Compositionality of Probabilistic Hennessy-Milner Logic through Structural Operational Semantics

Daniel Gebler[1] and Wan Fokkink[1,2]
{e.d.gebler,w.j.fokkink}@vu.nl

[1] VU University Amsterdam
[2] Eindhoven University of Technology

Abstract. We present a method to decompose HML formulae for reactive probabilistic processes. This gives rise to a compositional modal proof system for the satisfaction relation of probabilistic process algebras. The satisfaction problem of a probabilistic HML formula for a process term is reduced to the question of whether its subterms satisfy a derived formula obtained via the operational semantics.

1 Introduction

Probabilistic process algebras allow one to specify and reason about both qualitative and quantitative aspects of system behavior [2,5,12,17]. Transition system specifications (TSSs) associate to each process term a labeled transition system (LTS). We consider reactive probabilistic LTSs [22] (essentially Labeled Markov Chains), which are pure probabilistic systems for which the internal nondeterminism (i.e. how does the system react to an action) is fully probabilistic, while the external nondeterminism (i.e. which action label is selected by the environment for the system to perform) is unquantified. Modal logics have been designed to express properties of states in reactive probabilistic LTSs [22].

Larsen and Xinxin [21,23] developed for process languages in the de Simone format [27] a general approach to obtain a compositional proof system for the satisfaction relation of Hennessy-Milner logic (HML) formulae [16]. This technique was extended to TSSs in ready simulation and tyft/tyxt format [11]. We carry over this line of research to reactive probabilistic LTSs. In particular we extend the decomposition method from terms to distributions, as well as to modal operators for probabilistic processes. Thus, we obtain a compositional proof system for a probabilistic version of HML [24]. Moreover, the decomposition developed in this paper provides a basis for investigating connections between behavioral semantics, modal characterizations and structural operational semantics of probabilistic systems. In particular, it opens the door to deriving expressive and elegant congruence formats for probabilistic semantics in a structured way, following the approach of [6].

We develop a number of proof-theoretic facts for probabilistic TSSs. In detail, we provide an extension of proofs for probabilistic TSSs [20] to support the

derivation that a transition does not hold. Furthermore, we construct a collection of derived rules, called ruloids [7], that determine completely the behavior of each open term. Transition rules of probabilistic TSSs can be partitioned such that every partition allows to derive transitions of a total probability of 1 and different partitions are mutually exclusive [20]. We show that this partitioning can be lifted to ruloids. This fact is a corner stone of our compositional proof systems for probabilistic HML. Ruloids and ruloid partitions are used to decompose the diamond modality.

2 Preliminaries

In probabilistic labeled transition systems, transitions carry probabilities. We consider reactive probabilistic systems where each state is required to be semi-stochastic, i.e. the sum of the probabilities of all outgoing transitions for an action is either 0 (action cannot be performed) or 1 (fully quantified dynamic behavior). $Dist(S)$ is the set of probability measures on a countable set S, i.e. all functions $\mu \in S \to [0,1]$ with $\sum_{s \in S} \mu(s) = 1$. Let $\mu(T) = \sum_{s \in T} \mu(s)$ for $T \subseteq S$; $Supp(\mu) = \{s \in S \mid \mu(s) > 0\}$ denotes the support of μ; δ_s for $s \in S$ is the Dirac distribution with $\delta_s(s) = 1$ and $\delta_s(s') = 0$ for $s' \neq s$. $\{\!|$ and $|\!\}$ denotes multisets.

Definition 1. *A* probabilistic labeled transition system (PLTS) *is a tuple $\mathcal{M} = (S, Act, I, \to)$, with S a set of states, Act a set of actions, I a set of indices, and $\to \subseteq S \times Act \times (0,1] \times I \times S$, where for each $s \in S, a \in Act$,*

$$\sum \{\!| \, p \mid \exists i \in I, s' \in S : (s, a, p, i, s') \in \to |\!\} \in \{0, 1\}$$

$s \xrightarrow{a,p}_i s'$ denotes $(s, a, p, i, s') \in \to$, and $d(s, a) \in Dist(S)$ the measure with $d(s, a)(s') = \sum \{\!| \, p \mid \exists i \in I : s \xrightarrow{a,p}_i s' |\!\}$. Let $s \xrightarrow{a} \mu$ denote that the system evolves from state s by action a to distribution $\mu = d(s, a)$.

The first logical characterization of probabilistic bisimilarity for fully probabilistic reactive systems was provided in [22]. This logic is derived from Hennessy-Milner logic (HML) by decorating the diamond operator with a probability. It was generalized to the probabilistic modal logic L^N [24] for nondeterministic probabilistic systems (probabilistic automata). In the following we use this logic.

Definition 2. *[24] The syntax of probabilistic HML is:*

$$\varphi ::= \top \mid \neg\varphi \mid \bigwedge_{j \in J} \varphi_j \mid \langle a \rangle \varphi \mid [\varphi]_p$$

with $p \in [0,1]$, J a countable index set, and $a \in Act$. Let $\mathbb{O}$ denote the set of probabilistic HML formulae.

Definition 3. *[24] Let $\mathcal{M} = (S, Act, I, \to)$ be a PLTS. The satisfaction relation of probabilistic HML formulae $\models \subseteq Dist(S) \times \mathbb{O}$ is defined as follows:*

- *$\mu \models \top$ for each measure μ*

- $\mu \models \neg\varphi$ *iff* $\mu \not\models \varphi$
- $\mu \models \bigwedge_{j\in J} \varphi_j$ *iff* $\mu \models \varphi_j$ *for each* $j \in J$
- $\mu \models \langle a\rangle\varphi$ *iff for each* $s \in Supp(\mu)$ *there is a* $\nu \in Dist(S)$ *with* $s \xrightarrow{a} \nu$ *and* $\nu \models \varphi$
- $\mu \models [\varphi]_p$ *iff* $\mu(\{s \in S \mid \delta_s \models \varphi\}) \geq p$

We write $s \models \varphi$ for $\delta_s \models \varphi$.

Structural operational semantics (SOS) is defined by a transition system specification (TSS), which induces an LTS whose states are closed terms over an algebraic signature. Transitions are obtained inductively from the transition rules of the TSS. For a signature Σ and an infinite set of variables Var, $\mathbb{T}(\Sigma, Var)$ denotes the set of open Σ-terms over variables Var, and $T(\Sigma)$ the set of closed Σ-terms. Substitutions $\sigma : Var \to \mathbb{T}(\Sigma, Var)$ are extended to open Σ-terms as usual. Let $var(t)$ denote the set of variables in Σ-term t. Following [1], we develop separately the concepts of literals, rules and proofs, to emphasize the required probabilistic extensions to generate well-formed PLTSs. Labels are either pairs of an action and a probability denoting that the action can be executed with the given probability, or sets of actions denoting that all actions in the set can (or cannot) be executed with an unquantified probability.

Definition 4. *Let* $t, t' \in \mathbb{T}(\Sigma, Var)$*. A probabilistic* Σ*-literal is an expression* $t \xrightarrow{a,\pi}_\iota t'$ *(positive probabilistic* Σ*-literal),* $t \xrightarrow{B}$ *(positive unquantified* Σ*-literal) or* $t \xrightarrow{C}\!\!\!\!\!\!/\;\;$ *(negative unquantified* Σ*-literal), with* $a \in Act$ *and* $B, C \subseteq Act$*. In an open positive probabilistic* Σ*-literal, not only* t *and* t' *are open terms, but also* π *is a linear function on variables ranging over* $(0, 1]$*, and* ι *is a variable ranging over* $\mathcal{I}$*. A* Σ*-literal is closed if* $t, t' \in T(\Sigma)$*,* $\pi \in (0, 1]$ *and* $\iota \in \mathcal{I}$*.*

A positive Σ-literal is either a positive probabilistic Σ-literal or a positive unquantified Σ-literal. An unquantified Σ-literal is either a positive or negative unquantified Σ-literal. Subscript ι allows to distinguish different occurrences of the same probabilistic transition [15]. Subscripts are omitted if they are clear from the context. We say literal for Σ-literal if Σ is clear from the context.

Definition 5. *A probabilistic transition rule is of the form* $r = \frac{H}{t \xrightarrow{a,\pi}_\iota t'}$ *with* H *a set of open* Σ*-literals, called premises, and* $t \xrightarrow{a,\pi}_\iota t'$ *an open positive probabilistic* Σ*-literal, called the conclusion. We call* t *the source and* t' *the target, and write* $premises(r) = H$*,* $conc(r) = t \xrightarrow{a,\pi}_\iota t'$*,* $action(r) = a$*,* $index(r) = \iota$*,* $source(r) = t$ *and* $target(r) = t'$*.*

Open positive probabilistic and negative unquantified Σ-literals are called active resp. negative premises in [20]; open positive unquantified Σ-literals are called unquantified premises in [20] and move premises in [28].

A probabilistic TSS (PTSS) consists of a signature Σ, set of actions Act, and set of probabilistic transition rules R.

Definition 6. *[20] A reactive probabilistic transition rule r, for $f \in \Sigma$ and $a \in Act$, is of the form*

$$\frac{\{x_k \xrightarrow{a_k,\pi_k}_{\iota_k} y_k \mid k \in K\} \quad \{x_l \xrightarrow{B_l}| \mid l \in L\} \quad \{x_m \not\xrightarrow{C_m}| \mid m \in M\}}{f(x_1,\ldots,x_n) \xrightarrow{a,\pi}_{\iota} t}$$

with $t \in \mathbb{T}(\Sigma, \{x_1,\ldots,x_n\} \cup \{y_k \mid k \in K\})$, $K, L, M \subseteq \{1,\ldots,ar(f)\}$, for all $k \in K, l \in L, m \in M$, $a_k \in Act$, $B_l, C_m \subseteq Act$, π_k are variables ranging over $(0,1]$, ι_k are variables ranging over $\mathcal{I}$, $w_r \in (0,1]$, $\pi = w_r * \prod_{k\in K} \pi_k$ and $\iota = (r, [\iota_k]_{k\in K})$. We denote $weight(r) = w_r$, $pppremises(r) = \{x_k \xrightarrow{a_k,\pi_k}_{\iota_k} y_k \mid k \in K\}$, $pupremises(r) = \{x_l \xrightarrow{B_l} \mid l \in L\}$, $nupremises(r) = \{x_m \not\xrightarrow{C_m} \mid m \in M\}$, $var(r) = \{x_1,\ldots,x_n\} \cup \{y_k \mid k \in K\} \cup var(t)$.

We assume that the set of indices $\mathcal{I}$ is totally ordered and closed under building pairs of a rule name and a list of indices, i.e. for every rule r with positive probabilistic literals $\{x_k \xrightarrow{a_k,\pi_k}_{\iota_k} y_k \mid k \in K\}$ with $\iota_k \in \mathcal{I}$, we have $(r, [\iota_k]_{k\in K}) \in \mathcal{I}$. The weight of a rule defines the conditional probability of the conclusion, assuming that all premises hold. We define the operator $unquant(t \xrightarrow{a,\pi} t') = t \xrightarrow{\{a\}}$ that eliminates the quantification and the target term from a positive probabilistic literal and is identity for unquantified literals. It lifts in a natural way to sets of literals. Furthermore, for a set of literals H, the normalized set of literals is defined by merging actions of unquantified literals with equal source, i.e. $norm(H) = \{t \xrightarrow{a,\pi} t' \mid t \xrightarrow{a,\pi} t' \in H\} \cup \{t \xrightarrow{\hat{B}} \mid t \in \mathbb{T}(\Sigma, Var), \hat{B} = \cup_{t \xrightarrow{B} \in H} B, \hat{B} \neq \emptyset\} \cup \{t \not\xrightarrow{\hat{C}} \mid t \in \mathbb{T}(\Sigma, Var), \hat{C} = \cup_{t \not\xrightarrow{C} \in H} C, \hat{C} \neq \emptyset\}$.

A PTSS guarantees congruence of probabilistic bisimilarity [20]. A PTSS is well-formed if its induced PLTS satisfies the semi-stochasticity property. The following specification format ensures well-formedness. It is defined using rule partitions that describe sets of rules for which a given process either allows that from each rule a transition can be derived (premises of all rules are satisfied) or no transition can be derived (none of the premises is satisfied) and the rule weights sum up to a total probability mass of 1. The format is a mild relaxation of [20, Def. 7.2] by not enforcing equality of positive unquantified premises of rules in a partition, but only equality of positive premises irrespective of its quantification. This allows for more compact rules, without semantically redundant positive unquantified premises just to enforce the partitioning.

Definition 7. *[20] In a PTSS (Σ, Act, R), the set $R^{f,a}$ of reactive probabilistic transition rules for $f \in \Sigma$ and $a \in Act$, is partitioned into sets $R_1^{f,a}, \ldots, R_n^{f,a}$ such that the following conditions hold:*

1. *For each set $R_u^{f,a}$:*
   (a) *For each pair $r_1, r_2 \in R_u^{f,a}$ we have $norm(unquant(pppremises(r_1)) \cup pupremises(r_1)) = norm(unquant(pppremises(r_2)) \cup pupremises(r_2))$.*
   (b) *For each pair $r_1, r_2 \in R_u^{f,a}$ we have $nupremises(r_1) = nupremises(r_2)$.*
   (c) *The sum of weights of rules in $R_u^{f,a}$ is 1.*

2. *Given two sets $R_u^{f,a} \neq R_v^{f,a}$. For any rules $r_u \in R_u^{f,a}$ and $r_v \in R_v^{f,a}$ there is an index $1 \leq i \leq ar(f)$ such that r_u has a positive premise $x_i \xrightarrow{a_i,\pi_i}_{\iota_i} y_i$ or $x_i \xrightarrow{B_i}$ and r_v has a negative premise $x_i \not\xrightarrow{C_i}$ with $a_i \in C_i$ or $C_i \cap B_i \neq \emptyset$, respectively, or vica versa.*

1(a) and 1(b) ensure that either none or all rules of a partition can be applied, and 2 that only rules from one single partition can be applied. By 1(c), induced PLTSs satisfy the semi-stochasticity property [20, Thm. 7.8].

Example 1. If t_1 can perform an a-transition to t_1' with probability p_1 and t_2 to t_2' with probability p_2, their probabilistic alternative composition $t_1 +^p t_2$ can perform an a-transitions to t_1' with probability $p_1 * p$ and to t_2' with probability $p_2 * (1-p)$. If only one of the processes can perform an a-transition and this transition goes to t' with probability p', then $t_1 +^p t_2$ can perform an a-transition to t' with probability p'.

$$(r_a^{+1})\ \frac{x_1 \xrightarrow{a,\pi_1}_\iota y_1 \quad x_2 \xrightarrow{\{a\}}}{x_1 +^p x_2 \xrightarrow{a,\pi_1 * p}_{(r_a^{+1},\iota)} y_1} \qquad \frac{x_2 \xrightarrow{a,\pi_2}_\iota y_2 \quad x_1 \xrightarrow{\{a\}}}{x_1 +^p x_2 \xrightarrow{a,\pi_2 * (1-p)}_{(r_a^{+2},\iota)} y_2}\ (r_a^{+2})$$

$$(r_a^{+3})\ \frac{x_1 \xrightarrow{a,\pi_1}_\iota y_1 \qquad x_2 \not\xrightarrow{\{a\}}}{x_1 +^p x_2 \xrightarrow{a,\pi_1}_{(r_a^{+3},\iota)} y_1} \qquad \frac{x_2 \xrightarrow{a,\pi_2}_\iota y_2 \qquad x_1 \not\xrightarrow{\{a\}}}{x_1 +^p x_2 \xrightarrow{a,\pi_2}_{(r_a^{+4},\iota)} y_2}\ (r_a^{+4})$$

Rules r_a^{+1} to r_a^{+4} for operator $+$ and action a specify a PTSS with partitions $R_1^{+,a} = \{r_a^{+1}, r_a^{+2}\}$, $R_2^{+,a} = \{r_a^{+3}\}$ and $R_3^{+,a} = \{r_a^{+4}\}$. We note that the original rule format of [20, Def. 7.2] would require additionally the premises $x_1 \xrightarrow{\{a\}}$ in r_a^{+1} and $x_2 \xrightarrow{\{a\}}$ in r_a^{+2}. ■

Derivations are defined as inductive applications of closed transition rules. Negative literals are proved using the negation as failure principle [9] and the supported proof notion [13, Def. 8].

Definition 8. *[20] Let $P = (\Sigma, Act, R)$ be a PTSS and $t, s \in T(\Sigma)$. A closed Σ-literal $t \xrightarrow{a,p}_i s$ is derivable, denoted by $P \vdash t \xrightarrow{a,p}_i s$, if there is a closed substitution instance*

$$\frac{\{t_k \xrightarrow{a_k,p_k}_{i_k} s_k \mid k \in K\} \quad \{t_l \xrightarrow{B_l} \mid l \in L\} \quad \{t_m \not\xrightarrow{C_m} \mid m \in M\}}{t \xrightarrow{a,p}_i s}$$

of a rule $r \in R$, $p = w_r * \prod_{k \in K} p_k$ and $i = (r, [i_k]_{k \in K})$ such that

- *for all $k \in K$, $P \vdash t_k \xrightarrow{a_k,p_k}_{i_k} s_k$*
- *for all $l \in L$ and for all $b_l \in B_l$, $P \vdash t_l \xrightarrow{b_l,p_l}_{i_l} u_l$ for some p_l, i_l, u_l*

– *for all* $m \in M$ *and for all* $c_m \in C_m$, $P \not\vdash t_m \xrightarrow{c_m, p_m}_{i_m} u_m$ *for all* p_m, i_m, u_m.

$P \not\vdash t \xrightarrow{a,p}_i u$ *denotes there is no derivation of this transition.*

$P \vdash t \overset{a}{\not\to}$ denotes there are no p, i, s such that $P \vdash t \xrightarrow{a,p}_i s$. By $P \vdash t \xrightarrow{B}$ we denote that for all $b \in B$ there are some p, s such that $P \vdash t \xrightarrow{b,p} s$. By $P \vdash t \overset{C}{\not\to}$ we denote that $P \vdash t \overset{c}{\not\to}$ for all $c \in C$. We write $P \vdash t \xrightarrow{a,p} s$ if there is a rule r and a list of indices $[i_k]_{k \in K}$ such that $P \vdash t \xrightarrow{a,p}_{(r,[i_k]_{k\in K})} s$.

We say that literals $t \xrightarrow{a,p} s$ and $t \overset{a}{\not\to}$ deny each other. A proof system is consistent if it does not admit proofs of literals denying each other. Consistency of Def. 8 can be shown similar to consistency of the well-supported proof notion for nondeterministic TSSs [13]. A TSS is complete if for any $t \in T(\Sigma)$ either $P \vdash t \xrightarrow{a,p} s$ for some $s \in T(\Sigma)$ and $p \in (0, 1]$ or $P \vdash t \overset{a}{\not\to}$. PTSSs are GSOS-type TSSs [7], which guarantees the existence of a strict finite stratification [13]. Stratifiability of a PTSS is a sufficient condition for completeness.

3 Decomposition of Modal Formulae

This section shows how to decompose probabilistic HML formulae wrt. distributions over process terms. Section 3.1 constructs ruloids that are derived rules describing completely the set of provable literals of a PTSS. Furthermore, the partitioning of rules to ensure the semi-stochasticity property is lifted to ruloids. Section 3.2 provides the decomposition method for probabilistic HML formulae.

3.1 Ruloids and Ruloid Partitioning

Ruloids are derived transition rules describing completely the behavior of open terms [7]. Intuitively, they are compact proofs where intermediate proof steps are removed. While the source can be any term, the premises are simple and consist of only variables. Their proof-theoretical closure property (Thm. 1) gives them a prominent role in decomposing modalities.

The construction of ruloids is motivated by [7, Def. 7.4.2 and Thm. 7.4.3] and its reformulation in [14, Def. 14]. We prefer the constructive approach of the latter reference, which separates the definition of ruloids from the proof of their properties. Ruloids are constructed inductively by composing rules. The base case is defined by rules being ruloids. A ruloid ρ is constructed by taking an instance of a rule r and acting for each premise α as follows: If α is a positive literal, then a ruloid ρ_α with conclusion α is selected, and all premises of ρ_α are included in the premise of ρ. If α is a negative literal, then for every ruloid with conclusion being negated α, one of its premises is negated and included in the premises of ρ.

Literals(P) denotes the set of literals of PTSS P, and $RHS(r)$ the set of right-hand side variables of positive probabilistic premises of ruloid ρ. Just like rules the conclusion of a ruloid is indexed by a pair consisting of the ruloid name and a list of indices of the positive probabilistic premises. The ruloid name is

the concatenation of the rule name and the ruloid names applied to its positive premises.

Definition 9. *Let $P = (\Sigma, Act, R)$ be a PTSS. The set of P-ruloids $\mathcal{R}$ is the smallest set such that:*

- $\dfrac{x \xrightarrow{a,\pi}_{\iota} y}{x \xrightarrow{a,\pi}_{\iota} y}$ *is a P-ruloid with weight 1 for $x, y \in Var$, $a \in Act$, π a variable ranging over $(0,1]$ and ι a variable ranging over $\mathcal{I}$.*

- $$\frac{norm(\bigcup_{k\in K} H_k \ \cup \ \bigcup_{l\in L} H_l \ \cup \ \bigcup_{m\in M} H_m)}{\sigma(f(x_1,\ldots,x_n)) \xrightarrow{a,\pi}_{\iota} \sigma(t)}$$

  is a P-ruloid with weight $w = w_r * \prod_{k\in K} w_k$, transition probability $\pi = w * \prod_{k\in K} \prod_{k'\in K_k} \pi_{k,k'}$, rules $rs = r \cdot [\rho_k]_{k\in K} \cdot [\rho_l]_{l\in L}$ and index $\iota = (rs, [\iota_{k,k'}]_{k\in K, k'\in K_k})$ if there is a rule r

$$\frac{\{x_k \xrightarrow{a_k,\pi_k}_{\iota_k} y_k \mid k \in K\} \quad \{x_l \xrightarrow{B_l} \mid l \in L\} \quad \{x_m \not\xrightarrow{C_m} \mid m \in M\}}{f(x_1,\ldots,x_n) \xrightarrow{a, w_r * \prod_{k\in K} \pi_k}_{(r,[\iota_k]_{k\in K})} t}$$

  in R, and a substitution σ, such that the following properties hold:

  - *For every positive probabilistic literal $x_k \xrightarrow{a_k,\pi_k}_{\iota_k} y_k$, either*
    - *$\sigma(x_k)$ and $\sigma(y_k)$ are variables and $H_k = \{\sigma(x_k) \xrightarrow{a_k,\pi_k}_{\iota_k} \sigma(y_k)\}$, or*
    - *there is a P-ruloid $\rho_k = \dfrac{H_k}{\sigma(x_k) \xrightarrow{a_k,\pi_k}_{\iota_k} \sigma(y_k)}$ with weight w_k, the positive probabilistic premises in H_k are indexed by K_k and have probabilistic variables $\pi_{k,k'}$ and index variables $\iota_{k,k'}$ with $k' \in K_k$.*
  - *For every positive unquantified literal $x_l \xrightarrow{B_l}$, either*
    - *$\sigma(x_l)$ is a variable and $H_l = \{\sigma(x_l) \xrightarrow{B_l}\}$, or*
    - *for all $b \in B_l$ there is a P-ruloid $\rho_b = \dfrac{H_b}{\sigma(x_l) \xrightarrow{b,\pi_b} s}$ for some π_b, s and $H_l = \cup_{b\in B_l} unquant(H_b)$, $\rho_l = [\rho_b]_{b\in B_l}$.*
  - *For every negative unquantified literal $x_m \not\xrightarrow{C_m}$, either*
    - *$\sigma(x_m)$ is a variable and $H_m = \{\sigma(x_m) \not\xrightarrow{C_m}\}$, or*
    - *$H_m = neg_{C_m}(h_{C_m}(R_{C_m}))$ with*
      - *Define $\mathcal{R}_{C_m} = \{premises(\rho) \mid \rho \in \mathcal{R}, conc(\rho) = \sigma(x_m) \xrightarrow{c,\pi_c} s, c \in C_m\}$ the set of premises of all P-ruloids with conclusion $\sigma(x_m) \xrightarrow{c,\pi_c} s$ for some $c \in C_m$, π_c, s.*
      - *Define any mapping $h_{C_m} : \mathcal{R}_{C_m} \to Literals(P)$ by $h_{C_m}(L) = l$ with $l \in L$ for $L \in \mathcal{R}_{C_m}$.*
      - *Define any mapping $neg_{C_m} : Literals(P) \to Literals(P)$ that satisfies $neg_{C_m}(x \xrightarrow{a,\pi} y) = x \not\xrightarrow{\{a\}}$, $neg_{C_m}(x \xrightarrow{A}) = x \not\xrightarrow{\{a\}}$ for some $a \in A$ and $neg_{C_m}(x \not\xrightarrow{A}) = x \xrightarrow{\{a\}}$ for some $a \in A$.*

- *Right-hand side variables $RHS(\rho_k)$ are all pairwise disjoint and each $RHS(\rho_k)$ is disjoint with $\{x_1, \ldots, x_n\}$. All probabilistic variables $\pi_{k,k'}$ and index variables $\iota_{k,k'}$ are distinct.*

The ruloid construction for unquantified literals, i.e. the mapping $unquant(H_b)$ for positive unquantified literals and neg_{C_m} for negative unquantified literals, prevents that new probabilistic variables are introduced that would modify the probabilistic weight of the ruloid. Operators denoting parameters of rules like *premises*, *conc*, *source* carry over to ruloids. Furthermore, the rules applied to a ruloid ρ are denoted by $rules(\rho) = r \cdot [\rho_k]_{k \in K} \cdot [\rho_l]_{l \in L}$. The set of P-ruloids for a term $t \in \mathbb{T}(\Sigma, Var)$ and action $a \in Act$ is denoted by $\mathcal{R}^{t,a} = \{\rho \mid \rho \in \mathcal{R}, source(\rho) = t, action(\rho) = a\}$.

Example 2. Let $P = (\Sigma, Act, R)$ be the PTSS from Example 1. Consider the probabilistic summation $(x_1 +^{p_{12}} x_2) +^{p_{23}} x_3$, where only x_3 is able to perform an a-transition. The construction tree of the ruloid is as follows:

$$\dfrac{\dfrac{x_1 \overset{\{a\}}{\not\longrightarrow} \qquad x_2 \overset{\{a\}}{\not\longrightarrow}}{x_1 +^{p_{12}} x_2 \overset{\{a\}}{\not\longrightarrow} \qquad x_3 \xrightarrow{a,\pi_3}_{\iota} y_3}\ (1)}{(x_1 +^{p_{12}} x_2) +^{p_{23}} x_3 \xrightarrow{a,\pi_3}_{(\rho_a^{+4},\iota)} y_3}\ (2)$$

At (1) the rules ρ_a^{+1} to ρ_a^{+4} were applied to assure $x_1 +^{p_{12}} x_2 \overset{\{a\}}{\not\longrightarrow}$ by disproving $x_1 +^{p_{12}} x_2 \xrightarrow{\{a\}}$. In fact, the mapping h_{C_m} selects for each rule to disprove one literal from its premise and neg_{C_m} generates the literal which refutes it. The resulting ruloid is:

$$\dfrac{x_1 \overset{\{a\}}{\not\longrightarrow} \qquad x_2 \overset{\{a\}}{\not\longrightarrow} \qquad x_3 \xrightarrow{a,\pi_3}_{\iota} y_3}{(x_1 +^{p_{12}} x_2) +^{p_{23}} x_3 \xrightarrow{a,\pi_3}_{(\rho_a^{+4},\iota)} y_3}$$

■

The following theorem states the key property of ruloids (called soundness and specifically witnessing property in [7]). It formalizes a kind of completeness property of the form that every transition that can be proven from P has a corresponding P-ruloid where the provable transition is an instance of the conclusion of the P-ruloid. This shows that ruloids are exhaustive wrt. provable transitions. This will be used to decompose the diamond modality over an action a by providing a complete logical characterization of the preconditions and effects of the possible transitions with label a.

Theorem 1 (Ruloid theorem). *Let $P = (\Sigma, Act, R)$ be a PTSS. Then $P \vdash \sigma(t) \xrightarrow{a,p} u$ for $t \in \mathbb{T}(\Sigma, Var)$, $u \in T(\Sigma)$ and σ a closed substitution, iff there is a P-ruloid $\frac{H}{t \xrightarrow{a,p} v}$ and a closed substitution σ' with $P \vdash \sigma'(\alpha)$ for all $\alpha \in H$, $\sigma'(t) = \sigma(t)$ and $\sigma'(v) = u$.*

Next we construct the partitioning of ruloids. Intuitively, the partitioning of a set of ruloids is defined as lifting of the partitionings of the rules involved in their construction. The partitioning of ruloids with variables or terms with only one function symbol in the source handles explicitly α-equivalence. The partitioning of ruloids with source $t = f(t_1, \ldots, t_n)$ with at least one t_i being no variable handles α-equivalence indirectly by referring to the partitioning of rules involved in the construction. Like rule partitions, the ruloid partitions are well-formed under an adapted notion of derivability. This is required for the decomposition of the modalities.

Definition 10. *Let $P = (\Sigma, Act, R)$ be a PTSS, $t \in \mathbb{T}(\Sigma, Var)$ and $a \in Act$. The partitioning of ruloids $\mathcal{R}^{t,a}$ is defined by:*

- *$t = x$: There is one ruloid partition $\left\{ \begin{smallmatrix} x \xrightarrow{a,\pi}_\iota y \\ x \xrightarrow{a,\pi}_\iota y \end{smallmatrix} \mid y \in Var \right\}$.*
- *$t = f(x_1, \ldots, x_n)$: For every rule partition $R_u^{f,a}$ there is a ruloid partition $\mathcal{R}_u^{f(x_1,\ldots,x_n),a} = \{\sigma(r) \mid r \in R_u^{f,a}, \sigma$ a variable subsitution, $\sigma(x_i) = x_i$ for $1 \leq i \leq n\}$.*
- *$t = f(t_1, \ldots, t_n)$, some t_i is no variable: $\rho_1, \rho_2 \in \mathcal{R}_u^{t,a}$ iff $rules(\rho^1) = r^1 \cdot [\rho_k^1]_{k \in K^1} \cdot [\rho_l^1]_{l \in L^1}$, $rules(\rho^2) = r^2 \cdot [\rho_k^2]_{k \in K^2} \cdot [\rho_l^2]_{l \in L^2}$, for some v we have $r^1, r^2 \in R_v^{f,a}$ and for each $i \in K^1 \cup L^1$ we have $\rho_i^1, \rho_i^2 \in \mathcal{R}_{u_i}^{t_i,a_i}$ for some u_i.*

The ruloid partitioning of a term is fully defined by the ruloid partitionings of its subterms and the rule partitioning of its outermost function symbol. Note that for case $t = f(t_1, \ldots, t_n)$ the rule partitioning (Def. 7.1a) guarantees that $K^1 \cup L^1 = K^2 \cup L^2$. The ruloid partitions $\mathcal{R}_u^{f(x_1,\ldots,x_n),a}$ are the rule partitions $R_u^{f,a}$ including renaming of variables that are not used in the source.

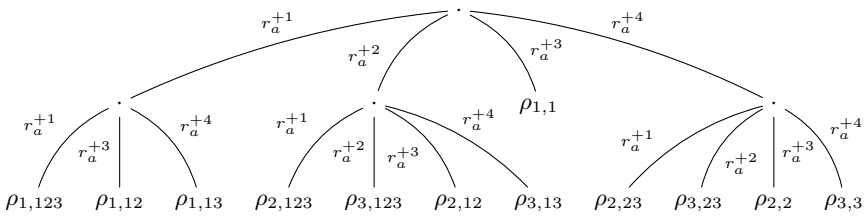

Figure 1. Ruloid derivations for the 3-fold probabilistic sum

Example 3. $t = x_1 +^{p_{12}} (x_2 +^{p_{23}} x_3)$ generates 12 ruloids (up to α-equivalence and variants generated by negative unquantified premises). The derivation tree in Fig. 1 shows the deduction of ruloids by rule concatenation. Ruloid names denote in the first parameter the target variable and in the second parameter which variables can perform an a-move. E.g., ruloid $\rho_{1,12}$ denotes that the target is y_1 and that x_1, x_2 can move but not x_3. The 4 ruloids with target y_3 are:

$$\frac{x_1 \xrightarrow{\{a\}} \quad x_2 \xrightarrow{\{a\}} \quad x_3 \xrightarrow{a,\pi_3}_{\iota} y_3}{x_1 +^{p_{12}} (x_2 +^{p_{23}} x_3) \xrightarrow[(r_a^{+2} r_a^{+3},\iota)]{a,\pi_3*(1-p_{12})(1-p_{23})} y_3}\ (\rho_{3,123})$$

$$\frac{x_1 \not\xrightarrow{\{a\}} \quad x_2 \xrightarrow{\{a\}} \quad x_3 \xrightarrow{a,\pi_3}_{\iota} y_3}{x_1 +^{p_{12}} (x_2 +^{p_{23}} x_3) \xrightarrow[(r_a^{+4} r_a^{+2},\iota)]{a,\pi_3*(1-p_{23})} y_3}\ (\rho_{3,23})$$

$$\frac{x_1 \xrightarrow{\{a\}} \quad x_2 \not\xrightarrow{\{a\}} \quad x_3 \xrightarrow{a,\pi_3}_{\iota} y_3}{x_1 +^{p_{12}} (x_2 +^{p_{23}} x_3) \xrightarrow[(r_a^{+2} r_a^{+4},\iota)]{a,\pi_3*(1-p_{12})} y_3}\ (\rho_{3,13})$$

$$\frac{x_1 \not\xrightarrow{\{a\}} \quad x_2 \not\xrightarrow{\{a\}} \quad x_3 \xrightarrow{a,\pi_3}_{\iota} y_3}{x_1 +^{p_{12}} (x_2 +^{p_{23}} x_3) \xrightarrow[(r_a^{+4} r_a^{+4},\iota)]{a,\pi_3} y_3}\ (\rho_{3,3})$$

Ruloids with target y_1 or y_2 are constructed similarly. Table 1 shows all ruloid partitions of the 3-fold probabilistic sum. The weights of every ruloid partition sum up to 1. E.g., ruloid partition $[R_1^{+,a}, R_1^{+,a}]$ with ruloids $\{\rho_{1,123}, \rho_{2,123}, \rho_{3,123}\}$ has weight $p_{12} + (1-p_{12})p_{23} + (1-p_{12})(1-p_{23}) = 1$. There are 12 ruloids for $x_1 +^{p_{12}} (x_2 +^{p_{23}} x_3)$, because 3 of the 4 rules of P have a positive literal on x_2 which can be instantiated by the 4 rules specifying the probabilistic sum. ■

Partition	Ruloids	Ruloid weights
$[R_1^{+,a}, R_1^{+,a}]$	$\{\rho_{1,123}, \rho_{2,123}, \rho_{3,123}\}$	$\mathit{weight}(\rho_{1,123}) = p_{12}$
		$\mathit{weight}(\rho_{2,123}) = (1-p_{12})p_{23}$
		$\mathit{weight}(\rho_{3,123}) = (1-p_{12})(1-p_{23})$
$[R_1^{+,a}, R_2^{+,a}]$	$\{\rho_{1,12}, \rho_{2,12}\}$	$\mathit{weight}(\rho_{1,12}) = p_{12},\ \mathit{weight}(\rho_{2,12}) = 1-p_{12}$
$[R_1^{+,a}, R_3^{+,a}]$	$\{\rho_{1,13}, \rho_{3,13}\}$	$\mathit{weight}(\rho_{1,13}) = p_{12},\ \mathit{weight}(\rho_{3,13}) = 1-p_{12}$
$[R_2^{+,a}]$	$\{\rho_{1,1}\}$	$\mathit{weight}(\rho_{1,1}) = 1$
$[R_3^{+,a}, R_1^{+,a}]$	$\{\rho_{2,23}, \rho_{3,23}\}$	$\mathit{weight}(\rho_{2,23}) = p_{23},\ \mathit{weight}(\rho_{3,23}) = 1-p_{23}$
$[R_3^{+,a}, R_2^{+,a}]$	$\{\rho_{2,2}\}$	$\mathit{weight}(\rho_{2,2}) = 1$
$[R_3^{+,a}, R_3^{+,a}]$	$\{\rho_{3,3}\}$	$\mathit{weight}(\rho_{3,3}) = 1$

Table 1. Ruloid partitions for the 3-fold probabilistic sum

We define $[\rho]_\alpha = \{\rho' \mid \mathit{rules}(\rho) = \mathit{rules}(\rho')\}$, the ruloid equivalence class containing all ruloids that were constructed by the same rules applied in the same order as ρ. This set contains beside ρ all those ruloids which differ from ρ only by α-equivalence (renaming) or by the selection of premises of rules to refute in the construction of negative unquantified literals. All ruloids in $[\rho]_\alpha$ have equal weight. The weight of $[\rho]_\alpha$ is defined to be $\mathit{weight}(\rho')$ for any $\rho' \in [\rho]_\alpha$. The weight of a set of ruloids R is defined as $\sum_{\varrho \in [R]_\alpha} \mathit{weight}(\varrho)$.

Well-formedness of rule partitions was proved in [20]. The following theorem shows well-formedness of ruloid partitions. A set of transitions is derivable from a ruloid partition $\mathcal{R}_u^{t,a}$ if each transition is derivable from a ruloid $\rho \in \mathcal{R}_u^{t,a}$ and different transitions $t \xrightarrow{a,p_1} t_1$ derived from ρ_1 and $t \xrightarrow{a,p_2} t_2$ derived from ρ_2 are derived from ruloids of different equivalence classes $[\rho_1]_\alpha \neq [\rho_2]_\alpha$.

Theorem 2 (Well-formedness of ruloid partitions). *Let $P = (\Sigma, Act, R)$ be a PTSS, $t \in \mathbb{T}(\Sigma, Var)$ a term and $\sigma : var(t) \to T(\Sigma)$ a closed substitution. If for each $x_i \in var(t)$ and $a_i \in Act$ the probability of transitions of $\sigma(x_i)$ with label a_i, if there are any, sum up to 1, then for each $a \in Act$ the probability of transitions of $\sigma(t)$ derivable from any ruloid partition $\mathcal{R}_u^{t,a}$, if there are any, sum up to* 1.

3.2 Decomposition of HML Formulae

We present a method to reduce the question whether a probability distribution over process terms satisfies a formula φ to the question whether its subterms satisfy one of those formulae obtained by decomposing the formula φ using the SOS rules of the process algebra. A formula φ is decomposed wrt. a distribution μ in multiple mappings $\psi : Var \to \mathbb{O}$ (Def. 11) such that for each closed substitution $\sigma : Var \to T(\Sigma)$ there is one mapping ψ such that for each variable x of a term in the support of μ its instance $\sigma(x)$ satisfies the decomposed formula $\psi(x)$ (Thm. 3).

The decomposition of propositional connectives is from [6,11]. The decomposition of $\neg\varphi$ expresses that none of the decompositions of φ hold. The decomposition of $\langle a \rangle \varphi$ wrt. distribution μ states that for each term t in the support of μ the decomposition of φ wrt. the distribution induced by some ruloid partition $\mathcal{R}_u^{t,a}$ holds. The decomposition of $[\varphi]_p$ characterizes that the decomposition of φ holds for some set of terms with probability mass at least p. Different variants to refute a ruloid (decomposition of negation), different ruloid partitions $\mathcal{R}_u^{t,a}, \mathcal{R}_v^{t,a}$ of a process term t and action a (decomposition of diamond modality) and probabilistic branching (decomposition of probability measure modality) lead to multiple decompositions $\psi \in \mathcal{P}(Var \to \mathbb{O})$.

For $\mu \in Dist(\mathbb{T}(\Sigma, Var))$ we define $var(\mu) = \cup_{t \in Supp} var(t)$. A set of ruloids R is target variable disjoint if for $\rho, \rho' \in R$ with $\rho \neq \rho'$ we have $(var(\rho) - var(source(\rho))) \cap (var(\rho') - var(source(\rho'))) = \emptyset$. Variable disjointness of sets of ruloids prevents unintended variable binding in decompositions where multiple ruloids are applied. For R a set of ruloids we call $R' \subseteq R$ minimal representative if $weight(R') = weight(R)$ and for each $\rho, \rho' \in R'$ with $\rho \neq \rho'$ we have $[\rho]_\alpha \neq [\rho']_\alpha$. Minimal representative subsets of a ruloid partition have only one representative for each equivalence class while still preserving the total probability mass of 1. A substitution $\sigma : Var \to \mathbb{T}(\Sigma, Var)$ is lifted to $\mu \in Dist(\mathbb{T}(\Sigma, Var))$ by $\sigma(\mu)(t) = \mu(\sigma^{-1}(t))$. A substitution σ is called μ-well-formed if for $t, t' \in Supp(\mu)$ with $t \neq t'$ we have $\sigma(t) \neq \sigma(t')$. A distribution $\mu \in Dist(\mathbb{T}(\Sigma, Var))$ is called well-formed if there is some μ-well-formed substitution. $\mathbb{DT}(\Sigma, Var) \subseteq Dist(\mathbb{T}(\Sigma, Var))$ denotes all well-formed distributions.

Definition 11. *Let $P = (\Sigma, Act, R)$ be a PTSS. We define $\cdot^{-1} : \mathbb{DT}(\Sigma, Var) \to (\mathbb{O} \to \mathcal{P}(Var \to \mathbb{O}))$ as the smallest function satisfying the following conditions:*

1. *$\mu^{-1}(\top) = \{\psi\}$ with $\psi(x) = \top$ for all $x \in Var$*
2. *$\psi \in \mu^{-1}(\neg\varphi)$ iff there is a function $h : \mu^{-1}(\varphi) \to var(\mu)$ such that*

$$\psi(x) = \begin{cases} \bigwedge\limits_{\chi \in h^{-1}(x)} \neg\chi(x) & \text{if } x \in var(\mu) \\ \top & \text{if } x \notin var(\mu) \end{cases}$$

3. *$\psi \in \mu^{-1}(\bigwedge_{i\in I} \varphi_i)$ iff there are $\psi_i \in \mu^{-1}(\varphi_i)$ for each $i \in I$ such that*

$$\psi(x) = \bigwedge_{i \in I} \psi_i(x) \quad \text{for all } x \in Var$$

4. *$\psi \in \mu^{-1}(\langle a\rangle\varphi)$ iff for each $t \in Supp(\mu)$ there is some minimal representative and target variable disjoint $R^t \subseteq \mathcal{R}_u^{t,a}$, a distribution $\nu^t \in Dist(\mathbb{T}(\Sigma, Var))$ defined by $\nu^t(target(\rho)) = weight(\rho)$ for $\rho \in R^t$, some $\chi^t \in (\nu^t)^{-1}(\varphi)$ s.t.*

$$\psi^t(x) = \begin{cases} \bigwedge\limits_{\substack{\rho \in R^t \\ H = premises(\rho)}} \Bigg[\chi^t(x) \wedge \Big(\bigwedge\limits_{(x \xrightarrow{a_k,\pi_k} y) \in H} \langle a_k\rangle \chi^t(y) \Big) \wedge \\ \qquad \Big(\bigwedge\limits_{(x \xrightarrow{B_l}) \in H} \bigwedge\limits_{b \in B_l} \langle b\rangle\top \Big) \wedge \Big(\bigwedge\limits_{(x \not\xrightarrow{C_m}) \in H} \bigwedge\limits_{c \in C} \neg\langle c\rangle\top \Big) \Bigg] & \text{if } x \in var(\mu) \\ \top & \text{if } x \notin var(\mu) \end{cases}$$

   and $\psi(x) = \bigwedge_{t \in Supp(\mu)} \psi^t(x)$

5. *$\psi \in \mu^{-1}([\varphi]_p)$ iff there is some $T \subseteq Supp(\mu)$ with $\mu(T) \geq p$ and for each $t \in T$ there is a $\psi^t \in \delta_t^{-1}(\varphi)$ such that*

$$\psi(x) = \bigwedge_{t \in T} \psi^t(x) \quad \text{for all } x \in Var$$

The decomposition of φ wrt. a term t is defined by $t^{-1}(\varphi) = \delta_t^{-1}(\varphi)$. The decomposition of $\langle a\rangle\varphi$ wrt. a distribution reflects the universal nature of the diamond modality that every term in the support of the distribution has to satisfy $\langle a\rangle\varphi$. The decomposition of $\langle a\rangle\varphi$ wrt. a term t, denoted $\psi^t \in t^{-1}(\langle a\rangle\varphi)$, uses a set of ruloids with total weight 1, i.e. the diamond modality reasons over all probabilistic moves (internal nondeterminism), but employs a minimal set of ruloids (only one single representative per ruloid equivalence class) to prevent double counting of probabilities.

The main theorem shows that using modal decomposition, the satisfaction problem of a probabilistic HML formula for a distribution over process terms can be reduced to the question whether its subterms satisfy the decomposed formulae.

Theorem 3 (Decomposition theorem). *Let $P = (\Sigma, Act, R)$ be a PTSS. For any well-formed distribution $\mu \in \mathbb{DT}(\Sigma, Var)$, closed μ-well-formed substitution $\sigma : Var \to T(\Sigma)$ and modal assertion $\varphi \in \mathbb{O}$:*

$$\sigma(\mu) \models \varphi \quad \Leftrightarrow \quad \exists \psi \in \mu^{-1}(\varphi). \forall t \in Supp(\mu). \forall x \in var(t) : \sigma(x) \models \psi(x)$$

4 Example: Decomposition of the Probabilistic Sum

Example 4. Consider the probabilistic sum of Example 1. The decomposition of $(x_1 +^p x_2)^{-1}(\langle a \rangle [\varphi]_q)$ leads for the partitions $R_1^{+,a}$ to $R_3^{+,a}$ to the calculation of $\mu_i^{-1}([\varphi]_q)$ with $\mu_1 = \{y_1 \mapsto p, y_2 \mapsto 1-p\}$ (partition $R_1^{+,a}$), $\mu_2 = \delta_{y_1}$ (partition $R_2^{+,a}$) and $\mu_3 = \delta_{y_2}$ (partition $R_3^{+,a}$). The calculation of $\mu_2^{-1}([\varphi]_q) = \{\psi_2\}$ with $\psi_2(y_1) = \varphi$ and $\psi_2(z) = \top$ for $z \neq y_1$, and $\mu_3^{-1}([\varphi]_q) = \{\psi_3\}$ with $\psi_3(y_2) = \varphi$ and $\psi_3(z) = \top$ for $z \neq y_2$ is trivial. For partition $R_2^{+,a}$ this gives $\psi_2(x_1) = \langle a \rangle \varphi$, $\psi_2(x_2) = \neg \langle a \rangle \top$ and for $R_3^{+,a}$ this gives $\psi_3(x_1) = \neg \langle a \rangle \top$, $\psi_3(x_2) = \langle a \rangle \varphi$. For $\mu_1^{-1}([\varphi]_q)$ there are four cases to distinguish, depending on the arithmetic relation between q, p and $1-p$ (Def. 11.5):

Case	Condition	$T \subseteq Supp(\mu_1)$
1	$q > p,\ q > 1-p$	$\{y_1, y_2\}$
2	$q < p,\ q > 1-p$	$\{y_1\}$
3	$q > p,\ q < 1-p$	$\{y_2\}$
4	$q < p,\ q < 1-p$	$\{y_1\}, \{y_2\}$

We omitted the cases where T contains more terms than necessary to satisfy the required probability mass q. We exemplify the decomposition by instantiating p and q. The decomposition of case 1 (say for $p = 0.3, q = 0.8$) gives $(x_1 +^{0.3} x_2)^{-1}(\langle a \rangle [\varphi]_{0.8}) = \{\psi_1^1\}$ with $\psi_1^1(x_1) = \psi_1^1(x_2) = \langle a \rangle \varphi$. The conditions $q > p$ and $q > 1-p$ assert that if both processes x_1,x_2 can move, none of both alone has enough probability mass to satisfy the probability measure modality. The decomposition reflects the intuition that if both processes x_1,x_2 can perform an a transition then φ has to hold after both transitions. Case 2 (say for $p = 0.8, q = 0.3$) gives $(x_1 +^{0.8} x_2)^{-1}(\langle a \rangle [\varphi]_{0.3}) = \{\psi_1^2\}$ with $\psi_1^2(x_1) = \langle a \rangle \varphi$, $\psi_1^2(x_2) = \langle a \rangle \top$. Case 3 (say for $p = 0.2, q = 0.7$) leads to $(x_1 +^{0.2} x_2)^{-1}(\langle a \rangle [\varphi]_{0.7}) = \{\psi_1^3\}$ with $\psi_1^3(x_1) = \langle a \rangle \top, \psi_1^3(x_2) = \langle a \rangle \varphi$. Cases 2 and 3 express that if one of the processes can perform a transition with enough probability mass to satisfy the probability measure modality then the target of this transition has to satisfy φ, i.e. y_1 satisfies φ if $p > q$ or y_2 satisfies φ if $1-p > q$. Case 4 (say for $p = 0.7, q = 0.2$) results in $(x_1 +^{0.7} x_2)^{-1}(\langle a \rangle [\varphi]_{0.2}) = \{\psi_1^4, \psi_2^4\}$ with $\psi_1^4(x_1) = \langle a \rangle \varphi$, $\psi_1^4(x_2) = \langle a \rangle \top$, $\psi_2^4(x_1) = \langle a \rangle \top, \psi_2^4(x_2) = \langle a \rangle \varphi$. In this case both probabilistic transitions have enough probability mass to satisfy the probability measure modality. Thus, the probabilistic branching lead to two different decompositions ψ_1^4 and ψ_2^4. ■

5 Future Work

The decomposition method presented in this paper can be extended in the following directions. The modal logic employed is L^N [24], which takes into account

probabilistic branching. Segala and Lynch provided a variant of probabilistic simulation where state transitions need to be matched only by convex combinations of distributions (combined transition) [26]. The decomposition method could be extended to the corresponding logic L_p^N that provides a modified diamond operator which uses combined transitions instead of state transitions. Furthermore, the decomposition method could be adapted to generative PLTSs, to probabilistic automata [25] which combine nondeterministic and probabilistic choice using the recently introduced rule format by [10], and to continuous-space Markov processes using Modular Markovian Logic [8].

Following the approach of [6], the decomposition method can be applied to systematically develop congruence formats for different behavioral semantics of probabilistic systems, such as strong and weak variants of bisimulation, simulation, and testing semantics. Behavioral equivalences for stochastic systems are e.g. Markovian bisimulation, Markovian testing, and probabilistic and Markovian trace semantics. Congruence formats have so far only been developed for probabilistic bisimulation for reactive probabilistic systems [4,20], generative probabilistic systems [20] and bisimulation for stochastic systems [18].

Bialgebraic semantics abstracts away from concrete notions of syntax and system behavior [29]. Klin combines bialgebraic semantics with a coalgebraic approach to modal logic to prove compositionality of process equivalences for languages defined by SOS [19]. He developed the SGSOS format to define well-behaved Markovian stochastic transition systems [18]. A closely related approach was taken by Bacci and Miculan for probabilistic processes with continuous probabilities [3]. It is worth investigating how our modal decomposition approach relates to bialgebraic methods.

Acknowledgements We are grateful to Simone Tini for discussions on structural properties of operational semantics for PLTSs, and to Bas Luttik for constructive feedback on the presentation of the research results.

References

1. Aceto, L., Fokkink, W., Verhoef, C.: Structural operational semantics. In: Handbook of Process Algebra, pp. 197–292. Elsevier (2001)
2. Aldini, A., Bravetti, M., Gorrieri, R.: A process-algebraic approach for the analysis of probabilistic noninterference. J. Comput. Secur. 12, 191–245 (2004)
3. Bacci, G., Miculan, M.: Structural operational semantics for continuous state probabilistic processes. In: Proc. CMCS'12. Lecture Notes in Computer Science, vol. ?, pp. 71–89. Springer (2012)
4. Bartels, F.: GSOS for probabilistic transition systems. In: Proc. CMCS'02. ENTCS, vol. 65, pp. 29–53. Elsevier (2002)
5. Bergstra, J., Baeten, J., Smolka, S.: Axiomatizing probabilistic processes: ACP with generative probabilities. Inf. Comput. 121, 234–254 (1995)
6. Bloom, B., Fokkink, W., van Glabbeek, R.: Precongruence formats for decorated trace semantics. ACM TOCL 5, 26–78 (2004)
7. Bloom, B., Istrail, S., Meyer, A.R.: Bisimulation can't be traced. J. ACM 42, 232–268 (1995)

8. Cardelli, L., Larsen, K., Mardare, R.: Modular Markovian logic. In: Proc. ICALP'11. LNCS, vol. 6756, pp. 380–391. Springer (2011)
9. Clark, K.L.: Negation as failure. In: Logic and Data Bases. pp. 293–322. Plenum Press (1978)
10. D'Argenio, P.R., Lee, M.D.: Probabilistic transition system specification: Congruence and full abstraction of bisimulation. In: Proc. FoSSaCS'12. LNCS, vol. 7213, pp. 452–466. Springer (2012)
11. Fokkink, W., van Glabbeek, R., de Wind, P.: Compositionality of Hennessy-Milner logic by structural operational semantics. Theor. Comput. Sci. 354, 421–440 (2006)
12. Giacalone, A., Jou, C., Smolka, S.: Algebraic reasoning for probabilistic concurrent systems. In: Proc. IFIP ProCoMet'90. pp. 443–458. North-Holland (1990)
13. van Glabbeek, R.: The meaning of negative premises in transition system specifications II. J. Logic Algebr. Program. 60-61, 229–258 (2004)
14. van Glabbeek, R.: On cool congruence formats for weak bisimulations. Theor. Comput. Sci. 412, 3283–3302 (2011)
15. van Glabbeek, R., Smolka, S., Steffen, B.: Reactive, generative, and stratified models of probabilistic processes. Inf. Comput. 121, 59–80 (1995)
16. Hennessy, M., Milner, R.: Algebraic laws for nondeterminism and concurrency. J. ACM 32, 137–161 (1985)
17. Jonsson, B., Yi, W., Larsen, K.: Probabilistic extensions of process algebras. In: Handbook of Process Algebra, pp. 685–710. Elsevier (2001)
18. Klin, B., Sassone, V.: Structural operational semantics for stochastic process calculi. In: Proc. FoSSaCS'08. LNCS, vol. 4962, pp. 428–433. Springer (2008)
19. Klin, B.: Structural operational semantics and modal logic, revisited. In: Proc. CMCS'10. ENTCS, vol. 264, pp. 155–175. Elsevier (2010)
20. Lanotte, R., Tini, S.: Probabilistic bisimulation as a congruence. ACM TOCL 10, 1–48 (2009)
21. Larsen, K.G.: Context-Dependent Bisimulation Between Processes. Ph.D. thesis, University of Edinburgh (1986)
22. Larsen, K.G., Skou, A.: Bisimulation through probabilistic testing. Inf. Comput. 94, 1–28 (1991)
23. Larsen, K.G., Xinxin, L.: Compositionality through an operational semantics of contexts. J. Log. Comput. 1, 761–795 (1991)
24. Parma, A., Segala, R.: Logical characterizations of bisimulations for discrete probabilistic systems. In: Proc. FoSSaCS'07, LNCS, vol. 4423, pp. 287–301. Springer (2007)
25. Segala, R.: Modeling and Verification of Randomized Distributed Real-Time Systems. Ph.D. thesis, MIT (1995)
26. Segala, R., Lynch, N.: Probabilistic simulations for probabilistic processes. Nordic J. of Computing 2, 250–273 (1995)
27. de Simone, R.: Higher-level synchronising devices in Meije-SCCS. Theor. Comput. Sci. 37, 245–267 (1985)
28. Tini, S.: Non-expansive epsilon-bisimulations for probabilistic processes. Theor. Comput. Sci. 411, 2202–2222 (2010)
29. Turi, D., Plotkin, G.: Towards a mathematical operational semantics. In: Proc. LICS'97. pp. 280–291. IEEE (1997)