Information and Computation 209 (2011) 154–172

Contents lists available at ScienceDirect

Information and Computation

journal homepage: www.elsevier.com/locate/ic

Probabilistic logical characterization

Holger Hermanns [a,b], Augusto Parma [c], Roberto Segala [c], Björn Wachter [d], Lijun Zhang [e,*]

[a] Saarland University – Computer Science, Saarbrücken, Germany
[b] INRIA Grenoble – Rhône-Alpes, France
[c] Departimento di Informatica, Università di Verona, Italy
[d] Computing Laboratory, University of Oxford, UK
[e] DTU Informatics, Technical University of Denmark, Denmark

ARTICLE INFO

Article history:
Received 25 June 2009
Revised 22 February 2010
Available online 3 December 2010

Keywords:
Probabilistic automata
Bisimulation
Simulation
Logical characterization

ABSTRACT

Probabilistic automata exhibit both probabilistic and non-deterministic choice. They are therefore a powerful semantic foundation for modeling concurrent systems with random phenomena arising in many applications ranging from artificial intelligence, security, systems biology to performance modeling. Several variations of bisimulation and simulation relations have proved to be useful as means to abstract and compare different automata. This paper develops a taxonomy of logical characterizations of these relations on image-finite and image-infinite probabilistic automata.

1. Introduction

Probabilistic automata (PAs) [1] feature both non-deterministic choice (as transition systems) and probabilistic choice (as Markov chains). Thanks to this expressiveness, they form a central model for distributed systems considered in, e.g., artificial intelligence, security, and the analysis of network protocols.

As in the setting of transition systems, bisimulation and simulation relations are means to compare the behavior of probabilistic automata [1–3]. The notable difference of PAs to transition systems is that a transition from some state s leads to a sucessor distribution μ over states instead of just a single successor state. A successor distribution μ gives the probability $\mu(s')$ of entering successor state s'. This probabilistic transition structure is reflected in the definition of simulation. A binary relation R is a simulation relation if, for all $(s, t) \in R$, t can mimic all stepwise behavior of s with respect to R. Intuitively, this means that every distribution μ leaving state s with label a has a distribution μ' leaving state t with the same label a such that the distributions μ and μ' are related: relations between distributions are established by *weight functions* [3]. The largest simulation preorder $\precsim$ is the union of all simulation relations R. This notion of simulation for PAs is a conservative extension of simulation for transition systems; the latter corresponds to the special case where only *Dirac* distributions ($\mu(s') = 1$ for some state s') are considered.

Probabilistic simulation [1], on the other hand, is a variation of simulation specific to the probabilistic world where a state t simulates a state s if and only if, for every transition leaving s, there is a corresponding *convex combination* of transitions leaving t. This condition is more relaxed because a transition of s can be matched by combining several transitions from t.

Strongly related to the concept of simulation are bisimulations. A bisimulation ($\sim$) relate states that behave in the same way, i.e., two states are in relation if they can mimic each other's stepwise behavior. As for simulations, this definition can also be relaxed to convex combinations of transitions, obtaining so-called probabilistic bisimulation [1].

Both simulation and bisimulation have various applications. Simulation relations can be used to prove the correctness of abstraction techniques in probabilistic model checking [4–7]. Simulation can also be used to verify security protocols [8].

* Corresponding author.
E-mail address: zhang@imm.dtu.dk (L. Zhang).

0890-5401/$ - see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.ic.2010.11.024

Bisimulation is the foundation of state-aggregation algorithms [9,10] that compress models by merging bisimilar states. State aggregation is routinely used as a preprocessing step before model checking. In general, simulation and bisimulation are very useful concepts of high practical and theoretical importance since they preserve important classes of temporal properties expressible in quantitative logics such as PCTL [11,12] and CSL [13,14].

This paper considers simulations, probabilistic simulations, bisimulations, and probabilistic bisimulations. We study logical characterizations, the connecting link of these relations with the logics in which temporal properties are expressed. A logic characterizes a relation if two conditions hold: (i) soundness: the validity of logical formulas is preserved by the relation and (ii) completeness: the logic is as expressive as the relation. So, a sound and complete characterization of, say, bisimulation means that two states are bisimilar if and only if they are equivalent with respect to the logic, i.e., they satisfy the same formulas.

If a logic does not characterize a bisimulation completely, this means that logically equivalent states may not be bisimilar. On the other hand, unsound characterization means that bisimilar states are distinguishable by the logic. Analogously, a logic characterizes a simulation preorder if a state simulates another state if and only if the simulating state fulfills all formulas fulfilled by the simulated state. Intuitively, soundness of a characterization guarantees preservation of properties. Soundness and completeness together guarantee that the considered relation is the coarsest relation guaranteeing preservation.

Our focus is on logical characterization for probabilistic automata. Parma and Segala [15] solved this characterization problem for strong (probabilistic) bisimulations. Technically, they extended the Hennessy–Milner logic of Larsen and Skou [2] with distribution semantics, which then enables a sound and complete characterization of bisimulation and probabilistic bisimulation for image-finite probabilistic automata.

1.1. The challenge

We continue and significantly extend the line of work on logical characterization by Parma and Segala [15] along two major dimensions:

- We study both simulation and bisimulation relations, instead of only bisimulations as in [15].
- We consider image-infinite PAs, i.e., infinite non-determinism between transitions with the same action label. Image infiniteness arises, for instance, when modeling systems reading inputs from an unbounded value domain, or if transition probabilities are only known up to a certain confidence interval due to uncertainties in estimation or measurement [16].

Parma and Segala [15] considered image-finite PAs. They proved soundness and completeness based on *bisimulation up to n*, denoted by $\sim_n$, as for labeled transition system [17]. The intersection $\cap_n \sim_n$ induces another relation $\sim_\omega : s \sim_\omega t$ iff $s \sim_n t$ for all $n \in \mathbb{N}$. For image-finite PAs, $\sim_\omega$ and $\sim$ coincide, and thus both the soundness and the completeness proof can be carried out by induction on n. However, for image-infinite PAs, this, unfortunately, does not hold anymore: relation $\sim_\omega$ is strictly coarser than $\sim$ for image-infinite PAs. Therefore different proof techniques are needed, which are sketched in the next paragraph, along with our contributions.

1.2. Contribution

This paper provides a complete taxonomy of the logical characterization of simulation and bisimulation on PAs. We give the first logical characterizations for image-infinite PAs:

- The first contribution of this paper is the alternative definition of simulation and bisimulation relations by a fixpoint characterization giving us insight into why $\sim$ and $\sim_\omega$ coincide for image-finite PAs and differ for image-infinite PAs. Using the fixpoint-based definition, we are able to prove, in a uniform and concise way, the respective results for simulations, probabilistic simulations, bisimulations and probabilistic bisimulations.
- For image-infinite PAs, we give logical characterization results for both $\sim$ and $\sim_\omega$. We show that the logic $\mathcal{L}$ introduced in [15] is even rich enough to characterize $\sim$ for image-infinite PAs. The proof in [15] exploits properties of simulation relation $\sim_\omega$ which do not fit with relation $\sim$ on image-infinite PAs. To this end, we develop a new proof strategy for the soundness and completeness proof of $\sim$. To characterize $\sim_\omega$ we prove that a fragment of the same logic, where formulas are of finite depth, is sufficient: the proof then proceeds by induction on n similar to [15] for image-finite PAs.
- For simulations, it turns out that a characterization proof along the lines of bisimulation, where formulas characterize equivalence classes, leads to a logic with uncountable conjunction. To avoid this, we employ an alternative but equivalent definition of simulation relations based on upwards-closed sets. The alternative definition enables us to prove that the negation-free sub-logic restricted to finite depth formulas characterizes the iteratively-defined simulation ($\precsim_\omega$) for image-infinite PAs. For the co-inductive simulation relation ($\precsim$), we show that the negation-free sub-logic characterizes simulation.
- We also prove that, for image-finite PAs, binary conjunction is sufficient to characterize simulation and bisimulation relations. This finding extends results of [18,19] where binary conjunction is shown to be sufficient for LMPs. Moreover, we extend all of the results to characterize probabilistic bisimulation and probabilistic simulation relations.

1.3. Outline

The paper is structured as follows: Section 2 gives the basic mathematical background, and Section 3 introduces simulation and bisimulation relations by fixpoint characterizations. In Section 4 we present an extension of the Hennessy–Milner logic for PAs. Logical characterizations for simulations and bisimulations are in Section 5 and Section 6, respectively. Section 7 discusses related works, and the paper is concluded by Section 8.

2. Preliminaries

In this section, we recall basic concepts like distributions, relations and well-known results from lattice theory. The lattice-theoretical notions admit an elegant treatment of infinite branching in connection with simulation and bisimulation relations over probabilistic automata (in Section 3).

2.1. Relation

Let S be a set. For a binary relation $R \subseteq S \times S$, we write $s\ R\ t$ if $(s,t) \in R$. A *preorder relation* R is a reflexive and transitive relation. A *partial order* R is a reflexive, antisymmetric and transitive relation. If R is a partial order, the pair (S,R) is called a partially ordered set, or poset for short. An *equivalence relation* is a reflexive, symmetric and transitive relation. An equivalence relation R partitions a set S into equivalence classes. For $s \in S$, we use $[s]_R$ to denote the unique equivalence class containing s. We drop the subscript R if the relation considered is clear from the context.

The *kernel* $\equiv_R$ of a preorder relation R is the largest equivalence relation contained in R. Let $R(s)$ denote the set $\{s' | (s,s') \in R\}$, and $R(A) = \cup_{s\in A} R(s)$ for $A \subseteq S$. A set A is *upwards R-closed* if it holds that $R(s) \subseteq A$ for all $s \in A$.

2.2. Complete lattice

Let P be a set and $\leq \subseteq P \times P$ a binary relation such that the pair $(P,\leq)$ is a partially ordered set. For a subset $P' \subseteq P$, a *lower bound* is an element $a \in P$ that is smaller than all elements of P', i.e., for all $a' \in P'$, $a \leq a'$. An element $a \in P$ is an *infimum* (or greatest lower bound) of P' if it is a lower bound of P' and all lower bounds $a^\dagger \in P$ of P' fulfill $a^\dagger \leq a$. Similarly, an *upper bound* of P' is an element that is greater than all elements of P', and a *supremum* is a least upper bound of P'.

Let $(L,\leq)$ be a partially ordered set. The pair $(L,\leq)$ is a (complete) lattice if each subset of L has both an infimum and a supremum in L. We use meet and join operators $\bigsqcap, \bigsqcup : 2^L \to L$ to denote these infima and suprema, respectively. For a given subset $L' \subseteq L$, the infimum is denoted by $\bigsqcap L'$ and the supremum by $\bigsqcup L'$.

Let S be a countable set. The power set of $S \times S$ forms a complete lattice with set inclusion $\subseteq$ as a partial order, and intersection as a meet $\bigsqcap = \bigcap$ and union $\bigsqcup = \bigcup$ as a join operator, respectively.

For a monotone function $f : L \to L$ over a lattice $(L,\leq)$, Tarski's theorem [20] guarantees existence of least and greatest fixpoints, *lfp* f and *gfp* f, respectively. Let $x \in L$. If $f(x) \leq x$, element x is called a *pre-fixpoint*. If $x \leq f(x)$, element x is called a *post-fixpoint*. The theorem guarantees that $Fix(f) = \{x \in L | f(x) = x\}$ is a lattice and that least and greatest fixpoint are given by the least pre-fixpoint and greatest post-fixpoint, respectively:

$$lfp(f) = \bigsqcap Fix(f) = \bigsqcap \{x \in L | f(x) \leq x\}$$
$$gfp(f) = \bigsqcup Fix(f) = \bigsqcup \{x \in L | f(x) \geq x\}.$$

As a shorthand notation we denote $\bigsqcup \{l_i | i \in \mathbb{N}\}$ by $\bigsqcup_{i\in\mathbb{N}} l_i$, and $\bigsqcap \{l_i | i \in \mathbb{N}\}$ by $\bigsqcap_{i\in\mathbb{N}} l_i$. Then, f is called *continuous* if, for all increasing sequences $l_0, l_1, \ldots$ (i.e., $l_i \leq l_{i+1}$ for all $i \in \mathbb{N}$) in the lattice L, we have $f(\bigsqcup_{i\in\mathbb{N}} l_i) = \bigsqcup_{i\in\mathbb{N}} f(l_i)$. Likewise, f is called *co-continuous* if, for all decreasing sequences $l_0, l_1, \ldots$ (i.e., such that $l_{i+1} \leq l_i$ for all $i \in \mathbb{N}$) in the lattice L, we have $f(\bigsqcap_{i\in\mathbb{N}} l_i) = \bigsqcap_{i\in\mathbb{N}} f(l_i)$.

2.3. Distribution

A *distribution* over S is a function $\mu : S \to \mathbb{R}_{\geq 0}$ such that $\sum_{s\in S} \mu(s) = 1$. We let $\mu(A)$ denote the sum $\sum_{s\in A} \mu(s)$ for all $A \subseteq S$. The *support* of μ is defined as the set $Supp(\mu) := \{s | \mu(s) > 0\}$. Denote by $Dist(S)$ the set of discrete probability distributions over S and, given an element $s \in S$, denote by δ_s the *Dirac distribution* on s that assigns probability 1 to s, i.e., $\delta_s(s) = 1$. Given a countable set of distributions $\{\mu_i\}_{i\in I}$ and a multi-set $\{p_i\}_{i\in I}$ of weights from the interval $[0,1]$ such that $\sum_{i\in I} p_i = 1$, we define the *convex combination* $\sum_{i\in I} p_i\mu_i$ of the distributions $\{\mu_i\}_{i\in I}$ as the probability distribution μ such that, for each $s \in S$, $\mu(s) = \sum_{i\in I} p_i\mu_i(s)$.

3. Simulation and bisimulation for probabilistic automata

In this section, we recall the definition of probabilistic automata. Further, we review the notions of simulations and bisimulations for them, and also probabilistic simulations and bisimulations [2,21,22].

As mentioned in Section 1, we introduce two kinds of simulation: the co-inductive ($\precsim$) and the iteratively-defined variant ($\precsim_\omega$). For simulations, it has been proved that $\precsim$ and $\precsim_\omega$ coincide for image-finite PAs. We will make use of this result and the corresponding results for probabilistic simulations and bisimulations. To this end, we provide an alternative way of defining bisimulation and simulation relations in terms of greatest fixpoints of suitable functions, just like in the setting of labeled transition systems [23]. We then use the alternative fixpoint-based definition to characterize (probabilistic) simulations and (probabilistic) bisimulations.

3.1. Probabilistic automata

We first recall the definition of probabilistic automaton [21], or PA for short.

Definition 3.1. A *probabilistic automaton* is a triple $\mathcal{M} = (S, Act, Steps)$, where S is a countable set of *states*, Act is a countable set of *actions*, and the relation $Steps \subseteq S \times Act \times Dist(S)$ is the *transition relation*.

Obviously, PAs comprise labeled transition systems (LTS) for the special case that for all $(s, a, \mu) \in Steps$, μ is a Dirac distribution.

We denote a transition $(s, a, \mu) \in Steps$ by $s \xrightarrow{a} \mu$. We refer to the distributions leaving a state s by action a as an a-distribution of s. We denote the set of a-distributions of a state s by $Steps_a(s) = \{\mu | s \xrightarrow{a} \mu\}$. We say that $\mathcal{M}$ is *image-finite* (resp. image-infinite) if for all $s \in S$ and $a \in Act$, the set $Steps_a(s)$ is finite (resp. countable). We remark that image finiteness does not necessarily mean that the number of states reachable with one transition is finite, as there may be infinitely many labels. In the rest of the paper, we prove results with and without the assumption of image-finiteness and we use the word "image-infinite" with the meaning "not necessarily image-finite", i.e., all PAs.

Let $\{s \xrightarrow{a} \mu_i\}_{i\in I}$ be a set of transitions, and let $\{p_i\}_{i\in I}$ be a multi-set of probabilities such that $\sum_{i\in I} p_i = 1$. Then the triple $(s, a, \sum_{i\in I} p_i\mu_i)$ is called a *combined transition* and is denoted by $s \overset{a}{\rightsquigarrow} \mu$, where $\mu = \sum_{i\in I} p_i\mu_i$.

3.2. Weight function

We recall the notion of *weight functions* (as proposed by Jonsson and Larsen and Segala [3,21]), which are used to lift relations between S to relations between probability distributions on S.

Definition 3.2. Let $R \subseteq S \times S$ be any relation. The *lifting* of relation R is a binary relation over distributions such that $\mu\ R\ \mu'$ iff there exists a *weight function* $\Delta : S \times S \longrightarrow [0, 1]$ with respect to R such that the following *lifting conditions* hold:

- $\Delta(s, s') > 0$ implies $s\ R\ s'$ for all $s, s' \in S$,
- $\mu(s) = \sum_{s'\in S} \Delta(s, s')$ for all $s \in S$, and
- $\mu'(s') = \sum_{s\in S} \Delta(s, s')$ for all $s' \in S$.

If $R \subseteq R'$, then, $\mu\ R\ \mu'$ implies that $\mu\ R'\ \mu'$ (with the same weight function). Moreover, if the relation R is symmetric, it holds that $\mu\ R\ \mu'$ iff $\mu'\ R\ \mu$. Below we recall some useful lemmas related to weight functions.

Lemma 3.1. *Let μ, μ' be distributions on $Dist(S)$, and let $R \subseteq S \times S$. Then, it holds:*

(a) [5] *Let R be a preorder on S. Then, $\mu\ R\ \mu'$ iff $\mu(U) \le \mu'(U)$ for each upwards R-closed set $U \subseteq S$.*
(b) [24,25] *$\mu\ R\ \mu'$ iff $\mu(U) \le \mu'(R(U))$ for each set $U \subseteq S$.*
(c) [25] *$\mu\ R\ \mu'$ iff $\mu(U) \le \mu'(R(U))$ for each set $U \subseteq Supp(\mu)$.*

This lemma provides another way of characterizing $\mu\ R\ \mu'$. If R is a preorder, U is R-closed implies that $R(U) = U$. Thus, in this case (a) and (b) trivially coincide. The characterization (b) is introduced in [24] for a more general class of models with continuous state space. The last characterization is a simplification of (b). With Lemma 3.1, it is easy to prove that for equivalence relation R, $\mu\ R\ \mu'$ is equivalent to that μ and μ' agree on each equivalence class:

Lemma 3.2. *Let R be an equivalence relation on S, and μ, μ' be distributions in $Dist(S)$. Then, $\mu\ R\ \mu'$ iff $\mu(C) = \mu'(C)$ for each equivalence class C of R.*

Proof. Assume $\mu\ R\ \mu'$ and let $C \in S/_R$. By Lemma 3.1 (C is upwards R-closed), $\mu(C) \le \mu'(C)$ holds. Exploiting the symmetry of R we have $\mu'\ R\ \mu$, which implies $\mu'(C) \le \mu(C)$, thus $\mu(C) = \mu(C')$. The other direction follows directly as each upwards R-closed set is a union of equivalence classes. □

The following lemma shows that for a non-increasing sequence of relations $\{R_i\}_{i\in I}$ and a converging sequence of distributions μ'_i, if $\mu\ R_i\ \mu'_i$ for all i, the limit distribution $\mu' = \lim \mu'_i$ is related with μ by the intersection $R = \cap_{i\in J} R_i$ of these relations.

Lemma 3.3. *Let S be a countable set. Let $J \subseteq \mathbb{N}$ be an infinite set of indices. Let $\{R_i\}_{i\in J}$ be an infinite sequence of decreasing relations on S, i.e., $R_{i+1} \subseteq R_i$ for all $i \in J$. Let $R = \cap_{i\in J} R_i$. Moreover, let $\mu, \mu', \mu'_i \in Dist(S)$ for all $i \in J$. Assume that $\{\mu'_i\}_{i\in J}$ converges to μ' point-wise: for all $s \in S$, it holds $\lim_{i\in J} \mu'_i(s) = \mu'(s)$. Then,*

$$\forall i \in J.\ (\mu\ R_i\ \mu'_i) \Rightarrow \mu\ R\ \mu'.$$

Proof. Let $A \subseteq Supp(\mu)$. By assumption for all $i \in \mathbb{N}$, it holds:

$$\mu(A) \leq \mu'(R_i(A)) = \mu'\left(\cap_{k=1}^{i} R_k(A)\right). \tag{1}$$

Obviously, $\lim_{i\to\infty} \cap_{k=1}^{i} R_k(A) = R(A)$. Taking the limit $i \to \infty$ on both side of Eq. (1) implies that $\mu(A) \leq \mu'(R(A))$ with $R = \cap_{i=1}^{\infty} R_i$. □

The above lemma was used to show that simulation agrees with simulation up to all n [26] for image-finite PAs (cf. Lemma 3.5). It is interesting to note that with Lemma 3.1, the proof is very straightforward. The proof in [26] is rather technical: it involves the construction of a weight function out of infinitely many existing weight functions (with respect to $\mu\ R_i\ \mu'_i$).

3.3. Simulation

We now review the notions of simulation, and bisimulation in terms of suitable monotone functions over the power set lattice (with set inclusion as a partial order).

We begin with simulation and consider the function $F_{\precsim}$ defined as follows:

$$F_{\precsim} : 2^{S\times S} \to 2^{S\times S},\ R \mapsto \left\{(s,t) \in S \times S \mid \forall s \xrightarrow{a} \mu\ \exists t \xrightarrow{a} \mu' :\ \mu\ R\ \mu'\right\}. \tag{2}$$

Intuitively, $F_{\precsim}(R)$ contains all pairs of states (s, s') such that each transition $s \xrightarrow{a} \mu$ can be matched by a corresponding transition $t \xrightarrow{a} \mu'$ with respect to the relation R. We call $F_{\precsim}$ the simulation function.

Definition 3.3. We say that a relation $R \in 2^{S\times S}$ is a *simulation relation* if R is a post-fixpoint of $F_{\precsim}$, i.e., $R \subseteq F_{\precsim}(R)$.

The greatest simulation preorder $\precsim$ is defined as the greatest fixpoint of $F_{\precsim}$. It holds that $s \precsim t$ if there exists a simulation R with $(s, t) \in R$. Function $F_{\precsim}$ is monotone. Recall that Tarski's fixpoint theorem [20] says that the fixpoints of a monotone function form a complete lattice and that the greatest fixpoint is the union of all post-fixpoints. This guarantees that $\precsim$ is well-defined and forms the greatest simulation relation, i.e., the union of all simulation relations. The following lemma shows that for image-finite PAs, $F_{\precsim}$ is co-continuous:

Lemma 3.4. *Let $\mathcal{M} = (S, Act, Steps)$ be an image-finite PA, and let the function $F_{\precsim}$ as defined in (2). Then, $F_{\precsim}$ is co-continuous.*

Proof. Let $l_0, l_1, \ldots$ be a decreasing sequence in the power set lattice. We need to show that $F_{\precsim}(\bigcap_{k\in\mathbb{N}} l_k) = \bigcap_{k\in\mathbb{N}} F_{\precsim}(l_k)$. First, let $(s, t) \in F_{\precsim}(\bigcap_{k\in\mathbb{N}} l_k)$. By definition, for all $s \xrightarrow{a} \mu$, there exists $t \xrightarrow{a} \mu'$ such that $\mu\ R\ \mu'$ with $R = \bigcap_{k\in\mathbb{N}} l_k$. Observe that $R \subseteq l_k$ for all $k \in \mathbb{N}$, thus $\mu\ l_k\ \mu'$ for all $k \in \mathbb{N}$. This implies that $(s, t) \in F_{\precsim}(l_k)$ for all $i \in \mathbb{N}$, thus $(s, t) \in \bigcap_{k\in\mathbb{N}} F_{\precsim}(l_k)$.

For the other direction let $(s, t) \in \bigcap_{k\in\mathbb{N}} F_{\precsim}(l_k)$, implying that $(s, t) \in F_{\precsim}(l_k)$ for all $k \in \mathbb{N}$. Thus, for all $s \xrightarrow{a} \mu$, there exists $t \xrightarrow{a} \mu'_k$ such that $\mu\ l_k\ \mu'_k$ (let Δ_k be the corresponding weight function) for all $k \in \mathbb{N}$. For image-finite PAs the Pigeonhole principle applies, and there must exist $\mu' \in Steps_a(t)$ such that $\mu'_k = \mu'$ for infinitely many $k \in K$, i.e., $\mu' = \lim_{k\in K} \mu'_k$. Since l_k is decreasing, by Lemma 3.3, we have $\mu\ R\ \mu'$ for $R = \bigcap_{k\in K} l_k$ implying $(s, t) \in F_{\precsim}(\bigcap_{k\in\mathbb{N}} l_k)$. □

Hennessy and Milner coined the term "simulation up to n" [17] for the following iterative sequence: $\precsim_0 = S \times S$ and $\precsim_n = F_{\precsim}(\precsim_{n-1}) = (F_{\precsim})^n(S \times S)$ for $n > 0$. Taking the intersection over all simulations up to n, we define the *ω-simulation relation* $\precsim_\omega = \bigcap_{n\in\mathbb{N}} \precsim_n$ where we let $(F_{\precsim})^0(S \times S) = S \times S$.

Sequence $\precsim_n$ is a special case of Kleene iteration, which, under certain conditions, converges to the greatest fixpoint of $F_{\precsim}$, in which case the largest simulation coincides with ω-simulation. This holds for finite PAs where additionally the sequence $\precsim_n$ eventually stabilizes, which leads to an iterative algorithm [27] to compute the largest simulation (and also the largest bisimulation with a different function). In the following, we scrutinize the somewhat more intricate relationship between *ω-simulation relation* and simulation in the more general setting of infinite PAs with finite and infinite branching, respectively.

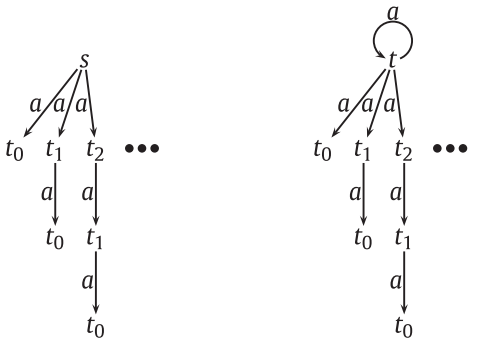

Fig. 1. Relations $\precsim$ and $\precsim_\omega$ do not coincide for image-infinite PAs.

First, we prove that $\precsim_\omega$ and $\precsim$ coincide for image-finite PAs exploiting that $F_{\precsim}$ is co-continuous. This result has already been established in [26, Lemma 3.7.6]. We restate it here, as it will be used to establish an corresponding result for probabilistic simulation relations.

Lemma 3.5. *Let $\mathcal{M} = (S, Act, Steps)$ be an image-finite PA. Then, $\precsim_\omega = \precsim$.*

Proof. One can show $\precsim \subseteq \precsim_n$ by induction on n. Thus, $\precsim \subseteq \precsim_\omega = \cap_n \precsim_n$. Since $\mathcal{M}$ is image-finite by assumption, applying Lemma 3.4, we get that $F_{\precsim}$ is co-continuous, which implies that $\precsim_\omega$ is a fixpoint:

$$F_{\precsim}(\precsim_\omega) = F_{\precsim}\left(\bigcap_{n\in\mathbb{N}} (F_{\precsim})^n(S\times S)\right) = \bigcap_{n\in\mathbb{N}} (F_{\precsim})^{n+1}(S\times S) = \precsim_\omega$$

and, because of $\precsim \subseteq \precsim_\omega$, it must be the greatest fixpoint. □

Lemma 3.5 guarantees that Kleene iteration converges to the greatest fixpoint. This is a generalization of a similar result for image-finite labeled transitions systems, where the simulation function can also be shown to be co-continuous implying that $\precsim = \precsim_\omega$ [23]. In general, $F_{\precsim}$ is not co-continuous for image-infinite PAs, and in that case, relation $\precsim_\omega$ may neither be a simulation nor a fixpoint of $F_{\precsim}$, as illustrated by the following simple example:

Example 3.1. Fig. 1 shows an image-infinite PA with $S = \{s, t, t_0, t_1, t_2, \dots\}$. Initially, we have $\precsim_0 = S \times S$. The absorbing state t_0 has no out-going transitions. So, by removing pairs (u, t_0) with $u \neq t_0$ from $\precsim_0$, we subsequently obtain $\precsim_1 = \precsim_0 \setminus \{(u, t_0) | u \neq t_0\}$. In the next step, we get the relation $\precsim_2 = \precsim_1 \setminus (\{(t_i, t_1) | i > 1\} \cup \{(s, t_1), (t, t_1)\})$ because t_1 leads directly to t_0 which cannot simulate successor states of t_i with $i > 1$ up to $\precsim_1$. Thus we have $\precsim_{i+1} = \precsim_i \setminus \{(t_j, t_i) | j > i\} \cup \{(s, t_i), (t, t_i)\}$. In the limit, we get the relation

$$\precsim_\omega = \{(u, v) | v \in \{s, t\}\} \cup \{(t_i, t_j) | i \leq j\}.$$

Notably, $\precsim_\omega$ is not a simulation (and thus also cannot be a fixpoint): $(t, s) \notin F_{\precsim}(\precsim_\omega)$ because t can go back to t while s *cannot* go to any state s' such that $t \precsim_\omega s'$. We note that $\precsim = \precsim_\omega \setminus \{(t, s)\}$ and thus $\precsim_\omega$ is clearly coarser.

Example 3.1 shows that $\precsim_\omega$ and $\precsim$ do not generally coincide in presence of infinite branching.
We observe that $\precsim$ and $\precsim_\omega$-simulation relations are not necessarily symmetric, as illustrated below.

Example 3.2. Consider the PA depicted in Fig. 2. Obviously, we have $s \precsim s'$ and $s \precsim_\omega s'$. However, the other direction can not be established, i.e., $s' \not\precsim s$: since the middle transition out of s' can not be simulated by any transition out of s. Similarly, it holds: $s' \not\precsim_\omega s$.

3.4. Probabilistic simulation

Probabilistic simulation is defined in the same way by replacing transitions with combined transitions so that the greatest probabilistic simulation is the greatest fixpoint of the function:

$$F_{\precsim^p} : 2^{S\times S} \to 2^{S\times S}, R \mapsto \left\{(s, t) \in S \times S | \forall s \xrightarrow{a} \mu\ \exists t \overset{a}{\rightsquigarrow} \mu' :\ \mu\ R\ \mu'\right\}. \tag{3}$$

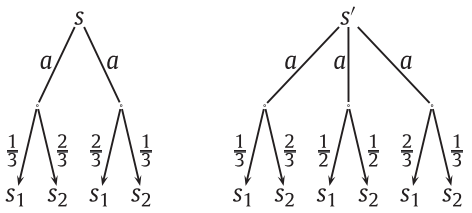

Fig. 2. PA illustrating simulation.

A relation $R \subseteq S \times S$ is a probabilistic simulation if it is a post-fixpoint of $F_{\precsim^p}$. The greatest probabilistic simulation preorder $\precsim^p$ is defined as the greatest fixpoint of $F_{\precsim^p}$. Similar to plain simulation, we define the *probabilistic ω-simulation* by $\precsim^p_\omega = \bigcap_{n\in\mathbb{N}} (F_{\precsim^p})^n (S \times S)$. Then, in general, it only holds that $\precsim^p \subseteq \precsim^p_\omega$, and, as for simulations, we can show that $\precsim^p$ and $\precsim^p_\omega$ coincide for image-finite PAs. The proof is, however, more complicated because of combined transitions. As a preparation for this proof, the following lemma shows that an infinite sequence of combined transitions contains at least a subsequence admitting a limit distribution, which corresponds to a combined transition. A similar result is shown in [28].

Lemma 3.6. *Let $\mathcal{M} = (S, Act, Steps)$ be an image-finite PA. Moreover, let $s \in S$, and let $\{s \overset{a}{\rightsquigarrow} \mu_k\}_{k\in I}$ be an infinite sequence of combined transitions, where $I \subseteq \mathbb{N}$ is an infinite set of indices. Then there exists a subset $J \subseteq I$ such that $\mu = \lim_{k\in J} \mu_k$ and $s \overset{a}{\rightsquigarrow} \mu$.*

Proof. Let $Steps_a(s) = \{\mu'_1, \ldots, \mu'_m\}$. Let $\mu_k = \sum_{j=1}^m q_{k,j}\mu'_j$ with $\sum_{j=1}^m q_{k,j} = 1$ for each $k \in I$. Consider the infinite sequence $(q_{k,1})_{k\in I}$. Since $q_{k,1} \in [0, 1]$ is bounded, there must exist an infinite index set $J_1 \subseteq I$ such that the subsequence $(q_{k,1})_{k\in J_1}$ is convergent. Inductively, for $m > 1$, we have an infinite index set $J := J_m \subseteq J_{m-1} \subseteq \ldots J_1$ such that $(q_{k,i})_{k\in J_i}$ is convergent for $i = 1, 2, \ldots, m$. We define μ by $\mu(s) = \lim_{k\in J} \mu_k(s)$ for all $s \in S$. For each $1 \leq j \leq m$, let $q_j = \lim_{k\in J} q_{k,j}$. Then,

$$\mu(s) = \lim_{k\in J} \mu_k(s) = \lim_{k\in J} \left(\sum_{j=1}^m q_{k,j}\mu'_i(s) \right) = \sum_{j=1}^m \left(\lim_{k\in J} q_{k,j} \right) \cdot \mu'_i(s) = \sum_{j=1}^m q_j\mu'_i(s)$$

implying that $\mu = \sum_{j=1}^m q_j\mu'_j$, implying further that μ is a combined transition: $s \overset{a}{\rightsquigarrow} \mu$. □

Now we show that $\precsim^p_\omega = \precsim^p$ for image-finite PAs. The Pigeonhole principle of Lemma 3.4 does not apply because of infinitely many combined transitions. This is remedied by exploiting the previous lemma.

Lemma 3.7. *Let $\mathcal{M} = (S, Act, Steps)$ be an image-finite PA, and let the function $F_{\precsim^p}$ as defined in (3). Then, $F_{\precsim^p}$ is co-continuous. Moreover, $\precsim^p_\omega = \precsim^p$.*

Proof. To show that $F_{\precsim^p}$ is co-continuous, let $l_0, l_1, \ldots$ with $l_k \subseteq S \times S$ and $l_{k+1} \subseteq l_k$ for all $k \in \mathbb{N}$. We show that $F_{\precsim^p}(\bigcap_{k\in\mathbb{N}} l_k) = \bigcap_{k\in\mathbb{N}} F_{\precsim^p}(l_k)$. The direction $F_{\precsim^p}(\bigcap_{k\in\mathbb{N}} l_k) \subseteq \bigcap_{k\in\mathbb{N}} F_{\precsim^p}(l_k)$ can be obtained as in the proof of Lemma 3.4 by using the combined transitions. For the other direction, let $(s, t) \in \bigcap_{n\in\mathbb{N}} F_{\precsim^p}(l_k)$, which implies that $(s, t) \in F_{\precsim^p}(l_k)$ for all $k \in \mathbb{N}$. By definition of $F_{\precsim^p}$, for all $s \xrightarrow{a} \mu$, there exists $t \overset{a}{\rightsquigarrow} \mu'_k$ such that $\mu\ l_k\ \mu'_k$ for all $k \in \mathbb{N}$. By Lemma 3.6, there exists a subsequence $\{\mu'_k\}_{k\in J}$ such that $\mu' := \lim_{k\in J} \mu'_k$ exists, and moreover, $t \overset{a}{\rightsquigarrow} \mu'$. By Lemma 3.3, we have $\mu\ R\ \mu'$ for $R = \bigcap_{k\in\mathbb{N}} l_k$. The co-continuity property implies then $\precsim^p_\omega = \precsim^p$ (cf. the proof of Lemma 3.5). □

By definition, $\precsim^p$ and $\precsim^p_\omega$ are coarser than $\precsim$ and $\precsim_\omega$, respectively. It is easy to see that the inclusion is strict. To see that, let us again consider states s and s' in the PA of Fig. 2. We have $s' \not\precsim s$, due to the middle transition leaving s' (Example 3.2), and $s' \precsim^p s$, since the middle transition can be simulated by combining the two transitions (each with probability 0.5) out of s.

The following example shows that, as simulation, probabilistic simulation is also not necessarily symmetric.

Example 3.3. Consider the PA depicted in Fig. 3. It holds that $s \precsim^p s'$: the left transition out of s can be expressed by taking the two transitions out of s' with equal probabilities, and the right transition out of s can be expressed by taking weights $\frac{1}{3}$ and $\frac{2}{3}$ of the two transitions, respectively. States s', s are not in the probabilistic simulation relation ($s' \not\precsim^p s$), since both transitions out of s reach s_1 with probability strictly less than $\frac{1}{2}$, and there is no way to combine them to simulate the left transition out of s'.

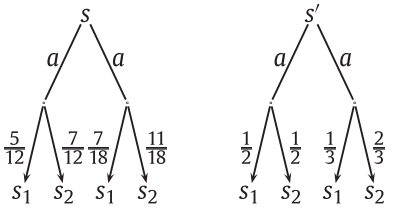

Fig. 3. PA illustrating probabilistic simulation.

3.5. Bisimulation

Bisimulations are also defined co-inductively in terms of greatest fixpoints. The corresponding function is a symmetric variation of the function for simulation:

$$F_\sim : 2^{S\times S} \to 2^{S\times S}, R \mapsto \left\{ (s,t) \in S\times S \;\middle|\; \begin{array}{l} \forall s \xrightarrow{a} \mu\, \exists t \xrightarrow{a} \mu' : \mu\ R\ \mu' \\ \forall t \xrightarrow{a} \mu'\, \exists s \xrightarrow{a} \mu : \mu\ R\ \mu' \end{array} \right\}.$$

Definition 3.4. We say that a relation $R \in 2^{S\times S}$ is a *bisimulation relation* if R is a post-fixpoint of $F_\sim$, i.e., $R \subseteq F_\sim(R)$.

The greatest bisimulation $\sim$ is defined as the greatest fixpoint *gfp* $F_\sim$, which is an equivalence relation. Analogous to simulation, we define *ω-bisimulation* $\sim_\omega = \bigcap_{n\in\mathbb{N}} (F_\sim)^n (S\times S)$ iteratively and, analogous to simulation, $\sim$ and $\sim_\omega$ coincide for image-finite PAs:

Lemma 3.8. *Let $\mathcal{M} = (S, Act, Steps)$ be an image-finite PA. Then, function $F_\sim$ is co-continuous. Moreover, $\sim_\omega = \sim$.*

Adapting the proofs of Lemma 3.4 and Lemma 3.5 to the above lemma is routine. Again, Lemma 3.8 does not hold for image-infinite PAs. Consider for instance Example 3.1, in which $(s,t) \in \sim_\omega$ but $(s,t) \notin \sim$.

Bisimulation can be expressed in terms of simulation. The following lemma shows that R is a bisimulation relation if and only if both R and R^{-1} are simulation relations:

Lemma 3.9. *Let $R \in 2^{S\times S}$ be a relation. Then, $R \subseteq F_\sim(R)$ iff $R \subseteq F_{\precsim}(R)$ and $R^{-1} \subseteq F_{\precsim}(R^{-1})$.*

Proof. Let us assume $R \subseteq F_\sim(R)$, which implies $R \subseteq F_{\precsim}(R)$ directly. Let $(t,s) \in R^{-1}$, i.e., $(s,t) \in R \subseteq F_\sim(R)$. By definition of $F_\sim$, for all $t \xrightarrow{a} \mu'$ there exists $s \xrightarrow{a} \mu$ with $\mu\ R\ \mu'$, thus we have $\mu'\ R^{-1}\ \mu$, implying $(t,s) \in F_{\precsim}(R^{-1})$. For the other direction assume $R \subseteq F_{\precsim}(R)$ and $R^{-1} \subseteq F_{\precsim}(R^{-1})$ and let $(s,t) \in R$. Firstly, $(s,t) \in F_{\precsim}(R)$ implies that for all $t \xrightarrow{a} \mu'$ there exists $s \xrightarrow{a} \mu$ with $\mu\ R\ \mu'$. Moreover, $(t,s) \in R^{-1}$, so $(t,s) \in F_{\precsim}(R^{-1})$ which implies that for all $t \xrightarrow{a} \mu'$ there exists $s \xrightarrow{a} \mu$ with $\mu'\ R^{-1}\ \mu$. Thus, $(s,t) \in F_\sim(R)$. □

The previous lemma says that R is a bisimulation if R and R^{-1} are simulations. The same statement holds for LTSs [29]: this is of no surprise as our PAs subsume LTSs. Usually bisimulations are required to be equivalences in the probabilistic setting [2,21], in which case the above lemma does not hold anymore. As in [30], our definition of bisimulation does not require R to be an equivalence relation.

3.6. Probabilistic bisimulation

The function $F_{\sim^p}$ for probabilistic bisimulation is defined analogously, however using combined transitions:

$$F_{\sim^p} : 2^{S\times S} \to 2^{S\times S}, R \mapsto \left\{ (s,t) \in S\times S \;\middle|\; \begin{array}{l} \forall s \xrightarrow{a} \mu\, \exists t \overset{a}{\rightsquigarrow} \mu' : \mu\ R\ \mu' \\ \forall t \xrightarrow{a} \mu'\, \exists s \overset{a}{\rightsquigarrow} \mu : \mu\ R\ \mu' \end{array} \right\}.$$

A relation $R \subseteq S\times S$ is a probabilistic bisimulation if it is a post-fixpoint of $F_{\sim^p}$. The greatest bisimulation $\sim^p$ is defined as the greatest fixpoint *gfp* $F_{\sim^p}$. It is easy to see that $\sim$ is an equivalence relation. Moreover, define probabilistic ω-bisimulation by $\sim^p_\omega = \bigcap_{n\in\mathbb{N}} (F_{\sim^p})^n (S\times S)$: it holds $\sim^p \subseteq \sim^p_\omega$ in general, and they coincide for image-finite PAs:

Lemma 3.10. *Let $\mathcal{M} = (S, Act, Steps)$ be an image-finite PA. Then, the function $F_{\sim^p}$ is co-continuous. Moreover, $\sim^p_\omega = \sim^p$.*

The proof follows along the line of the proof of Lemma 3.7 and is skipped.

For probabilistic systems, the maximal (or minimal) probability of reaching a certain set of states is of great interest [31]. It is well known that both bisimulation and probabilistic bisimulation preserve this class of properties. Being strictly coarser

than simple bisimulation, probabilistic bisimulation would lead to a smaller quotient in state aggregation. On the other hand, while both kinds of bisimulation can be decided in polynomial time [27,32], decision procedures for probabilistic bisimulation are more expensive than the ones for bisimulation.

4. Logics

In this section, we introduce the logic which will be used to characterize both (bi-)simulations and probabilistic (bi-)simulations. It is a probabilistic extension of Hennessy–Milner logic [17] with the probabilistic modal operator $[\varphi]_p$ and consists of the following set of formulas:

$$\varphi ::= \top | \neg\varphi | \bigwedge_{i\in I} \varphi_i | \langle a\rangle\varphi | [\varphi]_p$$

where $p \in [0,1]$, I is a countable index set and $a \in Act$. We shall use disjunctions which are expressible as $\bigvee_{i\in I}\varphi_i := \neg(\bigwedge_{i\in I}\varphi_i)$. The logic allows infinite conjunction (over the countable index set I) and is necessary for characterizing bisimulation for image-infinite PAs. The above logic is introduced in [15] to characterize (probabilistic) bisimulations for image-finite PAs.

Rather than in terms of single states, the semantics of the logic is given in terms of probability distributions to account for the specifics of probabilistic automata. Intuitively, a distribution μ satisfies the probabilistic formula $[\varphi]_p$ if the probability of the set of states satisfying φ is at least p. Together with conjunctions this allows us to characterize the distribution entirely.

Let $\mathcal{M} = (S, Act, Steps)$ be a PA, and let $\mu \in Dist(S)$. The semantics of φ is given by:

- $\mu \models \top$ holds for each probability distribution μ.
- $\mu \models \neg\varphi$ iff $\mu \not\models \varphi$.
- $\mu \models \bigwedge_{i\in I}\varphi_i$ iff, for each $i \in I$, $\mu \models \varphi_i$.
- $\mu \models \langle a\rangle\varphi$ iff, for each state $s \in Supp(\mu)$, *there exists a transition* $s \xrightarrow{a} \mu'$ such that $\mu' \models \varphi$.
- $\mu \models [\varphi]_p$ iff $\mu(\{s|\delta_s \models \varphi\}) \geq p$.

For the temporal operator $\langle a\rangle$, the transition can be either a normal transition $\xrightarrow{a}$ or a combined transition $\overset{a}{\rightsquigarrow}$. We will use the same logic to characterize both bisimulation and probabilistic bisimulation. For bisimulation, we require that there is a transition $s \xrightarrow{a} \eta$, and for probabilistic bisimulation, we require that there is a combined transition $s \overset{a}{\rightsquigarrow} \eta$ in the definition. By definition, it holds that $\mu \models \langle a\rangle\varphi$ if and only if, for each state $s \in Supp(\mu)$, $\delta_s \models \langle a\rangle\varphi$.

We let $\mathcal{L}$ and $\mathcal{L}_p$ denote the logic for bisimulation and probabilistic bisimulation, respectively. Note that $\mathcal{L}$ and $\mathcal{L}_p$ are syntactically identical, however semantically different. We will show later that, $\mathcal{L}$ and $\mathcal{L}_p$ characterize bisimulations and probabilistic bisimulations for image-infinite PAs. For image-finite PAs, binary conjunction suffices.

The logics $\mathcal{L}^{\precsim}$ and $\mathcal{L}_p^{\precsim}$ for simulations and probabilistic simulations are the negation-free sub-logics resulting from $\mathcal{L}$ and $\mathcal{L}_p$, respectively, which reflects that simulation relations need not be symmetric and is a common approach also pursued by [33,34]. More precisely, the logics consist of formulas:

$$\varphi ::= \top | \bigwedge_{i\in I}\varphi_i | \varphi \vee \varphi | \langle a\rangle\varphi | [\varphi]_p.$$

For a finite set of indices K, disjunction $\vee_{i\in K}\varphi_i$ is defined as usual. Again, $\mathcal{L}^{\precsim}$ and $\mathcal{L}_p^{\precsim}$ are syntactically identical and semantically different.

The logic for characterizing simulations has infinite conjunction, but interestingly, it only has binary disjunction. The infinite conjunction is necessary because of the image-infiniteness. The reason that binary disjunction is sufficient will be implied by an alternative characterization of simulations (see Lemma 5.2) which shows that it is sufficient to focus on finitely-generated sets.

We introduce some convenient notations. For a logic $\mathcal{L}$, the *depth* of $\varphi \in \mathcal{L}$ is the maximal nesting depth of temporal operators occurring in φ. Let $\mathcal{F}_{\mathcal{L}}$ be the set of the formulas of a given logic $\mathcal{L}$, let $\mathcal{F}_{\mathcal{L},n}$ denote the set of the formulas of $\mathcal{L}$ of depth at most n, and $\mathcal{F}_{\mathcal{L},\omega} = \cup_{n\in\mathbb{N}}\mathcal{F}_{\mathcal{L},n}$ the set formulas of finite depth. We also write $\mathcal{L}_\omega = \mathcal{F}_{\mathcal{L},\omega}$ for the sub-logic of $\mathcal{L}$ consisting of formulas of finite depth. Let $\mathcal{F}_{\mathcal{L}}(s)$ and $\mathcal{F}_{\mathcal{L}}(\mu)$ be the sets of the formulas of $\mathcal{L}$ that are satisfied by the state s and by the distribution μ, respectively. Moreover, we denote by $\mathcal{F}_{\mathcal{L},\omega}(s)$ and $\mathcal{F}_{\mathcal{L},\omega}(\mu)$ the sets of finite formulas of $\mathcal{L}$ that are satisfied by the state s and by the distribution μ, respectively. Given a logic $\mathcal{L}$, the notation $[\![\varphi]\!]_{\mathcal{L}} = \{s|s \models \varphi\}$ stands for the set of all the states that satisfy a formula φ of $\mathcal{L}$. If $\delta_s \models \varphi$, we also write $s \models \varphi$. Thus, it holds trivially $\mathcal{F}_{\mathcal{L}}(s) = \mathcal{F}_{\mathcal{L}}(\delta_s)$ and $\mathcal{F}_{\mathcal{L},n}(s) = \mathcal{F}_{\mathcal{L},n}(\delta_s)$ for all $n \in \mathbb{N}$. We drop the subscript $\mathcal{L}$ whenever it is clear from the context.

5. Logical characterization of simulation

In this section, we give logical characterizations of (probabilistic) simulation relations. We first provide a stronger condition than Lemma 3.1.(*a*) in Section 5.1, by showing that it is sufficient to consider a countable class of upwards R-closed sets. Then we present the characterization result for $\precsim$ and $\precsim_\omega$ for image-infinite PAs in Sections 5.2 and 5.3, respectively. In Section 5.4 we consider image-finite PAs and show that binary conjunction [1] is sufficient, exploiting the Pigeonhole principle. Section 5.5 treats probabilistic simulations.

5.1. Weight function for preorder

The following lemma states that any upwards R-closed set $U \subseteq S$ can be expressed as a union of equivalence classes of $\equiv_R$.

Lemma 5.1. *Let R be a preorder on S, and let $U \subseteq S$ be an upwards R-closed set. Then U is a union of equivalence classes of $\equiv_R$.*

Proof. Let $s \in U$ be any element of U. By definition, the whole class $[s]$ of $\equiv_R$ is contained in U. Thus for each equivalence class C of $\equiv_R$, either $C \subseteq U$ or $C \cap U = \emptyset$. Thus, R is a union of equivalence classes of $\equiv_R$. □

Let R be a preorder on S. For $A \subseteq S$, we let $cl(A)$ denote the smallest upwards R-closed set containing A. An upwards R-closed set U is *finitely-generated* if there is a finite family of classes $\{[s_1], \ldots, [s_k]\}$ of $\equiv_R$ generating U, i.e., $U = \cup_{i=1}^{k} [cl([s_i])]$. The set of equivalence classes $\equiv_R$ is countable, implying that the set of finitely-generated upwards R-closed sets is also countable.

Lemma 5.2. *Let $\mathcal{M} = (S, Act, Steps)$ be a PA and let $\mu, \mu' \in Dist(S)$. Let R be a preorder on S. Then $\mu \; R \; \mu'$ iff for each finitely-generated upwards R-closed set U, $\mu(U) \leq \mu'(U)$.*

Proof. If U is a finitely-generated upwards R-closed set, $\mu(U) \leq \mu'(U)$ follows trivially from Lemma 3.1.(*a*). For the other direction assume that for each finitely-generated upwards R-closed set U, $\mu(U) \leq \mu'(U)$. For the sake of contradiction let U be an upwards R-closed set with $\mu(U) > \mu'(U)$, and let $\epsilon := \mu(U) - \mu'(U) > 0$. By Lemma 5.1, $U = \bigcup_{i \in I} cl([s_i])$ with a (possibly countable) index set $I \subseteq \mathbb{N}$. Define $U_i = \bigcup_{\{j \mid j \leq i\}} cl([s_j])$ for $i \in I$. By definition, U_i is finitely-generated upwards R-closed set, implying $\mu(U_i) \leq \mu'(U_i)$ for $i \in I$. Observe the sequence $\{\mu(U_i)\}_{\{i \in I\}}$ is monotone, non-decreasing and converges to $\mu(U)$. Thus, there exists $m \in I$ with $\mu(U_m) > \mu(U) - \frac{\epsilon}{2}$, implying:

$$\mu(U_m) > \mu(U) - \frac{\epsilon}{2} = \mu'(U) + \frac{\epsilon}{2} > \mu'(U) \geq \mu'(U_m).$$

which is a contradiction. □

With the above lemma, we can give an alternative formulation of simulation (and, in an analogous way, a formulation for probabilistic simulation): a relation $R \subseteq S \times S$ is a *simulation* if for $s \; R \; s'$ and $s \xrightarrow{a} \mu$, there exists μ' such that $s' \xrightarrow{a} \mu'$ and for each finitely-generated upwards R-closed set U, $\mu(U) \leq \mu'(U)$. As a consequence of Lemma 5.2, it is sufficient to consider the countable set of finitely-generated upwards closed sets rather than the potentially uncountable set of upwards R-closed sets.

5.2. Logical characterization of $\precsim$ for image-infinite PAs

We would like to prove that $\mathcal{L}^{\precsim}$ characterizes $\precsim$. We first give the strategy of the proof as it will also be similar for other characterizations we shall consider later. In technical terms, we want to prove $s \precsim s'$ iff $\mathcal{F}_{\mathcal{L}^{\precsim}}(s) \subseteq \mathcal{F}_{\mathcal{L}^{\precsim}}(s')$.

- The soundness part requires to show that $s \precsim s'$ implies $\mathcal{F}_{\mathcal{L}^{\precsim}}(s) \subseteq \mathcal{F}_{\mathcal{L}^{\precsim}}(s')$. Exploiting $\mathcal{F}_{\mathcal{L}^{\precsim}}(s) = \mathcal{F}_{\mathcal{L}^{\precsim}}(\delta_s)$, we instead prove a more general statement about distributions:
$$\forall \mu, \mu' \in Dist(S).\ \mu \precsim \mu' \Longrightarrow \mathcal{F}_{\mathcal{L}^{\precsim}}(\mu) \subseteq \mathcal{F}_{\mathcal{L}^{\precsim}}(\mu') \tag{4}$$
which is usually achieved by structural induction on φ.
- For the completeness proof, we consider the relation $R = \{(s, s') \mid \mathcal{F}_{\mathcal{L}^{\precsim}}(s) \subseteq \mathcal{F}_{\mathcal{L}^{\precsim}}(s')\}$ and show that R is a simulation. Then, for each $(s, s') \in R$, we show that $(s, s') \in F_{\precsim}(R)$, i.e., $s \xrightarrow{a} \mu$ implies the existence of $s' \xrightarrow{a} \mu'$ such that $\mu \; R \; \mu'$. By Lemma 5.2, it is equivalent to show that $\mu(U) \leq \mu'(U)$ for each finitely-generated upwards R-closed set U. As there are only countably many such U, the countable conjunction operator is sufficient.

[1] The result for image-finite PAs can be considered as an extension of [5,33]: For LMPs [5] (image-finite PAs with continuous state space and deterministic transition with respect to the same action), Desharnais et al. characterized simulation completely with only binary conjunctions.

Theorem 5.3. *Given the logic $\mathcal{L}^{\precsim}$, for each pair of states s, s' of a PA, $s \precsim s'$ iff $\mathcal{F}(s) \subseteq \mathcal{F}(s')$.*

Proof. For soundness let $\mu, \mu' \in Dist(S)$ with $\mu \precsim \mu'$. Let $\varphi \in \mathcal{F}(\mu)$, we prove $\varphi \in \mathcal{F}(\mu')$, i.e., $\mu' \models \varphi$ by structural induction on φ (see (4)).

- If $\varphi = \top$, then the result is trivial.
- If $\varphi = \bigwedge_{i\in I} \psi_i$, then for each $i \in I$, $\mu \models \psi_i$. Since $\psi_i \in \mathcal{F}$ for each $i \in I$, then by induction, $\mu' \models \psi_i$. Thus, $\mu' \models \bigwedge_{i\in I} \psi_i$. The case $\varphi = \psi_1 \vee \psi_2$ is similar.
- If $\varphi = [\psi]_p$, then $\mu([\![\psi]\!]) \geq p$. By hypothesis of the structural induction, $[\![\psi]\!]$ is upwards $\precsim$-closed. By Lemma 3.1.(a), we have $\mu([\![\psi]\!]) \leq \mu'([\![\psi]\!])$, proving $\mu' \models \varphi$.
- If $\varphi = \langle a\rangle\psi$: we show $s_2 \models \varphi$ for arbitrary, fixed $s_2 \in Supp(\mu')$. We show first $\mu \precsim \mu'$ and $s_2 \in Supp(\mu')$ imply the existence of $s_1 \in Supp(\mu)$ with $s_1 \precsim s_2$. Let Δ denote the corresponding weight function w.r.t. $\mu \precsim \mu'$. We observe that: $0 < \mu'(s_2) = \sum_{s\in S} \Delta(s, s_2)$. Hence, there exists $s_1 \in Supp(\mu)$ such that $\Delta(s_1, s_2) > 0$. By the definition of weight function it holds thus $s_1 \precsim s_2$. Moreover, $\mu \models \varphi$ implies that there exists $s_1 \xrightarrow{a} \mu_1$ with $\mu_1 \models \psi$. Thus, there exists a transition $s_2 \xrightarrow{a} \mu_2$ such that $\mu_1 \precsim \mu_2$. By induction hypothesis, we have that $\mu_2 \models \psi$, thus $s_2 \models \varphi$. Thus, $\mu' \models \varphi$.

To show completeness, define $R = \{(s, s') | \mathcal{F}(s) \subseteq \mathcal{F}(s')\}$. Let $\{[s_j]\}_{j\in J}$ be an enumeration of the equivalence classes of $\equiv_R$ (the kernel of R). We first introduce the characterizing formula for upwards-closed set $cl([s_l])$ for $l \in J$. By definition of R, for each $m \in J$ with $s_m \notin cl([s_l])$, there exists a formula $\varphi_{lm} \in \mathcal{F}$ such that $s_l \models \varphi_{lm}$ and $s_m \not\models \varphi_{lm}$. For each $l \in J$, define $\varphi_l = \bigwedge_{s_m \notin cl([s_l])} \varphi_{lm}$. Then, by construction, for $l \in J$ we have $[\![\varphi_l]\!] = cl([s_l])$.

Now it remains to prove that R is a simulation relation. Let $(s, s') \in R$, and $s \xrightarrow{a} \mu$, we show that there exists a transition $s' \xrightarrow{a} \mu'$ with $\mu \; R \; \mu'$. Let $\{U_i\}_{i\in I}$ be the countable set of the finitely-generated upwards R-closed sets. By Lemma 5.2, it is sufficient to show that $\mu(U_i) \leq \mu'(U_i)$ for all $i \in I$. Since U_i is finitely-generated, for each $i \in I$, there exists a finite index set $K_i \subseteq J$ such that $U_i = \bigcup_{k\in K_i} cl([s_k])$. For each $i \in I$, define $\varphi_{K_i} = \vee_{l\in K_i} \varphi_l$. Since K_i is finite, the formula φ_{K_i} has only binary disjunctions. Then, φ_{K_i} is satisfied only by states in U_i, that is, $[\![\varphi_{K_i}]\!] = U_i$. Now, define $\varphi = \bigwedge_{i\in I} [\varphi_{K_i}]_{p_i}$ with $p_i = \mu(U_i)$ for $i \in I$. By definition, $\mu \models \varphi$, implying that $s \models \langle a\rangle\varphi$. By the definition of R, $s' \models \langle a\rangle\varphi$ as well. Thus, there exists a distribution μ' such that $s' \xrightarrow{a} \mu'$ and $\mu' \models \varphi$. By definition, $\mu'(U_i) = \mu'([\![\varphi_{K_i}]\!]) \geq p_i = \mu(U_i)$ for each $i \in I$, as needed. □

Theorem 5.3 states that the logic $\mathcal{L}^{\precsim}$ characterizes simulation soundly and completely. The following example illustrates that the infinite conjunction in the logic is actually needed for image-infinite models.

Example 5.1. Consider the PA depicted in Example 3.1 and recall that $t \not\precsim s$. Consider the formula φ_i defined as follows: $\varphi_0 = \top$, and $\varphi_{i+1} = \langle a\rangle\varphi_i$, and let $\varphi = \langle a\rangle \bigwedge_{i\in\mathbb{N}} \varphi_i$. If a state satisfies φ, the infinite conjunction in φ requires that after an action a, the successor state can perform still a sequence of n a-actions, for all n. Thus, the formula is satisfied by t but not s.

There is no way, however, to construct a formula with only binary conjunctions such that it is satisfied by t but not s. From both s and t, there is a sequence of n a-actions. The only additional behavior out of t is the infinite sequence of a-actions. Consider the formula φ which has only binary conjunctions and is satisfied by t. By induction, formula φ has only finite length, thus its satisfiability is witnessed by a sequence of a-actions with finite length. Obviously, such a sequence also exists from s. The key point is that the additional behavior of t does not contribute to the distinguishing power at all.

5.3. Logical characterization of $\precsim_\omega$ for image-infinite PAs

Now we consider the relation $\precsim_\omega$, which is strictly coarser than $\precsim$ for image-infinite PAs. By Theorem 5.3, $\mathcal{F}(s) \subseteq \mathcal{F}(s')$ implies that $s \precsim s'$, thus $s \precsim_\omega s'$. This implies that $\mathcal{L}^{\precsim}$ is complete for $\precsim_\omega$. The soundness, however, does not follow. In the following theorem, we use the fragment $\mathcal{F}_{\mathcal{L}^{\precsim},\omega}$, namely the set of formulas of finite depth, to characterize $\precsim_\omega$.

Theorem 5.4. *Given the logic $\mathcal{L}^{\precsim}$ restricted to formulas with finite depth, for each pair of states s, s' of a PA, $s \precsim_\omega s'$ iff $\mathcal{F}_\omega(s) \subseteq \mathcal{F}_\omega(s')$.*

Proof. For soundness let $s \precsim_\omega s'$, which implies $\delta_s \precsim_\omega \delta_{s'}$. Since $\mathcal{F}_\omega(s) = \mathcal{F}_\omega(\delta_s) = \cup_{n\in\mathbb{N}} \mathcal{F}_n(s)$, it is sufficient to show the following implication:

$$\forall \mu, \mu' \in Dist(S).\ \forall n \in \mathbb{N}.\ \mu \precsim_n \mu' \Longrightarrow \mathcal{F}_{\mathcal{L}^{\precsim},n}(\mu) \subseteq \mathcal{F}_{\mathcal{L}^{\precsim},n}(\mu'). \tag{5}$$

Let $\mu, \mu' \in Dist(S)$ be arbitrary distributions. We prove the implication by induction on n, where for each n we proceed by induction on the structure of the formula φ. The structural induction follows in exactly the same way as the proof of Theorem 5.3. The base case ($n = 0$) considers only formulas out of $\mathcal{F}_0$ which do not contain any formulas with $\langle a\rangle$. Since the first three cases of the inductive step below do not rely on the inductive hypothesis on n, they suffice the base case $n = 0$ as well. For the inductive step on n, suppose $\mu \precsim_n \mu' \Rightarrow \mathcal{F}_n(\mu) \subseteq \mathcal{F}_n(\mu')$. Let $\mu \precsim_{n+1} \mu'$ (with weight function Δ).

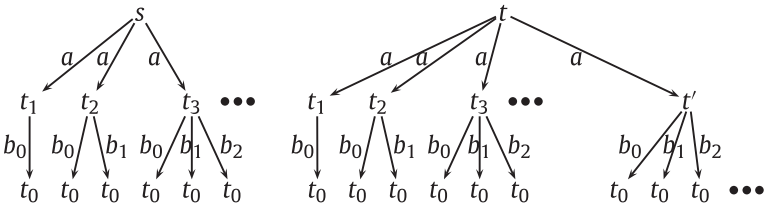

Fig. 4. An example for illustrating that finite conjunction is not sufficient to characterize $\precsim_\omega$.

Let $\varphi \in \mathcal{F}_{n+1}$, and assume $\varphi \in \mathcal{F}_{n+1}(\mu)$. It remains to prove $\varphi \in \mathcal{F}_{n+1}(\mu')$, i.e., $\mu' \models \varphi$. The cases $\varphi = \top$, $\bigwedge_{i\in I} \psi_i$ and $\psi_1 \vee \psi_2$ are easy. For other cases:

- If $\varphi = [\psi]_p$, then $\mu([\![\psi]\!]) \geq p$. By hypothesis of the structural induction, $[\![\psi]\!]$ is upwards $\precsim_{n+1}$-closed. By Lemma 3.1.(*a*), we have $\mu([\![\psi]\!]) \leq \mu'([\![\psi]\!])$, proving $\mu' \models \varphi$.
- If $\varphi = \langle a\rangle\psi$: $\varphi \in \mathcal{F}_{n+1}$ implies that $\psi \in \mathcal{F}_n$. We show $s_2 \models \varphi$ for arbitrary, fixed $s_2 \in \mathit{Supp}(\mu')$. Observe that $s_2 \in \mathit{Supp}(\mu')$ and $\mu \precsim_{n+1} \mu'$ implies that there exists $s_1 \in \mathit{Supp}(\mu)$ such that $\Delta(s_1, s_2) > 0$. By the definition of weight function, it holds that $(s_1, s_2) \in \precsim_{n+1}$. Moreover, $\mu \models \varphi$ implies that there exists $s_1 \xrightarrow{a} \mu_1$ with $\mu_1 \models \psi$. By definition of $\precsim_{n+1}$, there exists a transition $s_2 \xrightarrow{a} \mu_2$ such that $\mu_1 \precsim_n \mu_2$. Since $\psi \in \mathcal{F}_n$, by the inductive hypothesis on n, we have that $\mu_2 \models \psi$, implying that $s_2 \models \varphi$.

Now we prove completeness. Assume that $\mathcal{F}_\omega(s) \subseteq \mathcal{F}_\omega(s')$ holds. Recall $\mathcal{F}_\omega(s) = \cup_{n\in\mathbb{N}}\mathcal{F}_n(s)$. By induction on n, we have $\mathcal{F}_n(s) \subseteq \mathcal{F}_n(s')$ for all n. We define a family of relations R_n as follows: $R_n = \{(s, s') | \mathcal{F}_n(s) \subseteq \mathcal{F}_n(s')\}$. Obviously, R_n is a preorder for all n. It is sufficient to show $R_n \subseteq \precsim_n$ for all n. We prove the claim by induction on n. The base case is trivial since $s \precsim_0 s'$ holds. For the induction step, assume that $R_n \subseteq \precsim_n$. We need to show $R_{n+1} \subseteq \precsim_{n+1}$. Let $s\ R_{n+1}\ s'$ and $s \xrightarrow{a} \mu$. It suffices to find μ' such that $s' \xrightarrow{a} \mu'$ and $\mu\ R_n\ \mu'$. Since by definition, we then have $s \precsim_{n+1} s'$, implying $R_{n+1} \subseteq \precsim_{n+1}$.

To find the μ' with $s' \xrightarrow{a} \mu'$ and $\mu\ R_n\ \mu'$, we follow the same part of the completeness proof of Theorem 5.3: let $\{[s_j]\}_{j\in J}$ be an enumeration of the equivalence classes of $\equiv_{R_n}$. We first introduce the characterizing formula of upwards-closed set $cl([s_l])$ for $l \in J$. By definition of R_n, for each $m \in J$ with $s_m \notin cl([s_l])$, there exists a formula $\varphi_{lm} \in \mathcal{F}_n$ such that $s_l \models \varphi_{lm}$ and $s_m \not\models \varphi_{lm}$. For each $l \in J$, define $\varphi_l = \bigwedge_{s_m\notin cl([s_l])} \varphi_{lm}$. Then, by construction, for $l \in J$ we have $\varphi_l \in \mathcal{F}_n$ and $[\![\varphi_l]\!] = cl([s_l])$. Let $\{U_i\}_{i\in I}$ be the countable set of the finitely-generated upwards R_n-closed sets. By Lemma 5.2, it is sufficient to show that $\mu(U_i) \leq \mu'(U_i)$ for all $i \in I$. Since U_i is finitely-generated, there exists a finite index set $K_i \subseteq J$ such that $U_i = \bigcup_{k\in K_i} cl([s_k])$. For each $i \in I$, define $\varphi_{K_i} = \vee_{l\in K_i}\varphi_l$. Then, $\varphi_{K_i} \in \mathcal{F}_n$ is satisfied only by states in U_i, that is, $[\![\varphi_{K_i}]\!] = U_i$. Now, define $\varphi = \bigwedge_{i\in I}[\varphi_{K_i}]_{p_i}$ with $p_i = \mu(U_i)$ for $i \in I$. By definition, $\mu \models \varphi$, implying that $s \models \langle a\rangle\varphi$. Since $\langle a\rangle\varphi \in \mathcal{F}_{n+1}(s)$, by the definition of R_{n+1}, $s' \models \langle a\rangle\varphi$ as well. Thus, there exists a distribution μ' such that $s' \xrightarrow{a} \mu'$ and $\mu' \models \varphi$. By definition, $\mu'(U_i) = \mu'([\![\varphi_{K_i}]\!]) \geq p_i = \mu(U_i)$ for each $i \in I$, as needed. □

Note that the set of formulas in $\mathcal{L}$ with infinite depth has the power of distinguishing $\precsim$ and $\precsim_\omega$, which is the same case as for LTSs. In Example 5.1 we have constructed a formula with infinite depth for illustrating that binary conjunction is not sufficient for characterizing $\precsim$. In the following example we show that for LTSs (thus also for PAs) finite conjunction is also not sufficient to characterize $\precsim_\omega$.

Example 5.2. Consider Fig. 4. It is easy to see that $t \not\precsim_\omega s$. The formula φ defined as $\langle a\rangle \bigwedge_{i\in\mathbb{N}}\langle b_i\rangle\top$ is satisfied by t but not s. By structural induction, it is a routine exercise to show that with only binary conjunctions s and t cannot be differentiated.

5.4. Logical characterization of $\precsim$ for image-finite PAs

In this section, we consider image-finite PAs. Recall from Lemma 3.5, for an image-finite PA $\mathcal{M} = (S, \mathit{Act}, \mathit{Steps})$, $\precsim$ and $\precsim_\omega$ coincide. Given the logic $\mathcal{L}^{\precsim}$, then, together with Theorem 5.3 and Theorem 5.4, we have for $s, s' \in S$:

$$\mathcal{F}(s) \subseteq \mathcal{F}(s') \iff s \precsim s' \iff s \precsim_\omega s' \iff \mathcal{F}_\omega(s) \subseteq \mathcal{F}_\omega(s').$$

This implies that both $\mathcal{L}^{\precsim}$, and $\mathcal{L}_\omega^{\precsim}$ characterize $\precsim = \precsim_\omega$ for image-finite PAs. Stated differently, for image-finite PAs, the distinguishing power for formulas of infinite length disappears. We show in the following theorem an even stronger result, namely that the logic $\mathcal{L}^{\precsim}$ restricted to finite conjunction (thus formulas are also of finite depth) is sufficient to characterize simulation for image-finite PAs.

Theorem 5.5. *Given the logic $\mathcal{L}^{\precsim}$ restricted to only binary conjunctions, for each pair of states s, s' of an image-finite PA, $s \precsim s'$ iff $\mathcal{F}(s) \subseteq \mathcal{F}(s')$.*

Theorem 5.3 implies soundness trivially. The completeness proof of Theorem 5.3, however, is not strong enough anymore, since it is based on formulas with infinite conjunctions (namely formula φ_l). Below we show how to avoid this for image-finite PAs.

The crucial point is the construction of an infinite sequence of formulas of *finite* depth, whose behaviors converge to φ_l. This idea is borrowed from Desharnais et al. [5,18,33] where it is shown that binary conjunction is sufficient to characterize simulation and bisimulation for LMPs (image-finite PAs with continuous state space and deterministic transition with respect to the same action).

Proof. Assume $\mathcal{F}(s) \subseteq \mathcal{F}(s')$, and let the relation R, $\{[s_j]\}_{j\in J}$, $\{\varphi_{lm}\}_{m\notin cl([s_j])}$, $\{U_i\}_{i\in I}$ and the corresponding finite index sets $\{K_i\}_{i\in I}$ as defined in Theorem 5.3. We fix an arbitrary index $k \in J$. For each $l \in J$, define $\Phi_l^k = \bigwedge_{m\le k \wedge s_m \notin cl([s_l])} \varphi_{lm}$. Intuitively, Φ_l^k is satisfied by all the states in $cl([s_l])$, but not satisfied by states in $[s_x]$ with $s_x \notin cl([s_l]) \wedge x \le k$. However, since the maximal index of the finite conjunction is k, Φ_l^k may be satisfied by the states in $[s_x]$ with $x > k$. For $i \in I$, define $p_i = \mu(U_i)$, $\Phi_{K_i}^k = \vee_{l\in K_i} \Phi_l^k$ and $\Phi^k = \bigwedge_{j\in I\wedge j\le k} [\Phi_{K_j}^k]_{p_j}$. It holds that, for $i \in I$:

$$U_i \subseteq [\![\Phi_{K_i}^k]\!] \subseteq U_i \cup \bigcup_{j\in I\wedge j>k} cl([s_j]). \tag{6}$$

Let $(s, s') \in R$ and $s \xrightarrow{a} \mu$, we now show the existence of $s' \xrightarrow{a} \mu'$ with $\mu(U_i) = p_i \le \mu'(U_i)$ for all $i \in I$. Because of the left part of Eq. (6), we have $\mu(U_i) = p_i \le \mu([\![\Phi_{K_i}^k]\!])$ for all $i \le k$, implying $\mu \models \Phi^k$, thus $s \models \langle a\rangle \Phi^k$. Since k is arbitrary, $s \models \langle a\rangle \Phi^k$ for all $k \in J$. Since the index set K_i is finite for all $i \in I$, all of the formulas Φ^k are finite. Thus, by definition of R, $s' \models \langle a\rangle \Phi^k$ holds for all $k \in I$. The set $Steps_a(s')$ is finite for image-finite PAs, thus the Pigeonhole principle applies and, there exists $s' \xrightarrow{a} \mu'$ such that $\mu' \models \Phi^k$ for infinitely many indices $k \in Z$ with $Z \subseteq I$. This implies for $k \in Z$ and $i \in I$:

$$p_i \le \mu'([\![\Phi_{K_i}^k]\!]) \overset{(6)}{\le} \mu'(U_i) + \mu'\left(\bigcup_{j\in I\wedge j>k} cl([s_j])\right). \tag{7}$$

The sequence $\left\{\mu'\left(\bigcup_{j\in I\wedge j>k} cl([s_j])\right)\right\}_{k\in Z}$ is monotone non-increasing, and converges to 0. Taking $\lim_{k\to\infty}$ on both sides leads to $p_i \le \mu'(U_i)$ as needed. □

5.5. Probabilistic simulation

To simplify matters a bit, we first prove a lemma which generalizes the definition of probabilistic simulation. It shows that, if $s \precsim^p s'$, then each combined transition performed by s can be simulated by a combined transition of s'.

Lemma 5.6

1. *For each pair of states s, s', if $s \precsim^p s'$, then, for each combined transition $s \overset{a}{\rightsquigarrow} \mu$, there exists a combined transition $s' \overset{a}{\rightsquigarrow} \mu$ such that $\mu \precsim^p \mu'$.*
2. *For each pair of states s, s' and for each n, if $s \precsim^p_{n+1} s'$, then, for each combined transition $s \overset{a}{\rightsquigarrow} \mu$, there exists a combined transition $s' \overset{a}{\rightsquigarrow} \mu$ such that $\mu \precsim^p_n \mu'$.*

Proof. By definition, given $s \overset{a}{\rightsquigarrow} \mu$, there exists $\mu = \sum_{i\in I} p_i\mu_i$ with $\mu_i \in Steps_a(s)$ for $i \in I$. By definition, for each $\mu_i \in Steps_a(s)$, there exists a combined transition $s' \overset{a}{\rightsquigarrow} \mu_i'$ such that $\mu_i \precsim^p \mu_i'$. Define $\mu' = \sum_{i\in I} p_i\mu_i'$. This means that there exists a combined transition $s \overset{a}{\rightsquigarrow} \mu'$, and $\mu \precsim^p \mu'$ by construction. The proof of the second part follows in a similar way. □

The following theorem states the soundness and completeness result for the logic $\mathcal{L}_p^{\precsim}$ with respect to probabilistic simulation. For image-finite PAs, we also show that logic $\mathcal{L}_p^{\precsim}$ with only binary conjunction is sufficient.

Theorem 5.7

1. *Given the logic $\mathcal{L}_p^{\precsim}$, for each pair of states s and s' of a PA, $s \precsim^p s'$ iff $\mathcal{F}(s) \subseteq \mathcal{F}(s')$.*
2. *Given the logic $\mathcal{L}_p^{\precsim}$ restricted to formulas with finite depth, for each pair of states s and s' of a PA, $s \precsim^p_\omega s'$ iff $\mathcal{F}_\omega(s) \subseteq \mathcal{F}_\omega(s')$.*
3. *Given the logic $\mathcal{L}_p^{\precsim}$ restricted to only binary conjunctions, for each pair of states s, s' of an image-finite PA, $s \precsim^p s'$ iff $\mathcal{F}(s) \subseteq \mathcal{F}(s')$.*

Proof. The soundness of the theorem follows by the following statements:

$$\forall \mu, \mu' \in Dist(S).\ \mu \precsim^p \mu' \Longrightarrow \mathcal{F}_{\mathcal{L}_{\widetilde{p}}^{\precsim}}(\mu) \subseteq \mathcal{F}_{\mathcal{L}_{\widetilde{p}}^{\precsim}}(\mu')$$
$$\forall \mu, \mu' \in Dist(S).\ \forall n \in \mathbb{N}.\ \mu \precsim_n^p \mu' \Longrightarrow \mathcal{F}_{\mathcal{L}_{\widetilde{p}}^{\precsim},n}(\mu) \subseteq \mathcal{F}_{\mathcal{L}_{\widetilde{p}}^{\precsim},n}(\mu').$$

Combining with Lemma 5.6, the proof for them can be obtained by using combined transitions $\overset{a}{\rightsquigarrow}$ instead of $\xrightarrow{a}$ in the proofs of (4) and (5), respectively.

The completeness proofs proceed similarly to the completeness proofs of Theorems 5.3, 5.4 and 5.5, respectively, by using the adequate semantics for the temporal operator and combined transitions where necessary. The Pigeonhole principle of Theorem 5.5, however, does not apply to the last claim directly because there are infinitely many combined transitions, even for image-finite PAs. Fortunately, this can be repaired by exploiting Lemma 3.6: Let $s' \overset{a}{\rightsquigarrow} \mu'_k$ be the infinite sequence of combined transitions such that $\mu'_k \models \Phi^k$ for all $k \in I$ (cf. proof of Theorem 5.5). By Lemma 3.6, there exists a subsequence $\{\mu'_k\}_{k\in J'}$ such that $J' \subseteq I$ and $\mu' := \lim_{k\in J} \mu'_k$ exists, and moreover, $s' \overset{a}{\rightsquigarrow} \mu'$. Thus, $\mu'_k \models \Phi^k$ for infinitely many indices $k \in J'$. By the set inclusion in (6), for $k \in J'$ and $i \in I$, we have:

$$p_i \leq \mu'_k([\![\Phi^k_{K_i}]\!]) \overset{(6)}{\leq} \mu'_k(U_i) + \mu'_k\left(\bigcup_{j\in I \wedge j>k} cl([s_j])\right).$$

Similar to Inequality (7), taking the limit over $k \in J'$, we have $p_i \leq \lim_{k\in J'} \mu'_k(U_i) + 0 = \mu'(U_i)$ which completes the proof. □

6. Logical characterization of bisimulation

In this section, we consider logical characterization of bisimulations. As for simulations, we consider image-infinite PAs, and also the special case of image-finite PAs. For image-infinite PAs, we show that $\sim$ can be characterized by $\mathcal{L}$ in Theorem 6.1, and $\sim_\omega$ can be characterized by the sub-logic of $\mathcal{L}$ restricted to formulas with finite depth in Theorem 6.2. For image-finite PAs, it is then shown in Theorem 6.3 that $\mathcal{L}$ restricted to binary conjunction is sufficient.

We give a short discussion of the main differences to the corresponding proofs for simulations (Theorems 5.3, 5.4 and 5.5, respectively). Since the logic used to characterize simulations is a sub-logic of the corresponding one for characterizing bisimulations, the soundness proof needs to be extended with negations. To this end, the soundness proof has to be adjusted slightly (cf. (8)): for distributions μ, μ' and formula φ, $\mathcal{F}(\mu) = \mathcal{F}(\mu')$ is shown by structural induction. It is interesting to note that showing separately $\mathcal{F}(\mu) \subseteq \mathcal{F}(\mu')$ and $\mathcal{F}(\mu') \subseteq \mathcal{F}(\mu)$ would not work, as the induction step with respect to negations would then fail. The completeness proofs are, in general, less involved than the corresponding proofs for simulations because the characterizing formulas are easier to construct in presence of equivalence classes.

Theorem 6.1. *Given the logic $\mathcal{L}$, for each pair of states s, s' of a PA, $s \sim s'$ iff $\mathcal{F}(s) = \mathcal{F}(s')$.*

Proof. First, we show soundness. It is sufficient to show that:

$$\forall \mu, \mu' \in Dist(S).\ \mu \sim \mu' \Longrightarrow \mathcal{F}_{\mathcal{L}}(\mu) = \mathcal{F}_{\mathcal{L}}(\mu'). \tag{8}$$

Let $\mu, \mu' \in Dist(S), \mu \sim \mu'$ and $\varphi \in \mathcal{F}$: we show $\mu \models \varphi \Leftrightarrow \mu' \models \varphi$ by structural induction on φ. The cases $\varphi = \top$, $\bigwedge_{i\in I} \psi_i$ are trivial. Now we consider other cases:

- If $\varphi = \neg\psi$: $\mu \models \varphi \Leftrightarrow \neg(\mu \models \psi)$. By structural induction, we have the equivalence $\mu \models \psi \Leftrightarrow \mu' \models \psi$, thus $\mu \models \varphi \Leftrightarrow \neg(\mu' \models \psi) \Leftrightarrow \mu' \models \varphi$.
- If $\varphi = \langle a\rangle\psi$: Assuming $\mu \models \varphi$, we show that $\mu' \models \varphi$ (the other direction is similar). Let $s_2 \in Supp(\mu')$. Since $\mu'(s_2) > 0$ and $\mu \sim \mu'$, then $\mu'([s_2]) = \mu([s_2]) > 0$. Thus, there exists an element $s_1 \in Supp(\mu)$ such that $s_1 \sim s_2$. The fact that $\mu \models \varphi$ implies that there exists $s_1 \xrightarrow{a} \mu_1$ with $\mu_1 \models \psi$. Thus, there exists $s_2 \xrightarrow{a} \mu_2$ with $\mu_1 \sim \mu_2$. By induction hypothesis, we have that $\mu_2 \models \psi$, implying that $s_2 \models \varphi$. Then, $\mu' \models \varphi$ follows by definition.
- If $\varphi = [\psi]_p$: Assuming $\mu \models \varphi$, we show that $\mu' \models \varphi$ (the other direction is similar). Let $s, s' \in S$ with $s \sim s'$. By hypothesis, δ_s satisfies ψ iff $\delta_{s'}$ satisfies ψ. Thus, ψ is satisfied either by all or none of the states of an equivalence class of $\sim$, and $[\![\psi]\!]$ is a union of equivalence classes of $\sim$. Since $\mu \sim \mu'$ holds, $\mu([\![\psi]\!]) = \mu'([\![\psi]\!])$. Since $\mu \models \varphi$ implies that $\mu([\![\psi]\!]) \geq p$, thus $\mu'([\![\psi]\!]) \geq p$ and $\mu' \models [\psi]_p$ as needed.

For completeness, we define $R = \{(s, s') | \mathcal{F}_{\mathcal{L}}(s) = \mathcal{F}_{\mathcal{L}}(s')\}$. Obviously, R is an equivalence relation. It is sufficient to show that R is a bisimulation relation. Let $\{[s_j]\}_{j\in J}$ be an enumeration of the equivalence classes of R. By definition of R, for each $l, m \in J$, there exists a formula $\varphi_{lm} \in \mathcal{F}$ such that $s_l \models \varphi_{lm}$ and $s_m \not\models \varphi_{lm}$. For each $l \in J$, define $\varphi_l = \bigwedge_{m\neq l} \varphi_{lm}$, then, $[\![\varphi_l]\!] = [s_l]$.

Now let $(s, s') \in R$, and $s \xrightarrow{a} \mu$: it remains to show that there exists a transition $s' \xrightarrow{a} \mu'$ with $\mu([s_i]) = \mu'([s_i])$ for all $i \in J$. Define $\varphi = \bigwedge_{i\in J}[\varphi_i]_{p_i}$ with $p_i = \mu([s_i])$ for $i \in J$. By definition, $\mu \models \varphi$, implying that $s \models \langle a\rangle\varphi$. By the definition of R, $s' \models \langle a\rangle\varphi$ as well. Thus, there exists a distribution μ' such that $s' \xrightarrow{a} \mu'$ and $\mu' \models \varphi$. By definition, $\mu'([s_i]) = \mu'([\![\varphi_i]\!]) \geq p_i = \mu([s_i])$ for each $i \in J$. Since $\sum_{i\in J} p_i = 1$, we have $\mu([s_i]) = \mu'([s_i])$ for $i \in J$, as needed. □

Below we characterize the ω-bisimulation $\sim_\omega$. The soundness follows by structural induction on the formulas. Additionally, because of the iteratively defined $\sim_\omega$, another induction on n is needed. We give the full proof, which is not difficult in the light of the theory developed so far.

Theorem 6.2. *Given the logic $\mathcal{L}$ restricted to formulas with finite depth, for each pair of states s, s' of a PA, $s \sim_\omega s'$ iff $\mathcal{F}_\omega(s) = \mathcal{F}_\omega(s')$.*

Proof. For the soundness proof, we show the following implication:

$$\forall \mu, \mu' \in \mathit{Dist}(S).\ \forall n \in \mathbb{N}.\ \mu \sim_n \mu' \Longrightarrow \mathcal{F}_{\mathcal{L},n}(\mu) = \mathcal{F}_{\mathcal{L},n}(\mu'). \tag{9}$$

Let μ, μ' as above, we prove the implication by induction on n, where for each n we proceed by induction on the structure of the formula φ. The base case ($n = 0$) considers only formulas out of $\mathcal{F}_0$, which can be handled easily (cf. Theorem 5.4). For the inductive step on n, suppose soundness holds for n, i.e., $\mu \sim_n \mu' \Rightarrow \mathcal{F}_n(\mu) = \mathcal{F}_n(\mu')$. Let $\mu \sim_{n+1} \mu'$. It remains to prove $\mathcal{F}_{n+1}(\mu) = \mathcal{F}_{n+1}(\mu')$, i.e., for all $\varphi \in \mathcal{F}_{n+1}$, $\mu \models \varphi \Leftrightarrow \mu' \models \varphi$. The proof follows by structural induction on φ. The cases $\varphi = \top$, $\bigwedge_{i\in I} \psi_i$ are easy. Now we consider other cases:

- If $\varphi = \neg\psi$: $\mu \models \varphi \Leftrightarrow \neg(\mu \models \psi)$. Since $\psi \in \mathcal{F}_{n+1}$ as well, by structural induction, we have $\mu \models \psi \Leftrightarrow \mu' \models \psi$, thus $\mu \models \varphi \Leftrightarrow \neg(\mu' \models \psi) \Leftrightarrow \mu' \models \varphi$.
- If $\varphi = \langle a\rangle\psi$: assuming $\mu \models \varphi$, we show that $\mu' \models \varphi$ (the other direction is similar). Let $s_2 \in \mathit{Supp}(\mu')$. Since $\mu'(s_2) > 0$ and $\mu \sim_{n+1} \mu'$, then $\mu'([s_2]) = \mu([s_2]) > 0$, and there exists $s_1 \in \mathit{Supp}(\mu)$ such that $s_1 \sim_{n+1} s_2$. The fact that $\mu \models \varphi$ implies that there exists $s_1 \xrightarrow{a} \mu_1$ with $\mu_1 \models \psi$. Thus, there exists $s_2 \xrightarrow{a} \mu_2$ with $\mu_1 \sim_n \mu_2$. Since $\psi \in \mathcal{F}_n$, by induction hypothesis on n, it holds $\mu_2 \models \psi$, thus $s_2 \models \varphi$. Then, $\mu' \models \varphi$ follows by definition.
- If $\varphi = [\psi]_p$: assuming $\mu \models \varphi$, we show $\mu' \models \varphi$ (the other direction is similar). For $\psi \in \mathcal{F}_{n+1}$, $[\![\psi]\!]$ is a union of equivalence classes of $\sim_{n+1}$. Since $\mu \sim_{n+1} \mu'$ holds, we have $\mu([\![\psi]\!]) = \mu'([\![\psi]\!])$. Since $\mu \models \varphi$ implies that $\mu([\![\psi]\!]) \geq p$, thus $\mu'([\![\psi]\!]) \geq p$ and thus, $\mu' \models [\psi]_p$ as needed.

Now we prove completeness. Assume that $\mathcal{F}_\omega(s) = \mathcal{F}_\omega(s')$ holds. By induction on n, we get immediately $\mathcal{F}_n(s) = \mathcal{F}_n(s')$ for all n. We define a family of relations R_n as follows: $R_n = \{(s, s') | \mathcal{F}_n(s) = \mathcal{F}_n(s')\}$. Obviously, R_n is an equivalence relation for all n. It is sufficient to show $R_n \subseteq \sim_n$ for all n. We proceed by induction on n. The base case is trivial since $s \sim_0 s'$ holds. For the induction step, assume that $R_n \subseteq \sim_n$. We need to show $R_{n+1} \subseteq \sim_{n+1}$. Let $s\ R_{n+1}\ s'$ and $s \xrightarrow{a} \mu$. It suffices to find μ' such that $s' \xrightarrow{a} \mu'$ and $\mu\ R_n\ \mu'$, since then by induction hypothesis $\mu \sim_n \mu'$. By definition, we then have $s \sim_{n+1} s'$, implying $R_{n+1} \subseteq \sim_{n+1}$.

To find the μ' with $s' \xrightarrow{a} \mu'$ and $\mu\ R_n\ \mu'$, we follow the same part of the completeness proof of Theorem 6.1: let $\{[s_j]\}_{j\in J}$ be an enumeration of the equivalence classes of R_n. By definition of R_n, for each $l, m \in J$, there exists a formula $\varphi_{lm} \in \mathcal{F}_n$ such that $s_l \models \varphi_{lm}$ and $s_m \not\models \varphi_{lm}$. For each $l \in J$, define $\varphi_l = \bigwedge_{m\neq l} \varphi_{lm}$. Then, by construction, for $l \in J$ we have $\varphi_l \in \mathcal{F}_n$ and $[\![\varphi_l]\!] = [s_l]$. Now, define $\varphi = \bigwedge_{i\in J}[\varphi_i]_{p_i}$ with $p_i = \mu([s_i])$ for $i \in J$. By definition, $\mu \models \varphi$, implying that $s \models \langle a\rangle\varphi$. Since $\langle a\rangle\varphi \in \mathcal{F}_{n+1}(s)$, by the definition of R_{n+1}, $s' \models \langle a\rangle\varphi$ as well. Thus, there exists a distribution μ' such that $s' \xrightarrow{a} \mu'$ and $\mu' \models \varphi$. By definition, $\mu'([s_i]) = \mu'([\![\varphi_i]\!]) \geq p_i = \mu([s_i])$ for each $i \in I$. Since $\sum_{i\in J} p_i = 1$, we have $\mu([s_i]) = \mu'([s_i])$ for $i \in J$, as needed. □

In [15], image-finite PAs were considered, and it was shown that $\mathcal{L}$ (with infinite conjunction) characterizes bisimulation soundly and completely. In the following theorem we show that, as for simulations, binary conjunction is already sufficient to characterize bisimulations.

Theorem 6.3. *Given the logic $\mathcal{L}$ restricted to only binary conjunction, for each pair of states s, s' of an image-finite PA, $s \sim s'$ iff $\mathcal{F}(s) = \mathcal{F}(s')$.*

Proof. Theorem 6.1 implies soundness. For completeness let R and $\{[s_j]\}_{j\in J}$ be defined as there. We fix an arbitrary index $k \in J$. For each $l \in J$, define $\Phi_l^k = \bigwedge_{m\leq k} \varphi_{lm}$. It is then easy to show that for $l \in J$, it holds:

$$[s_l] \subseteq [\![\Phi_l^k]\!] \subseteq [s_l] \cup \bigcup_{j\in J\wedge j>k} [s_j]. \tag{10}$$

For $k \in J$, define $\Phi^k = \bigwedge_{j\in J\wedge j\leq k}[\Phi_j^k]_{p_j}$ where $p_j = \mu([s_j])$.

Let $(s, s') \in R$ and $s \xrightarrow{a} \mu$, we want to show that there exists a transition $s' \xrightarrow{a} \mu'$ with $\mu([s_i]) = \mu'([s_i])$, i.e., $p_i = \mu'([s_i])$ for all $i \in J$. For $i \in J$, by the set inclusion in (10), we have $\mu([\![\Phi_i^k]\!]) \geq \mu([s_i]) = p_i$ for $i \leq k$, implying $\mu \models \Phi^k$, thus $s \models \langle a \rangle \Phi^k$. By construction, all of the formulas Φ^k contain only binary conjunctions. By definition of R, $s' \models \langle a \rangle \Phi^k$ holds for all $k \in J$. The set $Steps_a(s')$ is finite for image-finite PAs, thus the Pigeonhole principle applies and, there exists $s' \xrightarrow{a} \mu'$ such that $\mu' \models \Phi^k$ for infinitely many indices $k \in Z$ with $Z \subseteq J$. This implies for $k \in Z$ and $i \in J$ with $i \leq k$:

$$p_i \leq \mu'([\![\Phi_i^k]\!]) \overset{(10)}{\leq} \mu'([s_i]) + \mu'\left(\bigcup_{j \in J \wedge j > k} [s_j]\right). \tag{11}$$

The sequence $\left\{\mu'\left(\bigcup_{j \in J \wedge j > k}[s_j]\right)\right\}_{k \in Z}$ is monotone non-increasing, and converges to 0. Taking $\lim_{k \to \infty}$ on both sides leads to $p_i \leq \mu'([s_i])$ as needed. □

6.1. Probabilistic bisimulation

Now we consider the logic $\mathcal{L}_p$ for probabilistic bisimulation. First, we prove a lemma which generalizes the definition of probabilistic bisimulation, showing that if two states s and s' are probabilistically bisimilar, then each *combined* transition performed by s can be simulated by a *combined* transition performed by the state s'.

Lemma 6.4

1. *For each pair of states s, s' and for each n, if $s \sim^p s'$, then, for each combined transition $s \overset{a}{\rightsquigarrow} \mu$, there exists a combined transition $s' \overset{a}{\rightsquigarrow} \mu'$ such that $\mu \sim^p \mu'$.*
2. *For each pair of states s, s' and for each n, if $s \sim^p_{n+1} s'$, then, for each combined transition $s \overset{a}{\rightsquigarrow} \mu$, there exists a combined transition $s' \overset{a}{\rightsquigarrow} \mu'$ such that $\mu \sim^p_n \mu'$.*

Proof. The proof follows in a similar way as the proof of Lemma 5.6. □

Theorem 6.5

1. *Given the logic $\mathcal{L}_p$, for each pair of states s, s' of a PA, $s \sim^p s'$ iff $\mathcal{F}(s) = \mathcal{F}(s')$.*
2. *Given the logic $\mathcal{L}_p$ restricted to formulas with finite depth, for each pair of states s, s' of a PA, $s \sim^p_\omega s'$ iff $\mathcal{F}_\omega(s) = \mathcal{F}_\omega(s')$.*
3. *Given the logic $\mathcal{L}_p$ restricted to only binary conjunction, for each pair of states s, s' of an image-finite PA, $s \sim^p s'$ iff $\mathcal{F}(s) = \mathcal{F}(s')$.*

Proof. The soundness follows directly by the following statements:

$$\forall \mu, \mu' \in Dist(S).\ \mu \sim^p \mu' \Longrightarrow \mathcal{F}_{\mathcal{L}_p}(\mu) = \mathcal{F}_{\mathcal{L}_p}(\mu')$$
$$\forall \mu, \mu' \in Dist(S).\ \forall n \in \mathbb{N}.\ \mu \sim^p_n \mu' \Longrightarrow \mathcal{F}_{\mathcal{L}_p,n}(\mu) = \mathcal{F}_{\mathcal{L}_p,n}(\mu').$$

Combining with Lemma 6.4, the proof for them can be obtained by using combined transitions $\overset{a}{\rightsquigarrow}$ instead of $\xrightarrow{a}$ in the proofs of (8) and (9), respectively. The completeness proof is similar to the completeness proof of Theorems 6.1, 6.2, 6.3, respectively, by using the adequate semantics for the temporal operator and combined transitions where necessary. The Pigeonhole principle used in Theorem 6.3 can be adapted exactly the same way as Theorem 5.7. □

7. Related work

7.1. Bisimulation

This paper gives a taxonomy of logical characterization results for probabilistic automata. While these are novel results for PA, logical characterizations of simulation and bisimulation for discrete-time and continuous-time Markov chains are well-studied.

For discrete-time Markov chains (DTMCs), the logic PCTL [11,34] characterizes bisimulations, while PCTL without next-state formulas characterizes weak bisimulations. The logic CSL characterizes bisimulations for continuous-time Markov chains (CTMCs), and CSL without next-state formulas characterizes weak bisimulations [34]. A subset of the logic CSL is actually sufficient for CTMCs and bisimulations even in a setting with continuous state spaces [35].

Hennessy and Milner [17] have introduced a simple modal logic with a single temporal operator $\langle a \rangle$. The operator $\langle a \rangle$ is interpreted over states: state s satisfies $\langle a \rangle \varphi$ if there exists a transition $s \xrightarrow{a} s'$ such that s' satisfies φ. They have shown that,

for usual image-finite labeled transition systems (LTSs), the logic characterizes bisimulation soundly and completely. van Glabbeek [36] has considered image-infinite LTSs, and has also extended the binary conjunction of the Hennessy and Milner logic with an infinite conjunction operator. With this extended logic (and sub-logic without negations) he has characterized bisimulation (and simulation) soundly and completely, and moreover, he has also characterized bisimulation up to $\sim_\omega$ with the sub-logic consisting of only formulas of finite depth.

For probabilistic systems, Larsen and Skou [2] equipped the modal operator $\langle a\rangle$ of Hennessy–Milner logic with a real value in the interval $p \in [0, 1]$ to characterize probabilistic transitions. Intuitively, state s satisfies $\langle a\rangle_p\varphi$ if there exists a transition $s \xrightarrow{a} \mu$ such that $\mu([\![\varphi]\!]) \geq p$, where $[\![\varphi]\!]$ can be computed recursively. It has been shown that this simple extension characterizes bisimulation for *reactive systems* [2] (non-determinism within the same action is not modeled), or labeled Markov processes [28] (reactive systems but with continuous state space). For probabilistic automata, Jonsson et al. [37] considered image-finite PAs with a *finite* set of states and showed that bisimulation and probabilistic bisimulation can be characterized by the following two-sorted logic:

$$\begin{aligned} F &::= \top \mid \neg F \mid F \wedge F \mid \langle a\rangle\varphi \\ \varphi &::= \top \mid \neg\varphi \mid \varphi \wedge \varphi \mid [F]_p. \end{aligned} \tag{12}$$

While non-deterministic formulas F are interpreted over states as usual, probabilistic formulas φ are interpreted over distributions. Thus our logic for (probabilistic) bisimulations, originally introduced in [15], can be considered as an integration of the two-sorted logic into one level. Recently, D'Argenio et al. [38] have extend that two-sorted logic to characterize bisimulations for non-deterministic labeled Markov processes.

7.2. Weak bisimulation

Weak bisimulation was first defined in the context of PAs by Segala and Lynch [1], and then formulated for alternating models by Philippou et al. [39]. Alternating models can be translated to PAs, and in [40] it is shown that the definition for alternating models is essentially the one for PAs. In [28], Desharnais et al. have defined an alternative equivalent definition of weak probabilistic bisimulation, and shown that the logic PCTL* is sufficient to characterize weak probabilistic bisimulations for image-finite alternating models. For the completeness proof, a requirement of compactness to the space of reachable distributions is needed. It is interesting to see whether the results of this paper can be extended to weak simulations and bisimulations for PAs, together with some compactness arguments along those of [28]. Partial results already appear in [41].

A logical characterization of an even weaker relation, called *trace distribution precongruence*, has been studied in [42]. A new operator $\oplus$, which has more distinguishing power with respect to distributions, has been introduced for this purpose.

7.3. Coalgebraic logic

Recently, modal logics have been extensively studied in the field of coalgebra. An overview of this work is given in [43].

In the coalgebraic approach, models are transition maps $\rho : W \to \mathcal{F}(W)$ that assign each $w \in W$ 'successors' $\rho(w)$ where $\mathcal{F}$ is a functor. For example, functor $\mathcal{F}$ might be $\mathcal{P}$ in which case w is assigned the set of states reachable from w in one step. PAs, as considered in this paper, correspond to transition maps of the form $\rho : W \to (\mathcal{P}(\mathcal{D}(W)))^{Act}$ where $\mathcal{D}(W)$ denotes the set of distributions over W. Intuitively, one associates a corresponding set of distributions over W to each $w \in W$ and every label $a \in Act$.

Modularity is a very important feature of the coalgebraic approach [44,45] which admits to logically characterize each component of the system, for instance the non-deterministic choices $\mathcal{P}(-)$ or probabilistic choices $\mathcal{D}(-)$, and then to combine these sub-logics (as multi-sorted logics). In this way, the logic to characterize strong bisimulation for PAs [46] (when instantiating particular parameters) yields the two-sorted logic by Jonsson et al. [37] (see (12)). Further, if infinite conjunction is allowed, image-infinite PAs can be characterized. Recently, the coalgebraic approach has been extended to deal with simulations [47,48]. In the context of PAs, the results are restricted to image-finite PAs and distributions with finite support.

The modular way of deriving logical characterizations for bisimulations and simulations is appealing because it generates composite modal logics along with the structure, thereby allowing for a more general structure. In this paper, we have stressed an orthogonal kind of modularity which concerns the step condition: if we design a new kind of observation on steps, we just use the same logic as before and only vary the diamond operator according to the new notion of step.

Let us give more insight into these two kinds of modularities. When considering the PA in Fig. 2, the composed modular logic is a two-sorted logic (see (12)) which distinguishes states s, s'. To see that, observe that non-deterministic formulas in the two-sorted logic are interpreted over states, and probabilistic formulas are interpreted over distributions. The middle transition is then characterized by a formula faithfully representing its distribution, and this formula cannot be satisfied by any transition out of s. While the coalgebraic modular approach is suitable for bisimulations and simulations, it is not straightforward how to extend it to characterize probabilistic bisimulations and simulations. Note that, states s, s' are probabilistic bisimilar, and moreover, they are also logically identified in terms of our logic, which is interpreted over distributions. The logic is essentially the same as the one for characterizing bisimulations, just by using appropriate combined

transitions in the semantics. For very similar reasons, our approach can be extended to characterize weak bisimulations in a straightforward manner (see Section 7.2). An interesting future work is to develop an approach which enjoys the advantages of both kinds of modularities.

8. Conclusion and future work

This paper has developed a taxonomy of logical characterizations for different simulation and bisimulation relations for probabilistic automata. These results extend previous work along two major dimensions: we study both simulation and bisimulation relations, and consider image-infinite PAs. Further, we give improved results for the image-finite case. In this paper we have considered full distributions, i.e., distribution μ with $\mu(S) = \sum_{s\in S} \mu(s) = 1$. Probabilistic systems with sub-distributions have also been considered in the literature [18,34]. However, we note that our results can be easily adapted to deal with sub-distributions.[2] As future work, we would like to extend our logic to provide sound and complete characterization of bisimulation for continuous-time Markov decision processes [49], or *Markov automata* [30], a related model.

Acknowledgments

The authors are grateful to Christian Eisentraut and James Worrel for insightful discussions. The last author, Lijun Zhang, thanks Ernst-Erich Doberkat and Alexander Kurz for an invitation to a Dagstuhl seminar on *Coalgebraic Logics*. The participants, especially Corina Cîrstea and Lutz Schröder, made valuable suggestions. Finally, we thank the anonymous referees for many constructive comments which helped improve the quality of the paper considerably.

The work of Holger Hermanns is supported by the DFG as part of the Transregional Collaborative Research Center SFB/TR 14 AVACS, by the NWO-DFG bilateral project ROCKS, and has received funding from the European Community's Seventh Framework Programme under Grant Agreement No. 214755. The research of Roberto Segala leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement No. INFSO-ICT-223844. The work of Lijun Zhang has received partial support from *MT-LAB*, a VKR Centre of Excellence. Part of this work was done while Lijun Zhang was at *Saarland University – Computer Science* and at *Computing Laboratory, University of Oxford*.

References

[1] R. Segala, N.A. Lynch, Probabilistic simulations for probabilistic processes, Nord. J. Comput. 2 (2) (1995) 250–273.
[2] K. Larsen, A. Skou, Bisimulation through probabilistic testing, Inform. Comput. 94 (1) (1991) 1–28.
[3] B. Jonsson, K. Larsen, Specification and refinement of probabilistic processes, in: LICS, 1991, pp. 266–277.
[4] P.R. D'Argenio, B. Jeannet, H.E. Jensen, K.G. Larsen, Reduction and refinement strategies for probabilistic analysis, in: PAPM-PROBMIV, 2002, pp. 57–76.
[5] J. Desharnais, V. Gupta, R. Jagadeesan, P. Panangaden, Approximating labeled Markov processes, Inform. Comput. 184 (1) (2003) 160–200.
[6] L. de Alfaro, P. Roy, Magnifying-lens abstraction for Markov decision processes, in: CAV, 2007, pp. 325–338.
[7] H. Hermanns, B. Wachter, L. Zhang, Probabilistic CEGAR, in: CAV, 2008, pp. 162–175.
[8] R. Canetti, L. Cheung, D.K. Kaynar, M. Liskov, N.A. Lynch, O. Pereira, R. Segala, Analyzing security protocols using time-bounded task-PIOAs, Discrete Event Dyn. Syst. 18 (1) (2008) 111–159.
[9] S. Derisavi, H. Hermanns, W.H. Sanders, Optimal state-space lumping in Markov chains, Inform. Process. Lett. 87 (6) (2003) 309–315.
[10] J.-P. Katoen, T. Kemna, I.S. Zapreev, D.N. Jansen, Bisimulation minimisation mostly speeds up probabilistic model checking, in: TACAS, 2007, pp. 87–101.
[11] H. Hansson, B. Jonsson, A calculus for communicating systems with time and probabilities, in: IEEE Real-Time Systems Symposium, 1990, pp. 278–287.
[12] H. Hansson, B. Jonsson, A logic for reasoning about time and reliability, Formal Asp. Comput. 6 (5) (1994) 512–535.
[13] A. Aziz, K. Sanwal, V. Singhal, R.K. Brayton, Model-checking continuous-time Markov chains, ACM Trans. Comput. Logic 1 (1) (2000) 162–170.
[14] C. Baier, B.R. Haverkort, H. Hermanns, J.-P. Katoen, Model-checking algorithms for continuous-time Markov chains, IEEE Trans. Softw. Eng. 29 (6) (2003) 524–541.
[15] A. Parma, R. Segala, Logical characterizations of bisimulations for discrete probabilistic systems, in: FOSSACS, vol. 4423, 2007, pp. 287–301.
[16] K. Chatterjee, T. Henzinger, K. Sen, Model-checking omega-regular properties of interval Markov chains, in: FoSSaCS, 2008, pp. 302–317.
[17] M. Hennessy, R. Milner, Algebraic laws for nondeterminism and concurrency, J. ACM 32 (1) (1985) 137–161.
[18] J. Desharnais, A. Edalat, P. Panangaden, Bisimulation for labelled Markov processes, Inform. Comput. 179 (2) (2002) 163–193.
[19] P. Panangaden, Labelled Markov Processes, Imperial College Press, 2009.
[20] A. Tarski, A lattice-theoretical fixpoint theorem and its applications, Pacific J. Math. 5 (2) (1955) 285–309.
[21] R. Segala, Modeling and verification of randomized distributed real-time systems, Ph.D. Thesis, MIT, 1995.
[22] R. Givan, T. Dean, M. Greig, Equivalence notions and model minimization in Markov decision processes, Artif. Intell. 147 (1–2) (2003) 163–223.
[23] D. Sangiorgi, Bisimulation: from the origins to today, in: LICS, 2004, pp. 298–302.
[24] J. Desharnais, F. Laviolette, M. Tracol, Approximate analysis of probabilistic processes: logic, simulation and games, in: QEST, 2008, pp. 264–273.
[25] L. Zhang, Decision algorithms for probabilistic simulations, Ph.D. Thesis, Universität des Saarlandes, 2008.
[26] C. Baier, On algorithmic verification methods for probabilistic systems, habilitations-schrift zur Erlangung der venia legendi der Fakultät für Mathematik and Informatik, Universität Mannheim, 1998.
[27] C. Baier, B. Engelen, M.E. Majster-Cederbaum, Deciding bisimilarity and similarity for probabilistic processes, J. Comput. Syst. Sci. 60 (1) (2000) 187–231.
[28] J. Desharnais, V. Gupta, R. Jagadeesan, P. Panangaden, Weak bisimulation is sound and complete for pCTL*, Inform. Comput. 208 (2) (2010) 203–219.
[29] R. Milner, A calculus of communicating systems, in: Lecture Notes in Computer Science, vol. 92, Springer, 1980.

[2] A critical reader will find out that the soundness proof (cf. Theorem 5.3) for formulas of the form $\langle a\rangle\varphi$ would not work anymore, for example for the case $\mu(S) = 0$ and $\mu'(S) > 0$. This can be remedied by showing a stronger statement of (4) by considering a subset of distribution pairs μ and μ' such that $\mu'(s') > 0$ implies that there exists s with $\mu(s) > 0$ and $s \precsim s'$.

[30] C. Eisentraut, H. Hermanns, L. Zhang, On probabilistic automata in continuos time, in: LICS, IEEE, 2010, pp. 342–351.
[31] A. Bianco, L. de Alfaro, Model checking of probabalistic and nondeterministic systems, in: FSTTCS, 1995, pp. 499–513.
[32] S. Cattani, R. Segala, Decision algorithms for probabilistic bisimulation, in: CONCUR, 2002, pp. 371–385.
[33] J. Desharnais, A logical characterization of simulation for labelled Markov chains, in: Probmiv, 1999, pp. 33–48.
[34] C. Baier, J.-P. Katoen, H. Hermanns, V. Wolf, Comparative branching-time semantics for Markov chains, Inform. Comput. 200 (2) (2005) 149–214.
[35] J. Desharnais, P. Panangaden, Continuous stochastic logic characterizes bisimulation of continuous-time Markov processes, J. Logic Algebra Program. 56 (1–2) (2003) 99–115.
[36] R. van Glabbeek, The linear time – branching time spectrum I, in: J. Bergstra, A. Ponse, S. Smolka (Eds.), Handbook of Process Algebra, Elsevier, 2001, pp. 3–99.
[37] B. Jonsson, K. Larsen, Y. Wang, Probabilistic extensions of process algebras, in: J. Bergstra, A. Ponse, S. Smolka (Eds.), Handbook of Process Algebra, Elsevier, 2001, pp. 685–710.
[38] P.R. D'Argenio, N. Wolovick, P.S. Terraf, P. Celayes, Nondeterministic labeled Markov processes: bisimulations and logical characterization, in: QEST, 2009, pp. 11–20.
[39] A. Philippou, I. Lee, O. Sokolsky, Weak bisimulation for probabilistic systems, in: CONCUR, 2000, pp. 334–349.
[40] R. Segala, A. Turrini, Comparative analysis of bisimulation relations on alternating and non-alternating probabilistic models, in: QEST, 2005, pp. 44–53.
[41] A. Parma, Axiomatic and logical characterizations of probabilistic preorders and trace semantics, Ph.D. Thesis, University of Verona, 2008.
[42] Y. Deng, R.J. van Glabbeek, M. Hennessy, C. Morgan, C. Zhang, Characterising testing preorders for finite probabilistic processes, in: LICS, 2007, pp. 313–325.
[43] C. Cîrstea, A. Kurz, D. Pattinson, L. Schröder, Y. Venema, Modal logics are coalgebraic, in: BCS Int. Acad. Conf., 2008, pp. 128–140.
[44] C. Cîrstea, A compositional approach to defining logics for coalgebras, Theor. Comput. Sci. 327 (1–2) (2004) 45–69.
[45] C. Cîrstea, D. Pattinson, Modular construction of complete coalgebraic logics, Theor. Comput. Sci. 388 (1–3) (2007) 83–108.
[46] L. Schröder, Expressivity of coalgebraic modal logic: the limits and beyond, Theor. Comput. Sci. 390 (2–3) (2008) 230–247.
[47] C. Cîrstea, On logics for coalgebraic simulation, Electron. Notes Theor. Comput. Sci. 106 (2004) 63–90.
[48] C. Cîrstea, A modular approach to defining and characterising notions of simulation, Inform. Comput. 204 (4) (2006) 469–502.
[49] M.R. Neuhäußer, J.-P. Katoen, Bisimulation and logical preservation for continuous-time Markov decision processes, in: CONCUR, 2007, pp. 412–427.