Disjunctive Probabilistic Modal Logic is Enough for Bisimilarity on Reactive Probabilistic Systems

Marco Bernardo[1] and Marino Miculan[2]

[1] Dip. di Scienze Pure e Applicate, Università di Urbino, Italy
[2] Dip. di Scienze Matematiche, Informatiche e Fisiche, Università di Udine, Italy

Abstract. Larsen and Skou characterized probabilistic bisimilarity over reactive probabilistic systems with a logic including true, negation, conjunction, and a diamond modality decorated with a probabilistic lower bound. Later on, Desharnais, Edalat, and Panangaden showed that negation is not necessary to characterize the same equivalence. In this paper, we prove that the logical characterization holds also when conjunction is replaced by disjunction, with negation still being not necessary. To this end, we introduce *reactive probabilistic trees*, a fully abstract model for reactive probabilistic systems that allows us to demonstrate expressiveness of the disjunctive probabilistic modal logic, as well as of the previously mentioned logics, by means of a compactness argument.

1 Introduction

Since its introduction [12], *probabilistic bisimilarity* has been used to compare probabilistic systems. It corresponds to Milner's *strong bisimilarity* for nondeterministic systems, and coincides with *lumpability* for Markov chains. Larsen and Skou [12] first proved that bisimilarity for *reactive probabilistic systems* can be given a *logical characterization*: two processes are bisimilar if and only if they satisfy the same set of formulas of a propositional modal logic similar to Hennessy-Milner logic [10]. In addition to the usual constructs $\top$, $\neg$, and $\wedge$, this logic features a diamond modality $\langle a \rangle_p \phi$, which is satisfied by a state if, after performing action a, the probability of being in a state satisfying ϕ is at least p.

Later on, Desharnais, Edalat, and Panangaden [6] showed that negation is *not* necessary for discrimination purposes, by working in a *continuous*-state setting. This result has no counterpart in the nonprobabilistic setting, where Hennessy-Milner logic without negation characterizes *simulation* equivalence, which is strictly coarser than bisimilarity [8] (while the two equivalences are known to coincide on reactive probabilistic systems [2]).

V. Biló, A. Caruso (Eds.): ICTCS 2016, Proceedings of the 17th Italian Conference on Theoretical Computer Science, 73100 Lecce, Italy, September 7–9 2016, pp. 203–217 published in CEUR Workshop Proceedins Vol-1720 at `http://ceur-ws.org/Vol-1720`

In this paper, we show that $\vee$ can be used in place of $\wedge$ without having to reintroduce negation: the constructs $\top$, $\vee$, and $\langle a \rangle_p$ suffice to characterize bisimilarity on reactive probabilistic systems. The intuition is that from a conjunctive distinguishing formula we can often derive a disjunctive one by suitably increasing some probabilistic lower bounds. Not even this result has a counterpart in the nonprobabilistic setting, where replacing conjunction with disjunction in the absence of negation yields trace equivalence (this equivalence does *not* coincide with bisimilarity on reactive probabilistic processes).

The proof of our result relies on a simple categorical construction of a semantics for reactive probabilistic systems, which we call *reactive probabilistic trees* (Sect. 3). This semantics is *fully abstract*, i.e., two states are probabilistically bisimilar if and only if they are mapped to the same reactive probabilistic tree. Moreover, the semantics is *compact*, in the sense that two (possibly infinite) trees are equal if and only if all of their *finite* approximations are equal. Hence, in order to prove that a logic characterizes probabilistic bisimilarity, it suffices to prove that it allows to discriminate finite reactive probabilistic trees. Indeed, given two different finite trees, we can construct a formula of the considered logic (by induction on the height of one of the trees) that tells the two trees apart and has a depth not exceeding the height of the two trees (Sect. 4). Our technique applies also to the logics in [12,6], for which it allows us to provide simpler proofs of adequacy, directly in a *discrete* setting. More generally, this technique can be used in any computational model that has a compact, fully abstract semantics.

2 Processes, Bisimilarity, and Logics

2.1 Reactive Probabilistic Processes and Strong Bisimilarity

Probabilistic processes can be represented as labeled transitions systems with probabilistic information used to determine which action is executed or which state is reached. Following the terminology of [9], we focus on *reactive* probabilistic processes, where every state has for each action at most one outgoing distribution over states; the choice among these arbitrarily many, differently labeled distributions is nondeterministic. For a countable (i.e., finite or countably infinite) set X, the set of *finitely supported* (a.k.a. simple) probability distributions over X is given by $D(X) = \{\Delta : X \to \mathbb{R}_{[0,1]} \mid |\mathit{supp}(\Delta)| < \omega, \sum_{x \in X} \Delta(x) = 1\}$, where the *support* of distribution Δ is defined as $\mathit{supp}(\Delta) \triangleq \{x \in X \mid \Delta(x) > 0\}$.

A *reactive probabilistic labeled transition system*, RPLTS for short, is a triple $(S, A, \longrightarrow)$ where S is a countable set of *states*, A is a countable set of *actions*, and $\longrightarrow \subseteq S \times A \times D(S)$ is a *transition relation* such that, whenever $(s, a, \Delta_1), (s, a, \Delta_2) \in \longrightarrow$, then $\Delta_1 = \Delta_2$.

An RPLTS can be seen as a directed graph whose edges are labeled by pairs $(a, p) \in A \times \mathbb{R}_{(0,1]}$. For every $s \in S$ and $a \in A$, if there are a-labeled edges outgoing from s, then these are finitely many (*image finiteness*), because the considered distributions are finitely supported, and the numbers on them add up to 1. As usual, we denote $(s, a, \Delta) \in \longrightarrow$ as $s \xrightarrow{a} \Delta$, where the set of reachable states coincides with $supp(\Delta)$. We also define cumulative reachability as $\Delta(S') = \sum_{s' \in S'} \Delta(s')$ for all $S' \subseteq S$.

Probabilistic bisimilarity for the class of reactive probabilistic processes was introduced by Larsen and Skou [12]. Let $(S, A, \longrightarrow)$ be an RPLTS. An equivalence relation $\mathcal{B}$ over S is a *probabilistic bisimulation* iff, whenever $(s_1, s_2) \in \mathcal{B}$, then for all actions $a \in A$ it holds that, if $s_1 \xrightarrow{a} \Delta_1$, then $s_2 \xrightarrow{a} \Delta_2$ and $\Delta_1(C) = \Delta_2(C)$ for all equivalence classes $C \in S/\mathcal{B}$. We say that $s_1, s_2 \in S$ are *probabilistically bisimilar*, written $s_1 \sim_{\mathrm{PB}} s_2$, iff there exists a probabilistic bisimulation including the pair (s_1, s_2).

2.2 Probabilistic Modal Logics

In our setting, a probabilistic modal logic is a pair formed by a set $\mathcal{L}$ of *formulas* and an RPLTS-indexed family of *satisfaction relations* $\models \subseteq S \times \mathcal{L}$. The *logical equivalence* induced by $\mathcal{L}$ over S is defined by letting $s_1 \cong_{\mathcal{L}} s_2$, where $s_1, s_2 \in S$, iff $s_1 \models \phi \iff s_2 \models \phi$ for all $\phi \in \mathcal{L}$. We say that $\mathcal{L}$ *characterizes* a binary relation $\mathcal{R}$ over S when $\mathcal{R} = \cong_{\mathcal{L}}$.

We are especially interested in probabilistic modal logics characterizing $\sim_{\mathrm{PB}}$. The logics considered in this paper are similar to Hennessy-Milner logic [10], but the diamond modality is decorated with a probabilistic lower bound as follows:

$$\mathrm{PML}_{\neg\wedge} : \phi ::= \top \mid \neg\phi \mid \phi \wedge \phi \mid \langle a \rangle_p \phi \qquad \mathrm{PML}_{\wedge} : \phi ::= \top \mid \phi \wedge \phi \mid \langle a \rangle_p \phi$$
$$\mathrm{PML}_{\neg\vee} : \phi ::= \top \mid \neg\phi \mid \phi \vee \phi \mid \langle a \rangle_p \phi \qquad \mathrm{PML}_{\vee} : \phi ::= \top \mid \phi \vee \phi \mid \langle a \rangle_p \phi$$

where $p \in \mathbb{R}_{[0,1]}$; trailing $\top$'s will be omitted for sake of readability. Their semantics with respect to an RPLTS state s is defined as usual, in particular:

$$s \models \langle a \rangle_p \phi \iff s \xrightarrow{a} \Delta \text{ and } \Delta(\{s' \in S \mid s' \models \phi\}) \geq p$$

Larsen and Skou [12] proved that $\mathrm{PML}_{\neg\wedge}$ (and hence $\mathrm{PML}_{\neg\vee}$) characterizes $\sim_{\mathrm{PB}}$. Desharnais, Edalat, and Panangaden [6] then proved in a *measure-theoretic* setting that $\mathrm{PML}_{\wedge}$ characterizes $\sim_{\mathrm{PB}}$ too, and hence negation is not necessary. This was subsequently redemonstrated by Jacobs and Sokolova [11] in the *dual adjunction* framework and by Deng and Wu [5] for a *fuzzy* extension of RPLTS. The main aim of this paper is to show that $\mathrm{PML}_{\vee}$ suffices as well.

3 Compact Characterization of Probabilistic Bisimilarity

3.1 Coalgebras for Probabilistic Systems

It is well known that the function D defined in Sect. 2.1 extends to a functor $D : \mathsf{Set} \to \mathsf{Set}$ whose action on morphisms is, for $f : X \to Y$, $D(f)(\Delta) = \lambda y.\Delta(f^{-1}(y))$. Then, every RPLTS corresponds to a coalgebra of the functor $B_{RP} : \mathsf{Set} \to \mathsf{Set}, B_{RP}(X) \triangleq (D(X) + 1)^A$. Indeed, for $S = (S, A, \longrightarrow)$, the corresponding coalgebra $(S, \sigma : S \to B_{RP}(S))$ is $\sigma(s) \triangleq \lambda a.(\text{if } s \xrightarrow{a} \Delta \text{ then } \Delta \text{ else } *)$. A *homomorphism* $h : (S, \sigma) \to (T, \tau)$ is a function $h : S \to T$ that respects the coalgebraic structures, i.e., $\tau \circ h = (B_{RP} h) \circ \sigma$. We denote by $Coalg(B_{RP})$ the category of B_{RP}-coalgebras and their homomorphisms.

Aczel and Mendler [1] introduced a general notion of bisimulation for coalgebras, which in our setting instantiates as follows:

Definition 1. *Let* (S_1, σ_1), (S_2, σ_2) *be* B_{RP}*-coalgebras. A relation* $\mathcal{R} \subseteq S_1 \times S_2$ *is a* B_{RP}-bisimulation *iff there exists a coalgebra structure* $\rho : \mathcal{R} \to B_{RP}\mathcal{R}$ *such that the projections* $\pi_1 : \mathcal{R} \to S_1$, $\pi_2 : \mathcal{R} \to S_2$ *are homomorphisms (i.e.,* $\sigma_i \circ \pi_i = B_{RP}\pi_i \circ \rho$ *for* $i = 1, 2$*). We say that* $s_1 \in S_1$, $s_2 \in S_2$ *are* B_{RP}-bisimilar, *written* $s_1 \sim s_2$*, iff there exists a* B_{RP}*-bisimulation including* (s_1, s_2)*.*

Proposition 1. *The probabilistic bisimilarity over an RPLTS* $(S, A, \longrightarrow)$ *coincides with the* B_{RP}*-bisimilarity over the corresponding coalgebra* (S, σ)*.*

B_{RP} is finitary (because we restrict to finitely supported distributions) and hence admits final coalgebra (cf. [3,15] and specifically [14, Thm. 4.6]). The final coalgebra is unique up-to isomorphism, and can be seen as the RPLTS whose elements are canonical representatives of all possible behaviors of any RPLTS:

Proposition 2. *Let* (Z, ζ) *be a final* B_{RP}*-coalgebra. For all* $z_1, z_2 \in Z$*:* $z_1 \sim z_2$ *iff* $z_1 = z_2$*.*

3.2 Reactive Probabilistic Trees

We now introduce *reactive probabilistic trees*, a representation of the final B_{RP}-coalgebra that can be seen as the natural extension to the probabilistic setting of *strongly extensional trees* used to represent the final $\mathcal{P}_f$-coalgebra [15].

Definition 2 (*RPT*). *An (A-labeled)* reactive probabilistic tree *is a pair* (X, succ) *where* $X \in \mathsf{Set}$ *and* $\mathit{succ} : X \times A \to \mathcal{P}_f(X \times \mathbb{R}_{(0,1]})$ *are such that the relation* $\leq$ *over* X*, defined by the rules* $\frac{}{x \leq x}$ *and* $\frac{x \leq y \quad z \in \mathit{succ}(y,a)}{x \leq z}$*, is a partial order with a least element, called* root*, and for all* $x \in X$ *and* $a \in A$*:*

1. *the set* $\{y \in X \mid y \leq x\}$ *is finite and well-ordered;*
2. *for all* $(x_1, p_1), (x_2, p_2) \in \mathit{succ}(x, a)$*: if* $x_1 = x_2$ *then* $p_1 = p_2$*; if the subtrees rooted at* x_1 *and* x_2 *are isomorphic then* $x_1 = x_2$*;*
3. *if* $\mathit{succ}(x, a) \neq \emptyset$ *then* $\sum_{(y,p) \in \mathit{succ}(x,a)} p = 1$*.*

Reactive probabilistic trees are unordered trees where each node for each action has either no successors or a finite set of successors, which are labeled with positive real numbers that add up to 1; moreover, subtrees rooted at these successors are all *different*. See the forthcoming Fig. 1 for some examples. In particular, the trivial tree is $\mathit{nil} \triangleq (\{\perp\}, \lambda x, a.\emptyset)$.

We denote by RPT, ranged over by t, t_1, t_2, the set of reactive probabilistic trees (possibly of infinite height), up-to isomorphism. For $t = (X, \mathit{succ})$, we denote its root by $\perp_t$, its a-successors by $t(a) \triangleq \mathit{succ}(\perp_t, a)$, and the subtree rooted at $x \in X$ by $t[x] \triangleq (\{y \in X \mid x \leq y\}, \lambda y, a.\mathit{succ}(y, a))$; thus, $\perp_{t[x]} = x$. We define $\mathit{height} : RPT \to \mathbb{N} \cup \{\omega\}$ as $\mathit{height}(t) \triangleq \sup\{1 + \mathit{height}(t') \mid (t', p) \in t(a), a \in A\}$ with $\sup \emptyset = 0$; hence, $\mathit{height}(\mathit{nil}) = 0$. We denote by $RPT_f \triangleq \{t \in RPT \mid \mathit{height}(t) < \omega\}$ the set of reactive probabilistic trees of finite height.

A (possibly infinite) tree can be *pruned* at any height n, yielding a finite tree where the removed subtrees are replaced by *nil*. The "pruning" function

$(\cdot)|_n : RPT \to RPT_f$, parametric in n, can be defined by first truncating the tree t at height n, and then collapsing isomorphic subtrees adding their weights.

We have now to show that RPT is (the carrier of) the final B_{RP}-coalgebra (up-to isomorphism). To this end, we reformulate B_{RP} in a slightly more "relational" format. We define a functor $D' : \mathsf{Set} \to \mathsf{Set}$ as follows:

$$D'X \triangleq \{\emptyset\} \cup \{U \in \mathcal{P}_f(X \times \mathbb{R}_{(0,1]}) \mid \textstyle\sum_{(x,p)\in U} p = 1 \text{ and } (x,p),(x,q) \in U \Rightarrow p = q\}$$
$$D'f \triangleq \lambda U \in D'X.\{(f(x), \textstyle\sum_{(x,p)\in U} p) \mid x \in \pi_1(U)\} \qquad \text{for any } f : X \to Y.$$

Proposition 3. *$D'^A \cong B_{RP}$, and $Coalg(D'^A) \cong Coalg(B_{RP})$; hence the (supports of the) final D'^A-coalgebra and the final B_{RP}-coalgebra are isomorphic.*

RPT is the carrier of the final B_{RP}-coalgebra (up-to isomorphism). In fact, RPT can be endowed with a D'^A-coalgebra structure $\rho : RPT \to (D'(RPT))^A$ defined, for $t = (X, succ)$, as $\rho(t)(a) \triangleq \{(t[x], p) \mid (x,p) \in succ(\bot_t, a)\}$.

Theorem 1. *(RPT, ρ) is a final B_{RP}-coalgebra.*

By virtue of Thm. 1, given an RPLTS $S = (S, A, \longrightarrow)$ there exists a unique coalgebra homomorphism $[\![\cdot]\!] : S \to RPT$, called the *(final) semantics* of S, which associates each state in S with its behavior. This semantics is *fully abstract*. Another key property of reactive probabilistic trees is that they are *compact*: two different trees can be distinguished by looking at their finite subtrees only.

Theorem 2 (Full abstraction). *Let $(S, A, \longrightarrow)$ be an RPLTS. For all $s_1, s_2 \in S$: $s_1 \sim_{\mathrm{PB}} s_2$ iff $[\![s_1]\!] = [\![s_2]\!]$.*

Theorem 3 (Compactness). *For all $t_1, t_2 \in RPT$: $t_1 = t_2$ iff for all $n \in \mathbb{N}$: $t_1|_n = t_2|_n$.*

Corollary 1. *Let $(S, A, \longrightarrow)$ be an RPLTS. For all $s_1, s_2 \in S$: $s_1 \sim_{\mathrm{PB}} s_2$ iff for all $n \in \mathbb{N}$: $[\![s_1]\!]|_n = [\![s_2]\!]|_n$.*

4 The Discriminating Power of $\mathrm{PML}_\vee$

By virtue of the categorical construction leading to Cor. 1, in order to prove that a modal logic characterizes $\sim_{\mathrm{PB}}$ over reactive probabilistic processes, it is enough to show that it can discriminate all reactive probabilistic trees of *finite* height. A specific condition on the depth of distinguishing formulas has also to be satisfied, where $depth(\phi)$ is defined as usual:

$$depth(\top) = 0 \qquad depth(\neg\phi') = depth(\phi') \qquad depth(\langle a\rangle_p \phi') = 1 + depth(\phi')$$
$$depth(\phi_1 \wedge \phi_2) = depth(\phi_1 \vee \phi_2) = \max(depth(\phi_1), depth(\phi_2))$$

Proposition 4. *Let $\mathcal{L}$ be one of the probabilistic modal logics in Sect. 2.2. If $\mathcal{L}$ characterizes $=$ over RPT_f and for any two nodes t_1 and t_2 of an arbitrary RPT_f model such that $t_1 \neq t_2$ there exists $\phi \in \mathcal{L}$ distinguishing t_1 from t_2 such that $depth(\phi) \leq \max(height(t_1), height(t_2))$, then $\mathcal{L}$ characterizes $\sim_{\mathrm{PB}}$ over the set of RPLTS models.*

In this section, we show the main result of the paper: the logical equivalence induced by $\mathrm{PML}_{\vee}$ has the same discriminating power as $\sim_{\mathrm{PB}}$. This result is accomplished in three steps. Firstly, we redemonstrate Larsen and Skou's result for $\mathrm{PML}_{\neg\wedge}$ in the RPT_f setting, which yields a proof that, with respect to the one in [12], is simpler and does not require the minimal deviation assumption (i.e., that the probability associated with any state in the support of the target distribution of a transition be a multiple of some value). This provides a proof scheme for the subsequent steps. Secondly, we demonstrate that $\mathrm{PML}_{\neg\vee}$ characterizes $\sim_{\mathrm{PB}}$ by adapting the proof scheme to cope with the replacement of $\wedge$ with $\vee$. Thirdly, we demonstrate that $\mathrm{PML}_{\vee}$ characterizes $\sim_{\mathrm{PB}}$ by further adapting the proof scheme to cope with the absence of $\neg$.

Moreover, we redemonstrate Desharnais, Edalat, and Panangaden's result for $\mathrm{PML}_{\wedge}$ through yet another adaptation of the proof scheme that, unlike the proof in [6], works directly on *discrete* state spaces without making use of measure-theoretic arguments. Avoiding the resort to measure theory was shown to be possible for the first time by Worrell in an unpublished note cited in [13].

4.1 $\mathrm{PML}_{\neg\wedge}$ Characterizes $\sim_{\mathrm{PB}}$: A New Proof

To show that the logical equivalence induced by $\mathrm{PML}_{\neg\wedge}$ implies node equality $=$, we reason on the contrapositive. Given two nodes t_1 and t_2 such that $t_1 \neq t_2$, we proceed by induction on the height of t_1 to find a distinguishing $\mathrm{PML}_{\neg\wedge}$ formula whose depth is not greater than the heights of t_1 and t_2. The idea is to exploit negation, so to ensure that certain distinguishing formulas are *satisfied* by a certain derivative t' of t_1 (rather than the derivatives of t_2 different from t'), then take the *conjunction* of those formulas preceded by a diamond decorated with the probability for t_1 of *reaching* t'.

The only non-trivial case is the one in which t_1 and t_2 enable the same actions. At least one of those actions, say a, is such that, after performing it, the two nodes reach two distributions $\Delta_{1,a}$ and $\Delta_{2,a}$ such that $\Delta_{1,a} \neq \Delta_{2,a}$. Given a node $t' \in supp(\Delta_{1,a})$ such that $\Delta_{1,a}(t') > \Delta_{2,a}(t')$, by the induction hypothesis there exists a $\mathrm{PML}_{\neg\wedge}$ formula $\phi'_{2,j}$ that distinguishes t' from a specific $t'_{2,j} \in supp(\Delta_{2,a}) \setminus \{t'\}$. We can assume that $t' \models \phi'_{2,j} \not\models t'_{2,j}$ otherwise, thanks to the presence of negation in $\mathrm{PML}_{\neg\wedge}$, it would suffice to consider $\neg\phi'_{2,j}$.

As a consequence, $t_1 \models \langle a\rangle_{\Delta_{1,a}(t')} \bigwedge_j \phi'_{2,j} \not\models t_2$ because $\Delta_{1,a}(t') > \Delta_{2,a}(t')$ and $\Delta_{2,a}(t')$ is the maximum probabilistic lower bound for which t_2 satisfies a formula of that form. Notice that $\Delta_{1,a}(t')$ may not be the maximum probabilistic lower bound for which t_1 satisfies such a formula, because $\bigwedge_j \phi'_{2,j}$ might be satisfied by other a-derivatives of t_1 in $supp(\Delta_{1,a}) \setminus \{t'\}$.

Theorem 4. *Let $(T, A, \longrightarrow)$ be in RPT_f and $t_1, t_2 \in T$. Then $t_1 = t_2$ iff $t_1 \models \phi \iff t_2 \models \phi$ for all $\phi \in \mathrm{PML}_{\neg\wedge}$. Moreover, if $t_1 \neq t_2$, then there exists $\phi \in \mathrm{PML}_{\neg\wedge}$ distinguishing t_1 from t_2 such that $depth(\phi) \leq \max(height(t_1), height(t_2))$.*

4.2 $\mathrm{PML}_{\neg\vee}$ Characterizes $\sim_{\mathrm{PB}}$: Adapting the Proof

Since $\phi_1 \wedge \phi_2$ is logically equivalent to $\neg(\neg\phi_1 \vee \neg\phi_2)$, it is not surprising that $\mathrm{PML}_{\neg\vee}$ characterizes $\sim_{\mathrm{PB}}$ too. However, the proof of this result will be useful to set up an outline of the proof of the main result of this paper, i.e., that $\mathrm{PML}_{\vee}$ characterizes $\sim_{\mathrm{PB}}$ as well.

Similar to the proof of Thm. 4, also for $\mathrm{PML}_{\neg\vee}$ we reason on the contrapositive and proceed by induction. Given t_1 and t_2 such that $t_1 \neq t_2$, we intend to exploit negation, so to ensure that certain distinguishing formulas are *not satisfied* by a certain derivative t' of t_1 (rather than the derivatives of t_2 different from t'), then take the *disjunction* of those formulas preceded by a diamond decorated with the probability for t_2 of *not reaching* t'.

In the only non-trivial case, for $t' \in \mathit{supp}(\Delta_{1,a})$ such that $\Delta_{1,a}(t') > \Delta_{2,a}(t')$, by the induction hypothesis there exists a $\mathrm{PML}_{\neg\vee}$ formula $\phi'_{2,j}$ that distinguishes t' from a specific $t'_{2,j} \in \mathit{supp}(\Delta_{2,a}) \setminus \{t'\}$. We can assume that $t' \not\models \phi'_{2,j} \Dashv t'_{2,j}$ otherwise, thanks to the presence of negation in $\mathrm{PML}_{\neg\vee}$, it would suffice to consider $\neg\phi'_{2,j}$. Therefore, $t_1 \not\models \langle a \rangle_{1-\Delta_{2,a}(t')} \bigvee_j \phi'_{2,j} \Dashv t_2$ because $1-\Delta_{2,a}(t') > 1-\Delta_{1,a}(t')$ and the maximum probabilistic lower bound for which t_1 satisfies a formula of that form cannot exceed $1 - \Delta_{1,a}(t')$. Notice that $1 - \Delta_{2,a}(t')$ is the *maximum* probabilistic lower bound for which t_2 satisfies such a formula, because that value is the probability with which t_2 does not reach t' after performing a.

Theorem 5. *Let* $(T, A, \longrightarrow)$ *be in* RPT_f *and* $t_1, t_2 \in T$. *Then* $t_1 = t_2$ *iff* $t_1 \models \phi \iff t_2 \models \phi$ *for all* $\phi \in PML_{\neg\vee}$. *Moreover, if* $t_1 \neq t_2$, *then there exists* $\phi \in PML_{\neg\vee}$ *distinguishing* t_1 *from* t_2 *such that* $\mathit{depth}(\phi) \leq \max(\mathit{height}(t_1), \mathit{height}(t_2))$.

4.3 Also $\mathrm{PML}_{\vee}$ Characterizes $\sim_{\mathrm{PB}}$

The proof that $\mathrm{PML}_{\vee}$ characterizes $\sim_{\mathrm{PB}}$ is inspired by the one for $\mathrm{PML}_{\neg\vee}$, thus considers the contrapositive and proceeds by induction. In the only non-trivial case, we will arrive at a point in which $t_1 \not\models \langle a \rangle_{1-(\Delta_{2,a}(t')+p)} \bigvee_{j \in J} \phi'_{2,j} \Dashv t_2$ for:

- a derivative t' of t_1, such that $\Delta_{1,a}(t') > \Delta_{2,a}(t')$, not satisfying any subformula $\phi'_{2,j}$;
- a suitable probabilistic value p such that $\Delta_{2,a}(t') + p < 1$;
- an index set J identifying certain derivatives of t_2 other than t'.

The choice of t' is crucial, because negation is no longer available in $\mathrm{PML}_{\vee}$. Different from the case of $\mathrm{PML}_{\neg\vee}$, this induces the introduction of p and the limitation to J in the format of the distinguishing formula. An important observation is that, in many cases, a disjunctive distinguishing formula can be obtained from a conjunctive one by suitably *increasing* some probabilistic lower bounds. An obvious exception is when the use of conjunction/disjunction is not necessary for telling two different nodes apart.

Example 1. The nodes t_1 and t_2 in Fig. 1(a) cannot be distinguished by any formula in which neither conjunction nor disjunction occurs. It holds that:

$$t_1 \models \langle a \rangle_{0.5} (\langle b \rangle_1 \wedge \langle c \rangle_1) \not\Dashv t_2 \qquad t_1 \not\models \langle a \rangle_{1.0} (\langle b \rangle_1 \vee \langle c \rangle_1) \Dashv t_2$$

Notice that, when moving from the conjunctive formula to the disjunctive one, the probabilistic lower bound decorating the a-diamond increases from 0.5 to 1 and the roles of t_1 and t_2 with respect to $\models$ are inverted. The situation is similar for

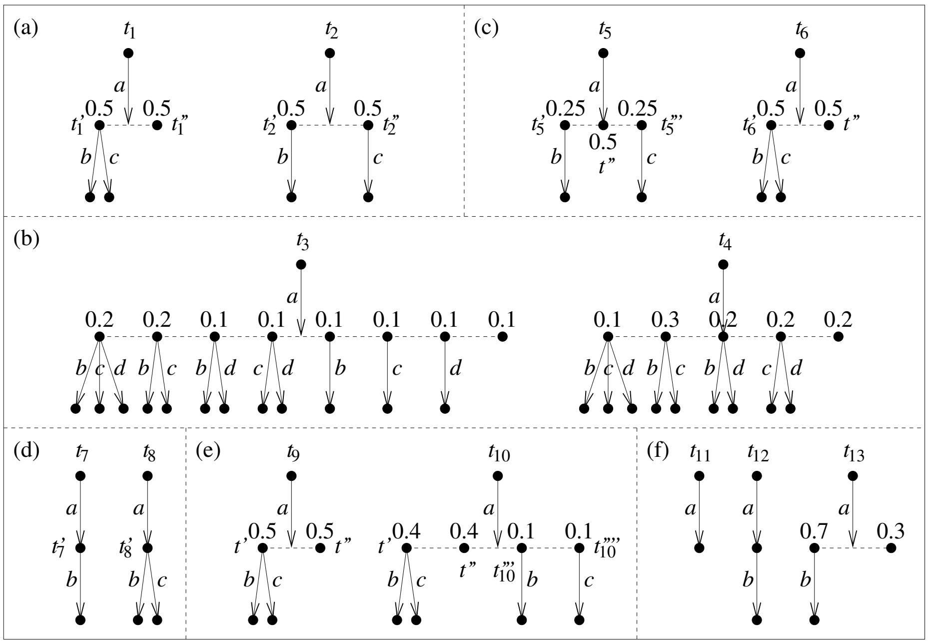

Fig. 1. RPT_f models used in the examples of Sects. 4.3 and 4.4.

the nodes t_3 and t_4 in Fig. 1(b), where two occurrences of conjunction/disjunction are necessary:

$$t_3 \models \langle a \rangle_{0.2} \, (\langle b \rangle_1 \wedge \langle c \rangle_1 \wedge \langle d \rangle_1) \not\models t_4 \qquad t_3 \models \langle a \rangle_{0.9} \, (\langle b \rangle_1 \vee \langle c \rangle_1 \vee \langle d \rangle_1) \not\models t_4$$

but the roles of t_3 and t_4 with respect to $\models$ cannot be inverted. ■

Example 2. For the nodes t_5 and t_6 in Fig. 1(c), it holds that:

$$t_5 \not\models \langle a \rangle_{0.5} \, (\langle b \rangle_1 \wedge \langle c \rangle_1) \Dashv t_6$$

If we replace conjunction with disjunction and we vary the probabilistic lower bound between 0.5 and 1, we produce no disjunctive formula capable of discriminating between t_5 and t_6. Nevertheless, a distinguishing formula belonging to $\mathrm{PML}_\vee$ exists with no disjunctions at all:

$$t_5 \not\models \langle a \rangle_{0.5} \, \langle b \rangle_1 \Dashv t_6$$ ■

The examples above show that the increase of some probabilistic lower bounds when moving from conjunctive distinguishing formulas to disjunctive ones takes place only in the case that the probabilities of reaching certain nodes have to be *summed up*. Additionally, we recall that, in order for two nodes to be related by $\sim_{\mathrm{PB}}$, they must enable the same actions, so focussing on a *single* action is enough for discriminating when only disjunction is available. Bearing this in mind, for any node t of finite height we define the set $\Phi_\vee(t)$ of $\mathrm{PML}_\vee$ formulas satisfied by t featuring:

– probabilistic lower bounds of diamonds that are *maximal* with respect to the satisfiability of a formula of that format by t (this is consistent with the observation in the last sentence before Thm. 5, and keeps the set $\Phi_\vee(t)$ finite);
– diamonds that arise only from *existing* transitions that depart from t (so to avoid useless diamonds in disjunctions and hence keep the set $\Phi_\vee(t)$ finite);
– disjunctions that stem only from *single* transitions of *different* nodes in the support of a distribution reached by t (transitions departing from the same node would result in formulas like $\bigvee_{h \in H} \langle a_h \rangle_{p_h} \phi_h$, with $a_{h_1} \neq a_{h_2}$ for $h_1 \neq h_2$, which are useless for discriminating with respect to $\sim_{\mathrm{PB}}$) and are preceded by a diamond decorated with the *sum* of the probabilities assigned to those nodes by the distribution reached by t.

Definition 3. *The set $\Phi_\vee(t)$ for a node t of finite height is defined by induction on height(t) as follows:*

– *If height$(t) = 0$, then $\Phi_\vee(t) = \emptyset$.*
– *If height$(t) \geq 1$ for t having transitions of the form $t \xrightarrow{a_i} \Delta_i$ with supp$(\Delta_i) = \{t'_{i,j} \mid j \in J_i\}$ and $i \in I \neq \emptyset$, then: $\Phi_\vee(t) = \{\langle a_i \rangle_1 \mid i \in I\} \cup$*

$$\bigcup_{i \in I} hplb\big(\bigcup_{\emptyset \neq J' \subseteq J_i} \{\langle a_i \rangle_{\sum_{j \in J'} \Delta_i(t'_{i,j})} \dot{\bigvee_{j \in J'}} \phi'_{i,j,k} \mid t'_{i,j} \in supp(\Delta_i), \phi'_{i,j,k} \in \Phi_\vee(t'_{i,j})\}\big)$$

where $\dot{\vee}$ is a variant of $\vee$ in which identical operands are not admitted (i.e., idempotence is forced) and hplb keeps only the formula with the highest probabilistic lower bound decorating the initial a_i-diamond among the formulas differring only for that bound.

To illustrate the definition given above, we exhibit some examples showing the usefulness of $\Phi_\vee$-sets for discrimination purposes. Given two different nodes that with the same action reach two different distributions, a good criterion for choosing t' (a derivative of the first node not satisfying certain formulas, to which the first distribution assigns a probability greater than the second one) seems to be the *minimality* of the $\Phi_\vee$-set.

Example 3. For the nodes t_7 and t_8 in Fig. 1(d), we have:

$$\Phi_\vee(t_7) = \{\langle a \rangle_1, \langle a \rangle_1 \langle b \rangle_1\} \qquad \Phi_\vee(t_8) = \{\langle a \rangle_1, \langle a \rangle_1 \langle b \rangle_1, \langle a \rangle_1 \langle c \rangle_1\}$$

A formula like $\langle a \rangle_1 (\langle b \rangle_1 \vee \langle c \rangle_1)$ is useless for discriminating between t_7 and t_8, because disjunction is between two actions enabled by the same node and hence constituting a nondeterministic choice. Indeed, such a formula is not part of $\Phi_\vee(t_8)$. While in the case of conjunction it is often necessary to concentrate on several alternative actions, in the case of disjunction it is convenient to focus on a single action per node when aiming at producing a distinguishing formula.

The fact that $\langle a \rangle_1 \langle c \rangle_1 \in \Phi_\vee(t_8)$ is a distinguishing formula can be retrieved as follows. Starting from the two identically labeled transitions $t_7 \xrightarrow{a} \Delta_{7,a}$ and $t_8 \xrightarrow{a} \Delta_{8,a}$ where $\Delta_{7,a}(t'_7) = 1 = \Delta_{8,a}(t'_8)$ and $\Delta_{7,a}(t'_8) = 0 = \Delta_{8,a}(t'_7)$, we have:

$$\Phi_\vee(t'_7) = \{\langle b \rangle_1\} \qquad \Phi_\vee(t'_8) = \{\langle b \rangle_1, \langle c \rangle_1\}$$

If we focus on t'_7 because $\Delta_{7,a}(t'_7) > \Delta_{8,a}(t'_7)$ and its $\Phi_\vee$-set is minimal, then $t'_7 \not\models \langle c \rangle_1 \models t'_8$ with $\langle c \rangle_1 \in \Phi_\vee(t'_8) \setminus \Phi_\vee(t'_7)$. As a consequence, $t_7 \not\models \langle a \rangle_1 \langle c \rangle_1 \models t_8$ where the value 1 decorating the a-diamond stems from $1 - \Delta_{8,a}(t'_7)$. ■

Example 4. For the nodes t_1 and t_2 in Fig. 1(a), we have:

$$\Phi_\vee(t_1) \;=\; \{\langle a\rangle_1,\ \langle a\rangle_{0.5}\langle b\rangle_1,\ \langle a\rangle_{0.5}\langle c\rangle_1\}$$
$$\Phi_\vee(t_2) \;=\; \{\langle a\rangle_1,\ \langle a\rangle_{0.5}\langle b\rangle_1,\ \langle a\rangle_{0.5}\langle c\rangle_1,\ \langle a\rangle_1\,(\langle b\rangle_1 \vee \langle c\rangle_1)\}$$

The formulas with two diamonds and no disjunction are identical in the two sets, so their disjunction $\langle a\rangle_{0.5}\langle b\rangle_1 \vee \langle a\rangle_{0.5}\langle c\rangle_1$ is useless for discriminating between t_1 and t_2. Indeed, such a formula is part of neither $\Phi_\vee(t_1)$ nor $\Phi_\vee(t_2)$. In contrast, their disjunction in which decorations of identical diamonds are summed up, i.e., $\langle a\rangle_1\,(\langle b\rangle_1 \vee \langle c\rangle_1)$, is fundamental. It belongs only to $\Phi_\vee(t_2)$ because in the case of t_1 the b-transition and the c-transition depart from the same node, hence no probabilities can be added.

The fact that $\langle a\rangle_1\,(\langle b\rangle_1 \vee \langle c\rangle_1) \in \Phi_\vee(t_2)$ is a distinguishing formula can be retrieved as follows. Starting from the two identically labeled transitions $t_1 \xrightarrow{a} \Delta_{1,a}$ and $t_2 \xrightarrow{a} \Delta_{2,a}$ where $\Delta_{1,a}(t'_1) = \Delta_{1,a}(t''_1) = 0.5 = \Delta_{2,a}(t'_2) = \Delta_{2,a}(t''_2)$ and $\Delta_{1,a}(t'_2) = \Delta_{1,a}(t''_2) = 0 = \Delta_{2,a}(t'_1) = \Delta_{2,a}(t''_1)$, we have:

$$\Phi_\vee(t'_1) \;=\; \{\langle b\rangle_1,\ \langle c\rangle_1\} \quad \Phi_\vee(t''_1) \;=\; \emptyset \quad \Phi_\vee(t'_2) \;=\; \{\langle b\rangle_1\} \quad \Phi_\vee(t''_2) \;=\; \{\langle c\rangle_1\}$$

If we focus on t''_1 because $\Delta_{1,a}(t''_1) > \Delta_{2,a}(t''_1)$ and its $\Phi_\vee$-set is minimal, then $t''_1 \not\models \langle b\rangle_1 \models t'_2$ with $\langle b\rangle_1 \in \Phi_\vee(t'_2) \setminus \Phi_\vee(t''_1)$ as well as $t''_1 \not\models \langle c\rangle_1 \models t''_2$ with $\langle c\rangle_1 \in \Phi_\vee(t''_2) \setminus \Phi_\vee(t''_1)$. Thus, $t_1 \not\models \langle a\rangle_1\,(\langle b\rangle_1 \vee \langle c\rangle_1) \models t_2$ where value 1 decorating the a-diamond stems from $1 - \Delta_{2,a}(t''_1)$. ■

Example 5. For the nodes t_5 and t_6 in Fig. 1(c), we have:

$$\Phi_\vee(t_5) \;=\; \{\langle a\rangle_1,\ \langle a\rangle_{0.25}\langle b\rangle_1,\ \langle a\rangle_{0.25}\langle c\rangle_1,\ \langle a\rangle_{0.5}\,(\langle b\rangle_1 \vee \langle c\rangle_1)\}$$
$$\Phi_\vee(t_6) \;=\; \{\langle a\rangle_1,\ \langle a\rangle_{0.5}\langle b\rangle_1,\ \langle a\rangle_{0.5}\langle c\rangle_1\}$$

The formulas with two diamonds and no disjunction are different in the two sets, so they are enough for discriminating between t_5 and t_6. In contrast, the only formula with disjunction, occurring in $\Phi_\vee(t_5)$, is useless because the probability decorating its a-diamond is equal to the one decorating the a-diamond of each of the two formulas with two diamonds in $\Phi_\vee(t_6)$.

The fact that $\langle a\rangle_{0.5}\langle b\rangle_1 \in \Phi_\vee(t_6)$ is a distinguishing formula can be retrieved as follows. Starting from the two identically labeled transitions $t_5 \xrightarrow{a} \Delta_{5,a}$ and $t_6 \xrightarrow{a} \Delta_{6,a}$ where $\Delta_{5,a}(t'_5) = \Delta_{5,a}(t'''_5) = 0.25$, $\Delta_{5,a}(t'') = 0.5 = \Delta_{6,a}(t'_6) = \Delta_{6,a}(t'')$, and $\Delta_{5,a}(t'_6) = 0 = \Delta_{6,a}(t'_5) = \Delta_{6,a}(t'''_5)$, we have:

$$\Phi_\vee(t'_5) \;=\; \{\langle b\rangle_1\} \quad \Phi_\vee(t'''_5) \;=\; \{\langle c\rangle_1\} \quad \Phi_\vee(t'_6) \;=\; \{\langle b\rangle_1,\ \langle c\rangle_1\} \quad \Phi_\vee(t'') \;=\; \emptyset$$

Notice that t'' might be useless for discriminating purposes because it has the same probability in both distributions, so we exclude it. If we focus on t'''_5 because $\Delta_{5,a}(t'''_5) > \Delta_{6,a}(t'''_5)$ and its $\Phi_\vee$-set is minimal after the exclusion of t'', then $t'''_5 \not\models \langle b\rangle_1 \models t'_6$ with $\langle b\rangle_1 \in \Phi_\vee(t'_6) \setminus \Phi_\vee(t'''_5)$, while no distinguishing formula is considered with respect to t'' as element of $supp(\Delta_{6,a})$ due to the exclusion of t'' itself. As a consequence, $t_5 \not\models \langle a\rangle_{0.5}\langle b\rangle_1 \models t_6$ where the value 0.5 decorating the a-diamond stems from $1 - (\Delta_{6,a}(t'''_5) + p)$ with $p = \Delta_{6,a}(t'')$. The reason for subtracting the probability that t_6 reaches t'' after performing a is that $t'' \not\models \langle b\rangle_1$.

We conclude by observing that focussing on t'' as derivative with the minimum $\Phi_\vee$-set is indeed problematic, because it would result in $\langle a\rangle_{0.5}\langle b\rangle_1$ when considering t'' as derivative of t_5, but it would result in $\langle a\rangle_{0.5}\,(\langle b\rangle_1 \vee \langle c\rangle_1)$ when considering t'' as derivative of t_6, with the latter formula not distinguishing between t_5 and t_6. Moreover, when focussing on t_5''', no formula ϕ' could have been found such that $t_5''' \not\models \phi' \dashv t''$ as $\Phi_\vee(t'') \subsetneq \Phi_\vee(t_5''')$. ■

The last example shows that, in the general format $\langle a \rangle_{1-(\Delta_{2,a}(t')+p)} \bigvee_{j \in J} \phi'_{2,j}$ for the $\mathrm{PML}_\vee$ distinguishing formula mentioned at the beginning of this subsection, the set J only contains any derivative of the second node different from t' to which the two distributions assign two *different* probabilities. No derivative of the two original nodes having the same probability in both distributions is taken into account even if its $\Phi_\vee$-set is minimal – because it might be useless for discriminating purposes – nor is it included in J – because there might be no formula satisfied by this node when viewed as a derivative of the second node, which is not satisfied by t'. Furthermore, the value p is the probability that the second node reaches the excluded derivatives that do *not* satisfy $\bigvee_{j \in J} \phi'_{2,j}$; note that the first node reaches those derivatives with the same probability p.

We present two additional examples illustrating some technicalities of Def. 3. The former example shows the usefulness of the operator $\dot{\vee}$ and of the function *hplb* for selecting the right t' on the basis of the minimality of its $\Phi_\vee$-set among the derivatives of the first node to which the first distribution assigns a probability greater than the second one. The latter example emphasizes the role played, for the same purpose as before, by formulas occurring in a $\Phi_\vee$-set whose number of nested diamonds is not maximal.

Example 6. For the nodes t_9 and t_{10} in Fig. 1(e), we have:

$$\Phi_\vee(t_9) = \{\langle a \rangle_1, \langle a \rangle_{0.5} \langle b \rangle_1, \langle a \rangle_{0.5} \langle c \rangle_1\}$$
$$\Phi_\vee(t_{10}) = \{\langle a \rangle_1, \langle a \rangle_{0.5} \langle b \rangle_1, \langle a \rangle_{0.5} \langle c \rangle_1, \langle a \rangle_{0.6} (\langle b \rangle_1 \vee \langle c \rangle_1)\}$$

Starting from the two identically labeled transitions $t_9 \xrightarrow{a} \Delta_{9,a}$ and $t_{10} \xrightarrow{a} \Delta_{10,a}$ where $\Delta_{9,a}(t') = \Delta_{9,a}(t'') = 0.5$, $\Delta_{10,a}(t') = \Delta_{10,a}(t'') = 0.4$, $\Delta_{10,a}(t_{10}''') = \Delta_{10,a}(t_{10}'''') = 0.1$, and $\Delta_{9,a}(t_{10}''') = \Delta_{9,a}(t_{10}'''') = 0$, we have:

$$\Phi_\vee(t') = \{\langle b \rangle_1, \langle c \rangle_1\} \quad \Phi_\vee(t'') = \emptyset \quad \Phi_\vee(t_{10}''') = \{\langle b \rangle_1\} \quad \Phi_\vee(t_{10}'''') = \{\langle c \rangle_1\}$$

If we focus on t'' because $\Delta_{9,a}(t'') > \Delta_{10,a}(t'')$ and its $\Phi_\vee$-set is minimal, then $t'' \not\models \langle b \rangle_1 \dashv t'$ with $\langle b \rangle_1 \in \Phi_\vee(t') \setminus \Phi_\vee(t'')$, $t'' \not\models \langle b \rangle_1 \dashv t_{10}'''$ with $\langle b \rangle_1 \in \Phi_\vee(t_{10}''') \setminus \Phi_\vee(t'')$, and $t'' \not\models \langle c \rangle_1 \dashv t_{10}''''$ with $\langle c \rangle_1 \in \Phi_\vee(t_{10}'''') \setminus \Phi_\vee(t'')$. Thus, $t_9 \not\models \langle a \rangle_{0.6} (\langle b \rangle_1 \vee \langle c \rangle_1) \dashv t_{10}$ where the formula belongs to $\Phi_\vee(t_{10})$ and the value 0.6 decorating the a-diamond stems from $1 - \Delta_{10,a}(t'')$.

If $\vee$ were used in place of $\dot{\vee}$, then in $\Phi_\vee(t_{10})$ we would also have formulas like $\langle a \rangle_{0.5} (\langle b \rangle_1 \vee \langle b \rangle_1)$ and $\langle a \rangle_{0.5} (\langle c \rangle_1 \vee \langle c \rangle_1)$. These are useless in that logically equivalent to other formulas already in $\Phi_\vee(t_{10})$ in which disjunction does not occur and, most importantly, would apparently augment the size of $\Phi_\vee(t_{10})$, an inappropriate fact in the case that t_{10} were a derivative of some other node instead of being the root of a tree.

If *hplb* were not used, then in $\Phi_\vee(t_{10})$ we would also have formulas like $\langle a \rangle_{0.1} \langle b \rangle_1$, $\langle a \rangle_{0.4} \langle b \rangle_1$, $\langle a \rangle_{0.1} \langle c \rangle_1$, and $\langle a \rangle_{0.4} \langle c \rangle_1$, in which the probabilistic lower bounds of the a-diamonds are not maximal with respect to the satisfiability of formulas of that form by t_{10}; those with maximal probabilistic lower bounds associated with a-diamonds are $\langle a \rangle_{0.5} \langle b \rangle_1$ and $\langle a \rangle_{0.5} \langle c \rangle_1$, which already belong to $\Phi_\vee(t_{10})$. In the case that t_9 and t_{10} were derivatives of two nodes under comparison instead of being the roots of two trees, the presence of those additional formulas in $\Phi_\vee(t_{10})$ may lead to focus on t_{10} instead of t_9 – for reasons that will be clear in Ex. 8 – thereby producing no distinguishing formula. ■

Example 7. For the nodes t_{11}, t_{12}, t_{13} in Fig. 1(f), we have:
$\Phi_\vee(t_{11}) = \{\langle a\rangle_1\}$ $\Phi_\vee(t_{12}) = \{\langle a\rangle_1, \langle a\rangle_1\langle b\rangle_1\}$ $\Phi_\vee(t_{13}) = \{\langle a\rangle_1, \langle a\rangle_{0.7}\langle b\rangle_1\}$
Let us view them as derivatives of other nodes, rather than roots of trees. The presence of formula $\langle a\rangle_1$ in $\Phi_\vee(t_{12})$ and $\Phi_\vee(t_{13})$ – although it has not the maximum number of nested diamonds in those two sets – ensures the minimality of $\Phi_\vee(t_{11})$ and hence that t_{11} is selected for building a distinguishing formula. If $\langle a\rangle_1$ were not in $\Phi_\vee(t_{12})$ and $\Phi_\vee(t_{13})$, then t_{12} and t_{13} could be selected, but no distinguishing formula satisfied by t_{11} could be obtained. ■

The criterion for selecting the right t' based on the minimality of its $\Phi_\vee$-set has to take into account a further aspect related to *formulas without disjunctions*. If two derivatives – with different probabilities in the two distributions – have the same formulas without disjunctions in their $\Phi_\vee$-sets, then a distinguishing formula for the two nodes will have disjunctions in it (see Exs. 4 and 6). If the formulas without disjunctions are different between the two $\Phi_\vee$-sets, then one of them will tell the two derivatives apart (see Ex. 3).

A particular instance of the second case is the one in which for each formula without disjunctions in one of the two $\Phi_\vee$-sets there is a variant in the other $\Phi_\vee$-set – i.e., a formula without disjunctions that has the same format but may differ for the values of some probabilistic lower bounds – and vice versa. In this event, *regardless of the minimality* of the $\Phi_\vee$-sets, it has to be selected the derivative such that (i) for each formula without disjunctions in its $\Phi_\vee$-set there exists a variant in the $\Phi_\vee$-set of the other derivative such that the probabilistic lower bounds in the former formula are $\leq$ than the corresponding bounds in the latter formula and (ii) at least one probabilistic lower bound in a formula without disjunctions in the $\Phi_\vee$-set of the selected derivative is $<$ than the corresponding bound in the corresponding variant in the $\Phi_\vee$-set of the other derivative. We say that the $\Phi_\vee$-set of the selected derivative is a $(\leq, <)$*-variant* of the $\Phi_\vee$-set of the other derivative.

Example 8. Let us view the nodes t_5 and t_6 in Fig. 1(c) as derivatives of other nodes, rather than roots of trees. Based on their $\Phi_\vee$-sets shown in Ex. 5, we should focus on t_6 because $\Phi_\vee(t_6)$ contains fewer formulas. However, by so doing, we would be unable to find a distinguishing formula in $\Phi_\vee(t_5)$ that is not satisfied by t_6. Indeed, if we look carefully at the formulas without disjunctions in $\Phi_\vee(t_5)$ and $\Phi_\vee(t_6)$, we note that they differ only for their probabilistic lower bounds: $\langle a\rangle_1 \in \Phi_\vee(t_6)$ is a variant of $\langle a\rangle_1 \in \Phi_\vee(t_5)$, $\langle a\rangle_{0.5}\langle b\rangle_1 \in \Phi_\vee(t_6)$ is a variant of $\langle a\rangle_{0.25}\langle b\rangle_1 \in \Phi_\vee(t_5)$, and $\langle a\rangle_{0.5}\langle c\rangle_1 \in \Phi_\vee(t_6)$ is a variant of $\langle a\rangle_{0.25}\langle c\rangle_1 \in \Phi_\vee(t_5)$. Therefore, we must focus on t_5 because $\Phi_\vee(t_5)$ contains formulas without disjunctions such as $\langle a\rangle_{0.25}\langle b\rangle_1$ and $\langle a\rangle_{0.25}\langle c\rangle_1$ having smaller bounds: $\Phi_\vee(t_5)$ is a $(\leq, <)$-variant of $\Phi_\vee(t_6)$.

Consider now the nodes t_9 and t_{10} in Fig. 1(e), whose $\Phi_\vee$-sets are shown in Ex. 6. If function *hplb* were not used and hence $\Phi_\vee(t_{10})$ also contained $\langle a\rangle_{0.1}\langle b\rangle_1$,

$\langle a\rangle_{0.4}\langle b\rangle_1$, $\langle a\rangle_{0.1}\langle c\rangle_1$, and $\langle a\rangle_{0.4}\langle c\rangle_1$, then the formulas without disjunctions in $\Phi_\vee(t_9)$ would no longer be equal to those in $\Phi_\vee(t_{10})$. More precisely, the formulas without disjunctions would be similar between the two sets, with those in $\Phi_\vee(t_{10})$ having smaller probabilistic lower bounds, so that we would erroneously focus on t_{10}. ■

Summing up, in the $\mathrm{PML}_\vee$ distinguishing formula $\langle a\rangle_{1-(\Delta_{2,a}(t')+p)} \bigvee_{j\in J} \phi'_{2,j}$, the steps for choosing the derivative t', on the basis of which each subformula $\phi'_{2,j}$ is then generated so that it is not satisfied by t' itself, are the following:

1. Consider only derivatives to which $\Delta_{1,a}$ assigns a probability greater than the one assigned by $\Delta_{2,a}$.
2. Within the previous set, eliminate all the derivatives whose $\Phi_\vee$-sets have $(\leq, <)$-variants.
3. Among the remaining derivatives, focus on one of those having a minimal $\Phi_\vee$-set.

Theorem 6. *Let $(T, A, \longrightarrow)$ be in RPT_f and $t_1, t_2 \in T$. Then $t_1 = t_2$ iff $t_1 \models \phi \iff t_2 \models \phi$ for all $\phi \in PML_\vee$. Moreover, if $t_1 \neq t_2$, then there exists $\phi \in PML_\vee$ distinguishing t_1 from t_2 such that $depth(\phi) \leq \max(height(t_1), height(t_2))$.*

4.4 $\mathrm{PML}_\wedge$ Characterizes $\sim_{\mathrm{PB}}$: A Direct Proof for Discrete Systems

By adapting the proof of Thm. 6 consistently with the proof of Thm. 4, we can also prove that $\mathrm{PML}_\wedge$ characterizes $\sim_{\mathrm{PB}}$ by working directly on *discrete* state spaces.

The idea is to obtain $t_1 \models \langle a\rangle_{\Delta_{1,a}(t')+p} \bigwedge_{j\in J} \phi'_{2,j} \not\models t_2$. For any node t of finite height, we define the set $\Phi_\wedge(t)$ of $\mathrm{PML}_\wedge$ formulas satisfied by t featuring, in addition to maximal probabilistic lower bounds and diamonds arising only from transitions of t as for $\Phi_\vee(t)$, conjunctions that (i) stem only from transitions departing from the *same node* in the support of a distribution reached by t and (ii) are preceded by a diamond decorated with the *sum* of the probabilities assigned by that distribution to that node and other nodes with the *same transitions* considered for that node. Given t having transitions of the form $t \xrightarrow{a_i} \Delta_i$ with $supp(\Delta_i) = \{t'_{i,j} \mid j \in J_i\}$ and $i \in I \neq \emptyset$, we let: $\Phi_\wedge(t) = \{\langle a_i\rangle_1 \mid i \in I\} \cup \bigcup_{i\in I} splb(\{\!|\, \langle a_i\rangle_{\Delta_i(t'_{i,j})} \bigwedge_{k\in K'} \phi'_{i,j,k} \mid \emptyset \neq K' \subseteq K_{i,j}, t'_{i,j} \in supp(\Delta_i), \phi'_{i,j,k} \in \Phi_\wedge(t'_{i,j}) \,|\!\})$ where $\{\!|$ and $|\!\}$ are multiset parentheses, $K_{i,j}$ is the index set for $\Phi_\wedge(t'_{i,j})$, and function *splb* merges all formulas possibly differring only for the probabilistic lower bound decorating their initial a_i-diamond by summing up those bounds (such formulas stem from different nodes in $supp(\Delta_i)$).

A good criterion for choosing t' occurring in the $\mathrm{PML}_\wedge$ distinguishing formula at the beginning of this subsection is the *maximality* of the $\Phi_\wedge$-set. Moreover, in that formula J only contains any derivative of the second node different from t' to which the two distributions assign two *different* probabilities, while p is the probability of reaching derivatives having the *same* probability in both distributions that *satisfy* $\bigwedge_{j\in J} \phi'_{2,j}$. Finally, when selecting t', we have to leave out all the derivatives whose $\Phi_\wedge$-sets have $(\leq, <)$-variants.

Theorem 7. *Let* $(T, A, \longrightarrow)$ *be in* RPT_f *and* $t_1, t_2 \in T$. *Then* $t_1 = t_2$ *iff* $t_1 \models \phi \iff t_2 \models \phi$ *for all* $\phi \in PML_\wedge$. *Moreover, if* $t_1 \neq t_2$, *then there exists* $\phi \in PML_\wedge$ *distinguishing* t_1 *from* t_2 *such that* $depth(\phi) \leq \max(height(t_1), height(t_2))$.

5 Conclusions

In this paper, we have studied modal logic characterizations of strong bisimilarity over reactive probabilistic processes. Starting from previous work by Larsen and Skou [12] (who provided a characterization based on a probabilistic extension of Hennessy-Milner logic) and by Desharnais, Edalat, and Panangaden [6] (who showed that negation is not necessary), we have proved that conjunction can be replaced by disjunction without having to reintroduce negation. Thus, in the reactive probabilistic setting, conjunction and disjunction are interchangeable to characterize (bi)simulation equivalence, while they are both necessary for simulation preorder [7]. As a side result, with our proof technique we have provided alternative proofs of the expressiveness of $\mathrm{PML}_{\neg\wedge}$ and $\mathrm{PML}_\wedge$.

The intuition behind our result is that from a conjunctive distinguishing formula it is often possible to derive a disjunctive one by suitably increasing some probabilistic lower bounds. On the model side, this corresponds to summing up the probabilities of reaching certain states that are in the support of a target distribution. In fact, a state of an RPLTS can be given a semantics as a *reactive probabilistic tree*, and hence it is characterized by the countable set of formulas (approximated by the $\Phi_\vee$-set) obtained by doing finite visits of the tree.

On the application side, the $\mathrm{PML}_\vee$-based characterization of bisimilarity over reactive probabilistic processes may help to prove a conjecture in [4]. This work studies the discriminating power of three different testing equivalences respectively using reactive probabilistic tests, fully nondeterministic tests, and nondeterministic and probabilistic tests. Numerous examples lead to conjecture that testing equivalence based on nondeterministic and probabilistic tests may have the same discriminating power as bisimilarity. Given two $\sim_{\mathrm{PB}}$-inequivalent reactive probabilistic processes, the idea of the tentative proof is to build a distinguishing nondeterministic and probabilistic test from a distinguishing $\mathrm{PML}_\wedge$ formula. One of the main difficulties with carrying out such a proof, i.e., the fact that choices within tests fit well together with disjunction rather than conjunction, may be overcome by starting from a distinguishing $\mathrm{PML}_\vee$ formula.

References

1. P. Aczel and N. Mendler. A final coalgebra theorem. In *Proc. of the 3rd Conf. on Category Theory and Computer Science (CTCS 1989)*, volume 389 of *LNCS*, pages 357–365. Springer, 1989.
2. C. Baier and M. Kwiatkowska. Domain equations for probabilistic processes. *Mathematical Structures in Computer Science*, 10:665–717, 2000.
3. M. Barr. Terminal coalgebras in well-founded set theory. *Theoretical Computer Science*, 114:299–315, 1993.

4. M. Bernardo, D. Sangiorgi, and V. Vignudelli. On the discriminating power of testing equivalences for reactive probabilistic systems: Results and open problems. In *Proc. of the 11th Int. Conf. on the Quantitative Evaluation of Systems (QEST 2014)*, volume 8657 of *LNCS*, pages 281–296. Springer, 2014.
5. Y. Deng and H. Wu. Modal characterisations of probabilistic and fuzzy bisimulations. In *Proc. of the 16th Int. Conf. on Formal Engineering Methods (ICFEM 2014)*, volume 8829 of *LNCS*, pages 123–138. Springer, 2014.
6. J. Desharnais, A. Edalat, and P. Panangaden. Bisimulation for labelled Markov processes. *Information and Computation*, 179:163–193, 2002.
7. J. Desharnais, V. Gupta, R. Jagadeesan, and P. Panangaden. Approximating labelled Markov processes. *Information and Computation*, 184:160–200, 2003.
8. R.J. van Glabbeek. The linear time – branching time spectrum I. In *Handbook of Process Algebra*, pages 3–99. Elsevier, 2001.
9. R.J. van Glabbeek, S.A. Smolka, and B. Steffen. Reactive, generative and stratified models of probabilistic processes. *Information and Computation*, 121:59–80, 1995.
10. M. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *Journal of the ACM*, 32:137–162, 1985.
11. B. Jacobs and A. Sokolova. Exemplaric expressivity of modal logics. *Journal of Logic and Computation*, 20:1041–1068, 2010.
12. K.G. Larsen and A. Skou. Bisimulation through probabilistic testing. *Information and Computation*, 94:1–28, 1991.
13. P. Panangaden. Probabilistic bisimulation. In *Advanced Topics in Bisimulation and Coinduction*, pages 300–334. Cambridge University Press, 2011.
14. E.P. de Vink and J.J.M.M. Rutten. Bisimulation for probabilistic transition systems: A coalgebraic approach. *Theoretical Computer Science*, 221:271–293, 1999.
15. J. Worrell. On the final sequence of a finitary set functor. *Theoretical Computer Science*, 338:184–199, 2005.