Logical Characterizations of Bisimulations for Discrete Probabilistic Systems*

Augusto Parma and Roberto Segala

Dipartimento di Informatica - Università di Verona

Abstract. We give logical characterizations of bisimulation relations for the probabilistic automata of Segala in terms of three Hennessy-Milner style logics. The three logics characterize strong, strong probabilistic and weak probabilistic bisimulation, and differ only for the kind of diamond operator used. Compared to the Larsen and Skou logic for reactive systems, these logics introduce a new operator that measures the probability of the set of states that satisfy a formula. Moreover, the satisfaction relation is defined on measures rather than single states.
We rederive previous results of Desharnais et. al. by defining sublogics for Reactive and Alternating Models viewed as restrictions of probabilistic automata. Finally, we identify restrictions on probabilistic automata, weaker than those imposed by the Alternating Models, that preserve the logical characterization of Desharnais et. al. These restrictions require that each state either enables several ordinary transitions or enables a single probabilistic transition.

1 Introduction

In concurrency, tools like process algebras, axiomatizations and logical characterizations are useful to study the properties of systems and the relations that exist between them in a very simple way. Bisimulation is a simple and useful relation that describes the operational equivalence of concurrent systems. Logical characterizations permit to understand what properties are preserved by bisimulation. In particular, two processes are bisimilar if and only if they satisfy the same formulas of the logic.

Concurrent system are also studied in the presence of randomization, and most of the results in the framework of labeled transition systems have been extended to the probabilistic nondeterministic setting. Probabilistic automata [14], also known as *non-alternating models*, are a conservative extension of labeled transition systems where a state may enable several probabilistic transitions with the same label, each one leading to a discrete probability measure over states. This model permits to describe processes where probability and nondeterminism interact together.

The goal of this paper is to study logical characterizations of bisimulations for probabilistic automata in the context of Hennessy-Milner style logics [8]. Logical

* Supported by INRIA project ProNoBiS and MIUR project AIDA.

characterizations have been studied already by Larsen and Skou [11] for reactive systems [6] and by Desharnais et. al. [5] for labeled concurrent Markov chains (*alternating model*) [7, 13]. These logics are derived from the Hennessy-Milner logic by replacing the diamond operator with a probabilistic diamond operator that measures bounds on the probability of performing an externally visible action and then satisfying some formula. Unfortunately, such characterizations are not adequate for probabilistic automata where, as opposed to reactive systems and alternating models, probability and nondeterminism coexist in the same states.

Our main contribution is a Hennessy-Milner logic that keeps the original diamond operator of [8], is defined on measures over states rather than on single states, and includes a new operator $[\phi]_p$ that is true whenever the probability of the states that satisfy a formula ϕ is at least p. Thus, a conjunction of formulas with such operator can characterize entire probability measures. We study three logics for strong, strong probabilistic and weak probabilistic bisimulation, respectively, each one differing only on the definition of the diamond operator to account for the kind of transitions that are used in the definition of the bisimulation relation.

We then view the logics studied for the reactive and alternating models as restrictions of our logic, where $\Diamond_p \phi$ can be encoded by $\Diamond a[\phi]_p$, and we rederive the known logical characterizations for such systems. In particular, for the alternating models we study minimal restrictions to impose on probabilistic automata so that the logical characterizations of [5] continue to hold. It turns out that it is sufficient to require that each state that enables a probabilistic transition enables only one transition. That is, each probabilistic choice should have a state that describes it. In this way, indeed, the characterization of bisimulation in terms of maximal probabilities [13, 5], which is the key technical machinery to derive the corresponding logical characterizations, continues to hold.

The paper is organized as follows. Section 2 gives some preliminary mathematical notions; Section 3 defines probabilistic automata and related concepts; Section 4, recalls the definition for Hennessy-Milner logic [8] and introduces our logics for probabilistic automata; Section 5 recalls the results for reactive and alternating systems and compares them with our results; Section 6 gives two logics for strong and weak probabilistic bisimulation for the restriction of probabilistic automata where states that enable probabilistic transitions enable only one transition, which embed all known alternating models; Section **??** gives some concluding remarks.

2 Mathematical Preliminaries

Given a set S, a *σ-algebra* over S is a family Σ of subsets of S that is closed under complementation and countable union. A *measurable space* is the pair (S, Σ), and each element of Σ is called a *measurable set*. The σ-algebra *generated* by a family G of subsets of S is the smallest σ-algebra including G, and is denoted by $\sigma(G)$. Given a measurable space (S, Σ), a *measure* over (S, Σ) is a function $\mu \colon \Sigma \to \Re^+$ such that, for every countable family $\{A_i\}_I \subseteq \Sigma$ of pairwise disjoint

measurable sets, $\mu(\cup_I A_i) = \sum_I \mu(A_i)$. A *(sub-)probability measure* is a measure $\mu\colon \Sigma \to [0,1]$ for which $(\mu(S) \leq 1)\ \mu(S) = 1$. Probability measures are ranged over by $\mu, \eta, \ldots$ and we propagate indices and primes where necessary. A set $A \subseteq S$ is called a *support* for a measure μ on Σ if $\mu(S - A) = 0$. Denote by $(SubDisc(S))$ $Disc(S)$ the set of discrete (sub-)probability measures over S and, given an element $s \in S$, denote by $\delta(s)$ the probability measure that assigns probability 1 to $\{s\}$. This is called the *Dirac measure* on s. Given a countable set of distributions $\{\mu_i\}_I$ and a set $\{p_i\}_I$ of real numbers in $[0,1]$ such that $\sum_I p_i = 1$, define the *convex combination* $\sum_I p_i\mu_i$ of $\{\mu_i\}_I$ as the probability measure μ such that, for each set X, $\mu(X) = \sum_I p_i\mu_i(X)$.

Sometimes it is necessary to lift a relation over sets to a relation over measures on sets. We give here a definition proposed in [14] using an idea of [9]. Let $\mathcal{R} \subseteq X \times Y$. The *lifting* of $\mathcal{R}$ is a new relation $\mathcal{L}(R) \subseteq Disc(X) \times Disc(Y)$, such that $\mu_1\ \mathcal{L}(\mathcal{R})\ \mu_2$ iff there exists a *weight function* (or *witness function*) $\omega\colon X \times Y \longrightarrow [0,1]$ such that the following *lifting conditions* hold:

1. $\forall (x,y) \in X \times Y$, if $\omega(x,y) > 0$ then $x\ \mathcal{R}\ y$;
2. $\forall x \in X, \sum_{y \in Y} \omega(x,y) = \mu_1(x)$;
3. $\forall y \in Y, \sum_{x \in X} \omega(x,y) = \mu_2(y)$.

If $\mathcal{R}$ is an equivalence relation, then for each pair of measures μ_1, μ_2, it can be shown that $\mu_1\ \mathcal{L}(R)\ \mu_2$ if and only if $\mu([t]) = \mu'([t])$ for each equivalence class $[t]$ of $\mathcal{R}$. In the following we will use $\mathcal{R}$ instead of $\mathcal{L}(\mathcal{R})$ if it is clear from the contest that we refer to a lifted relation. A set E is *$\mathcal{R}$-closed* if $E = \{s \mid \exists r \text{ s.t. } s\ \mathcal{R}\ r\}$, that is, it is a collection of equivalence classes of $\mathcal{R}$.

3 Probabilistic Automata

In this section we recall some concepts of ordinary automata theory that will be useful to understand the definitions of executions, traces, combined transitions, schedulers, weak combined transitions and bisimulation relations for probabilistic automata. All the definitions concerning ordinary automata are standard and the definition for probabilistic automata are taken from [14].

An *automaton* is a tuple $\mathcal{A} = (S, Act, \mathcal{D})$ where S is the set of *states*, Act is the set of *actions*, and $\mathcal{D} \subseteq S \times Act \times S$ is the *transition relation*. Each triple $(s,a,s') \in \mathcal{D}$ is called a *transition*, and is denoted by $s \xrightarrow{a} s'$. The set Act is partitioned into two sets E, H of *external* and *internal* actions, respectively. For the purpose of this paper we assume that $H = \{\tau\}$.

Probabilistic automata are conservative extensions of Labeled Transition Systems where transitions lead to discrete probability measures over states instead of single states. Indeed, an ordinary automaton can be seen as a probabilistic automaton where each transition leads to a Dirac measure. A *probabilistic automaton* is a tuple $\mathcal{P} = (S, Act, \mathcal{D})$, where S is the set of *states*, Act is the set of *actions*, and $\mathcal{D}$ is the *transition relation*, where $\mathcal{D} \subseteq S \times Act \times Disc(S)$. Denote a transition $(s,a,\mu) \in \mathcal{D}$ by $s \xrightarrow{a} \mu$. States and actions are ranged over by $s, r, t, \ldots$ and $a, b, \ldots$, respectively.

An *execution* of a probabilistic automaton $\mathcal{P}$ is a finite or infinite sequence $\alpha = s_0 a_1 s_1 a_2 s_2 \cdots$ of alternating states and actions, starting with a state and, if the sequence is finite, ending in a state, where for each i, there exists a measure μ such that $(s_i, a_{i+1}, \mu) \in \mathcal{D}$ and $\mu(s_{i+1}) > 0$. State s_0 is called the first state of α and is denoted by $\mathit{fstate}(\alpha)$. If α is a finite sequence, then the last state of α is denoted by $\mathit{lstate}(\alpha)$. Denote by $\mathit{execs}(\mathcal{P})$ the set of executions of $\mathcal{P}$ and by $\mathit{execs}^*(\mathcal{P})$ the set of finite executions of $\mathcal{P}$. Executions are the result of the resolution of both probabilistic and nondeterministic choices. If we resolve nondeterministic choices only, then we obtain a structure on which we can study probability measures over executions. Nondeterminism is resolved in a randomized way by an entity called scheduler.

A *scheduler* for a probabilistic automaton $\mathcal{P}$ is a function $\sigma\colon \mathit{execs}^*(\mathcal{P}) \to \mathit{SubDisc}(\mathcal{D})$ such that $\sigma(\alpha)(s, a, \mu) > 0$ implies $s = \mathit{lstate}(\alpha)$. A scheduler σ is *deterministic* if for each finite execution α, $\sigma(\alpha) \equiv 0$ or $\sigma(\alpha) = \delta(tr)$, with $tr \in \mathcal{D}$. A scheduler and a starting state $\overline{s}$ induce a probability measure over executions on a σ-field whose construction is standard. Specifically, we consider the σ-field generated by *cones*, where the cone of a finite execution α, denoted by C_α, is the set of executions that have α as a prefix, i.e., $C_\alpha = \{\alpha' \in \mathit{execs}(\mathcal{P}) \mid \alpha \leq \alpha'\}$. Fixed a starting state s_0, the measure of a cone C_α, where $\alpha = s_0 a_1 s_1 \cdots s_k$, is defined as follows:

$$\mu(C_\alpha) = \prod_{i \in \{0,k-1\}} \left(\sum_{(s_i, a_{i+1}, \mu') \in \mathcal{D}} \sigma(s_0 a_1 \cdots a_i s_i)(s_i, a_{i+1}, \mu') \mu'(s_{i+1}) \right).$$

Standard measure theoretical arguments ensure that the measure defined on cones extends uniquely to a measure defined on the generated σ-field.

Let $\{s \xrightarrow{a} \mu_i\}_{i \in I}$ be a collection of transitions of $\mathcal{P}$, and let $\{p_i\}_{i \in I}$ be a collection of probabilities such that $\sum_{i \in I} p_i = 1$. Then the triple $\{s, a, \sum_{i \in I} p_i \mu_i\}$ is called a *combined transition*. Combined transitions represent the result of choosing the transitions randomly from some state s. They are useful in the definition of probabilistic bisimulations.

We say that $s \stackrel{a}{\Longrightarrow} s'$ is a *weak transition* of an automaton $\mathcal{A}$ if there is a finite execution α of $\mathcal{A}$ with $\mathit{fstate}(\alpha) = s$ and $\mathit{lstate}(\alpha) = s'$, and such that $\mathit{trace}(\alpha) = \mathit{trace}(a)$, where the trace function restricts a sequence to external actions only. In other words, a weak transition is a way to abstract from internal computation. For probabilistic automata, consider a measure μ, induced by a scheduler σ from a starting state $\overline{s}$, that assigns probability 1 to the set of all finite executions with trace a. Let μ' be the measure defined by $\mu'(s) = \mu(\{\alpha \mid \mathit{lstate}(\alpha) = s\})$. Then $s \stackrel{a}{\Longrightarrow} \mu'$ is a *weak combined transition* of $\mathcal{P}$. The term "combined" reflects the fact that σ is a randomized scheduler.

We define three types of bisimulation relations that will be studied in the rest of this paper. These relations differ for the kind of transitions used.

1. An equivalence relation $\mathcal{R} \subseteq S \times S$ is a *strong bisimulation* if for each pair s, r of states such that $s \,\mathcal{R}\, r$ and for each transition $s \xrightarrow{a} \mu$, there exists μ' such that $r \xrightarrow{a} \mu'$ and $\mu \,\mathcal{R}\, \mu'$. Denote by $\sim$ the largest bisimulation.

2. An equivalence relation $\mathcal{R} \subseteq S \times S$ is a *strong probabilistic bisimulation* if for each pair s, r of states such that $s \mathcal{R} r$ and for each transition $s \xrightarrow{a} \mu$, there exists a combined transition $r \xrightarrow{a} \mu'$ such that $\mu \mathcal{R} \mu'$. Denote by $\sim^p$ the largest probabilistic bisimulation.
3. An equivalence relation $\mathcal{R} \subseteq S \times S$ is a *weak probabilistic bisimulation* if for each pair s, r of states such that $s \mathcal{R} r$ and for each transition $s \xrightarrow{a} \mu$, there exists a weak combined transition $r \stackrel{a}{\Longrightarrow} \mu'$ such that $\mu \mathcal{R} \mu'$. Denote by $\approx^p$ the largest weak probabilistic bisimulation.

There would be a fourth obvious relation that uses weak transitions induced by deterministic schedulers. However, this relation is not transitive, as shown in [3], and thus it is not interesting.

We recall an alternative way of defining bisimulation [8] as $\bigcap_{i \geq 0} \sim_n$, where $\sim_0 = S \times S$ (all states are related) and for each pair of states s, r, $s \sim_{n+1} r$ if for each action a, $s \xrightarrow{a} \mu$ implies that there exists μ' such that $r \xrightarrow{a} \mu'$ and $\mu \sim_n \mu'$. The same definition style applies to strong probabilistic and weak probabilistic bisimulation, as well.

4 Hennessy-Milner Logic for Probabilistic Automata

In this section, we give logical characterizations of bisimulations for probabilistic automata. We start by recalling the logic from [8]; then we analyze in detail the logics for strong, strong probabilistic and weak probabilistic bisimulations.

4.1 Hennessy-Milner Logic

The syntax of the Hennessy-Milner Logic [8] is the following:

$$\mathcal{L}^{hm} ::= \top \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \Diamond a\varphi.$$

The satisfaction relation $\models \subseteq S \times \mathcal{F}$ is defined by structural induction on the formulas of $\mathcal{L}^{hm}$ as follows:

- $s \models \top$ for each state s
- $s \models \neg\varphi$ iff $s \not\models \varphi$
- $s \models \varphi_1 \wedge \varphi_2$ iff $s \models \varphi_1$ and $s \models \varphi_2$
- $s \models \Diamond a\varphi$ iff there exists a transition $s \xrightarrow{a} s'$ and $s' \models \varphi$.

The only non-trivial operator is the "diamond" $\Diamond$, which is used to describe the existence of transitions. It was shown in [8] that the logic $\mathcal{L}^{hm}$ characterizes strong bisimulation for ordinary automata. In particular, two states s and r of an automaton are bisimilar if and only if they satisfy the same formulas of $\mathcal{L}^{hm}$. If we extend the logic above with a countably infinite conjunction, then the characterization of strong bisimulation holds also for automata with countably many states. In this paper we deal with countable state spaces, and therefore we use an infinitary conjunction operator. However, our results hold for finite conjunction operators and finite-state spaces.

The logics that we study in this paper share a lot of structure of $\mathcal{L}^{hm}$, thus, we introduce here some useful notation. We let $\varphi, \psi, \ldots$ range over formulas, and we define the *depth* of a formula φ as the maximum number of nested diamond operators that occur in φ. We let $\mathcal{F}_{\mathcal{L}}$ denote the set of the formulas of the logic $\mathcal{L}$, and let $\mathcal{F}_{\mathcal{L},n}$ denote set of the formulas of $\mathcal{L}$ of depth at most n. We define a new relation $\bowtie_{\mathcal{L}} \subseteq S \times S$ such that $s \bowtie_{\mathcal{L}} r$ if and only if $\mathcal{F}_{\mathcal{L}}(s) = \mathcal{F}_{\mathcal{L}}(r)$, and similarly we define $\bowtie_{\mathcal{L},n} \subseteq S \times S$ as the relation such that $s \bowtie_{\mathcal{L},n} r$ if and only if $\mathcal{F}_{\mathcal{L},n}(s) = \mathcal{F}_{\mathcal{L},n}(r)$. We drop the subscript $\mathcal{L}$ whenever it is clear from the contest. Finally, denote by $[\![\varphi]\!]$ the set of all the states that satisfy φ.

4.2 Hennessy-Milner Logic for Strong Bisimulation

The main difference between probabilistic automata and ordinary automata is that in probabilistic automata, the target of each transition is a probability measure. Thus, informally, our logic should be able to distinguish the properties of a set of states rather than single states. ¿From every state there might be several outgoing transitions labeled by the same action. Thus, a naive extension of $\Diamond$, where we study the probability of a formula in the target of a transition [11] does not suffice. Our proposal is to define a new operator that, together with conjunction, can characterize exactly a probability measure. The syntax of the logic $\mathcal{L}^N$ for strong bisimulation is the following:

$$\mathcal{L}^N ::= \top \mid \neg\varphi \mid \bigwedge_I \varphi_i \mid \Diamond a\varphi \mid [\varphi]_p.$$

The semantics of this logic is given in terms of probability measures over states rather than single states. Specifically, the satisfaction relation is defined as follows:

- $\mu \models \top$ for each measure μ
- $\mu \models \neg\varphi$ iff $\mu \not\models \varphi$
- $\mu \models \bigwedge_I \varphi_i$ iff for each $i \in I$, $\mu \models \varphi_i$
- $\mu \models \Diamond a\varphi$ iff for each $s \in \mathit{supp}(\mu)$ there exists a distribution η and a transition $s \xrightarrow{a} \eta$ such that $\eta \models \varphi$
- $\mu \models [\varphi]_p$ iff $\mu([\![\varphi]\!]) \geq p$.

The first three clauses are trivial extensions of those of the Hennessy-Milner logic. The diamond operator is exactly that of $\mathcal{L}^{hm}$ if we restrict our study to Dirac distributions, and the operator $[\cdot]_p$ expresses the probability of a set of states with respect to a given probability measure.

The rest of this section is dedicated to the proofs of soundness and completeness of $\mathcal{L}^N$. We start with a few preliminary lemmas that are used to prove the soundness and completeness of $\mathcal{L}^N$. This first lemma states that, when considering logics with negation, if two states satisfy two different sets of formulas, then none of these sets is contained in the other.

Lemma 1. *Given a logic with negation, for each pair of states s and r of a probabilistic automaton, if $\mathcal{F}(s) \neq \mathcal{F}(r)$ then $\mathcal{F}(s) \not\subseteq \mathcal{F}(r)$.*

The second lemma shows that the states of a probabilistic automaton satisfy the same sets of formulas of depth zero.

Lemma 2. *For each pair of states s, r, $\mathcal{F}_0(s) = \mathcal{F}_0(r)$.*

The third lemma relates diamond formulas with probability measures and the states in their support.

Lemma 3. *For each measure μ, such that $\mu \models \Diamond a\varphi$, $\mu \models \varphi$ iff for each $s \in supp(\mu)$, $s \models \varphi$.*

The last lemma states that the lifting of $\bowtie_n$ preserves the sets of formulas satisfied by two probability distributions μ and μ'.

Lemma 4. *Let $\mathcal{R}$ be a subset of $\bowtie_n$. Then, for each pair of distributions μ, μ', $\mu \mathcal{R} \mu'$ implies $\mathcal{F}_n(\mu) = \mathcal{F}_n(\mu')$.*

We are now ready to prove the soundness and completeness of the logic $\mathcal{L}^N$ for probabilistic automata.

Theorem 1. *Given the logic $\mathcal{L}^N$, for each pair of states s, r of a probabilistic automaton, $s \sim r$ iff $\mathcal{F}(s) = \mathcal{F}(r)$.*

Proof. By induction on n, we show that $s \sim_n r$ iff $\mathcal{F}_n(s) = \mathcal{F}_n(r)$ for each $n \geq 0$. The base case follows trivially by Lemma 2 and the definition of $\sim_0$ (all states are related). For the inductive step we prove separately the two directions of our claim.

($\Longrightarrow$). Let $s \sim_{n+1} r$. We show by induction on the structure of a formula $\varphi \in \mathcal{F}_{n+1}$ that $s \models \varphi$ iff $r \models \varphi$. Let $s \models \varphi$ (the case for $r \models \varphi$ is symmetric). If $\varphi = \top$, then $r \models \varphi$ trivially. If $\varphi = \neg\psi$, then $s \not\models \psi$ and by structural induction, $r \not\models \psi$. Thus, $r \models \neg\psi$. If $\varphi = \bigwedge_I \psi_i$, then for each $i \in I$, $s \models \psi_i$. By structural induction, $r \models \psi_i$ for each $i \in I$ and thus, $r \models \varphi$. If $\varphi = [\psi]_p$, then either $p = 0$ or $s \models \psi$. In the first case $r \models \varphi$ trivially; in the second case, by structural induction, $r \models \psi$ and thus, $r \models \varphi$. If $\varphi = \Diamond a\psi$, then $\psi \in \mathcal{F}_n$. By definition, there exists a transition $s \xrightarrow{a} \mu$ such that $\mu \models \psi$. Since $s \sim_{n+1} r$, there exists a distribution μ' and a transition $r \xrightarrow{a} \mu'$ such that $\mu \sim_n \mu'$. By induction on n, $\sim_n \subseteq \bowtie_n$. Thus, by Lemma 4 and since $\mu \sim_n \mu'$, $\mathcal{F}_n(\mu) = \mathcal{F}_n(\mu')$. Since $\psi \in \mathcal{F}_n$, and since $\mu \models \psi$, then also $\mu' \models \psi$. That is, $r \models \Diamond a\psi$.

($\Longleftarrow$). We show that $s \not\sim_{n+1} r$ implies $\mathcal{F}_{n+1}(s) \neq \mathcal{F}_{n+1}(r)$. Let $\{[t_i]_n\}_I$ be an enumeration of the equivalence classes of $\sim_n$. By induction on n and by Lemma 1, for each $i, j \in I$, if $i \neq j$, there exists a formula $\varphi_{ij} \in \mathcal{F}_n$ such that $t_i \models \varphi_{ij}$ and $t_j \not\models \varphi_{ij}$. For each $i \in I$, define $\varphi_i = \bigwedge_{j \in I \setminus \{i\}} \varphi_{ij}$. Then φ_i is satisfied only by the states of $[t_i]_n$. Let $s \not\sim_{n+1} r$ and suppose, for the sake of contradiction, that $\mathcal{F}_{n+1}(s) = \mathcal{F}_{n+1}(r)$. Without loss of generality, there exists a transition $s \xrightarrow{a} \mu$ such that there is no transition $r \xrightarrow{a} \mu'$ with $\mu \sim_n \mu'$. For each $i \in I$ let $p_i = \mu([t_i]_n)$. Now, define $\varphi = \bigwedge_I [\varphi_i]_{p_i}$. By definition, $\mu \models \varphi$. Furthermore, $\varphi \in \mathcal{F}_n$. By the semantics of $\Diamond$, $s \models \Diamond a\varphi$. Since $\Diamond a\varphi \in \mathcal{F}_{n+1}$, by hypothesis, $r \models \Diamond a\varphi$ as well. Thus, there exists a distribution μ'' such that $r \xrightarrow{a} \mu''$ and $\mu'' \models \varphi$. This means that for each $i \in I$, $\mu''([t_i]_n) \geq p_i$. Since $\sum_I p_i = 1$ and since $\sum_I \mu''([t_i]_n) = 1$, then for each $i \in I$, $\mu''([t_i]_n) = p_i$. That is, for each $i \in I$, $\mu([t_i]_n) = \mu''([t_i]_n)$, which means that $\mu \sim_n \mu''$, a contradiction.

4.3 Hennessy-Milner Logic for Strong Probabilistic Bisimulation

In the definition of probabilistic bisimulation, a transition can be matched by combining transitions. Thus, it is reasonable to believe that the diamond for strong probabilistic bisimulation should take into account this possibility. Indeed, the logic $\mathcal{L}_p^N$ for strong probabilistic bisimulation is obtained by replacing the operator $\Diamond$ with $\Diamond\!\!\!\!-$. The syntax of $\mathcal{L}_p^N$ is:

$$\mathcal{L}_p^N ::= \top \mid \neg\varphi \mid \bigwedge_I \varphi_i \mid \Diamond\!\!\!\!-a\varphi \mid [\varphi]_p.$$

The semantics of the operator $\Diamond\!\!\!\!-$ is:

- $\mu \models \Diamond\!\!\!\!-a\varphi$ iff for each $s \in supp(\mu)$ there exists a distribution η and a *combined transition* $s \xrightarrow{a} \eta$ such that $\eta \models \varphi$.

Since, as shown in [16], $\sim^p$ is weaker than $\sim$, adding the operator $\Diamond\!\!\!\!-$ to $\mathcal{L}^N$ does not change its expressivity. Hence, the operator $\Diamond\!\!\!\!-$ is weaker than $\Diamond$. Soundness and completeness of $\mathcal{L}_p^N$ are stated by the following theorem.

Theorem 2. *Given the logic $\mathcal{L}_p^N$, for each pair of states s, r of a probabilistic automaton, $s \sim^p r$ iff $\mathcal{F}(s) = \mathcal{F}(r)$.*

Proof outline. Lemma 1, 2, 3 and 4 hold also here. Then, the proof of this theorem follows the lines of that of Theorem 1, by replacing strong transitions with combined transitions in the appropriate places. □

4.4 Logic for Weak Probabilistic Bisimulation

The definition of the logic $\mathcal{L}_w^N$ follows the same ideas of $\mathcal{L}_p^N$. We replace the $\Diamond$ of $\mathcal{L}^N$ with operator $\Diamond\!\!\!\!-^w$, and the new syntax is:

$$\mathcal{L}_w^N ::= \top \mid \neg\varphi \mid \bigwedge_I \varphi_i \mid \Diamond\!\!\!\!-^w a\varphi \mid [\varphi]_p.$$

The semantics of $\Diamond\!\!\!\!-^w$ is:

- $\mu \models \Diamond\!\!\!\!-^w a\varphi$ iff for each $s \in supp(\mu)$ there exists a distribution η and a *weak combined transition* $s \stackrel{a}{\Longrightarrow} \eta$ such that $\eta \models \varphi$.

By the preceding considerations, we can easily infer that the operator $\Diamond\!\!\!\!-^w$ is weaker than $\Diamond\!\!\!\!-$. As for strong probabilistic bisimulation, we can prove that $\mathcal{L}_w^N$ characterizes weak probabilistic bisimulation.

Theorem 3. *Given the logic $\mathcal{L}_w^N$, for each pair of states s, r of a probabilistic automaton, $s \approx^p r$ iff $\mathcal{F}(s) = \mathcal{F}(r)$.*

Proof outline. Lemma 1, 2, 3 and 4 hold also here. Then, the proof of this theorem follows the lines of that of Theorem 1, by replacing strong transitions with weak combined transitions in the appropriate places. □

5 Hennessy-Milner Logic for Reactive Systems

Reactive systems [6] are essentially *deterministic* probabilistic automata, i.e., for each state and for each label, there exists at most one transition. There is already a logical characterization of bisimulation for reactive systems by Larsen and Skou [11]. The syntax of the Larsen and Skou logic is the following:

$$\mathcal{L}^{ls} ::= \top \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \Diamond_p a\varphi,$$

where p is a rational number in $[0, 1]$. The only new operator is $\Diamond_p$, whose semantics is:

- $s \models \Diamond_p a\varphi$ iff there exists a transition $s \xrightarrow{a} \mu$ such that $\mu([\![\varphi]\!]) \geq p$.

Desharnais, Panangaden et. al. [4] have shown that negation is not necessary to characterize bisimulation for reactive systems. Moreover, they have shown that infinitary conjunction is not needed even if the state space is uncountable, and can be replaced by a finite conjunction operator. The syntax of their logic is the following:

$$\mathcal{L}^{R} ::= \top \mid \varphi_1 \wedge \varphi_2 \mid \Diamond_p a\varphi.$$

It is immediate to see that $\mathcal{L}^R$ is a sublogic of $\mathcal{L}^{ls}$. We can see the logic $\mathcal{L}^R$ as a sublogic of $\mathcal{L}^N$ as well. From this, we see clearly that negation is needed to handle nondeterminism. Also the operator $[\cdot]_p$ is necessary when nondeterminism is present. However, as shown in the next section, this operator can be dropped in favor of $\Diamond_p$ if nondeterminism is partially restricted.

6 Hennessy-Milner Logic for Alternating Models

In this section, we define two logics for strong and weak probabilistic bisimulation for a restriction of probabilistic automata that embeds the alternating models and we show that the logical characterization of [5] continues to hold.

We say that a probabilistic automaton is *alternating* if the states that enable a non-Dirac transition enable only one transition. We call *probabilistic* those states that enable non-Dirac transitions, and *nondeterministic* all the other states. This definition of alternating probabilistic automaton, indeed, describes a class of systems that is more general than the labeled concurrent Markov chains of Hansson [7] and of Philippou et. al. [13], since it does not impose any alternation between nondeterministic and probabilistic states, and it allows probabilistic transitions to be labeled by external actions. As shown in [16], the notion of bisimulation of this paper coincides with those of Hansson and of Philippou et. al. when applied to their models. Thus, a logical characterization for alternating probabilistic automata is also a logical characterization for the alternating models.

Following the lines of [5], we restrict to compact systems when studying weak probabilistic bisimulation. Indeed, the logical characterization does not hold in general for non-compact systems. We do not handle strong probabilistic bisimulation explicitly since it coincides with strong bisimulation [16].

6.1 Hennessy-Milner Logic for Strong Bisimulation

Since in alternating probabilistic automata each probabilistic transition is described by some state, then intuitively the target measure of a probabilistic transition that leaves from a state s be studies by observing the probability of reaching each equivalence class from s. For this reason the operator $\Diamond_p$ should suffice. Indeed, bisimulation relations can be characterized in terms of maximal probabilities of reaching equivalence classes (Lemma 5), and thus, an operator $\Diamond_p$ suffices.

The overall idea of maximal probabilities is taken from [13]. The syntax of the logic $\mathcal{L}^A$ for strong bisimulation is the following:

$$\mathcal{L}^A ::= \top \mid \neg\varphi \mid \bigwedge_I \varphi_i \mid \Diamond_p a\varphi.$$

The semantics of the operator $\Diamond_p$ is exactly the same as for reactive systems. Note that if we drop the operator $[\cdot]_p$, it is no more necessary to define the satisfaction relation on measures, since it can be defined on single states. In a similar way as in [13], for each action a and for each equivalence class $[t]$ of $\sim$, we define $\overline{\mu}_{s,a}([t])$ as the maximal probability to reach $[t]$ from s with a strong transition labeled a. The following lemma relates maximal probabilities and strong bisimulation.

Lemma 5. *For each pair of states s and r of an alternating automaton, if $\overline{\mu}_{s,a}([t]) = \overline{\mu}_{r,a}([t])$ for each action a and each equivalence class $[t]$ of $\sim$, then $s \sim r$.*

Proof. Let $\{[t_i]\}_I$ be an enumeration of the equivalence classes of $\sim$. Without loss of generality, we distinguish the following cases.

1. s is nondeterministic. Let $s \xrightarrow{a} \mu$. Then, μ is a Dirac measure $\delta(s')$. Let $k \in I$ be the index of the class such that $s' \in [t_k]$. Then, $\mu([t_k]) = 1$. This means that $\mu([t_k]) = \overline{\mu}_{s,a}([t_k])$. Then, by hypothesis, there exists μ' such that $\mu'([t_k]) = \overline{\mu}_{r,a}([t_k])$ and $\mu'([t_k]) = 1$. By definition, for each equivalence class $[t_j]$, $\mu'([t_j]) = 0$. Thus, $\mu \sim \mu'$.
2. s is probabilistic. Then, let $s \xrightarrow{a} \mu$ be the only transition from s. By definition, for each $i \in I$, $\mu([t_i]) = \overline{\mu}_{s,a}([t_i])$. If r is probabilistic, then by hypothesis, $r \xrightarrow{a} \mu'$ is the only transition from r, and μ, μ' agree on all the equivalence classes. If r is nondeterministic, then each transition is of the form $r \xrightarrow{a} \delta(r')$ and for each $i \in I$, $\delta([t_i]) = \overline{\mu}_{r,a}([t_i]) = 1$ only if $r' \in [t_i]$. By hypothesis, there exists an equivalence class $[t_k]$ such that $\mu([t_k]) = 1$. This also implies that all the target Dirac distributions $\delta(r')$ reached from r are related, since by hypothesis, each r' must belong to $[t_k]$. Thus, for each transition $r \xrightarrow{a} \delta(r')$, $\mu \sim \delta(r')$.

Now we can prove the completeness of $\mathcal{L}^A$ using the result of the previous lemma.

Theorem 4. *Given the logic $\mathcal{L}^A$, for each pair of states s, r of an alternating automaton, $s \sim r$ iff $\mathcal{F}(s) = \mathcal{F}(r)$.*

Proof. ($\Longrightarrow$). Soundness follows by Theorem 1, by the fact that alternating automata are a special case of probabilistic automata via embedding [16] and since $\mathcal{L}^A$ is a sublogic of $\mathcal{L}^N$.
($\Longleftarrow$). Let $s \bowtie r$, and let $\{\langle t_i \rangle\}_I$ be an enumeration of the equivalence classes of $\bowtie$. We show that $\bowtie$ is a bisimulation between s and r that is, by Lemma 5, for each action a and for each $i \in I$, $\overline{\mu}_{s,a}(\langle t_i \rangle) = \overline{\mu}_{r,a}(\langle t_i \rangle)$. By hypothesis and by Lemma 1, for each pair of classes $\langle t_i \rangle, \langle t_j \rangle$, there exists a formula φ_{ij} such that $t_i \models \varphi_{ij}$ and $t_j \not\models \varphi_{ij}$. For each $i \in I$, let $\varphi_i = \bigwedge_{I \smallsetminus \{i\}} \varphi_{ij}$. Then, φ_i is satisfied only by the states of $\langle t_i \rangle$. For the sake of contradiction, suppose that there exists an action a and a class $\langle t_k \rangle$ such that $\overline{\mu}_{s,a}(\langle t_k \rangle) \neq \overline{\mu}_{r,a}(\langle t_k \rangle)$. For each $i \in I$, let $\mu(\langle t_i \rangle) = \overline{\mu}_{s,a}(\langle t_i \rangle)$ and $\mu'(\langle t_i \rangle) = \overline{\mu}_{s,a}(\langle t_i \rangle)$. Without loss of generality, let $\mu'(\langle t_k \rangle) < \mu(\langle t_k \rangle)$ Then, there exists a rational p such that $\mu'(\langle t_k \rangle) < p < \mu(\langle t_k \rangle)$. By definition, $s \models \Diamond_p a \varphi_k$. By hypothesis, $r \models \Diamond_p a \varphi_k$ as well. This means that there exists a measure μ'' such that $r \xrightarrow{a} \mu''$ and $\mu''([\![\varphi_k]\!]) \geq p$. By hypothesis, $[\![\varphi_k]\!] = \langle t_k \rangle$, and by definition, $\mu''(\langle t_k \rangle) \leq \mu'(\langle t_k \rangle)$, a contradiction.

6.2 Hennessy-Milner Logic for Weak Probabilistic Bisimulation

As shown by Desharnais et. al. [5], in countable-state systems compactness implies that maximal probabilities work correctly, that is, for each maximal probability reachable, there is a corresponding weak probabilistic transition giving the same probability. This requirements is not needed in finite-state systems [13] since finite systems are compact. In the following, we will implicitly assume that the alternating models considered are compact, thus allowing us to handle maximal probabilities in our proofs.

The logical characterizing weak bisimulation for labeled concurrent Markov chains [5] is reported in the following:

$$\mathcal{L}^A_w ::= \top \mid \neg\varphi \mid \bigwedge_I \varphi_i \mid \langle\!\langle \rangle\!\rangle^w_p a\varphi.$$

In [5], disjunction is also used since it simplifies their proof of completeness, but it is not necessary. This logic is exactly that of Larsen and Skou, except for the diamond operator, whose semantics $\langle\!\langle \rangle\!\rangle^w_p$ is defined as follows:

- $s \models \langle\!\langle \rangle\!\rangle^w_p a\varphi$ iff $\overline{\mu}_{s,a}([\![\varphi]\!]) \geq p$.

This definition underlines the strict correlation between weak bisimulation for alternating models and maximal probabilities. Philippou et. al. [13] restrict their study to deterministic schedulers, while Desharnais et. al. [5] permit linear combination of deterministically scheduled paths to reach maximal probabilities. These linear combinations reflect the concept of *convex combinations* for probabilistic automata. Anyway, deterministic schedulers are enough to reach maximal probabilities, allowing us to simplify some proofs using deterministic schedulers instead of randomized ones.

Keeping the same notation of the previous section, for each action a and for each formula φ, $\overline{\mu}_{s,a}([\![\varphi]\!])$ is defined as the maximal probability (over all schedulers) of $[\![\varphi]\!]$ over all the distributions reached via *weak combined transitions* from s with label a. Like for strong bisimulation, for each action a and for each formula φ, we can state that $\langle\!\langle a \rangle\!\rangle^w_p a\varphi \equiv \langle\!\langle a \rangle\!\rangle^w a[\varphi]_p$. In the following, we prove the completeness of the logic $\mathcal{L}^A_w$, extending some results of [5] to our definition of alternating model.

We define a new relation $\doteq$ such that, for each pair of states s, r of an alternating automaton, $s \doteq r$ iff

- s and r are nondeterministic and for each action a and for each $\doteq$-closed set E, $\overline{\mu}_{s,a}(E) = \overline{\mu}_{r,a}(E)$, or
- s is probabilistic with action τ and for each $\doteq$-closed set E such that $s \notin E$, $\overline{\mu}_{s,\tau}(E) = \overline{\mu}_{r,\tau}(E)$, or
- s is probabilistic with external action and for each $\doteq$-closed set E, $\overline{\mu}_{s,a}(E) = \overline{\mu}_{r,a}(E)$.

The following lemma states a property of deterministic schedulers [1], and permits to use indifferently deterministic or randomized schedulers when calculating maximal probabilities. The assumption is to work in compact systems, since this result requires that each set considered must be reachable by a weak transition.

Lemma 6. *In compact systems, maximal probabilities can be reached with deterministic schedulers.*

The next lemma shows that the relation $\bowtie$ implies the relation $\doteq$ which directly talks about maximal probabilities reachable. This result is basilar to prove the soundness of the logic $\mathcal{L}^N_w$.

Lemma 7. *For each pair of states s, r of an alternating automaton, if $s \bowtie r$ then $s \doteq r$.*

Proof. Let $s \bowtie r$, and let $\{\langle t_i \rangle\}_I$ be an enumeration of the equivalence classes of $\bowtie$. We prove a stronger result, showing that for each action a and for each equivalence class $\langle t_k \rangle$, $\overline{\mu}_{s,a}(\langle t_k \rangle) = \overline{\mu}_{r,a}(\langle t_k \rangle)$, which directly implies that $s \doteq r$. By hypothesis and by Lemma 1, for each pair of classes $\langle t_i \rangle, \langle t_j \rangle$, there exists a formula φ_{ij} such that $t_i \models \varphi_{ij}$ and $t_j \not\models \varphi_{ij}$. For each $i \in I$, let $\varphi_i = \bigwedge_{I \setminus \{i\}} \varphi_{ij}$. Then, φ_i is satisfied only by the states of $\langle t_i \rangle$. For the sake of contradiction, suppose that there exists an action a and a class $\langle t_k \rangle$ such that $\overline{\mu}_{s,a}(\langle t_k \rangle) \neq \overline{\mu}_{r,a}(\langle t_k \rangle)$. Without loss of generality, let $\overline{\mu}_{s,a}(\langle t_k \rangle) < \overline{\mu}_{r,a}(\langle t_k \rangle)$. Then, there exists a rational p such that $\overline{\mu}_{s,a}(\langle t_k \rangle) < p < \overline{\mu}_{r,a}(\langle t_k \rangle)$. By definition, $r \models \langle\!\langle a \rangle\!\rangle^w_p a\varphi_k$ since $\overline{\mu}_{r,a}([\![\varphi_k]\!]) \geq p$. By hypothesis, $s \models \langle\!\langle a \rangle\!\rangle^w_p a\varphi_k$, that is, $\overline{\mu}_{s,a}([\![\varphi_k]\!]) \geq p$. Then, $\overline{\mu}_{s,a}(\langle t_k \rangle) \geq p$, a contradiction.

Theorem 5 extends a result by [5] to alternating automata. This theorem is necessary to prove the completeness of the logic for weak probabilistic bisimulation in Theorem 6.

Theorem 5. *The relation $\doteq$ is a weak probabilistic bisimulation.*

Proof outline. The proof follows the lines of Theorem 2 of [5], considering also probabilistic states enabling an external transition. □

Theorem 6. *Given the logic $\mathcal{L}_w^A$, for each pair of states s, r of an alternating automaton, $s \approx^p r$ iff $\mathcal{F}(s) = \mathcal{F}(r)$.*

Proof outline. Soundness follows by Theorem 1, by the fact that alternating automata are a special case of probabilistic automata via embedding [16] and since $\mathcal{L}_w^A$ is a sublogic of $\mathcal{L}^N$. Completeness follows by Theorem 5 and Lemma 7. □

Model	Logic	Syntax	Bisimulation
Non-Alternating	$\mathcal{L}^N$	$\top \mid \neg\varphi \mid \wedge_I \varphi_i \mid \Diamond a\varphi \mid [\varphi]_p$	$\sim$
	$\mathcal{L}_p^N$	$\top \mid \neg\varphi \mid \wedge_I \varphi_i \mid \Diamond a\varphi \mid [\varphi]_p$	$\sim^p$
	$\mathcal{L}_w^N$	$\top \mid \neg\varphi \mid \wedge_I \varphi_i \mid \Diamond^w a\varphi \mid [\varphi]_p$	$\approx^p$
Alternating	$\mathcal{L}^A$	$\top \mid \neg\varphi \mid \wedge_I \varphi_i \mid \Diamond_p a\varphi$	$\sim$
	$\mathcal{L}_w^A$	$\top \mid \neg\varphi \mid \wedge_I \varphi_i \mid \Diamond_p^w a\varphi$	$\approx^p$
Reactive	$\mathcal{L}^R$	$\top \mid \varphi_1 \wedge \varphi_2 \mid \Diamond_p a\varphi$	$\sim$

Table 1. Hennessy-Milner logics for discrete probabilistic systems.

7 Concluding Remarks

We have studied logical characterizations, in terms of Hennessy-Milner style logics, of strong, strong probabilistic and weak probabilistic bisimulations for probabilistic automata [14]. Our logics are defined on measures over states rather than on single states, and add a new operator the classical Hennessy-Milner logic that measures the probability of the set of states that satisfy a formula. Compared to other existing logics for reactive and alternating systems [11, 5], our logics keep the $\Diamond$ operator of Hennessy-Milner rather than replacing it with $\Diamond_p$, at the cost of adding a more powerful operator to measure probabilities.

We have studied restrictions on probabilistic automata that embed the alternating models and at the same time can be characterized by the logics of [5]. These restrictions impose that each state that enables a probabilistic transition enables only one transition, which is the key property to keep alternative characterizations of bisimulation relations in terms of maximal probabilities [13, 5]. This result is important because it explains what are the key features of the

alternating models that make them more tractable from the algorithmic point of view. Recall, indeed that weak bisimulations are decidable in polynomial time in the alternating models [13] due to their characterization in terms of maximal probabilities, while they are decidable in exponential time for probabilistic automata [1].

Our long term goal is to extend the theory of probabilistic automata to non-discrete probability measures. The logical characterizations studied in this paper will provide us important guidelines for the definitions to propose in this more general setting.

References

1. S. Cattani and R. Segala. Decision algorithms for probabilistic bisimulation. In P. Jankar and M. Kretinsky, editors, *Proceedings of CONCUR 2002,* Brno, Czech Republic, volume 2421 of *Lecture Notes in Computer Science*, pages 371–385. Springer-Verlag, 2002.
2. S. Cattani, R. Segala, M. Kwiatkowska, and G. Norman. Stochastic transition systems for continuous state space and nondeterminism. 2005.
3. Yuxin Deng. *Axiomatisations and Types for Probabilistic and Mobile Processes.* PhD thesis, Ecole des Mines de Paris, 2005.
4. J. Desharnais, A. Edalat, and P. Panangaden. A logical chracterization of bisimulation for labelled markov processes. *Proceedings of the 13th IEEE Symposium On Logic In Computer Science*, 179(2):478–489, 1998.
5. J. Desharnais, V. Gupta, R. Jagadeesan, and P. Panangaden. Weak bisimulation is sound and complete for PCTL. In M. Ketnsky L. Brim, P. Janar and A. Kuera, editors, *Proc. CONCUR 2002*, volume 2421 of *LNCS*, pages 355–370, 2002.
6. R.J. van Glabbeek, S.A. Smolka, B. Steffen, and C.M.N. Tofts. Reactive, generative, and stratified models of probabilistic processes. In *Proceedings* 5^{th} *Annual Symposium on Logic in Computer Science,* Philadelphia, USA, pages 130–141. IEEE Computer Society Press, 1990.
7. H. Hansson. *Time and Probability in Formal Design of Distributed Systems.* PhD thesis, Department of Computer Science, Uppsala University, 1991.
8. M. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *Journal of the ACM*, 32(1):137–161, 1985.
9. B. Jonsson and K.G. Larsen. Specification and refinement of probabilistic processes. In *Proceedings of the 6th IEEE Symposium on Logic in Computer Science*, pages 266–277, Amsterdam, July 1991.
10. R. Keller. Formal verification of parallel programs. *Communications of the ACM*, 7(19):561–572, 1976.
11. K.G. Larsen and A. Skou. Bisimulation through probabilistic testing. *Information and Computation*, 94(1):1–28, September 1991.
12. N. Lynch, R. Segala, and F. Vaandrager. Compositionality for probabilistic automata. In D. Lugiez R. Amadio, editor, *Proceedings of CONCUR 2003,* Marseille, France, volume 2761 of *Lecture Notes in Computer Science*, pages 208–221. Springer-Verlag, 2003.
13. A. Philippou, I. Lee, and O. Sokolsky. Weak bisimulation for probabilistic systems. In C. Palamidessi, editor, *Proceedings of CONCUR 2000,* University Park, PA, USA, volume 1877 of *Lecture Notes in Computer Science*, pages 334–349. Springer-Verlag, 2000.

14. R. Segala. *Modeling and Verification of Randomized Distributed Real-Time Systems*. PhD thesis, MIT, Dept. of Electrical Engineering and Computer Science, 1995. Also appears as technical report MIT/LCS/TR-676.
15. R. Segala and N.A. Lynch. Probabilistic simulations for probabilistic processes. In B. Jonsson and J. Parrow, editors, *Proceedings of CONCUR 94,* Uppsala, Sweden, volume 836 of *Lecture Notes in Computer Science*, pages 481–496. Springer-Verlag, 1994.
16. Roberto Segala and Andrea Turrini. Comparative analysis of bisimulation relations on alternating and non-alternating probabilistic models. In *Proceedings of the Second International Conference on Quantitative Evaluation SysTems (QEST) 2005*, September 2005.