BISIMULATIONS MEET PCTL EQUIVALENCES FOR PROBABILISTIC AUTOMATA

LEI SONG, LIJUN ZHANG, AND JENS CHR. GODSKESEN

IT University of Copenhagen, Denmark
e-mail address: leis@itu.dk

DTU Informatics, Technical University of Denmark
e-mail address: zhang@imm.dtu.dk

IT University of Copenhagen, Denmark
e-mail address: jcg@itu.dk

Abstract. Probabilistic automata (PA) [24] have been successfully applied in formal verification of concurrent and stochastic systems. Efficient model checking algorithms have been studied, where the most often used logics for expressing properties are based on PCTL [11] and its extension PCTL* [4]. Various behavioral equivalences are proposed, as a powerful tool for abstraction and compositional minimization for PAs. Unfortunately, the behavioral equivalences are well-known to be strictly stronger than the logical equivalences induced by PCTL or PCTL*. This paper introduces novel notions of strong bisimulation relations, which characterizes PCTL and PCTL* exactly. We extend weak bisimulations characterizing PCTL and PCTL* without next operator, respectively. Further, we also extend the framework to simulations. Thus, our paper bridges the gap between logical and behavioral equivalences and preorders in this setting.

1. Introduction

Probabilistic automata (PA) [24] have been successfully applied in formal verification of concurrent and stochastic systems. Efficient model checking algorithms have been studied, where properties are mostly expressed in the logic PCTL, introduced in [11] for Markov chains, and later extended in [4] for Markov decision processes, where PCTL is also extended to PCTL*.

To combat the infamous state space problem in model checking, various behavioral equivalences, including strong and weak bisimulations, are proposed for PAs. Indeed, they turn out to be a powerful tool for abstraction for PAs, since bisimilar states implies that they satisfy exactly the same PCTL formulae. Thus, bisimilar states can be grouped together,

1998 ACM Subject Classification: G.3: Probability and statistics—Markov processes; F.4.1 [Mathematical logic and formal languages]: Mathematical logic—Temporal logic; F.3.1 [Logics and meanings of programs]: Specifying and verifying and reasoning about programs—Mechanical verification. General terms: Performance; Verification.

Key words and phrases: PCTL, Probabilistic automata, Characterization, Bisimulation.

An extended abstract of the paper has appeared in [26].

LOGICAL METHODS
IN COMPUTER SCIENCE
DOI:10.2168/LMCS-???

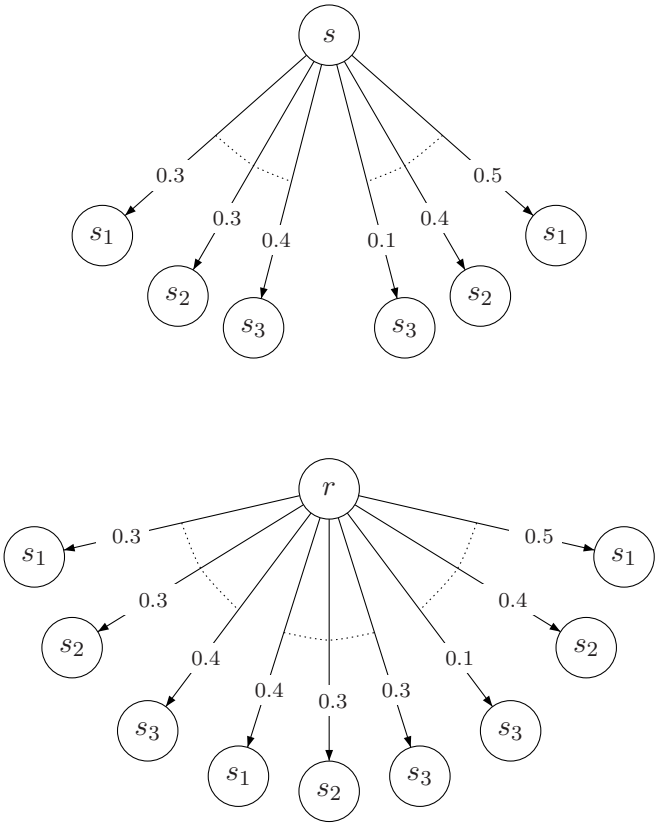

Figure 1: Counterexample of strong probabilistic bisimulation.

allowing one to construct smaller quotient automata before analyzing the model. Moreover, the nice compositional theory for PAs is exploited for compositional minimization [5], namely minimizing the automata before composing the components together.

For Markov chains, i.e., PAs without nondeterministic choices, the logical equivalence implies also bisimilarity, as shown in [3]. Unfortunately, it does not hold in general, namely PCTL equivalence is strictly coarser than bisimulation – and their extension probabilistic bisimulation – for PAs. Even there is such a gap between behavior and logical equivalences, bisimulation based minimization is extensively studied in the literatures to leverage the state space explosion, for instance see [6, 1, 18].

The main reason for the gap can be illustrated by the following example. Consider the PAs in Fig.1 assuming that s_1, s_2, s_3 are three absorbing states with different state properties. It is easy to see that s and r are PCTL equivalent: the additional middle transition out of r does not change the extreme probabilities, the interval of probabilities in which the three observing states can be reached is not changed. Existing bisimulations differentiate s and r, mainly because the middle transition out of r cannot be matched by any transition (or combined transition) of s. Bisimulation requires that the complete distribution of a transition must be matched, which is in this case too strong, as it differentiates states satisfying the same PCTL formulae.

In this paper we will bridge this gap. We introduce novel notions of behavioral equivalences which characterize (both soundly and completely) PCTL, PCTL* and their sublogics. Summarizing, our contributions are:

- A new bisimulation characterizing PCTL* soundly and completely. The bisimulation arises from a converging sequence of equivalence relations, each of which characterizes bounded PCTL*.
- Branching bisimulations which correspond to PCTL and bounded PCTL equivalences.
- We then extend our definitions to weak bisimulations, which characterize sublogics of PCTL and PCTL* with only unbounded path formulae.
- Further, we extend the framework to simulations as well as their characterizations.

Organization of the paper. Section 2 introduces some notations. In Section 3 we recall definitions of probabilistic automata, bisimulation relations by Segala [23]. We also recall the logic PCTL* and its sublogics. Section 4 introduces the novel strong and strong branching bisimulations, and proves that they agree with PCTL* and PCTL equivalences, respectively. Section 5 extends them to weak (branching) bisimulations, and Section 6 extends the framework to simulations. We discuss the coarsest congruent bisimulations and simulations in Section 8, and the extension to countable states in Section 7. In Section 9 we discuss related work, and Section 10 concludes the paper.

2. Preliminaries

Distributions. For a *finite* set S, a distribution is a function $\mu : S \to [0,1]$ satisfying $|\mu| := \sum_{s\in S} \mu(s) \leq 1$. We denote by $Dist(S)$ the set of distributions over S. We shall use $s, r, t, \ldots$ and $\mu, \nu \ldots$ to range over S and $Dist(S)$, respectively. Given a set of distributions $\{\mu_i\}_{1\leq i\leq n}$, and a set of positive weights $\{w_i\}_{1\leq i\leq n}$ such that $\sum_{1\leq i\leq n} w_i = 1$, the *convex combination* $\mu = \sum_{1\leq i\leq n} w_i \cdot \mu_i$ is the distribution such that $\mu(s) = \sum_{1\leq i\leq n} w_i \cdot \mu_i(s)$ for each $s \in S$. The support of μ is defined by $supp(\mu) := \{s \in S \mid \mu(s) > 0\}$. For an equivalence relation $\mathcal{R}$, we write $\mu\ \mathcal{R}\ \nu$ if it holds that $\mu(C) = \nu(C)$ for all equivalence classes $C \in S/\mathcal{R}$. A distribution μ is called *Dirac* if $|supp(\mu)| = 1$, and we let $\mathcal{D}_s$ denote the Dirac distribution with $\mathcal{D}_s(s) = 1$.

Downward Closure. Below we define the downward closure of a subset of states.

Definition 1. For a relation $\mathcal{R}$ over S and $C \subseteq S$, define $\mathcal{R}^{\downarrow}(C) = \{s' \mid s'\ \mathcal{R}\ s \wedge s \in C\}$. We say C is $\mathcal{R}$ *downward closed* iff $C = \mathcal{R}^{\downarrow}(C)$.

We use $\mathcal{R}^{\downarrow}(s)$ as the shorthand of $\mathcal{R}^{\downarrow}(\{s\})$, and $\mathcal{R}^{\downarrow} = \{\mathcal{R}^{\downarrow}(C) \mid C \subseteq S\}$ to denote the set of all $\mathcal{R}$ downward closed sets.

3. Probabilistic automaton, PCTL* and bisimulations

3.1. **Probabilistic automaton.** We recall the notion of a probabilistic automaton introduced by Segala [23]. We omit the set of actions, since they do not appear in the logic PCTL we shall consider later. Note that the bisimulation we shall introduce later can be extended to PA with actions directly.

Definition 2. A *probabilistic automaton* is a tuple $\mathcal{P} = (S, \rightarrow, IS, AP, L)$ where S is a finite set of states, $\rightarrow \subseteq S \times Dist(S)$ is a transition relation, $IS \subseteq S$ is a set of initial states, AP is a set of atomic propositions, and $L : S \rightarrow 2^{AP}$ is a labeling function.

As usual we only consider image-finite PAs, i.e. $\{\mu \mid (s, \mu) \in \rightarrow\}$ is finite for each $s \in S$. A transition $(s, \mu) \in \rightarrow$ is denoted by $s \rightarrow \mu$. Moreover, we write $\mu \rightarrow \mu'$ iff for each $s \in supp(\mu)$ there exists $s \rightarrow \mu_s$ such that $\mu'(r) = \sum_{s \in supp(\mu)} \mu(s) \cdot \mu_s(r)$.

A *path* is a finite or infinite sequence $\omega = s_0 s_1 s_2 \ldots$ of states. For each $i \geq 0$ there exists a distribution μ such that $s_i \rightarrow \mu$ and $\mu(s_{i+1}) > 0$. We use $lstate(\omega)$ and $l(\omega)$ to denote the last state of ω and the length of ω respectively if ω is finite. The sets $Path$ is the set of all paths, and $Path(s_0)$ are those starting from s_0. Similarly, $Path^*$ is the set of finite paths, and $Path^*(s_0)$ are those starting from s_0. Also we use $\omega[i]$ to denote the $(i+1)$-th state for $i \geq 0$, $\omega|^i$ to denote the fragment of ω ending at $\omega[i]$, and $\omega|_i$ to denote the fragment of ω starting from $\omega[i]$.

We introduce the definition of a *scheduler* to resolve nondeterminism. A scheduler is a function $\sigma : Path^* \rightarrow Dist(\rightarrow)$ such that $\sigma(\omega)(s, \mu) > 0$ implies $s = lstate(\omega)$. A scheduler σ is *deterministic* if it returns only Dirac distributions, that is, the next step is chosen deterministically.

The *cone* of a finite path ω, denoted by C_ω, is the set of paths having ω as their prefix, i.e., $C_\omega = \{\omega' \mid \omega \leq \omega'\}$ where $\omega' \leq \omega$ iff ω' is a prefix of ω. Fixing a starting state s_0 and a scheduler σ, the measure $Prob_{\sigma,s_0}$ of a cone C_ω, where $\omega = s_0 s_1 \ldots s_k$, is defined inductively as follows: $Prob_{\sigma,s_0}(C_\omega)$ equals 1 if $k = 0$, and for $k > 0$,

$$Prob_{\sigma,s_0}(C_\omega) = Prob_{\sigma,s_0}(C_{\omega|^{k-1}}) \cdot \left(\sum_{(s_{k-1},\mu') \in \rightarrow} \sigma(\omega|^{k-1})(s_{k-1}, \mu') \cdot \mu'(s_k) \right)$$

Let $\mathcal{B}$ be the smallest algebra that contains all the cones and is closed under complement and countable unions. [1] $Prob_{\sigma,s_0}$ can be extended to a unique measure on $\mathcal{B}$.

Given a relation $\mathcal{R}$ over S, $(\mathcal{R}^{\downarrow})^i$ is the *Cartesian* product of $\mathcal{R}^{\downarrow}$ with itself i times. Each element of $(\mathcal{R}^{\downarrow})^i$ is a *downward closed set of paths*. Let $(\mathcal{R}^{\downarrow})^* = \cup_{i \geq 1} (\mathcal{R}^{\downarrow})^i$, and define $l(\Omega) = n$ for $\Omega \in (\mathcal{R}^{\downarrow})^n$. For $\Omega = C_0 C_1 \ldots C_n \in (\mathcal{R}^{\downarrow})^*$, the $\mathcal{R}$ *downward closed cone* C_Ω is defined as $C_\Omega = \{C_\omega \mid \omega \in \Omega\}$, where $\omega \in \Omega$ iff $\omega[i] \in C_i$ for $0 \leq i \leq n$.

For distributions μ_1 and μ_2, we define $\mu_1 \times \mu_2$ by $(\mu_1 \times \mu_2)((s_1, s_2)) = \mu_1(s_1) \times \mu_2(s_2)$. Following [2] we also define the interleaving of PAs:

Definition 3. Let $\mathcal{P}_i = (S_i, \rightarrow_i, IS_i, AP_i, L_i)$ be two PAs with $i = 1, 2$. The *interleaved parallel composition* $\mathcal{P}_1 \,||\, \mathcal{P}_2$ is defined by:

$$\mathcal{P}_1 \,||\, \mathcal{P}_2 = (S_1 \times S_2, \rightarrow, IS_1 \times IS_2, AP_1 \times AP_2, L)$$

where $L((s_1, s_2)) = L_1(s_1) \times L_2(s_2)$ and $(s_1, s_2) \rightarrow \mu$ iff either $s_1 \rightarrow \mu_1$ and $\mu = \mu_1 \times \mathcal{D}_{s_2}$, or $s_2 \rightarrow \mu_2$ and $\mu = \mathcal{D}_{s_1} \times \mu_2$.

[1] By standard measure theory this algebra is a *σ-algebra* and all its elements are the measurable sets of paths.

Table 1: Summary of PCTL^* and its sublogics

Logic	ψ	Note
PCTL^*	$\varphi \mid \psi_1 \wedge \psi_2 \mid \neg\psi \mid \mathsf{X}\,\psi \mid \psi_1 \,\mathsf{U}\, \psi_2$	
PCTL^{*-}	$\varphi \mid \psi_1 \wedge \psi_2 \mid \neg\psi \mid \mathsf{X}\,\psi$	
PCTL^{*-}_i	$\varphi \mid \psi_1 \wedge \psi_2 \mid \neg\psi \mid \mathsf{X}\,\psi$	$Depth(\psi) \leq i$
PCTL	$\mathsf{X}\,\varphi \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \mid \varphi_1 \,\mathsf{U}^{\leq n}\, \varphi_2$	
PCTL^-	$\mathsf{X}\,\varphi \mid \varphi_1 \,\mathsf{U}^{\leq n}\, \varphi_2$	
PCTL^-_i	$\mathsf{X}\,\varphi \mid \varphi_1 \,\mathsf{U}^{\leq j}\, \varphi_2$	$j \leq i$

3.2. PCTL^* **and its sublogics.** We introduce the syntax of PCTL [11] and PCTL^* [4] which are probabilistic extensions of CTL and CTL^* respectively. PCTL^* over the set AP of atomic propositions are formed according to the following grammar:

$$\varphi ::= a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \mathcal{P}_{\bowtie q}(\psi)$$
$$\psi ::= \varphi \mid \psi_1 \wedge \psi_2 \mid \neg\psi \mid \mathsf{X}\,\psi \mid \psi_1 \,\mathsf{U}\, \psi_2$$

where $a \in AP$, $\bowtie \in \{<, >, \leq, \geq\}$, $q \in [0, 1]$. We refer to φ and ψ as (PCTL^*) state and path formulae, respectively.

The satisfaction relation $s \models \varphi$ for state formulae is defined in a standard manner for boolean formulae. For the probabilistic operator, it is defined by

$$s \models \mathcal{P}_{\bowtie q}(\psi) \text{ iff } \forall \sigma. Prob_{\sigma,s}(\{\omega \in Path(s) \mid \omega \models \psi\}) \bowtie q.$$

The satisfaction relation $\omega \models \psi$ for path formulae is defined exactly the same as for LTL formulae, for example $\omega \models \mathsf{X}\,\psi$ iff $\omega|_1 \models \psi$, and $\omega \models \psi_1 \,\mathsf{U}\, \psi_2$ iff there exists $j \geq 0$ such that $\omega|_j \models \psi_2$ and $\omega|_k \models \psi_1$ for all $0 \leq k < j$.

Sublogics. The depth of path formula ψ of PCTL^* free of U operator, denoted by $Depth(\psi)$, is defined by the maximum number of embedded X operators appearing in ψ, that is,

- $Depth(\varphi) = 0$,
- $Depth(\psi_1 \wedge \psi_2) = \max\{Depth(\psi_1), Depth(\psi_2)\}$,
- $Depth(\neg\psi) = Depth(\psi)$ and
- $Depth(\mathsf{X}\,\psi) = 1 + Depth(\psi)$.

Then, we let PCTL^{*-} be the sublogic of PCTL^* without the until ($\psi_1 \,\mathsf{U}\, \psi_2$) operator. Moreover, PCTL^{*-}_i is a sublogic of PCTL^{*-} where for each ψ we have $Depth(\psi) \leq i$.

The sublogic PCTL is obtained by restricting the path formulae to:

$$\psi ::= \mathsf{X}\,\varphi \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \mid \varphi_1 \,\mathsf{U}^{\leq n}\, \varphi_2$$

Note the bounded until formula does not appear in PCTL^* as it can be encoded by nested next operator. PCTL^- is defined in a similar way as for PCTL^{*-}. Moreover we let PCTL^-_i be the sublogic of PCTL^- where only bounded until operator $\varphi_1 \,\mathsf{U}^{\leq j}\, \varphi_2$ with $j \leq i$ is allowed. The syntax of state formulas of all these logics is the same, while we summarize the differences of the syntax of their path formulas in Table 1.

Logical equivalence. For a logic $\mathcal{L}$, we say that s and r are $\mathcal{L}$-equivalent, denoted by $s \sim_{\mathcal{L}} r$, if they satisfy the same set of formulae of $\mathcal{L}$, that is $s \models \varphi$ iff $r \models \varphi$ for all formulae φ in $\mathcal{L}$. The logic $\mathcal{L}$ can be PCTL^* or one of its sublogics.

3.3. **Strong probabilistic bisimulation.** In this section we introduce the definition of strong probabilistic bisimulation [24]. Let $\{s \to \mu_i\}_{i\in I}$ be a collection of transitions of $\mathcal{P}$, and let $\{p_i\}_{i\in I}$ be a collection of probabilities with $\sum_{i\in I} p_i = 1$. Then $(s, \sum_{i\in I} p_i \cdot \mu_i)$ is called a *combined transition* and is denoted by $s \to_{\mathsf{P}} \mu$ where $\mu = \sum_{i\in I} p_i \cdot \mu_i$.

Definition 4. An equivalence relation $\mathcal{R} \subseteq S \times S$ is a strong probabilistic bisimulation iff $s\ \mathcal{R}\ r$ implies that $L(s) = L(r)$ and for each $s \to \mu$, there exists a combined transition $r \to_{\mathsf{P}} \mu'$ such that $\mu\ \mathcal{R}\ \mu'$.

We write $s \sim_{\mathsf{P}} r$ whenever there is a strong probabilistic bisimulation $\mathcal{R}$ such that $s\ \mathcal{R}\ r$.

It was shown in [24] that $\sim_{\mathsf{P}}$ is preserved by $||$, that is, $s \sim_{\mathsf{P}} r$ implies $s\,||\,t \sim_{\mathsf{P}} r\,||\,t$ for any t. Also strong probabilistic bisimulation is sound for PCTL which means that if $s \sim_{\mathsf{P}} r$ then for any state formula φ of PCTL, $s \models \varphi$ iff $r \models \varphi$. But the other way around is not true, i.e. strong probabilistic bisimulation is not complete for PCTL, as illustrated by the following example.

Example 1. Consider again the two PAs in Fig. 1 and assume that $L(s) = L(r)$ and $L(s_1) \neq L(s_2) \neq L(s_3)$. In addition, s_1, s_2, and s_3 only have one transition to themselves with probability 1. The only difference between the left and right automata is that the right automaton has an extra step. It is not hard to see that $s \sim_{\mathsf{PCTL}^*} r$. By Definition 4 $s \not\sim_{\mathsf{P}} r$ since the middle transition of r cannot be simulated by s even with combined transition. So we conclude that strong probabilistic bisimulation is not complete for PCTL^* as well as for PCTL.

It should be noted that PCTL^* distinguishes more states in a PA than PCTL. Refer to the following example.

Example 2. Suppose s and r are given by Fig. 1 where each of s_1, s_2, and s_3 is extended with a transition such that $s_1 \to \mu_1$ with $\mu_1(s_1) = 0.6$ and $\mu_1(s_4) = 0.4$, $s_2 \to \mu_2$ with $\mu_2(s_4) = 1$, and $s_3 \to \mu_3$ with $\mu_3(s_3) = 0.5$ and $\mu_3(s_4) = 0.5$. Here we assume that every state satisfies different atomic propositions except that $L(s) = L(r)$. Then it is not hard to see $s \sim_{\mathsf{PCTL}} r$ while $s \not\sim_{\mathsf{PCTL}^*} r$. Consider the PCTL^* formula

$$\varphi = \mathcal{P}_{\leq 0.38}(\mathsf{X}(L(s_1) \vee L(s_3)) \wedge \mathsf{X}\,\mathsf{X}(L(s_1) \vee L(s_3))),$$

it holds $s \models \varphi$ but $r \not\models \varphi$. Note that φ is not a well-formed PCTL formula. Indeed, states s and r are PCTL-equivalent.

We have the following theorem:

Theorem 1. (1) $\sim_{\mathsf{PCTL}}$, $\sim_{\mathsf{PCTL}^*}$, $\sim_{\mathsf{PCTL}^-}$, $\sim_{\mathsf{PCTL}_i^-}$, $\sim_{\mathsf{PCTL}^{*-}}$, $\sim_{\mathsf{PCTL}_i^{*-}}$, and $\sim_{\mathsf{P}}$ are equivalence relations for any $i \geq 1$.

(2) $\sim_{\mathsf{P}} \subset \sim_{\mathsf{PCTL}^*} \subset \sim_{\mathsf{PCTL}}$.

(3) $\sim_{\mathsf{PCTL}^{*-}} \subset \sim_{\mathsf{PCTL}^-}$.

(4) $\sim_{\mathsf{PCTL}_1^{*-}} = \sim_{\mathsf{PCTL}_1^-}$.

(5) $\sim_{\mathsf{PCTL}_i^{*-}} \subset \sim_{\mathsf{PCTL}_i^-}$ for any $i > 1$.

(6) $\sim_{\mathsf{PCTL}} \subset \sim_{\mathsf{PCTL}^-} \subset \sim_{\mathsf{PCTL}^-_{i+1}} \subset \sim_{\mathsf{PCTL}^-_i}$ for all $i \geq 0$.
(7) $\sim_{\mathsf{PCTL}^*} \subset \sim_{\mathsf{PCTL}^{*-}} \subset \sim_{\mathsf{PCTL}^{*-}_{i+1}} \subset \sim_{\mathsf{PCTL}^{*-}_i}$ for all $i \geq 0$.

Proof. We take $\sim_{\mathsf{PCTL}}$ as an example and the others can be proved in a similar way. The reflexivity is trivial. If $s \sim_{\mathsf{PCTL}} r$, then we also have $r \sim_{\mathsf{PCTL}} s$ since s and r satisfy the same set of formulae, we prove the symmetry of $\sim_{\mathsf{PCTL}}$. Now we prove the transitivity, that is, for any s, r, t if we have $s \sim_{\mathsf{PCTL}} r$ and $r \sim_{\mathsf{PCTL}} t$, then $s \sim_{\mathsf{PCTL}} t$. It is also easy, since s and r satisfy the same set of formulae, and r and t satisfy the same set of formulae by $s \sim_{\mathsf{PCTL}} r$ and $r \sim_{\mathsf{PCTL}} t$, as result $s \models \varphi$ implies $t \models \varphi$ and vice versa for any φ, so $s \sim_{\mathsf{PCTL}} t$. We conclude that $\sim_{\mathsf{PCTL}}$ is an equivalence relation.

The proof of $\sim_{\mathsf{P}} \subset \sim_{\mathsf{PCTL}}$ can be found in [24] while the proof of $\sim_{\mathsf{P}} \subset \sim_{\mathsf{PCTL}^*}$ can be proved in a similar way. $\sim_{\mathsf{PCTL}^*} \subset \sim_{\mathsf{PCTL}}$ is trivial since PCTL is a subset of PCTL^*.

The proofs of Clause 3 and 5 are obvious since $\sim_{\mathsf{PCTL}^-}$ is a subset of $\sim_{\mathsf{PCTL}^{*-}}$ while $\sim_{\mathsf{PCTL}^-_i}$ is a subset of $\sim_{\mathsf{PCTL}^{*-}_i}$.

We now prove that $\sim_{\mathsf{PCTL}^{*-}_1} = \sim_{\mathsf{PCTL}^-_1}$. It is sufficient to prove that PCTL^-_1 and PCTL^{*-}_1 have the same expressiveness. $\sim_{\mathsf{PCTL}^{*-}_1} \subseteq \sim_{\mathsf{PCTL}^-_1}$ is easy since PCTL^-_1 is a subset of PCTL^{*-}_1. We now show how formulae of PCTL^{*-}_1 can be encoded by formulae of PCTL^-_1. It is not hard to see that the syntax of path formulae of PCTL^{*-}_1 can be rewritten as:

$$\psi ::= \varphi \mid \mathsf{X}\,\varphi \mid \neg\psi \mid \psi_1 \wedge \psi_2$$

where we replace $\mathsf{X}\,\psi$ with $\mathsf{X}\,\varphi$ since PCTL^{*-}_1 only allows path formulae whose depth is less or equal than 1. Since $\neg\,\mathsf{X}\,\varphi = \mathsf{X}\neg\varphi$, the syntax can refined further by deleting $\neg\psi$, that is,

$$\psi ::= \varphi \mid \mathsf{X}\,\varphi \mid \psi_1 \wedge \psi_2$$

Then the only left cases we need to consider are $\mathcal{P}_{\bowtie q}(\varphi)$, $\mathcal{P}_{\bowtie q}(\mathsf{X}\,\varphi_1 \wedge \mathsf{X}\,\varphi_2)$, and $\mathcal{P}_{\bowtie q}(\mathsf{X}\,\varphi_1 \wedge \varphi_2)$,

(1) $s \models \mathcal{P}_{\geq q}(\varphi)$ iff $s \models \varphi$,
(2) $s \models \mathcal{P}_{\geq q}(\mathsf{X}\,\varphi_1 \wedge \mathsf{X}\,\varphi_2)$ iff $s \models \mathcal{P}_{\geq q}(\mathsf{X}(\varphi_1 \wedge \varphi_2))$,
(3) $s \models \mathcal{P}_{\geq q}(\mathsf{X}\,\varphi_1 \wedge \varphi_2)$ iff $s \models \varphi_2 \wedge \mathcal{P}_{\geq q}(\mathsf{X}\,\varphi_1)$.

Here we assume that $0 < q \leq 1$, other cases are similar and are omitted.

The proofs of Clauses 6 and 7 are straightforward. □

4. A novel strong bisimulation

This section presents our main contribution of the paper: we introduce a novel notion of strong bisimulation and strong branching bisimulation. We shall show that they agree with PCTL and PCTL^* equivalences, respectively. As a preparation step we introduce the strong 1-depth bisimulation.

4.1. Strong 1-depth bisimulation.

Definition 5. A relation $\mathcal{R} \subseteq S \times S$ is a strong 1-depth bisimulation if $s\ \mathcal{R}\ r$ implies that $L(s) = L(r)$ and for any $\mathcal{R}$ downward closed set C

(1) for each $s \to \mu$, there exists $r \to \mu'$ such that $\mu'(C) \geq \mu(C)$,
(2) for each $r \to \mu$, there exists $s \to \mu'$ such that $\mu'(C) \geq \mu(C)$.

We write $s \sim_1 r$ whenever there is a strong 1-depth bisimulation $\mathcal{R}$ such that $s\ \mathcal{R}\ r$.

The – though very simple – definition requires only one step matching of the distributions out of s and r. The essential difference to the standard definition is: the quantification of the downward closed set comes before the quantification over transition. This is indeed the key of the new definition of bisimulations. Note in Definition 5 of [26] we require that $\mathcal{R}$ is a preorder, while the $\mathcal{R}$ in Definition 5 can be any relation, but this will not affect the main results shown in this paper. The following theorem shows that $\sim_1$ agrees with $\sim_{\mathsf{PCTL}_1^-}$ and $\sim_{\mathsf{PCTL}_1^{*-}}$ which is also an equivalence relation:

Lemma 1. $\sim_{\mathsf{PCTL}_1^-} = \sim_1 = \sim_{\mathsf{PCTL}_1^{*-}}$.

Proof. According to Clause (4) of Theorem 1, it is enough to prove that $\sim_{\mathsf{PCTL}_1^-} = \sim_1$. We defer to proof to Theorem 3. □

Note that in Definition 5 we consider all the $\mathcal{R}$ downward closed sets since it is not enough to only consider the $\mathcal{R}$ downward closed sets in $\{\mathcal{R}^{\downarrow}(s) \mid s \in S\}$, refer to the following counterexample.

Counterexample 1. Suppose that there are four absorbing states s_1, s_2, s_3, and s_4 which are assigned with different atomic propositions. Suppose we have two processes s and r such that $L(s) = L(r)$, and $s \to \mu_1$, $s \to \mu_2$, $r \to \nu_1$, $r \to \nu_2$ where $\mu_1(s_1) = 0.5$, $\mu_1(s_2) = 0.5$, $\mu_2(s_3) = 0.5$, $\mu_2(s_4) = 0.5$, $\nu_1(s_1) = 0.5$, $\nu_1(s_3) = 0.5$, $\nu_2(s_2) = 0.5$, $\nu_2(s_4) = 0.5$. If we only consider the $\mathcal{R}$ downward closed sets in $\{\mathcal{R}^{\downarrow}(s) \mid s \in S\}$ where $S = \{s, r, s_1, s_2, s_3, s_4\}$, then we will conclude that $s \sim_1 r$, but $r \models \varphi$ while $s \not\models \varphi$ where $\varphi = \mathcal{P}_{\geq 0.5}(\mathsf{X}(L(s_1) \vee L(s_2)))$.

It turns out that $\sim_1$ is preserved by $||$, implying that $\sim_{\mathsf{PCTL}_1^-}$ and $\sim_{\mathsf{PCTL}_1^{*-}}$ are preserved by $||$ as well.

Theorem 2. $s \sim_1 r$ implies that $s \,||\, t \sim_1 r \,||\, t$ for any t.

Proof. We need to prove that for each $\sim_1$ closed set C and $s \,||\, t \to \mu$, there exists $r \,||\, t \to \mu'$ such that $\mu'(C) \geq \mu(C)$ and vice versa. This can be prove by structural induction on $s \,||\, t$ and $r \,||\, t$. By the definition of $||$ operator, if $s \,||\, t \to \mu$, then either $s \to \mu_s$ with $\mu = \mu_s \,||\, \mathcal{D}_t$, or $t \to \mu_t$ with $\mu = \mathcal{D}_s \,||\, \mu_t$. We only consider the case when $\mu = \mu_s \,||\, \mathcal{D}_t$ since the other one is similar. We have known that $s \sim_1 r$, so for each C' if $s \to \mu_s$, then there exists $r \to \mu_r$ such that $\mu_r(C') \geq \mu_s(C')$. By induction, if $s' \sim_1 r'$ for $s', r' \in C'$, then $s' \,||\, t \sim_1 r' \,||\, t$. So for each C and $s \,||\, t \to \mu$, there exists $r \,||\, t \to \mu'$ such that $\mu'(C) \geq \mu(C)$. □

Remark 1. We note that for Kripke structures (PA with only Dirac distributions) $\sim_1$ agrees with the usual strong bisimulation by Milner [20].

4.2. **Strong branching bisimulation.** Now we extend the relation $\sim_1$ to strong i-step bisimulations. Then, the intersection of all of these relations gives us the new notion of strong branching bisimulation, which we show to be the same as $\sim_{\mathsf{PCTL}}$. Recall that Theorem 1 states that $\sim_{\mathsf{PCTL}}$ is strictly coarser than $\sim_{\mathsf{PCTL}^*}$, which we shall consider in the next section.

Following the approach in [27] we define $Prob_{\sigma,s}(C, C', n, \omega)$ which denotes the probability from s to states in C' via states in C possibly in at most n steps under scheduler σ, where ω is used to keep track of the path and only deterministic schedulers are considered in the

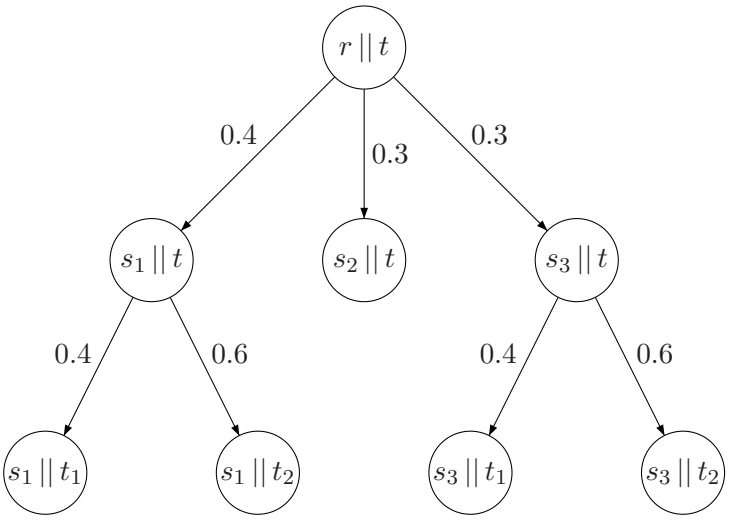

Figure 2: $\sim_i^{\mathsf{b}}$ is not compositional when $i > 1$

following. Formally, $Prob_{\sigma,s}(C, C', n, \omega)$ equals 1 if $s \in C'$, and else if $n > 0 \wedge (s \in C \setminus C')$, then

$$Prob_{\sigma,s}(C, C', n, \omega) = \sum_{r \in supp(\mu')} \mu'(r) \cdot Prob_{\sigma,r}(C, C', n-1, \omega r). \tag{4.1}$$

where $\sigma(\omega)(s, \mu') = 1$, otherwise $Prob_{\sigma,s}(C, C', n, \omega)$ equals 0.

Strong i-depth branching bisimulation is a straightforward extension of strong 1-depth bisimulation, where instead of considering only one immediate step, we consider up to i steps. We let $\sim_1^{\mathsf{b}} = \sim_1$ in the following.

Definition 6. A relation $\mathcal{R} \subseteq S \times S$ is a strong i-depth branching bisimulation with $i > 1$ if $s \; \mathcal{R} \; r$ implies $s \;\sim_{i-1}^{\mathsf{b}}\; r$ and for any $\mathcal{R}$ downward closed sets C, C',

(1) for each scheduler σ, there exists a scheduler σ' such that

$$Prob_{\sigma',r}(C, C', i, r) \geq Prob_{\sigma,s}(C, C', i, s),$$

(2) for each scheduler σ, there exists a scheduler σ' such that

$$Prob_{\sigma',s}(C, C', i, s) \geq Prob_{\sigma,r}(C, C', i, r).$$

We write $s \;\sim_i^{\mathsf{b}}\; r$ whenever there is a strong i-depth branching bisimulation $\mathcal{R}$ such that $s \; \mathcal{R} \; r$. The strong branching bisimulation $\sim^{\mathsf{b}}$ is defined as $\sim^{\mathsf{b}} = \cap_{i \geq 1} \sim_i^{\mathsf{b}}$.

The following lemma shows that $\sim_i^{\mathsf{b}}$ is an equivalence relation, and moreover, $\sim_i^{\mathsf{b}}$ decreases until a fixed point is reached.

Lemma 2. (1) $\sim^{\mathsf{b}}$ and $\sim_i^{\mathsf{b}}$ are equivalence relations for any $i > 1$.

(2) $\sim_j^{\mathsf{b}} \subseteq \sim_i^{\mathsf{b}}$ provided that $1 \leq i \leq j$.

(3) There exists $i \geq 1$ such that $\sim_j^{\mathsf{b}} = \sim_k^{\mathsf{b}}$ for any $j, k \geq i$.

Proof. We only show the proof of transitivity of $\sim_i^{\mathsf{b}}$. Suppose that $s \;\sim_i^{\mathsf{b}}\; t$ and $t \;\sim_i^{\mathsf{b}}\; r$, we need to prove that $s \;\sim_i^{\mathsf{b}}\; r$. By Definition 6, we know there exists strong i-depth branching bisimulations $\mathcal{R}_1$ and $\mathcal{R}_2$ such that $s \; \mathcal{R}_1 \; t$ and $t \; \mathcal{R}_2 \; r$. Let

$$\mathcal{R} = \mathcal{R}_1 \circ \mathcal{R}_2 = \{(s_1, s_3) \mid \exists s_2.(s_1 \; \mathcal{R}_1 \; s_2 \wedge s_2 \; \mathcal{R}_2 \; r)\},$$

it is enough to show that $\mathcal{R}$ is a strong i-depth branching bisimulation. Note $\mathcal{R}_1 \cup \mathcal{R}_2 \subseteq \mathcal{R}$, since for each $s_1 \mathcal{R}_1 s_2$ we also have $s_2 \mathcal{R}_2 s_2$ due to reflexivity, thus $s_1 \mathcal{R} s_2$, similarly we can show that $\mathcal{R}_2 \subseteq \mathcal{R}$. Therefore for any $\mathcal{R}$ downward closed sets C and C', they are also $\mathcal{R}_1$ and $\mathcal{R}_2$ downward closed. Therefore if there exists σ such that $Prob_{\sigma,s}(C, C', i) > 0$, then there exists σ' such that $Prob_{\sigma',t}(C, C', i) \geq Prob_{\sigma,s}(C, C', i)$. Since we also have $t \sim_i^{\mathsf{b}} r$, thus there exists σ'' such that $Prob_{\sigma'',r}(C, C', i) \geq Prob_{\sigma',t}(C, C', i) \geq Prob_{\sigma,s}(C, C', i)$. This completes the proof of transitivity.

The proof of Clause (2) is straightforward from Definition 8, since $s \sim_j^{\mathsf{b}} r$ implies $s \sim_{j-1}^{\mathsf{b}} r$ when $j > 1$.

It is straightforward from the Definition 6 that $\sim_i^{\mathsf{b}}$ is getting more discriminating as i increases. In a PA only with finite states the maximum number of equivalence classes is equal to the number of states, as result we can guarantee that $\sim_n^{\mathsf{b}} = \sim^{\mathsf{b}}$ where n is the total number of states. □

Let $\mathcal{R}$ be an equivalence over S. The set $C \subseteq S$ is said to be $\mathcal{R}$ closed iff $s \in C$ and $s \mathcal{R} r$ implies $r \in C$. $C_{\mathcal{R}}$ is used to denote the least $\mathcal{R}$ closed set which contains C.

Definition 7. Two paths $\omega_1 = s_0 s_1 \ldots$ and $\omega_2 = r_0 r_1 \ldots$ are strong i-depth branching bisimilar, written as $\omega_1 \sim_i^{\mathsf{b}} \omega_2$, iff $\omega_1[j] \sim_i^{\mathsf{b}} \omega_2[j]$ for all $0 \leq j \leq i$.

We first define the $\sim_i^{\mathsf{b}}$ closed paths i.e.p the set Ω of paths is $\sim_i^{\mathsf{b}}$ *closed* if for any $\omega_1 \in \Omega$ and ω_2 such that $\omega_1 \sim_i^{\mathsf{b}} \omega_2$, it holds that $\omega_2 \in \Omega$. Let $\mathcal{B}_{\sim_i^{\mathsf{b}}} = \{\Omega \subseteq \mathcal{B} \mid \Omega \text{ is } \sim_i^{\mathsf{b}} \text{ closed}\}$. By standard measure theory $\mathcal{B}_{\sim_i^{\mathsf{b}}}$ is measurable. The $\sim_i$ for paths can be defined similarly and is omitted here.

It is not hard to show that $\sim_i^{\mathsf{b}}$ characterizes PCTL_i^-. Moreover, we show that $\sim^{\mathsf{b}}$ agrees with PCTL equivalence.

Theorem 3. $\sim_{\mathsf{PCTL}_i^-} = \sim_i^{\mathsf{b}}$ for any $i \geq 1$, moreover $\sim_{\mathsf{PCTL}} = \sim^{\mathsf{b}}$.

Proof. In the following, we will use $Sat(\varphi) = \{s \in S \mid s \models \varphi\}$ to denote the set of states which satisfy φ. Similarly, $Sat(\psi) = \{\omega \in Path(s_0) \mid \omega \models \psi\}$ is the set of paths which satisfy ψ.

Let $\mathcal{R} = \{(s, r) \mid s \sim_{\mathsf{PCTL}_i^-} r\}$. In order to prove that $s \sim_{\mathsf{PCTL}_i^-} r$ implies $s \sim_i^{\mathsf{b}} r$ for any s and r, we need to show that for any $\mathcal{R}$ closed sets C, C' and scheduler σ, there exists a scheduler σ' such that $Prob_{\sigma',r}(C, C', i, r) \geq Prob_{\sigma,s}(C, C', i, s)$ and vice versa provided that $s \mathcal{R} r$. Suppose there are n different equivalence classes in a finite PA. Let φ_{C_i,C_j} be a state formula such that $Sat(\varphi_{C_i,C_j}) \supseteq C_i$ and $Sat(\varphi_{C_i,C_j}) \cap C_j = \emptyset$, here $1 \leq i \neq j \leq n$ and $C_i, C_j \in S/\mathcal{R}$ are two different equivalence classes. Formula like φ_{C_i,C_j} always exists, otherwise there will not exist a formula which is fulfilled by states in C_i, but not fulfilled by states in C_j, that is, states in C_i and C_j satisfy the same set of formulae, this is against the assumption that C_i and C_j are two different equivalence classes. Let $\varphi_{C_i} = \bigwedge_{1 \leq j \neq i \leq n} \varphi_{C_i,C_j}$, it is not hard to see that $Sat(\varphi_{C_i}) = C_i$. For a $\mathcal{R}$ closed set C, it holds

$$\varphi_C = \bigvee_{C' \in S/\mathcal{R} \wedge C' \subseteq C} \varphi_{C'},$$

then $Sat(\varphi_C) = C$. Now suppose $Prob_{\sigma,s}(C, C', i, s) = q$, then we know $s \models \neg \mathcal{P}_{<q} \psi$ where

$$\psi = \varphi_C \, \mathsf{U}^{\leq j} \, \varphi_{C'}.$$

By assumption $r \models \neg\mathcal{P}_{<q}\psi$, so there exists a scheduler σ' such that $Prob_{\sigma',r}(C, C', i, r) \geq q$, that is, $Prob_{\sigma',r}(C, C', i, r) \geq Prob_{\sigma,s}(C, C', i, s)$. The other case is similar and is omitted here.

The proof of $\sim_i^{\mathsf{b}} \subseteq \sim_{\mathsf{PCTL}_i^-}$ is by structural induction on the syntax of state formula φ and path formula ψ of PCTL_i^-, that is, we need to prove the following two results simultaneously.

(1) $s \sim_i^{\mathsf{b}} r$ implies that $s \models \varphi$ iff $r \models \varphi$ for any state formula φ.

(2) $\omega_1 \sim_i^{\mathsf{b}} \omega_2$ implies that $\omega_1 \models \psi$ iff $\omega_2 \models \psi$ for any path formula ψ.

We only consider $\varphi = \mathcal{P}_{\leq q}(\psi)$ where $\psi = \varphi_1 \,\mathsf{U}^{\leq i}\, \varphi_2$, since other cases are similar. According to the semantics $s \models \varphi$ iff $\forall\sigma.Prob_{\sigma,s}(\{\omega \mid \omega \models \psi\}) \leq q$. By induction $\Omega = \{\omega \mid \omega \models \psi\}$ is $\sim_i^{\mathsf{b}}$ closed. We need to show that $l(\Omega) = i$ and there exists two $\sim_i^{\mathsf{b}}$ closed sets C, C' such that $\Omega = \bigcup_{0\leq k<i} C^k C'$, this is straightforward by the semantics of $\mathsf{U}^{\leq i}$. We prove by contraction, and assume $s \models \varphi$ and $r \not\models \varphi$. Then for any σ, we have $Prob_{\sigma,s}(\Omega) \leq q$. Since $r \not\models \varphi$, there exists σ' such that $Prob_{\sigma',r}(\Omega) > q$, thus there does not exist σ such that $Prob_{\sigma,s}(C, C', i, s) \geq Prob_{\sigma',r}(C, C', i, r)$, which contradicts with assumption $s \sim_i^{\mathsf{b}} r$. Therefore $r \models \varphi$, and $s \sim_{\mathsf{PCTL}_i^-} r$.

The proof of $\sim_{\mathsf{PCTL}} = \sim^{\mathsf{b}}$ is based on the fact that $\varphi_1 \,\mathsf{U}\, \varphi_2 = \varphi_1 \,\mathsf{U}^{\leq\infty}\, \varphi_2$. □

Intuitively, since $\sim_i^{\mathsf{b}}$ decreases as i increases, for any PA $\sim_i^{\mathsf{b}}$ will eventually converge to PCTL equivalence.

Recall $\sim_1^{\mathsf{b}}$ is compositional by Theorem 2, which unfortunately is not the case for $\sim_i^{\mathsf{b}}$ with $i > 1$. This is illustrated by the following example:

Counterexample 2. $s \sim_i^{\mathsf{b}} r$ does not imply $s \,||\, t \sim_i^{\mathsf{b}} r \,||\, t$ for any t generally if $i > 1$.

We have shown in Example 1 that $s \sim_{\mathsf{PCTL}} r$. If we compose s and r with t where t only has a transition to μ such that $\mu(t_1) = 0.4$ and $\mu(t_2) = 0.6$, then it turns out that $s \,||\, t \not\sim_{\mathsf{PCTL}} r \,||\, t$. Since there exists $\varphi = \mathcal{P}_{\leq 0.34}\psi$ with

$$\psi = ((L(s \,||\, t) \vee L(s_1 \,||\, t) \vee (L(s_3 \,||\, t)))\, \mathsf{U}^{\leq 2} (L(s_1 \,||\, t_2) \vee L(s_3 \,||\, t_1)))$$

such that $s \,||\, t \models \varphi$ but $r \,||\, t \not\models \varphi$, as there exists a scheduler σ such that the probability of paths satisfying ψ in $Prob_{\sigma,r}$ equals 0.36. Fig. 2 shows the execution of r guided by the scheduler σ, and we assume all the states in Fig. 2 have different atomic propositions except that $L(s \,||\, t) = L(r \,||\, t)$. It is similar for $\sim_{\mathsf{PCTL}^*}$.

Note that φ is also a well-formed state formula of PCTL_2^-, so $\sim_{\mathsf{PCTL}_i^-}$ as well as $\sim_i^{\mathsf{b}}$ are not compositional if $i \geq 2$.

4.3. **Strong bisimulation.** In this section we introduce a new notion of strong bisimulation and show that it characterizes $\sim_{\mathsf{PCTL}^*}$. Given a relation $\mathcal{R}$, a $\mathcal{R}$ downward closed cone C_Ω and a measure $Prob$, the value of $Prob(C_\Omega)$ can be computed by summing up the values of all $Prob(C_\omega)$ with $\omega \in \Omega$. We let $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ be a set of $\mathcal{R}$ downward closed set of paths, then $C_{\widetilde{\Omega}}$ is the corresponding set of $\mathcal{R}$ downward closed cones, that is, $C_{\widetilde{\Omega}} = \cup_{\Omega\in\widetilde{\Omega}} C_\Omega$. Define $l(\widetilde{\Omega}) = Max\{l(\Omega) \mid \Omega \in \widetilde{\Omega}\}$ as the maximum length of Ω in $\widetilde{\Omega}$. To compute $Prob(C_{\widetilde{\Omega}})$, we cannot sum up the value of each $Prob(C_\Omega)$ such that $\Omega \in \widetilde{\Omega}$ as before since we may have a path ω such that $\omega \in \Omega_1$ and $\omega \in \Omega_2$ where $\Omega_1, \Omega_2 \in \widetilde{\Omega}$, so we have to remove these

duplicate paths and make sure each path is considered once and only once as follows where we abuse the notation and write $\omega \in \widetilde{\Omega}$ iff $\exists \Omega.(\Omega \in \widetilde{\Omega} \wedge \omega \in \Omega)$:

$$Prob(C_{\widetilde{\Omega}}) = \sum_{\omega \in \widetilde{\Omega} \wedge \nexists \omega' \in \widetilde{\Omega}.\omega' \leq \omega} Prob(C_\omega) \tag{4.2}$$

Note Equation 4.2 can be extended to compute the probability of any set of cones in a given measure.

The definition of strong i-depth bisimulation is as follows where $\sim_1 = \sim_1^{\mathsf{b}}$.

Definition 8. A relation $\mathcal{R} \subseteq S \times S$ is a strong i-depth bisimulation if $i > 1$ and $s \ \mathcal{R} \ r$ implies that $s \ \sim_{i-1} \ r$ and for any $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ with $l(\widetilde{\Omega}) = i$

(1) for each scheduler σ, there exists σ' such that $Prob_{\sigma',r}(C_{\widetilde{\Omega}}) \geq Prob_{\sigma,s}(C_{\widetilde{\Omega}})$,
(2) for each scheduler σ, there exists σ' such that $Prob_{\sigma',s}(C_{\widetilde{\Omega}}) \geq Prob_{\sigma,r}(C_{\widetilde{\Omega}})$.

We write $s \ \sim_i \ r$ whenever there is a i-depth strong bisimulation $\mathcal{R}$ such that $s \ \mathcal{R} \ r$. The strong bisimulation $\sim$ is defined as $\sim \ = \ \cap_{i \geq 1} \sim_i$.

Similar to $\sim_i^{\mathsf{b}}$, the relation $\sim_i$ forms a chain of equivalence relations where the strictness of $\sim_i$ increases as i increases, and $\sim_i$ will converge finally in a PA.

Lemma 3. (1) $\sim_i$ is an equivalence relation for any $i > 1$.
(2) $\sim_j \subseteq \sim_i$ provided that $1 \leq i \leq j$.
(3) There exists $i \geq 1$ such that $\sim_j = \sim_k$ for any $j, k \geq i$.

Proof. (1) We only prove the transitivity since the reflexivity and symmetry are easy. Suppose that $s \ \sim_i \ r$ and $r \ \sim_i \ t$, we need to show that $s \ \sim_i \ t$. According to Definition 8, we know there exists strong i-depth bisimulations $\mathcal{R}_1$ and $\mathcal{R}_2$ such that $s \ \mathcal{R}_1 \ t$ and $t \ \mathcal{R}_2 \ r$. Let

$$\mathcal{R} = \mathcal{R}_1 \circ \mathcal{R}_2 = \{(s_1, s_3) \mid \exists s_2.(s_1 \ \mathcal{R}_1 \ s_2 \wedge s_2 \ \mathcal{R}_2 \ r)\},$$

it is enough to show that $\mathcal{R}$ is a strong i-depth bisimulation. Similar as in the proof of Lemma 2, if $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$, then it also holds that $\widetilde{\Omega} \subseteq (\mathcal{R}_1^{\downarrow})^*$ and $\widetilde{\Omega} \subseteq (\mathcal{R}_2^{\downarrow})^*$. Thus for each $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ with $l(\widetilde{\Omega}) = i$, and scheduler σ of s, there exists σ' of r such that $Prob_{\sigma',r}(\widetilde{\Omega}) \geq Prob_{\sigma,s}(\widetilde{\Omega})$. Since $r \ \sim_i \ t$, there exists scheduler σ'' of t such that

$$Prob_{\sigma'',t}(\widetilde{\Omega}) \geq Prob_{\sigma',r}(\widetilde{\Omega}) \geq Prob_{\sigma,s}(\widetilde{\Omega}).$$

The other direction is similar and omitted here, thus $s \ \sim_i \ t$.
(2) The proof is straightforward from Definition 8.
(3) Since there are only finitely many states, thus there are only finitely many equivalence classes, such i always exists.

□

Below we show that $\sim_i$ characterizes $\sim_{\mathsf{PCTL}_i^{*-}}$ for all $i \geq 1$, where $\sim = \bigcap\limits_{n \geq 1} \sim_n$.

Theorem 4. $\sim_{\mathsf{PCTL}_i^{*-}} = \sim_i$ for any $i \geq 1$, moreover $\sim_{\mathsf{PCTL}^*} = \sim$.

Proof. Let $\mathcal{R} = \{(s, r) \mid s \ \sim_{\mathsf{PCTL}_i^{*-}} \ r\}$, we need to show that $\mathcal{R}$ is strong i-depth bisimulation in order to prove that $s \ \sim_{\mathsf{PCTL}_i^{*-}} \ r$ implies $s \ \sim_i \ r$ for any s and r. According to Definition 8, we need to show that for any $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ with $l(\widetilde{\Omega}) = i$ and scheduler σ, there exists a scheduler σ' such that $Prob_{\sigma',r}(C_{\widetilde{\Omega}}) \leq Prob_{\sigma,s}(C_{\widetilde{\Omega}})$ and vice versa provided that

$s \mathcal{R} r$. Following the way in the proof of Theorem 3, we can construct a formula φ_C such that $Sat(\varphi_C) = C$ where C is a $\mathcal{R}$ closed set. Suppose $\Omega = C_0C_1 \ldots C_j$ with $j \leq i$, then

$$\psi_\Omega = \varphi_{C_0} \wedge \mathsf{X}(\varphi_{C_1} \wedge \ldots \wedge \mathsf{X}(\varphi_{C_{j-1}} \wedge \mathsf{X}\,\varphi_{C_j}))$$

can be used to characterize Ω, that is, $Sat(\psi_\Omega) = C_\Omega$. Let $\psi = \bigvee_{\Omega \in \widetilde{\Omega}} \psi_\Omega$, then $Sat(\psi) = C_{\widetilde{\Omega}}$. As a result $s \models \neg\mathcal{P}_{<q}\psi$ where $q = Prob_{\sigma,s}(C_{\widetilde{\Omega}})$. By assumption $r \models \neg\mathcal{P}_{<q}\psi$, so there exists a scheduler σ' such that $Prob_{\sigma',r}(C_{\widetilde{\Omega}}) \geq q$, that is, $Prob_{\sigma',r}(C_{\widetilde{\Omega}}) \geq Prob_{\sigma,s}(C_{\widetilde{\Omega}})$. The other case is similar and is omitted here.

The proof of $\sim_i \subseteq \sim_{\mathsf{PCTL}_i^{*-}}$ is by structural induction on the syntax of state formula φ and path formula ψ of PCTL_i^{*-}, that is, we need to prove the following two results simultaneously.

(1) $s \sim_i r$ implies that $s \models \varphi$ iff $r \models \varphi$ for any state formula φ of PCTL_i^{*-}.

(2) $\omega_1 \sim_i \omega_2$ implies that $\omega_1 \models \psi$ iff $\omega_2 \models \psi$ for any path formula ψ of PCTL_i^{*-}.

We only consider $\varphi = \mathcal{P}_{\leq q}(\psi)$ where $\psi = \psi_1 \,\mathsf{U}^{\leq i}\, \psi_2$, since other cases are similar. By induction $\widetilde{\Omega} = \{\omega \mid \omega \models \psi\}$ is $\sim_i$ closed, and also $l(\widetilde{\Omega}) = i$. We prove by contradiction, and assume that $s \models \varphi$ and $r \not\models \varphi$. According to the semantics $s \models \varphi$ iff $\forall\sigma.Prob_{\sigma,s}(\widetilde{\Omega}) \leq q$. If $r \not\models \varphi$, then there exists σ' such that $Prob_{\sigma',r}(\widetilde{\Omega}) > q$, consequently for such σ' of r there does not exist σ of s such that $Prob_{\sigma,s}(\widetilde{\Omega}) \geq Prob_{\sigma',r}(\widetilde{\Omega})$ which contradicts with assumption that $s \sim_i r$, therefore $r \models \varphi$ and $s \sim_{\mathsf{PCTL}_i^{*-}} r$.

The proof of $\sim_{\mathsf{PCTL}^*} = \sim$ is based on the fact that $\psi_1 \,\mathsf{U}\, \psi_2 = \psi_1 \,\mathsf{U}^{\leq\infty}\, \psi_2$. □

Recall by Lemma 3, there exists $i > 0$ such that $\sim_{\mathsf{PCTL}^*} = \sim_i$.

For the same reason as strong i-depth branching bisimulation, $\sim_i$ is not preserved by $||$ when $i > 1$.

Counterexample 3. $s \sim_i r$ does not imply $s \,||\, t \sim_i r \,||\, t$ for any t generally if $i > 1$. This can be shown by using the same arguments as in Counterexample 2.

4.4. **Taxonomy for strong bisimulations.** Fig. 3 summaries the relationship among all these bisimulations and logical equivalences. The arrow $\rightarrow$ denotes $\subseteq$ and $\nrightarrow$ denotes $\nsubseteq$. We also abbreviate $\sim_{\mathsf{PCTL}}$ as PCTL, and it is similar for other logical equivalences. Congruent relations with respect to the $||$ operator are shown in circles, and non-congruent relations are shown in boxes. Segala has considered another strong bisimulation in [24], which can be defined by replacing the $r \rightarrow_{\mathsf{P}} \mu'$ with $r \rightarrow \mu'$ and thus is strictly stronger than $\sim_{\mathsf{P}}$. It is also worth mentioning that all the bisimulations shown in Fig.3 coincide with the strong bisimulation defined in [3] in the DTMC setting which can be seen as a special case of PA (i.e., deterministic probabilistic automata).

5. Weak bisimulations

As in [3] we use $\mathsf{PCTL}_{\setminus \mathsf{X}}$ to denote the subset of PCTL without next operator $\mathsf{X}\,\varphi$ and bounded until $\varphi_1 \,\mathsf{U}^{\leq n}\, \varphi_2$. Similarly, $\mathsf{PCTL}^*_{\setminus \mathsf{X}}$ is used to denote the subset of PCTL^* without next operator $\mathsf{X}\,\psi$. In this section we shall introduce weak bisimulations and study their relation to $\sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$ and $\sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$, respectively. Before this we should point out that $\sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$ implies $\sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$ but the other direction does not hold. Refer to the following example.

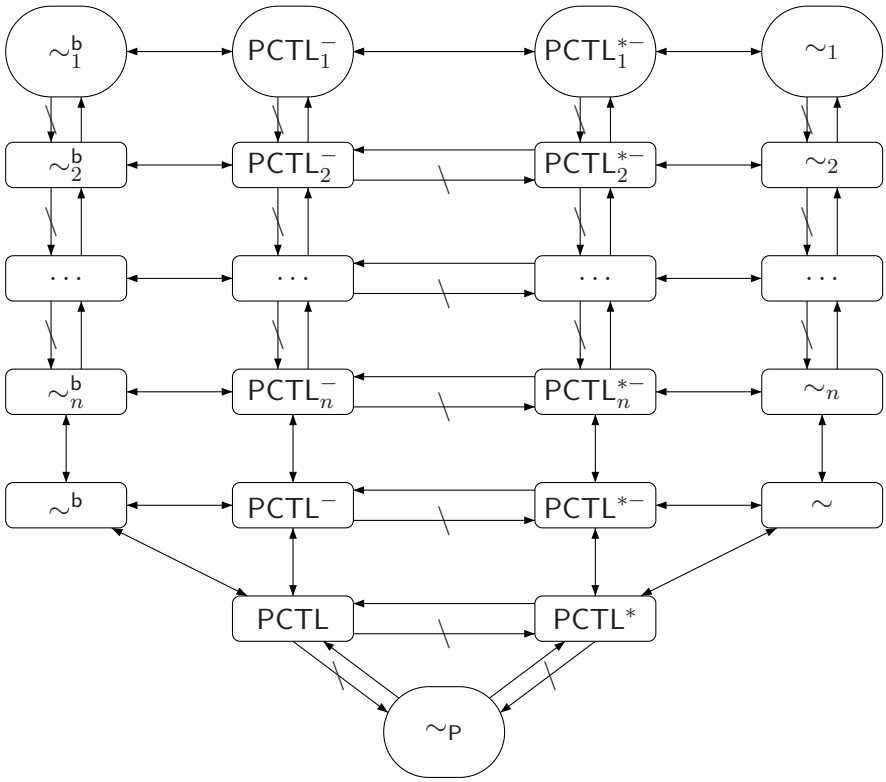

Figure 3: Relationship of different equivalences in strong scenario.

Example 3. Suppose s and r are given by Fig. 1 where each of s_1 and s_3 is attached with one transition respectively, that is, $s_1 \to \mu_1$ such that $\mu_1(s_4) = 0.4$ and $\mu_1(s_5) = 0.6$, $s_3 \to \mu_3$ such that $\mu_3(s_4) = 0.4$ and $\mu_3(s_5) = 0.6$. In addition, s_2, s_4 and s_5 only have a transition with probability 1 to themselves, and all these states are assumed to have different atomic propositions. Then $s \sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}} r$ but $s \not\sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} r$, since we have a path formula

$$\psi = ((L(s) \vee L(s_1)) \,\mathsf{U}\, L(s_5)) \vee ((L(s) \vee L(s_3)) \,\mathsf{U}\, L(s_4))$$

such that $s \models \mathcal{P}_{\leq 0.34}\psi$ but $r \not\models \mathcal{P}_{\leq 0.34}\psi$, since there exists a scheduler σ where the probability of path formulae satisfying ψ in $Prob_{\sigma,r}$ is equal to $Prob_{\sigma,r}(ss_1s_5)+Prob_{\sigma,r}(ss_3s_4) = 0.36$. Note ψ is not a well-formed path formula of $\mathsf{PCTL}_{\setminus \mathsf{X}}$.

5.1. **Branching probabilistic bisimulation by Segala.** Before introducing our weak bisimulations, we give the classical definition of branching probabilistic bisimulation proposed in [24]. Given an equivalence relation $\mathcal{R}$, s can evolve into μ by a *branching transition*, written as $s \Rightarrow^{\mathcal{R}} \mu$, iff i) $\mu = \mathcal{D}_s$, or ii) $s \to \mu'$ and

$$\mu = \sum_{r \in (supp(\mu') \cap [s]) \wedge r \Rightarrow^{\mathcal{R}} \mu_r} \mu'(r) \cdot \mu_r + \sum_{r \in supp(\mu') \setminus [s]} \mu'(r) \cdot \mathcal{D}_r$$

where $[s]$ denotes the equivalence class containing s. Stated differently, $s \Rightarrow^{\mathcal{R}} \mu$ means that s can evolve into μ only via states in $[s]$. Accordingly, *branching combined transition* $s \Rightarrow^{\mathcal{R}}_{\mathrm{P}} \mu$ can be defined based on the branching transition, i.e. $s \Rightarrow^{\mathcal{R}}_{\mathrm{P}} \mu$ iff there exists a

collection of branching transitions $\{s \Rightarrow^{\mathcal{R}} \mu_i\}_{i\in I}$, and a collection of probabilities $\{p_i\}_{i\in I}$ with $\sum_{i\in I} p_i = 1$ such that $\mu = \sum_{i\in I} p_i \cdot \mu_i$.

We give the definition branching probabilistic bisimulation as follows:

Definition 9. An equivalence relation $\mathcal{R} \subseteq S \times S$ is a branching probabilistic bisimulation iff $s\ \mathcal{R}\ r$ implies that $L(s) = L(r)$ and for each $s \to \mu$, there exists $r \Rightarrow_{\mathrm{P}}^{\mathcal{R}} \mu'$ such that $\mu\ \mathcal{R}\ \mu'$.

We write $s \simeq_{\mathsf{P}} r$ whenever there is a branching probabilistic bisimulation $\mathcal{R}$ such that $s\ \mathcal{R}\ r$.

The following properties concerning branching probabilistic bisimulation are taken from [24]:

Lemma 4 ([24]). (1) $\simeq_{\mathsf{P}} \subseteq \sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} \subseteq \sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$.

(2) $\simeq_{\mathsf{P}}$ is preserved by $||$.

5.2. **A novel weak branching bisimulation.** Similar to the definition of bounded reachability $Prob_{\sigma,s}(C, C', n, \omega)$, we define the function $Prob_{\sigma,s}(C, C', \omega)$ which denotes the probability from s to states in C' possibly via states in C. Again ω is used to keep track of the path which has been visited. Formally, $Prob_{\sigma,s}(C, C', \omega)$ is equal to 1 if $s \in C'$, $Prob_{\sigma,s}(C, C', \omega)$ is equal to 0 if $s \notin C$, otherwise when $\sigma(\omega)(s, \mu') = 1$,

$$Prob_{\sigma,s}(C, C', \omega) = \sum_{r\in supp(\mu')} \mu'(r) \cdot Prob_{\sigma,r}(C, C', \omega r). \tag{5.1}$$

The definition of weak branching bisimulation is as follows:

Definition 10. A relation $\mathcal{R} \subseteq S \times S$ is a weak branching bisimulation if $s\ \mathcal{R}\ r$ implies that $L(s) = L(r)$ and for any $\mathcal{R}$ downward closed sets C, C'

(1) for each scheduler σ, there exists σ' such that $Prob_{\sigma',r}(C, C', r) \geq Prob_{\sigma,s}(C, C', s)$,
(2) for each scheduler σ, there exists σ' such that $Prob_{\sigma',s}(C, C', s) \geq Prob_{\sigma,r}(C, C', r)$.

We write $s \approx^{\mathsf{b}} r$ whenever there is a weak branching bisimulation $\mathcal{R}$ such that $s\ \mathcal{R}\ r$.

The following theorem shows that $\approx^{\mathsf{b}}$ is an equivalence relation. Also different from the strong cases where we use a series of equivalence relations to either characterize or approximate $\sim_{\mathsf{PCTL}}$ and $\sim_{\mathsf{PCTL}^*}$, in the weak scenario we show that $\approx^{\mathsf{b}}$ itself is enough to characterize $\sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$. Intuitively because in $\sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$ only unbounded until operator is allowed in path formula which means we abstract from the number of steps to reach certain states.

Theorem 5. (1) $\approx^{\mathsf{b}}$ is an equivalence relation.

(2) $\approx^{\mathsf{b}} = \sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$.

Proof. (1) The proof is similar as the proof of Clause (1) of Lemma 2.

(2) In order to prove that $s \sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}} r$ implies $s \approx^{\mathsf{b}} r$ for any s and r, we need to prove that $\mathcal{R} = \{(s, r) \mid s \sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}} r\}$ is a weak branching bisimulation. Therefore we need to show that for any $\mathcal{R}$ closed sets C, C' and scheduler σ of s, there exists a scheduler σ' of r such that $Prob_{\sigma',r}(C, C', r) \geq Prob_{\sigma,s}(C, C', s)$ and vice versa provided that $s\ \mathcal{R}\ r$. Following the way in the proof of Theorem 3, we can construct a formula φ_C such that $Sat(\varphi_C) = C$ where C is a $\mathcal{R}$ closed

set. Let $\psi = \varphi_C \,\mathsf{U}\, \varphi_{C'}$, then it is not hard to see that $s \models \neg\mathcal{P}_{<q}\psi$ where $q = Prob_{\sigma,s}(C, C', s)$. By assumption $r \models \neg\mathcal{P}_{<q}\psi$, so there exists a scheduler σ' such that $Prob_{\sigma',r}(C, C', r) \geq q$, that is, $Prob_{\sigma',r}(C, C', r) \geq Prob_{\sigma,s}(C, C', s)$. The other case is similar and is omitted here.

The proof of $\approx^{\mathsf{b}} \subseteq \sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$ is by structural induction on the syntax of state formula φ and path formula ψ of $\mathsf{PCTL}_{\setminus \mathsf{X}}$, that is, we need to prove the following two results simultaneously.

(a) $s \approx^{\mathsf{b}} r$ implies that $s \models \varphi$ iff $r \models \varphi$ for any state formula φ.

(b) $\omega_1 \approx^{\mathsf{b}} \omega_2$ implies that $\omega_1 \models \psi$ iff $\omega_2 \models \psi$ for any path formula ψ.

We only consider $\varphi = \mathcal{P}_{\leq q}(\psi)$ with $\psi = \varphi_1 \,\mathsf{U}\, \varphi_2$ since the other cases are similar. By induction $Sat(\varphi_1)$ and $Sat(\varphi_2)$ are $\approx^{\mathsf{b}}$ closed, moreover $Prob_{\sigma,s}(\{\omega \mid \omega \models \psi\}) = Prob_{\sigma,s}(Sat(\varphi_1), Sat(\varphi_2), s)$ by Equation (5.1) for any σ. We prove by contradiction, and assume that $s \models \varphi$ and $r \not\models \varphi$. According to the semantics, $s \models \varphi$ iff $\forall\sigma.Prob_{\sigma,s}(Sat(\varphi_1), Sat(\varphi_2), s) \leq q$. If $r \not\models \varphi$, then there exists σ' of r such that $Prob_{\sigma',r}(Sat(\varphi_1), Sat(\varphi_2), r) > q$, therefore for such σ', there does not exist σ of s such that $Prob_{\sigma,s}(Sat(\varphi_1), Sat(\varphi_2), s) \geq Prob_{\sigma',r}(Sat(\varphi_1), Sat(\varphi_2), r)$, which contradicts with the assumption $s \approx^{\mathsf{b}} r$. As a result, it must hold that $r \models \varphi$, and $s \sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}} r$.

□

As in the strong scenario, $\approx^{\mathsf{b}}$ suffers from the same problem as $\sim_i^{\mathsf{b}}$ and $\sim_i$ with $i > 1$, that is, it is not preserved by $||$.

Counterexample 4. $s \approx^{\mathsf{b}} r$ does not always imply $s \,||\, t \approx^{\mathsf{b}} r \,||\, t$ for any t. This can be shown in a similar way as Counterexample 2 since the result will still hold even if we replace the bounded until formula with unbounded until formula in Counterexample 2.

5.3. **Weak bisimulation.** In order to define weak bisimulation we consider stuttering paths. Let Ω be a finite $\mathcal{R}$ downward closed path, then

$$C_{\Omega_{st}} = \begin{cases} C_\Omega & l(\Omega) = 1 \\ \bigcup\limits_{\forall 0 \leq i < n. \forall k_i \geq 0} C_{(\Omega[0])^{k_0} \ldots (\Omega[n-2])^{k_{n-2}} \Omega[n-1]} & l(\Omega) = n \geq 2 \end{cases} \tag{5.2}$$

is the set of $\mathcal{R}$ downward closed paths which contains all stuttering paths, where $\Omega[i]$ denotes the $(i+1)$-th element in Ω such that $0 \leq i < l(\Omega)$. Accordingly, $C_{\widetilde{\Omega}_{st}} = \bigcup\limits_{\Omega \in \widetilde{\Omega}} C_{\Omega_{st}}$ contains all the stuttering paths of each $\Omega \in \widetilde{\Omega}$. Given a measure $Prob$, $Prob(\widetilde{\Omega}_{st})$ can be computed by Equation (4.2).

Now we are ready to give the definition of weak bisimulation as follows:

Definition 11. A relation $\mathcal{R} \subseteq S \times S$ is a weak bisimulation if $s \,\mathcal{R}\, r$ implies that $L(s) = L(r)$ and for any $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$

(1) for each scheduler σ, there exists σ' such that $Prob_{\sigma',r}(C_{\widetilde{\Omega}_{st}}) \geq Prob_{\sigma,s}(C_{\widetilde{\Omega}_{st}})$,

(2) for each scheduler σ, there exists σ' such that $Prob_{\sigma',s}(C_{\widetilde{\Omega}_{st}}) \geq Prob_{\sigma,r}(C_{\widetilde{\Omega}_{st}})$.

We write $s \approx r$ whenever there is a weak bisimulation $\mathcal{R}$ such that $s \,\mathcal{R}\, r$.

The following theorem shows that $\approx$ is an equivalence relation. For the same reason as in Theorem 5, $\approx$ is enough to characterize $\sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$ which gives us the following theorem.

Theorem 6. (1) $\approx$ is an equivalence relation.
(2) $\approx = \sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$.

Proof. (1) The proof is similar as the proof of Clause (1) of Lemma 2.

(2) Let $\mathcal{R} = \{(s,r) \mid s \sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} r\}$, in order to prove that $s \sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} r$ implies $s \approx r$ for any s and r, it is enough to show that $\mathcal{R}$ is a weak bisimulation. We need to show that for any $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ and scheduler σ, there exists a scheduler σ' such that $Prob_{\sigma',r}(C_{\widetilde{\Omega}_{st}}) \geq Prob_{\sigma,s}(C_{\widetilde{\Omega}_{st}})$ and vice versa provided that $s \mathcal{R} r$. Following the way in the proof of Theorem 3, we can construct a formula φ_C such that $Sat(\varphi_C) = C$ where C is a $\mathcal{R}$ closed set. Let $\psi_\Omega = \varphi_{C_0} \mathsf{U} \ldots \varphi_{C_n}$ where $\Omega = C_{C_0 \ldots C_n}$, then $\psi_{\widetilde{\Omega}} = \bigvee_{\Omega \in \widetilde{\Omega}} \psi_\Omega$. It is easy to see that $s \models \neg \mathcal{P}_{<q} \psi$ where $q = Prob_{\sigma,s}(C_{\widetilde{\Omega}_{st}})$ and $\psi = \psi_{\widetilde{\Omega}}$. By assumption $r \models \neg \mathcal{P}_{<q}\psi$, so there exists a scheduler σ' such that $Prob_{\sigma',r}(C_{\widetilde{\Omega}_{st}}) \geq q$, that is, $Prob_{\sigma',r}(C_{\widetilde{\Omega}_{st}}) \geq Prob_{\sigma,s}(C_{\widetilde{\Omega}_{st}})$. The other case is similar and is omitted here.

The proof of $\approx \subseteq \sim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$ is by structural induction on the syntax of state formula φ and path formula ψ of $\mathsf{PCTL}^*_{\setminus \mathsf{X}}$, that is, we need to prove the following two results simultaneously.

(a) $s \approx r$ implies that $s \models \varphi$ iff $r \models \varphi$ for any state formula φ.
(b) $\omega_1 \approx \omega_2$ implies that $\omega_1 \models \psi$ iff $\omega_2 \models \psi$ for any path formula ψ.

To make the proof clearer, we rewrite the syntax of $\mathsf{PCTL}^*_{\setminus \mathsf{X}}$ as follows which is equivalent to the original definition.

$$\psi ::= \varphi \mid \psi_1 \vee \psi_2 \mid \neg\psi \mid \psi_1 \mathsf{U} \psi_2$$

We only consider $\varphi = \mathcal{P}_{\leq q}(\psi)$ here. We need to prove that for each σ for each ψ, there exists $\widetilde{\Omega} \subseteq (\approx^{\downarrow})^\infty$ such that $Prob_{\sigma,s}(\widetilde{\Omega}) = Prob_{\sigma,s}(Sat(\psi))$. The proof is by structural induction on ψ as follows:

(a) $\psi = \varphi'$. By induction $Sat(\varphi')$ is $\approx$ closed. Let $\widetilde{\Omega} = \{Sat(\varphi')\}$, then $Prob_{\sigma,s}(\widetilde{\Omega}) = Prob_{\sigma,s}(Sat(\psi))$.
(b) $\psi = \psi_1 \vee \psi_2$. By induction there exists $\widetilde{\Omega}'$ and $\widetilde{\Omega}''$ such that $Prob_{\sigma,s}(Sat(\psi_1)) = Prob_{\sigma,s}(C_{\widetilde{\Omega}'_{st}})$ and $Prob_{\sigma,s}(Sat(\psi_2)) = Prob_{\sigma,s}(C_{\widetilde{\Omega}''_{st}})$. It is not hard to see that $\widetilde{\Omega} = \widetilde{\Omega}' \cup \widetilde{\Omega}''$ will be enough.
(c) $\psi = \psi_1 \mathsf{U} \psi_2$. By induction there exists $\widetilde{\Omega}'$ and $\widetilde{\Omega}''$ such that $Prob_{\sigma,s}(Sat(\psi_1)) = Prob_{\sigma,s}(C_{\widetilde{\Omega}'_{st}})$ and $Prob_{\sigma,s}(Sat(\psi_2)) = Prob_{\sigma,s}(C_{\widetilde{\Omega}''_{st}})$. Let $\widetilde{\Omega} = \{\Omega'\Omega'' \mid \Omega' \in \widetilde{\Omega}' \wedge \Omega'' \in \widetilde{\Omega}''\}$, then $Prob_{\sigma,s}(\widetilde{\Omega}) = Prob_{\sigma,s}(Sat(\psi))$.
(d) $\psi = \neg\psi'$. $s \models \mathcal{P}_{\geq q}(\psi)$ iff $s \models \mathcal{P}_{<1-q}(\psi')$, so ψ can be reduced to another formula without $\neg$ operator.

The following proof is routine and is omitted here.

□

Not surprisingly $\approx$ is not preserved by $||$.

Counterexample 5. $s \approx r$ does not always imply $s \,||\, t \approx r \,||\, t$ for any t. This can be shown by using the same arguments as in Counterexample 4.

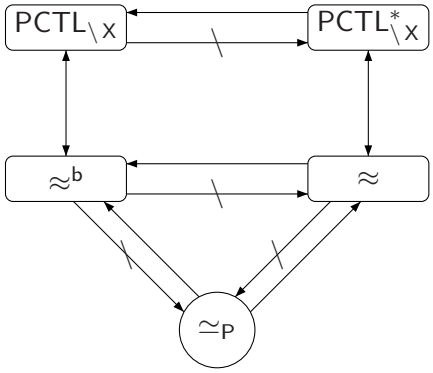

Figure 4: Relationship of different equivalences in weak scenario.

5.4. **Taxonomy for weak bisimulations.** As in the strong cases we summarize the relation of the equivalences in the weak scenario in Fig. 4 where all the denotations have the same meaning as Fig. 3. Compared to Fig. 3, Fig. 4 is much simpler because the step-indexed bisimulations are absent. As in strong cases, here we do not consider the standard definition of branching bisimulation which is a strict subset of $\simeq_{\mathsf{P}}$ and can be defined by replacing $\Rightarrow_{\mathrm{P}}^{\mathcal{R}}$ with $\Rightarrow^{\mathcal{R}}$ in Definition 9. Again not surprisingly all the relations shown in Fig. 4 coincide with the weak bisimulation defined in [3] in the DTMC setting.

6. Simulations

In Section 4 and 5 we discuss bisimulations and their characterizations. Usually two states s and r are bisimilar iff s can mimic stepwise all the transitions of r and vice versa. In this section we relax the conditions of bisimulations, and only requires one direction mimicking, which introduces us the definitions of simulations. Simulations are preorders on the states, which has been used widely for verification purpose [20, 15, 13, 24, 3]. Intuitively, if r simulates s, then r can be seen as a correct implementation of s. Since s is more abstract and contains less details, it is much easier to be analyzed. We also discuss the characterization of simulations w.r.t. the safe fragments of PCTL and PCTL*. First let us introduce the safe fragment of PCTL*, denoted by PCTL^*_{safe}, which is a fragment of PCTL* without negative operators except for the atomic propositions, and is defined by the following syntax:

$$\varphi ::= a \mid \neg a \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \mathcal{P}_{\leq q}(\psi)$$
$$\psi ::= \varphi \mid \psi_1 \wedge \psi_2 \mid \psi_1 \vee \psi_2 \mid \mathsf{X}\,\psi \mid \psi_1 \,\mathsf{U}\, \psi_2$$

where $a \in AP$ and $q \in [0,1]$. Accordingly the safe fragment of PCTL, denoted by PCTL_{safe}, is a sub logic of PCTL^*_{safe} where only the path formula is constrained to be the following form:

$$\psi ::= \mathsf{X}\,\varphi \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \mid \varphi_1 \,\mathsf{U}^{\leq n}\, \varphi_2.$$

We write $s \preceq_{\mathsf{PCTL}^*_{safe}} r$ iff $r \models \varphi$ implies that $s \models \varphi$ for any φ of PCTL^*_{safe}, and similarly for other sub-logics.

Again we first introduce the strong probabilistic simulation introduced in [24] before doing so we need to define the *weight function* in the way as [16].

Definition 12. Let $\mathcal{R} = S \times S$ be a relation over S. A weight function for μ and ν with respect to $\mathcal{R}$ is a function $\Delta : S \times S \mapsto [0,1]$ such that:

- $\Delta(s,r) > 0$ implies that $s \ \mathcal{R} \ r$,
- $\mu(s) = \sum_{r \in S} \Delta(s,r)$ for any $s \in S$,
- $\nu(r) = \sum_{s \in S} \Delta(s,r)$ for any $r \in S$.

We write $\mu \ \sqsubseteq_{\mathcal{R}} \ \nu$ iff there exists a weight function for μ and ν with respect to $\mathcal{R}$.

Below follows the definition of strong probabilistic simulation.

Definition 13. A relation $\mathcal{R} \subseteq S \times S$ is a strong probabilistic simulation iff $s \ \mathcal{R} \ r$ implies that $L(s) = L(r)$ and for each $s \to \mu$, there exists a combined transition $r \to_{\mathsf{P}} \mu'$ such that $\mu \ \sqsubseteq_{\mathcal{R}} \ \mu'$.

We write $s \ \prec_{\mathsf{P}} \ r$ whenever there is a strong probabilistic simulation $\mathcal{R}$ such that $s \ \mathcal{R} \ r$.

It was shown in [24] that $\sqsubseteq_{\mathcal{R}}$ is congruent, i.e. $s \ \prec_{\mathsf{P}} \ r$ implies that $s \,||\, t \ \prec_{\mathsf{P}} \ r \,||\, t$ for any t. But not surprisingly, it turns out that the strong probability simulation is too fine w.r.t $\prec_{\mathsf{PCTL}_{safe}}$ and $\prec_{\mathsf{PCTL}^*_{safe}}$ which can be seen from Example 1. Similarly we have the correspondent theorem of Theorem 1 in the simulation scenario where we only consider the safe fragment of the logics, thus the subscription *safe* is often omitted for readability.

Theorem 7. (1) $\prec_{\mathsf{PCTL}}$, $\prec_{\mathsf{PCTL}^*}$, $\prec_{\mathsf{PCTL}^-}$, $\prec_{\mathsf{PCTL}^-_i}$, $\prec_{\mathsf{PCTL}^{*-}}$, $\prec_{\mathsf{PCTL}^{*-}_i}$, and $\prec_{\mathsf{P}}$ are preorders for any $i \geq 1$.

(2) $\prec_{\mathsf{P}} \subset \prec_{\mathsf{PCTL}^*} \subset \prec_{\mathsf{PCTL}}$.

(3) $\prec_{\mathsf{PCTL}^{*-}} \subset \prec_{\mathsf{PCTL}^-}$.

(4) $\prec_{\mathsf{PCTL}^{*-}_1} = \prec_{\mathsf{PCTL}^-_1}$.

(5) $\prec_{\mathsf{PCTL}^{*-}_i} \subset \prec_{\mathsf{PCTL}^-_i}$ for any $i > 1$.

(6) $\prec_{\mathsf{PCTL}} \subset \prec_{\mathsf{PCTL}^-} \subseteq \prec_{\mathsf{PCTL}^-_{i+1}} \subset \prec_{\mathsf{PCTL}^-_i}$ for all $i \geq 0$.

(7) $\prec_{\mathsf{PCTL}^*} \subset \prec_{\mathsf{PCTL}^{*-}} \subset \prec_{\mathsf{PCTL}^{*-}_{i+1}} \subset \prec_{\mathsf{PCTL}^{*-}_i}$ for all $i \geq 0$.

Proof. For Clause (1) we only prove that $\prec_{\mathsf{PCTL}}$ is a preorder since the others are similar. The reflexivity is trivial as $s \ \prec_{\mathsf{PCTL}} \ s$ for any s. Suppose that $s \ \prec_{\mathsf{PCTL}} \ t$ and $t \ \prec_{\mathsf{PCTL}} \ r$, then we need to prove that $s \ \prec_{\mathsf{PCTL}} \ r$ in order to the transitivity. According to the definition of $\prec_{\mathsf{PCTL}}$, we need to prove that $r \models \varphi$ implies $s \models \varphi$ for any φ. Suppose that $r \models \varphi$ for some φ, then $t \models \varphi$ because of $t \ \prec_{\mathsf{PCTL}} \ r$, moreover since $s \ \prec_{\mathsf{PCTL}} \ t$, hence $s \models \varphi$ which completes the proof.

The proof of Clause (2) can be found in [24]. Since we have shown in Theorem 1 that PCTL^-_1 and PCTL^{*-}_1 have the same expressiveness, thus the proof of Clause (4) is straightforward. The proofs of all the other clauses are trivial. □

6.1. **Strong i-depth branching simulation.** Following Section 4.2 we can define strong i-depth branching simulation which can be characterized by $\prec_{\mathsf{PCTL}^-_i}$. Let $s \ \prec^{\mathsf{b}}_0 \ r$ iff $L(s) = L(r)$, then

Definition 14. A relation $\mathcal{R} \subseteq S \times S$ is a strong i-depth branching simulation with $i \geq 1$ iff $s \ \mathcal{R} \ r$ implies that $s \ \prec^{\mathsf{b}}_{i-1} \ r$ and for any $\mathcal{R}$ downward closed sets C, C', and any scheduler σ, there exists σ' such that $Prob_{\sigma',r}(C, C', i) \geq Prob_{\sigma,s}(C, C', i)$.

We write $s \ \prec^{\mathsf{b}}_i \ r$ whenever there is a strong i-depth branching simulation $\mathcal{R}$ such that $s \ \mathcal{R} \ r$. The strong branching simulation $\prec^{\mathsf{b}}$ is defined as $\prec^{\mathsf{b}} = \cap_{i \geq 0} \prec^{\mathsf{b}}_i$.

Below we show the similar properties of strong i-depth branching simulations.

Lemma 5. (1) $\prec^{\mathsf{b}}$ and $\prec^{\mathsf{b}}_i$ are preorders for any $i \geq 0$.
(2) $\prec^{\mathsf{b}}_j \subseteq \prec^{\mathsf{b}}_i$ provided that $0 \leq i \leq j$.
(3) There exists $i \geq 0$ such that $\prec^{\mathsf{b}}_j = \prec^{\mathsf{b}}_k$ for any $j, k \geq i$.

Proof. (1) The reflexivity is trivial, we only prove the transitivity. Suppose that $s_1 \prec^{\mathsf{b}}_i s_2$ and $s_2 \prec^{\mathsf{b}}_i s_3$, we need to prove that $s_1 \prec^{\mathsf{b}}_i s_3$. By Definition 14 there exists strong simulation $\mathcal{R}_1$ and $\mathcal{R}_2$ such that $s_1 \mathcal{R}_1 s_2$ and $s_2 \mathcal{R}_2 s_3$. Let $\mathcal{R} = \mathcal{R}_1 \circ \mathcal{R}_2 = \{(s_1, s_3) \mid \exists s_2.(s_1 \mathcal{R}_1 s_2 \wedge s_2 \mathcal{R}_2 s_3)\}$, it is enough to prove that $\mathcal{R}$ is strong i-depth branching simulation. Due to the reflexivity, any $\mathcal{R}$ downward closed set C is also $\mathcal{R}_1$ and $\mathcal{R}_2$ downward closed. Therefore for any $\mathcal{R}$ downward closed sets C, C', if $Prob_{\sigma,s_1}(C, C', i) > 0$ for a scheduler σ, then there exists σ' such that $Prob_{\sigma',s_2}(C, C', i) \geq Prob_{\sigma,s_1}(C, C', i)$ according to Definition 14. Similarly, there exists σ'' such that $Prob_{\sigma'',s_3}(C, C', i) \geq Prob_{\sigma',s_2}(C, C', i) \geq Prob_{\sigma,s_1}(C, C', i)$, and $\mathcal{R}$ is indeed a strong i-depth branching simulation. This completes the proof.
(2) It is straightforward from Definition 14.
(3) Since there are only finite states, thus only finite equivalence classes, such i always exists.

□

Our strong i-depth branching simulation coincides with $\prec_{\mathsf{PCTL}^-_i}$ for each i, therefore $\prec_{\mathsf{PCTL}}$ is equivalent to $\prec^{\mathsf{b}}$ as shown by the following theorem.

Theorem 8. $\prec_{\mathsf{PCTL}^-_i} = \prec^{\mathsf{b}}_i$ for any $i \geq 1$, and moreover $\prec_{\mathsf{PCTL}} = \prec^{\mathsf{b}}$.

Proof. We first prove that $\prec_{\mathsf{PCTL}^-_i}$ implies $\prec^{\mathsf{b}}_i$. Let $\mathcal{R} = \{(s, r) \mid s \prec_{\mathsf{PCTL}^-_i} r\}$, it is enough to prove that $\mathcal{R}$ is a strong i-depth branching simulation. Suppose that $s \mathcal{R} r$, we need to prove that for any $\mathcal{R}$ downward closed sets C, C' and scheduler σ of s, there exists σ' of r such that $Prob_{\sigma',r}(C, C', i) \geq Prob_{\sigma,s}(C, C', i)$. Note that $Sat(\varphi)$ is a $\mathcal{R}$ downward closed set for any φ. Since the states space is finite, for each $\mathcal{R}$ downward closed set C, there exists φ_C such that $Sat(\varphi_C) = C$. Assume that there exists $\mathcal{R}$ downward closed sets C, C' and σ such that $Prob_{\sigma',r}(C, C', i) < Prob_{\sigma,s}(C, C', i)$ for all schedulers σ' of r. Then there exists q such that $r \models \mathcal{P}_{\leq q}(\psi)$ but $s \not\models \mathcal{P}_{\leq q}(\psi)$ where $\psi = \varphi_C \, \mathsf{U}^{\leq i} \, \varphi_{C'}$, this contradicts with the assumption that $s \prec_{\mathsf{PCTL}^-_i} r$. Therefore $\mathcal{R}$ is a strong i-depth branching bisimulation.

In order to prove that $\prec^{\mathsf{b}}_i$ implies $\prec_{\mathsf{PCTL}^-_i}$, we need to prove that whenever $s \prec^{\mathsf{b}}_i r$ and $r \models \varphi$, we also have $s \models \varphi$. We prove by structural induction on φ, and only consider the case when $\varphi = \mathcal{P}_{\leq q}(\varphi_1 \, \mathsf{U}^{\leq i} \, \varphi_2)$ since all the others are trivial. By induction $Sat(\varphi_1)$ and $Sat(\varphi_2)$ are $\prec^{\mathsf{b}}_i$ downward closed, therefore if $r \models \mathcal{P}_{\leq q}(\varphi_1 \, \mathsf{U}^{\leq i} \, \varphi_2)$, but $s \not\models \mathcal{P}_{\leq q}(\varphi_1 \, \mathsf{U}^{\leq i} \, \varphi_2)$, then there exists σ of s such that there does not exist σ' such that $Prob_{\sigma',r}(Sat(\varphi_1), Sat(\varphi_2), i) \geq Prob_{\sigma,s}(Sat(\varphi_1), Sat(\varphi_2), i)$ which contradicts with the assumption that $s \prec^{\mathsf{b}}_i r$. □

In Counterexample 2 we have shown the $\sim^{\mathsf{b}}_i$ is not compositional for $i > 1$, using the same arguments we can show that $\prec^{\mathsf{b}}_i$ is not compositional either for $i > 1$, thus we have

Theorem 9. $s \prec^{\mathsf{b}}_1 r$ implies that $s \,||\, t \prec^{\mathsf{b}}_1 r \,||\, t$ for any t, while $\prec^{\mathsf{b}}_i$ with $i > 1$ is not compositional in general.

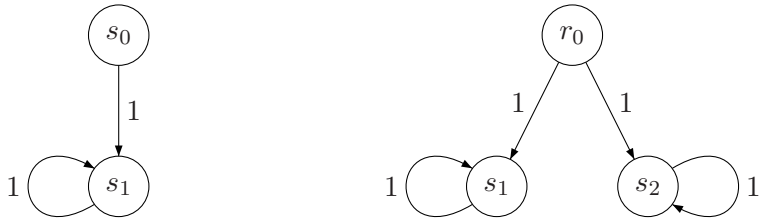

Figure 5: $s_0 \not\prec_{\mathsf{PCTL}_{live}} r_0$.

Proof. Let $\mathcal{R} = \{(s \,||\, t, r \,||\, t) \mid s \prec_1^{\mathsf{b}} r\}$, it is enough to show that $\mathcal{R}$ is a strong 1-depth simulation. Let C, C' be two $\mathcal{R}$ downward closed sets, there are several cases we need to consider:

(1) If $s \,||\, t \notin C$, then $Prob_{\sigma, s\,||\,t}(C, C', 1) = 0$. Since C is $\mathcal{R}$ downward closed, $r \,||\, t \notin C$ by induction, thus there exists σ' such that $Prob_{\sigma', r\,||\,t}(C, C', 1) \geq Prob_{\sigma, s\,||\,t}(C, C', 1)$.

(2) If $s \,||\, t \in C$, and for each scheduler σ, there exists $s \,||\, t \to \mu$ such that $\mu(C') = Prob_{\sigma, s\,||\,t}(C, C', 1)$. According to Definition 3, $s \,||\, t \to \mu$ iff either $s \to \mu_s$ such that $\mu_s \,||\, \mathcal{D}_t = \mu$, or $t \to \mu_t$ such that $\mathcal{D}_s \,||\, \mu_t = \mu$. We only consider the first case, since the other one is similar. Since $\mu_s \,||\, \mathcal{D}_t = \mu$, there exists $\mathcal{R}$ downward closed set C'' such that $\mu_s(C'') = \mu(C')$. The following proof is then straightforward.

Note that Counterexample 2 also applies here, thus $\prec_i^{\mathsf{b}}$ is not compositional when $i > 1$. □

Remark 2. The safe fragment of PCTL we adopt in this paper is slightly different from [3] where two new operators $\widetilde{\mathsf{X}}$ and $\widetilde{\mathsf{U}}$ are introduced, called weak next and until respectively, and the $\mathcal{P}_{\leq q}(\psi)$ is replaced by $\mathcal{P}_{\geq q}(\psi)$. The semantics of $\widetilde{\mathsf{X}}$ and $\widetilde{\mathsf{U}}$ are defined as follows where $|\omega|$ denotes the length of ω:

$$\omega \models \widetilde{\mathsf{X}}\varphi \text{ iff } (|\omega| < 1 \vee \omega[i] \models \varphi)$$

$$\omega \models \varphi_1 \widetilde{\mathsf{U}} \varphi_2 \text{ iff } (\omega \models \varphi_1 \,\mathsf{U}\, \varphi_2 \vee \forall i \leq |\omega|.\omega[i] \models \varphi_1)$$

Similarly we can also define the weak counterpart of bounded until $\widetilde{\mathsf{U}}^{\leq n}$. Due to duality between X, $\mathsf{U}^{\leq n}$, U and their weak counterparts, these two variants of safe PCTL are essentially equivalent, refer to [3] for detail discussion.

Let PCTL_{live} denote the liveness fragment of PCTL in [3] which is the same as PCTL_{safe} except that $\mathcal{P}_{\leq q}(\psi)$ is replaced with $\mathcal{P}_{\geq q}(\psi)$. We say $s \prec_{\mathsf{PCTL}_{live}} r$ iff $s \models \varphi$ implies $r \models \varphi$ for any state formula of PCTL_{live}. Even though it has been shown in [3] that $\prec_{\mathsf{PCTL}_{safe}}$ and $\prec_{\mathsf{PCTL}_{live}}$ are equivalent for DTMC (PA without nondeterministic choices), the result is not true for PA. Refer to the following example.

Example 4. Consider the two states s_0 and r_0 shown in Fig. 5, where we assume that all the states have different labels except that $L(s_0) = L(r_0)$. It is easy to check that $s_0 \prec_{\mathsf{P}} r_0$, thus $s_0 \prec_{\mathsf{PCTL}_{safe}} r_0$ according to Clause (2) of Theorem 7, but we have $s_0 \not\prec_{\mathsf{PCTL}_{live}} r_0$. Let $\varphi = \mathcal{P}_{\geq 1}(L(s_0) \,\mathsf{U}\, L(s_1))$ which is a valid state formula of PCTL_{live}, it is obvious that $s_0 \models \varphi$, but $r_0 \not\models \varphi$ since the minimal probability of r_0 reaching state s_1 is equal to 0 i.e. by choosing the transition to s_2.

6.2. **Strong i-depth simulation.** In this section we introduce strong i-depth simulation which can be characterized by $\prec_{\mathsf{PCTL}_i^{*-}}$. Below follows the definition of strong i-depth simulation where $\prec_0 = \prec_0^{\mathsf{b}}$.

Definition 15. A relation $\mathcal{R} \subseteq S \times S$ is a strong i-depth simulation with $i \geq 1$ iff $s \ \mathcal{R} \ r$ implies that $s \ \prec_{i-1} \ r$ and for any $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ with $l(\widetilde{\Omega}) = i$ and any scheduler σ, there exists σ' such that $Prob_{\sigma',r}(C_{\widetilde{\Omega}}) \geq Prob_{\sigma,s}(C_{\widetilde{\Omega}})$.

We write $s \ \prec_i \ r$ whenever there is a i-depth strong simulation $\mathcal{R}$ such that $s \ \mathcal{R} \ r$. The strong simulation $\prec$ is defined as $\prec = \cap_{i \geq 0} \prec_i$.

Below we show the similar properties of strong i-depth simulations.

Lemma 6. (1) $\prec$ and $\prec_i$ are preorders for any $i \geq 0$.
(2) $\prec_j \subseteq \prec_i$ provided that $0 \leq i \leq j$.
(3) There exists $i \geq 0$ such that $\prec_j = \prec_k$ for any $j, k \geq i$.

Proof. (1) This clause can be proved in a similar way as Clause (1) of Lemma 5.
(2) According to Definition 15, as i is growing, $\prec_i$ is getting finer.
(3) The proof is based on the fact that the states are finitely many, with the similar argument as in Clause (3) of Lemma 5.

□

Our strong i-depth simulation coincides with $\prec_{\mathsf{PCTL}_i^{*-}}$ for each i, therefore $\prec_{\mathsf{PCTL}^*}$ is equivalent to $\prec$ as shown by the following theorem.

Theorem 10. $\prec_{\mathsf{PCTL}_i^{*-}} = \prec_i$ for any $i \geq 1$, and moreover $\prec_{\mathsf{PCTL}^*} = \prec$.

Proof. We first prove that $s \ \prec_{\mathsf{PCTL}_i^{*-}} \ r$ implies $s \ \prec_i \ r$ for any s and r. Let $\mathcal{R} = \{(s,r) \mid s \ \prec_{\mathsf{PCTL}_i^{*-}} \ r\}$, we need to show that for any $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ with $l(\widetilde{\Omega}) \leq i$ and scheduler σ, there exists a scheduler σ' such that $Prob_{\sigma',r}(C_{\widetilde{\Omega}}) \geq Prob_{\sigma,s}(C_{\widetilde{\Omega}})$ whenever $s \ \mathcal{R} \ r$. By induction, there exists a formula φ_C such that $Sat(\varphi_C) = C$ where C is $\mathcal{R}$ downward closed set. Suppose $\Omega = C_0 C_1 \ldots C_j$ with $j \leq i$, then

$$\psi_\Omega = \varphi_{C_0} \wedge \mathsf{X}(\varphi_{C_1} \wedge \ldots \wedge \mathsf{X}(\varphi_{C_{j-1}} \wedge \mathsf{X}\,\varphi_{C_j}))$$

can be used to characterize Ω, that is, $Sat(\psi_\Omega) = C_\Omega$. Let $\psi = \bigvee_{\Omega \in \widetilde{\Omega}} \psi_\Omega$, then $Sat(\psi) = C_{\widetilde{\Omega}}$. We prove by contradiction. Suppose that there does not exist σ' such that $Prob_{\sigma',r}(C_{\widetilde{\Omega}}) \geq Prob_{\sigma,s}(C_{\widetilde{\Omega}})$, then there exists q such that $r \models \mathcal{P}_{\leq q}\psi$, but $s \not\models \mathcal{P}_{\leq q}\psi$ which contradicts with the assumption that $s \ \prec_{\mathsf{PCTL}_i^{*-}} \ r$, so there exists a scheduler σ' such that $Prob_{\sigma',r}(C_{\widetilde{\Omega}}) \geq q = Prob_{\sigma,s}(C_{\widetilde{\Omega}})$. The other case is similar and is omitted here.

The proof of $\prec_i \subseteq \prec_{\mathsf{PCTL}_i^{*-}}$ is by structural induction on the syntax of state formula φ and path formula ψ of safe PCTL_i^{*-}, that is, we need to prove the following two results simultaneously.

(1) $r \models \varphi$ implies $s \models \varphi$ for any state formula φ provided that $s \ \prec_i \ r$.
(2) $\omega_2 \models \psi$ implies $\omega_1 \models \psi$ for any path formula ψ provided that $\omega_1 \ \prec_i \ \omega_2$.

We only consider $\varphi = \mathcal{P}_{\leq q}(\psi)$ here. Suppose that $r \models \varphi$, i.e. $\forall \sigma. Prob_{\sigma,r}(\{\omega \mid \omega \models \psi\}) \leq q$, we need to show that $s \models \varphi$. We prove by contradiction, and assume that $s \not\models \varphi$, i.e. there exists σ such that $Prob_{\sigma,s}(\{\omega \mid \omega \models \psi\}) > q$. By induction $\{\omega \mid \omega \models \psi\}$ is $\prec_i$ downward closed, that is, there exists $\widetilde{\Omega} = \{\omega \mid \omega \models \psi\}$, and moreover $l(\widetilde{\Omega}) \leq i$ since the depth of ψ is

at most i. Since $r \models \varphi$, there does not exists σ' such that $Prob_{\sigma',r}(C_{\widetilde{\Omega}}) \geq Prob_{\sigma,s}(C_{\widetilde{\Omega}}) = q$, which contradicts the assumption that $s \prec_i r$, thus it holds that $s \models \varphi$. □

Similarly, we can show that $\prec_i$ is not compositional either for $i > 1$, thus we have

Theorem 11. *$s \prec_1 r$ implies that $s \,||\, t \prec_1 r \,||\, t$ for any t, while $\prec_i$ with $i > 1$ is not compositional in general.*

Proof. According to Theorem 8 and 10, and Clause (4) of Theorem 7, $\prec_1^{\mathsf{b}} = \prec_1$, thus the result is straightforward according to Theorem 9. □

6.3. **Weak simulations.** Given the results for weak bisimulations from Section 5, the characterization of weak simulations is straightforward. Let us first introduce the definition of branching probabilistic simulation by Segala as follows:

Definition 16. A relation $\mathcal{R} \subseteq S \times S$ is a branching probabilistic simulation iff $s \,\mathcal{R}\, r$ implies that $L(s) = L(r)$ and for each $s \to \mu$, there exists $r \Rightarrow_{\mathrm{P}}^{\mathcal{R}} \mu'$ such that $\mu \,\mathcal{R}\, \mu'$.

We write $s \precsim_{\mathsf{P}} r$ whenever there is a branching probabilistic simulation $\mathcal{R}$ such that $s \,\mathcal{R}\, r$.

From [24] we know that $\precsim_{\mathsf{P}}$ is compositional, but it is too fine for $\precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$ as well as $\precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$, therefore along the line of weak bisimulations, we come out similar results for weak simulations. Below follows the definition of weak branching simulation.

Definition 17. A relation $\mathcal{R} \subseteq S \times S$ is a weak branching simulation iff $s \,\mathcal{R}\, r$ implies that $L(s) = L(r)$ and for any $\mathcal{R}$ downward closed sets C, C' and any scheduler σ, there exists σ' such that $Prob_{\sigma',r}(C, C', r) \geq Prob_{\sigma,s}(C, C', s)$.

We write $s \precsim^{\mathsf{b}} r$ whenever there is a weak branching simulation $\mathcal{R}$ such that $s \,\mathcal{R}\, r$.

Due to Counterexample 4, $\precsim^{\mathsf{b}}$ is not compositional, but it coincides with $\precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$ as shown by the following theorem.

Theorem 12. *$\precsim^{\mathsf{b}}$ is a preorder, and $\precsim^{\mathsf{b}} = \precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$.*

Proof. (1) The proof is similar as the proof Clause (1) of Lemma 5.

(2) In order to prove that $s \precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}} r$ implies $s \precsim^{\mathsf{b}} r$ for any s and r, it is enough to show that $\mathcal{R} = \{(s, r) \mid s \precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}} r\}$ is a weak branching simulation i.e. we need to prove that for any $\mathcal{R}$ downward closed sets C, C' and scheduler σ, there exists a scheduler σ' such that $Prob_{\sigma',r}(C, C', r) \geq Prob_{\sigma,s}(C, C', s)$ provided that $s \,\mathcal{R}\, r$. Let φ_C be a formula such that $Sat(\varphi_C) = C$ where C is a $\mathcal{R}$ downward closed set. We prove by contradiction. Suppose that there does not exist σ' such that $Prob_{\sigma',r}(C, C', r) \geq Prob_{\sigma,s}(C, C', s)$, then there exists q such that $r \models \mathcal{P}_{\leq q}\psi$ where $\psi = \varphi_C \,\mathsf{U}\, \varphi_{C'}$, but $s \not\models \mathcal{P}_{\leq q}\psi$, which contradicts with the assumption that $s \precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}} r$. Therefore there must exist a scheduler σ' such that $Prob_{\sigma',r}(C, C', r) \geq Prob_{\sigma,s}(C, C', s)$. The other case is similar and is omitted here.

The proof of $\precsim^{\mathsf{b}} \subseteq \precsim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$ is by structural induction on the syntax of state formula φ and path formula ψ of safe $\mathsf{PCTL}_{\setminus \mathsf{X}}$, that is, we need to prove the following two results simultaneously.

(a) $r \models \varphi$ implies $s \models \varphi$ for any state formula φ provided that $s \precsim^{\mathsf{b}} r$.

(b) $\omega_2 \models \psi$ implies that $\omega_1 \models \psi$ for any path formula ψ provided that $\omega_1 \precsim^{\mathsf{b}} \omega_2$.

We only consider $\varphi = \mathcal{P}_{\leq q}(\psi)$ where $\psi = \varphi_1 \mathsf{U} \varphi_2$ since the other cases are similar. Suppose that $r \models \varphi$, we need to prove that $s \models \varphi$. We prove by contradiction, and assume that $s \not\models \varphi$, then there exists σ such that $Prob_{\sigma,s}(\{\omega \mid \omega \models \psi\}) > q$. By induction $Sat(\varphi_1)$ and $Sat(\varphi_2)$ are $\precsim^{\mathsf{b}}$ downward closed, thus $Prob_{\sigma,s}(Sat(\varphi_1), Sat(\varphi_2), s) = Prob_{\sigma,s}(\{\omega \mid \omega \models \psi\}) > q$. Since $r \models \varphi$, there does not exist σ' such that $Prob_{\sigma,r}(Sat(\varphi_1), Sat(\varphi_2), r) \geq Prob_{\sigma,s}(Sat(\varphi_1), Sat(\varphi_2), s)$ which contradicts with the assumption that $s \precsim^{\mathsf{b}} r$, thus $s \models \varphi$, and $s \precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} r$. □

The weak simulation equivalent to $\precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$ can also be obtained in a straightforward way by adapting Definition 11.

Definition 18. A relation $\mathcal{R} \subseteq S \times S$ is a weak simulation iff $s \mathcal{R} r$ implies that $L(s) = L(r)$ and for any $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ and any scheduler σ, there exists σ' such that $Prob_{\sigma',r}(C_{\widetilde{\Omega}_{st}}) \leq Prob_{\sigma,s}(C_{\widetilde{\Omega}_{st}})$.

We write $s \precsim r$ whenever there is a weak simulation $\mathcal{R}$ such that $s \mathcal{R} r$.

Again $\precsim$ is not compositional, but it coincides with $\precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$, therefore we have the following theorem.

Theorem 13. $\precsim$ is a preorder, and $\precsim = \precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$.

Proof. (1) Again the reflexibility of $\precsim$ is trivial. We only prove the transitivity of $\precsim$. Suppose that $s \precsim r$ and $r \precsim t$, then for any $\widetilde{\Omega} \subseteq (\precsim^{\downarrow})^*$ and scheduler σ, there exists σ' such that $Prob_{\sigma',r}(C_{\widetilde{\Omega}_{st}}) \leq Prob_{\sigma,s}(C_{\widetilde{\Omega}_{st}})$. Since we also have $r \precsim^{\mathsf{b}} t$, so there exists σ'' such that $Prob_{\sigma'',t}(C_{\widetilde{\Omega}_{st}}) \leq Prob_{\sigma',r}(C_{\widetilde{\Omega}_{st}}) \leq Prob_{\sigma,s}(C_{\widetilde{\Omega}_{st}})$. This proves the transitivity of $\precsim$.

(2) In order to prove that $\precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} \subseteq \precsim$, it is enough to show that $\mathcal{R} = \{(s, r) \mid s \precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} r\}$ is a weak branching simulation i.e. we need to prove that for any $\widetilde{\Omega} \subseteq (\mathcal{R}^{\downarrow})^*$ and scheduler σ, there exists a scheduler σ' such that $Prob_{\sigma',r}(C_{\widetilde{\Omega}_{st}}) \leq Prob_{\sigma,s}(C_{\widetilde{\Omega}_{st}})$ provided that $s \mathcal{R} r$. By induction $C_{\widetilde{\Omega}_{st}}$ is $\mathcal{R}$ downward closed, thus there exists ψ such that $Sat(\psi) = C_{\widetilde{\Omega}_{st}}$. We prove by contradiction. Suppose that there does not exist σ' such that $Prob_{\sigma',r}(C_{\widetilde{\Omega}_{st}}) \leq Prob_{\sigma,s}(C_{\widetilde{\Omega}_{st}}) = q$, then $r \models \mathcal{P}_{>q}(\psi)$, but apparently $s \not\models \mathcal{P}_{>q}\psi$, which contradicts with the assumption that $s \precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} r$. Therefore there must exist a scheduler σ' such that $Prob_{\sigma',r}(C_{\widetilde{\Omega}_{st}}) \leq Prob_{\sigma,s}(C_{\widetilde{\Omega}_{st}})$.

The proof of $\precsim \subseteq \precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}}$ is by structural induction on the syntax of state formula φ and path formula ψ of safe $\mathsf{PCTL}^*_{\setminus \mathsf{X}}$, that is, we need to prove the following two results simultaneously.

(a) $r \models \varphi$ implies $s \models \varphi$ for any state formula φ provided that $s \precsim r$.

(b) $\omega_2 \models \psi$ implies that $\omega_1 \models \psi$ for any path formula ψ provided that $\omega_1 \precsim \omega_2$.

We only consider $\varphi = \mathcal{P}_{\geq q}(\psi)$ since the other cases are similar. Suppose that $r \models \varphi$, we need to prove that $s \models \varphi$. We prove by contradiction, and assume that $s \not\models \varphi$, then there exists σ such that $Prob_{\sigma,s}(\{\omega \mid \omega \models \psi\}) < q$. By induction $\{\omega \mid \omega \models \psi\}$ is $\precsim$ downward closed, thus there exists $\widetilde{\Omega}_{st}$ such that $\widetilde{\Omega}_{st} = \{\omega \mid \omega \models \psi\}$. Since $r \models \varphi$, there does not exist σ' such that $Prob_{\sigma,r}(\widetilde{\Omega}_{st}) \leq Prob_{\sigma,s}(\widetilde{\Omega}_{st}) = q$ which contradicts with the assumption that $s \precsim r$, thus $s \models \varphi$, and $s \precsim_{\mathsf{PCTL}^*_{\setminus \mathsf{X}}} r$.

□

6.4. **Simulation kernels and summary.** Let $\mathcal{R}^{-1}$ denote the reverse of $\mathcal{R}$, then $\mathcal{R}\cap\mathcal{R}^{-1}$ is the simulation kernel. In this section we will show the relation between the simulation kernels and their correspondent bisimulations. Not surprisingly, the simulation kernels are coarser than the bisimulations as shown in the following theorem.

Theorem 14. (1) $\sim_i^{\mathsf{b}} \subset (\prec_i^{\mathsf{b}} \cap (\prec_i^{\mathsf{b}})^{-1})$.
(2) $\sim_i \subset (\prec_i \cap \prec_i^{-1})$.
(3) $\approx^{\mathsf{b}} \subset (\precapprox^{\mathsf{b}} \cap (\precapprox^{\mathsf{b}})^{-1})$.
(4) $\approx \subset (\precapprox \cap \precapprox^{-1})$.

Proof. We only prove the first clause here, since the others are quite similar. The proof of $\sim_i^{\mathsf{b}} \subseteq \prec_i^{\mathsf{b}} \cap (\prec_i^{\mathsf{b}})^{-1}$ is trivial and omitted here. To show that $\prec_i^{\mathsf{b}} \cap (\prec_i^{\mathsf{b}})^{-1}$ is strictly coarser than $\sim_i^{\mathsf{b}}$, it is enough to give a counterexample. Suppose we have three states s_1, s_2, and s_3 such that $s_1 \prec_i^{\mathsf{b}} s_2 \prec_i^{\mathsf{b}} s_3$ but $s_3 \not\prec_i^{\mathsf{b}} s_2 \not\prec_i^{\mathsf{b}} s_1$. Let s and r be two states such that $L(s) = L(r)$. In addition s has three transitions: $s \to \mathcal{D}_{s_1}$, $s \to \mathcal{D}_{s_2}$, $s \to \mathcal{D}_{s_3}$, and r only has two transitions: $s \to \mathcal{D}_{s_1}$, $s \to \mathcal{D}_{s_3}$. Then it should be easy to check that $s \prec_i^{\mathsf{b}} r$ and $r \prec_i^{\mathsf{b}} s$, the only non-trivial case is when $s \to \mathcal{D}_{s_2}$. Since $s_2 \prec_i^{\mathsf{b}} s_3$, thus there exists $r \to \mathcal{D}_{s_3}$ such that $\mathcal{D}_{s_2} \sqsubseteq_{\prec_i^{\mathsf{b}}} \mathcal{D}_{s_3}$. But obviously $s \not\prec_i^{\mathsf{b}} r$, since the transition $s \to \mathcal{D}_{s_2}$ cannot be simulated by any transition of r. □

We summarize the preorders in strong and weak scenarios in Fig. 6 and 7 respectively, note we omit the subscript s denoting safe fragment for the logic preorders as before.

7. Countable states

Until now we have only considered PAs with finitely many states. In this section we will show that these results also apply for PAs with countable states. Assume S is a countable set of states S. We adopt the method used in [8] to deal with strong branching bisimulation since all the other cases are similar. First we recall some standard notations from topology theory. Given a metric space (S, d) where d is a metric, a sequence $\{s_i \mid i \geq 0\}$ converges to s iff for any $\epsilon > 0$, there exists n such that $d(s_m, s) < \epsilon$ for any $m \geq n$. A metric space (S, d) is compact if every infinite sequence has a convergent subsequence to an element in S. Refer to [8] for more details.

Below follows the definition of metric over distributions from [8].

Definition 19. Given two distributions $\mu, \nu \in Dist(S)$, the metric d is defined by $d(\mu, \nu) = Sup_{C\subseteq S}|\mu(C) - \nu(C)|$.

Since the metric is defined over distributions while in Definition 9 we did not consider distributions explicitly, thus we need to adapt the definition of $Prob_{\sigma,s}(C, C', n)$ in the following way: $s \stackrel{n,C}{\Longrightarrow} \mu$ iff either i) $\mu = \mathcal{D}_s$, or ii) $s \to \nu$ such that

$$\sum_{\forall r\in Supp(\nu).r \stackrel{n-1,C}{\Longrightarrow} \nu_r} \nu(r) \cdot \nu_r = \mu.p$$

It is obvious that for each σ, C, C', and n, there exists $s \stackrel{n,C}{\Longrightarrow} \mu$ such that $\mu(C') = Prob_{\sigma,s}(C, C', n)$.

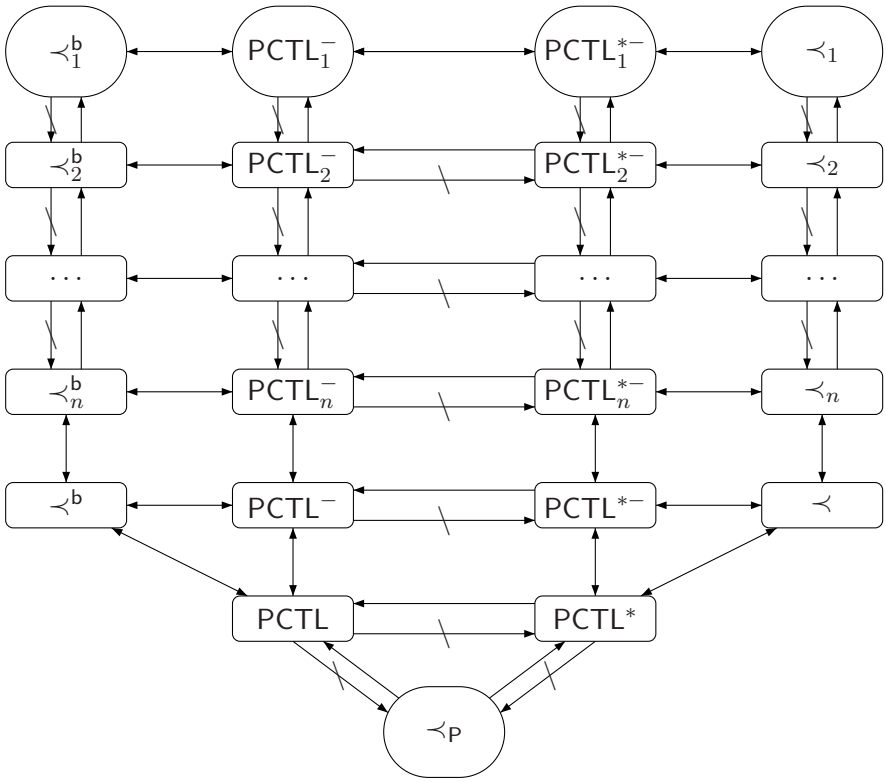

Figure 6: Relationship of different preorders in strong scenario.

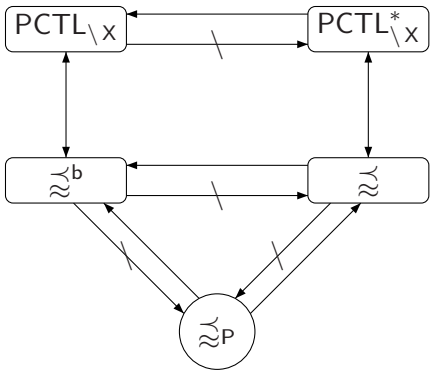

Figure 7: Relationship of different preorders in weak scenario.

Now we can define the compactness of probabilistic automata as in [8] with a slight difference.

Definition 20. Given a probabilistic automaton $\mathcal{P}$, $\mathcal{P}$ is i-compact iff the metric space $(\{\mu \mid s \stackrel{i,C}{\Longrightarrow} \mu\}, d)$ is compact for each $s \in S$ and $\sim_i^{\mathsf{b}}$ closed set C.

As mentioned in [8, 22], the convex closure does not change the compactness, thus we can extend $\stackrel{n,C}{\Longrightarrow}$ to allow combined transitions in a standard way without changing anything,

but for simplicity we omit this. A probabilistic automaton is *compact* iff it is i-compact for any $i \geq 1$.

We introduce the definition of *capacity* as follows.

Definition 21. Given a set of states S and a σ-algebra $\mathcal{B}$, a capacity on $\mathcal{B}$ is a function $Cap : \mathcal{B} \to (R^+ \cup \{0\})$ such that[2]:

(1) $Cap(\emptyset) = 0$,
(2) whenever $C_1 \subseteq C_2$ with $C_1, C_2 \in \mathcal{B}$, then $Cap(C_1) \leq Cap(C_2)$,
(3) whenever there exists $C_1 \subseteq C_2 \subseteq \ldots$ such that $\cup_{i\geq 1} C_i = C$, or $C_1 \supseteq C_2 \supseteq \ldots$ such that $\cap_{i\geq 1} C_i = C$, then $\lim_{i\to\infty} Cap(C_i) = Cap(C)$.

A capacity Cap is *sub-additive* iff $Cap(C_1 \cup C_2) \leq Cap(C_1) + Cap(C_2)$ for any $C_1, C_2 \in \mathcal{B}$.

Different from [8], the value of $Prob_{\sigma,s}(C, C', n)$ depends on both C and C'. Let $PreCap^C_{s,n}(C') = Sup_\sigma Prob_{\sigma,s}(C, C', n)$ and $PostCap^{C'}_{s,n}(C) = Sup_\sigma Prob_{\sigma,s}(C, C', n)$ i.e. given a C' $PreCap^C_{s,n}$ will return the maximum probability from s to C' in at most n steps via only states in C, similar for $PostCap^{C'}_{s,n}$. The following lemma shows that both $PreCap^C_{s,n}$ and $PostCap^{C'}_{s,n}$ are sub-additive capacities.

Lemma 7. $PreCap^C_{s,n}$ and $PostCap^{C'}_{s,n}$ are sub-additive capacities on $\mathcal{B}$ where $\mathcal{B}$ is the σ-algebra only containing $\sim^{\mathsf{b}}_i$ closed sets.

Proof. Refer to the proof of Lemma 5.2 in [8]. □

Now we can show that the following results are still valid as long as the given probabilistic automaton is compact even when it contains infinitely countable states.

Theorem 15. Given a compact probabilistic automata,

(1) $\sim^{\mathsf{b}}_n = \sim_{\mathsf{PCTL}^-_n}$,
(2) there exists $n \geq 0$ such that $\sim^{\mathsf{b}}_n = \sim_{\mathsf{PCTL}}$.

Proof. (1) The proof of $\sim^{\mathsf{b}}_n \subseteq \sim_{\mathsf{PCTL}^-_n}$ is similar with the proof of Theorem 3, and is omitted here. We prove that $\sim_{\mathsf{PCTL}^-_n} \subseteq \sim^{\mathsf{b}}_n$ in the sequel following the proof of Theorem 6.10 in [8]. Let $\mathcal{R} = \{(s, r) \mid s \sim_{\mathsf{PCTL}^-_n} r\}$, we need to prove that $\mathcal{R}$ is a strong i-depth branching bisimulation. In order to do so, we need to prove that for any $(s, r) \in \mathcal{R}$, $PreCap^C_{s,n}(C') = PreCap^C_{r,n}(C')$ for each $\mathcal{R}$ closed sets C and C'. Since both C and C' may be countable union of equivalence classes while each equivalence class can only be characterized by countable many formulas, therefore we have $C = \cup^\infty_{i=1}(\cap^\infty_{j=1} C_{i,j})$ and $C' = \cup^\infty_{i=1}(\cap^\infty_{j=1} C'_{i,j})$ where $\cap^\infty_{j=1} C_{i,j}$ corresponds the i-th equivalence class in C, and $C_{i,j}$ corresponds the set of states determining by the j-th formula satisfied by i-th equivalence class, similar for $\cap^\infty_{j=1} C'_{i,j}$ and $C'_{i,j}$. Similar as [8], let $B_k = \cap^\infty_{j=1}(\cup^k_{i=1} C_{i,j})$, $A^l_k = \cap^l_{j=1}(\cup^k_{i=1} C_{i,j})$, and $B'_k = \cap^\infty_{j=1}(\cup^k_{i=1} C'_{i,j})$, $A'^l_k = \cap^l_{j=1}(\cup^k_{i=1} C'_{i,j})$. It is easy to see that B_k and B'_k are increasing sequences of $\mathcal{R}$ closed sets such that $\cup^\infty_{k=1} B_k = C$, and $\cup^\infty_{k=1} B'_k = C'$, while A^l_k and A'^l_k are decreasing sequences of $\mathcal{R}$ closed sets such that $\cap^\infty_{l=1} A^l_k = B_k$ and $\cap^\infty_{l=1} A'^l_k = B'_k$. Both A^l_k and A'^l_k only contain conjunction and disjunction of finite formulas, thus can be described by PCTL^-_i. The following proof is straightforward due to $s \sim_{\mathsf{PCTL}^-_i} r$ and Lemma 7.

[2] R^+ is the set of positive real numbers.

(2) Suppose that $\sim_{\mathsf{PCTL}} \subset \sim_n^{\mathsf{b}}$ for any $n \geq 0$ which means that there exists s and r such that $s \sim_n^{\mathsf{b}} r$ for any $n \geq 0$, but $s \not\sim_{\mathsf{PCTL}} r$. As a result there exists C, C' and σ such that $\lim_{i\to\infty} Prob_{\sigma,s}(C, C', i) > 0$, but there does not exist σ' such that $\lim_{i\to\infty} Prob_{\sigma',r}(C, C', i) \geq \lim_{i\to\infty} Prob_{\sigma,s}(C, C', i)$. In the other word, $\lim_{i\to\infty} Prob_{\sigma',r}(C, C', i) < \lim_{i\to\infty} Prob_{\sigma,s}(C, C', i)$ for any σ' which indicates that there exists $n \geq 0$ such that $Prob_{\sigma',r}(C, C', n) < Prob_{\sigma,s}(C, C', n)$ for any σ', therefore $s \not\sim_{\mathsf{PCTL}_i^-} r$ which contradicts with our assumption.

□

In a similar way we can extend the results of this section to strong bisimulations and weak bisimulations, we skip their proofs here. For the simulations, we need to do more work, since there may be uncountable many downward closed sets. We prove along the line of [14]. The following lemma is similar as Lemma 5.1 in [14] with only slight differences: i) we consider downward closed sets instead of upward closed sets, ii) we do not require $\mathcal{R}$ to be a preorder, but these do not change the proof.

Lemma 8 (Lemma 5.1 [14])**.** Let $\mathcal{R} \subseteq S \times S$ be a relation, and $C \subseteq S$ be a $\mathcal{R}$ downward closed set, then C is a union of equivalence classes of $\equiv_{\mathcal{R}}$ where $\equiv_{\mathcal{R}}$ is the largest equivalence relation contained in $\mathcal{R}$.

Given a $\mathcal{R}$ downward closed set C, we say C is *finitely generated* if there exists a finite set of equivalence classes of $\{C_i \in S/\equiv_{\mathcal{R}}\}_{i\in I}$ such that $C = \cup_{i\in I} C_i$. Since the set of the equivalence classes in $S/\equiv_{\mathcal{R}}$ is countable, thus the set of finitely generated $\mathcal{R}$ downward closed set is also countable [14]. The following lemma shows an alternative definition of $\prec_i^{\mathsf{b}}$ in Definition 14 where we only focus on finitely generated downward closed sets:

Lemma 9. A relation $\mathcal{R} \subseteq S \times S$ is a strong i-depth branching simulation with $i \geq 1$ iff $s\ \mathcal{R}\ r$ implies that $s \prec_{i-1}^{\mathsf{b}} r$ and for any finitely generated $\mathcal{R}$ downward closed sets C, C', and any scheduler σ, there exists σ' such that $Prob_{\sigma',r}(C, C', i) \geq Prob_{\sigma,s}(C, C', i)$.

We write $s \prec_i^{\mathsf{b}} r$ whenever there is a strong i-depth branching simulation $\mathcal{R}$ such that $s\ \mathcal{R}\ r$.

Proof. The proof is similar as the proof of Lemma 5.2 in [14]. Let $(\prec_i^{\mathsf{b}})'$ denote the new definition, we need to prove that $s \prec_i^{\mathsf{b}} r$ iff $s\ (\prec_i^{\mathsf{b}})'\ r$. Since finitely generated $\mathcal{R}$ downward closed sets are special cases of $\mathcal{R}$ downward closed sets, it is trivial to see that $s \prec_i^{\mathsf{b}} r$ implies $s\ (\prec_i^{\mathsf{b}})'\ r$. We prove that $s\ (\prec_i^{\mathsf{b}})'\ r$ implies $s \prec_i^{\mathsf{b}} r$ by contradiction. Suppose that for any finitely generated $\mathcal{R}$ downward closed sets C, C' and σ, there exists σ' such that $Prob_{\sigma',r}(C, C', i) \geq Prob_{\sigma,s}(C, C', i)$, but there exists $\mathcal{R}$ downward closed sets C, C' and σ such that $Prob_{\sigma',r}(C, C', i) < Prob_{\sigma,s}(C, C', i)$ for any σ'. Let σ be a scheduler such that $Prob_{\sigma',r}(C, C', i) < Prob_{\sigma,s}(C, C', i)$ for any σ' and $\epsilon = Prob_{\sigma,s}(C, C', i) - Prob_{\sigma',r}(C, C', i) > 0$. According to Lemma 8, there exists sets of equivalences classes: $\{C_j \in S/\equiv_{\mathcal{R}}\}_{j\in J}$ and $\{C_k \in S/\equiv_{\mathcal{R}}\}_{k\in K}$ such that $C = \cup_{j\in J} C_i$ and $C' = \cup_{k\in K} C_k$ where J, K are (infinite) sets of indexes. Define two sequences of finitely generated $\mathcal{R}$ downward closed sets:

$$\{C_{\leq j} = \cup_{j'\in J\wedge j'\leq j} \mid j \in J\},$$
$$\{C_{\leq k} = \cup_{k'\in K\wedge k'\leq k} \mid k \in K\}.$$

Obviously both $Prob_{\sigma,s}(C, C_{\leq k}, i)$ and $Prob_{\sigma,s}(C_{\leq j}, C', i)$ are monotone, non-decreasing and converge to $Prob_{\sigma,s}(C, C', i)$ for any C and C'. Therefore there exists $j \in J$ and $k \in K$ such that

$$Prob_{\sigma,s}(C_{\leq j}, C', i) > Prob_{\sigma,s}(C, C', i) - \frac{\epsilon}{4}, \text{ and}$$

$$Prob_{\sigma,s}(C_{\leq j}, C_{\leq k}, i) > Prob_{\sigma,s}(C_{\leq j}, C', i) - \frac{\epsilon}{4}.$$

This implies

$$Prob_{\sigma,s}(C_{\leq j}, C_{\leq k}, i) > Prob_{\sigma,s}(C, C', i) - \frac{\epsilon}{2}$$
$$= Prob_{\sigma',r}(C, C', i) + \frac{\epsilon}{2} > Prob_{\sigma',r}(C, C', i) \geq Prob_{\sigma,s}(C_{\leq j}, C_{\leq k}, i),$$

which contradicts with the assumption. □

By Lemma 9 it is enough to consider all the finitely generated $\prec_i^{\mathsf{b}}$ downward closed sets in Definition 20 which is countable. The extension of Theorem 8 to the countable state space is then routine, and is omitted here. Moreover the definitions of other variants of simulations in Section 6 can be adopted to only consider finitely generated downward closed sets too, thus their logic characterizations can also be extended to countable states.

8. The coarsest congruent bisimulations and simulations

Before we have shown that $\sim_{\mathsf{P}}$ is congruent but cannot be characterized by $\sim_{\mathsf{PCTL}}$ completely since it is too fine. On the other hand, there exists $\sim_n^{\mathsf{b}}$ which can be characterized by $\sim_{\mathsf{PCTL}}$, but it is not congruent generally, this indicates that $\sim_{\mathsf{PCTL}}$ is essentially not congruent. Therefore a natural question one may ask is that what is the largest subset of $\sim_{\mathsf{PCTL}}$ which is congruent. The following theorem shows that $\sim_{\mathsf{P}}$ is such coarsest congruent relation in $\sim_{\mathsf{PCTL}}$ assuming that the given probabilistic automaton is compact.

Theorem 16. $\sim_{\mathsf{P}}$ is the coarsest congruent equivalence relation in $\sim_{\mathsf{PCTL}}$.

Proof. We prove by contradiction. Suppose that there exists $\sim_{\mathsf{P}} \subset \simeq \subset \sim_{\mathsf{PCTL}}$ such that $\simeq$ is congruent. Since $\sim_{\mathsf{P}} \subset \simeq$, there exists s and r such that $s \simeq r$ but $s \not\sim_{\mathsf{P}} r$. According to Definition 4 there exists $s \to \mu$ such that there does not exist $r \to_{\mathsf{P}} \nu$ with $\mu \sim_{\mathsf{P}} \nu$. The idea is to show that there always exists t such that $s \,||\, t \not\sim_{\mathsf{PCTL}} r \,||\, t$ in this case, then it is enough to give a formula φ such that $r \,||\, t \models \varphi$, but $s \,||\, t \not\models \varphi$.

Let $Supp(\mu) = \{s_1, s_2, \ldots\}$ and $\mu(s_i) = a_i$[3] with $i \geq 1$. Without losing of generality we assume that there exists $s \to \mu$ such that for any two (combined) transitions of r: $r \to_{\mathsf{P}} \nu_1$ and $r \to_{\mathsf{P}} \nu_2$, there does not exist $0 \leq w_1, w_2 \leq 1$ such that $w_1 + w_2 = 1$ and $\mu \sim_{\mathsf{P}} (w_1 \cdot \nu_1 + w_2 \cdot \nu_2)$ (every combined transition of r can be seen as a combined transition of two other combined transitions of r). Let $\nu_1(s_i) = b_i$ and $\nu_2(s_i) = c_i$ in the following, then there must exist $i \neq j \geq 1$ such that there does not exist $0 \leq w_1, w_2 \leq 1$ such that $w_1 \cdot b_i + w_2 \cdot c_i = a_i$ and $w_1 \cdot b_j + w_2 \cdot c_j = a_j$ with $w_1 + w_2 = 1$, otherwise we will have $\mu \sim_{\mathsf{P}} (w_1 \cdot \nu_1 + w_2 \cdot \nu_2)$ which contradicts with the assumption. There are nine possible cases in total depending on the relation between a_i, a_j and b_i, c_i, b_j, c_j. Most of the cases are trivial except when $a_i \in [b_i, c_i]$ and $a_j \in [c_j, b_j]$. [4] For instance if $a_i > b_i, c_i$, r will evolve into s_i with probability less than a_i which is not the case for s, thus $s \not\sim_{\mathsf{PCTL}} r$ which contradicts with the assumption. Considering the following inequations where ρ_1 and ρ_2 are two variables with values in $[0, 1]$:

$$a_i \cdot \rho_1 + a_j \cdot \rho_2 < b_i \cdot \rho_1 + b_j \cdot \rho_2, \tag{8.1}$$

$$a_i \cdot \rho_1 + a_j \cdot \rho_2 < c_i \cdot \rho_1 + c_j \cdot \rho_2 \tag{8.2}$$

[3]For simplicity we assume that $s_i (i \geq 1)$ belong to different equivalence classes.

[4]We assume here that $c_i \geq b_i$ and $b_j \geq c_j$

which can be transformed into the following forms:

$$(a_i - b_i) \cdot \rho_1 < (b_j - a_j) \cdot \rho_2, \tag{8.3}$$

$$(a_i - c_i) \cdot \rho_1 < (c_j - a_j) \cdot \rho_2. \tag{8.4}$$

Note that $(a_i - b_i)$, $(a_i - c_i)$, $(b_j - a_j)$, and $(c_j - a_j)$ cannot be 0 at the same time, so there always exists $0 \leq \rho_1, \rho_2 \leq 1$ such that $a_i \cdot \rho_1 + a_j \cdot \rho_2$ is either greater or smaller than both of $b_i \cdot \rho_1 + b_j \cdot \rho_2$ and $c_i \cdot \rho_1 + c_j \cdot \rho_2$. By simple calculation whenever $\rho_1 \in (\frac{b_j - a_j}{a_i - b_i} \cdot \rho_2, \frac{a_j - c_j}{c_i - a_i} \cdot \rho_2)$ (it is not possible for $\frac{b_j - a_j}{a_i - b_i} = \frac{a_j - c_j}{c_i - a_i}$, otherwise there exists $0 \leq w_1, w_2 \leq 1$ such that $w_1 \cdot b_i + w_2 \cdot c_i = a_i$ and $w_1 \cdot b_j + w_2 \cdot c_j = a_j$ with $w_1 + w_2 = 1$), then $a_i \cdot \rho_1 + a_j \cdot \rho_2$ is smaller than $b_i \cdot \rho_1 + b_j \cdot \rho_2$ and $c_i \cdot \rho_1 + c_j \cdot \rho_2$. Let t be a state such that it can only evolve into t_1 with probability ρ_1 and t_2 with probability ρ_2 where $\rho_1 + \rho_2 = 1$ and $\rho_1 \in (\frac{b_j - a_j}{a_i - b_i} \cdot \rho_2, \frac{a_j - c_j}{c_i - a_i} \cdot \rho_2)$, obviously such t always exists. Assume that all the states have distinct labels except for s and r, moreover let

$$\psi = ((L(s \,||\, t) \vee L(s_i \,||\, t) \vee (L(s_j \,||\, t))) \,\mathsf{U}^{\leq 2} (L(s_i \,||\, t_1) \vee L(s_j \,||\, t_2))),$$

it is not hard to see that the minimum probability of the paths of $s \,||\, t$ satisfying ψ is at most $a_i \cdot \rho_1 + a_j \cdot \rho_2$ i.e. when $s \,||\, t$ first performs the transition $s \to \mu$ of s and then performs the transition $t \to \{\rho_1 : t_1, \rho_2 : t_2\}$ of t. Let $r \to_{\mathsf{P}} \nu$ be the transition such that when $r \,||\, t$ first performs it and then performs $t \to \{\rho_1 : t_1, \rho_2 : t_2\}$, the probability of the paths of $r \,||\, t$ satisfying ψ is minimal. Since $\nu(s_i) \cdot \rho_1 + \nu(s_j) \cdot \rho_2 > a_i \cdot \rho_1 + a_j \cdot \rho_2$, we have $r \,||\, t \models \mathcal{P}_{\geq q}\psi$ but $s \,||\, t \not\models \mathcal{P}_{\geq q}\psi$ where $q = \nu(s_i) \cdot \rho_1 + \nu(s_j) \cdot \rho_2$. In other words $s \,||\, t \;\not\sim_{\mathsf{PCTL}}\; r \,||\, t$, as a result $s \,||\, t \;\not\simeq\; r \,||\, t$, so $\simeq$ is not congruent. When all the states do not have distinct labels, we can always construct formulas to distinguish them, since the probabilistic automaton is compact and these states are in different equivalence classes by assumption, the following proof is the same. This completes our proof. □

Theorem 16 can be extended to identify the coarsest congruent weak bisimulation in $\sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$, and the coarsest congruent strong and weak simulations in $\prec_{\mathsf{PCTL}}$ and $\precapprox_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$ respectively.

Theorem 17. (1) $\simeq_{\mathsf{P}}$ is the coarsest congruent equivalence relation in $\sim_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$,
(2) $\prec_{\mathsf{P}}$ is the coarsest congruent preorder in $\prec_{\mathsf{PCTL}}$,
(3) $\precapprox_{\mathsf{P}}$ is the coarsest congruent preorder in $\precapprox_{\mathsf{PCTL}_{\setminus \mathsf{X}}}$.

Proof. The proof is similar with the proof of Theorem 16 and we only sketch the proof of Clause (2) here. According to Lemma 5.2 in [14], $\mu \;\mathcal{R}\; \nu$ iff for each finitely generated $\mathcal{R}$ downward closed set C, $\mu(C) \leq \nu(C)$ where $\mathcal{R} \subseteq S \times S$ is a preorder. In order to prove that $\prec_{\mathsf{P}}$ is the coarsest congruent preorder in $\prec_{\mathsf{PCTL}}$, we need to show that for any $\preceq$ such that $\prec_{\mathsf{P}} \subset \preceq \subset \prec_{\mathsf{PCTL}}$, it holds that $\preceq$ is not congruent i.e. there exists s, r, and t such that $s \;\preceq\; r$, but $s \,||\, t \;\not\preceq\; r \,||\, t$. First assume that $\preceq$ is a congruence, and we then prove by contradiction as in Theorem 16 and show that if $s \;\preceq\; r$ and $s \;\not\prec_{\mathsf{P}}\; r$, there exists t such that $s \,||\, t \;\not\prec_{\mathsf{PCTL}}\; r \,||\, t$, thus $s \,||\, t \;\not\preceq\; r \,||\, t$ which contradicts with the assumption that $\preceq$ is a congruence. Since $s \;\not\prec_{\mathsf{P}}\; r$, then there exists $s \to \mu$ such that there does not exist $r \to_{\mathsf{P}} \nu$ with $\mu \;\sqsubseteq_{\prec_{\mathsf{P}}}\; \nu$. With the same argument as in Theorem 16 and Lemma 5.2 in [14], there exists t and ψ such that $r \,||\, t \models \mathcal{P}_{\geq q}\psi$ but $s \,||\, t \not\models \mathcal{P}_{\geq q}\psi$ i.e. $s \,||\, t \;\not\prec_{\mathsf{PCTL}}\; r \,||\, t$, thus $\preceq$ is not congruent. □

9. Related work

For Markov chains, i.e., deterministic probabilistic automata, the logic PCTL characterizes bisimulations, and PCTL without X operator characterizes weak bisimulations [10, 3]. As pointed out in [24], probabilistic bisimulation is sound, but not complete for PCTL for PAs. In the literature, various extensions of the Hennessy-Milner logic [12] are considered for characterizing bisimulations. Larsen and Skou [19] considered such an extension of Hennessy-Milner logic, which characterizes bisimulation for *alternating automaton* [19], or labeled Markov processes [8] (PAs but with continuous state space). For probabilistic automata, Jonsson *et al.* [17] considered a two-sorted logic in the Hennessy-Milner style to characterize strong bisimulations. In [14], the results are extended for characterizing also simulations.

Weak bisimulation was first defined in the context of PAs by Segala [24], and then formulated for alternating models by Philippou *et al.* [21]. The seemingly very related work is by Desharnais et al. [8], where it is shown that PCTL^* is sound and complete with respect to weak bisimulation for alternating automata. The key difference is that the model they have considered is not the same as probabilistic automata considered in this paper. Briefly, in alternating automata, states are either nondeterministic like in transition systems, or stochastic like in discrete-time Markov chains. As discussed in [25], a probabilistic automaton can be transformed to an alternating automaton by replacing each transition $s \to \mu$ by two consecutive transitions $s \to s'$ and $s' \to \mu$ where s' is the new inserted state. Surprisingly, for alternating automata, Desharnais et al. have shown that weak bisimulation – defined in the standard manner – characterizes PCTL^* formulae. The following example illustrates why it works in that setting, but fails for probabilistic automata.

Example 5. Refer to Fig. 1, we need to add three additional states s_{μ_1}, s_{μ_2}, and s_{μ_3} in order to transform s and r to alternating automata. The resulting automata are shown in Fig. 8. Suppose that s_1, s_2, and s_3 are three absorbing states with different atomic propositions, so they are not (weak) bisimilar, as a result s_{μ_1}, s_{μ_2} and s_{μ_3} are not (weak) bisimilar either since they can evolve into s_1, s_2, and s_3 with different probabilities. Therefore s and r are not (weak) bisimilar. Let $\varphi = \mathcal{P}_{\geq 0.4}(\mathsf{X}\, L(s_1)) \wedge \mathcal{P}_{\geq 0.3}(\mathsf{X}\, L(s_2)) \wedge \mathcal{P}_{\geq 0.3}(\mathsf{X}\, L(s_3))$, it is not hard to see that $s_{\mu_2} \models \varphi$ but $s_{\mu_1}, s_{\mu_3} \not\models \varphi$, so $s \models \mathcal{P}_{\leq 0}(\mathsf{X}\, \varphi)$ while $r \not\models \mathcal{P}_{\leq 0}(\mathsf{X}\, \varphi)$. When working in the setting of probabilistic automata, s_{μ_1}, s_{μ_2}, and s_{μ_3} will not be considered as states, so we cannot use the above arguments for alternating automata anymore.

In the definition of $\sim_1$ and $\prec_1$, we choose first the downward closed set C before the successor distribution to be matched, which is the key for achieving our new notion of bisimulations and simulations. This approach was also adopted in [9] to define the priori ϵ-bisimulation and simulation. It turns out that when $\epsilon = 0$, the priori ϵ-bisimulation coincides with $\sim_1$. The priori ϵ-bisimulation was shown to be sound and complete w.r.t. an extension of Hennessy-Milner logic, similarly for the priori ϵ-simulation. Finally, the priori ϵ-bisimulation was also used to define pseudo-metric between PAs in [9, 7]. The definition of priori 0-simulation in [9], denoted as $\prec_1'$, is however not equivalent to $\prec_1$. In the definition of $\prec_1'$, the upward closed sets are considered while in the definition of $\prec_1$ we consider downward closed sets. If we adopt the definition of $\prec_1'$ here, Theorem 8 will not be valid anymore. Refer to the following example.

Example 6. Consider the two states s_0 and r_0 in Fig. 9 where all the states have different labels except that $L(s_0) = L(r_0)$, and the transitions of s_1 and s_2 are omitted. Moreover

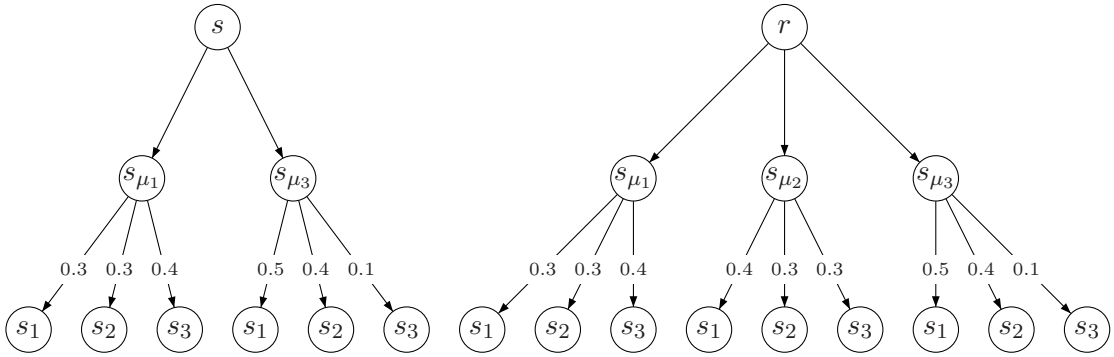

Figure 8: Alternating automata.

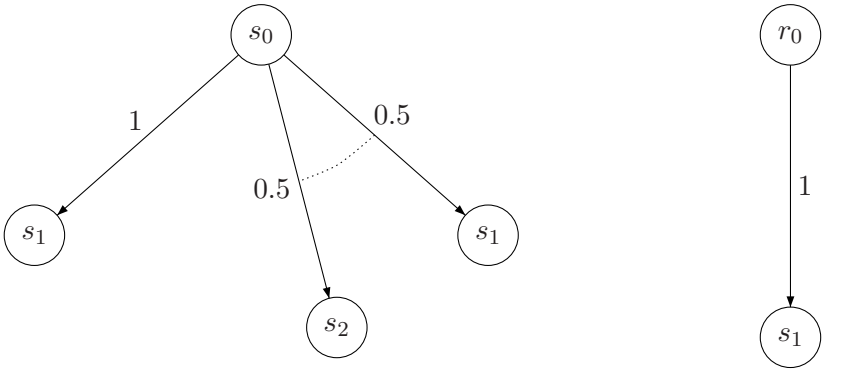

Figure 9: $\prec_i' \neq \prec_{\mathsf{PCTL}_1^-}$.

we assume that $s_2 \prec_1' s_1$, but $s_1 \not\prec_1' s_2$. Let $\mathcal{R} = \{(s_0, r_0), (s_1, s_1), (s_2, s_1)\}$, in order to show that $\mathcal{R}$ is a priori 0-simulation, we need to check that for each $\mathcal{R}$ upward closed set C and $s_0 \to \mu$, there exists $r_0 \to \nu$ such that $\mu(C) \leq \nu(C)$. The only non-trivial cases are when $C = \{s_1\}$ or $\{s_2, s_1\}$, thus $s_0 \prec_1' r_0$. But we will show that $s_0 \not\prec_{\mathsf{PCTL}_1^-} r_0$. By contradiction, assume that $\prec_1' = \prec_{\mathsf{PCTL}_1^-}$. Let $\varphi = \mathcal{P}_{\leq 0}(\mathsf{X}\,\varphi_{s_2})$ where φ_{s_2} is a formula such that $s_2 \models \varphi_{s_2}$ but $s_1 \not\models \varphi_{s_2}$. Since $s_1 \not\prec_1' s_2$, such formula always exists by assumption. It is easy to see that $r_0 \models \varphi$, but $s_0 \not\models \varphi$ since the maximal probability from s_0 to s_2 in one step is equal to 0.5, thus we get contradiction, and $\prec_1' \neq \prec_{\mathsf{PCTL}_1^-}$.

10. Conclusion and future work

In this paper we have introduced novel notions of bisimulations for probabilistic automata. They are coarser than the existing bisimulations, and most importantly, we show that they agree with logical equivalences induced by PCTL^* and its sublogics. Even though we in this paper have not considered actions, it is worth noting that actions can be easily added, and all the results relating (weak) bisimulations hold straightforwardly. On the other side,

the (weak) bisimulations are then strictly finer than the logical equivalences, because of the presence of these actions, similarly for simulations.

As future work, we plan to study decision algorithms for our new (strong and weak) bisimulation and simulation relations.

Acknowledgement

The authors are supported by IDEA4CPS and the VKR Center of Excellence MT-LAB. We thank Johann Schuster for detailed comments on an early version of this draft.

References

[1] C. Baier, B. Engelen, and M. E. Majster-Cederbaum. Deciding bisimilarity and similarity for probabilistic processes. *J. Comput. Syst. Sci.*, 60(1):187–231, 2000.

[2] C. Baier and J.-P. Katoen. *Principles of model checking*. MIT Press, 2008.

[3] C. Baier, J.-P. Katoen, H. Hermanns, and V. Wolf. Comparative branching-time semantics for markov chains. *Inf. Comput.*, 200(2):149–214, 2005.

[4] A. Bianco and L. De Alfaro. Model checking of probabilistic and nondeterministic systems. In *FSTTCS*, pages 499–513. Springer, 1995.

[5] H. Boudali, P. Crouzen, and M. Stoelinga. A rigorous, compositional, and extensible framework for dynamic fault tree analysis. *IEEE Transactions on Dependable and Secure Computing*, 99(1), 2009.

[6] S. Cattani and R. Segala. Decision algorithms for probabilistic bisimulation. In *CONCUR*, pages 371–385, 2002.

[7] L. de Alfaro, R. Majumdar, V. Raman, and M. Stoelinga. Game relations and metrics. In *LICS*, pages 99–108, 2007.

[8] J. Desharnais, V. Gupta, R. Jagadeesan, and P. Panangaden. Weak bisimulation is sound and complete for pctl*. *Inf. Comput.*, 208(2):203–219, 2010.

[9] J. Desharnais, M. Tracol, and A. Zhioua. Computing distances between probabilistic automata. In *QAPL*, pages 148–162, 2011.

[10] H. Hansson and B. Jonsson. A Calculus for Communicating Systems with Time and Probabitilies. In *IEEE Real-Time Systems Symposium*, pages 278–287, 1990.

[11] H. Hansson and B. Jonsson. A logic for reasoning about time and reliability. *Formal aspects of computing*, 6(5):512–535, 1994.

[12] M. Hennessy and R. Milner. Algebraic Laws for Nondeterminism and Concurrency. *J. ACM*, 32(1):137–161, 1985.

[13] M. R. Henzinger, T. A. Henzinger, and P. W. Kopke. Computing simulations on finite and infinite graphs. In *Proceedings of the 36th Annual Symposium on Foundations of Computer Science*, FOCS '95, pages 453–462, Washington, DC, USA, 1995. IEEE Computer Society.

[14] H. Hermanns, A. Parma, R. Segala, B. Wachter, and L. Zhang. Probabilistic logical characterization. *Inf. Comput.*, 209(2):154–172, 2011.

[15] B. Jonsson. Simulations between specifications of distributed systems. In *Proceedings of the 2nd International Conference on Concurrency Theory*, CONCUR '91, pages 346–360, London, UK, 1991. Springer-Verlag.

[16] B. Jonsson and K. Larsen. Specification and refinement of probabilistic processes. In *LICS*, pages 266–277, 1991.

[17] B. Jonsson, K. Larsen, and Y. Wang. Probabilistic extensions of process algebras. In J. Bergstra, A. Ponse, and S. Smolka, editors, *Handbook of Process Algebra*, pages 685–710. Elsevier, 2001.

[18] J.-P. Katoen, T. Kemna, I. S. Zapreev, and D. N. Jansen. Bisimulation minimisation mostly speeds up probabilistic model checking. In *TACAS*, pages 87–101, 2007.

[19] K. Larsen and A. Skou. Bisimulation through probabilistic testing. *Inf. Comput.*, 94(1):1–28, 1991.

[20] R. Milner. *Communication and concurrency*. Prentice Hall International Series in Computer Science, 1989.

[21] A. Philippou, I. Lee, and O. Sokolsky. Weak Bisimulation for Probabilistic Systems. In *CONCUR*, pages 334–349, 2000.
[22] H. Schaefer, M. Wolff, and M. Wolff. *Topological vector spaces*, volume 3. Springer Verlag, 1999.
[23] R. Segala. *Modeling and Verification of Randomized Distributed Realtime Systems*. PhD thesis, MIT, 1995.
[24] R. Segala and N. A. Lynch. Probabilistic Simulations for Probabilistic Processes. *Nord. J. Comput.*, 2(2):250–273, 1995.
[25] R. Segala and A. Turrini. Comparative analysis of bisimulation relations on alternating and non-alternating probabilistic models. In *QEST*, pages 44–53, 2005.
[26] L. Song, L. Zhang, and J. Godskesen. Bisimulations meet pctl equivalences for probabilistic automata. In *CONCUR*, pages 108–123, 2011.
[27] R. van Glabbeek and W. Weijland. Branching time and abstraction in bisimulation semantics. *Journal of the ACM (JACM)*, 43(3):555–600, 1996.