Stuttering for Abstract Probabilistic Automata[1]

Benoît Delahaye[a], Kim G. Larsen[b], Axel Legay[a]

[a]*INRIA/IRISA, Rennes, France*
[b]*Aalborg University, Denmark*

Abstract

Probabilistic Automata (PAs) are a widely-recognized mathematical framework for the specification and analysis of systems with non-deterministic and stochastic behaviors. In a series of recent papers, we proposed Abstract Probabilistic Automata (APAs), a new abstraction framework for representing possibly infinite sets of PAs. We have developed a complete abstraction theory for APAs, and also proposed the first specification theory for them. APAs support both satisfaction and refinement operators, together with classical stepwise design operators.

One of the major drawbacks of APAs is that the formalism cannot capture PAs with hidden actions – such actions are however necessary to describe behaviors that shall not be visible to a third party. In this paper, we revisit and extend the theory of APAs to such context. Our first main result takes the form of proposal for a new probabilistic satisfaction relation that captures several definitions of PAs with hidden actions. Our second main contribution is to revisit all the operations and properties defined on APAs for such notions of PAs. Finally, we also establish the first link between stochastic modal logic and APAs, hence linking an automata-based specification theory to a logical one.

Keywords: Specification theory, probabilistic Automata, stuttering, logical characterization, refinement

1. Introduction

Nowadays, systems are tremendously big and complex and mostly result from the assembling of several components. These components are usually designed by teams working *independently* but with a common agreement on what the interface of each

[1]This paper is an extended version of a conference paper presented at LFCS 2013 [1]. The main differences are in the presentation of the theory, the addition of proofs for main theorems, and new examples and definitions.

component should be. These interfaces, also called specifications, precise the behaviors expected from each component as well as the environment in which they can be used, but do not impose any constraint on how the components are implemented.

Instead of relying on Word/Excel text documents or modeling languages such as UML/XML, as is usually done in practice, a series of recent works recommend relying most possibly on mathematically sound formalisms. Mathematical foundations that allow to reason at the abstract level of interfaces, in order to infer properties of the global implementation, and to design or to advisedly (re)use components is a very active research area, known as *compositional reasoning* [2]. Any good specification theory shall be equipped with a *satisfaction relation* (to decide whether an implementation satisfies a specification), a *refinement relation* (to compare sets of implementations), a *logical conjunction* (to compute intersection of sets of implementations), and a *structural composition* (to combine specifications). Additionally, properties such as precongruence of composition with respect to refinement [2] shall also be satisfied.

Building good specification theories has been the subject of intensive studies among which one finds classical logical specifications, various process algebrae such as CSP, or Input/Output automata/interfaces (see [3, 4, 5]). Recently, a new series of works has concentrated on *modal specifications* [6], a language theoretic account of a fragment of the modal mu-calculus logic which is known to admit a more flexible and easy-to-use compositional refinement method than those carried out in CSP [6, 7, 8].

As soon as systems include randomized algorithms, probabilistic protocols, or interact with physical environment, probabilistic models are required to reason about them. This is exacerbated by requirements for fault tolerance, when systems need to be analyzed quantitatively for the amount of failure they can tolerate, or for the delays that may appear. As Henzinger and Sifakis [2] point out, introducing probabilities into design theories allows assessing dependability of IT systems in the same manner as commonly practiced in other engineering disciplines.

In recent works [9, 10], we proposed Constraint Markov Chains (CMCs), a complete specification theory for pure stochastic systems, namely Markov Chains (MCs). Roughly speaking, a CMC is a MC equipped with a constraint on the next-state probabilities from any state. An implementation for a CMC is thus a MC, whose next-state probability distribution satisfies the constraint associated with each state. Contrary to Interval Markov Chains where sets of distributions are represented by intervals, CMCs are closed under both composition and conjunction. Later, in [11], the CMC approach was extended to handle those systems that combine both stochastic and nondeterministic behaviors, i.e., Probabilistic Automata (PA). APAs, is the result of combining Modal Automata and CMCs – the abstractions for labelled transition systems and Markov Chains, respectively. Like other modal-based specification theories, our formalism can be used in various areas, including abstract model checking and com-

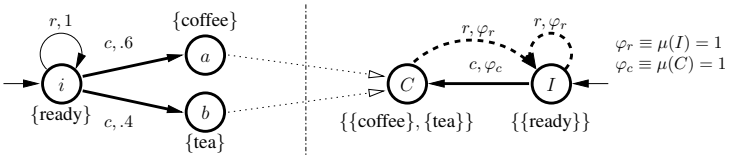


Figure 1: Implementation PA (left) and specification APA (right) of a coffee machine.

positional reasoning.

The specification theory induced by APAs is more expressive than any classical specification theories where both implementations and specifications are represented by the same object. As an example, Segala's theory assumes that both specifications and implementations are represented with PAs [12, 13]. Such an approach does not permit to represent an infinite set of non-deterministic behaviors in a finite way. On the other hand, while satisfaction relation between PAs[14] can be expressed with classical notions of (stochastic) simulations [12], ours requires the use of a rather more complex definition of equivalence relation. Consider the implementation (left) and specification (right) of a coffee machine given in Figure 1. The specification specifies that there are two possible transitions from initial state I: a may transition labeled with action r (reset) and a must transition labeled with action c (coin). May transitions, which may not be implemented, are represented with dashed arrows. Must transitions, which shall be present in any implementation of the specification, are represented with plain arrows. The probability distributions associated with these actions are specified by the constraints φ_r and φ_c, respectively. One can see that the implementation gives a more precise behavior of the coffee machine: action r loops back to initial state i with probability 1, while coin leads to state a (coffee) with probability $.6$ and to state b (tea) with probability $.4$. Satisfaction between implementation and specification lifts the classical notion of simulation for PAs to APAs as follows: (1) all must transitions of the specification must be matched with transitions in the implementations, and (2) all transitions in the implementation must be matched with may transitions in the specification. Additionally, we have to check that the probability distributions in the implementation are matched with probability distributions in the specification that satisfy the given constraints.

Contribution. In the process of incremental design (as well as for other applications), it may be necessary to incrementally widen the scope of implementations. Usually, the latter is done by permitting the addition of hidden actions also called stutter steps [12, 15] in the implementation. In some cases, such stetter steps are even considered at the specification level [15]. Introducing such actions is known to complicate the definition and the computation of operations such as bisimulation/simulation [12]. Moreover, it may break up some properties such as precongruence of refinement with

respect to composition [12]. The objective of this paper is to extend the APA specification theory by considering implementations with stuttering steps. Our first contribution is the definition of a new stochastic satisfaction relation for APAs. This relation generalizes stochastic simulation to the APA level. We then study various notions of stuttering and compare their expressivity. We also study the impact of adding stuttering on various properties such as precongruence of refinement with respect to composition. Finally, we define and study ML-(A)PA that is a new modal logic for APAs and stuttering PAs. ML-(A)PA generalizes the PML logic [16, 17] of Larsen et al. from PAs to APAs and stuttering PAs.

Related work. A wide spectrum of different approaches study stuttering for non stochastic systems [18] and stochastic ones [19, 20, 21]. In [21], the authors define weak bisimulation for fully probabilistic processes. This is in contrast with our model that combines both probabilistic and non-deterministic aspects. In [19, 20], weak bisimulation is extended to *strictly alternating* systems that combine both non-determinism and probabilities. Although such systems are similar to PAs, it is known that weak (branching) bisimulation for alternating systems is incomparable to weak bisimulation for non-alternating systems [22]. Moreover, it is worth mentioning that above mentioned works report on computing and checking weak bisimulation between probabilistic systems, while our aim is to propose a notion of weak simulation (satisfaction) between a probabilistic system and a probabilistic specification that represents a possibly infinite set of implementations.

In [23], the author defines a notion of constraints on states to represent sets of probability distributions. Although this formalism resembles the one of constraints used in APAs, the constraints in [23] are used in a different context. Indeed, while we use constraints to represent sets of probabilistic transitions, [23] uses them to replace the non-deterministic choice between internal transitions by probability distributions.

Finally we mention that the problem of defining compositionality in the probabilistic setting with hidden steps has also been addressed in various settings [22, 24, 25, 26, 23, 27]. In particular [26] defines a general parallel composition operator for CSP that deals with hidden steps, and [27] suggests the removal of hidden steps through a transformation of CSP models. In both papers, the systems considered are strictly alternating and results are obtained with respect to a ready-trace notion of equivalence on processes, which makes it incomparable to our notion of stuttering satisfaction between specifications and implementations.

Structure. The paper is structured as follows. Section 2 recalls general background on Probabilistic Automata and Abstract Probabilistic Automata, and proposes a new notion of probabilistic satisfaction. Section 3 presents our first contribution that is a study of the definition of stuttering for APAs. In Section 4, we introduce our second contribution that is the modal logic ML-(A)PA. Section 5 discusses the problem of

composing (A)PAs. Finally, Section 6 concludes the paper.

2. A Probabilistic Satisfaction for Abstract Probabilistic Automata

In this section, we briefly survey the concepts of Probabilistic Automata (PA) and Abstract Probabilistic Automata (APAs). The reader is directed to [11, 28] for more details. We also propose a new notion of probabilistic satisfaction inspired by probabilistic simulation [29].

2.1. Abstract Probabilistic Automata

Let *Dist*(S) denote a set of all discrete probability distributions over a finite set S and $\mathbb{B}_2 = \{\top, \bot\}$.

Definition 1 (PA [12]). *A PA is a tuple (S, A, L, AP, V, s_0), where S is a finite set of states with the initial state $s_0 \in S$, A is a finite set of actions, L: $S \times A \times$ Dist$(S) \rightarrow \mathbb{B}_2$ is a (two-valued transition) function, AP is a finite set of atomic propositions and V: $S \rightarrow 2^{AP}$ is a state-labeling function.*

Consider a state s, an action a, and a probability distribution μ. The value of $L(s, a, \mu)$ is set to $\top$ in case there exists a transition from s under action a to a distribution μ on successor states. In other cases, we have $L(s, a, \mu) = \bot$.

We now switch to Abstract Probabilistic Automata (APA)[11], that is a specification theory for PAs. Let S be a finite set. We define $C(S)$ to be the set of constraints defined over discrete probability distributions on S. Each element $\varphi \in C(S)$ describes a set of distributions: *Sat*$(\varphi) \subseteq$ *Dist*(S). Let $\mathbb{B}_3 = \{\top, ?, \bot\}$. APAs are formally defined as follows.

Definition 2 (APA [11]). *An APA is a tuple (S, A, L, AP, V, s_0), where S is a finite set of states, $s_0 \in S$, A is a finite set of actions, and AP is a finite set of atomic propositions. $L : S \times A \times C(S) \rightarrow \mathbb{B}_3$ is a* three-*valued distribution-constraint function, and $V : S \rightarrow 2^{2^{AP}}$ maps each state in S to a set of admissible labelings.*

APAs play the role of specifications in our framework. An APA transition abstracts transitions of a certain unknown PA, called its implementation. Given a state s, an action a, and a constraint φ, the value of $L(s, a, \varphi)$ gives the modality of the transition. Here, $\mathbb{B}_3 = \{\bot, ?, \top\}$ denotes a *lattice* with the ordering $\bot < ? < \top$ and meet ($\sqcap$) and join ($\sqcup$) operators. More precisely the value $\top$ means that transitions under a must exist in the PA to some distribution in *Sat*(φ); $?$ means that these transitions are allowed to exist; $\bot$ means that such transitions must not exist. Again L may be partial. A lack of value for given argument is equivalent to the $\bot$ value, so we will sometimes avoid

defining $\perp$-value rules in constructions to avoid clutter, and occasionally will say that something applies if L takes the value of $\perp$, meaning that it is either taking this value or it is undefined. The function V labels each state with a subset of the powerset of AP, which models a disjunctive choice of possible combinations of atomic propositions. We occasionally write $\mathsf{Must}(s)$ for the set of actions a such that there exists φ, so that $L(s, a, \varphi) = \top$, and write $\mathsf{May}(s)$ for the set of actions b such that there exists φ, so that $L(s, b, \varphi) \neq \perp$. Remark that in our formalism, $\mathsf{Must}(s) \subseteq \mathsf{May}(s)$. This implies that we do not allow inconsistencies at the level of modalities, i.e. required but not allowed transitions.

2.2. A Probabilistic Satisfaction for APA

We now study the notion of satisfaction that relates a probabilistic automata $P = (S_P, A, L_P, AP, V_P, s_0^P)$ to its corresponding APA specification $N = (S, A, L, AP, V, s_0)$, The notion of satisfaction proposed in [11] directly relates distributions in P to distributions in N. As in the notion of probabilistic forward simulation presented in [14], we now extend this notion to account for linear combinations of distributions in N, hence generalizing results in [11].

Definition 3 (Simulation [11]). *Let S and S' be non-empty sets, and μ, μ' be distributions; $\mu \in Dist(S)$ and $\mu' \in Dist(S')$. We say that μ is* simulated *by μ' with respect to a relation $\mathcal{R} \subseteq S \times S'$ and a* correspondence function *$\delta : S \to (S' \to [0, 1])$ iff*

1. *for all $s \in S$, $\delta(s)$ is a distribution on S' if $\mu(s) > 0$,*
2. *for all $s' \in S'$, $\sum_{s \in S} \mu(s) \cdot \delta(s)(s') = \mu'(s')$, and*
3. *whenever $\delta(s)(s') > 0$ then $(s, s') \in \mathcal{R}$.*

We write $\mu \Subset^{\delta}_{\mathcal{R}} \mu'$ meaning that μ is simulated by μ' with respect to $\mathcal{R}$ and δ, and we write $\mu \Subset_{\mathcal{R}} \mu'$ iff there exists a function δ such that $\mu \Subset^{\delta}_{\mathcal{R}} \mu'$.

Probabilistic satisfaction extends APA satisfaction as defined in [11] by allowing linear combinations of distibutions on the abstract side. We shall see that linear combinations are needed when introducing stuttering, hence this generalization.

Definition 4 (Probabilistic Satisfaction). *Let $P = (S_P, A, L_P, AP, V_P, s_0^P)$ be a PA and $N = (S, A, L, AP, V, s_0)$ be an APA. A binary relation $\mathcal{R} \subseteq S_P \times S$ is a probabilistic satisfaction relation iff, for any $(s, s') \in \mathcal{R}$, the following conditions hold:*

- *for all $a \in A$ and $\varphi' \in C(S)$ such that $L(s', a, \varphi') = \top$, there exists a distribution $\mu_P \in Dist(S_P)$ such that $L_P(s, a, \mu_P) = \top$ and there exists $\mu' \in Sat(\varphi')$ such that $\mu_P \Subset_{\mathcal{R}} \mu'$,*

- *for all* $a \in A$ *and* $\mu_P \in Dist(S_P)$ *such that* $L_P(s, a, \mu_P) = \top$*, there exists* $\varphi_1, \dots \varphi_n \in C(S)$ *such that for all* i*,* $L(s', a, \varphi_i) \neq \bot$ *and there exists* $\mu_i \in Sat(\varphi_i)$ *and* $\rho_i \in [0, 1]$ *such that* $\sum_i \rho_i = 1$ *and* $\mu_P \Subset_{\mathcal{R}} (\sum_i \rho_i \mu_i)$*, and*
- $V_P(s) \in V(s')$.

We say that P probabilistically satisfies N, written $P \models_{\mathbb{P}} N$ iff there exists a probabilistic satisfaction relation $\mathcal{R}$ such that $s_0^P \mathcal{R} s_0$. The set of probabilistic implementations of APA N is defined by $[\![N]\!]_{\mathbb{P}} = \{P \mid P \models_{\mathbb{P}} N\}$.

It is easy to see that this extension of satisfaction is conservative with respect to all the good properties presented in [11]. In the rest of this paper, we study the impact of adding stuttering to the specification theory.

3. Stuttering for Abstract Probabilistic Automata

We now study an extension of the APAs specification theory where implementations may have stutter steps. Although several notions of stuttering for PA have already been studied [30, 31, 32], our purpose in this paper is to relate the notion of stuttering with the notion of satisfaction for APAs. For doing so, we introduce a new notion of stuttering that can be easily linked to probabilistic satisfaction for APAs, as presented in Definition 4. In the rest of this section, we first introduce various notions of stuttering for PAs and then extend the satisfaction relation to them. Later, we shall study the impact of stuttering on refinement and structural/logical composition.

3.1. Introducing Stutter Actions

Consider a PA $P = (S_P, A, L_P, AP, V_P, s_0^P)$. We must assume that any state s' that can be reached from a state s by following a sequence of hidden actions $\mathcal{H} \subseteq A_P$ cannot be distinguished from s, i.e., have the same valuation as s.

Definition 5 (Consistent set of hidden actions). *Let* $P = (S_P, A_P, L_P, AP, V_P, s_0^P)$ *and let* $\mathcal{H} \subseteq A_P$*. We say that* $\mathcal{H}$ *is a consistent set of hidden actions regarding* P *if* $\forall s \in S_P$ *and* $\forall a \in \mathcal{H}$*, if there exists* $\mu \in Dist(S_P)$ *such that* $L_P(s, a, \mu) = \top$*, then* $\forall s' \in S$*, we have* $\mu(s') > 0 \Rightarrow V_P(s') = V_P(s)$.

The following example shows that, as it is the case for other specifications theories (see e.g. [33]), there are various ways to formally define a stuttering transition.

Example 1. *Consider the stuttering PA* P *given in Figure 2, and whose set of consistent hidden action is given by* $\{m, e\}$*.* P *represents a coffee machine that has two modes. Action* m *allows choosing between the two modes. In mode* A*, represented by*

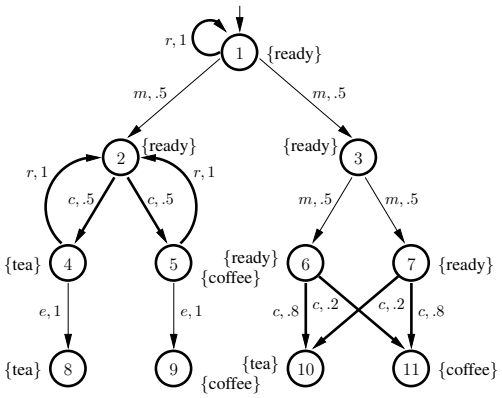


Figure 2: Stuttering PA P with m and e as hidden actions.

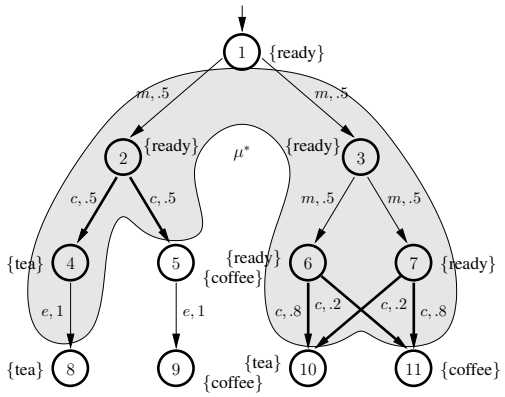


Figure 3: Stuttering transition $1 \rightarrow^* \mu^*$ in P where stuttering happens both before and after visible action c.

state 2 and its successors, the action c leads to states labeled with tea and coffee with probability $.5$ each. From states 4 and 5, either the coffee machine can be reset with action r, but will stay in the same mode, or can suffer an error (action e) that leads to deadlock states 8 and 9. In mode B, one can again choose a sub-mode with action m, leading to states 6 and 7 that deliver tea and coffee with different probabilities.
Considering different notions of stuttering will lead to different sets of executions for the PA P. As an example, stuttering could be restricted to happen only before visible actions. The execution presented in Figure 4 represents a stuttering execution $1 \xrightarrow{c}{}^* \mu_0^*$ (informally, one can reach distribution μ_0^* from state 1 by following action c interleaved with hidden actions), where the internal action m happens before the visible action c, leading to a distribution μ_0^*. Remark that such an execution could not be considered if we restricted stuttering to happen only after a visible action. The unfolding of P given in Figure 5 presents two stuttering executions $1 \xrightarrow{r}{}^* \mu_1^*$ and $2 \xrightarrow{c}{}^* \mu_2^*$ where in both cases stuttering only happens after the visible action. Again, such executions could not be considered if we restricted stuttering to happen only before a visible action. Finally, the execution presented in Figure 3 represents a stuttering transition $1 \xrightarrow{c}{}^* \mu^*$ in P where stuttering happens both before and after the visible action c.

As illustrated in the example above, the choice made in the definition of stuttering will have a strong impact on the executions allowed in PAs. In order to be as general as possible, we choose to allow stuttering to happen both before and after visible actions. The only restriction we make is that stuttering cannot happen independently of visible

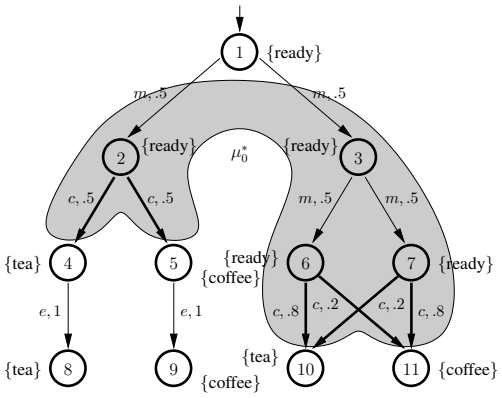


Figure 4: Stuttering transition $1 \rightarrow^* \mu_0^*$ in PA P of Figure 2 where stuttering happens before visible action c.

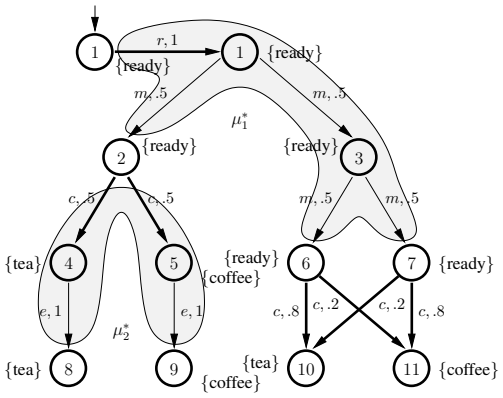


Figure 5: Stuttering transitions $1 \rightarrow^* \mu_1^*$ and $2 \rightarrow^* \mu_2^*$ in PA P of Figure 2 where stuttering happens after visible actions r and c.

actions, that is, for each stuttering transition, a visible action must be taken. This leads to the following definition.

Definition 6 (Stuttering transitions for PAs). *Let $P = (S_P, A_P, L_P, AP, V_P, s_0^P)$ be a PA, and let $\mathcal{H} \subseteq A_P$ be a consistent set of hidden actions. We define the notion of $\mathcal{H}$-stuttering recursively as follows:*

Base case: *For all $s \in S_P$, $a \in A_P$ and $\mu \in Dist(S_P)$, we say that $s \xrightarrow[\mathcal{H}]{a} {}^1\mu$ iff $L(s, a, \mu) = \top$. As a shortcut, we write $s \xrightarrow[\mathcal{H}]{\tau} {}^1\mu$ if there exists $b \in \mathcal{H}$ such that $s \xrightarrow[\mathcal{H}]{b} {}^1\mu$.*

Recursion: *For all $s \in S_P$, $k > 1$, $a \in A_P$ and $\mu^* \in Dist(S_P)$, we say that $s \xrightarrow[\mathcal{H}]{a} {}^k\mu^*$ iff*

1. *either $a \notin \mathcal{H}$ and there exists $\mu_1 \in Dist(S_P)$ and $b \in \mathcal{H}$ such that $L(s, b, \mu_1) = \top$ and the following conditions hold:*
   - *for all states $r \in S_P$ such that $\mu_1(r) > 0$, there exists $k' < k$ and $\mu_r \in Dist(S_P)$ such that $r \xrightarrow[\mathcal{H}]{a} {}^{k'}\mu_r$, and*
   - *for all $s' \in S_P$,*

$$\mu^*(s') = \sum_{r \in S_P} \mu_1(r)\mu_r(s'),$$

2. *or there exists* $\mu_1 \in Dist(S_P)$ *such that* $L(s,a,\mu_1) = \top$ *and a subset* $R \subseteq S_P$ *such that the following conditions hold:*
   - *for all states* $r \in R$*, we have* $\mu_1(r) > 0$ *and there exists* $k' < k$ *and* $\mu_r \in Dist(S_P)$ *such that* $r \xrightarrow[\mathcal{H}]{\tau}{}^{k'} \mu_r$*, and*
   - *for all* $s' \in S_P$*,*

$$\mu^*(s') = \begin{cases} \sum_{r \in R} \mu_1(r)\mu_r(s') & \text{if } s' \in R \\ \mu_1(s') + \sum_{r \in R} \mu_1(r)\mu_r(s') & \text{otherwise.} \end{cases}$$

We say that $s \xrightarrow[\mathcal{H}]{a}{}^* \mu^*$ *if there exists* $k > 0$ *such that* $s \xrightarrow[\mathcal{H}]{a}{}^k \mu^*$.

Informally stuttering can happen either before (case 1) or after (case 2) taking the visible action a. Remark that both cases are not exclusive and can interleave. If stuttering occurs before action a, then all successor states r must admit a stuttering transition involving a. In such case, the overall probability of reaching a state s' is the sum through all stuttering paths. If stuttering occurs after action a, then we denote by R the set of successor states from which we stutter, and by $S_P \setminus R$ the set of states in which we stop. Remark that the set R is dynamic in the sense that a different set R may be chosen for each step of a stuttering transition. In this case the overall probability of going to a state $s' \in R$ is the sum through all stuttering paths, while the overall probability of going to a state $s' \notin R$ is the addition of the probabilities of going to s' directly (without stutter) with the the sum through all stuttering paths.

In the rest of the paper, we denote by $\xrightarrow[\mathcal{H}]{a}{}^*_A$ (resp. $\xrightarrow[\mathcal{H}]{a}{}^*_B$) stuttering transitions where stuttering only happens after (resp. before) the visible action a, obtained by removing item 1. (resp. 2.) from the recursive part of Definition 6.

Example 2. *Consider the PA* $P = (S_P, A_P, L_P, AP, V_P, 1)$ *given in Figure 2, and a distribution* μ^* *such that* $\mu^*(5) = \mu^*(8) = \mu^*(10) = \mu^*(11) = .25$*. The situation is represented in Figure 3. Let us see how to derive that* $1 \xrightarrow[\{e,m\}]{c}{}^3 \mu^*$*. We follow the following description.*

1. *for* $[1 \xrightarrow[\{e,m\}]{c}{}^3 \mu^*]$*., we have* $c \notin \{e,m\}$ *and* $L_P(1,m,\mu_1) = \top$ *with* $m \in \{e,m\}$ *(case 1). states* 2 *and* 3 *are the only states for which* μ_1 *gives a non-zero probability, and* $2 \xrightarrow[\{e,m\}]{c}{}^2 \mu_2$ *and* $3 \xrightarrow[\{e,m\}]{c}{}^2 \mu_3$*, with* $\mu^*(s') = \mu_1(2)\mu_2(s') + \mu_1(3)\mu_3(s')$*.*
2. *for* $[2 \xrightarrow[\{e,m\}]{c}{}^2 \mu_2]$*., we have* $L_P(2,c,\mu_2') = \top$ *(case 2) and there exists* $R = \{4\} \subseteq S_P$ *such that* $\mu_2'(4) > 0$ *and* $4 \xrightarrow[\{e,m\}]{\tau}{}^1 \mu_4$*. In addition, we obtain after simplifications:* $\mu_2 : \begin{cases} 8 \mapsto \mu_2'(4)\mu_4(8) = .5 \\ 5 \mapsto \mu_2'(5) + 0 = .5 \end{cases}$

We observe that $[4 \xrightarrow[\{e,\,m\}]{\tau} {}^1\mu_4]$ *is a base case.*

3. $[3 \xrightarrow[\{e,\,m\}]{c} {}^2\mu_3]$**.** *We have* $c \notin \{e, m\}$ *and* $L_P(3, m, \mu'_3) = \top$ *with* $m \in \{e, m\}$ *(case 1). states* 6 *and* 7 *are the only states for which* μ'_3 *gives a non-zero probability, and* $6 \xrightarrow[\{e,\,m\}]{c} {}^1\mu_6$ *and* $7 \xrightarrow[\{e,\,m\}]{c} {}^1\mu_7$ *with* $\mu_3(s') = \mu'_3(6)\mu_6(s') + \mu'_3(7)\mu_7(s')$*. We observe that* $[6 \xrightarrow[\{e,\,m\}]{c} {}^1\mu_6]$ *and* $[7 \xrightarrow[\{e,\,m\}]{c} {}^1\mu_7]$ *are base cases.*

Finally, we obtain the following result:

$\boldsymbol{\mu^*(5)} = \mu_1(2)(\mu'_2(5)) = .25$ $\quad$ $\boldsymbol{\mu^*(10)} = \mu_1(3)(\mu'_3(6)\mu_6(10) + \mu'_3(7)\mu_7(10)) = .25$

$\boldsymbol{\mu^*(8)} = \mu_1(2)(\mu'_2(4)\mu_4(8)) = .25$ $\quad$ $\boldsymbol{\mu^*(11)} = \mu_1(3)(\mu'_3(6)\mu_6(11) + \mu'_3(7)\mu_7(11)) = .25$

3.2. On Stutter Satisfaction

We now introduce the notion of stutter satisfaction, that is an extension of Definition 4 for stuttering PAs.

Definition 7 (Stutter Satisfaction). *Let* $P = (S_P, A_P, L_P, AP, V_P, s_0^P)$ *be a PA, let* $N = (S, A, L, AP, V, s_0)$ *be an APA such that* $A \subseteq A_P$ *and* $\mathcal{H} = A_P \setminus A$ *is a consistent set of hidden actions for* P*. A binary relation* $\mathcal{R} \subseteq S_P \times S$ *is a* stutter satisfaction relation *iff, for any* $(s, s') \in \mathcal{R}$*, the following conditions hold:*

1. *for all* $a \in A$ *and* $\varphi' \in C(S)$*, if* $L(s', a, \varphi') = \top$*, then there exists a distribution* $\mu^* \in Dist(S_P)$ *such that* $s \xrightarrow[\mathcal{H}]{a} {}^*\mu^*$ *and there exists* $\mu \in Sat(\varphi')$ *such that* $\mu^* \Subset_{\mathcal{R}} \mu$*,*
2. *for all* $\mu^* \in Dist(S_P)$ *and* $a \in A$ *such that* $s \xrightarrow[\mathcal{H}]{a} {}^*\mu^*$*, there exist constraints* $\varphi_1, \ldots \varphi_n \in C(S)$ *such that for all* i*,* $L(s', a, \varphi_i) \neq \bot$ *and there exist* $\rho_i \in [0, 1]$ *and* $\mu_i \in Sat(\varphi_i)$ *such that* $\sum_i \rho_i = 1$ *and* $\mu^* \Subset_{\mathcal{R}} (\sum_i \rho_i \mu_i)$*, and*
3. $V_P(s) \in V(s')$*.*

We say that $P = (S_P, A_P, L_P, AP, V_P, s_0^P)$ stutter-satisfies $N = (S, A, L, AP, V, s_0)$, written $P \models^* N$, iff $A \subseteq A_P$, $\mathcal{H} = A_P \setminus A$ is a consistent set of hidden actions for P, and there exists a stutter satisfaction relation $\mathcal{R}$ such that $s_0^P \,\mathcal{R}\, s_0$. The set of stuttering implementations of APA N is given by $[\![N]\!]^* = \{P \mid P \models^* N\}$. Algorithms to decide such satisfaction relation can be obtained directly from those proposed in [10, 28] for the case where there are no cycles involving only stuttering actions. Otherwise, the problem is still open. Notice that stuttering satisfaction reduces to probabilistic satisfaction when the set of hidden actions $\mathcal{H}$ is empty. Hence stuttering satisfaction is a *conservative* extension of probabilistic satisfaction.

Example 3. *The PA P given in Figure 2 satisfies the specification of the coffee machine of Figure 1 with the notion of stuttering satisfaction given above. The stuttering satisfaction relation $\mathcal{R}$ is as follows: $\mathcal{R} = \{(\{1,2,3,6,7\}, I), (\{4,5,8,9,10,11\}, C)\}$. We show how state 1 of P satisfies state I of the specification and leave it to the reader to verify that the rest of the relation $\mathcal{R}$ satisfies the axioms of Definition 7 above.*

- *In the specification, we have $L(I, c, \varphi_c) = \top$. There exists a matching distribution in P: we have $1 \xrightarrow[\{e,\,m\}]{c}{}^{3}\mu^*$, with μ^* defined in Example 2, and $\mu^* \Subset_{\mathcal{R}} \mu_c$ with $\mu_c : C \mapsto 1 \in Sat(\varphi_c)$,*
- *in the implementation, we can verify that for all $a \in \{r, c\}$ and μ_P^* such that $1 \xrightarrow[\{e,\,m\}]{a}{}^{*}\mu_P^*$, we have a matching constraint and distribution in the specification: either φ_r or φ_c, and*
- *$V_P(1) = \{$ready$\} \in V(I) = \{\{$ready$\}\}$.*

Remark that the choice we made on the definition of stutter transitions by allowing stuttering to happen both before and after the visible action strongly influences the notion of stuttering satisfaction. We denote by $\models^*_A$ (resp. $\models^*_B$) the notion of satisfaction obtained by replacing the general notion of stutter transition $\xrightarrow[\mathcal{H}]{a}{}^{*}$ with the restricted notion $\xrightarrow[\mathcal{H}]{a}{}^{*}_{A}$ (resp. $\xrightarrow[\mathcal{H}]{a}{}^{*}_{B}$). The following theorem states that the different notions of stutter satisfaction $\models^*$, $\models^*_A$ and $\models^*_B$ cannot be compared in general.

Theorem 1. *There exists PAs P, P_A and P_B and an APA N such that:*

$$\begin{array}{ccc} P \models^*_A N & P \models^*_B N & P \models^* N \\ P_A \models^*_A N & P_A \not\models^*_B N & P_A \not\models^* N \\ P_B \not\models^*_A N & P_B \models^*_B N & P_B \models^* N \end{array}$$

Proof. Consider PAs P_B and P_A given in Figures 6 and 7. Both represent different implementations of a coffee machine with hidden actions m and e. One can see that PA P_B cannot satisfy the specification N of the coffee machine given in Figure 1 if we only allow stutter to happen after visible actions. Indeed, in this case, there is no possible transition from Initial state 1 in P_B. On the contrary, if we allow stutter to happen only before visible actions, then P_B satisfies N. If stuttering is allowed to happen both before and after the visible actions, then P_B also satisfies N. Thus, we have the following:

$$P_B \not\models^*_A N, \quad P_B \models^*_B N, \quad P_B \models^* N.$$

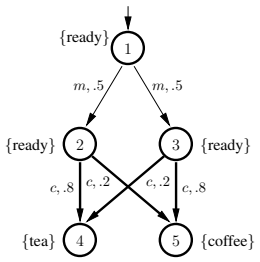


Figure 6: PA P_B with internal action m.

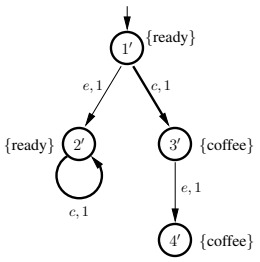


Figure 7: PA P_A with internal action e.

Consider now PA P_A given in Figure 7. In P_A, an error can happen from initial state $1'$ using hidden action e to lead in a bad state $2'$. This state is not conform to the specification and prevents P_A from satisfying N if stutter can happen before visible actions. However, if stuttering is only allowed to happen after visible actions, then State $2'$ is not reachable anymore in P_A. Thus, we obtain the following:

$$P_A \models^*_A N, \quad P_A \not\models^*_B N, \quad P_B \not\models^* N.$$

Finally, in the case of PA P given in Figure 2, we have that

$$P \models^*_A N, \quad P \models^*_B N, \quad P \models^* N.$$

□

Refinement. We now consider *refinement*, that is a relation that allows us to compare APAs in terms of sets of implementations. In Segala's theory, refinement boils down to (stochastic) simulation. In the context of APAs, refinement usually extends the definition of satisfaction. Extending Definition 7 would require to consider stuttering in the specification itself, which is not the topic of this paper. For this reason, we use the refinement relation proposed in [28].

Definition 8 (Refinement [28]). *Let $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A, L', AP, V', s'_0)$ be APAs. $\mathcal{R} \subseteq S \times S'$ is a* refinement *relation iff, for all $(s, s') \in \mathcal{R}$, the following conditions hold:*

1. $\forall a \in A$, $\forall \varphi' \in C(S')$, *if* $L'(s', a, \varphi') = \top$, *then* $\exists \varphi \in C(S) : L(s, a, \varphi) = \top$ *and* $\forall \mu \in Sat(\varphi)$, $\exists \mu' \in Sat(\varphi')$ *such that* $\mu \Subset_{\mathcal{R}} \mu'$,
2. $\forall a \in A$, $\forall \varphi \in C(S)$, *if* $L(s, a, \varphi) \neq \bot$, *then* $\forall \mu \in Sat(\varphi)$, $\exists \varphi' \in C(S') : L'(s', a, \varphi') \neq \bot$ *and* $\exists \mu' \in Sat(\varphi')$ *such that* $\mu \Subset_{\mathcal{R}} \mu'$, *and*
3. $V(s) \subseteq V'(s')$.

We say that N refines N', denoted $N \preceq_W N'$, iff there exists a refinement relation relating s_0 and s'_0. In [28], it is shown that for two given APAs N_1 and N_2, we have $N_1 \preceq_W N_2 \Rightarrow [\![N_1]\!] \subseteq [\![N_2]\!]$, where $[\![N_i]\!]$ represent PAs without stuttering steps. The following theorem extends this result to the case of PAs with stuttering steps.

Theorem 2. *Let P be a PA and let N and N' be APAs. If $P \models^* N$ and $N \preceq_W N'$, then $P \models^* N'$.*

Proof. Let $P = (S_P, A_P, L_P, AP, V_P, s_0^P)$ be a PA and let $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A, L', AP, V', s'_0)$ be APAs. Assume that $P \models^* N$ and $N \preceq_W N'$. Let $\mathcal{H} = A_P \setminus A$ be the set of hidden actions in P. Let $\mathcal{R}_\mathcal{H}$ and $\mathcal{R}'$ be the relations such that $P \models^* N$ and $N \preceq_W N'$, respectively. Consider the relation $\mathcal{R}'_\mathcal{H} \subseteq S_P \times S'$ such that $s_P \, \mathcal{R}'_\mathcal{H} \, s'$ iff there exists $s \in S$ such that $s_P \, \mathcal{R}_\mathcal{H} \, s$ and $s \, \mathcal{R}' \, s'$. We prove that $\mathcal{R}'_\mathcal{H}$ is a stutter satisfaction relation.

Let $s_P \in S_P$ and $s' \in S'$ such that $s_P \, \mathcal{R}'_\mathcal{H} \, s'$, and let $s \in S$ be the associated state in N.

1. Let $a \in A$ and $\varphi' \in C(S')$ such that $L'(s', a, \varphi') = \top$. By $\mathcal{R}'$, there exists $\varphi \in C(S)$ such that $L(s, a, \varphi) = \top$ and $\forall \mu \in Sat(\varphi) \exists \mu' \in Sat(\varphi') : \mu \Subset_{\mathcal{R}'} \mu'$. By $\mathcal{R}_\mathcal{H}$, there exists a distribution $\mu^* \in Dist(S_P)$ such that $s_P \xrightarrow[\mathcal{H}]{a} {}^*\mu^*$ and there exists $\mu \in Sat(\varphi)$ such that $\mu^* \Subset_{\mathcal{R}_\mathcal{H}} \mu$. Let $\delta_\mathcal{H} : S_P \to (S \to [0,1])$ be the correspondence function witnessing $\mu^* \Subset^{\delta_\mathcal{H}}_{\mathcal{R}_\mathcal{H}} \mu$. Let $\mu' \in Sat(\varphi')$ such that $\mu \Subset_{\mathcal{R}'} \mu'$ and let $\delta' : S \to (S' \to [0,1])$ be the witnessing correspondence function. We show that $\mu^* \Subset_{\mathcal{R}'_\mathcal{H}} \mu'$. Consider the function $\delta'_\mathcal{H} : S_P \to (S' \to [0,1])$ such that $\delta'_\mathcal{H}(s'_P)(s'_1) = \sum_{s_1 \in S} \delta_\mathcal{H}(s'_P)(s_1)\delta'(s_1)(s'_1)$. We show that $\delta'_\mathcal{H}$ is a correspondence function such that $\mu^* \Subset^{\delta'_\mathcal{H}}_{\mathcal{R}'_\mathcal{H}}$.
   (a) Let $s'_P \in S_P$. By construction, we have that $\sum_{s'_1 \in S'} \delta'_\mathcal{H}(s'_P)(s'_1) = 1$.
   (b) Let $s'_1 \in S'$.

$$\begin{aligned}
\sum_{s'_P \in S_P} \mu^*(s'_P)\delta'_\mathcal{H}(s'_P)(s'_1) &= \sum_{s'_P \in S_P} \mu^*(s'_P) \sum_{s_1 \in S} \delta_\mathcal{H}(s'_P)(s_1)\delta'(s_1)(s'_1) \\
&= \sum_{s_1 \in S} \sum_{s'_P \in S_P} \mu^*(s'_P)\delta_\mathcal{H}(s'_P)(s_1)\delta'(s_1)(s'_1) \\
&= \sum_{s_1 \in S} \delta'(s_1)(s'_1) \sum_{s'_P \in S_P} \mu^*(s'_P)\delta_\mathcal{H}(s'_P)(s_1) \\
&= \sum_{s_1 \in S} \mu(s_1)\delta'(s_1)(s'_1) = \mu'(s'_1).
\end{aligned}$$

(c) Assume that $\delta'_{\mathcal{H}}(s'_P)(s') > 0$. Then there exists $s_1 \in S$ such that $\delta_{\mathcal{H}}(s'_P)(s_1) > 0$ and $\delta'(s_1)(s'_1) > 0$. Therefore $s'_P \, \mathcal{R}_{\mathcal{H}} \, s_1$ and $s_1 \, \mathcal{R}' \, s'_1$. Thus, by definition, $s'_P \, \mathcal{R}'_{\mathcal{H}} \, s'_1$.

2. Let $a \in A$ and $\mu^* \in Dist(S_P)$ such that $s \xrightarrow[\mathcal{H}]{a} {}^*\mu^*$. By $\mathcal{R}_{\mathcal{H}}$, there exist $\varphi_1, \dots \varphi_n \in C(S)$ such that, for all i, $L(s, a, \varphi_i) \neq \bot$ and there exists $\rho_i \in [0, 1]$ and $\mu_i \in Sat(\varphi_i)$ such that $\sum_i \rho_i = 1$ and $\mu^* \Subset_{\mathcal{R}_{\mathcal{H}}} (\sum_i \rho_i \mu_i)$. Let $\delta_{\mathcal{H}}$ be the associated correspondence function. By $\mathcal{R}'$, there exist $\varphi'_1, \dots \varphi'_n \in C(s')$ such that, for all i, $L'(s', a, \varphi'_i) \neq \bot$ and $\forall \mu_i \in Sat(\varphi_i) \exists \mu'_i \in Sat(\varphi'_i) : \mu_i \Subset_{\mathcal{R}'} \mu'_i$. Let δ_i be the correspondence functions such that $\mu_i \Subset^{\delta_i}_{\mathcal{R}'} \mu'_i$. For all $s' \in S_P$, if $\mu^*(s') = 0$, then define $\delta'(s')(s'_2) = 0$ for all s'_2. Otherwise, define δ' as follows:

$$\delta'(s')(s'_2) = \sum_{s'_1 \in S_1^+} \delta_{\mathcal{H}}(s')(s'_1) \frac{\sum_{i=1}^n \rho_i \mu_i(s'_1) \delta_i(s'_1)(s'_2)}{\sum_{j=1}^n \rho_j \mu_j(s'_1)}$$

where S_1^+ is the set of states s'_1 in S_1 such that there exists i such that $\mu_i(s'_1) > 0$. We can safely assume that whenever $s'_1 \notin S_1^+$, we have $\delta_{\mathcal{H}}(s')(s'_1) = 0$. It follows that δ' is a correspondence function and that $\mu^* \Subset^{\delta'}_{\mathcal{R}'_{\mathcal{H}}} (\sum_i \rho_i \mu'_i)$.

3. By $\mathcal{R}_{\mathcal{H}}$, we have $V_P(s_P) \in V(s)$, and by $\mathcal{R}'$, we have $V(s) \subseteq V'(s')$. Thus $V_P(s_P) \in V'(s')$.

Since $s_0^P \, \mathcal{R}'_{\mathcal{H}} \, s'_0$, we conclude that $\mathcal{R}'_{\mathcal{H}}$ is a stutter satisfaction relation, and therefore $P \models_{\mathcal{H}} N'$. □

Conjunction. We now turn our attention to conjunction, an operation that allows us to combine requirements of several specifications. The main property of conjunction of two APAs is that it represents the intersection of their sets of implementations. We first recap the definition of conjunction between APA introduced in [28]. We then show that this definition conserves its properties even in the presence of stuttering in the implementations.

Definition 9 (Conjunction [28]). *Let $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A, L', AP, V', s'_0)$ be APAs sharing action and proposition sets. Their conjunction $N \owedge N'$ is the APA $(S \times S', A, \tilde{L}, AP, \tilde{V}, (s_0, s'_0))$ where $\tilde{V}((s, s')) = V(s) \cap V'(s')$ and*

$$\frac{a \in (\mathsf{Must}(s') \setminus \mathsf{May}(s)) \cup (\mathsf{Must}(s) \setminus \mathsf{May}(s'))}{\tilde{L}((s,s'),a,\mathit{false}) = \top}, \tag{1}$$

$$\frac{a \in (\mathsf{May}(s) \setminus \mathsf{May}(s')) \cup (\mathsf{May}(s') \setminus \mathsf{May}(s))}{\tilde{L}((s,s'),a,\tilde{\varphi}) = \bot}, \tag{2}$$

$$\frac{a \in \mathsf{May}(s) \cap \mathsf{May}(s') \qquad L(s,a,\varphi) \neq \bot \qquad L'(s',a,\varphi') \neq \bot}{\tilde{L}((s,s'),a,\tilde{\varphi}) = ?}, \tag{3}$$

where $\tilde{\varphi} \in C(S \times S')$ *such that* $\tilde{\mu} \in \mathit{Sat}(\tilde{\varphi})$ *iff both*

distribution $\mu : t \to \sum_{t' \in S'} \tilde{\mu}((t,t'))$ *is in* $\mathit{Sat}(\varphi)$ *and*

distribution $\mu' : t' \to \sum_{t \in S} \tilde{\mu}((t,t'))$ *is in* $\mathit{Sat}(\varphi')$.

$$\frac{a \in \mathsf{Must}(s) \qquad L(s,a,\varphi) = \top}{\tilde{L}((s,s'),a,\tilde{\varphi}^{\top}) = \top}, \tag{4}$$

where $\tilde{\varphi}^{\top} \in C(S \times S')$ *such that* $\tilde{\mu} \in \mathit{Sat}(\tilde{\varphi})$ *iff both*

the distribution $\mu : t \to \sum_{t' \in S'} \tilde{\mu}((t,t'))$ *is in* $\mathit{Sat}(\varphi)$, *and*

there exists $\varphi' \in C(S')$ *with* $L'(s',a,\varphi') \neq \bot$ *and the distribution* $\mu' : t' \to \sum_{t \in S} \tilde{\mu}((t,t'))$ *is in* $\mathit{Sat}(\varphi')$.

$$\frac{a \in \mathsf{Must}(s') \qquad L'(s',a',\varphi') = \top}{\tilde{L}((s,s'),a,\tilde{\varphi'}^{\top}) = \top}, \tag{5}$$

where $\tilde{\varphi}^{\top} \in C(S \times S')$ *is such that* $\tilde{\mu} \in \mathit{Sat}(\tilde{\varphi})$ *iff both*

there exists $\varphi \in C(S)$ *such that* $L(s,a,\varphi) \neq \bot$ *and the distribution* $\mu : t \to \sum_{t' \in S'} \tilde{\mu}((t,t'))$ *is in* $Sat(\varphi)$, *and*

the distribution $\mu' : t' \to \sum_{t \in S} \tilde{\mu}((t,t'))$ *is in* $Sat(\varphi')$.

We now show that conjunction is the greatest lower bound with respect to refinement [28], i.e. for all APAs N_1, N_2 and N_3, $(N_1 \preceq_W N_2) \wedge (N_1 \preceq_W N_3) \iff N_1 \preceq_W (N_2 \mathbin{\mathbb{O}} N_3)$. In fact, we can show a more elaborated result, that is conjunction coincides with the intersection of sets of (stuttering) implementations: for all N_1 and N_2, $[\![N_1]\!] \cap [\![N_2]\!] = [\![N_1 \mathbin{\mathbb{O}} N_2]\!]$. We first show that conjunction is sound.

Lemma 1 (Conjunction is sound). *Given two APAs N_1 and N_2, it holds that* $[\![N_1 \owedge N_2]\!]^* \subseteq [\![N_1]\!]^* \cap [\![N_2]\!]^*$.

Proof. Let $N_1 = (S_1, A, L_1, AP, V_1, s_0^1)$ and $N_2 = (S_2, A, L_2, AP, V_2, s_0^2)$ be two APAs, and let $N_1 \owedge N_2 = (S \times S', A \cup A', \tilde{L}, \Sigma \cup \Sigma', \tilde{V}, (s_0^1, s_0^2))$ be their conjunction, defined as in [28].

Let $P = (S, A', L, AP, V, s_0)$ be a PA such that $P \models^* N_1 \owedge N_2$. We prove that $P \models^* N_1$ and $P \models^* N_2$. Let $\mathcal{R} \subseteq S \times (S_1 \times S_2)$ be the stuttering relation witnessing $P \models^* N_1 \owedge N_2$. Define the relations $\mathcal{R}_1 \subseteq S \times S_1$ and $\mathcal{R}_2 \subseteq S \times S_2$ such that $(s, s_1) \in \mathcal{R}_1$ iff there exists $s_2 \in S_2$ such that $(s, (s_1, s_2)) \in \mathcal{R}$ and $(s, s_2) \in \mathcal{R}_2$ iff there exists $s_1 \in S_1$ such that $s, (s_1, s_2) \in \mathcal{R}$. We prove that $\mathcal{R}_1$ is a stuttering satisfaction relation. The proof for $\mathcal{R}_2$ is symmetric.
Let $s \in S$ and $s_1 \in S_1$ such that $(s, s_1) \in \mathcal{R}_1$ By construction there exists $s_2 \in S_2$ such that $(s, (s_1, s_2)) \in \mathcal{R}$.

1. Let $a \in A$ and $\varphi^1 \in C(S_1)$ such that $L_1(s_1, a, \varphi^1) = \top$. By construction of $N_1 \owedge N_2$, there exists $\tilde{\varphi} \in C(S_1 \times S_2)$ such that $\tilde{(L)}((s_1, s_2), a, \tilde{\varphi}) = \top$, and $\tilde{\varphi}$ is such that $\tilde{\mu} \in Sat(\tilde{\varphi})$ iff the distribution $\mu^1 : s_1' \mapsto \sum_{s_2' \in S_2} \tilde{\mu}((s_1', s_2'))$ is in $Sat(\varphi_1)$ and there exists $\varphi_2 \in C(S_2)$ such that $L_2(s_2, a, \varphi_2) \neq \bot$ and the distribution $\mu_2 : s_2' \mapsto \sum_{s_1' \in S_1} \tilde{\mu}((s_1', s_2'))$ is in $Sat(\varphi_2)$.
   By $\mathcal{R}$, there exists $\mu^* \in Dist(S)$ such that $s \xrightarrow[\mathcal{H}]{a}{}^* \mu^*$ and there exists $\tilde{\mu} \in Sat(\tilde{\varphi})$ such that $\mu^* \Subset_{\mathcal{R}} \tilde{\mu}$. Let $\mu^1 : s_1' \mapsto \sum_{s_2' \in S_2} \tilde{\mu}((s_1', s_2'))$ be the projection of $\tilde{\mu}$ on S_1. By construction of $\tilde{\varphi}$, we have $\mu^1 \in Sat(\varphi_1)$. Let $\tilde{\delta}$ be the correspondence function such that $\mu^* \Subset^{\tilde{\delta}}_{\mathcal{R}} \tilde{\mu}$ and define δ_1 such that, for all $s' \in S$ and $s_1' \in S_1$, $\delta_1(s')(s_1') = \sum_{s_2' \in S_2} \tilde{\delta}(s')(s_1', s_2')$. By construction, δ_1 is a correspondence function and we have $\mu^* \Subset^{\delta_1}_{\mathcal{R}_1} \mu^1$.
2. Let $\mu^* \in Dist(S)$ and $a \in A$ such that $s \xrightarrow[\mathcal{H}]{a}{}^* \mu^*$. By $\mathcal{R}$, there exists $\tilde{\varphi}_1, \ldots \tilde{\varphi}_n \in C(S_1 \times S_2)$ such that for all i, $\tilde{L}((s_1, s_2), a, \tilde{\varphi}_i) \neq \bot$ and there exists $\rho_i \in [0, 1]$ and $\tilde{\mu}_i \in Sat(\tilde{\varphi}_i)$ such that $\sum_i \rho_i = 1$ and $\mu^* \Subset_{\mathcal{R}} (\sum_i \rho_i \tilde{\mu}_i)$.
   By construction of $N_1 \owedge N_2$, there exists $\varphi_1^1, \ldots \varphi_n^1 \in C(S_1)$ such that for all i, $L_1(s_1, a, \varphi_i^1) \neq \bot$ and $\mu_i^1 : s_1' \mapsto \sum_{s_2' \in S_2} \tilde{\mu}_i((s_1', s_2')) \in Sat(\varphi_i)$. As a consequence, as above, we have $\mu^* \Subset_{\mathcal{R}_1} (\sum_i \rho_i \mu_i^1)$.
3. By construction, $V_P(s) \in \tilde{V}((s_1, s_2)) = V_1(s_1) \cap V_2(s_2)$, thus $V_P(s) \in V_1(s_1)$.

Finally, $\mathcal{R}_1$ is a stuttering satisfaction relation. Moreover, we have $s_0 \, \mathcal{R}(s_0^1, s_0^2)$, thus $s_0 \, \mathcal{R}_1 \, s_0^1$ and $P \models^* N_1$. Symmetrically, $P \models^* N_2$. Finally, we have $[\![N_1 \owedge N_2]\!]^* \subseteq [\![N_1]\!]^* \cap [\![N_2]\!]^*$. □

We now show that conjunction is complete.

Lemma 2 (Conjunction is complete). *Given two APAs N_1 and N_2, it holds that* $[\![N_1]\!]^* \cap [\![N_2]\!]^* \subseteq [\![N_1 \owedge N_2]\!]^*$.

Proof. Let $N_1 = (S_1, A, L_1, AP, V_1, s_0^1)$ and $N_2 = (S_2, A, L_2, AP, V_2, s_0^2)$ be two APAs, and let $N_1 \owedge N_2 = (S \times S', A \cup A', \tilde{L}, \Sigma \cup \Sigma', \tilde{V}, (s_0^1, s_0^2))$ be their conjunction, defined as in [28].

Let $P = (S, A', L, AP, V, s_0)$ be a PA such that $P \models^* N_1$ and $P \models^* N_2$. We prove that $P \models^* N_1 \owedge N_2$. Let $\mathcal{H} = A' \setminus A$. Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be the stuttering satisfaction relations associated to $P \models^* N_1$ and $P \models^* N_2$ respectively. Let $\mathcal{R} \subseteq S \times (S_1 \times S_2)$ be the relation such that $s\,\mathcal{R}(s_1, s_2)$ iff $s\,\mathcal{R}_1\,s_1$ and $s\,\mathcal{R}_2\,s_2$. We prove that $\mathcal{R}$ is a stuttering satisfaction relation.
Let $s \in S$ and $(s_1, s_2) \in S_1 \times S_2$ be such that $s\,\mathcal{R}(s_1, s_2)$. By construction, we have $s\,\mathcal{R}_1\,s_1$ and $s\,\mathcal{R}_2\,s_2$.

1. Let $a \in A$ and $\tilde{\varphi} \in C(S_1 \times S_2)$ such that $\tilde{L}((s_1, s_2), a, \tilde{phi}) = \top$. By construction of $N_1 \owedge N_2$, there are two cases.
   (a) There exists $\varphi_1 \in C(S_1)$ such that $L_1(s_1, a, \varphi_1) = \top$ and $\tilde{\varphi}$ is such that $\tilde{\mu} \in Sat(\tilde{\varphi})$ iff the distribution $\mu_1 : s_1' \mapsto \sum_{s_2' \in S_2} \tilde{\mu}((s_1', s_2'))$ is in $Sat(\varphi_1)$ and there exists $\varphi_2 \in C(S_2)$ such that $L_2(s_2, a, \varphi_2) \neq \bot$ and the distribution $\mu_2 : s_2' \mapsto \sum_{s_1' \in S_1} \tilde{\mu}((s_1', s_2'))$ is in $Sat(\varphi_2)$.
   (b) There exists $\varphi_2 \in C(S_2)$ such that $L_2(s_2, a, \varphi_2) = \top$ and $\tilde{\varphi}$ is such that $\tilde{\mu} \in Sat(\tilde{\varphi})$ iff the distribution $\mu_2 : s_2' \mapsto \sum_{s_1' \in S_1} \tilde{\mu}((s_1', s_2'))$ is in $Sat(\varphi_2)$ and there exists $\varphi_1 \in C(S_1)$ such that $L_1(s_1, a, \varphi_1) \neq \bot$ and the distribution $\mu_1 : s_1' \mapsto \sum_{s_2' \in S_2} \tilde{\mu}((s_1', s_2'))$ is in $Sat(\varphi_1)$.

   Assume that case (a) holds (case (b) is symmetric). Then, by $\mathcal{R}_1$, there exists a distribution $\mu^* \in Dist(S)$ such that $s \xrightarrow[\mathcal{H}]{a} {}^*\mu^*$ and there exists $\mu_1 \in Sat(\varphi_1)$ such that $\mu^* \Subset_{\mathcal{R}_1} \mu_1$. Moreover, by $\mathcal{R}_2$, there exists $\varphi_2 \in C(S_2)$ such that $L_2(s_2, a, \varphi_2) \neq \bot$ and there exists $\mu_2 \in Sat(\varphi_2)$ such that $\mu^* \Subset_{\mathcal{R}_2} \mu^2$. Let δ^1 and δ^2 be the associated correspondence functions, and let $\tilde{\mu}$ be the distribution such that for all $s_1' \in S_1$ and $s_2' \in S_2$, $\tilde{\mu}((s_1', s_2')) = \mu_1(s_1)\mu_2(s_2)$. By construction, we have $\tilde{\mu} \in Sat(\tilde{\varphi})$. Let $\delta : S \to ((s_1 \times S_2) \to [0, 1])$ be such that, for all $s \in S$, $s_1' \in S_1$ and $s_2' \in S_2$, $\delta(s)((s_1', s_2')) = \delta^1(s_1')\delta^2(s_2')$. Again, by construction, we have that $\mu \Subset_{\mathcal{R}}^{\delta} \tilde{\mu}$.
   Thus there exists $\mu^* \in Dist(S)$ such that $s \xrightarrow[\mathcal{H}]{a} {}^*\mu^*$ and there exists $\tilde{\mu} \in Sat(\tilde{\varphi})$ such that $\mu^* \Subset_{\mathcal{R}} \tilde{\mu}$.
2. Let $\mu^* \in Dist(S)$ and $a \in A$ such that $s \xrightarrow[\mathcal{H}]{a} {}^*\mu^*$. By $\mathcal{R}_1$ and $\mathcal{R}_2$, there exist constraints $\varphi_1^1, \ldots \varphi_n^1 \in C(S_1)$ and $\varphi_1^2, \ldots \varphi_m^2 \in C(S_2)$ such that for all i, j, $L_1(s_1, a, \varphi_i^1) \neq \bot$, $L_2(s_2, a, \varphi_j^2) \neq \bot$, and there exist distributions $\mu_i^1 \in Sat(\varphi_i^1)$

and $\mu_j^2 \in Sat(\varphi_j^2)$ and coefficients ρ_i^1, $\rho_j^2 \in [0,1]$ such that $\sum_i \rho_i^1 = \sum_j \rho_j^2 = 1$ and $\mu^* \Subset_{\mathcal{R}_1} (\sum_i \rho_i^1 \mu_i^1)$ and $\mu^* \Subset_{\mathcal{R}_2} (\sum_j \rho_j^2 \mu_j^2)$. Thus, by construction of $N_1 \oslash N_2$, there exist constraints $\tilde{\varphi_{i,j}} \in C(S_1 \times S_2)$ such that $\tilde{L}((s_1,s_2),a,\tilde{\varphi_{i,j}}) =?$ and $\tilde{\mu_{i,j}} \in Sat(\tilde{\varphi_{i,j}})$ iff the distribution $\mu_{i,j}^1 : s_1' \mapsto \sum_{s_2' \in S_2} \tilde{\mu_{i,j}}((s_1',s_2'))$ is in $Sat(\varphi_i^1)$ and the distribution $\mu_{i,j}^2 : s_2' \mapsto \sum_{s_1' \in S_1} \tilde{\mu_{i,j}}((s_1',s_2'))$ is in $Sat(\varphi_j^2)$.
Let $\tilde{\mu_{i,j}}$ be the distributions such that $\tilde{\mu_{i,j}} : (s_1',s_2') \mapsto \mu_i^1(s_1')\mu_j^2(s_2')$. As above, we have that for all i,j, $\tilde{\mu_{i,j}} \in Sat(\tilde{\varphi_{i,j}})$. Moreover, $\sum_{i,j} \rho^1 i \rho_j^2 = 1$ and $\mu^* \Subset_{\mathcal{R}} \sum_{i,j} \rho_i^1 \rho_j^2 \tilde{\mu_{i,j}}$.

3. By construction, $V_P(s) \in V_1(s_1)$ and $V_P(s) \in V_2(s_2)$, thus $V_P(s) \in \tilde{V}((s_1,s_2)) = V_1(s_1) \cap V_2(s_2)$.

Thus, $\mathcal{R}$ is a stuttering satisfaction relation. Moreover, we have $s\,\mathcal{R}(s_0^1,s_0^2)$ by construction, thus $P \models^* N_1 \oslash N_2$. Finally, we have $[\![N_1]\!]^* \cap [\![N_2]\!]^* \subseteq [\![N_1 \oslash N_2]\!]^*$. □

From the above two lemmas, it follows that the conjunction of two APAs exactly represents the intersection of their sets of implementations.

Theorem 3. *Given two APAs N_1 and N_2, it holds that $[\![N_1]\!]^* \cap [\![N_2]\!]^* = [\![N_1 \oslash N_2]\!]^*$.*

Proof. The above theorem holds by double inclusion, following Lemmas 1 and 2. □

4. Logical characterization

We now turn our attention to proposing a modal logic *ML-(A)PA* for PAs and APAs. This logic resembles the Probabilistic Modal Logic PML [16, 17]. The main differences between PML and ML-(A)PA are that (1) ML-(A)PA is designed to specify properties for both PAs and APAs, while PML is restricted to PAs, (2) The semantics of ML-(A)PA for PAs considers stuttering transitions, while PML does not, and finally (3) unlike PML, ML-(A)PA is disjunction and negation-free. We first give the syntax of ML-(A)PA and semantics for PAs and APAs, then we study its soundness and completeness.

$$\psi ::= V_{\text{val}} \quad | \quad \psi_1 \wedge \psi_2 \quad | \quad \langle a \rangle_{\triangleright p} \psi' \quad | \quad [a]_{\triangleright p} \psi',$$

where $V_{\text{val}} \in 2^{2^{AP}}$, $a \in A$, $\triangleright \in \{\geq, >\}$, and p is a rational in $[0,1]$. Let $F(A,AP)$ be the set of formulas over A and AP.

We define the semantics of ML-(A)PA for both PAs and APAs. Let $P = (S_P, A_P, L_P, AP, V_P, s_0^P)$ be a PA and let $N = (S, A, L, AP, V, s_0)$ be an APA. Assume that $A \subseteq A_P$ is a set of actions such that $\mathcal{H} = A_P \setminus A$ is a consistent set of hidden actions for P. We define the satisfaction relation between states of P (resp. N) and formulas

	PA Semantics	**APA Semantics**
ψ	$s \models^* \psi \iff$	$s \models \psi \iff$
V_{val}	$V_P(s) \in V_{\text{val}}$	$V(s) \subseteq V_{\text{val}}$
$\psi_1 \wedge \psi_2$	$s \models^* \psi_1$ and $s \models^* \psi_2$	$s \models \psi_1$ and $s \models \psi_2$
$\langle a \rangle_{\triangleright p} \psi'$	$\exists \mu^* \in Dist(S_P)$ s.t. $s \xrightarrow[\mathcal{H}]{a}{}^* \mu^*$ and $\left(\sum_{\{s' \mid s' \models^* \psi'\}} \mu^*(s') \triangleright p\right)$	$\exists \varphi \in C(S)$ s.t. $L(s,a,\varphi) = \top$ and $\left(\forall \mu \in Sat(\varphi) : \sum_{\{s' \mid s' \models \psi'\}} \mu(s') \triangleright p\right)$
$[a]_{\triangleright p} \psi'$	$\forall \mu^* \in Dist(S_P)$, if $s \xrightarrow[\mathcal{H}]{a}{}^* \mu^*$, then $\left(\sum_{\{s' \mid s' \models^* \psi'\}} \mu^*(s') \triangleright p\right)$	$\forall \varphi \in C(S)$, if $L(s,a,\varphi) \neq \bot$, then $\left(\forall \mu \in Sat(\varphi) : \sum_{\{s' \mid s' \models \psi'\}} \mu(s') \triangleright p\right)$

Figure 8: Semantics of ML-(A)PA for PAs and APAs.

in $F(A, AP)$ by induction as in Figure 8. We say that P satisfies ψ, written $P \models^* \psi$, iff $A_P \setminus A$ is a consistent set of hidden actions for P and $s_0^P \models^* \psi$. We say that N satisfies ψ, written $N \models \psi$, iff $s_0 \models \psi$. The logic ML-(A)PA and its relation to PAs/APAs is illustrated in the following example.

Example 4. *Consider the specification of a coffee machine N given in Figure 1 and the implementation P of the coffee machine given in Figure 2. Let $A = \{r, c\}$ and $AP = \{\mathsf{ready}, \mathsf{tea}, \mathsf{coffee}\}$ and consider the following formulas in $F(A, AP)$:*

$$\psi_1 ::= [c]_{\geq 1}\{\{\mathsf{coffee}\}, \{\mathsf{tea}\}\} \qquad \psi_3 ::= \langle c \rangle_{\geq .5}\{\{\mathsf{coffee}\}\}$$
$$\psi_2 ::= [r]_{\geq 1}\left([c]_{\geq 1}\{\{\mathsf{coffee}\}, \{\mathsf{tea}\}\}\right) \qquad \psi_4 ::= \{\{\mathsf{ready}\}\} \wedge \langle c \rangle_{\geq 1}\left([r]_{\geq 1}\{\{\mathsf{ready}\}\}\right)$$

One can verify that $N \models \psi_1$, $N \models \psi_2$ and $N \models \psi_4$ and that N does not satisfy ψ_3. Indeed, state C of N does not satisfy the formula $\{\{\mathsf{coffee}\}\}$. However, one can verify that $P \models^* \psi_1 \wedge \psi_2 \wedge \psi_3 \wedge \psi_4$. In particular, the satisfaction of ψ_3 is ensured by the existence of a distribution μ^* given in Figure 3 such that $1 \xrightarrow[\{e,\, m\}]{c}{}^* \mu^*$ in P and $\mu^*(\{\mathsf{coffee}\}) = .5$.

We now show that ML-(A)PA is sound and complete with respect to stutter satisfaction. We start with soundness: for all APA $N = (S, A, L, AP, V, s_0)$ and for all formula $\psi \in F(A, AP)$, if N satisfies ψ, then all (stuttering) implementations of N also satisfy ψ. This is formalized in the following theorem.

Theorem 4 (Soundness). *Let $N = (S, A, L, AP, V, s_0)$ be an APA and $\psi \in F(A, AP)$ be a formula. If $N \models \psi$, then for all PA $P = (S_P, A_P, L_P, AP, V_P, s_0^P)$ such that $P \models^* N$, it holds that $P \models^* \psi$.*

Proof. If N is inconsistent, i.e. $[\![N]\!]^* = \emptyset$, then the theorem trivially holds. Let $N = (S, A, L, AP, V, s_0)$ be a consistent APA, and assume that N is pruned, i.e. N has no inconsistent states. Let $\psi \in F(A, AP)$ such that $N \models \psi$. Let $P = (S_P, A_P, L_P, AP, V_P, s_0^P)$ such that $P \models^* N$. Let $\mathcal{H} = A_P \setminus A$ be the set of hidden actions in P. Since $P \models^* N$, we know that $\mathcal{H}$ is a consistent set of hidden actions for P. Let $\mathcal{R}_\mathcal{H}$ be the stutter satisfaction relation witnessing $P \models^* N$. We now prove that $P \models^* \psi$ by induction on the structure of ψ.

Base case Assume that $\psi = V_{\text{val}} \in 2^{2^{AP}}$. Since $N \models \psi$, we have $s_0 \models V_{\text{val}}$. Thus, $V(s_0) \subseteq V_{\text{val}}$. Since $P \models^* N$, we have $V_P(s_0^P) \in V(s_0)$. As a consequence, $V_P(s_0^P) \in V_{\text{val}}$ and $s_0^P \models^* V_{\text{val}}$. Therefore, $P \models^* \psi$.

Inductive step There are three cases that we treat separately.

1. $\wedge$. Assume that $\psi = \psi_1 \wedge \psi_2$. Since $N \models \psi$, we have that $s_0 \models \psi_1$ and $s_0 \models \psi_2$. By induction, we thus have that $s_0^P \models^* \psi_1$ and $s_0^P \models^* \psi_2$. As a consequence, we have $s_0^P \models^* \psi_1 \wedge \psi_2$, and therefore $P \models^* \psi$.

2. $\langle\ \rangle$. Assume that $\psi = \langle a \rangle_{\triangleright p} \psi'$. Since $N \models \psi$, there must exist $\varphi \in C(S)$ such that $L(s_0, a, \varphi) = \top$, and for all $\mu \in Sat(\varphi)$,

$$\sum_{\{s' \mid s' \models \psi'\}} \mu(s') \triangleright p.$$

By $\mathcal{R}_\mathcal{H}$, there must exists a distribution $\mu^* \in Dist(S_P)$ such that $s_0^P \xrightarrow{a}_\mathcal{H}{}^* \mu^*$ and there exist $\mu \in Sat(\varphi)$ such that $\mu^* \Subset_{\mathcal{R}_\mathcal{H}} \mu$.

By definition of $\Subset_{\mathcal{R}_\mathcal{H}}$, we know that there exists a correspondence function $\delta : S_P \to (S \to [0,1])$ such that

$$\sum_{\{s' \in S \mid s' \models \psi'\}} \mu(s') = \sum_{\{s' \in S \mid s' \models \psi'\}} \sum_{s_P{}' \in S_P} \mu^*(s_P{}')\delta(s_P{}')(s').$$

By induction, we have that if $s' \models \psi'$, then for all $s_P{}' \in S_P$ such that $(s'_P, s') \in \mathcal{R}_\mathcal{H}$, it holds that $s'_P \models^* \psi'$. Thus, for all $s'_P \in S_P$, if $s_P{}' \not\models^* \psi'$, then $(s'_P, s') \notin$

$\mathcal{R}_{\mathcal{H}}$, thus $\delta(s_P{}')(s') = 0$. Therefore,

$$\begin{aligned}\sum_{\{s' \in S \mid s' \models \psi'\}} \mu(s') &= \sum_{\{s' \in S \mid s' \models \psi'\}} \sum_{\{s_P{}' \in S_P \mid s_P{}' \models^* \psi'\}} \mu^*(s_P{}')\delta(s_P{}')(s') \\ &= \sum_{\{s_P{}' \in S_P \mid s_P{}' \models^* \psi'\}} \sum_{\{s' \in S \mid s' \models \psi'\}} \mu^*(s_P{}')\delta(s_P{}')(s') \\ &= \sum_{\{s_P{}' \in S_P \mid s_P{}' \models^* \psi'\}} \left(\mu^*(s_P{}') \sum_{\{s' \in S \mid s' \models \psi'\}} \delta(s_P{}')(s') \right).\end{aligned}$$

Since for all $s'_P \in S_P$, it holds that $\sum_{s' \in S} \delta(s'_P)(s') = 1$, we thus have

$$\sum_{\{s' \in S \mid s' \models \psi'\}} \mu(s') \leq \sum_{\{s_P{}' \in S_P \mid s_P{}' \models^* \psi'\}} \mu^*(s_P{}').$$

Moreover, we have by induction that $\sum_{\{s' \in S \mid s' \models \psi'\}} \mu(s') \rhd p$, thus $\sum_{\{s_P{}' \in S_P \mid s_P{}' \models^* \psi'\}} \mu^*(s_P{}') \geq \sum_{\{s' \in S \mid s' \models \psi'\}} \mu(s') \rhd p$. Therefore, $s_0^P \models^* \langle a \rangle_{\rhd p} \psi'$ and $P \models^* \psi$.

3. $[\ ]$. Assume that $\psi = [a]_{\rhd p} \psi'$. Since $N \models \psi$, we have that for all $\varphi \in C(S)$ such that $L(s_0, a, \varphi) \neq \bot$ and for all $\mu \in Sat(\varphi)$, it holds that

$$\sum_{\{s' \in S \mid s' \models \psi'\}} \mu(s') \rhd p.$$

Let $\mu^* \in Dist(S_P)$ such that $s_0^P \xrightarrow[\mathcal{H}]{a}{}^* \mu^*$. By $\mathcal{R}_{\mathcal{H}}$, there must exist $\varphi_1, \ldots \varphi_n \in C(S)$ such that, for all i, $L(s_0, a, \varphi_i) \neq \bot$, and there must exist $c_i \in [0, 1]$ and $\mu_i \in Sat(\varphi_i)$ such that $\sum_i c_i = 1$ and $\mu^* \Subset_{\mathcal{R}_{\mathcal{H}}} (\sum_i c_i \mu_i)$. Let $\mu = \sum_i c_i \mu_i$.

By definition of $\Subset_{\mathcal{R}_{\mathcal{H}}}$, there must exist a correspondence function $\delta : S_P \to (S \to [0, 1])$ such that

$$\sum_{\{s' \in S \mid s' \models \psi'\}} \mu(s') = \sum_{\{s' \in S \mid s' \models \psi'\}} \sum_{s_P{}' \in S_P} \mu^*(s_P{}')\delta(s_P{}')(s').$$

Since $s_0 \models \psi$, we know that for all i, we have

$$\sum_{\{s' \in S \mid s' \models \psi'\}} \mu_i(s') \rhd p.$$

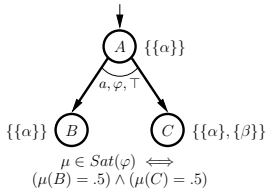


Figure 9: APA $N_{\leq}$ such that $N_{\leq} \not\models \psi_5$.

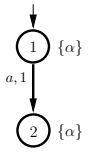


Figure 10: PA $P_{\leq}$ such that $P_{\leq} \models^* N_{\leq}$ and $P_{\leq} \not\models^* \psi_5$.

Therefore, we also have:

$$\begin{aligned}\sum_{\{s' \in S \mid s' \models \psi'\}} \mu(s') &= \sum_{\{s' \in S \mid s' \models \psi'\}} \sum_i c_i \mu_i(s') \\ &= \sum_i c_i \Big(\sum_{\{s' \in S \mid s' \models \psi'\}} \mu_i(s') \Big) \\ &\rhd \sum_i c_i p = p.\end{aligned}$$

As above, we can prove that $\sum_{\{s_P' \in S_P \mid s_P' \models^* \psi'\}} \mu^*(s_P') \rhd p$.

Therefore, we have that for all $\mu^* \in Dist(S_P)$ such that $s_0^P \xrightarrow[\mathcal{H}]{a}{}^* \mu^*$, it holds that $\sum_{\{s_P' \in S_P \mid s_P' \models^* \psi'\}} \mu^*(s_P') \rhd p$. Thus $s_0^P \models^* [a]_{\rhd p}\psi'$ and $P \models^* \psi$.

□

It is worth mentioning that soundness would not hold if ML-(A)PA was equipped with negation or with the comparison operators $\{<, \leq\}$. This is illustrated in the following example.

Example 5. *Assume that ML-(A)PA is equipped with the dual comparison operator $\leq$. Consider the formula $\psi_5 ::= [a]_{\leq .5}\{\{\alpha\}\}$.*
Consider APA $N_{\leq}$ given in Figure 9. Since $\{\{\alpha\}, \{\beta\}\} \not\subseteq \{\{\alpha\}\}$, we have that state C of $N_{\leq}$ does not satisfy $\{\{\alpha\}\}$. It thus follows that $N_{\leq} \not\models \psi_5$. Now consider PA $P_{\leq}$ given in Figure 10. One can verify that $P_{\leq} \models^* N_{\leq}$. However, since state 2 of $P_{\leq}$ satisfies $\{\{\alpha\}\}$, we have that $P_{\leq} \not\models^* \psi_5$. A similar example can be produced to prove that ML-(A)PA would not be sound if equipped with negation.

We now show that ML-(A)PA is complete with respect to stutter satisfaction, i.e. for all APA $N = (S, A, L, AP, V, s_0)$ and for all formula $\psi \in F(A, AP)$, if all (stutter) implementations of N satisfy ψ then N also satisfies ψ. This is formalized in the following theorem.

Theorem 5 (Completeness). *Let $N = (S, A, L, AP, V, s_0)$ be a consistent APA and let $\psi \in F(A, AP)$. It holds that $(\forall P \in [\![N]\!]^*, P \not\models^* \psi) \Longrightarrow N \not\models \psi$.*

This theorem is proved using induction on the structure of the formula. Given an APA $N = (S, A, L, AP, V, s_0)$, we use the notation (N, s) for the APA N with initial state s_0 replaced by s.

Proof. We give a proof for the contraposition of the statement:

$$N \not\models \psi \Longrightarrow \exists P \in [\![N]\!]^* : P \not\models^* \psi.$$

Let $N = (S, A, L, AP, V, s_0)$ be a consistent APA, and assume that N is pruned. Let ψ be a formula such that $N \not\models \psi$. The proof uses induction on the structure of ψ. For each case, we build an implementation P of N such that $P \not\models^* \psi$. Notice that stuttering satisfaction for APAs reduces to probabilistic satisfaction when the set of hidden actions is empty. Moreover, recall that the classical notion of implementation presented in [11] implies probabilistic satisfaction. In the following, we prove that

$$N \not\models \psi \Longrightarrow \exists P \in [\![N]\!]_{\mathbb{P}} : P \not\models^* \psi.$$

Since for all APA N, $[\![N]\!]_{\mathbb{P}} \subseteq [\![N]\!]^*$, this is enough to prove the theorem.

Base case Assume that $\psi = V_{\text{val}} \in 2^{2^{AP}}$. Since $N \not\models \psi$, we have that $V(s_0) \not\subseteq V_{\text{val}}$. Thus, there exists $v \in V(s_0)$ such that $v \notin V_{\text{val}}$. Let $P = (S_P, A, L_P, AP, V_P, s_0^P)$ be a PA such that $P \models_{\mathbb{P}} N$ and $V_P(s_0^P) = v$. Such a P exists because N is consistent. Since $V_P(s_0^P) = v \notin V_{\text{val}}$, we have that $s_0^P \not\models^* V_{\text{val}}$, and therefore $P \not\models^* \psi$.

Inductive step There are three cases that we treat separately.

1. $\wedge$. Assume that $\psi = \psi_1 \wedge \psi_2$. Since $N \not\models \psi$, we have $s_0 \not\models \psi_1$ or $s_0 \not\models \psi_2$. Assume that $s_0 \not\models \psi_1$; By induction, there exists $P = (S_P, A, L_P, AP, V_P, s_0^P) \in [\![N]\!]^*$ such that $s_0^P \not\models^* \psi_1$, thus $s_0^P \not\models^* \psi_1 \wedge \psi_2 = \psi$. The other case is symmetric.

2. $\langle\ \rangle$. Assume that $\psi = \langle a \rangle_{\triangleright p} \psi'$. Since $N \not\models \psi$, we have that for all $\varphi \in C(S)$ such that $L(s_0, a, \varphi) = \top$, there exists a distribution $\mu_{\text{bad}}^{\varphi} \in Sat(\varphi)$ such that

$$\sum_{\{s \mid s \models \psi'\}} \mu_{\text{bad}}^{\varphi}(s) \not\triangleright p.$$

For all $s \in S$ we define the following:

- If $s \models\!\!\!\models \psi'$, then by soundness and consistency, there exists an implementation $P_s = (S_s, A, L_{P_s}, AP, V_{P_s}, t_0^s)$ that probabilistically satisfies (N, s) and such that $P_s \models\!\!\!\models^* \psi'$. Let $\mathcal{R}_s \subseteq S_s \times S$ be the satisfaction relation witnessing $P_s \models_{\mathbb{P}} (N, s)$.
- If $s \not\models\!\!\!\models \psi'$, then by induction, there exists a PA $P_s = (S_s, A, L_{P_s}, AP, V_{P_s}, t_0^s)$ such that $P_s \models_{\mathbb{P}} (N, s)$ and $P_s \not\models\!\!\!\models^* \psi'$. Let $\mathcal{R}_s \subseteq S_s \times S$ the probabilistic satisfaction relation witnessing $P_s \models_{\mathbb{P}} (N, s)$.

We now provide an implementation P that probabilistically sastisfies N and such that $P \not\models\!\!\!\models^* \psi$. Let $P = (S_P, A, L_P, AP, V_P, s_i)$, where $S_P := \{s_i\} \cup \bigcup_{s \in S} S_s$. The initial state s_i of P will mimic all must-transitions from s_0 to the initial states of P_s, for all $s \in S$.

- For all $\varphi \in C(S)$ st. $L(s_0, a, \varphi) = \top$, recall that there exists a distribution $\mu^{\varphi}_{\text{bad}} \in Sat(\varphi)$ such that $\sum_{\{s \in S \mid s \models\!\!\!\models \psi'\}} \mu^{\varphi}_{\text{bad}}(s) \not\rhd p$. Given such a constraint φ and the associated distribution $\mu^{\varphi}_{\text{bad}}$, define the distribution $\rho^{\varphi} \in Dist(S_P)$ as follows: for all $t \in S_P$, if there exists $s \in S$ such that $t = t_0^s$, then $\rho^{\varphi}(t) = \mu^{\varphi}_{\text{bad}}(s)$. Otherwise, $\rho^{\varphi}(t) = 0$.

  Define the following transitions in P: for all $\varphi \in C(S)$ such that $L(s_0, a, \varphi) = \top$, let $L_P(s_i, a, \rho^{\varphi}) = \top$.
- By consistency, we know that for all $b \in A \setminus \{a\}$ and $\varphi \in C(S)$ st. $L(s_0, b, \varphi) = \top$, there exists at least one distribution $\mu^{\varphi} \in Sat(\varphi)$. Given such a constraint φ, we pick up arbitrarily one distribution $\mu^{\varphi} \in Sat(\varphi)$ and define $\rho^{\varphi} \in Dist(S_P)$ as follows: for all $t \in S_P$, if there exists $s \in S$ such that $t = t_0^s$, then $\rho^{\varphi}(t) = \mu^{\varphi}(s)$. Otherwise, $\rho^{\varphi}(t) = 0$.

  Define the following transitions in P: for all $b \in A \setminus \{a\}$ and for all $\varphi \in C(S)$ such that $L(s_0, b, \varphi) = \top$, let $L_P(s_i, b, \rho^{\varphi}) = \top$.
- Let $V_P(s_i)$ be chosen arbitrarily in $V(s_0)$.

All potential successors t of s_i in P, are the initial states t_0^s of PAs P_s. This is illustrated in Figure 11.

Formally, for all $s \in S$ and $t \in S_s$, define the following:

- for all $b \in A$ and $\mu \in Dist(S_s)$ such that $L_{P_s}(t, b, \mu) = \top$, let $L_P(t, b, \rho^{\mu}) = \top$ with $\rho^{\mu} \in Dist(S_P)$ defined as follows.

$$\rho^{\mu}(t') = \begin{cases} \mu(t') & \text{if } t' \in S_s \\ 0 & \text{otherwise.} \end{cases}$$

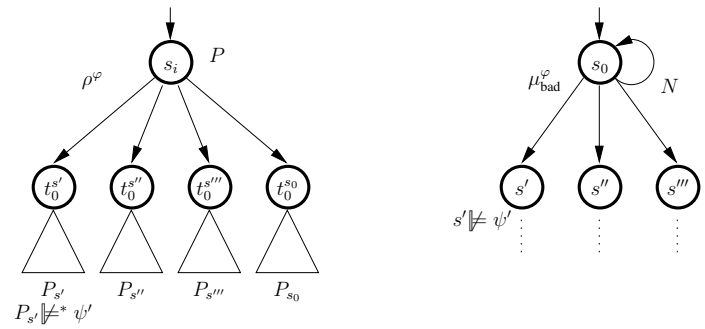


Figure 11: Constructing P from N (only illustrating μ^φ_{bad} in N, and not the full constraint).

- $V_P(t) = V_{P_s}(t)$

We now show that $P \models_{\mathbb{P}} N$. Define the relation $\mathcal{R} = \{(s_i, s_0)\} \cup \bigcup_{s' \in S} \mathcal{R}_{s'}$ over $S_P \times S$. We now prove that $\mathcal{R}$ is a probabilistic satisfaction relation.

Let $(t, s) \in \mathcal{R}$.

- If $(t, s) = (s_i, s_0)$, then
  - Let $b \in A$ and $\varphi \in C(S)$ st. $L(s_0, b, \varphi) = \top$. By construction of P, there exists $\rho^\varphi \in Dist(S_P)$ st. $L_P(s_i, b, \rho^\varphi) = \top$. Define the correspondence function $\delta : S_P \to (S \to [0, 1])$ such that $\delta(t')(s') = 1$ if $t' = t_0^{s'}$ and $\delta(t')(s') = 0$ otherwise. Then, by construction, there exists $\mu \in Sat(\varphi)$ such that $\rho^\varphi \Subset^\delta_{\mathcal{R}} \mu$.
  - Let $b \in A$ and $\rho \in Dist(S_P)$ st. $L_P(s_i, b, \rho) = \top$. By construction, there must exist a constraint $\varphi \in C(S)$ such that $L(s_0, b, \varphi) \neq \bot$ and $\rho = \rho^\varphi$. As above, there thus exists $\mu \in Sat(\varphi)$ such that $\rho^\varphi \Subset_{\mathcal{R}} \mu$.
  - $V_P(s_i) \in V(s_0)$,
- If (t, s) is not (s_i, s_0), then there exists $s'' \in S$ such that $(t, s) \in \mathcal{R}_{s''}$. As a consequence, remark that $t \in S_{s''}$.
  - Let $b \in A$ and $\varphi \in C(S)$ st. $L(s, b, \varphi) = \top$. By $\mathcal{R}_{s''}$, there exists $\mu \in Dist(S_{s''})$ such that $L_{P_{s''}}(t, b, \mu) = \top$ and there exists a correspondence function $\delta : S_{s''} \to (S \to [0, 1])$ and a distribution $\mu' \in Sat(\varphi)$ such that $\mu \Subset^\delta_{\mathcal{R}_{s''}} \mu'$.
    Define the correspondence function $\delta_P : S_P \to (S \to [0, 1])$ such that $\delta_P(t')(s') = \delta(t')(s')$ if $t' \in S_{s''}$, and $\delta_P(t')(s') = 0$ otherwise.

Let $\rho^\mu \in Dist(S_P)$ such that $\rho^\mu(t') = \mu(t')$ if $t' \in S_{s''}$, and $\rho^\mu(t') = 0$ otherwise. By construction, we have that $L_P(t, b, \rho^\mu) = \top$. We now show that $\rho^\mu \Subset^{\delta_P}_{\mathcal{R}} \mu'$.

* Let $t' \in S_P$ such that $\rho^\mu(t') > 0$. By construction we thus have $t' \in S_{s''}$, and

$$\sum_{s' \in S} \delta_P(t')(s') = \sum_{s' \in S} \delta(t')(s') = 1.$$

* Let $s' \in S$. We have

$$\sum_{t' \in S_P} \rho^\mu(t')\delta_P(t')(s') = \sum_{t' \in S_{s''}} \mu(t')\delta(t')(s') = \mu'(s').$$

* If $\delta_P(t')(s') > 0$, then $t' \in S_{s''}$ and $\delta(t')(s') > 0$. By $\mathcal{R}_{s''}$, we thus have $(t', s') \in \mathcal{R}_{S_{s''}}$ and therefore, $(t', s') \in \mathcal{R}$.

Finally, there exists $\rho^\mu \in Dist(S_P)$ such that $L_P(t, b, \rho^\mu) = \top$ and there exists $\mu' \in Sat(\varphi)$ such that $\rho^\mu \Subset_{\mathcal{R}} \mu'$.

– Let $b \in A$ and $\rho \in Dist(S_P)$ st. $L_P(t, b, \rho) = \top$. By construction, there exists a distribution $\mu \in Dist(S_{s''})$ such that $\rho = \rho^\mu$ and $L_{P_{s''}}(t, b, \mu) = \top$. Thus, by $\mathcal{R}_{s''}$, there exists $\varphi_1, \dots \varphi_n \in C(S)$ such that $L(s, b, \varphi_i) \neq \bot$, and there exists $\mu_i \in Sat(\varphi_i)$ and $c_i \in [0, 1]$ such that $\sum_i c_i = 1$ and $\mu_P \Subset_{\mathcal{R}} (\sum_i c_i\mu_i)$. Let $\mu' = \sum_i c_i\mu_i$ and $\delta : S_{s''} \to (S \to [0, 1])$ be the correspondence function witnessing $\mu \Subset^{\delta}_{\mathcal{R}_{s''}} \mu'$.
Define the correspondence function $\delta_P : S_P \to (S \to [0, 1])$ such that $\delta_P(t')(s') = \delta(t')(s')$ if $t' \in S_{s''}$, and $\delta_P(t')(s') = 0$ otherwise. As above, we can prove that $\rho \Subset^{\delta_P}_{\mathcal{R}} \mu'$.
Finally, there exists $\varphi_1, \dots \varphi_n \in C(S)$ such that $L(s, b, \varphi_i) \neq \bot$ and there exists $\mu_i \in Sat(\varphi_i)$ and $c_i \in [0, 1]$ such that $\sum_i c_i = 1$ and $\rho \Subset_{\mathcal{R}} (\sum_i c_i\mu_i)$.

– Since $(t, s) \in \mathcal{R}_{s''}$, we have that $V_{P_{s''}}(t) \in V(s)$. Since $V_P(t) = V_{P_{s''}}(t)$, we thus have $V_P(t) \in V(s)$.

Finally, $\mathcal{R}$ is a probabilistic satisfaction relation. Since, by construction, we have $(s_i, s_0) \in \mathcal{R}$, we conclude that $P \models_{\mathbb{P}} N$.

We now prove that $P \not\models^* \psi = \langle a \rangle_{\triangleright p}\psi'$. Let $\rho \in Dist(S_P)$ such that $s_i \xrightarrow[\emptyset]{a}{}^* \rho$. Since P is non-stuttering, this amounts to $L_P(s_i, a, \rho) = \top$. By definition, for all $t \in S_P$, if $\rho(t) > 0$, then there exists $\varphi \in C(S)$ and $\mu^{\varphi}_{\text{bad}} \in Sat(\varphi)$ such that

for all $t' \in S_P$, if there exists $s \in S$ such that $t' = t_0^s$, then $\rho(t) = \mu_{\text{bad}}^{\varphi}(s)$ and otherwise $\rho(t) = 0$. Moreover, by construction of P, if $s' \in S$ and $s' \not\models \psi'$, then $t_0^{s'} \not\models^* \psi'$. As a consequence, we have

$$\sum_{\{t \in S_P \mid t \models^* \psi'\}} \rho(t) = \sum_{\left\{s \in S \mid t_0^s \models^* \psi'\right\}} \rho(t_0^s) \leq \sum_{\{s \in S \mid s \models \psi'\}} \mu_{\text{bad}}^{\varphi}(s) \not\triangleright p.$$

Therefore, $P \not\models^* \langle a \rangle_{\triangleright p} \psi$.

3. [ ]. Assume that $\psi = [a]_{\triangleright p} \psi'$. Since $N \not\models \psi$, there exists a constraint $\varphi_{\text{bad}} \in C(S)$ st. $L(s_0, a, \varphi_{\text{bad}}) \neq \bot$ and there exists a distribution $\mu_{\text{bad}} \in Sat(\varphi_{\text{bad}})$ such that

$$\sum_{\{s \in S \mid s \models \psi'\}} \mu_{\text{bad}}(s) \not\triangleright p.$$

For all $s \in S$ we define the following:

- if $s \models \psi$, then by soundness and consistency, there exists an implementation $P_s = (S_s, A, L_{P_s}, AP, V_{P_s}, t_0^s)$ such that $P_s \models_{\mathbb{P}} (N, s)$ and $P_s \models^* \psi$. Let $\mathcal{R}_s \subseteq S_s \times S$ be the satisfaction relation witnessing $P_s \models_{\mathbb{P}} (N, s)$.
- if $s \not\models \psi'$, then, by induction, there exists an implementation $P_s = (S_s, A, L_{P_s}, AP, V_{P_s}, t_0^s)$ such that $P_s \models_{\mathbb{P}} (N, s)$ and $P_s \not\models^* \psi'$. Let $\mathcal{R}_s \subseteq S_s \times S$ be the probabilistic satisfaction relation witnessing $P_s \models_P (N, s)$.

Using a similar implementation P as the one defined in the previous case, we obtain that $P \models_{\mathbb{P}} N$ and $P \not\models^* \psi$.

□

It is worth mentioning that completeness would not hold if ML-(A)PA was equipped with disjunction. This is illustrated in the following example, adapted from [8].

Example 6. *Let $N_\vee = (\{A, B\}, \{a\}, L_\vee, \{\alpha, \beta\}, V_\vee, A)$ be an APA such that $V_\vee(A) = V_\vee(B) = \{\{\alpha\}\}$ and $L(A, a, \varphi) =?$ with $\mu \in Sat(\varphi)$ iff $\mu(B) = 1$. Assume that ML-(A)PA is extended with disjunction and consider the formula $\psi_6 ::= \langle a \rangle_{\geq 1}\{\{\alpha\}\} \vee [a]_{\geq 1}\{\{\beta\}\}$. Since state A does not have any must transition, we have that $N_\vee \not\models \langle a \rangle_{\geq 1}\{\{\alpha\}\}$. Moreover, since $V_\vee(B) \not\subseteq \{\{\beta\}\}$, we have that $N_\vee \not\models [a]_{\geq 1}\{\{\beta\}\}$. As a consequence, $N_\vee \not\models \psi_6$. However, any implementation of $N_\vee$ either contains no transition at all, thus satisfying $[a]_{\geq 1}\{\{\beta\}\}$, or it contains a transition leading to $\{\alpha\}$ with probability 1, thus satisfying $\langle a \rangle_{\geq 1}\{\{\alpha\}\}$. As a consequence, $\forall P \in [\![N_\vee]\!]^*, P \models^* \psi_6$.*

In addition to being sound and complete with respect to stutter satisfaction, ML-(A)PA also matches the notion of conjunction of APAs, as shown in the following theorem.

Theorem 6. *Let N_1 and N_2 be two APAs and let ψ_1 and ψ_2 be two formulas. If $N_1 \Vdash \psi_1$ and $N_2 \Vdash \psi_2$ then $(N_1 \otimes N_2) \Vdash (\psi_1 \wedge \psi_2)$.*

Proof. Let N_1 and N_2 be two APAs and let ψ_1 and ψ_2 be two formulas such that $N_1 \models_A \psi_1$ and $N_2 \models_A \psi_2$. We know that conjunction of APAs matches the intersection of their sets of implementations. Thus for all PA P such that $P \models N_1 \wedge N_2$, we have $P \models N_1$ and $P \models N_2$. By soundness of our logic, we thus have $P \models \psi_1$ and $P \models \psi_2$. Thus $P \models \psi_1 \wedge \psi_2$. Hence, for all P such that $P \models N_1 \wedge N_2$, it holds that $P \models \psi_1 \wedge \psi_2$. Thus, by completeness of the logic, it holds that $N_1 \wedge N_2 \models_A \psi_1 \wedge \psi_2$. □

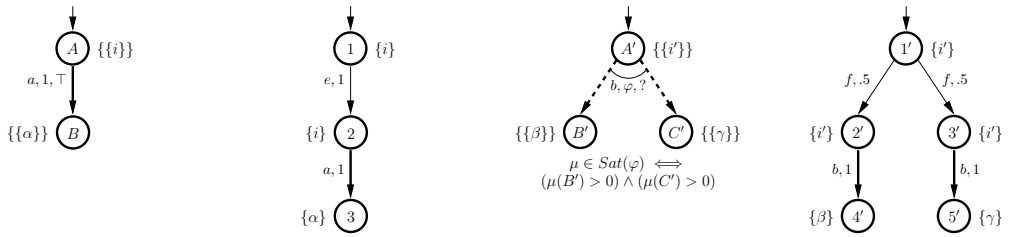
5. On composition of APAs and Stuttering

We now show that the notion of structural composition that allows to combine APAs does not preserve precongruence of refinement. Consider the classical notion of composition between PAs, originally proposed by Segala [12] and extended to the setting of APAs [11]. This notion of composition allows to synchronize on a common set of actions $\bar{A}$ while allowing independent progress on the complement of $\bar{A}$. When composing APAs, the resulting constraint represents products of distributions satisfying the original constraints. We recall the formal definition of composition of APAs from [11, 28].

Definition 10 (Parallel composition of APAs [28]). *Let $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A', L', AP', V', s'_0)$ be APAs and assume $AP \cap AP' = \emptyset$. The parallel composition of N and N' w.r.t. synchronization set $\bar{A} \subseteq A \cap A'$, written as $N \|_{\bar{A}} N'$, is given as $N \|_{\bar{A}} N' = (S \times S', A \cup A', \tilde{L}, AP \cup AP', \tilde{V}, (s_0, s'_0))$ where*

- *$\tilde{L}$ is defined as follows:*
  - *For all $(s, s') \in S \times S'$, $a \in \bar{A}$, if there exists $\varphi \in C(S)$ and $\varphi' \in C(S')$, such that $L(s, a, \varphi) \neq \bot$ and $L'(s', a, \varphi') \neq \bot$, define $\tilde{L}((s, s'), a, \tilde{\varphi}) = L(s, a, \varphi) \sqcap L'(s', a, \varphi')$ with $\tilde{\varphi}$ the new constraint in $C(S \times S')$ such that $\tilde{\mu} \in Sat(\tilde{\varphi})$ iff there exists $\mu \in Sat(\varphi)$ and $\mu' \in Sat(\varphi')$ such that $\tilde{\mu}(u, v) = \mu(u) \cdot \mu'(v)$ for all $u \in S$ and $v \in S'$.*

    If either for all $\varphi \in C(S)$, we have $L(s, a, \varphi) = \bot$, or $\forall \varphi' \in C(S')$, we have $L'(s', a, \varphi') = \bot$ then for all $\tilde{\varphi} \in C(S \times S')$, $\tilde{L}((s, s'), a, \tilde{\varphi}) = \bot$.



(a) APA N_1. (b) Stuttering PA P_1 such that $P_1 \models^* N_1$. Internal action is e. (c) APA N_2. (d) Stuttering PA P_2 such that $P_2 \models^* N_2$. Internal action is f.

Figure 12: APA specifications and stuttering PA implementations showing that $(P_1 \parallel_\emptyset P_2) \not\models^* (N_1 \parallel_\emptyset N_2)$.

  - *For all* $(s, s') \in S \times S'$, $a \in A \setminus \bar{A}$, *and for all* $\varphi \in C(S)$, *define* $\tilde{L}((s, s'), a, \tilde{\varphi}) = L(s, a, \varphi)$ *with* $\tilde{\varphi}$ *the new constraint in* $C(S \times S')$ *such that* $\tilde{\mu} \in Sat(\tilde{\varphi})$ *iff for all* $u \in S$ *and* $v \neq s'$, $\tilde{\mu}(u, v) = 0$ *and the distribution* μ *such that* $\mu(t) = \tilde{\mu}(t, s')$ *is in* $Sat(\varphi)$.
  - *For all* $(s, s') \in S \times S'$, $a \in A' \setminus \bar{A}$, *and for all* $\varphi' \in C(S')$, *define* $\tilde{L}((s, s'), a, \tilde{\varphi}') = L'(s', a, \varphi')$ *with* $\tilde{\varphi}'$ *the new constraint in* $C(S \times S')$ *such that* $\tilde{\mu}' \in Sat(\tilde{\varphi}')$ *iff for all* $u \neq s$ *and* $v \in S'$, $\tilde{\mu}'(u, v) = 0$ *and the distribution* μ' *such that* $\mu'(t') = \tilde{\mu}'(s, t')$ *is in* $Sat(\varphi')$.

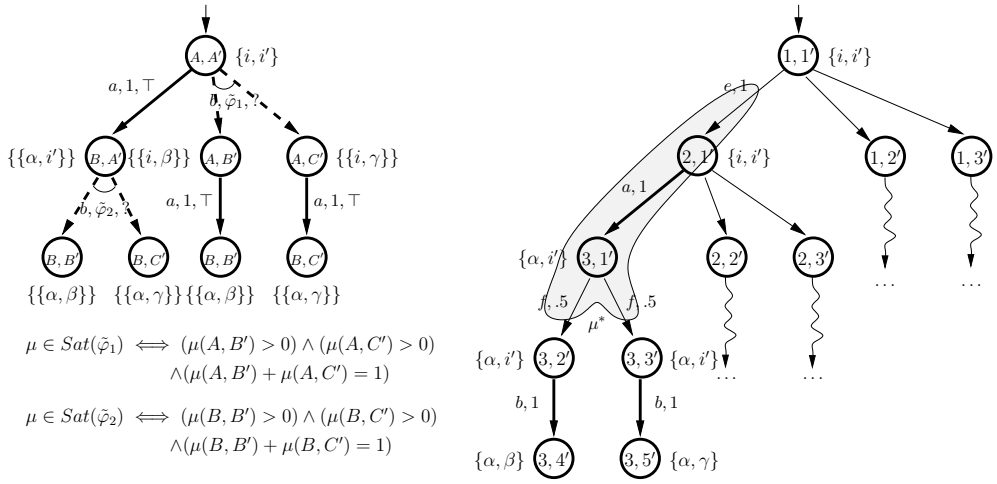
- $\tilde{V}$ *is defined as follows: for all* $(s, s') \in S \times S'$, $\tilde{V}((s, s')) = \{\tilde{B} = B \cup B' \mid B \in V(s)$ *and* $B' \in V'(s')\}$.

Unfortunately, the notion of stuttering satisfaction as presented in Section 3 is not compatible with composition. This is formalized in the following theorem.

Theorem 7. *There exists two compatible (in the sense of composition) PAs* P_1 *and* P_2 *and two compatible (in the sense of composition) APAs* N_1 *and* N_2 *such that* $P_1 \models^* N_1$, $P_2 \models^* N_2$ *and* $P_1 \parallel_{\bar{A}} P_2 \not\models^* N_1 \parallel_{\bar{A}} N_2$.

Proof. Consider PAs P_1 and P_2 and APAs N_1 and N_2 given in Figure 12. We have that $P_1 \models^* N_1$ and $P_2 \models^* N_2$. Let $\bar{A} = \emptyset$ be the synchronization set. The composition of the specifications $N = N_1 \parallel_\emptyset N_2$ is given in Figure 13a. The composition of implementations $P = P_1 \parallel_\emptyset P_2$ is partly sketched in Figure 13b. Let μ^* be the distribution in $P_1 \parallel_\emptyset P_2$ such that $\mu^*(3, 2') = \mu^*(3, 3') = .5$. The stuttering transition $(1, 1') \xrightarrow[\{e,\, f\}]{a} {}^*\mu^*$ in P is shown in Figure 13b.

States $(3, 2')$ and $(3, 3')$ of P cannot satisfy state (B, A') of N. Indeed, the outgoing transitions of states $(3, 2')$ and $(3, 3')$ cannot be redistributed to satisfy constraint



(a) APA $N = N_1 \parallel_\emptyset N_2$.

(b) Stuttering transition in $P = P_1 \parallel_\emptyset P_2$.

Figure 13: APA $N_1 \parallel_\emptyset N_2$ and stuttering transition in $P_1 \parallel_\emptyset P_2$ preventing satisfaction.

$\tilde{\varphi}_2$. As a consequence, the transition $(1, 1') \xrightarrow[\{e,f\}]{a} {}^*\mu^*$ in P cannot match the transition $(A, A') \xrightarrow{a,1} (B, A')$ in N. Thus $(P_1 \parallel_\emptyset P_2) \not\models^* (N_1 \parallel_\emptyset N_2)$. □

The reason for this setback is the well known problem of distributed scheduling [34]. When composing two stuttering PAs, one allows interleaving of atomic stuttering steps from both sides, which generates extra behaviors. Our solution is to transform a PA P with a consistent set of hidden actions $\mathcal{H}$ into a non-stuttering PA $\widehat{P}^{\mathcal{H}}$ that satisfies the same APA specifications as P. This transformation removes stuttering by computing all the distributions that can be reached with stuttering in P and inserting them in the transition function of $\widehat{P}^{\mathcal{H}}$.

Definition 11. *Let $P = (S_P, A_P, L_P, AP, V_P, s_0^P)$ be a PA and let $\mathcal{H}$ be a consistent set of hidden actions for P. Define the PA $\widehat{P}^{\mathcal{H}} = (S_P, A_P \setminus \mathcal{H}, \widehat{L}_P^{\mathcal{H}}, AP, V_P, s_0^P)$ such that*

$$\forall s \in S, a \in A_P \setminus \mathcal{H}, \mu \in Dist(S),\ \widehat{L}_P^{\mathcal{H}}(s, a, \mu) = \top \iff s \xrightarrow[\mathcal{H}]{a} {}^*\mu \text{ in } P.$$

By construction, $\widehat{P}^{\mathcal{H}}$ is such that for all APA $N = (S, A_P \setminus \mathcal{H}, L, AP, V, s_0)$, we have

$$P \models^* N \iff \widehat{P}^{\mathcal{H}} \models N.$$

We have the following theorem.

Theorem 8. *Let* $P_1 = (S_P^1, A_P^1, L_P^1, AP^1, V_P^1, s_0^{P_1})$ *and* $P_2 = (S_P^2, A_P^2, L_P^2, AP^2, V_P^2, s_0^{P_2})$ *be two PAs such that* $AP^1 \cap AP^2 = \emptyset$*. Let* $N_1 = (S^1, A^1, L^1, AP^1, V^1, s_0^1)$ *and* $N_2 = (S^2, A^2, L^2, AP^2, V^2, s_0^2)$ *be APAs such that* $\mathcal{H}_1 = A_P^1 \setminus A_1$ *and* $\mathcal{H}_2 = A_P^2 \setminus A_2$ *are consistent sets of hidden actions for* P_1 *and* P_2 *respectively, with* $\mathcal{H}_1 \cap A_2 = \mathcal{H}_2 \cap A_1 = \emptyset$*. For all* $\bar{A} \subseteq A_1 \cap A_2$*, we have the following:*

$$\text{if } P_1 \models^* N_1 \text{ and } P_2 \models^* N_2 \text{ then } \widehat{P_1}^{\mathcal{H}_1} \parallel_{\bar{A}} \widehat{P_2}^{\mathcal{H}_2} \models N_1 \parallel_{\bar{A}} N_2.$$

6. Future work

As future work, we plan to extend our study to other operations on APAs which have been left out in this paper. In particular, once the APA framework is equipped with a quotienting operator, studying the relation between stuttering and quotienting will be of great interest. We also plan on extending specifications with stuttering. This is complex as one will have to define a notion of may/must stutter transition in the specification APAs. The main problem is the constraints on distributions: the recursive step in the stutter transitions will have to take into account and propagate that the stutter remains valid for any solution of the constraints.

References

[1] B. Delahaye, K. G. Larsen, A. Legay, Stuttering for abstract probabilistic automata, in: LFCS, LNCS, Springer, 2013.

[2] T. A. Henzinger, J. Sifakis, The embedded systems design challenge, in: FM, Vol. 4085 of LNCS, Springer, 2006, pp. 1–15.

[3] H. Hermanns, U. Herzog, J. Katoen, Process algebra for performance evaluation, TCS 274 (1-2) (2002) 43–87.

[4] L. de Alfaro, T. A. Henzinger, Interface automata, in: FSE, ACM Press, 2001, pp. 109–120.

[5] N. Lynch, M. R. Tuttle, An introduction to Input/Output automata, CWI-quarterly 2 (3).

[6] K. G. Larsen, Modal specifications, in: AVMS, Vol. 407 of LNCS, 1989, pp. 232–246.

[7] J.-B. Raclet, Quotient de spécifications pour la réutilisation de composants, Ph.D. thesis, Université de Rennes I, (In French) (december 2007).

[8] S. S. Bauer, L. Juhl, K. G. Larsen, A. Legay, J. Srba, Extending modal transition systems with structured labels, MSCS 22 (2012) 1–37.

[9] B. Caillaud, B. Delahaye, K. G. Larsen, A. Legay, M. L. Pedersen, A. Wasowski, Constraint markov chains, Theor. Comput. Sci. 412 (34) (2011) 4373–4404.

[10] B. Delahaye, K. G. Larsen, A. Legay, M. L. Pedersen, A. Wąsowski, New Results on Constraint Markov Chains, Performance EvaluationTo appear.

[11] B. Delahaye, J.-P. Katoen, K. Larsen, A. Legay, M. Pedersen, F. Sher, A. Wąsowski, Abstract probabilistic automata., in: VMCAI, LNCS, Springer, 2011.

[12] R. Segala, N. A. Lynch, Probabilistic simulations for probabilistic processes, NJC 2 (2) (1995) 250–273.

[13] S. Mitra, N. A. Lynch, Proving approximate implementations for probabilistic i/o automata, Electr. Notes Theor. Comput. Sci. 174 (8) (2007) 71–93.

[14] N. A. Lynch, R. Segala, F. W. Vaandrager, Compositionality for probabilistic automata, in: CONCUR, Vol. 2761 of LNCS, Springer, 2003, pp. 204–222.

[15] S. S. Bauer, P. Mayer, A. Schroeder, R. Hennicker, On weak modal compatibility, refinement, and the mio workbench, in: TACAS, Vol. 6015 of LNCS, Springer, 2010, pp. 175–189.

[16] K. G. Larsen, A. Skou, Bisimulation through probabilistic testing, in: POPL, 1989, pp. 344–352.

[17] K. G. Larsen, A. Skou, Compositional verification of probabilistic processes, in: CONCUR, Vol. 630 of LNCS, Springer, 1992, pp. 456–471.

[18] R. J. van Glabbeek, The linear time - branching time spectrum ii, in: CONCUR, Vol. 715 of LNCS, Springer, 1993, pp. 66–81.

[19] A. Philippou, I. Lee, O. Sokolsky, Weak bisimulation for probabilistic systems, in: CONCUR, Vol. 1877 of LNCS, Springer, 2000, pp. 334–349.

[20] S. Andova, T. A. C. Willemse, Branching bisimulation for probabilistic systems: Characteristics and decidability, Theor. Comput. Sci. 356 (3) (2006) 325–355.

[21] C. Baier, H. Hermanns, Weak bisimulation for fully probabilistic processes, in: CAV, Vol. 1254 of LNCS, Springer, 1997, pp. 119–130.

[22] R. Segala, Modeling and verification of randomized distributed real-time systems, Ph.D. thesis, MIT (1995).

[23] S. Georgievska, Probability and hiding in concurrent processes, Ph.D. thesis, Eindhoven University of Technology (2011).

[24] C. Morgan, A. McIver, K. Seidel, J. W. Sanders, Refinement-oriented probability for csp, Formal Asp. Comput. 8 (6).

[25] G. Lowe, Representing nondeterministic and probabilistic behaviour in reactive processes, Formal Asp. Comput. 3 (1993) 1.

[26] S. Georgievska, S. Andova, Composing systems while preserving probabilities, in: EPEW, Vol. 6342 of LNCS, Springer, 2010, pp. 268–283.

[27] S. Georgievska, S. Andova, Probabilistic csp: Preserving the laws via restricted schedulers, in: MMB/DFT, Vol. 7201 of LNCS, Springer, 2012, pp. 136–150.

[28] B. Delahaye, J.-P. Katoen, K. G. Larsen, A. Legay, M. L. Pedersen, F. Sher, A. Wasowski, New Results on Abstract Probabilistic Automata, in: ACSD, IEEE Computer, 2011.

[29] R. Segala, N. Lynch, Probabilistic simulations for probabilistic processes, in: CONCUR, Vol. 836 of LNCS, springer, 1994, pp. 481–496.

[30] R. Segala, Probability and nondeterminism in operational models of concurrency, in: CONCUR, Vol. 4137 of Lecture Notes in Computer Science, Springer, 2006, pp. 64–78.

[31] C. Eisentraut, H. Hermanns, L. Zhang, On probabilistic automata in continuous time, in: LICS, IEEE Computer Society, 2010, pp. 342–351.

[32] Y. Deng, R. J. van Glabbeek, M. Hennessy, C. Morgan, Testing finitary probabilistic processes, in: CONCUR, Vol. 5710 of Lecture Notes in Computer Science, Springer, 2009, pp. 274–288.

[33] D. Fischbein, V. A. Braberman, S. Uchitel, A sound observational semantics for modal transition systems, in: ICTAC, Vol. 5684 of LNCS, Springer, 2009, pp. 215–230.

[34] S. Giro, P. R. D'Argenio, L. M. F. Fioriti, Partial order reduction for probabilistic systems: A revision for distributed schedulers, in: CONCUR, Vol. 5710 of LNCS, Springer, 2009, pp. 338–353.