr{A} \times (Q{\times}\Gamma^*))$ be the (unique) distribution satisfying $\mu[\beta](a, p\alpha\beta) = \mu(a, p\alpha)$ for all $a \in \mathscr{A}$ and $p\alpha \in Q{\times}\Gamma^*$.

To Δ we associate a pTS $\mathscr{S}_\Delta = (Q{\times}\Gamma^*, \mathscr{A}, D)$ where D is the least set of transitions such that whenever $pX \hookrightarrow \mu$ is a rule of δ, then $pX\beta \to \mu[\beta]$ for every $\beta \in \Gamma^*$.

For the rest of this section, we fix a pPDA $\Delta = (Q,\Gamma,\mathscr{A},\delta)$ of size m and a finite-state pTS $\mathscr{S} = (F,\mathscr{A},D)$ of size n (the size of a given $\mu \in \mathit{Disc}(\mathscr{A} \times (Q{\times}\Gamma^*))$ is defined similarly as in Lemma 3). In our complexity estimations we also use the parameter $z = |F|^{|Q|}$.

We start by recalling some notions and results of [28]. To simplify our notation, we introduce all notions directly in the probabilistic setting. We denote $F_\perp = F \cup \{\perp\}$, where $\perp \notin F$ stands for "undefined".

Definition 7 For every $p\alpha \in Q{\times}\Gamma^*$ we define the set $M_{p\alpha} = \{q \in Q \mid p\alpha \to^* q\varepsilon\}$. A function $\mathscr{F} : Q \to F_\perp$ is *compatible* with $p\alpha$ iff $\mathscr{F}(q) \neq \perp$ for every $q \in M_{p\alpha}$. The class of all functions that are compatible with $p\alpha$ is denoted $\mathit{Comp}(p\alpha)$.

For every $p\alpha \in Q{\times}\Gamma^*$ and every $\mathscr{F} \in \mathit{Comp}(p\alpha)$ we define the configuration $p\alpha\mathscr{F}$ whose transitions are determined by the following rules:

$$\frac{p\alpha \to \mu}{p\alpha\mathscr{F} \to \mu[\mathscr{F}]}\,\mathscr{F} \in \mathit{Comp}(p\alpha) \qquad\qquad \frac{\mathscr{F}(p) \to \nu}{p\mathscr{F} \to \nu_{\mathscr{F}}}\,\mathscr{F} \in \mathit{Comp}(p\varepsilon)$$

Here $\mu[\mathscr{F}] \in \mathit{Disc}(\mathscr{A} \times (Q{\times}\Gamma^*{\times}\{\mathscr{F}\}))$ is the unique distribution such that $\mu[\mathscr{F}](a, q\beta\mathscr{F}) = \mu(a, q\beta)$ for all $q\beta \in Q{\times}\Gamma^*$, and $\nu_{\mathscr{F}}$ is the unique distribution which returns a non-zero value only for (some) pairs of the form $(a, p\mathscr{F}[s/p])$, where $\nu(a, p\mathscr{F}[s/p]) = \nu(a, s)$. Here $\mathscr{F}[s/p] : Q \to F_\perp$ is the function which returns the same result as $\mathscr{F}$ for every argument except for p where $\mathscr{F}[s/p](p) = s$. In other words, $p\alpha\mathscr{F}$ behaves like $p\alpha$ until the point when the stack is emptied and a configuration of the form $q\varepsilon$ is entered; from that point on, $p\alpha\mathscr{F}$ behaves like $\mathscr{F}(q)$. Note that if $\mathscr{F} \in \mathit{Comp}(p\alpha)$ and $p\alpha \to^* q\beta$, then $\mathscr{F} \in \mathit{Comp}(q\beta)$. We also put

- $\mathit{Stack}(\Delta, F) = \Gamma^* \cup \{\alpha\mathscr{F} \mid \alpha \in \Gamma^*, \mathscr{F} : Q \to F_\perp\}$
- $\mathscr{P}(\Delta, F) = \{p\alpha \mid p\alpha \in Q{\times}\Gamma^*\} \cup \{p\alpha\mathscr{F} \mid p\alpha \in Q{\times}\Gamma^*, \mathscr{F} \in \mathit{Comp}(p\alpha)\}$

Definition 8 We say that an equivalence E over $\mathscr{P}(\Delta,F) \cup F$ is a *right pPDA congruence* (for Δ and $\mathscr{S}$) iff the following conditions are satisfied:

- For every $p\alpha \in Q \times \Gamma^*$ and all $\varphi, \psi \in \mathit{Stack}(\Delta,F)$ we have that if $(q\varphi, q\psi) \in E$ for each $q \in M_{p\alpha}$, then also $(p\alpha\varphi, p\alpha\psi) \in E$.
- $(p\mathscr{F}, \mathscr{F}(p)) \in E$ for every $p\mathscr{F} \in \mathscr{P}(\Delta,F)$.

Let R be a binary relation over $\mathscr{P}(\Delta,F) \cup F$. The least right pPDA congruence over $\mathscr{P}(\Delta,F) \cup F$ subsuming R is denoted $\mathit{Rcon}(R)$. Further, $\mathit{Rprecon}(R)$ denotes the least binary relation L over $\mathscr{P}(\Delta,F) \cup F$ satisfying the following conditions:

- $R \subseteq L$;
- for every $p\alpha \in Q \times \Gamma^*$ and all $\varphi, \psi \in \mathit{Stack}(\Delta,F)$ we have that if $(q\varphi, q\psi) \in L$ for each $q \in M_{p\alpha}$, then also $(p\alpha\varphi, p\alpha\psi) \in L$.

In general, the least equivalence subsuming $\mathit{Rprecon}(R)$ is a *proper* subset of $\mathit{Rcon}(R)$ (cf. Lemma 4). The relationship between $\mathit{Rprecon}(R)$ and $\mathit{Rcon}(R)$ is revealed in the following lemma:

Lemma 13 *Let R be a binary relation over $\mathscr{P}(\Delta,F) \cup F$. For every $i \in \mathbb{N}_0$ we define a binary relation R^i over $\mathscr{P}(\Delta,F) \cup F$ inductively as follows:*

- $R^0 = R$
- *R^{i+1} is the least equivalence over $\mathscr{P}(\Delta,F) \cup F$ subsuming $\mathit{Rprecon}(R^i)$.*

Then $\mathit{Rcon}(R) = \bigcup_{i \in \mathbb{N}_0} R^i$.

Proof Clearly $\bigcup_{i \in \mathbb{N}_0} R^i \subseteq \mathit{Rcon}(R)$. We prove that $\bigcup_{i \in \mathbb{N}_0} R^i$ is a right pPDA congruence. Let $p\alpha$ be a process of Δ, and let $\varphi, \psi \in \mathit{Stack}(\Delta,F)$ where for each $q \in M_{p\alpha}$ we have that $(q\varphi, q\psi) \in \bigcup_{i \in \mathbb{N}_0} R^i$. Then for each $q \in M_{p\alpha}$ there exists i_q such that $(q\varphi, q\psi) \in R^{i_q}$. Since $R^i \subseteq R^j$ for $i \leq j$, we obtain that $(q\varphi, q\psi) \in R^{\max\{i_q \mid q \in M_{p\alpha}\}}$ for each $q \in M_{p\alpha}$. But then $(p\alpha\varphi, p\alpha\psi) \in R^{1+\max\{i_q \mid q \in M_{p\alpha}\}}$. □

For the rest of this section, let us fix a right pPDA congruence $\stackrel{\circ}{=}$ over $\mathscr{P}(\Delta,F) \cup F$ which is decidable over F and satisfies the following transfer property: if $s \stackrel{\circ}{=} t$ and $s \rightarrow^* s'$, then there exists t' such that $t \rightarrow^* t'$ and $s' \stackrel{\circ}{=} t'$. The following definitions are also borrowed from [28].

Definition 9 Let $\varphi \in \mathit{Stack}(\Delta,F)$ and $\mathscr{F} : Q \rightarrow F_\perp$. We write $\varphi \stackrel{\circ}{=} \mathscr{F}$ iff for all $p \in Q$ we have that if $\mathscr{F}(p) \neq \perp$, then $p\varphi \stackrel{\circ}{=} \mathscr{F}(p)$.

Further, for every relation $K \subseteq \mathit{Stack}(\Delta,F) \times (F_\perp)^Q$ we define the set $I(K)$ of *K-instances* as follows: $I(K) = \{(p\varphi, \mathscr{F}(p)) \mid (\varphi, \mathscr{F}) \in K, \mathscr{F}(p) \neq \perp\}$.

Definition 10 Let $K = \{(\varepsilon, \mathscr{F}) \mid \varepsilon \stackrel{\circ}{=} \mathscr{F}\} \cup \{(\mathscr{G}, \mathscr{F}) \mid \mathscr{G} \stackrel{\circ}{=} \mathscr{F}\} \cup K'$ where $K' \subseteq \Gamma \times (F_\perp)^Q \cup ((\Gamma \times (F_\perp)^Q) \times (F_\perp)^Q)$. That is, K' consists of (some) pairs of the form $(X, \mathscr{F})$ and $(X\mathscr{G}, \mathscr{F})$. We say that K is *well-formed* iff K satisfies the following conditions:

- if $(X\mathscr{G}, \mathscr{F}) \in K$ and $\mathscr{F}(p) \neq \perp$, then $\mathscr{G} \in \mathit{Comp}(pX)$;
- if $(X, \mathscr{F}) \in K$ and $(\mathscr{F}, \mathscr{H}) \in K$, then also $(X, \mathscr{H}) \in K$;
- if $(X\mathscr{G}, \mathscr{F}) \in K$ and $(\mathscr{F}, \mathscr{H}) \in K$, then also $(X\mathscr{G}, \mathscr{H}) \in K$.

It is clear that there are only finitely many well-formed sets, and that there exists the largest well-formed set G whose size is $\mathscr{O}(|\Gamma| \cdot |F|^{2\cdot|Q|})$. Observe that G is effectively constructible because $\doteq$ is decidable over F.

Intuitively, well-formed sets are finite representations of certain infinite relations between the states of $\mathscr{P}(\Delta, F)$ and F, which are "generated" from well-formed sets using the rules introduced in our next definition.

Definition 11 Let K be a well-formed set. The *closure of* K, denoted $Clo(K)$, is the least set L satisfying the following conditions:

(1) $K \subseteq L$;
(2) if $(\alpha\mathscr{G}, \mathscr{F}) \in L$, $(\varepsilon, \mathscr{G}) \in K$, and $\alpha{\neq}\varepsilon$, then $(\alpha, \mathscr{F}) \in L$;
(3) if $(\alpha\mathscr{G}, \mathscr{F}) \in L$, $(\mathscr{H}, \mathscr{G}) \in K$, and $\alpha{\neq}\varepsilon$, then $(\alpha\mathscr{H}, \mathscr{F}) \in L$;
(4) if $(\alpha\mathscr{G}, \mathscr{F}) \in L$, $(X, \mathscr{G}) \in K$, and $\alpha{\neq}\varepsilon$, then $(\alpha X, \mathscr{F}) \in L$;
(5) if $(\alpha\mathscr{G}, \mathscr{F}) \in L$, $(X\mathscr{H}, \mathscr{G}) \in K$, and $\alpha{\neq}\varepsilon$, then $(\alpha X\mathscr{H}, \mathscr{F}) \in L$.

Further, we define $Gen(K) = I(Clo(K))$.

Observe that Clo and Gen are monotonic and that $Gen(K) \subseteq \mathscr{P}(\Delta, F) \times F$ for every well-formed set K.

An important property of Gen is that it generates only "congruent pairs" as stated in the following lemma.

Lemma 14 *Let K be a well-formed set. Then $Gen(K) \subseteq Rcon(I(K))$.*

Proof The closure $Clo(K)$ can be expressed as $Clo(K) = \bigcup_{i\in\mathbb{N}_0} Clo^i(K)$, where $Clo^0(K) = K$ and $Clo^{i+1}(K)$ consists exactly of those pairs which are either in $Clo^i(K)$ or can be derived from K and $Clo^i(K)$ by applying one of the rules (2)-(5) of Definition 11.

We prove that for all $(\varphi, \mathscr{F}) \in Clo^i(K)$ and $p \in Q$ such that $\mathscr{F}(p) \neq \bot$ we have that $(p\varphi, \mathscr{F}(p)) \in Rcon(I(K))$. By induction in i:

- $(\varphi, \mathscr{F}) \in Clo^0(K) = K$. Then immediately $(p\varphi, \mathscr{F}(p)) \in I(K) \subseteq Rcon(I(K))$ for every $p \in Q$ such that $\mathscr{F}(p) \neq \bot$.
- $(\varphi, \mathscr{F}) \in Clo^{i+1}(K) \smallsetminus Clo^i(K)$. Let $p \in Q$ be a state such that $\mathscr{F}(p) \neq \bot$. Then $\varphi = \alpha\gamma$ where $(\gamma, \mathscr{G}) \in K$ and $(\alpha\mathscr{G}, \mathscr{F}) \in Clo^i(K)$. By induction hypothesis we have that $(p\alpha\mathscr{G}, \mathscr{F}(p)) \in Rcon(I(K))$. Moreover, for each $q \in M_{p\alpha}$ it holds that $\mathscr{G}(q) \neq \bot$ and thus $(q\gamma, \mathscr{G}(q)) \in I(K)$. It follows that $(p\alpha\gamma, p\alpha\mathscr{G}), (p\alpha\mathscr{G}, \mathscr{F}(p)) \in Rcon(I(K))$ because $Rcon(I(K))$ is a right pPDA congruence, and hence also $(p\alpha\gamma, \mathscr{F}(p)) \in Rcon(I(K))$ as needed. □

The following well-formed set is especially important.

Definition 12 The *base* $\mathscr{B}$ is defined as follows: $\mathscr{B} = \{(\varepsilon, \mathscr{F}) \mid \varepsilon \doteq \mathscr{F}\} \cup \{(\mathscr{G}, \mathscr{F}) \mid \mathscr{G} \doteq \mathscr{F}\} \cup \{(X, \mathscr{F}) \mid X \doteq \mathscr{F}\} \cup \{(X\mathscr{G}, \mathscr{F}) \mid X\mathscr{G} \doteq \mathscr{F}\}$.

The importance of $\mathscr{B}$ is clarified in the next lemma, whose proof is the same as in [28] (we include this proof for the sake of completeness).

Lemma 15 *$Gen(\mathscr{B})$ coincides with $\doteq$ over $\mathscr{P}(\Delta, F) \times F$.*

Proof We show that $\alpha \doteq \mathscr{F}$ iff $(\alpha,\mathscr{F}) \in \mathit{Clo}(\mathscr{B})$, and $\alpha\mathscr{G} \doteq \mathscr{F}$ iff $(\alpha\mathscr{G},\mathscr{F}) \in \mathit{Clo}(\mathscr{B})$.

For the "$\Leftarrow$" direction, it suffices to show that all of the rules introduced in Definition 11 preserve $\doteq$. We give an explicit proof just for (5) (the other cases follow similarly). Let $\alpha\mathscr{G} \doteq \mathscr{F}$ and $X\mathscr{H} \doteq \mathscr{G}$. We show that $\alpha X\mathscr{H} \doteq \mathscr{F}$. So, let $p \in Q$ such that $\mathscr{F}(p) \neq \bot$. We need to prove that $p\alpha X\mathscr{H} \doteq \mathscr{F}(p)$. Since $\alpha\mathscr{G} \doteq \mathscr{F}$, we know that $p\alpha\mathscr{G} \doteq \mathscr{F}(p)$. Hence, it suffices to show that $p\alpha X\mathscr{H} \doteq p\alpha\mathscr{G}$. But this follows immediately from $X\mathscr{H} \doteq \mathscr{G}$ because $\doteq$ is a right pPDA congruence (see Definition 8).

The other direction is shown by induction on the length of α. If $\alpha = \varepsilon$, we are done immediately because for all $\varepsilon \doteq \mathscr{F}$ and $\mathscr{G} \doteq \mathscr{F}$ we have that $(\varepsilon,\mathscr{F})$ and $(\mathscr{G},\mathscr{F})$ are in $\mathscr{B}$. Now assume that $\alpha = \beta X$, and let $\beta X \doteq \mathscr{F}$ (the case when $\beta X\mathscr{G} \doteq \mathscr{F}$ follows in the same way and therefore it is not considered explicitly). Let us define the function $\mathscr{G} : Q \to F_\bot$ as follows (for purposes of this definition, fix an arbitrary linear ordering over F):

$$\mathscr{G}(q) = \begin{cases} \text{the least } f \text{ s.t. } qX \doteq f & \text{if } \exists p \in Q \text{ s.t. } \mathscr{F}(p) \neq \bot \text{ and } p\beta \to^* q\varepsilon; \\ \bot & \text{otherwise.} \end{cases}$$

First, let us verify that $\mathscr{G}$ is correctly defined, i.e., if $q \in Q$ for which there is $p \in Q$ where $\mathscr{F}(p) \neq \bot$ and $p\beta \to^* q\varepsilon$, then there is *at least one* $f \in F$ such that $qX \doteq f$. Since $\mathscr{F}(p) \neq \bot$ and $\beta X \doteq \mathscr{F}$, we have that $p\beta X \doteq \mathscr{F}(p)$. As $p\beta \to^* q\varepsilon$, we also have that $p\beta X \to^* qX$ and by definition of $\doteq$ there must be some $f \in F$ such that $qX \doteq f$.

Now we can readily confirm that $\beta\mathscr{G} \doteq \mathscr{F}$ and $X \doteq \mathscr{G}$ just by applying the definition of $\mathscr{G}$ above. This means that $(\beta\mathscr{G},\mathscr{F}) \in \mathit{Clo}(\mathscr{B})$ (by induction hypothesis), $(X,\mathscr{G}) \in \mathscr{B}$ (by definition of $\mathscr{B}$), and hence also $(\beta X,\mathscr{F}) \in \mathit{Clo}(\mathscr{B})$ by applying the rule (4) of Definition 11. □

Let $(\mathscr{W},\subseteq)$ be the complete lattice of all well-formed sets, and let $\mathit{Exp} : \mathscr{W} \to \mathscr{W}$ be a function satisfying the following conditions:

1. $\mathit{Exp}(\mathscr{B}) = \mathscr{B}$.
2. Exp is monotonic, i.e. $K \subseteq L$ implies $\mathit{Exp}(K) \subseteq \mathit{Exp}(L)$.
3. If $K = \mathit{Exp}(K)$, then $\mathit{Gen}(K) \subseteq \doteq$.
4. The membership to $\mathit{Exp}(K)$ is decidable.

According to condition 1, the base $\mathscr{B}$ is a fixed-point of *Exp*. In fact, $\mathscr{B}$ is the *greatest fixed-point* of *Exp*. To see this, suppose that $K = \mathit{Exp}(K)$ for some well-formed set K. By definition of $\mathit{Gen}(K)$ and condition 3 we have that $I(K) \subseteq I(\mathit{Clo}(K)) = \mathit{Gen}(K) \subseteq \doteq$. Since for each $(\varphi,\mathscr{F}) \in K$ we have that $\mathscr{F}(p) \neq \bot$ implies $p\varphi \doteq \mathscr{F}(p)$, we can conclude that $(\varphi,\mathscr{F}) \in \mathscr{B}$. Hence, $\mathscr{B}$ can be computed by a simple algorithm which iterates *Exp* on G until a fixed-point is found (remember that G is the largest well-formed set).

The conditions 1–4 above are formulated in the same way as in [28] except for condition 3 which is slightly different. The point is that the "new version" of condition 3 can be checked in a relatively simple way with the help of the (new) algebraic observations presented above. This is the main difference from the original method presented in [28].

Similarly as in [28], we use finite multi-automata to represent certain infinite subsets of $\mathscr{P}(\Delta,F)$.

Definition 13 A *multi-automaton* is a tuple $\mathscr{M} = (S, \Sigma, \gamma, Acc)$ where

- S is a finite set of *states* such that $Q \subseteq S$ (i.e, the control states of Δ are among the states of $\mathscr{M}$);
- $\Sigma = \Gamma \cup \{\mathscr{F} \mid \mathscr{F} : Q \to F_\perp\}$ is the *input alphabet* (the alphabet has a special symbol for each $\mathscr{F} : Q \to F_\perp$);
- $\gamma : S \times (\Sigma \cup \{\varepsilon\}) \to 2^S$ is a *transition function* (with ε-transitions);
- $Acc \subseteq S$ is a set of *accepting states*.

The function γ determines a unique function $\hat{\gamma} : S \times \Sigma^* \to 2^S$ defined inductively as follows:

- $\hat{\gamma}(s, \varepsilon)$ is the least set E such that $s \in E$ and $\gamma(t, \varepsilon) \subseteq E$ for every $t \in E$;
- $\hat{\gamma}(s, a) = \bigcup_{s' \in \hat{\gamma}(s,\varepsilon)} \bigcup_{s'' \in \gamma(s',a)} \hat{\gamma}(s'', \varepsilon)$;
- $\hat{\gamma}(s, wa) = \bigcup_{s' \in \hat{\gamma}(s,w)} \hat{\gamma}(s', a)$.

Every multi-automaton $\mathscr{M}$ then determines a unique set

$$\mathscr{L}(\mathscr{M}) = \{pw \mid p \in Q, w \in \Sigma^*, \hat{\gamma}(p, w) \cap Acc \neq \emptyset\}$$

The following tool will be useful for deciding the membership to $Exp(K)$.

Lemma 16 *Let K be a well-formed set. The relation $R = (\equiv_{Gen(K)} \cap (F \times F))$ is computable in time polynomial in m, n, z. Moreover, for each equivalence class $C \in F/R$ there is a multi-automaton $\mathscr{M}_{K,C}$ accepting the set $C' \subseteq \mathscr{P}(\Delta, F)$ where $C \cup C' \in (\mathscr{P}(\Delta, F) \cup F)/{\equiv_{Gen(K)}}$. The multi-automaton $\mathscr{M}_{K,C}$ is constructible in time polynomial in m, n, z.*

Proof First we prove that for each $f \in F$ there is a multi-automaton $\mathscr{M}_{K,f}$ constructible in time polynomial in m, n, z such that $\mathscr{L}(\mathscr{M}_{K,f}) = \{p\varphi \mid (p\varphi, f) \in Gen(K)\}$ (this construction is the same as in [28]). We put $\mathscr{M}_{K,f} = (S, \Sigma, \gamma, Acc)$ where

- $S = Q \cup \{s_{\mathscr{F}} \mid \mathscr{F} : Q \to F_\perp\} \cup \{A\}$
- $Acc = \{A\}$
- γ is defined as follows (where $p \in Q$, $X \in \Gamma$, and $\mathscr{G} : Q \to F_\perp$):
  - $\gamma(p, \varepsilon) = \{s_{\mathscr{G}} \mid \exists \mathscr{F} : (\mathscr{G}, \mathscr{F}) \in K \text{ and } \mathscr{F}(p) = f\} \cup U$, where U is either $\{A\}$ or $\emptyset$ depending on whether $(\varepsilon, \mathscr{F}) \in K$ for some $\mathscr{F}$ such that $\mathscr{F}(p) = f$ or not, respectively.
  - $\gamma(p, X) = \{s_{\mathscr{G}} \mid \exists \mathscr{F} : (X\mathscr{G}, \mathscr{F}) \in K \text{ and } \mathscr{F}(p) = f\} \cup U$, where U is either $\{A\}$ or $\emptyset$ depending on whether $(X, \mathscr{F}) \in K$ for some $\mathscr{F}$ such that $\mathscr{F}(p) = f$ or not, respectively.
  - $\gamma(s_{\mathscr{G}}, \varepsilon) = \{s_{\mathscr{H}} \mid (\mathscr{H}, \mathscr{G}) \in K\} \cup U$, where U is either $\{A\}$ or $\emptyset$ depending on whether $(\varepsilon, \mathscr{G}) \in K$ or not, respectively.
  - $\gamma(s_{\mathscr{G}}, X) = \{s_{\mathscr{H}} \mid (X\mathscr{H}, \mathscr{G}) \in K\} \cup U$, where U is either $\{A\}$ or $\emptyset$ depending on whether $(X, \mathscr{G}) \in K$ or not, respectively.
  - $\gamma(s_{\mathscr{G}}, \mathscr{G}) = \{A\}$.
  - For the other arguments, γ returns $\emptyset$.

It is easy to check that $\mathscr{L}(\mathscr{M}_{K,f}) = \{p\varphi \mid (p\varphi, f) \in Gen(K)\}$ as required.

The relation R can be computed as follows. Let us define another relation $R' = \{(f, g) \mid \mathscr{L}(\mathscr{M}_{K,f}) \cap \mathscr{L}(\mathscr{M}_{K,g}) \neq \emptyset\} \subseteq F \times F$. It is easy to verify that $R = {\equiv_{R'}}$ and that R' is computable in time polynomial in m, n, z. Now suppose that $C \in F/R$. Clearly $C' = \bigcup_{f \in C} \mathscr{L}(\mathscr{M}_{K,f})$, and hence the multi-automaton $\mathscr{M}_{K,C}$ can be computed in time polynomial in m, n, z. □

5.1 Deciding $\simeq$ between pPDA and pFS processes

We apply the abstract framework presented in the previous section. That is, we show that $\simeq$ is a right pPDA congruence and define an appropriate function *Exp* satisfying the four conditions given earlier. We start with an auxiliary result (cf. Lemma 5).

Lemma 17 *Let R be a binary relation over $\mathscr{P}(\Delta,F) \cup F$. Then R expands in $Rcon(R)$ iff $Rcon(R)$ expands in $Rcon(R)$.*

Proof The "$\Leftarrow$" direction is obvious. For the other direction, recall that $Rcon(R) = \bigcup_{i\in\mathbb{N}_0} R^i$, where R^i is the family of relations introduced in Lemma 13. By induction on i we show that each R^i expands in $Rcon(R)$. The base case when $i=0$ is immediate, because $R^0 = R$. It remains to show that if R^i expands in $Rcon(R)$, then R^{i+1} also expands in $Rcon(R)$. By definition, R^{i+1} is the least equivalence subsuming $Rprecon(R^i)$. Hence, it actually suffices to show that $Rprecon(R^i)$ expands in $Rcon(R)$, because then the least equivalence subsuming $Rprecon(R^i)$ also expands in $Rcon(R)$ by using the same arguments as in Lemma 5.

By definition of $Rprecon(R^i)$, every pair of $Rprecon(R^i) \smallsetminus R^i$ is of the form $(p\alpha\varphi, p\alpha\psi)$ where $(q\varphi, q\psi) \in R^i \subseteq Rcon(R)$ for every $q \in M_{p\alpha}$. We need to show that $(p\alpha\varphi, p\alpha\psi)$ expands in $Rcon(R)$. In the case when $\alpha = \varepsilon$ we are done immediately. Now suppose $\alpha \neq \varepsilon$. Then each transition of $p\alpha\varphi$ is of the form $p\alpha\varphi \twoheadrightarrow \mu[\varphi]$ where $p\alpha \twoheadrightarrow \mu$. Consider the transition $p\alpha\psi \twoheadrightarrow \mu[\psi]$. We claim that $(\mu[\varphi], \mu[\psi]) \in Rcon(R)$. To see this, it suffices to realize that $(r\beta\varphi, r\beta\psi) \in Rcon(R)$ for every $r\beta \in succ(p\alpha)$, which follows immediately from the fact that $M_{r\beta} \subseteq M_{p\alpha}$ and $(q\varphi, q\psi) \in Rcon(R)$ for every $q \in M_{p\alpha}$. □

Since $\simeq$ expands in $\simeq$, it also expands in $Rcon(\simeq)$ and hence $Rcon(\simeq) = \simeq$ due to Lemma 17. Thus we obtain the following:

Lemma 18 *$\simeq$ is a right pPDA congruence.*

Now we can define the promised function *Exp*.

Definition 14 Given a well-formed set K, the set $Exp(K)$ consists of all pairs $(\varphi, \mathscr{F}) \in K$ such that for each $p \in Q$ we have that if $\mathscr{F}(p) \neq \bot$, then $(p\varphi, \mathscr{F}(p))$ expands in $\equiv_{Gen(K)}$.

It remains to verify that *Exp* satisfies the four conditions formulated in the previous section. Condition 1 ($Exp(\mathscr{B}) = \mathscr{B}$) follows easily from the fact that $Gen(\mathscr{B})$ coincides with $\simeq$ over $\mathscr{P}(\Delta,F) \times F$, because if $(p\varphi, \mathscr{F}(p)) \in I(\mathscr{B})$, then $\simeq \,=\, \equiv_{Gen(\mathscr{B})}$ over $succ(p\varphi) \cup succ(\mathscr{F}(p))$. Condition 2 (monotonicity) is obvious. Conditions 3 and 4 are proven below.

Lemma 19 *$Exp(K) = K$ implies $\equiv_{Gen(K)} \subseteq \simeq$.*

Proof $Exp(K) = K$ implies that each pair of $I(K)$ expands in $\equiv_{Gen(K)}$. Since $Gen(K) \subseteq Rcon(I(K))$ (see Lemma 14) and $Rcon(I(K))$ is an equivalence, we also have that $\equiv_{Gen(K)} \subseteq Rcon(I(K))$. This means that $I(K)$ expands in $Rcon(I(K))$ and thus we obtain $\equiv_{Gen(K)} \subseteq Rcon(I(K)) \subseteq \simeq$ by Lemma 17. □

Lemma 20 *$Exp(K)$ is computable in time polynomial in m,n,z.*

Proof Let $(p\alpha, \mathscr{F}(p)) \in I(K)$ and $U = succ(p\alpha) \cup succ(\mathscr{F}(p))$. It follows immediately from Lemma 16 that the equivalence relation $\equiv_{Gen(K)} \cap (U \times U)$ can be computed in time polynomial in m,n,z. The claim then follows from Lemma 3.

□

Now we can formulate our next theorem.

Theorem 4 *Let $pX \in Q \times \Gamma$ and $f \in F$. It is decidable in time polynomial in m,n,z whether $pX \simeq f$. That is, the problem is decidable in exponential time for general pPDA, and in polynomial time for every subclass of pPDA where the number of control states is bounded by some constant (in particular, this applies to pBPA).*

Proof The algorithm computes the base $\mathscr{B}$ by first computing the largest well-formed relation G and then iterating *Exp* until a fixed-point is found. Then, it suffices to find out if there is a pair $(X, \mathscr{F}) \in \mathscr{B}$ such that $\mathscr{F}(p) = f$. Note that this takes time polynomial in m,n,z, because

- G is computable in time polynomial in m,n,z. This is because the size of G is $\mathscr{O}(|\Gamma| \cdot |F|^{2 \cdot |Q|})$ and $\simeq$ over finite-state systems is decidable in polynomial time [15].
- *Exp* is computable in time polynomial in m,n,z due to Lemma 20.
- The algorithm needs at most $|G|$, i.e., $\mathscr{O}(|\Gamma| \cdot |F|^{2 \cdot |Q|})$ iterations to reach a fixed-point. □

6 Conclusions

The results presented in this paper show that various forms of probabilistic bisimilarity are decidable over certain classes of infinite-state probabilistic systems. In particular, this paper advocates the use of algebraic methods which were originally developed for non-probabilistic systems. These methods turn out to be surprisingly robust and can be applied also in the probabilistic setting.

An obvious question is whether the decidability/tractability results for other non-probabilistic infinite-state models can be extended to the probabilistic case. We conjecture that the answer is positive in many cases, and we hope that the results presented in this paper provide some hints and guidelines on how to achieve that. Another interesting question is whether we could do better than in the non-probabilistic case. In particular, undecidability results and lower complexity bounds do not carry over to fully probabilistic variants of infinite-state models (fully probabilistic systems are probabilistic systems where each state s has at most most one out-going transition $s \to \mu$). It is still possible that methods specifically tailored to fully probabilistic models might produce better results than their non-probabilistic counterparts. This also applies to probabilistic variants of other behavioural equivalences, such as trace or simulation equivalence.

References

1. Abdulla, P., Baier, C., Iyer, S., Jonsson, B.: Reasoning about probabilistic channel systems. In: Proceedings of CONCUR 2000, *Lecture Notes in Computer Science*, vol. 1877, pp. 320–330. Springer (2000)

2. Abdulla, P., Bertrand, N., Rabinovich, A., Schnoebelen, P.: Verification of probabilistic systems with faulty communication. Information and Computation **202**(2), 141–165 (2005)
3. Abdulla, P., Henda, N., Mayr, R.: Verifying infinite Markov chains with a finite attractor or the global coarseness property. In: Proceedings of LICS 2005, pp. 127–136. IEEE Computer Society Press (2005)
4. Abdulla, P., Rabinovich, A.: Verification of probabilistic systems with faulty communication. In: Proceedings of FoSSaCS 2003, *Lecture Notes in Computer Science*, vol. 2620, pp. 39–53. Springer (2003)
5. de Alfaro, L., Kwiatkowska, M., Norman, G., Parker, D., Segala, R.: Symbolic model checking of probabilistic processes using MTBDDs and the Kronecker representation. In: Proceedings of TACAS 2000, *Lecture Notes in Computer Science*, vol. 1785, pp. 395–410. Springer (2000)
6. Aziz, A., Singhal, V., Balarin, F., Brayton, R., Sangiovanni-Vincentelli, A.: It usually works: The temporal logic of stochastic systems. In: Proceedings of CAV'95, *Lecture Notes in Computer Science*, vol. 939, pp. 155–165. Springer (1995)
7. Baeten, J., Bergstra, J., Klop, J.: On the consistency of Koomen's fair abstraction rule. Theoretical Computer Science **51**(1), 129–176 (1987)
8. Baier, C., Bertrand, N., Schnoebelen, P.: A note on the attractor-property of infinite-state Markov chains. Information Processing Letters **97**(2), 58–63 (2006)
9. Baier, C., Engelen, B.: Establishing qualitative properties for probabilistic lossy channel systems: an algorithmic approach. In: Proceedings of 5th International AMAST Workshop on Real-Time and Probabilistic Systems (ARTS'99), *Lecture Notes in Computer Science*, vol. 1601, pp. 34–52. Springer (1999)
10. Baier, C., Hermanns, H., Katoen, J.: Probabilistic weak simulation is decidable in polynomial time. Information Processing Letters **89**(3), 123–130 (2004)
11. Bianco, A., de Alfaro, L.: Model checking of probabalistic and nondeterministic systems. In: Proceedings of FST&TCS'95, *Lecture Notes in Computer Science*, vol. 1026, pp. 499–513. Springer (1995)
12. Brázdil, T., Esparza, J., Kučera, A.: Analysis and prediction of the long-run behavior of probabilistic sequential programs with recursion. In: Proceedings of FOCS 2005, pp. 521–530. IEEE Computer Society Press (2005)
13. Brázdil, T., Kučera, A.: Computing the expected accumulated reward and gain for a subclass of infinite Markov chains. In: Proceedings of FST&TCS 2005, *Lecture Notes in Computer Science*, vol. 3821, pp. 372–383. Springer (2005)
14. Burkart, O., Caucal, D., Moller, F., Steffen, B.: Verification on infinite structures. Handbook of Process Algebra pp. 545–623 (1999)
15. Cattani, S., Segala, R.: Decision algorithms for probabilistic bisimulation. In: Proceedings of CONCUR 2002, *Lecture Notes in Computer Science*, vol. 2421, pp. 371–385. Springer (2002)
16. Courcoubetis, C., Yannakakis, M.: Verifying temporal properties of finite-state probabilistic programs. In: Proceedings of FOCS'88, pp. 338–345. IEEE Computer Society Press (1988)
17. Courcoubetis, C., Yannakakis, M.: The complexity of probabilistic verification. Journal of the Association for Computing Machinery **42**(4), 857–907 (1995)
18. Esparza, J., Kučera, A., Mayr, R.: Model-checking probabilistic pushdown automata. In: Proceedings of LICS 2004, pp. 12–21. IEEE Computer Society Press (2004)
19. Esparza, J., Kučera, A., Mayr, R.: Quantitative analysis of probabilistic pushdown automata: Expectations and variances. In: Proceedings of LICS 2005, pp. 117–126. IEEE Computer Society Press (2005)
20. Etessami, K., Yannakakis, M.: Algorithmic verification of recursive probabilistic systems. In: Proceedings of TACAS 2005, *Lecture Notes in Computer Science*, vol. 3440, pp. 253–270. Springer (2005)
21. Etessami, K., Yannakakis, M.: Checking LTL properties of recursive Markov chains. In: Proceedings of 2nd Int. Conf. on Quantitative Evaluation of Systems (QEST'05), pp. 155–165. IEEE Computer Society Press (2005)
22. Etessami, K., Yannakakis, M.: Recursive Markov chains, stochastic grammars, and monotone systems of non-linear equations. In: Proceedings of STACS'2005, *Lecture Notes in Computer Science*, vol. 3404, pp. 340–352. Springer (2005)
23. Hansson, H., Jonsson, B.: A logic for reasoning about time and reliability. Formal Aspects of Computing **6**, 512–535 (1994)

24. Hirshfeld, Y.: Congruences in commutative semigroups. Technical report ECS-LFCS-94-291, Department of Computer Science, University of Edinburgh (1994)
25. Huth, M., Kwiatkowska, M.: Quantitative analysis and model checking. In: Proceedings of LICS'97, pp. 111–122. IEEE Computer Society Press (1997)
26. Iyer, S., Narasimha, M.: Probabilistic lossy channel systems. In: Proceedings of TAPSOFT'97, *Lecture Notes in Computer Science*, vol. 1214, pp. 667–681. Springer (1997)
27. Jonsson, B., Yi, W., Larsen, K.: Probabilistic extensions of process algebras. Handbook of Process Algebra pp. 685–710 (1999)
28. Kučera, A., Mayr, R.: A generic framework for checking semantic equivalences between pushdown automata and finite-state automata. In: Proceedings of IFIP TCS'2004, pp. 395–408. Kluwer (2004)
29. Kwiatkowska, M.: Model checking for probability and time: from theory to practice. In: Proceedings of LICS 2003, pp. 351–360. IEEE Computer Society Press (2003)
30. Larsen, K., Skou, A.: Bisimulation through probabilistic testing. Information and Computation **94**(1), 1–28 (1991)
31. Rabinovich, A.: Quantitative analysis of probabilistic lossy channel systems. In: Proceedings of ICALP 2003, *Lecture Notes in Computer Science*, vol. 2719, pp. 1008–1021. Springer (2003)
32. Rédei, L.: The Theory of Finitely Generated Commutative Semigroups. Pergamon Press (1965)
33. Segala, R., Lynch, N.: Probabilistic simulations for probabilistic processes. NJC **2**(2), 250–273 (1995)