Abstract Probabilistic Automata[☆]

Benoît Delahaye[a], Joost-Pieter Katoen[b], Kim G. Larsen[a], Axel Legay[c], Mikkel L. Pedersen[a], Falak Sher[b], Andrzej Wąsowski[d]

[a] *Aalborg University, Denmark*
[b] *RWTH Aachen University, Germany*
[c] *INRIA/IRISA, Rennes, France*
[d] *IT University of Copenhagen, Denmark*

Abstract

Probabilistic Automata (PAs) are a widely-recognized mathematical framework for the specification and analysis of systems with non-deterministic and stochastic behaviors. This paper proposes Abstract Probabilistic Automata (APAs), that is a novel abstraction model for PAs. In APAs uncertainty of the non-deterministic choices is modeled by may/must modalities on transitions while uncertainty of the stochastic behaviour is expressed by (underspecified) stochastic constraints. We have developed a complete abstraction theory for PAs, and also propose the first specification theory for them. Our theory supports both satisfaction and refinement operators, together with classical stepwise design operators. In addition, we study the link between specification theories and abstraction in avoiding the state-space explosion problem.

Keywords: specification; abstraction; compositional reasoning; interface automata; probabilistic automata

1. Introduction

One of the main research areas in computer science consists in studying new specification formalisms for reasoning on system's behaviors. Among existing such formalisms one finds the one of Transition Systems (TS). In TS, the behavior of the system is represented by states modeling the current values of the variables, and a relation between states, called transitions, representing the evolution of the system, i.e., update of variables. Transitions are often labeled with actions representing the possibly non-deterministic decisions taken at a

[☆]This paper is based on [1] and [2], that have appeared in the 12th International Conference on Verification, Model Checking, and Abstract Interpretation and the 11th International Conference on Application of Concurrency to System Design, respectively.

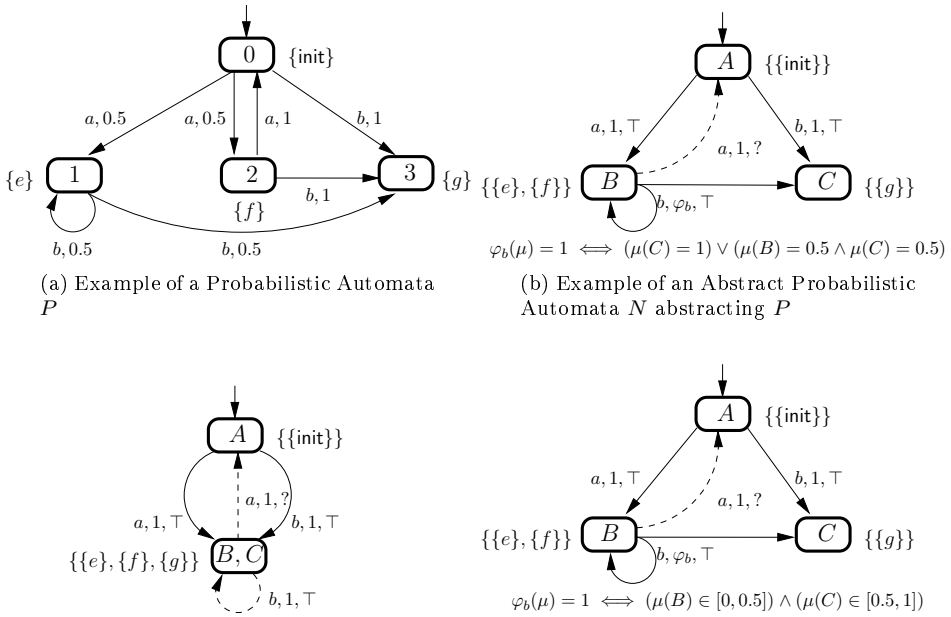
Email addresses: benoit.delahaye@irisa.fr (Benoît Delahaye), katoen@cs.rwth-aachen.de (Joost-Pieter Katoen), kgl@cs.aau.dk (Kim G. Larsen), axel.legay@irisa.fr (Axel Legay), mikkelp@cs.aau.dk (Mikkel L. Pedersen), chfalak@gmail.com (Falak Sher), wasowski@itu.dk (Andrzej Wąsowski)

given moment of time to govern this evolution. TSs are acknowledged to be a simple but elegant formalism powerful enough to capture the control-flow of programming languages; the formalism is used in most of existing formal validation techniques proposed in the literature [3].

As systems become more and more complex, it is necessary to add new features to TSs. Such features can be used either to capture new phenomena such as continuous evolution, or to reason on new properties of the system such as energy consumption. Particularly, 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 [4] point out, introducing probabilities into design theories allows assessing dependability of IT systems in the same manner as commonly practiced in other engineering disciplines.

Probabilistic Automata (PAs) constitute a mathematical framework for the specification and analysis of non-deterministic probabilistic systems. PAs are TSs whose evolution depends not only on non-deterministic actions but also on a probability distribution that, together with the action, drives the choice of the successor state. PAs have been developed by Segala [5] to model and analyze asynchronous, concurrent systems with discrete probabilistic choices in a formal and precise way. PAs are akin to Markov decision processes (MDPs). A detailed comparison with models such as MDPs, as well as generative and reactive probabilistic transition systems is given in [6]. PAs are recognized as an adequate formalism for randomized distributed algorithms and fault tolerant systems. They are used as semantics model for formalisms such as probabilistic process algebra [7] and a probabilistic variant of Harel's statecharts [8]. An input-output version of PAs is the basis of PIOA and variants thereof [9, 10]. PAs have been enriched with notions such as weak and strong (bi)simulations [5], decision algorithms for these notions [11] and a statistical testing theory [12]. This paper brings two new contributions to the field of probabilistic automata: the theories of *abstraction* and of *specification*.

As a first main contribution, we propose several abstraction techniques for PAs. Abstraction is pivotal to combating the state space explosion problem in the modeling and verification of realistic systems such as randomized distributed algorithms. It aims at model reduction by collapsing sets of concrete states to abstract states, e.g., by partitioning the concrete state space. This paper presents a three-valued abstraction of PAs. The main design principle of our model, named *Abstract Probabilistic Automata* (APAs), is to abstract sets of distributions by constraint functions. This generalizes earlier work on interval-based abstraction of probabilistic systems [13, 14, 15]. To abstract from action transitions, we introduce *may* (?) and *must* ($\top$) modalities in the spirit of modal transition systems [16]. If all states in a partition p have a must-transition on action a to some state in partition p', the abstraction yields a must-transition between p and p'. If some of the p-states have no such transition while others do, it gives rise to a may-transition between p and p'. Our model can be viewed



(a) Example of a Probabilistic Automata P

(b) Example of an Abstract Probabilistic Automata N abstracting P

(c) Example of an Abstract Probabilistic Automata N' abstracting N

(d) Example of an Abstract Probabilistic Automata N'' abstracting N

Figure 1: Examples of PA, APA and abstraction

as a combination of both Modal Automata [17] and Constraint Markov Chains (CMC) [18, 19] that are abstractions for transition systems and Markov Chains, respectively. APAs can further be abstracted by merging their states or by simplifying their corresponding constraints. We shall see that those abstractions introduce new behaviors in the corresponding PAs, but that their precision can be controlled. Concretely, the PA of Figure 1a gives the choice between two non-deterministic actions a and b, both of them inducing a probability distribution on the set of successor states. In addition, all states are equipped with sets of atomic propositions. Assuming that both state 1 and 2 belong to the same partition B and that states 0 and 3 are mapped to partitions A and C, respectively, we obtain the APA given in Figure 1b. Notice that, in order to merge states 1 and 2 into a single state B, one has to consider sets of sets of atomic propositions. There one can see that there is a must transition from A to B as any state in A goes to a state in B with action a. However, the transition from B to A is a may transition as there are states in B (here state 2) for which action a does not lead to a state in A. The case of action b illustrates the use of constraints to match the original distributions starting from states in B.

As a second major contribution, we also propose a new specification theory for PAs. Our study is motivated by the observation that several industrial sectors involving complex embedded systems have recently experienced deep

changes in their organization, aerospace and automotive being the most prominent examples. In the past, they were organized around vertically integrated companies, supporting in-house design activities from specification to implementation. Nowadays, systems are tremendously big and complex, and it is almost impossible for one single team to have the complete control of the entire chain of design from the specification to the implementation. In fact, complex systems now result from the assembling of several components. These many components are in general designed by teams, working *independently* but with a common agreement on what the interface of each component should be. Such an interface specifies the behaviors expected from the component as well as the environment in which it can be used. The main advantage is that it does not impose any constraint on the way the component is implemented, hence allowing for independent implementation. According to state of practice, interfaces are typically described using Word/Excel text documents or modeling languages such as UML/XML. We instead recommend to follow a more mathematical approach relying most possibly on mathematically sound formalisms, thus best reducing ambiguities. Our new theory is equipped with all essential ingredients of a compositional design methodology: a satisfaction relation (to decide whether a PA is an implementation of an APA), a consistency check (to decide whether the specification admits an implementation), a refinement (to compare specifications in terms of inclusion of sets of implementations), logical composition (to compute the intersection of sets of implementations), and structural composition (to combine specifications). Our framework also supports incremental design [20]. To the best of our knowledge, the theory of APAs is the first specification theory for PAs where both logical and structural compositions can be computed within the same framework.

Our notions of refinement and satisfaction are, as usual, characterized in terms of inclusion of sets of implementations. Our notion of satisfaction is a compatible extension of the classical notion of probabilistic bisimulation [5, 21]. More precisely, one can show that two PAs that are probabilistic bisimilar satisfy exactly the same APAs. One of our other important theorems shows that for the class of deterministic APAs, refinement coincides with inclusion of sets of implementations. This latter result is obtained by a reduction from APAs to CMCs, for which a similar result holds. Hence, APAs can also be viewed as a specification theory for Markov Chains (MCs). The model is as expressive as CMCs, and hence more expressive than other theories for stochastic systems such as Interval Markov Chains [13, 22, 14].

Our last contribution is to propose several *abstraction-based* methodologies that allow to simplify the behavior of APAs with respect to the refinement relation – as we pointed above, abstraction is crucial to avoid state-space explosion. We show that our abstraction preserves refinement, and that refinement is a pre-congruence with respect to parallel composition. These results provide the key ingredients to allow *compositional* abstraction of PAs. Consider again the APA N of Figure 1b. This APA can be further abstracted by merging partitions B and C, which leads to the APA N' given in Figure 1c. Since there must be an a transition from A to B in N, there is a must a transition from A to (B, C) in

N'. Inversely, since only one state out of two in (B, C) requires a b transition to B or C, the abstracted state (B, C) will allow but not require this b transition. The consequence of this abstraction is not only the reduction of the state space, but also a simplification of the constraint associated to action b in state (B, C). Another way of abstracting the APA of Figure 1b is to simplify the constraints by approximating them with intervals, as illustrated in Figure 1d.

Organisation of the paper. In Section 2, we introduce the concepts of PAs and APAs as well as several of their properties. Section 3 is concerned with several notions of refinements and abstractions as well as the relation between satisfaction and probabilistic bisimulation. Section 4 introduces the notion of consistency and structural composition (aka conjunction), while Section 5 proposes a compositional reasoning theory based on APAs. Section 6 studies the strong link between APAs and CMCs and proposes results for the class of deterministic APAs. Since all the previous results are obtained for APAs with equal sets of actions and atomic propositions, Section 7 presents a methodology for extending sets of actions and atomic propositions, showing that all our results carry over to APAs with dissimilar alphabets. Finally, Section 8 concludes the paper. For clarity of the presentation, some repetitive proofs have been lifted to an appendix.

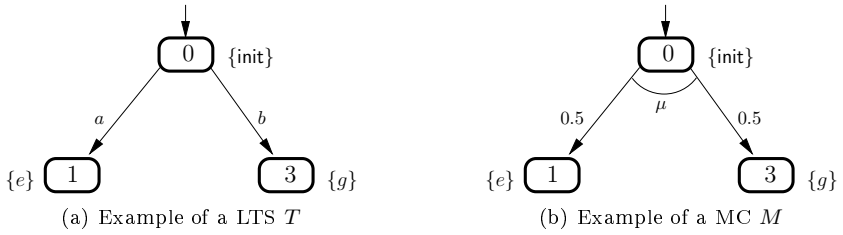
2. Specifications and Implementations

In this section, we present the basic notions used in our formalism. We first introduce the definitions of *Labeled Transition Systems (LTS)* and *Markov Chains (MC)*, which are classical notions of implementations, and then present *Probabilistic Automata (PA)*, that unify LTSs and MCs. We then introduce *Modal Transition Systems* and *Constraint Markov Chains*, two classical notions of specification theories for LTS and MC respectively. Finally, we present a new notion of *Abstract Probabilistic Automata (APA)*, a finite representation for a possibly infinite set of PAs. APAs will act as a specification theory for PAs. Let Act be a universe of actions.

Implementations. Labeled transition systems are usually used to represent non-stochastic systems. We first introduce their definition.

Definition 1 (Labeled Transition System)**.** *A* Labeled Transition System *is a tuple (S, A, L, AP, V, s_0), where S is a finite set of states with initial state $s_0 \in S$, $A \subseteq \mathsf{Act}$ is a finite set of actions, L: $S \times A \times S \to \mathbb{B}_2$ is a* two-valued *transition function, AP is a finite set of atomic propositions, and V: $S \to 2^{AP}$ is a state-labeling function.*

The set $\mathbb{B}_2 = \{\bot, \top\}$ denotes a *lattice* with the ordering $\bot < \top$ and meet ($\sqcap$) and join ($\sqcup$) operators. The transition function L identifies the *transitions* of the automaton: L associates (1) the value $\top$ to a triple (s, a, s') whenever there is a transition from state s to state s' labeled with action a, and (2) $\bot$ otherwise.



(a) Example of a LTS T (b) Example of a MC M

Figure 2: Examples of LTS and MC

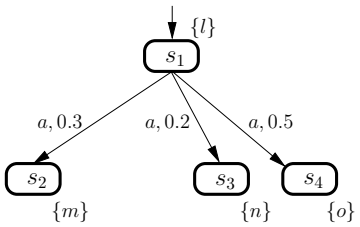


Figure 3: A PA with a single transition to a distribution $[0, 0.3, 0.2, 0.5]$

An example of a LTS T is given in Figure 2a, where transitions with value $\bot$ are left out of the picture.

When moving to the stochastic setting, the simplest notion of implementation is the one of Markov Chain.

Definition 2 (Markov Chain)**.** *A* Markov Chain *is a tuple* (S, π, AP, V, s_0)*, where* S *is a finite set of states with initial state* $s_0 \in S$*,* $\pi : S \to Dist(S)$ *is a probability transition function:* $\sum_{s' \in S} \pi(s)(s') = 1$ *for all* $s \in S$*,* AP *is a finite set of atomic propositions, and* V*:* $S \to 2^{AP}$ *is a state-labeling function.*

We use $Dist(S)$ to denote a set of *probability distributions* on the finite set S. An example of a MC M is given in Figure 2b, where transitions with probability 0 are left out of the picture.

A PA [5] resembles a LTS, but its transitions target probability distributions over states instead of single states. Hence, PAs can be seen as a combination of MCs and LTSs.

Definition 3 (Probabilistic Automata)**.** *A* probabilistic automaton (PA) *is a tuple* (S, A, L, AP, V, s_0)*, where* S *is a finite set of states with initial state* $s_0 \in S$*,* $A \subseteq \mathsf{Act}$ *is a finite set of actions,* L*:* $S \times A \times Dist(S) \to \mathbb{B}_2$ *is a* two-*valued transition function,* AP *is a finite set of atomic propositions, and* V*:* $S \to 2^{AP}$ *is a state-labeling function.*

We write $s \xrightarrow{a} \mu$ meaning $L(s, a, \mu) = \top$. In the rest of the paper, we assume that PAs are *finitely branching*, i.e., for any state s, the number of pairs (a, μ)

such that $s \xrightarrow{a} \mu$ is finite. The *labeling function* V indicates the propositions (or properties) that are valid in a state. Hence a *Markov Chain*, as defined previously, is a PA with a single action and a single outgoing transition from each state, i.e. for each $s \in S$ there exists exactly one triple (s, a, μ) such that $L(s, a, \mu) = \top$. Without loss of generality, we assume in the rest of the paper that $\mathsf{Act} \cap AP = \emptyset$ for all PAs.

Example. *Figure 3 presents a PA with* $L(s_1, a, \mu) = \top$*, where* $\mu(s_2) = 0.3$*,* $\mu(s_3) = 0.2$*, and* $\mu(s_4) = 0.5$*. We adopt a notational convention that represents* $L(s_1, a, \mu) = \top$ *by a set of arrows with tails located close to each other on the boundary of* s_1*, and heads targeting the states in the support of* μ*.*

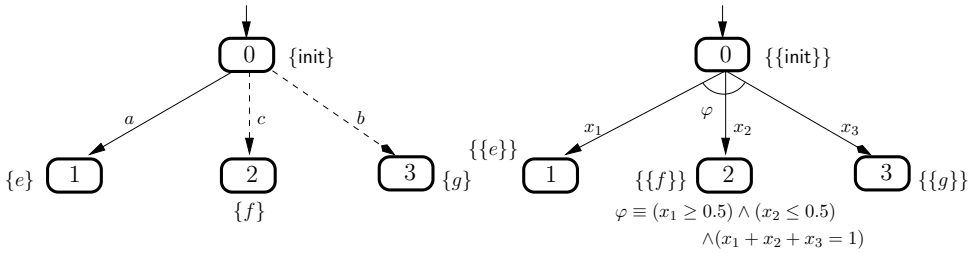
Specifications. We now introduce *Abstract Probabilistic Automata*, that is a specification formalism for PAs. APAs are the combinations of Modal Transition Systems and Constraint Markov Chains—specification formalisms for labeled transition systems and Markov Chains, respectively. We first briefly introduce Modal Transition Systems and Constraint Markov Chains, and then move to APAs.

A *Modal Transition System (MTS)* [23, 16] is an automaton whose transitions are typed with *may* and *must* modalities. Informally, a must transition is available in every model of the specification, while a may transition may be absent in some design.

Definition 4 (Modal Transition System)**.** *A* Modal Transition System *is a tuple* (S, A, L, AP, V, s_0)*, where* S *is a finite set of states with initial state* $s_0 \in S$*,* $A \subseteq \mathsf{Act}$ *is a finite set of actions,* $L\colon S \times A \times S \to \mathbb{B}_3 = \{\bot, ?, \top\}$ *is a* three-valued transition function*,* AP *is a finite set of atomic propositions, and* $V\colon S \to 2^{AP}$ *is a state-labeling function. Transitions* (s, a, s') *with* $L(s, a, s') =?$ *are called* may *transitions, and transitions* (s, a, s') *with* $L(s, a, s') = \top$ *are called* must *transitions.*

Here, $\mathbb{B}_3 = \{\bot, ?, \top\}$ denotes a *lattice* with the ordering $\bot < ? < \top$ and meet ($\sqcap$) and join ($\sqcup$) operators. An example of an MTS N is given in Figure 4a. There, and throughout the paper, may transitions are represented by dashed arrows and must transitions by plain ones. One can easily see that LTS T given in Figure 2a is an implementation of N. Indeed, the must transition from state 0 to state 1 with action a in N is present in T, while the transition from state 0 to state 3 with action c in T corresponds to a may transition in N and all state labels are matching.

A *Constraint Markov Chain* (CMC) [18, 19] is a MC equipped with a constraint on the next-state probabilities from any state. Roughly speaking, an implementation of a CMC is a MC, whose next-state probability distributions satisfy the constraint associated with each state. A constraint function $\varphi : \mathit{Dist}(S) \to \{0, 1\}$ represents a set of distributions on S. Let $\mathit{Sat}(\varphi)$ denote the set of distributions μ that satisfy constraint function φ (i.e. such that $\varphi(\mu) = 1$), and $C(S)$ the set of constraint functions defined on state space S.



(a) Example of a MTS N

(b) Example of a CMC C

Figure 4: Examples of MTS and CMC

Definition 5 (Constraint Markov Chain)**.** *A* Constraint Markov Chain *is a tuple $C = (S, \psi, AP, V, s_0)$ where S is a finite set of states with initial state $s_0 \in S$, $\psi : S \to C(S)$ is a state-constraint function, AP is a set of atomic propositions, and $V : S \to 2^{2^{AP}}$ is a state labeling function.*

For each state $s \in S$, the state-constraint function ψ is such that, for all distributions π on S, $\psi(s)$ is a constraint function as defined above. Intuitively, $\psi(s)(\pi) = 1$ iff distribution π is allowed in state s. 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, thus allowing a higher level of abstraction w.r.t. implementations.

An example of a CMC C is given in Figure 4b. Remark that the MC M given in Figure 2b is an implementation of C. Indeed, the distribution μ outgoing from state 0 in M agrees with the constraint φ specified in C and the sets of atomic propositions in M are included in the labels specified in C.
A CMC whose constraints are of the form $l \leq \mu \leq r$, where l, r are constant vectors and μ is a probability distribution over the state space is called an Interval Markov Chain (IMC) [13].

We now present the central definition of the paper:

Definition 6 (Abstract Probabilistic Automata)**.** *An* Abstract Probabilistic Automaton (APA) *is a tuple (S, A, L, AP, V, s_0) where S, A, AP are finite sets of states, actions, and atomic propositions respectively, $s_0 \in S$ is the initial state, $L : S \times A \times C(S) \longrightarrow \mathbb{B}_3$ is a* three-*valued state-constraint function, and $V : S \longrightarrow 2^{2^{AP}}$ maps a state onto a set of admissible valuations.*

A CMC is thus an APA, where for each $s \in S$, there exists exactly one triple (s, a, φ) such that $L(s, a, \varphi) = \top$. The labeling $L(s, a, \varphi)$ identifies the "type" of the constraint function $\varphi \in C(S)$: $\top$, ? and $\bot$ indicate a *must*, a *may* and the absence (forbidden) of a constraint function, respectively. Without loss of generality, we assume in the rest of the paper that $\mathsf{Act} \cap AP = \emptyset$ for all APAs.

In practice, as will be seen in later definitions, a lack of value for given argument is equivalent to the $\bot$ value, so we will sometimes avoid defining

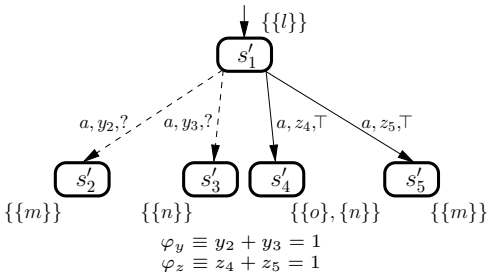


Figure 5: An APA N with two transitions: *may* to constraint φ_y and *must* to φ_z

$\perp$-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.

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.

We could have limited ourselves to constraints denoting unions of intervals. However, as for CMCs, polynomial constraints are needed to support *both* conjunction *and* parallel composition [19]. Later, we shall see that almost all APAs whose states are labelled with a set of subsets of atomic propositions can be turned into an equivalent (in the sense of implementations set) APA whose states are labeled with a set that contains only a single subset of atomic propositions.

Finally, observe that a PA is an APA in which every transition (s, a, φ) is a *must*-transition with $|Sat(\varphi)| = 1$, and each state-label consists of a single set of propositions.

Example. *Consider the APA N given in Fig. 5. State s'_1 has two outgoing transitions: a* may *a-transition (s'_1, a, φ_y) and a* must *a-transition (s'_1, a, φ_z). The φ_y and φ_z constraints are shown under the automaton in the figure.*

The constraints allow that each of the automaton's two transitions can cover multiple transitions in a concrete implementation PA. As an example, the a-transition $(s_1, a, (0, 0.3, 0.2, 0.5))$ of the PA given in Fig. 3 matches the must *a-transition (s'_1, a, φ_z): if we write $z_4 = 0.2 + 0.5$ the sum of all probabilities going to states whose valuations are in the set specified in s'_4, and $z_5 = 0.3$ the sum of all probabilities going to states whose valuations are in the set specified in s'_5, then we can verify that $z'_4 + z'_5 = 1$, hence satisfying φ_z. In order to avoid clutter, the transitions that do not admit any positive probabilities are not represented in the figures.*

In the rest of the paper we distinguish the class of deterministic APAs. The distinction will be of particular importance when comparing APAs in Section 3.1. We first present the definition of determinism for CMCs and MTS, as

introduced in [18, 19]. We say that a CMC $C = (S, \psi, AP, V, s_0)$ is deterministic if and only if for all states $s, s', s'' \in S$, if there exists $\pi' \in Dist(S)$ such that $(\psi(s)(\pi') \wedge (\pi'(s') \neq 0))$ and $\pi'' \in Dist(S)$ such that $(\psi(s)(\pi'') \wedge (\pi''(s'') \neq 0))$, then we have that $V(s') \cap V(s'') = \emptyset$.

We say that a MTS $N = (S, A, L, AP, V, s_0)$ is deterministic if and only if there is at most one outgoing transition for each action in all states, i.e. $\forall s \in S, \forall a \in A, |\{s' \mid L(s, a, s') \neq \bot\}| \leq 1$.

In APAs, the non-determinism can arise due to sets of valuations in states, like for CMCs, or due to actions that label transitions, like for MTS. Informally, an APA is (1) *action-deterministic* if there is at most one outgoing transition for each action in all states; and (2) *valuation-deterministic* if two states with overlapping atomic propositions can never be reached with the same transition. Remark that the definition for valuation-determinism is similar to the notion of determinism for CMCs presented above.

Definition 7 (Determinism)**.** *An APA $N = (S, A, L, AP, V, s_0)$ is*

- action-deterministic *if* $\forall s \in S, \forall a \in A,\ |\{\varphi \in C(S) \mid L(s, a, \varphi) \neq \bot\}| \leq 1$.
- valuation-deterministic *if* $\forall s \in S, \forall a \in A, \forall \varphi \in C(S)$ *with* $L(s, a, \varphi) \neq \bot$*:*

$$\forall \mu', \mu'' \in Sat(\varphi), s', s'' \in S,\ (\mu'(s') > 0 \wedge \mu''(s'') > 0\ \Rightarrow V(s') \cap V(s'') = \emptyset)\,.$$

An APA N is deterministic *if and only if it is action-deterministic and valuation-deterministic.*

Satisfaction. We relate APA specifications to PAs implementing them by extending the definitions of satisfaction for probabilistic systems introduced in [13]. In this section, we only consider PAs / APAs with equal sets of actions and equal sets of atomic propositions. The case of dissimilar alphabets is treated in Section 7.

The following notion of *simulation* characterizes equivalent distributions according to a given relation on sets of states. This definition is similar to the one given in [13]. In Section 3.2, we show how this notion of simulation and the subsequent notion of satisfaction are related to the classical notion of probabilistic bisimulation for probabilistic automata [5].

Definition 8 (Simulation)**.** *Let S and S' be non-empty finite sets of states. Given $\mu \in Dist(S)$, $\mu' \in Dist(S')$, a function $\delta : S \to (S' \to [0, 1])$, and a binary relation $R \subseteq S \times S'$, μ is simulated by μ' with respect to R and δ, denoted $\mu \Subset_R^\delta \mu'$, if and only if*

1. *for all $s \in S$, if $\mu(s) > 0$, then $\delta(s) \in Dist(S')$,*
2. *for all $s' \in S'$, $\sum_{s \in S} \mu(s)\delta(s)(s') = \mu'(s')$, and*
3. *for all $s, s' \in S$, if $\delta(s)(s') > 0$, then $(s, s') \in R$.*

In the rest of the paper, we write $\mu \Subset_R \mu'$ whenever there exists a function δ such that $\mu \Subset_R^\delta \mu'$. Such δ is called a correspondence function.

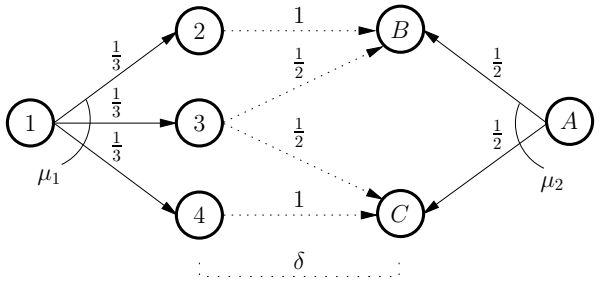


Figure 6: A simulation between distributions μ_1 and μ_2 with respect to relation $\mathcal{R} = \{(1, A), (2, B), (3, B), (3, C), (4, C)\}$ and a correspondence function δ.

Example. *Simulation is illustrated in Fig. 6, where distribution μ_1 is simulated by distribution μ_2 with respect to the relation $\mathcal{R} = \{(1, A), (2, B), (3, B), (3, C), (4, C)\}$. In the picture, the correspondence function δ is represented by the labeled dashed arrows.*

We now define a satisfaction relation between PAs and APAs. Remark that this definition is a mix between the notion of satisfaction for MTS [23, 16] and the notion of satisfaction for CMCs [18, 19].

Definition 9 (Satisfaction Relation)**.** *Let $P = (S, A, L, AP, V, s_0)$ be a PA and $N = (S', A, L', AP, V', s'_0)$ be an APA. $R \subseteq S \times S'$ is a* satisfaction relation *if and only if, for any $(s, s') \in R$, the following conditions hold:*

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

P satisfies N, denoted $P \models N$, if and only if there exists a satisfaction relation relating s_0 and s'_0. If $P \models N$, P is called an implementation *of N.*

Thus, a PA P is an implementation of an APA N if and only if any must-transition of N is matched by a must-transition of P that is simulated by one of the probability distributions specified by the constraint, and reversely, P does not contain must-transitions that do not have a corresponding (may- or must-) transition in N. The set of implementations of N is denoted by $[\![N]\!] = \{P \mid P \models N\}$.

Example. *The relation $R = \{(s_1, s'_1), (s_2, s'_5), (s_3, s'_4), (s_4, s'_4)\}$ is a satisfaction relation between the PA P (Fig. 3) and the APA N (Fig. 5). Indeed, all pairs $(s, s') \in R$ have matching valuations, and the outgoing must transition from s'_1 is matched by the outgoing transition from s_1 (see previous example).*

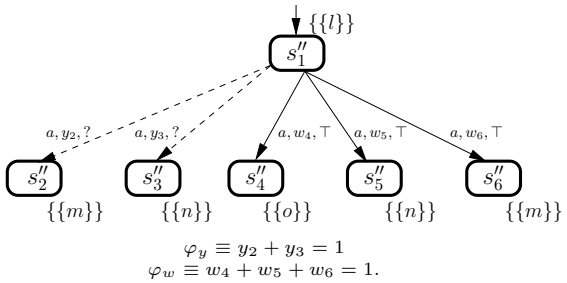


Figure 7: Normalization $\mathcal{N}(N)$ of the APA N presented in Fig. 5

Single valuation normal form. As for CMCs [18, 19], a large class of APAs whose states are labeled with a set of subsets of atomic propositions can be turned into an equivalent APA (in terms of sets of implementations) whose states are labeled with sets that contain a single subset of atomic propositions. The latter are called APAs in *single valuation normal form*. Single valuation normal form makes the manipulation of satisfaction/refinement relations easier. However, as we shall see, building the single valuation normal form of a given APA may lead to an exponential blowup in the number of states.

Definition 10 (Single Valuation Normal Form)**.** *An APA $N = (S, A, L, AP, V, s_0)$ is in* single valuation normal form *(SVNF) iff all its admissible valuations sets are singletons, i.e. $\forall s \in S, |V(s)| = 1$.*

It turns out that any APA with a single valuation in the initial state can be turned into an APA in single valuation normal form that admits the same set of implementations. This transformation is called *normalization*.

We introduce it with an example, first. Consider the APA N in Fig. 5. Since the valuation of state s'_4 is not a singleton, N is not in SVNF. In the normalization process we translate each state of the original APA into a collection of states—one per each valuation. This mapping is captured by a *normalization function*; the following function $\mathcal{N}$ is the normalization function for our example. Note that the only interesting case is for state s'_4:

$$s'_1 \mapsto \{s''_1\},\ s'_2 \mapsto \{s''_2\},\ s'_3 \mapsto \{s''_3\},\ s'_4 \mapsto \{s''_4, s''_5\},\ s'_5 \mapsto \{s''_6\}.$$

Subsequently, each probability distribution constraint targeting a split state, needs to be rewritten, so that the sum of the split probabilities, substituted for the original value, still satisfies the constraint. Applying the normalization to N results in the APA $\mathcal{N}(N)$ given in Fig. 7. State s'_4 of N is split into states s''_4 and s''_5 in $\mathcal{N}(N)$. The combined probability of reaching these states in $\mathcal{N}(N)$, namely $w_4 + w_5$, is substituted for z_4 in φ_z—the original probability of reaching s'_4 in N.

Definition 11 (Normalization)**.** *Let $N = (S, A, L, AP, V, s_0)$ be an APA. Let S' be a set of states and let $\mathcal{N} : S \to 2^{S'}$ be a function such that*

1. $S' = \bigcup_{s \in S} \mathcal{N}(s)$,
2. *For all* $s_1, s_2 \in S$ *such that* $s_1 \neq s_2$, $\mathcal{N}(s_1) \cap \mathcal{N}(s_2) = \emptyset$,
3. *for all* $s \in S$, $|\mathcal{N}(s)| = |V(s)|$.

If $|V(s_0)| = 1$, *then the normalization of* N, *denoted* $\mathcal{N}(N)$, *is the APA* $\mathcal{N}(N) = (S', A, L', AP, V', \mathcal{N}(s_0))$ *such that*

1. *For all* $s' \in S'$, $|V'(s')| = 1$,
2. *For all* $s \in S$, $V(s) = \bigcup_{s' \in \mathcal{N}(s)} V'(s')$,
3. *For all* $s \in S$, *for* $s'_1, s'_2 \in \mathcal{N}(s)$, $s'_1 \neq s'_2 \iff V'(s'_1) \neq V'(s'_2)$, *and*
4. *for all* $s \in S$ *and* $a \in A$, *if there exists* $\varphi \in C(S)$ *such that* $L(s, a, \varphi) \neq \bot$, *then for all* $s' \in \mathcal{N}(s)$, $L'(s', a, \varphi') = L(s, a, \varphi)$ *for* $\varphi' \in C(S')$ *such that* $Sat(\varphi') = \{\mu' \in Dist(S') | \mu : s \mapsto \sum_{u \in \mathcal{N}(s)} \mu'(u) \in Sat(\varphi)\}$.

Remark 1. *In the above definition, a set* S' *and a function* $\mathcal{N}$ *always exist. However, when* $|V(s_0)| \neq 1$, *any normalization of* N *would need to have several initial states, which we do not consider here.*

Clearly, $\mathcal{N}(N)$ is an APA in single valuation normal form.

The following theorem asserts that normalization preserves implementations.

Theorem 12. *For any APA* $N = (S, A, L, AP, V, s_0)$ *with* $|V(s_0)| = 1$, $[\![N]\!] = [\![\mathcal{N}(N)]\!]$.

Proof. Let $N = (S, A, L, AP, V, s_0)$ be an APA such that $|V(s_0)| = 1$, and let $\mathcal{N}(N) = (S', A, L', AP, V', \mathcal{N}(s_0))$ be the normalization of N, given the function $\mathcal{N} : S \to 2^{S'}$. We prove the two directions separately.

• $[\![N]\!] \subseteq [\![\mathcal{N}(N)]\!]$: Let $P = (S_P, A, L_P, AP, V_P, s_0^P)$ be any PA such that $P \in [\![N]\!]$ with satisfaction relation $\mathcal{R} \subseteq S_P \times S$. We show that $P \in [\![\mathcal{N}(N)]\!]$. Let $\mathcal{R}' \subseteq S_P \times S'$ be the relation such that $p \mathcal{R}' s'$ iff $(V_P(p) \in V'(s')$ and $(p \mathcal{R} \mathcal{N}^{-1}(s'))$, where $\mathcal{N}^{-1}(s')$ is the unique state s such that $s' \in \mathcal{N}(s)$. We prove that $\mathcal{R}'$ is a satisfaction relation relating s_0^P and $\mathcal{N}(s_0)$.
Let $p \in S_P$ and $s' \in S'$ be such that $p \mathcal{R}' s'$, and let $s = \mathcal{N}^{-1}(s')$. We show that $\mathcal{R}'$ satisfies the axioms of a satisfaction relation.

1. Let $a \in A$ and $\varphi' \in C(S')$ such that $L'(s', a, \varphi') = \top$. By definition of $\mathcal{N}(N)$, there must exist a constraint $\varphi \in C(S)$ such that $L(s, a, \varphi) = \top$ and for all $\mu' \in Sat(\varphi')$, the distribution $\mu : t \mapsto \sum_{u \in \mathcal{N}(t)} \mu'(u)$ is in $Sat(\varphi)$.
   Since $P \models N$, there exists $\mu_P \in Dist(S_P)$ such that $L_P(p, a, \mu_P) = \top$ and $\exists \mu \in Sat(\varphi)$ such that $\mu_P \Subset_{\mathcal{R}} \mu$. We will now show that $\exists \mu' \in Sat(\varphi')$ such that $\mu_P \Subset_{\mathcal{R}'} \mu'$.
   Let $\delta : S_P \to (S \to [0, 1])$ be the correspondence function witnessing $\mu_P \Subset_{\mathcal{R}} \mu$. Let $\delta' : S_P \to (S' \to [0, 1])$ be such that $\delta'(q)(t) = \delta(q)(\mathcal{N}^{-1}(t))$ if $V_P(q) \in V'(t)$, and 0 otherwise.
   Let μ' be the distribution on S' such that $\mu'(t) = \sum_{q \in S_P} \mu_P(q) \delta'(q)(t)$. The following holds:

(a) Let $q \in S_P$ such that $\mu_P(q) > 0$. By $\mathcal{R}$, we have that $\delta(q)$ is a distribution on S. Let $r \in S$ such that $\delta(q)(r) > 0$. By construction of $\mathcal{N}(N)$, there exists a single $t \in S'$ such that $t \in \mathcal{N}(r)$ and $V(q) \in V(t)$. As a consequence, for all $r \in S$, $\sum_{t \in \mathcal{N}(r)} \delta'(q)(t) = \delta(q)(r)$. Thus, we have $\sum_{t \in S'} \delta'(q)(t) = \sum_{r \in S} \delta(q)(r)$. Finally $\delta'(q)$ is also a distribution on S'.

(b) By construction, we have that for all $t \in S'$,

$$\mu'(t) = \sum_{q \in S_P} \mu_P(q)\delta'(q)(t).$$

(c) Let $q \in S_P$ and $t \in S'$ such that $\delta'(q)(t) > 0$. By construction of δ', we have that (1) $\delta(q)(\mathcal{N}^{-1}(t)) > 0$ and (2) $V(q) \in V(t)$. By (1), we have that $q \,\mathcal{R}\, \mathcal{N}^{-1}(t)$. As a consequence, by definition of $\mathcal{R}'$ and (2), we have $q \,\mathcal{R}'\, t$.

Thus $\mu_P \Subset_{\mathcal{R}'} \mu'$. We now prove that $\mu' \in Sat(\varphi')$. Let $\mu^0(r) = \sum_{t \in \mathcal{N}(r)} \mu'(t)$. By definition of μ', we have

$$\begin{aligned}
\mu^0(r) = \sum_{t \in \mathcal{N}(r)} \mu'(t) &= \sum_{t \in \mathcal{N}(r)} \sum_{q \in S_P} \mu_P(q)\delta'(q)(t) \\
&= \sum_{q \in S_P} \mu_P(q) \sum_{t \in \mathcal{N}(r)} \delta'(q)(t) \\
&= \sum_{q \in S_P} \mu_P(q)\delta(q)(r) = \mu(r)
\end{aligned}$$

Thus $\mu^0 = \mu \in Sat(\varphi)$ and by definition of φ', we have $\mu' \in Sat(\varphi')$.
Finally, there exists $\mu_P \in Dist(S_P)$ such that $L_P(p, a, \mu_P) = \top$ and there exists $\mu' \in Sat(\varphi')$ such that $\mu_P \Subset_{\mathcal{R}'} \mu'$.

2. Let $a \in A$ and $\mu_P \in Dist(S_P)$, such that $L_P(p, a, \mu_P) = \top$. By a similar argument, there exists $\varphi' \in C(S')$ such that $L'(s, a, \varphi') \neq \bot$ and there exists $\mu' \in Sat(\varphi')$ such that $\mu_P \Subset_{\mathcal{R}'} \mu'$.
3. By construction of $\mathcal{R}'$, we know that $V_P(p) \in V'(s')$.

We conclude that $s_0^P \,\mathcal{R}'\, \mathcal{N}(s_0)$, since $V_P(s_0^P) \in V(s_0) = V'(\mathcal{N}(s_0))$ and $s_0^R \,\mathcal{R}\, \mathcal{N}^{-1}(\mathcal{N}(s_0)))$ which is equivalent to saying that $s_0^P \,\mathcal{R}\, s_0$.

• $[\![N]\!] \supseteq [\![\mathcal{N}(N)]\!]$: Let $P = (S_P, A, L_P, AP, V_P, s_0^P)$ be any PA such that $P \in [\![\mathcal{N}(N)]\!]$ with satisfaction relation $\mathcal{R}' \subseteq S_P \times S'$ with $s_0^P \,\mathcal{R}\, s_0$. We show that $P \in [\![N]\!]$. Let $\mathcal{R} \subseteq S_P \times S$ be the relation such that $p \,\mathcal{R}\, s$ iff there exists $s' \in \mathcal{N}(s)$ such that $p \,\mathcal{R}'\, s'$. By a similar reasoning as in the previous case, $\mathcal{R}$ is a satisfaction relation and $s_0^P \,\mathcal{R}\, s_0$, thus $P \models N$.

□

In the rest of the paper, we sometimes require that APAs are in single valuation normal form in order to make the manipulation of satisfaction/refinement relations easier. By the above theorem, there is no loss of generality in making this assumption when the initial state is already in single valuation normal form. When it is not, it is equivalent to consider a set of APAs with inital states in single valuation normal form, one for each valuation of the original initial state.

3. Refinement, Bisimulation and Abstraction

Being able to compare specifications is central to stepwise design. Systematic comparison enables simplification of specifications (abstraction) and adding details to specifications (elaboration). Usually, specifications are compared using a *refinement* relation. In this section, we first introduce several notions of refinement for APAs and study their ordering. Then we show that our formalism is backward-compatible with the classical notion of bisimulation for PA [5, 21]. Finally, we propose two notions of abstraction for APAs.

3.1. Refinement

A refinement compares APAs with respect to their sets of implementations. More precisely, if APA N refines APA N', then the set of implementations of N should be included in the one of N'. The ultimate refinement relation that can be defined between APAs is thus *Thorough Refinement* that exactly corresponds to inclusion of sets of implementations.

Definition 13 (Thorough Refinement)**.** *Let $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A, L', AP, V', s'_0)$ be APAs. N thoroughly refines N', denoted $N \preceq_T N'$, iff $[\![N]\!] \subseteq [\![N']\!]$.*

For most specification theories, it is known that deciding thorough refinement is computationally intensive (see for example [24]). For many models such as Modal automata or CMCs, one can partially avoid the problem by working with a syntactical notion of refinement. This definition, which is typically strictly stronger than thorough refinement, is easier to check. The difference between syntactic and semantic refinements resembles the difference between simulations and trace inclusion for transition systems.

We consider three syntactic refinements. These relations extend two well known refinement relations for CMCs and IMCs by combining them with the refinement defined on modal automata. By tweaking the alternation of quantifiers in the associated formulas, one can define several syntactical notions of refinements with different expressivity. For the sake of completeness, we define all three notions and compare their granularity. We start with the strong refinement.

Definition 14 (Strong Refinement)**.** *Let $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A, L', AP, V', s'_0)$ be APAs. $R \subseteq S \times S'$ is a* strong refinement *relation if and only if, for all $(s, s') \in R$, 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 there exists a correspondence function* $\delta : S \to (S' \to [0, 1])$ *such that* $\forall \mu \in Sat(\varphi)$, $\exists \mu' \in Sat(\varphi')$ *with* $\mu \Subset_R^\delta \mu'$,
2. $\forall a \in A$, $\forall \varphi \in C(S)$, *if* $L(s, a, \varphi) \neq \bot$, *then* $\exists \varphi' \in C(S') : L'(s', a, \varphi') \neq \bot$ *and there exists a correspondence function* $\delta : S \to (S' \to [0, 1])$ *such that* $\forall \mu \in Sat(\varphi)$, $\exists \mu' \in Sat(\varphi')$ *with* $\mu \Subset_R^\delta \mu'$, *and*
3. $V(s) \subseteq V'(s')$.

We say that N strongly refines N', denoted $N \preceq_S N'$, if and only if there exists a strong refinement relation relating s_0 and s'_0.

Observe that strong refinement imposes a "fixed-in-advance" correspondence function δ in the simulation relation between distributions. In this way, it strongly resembles the notion of satisfaction presented in Definition 9. This assumption is lifted with the definition of *weak refinement*:

Definition 15 (Weak Refinement)**.** *Let $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A, L', AP, V', s'_0)$ be APAs. $R \subseteq S \times S'$ is a* weak refinement *relation if and only if, for all $(s, s') \in R$, 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* $\mu \Subset_R \mu'$,
2. $\forall a \in A$, $\forall \varphi \in C(S)$, *if* $L(s, a, \varphi) \neq \bot$, *then* $\exists \varphi' \in C(S') : L'(s', a, \varphi') \neq \bot$ *and* $\forall \mu \in Sat(\varphi)$, $\exists \mu' \in Sat(\varphi')$ *such that* $\mu \Subset_R \mu'$, *and*
3. $V(s) \subseteq V'(s')$.

We say that N weakly refines N', denoted $N \preceq N'$, if and only if there exists a weak refinement relation relating s_0 and s'_0.

Weak weak refinement weakens the assumption even more by allowing to choose, for each solution of the left constraint, both a different correspondence function *and* a different constraint (transition) to which it will be linked:

Definition 16 (Weak Weak Refinement)**.** *Let $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A, L', AP, V', s'_0)$ be APAs. $R \subseteq S \times S'$ is a* weak weak refinement *relation if and only if, for all $(s, s') \in R$, 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* $\mu \Subset_R \mu'$,
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* $\mu \Subset_R \mu'$, *and*
3. $V(s) \subseteq V'(s')$.

We say that N weakly weakly refines N', denoted $N \preceq_W N'$, if and only if there exists a weak weak refinement relation relating s_0 and s'_0.

It is easy to see that the above definitions are combinations of the definitions of strong and weak refinement of CMCs with the *modal refinement* of Modal Automata. Hence algorithms for checking weak weak, weak, and strong refinements for APAs can be obtained by combining existing fixed-point algorithms for CMCs [19] and Modal Automata [17]. For the class of polynomial-constraint APAs, the upper bound for deciding weak/strong refinement is thus exponential in the number of states and doubly-exponential in the size of the constraints [19]. Notice that all three refinement relations are preorders on the set of APAs.

Weak weak, weak, and strong refinement all imply inclusion of sets of implementations. However, the converse is not true. The following theorem classifies the refinement relations.

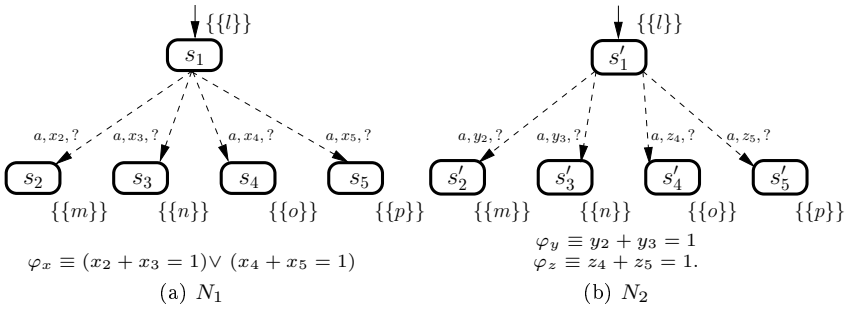


Figure 8: APAs N_1 and N_2 such that $N_1 \preceq_W N_2$, but not $N_1 \preceq N_2$.

Theorem 17. *Thorough refinement is strictly finer than weak weak refinement, weak weak refinement is strictly finer than weak refinement, and weak refinement is strictly finer than strong refinement. That is,*

$$(\preceq_T) \supsetneq (\preceq_W) \supsetneq (\preceq) \supsetneq (\preceq_S).$$

Proof. We first prove the inclusions, and then show that all of them are strict.

• $(\preceq_T) \supseteq (\preceq_W) \supseteq (\preceq) \supseteq (\preceq_S)$: By a swap of quantifiers in the definitions, it is obvious that strong refinement implies weak refinement, and that weak refinement implies weak weak refinement. We prove that weak weak refinement implies thorough refinement. Let $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A, L', AP, V', s'_0)$ be APAs such that $N \preceq_W N'$ with a weak weak refinement relation $\mathcal{R}' \subseteq S \times S'$.
If $[\![N]\!] = \emptyset$, we have $[\![N]\!] \subseteq [\![N']\!]$. Otherwise, let $P = (S_P, A, L_P, AP, V_P, s_0^P)$ be a PA such that $P \models N$. Then there exists a satisfaction relation $\mathcal{R}'' \subseteq S_P \times S$ such that $s_0^P \,\mathcal{R}''\, s_0$.
Let $\mathcal{R} \subseteq S_P \times S'$ be the relation such that $u \,\mathcal{R}\, w$ iff there exists $v \in S$ such that $u \,\mathcal{R}''\, v$ and $v \,\mathcal{R}'\, w$. The proof that $\mathcal{R}$ is a satisfaction relation is standard and follows the same lines as the proof of Theorem 12. We give the key arguments of this proof and report the details to Appendix A.

Let $u \in S_P$ and $w \in S'$ be such that $u \,\mathcal{R}\, w$, and let $v \in S$ be such that $u \,\mathcal{R}''\, v$ and $v \,\mathcal{R}'\, w$.

- Let $a \in A'$ and $\varphi' \in C(S')$ be such that $L'(w, a, \varphi') = \top$. By $\mathcal{R}'$, there exists $\varphi \in C(S)$ such that $L(v, a, \varphi) = \top$ and $\forall \mu \in Sat(\varphi), \exists \mu' \in Sat(\varphi')$ such that $\mu \Subset_{R'} \mu'$. Moreover, by $\mathcal{R}''$, there exists $\mu_P \in Dist(S_P)$ such that $L_P(u, a, \mu_P) = \top$ and $\mu_S \in Sat(\varphi)$ such that $\mu_P \Subset_{R''} \mu_S$.

  Let $\mu_S \in Dist(S)$ and $\mu' \in Dist(S')$ be such that $\mu_P \Subset_{R''} \mu_S$ and $\mu_S \Subset_{R'} \mu'$. Let $\delta'' : S_P \to (S \to [0,1])$ and $\delta' : S \to (S' \to [0,1])$ be the correspondence functions witnessing $\mu_P \Subset^{\delta''}_{R''} \mu_S$ and $\mu_S \Subset^{\delta'}_{R'} \mu'$ respectively. The correspondence function for $\mathcal{R}$ is $\delta : S_P \to (S' \to [0,1])$ such that $\delta(s)(t) = \sum_{r \in S} \delta''(s)(r)\delta'(r)(t)$. It follows that $\mu_P \Subset^{\delta}_{\mathcal{R}} \mu'$.

- Let $a \in A$ and $\mu_P \in Dist(S_P)$ be such that $L_P(u, a, \mu) \neq \bot$. By $\mathcal{R}''$, there exists $\varphi \in C(S)$ such that $L(v, a, \varphi) \neq \bot$ and $\exists \mu_S \in Sat(\varphi)$ such that $\mu_P \Subset_{R''} \mu_S$. Moreover, by $\mathcal{R}'$, we have that for all $\mu \in Sat(\varphi)$, there exists $\varphi' \in C(S')$ such that $L'(w, a, \varphi') \neq \bot$ and $\mu' \in Sat(\varphi')$ such that $\mu \Subset_{R'} \mu'$.

  Let $\mu_S \in Dist(S)$ be such that $\mu_P \Subset_{R''} \mu_S$. Let $\varphi' \in Dist(S')$ be such that $L'(w, a, \varphi') \geq ?$ and let $\mu' \in Sat(\varphi')$ such that $\mu_S \Subset_{R'} \mu'$. Let $\delta'' : S_P \to (S \to [0,1])$ and $\delta' : S \to (S' \to [0,1])$ be the correspondence functions witnessing $\mu_P \Subset^{\delta''}_{R''} \mu_S$ and $\mu_S \Subset^{\delta'}_{R'} \mu'$ respectively. The correspondence function for $\mathcal{R}$ is $\delta : S_P \to (S' \to [0,1])$ such that $\delta(s)(t) = \sum_{r \in S} \delta''(s)(r)\delta'(r)(t)$. It follows that $\mu_P \Subset^{\delta}_{\mathcal{R}} \mu'$.

Thus $\mathcal{R}$ is a satisfaction relation. Moreover, since $s_0^P \,\mathcal{R}''\, s_0$ and $s_0 \,\mathcal{R}'\, s_0'$, we have that $s_0^P \,\mathcal{R}\, s_0'$, and we conclude that $P \in [\![N']\!]$, therefore $N \preceq_T N'$.

- $\preceq_W \neq \preceq$: We show that for APAs N_1 and N_2, given in Fig. 8, we have $N_1 \preceq_W N_2$, but $N_1 \not\preceq N_2$.

  - $N_1 \preceq_W N_2$: We show that $\mathcal{R} = \{(s_1, s_1'), (s_2, s_2'), (s_3, s_3'), (s_4, s_4'), (s_5, s_5')\}$ is a weak weak refinement relation. By construction, the pairs (s_2, s_2'), (s_3, s_3'), (s_4, s_4') and (s_5, s_5') satisfy the axioms of a weak weak refinement relation. We now show that the pair of initial state (s_1, s_1') also satisfies the axioms of a weak weak refinement relation. For distributions $\mu \in Sat(\varphi_x)$ such that $\mu(s_2) > 0$ or $\mu(s_3) > 0$ we choose the constraint φ_y, and for other distributions we choose φ_z. It is then clear that

    $$\forall \mu \in Sat(\varphi_x), \exists \varphi' \in \{\varphi_y, \varphi_z\}, \exists \mu' \in Sat(\varphi') : \mu \Subset_R \mu'.$$

  - $N_1 \not\preceq N_2$: There exists no constraint $\varphi' \in C(S')$ such that $L'(s_1', a, \varphi') \neq \bot$ and $\forall \mu \in Sat(\varphi_x), \exists \mu' \in Sat(\varphi') : \mu \Subset_R \mu'$.

- $\preceq \neq \preceq_S$: We now show that for the APAs N_3 and N_4, given in Fig. 9, we have $N_3 \preceq N_4$, but $N_3 \not\preceq_S N_4$.

  - $N_3 \preceq N_4$: We show that $\mathcal{R} = \{(s_1, s_1'), (s_2, s_2'), (s_3, s_3'), (s_3, s_4'), (s_4, s_5')\}$ is a weak refinement relation. Again, the pairs (s_2, s_2'), (s_3, s_3'), (s_3, s_4') and (s_4, s_5') all satisfy the axioms of a weak refinement relation by construction. We now show that the pair of initial states (s_1, s_1') also satisfies the axioms of a weak refinement relation.

    There is a constraint function $\varphi_x \in C(S)$ such that $L(s_1, a, \varphi_x) = ?$ and a constraint function $\varphi_y \in C(S')$ such that $L(s_1', a, \varphi_y) = ?$. We now show that $\forall \mu \in Sat(\varphi_x), \exists \mu' \in Sat(\varphi_y) : \mu \Subset_R \mu'$. Let $\mu \in Sat(\varphi_x)$ and let $\delta : S \to (S' \to [0,1])$ be given as

    $$(s_1, s_1') \mapsto 1,\ (s_2, s_2') \mapsto 1,\ (s_3, s_3') \mapsto \gamma,\ (s_3, s_4') \mapsto 1 - \gamma,\ (s_4, s_5') \mapsto 1,$$

    where $\gamma = \frac{0.7 - \mu(s_2)}{\mu(s_3)}$, if $\mu(s_2) \leq 0.7$, and $\gamma = \frac{0.8 - \mu(s_2)}{\mu(s_3)}$ otherwise.

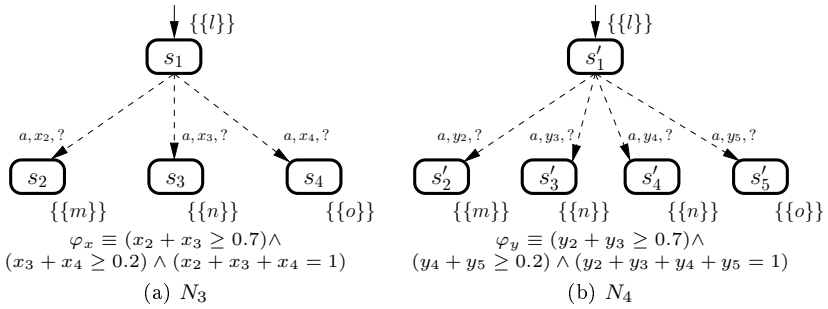


Figure 9: APAs N_3 and N_4 such that $N_3 \preceq N_4$, but not $N_3 \preceq_S N_4$.

1. By definition of δ, for each $s \in S$, $\delta(s)$ is a distribution on S'.
2. Assume that $\mu(s_2) \leq 0.7$. For $s'_3, s'_4 \in S'$, we have

$$\sum_{s \in S} \mu(s)\delta(s)(s'_3) = \mu(s_3)\frac{0.7 - \mu(s_2)}{\mu(s_3)} = 0.7 - \mu(s_2),$$

$$\sum_{s \in S} \mu(s)\delta(s)(s'_4) = \mu(s_3)\left(1 - \frac{0.7 - \mu(s_2)}{\mu(s_3)}\right)$$

$$= \mu(s_3) - 0.7 + \mu(s_2).$$

   Using this observation, $\mu' : S' \to [0,1]$, given by $s'_1 \mapsto \mu(s_1)$, $s'_2 \mapsto \mu(s_2)$, $s'_3 \mapsto 0.7 - \mu(s_2)$, $s'_4 \mapsto \mu(s_3) - 0.7 + \mu(s_2)$, and $s'_5 \mapsto \mu(s_4)$, is a distribution on S', $\mu' \in Sat(\varphi_y)$, and $\mu \in^{\delta}_{R} \mu'$. The proof is similar if $\mu(s_2) > 0.7$.
3. Pairs (s, s') for which $\delta(s)(s') > 0$ are related by $\mathcal{R}$ by construction.

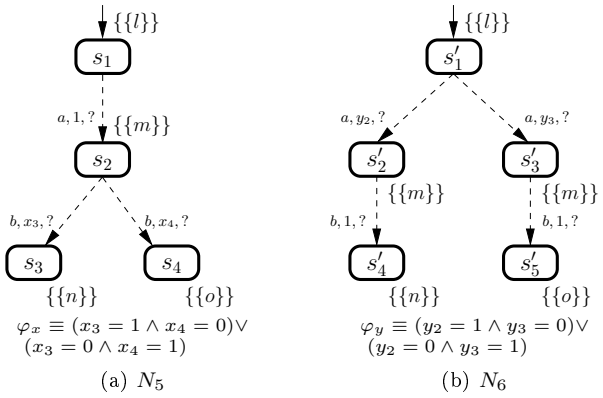
For valuations in s_1 and s'_1, respectively, it holds that $\{\{l\}\} \subseteq \{\{l\}\}$.

- $N_3 \not\preceq_S N_4$: Suppose that there exists a satisfaction relation $\mathcal{R}'$, and let δ' be the correspondence function witnessing relation of s_1 and s'_1. The valuations require that δ' must be of the same type as δ above with $\gamma \geq 0$ (here γ is constant). Consider the following two distributions over S, μ_1 and μ_2 given by

$$\mu_1 : \ s_1 \mapsto 0, \ s_2 \mapsto 0.6, \ s_3 \mapsto 0.1, \ s_4 \mapsto 0.3$$
$$\mu_2 : \ s_1 \mapsto 0, \ s_2 \mapsto 0.8, \ s_3 \mapsto 0.1, \ s_4 \mapsto 0.1.$$

  The 2 following properties must hold: (1) $\exists \mu'_1 \in Dist(S'), \forall s' \in S' : \sum_{s \in S} \mu_1(s)\delta(s)(s') = \mu'_1(s')$ and (2) $\exists \mu'_2 \in Dist(S'), \forall s' \in S' : \sum_{s \in S} \mu_2(s)\delta(s)(s') = \mu'_2(s')$. However, (1) requires that $\gamma = 1$, and (2) requires that $\gamma = 0$, which shows that such a strong refinement relation cannot exist.

- $\preceq_T \neq \preceq_W$: Finally, we show that for the APAs N_5 and N_6, given in Fig. 10, we have $N_5 \preceq_T N_6$, but $N_5 \not\preceq_W N_6$.



(a) N_5 (b) N_6

Figure 10: APAs N_5 and N_6 such that $N_5 \preceq_T N_6$, but not $N_5 \preceq_W N_6$.

- $N_5 \preceq_T N_6$: It is easy to see that any PA satisfying N_5 will also satisfy N_6.
- $N_5 \not\preceq_W N_6$: Consider the pair (s_2, s'_2). $Sat(\varphi_x) = \{\mu_1, \mu_2\}$, where $\mu_1(s_3) = 1$ and $\mu_2(s_4) = 1$. Let μ'_2 be the distribution over N_6 assigning probability 1 to s'_4. A correspondence function δ such that $\mu_2 \Subset^{\delta}_{\mathcal{R}} \mu'_2$ cannot exist, since such a δ will satisfy that $\delta(s_4)(s'_4) = 1$ and this pair cannot be related because $\{\{o\}\} \not\subseteq \{\{n\}\}$. The same applies for (s_2, s'_3). This implies that $N_5 \not\preceq_W N_6$.

□

We have just seen that, in general, thorough refinement is strictly finer than any syntactical refinement. In Section 6.2, we will show that the thorough, weak weak, weak, and strong refinement coincide on the class of deterministic APAs. In the rest of this paper, each time that we show that a refinement relation holds, we prove it for the strongest possible version of refinement.

3.2. Bisimulation

In this section, we first introduce the classical notion of bisimulation for PAs [21]. Then, we show that the specification theory we propose in this paper is backwards-compatible, in the sense that bisimilar PAs satisfy the same specifications. The section is structured as follows. First, we recap the definition of bisimulation for PAs. Then, in Theorem 20, we propose a characterization of bisimulation based on the notion of satisfaction. Finally, Theorem 22 presents the main result of the section, i.e. bisimilar APAs satisfy the same specifications. Detailed proofs of the theorems are given in Appendix B.
The following definition presents the classical notion of bisimulation proposed in [21].

Definition 18 (Bisimulation)**.** *Let $P = (S, A, L, AP, V, s_0)$ and $P' = (S', A, L', AP, V', s'_0)$ be PAs with no unreachable states. We say that $\mathcal{R} \subseteq S \times S'$ is a bisimulation relation iff whenever $(s, s') \in \mathcal{R}$, the following holds:*

- $V(s) = V'(s')$, *and*
- $\forall a \in A$, $\exists \mu \in Dist(S)$ *such that* $L(s,a,\mu) = \top$ *if and only if there exists* $\mu' \in Dist(S')$ *such that* $L'(s',a,\mu') = \top$ *and, for each equivalence class* $T \in (S \cup S')/\mathcal{R}^*$, $\mu(T) = \mu'(T)$, *where* $\mathcal{R}^*$ *denotes the reflexive, symmetric, transitive closure of* $\mathcal{R}$ *on* $(S \cup S')$.

P and P' are bisimilar, written $P \simeq P'$, if and only if there exists a bisimulation relation $\mathcal{R}$ such that $s_0 \,\mathcal{R}\, s'_0$.

Characterization. We now propose a methodology that uses the satisfaction relation and a lifting algorithm from PAs to APAs in order to decide whether two given PAs are bisimilar. This methodology and the subsequent theorem 20 will be of particular interest for proving backward compatibility.

It turns out that bisimulation between two given PAs holds whenever, when lifted to APAs, they admit the same implementations. In the following, we first formally define the lifting from PAs to APAs. We then propose a formal syntactical characterization of bisimilar PAs.

Definition 19 (Lifting)**.** *Let $P = (S, A, L, AP, V, s_0)$ be a PA. We define the lifting of P, denoted $\widetilde{P} = (S, A, \tilde{L}, AP, \tilde{V}, s_0)$ as the APA where*

- *for all $s \in S$, $a \in A$, and $\varphi \in C(S)$, $\tilde{L}(s,a,\varphi) = \top$ if and only if there exists $\mu \in Dist(S)$ such that $L(s,a,\mu) = \top$ and $Sat(\varphi) = \{\mu\}$, and*
- *for all $s \in S$, $\tilde{V}(s) = \{V(s)\}$.*

Informally, the lifting $\widetilde{P}$ of P extends state valuations to sets containing only the original valuations, and contains only single-solution constraints based on the original distributions of P.

We propose the following theorem:

Theorem 20. *Let P and P' be PAs. We have that $P \simeq P' \iff P \models \widetilde{P'}$.*

Proof. We give a sketch of the proof, while a detailed version is given in Appendix B.1. Let $P = (S, A, L, AP, V, s_0)$ and $P' = (S', A, L', AP, V', s'_0)$ be PAs, and let $\widetilde{P'} = (S', A, \tilde{L'}, AP, \tilde{V'}, s'_0)$ be the lifting of P'.

• $P \simeq P' \Rightarrow P \models \widetilde{P'}$: Assume that $P \simeq P'$ with relation $\mathcal{R}_b$. It happens that $\mathcal{R}_b$ is a satisfaction relation such that $P \models \widetilde{P'}$.

• $P \simeq P' \Leftarrow P \models \widetilde{P'}$: Assume that $P \models \widetilde{P'}$ with satisfaction relation $\mathcal{R}$. We prove that $P \simeq P'$.

Let $\mathcal{R}^*$ denote the reflexive, transitive, symmetric closure of the relation $\mathcal{R}$ over $S \cup S'$, and let $\mathcal{R}_b \subseteq S \times S'$ be the relation such that $s \,\mathcal{R}_b\, s'$ iff $s \,\mathcal{R}^*\, s'$. It follows that $\mathcal{R}_b$ is a bisimulation relation and that $s_0 \,\mathcal{R}_b\, s'_0$. We thus conclude that $P \simeq P'$.

□

Backward Compatibility. We now move to the main result of the section: bisimilar PAs satisfy the same APAs. We first relate lifting and refinement.

Lemma 21. *Let P be a PA and let N be an APA. The following holds:*

$$P \models N \iff \widetilde{P} \preceq N.$$

Proof. • $P \models N \Rightarrow \widetilde{P} \preceq N$: Let $P = (S, A, L, AP, V, s_0)$ be a PA and let $N = (S', A, L', AP, V', s'_0)$ be an APA such that $P \models N$ with relation $\mathcal{R}_s$. Let $\widetilde{P} = (S, A, \tilde{L}, AP, \tilde{V}, s_0)$ be the lifting of P. It happens that $\mathcal{R}_s$ is also a weak refinement relation between $\widetilde{P}$ and N. The proof is standard and reported in Appendix B.2.

Since $\mathcal{R}$ is a weak refinement relation and, by construction, $s_0 \,\mathcal{R}\, s'_0$, we conclude that $\widetilde{P} \preceq N$.

• $P \models N \Leftarrow \widetilde{P} \preceq N$: Let $P = (S, A, L, AP, V, s_0)$ be a PA, let $\widetilde{P} = (S, A, \tilde{L}, AP, \tilde{V}, s_0)$ be the lifting of P and let $N = (S', A, L', AP, V', s'_0)$ be an APA such that $\widetilde{P} \preceq N$ with relation $\mathcal{R}_r$. Again, $\mathcal{R}_r$ is also a satisfaction relation between P and N. The proof is standard and given in Appendix B.2.

Since $\mathcal{R}$ is a satisfaction relation and, by construction, $s_0 \,\mathcal{R}\, s'_0$, we conclude that $P \models N$.

□

Observe that, by the two previous results, we obtain that the lifting of two bisimilar PAs have equal sets of implementations:

$$P \simeq P' \iff [\![\widetilde{P}]\!] = [\![\widetilde{P'}]\!].$$

We now present the main result of the section, that is that bisimilar PAs satisfy the same specifications.

Theorem 22. *Let P and P' be PAs such that $P \simeq P'$. For all APA N, it holds that $P \models N \iff P' \models N$.*

Proof. Let P and P' be PAs such that $P \simeq P'$, and let N be an APA such that $P \models N$. Consider the liftings $\widetilde{P}$ and $\widetilde{P'}$ of P and P'. By Lemma 21, we have $\widetilde{P} \preceq N$. Moreover, by Theorem 20, we have $P' \models \widetilde{P}$. Since weak refinement implies implementation set inclusion, we thus have that $P' \models N$. By symmetry, we thus have that for all APA N, $P \models N \iff P' \models N$. □

3.3. Abstraction

We now propose two different notions of abstraction. The first notion, called *state-based* abstraction amounts to grouping sets of states into single abstract states. The aim of state-based abstraction is to reduce the complexity of APAs by reducing their state space. The second notion, called *constraint-based* abstraction, amounts to abstracting complex constraints into the smallest interval constraints that encompass all their solutions. The aim of constraint-based abstraction is to reduce the complexity of the constraints. Indeed, as shown in [22],

manipulating interval constraints allows for less complex algorithms in general. Observe that both notions of abstraction can be combined.

State-based abstraction. The aim of this abstraction is to partition the state space, i.e., group (disjoint) sets of states into a single abstract state. Let N and M be APA with state space S and S', respectively. An *abstraction* function $\alpha : S \to S'$ is a surjection. The inverse of abstraction function α is the *concretization* function $\gamma : S' \to 2^S$. The state $\alpha(s)$ denotes the abstract counterpart of state s while $\gamma(s')$ represents the set of all (concrete) states that are represented by the abstract state s'. Abstraction is lifted to distributions as follows. The abstraction of $\mu \in Dist(S)$, denoted $\alpha(\mu) \in Dist(S')$, is uniquely defined by $\alpha(\mu)(s') = \mu(\gamma(s'))$ for all $s' \in S'$. Abstraction is lifted to sets of states, or sets of distributions in a pointwise manner. It follows that $\varphi' = \alpha(\varphi)$ if and only if $Sat(\varphi') = \alpha(Sat(\varphi))$. The cartesian product of two abstraction functions is given as follows: $(\alpha_1 \times \alpha_2)(s_1, s_2) = (\alpha_1(s_1), \alpha_2(s_2))$. These ingredients provide the basis to define the state abstraction of an APA.

Definition 23 (State-based Abstraction)**.** *Given APA $N = (S, A, L, AP, V, s_0)$, the abstraction function $\alpha : S \to S'$ induces the APA $\alpha(N) = (S', A, L', AP, V', \alpha(s_0))$, where for all $a \in A$, $s' \in S'$ and $\varphi' \in C(S')$:*

$$L'(s', a, \varphi') = \begin{cases} \top & \text{if } \forall s \in \gamma(s') : \exists \varphi \in C(S) : L(s, a, \varphi) = \top, \text{ and} \\ & Sat(\varphi') = \alpha\big(\bigcup_{(s,\varphi) \in \gamma(s') \times C(S) : L(s,a,\varphi) = \top} Sat(\varphi)\big) \qquad (a) \\ ? & \text{if } \exists s \in \gamma(s') : \exists \varphi \in C(S) : L(s, a, \varphi) \geq ?, \text{ and} \\ & Sat(\varphi') = \alpha\big(\bigcup_{(s,\varphi) \in \gamma(s') \times C(S) : L(s,a,\varphi) \neq \bot} Sat(\varphi)\big) \qquad (b) \\ \bot & \text{otherwise} \qquad (c) \end{cases}$$

$$\text{and } V'(s') = \bigcup\nolimits_{\forall s \in \gamma(s')} V(s)$$

Item (a) asserts that if there are must transitions (s, a, φ) from all states $s \in \gamma(s')$, then the must transition (s', a, φ') represents their total behavior. Item (b) asserts that a may a-transition emanating from s' represents the total behaviour of all may and must transitions (s, a, φ) for all $s \in \gamma(s')$. Item (c) asserts that if no state in $\gamma(s')$ has an a-transition, then s' also does not have an a-transition.

The result of abstracting APA N is the APA $\alpha(N)$ that is able to mimic all behaviours of N, but possibly exhibits more behaviour.

Example. *Consider the APA $N = (S, A, L, AP, V, s_0)$ depicted in Fig. 11a. Let the abstraction function $\alpha : S \to S'$ be given by $\alpha(s_1) = s'_1$, $\alpha(s_2) = \alpha(s_3) = s'_{23}$, $\alpha(s_4) = s'_4$, $\alpha(s_5) = s'_5$, and $\alpha(s_6) = s'_6$. The APA $\alpha(N)$ obtained following Definition 23 is depicted in Figure 11b. State s'_1 has a single outgoing must a-transition, corresponding to the outgoing must a-transition of s_1, where target states are collapsed and the constraint is simplified accordingly. State s'_{23} has two outgoing transitions: (1) a must a-transition because both s_2 and s_3 have*

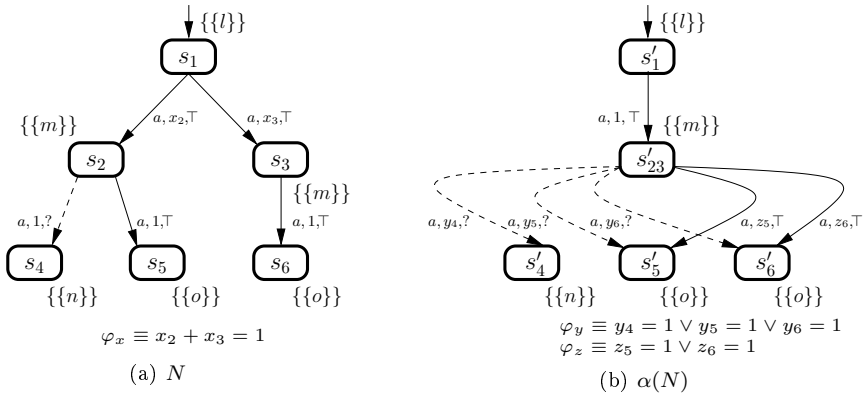


Figure 11: APA N and and its state abstraction $\alpha(N)$

must a-outgoing transitions (item (a) of Definition 23), with a constraint that represents the union of the constraints of the original must transitions; and (2) a may a-transition because s_2 has a may a-transition (item (b) of Definition 23), with a constraint that represents the union of the constraints of all outgoing a-transitions of s_2 and s_3.

Observe that the abstract version of an APA is always weaker in term of refinement than the original APA.

Lemma 24. *For all APA N and abstraction function α, $N \preceq_S \alpha(N)$.*

Proof. Let $N = (S, A, L, AP, V, s_0)$ be an APA and let $\alpha : S \to S'$ be an abstraction function. Consider the state abstraction $\alpha(N) = (S', A, L', AP, V', \alpha(s_0))$. Let $\mathcal{R} \subseteq S \times S'$ be the relation such that $s \mathcal{R} s'$ iff $s' = \alpha(s)$. The proof that $\mathcal{R}$ is a strong refinement relation is standard. The key point of this proof is to use the following correspondence functions: $\delta : S \to (S' \to [0, 1])$ such that $\delta(u)(v) = 1$ if $\alpha(u) = v$, and 0 otherwise. For the sake of completeness, the full proof is reported in Appendix C. □

Observe that by the ordering of refinement relations given in Theorem 17, it also holds that $N \preceq \alpha(N)$, $N \preceq_W \alpha(N)$ and $N \preceq_T \alpha(N)$.

Constraint-based abstraction. Given a constraint $\varphi \in C(S)$, we say that φ is an interval constraint if there exist closed intervals $\{I_s^\varphi | s \in S\}$ such that $\forall \mu, \mu \in Sat(\varphi) \iff \bigwedge_{s \in S}(\mu(s) \in I_s^\varphi)$. If, for all $s \in S$, $a \in A$, and $\varphi \in C(S)$ such that $L(s, a, \varphi) \neq \bot$, it holds that φ is an interval constraint, then we call N an Interval Probabilistic Automaton (IPA).

The following notion of abstraction abstracts an APA with the smallest IPA encompassing all its implementations.

Definition 25 (Constraint-based Abstraction)**.** *Let $N = (S, A, L, AP, V, s_0)$ be an APA. The constraint-abstracted APA $\chi(N) = (S, A, L', AP, V, s_0)$ is defined*

such that for all states $s \in S$ and $a \in A$, if there exists $\varphi \in C(S)$ such that $L(s,a,\varphi) \neq \bot$, then $L'(s,a,\varphi') = L(s,a,\varphi)$ for $\varphi' \in C(S)$ defined as

$$Sat(\varphi') = \left\{ \mu' \in Dist(S) \,\middle|\, \bigwedge_{s' \in S} \mu'(s') \in I^{\varphi}_{s'} \right\},$$

where $\{I^{\varphi}_{s'} | s' \in S\}$ are the smallest closed intervals such that $\forall \mu \in Sat(\varphi) : \bigwedge_{s' \in S} \mu(s') \in I^{\varphi}_{s'}$.

As expected, constraint-based abstraction is an abstraction with respect to strong refinement.

Lemma 26. *For any APA N, it holds that $N \preceq_S \chi(N)$.*

Proof. Let $N = (S, A, L, AP, V, s_0)$ be an APA and let $\chi(N) = (S, A, L', AP, V, s_0)$ be the constraint-abstraction of N. Let $\mathcal{R} = S \times S$ be the identity relation. The proof that $\mathcal{R}$ is a strong refinement relation is standard. The key point of this proof is to use identity correspondence functions. For the sake of completeness, the full proof is given in Appendix D. □

We now show that if N is a valuation-deterministic APA in SVNF, then $\chi(N)$ is the smallest IPA in SVNF abstracting N with respect to weak refinement. However, when N and $\chi(N)$ are not in SVNF, it is possible to abstract N in different ways by grouping states with different valuations, leading to abstractions that cannot be compared with $\chi(N)$ using the refinement relations.

Theorem 27. *For any valuation-deterministic APA N in SVNF and IPA N' in SVNF, $N \preceq N'$ implies $\chi(N) \preceq N'$.*

Proof. Let $N = (S, A, L, AP, V, s_0)$ be a valuation-deterministic APA, and let $N' = (S', A, L', AP, V', s'_0)$ be an IPA, both in SVNF, such that $N \preceq N'$ with a weak refinement relation $\mathcal{R}$. Let $\chi(N) = (S, A, L'', AP, V, s_0)$ be the constraint abstraction of N. Let $\mathcal{R}' := \mathcal{R}$. Although $\mathcal{R}$ and $\mathcal{R}'$ are equal, we chose to use two different notations to stress the fact that the former is a weak refinement relation between N and N' while the latter is a relation between $\chi(N)$ and N'. We prove that $\mathcal{R}'$ is a weak refinement relation such that $\chi(N) \preceq N'$. Let $s \in S$ and $s' \in S'$ such that $s \,\mathcal{R}'\, s'$. We show that $\mathcal{R}'$ satisfies the axioms of a weak refinement relation.

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 construction of $\chi(N)$, there exists $\varphi_I \in C(S)$ (the constraint-abstraction of φ) such that $L''(s, a, \varphi_I) = \top$ and $Sat(\varphi_I) = \{\mu'' \in Dist(S) | \bigwedge_{s'' \in S} \mu''(s'') \in I^{\varphi}_{s''}\}$ with $\{I^{\varphi}_{s''} | s'' \in S\}$ the smallest closed intervals such that $\forall \mu \in Sat(\varphi) : \bigwedge_{s'' \in S} \mu(s'') \in I^{\varphi}_{s''}$.
   Define $\mathcal{R}'(s_1) = \{s'_1 \in S' | s_1 \,\mathcal{R}'\, s'_1\}$ for all $s_1 \in S$. Observe that for all $s_1 \neq s_2$, $\varphi \in C(S)$, and $a \in A$ such that $L(s, a, \varphi) \neq \bot$, if there exists $\mu_1, \mu_2 \in Sat(\varphi)$ with $\mu_1(s_1) > 0$ and $\mu_2(s_2) > 0$, then, since N is

valuation-deterministic and N' is in SVNF, $\mathcal{R}'(s_1) \cap \mathcal{R}'(s_2) = \emptyset$ (observation A).
Let $\{I_{s_1}^{\varphi_I} = [l_{s_1}, u_{s_1}] | s_1 \in S\}$ be the intervals associated with φ_I, and let $\{I_{s_1'}^{\varphi'} = [l'_{s_1'}, u'_{s_1'}] | s_1' \in S\}$ be the intervals associated with φ'. Let $a \in A$ and $\varphi \in C(S)$ such that $L(s, a, \varphi) \neq \bot$. Let $s_1 \in S$. By minimality of the interval constraints in $\chi(N)$, there exists $\mu \in Sat(\varphi)$ such that $\mu(s_1) = l_{s_1}$. Since $s \mathcal{R} s'$, there exists $\delta : S \to Dist(S')$ such that

$$\forall s_1' \in S' : \sum_{s_2 \in S} \mu(s_2)\delta(s_2)(s_1') = \mu'(s_1'),$$

for some $\mu' \in Sat(\varphi')$, where $L'(s', a, \varphi') \neq \bot$.
For δ, we deduce that $\forall s_1' \notin \mathcal{R}'(s_1), \delta(s_1)(s_1') = 0$ and $\forall s_2 \neq s_1, \forall s_1' \in \mathcal{R}'(s_2), \delta(s_2)(s_1') = 0$. By the first deduction, $\forall s_1' \in \mathcal{R}'(s_1), \mu(s_1)\delta(s_1)(s_1') \geq l'_{s_1'}$ and by the second, $\sum_{s_1' \in \mathcal{R}'(s_1)} \mu(s_2)\delta(s_2)(s_1') = l_{s_1}$. As a consequence, $l_{s_1} \geq \sum_{s_1' \in \mathcal{R}'(s_1)} l'_{s_1'}$, and similarly, we obtain $u_{s_1} \leq \sum_{s_1' \in \mathcal{R}'(s_1)} u'_{s_1'}$.
Let $\mu_I \in Sat(\varphi_I)$. We now prove that there exists $\mu_I' \in Sat(\varphi')$ such that $\mu_I \Subset_{\mathcal{R}'} \mu_I'$. For all $s_1 \in S$, define the correspondence function $\delta' : S \to Dist(S')$ as follows: if $\mu_I(s_1) = 0$, then $\delta'(s_1)(s_1') = 0$ for all $s_1' \in S'$ and otherwise,

$$\delta'(s_2)(s_1') = \begin{cases} \frac{1}{\mu_I(s_2)} \left(l'_{s_1'} + \frac{(u'_{s_1'} - l'_{s_1'})(\mu_I(s_2) - \sum_{s_2' \in \mathcal{R}'(s_2)} l'_{s_2'})}{\sum_{s_2' \in \mathcal{R}'(s_2)} (u'_{s_2'} - l'_{s_2'})} \right) & \text{if } s_1' \in \mathcal{R}'(s_2) \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

Let $\mu_I' \in Dist(S')$ such that $\mu_I'(s_1') = \sum_{s_2 \in S} \mu_I(s_2)\delta(s_2)(s_1')$. We prove that $\mu_I \Subset^{\delta'}_{\mathcal{R}'} \mu_I'$.

(a) By construction, if $\mu_I(s_1) > 0$, then $\sum_{s_1' \in S'} \delta'(s_1)(s_1') = 1$.

(b) Let $s^{*\prime} \in S'$. By observation A, there exists at most one $s^* \in S$ such that $\mu_I(s^*) > 0$ and $s^{*\prime} \in \mathcal{R}'(s^*)$. There are two cases:

- If no such s^* exists, then $l'_{s^{*\prime}} = \sum_{s_2 \in S} \mu_I(s_2)\delta'(s_2)(s^{*\prime}) = 0$ and we have
$$l'_{s^{*\prime}} \leq \mu_I'(s^{*\prime}) \leq u'_{s^{*\prime}}.$$
- Otherwise, we have
$$\sum_{s_2 \in S} \mu_I(s_2)\delta'(s_2)(s^{*\prime}) = \mu_I(s^*)\delta'(s^*)(s^{*\prime}) = l'_{s^{*\prime}} + \frac{(u'_{s^{*\prime}} - l'_{s^{*\prime}})(\mu_I(s^*) - \sum_{s_2' \in \mathcal{R}'(s^*)} l'_{s_2'})}{\sum_{s_2' \in \mathcal{R}'(s^*)} (u'_{s_2'} - l'_{s_2'})}.$$
Since $\sum_{s_2' \in \mathcal{R}'(s_2)} l'_{s_2'} \leq l_{s^*} \leq \mu_I(s^*)$, we have that
$$\mu_I'(s^{*\prime}) = \sum_{s_2 \in S} \mu_I(s_2)\delta'(s_2)(s^{*\prime}) \geq l'_{s^{*\prime}}.$$

Similarly,

$$\mu'_I(s^{*\prime}) = \sum_{s_2 \in S} \mu_I(s_2)\delta'(s_2)(s^{*\prime}) \leq u'_{s^{*\prime}}.$$

We conclude that $\forall s'_1 \in S', \mu'_I(s'_1) \in I'_{s'_1}$. Thus $\mu'_I \in Sat(\varphi')$.

(c) Assume that $\delta'(s_1)(s'_1) > 0$. Then $s'_1 \in \mathcal{R}'(s_1)$, and $s_1 \,\mathcal{R}'\, s'_1$.

We conclude that there exists $\mu'_I \in Sat(\varphi')$ such that $\mu_I \Subset_{\mathcal{R}'} \mu'_I$.

2. Let $a \in A$ and $\varphi_I \in C(S)$ such that $L''(s, a, \varphi_I) \neq \bot$. By construction, there exists $\varphi \in C(S)$ such that $L(s, a, \varphi) \neq \bot$. By refinement, there exists $\varphi' \in C(S')$ such that $L'(s', a, \varphi') \neq \bot$ and $\forall \mu \in Sat(\varphi) \exists \mu' \in Sat(\varphi') : \mu \Subset_{\mathcal{R}} \mu'$. Using the same reasoning as above, we can prove that $\forall \mu_I \in Sat(\varphi_I)$, there exists $\mu'_I \in Sat(\varphi')$ such that $\mu_I \Subset_{\mathcal{R}} \mu'_I$.
3. Clearly, $V(s) \subseteq V'(s')$, as valuations in N and $\chi(N)$ are equal.

This proves that $\mathcal{R}'$ is a weak refinement relation. As $s_0 \,\mathcal{R}'\, s'_0$, we conclude that $\chi(N) \preceq N'$. □

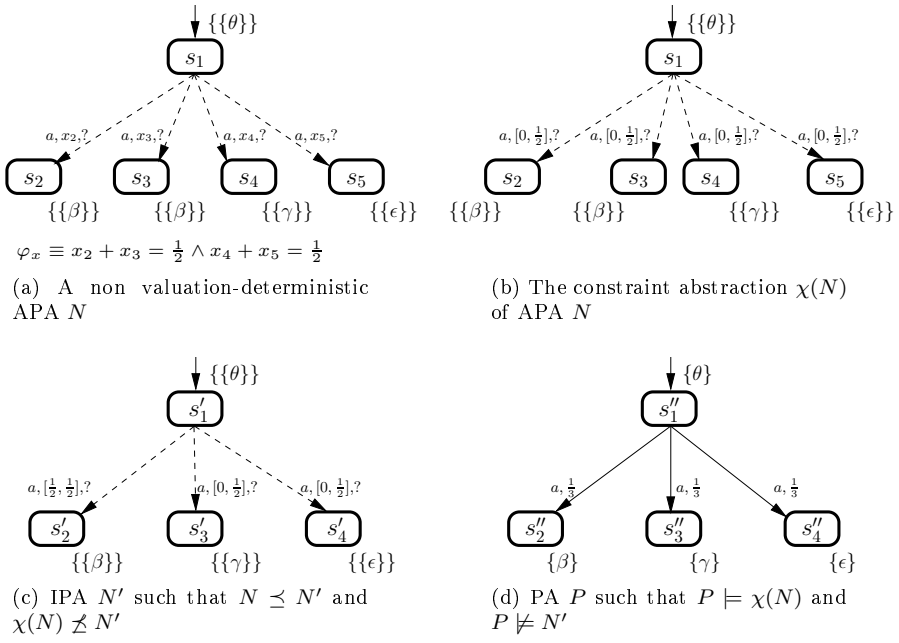
Observe that the above theorem does not hold for strong refinement: If N' is an IPA in SVNF such that $N \preceq_S N'$, then we have $\chi(N) \preceq N'$ but not necessarily $\chi(N) \preceq_S N'$.

Example. *We show that Thm. 27 does not hold when the APA N is not valuation-deterministic. Consider APA N and IPA N' given in Fig. 12a and 12c respectively. It is easy to see that N is not valuation-deterministic, and that $N \preceq N'$. Let $\chi(N)$ be the constraint-based abstraction of N, as given in Fig. 12b. Consider PA P given in Fig. 12d. It is easy to see that $P \models \chi(N)$, but $P \not\models N'$. Thus, by Theorem 17, $\chi(N) \not\preceq N'$.*

Notice that Thm. 27 holds regardless whether N is action-deterministic. It turns out that if N is not action-deterministic, then the theorem holds for weak refinement, but not for weak weak refinement. Fig. 13 illustrates a counter example. This is not suprising as, because of the swap of quantifiers in its definition, weak weak refinement can take more advantage of action non-determinism than weak refinement.

Although state-based abstraction and constraint-based abstraction are both abstractions, they cannot be compared in general in terms of refinement. This statement is illustrated in the following example.

Example. *Consider APA N given in Fig. 14a. Fig. 14b illustrates the state-based abstraction of N where state s_2 and s_3 are grouped, and Fig. 14c illustrates the constraint-abstraction of N. It is easy to see that $\alpha(N) \not\preceq \chi(N)$. Indeed, state s'_2 cannot refine either state s''_2 or s''_3, because their valuations do not coincide. Also $\chi(N) \not\preceq \alpha(N)$, because their constraints do not match.*



(a) A non valuation-deterministic APA N

(b) The constraint abstraction $\chi(N)$ of APA N

(c) IPA N' such that $N \preceq N'$ and $\chi(N) \not\preceq N'$

(d) PA P such that $P \models \chi(N)$ and $P \not\models N'$

Figure 12: Example that constraint abstraction does not preserve $\preceq$ for non valuation-deterministic APAs

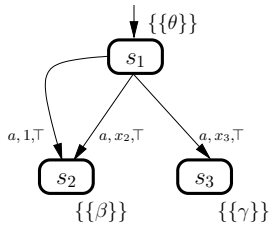
4. Consistency, Pruning and Conjunction

We now turn our attention to deciding whether there exist implementations satisfying one or several specifications. When considering only one specification, this problem is called *consistency*. In the following subsection, we first formally define consistency and then propose an algorithm to decide if a given APA is consistent. We then move to the problem of deciding whether several APAs admit a common implementation. We propose an operation, called *conjunction*, that combines requirements of several APAs into a single APA whose implementations are exactly those implementations that satisfy all original APAs.

4.1. Consistency and Pruning

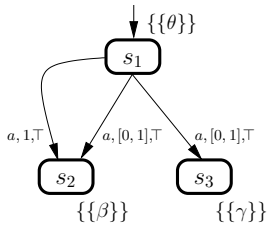
Definition 28 (Consistency)**.** *An APA N is* consistent *if and only if it admits at least one implementation, i.e. $[\![N]\!] \neq \emptyset$.*

We say that a state s is *consistent* if $V(s) \neq \emptyset$ and $L(s, a, \varphi) = \top \implies Sat(\varphi) \neq \emptyset$. An APA is *locally consistent* if all its states are consistent. It is easy to see that a locally consistent APA is consistent. However, inconsistency of a state does not imply inconsistency of the specification. In order to decide whether a specification is consistent, we proceed as usual and propagate inconsistent states with the help of a *pruning operator* β that filters out distributions

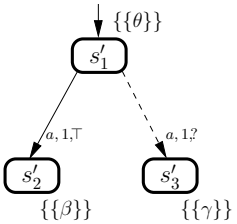


$\varphi_x \equiv x_2 = 1 \vee x_3 = 1$

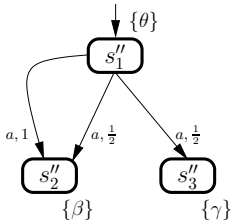
(a) A non action-deterministic APA N



(b) The constraint abstraction $\chi(N)$ of APA N

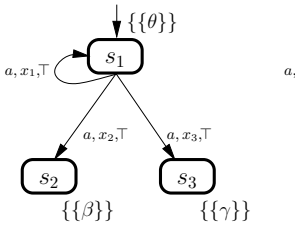


(c) IPA N' such that $N \preceq_W N'$ and $\chi(N) \not\preceq_W N'$



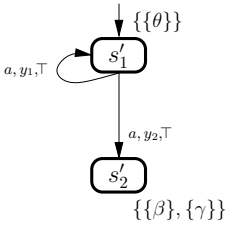
(d) PA P such that $P \models \chi(N)$ and $P \not\models N'$

Figure 13: Example that Thm. 27 does not hold for weak weak refinement with a non action-deterministic APA



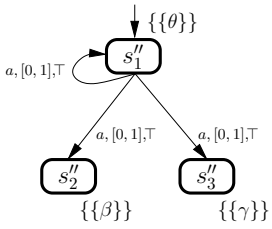
$\varphi_x \equiv x_1 = 1 \vee x_2 + x_3 = 1$

(a) An APA N



$\varphi_y \equiv y_1 = 1 \vee y_2 = 1$

(b) $\alpha(N)$

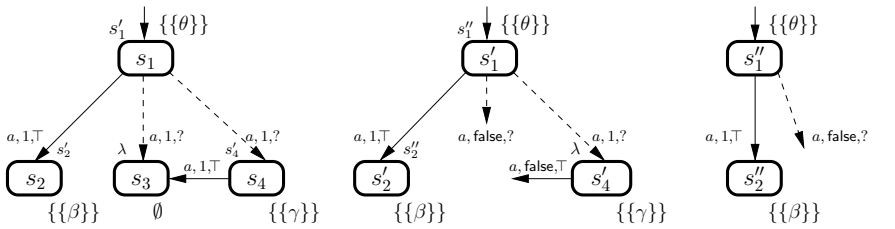


(c) $\chi(N)$

Figure 14: $\alpha(N)$ and $\chi(N)$ cannot be compared in terms of refinement

leading to inconsistent states. This operator is applied until a fixed point is reached, i.e., until the specification does not contain inconsistent states (it is locally consistent). We now formally define the pruning operator.

Definition 29 (Pruning)**.** *Let $N = (S, A, L, AP, V, s_0)$ be an APA with $\lambda \notin S$ and let $T \subseteq S$ be the set of inconsistent states in N. Let $\nu : S \to \{\lambda\} \cup S \setminus T$ be defined by $\nu(s) = \lambda$ if $s \in T$, and $\nu(s) = s$ otherwise. Let β be a pruning function defined by: If $\nu(s_0) = \lambda$, then $\beta(N)$ is the empty APA. Otherwise,*



(a) APA N (b) APA $\beta(N)$ (c) APA $\beta^2(N) = \beta^*(N)$

Figure 15: APAs N, $\beta(N)$ and $\beta^2(N) = \beta^*(N)$

$\beta(N) = (S', A, L', AP, V', s_0)$ with $S' = S \setminus T$, and for all $s \in S'$, $a \in A$, $p \in AP$ and $\varphi \in C(S')$,

$$L'(s,a,\varphi) = \begin{cases} \bot & \text{if } \overline{\varphi}^{s,a} = \emptyset \\ \bigsqcup_{\overline{\varphi} \in \overline{\varphi}^{s,a}} L(s,a,\overline{\varphi}) & \text{otherwise} \end{cases}$$
$$V'(s) = V(s)$$

where $\overline{\varphi}^{s,a}$ is the set of constraints on S, reachable from state s with label a, that match φ when restricted to S'. More formally,

$$\overline{\varphi}^{s,a} = \{\overline{\varphi} \in C(S) \mid \quad L(s,a,\overline{\varphi}) \neq \bot \text{ and } \mu \in Sat(\varphi) \text{ iff } \exists \overline{\mu} \in Sat(\overline{\varphi}) \text{ s.t.} \\ \forall s \in S', \overline{\mu}(s) = \mu(s), \text{ and } \forall t \in T, \overline{\mu}(t) = 0\}.$$

All states in T are mapped onto λ and are removed from APA N. APA $\beta(N)$ obtained by pruning may still contain inconsistent states. Therefore, we repeat pruning until a fixpoint is reached such that $\beta^n(N) = \beta^{n+1}(N)$, where n represents the number of iterations. The existence of this fixpoint is guaranteed as N is finite. Some of the operations (conjunction and composition) may introduce inconsistent states, and are succeeded by a pruning phase to remove such states.

Example. *Consider APA N given in Fig. 15a. State s_3 of N is inconsistent because of an empty valuation. The first round of pruning thus removes state s_3 and yields APA $\beta(N)$ given in Fig. 15b. Since state s_3 has been removed, transitions that used to lead to s_3 now have the constraint* false*, which admits no solution. The outgoing must transition of state s_4 thus becomes inconsistent. As a consequence, the next round of pruning removes state s_4 and yields APA $\beta^2(N)$ given in Fig. 15c. Since there are no more inconsistencies, it follows that $\beta^*(N) = \beta^2(N)$.*

Pruning preserves the set of implementations, as formalized in the following theorem.

Theorem 30. *For any APA N, it holds that $[\![N]\!] = [\![\beta(N)]\!]$.*

Proof. Let $N = (S, A, L, AP, V, s_0)$ be an APA. Let T be the set of inconsistent states of N and let $\beta(N)$ be the corresponding APA using the pruning operator of Definition 29. The result is trivial if $\beta(N)$ is empty. Otherwise, suppose that $\beta(N) = (S', A, L', AP, V', s_0)$, and let $P = (Q, A, L_P, AP, V_P, q_0)$ be a PA. We prove that $P \models N \iff P \models \beta(N)$.

• $P \models N \Rightarrow P \models \beta(N)$: Suppose that $P \models N$, and let $\mathcal{R} \subseteq Q \times S$ be the corresponding satisfaction relation. Define the relation $\mathcal{R}' = \mathcal{R} \cap (Q \times S')$. The proof that $\mathcal{R}'$ is a satisfaction relation is standard. The key argument relies on the fact that all the states $s \in S$ such that there exists $q \in Q$ with $q \mathcal{R} s$ are consistent, i.e. $s \notin T$. Thus, considering the restriction of the relation $\mathcal{R}$ to $S \setminus T$ preserves implementations. For the sake of completeness, the detailed proof is given in Appendix E.

• $P \models N \Leftarrow P \models \beta(N)$: Suppose that $P \models \beta(N)$, and let $\mathcal{R}' \subseteq Q \times S'$ be the corresponding satisfaction relation. By construction, the extension $\mathcal{R}$ of $\mathcal{R}'$ to $Q \times S$ is a satisfaction relation such that $q_0 \mathcal{R} s_0$. Thus $P \models N$.

□

Observe that the above theorem only holds for thorough refinement. Indeed, any syntactic notion of refinement between N and $\beta(N)$ fails because some (potentially reachable) states of N are removed, and thus find no counterpart in $\beta(N)$.

4.2. Conjunction

Conjunction, also called *logical composition*, allows combining two specifications into a single specification that has the conjunctive behavior of the two operands. More precisely, a conjuncted specification admits the intersection of sets of implementations of its constituents. The conjunction operation is a mix between the corresponding operations for modal automata [25] and CMCs [19]. The main lines of the general conjunction operator that we define hereafter are as follows: (1) a must transition on one side that has no counterpart on the other side yields an inconsistent transition, (2) a may transition on one side that has no counterpart on the other side yields no transition, (3) the combination of two transitions (may or must) yields a may transition to a combination of the constraints, and in addition, (4, 5) a must transition on one side yields a must transition in the conjunction to a constraint combining the constraint associated to the original must transition with a disjunction of all admissible constraints on the other side. Notice that, although items (1,2,3) are very close to the definitions of conjunction for modal automata and CMCs, items (4,5) are more involved. Indeed, the general definition we present here needs to handle action non-determinism, which is not taken care of in CMCs or modal automata. In fact a simpler notion of conjunction can be defined for deterministic APAs [1, 2].

Notice that conjunction may introduce inconsistent transitions through (1) and should thus be followed by applying the pruning operator β^*.

Definition 31. *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 $N \wedge N'$ 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*

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

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

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

where $\tilde{\varphi} \in C(S \times S')$ such that $\tilde{\mu} \in \mathit{Sat}(\tilde{\varphi})$ if and only if

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 $\tilde{\mu} \in \mathit{Sat}(\tilde{\varphi}^{\top})$ if and only if 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 $\tilde{\mu}' \in \mathit{Sat}(\tilde{\varphi}'^{\top})$ if and only if 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 $\mathit{Sat}(\varphi)$, and
the distribution $\mu' : t' \to \sum_{t \in S} \tilde{\mu}'((t, t'))$ is in $\mathit{Sat}(\varphi')$.

Note that conjunction $\wedge$ is symmetric.

We conclude the section by showing that conjunction is the greatest lower bound with respect to weak weak refinement.

[1] Recall that $\forall s, \mathsf{Must}(s) \subseteq \mathsf{May}(s)$

Theorem 32. *Let N_1, N_2, and N_3 be consistent APAs sharing action and atomic proposition sets. It holds that*

- $\beta^*(N_1 \wedge N_2) \preceq_W N_1$.
- *If $N_3 \preceq_W N_1$ and $N_3 \preceq_W N_2$, then $N_3 \preceq_W \beta^*(N_1 \wedge N_2)$.*

Proof. Let $N_1 = (S_1, A, L_1, AP, V_1, s_0^1)$ and $N_2 = (S_2, A, L_2, AP, V_2, s_0^2)$ and $N_3 = (S_3, A, L_3, AP, V_3, s_0^3)$ be three APAs. Let $N_1 \wedge N_2 = (S_1 \times S_2, A, \tilde{L}, AP, \tilde{V}, (s_0^1, s_0^2))$ be the conjunction of N_1 and N_2 defined as in Definition 31. We prove the claims separately.

• $\beta^*(N_1 \wedge N_2) \preceq_W N_1$: Obviously, if $N_1 \wedge N_2$ is inconsistent, then $\beta^*(N_1 \wedge N_2)$ is empty and refines N_1 with the empty refinement relation. Suppose now that $\beta^*(N_1 \wedge N_2) = (S^\wedge, A, L^\wedge, AP, V^\wedge, (s_0^1, s_0^2))$, with $S^\wedge \subseteq S_1 \times S_2$, not empty. Define the relation $\mathcal{R} \subseteq S^\wedge \times S_1$ such that for all $(s, s') \in S^\wedge$ and $t \in S_1$, $(s, s')\,\mathcal{R}\,t$ iff $s = t$. We prove that $\mathcal{R}$ is a weak weak refinement relation. Let $(s, s') \in S^\wedge$ such that $(s, s')\,\mathcal{R}\,s$. We show that $\mathcal{R}$ satisfies the axioms of a weak weak refinement relation.

1. let $a \in A$ and $\varphi \in C(S_1)$ such that $L_1(s, a, \varphi) = \top$. Since $(s, s') \in S^\wedge$, we have that $a \in \mathsf{May}(s')$. Let $\tilde{\varphi} \in C(S_1 \times S_2)$ such that $\tilde{\mu} \in Sat(\tilde{\varphi})$ iff
   - the distribution $\mu : t \to \sum_{t' \in S_2} \tilde{\mu}((t, t'))$ is in $Sat(\varphi)$, and
   - there exists a distribution $\varphi' \in C(S_2)$ such that $L_2(s', a, \varphi') \neq \bot$ and the distribution $\mu' : t' \to \sum_{t \in S_1} \tilde{\mu}((t, t'))$ is in $Sat(\varphi')$.

   By definition of $N_1 \wedge N_2$, we have that $\tilde{L}((s, s'), a, \tilde{\varphi}) = \top$. Consider now $\varphi^\wedge \in C(S^\wedge)$ the constraint such that $\mu^\wedge \in Sat(\varphi^\wedge)$ iff there exists $\tilde{\mu} \in Sat(\tilde{\varphi})$ such that $\forall r \in S^\wedge, \mu^\wedge(r) = \tilde{\mu}(r)$ and $\forall r \in (S_1 \times S_2) \setminus S^\wedge, \tilde{\mu}(r) = 0$. According Definition 29, $L^\wedge((s, s'), a, \varphi^\wedge) = \sqcup_{\psi \in \overline{\varphi^\wedge}^{(s,s'),a}} \tilde{L}((s, s'), a, \psi)$.

   Since $\tilde{\varphi} \in \overline{\varphi^\wedge}^{(s,s'),a}$, it holds that $L^\wedge((s, s'), a, \varphi^\wedge) = \top$.
   Thus there exists $\varphi^\wedge \in C(S^\wedge)$ such that $L^\wedge((s, s'), a, \varphi^\wedge) = \top$. Moreover, define the correspondence function $\delta : S^\wedge \to (S_1 \to [0, 1])$ such that $\delta((r, r'))(r'') = 1$ iff $r'' = r$. Let $\mu^\wedge \in Sat(\varphi^\wedge)$, $\tilde{\mu}$ the corresponding distribution in $Sat(\tilde{\varphi})$, and μ the distribution such that $\mu : r \in S_1 \mapsto \sum_{r' \in S_2} \tilde{\mu}((r, r'))$. By definition, μ is in $Sat(\varphi)$ and by construction, we have $\mu^\wedge \Subset^\delta_{\mathcal{R}} \mu$. For the sake of completeness, a detailed proof of this fact is given in Appendix F.
2. Let $a \in A$ and $\varphi^\wedge \in C(S^\wedge)$ such that $L^\wedge((s, s'), a, \varphi^\wedge) \neq \bot$. By definition of $L^\wedge$, there exists $\tilde{\varphi} \in \overline{\varphi^\wedge}^{t,a}$. Thus, $\tilde{L}((s, s'), a, \tilde{\varphi} \neq \bot$ in $N_1 \wedge N_2$, and a distribution $\mu^\wedge$ satisfies $\varphi^\wedge$ iff there exists a distribution $\tilde{\mu} \in Sat(\tilde{\varphi})$ such that $\mu^\wedge(r) = \tilde{\mu}(r)$ for all $r \in S^\wedge$ and $\tilde{\mu}(r) = 0$ for all $r \in S_1 \times S_2 \setminus S^\wedge$. Since $S^\wedge$ contains only consistent states, there exists $\mu^\wedge \in Sat(\varphi^\wedge)$. Let $\tilde{\mu} \in Sat(\tilde{\varphi})$ be a corresponding distribution in $\tilde{\varphi}$. There are 3 cases.
   - If $a \notin \mathsf{Must}(s)$ and $a \notin \mathsf{Must}(s')$, then by Definition 31, there exists $\varphi \in C(S_1)$ and $\varphi' \in C(S_2)$ such that $L_1(s, a, \varphi) \neq \bot$ and

$L_2(s', a, \varphi') \neq \bot$. Moreover, $\tilde{\varrho} \in Sat(\tilde{\varphi})$ iff the distributions $\varrho : r \in S_1 \mapsto \sum_{r' \in S_2} \tilde{\varrho}((r, r'))$ and $\varrho' : r' \in S_2 \mapsto \sum_{r \in S_1} \tilde{\varrho}((r, r'))$ are respectively in $Sat(\varphi)$ and in $Sat(\varphi')$. Since $\tilde{\mu} \in Sat(\tilde{\varphi})$, let μ and μ' be the corresponding distributions in $Sat(\varphi)$ and $Sat(\varphi')$. Define the correspondence function $\delta : S^\wedge \to (S_1 \to [0,1])$ such that $\delta((r, r'))(r'') = 1$ iff $r'' = r$. As above, we have $\mu^\wedge \Subset^\delta_{\mathcal{R}} \mu$.

- Otherwise, if $a \in \mathsf{Must}(s)$ and there exists $\varphi \in C(S_1)$ such that $\tilde{\varphi}$ is such that $\tilde{\varrho} \in Sat(\tilde{\varphi})$ iff
  - the distribution $\varrho : r \to \sum_{r' \in S_2} \tilde{\varrho}((r, r'))$ is in $Sat(\varphi)$, and
  - there exists a distribution $\varphi' \in C(S_2)$ such that $L_2(s', a, \varphi') \neq \bot$ and the distribution $\varrho' : r' \to \sum_{r \in S_1} \tilde{\varrho}((r, r'))$ is in $Sat(\varphi')$.

  Since $\tilde{\mu} \in Sat(\tilde{\varphi})$, let $\varphi' \in C(S_2)$ be the corresponding constraint on S_2 such that $L_2(s', a, \varphi') \neq \bot$. Let μ and μ' be the corresponding distributions in $Sat(\varphi)$ and $Sat(\varphi')$. Define the correspondence function $\delta : S^\wedge \to (S_1 \to [0,1])$ such that $\delta((r, r'))(r'') = 1$ iff $r'' = r$. As above, we have $\mu^\wedge \Subset^\delta_{\mathcal{R}} \mu$. The same holds in the symmetric case.

Finally, in any case, there exists $\varphi \in C(S_1)$ such that $L_1(s, a, \varphi) \neq \bot$ and there exists $\mu \in Sat(\varphi)$ such that $\mu^\wedge \Subset_{\mathcal{R}} \mu$.

3. By definition, $V^\wedge((s, s')) = \tilde{V}((s, s')) = V_1(s) \cap V_2(s') \subseteq V_1(s)$.

Finally, $\mathcal{R}$ is a weak weak refinement relation, and we have $\beta^*(N_1 \wedge N_2) \preceq_W N_1$.

• if $N_3 \preceq_W N_1$ and $N_3 \preceq_W N_2$, then $N_3 \preceq_W \beta^*(N_1 \wedge N_2)$: Let $\mathcal{R}_1 \subseteq S_3 \times S_1$ and $\mathcal{R}_2 \subseteq S_3 \times S_2$ be the weak weak refinement relations such that $N_3 \preceq_W N_1$ and $N_3 \preceq_W N_2$. Obviously, if $N_1 \wedge N_2$ is fully inconsistent, then $\beta^*(N_1 \wedge N_2)$ is empty. In this case, there are no consistent APAs refining both N_1 and N_2. As a consequence, N_3 is inconsistent, which violates the hypothesis. Suppose now that $\beta^*(N_1 \wedge N_2) = (S^\wedge, A, L^\wedge, AP, V^\wedge, (s_0^1, s_0^2))$, with $S^\wedge \subseteq S_1 \times S_2$, is not empty. Define the relation $\mathcal{R}^\wedge \subseteq S_3 \times S^\wedge$ such that $s'' \mathcal{R}^\wedge (s, s') \in S^\wedge$ iff $s'' \mathcal{R} s \in S_1$ and $s'' \mathcal{R}' s' \in S_2$. We prove that $\mathcal{R}^\wedge$ is a weak weak refinement relation. Let $s \in S_1, s' \in S_2$ and $s'' \in S_3$ such that $s'' \mathcal{R}^\wedge (s, s')$. We show that $\mathcal{R}^\wedge$ satisfies the axioms of a weak weak refinement relation.

1. Let $a \in A$ and $\varphi^\wedge \in C(S^\wedge)$ such that $L^\wedge((s, s'), a, \varphi^\wedge) = \top$. By definition, we have $\tilde{L}((s, s'), a, \tilde{\varphi}) = \top$ with $\tilde{\varphi} \in C(S_1 \times S_2)$ such that $\mu^\wedge \in Sat(\varphi^\wedge)$ iff there exists $\tilde{\mu} \in Sat(\tilde{\varphi})$ such that $\mu^\wedge(r) = \tilde{\mu}(r)$ for all $r \in S^\wedge$ and $\tilde{\mu}(r) = 0$ for all $r \in S_1 \times S_2 \setminus S^\wedge$. There are 2 cases.

   - Suppose that $a \in \mathsf{Must}(s)$ and there exists $\varphi \in C(S_1)$ such that $L_1(s, a, \varphi) = \top$, and $\tilde{\varrho} \in Sat(\tilde{\varphi})$ iff
     - the distribution $\varrho : t \to \sum_{t' \in S_2} \tilde{\varrho}((t, t'))$ is in $Sat(\varphi)$, and
     - there exists a distribution $\varphi' \in C(S_2)$ such that $L_2(s', a, \varphi') \neq \bot$ and the distribution $\varrho' : t' \to \sum_{t \in S_1} \tilde{\varrho}((t, t'))$ is in $Sat(\varphi')$.

Since $L_1(s,a,\varphi) = \top$ and $s'' \mathcal{R}_1 s$, there exists $\varphi'' \in C(S_3)$ such that $L_3(s'',a,\varphi'') = \top$ and $\forall \mu'' \in Sat(\varphi''), \exists \mu \in Sat(\varphi)$, such that $\mu'' \Subset_{\mathcal{R}_1} \mu$ (1).

Since $L_3(s'',a,\varphi'') = \top$ and $s'' \mathcal{R}_2 s'$, we have that $\forall \mu'' \in Sat(\varphi'')$, there exist $\varphi' \in C(S_2)$ such that $L_2(s',a,\varphi') \neq \bot$ and $\mu' \in Sat(\varphi')$ such that $\mu'' \Subset_{\mathcal{R}_2} \varrho'$ (2).

Let $\mu'' \in Sat(\varphi'')$. By (1) and (2), there exists $\mu \in Sat(\varphi)$, $\varphi' \in C(S_2)$ such that $L_2(s',a,\varphi') \neq \bot$ and $\mu' \in Sat(\varphi')$ such that $\mu'' \Subset_{\mathcal{R}_1} \mu$ and $\mu'' \Subset_{\mathcal{R}_2} \mu'$. Since (s,s') and s'' are consistent, remark that for all (r,r') in $S_1 \times S_2 \setminus S^\wedge$, we cannot have $s'' \mathcal{R}_1 r$ and we cannot have $s'' \mathcal{R}_2 r'$ (3).

We now build $\mu^\wedge \in Sat(\varphi^\wedge)$ such that $\mu'' \Subset_{\mathcal{R}^\wedge} \mu^\wedge$.

Let δ and δ' be the correspondence functions such that $\mu'' \Subset^{\delta}_{\mathcal{R}_1} \mu$ and $\mu'' \Subset^{\delta'}_{\mathcal{R}_2} \mu'$. Define the correspondence function $\delta'' : S_3 \to (S^\wedge \to [0,1])$ such that for all $r'' \in S_3$ and $(r,r') \in S^\wedge$, $\delta''(r'')((r,r')) = \delta(r'')(r)\delta'(r'')(r')$. We build $\mu^\wedge$ and prove that $\mu'' \Subset^{\delta''}_{\mathcal{R}^\wedge} \mu^\wedge$.

- For all $r'' \in S_3$, if $\mu''(r'') > 0$, both $\delta(r'')$ and $\delta'(r'')$ are distributions. By (3), we know that for all $(r,r') \in S_1 \times S_2 \setminus S^\wedge$, $\delta(r'')(r) = \delta'(r'')(r') = 0$. As a consequence, $\delta''(r'')$ is a distribution on $S^\wedge$.
- Define $\mu^\wedge(r,r') = \sum_{r'' \in S_3} \mu''(r'')\delta''(r'')((r,r'))$. It follows that $\mu^\wedge \in Sat(\varphi^\wedge)$. For the sake of completeness, a detailed proof of this fact is given in Appendix F.
- If $\delta''(r'')((r,r')) > 0$, then by definition $\delta(r'')(r) > 0$ and $\delta'(r'')(r') > 0$. As a consequence, $r'' \mathcal{R}_1 r$ and $r'' \mathcal{R}_2 r'$, thus $r'' \mathcal{R}^\wedge (r,r')$.

Finally, $\mu'' \Subset_{\mathcal{R}^\wedge} \mu^\wedge$ and $\mu^\wedge \in Sat(\varphi^\wedge)$. The same holds for the symmetric case.

2. Let $a \in A$ and $\varphi'' \in C(S_3)$ such that $L_3(s'',a,\varphi'') \neq \bot$. Let $\mu'' \in Sat(\varphi'')$. Since $s'' \mathcal{R}_1 s$ and $s'' \mathcal{R}_2 s'$, there must exist $\varphi \in C(S_1)$, $\mu \in Sat(\varphi)$, $\varphi' \in C(S_2)$ and $\mu' \in Sat(\varphi')$ such that $L_1(s,a,\varphi) \neq \bot$, $L_2(s',a,\varphi') \neq \bot$, $\mu'' \Subset_{\mathcal{R}_1} \mu$ and $\mu'' \Subset_{\mathcal{R}_2} \mu'$. As a consequence, $\tilde{L}((s,s'),a,\tilde{\varphi}) \neq \bot$, with $\tilde{\varphi} \in C(S_1 \times S_2)$ such that $\tilde{\varrho} \in Sat(\tilde{\varphi})$ iff the distributions $\varrho : r \in S_1 \mapsto \sum_{r' \in S_2} \tilde{\varrho}((r,r'))$ and $\varrho' : r' \in S_2 \mapsto \sum_{r \in S_1} \tilde{\varrho}((r,r'))$ are respectively in $Sat(\varphi)$ and in $Sat(\varphi')$. Moreover, since s'' and (s,s') are consistent, there exists $\varphi^\wedge \in C(S^\wedge)$ such that $L^\wedge((s,s'),a,\varphi^\wedge) \neq \bot$ and $\varrho^\wedge \in Sat(\varphi^\wedge)$ iff there exists $\tilde{\varrho} \in Sat(\tilde{\varphi})$ such that $\varrho^\wedge(r,r') = \tilde{\varrho}(r,r')$ for all $(r,r') \in S^\wedge$ and $\tilde{\varrho}(r,r') = 0$ for all $(r,r') \in S_1 \times S_2 \setminus S^\wedge$.
Let δ and δ' the correspondence functions such that $\mu'' \Subset^{\delta}_{\mathcal{R}_1} \mu$ and $\mu'' \Subset^{\delta'}_{\mathcal{R}_2} \mu'$. Since s'' and (s,s') are consistent, we know that (1) for all $(r,r') \in S_1 \times S_2 \setminus S^\wedge$, we have $\mu(r) = \mu'(r') = 0$ and (2) for all $r'' \in S_3$ and $(r,r') \in S_1 \times S_2 \setminus S^\wedge$, we cannot have $r'' \mathcal{R}_1 r$ and we cannot have $r'' \mathcal{R}_2 r'$.

Define the correspondence function $\delta'' : S_3 \to (S^\wedge \to [0,1])$ such that for all $r'' \in S_3$ and $(r, r') \in S^\wedge$, $\delta''(r'')((r,r')) = \delta(r'')(r)\delta'(r'')(r')$. We now build $\mu^\wedge$ such that $\mu'' \Subset^{\delta''}_{\mathcal{R}^\wedge} \mu^\wedge$ and prove that $\mu^\wedge \in Sat(\varphi^\wedge)$.

- For all $r'' \in S_3$, if $\mu''(r'') > 0$, both $\delta(r'')$ and $\delta'(r'')$ are distributions. By (2), we know that for all $(r, r') \in S_1 \times S_2 \setminus S^\wedge$, $\delta(r'')(r) = \delta'(r'')(r') = 0$. As a consequence, $\delta''(r'')$ is a distribution on $S^\wedge$.
- Define $\mu^\wedge(r, r') = \sum_{r'' \in S_3} \mu''(r'')\delta''(r'')((r, r'))$. As above, we can prove that $\mu^\wedge \in Sat(\varphi^\wedge)$.
- If $\delta''(r'')((r, r')) > 0$, then by definition $\delta(r'')(r) > 0$ and $\delta'(r'')(r') > 0$. As a consequence, $r'' \,\mathcal{R}_1\, r$ and $r'' \,\mathcal{R}_2\, r'$, thus $r'' \,\mathcal{R}^\wedge (r, r')$.

Finally, there exists $\varphi^\wedge \in C(S^\wedge)$ such that $L^\wedge((s, s'), a, \varphi^\wedge) \neq \bot$ and $\mu^\wedge \in Sat(\varphi^\wedge)$ such that $\mu'' \Subset_{\mathcal{R}^\wedge} \mu^\wedge$.

3. Since $s'' \,\mathcal{R}_1\, s$ and $s'' \,\mathcal{R}_2\, s'$, we have $V_3(s'') \subseteq V_1(s) \cap V_2(s') = V^\wedge((s, s'))$.

Thus, $\mathcal{R}^\wedge$ is a weak weak refinement relation between N_3 and $\beta^*(N_1 \wedge N_2)$. Moreover, we know that $s_0^3 \,\mathcal{R}_1\, s_0^1$, $s_0^3 \,\mathcal{R}_2\, s_0^2$, and (s_0^1, s_0^2) is consistent. As a consequence $s_0^3 \,\mathcal{R}^\wedge (s_0^1, s_0^2)$ and $N_3 \preceq_W \beta^*(N_1 \wedge N_2)$.

□

From the above theorem, we can easily deduce that the set of implementations of the conjunction of two given APAs is exactly the intersection of their sets of implementations.

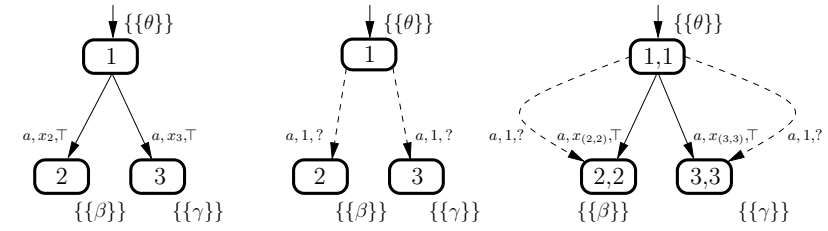
Corollary 33. *For APAs N_1 and N_2, it holds that $[\![\beta^*(N_1 \wedge N_2)]\!] = [\![N_1]\!] \cap [\![N_2]\!]$.*

Proof. Let N_1 and N_2 be APAs. We prove the result by double inclusion.

By Theorem 32, we have that $\beta^*(N_1 \wedge N_2) \preceq_W N_1$. By Theorem 17, we thus have $[\![\beta^*(N_1 \wedge N_2)]\!] \subseteq [\![N_1]\!]$. By symmetry, we also obtain that $[\![\beta^*(N_1 \wedge N_2)]\!] \subseteq [\![N_2]\!]$, and thus $[\![\beta^*(N_1 \wedge N_2)]\!] \subseteq [\![N_1]\!] \cap [\![N_2]\!]$.

Recall that every PA P can be seen as an APA in SVNF with no may transitions and with only single point constraints. Moreover, recall that all notions of refinement boil down to satisfaction when the left operand is a PA, i.e. for all PA P and for all APA N, we have $P \models N \iff P \preceq_W N \iff P \preceq N \iff P \preceq_S N$. Let P be a PA such that $P \in [\![N_1]\!] \cap [\![N_2]\!]$. By definition, we have $P \models N_1$ and $P \models N_2$, and as a consequence $P \preceq_W N_1$ and $P \preceq_W N_2$. By Theorem 32, we thus have $P \preceq_W \beta^*(N_1 \wedge N_2)$ and as a consequence $P \models \beta^*(N_1 \wedge N_2)$. Therefore, we have $[\![N_1]\!] \cap [\![N_2]\!] \subseteq [\![\beta^*(N_1 \wedge N_2)]\!]$, which concludes the proof. □

The above result is surprising. Indeed, in many theories for non-deterministic systems such as modal automata, there is no syntactical notion of conjunction that allows to compute sets of implementation [26]. Observe also that Theorem 32 holds for weak-weak refinement but neither for weak nor strong refinements. Consider APAs N_1 and N_2, and their conjunction $\beta^*(N_1 \wedge N_2)$ given in Fig. 16. It is easy to see that $\beta^*(N_1 \wedge N_2)$ cannot refine N_2 with a weak



(a) APA N_1 (b) APA N_2 (c) APA $\beta^*(N_1 \wedge N_2)$

Figure 16: APAs N_1, N_2 and their conjunction $\beta^*(N_1 \wedge N_2)$ such that $\beta^*(N_1 \wedge N_2) \not\preceq N_2$.

refinement relation. Indeed, the constraint $\varphi_x^\wedge$ present in state $(1,1)$ cannot be redistributed to a given constraint in N_2 without knowing in advance which of its solutions is considered. This again illustrates the power of interleaving constraints and modalities through weak refinement.

5. Compositional Reasoning

We now propose a composition operation mixing the properties of the composition operation on modal transition systems and the composition operation on CMCs. We then show how composition and abstraction can collaborate to avoid state-space explosion in a component-wise manner.

In our theory, the composition operation is parametrized with a set of synchronization actions like in CSP. This set allows to specify on which actions the two specifications should collaborate and on which actions they can behave individually. The intuition is as follows: synchronizing transitions have the lowest modality of the original transitions, and lead to a constraint whose solutions are product distributions of solutions of the original constraints; and non-synchronizing transitions keep their modality and impose that the other component stays in its current state.

Definition 34 (Parallel composition of APAs)**.** *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' with respect to synchronization set $\overline{A} \subseteq A \cap A'$, written as $N \| _{\overline{A}} N'$, is given as $N \| _{\overline{A}} N' = (S \times S', A \cup A', \tilde{L}, AP \cup AP', \tilde{V}, (s_0, s'_0))$ where*

- *$\tilde{L}$ is defined as follows:*
  - *For all $(s, s') \in S \times S'$, $a \in \overline{A}$, 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 $\tilde{\mu} \in Sat(\tilde{\varphi})$ if and only if there exists $\mu \in Sat(\varphi)$*

and $\mu' \in Sat(\varphi')$ *such that* $\tilde{\mu}(u,v) = \mu(u)\mu'(v)$ *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* $\tilde{\varphi} \in C(S \times S')$, $\tilde{L}((s,s'),a,\tilde{\varphi}) = \bot$.

- *For all* $(s,s') \in S \times S'$, $a \in A \setminus \overline{A}$, *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* $\tilde{\mu} \in Sat(\tilde{\varphi})$ *if and only if for all* $u \in S$ *and* $v \neq s', \tilde{\mu}(u,v) = 0$ *and the distribution* $\mu : t \mapsto \tilde{\mu}(t,s')$ *is in* $Sat(\varphi)$.
- *For all* $(s,s') \in S \times S'$, $a \in A' \setminus \overline{A}$, *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* $\tilde{\mu'} \in Sat(\tilde{\varphi}')$ *if and only if for all* $u \neq s$ *and* $v \in S', \tilde{\mu'}(u,v) = 0$ *and the distribution* $\mu' : t' \mapsto \tilde{\mu'}(s,t')$ *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* $B' \in V'(s')\}$.

Contrary to the conjunction operation, composition is defined for dissimilar alphabets. Since PAs are a restriction of APAs, their composition is defined in the same way. Remark that this boils down to the standard notion of parallel composition for PAs [5]. By inspecting Definition 34, one can see that the composition of two APAs whose constraints are systems of linear inequalities (or polynomial constraints) may lead to an APA whose constraints are polynomial. One can also see that the conjunction of two APAs with polynomial constraints is an APA with polynomial constraints. The class of polynomial constraints APAs is thus closed under all compositional design operations.

The following theorem characterizes the relation between parallel composition and refinement.

Theorem 35. *Given a synchronization set* $\overline{A}$, *all notions of refinement are a precongruence with respect to the parallel composition operator* $\|_{\overline{A}}$ *defined above, i.e. if* $N_1 \ltimes N_1'$ *and* $N_2 \ltimes N_2'$, *then* $N_1 \|_{\overline{A}} N_2 \ltimes N_1' \|_{\overline{A}} N_2'$, *for* $\ltimes \in \{\preceq_T, \preceq_W, \preceq, \preceq_S\}$.

Proof. We provide the proof for $\ltimes = \preceq$. The other proofs are similar.

Let $N_1 = (S_1, A_1, L_1, AP_1, V_1, s_0^1)$, $N_2 = (S_2, A_2, L_2, AP_2, V_2, s_0^2)$, $N_1' = (S_1', A_1, L_1', AP_1, V_1', s_0^{1'})$ and $N_2' = (S_2', A_2, L_2', AP_2, V_2', s_0^{2'})$ be APAs such that $AP_1 \cap AP_2 = \emptyset$. Let $\overline{A} \subseteq A_1 \cap A_2$. Assume that $N_1 \preceq N_1'$ and $N_2 \preceq N_2'$ with weak refinement relations $\mathcal{R}_1$ and $\mathcal{R}_2$, respectively. Let $N_1 \|_{\overline{A}} N_2 = (S_1 \times S_2, A_1 \cup A_2, L, AP_1 \cup AP_2, V, (s_0^1, s_0^2))$ and $N_1' \|_{\overline{A}} N_2' = (S_1' \times S_2', A_1 \cup A_2, L', AP_1 \cup AP_2, V', (s_0^{1'}, s_0^{2'}))$.

Let $\mathcal{R} \subseteq (S_1 \times S_2) \times (S_1' \times S_2')$ be the relation such that $(s_1, s_2)\,\mathcal{R}(s_1', s_2')$ iff $s_1 \,\mathcal{R}_1\, s_1'$ and $s_2 \,\mathcal{R}_2\, s_2'$. We now show that $\mathcal{R}$ is a weak refinement relation such that $N_1 \|_{\overline{A}} N_2 \preceq N_1' \|_{\overline{A}} N_2'$.

Assume that $(s_1, s_2)\,\mathcal{R}(s_1', s_2')$. We show that $\mathcal{R}$ satisfies the axioms of a weak refinement relation.

1. Let $a \in A_1 \cup A_2$ and $\varphi' \in C(S_1' \times S_2')$ such that $L'((s_1', s_2'), a, \varphi') = \top$. There are three cases:

- If $a \in \overline{A}$, then there exists $\varphi'_1 \in C(S'_1)$ and $\varphi'_2 \in C(S'_2)$ such that $L'_1(s'_1, a, \varphi'_1) = L'_2(s'_2, a, \varphi'_2) = \top$ and $\mu' \in Sat(\varphi')$ iff there exists $\mu'_1 \in Sat(\varphi'_1)$ and $\mu'_2 \in Sat(\varphi'_2)$ such that $\mu' = \mu'_1\mu'_2$. Since $s_1 \mathcal{R}_1 s'_1$ and $s_2 \mathcal{R}_2 s'_2$, there exists $\varphi_1 \in C(S_1)$ and $\varphi_2 \in C(S_2)$ with $L_1(s_1, a, \varphi_1) = L_2(s_2, a, \varphi_2) = \top$ and $\forall \mu_1 \in Sat(\varphi_1), \exists \mu'_1 \in Sat(\varphi'_1) : \mu_1 \Subset_{\mathcal{R}_1} \mu'_1$ and $\forall \mu_2 \in Sat(\varphi_2), \exists \mu'_2 \in Sat(\varphi'_2) : \mu_2 \Subset_{\mathcal{R}_2} \mu'_2$.

  Define $\varphi \in C(S_1 \times S_2)$ such that $Sat(\varphi) = Sat(\varphi_1)Sat(\varphi_2)$. By definition of $N_1 \|_{\overline{A}} N_2$, we have $L((s_1, s_2), a, \varphi) = \top$. Let $\mu \in Sat(\varphi)$. Then there exist $\mu_1 \in Sat(\varphi_1)$ and $\mu_2 \in Sat(\varphi_2)$ such that $\mu = \mu_1\mu_2$. Since $s_1 \mathcal{R}_1 s'_1$ and $s_2 \mathcal{R}_2 s'_2$, there exist $\mu'_1 \in Sat(\varphi'_1)$, $\mu'_2 \in Sat(\varphi'_2)$ and correspondence functions $\delta_1 : S_1 \to (S'_1 \to [0,1])$ and $\delta_2 : S_2 \to (S'_2 \to [0,1])$, such that $\mu_1 \Subset^{\delta_1}_{\mathcal{R}_1} \mu'_1$ and $\mu_2 \Subset^{\delta_2}_{\mathcal{R}_2} \mu'_2$.

  Define the correspondence function $\delta : (S_1 \times S_2) \to ((S'_1 \times S'_2) \to [0,1])$ as $\delta(u,v)(u',v') = \delta_1(u)(u') \cdot \delta_2(v)(v')$. Consider the distribution μ' such that $\mu' = \mu'_1\mu'_2$. By construction, $\mu' \in Sat(\varphi')$ and $\mu \Subset^{\delta}_{\mathcal{R}} \mu'$. For the sake of completeness, a detailed proof of this fact is given in Appendix G.

- If $a \in A_1 \setminus \overline{A}$, then there exists $\varphi'_1 \in C(S'_1)$ such that $L'_1(s'_1, a, \varphi'_1) = \top$. Since $s_1 \mathcal{R}_1 s'_1$, there exists $\varphi_1 \in C(S_1)$ with $L_1(s_1, a, \varphi_1) = \top$ and $\forall \mu_1 \in Sat(\varphi_1), \exists \mu'_1 \in Sat(\varphi'_1)$ such that $\mu_1 \Subset_{\mathcal{R}_1} \mu'_1$.

  Define $\varphi \in C(S_1 \times S_2)$ such that $\mu \in Sat(\varphi)$ iff for all $u \in S_1$ and $v \neq s_2, \mu(u,v) = 0$ and the distribution $\mu_1 : t \mapsto \mu(t, s_2)$ is in $Sat(\varphi_1)$. By definition of $N_1 \|_{\overline{A}} N_2$, we have $L((s_1, s_2), a, \varphi) = \top$. Let $\mu \in Sat(\varphi)$. Then there exists a $\mu_1 \in Sat(\varphi_1)$ such that μ_1 can be written as $t \mapsto \mu(t, s_2)$ and furthermore there exists $\mu'_1 \in Sat(\varphi'_1)$ and a correspondence function $\delta_1 : S_1 \to (S'_1 \to [0,1])$ such that $\mu_1 \Subset^{\delta_1}_{\mathcal{R}_1} \mu'_1$.

  Define the correspondence function $\delta : (S_1 \times S_2) \to ((S'_1 \times S'_2) \to [0,1])$ as $\delta(u,v)(u',v') = \delta(u)(u')$ if $v = s_2$ and $v' = s'_2$, and 0 otherwise. Consider the distribution μ' over $S'_1 \times S'_2$ such that for all $u' \in S'_1$ and $v' \neq s'_2$, $\mu'(u', v') = 0$ and for all $u' \in S'_1$ $\mu'(u', s'_2) = \mu'_1(u')$. By construction, $\mu' \in Sat(\varphi')$ and $\mu \Subset^{\delta}_{\mathcal{R}} \mu'$. For the sake of completeness, a detailed proof of this fact is given in Appendix G.

- If $a \in A_2 \setminus \overline{A}$, the proof is similar.

2. Let $a \in A_1 \cup A_2$ and $\varphi \in C(S_1 \times S_2)$ such that $L((s_1, s_2), a, \varphi) \neq \bot$. There are three cases:

   - If $a \in \overline{A}$, then there exists $\varphi_1 \in C(S_1)$ and $\varphi_2 \in C(S_2)$ such that $L_1(s_1, a, \varphi_1) \neq \bot$, $L_2(s_2, a, \varphi_2) \neq \bot$, and $\mu \in Sat(\varphi)$ iff there exist $\mu_1 \in Sat(\varphi_1)$ and $\mu_2 \in Sat(\varphi_2)$ such that $\mu = \mu_1\mu_2$. Since $s_1 \mathcal{R}_1 s'_1$ and $s_2 \mathcal{R}_2 s'_2$, there exists $\varphi'_1 \in C(S'_1)$ and $\varphi'_2 \in C(S'_2)$ with $L'_1(s'_1, a, \varphi'_1) \neq \bot$, $L'_2(s'_2, a, \varphi'_2) \neq \bot$, and $\forall \mu_1 \in Sat(\varphi_1), \exists \mu'_1 \in Sat(\varphi'_1) : \mu_1 \Subset_{\mathcal{R}_1} \mu'_1$ and $\forall \mu_2 \in Sat(\varphi_2), \exists \mu'_2 \in Sat(\varphi'_2) : \mu_2 \Subset_{\mathcal{R}_2} \mu'_2$.

Define $\varphi' \in C(S_1' \times S_2')$ such that $Sat(\varphi') = Sat(\varphi_1')Sat(\varphi_2')$. By definition of $N_1' \| _{\overline{A}} N_2'$, we have $L'((s_1', s_2'), a, \varphi') \neq \bot$. Let $\mu \in Sat(\varphi)$. By definition of φ, there exist $\mu_1 \in Sat(\varphi_1)$ and $\mu_2 \in Sat(\varphi_2)$ such that $\mu = \mu_1\mu_2$. Furthermore, since $s_1 \mathcal{R}_1 s_1'$ and $s_2 \mathcal{R}_2 s_2'$, there exist $\mu_1' \in Sat(\varphi_1')$, $\mu_2' \in Sat(\varphi_2')$ and two correspondence functions $\delta_1 : S_1 \to (S_1' \to [0,1])$ and $\delta_2 : S_2 \to (S_2' \to [0,1])$ such that $\mu_1 \Subset^{\delta_1}_{\mathcal{R}_1} \mu_1'$ and $\mu_2 \Subset^{\delta_2}_{\mathcal{R}_2} \mu_2'$.
Define the correspondence function $\delta : (S_1 \times S_2) \to ((S_1' \times S_2') \to [0,1])$ such that, for all u, u', v, v', $\delta(u,v)(u',v') = \delta_1(u)(u') \cdot \delta_2(v)(v')$. By the same calculations as above, we know that the distribution μ' over $S_1' \times S_2'$ constructed as $\mu' = \mu_1'\mu_2'$ is in $Sat(\varphi')$ and gives that $\mu \Subset^{\delta}_{\mathcal{R}} \mu'$.

- If $a \in A_1 \setminus \overline{A}$, then there exists $\varphi_1 \in C(S_1)$ such that $L_1(s_1, a, \varphi_1) \neq \bot$. Since $s_1 \mathcal{R}_1 s_1'$, there exists $\varphi_1' \in C(S_1')$ with $L_1'(s_1', a, \varphi_1') \neq \bot$ and $\forall \mu_1 \in Sat(\varphi_1), \exists \mu_1' \in Sat(\varphi_1') : \mu_1 \Subset_{\mathcal{R}_1} \mu_1'$.
  Define $\varphi' \in C(S_1' \times S_2')$ such that $\mu' \in Sat(\varphi')$ iff for all $u' \in S_1'$ and $v' \neq s_2', \mu(u', v') = 0$ and the distribution $\mu_1' : t \mapsto \mu(t, s_2')$ is in $Sat(\varphi_1')$. By definition of $N_1' \| _{\overline{A}} N_2'$, we have $L'((s_1', s_2'), a, \varphi') \neq \bot$. Let $\mu \in Sat(\varphi)$. Let μ_1 be the distribution on S_1 such that for all $t \in S_1$, $\mu_1(t) = \mu(t, s_2)$. By definition, $\mu_1 \in Sat(\varphi_1)$. Let $\mu_1' \in Sat(\varphi_1')$ and a correspondence function $\delta_1 : S_1 \to (S_1' \to [0,1])$ such that $\mu_1 \Subset^{\delta_1}_{\mathcal{R}_1} \mu_1'$.
  Define the correspondence function $\delta : (S_1 \times S_2) \to ((S_1' \times S_2') \to [0,1])$ such that for all u, u', v, v', $\delta(u,v)(u',v') = \delta_1(u)(u')$ if $v = s_2$ and $v' = s_2'$, and 0 otherwise. By the same calculations as above, we know that the distribution $\mu' \in Sat(\varphi')$ such that for all $u' \in S_1'$ and $v' \neq s_2'$, $\mu'(u', v') = 0$ and for all $u' \in S_1'$, $\mu_1' = \mu'(u', s_2')$, gives that $\mu \Subset^{\delta}_{\mathcal{R}} \mu'$.
- If $a \in A_2 \setminus \overline{A}$, the proof is similar.

3. For atomic propositions we have that, $V((s_1, s_2)) = V_1(s_1) \cup V_2(s_2)$ and $V'((s_1', s_2')) = \{B = B_1 \cup B_2 \mid B_1 \in V_1'(s_1') \text{ and } B_2 \in V_2'(s_2')\}$. Since $s_1 \mathcal{R}_1 s_1'$ and $s_2 \mathcal{R}_2 s_2'$, we know by definition that $V_1(s_1) \in V_1'(s_1')$ and $V_2(s_2) \in V_2'(s_2')$. Considering $B_1 = V_1(s_1)$ and $B_2 = V_2(s_2)$, we thus have that $V((s_1, s_2)) \in V'((s_1', s_2'))$.

By observing that $(s_0^1, s_0^2)\, \mathcal{R}(s_0^{1'}, s_0^{2'})$, since $s_0^1 \mathcal{R}_1 s_0^{1'}$ and $s_0^2 \mathcal{R}_2 s_0^{2'}$, we conclude that $\mathcal{R}$ is a weak refinement relation. □

The facts that abstraction preserves strong refinement (cf. Lemma 24), and that strong refinement is a precongruence with respect to parallel composition, enable us to apply abstraction in a component-wise manner. That is to say, rather than first generating (the typically large PA) $M \| _{\overline{A}} N$, and then applying abstraction, it allows for first applying abstraction, yielding $\alpha_1(M)$ and $\alpha_2(N)$, respectively, and then constructing $\alpha_1(M) \| _{\overline{A}} \alpha_2(N)$. Possibly a further abstraction of $\alpha_1(M) \| _{\overline{A}} \alpha_2(N)$ can be employed. The next theorem shows that

component-wise abstraction is as powerful as applying the combination of the "local" abstractions to the entire model.

Theorem 36. *Let M and N be APAs, $\overline{A}$ a synchronization set, and α_1, α_2 be abstraction functions. The following holds:*

$$\alpha_1(M) \parallel_{\overline{A}} \alpha_2(N) = (\alpha_1 \times \alpha_2)(M \parallel_{\overline{A}} N) \qquad \textit{up to isomorphism.}$$

Proof. Let $M = (S, A, L, AP, V, s_0)$ and $N = (S'', A'', L'', AP'', V'', s_0'')$ be APAs and let $\overline{A} \subseteq A \cap A''$ be a synchronization set such that the parallel composition of M and N is given as $M \| _{\overline{A}} N = (S \times S'', A \cup A'', \tilde{L}, AP \cup AP'', \tilde{V}, (s_0, s_0''))$.

Let $\alpha_1 : S \to S'$ and $\alpha_2 : S'' \to S'''$. Let $\alpha_1(M) = (S', A, L', AP, V', \alpha_1(s_0))$, $\alpha_2(N) = (S''', A'', L''', AP'', V''', \alpha_2(s_0''))$ and $(\alpha_1 \times \alpha_2)(M \| _{\overline{A}} N) = (S' \times S''', A \cup A'', \tilde{L}', AP \cup AP'', \tilde{V}', (\alpha_1(s_0), \alpha_2(s_0'')))$ be the induced APA. Let $\alpha_1(M) \| _{\overline{A}} \alpha_2(N) = (S' \times S''', A \cup A'', \tilde{L}'', AP \cup AP'', \tilde{V}'', (\alpha_1(s_0), \alpha_2(s_0'')))$.

Notice that the signatures of $\alpha_1(M) \| _{\overline{A}} \alpha_2(N)$ and $(\alpha_1 \times \alpha_2)(M \| _{\overline{A}} N)$ only differ on constraint functions and valuation functions. We establish the result by proving the following: for all $(s', s''') \in S' \times S'''$, $a \in A \cup A''$, and $\tilde{\varphi} \in C(S' \times S''')$, we have $\tilde{V}'((s', s''')) = \tilde{V}''((s', s'''))$ and $\tilde{L}'((s', s'''), a, \tilde{\varphi}) = \tilde{L}''((s', s'''), a, \tilde{\varphi})$.

Let $(s', s''') \in S' \times S'''$.

- The valuation of (s', s''') in $\alpha_1(M) \| _{\overline{A}} \alpha_2(N)$ is

$$\begin{aligned}
\tilde{V}''((s', s''')) &= \{B \cup B' | B \in V'(s') \wedge B' \in V'''(s''')\} \\
&= \bigcup_{(s,s'') \in (\gamma_1 \times \gamma_2)(s', s''')} \{B \cup B' | B \in V(s) \wedge B' \in V''(s'')\} \\
&= \bigcup_{(s,s'') \in (\gamma_1 \times \gamma_2)(s', s''')} \tilde{V}((s, s'')) \\
&= \tilde{V}'((s', s''')).
\end{aligned}$$

- For constraint functions we have the following:
  - Let $a \in \overline{A}$ and $\tilde{\varphi}' \in C(S' \times S''')$ such that $\tilde{L}'((s', s'''), a, \tilde{\varphi}') = \top$: then for all $(s, s'') \in (\gamma_1 \times \gamma_2)(s', s''')$, we have that there exists $\varphi_{M \| N} \in C(S \times S'')$ yielding $\tilde{L}((s, s''), a, \varphi_{M \| N}) = \top$ and

$$Sat(\tilde{\varphi}') = (\alpha_1 \times \alpha_2) \left(\bigcup_{\substack{((s,s''), \varphi_{M \| N}) \in (\gamma_1 \times \gamma_2)(s', s''') \times C(S \times S''): \\ L((s,s''), a, \varphi_{M \| N}) = \top}} Sat(\varphi_{M \| N}) \right). \tag{6}$$

    For each of these $\varphi_{M \| N}$, we have, by the definition of parallel composition, that there exists $\varphi_M \in C(S)$ and $\varphi_N \in C(S'')$ such that $L(s, a, \varphi_M) = \top$ and $L''(s'', a, \varphi_N) = \top$ and $\mu_{M \| N} \in Sat(\varphi_{M \| N})$ iff there exists $\mu_M \in Sat(\varphi_M)$ and $\mu_N \in Sat(\varphi_N)$ st. $\mu_{M \| N}(u, v) =$

$\mu_M(u)\mu_N(v)$ for all $(u,v) \in S \times S''$. Define $\varphi_{\alpha_1(M)} \in C(S')$, such that $Sat(\varphi_{\alpha_1(M)})$ is the abstraction of the union of satisfaction sets of such φ_M. Similarly, define $\varphi_{\alpha_2(N)} \in C(S''')$, such that $Sat(\varphi_{\alpha_2(N)})$ is the abstraction of the union of satisfaction sets of such φ_N. That is,

$$Sat(\varphi_{\alpha_1(M)}) = \alpha_1(\bigcup\nolimits_{(s,\varphi_M)\in\gamma_1(s')\times C(S):L(s,a,\varphi_M)=\top} Sat(\varphi_M)) \quad (7)$$

$$Sat(\varphi_{\alpha_2(N)}) = \alpha_2(\bigcup\nolimits_{(s'',\varphi_N)\in\gamma_2(s''')\times C(S):L(s'',a,\varphi_N)=\top} Sat(\varphi_N))$$

We will now have that $L'(s', a, \varphi_{\alpha_1(M)}) = \top$ and $L'''(s''', a, \varphi_{\alpha_2(N)}) = \top$. The definition of parallel composition implies that $\tilde{L}''((s', s'''), a, \tilde{\varphi}'') = \top$ and $\mu_{\alpha_1(M)\|\alpha_2(N)} \in Sat(\tilde{\varphi}'')$ iff there exists $\mu_{\alpha_1(M)} \in Sat(\varphi_{\alpha_1(M)})$ and $\mu_{\alpha_2(N)} \in Sat(\varphi_{\alpha_2(N)})$ st. $\mu_{\alpha_1(M)\|\alpha_2(N)}(u,v) = \mu_{\alpha_1(M)}(u)\mu_{\alpha_2(N)}(v)$ for all $(u,v) \in S \times S''$. It is clear that $Sat(\tilde{\varphi}') = Sat(\tilde{\varphi}'')$.

The proof is similar if $\tilde{L}'((s', s'''), a, \tilde{\varphi}') =?$.

- Let $a \notin \overline{A}$ (or wlog. $a \in A \setminus \overline{A}$) and $\tilde{\varphi}' \in C(S' \times C''')$ such that $\tilde{L}'((s', s'''), a, \tilde{\varphi}') = \top$: then for all $(s, s'') \in (\gamma_1 \times \gamma_2)(s', s''')$, we have that there exists $\varphi_{M\|N} \in C(S \times S'')$ yielding $\tilde{L}((s, s''), a, \varphi_{M\|N}) = \top$ and $\tilde{\varphi}'$ is defined as in Equation 6. For each of these $\varphi_{M\|N}$, we have, by the definition of parallel composition, that there exists $\varphi_M \in C(S)$ such that $L(s, a, \varphi_M) = \top$ and $\mu_{M\|N} \in Sat(\varphi_{M\|N})$ iff for all $u \in S$ and $v \neq s''$, $\mu_{M\|N}(u, v) = 0$ and $\mu_{M\|N}(u, s'') = \varphi_M(u)$. Define $\varphi_{\alpha_1(M)} \in C(S')$, such that $Sat(\varphi_{\alpha_1(M)})$ is the abstraction of the union of satisfaction sets of such φ_M i.e. as in Equation 7. We will now have that $L'(s', a, \varphi_{\alpha_1(M)}) = \top$. The definition of parallel composition implies that $\tilde{L}''((s', s'''), a, \tilde{\varphi}'') = \top$ and $\mu_{\alpha_1(M)\|\alpha_2(N)} \in Sat(\tilde{\varphi}'')$ iff there exists $\mu_{\alpha_1 M} \in Sat(\varphi_{\alpha_1 M})$ st. for all $u \in S'$ and $v \neq s'''$, $\mu_{\alpha_1(M)\|\alpha_2(N)}(u, v) = 0$ and $\mu_{\alpha_1(M)\|\alpha_2(N)}(u, s''') = \mu_{\alpha_1(M)}(u)$. It is clear that $Sat(\tilde{\varphi}') = Sat(\tilde{\varphi}'')$.

  The proof is similar if $\tilde{L}'((s', s'''), a, \tilde{\varphi}') =?$.

□

The above theorem helps avoiding state-space explosion when combining systems by allowing for abstraction as soon as possible.

This result cannot be transferred to the notion of constraint-abstraction. Indeed, as shown for Interval Markov Chains [22], the parallel composition of two IPAs is not an IPA. However, we can prove the following proposition, relating composition, constraint-abstraction and refinement.

Proposition 37. *Let $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A', L', AP', V', s'_0)$ be APAs with $AP \cap AP' = \emptyset$. For $\overline{A} \subseteq A \cap A'$, $\chi(N)\|_{\overline{A}}\chi(N') \preceq_S \chi(N\|_{\overline{A}}N')$.*

Proof. Let $N\|_{\overline{A}}N' = (S \times S', A \cup A', L_\|, AP \cup AP', V_\|, (s_0, s'_0))$, $\chi(N) = (S, A, L^\chi_N, AP, V^\chi_N, s_0)$, $\chi(N') = (S', A', L^\chi_{N'}, AP', V^\chi_{N'}, s'_0)$, $\chi(N)\|_{\overline{A}}\chi(N') = (S \times S', A \cup A', L^\|_\chi, AP \cup AP', V^\|_\chi, (s_0, s'_0))$, and $\chi(N\|_{\overline{A}}N') = (S \times S', A \cup A', L^\chi_\|, AP \cup AP', V^\chi_\|, (s_0, s'_0))$. As $\chi(N)\|_{\overline{A}}\chi(N')$ and $\chi(N\|_{\overline{A}}N')$ have similar state space, structure, valuations, and initial states, we consider the identity relation $\mathcal{R} = \mathrm{Id}_{S\times S'}$ and show that it is a strong refinement relation. Let $s_1 \in S$ and $s'_1 \in S'$ such that $(s_1, s'_1)\,\mathcal{R}(s_1, s'_1)$. We show that $\mathcal{R}$ satisfies the axioms of a strong refinement relation. All the correspondence functions we consider are the identity functions.

1. Let $a \in A \cup A'$, $\varphi^\chi_\| \in C(S \times S')$ such that $L^\chi_\|((s_1, s'_1), a, \varphi^\chi_\|) = \top$. Then by construction of $\chi(N\|_{\overline{A}}N')$, there exists $\varphi_\| \in C(S \times S')$ such that $L_\|((s_1, s'_1), a, \varphi_\|) = \top$.
   - If $a \in \overline{A}$, then there exists $\varphi \in C(S)$ and $\varphi' \in C(S')$ such that $L(s_1, a, \varphi) = \top$ and $L'(s'_1, a, \varphi') = \top$ and $\mu_\| \in Sat(\varphi_\|)$ iff there exists $\mu \in Sat(\varphi)$ and $\mu' \in Sat(\varphi')$ such that $\mu_\|(u, v) = \mu(u)\mu'(v)$ for all $u \in S$ and $v \in S'$. By construction of $\chi(N)$ and $\chi(N')$, there exists $\varphi^\chi_N \in C(S)$ and $\varphi^\chi_{N'} \in C(S')$ such that $L^\chi_N(s_1, a, \varphi^\chi_N) = \top$ and $L^\chi_{N'}(s'_1, a, \varphi^\chi_{N'}) = \top$. This means that there exists $\varphi^\|_\chi \in C(S \times S')$ such that $L^\|_\chi((s_1, s'_1), a, \varphi^\|_\chi) = \top$, where $\mu^\|_\chi \in Sat(\varphi^\|_\chi)$ iff there exists $\mu^\chi_N \in Sat(\varphi^\chi_N)$ and $\mu^\chi_{N'} \in Sat(\varphi^\chi_{N'})$ such that $\mu^\|_\chi(u, v) = \mu^\chi_N(u)\mu^\chi_{N'}(v)$ for all $u \in S$ and $v \in S'$. We now show that $\forall \mu^\|_\chi \in Sat(\varphi^\|_\chi) \exists \mu^\chi_\| \in Sat(\varphi^\chi_\|) : \mu^\|_\chi \Subset_\mathcal{R} \mu^\chi_\|$ by showing that $\mu^\|_\chi \in Sat(\varphi^\chi_\|)$ (and indeed $\mu^\|_\chi \Subset_\mathcal{R} \mu^\|_\chi$). Assume that $\mu^\|_\chi \notin Sat(\varphi^\chi_\|)$. By definition, there exists $\mu^\chi_N \in Sat(\varphi^\chi_N)$ and $\mu^\chi_{N'} \in Sat(\varphi^\chi_{N'})$ such that $\mu^\|_\chi(u, v) = \mu^\chi_N(u)\mu^\chi_{N'}(v)$ for all $u \in S$ and $v \in S'$. Let $(I^N_u)_{u\in S}$, $(I^{N'}_v)_{v\in S'}$, and $I^\|_{(u,v)} = [m^\|_{(u,v)}, M^\|_{(u,v)}])_{(u,v)\in S'}$ be the intervals associated with φ^χ_N, $\varphi^\chi_{N'}$, and $\varphi^\|_\chi$, respectively.

     If $\mu^\|_\chi \notin Sat(\varphi^\chi_\|)$, there must exists $u' \in S$ and $v' \in S'$ such that $\mu^\chi_N(u')\mu^\chi_{N'}(v') \notin I^\|_{(u',v')}$, that is, $\mu^\chi_N(u')\mu^\chi_{N'}(v') < m^\|_{(u',v')}$ or $\mu^\chi_N(u')\mu^\chi_{N'}(v') > M^\|_{(u',v')}$; assume the latter. By convexity and minimality of $I^N_{u'}$ and $I^{N'}_{v'}$, for all constants $\epsilon > 0$, there must exist $\mu \in Sat(\varphi)$ and $\mu' \in Sat(\varphi')$ such that $\mu^\chi_N(u') - \mu(u') < \epsilon$ and $\mu^\chi_{N'}(v') - \mu'(v') < \epsilon$. For $\epsilon = \frac{\mu^\chi_N(u')\mu^\chi_{N'}(v') - M^\|_{(u',v')}}{2}$, we have that $\mu(u')\mu'(v') > M^\|_{(u',v')}$. However, the distribution $\mu_\|$ defined as $\mu_\|(u, v) = \mu(u)\mu'(v)$ for all $u \in S$ and $v \in S'$, will satisfy $\varphi_\|$, which contradicts the definition of $I^\|_{(u',v')}$. As a consequence, $\mu^\|_\chi \in Sat(\varphi^\chi_\|)$.
   - If $a \notin \overline{A}$, then assume that $a \in A$. Then there exists $\varphi \in C(S)$ such that $L(s_1, a, \varphi) = \top$ and $\mu_\| \in Sat(\varphi_\|)$ iff for all $u \in S$, $u \neq s_1$, and $v \in S'$, $\mu_\|(u, v) = 0$ and there exists $\mu \in Sat(\varphi)$ such that

$\mu(v) = \mu_{\|}(s_1, v)$ for all $v \in S'$. By construction of $\chi(N)$, there exists $\varphi_N^\chi \in C(S)$ such that $L_N^\chi(s_1, a, \varphi_N^\chi) = \top$. This means that there exists $\varphi_\chi^{\|} \in C(S \times S')$ such that $L_\chi^{\|}((s_1, s_1'), a, \varphi_\chi^{\|}) = \top$, where $\mu_\chi^{\|} \in Sat(\varphi_\chi^{\|})$ iff for all $u \in S$, $u \neq s_1$, and $v \in S'$, $\mu_\chi^{\|}(u, v) = 0$ and there exists $\mu_N^\chi \in Sat(\varphi_N^\chi)$ such that $\mu_N^\chi(v) = \mu_\chi^{\|}(s_1, v)$ for all $v \in S'$. As above, it holds that $\forall \mu_\chi^{\|} \in Sat(\varphi_\chi^{\|}), \exists \mu_{\|}^\chi \in Sat(\varphi_{\|}^\chi) : \mu_\chi^{\|} \Subset_{\mathcal{R}} \mu_{\|}^\chi$.

2. Let $a \in A \cup A'$, $\varphi_\chi^{\|} \in C(S \times S')$ such that $L_\chi^{\|}((s_1, s_1'), a, \varphi_\chi^{\|}) \neq \bot$.
   - If $a \in \overline{A}$, then there exists $\varphi_N^\chi \in C(S)$ and $\varphi_{N'}^\chi \in C(S')$ such that $L_N^\chi(s_1, a, \varphi_N^\chi) \neq \bot$ and $L_{N'}^\chi(s_1', a, \varphi_{N'}^\chi) \neq \bot$ and $\mu_\chi^{\|} \in Sat(\varphi_\chi^{\|})$ iff there exists $\mu_N^\chi \in Sat(\varphi_N^\chi)$ and $\mu_{N'}^\chi \in Sat(\varphi_{N'}^\chi)$ such that $\mu_\chi^{\|}(u, v) = \mu_N^\chi(u)\mu_{N'}^\chi(v)$ for all $u \in S$ and $v \in S'$. By construction of $\chi(N)$ and $\chi(N')$, there exists $\varphi \in C(S)$ and $\varphi' \in C(S')$ such that $L(s_1, a, \varphi) = L_N^\chi(s_1, a, \varphi_N^\chi)$ and $L'(s_1', a, \varphi') = L_{N'}^\chi(s_1', a, \varphi_{N'}^\chi)$. This gives rise to the existence of $\varphi_{\|} \in C(S \times S')$ such that $L_{\|}((s_1, s_1'), a, \varphi_{\|}) \neq \bot$ and $\mu_{\|} \in Sat(\varphi_{\|})$ iff there exists $\mu \in Sat(\varphi)$ and $\mu' \in Sat(\varphi')$ such that $\mu_{\|}(u, v) = \mu(u)\mu'(v)$ for all $u \in S$ and $v \in S'$. By construction of $\chi(N \|_{\overline{A}} N')$, there exists $\varphi_{\|}^\chi \in C(S \times S')$ such that $L_{\|}^\chi((s_1, s_1'), a, \varphi_{\|}^\chi) \neq \bot$. As above, $\forall \mu_\chi^{\|} \in Sat(\varphi_\chi^{\|}) \exists \mu_{\|}^\chi \in Sat(\varphi_{\|}^\chi) : \mu_\chi^{\|} \Subset_{\mathcal{R}} \mu_{\|}^\chi$.
   - If $a \notin \overline{A}$, then assume that $a \in A$. Again, we can show existence of $\varphi_{\|}^\chi \in C(S \times S')$ such that $L_{\|}^\chi((s_1, s_1'), a, \varphi_{\|}^\chi) \neq \bot$ and $\forall \mu_\chi^{\|} \in Sat(\varphi_\chi^{\|}) \exists \mu_{\|}^\chi \in Sat(\varphi_{\|}^\chi) : \mu_\chi^{\|} \Subset_{\mathcal{R}} \mu_{\|}^\chi$.

We conclude that $\chi(N) \|_{\overline{A}} \chi(N') \preceq_S \chi(N \|_{\overline{A}} N')$. □

6. Deterministic APAs

In this section, we focus on the class of deterministic APAs. Like in any specification theory, deterministic specifications form a class with interesting properties. First, notice that action-deterministic APAs allow for more convenient definitions for refinement and conjunction, as explained in [2, 1]. In the following, we first propose an algorithm that can be applied to any APA N and provides a deterministic APA $\varrho(N)$ that abstracts N. Then, we study the strong link between CMCs and APAs and prove that, like for CMCs [18, 19], all the notions of refinement coincide for deterministic specifications.

6.1. Determinisation

As explained in [2], the use of non-determinism changes expressiveness of APAs with respect to the known conjunction operator. In fact, non-deterministic APAs are *generally* more expressive than deterministic ones. Fig. 17 presents a non-deterministic APA, whose set of implementations cannot be specified by a single deterministic APA. States 2 and 3 have overlapping labels (so state 1

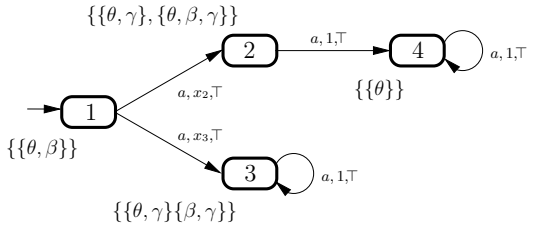


Figure 17: A (valuation) non-deterministic APA whose set of implementations cannot be obtained with a deterministic APA.

has non-deterministic behaviour). We cannot put these states on two separate a-transitions as this introduces action non-determinism. We cannot merge them either, as their subsequent evolutions are different (and for the same reason we cannot factor $\{\theta, \gamma\}$ to a separate state).

Nevertheless, the use of deterministic abstractions of non-deterministic behaviours is an interesting alternative to relying on more complex refinements and more complex operators. Below, we present a determinisation algorithm that can be applied to any APA N, producing a deterministic APA $\varrho(N)$, such that $N \preceq_S \varrho(N)$.

Our algorithm is based on subset construction and resembles the determinisation procedure for modal transition systems described in [27].

Let $N = (S, A, L, AP, V, s_0)$ be a (consistent) APA in SVNF. Given a set of states $Q \subseteq S$, an action $a \in A$ and a valuation $\theta \subseteq AP$ we define $\mathsf{Reach}(Q, a, \theta)$ to be the maximal set of states with valuation θ that can be reached with a non-zero probability using a distribution μ satisfying a constraint φ such that $L(q, a, \varphi) \neq \bot$ for some $q \in Q$. Formally, $\mathsf{Reach} : 2^S \times A \times 2^{AP} \to 2^S$ is defined by:

$$\mathsf{Reach}(Q, a, \theta) = \bigcup \{ s \in S \mid V(s) = \{\theta\} \text{ and } \exists q \in Q,$$
$$\exists \varphi \in C(S), \exists \mu \in \mathit{Sat}(\varphi),\ L(q, a, \varphi) \neq \bot \text{ and } \mu(s) > 0 \}$$

We lift this definition to all possible labellings as follows:

$$\mathsf{Reach}(Q, a) = \{ \mathsf{Reach}(Q, a, \theta) \mid \theta \in 2^{AP} \}$$

We also extend the definition to sets of actions as follows: let $B \subseteq A$,

$$\mathsf{Reach}(Q, B) = \bigcup_{a \in B} \mathsf{Reach}(Q, a)$$

Now let $n > 1$ and define the n-step reachability as

$$\mathsf{Reach}^n(Q, B) = \mathsf{Reach}^{n-1}(Q, B) \cup \bigcup_{Q' \in \mathsf{Reach}^{n-1}(Q, B)} \mathsf{Reach}(Q', B)$$

where $\mathsf{Reach}^1(Q,B) = \mathsf{Reach}(Q,B)$.
We denote the fixpoint of Reach as follows:

$$\mathsf{Reach}^*(Q,B) = \bigcup_{n=1}^{\infty} \mathsf{Reach}^n(Q,B).$$

Now, by construction, the following properties hold:

- For all $Q \subseteq S$ and $a \in A$, for all $Q', Q'' \in \mathsf{Reach}(Q,a)$, if $Q' \neq Q''$ then $Q' \cap Q'' = \emptyset$, and
- For all $Q \subseteq S$, $B \subseteq A$ and $Q' \in \mathsf{Reach}^*(Q,B)$, there exists $\theta \in 2^{AP}$ such that $\forall q' \in Q'$, we have $V(q') = \{\theta\}$.

We will now use the notion of reachability in our determinisation construction. Remark that the determinisation algorithm highly relies on the single valuation normal form of the APA. In order to use it on any APA (with single valuation in the initial state), it is thus necessary to use the normalization algorithm first, as defined in Definition 11.

Definition 38 (Determinisation)**.** *Let $N = (S, A, L, AP, V, s_0)$ be a consistent APA in SVNF. A deterministic APA for N is the APA $\varrho(N) = (S', A, L', AP, V', \{s_0\})$ such that*

- $S' = \{s_0\} \cup \mathsf{Reach}^*(\{s_0\}, A)$
- *V' is such that $V'(Q) = \{\theta\}$ if and only if $\forall q \in Q. V(q) = \{\theta\}$. There always exists exactly one such θ by construction*
- *L' is defined as follows: Let $Q \in S'$ and $a \in A$.*
  - *If, for all $q \in Q$, we have that $\forall \varphi \in C(S)$, $L(q,a,\varphi) = \bot$, then define $L'(Q,a,\varphi') = \bot$ for all $\varphi' \in C(S')$.*
  - *Otherwise, define $\varphi' \in C(S')$ such that $\mu' \in Sat(\varphi')$ if and only if (1) $\forall Q' \notin \mathsf{Reach}(Q,a)$, we have $\mu'(Q') = 0$, and (2) there exists $q \in Q$, $\varphi \in C(S)$ and $\mu \in Sat(\varphi)$ such that $L(q,a,\varphi) \neq \bot$ and $\forall Q' \in \mathsf{Reach}(Q,a)$, $\mu'(Q') = \sum_{q' \in Q'} \mu(q')$. Then define*

$$L'(Q,a,\varphi') = \begin{cases} \top \text{ if } \begin{array}{c} \forall q \in Q, \exists \varphi \in C(S): \\ L(q,a,\varphi) = \top \end{array} \\ ? \text{ otherwise} \end{cases}$$

Example. *Consider the non-deterministic APA $\mathcal{N}(N)$ given in Figure 7. Using Definition 38, we obtain the APA $\varrho(\mathcal{N}(N))$ given in Figure 18.*

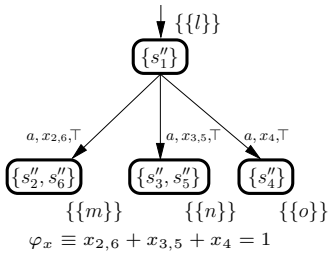


Figure 18: Determinisation $\varrho(\mathcal{N}(N))$ of the APA $\mathcal{N}(N)$ given in Figure 7.

By construction, $\varrho(N)$ is action- and valuation-deterministic. As expected, determinisation is an abstraction, but more than that it is also the smallest deterministic abstraction of N. This is formalized in the following theorem.

Theorem 39. *Let N be an APA in SVNF. The following statements hold:*

1. $N \preceq_S \varrho(N)$, *and*
2. *for all deterministic APA N' in SVNF, if $N \preceq N'$, then $\varrho(N) \preceq N'$.*

Proof. Let $N = (S, A, L, AP, V, s_0)$ be a (consistent) APA in SVNF. Let $\varrho(N) = (S', A, L', AP, V', \{s_0\})$ be the determinisation of N defined as in Definition 38. We prove the two statements separately.
1. We prove that $N \preceq_S \varrho(N)$ by providing the following strong refinement relation. Let $\mathcal{R} \subseteq S \times S'$ be the relation such that $s \mathcal{R} Q \iff s \in Q$ for all $Q \in S'$. The proof that $\mathcal{R}$ is a strong refinement relation is standard. For the sake of completeness, a detailed proof is given in Appendix H.
2. Let $N' = (T, A, L^T, AP, V^T, t_0)$ be a deterministic APA in SVNF. Assume that $N \preceq N'$ with weak refinement relation $\mathcal{R} \subseteq S \times T$ (notice that since N' is deterministic, weak refinement coincides with weak weak refinement). Let $\mathcal{R}' \subseteq S' \times T$ be the relation such that $Q \mathcal{R}' t$ if and only if $q \mathcal{R} t$ for all $q \in Q$. We prove that $\mathcal{R}'$ is a weak refinement relation. Let $(Q, t) \in \mathcal{R}'$.

1. Let $a \in A$ and $\varphi^t \in C(T)$ be such that $L^T(t, a, \varphi^t) = \top$. By definition of $\mathcal{R}'$, for all $s \in Q$, we have $(s, t) \in \mathcal{R}$. Thus, by definition of $\mathcal{R}$, for all $s \in Q$, there exists $\varphi^s \in C(S)$ such that $L(s, a, \varphi^s) = \top$ and for all $\mu_s \in Sat(\varphi^s)$, there exists $\mu_s^t \in Sat(\varphi^t)$ such that $\mu_s \Subset_{\mathcal{R}} \mu_s^t$. As a consequence, by definition of $\varrho(N)$, there exists $\varphi' \in C(S')$ such that $L(Q, a, \varphi') = \top$.
   Let $\mu' \in Sat(\varphi')$. By construction of φ', there exists $s \in Q, \varphi^s \in C(S)$ and $\mu \in Sat(\varphi^s)$ such that $L(s, a, \varphi^s) \neq \bot$ and for all $Q' \in \mathsf{Reach}(Q, a)$, $\mu'(Q') = \sum_{s' \in Q'} \mu(s')$. Since $(Q, t) \in \mathcal{R}'$, we have $(s, t) \in \mathcal{R}$ and therefore there exists $\varphi'^t \in C(T)$ such that $L^T(t, a, \varphi'^t) \neq \bot$. By determinism of N', we have $\varphi'^t = \varphi^t$. Moreover, there must exist a correspondence function δ^s and $\mu^t \in Sat(\varphi^t)$ such that $\mu \Subset_{\mathcal{R}}^{\delta^s} \mu^t$. Let $\delta : S' \to (T \to [0, 1])$ be such that $\delta(Q')(t) = \sum_{s' \in Q'} \frac{\mu(s')\delta^s(s')(t)}{\mu'(Q')}$ if $\mu'(Q') > 0$ and 0 otherwise. We now show that δ is a correspondence function and that $\mu' \Subset_{\mathcal{R}'}^{\delta} \mu^t$.

- Let $Q' \in S'$ be such that $\mu'(Q') > 0$. As a consequence, for all $s' \in Q$ such that $\mu(s') > 0$, $\delta^s(s') \in Dist(T)$. As a consequence, $\sum_{s' \in Q'} \frac{\mu(s')\delta^s(s')(t)}{\mu(Q')}$ is also a distribution on T and $\delta(Q') \in Dist(T)$.
- Let $t' \in T$, we have

$$\begin{aligned}\sum_{Q' \in S'} \mu'(Q')\delta(Q')(t') &= \sum_{Q' \in S' \mid \mu'(Q')>0} \mu'(Q') \sum_{s' \in Q'} \frac{\mu(s')\delta^s(s')(t)}{\mu'(Q')} \\ &= \sum_{Q' \in S' \mid \mu'(Q')>0} \sum_{s' \in Q'} \mu(s')\delta^s(s')(t) \\ &= \sum_{s' \in S} \mu(s')\delta^s(s')(t) \\ &= \mu^t(t)\end{aligned}$$

- Let $(Q', t') \in S' \times T$ be such that $\delta(Q')(t') > 0$. Since $Q' \in \mathsf{Reach}(Q, a)$ by construction, we have that for all $s' \in Q'$, there exists $s^r \in Q$, $\varphi^r \in C(S)$ and $\mu^r \in Sat(\varphi^r)$ such that $L(s, a, \varphi^r) \neq \bot$ and $\mu^r(s') > 0$. Since $(s, t) \in \mathcal{R}$ and by determinism of N', we can show that $(s', t') \in \mathcal{R}$. Therefore we have that $(s', t') \in \mathcal{R}$ for all $s' \in Q'$ and consequently $(Q', t') \in \mathcal{R}'$.

As a consequence, $\mu' \Subset^{\delta}_{\mathcal{R}'} \mu^t$.

2. Let $a \in A$ and $\varphi' \in C(S')$ be such that $L'(Q, a, \varphi') \neq \bot$. By construction, there must thus exist $s \in Q$ and $\varphi^s \in C(S)$ such that $L(s, a, \varphi^s) \neq \bot$. Therefore, since $(s, t) \in \mathcal{R}$, there must exist $\varphi^t \in C(T)$ such that $L^T(t, a, \varphi^t) \neq \bot$. Then, by the same reasoning as above, we can show that for all $\mu' \in Sat(\varphi')$, there exists $\mu^t \in Sat(\varphi^t)$ such that $\mu' \Subset_{\mathcal{R}'} \mu^t$.
3. Recall that there exists $\theta \in 2^{AP}$ such that $V(s) = \theta$ for all $s \in Q$. Since $(s, t) \in \mathcal{R}$ for all $s \in Q$, we have $\theta \subseteq V^T(t)$ and therefore $V'(Q) \subseteq V^T(t)$.

Finally, $\mathcal{R}'$ is a weak refinement relation. Moreover, $(\{s_0\}, t_0) \in \mathcal{R}'$ by construction, and thus $\varrho(N) \preceq N'$. □

6.2. Completeness and Relation with CMCs

In this section, we show that thorough and strong refinements coincide for deterministic APAs. For doing so, we will compare the expressive power of APAs and CMCs, showing that APAs can act as a specification theory for MCs. Remark that single valuation normal form of CMCs is defined similarly as for APAs. The satisfaction relation between MCs and CMCs as well as the notions of weak and strong refinements are also defined similarly as for APAs.

On the relation between CMCs and APAs. We now show that APAs can act as a specification theory for MCs. For doing so, we propose a satisfaction relation between MCs and APAs. Our definition is in two steps. First we show how to use PAs as a specification theory for MCs. Then, we use the existing satisfaction relation between PAs and APAs to conclude.

Since MCs do not directly allow choices between actions, we use *bipartite* MCs in the following. Their state space is partitioned into *action-states* (Q_D in the definition below) and *distribution-states* (Q_N in the definition below), and an execution of a bipartite MC is a succession of alternations between action-states and distribution-states.

Definition 40 (MC-PA Satisfaction)**.** *Let $P = (S, A, L, AP, V, s_0)$ be a PA*[1]*. Let $M = (Q, \pi, A_M, V_M, q_0)$ be a bipartite Markov chain such that (1) $Q = Q_N \cup Q_D$, with $Q_N \cap Q_D = \emptyset$, for all $q, q' \in Q_N, \pi(q)(q') = 0$ and for all $q, q' \in Q_D$, $\pi(q)(q') = 0$, (2) $q_0 \in Q_D$, and (3) $A_M = A \cup AP$. Let $\mathcal{R} \subseteq Q_D \times S$. $\mathcal{R}$ is a satisfaction relation if and only if whenever $q \mathcal{R} s$, we have*

1. *$V_M(q) = V(s)$.*
2. *For $a \in A$ and $\mu \in Dist(S)$ such that $L(s, a, \mu) = \top$, there exists $q' \in Q_N$ such that $V_M(q') = V(s) \cup \{a\}$, $\pi(q)(q') > 0$, and $\pi(q') \Subset_{\mathcal{R}} \mu$.*
3. *For all $q' \in Q_N$ such that $\pi(q)(q') > 0$, there exists $a \in A$ and $\mu \in Dist(S)$ such that $V_M(q') = V(s) \cup \{a\}$, $L(s, a, \mu) = \top$, and $\pi(q') \Subset_{\mathcal{R}} \mu$.*

We say that M satisfies P if and only if there exists a satisfaction relation $\mathcal{R}$ such that $q_0 \mathcal{R} s_0$.

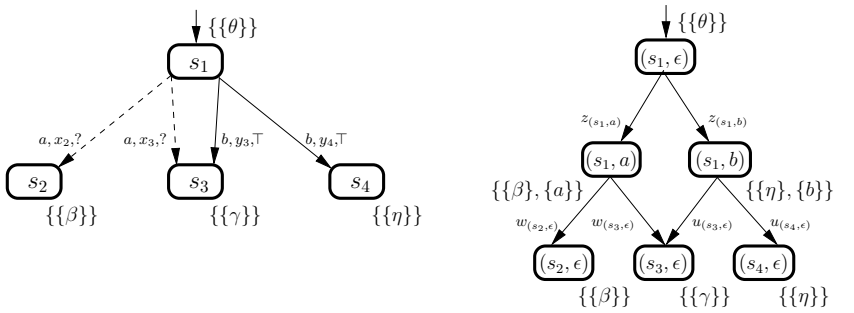
The satisfaction relation between MCs and APAs follows directly. We say that a MC M satisfies an APA N, which we write $M \models_{MC} N$, if and only if there exists a PA P such that M satisfies P and P satisfies N. The set of MC-implementation of APA N is denoted $[\![N]\!]_{MC}$.

Expressivity Completeness. In the previous paragraph, we have proposed a satisfaction relation for MCs with respect to APAs. We now propose a transformation that associates to every deterministic APA in SVNF a deterministic CMC in SVNF representing the same set of MC-implementations. The purpose of this transformation is to show that deterministic APAs do not allow for describing a larger class of Markov Chains than deterministic CMCs.

Definition 41 (Transformation $\widehat{\ }$)**.** *Let $N = (S, A, L, AP, V, s_0)$ be a deterministic APA. Let ϵ be a fresh variable. The CMC corresponding to N is $\widehat{N} = (\widehat{Q}, \psi, \widehat{A}, \widehat{V}, \widehat{q_0})$, with*

- $\widehat{Q} = S \times (A \cup \{\epsilon\})$,
- $\widehat{q_0} = (s_0, \epsilon)$,
- $\widehat{A} = AP \cup A$,
- $\widehat{V}((s, \epsilon)) = V(s)$ *for all* s,
- $\widehat{V}((s, a)) = \{B \cup \{a\} \mid B \in V(s)\}$ *for all* s *and* $a \in A$, *and*

[1] Recall that we assume $\mathsf{Act} \cap AP = \emptyset$ for all PAs/APAs



(a) N (b) $\widehat{N}$

Figure 19: APA N and CMC $\widehat{N}$

- *ψ is such that*
  - *For all $(s,\epsilon) \in \widehat{Q}$, $\psi((s,\epsilon))(\pi) = 1$ if and only if*

$$\begin{cases} \pi((s,\epsilon)) = 0 \\ \forall s' \neq s, b \in A \cup \{\epsilon\},\ \pi((s',b)) = 0 \\ \forall a \in \mathsf{Must}(s),\ \pi(s,a) > 0 \\ \forall a \notin \mathsf{May}(s),\ \pi(s,a) = 0 \end{cases}$$

  - *For all $a \in A$ and $(s,a) \in \widehat{Q}$, $\psi((s,a))(\pi) = 1$ if and only if (1) for all $s' \in S$ and $b \in A$, we have $\pi((s',b)) = 0$ and (2) the distribution $\pi' : s' \mapsto \pi((s',\epsilon))$ is such that there exists $\varphi \in C(S)$ such that $L(s,a,\varphi) \neq \bot$ and $\pi' \in Sat(\varphi)$.*

Informally, this transformation builds a CMC with a bipartite state space. The non-determinism inherent to APAs in the choice of actions is simulated by new states of the form (s,a) for each action a that can be taken from state s. The probability of reaching state (s,a) emulates the modality of taking the corresponding a-transition, and the constraint associated to state (s,a) matches the constraint associated to the corresponding a-transition.

Example. *Consider the APA N given in Figure 19a. Applying the transformation given in Definition 41 to N yields the CMC $\widehat{N}$ given in Figure 19b.*

By construction, the CMC $\widehat{N}$ is deterministic and in single valuation normal form. As expected, this transformation yields a CMC that admits the same set of MC-implementations as the original APA. This is formalized in the following theorem.

Theorem 42. *For all deterministic APA N in SVNF, the CMC $\widehat{N}$ is such that $[\![N]\!]_{MC} = [\![\widehat{N}]\!]$.*

Proof. We prove the two directions separately.

• $M \models_{\mathrm{MC}} N \Rightarrow M \models_{\mathrm{CMC}} \widehat{N}$: Let $M = (Q, \pi, A_M, V_M, q_0)$ be a Markov Chain. We first prove that if $M \models_{\mathrm{MC}} N$, then $M \models_{\mathrm{CMC}} \widehat{N}$. Suppose that there exists a PA $P = (S_P, A, L_P, AP, V_P, s_0^P)$ such that M satisfies P and $P \models N$. Let $\widehat{N} = (\widehat{Q}, \psi, \widehat{A}, \widehat{V}, \widehat{q_0})$ be the transformation of N following Definition 41. By the satisfaction relation between M and P, we obtain that $A_M = A \cup AP$ and $Q = Q_N \cup Q_D$. Let $\mathcal{R}^{MC} \subseteq Q_D \times S_P$ be the satisfaction relation witnessing that M satisfies P. Let $\mathcal{R}^{\mathrm{PA}} \subseteq S_P \times S$ be the satisfaction relation witnessing $P \models N$. Consider the relation $\mathcal{R} \subseteq Q \times \widehat{Q}$ such that

- $q\,\mathcal{R}(s, \epsilon)$ iff there exists $p \in S_p$ such that $q\,\mathcal{R}^{MC}\,p$ and $p\,\mathcal{R}^{\mathrm{PA}}\,s$, and
- for all $a \in A$, $q\,\mathcal{R}(s, a)$ iff there exists $q' \in Q$ such that
  - $\pi(q')(q) > 0$,
  - $V_M(q) = V_M(q') \cup \{a\}$, and
  - $q'\,\mathcal{R}(s, \epsilon)$.

The proof that $\mathcal{R}$ is a satisfaction relation for CMCs is standard. For the sake of completeness, the full proof is given in Appendix I.

Moreover, we have that $q_0\,\mathcal{R}(s_0, \epsilon)$, which gives that $M \models_{\mathrm{CMC}} \widehat{N}$.

• $M \models_{\mathrm{MC}} N \Leftarrow M \models_{\mathrm{CMC}} \widehat{N}$: Let $M = (Q, \pi, A_M, V_M, q_0)$ be a Markov Chain. We prove that if $M \models_{\mathrm{CMC}} \widehat{N}$, then $M \models_{\mathrm{MC}} N$, i.e. there exists a PA P such that M satisfies P and $P \models N$. Let $\widehat{N} = (\widehat{Q}, \psi, \widehat{A}, \widehat{V}, \widehat{q_0})$ be the transformation of N following Definition 41.
Let $\mathcal{R}$ be the satisfaction relation for CMCs witnessing that $M \models_{\mathrm{CMC}} \widehat{N}$. First observe that, by $\mathcal{R}$, the Markov chain M satisfies the following properties: Let $Q_D = \{q \in Q \mid \exists s \in S,\ q\,\mathcal{R}(s, \epsilon)\}$ and $Q_N = \{q \in Q \mid \exists s \in S, a \in A,\ q\,\mathcal{R}(s, a)\}$, we have

- $Q_D \cap Q_N = \emptyset$ because of their valuations and $\mathcal{R}$,
- $\forall q, q' \in Q_D$, $\pi(q)(q') = 0$ and $\forall q, q' \in Q_N$, $\pi(q)(q') = 0$,
- $q_0 \in Q_D$, and
- $A_M = A \cup AP$.

Define the PA $P = (S_P, A, L_P, AP, V_P, s_0^P)$ such that $S_P = Q_D$, with $s_0^P = q_0$, V_P is such that for all $q \in Q_D$, $V_P(q) = V_M(q)$, and L_P is such that for all $s \in S_P$, $a \in A$ and for all distribution ϱ over S_P, $L(s, a, \varrho) = \top$ iff there exists $q' \in Q_N$ such that

- $\pi(q)(q') > 0$,
- $V(q') = V(q) \cup \{a\}$, and
- $\varrho = \pi(q')$.

By construction, M satisfies P using the identity relation on Q_D. We now prove that $P \models N$. Let $\mathcal{R}^{\text{PA}} \subseteq S_P \times S$ the relation such that $p \mathcal{R}^{\text{PA}} s$ iff $p \mathcal{R}(s, \epsilon)$. The proof that $\mathcal{R}^{\text{PA}}$ is a satisfaction relation for APA is standard and given in Appendix I. By construction, we have that $s_0^P \mathcal{R}^{\text{PA}} s_0$, thus $P \models N$. As a consequence, we have that there exists a PA P such that M satisfies P and $P \models N$. Thus $M \models_{\text{MC}} N$. □

We have just shown that for all APA N, there exists a CMC $\widehat{N}$ such that $[\![N]\!]_{\text{MC}} = [\![\widehat{N}]\!]_{\text{CMC}}$. The reverse of the theorem also holds up to a syntactical transformation that preserves sets of implementations. Since CMCs are not equipped with actions, this transformation adds a single action to all valuations of the original CMC in order to provide actions for the transitions of the equivalent APA. Additionally, it duplicates the state-space in order to obtain a bipartite CMC with bipartite MCs as implementations.

Consider a MC $M = (Q, \pi, A, V, q_0)$ and a fresh variable for actions $\theta \notin A$. Let $\check{M} = (Q_N \cup Q_P, \check{\pi}, A \cup \{\theta\}, \check{V}, q_0^D)$ be the MC such that

- $Q_D = \{q^D \mid q \in Q\}$,
- $Q_N = \{q^N \mid q \in Q\}$,
- $\check{V}$ is such that $\check{V}(q) = V(q)$ if $q \in Q_D$ and $\check{V}(q) = V(q) \cup \{\theta\}$ if $q \in Q_N$, and
- $\check{\pi}$ is such that
  - for all $q^D \in Q_D$, $\check{\pi}(q^D)(q^N) = 1$, and
  - for all $q^N \in Q_N$, $\check{\pi}(q^N)(q') = \pi(q)(q')$ if $q' \in Q_D$ and 0 otherwise.

This transformation naturally extends to CMCs. Obviously, it follows that for all MC M and CMC C, we have $M \models_{\text{CMC}} C \iff \check{M} \models_{\text{CMC}} \check{C}$. The transformation from CMC $\check{M}$ to an APA is then obvious, and preserves the set of implementations.

This result together with Theorems 27 and 29 of [28] leads to the following important result.

Theorem 43. *For deterministic APAs with single valuations in the initial state, strong refinement coincides with thorough, weak-weak and weak refinement.*

Proof. Let $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A, L', AP, V', s_0')$ be two pruned deterministic APA in single valuation normal form. From Theorem 17, we know that strong refinement implies thorough refinement. We now prove that the reverse also holds.

Suppose that $[\![N]\!] \subseteq [\![N']\!]$. We prove that $N \preceq_S N'$.
Let $\widehat{N} = (\widehat{Q}, \psi, \widehat{A}, \widehat{V}, \widehat{q_0})$ and $\widehat{N'} = (\widehat{Q'}, \psi', \widehat{A}, \widehat{V'}, \widehat{q_0'})$ be the CMCs equivalent to N and N' (up to MC satisfaction) obtained by the transformation proposed in Definition 41. By Definition of $[\![\cdot]\!]_{\text{MC}}$, we have that $[\![N]\!]_{\text{MC}} \subseteq [\![N']\!]_{\text{MC}}$. As a consequence, by Theorem 42, we have that $[\![\widehat{N}]\!]_{\text{CMC}} \subseteq [\![\widehat{N'}]\!]_{\text{CMC}}$. Since $\widehat{N}$

and $\widehat{N'}$ are deterministic CMCs in single valuation normal form, we have, by Theorem 18 of [18], that $\widehat{N} \preceq^{\mathrm{CMC}} \widehat{N'}$ with a strong refinement relation between CMCs.
Let $\widehat{\mathcal{R}}$ be the strong refinement relation between CMCs such that $\widehat{N} \preceq^{\mathrm{CMC}} \widehat{N'}$. Define the relation $\mathcal{R} \subseteq S \times S'$ such that $s \,\mathcal{R}\, s'$ iff $(s, \epsilon)\widehat{\mathcal{R}}(s', \epsilon)$. We prove that $\mathcal{R}$ is indeed a strong refinement relation on APAs. Let $s \in S$ and $t \in S'$ such that $s \,\mathcal{R}\, t$. We show that $\mathcal{R}$ satisfies the axioms of a strong refinement relation for APAs.

1. Let $a \in A$ and $\varphi' \in C(S')$ such that $L'(t, a, \varphi') = \top$. By construction, we have $(s, \epsilon)\widehat{\mathcal{R}}(t, \epsilon)$, thus there exists a correspondence function $\widehat{\delta}$ such that for all distribution π satisfying $\psi((s, \epsilon))$ we have that $\pi' = \pi\widehat{\delta}$ satisfies $\psi'((t, \epsilon))$. By construction, of ψ', we thus have that $\pi'((s, a)) > 0$. As a consequence, there exists $(s', b) \in \widehat{Q}$ such that $\pi((s', b)) > 0$ and $\widehat{\delta}((s', b)(t, a)) > 0$. By definition of $\widehat{\delta}$ and ψ, we have that $s' = s$ and $b = a$. Thus $\pi((s, a)) > 0$. Since this holds for all $\pi \in Sat(\psi)$, we have $a \in \mathsf{Must}(s)$. Thus there exists $\varphi \in C(S)$ such that $L(s, a, \varphi) \neq \top$.
   Moreover, we have that $(s, a)\widehat{\mathcal{R}}(t, a)$. Let $\widehat{\delta'}$ be the associated correspondence function. Let $\mu \in Sat(\varphi)$ and let $\mu' \in Dist(\widehat{Q})$ such that for all $s' \in S$ and $b \in A$, $\mu'((s', \epsilon)) = \mu(s')$ and $\mu'((s', b)) = 0$. By definition, we have that μ' satisfies $\psi((s, a))$. Thus, we have that $\varrho' = \mu'\widehat{\delta'}$ satisfies $\psi'((t, a))$. As a consequence, the distribution $\varrho \in Dist(S')$ such that $\varrho(t') = \varrho'((t', \epsilon))$ for all t' is such that there exists φ'' such that $L'(t, a, \varphi'') \neq \bot$ and $\varrho \in Sat(\varphi'')$. By action-determinism of N', we have that $\varphi'' = \varphi'$.
   Let δ be the correspondence function such that $\delta(s')(t') = \widehat{\delta'}((s', \epsilon))((t', \epsilon))$. We prove that $\mu \Subset^{\delta}_{\mathcal{R}} \varrho$.
   (a) Let $s' \in S$ such that $\mu(s') > 0$. As a consequence, $\mu'((s', \epsilon)) > 0$. As a consequence, by definition of $\widehat{\delta'}$, we have that $\widehat{\delta'}((s', \epsilon))$ is a distribution over $\widehat{Q'}$. Moreover, since $\varrho' = \mu'\widehat{\delta'}$ satisfies $\psi'((t, a))$, we have that for all $t' \in T$ and $b \in A$, $\varrho'((t', b)) = 0$. As a consequence, we have that for all $t' \in T$ and $b \in A$, $\widehat{\delta'}((s', \epsilon))((t', b)) = 0$. Thus $\delta(s')$ is a correct distribution over Q'.
   (b) By definition, we have $\varrho' = \mu'\widehat{\delta'}$. Since $\mu((s', b)) = 0$ for all $b \in A$, and since $\widehat{\delta'}((s', \epsilon))((t', b)) = 0$ for all $s' \in S$, $t' \in S'$ and $b \in A$, we have that $\varrho = \mu\delta$. As a consequence, we have that for all $t' \in S'$,
   $$\sum_{s' \in S} \mu(s')\delta(s')(t') = \varrho(t').$$
   (c) Let $s' \in S$ and $t' \in T$ such that $\delta(s')(t') > 0$. By definition of δ, we have $\delta'((s', \epsilon))((t', \epsilon)) > 0$. Thus $(s', \epsilon)\widehat{\mathcal{R}}(t', \epsilon)$, and consequently $s' \,\mathcal{R}\, t'$.
   Therefore, we have that $\mu \Subset^{\delta}_{\mathcal{R}} \varrho$.

2. Let $a \in A$ and $\varphi \in C(S)$ such that $L(s,a,\varphi) \neq \bot$. By construction, we have $(s,\epsilon)\widehat{\mathcal{R}}(t,\epsilon)$, thus there exists a correspondence function $\widehat{\delta}$ such that for all distribution π satisfying $\psi((s,\epsilon))$ we have that $\pi' = \pi\widehat{\delta}$ satisfies $\psi'((t,\epsilon))$. By construction of ψ, and because N is pruned, there must exist $\pi \in Dist(\widehat{Q})$ satisfying $\psi((s,\epsilon))$, with $\pi((s,a)) > 0$. As a consequence, $\widehat{\delta}$ defines a distribution on $\widehat{Q'}$, thus there exists $(t',b) \in \widehat{Q'}$ such that $\widehat{\delta}((s,a))((t',b)) > 0$. By the recursion axiom, we have $b = a$. Let $\pi' = \pi\widehat{\delta}$, we have $\pi'((t',a)) > 0$. Since π' satisfies $\psi'((t,\epsilon))$, we have that necessarily $t' = t$. As a consequence, by definition of ψ', there must exist $\varphi' \in C(S')$ such that $L'(t,a,\varphi') \neq \bot$. As above, we can prove that there exists δ such that for all $\mu \in Sat(\varphi)$, there exists $\varrho \in Sat(\varphi')$ such that $\mu \Subset^{\delta}_{\mathcal{R}} \varrho$.
3. Since $(s,\epsilon)\widehat{\mathcal{R}}(t,\epsilon)$, we have that $V(s) \subseteq V'(s')$.

Finally, $\mathcal{R}$ is a strong refinement relation. Moreover, we have by construction that $s_0 \,\mathcal{R}\, t_0$, thus $N \preceq_S N'$.
By the ordering of the refinement relations presented in Theorem 17, it follows that $\mathcal{R}$ is also a weak and a weak-weak refinement relation.

□

7. Extensions of Alphabets (Dissimilar Alphabets)

So far, the specification theory of APAs has required that all specifications share same alphabets of actions and atomic propositions. We are now going to lift this restriction by introducing the alphabet extension mechanism. As for the extension of modal transition systems [16], there exist two ways of extending alphabets [29]: it is necessary to choose the modality of transitions for new actions introduced depending on the operation being applied to the result.

The weak extension is used when conjoining specifications with different alphabets. This extension adds may loop transitions for all new actions and extends the sets of atomic propositions in a classical way:

Definition 44 (Weak extension)**.** *Let $N = (S, A, L, AP, V, s_0)$ be an APA, and let A' and AP' be sets of actions and atomic propositions such that $A \subseteq A'$ and $AP \subseteq AP'$. Let the weak extension of N to (A', AP') be the APA $N{\Uparrow}(A', AP') = (S, A', L', AP', V', s_0)$ such that for all states $s \in S$:*

- $L'(s,a,\varphi) = L(s,a,\varphi)$ *if* $a \in A$,
- $L'(s,a,\varphi) = ?$ *if* $a \in A' \backslash A$ *and* φ *only admits a single point distribution* μ *such that* $\mu(s) = 1$.
- $V'(s) = \{B \subseteq AP' \mid B \cap AP \in V(s)\}$.

A different extension, the strong one, is used in parallel composition. This extension adds must self-loops for all new actions and extends the sets of atomic propositions in a classical way.

Definition 45 (Strong extension)**.** *Let $N = (S, A, L, AP, V, s_0)$ be an APA, and let A' and AP' be sets of actions and atomic propositions such that $A \subseteq A'$ and $AP \subseteq AP'$. Define the extension for composition of N to A', AP', written $N \uparrow^{A',AP'}$ to be the APA $N \uparrow^{A',AP'} = (S, A', L', AP', V', s_0)$ such that*

- *for all $s \in S$, $a \in A$ and $\varphi \in C(S)$, $L'(s, a, \varphi) = L(s, a, \varphi)$,*
- *for all $s \in S$ and $a \in A' \setminus A$, define $L(s, a, \varphi) = \top$, with φ such that $\mu \in Sat(\varphi)$ if and only if $\mu(s) = 1$, and*
- *for all $s \in S$, $V'(s) = \{B \subseteq AP' \mid B \cap AP \in V(s)\}$.*

These different notions of extension give rise to different notions of satisfaction and refinement between structures with dissimilar sets of actions. Satisfaction (or refinement) between structures with different sets of actions is defined as the satisfaction (respectively refinement) between the structures after extension to a union of their alphabets.

By construction, all the results presented in the paper for conjunction and composition of PAs / APAs sharing alphabets of actions and atomic propositions safely extend to the setting of PAs / APAs with dissimilar alphabets, provided that the right extension is applied first.

8. Conclusion

This paper presents Abstract Probabilistic Automata, a new abstraction theory for Probabilistic Automata. The main contributions of the paper are:

- A new abstraction theory for Probabilistic Automata through APAs.
- A new specification theory for PAs using APAs as a specification language. Our theory is equipped with a parallel composition and conjunction operators, and satisfaction and refinement relations.
- A complete characterization of semantic and syntactic notions of refinement, and the characterization of a class of APAs on which they coincide.
- A compositional abstraction technique for APAs which can be used to combate the state-space explosion problem.
- A proof that the proposed formalism is backward compatible with classical notions of probabilistic bisimulation / parallel composition of Probabilistic Automata.

There are various directions for future research. The first of them is to implement and evaluate our results. This would require to design efficient algorithms for the compositional design operators. Also, it would be of interest to embed our abstraction procedure in a CEGAR model checking algorithm. Another interesting direction would be to design an algorithm to decide thorough

refinement and characterize the complexity of this operation. Finally, one could also consider a continuous-timed extension of our model inspired by [30].

Acknowledgements. This work was supported by the European STREP-COMBEST project no. 215543, by VKR Centre of Excellence MT-LAB, by "Action de Recherche Collaborative" ARC (TP)I, and by the EU FP7 project MoVeS.

References

[1] B. Delahaye, J.-P. Katoen, K. Larsen, A. Legay, M. Pedersen, F. Sher, A. Wasowski, Abstract Probabilistic Automata, in: Verification, Model Checking, and Abstract Interpretation (VMCAI), Vol. 6538 of LNCS, Springer, 2011, pp. 324–339.

[2] B. Delahaye, J.-P. Katoen, K. Larsen, A. Legay, M. Pedersen, F. Sher, A. Wasowski, New Results on Abstract Probabilistic Automata, in: Application of Concurrency to System Design (ACSD), IEEE, 2011, pp. 118–127.

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

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

[5] R. Segala, N. A. Lynch, Probabilistic Simulations for Probabilistic Processes, Nordic Journal of Computing (NJC) 2 (2) (1995) 250–273.

[6] R. Segala, Probability and Nondeterminism in Operational Models of Concurrency, in: Concurrency Theory (CONCUR), Vol. 4173 of LNCS, Springer, 2006, pp. 64–78.

[7] A. Parma, R. Segala, Axiomatization of Trace Semantics for Stochastic Nondeterministic Processes, in: Quantitative Evaluation of Systems (QEST), IEEE, 2004, pp. 294–303.

[8] D. N. Jansen, H. Hermanns, J.-P. Katoen, A Probabilistic Extension of UML Statecharts, in: Formal Techniques in Real-Time and Fault-Tolerant Systems (FTRTFT), Vol. 2469 of LNCS, Springer, 2002, pp. 355–374.

[9] L. Cheung, N. A. Lynch, R. Segala, F. W. Vaandrager, Switched PIOA: Parallel Composition via Distributed Scheduling, Theoretical Computer Science TCS 365 (1-2) (2006) 83–108.

[10] R. Canetti, L. Cheung, D. K. Kaynar, M. Liskov, N. A. Lynch, O. Pereira, R. Segala, Analyzing Security Protocols using Time-Bounded Task-PIOAs, Discrete Event Dynamic Systems 18 (1) (2008) 111–159.

[11] S. Cattani, R. Segala, Decision Algorithms for Probabilistic Bisimulation, in: Concurrency Theory (CONCUR), Vol. 2421 of LNCS, Springer, 2002, pp. 371–385.

[12] L. Cheung, M. Stoelinga, F. W. Vaandrager, A Testing Scenario for Probabilistic Processes, Journal of the ACM (JACM) 54 (6).

[13] B. Jonsson, K. G. Larsen, Specification and Refinement of Probabilistic Processes, in: Logic in Computer Science (LICS), IEEE, 1991, pp. 266–277.

[14] H. Fecher, M. Leucker, V. Wolf, Don't Know in Probabilistic Systems, in: Model Checking Software, Vol. 3925 of LNCS, Springer, 2006, pp. 71–88.

[15] J.-P. Katoen, D. Klink, M. Leucker, V. Wolf, Three-Valued Abstraction for Continuous-Time Markov Chains, in: Computer Aided Verification (CAV), Vol. 4590 of LNCS, Springer, 2007, pp. 316–329.

[16] K. G. Larsen, B. Thomsen, A Modal Process Logic, in: Logic in Computer Science (LICS), IEEE, 1988, pp. 203–210.

[17] K. G. Larsen, Modal Specifications, in: Automatic verification methods for finite state systems (AVMFSS), Vol. 407, Springer, 1989, pp. 232–246.

[18] B. Caillaud, B. Delahaye, K. G. Larsen, A. Legay, M. L. Pedersen, A. Wąsowski, Compositional Design Methodology with Constraint Markov Chains, in: Quantitative Evaluation of Systems (QEST), IEEE, 2010, pp. 123 –132.

[19] B. Caillaud, B. Delahaye, K. G. Larsen, A. Legay, M. L. Pedersen, A. Wasowski, Constraint Markov Chains, Theoretical Computer Science (TCS) 412 (34) (2011) 4373 – 4404.

[20] L. de Alfaro, T. A. Henzinger, Interface-based Design, in: Engineering Theories of Software-intensive Systems, Vol. 195 of NATO Science Series: Mathematics, Physics, and Chemistry, Springer, 2005, pp. 83–104.

[21] K. G. Larsen, A. Skou, Bisimulation through Probabilistic Testing (preliminary report), in: Principles of Programming Languages (POPL), ACM, 1989, pp. 344–352.

[22] B. Delahaye, K. G. Larsen, A. Legay, M. L. Pedersen, A. Wąsowski, Decision problems for interval Markov chains, in: Language and Automata Theory and Applications (LATA), Springer, 2011, pp. 274–285.

[23] K. Larsen, U. Nyman, A. Wąsowski, Modal I/O Automata for Interface and Product Line Theories, in: Programming Languages and Systems (PLS), Vol. 4421 of LNCS, Springer, 2007, pp. 64–79.

[24] N. Benes, J. Kretínský, K. G. Larsen, J. Srba, Checking Thorough Refinement on Modal Transition Systems is EXPTIME-complete, in: International Colloquium on Theoretical Aspects of Computing (ICTAC), Vol. 5684 of LNCS, Springer, 2009, pp. 112–126.

[25] J.-B. Raclet, E. Badouel, A. Benveniste, B. Caillaud, A. Legay, R. Passerone, Modal Interfaces: Unifying Interface Automata and Modal Specifications, in: Embedded Sofware (EMSOFT), ACM, 2009, pp. 87–96.

[26] D. Fischbein, S. Uchitel, On correct and complete strong merging of partial behaviour models, in: SIGSOFT FSE, ACM, 2008, pp. 297–307.

[27] N. Benes, J. Kretínský, K. G. Larsen, J. Srba, On Determinism in Modal Transition Systems, Theoretical Computer Science (TCS) 410 (41) (2009) 4026–4043.

[28] 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.

[29] J.-B. Raclet, E. Badouel, A. Benveniste, B. Caillaud, R. Passerone, Why Are Modalities Good for Interface Theories?, in: Application of Concurrency to System Design (ACSD), IEEE, 2009, pp. 119–127.

[30] J.-P. Katoen, D. Klink, M. R. Neuhäußer, Compositional Abstraction for Stochastic Systems, in: Formal Modeling and Analysis of Timed Systems (FORMATS), Vol. 5813 of LNCS, Springer, 2009, pp. 195–211.

Appendix A. Details of the proof of Theorem 17

• $(\preceq_T) \supseteq (\preceq_W) \supseteq (\preceq) \supseteq (\preceq_S)$: By a swap of quantifiers in the definitions, it is obvious that strong refinement implies weak refinement, and that weak refinement implies weak weak refinement. We prove that weak weak refinement implies thorough refinement. Let $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A, L', AP, V', s'_0)$ be APAs such that $N \preceq_W N'$ with a weak weak refinement relation $\mathcal{R}' \subseteq S \times S'$. If $[\![N]\!] = \emptyset$, we have $[\![N]\!] \subseteq [\![N']\!]$. Otherwise, let $P = (S_P, A, L_P, AP, V_P, s_0^P)$ be a PA such that $P \models N$. Then there exists a satisfaction relation $\mathcal{R}'' \subseteq S_P \times S$ such that $s_0^P \,\mathcal{R}''\, s_0$.
Let $\mathcal{R} \subseteq S_P \times S'$ be the relation such that $u \,\mathcal{R}\, w$ iff there exists $v \in S$ such that $u \,\mathcal{R}''\, v$ and $v \,\mathcal{R}'\, w$. We prove that $\mathcal{R}$ is a satisfaction relation.
Let $u \in S_P$ and $w \in S'$ such that $u \,\mathcal{R}\, w$, and let $v \in S$ such that $u \,\mathcal{R}''\, v$ and $v \,\mathcal{R}'\, w$. We show that $\mathcal{R}$ satisfies the axioms of a satisfaction relation.

1. Let $a \in A'$ and $\varphi' \in C(S')$ such that $L'(w, a, \varphi') = \top$. By $\mathcal{R}'$, there exists $\varphi \in C(S)$ such that $L(v, a, \varphi) = \top$ and $\forall \mu \in Sat(\varphi), \exists \mu' \in Sat(\varphi')$ such that $\mu \Subset_{R'} \mu'$. Moreover, by $\mathcal{R}''$, there exists $\mu_P \in Dist(S_P)$ such that $L_P(u, a, \mu_P) = \top$ and $\exists \mu_S \in Sat(\varphi) : \mu_P \Subset_{R''} \mu_S$.
   Take $\mu_S \in Dist(S)$ such that $\mu_P \Subset_{R''} \mu_S$ and choose $\mu' \in Dist(S')$ such that $\mu_S \Subset_{R'} \mu'$. Let $\delta'' : S_P \to (S \to [0,1])$ and $\delta' : S \to (S' \to [0,1])$ be the correspondence functions witnessing $\mu_P \Subset^{\delta''}_{R''} \mu_S$ and $\mu_S \Subset^{\delta'}_{R'} \mu'$, respectively. Let $\delta : S_P \to (S' \to [0,1])$ such that $\delta(s)(t) = \sum_{r \in S} \delta''(s)(r)\delta'(r)(t)$. We prove that $\mu_P \Subset^{\delta}_{\mathcal{R}} \mu'$:
   (a) Let $s \in S_P$ such that $\mu_P(s) > 0$. We have

$$\begin{aligned}\sum_{t \in S'} \delta(s)(t) &= \sum_{t \in S'} \sum_{r \in S} \delta''(s)(r)\delta'(r)(t) \\ &= \left(\sum_{r \in S} \delta''(s)(r)\right)\left(\sum_{t \in S'} \delta'(r)(t)\right) = 1.\end{aligned}$$

   Thus $\delta(s)$ defines a distribution on S'.
   (b) Let $t \in S'$. We have

$$\begin{aligned}\sum_{s \in S_P} \mu_P(s)\delta(s)(t) &= \sum_{s \in S_P} \mu_P(s) \sum_{r \in S} \delta''(s)(r)\delta'(r)(t) \\ &= \sum_{r \in S} \delta'(r)(t) \sum_{s \in S_P} \mu_P(s)\delta''(s)(r) \\ &= \sum_{r \in S} \delta'(r)(t)\mu_S(r) = \mu'(t).\end{aligned}$$

   (c) Let $s \in S_P$ and $t \in S'$ such that $\delta(s)(t) > 0$. By definition of δ, there exists $r \in S$ such that $\delta''(s)(r) > 0$ and $\delta'(r)(t) > 0$. By definition of δ' and δ'', we thus have $s \,\mathcal{R}''\, r$ and $r \,\mathcal{R}'\, t$. By definition of $\mathcal{R}$, we thus have $s \,\mathcal{R}\, t$.
   Thus there exists $\mu_P \in Dist(S_P)$ such that $L_P(u, a, \mu_P) = \top$ and there exists $\mu' \in Sat(\varphi')$ such that $\mu_P \Subset_{\mathcal{R}} \mu'$.

2. Let $a \in A$ and $\mu_P \in Dist(S_P)$ such that $L_P(u,a,\mu) \neq \bot$. By $\mathcal{R}''$, there exists $\varphi \in C(S)$ such that $L(v,a,\varphi) \neq \bot$ and $\exists \mu_S \in Sat(\varphi)$ such that $\mu_P \Subset_{R''} \mu_S$. Moreover, by $\mathcal{R}'$, we have that for all $\mu \in Sat(\varphi)$, there exists $\varphi' \in C(S')$ such that $L'(w,a,\varphi') \neq \bot$ and $\exists \mu' \in Sat(\varphi')$ such that $\mu \Subset_{R'} \mu'$.
   Choose $\mu_S \in Dist(S)$ such that $\mu_P \Subset_{R''} \mu_S$ and choose $\varphi' \in Dist(S')$ such that $L'(w,a,\varphi') \geq ?$ and there exists $\mu' \in Sat(\varphi')$ with $\mu_S \Subset_{R'} \mu'$. Let $\delta'' : S_P \to (S \to [0,1])$ and $\delta' : S \to (S' \to [0,1])$ be the correspondence functions witnessing $\mu_P \Subset^{\delta''}_{R''} \mu_S$ and $\mu_S \Subset^{\delta'}_{R'} \mu'$ respectively. Let $\delta : S_P \to (S' \to [0,1])$ such that $\delta(s)(t) = \sum_{r \in S} \delta''(s)(r)\delta'(r)(t)$. Using the same reasoning as above, we deduce that $\mu_P \Subset^{\delta}_{\mathcal{R}} \mu'$.
3. Since $u \,\mathcal{R}''\, v$, we have that $V_P(u) \in V(v)$. Moreover, since $v \,\mathcal{R}'\, w$, we have that $V(v) \subseteq V'(w)$. As a consequence, $V_P(u) \in V'(w)$.

Since $s_0^P \,\mathcal{R}''\, s_0$ and $s_0 \,\mathcal{R}'\, s_0'$, we have that $s_0^P \,\mathcal{R}\, s_0'$, and we conclude that $\mathcal{R}$ is a satisfaction relation. Therefore $P \in [\![N']\!]$, and $N \preceq_T N'$.

Appendix B. Details for Section 3.2

We first give an equivalent and constructive version of the definition for probabilistic bisimulation. In order to produce constructive results, we will use this definition throughout the section instead of Definition 18.

Definition 46 (Probabilistic Bisimulation)**.** *Let $P = (S, A, L, AP, V, s_0)$ and $P' = (S', A, L', AP, V', s_0')$ be PAs with no unreachable states. We say that $\mathcal{R} \subseteq S \times S'$ is a probabilistic bisimulation relation if and only if the following conditions hold:*

- *There exists $n \in \mathbb{N}$ and partitions $(S_1, \ldots, S_n)$ and $(S_1', \ldots, S_n')$ of S and S', respectively, such that*
  - *for all $i \in \{1, \ldots, n\}$, and for all $s_1 \in S_i$ and $s_2 \in S_i'$, it holds that $(s_1, s_2) \in \mathcal{R}$, and*
  - *for all $i \in \{1, \ldots, n\}$ and for all $j \in \{1, \ldots, n\}$ such that $i \neq j$ and for all $s_1 \in S_i$ and $s_2 \in S_j'$ it holds that $(s_1, s_2) \notin \mathcal{R}$.*
- *Whenever $(s, s') \in \mathcal{R}$,*
  - *$V(s) = V'(s')$, and*
  - *for all $a \in A$, there exists $\mu \in Dist(S)$ such that $L(s,a,\mu) = \top$ if and only if there exists $\mu' \in Dist(S')$ such that $L'(s',a,\mu') = \top$ such that $\forall i \in \{1, \ldots, n\}, \sum_{s_1 \in S_i} \mu(s_1) = \sum_{s_2 \in S_i'} \mu'(s_2)$.*

P and P' are probabilistically bisimilar, written $P \simeq P'$, if and only if there exists a probabilistic bisimulation relation such that $s_0 \,\mathcal{R}\, s_0'$.

As expected, the lifting $\widetilde{P}$ of P yields a specification that P satisfies. This is formalized in the following lemma.

Lemma 47. *Given a PA P, it holds that $P \models \widetilde{P}$.*

Proof. Let $P = (S, A, L, AP, V, s_0)$ be a PA and let $\widetilde{P} = (S, A, \tilde{L}, AP, \tilde{V}, s_0)$ be its lifting. Let $\mathcal{R} \subseteq S \times S$ be the identity relation on S. We prove that $\mathcal{R}$ is a satisfaction relation such that $P \models \widetilde{P}$. Let $s \in S$. We show that $\mathcal{R}$ satisfies the axioms of a satisfaction relation.

- Let $a \in A$ and $\varphi \in C(S)$ such that $\widetilde{L}(s,a,\varphi) = \top$. By construction of $\widetilde{P}$, there exists $\mu \in Dist(S)$ such that $Sat(\varphi) = \{\mu\}$ and $L(s,a,\mu) = \top$. By construction, we thus have $\mu \Subset_{\mathcal{R}} \mu$.
- Let $a \in A$ and $\mu \in Dist(S)$ such that $L(s,a,\mu) = \top$. By construction of $\widetilde{P}$, there exists $\varphi \in C(S)$ such that $\widetilde{L}(s,a,\varphi) = \top$, with $Sat(\varphi) = \{\mu\}$. Again, by construction, we have $\mu \Subset_{\mathcal{R}} \mu$.
- By construction $V(s) \in \{V(s)\} = \widetilde{V}(s)$.

Since $s_0 \,\mathcal{R}\, s_0$, we conclude that $P \models \widetilde{P}$. □

Appendix B.1. Detailed proof for Theorem 20

The proof of the theorem is preceded by the following lemma.

Lemma 48. *Let $P = (S, A, L, AP, V, s_0)$ and $P' = (S', A, L', AP, V', s'_0)$ be PAs with no unreachable states such that $P \models \widetilde{P'}$ with a satisfaction relation $\mathcal{R}$. There exists $n > 0$ and partitions $S_1, \ldots S_n$ of S and $S'_1, \ldots, S'_n$ of S' such that, for all $i \in \{1, \ldots, n\}$, $s \in S_i$ and $s' \in S'_i$, either*

- *$s \,\mathcal{R}\, s'$ or*
- *there exists $k \in \mathbb{N}$, $s_1, \ldots, s_k \in S_i$ and $s'_1, \ldots, s'_k \in S'_i$ such that*

$$\begin{array}{rll} s \,\mathcal{R}\, s'_1 & s_1 \,\mathcal{R}\, s'_1 & \wedge \\ s_1 \,\mathcal{R}\, s'_2 & s_2 \,\mathcal{R}\, s'_2 & \wedge \\ & & \vdots \\ & s_k \,\mathcal{R}\, s' & \end{array}$$

Let $P = (S, A, L, AP, V, s_0)$ and $P' = (S', A, L', AP, V', s'_0)$ be PAs with no unreachable states such that $P \models \widetilde{P'}$ by a satisfaction relation $\mathcal{R}$. We prove that there exists $n > 0$ and partitions $S_1, \ldots S_n$ of S and $S'_1, \ldots, S'_n$ of S' such that, for all $i \in \{1, \ldots, n\}$, $s \in S_i$ and $s' \in S'_i$, either

- $s \,\mathcal{R}\, s'$ or
- there exists $k \in \mathbb{N}$, $s_1, \ldots, s_k \in S_i$ and $s'_1, \ldots, s'_k \in S'_i$ such that

$$\begin{array}{rll} s \,\mathcal{R}\, s'_1 & s_1 \,\mathcal{R}\, s'_1 & \wedge \\ s_1 \,\mathcal{R}\, s'_2 & s_2 \,\mathcal{R}\, s'_2 & \wedge \\ & & \vdots \\ & s_k \,\mathcal{R}\, s' & \end{array}$$

Proof. Let $P = (S, A, L, AP, V, s_0)$ and $P' = (S', A, L', AP, V', s'_0)$ be PAs with no unreachable states such that $P \models \widetilde{P'}$ by satisfaction relation $\mathcal{R}$.

We first propose the following procedure in order to build the partitions of S and S', and then prove the lemma by induction on this procedure.

Let S be partitioned into singleton sets $T_1 = \{s_1\}, \ldots, T_{|S|} = \{s_{|S|}\}$ and let $U_1, \cdots, U_{|S|}$ be the partition of S' such that $\forall 1 \leq i \leq |S| : U_i = \{s' \in S' | s_i \,\mathcal{R}\, s'\}$. Since there are no unreachable states in P and P', it is obvious that $U = U_1 \cup \ldots \cup U_{|S|}$. The procedure is as follows:

- Let i be the smallest integer such that there exists $j > i$ such that $U_i \cap U_j \neq \emptyset$, if it exists.

For all $l < i$ and $i < l < j$, let $U'_l = U_l$ and $T'_l = T_l$;

Let $U'_i = U_i \cup U_j$ and $T'_i = T_i \cup T_j$;

For all $l \geq j$, let $U'_l = U_{l+1}$ and $T'_l = T_{l+1}$;

Repeat.

- If there is no such i, then stop.

Let $(S_1, \ldots, S_n)$ and $(S'_1, \ldots, S'_n)$ denote the partitions of S and S' upon termination.

Remark that, at all iterations of the above procedure, it trivially holds that

$$\forall l, U_l = \bigcup_{s \in T_l} \{s' \in S' \mid s \mathcal{R} s'\}.$$

We now prove the lemma using induction on the number of steps performed using the above procedure.

- Let $U_1^{(0)}, \ldots, U_k^{(0)}$ and $T_1^{(0)}, \ldots, T_k^{(0)}$ be the partitions in the initial state. By construction, for all $i \in \{1, \ldots, k\}$, if $s \in U_i^{(0)}$ and $s' \in T_i^{(0)}$, then $s \mathcal{R} s'$.
- Let $U_1^{(k)}, \ldots, U_l^{(k)}$ and $T_1^{(k)}, \ldots, T_l^{(k)}$ be the sets obtained after step k of the procedure and assume that the conclusion of the lemma holds after this step. Let i and j be the indexes used in step $k+1$ of the procedure. Let $U_1^{(k+1)}, \ldots, U_m^{(k+1)}$ and $T_1^{(k+1)}, \ldots, T_m^{(k+1)}$ be the partitions obtained after step $k+1$ of the procedure. Let $q \in \{1, \ldots, m\}$ and let $s \in T_q^{k+1}$ and $s' \in U_q^{k+1}$. If $q \neq i$ then the conclusions obviously hold.

  If $q = i$, then there are 3 cases

  1. If $s \in T_i^k$ and $s' \in U_i^k$ or $s \in T_j^k$ and $s' \in U_j^k$, then the conclusions hold by induction.
  2. If $s \in T_i^k$ and $s' \in U_j^k$, then by construction of i and j, we have that $U_i^k \cap U_j^k \neq \emptyset$. Thus, there must exist $s^{*\prime} \in U_i^k \cap U_j^k$ and $s_1^* \in T_j^k$ such that $s_1^* \mathcal{R} s^{*\prime}$. By the induction hypothesis, there exists $r, t \in \mathbb{N}$, $s_1^i, \ldots, s_r^i \in T_i^k$, $s_1^j, \ldots, s_t^j \in T_j^k$, $s_1^{i\prime}, \ldots, s_r^{i\prime} \in U_i^k$ and $s_1^{j\prime}, \ldots, s_t^{j\prime} \in U_j^k$, such that

$$\begin{array}{lll} s \mathcal{R} s_1^{i\prime} & s_1^i \mathcal{R} s_1^{i\prime} & \wedge \\ & \ldots & \\ s_r^i = \mathcal{R} s^{*\prime} & & \wedge \\ s_1^* \mathcal{R} s^{*\prime} & s_1^j \mathcal{R} s^{*\prime} & \wedge \\ & \ldots & \\ & s_t^j \mathcal{R} s' & \end{array}$$

     Since $U_i^{k+1} = U_i^k \cup U_j^k$ and $T_i^{k+1} = T_i^k \cup T_j^k$, the above construction gives that the lemma holds after step $k+1$ of the procedure.
  3. If $s \in T_j^k$ and $s' \in U_i^k$, a symmetric reasoning applies.

We conclude that the lemma holds for the partition obtained upon termination of the procedure.

□

We now give the detailed proof of Theorem 20. Let P and P' be PAs. We prove that $P \simeq P' \iff P \models \widetilde{P'}$.

Proof. We prove the two directions separately.

• $P \simeq P' \Rightarrow P \models \widetilde{P'}$: Let $P = (S, A, L, AP, V, s_0)$ and $P' = (S', A, L', AP, V', s'_0)$ be PAs such that $P \simeq P'$ with relation $\mathcal{R}_b$. Let $\widetilde{P'} = (S', A, \tilde{L'}, AP, \tilde{V'}, s'_0)$ be the lifting of P'. Let $S_1, \ldots, S_n$ and $S'_1, \ldots, S'_n$ be the partitions of S and S' respectively, according to $\mathcal{R}_b$. Let $\mathcal{R} \subseteq S \times S'$ be the relation such that $s \,\mathcal{R}\, s'$ iff $s \,\mathcal{R}_b\, s'$. We prove that $\mathcal{R}$ is a satisfaction relation such that $P \models \widetilde{P'}$.

Let $s \in S$ and $s' \in S'$ such that $s \,\mathcal{R}\, s'$. We show that $\mathcal{R}$ satisfies the axioms of a satisfaction relation.

1. Let $a \in A$ and $\varphi' \in C(S')$ such that $\widetilde{L'}(s', a, \varphi') = \top$. By construction of $\widetilde{P'}$, there exists $\mu' \in Dist(S')$ such that $L'(s', a, \mu') = \top$ and $Sat(\varphi') = \{\mu'\}$. Hence, by $\mathcal{R}_b$, there exists $\mu \in Dist(S)$ such that $L(s, a, \mu) = \top$ and for all $1 \leq i \leq n$, $\mu(S_i) = \mu'(S_i)$. We now prove that $\mu \Subset_{\mathcal{R}} \mu'$.
   Let $\delta : S \to (S' \to [0, 1])$ be a function defined as follows: Let $s_1 \in S$ and $1 \leq i \leq n$ such that $s_1 \in S_i$. Then for all $s'_1 \in S'$, let $\delta(s_1)(s'_1) = 0$ if $s'_1 \notin S'_i$ or $\mu(s_1) = 0$. Otherwise, let $\delta(s_1)(s'_1) = \frac{\mu'(s'_1)}{\mu'(S'_i)}$ (by $\mathcal{R}_b$, we know that $\mu'(S'_i) = \mu(S_i) > 0$).
   (a) Let $s_1 \in S$ and $1 \leq i \leq n$ such that $s_1 \in S_i$ and $\mu(s_1) > 0$. By construction, we have the following:
   $$\begin{aligned}\sum_{s'_1 \in S'} \delta(s_1)(s'_1) &= \sum_{s'_1 \in S'_i} \delta(s_1)(s'_1) \\ &= \sum_{s'_1 \in S'_i} \frac{\mu'(s'_1)}{\mu'(S'_i)} = 1.\end{aligned}$$
   (b) Let $s'_1 \in S'$ and $1 \leq i \leq n$ such that $s'_1 \in S'_i$. If $\mu'(S'_i) = 0$, then $\mu(S_i) = 0$ by $\mathcal{R}_b$ and by construction, $\sum_{s_1 \in S} \mu(s_1)\delta(s_1)(s'_1) = 0 = \mu'(s'_1)$. Otherwise, we have the following:
   $$\begin{aligned}\sum_{s_1 \in S} \mu(s_1)\delta(s_1)(s'_1) &= \sum_{s_1 \in S_i} \mu(s_1)\delta(s_1)(s'_1) \\ &= \sum_{s_1 \in S_i} \mu(s_1)\frac{\mu'(s'_1)}{\mu'(S'_i)} \\ &= \frac{\mu'(s'_1)}{\mu'(S'_i)} \sum_{s_1 \in S_i} \mu(s_1) \\ &= \mu'(s'_1)\frac{\mu(S_i)}{\mu'(S'_i)} = \mu'(s'_1).\end{aligned}$$
   (c) Let $s_1 \in S$ and $s'_1 \in S'$ such that $\delta(s_1)(s'_1) > 0$. Then by construction there exists $1 \leq i \leq n$ such that $s_1 \in S_i$ and $s'_1 \in S'_i$. Hence $s_1 \,\mathcal{R}_b\, s'_1$, and thus $s_1 \,\mathcal{R}\, s'_1$.
   Consequently, we have $\mu \Subset_{\mathcal{R}} \mu'$.
2. Let $a \in A$ and $\mu \in Dist(S)$ such that $L(s, a, \mu) = \top$. Then, by $\mathcal{R}_b$, there exists $\mu' \in Dist(S')$ such that $L'(s', a, \mu') = \top$. By construction of $\widetilde{P'}$, there exists $\varphi' \in C(S)$ such that $\widetilde{L'}(s', a, \varphi') = \top$ and $Sat(\varphi') = \{\mu'\}$.
   We now show that $\mu \Subset_R \mu'$. Define the correspondence function $\delta : S \to (S' \to [0, 1])$ as follows: let $s_1 \in S$ and let $1 \leq i \leq n$ such that $s_1 \in S_i$. Define $\delta(s_1)(s'_1) = \frac{\mu'(s'_1)}{\sum_{s' \in S'_i} \mu'(s')}$, if $s'_1 \in S'_i$, and 0 otherwise.

(a) Let $s_1 \in S$ and assume that $s_1 \in S_i$ for some $i \in \{1, \ldots, n\}$.

$$\begin{aligned}\sum_{s_1' \in S'} \delta(s_1)(s_1') &= \sum_{s_1' \in S_i'} \delta(s_1)(s_1') \\ &= \sum_{s_1' \in S_i'} \frac{\mu'(s_1')}{\sum_{s' \in S_i'} \mu'(s')} = 1.\end{aligned}$$

(b) Let $s_1' \in S'$ and assume that $s_1' \in S_i'$ for some $i \in \{1, \ldots, n\}$.

$$\begin{aligned}\sum_{s_1 \in S} \mu(s_1)\delta(s_1)(s_1') &= \sum_{s_1 \in S_i} \mu(s_1)\delta(s_1)(s_1') \\ &= \sum_{s_1 \in S_i} \mu(s_1) \frac{\mu'(s_1')}{\sum_{s' \in S_i'} \mu'(s')} \\ &= \frac{\mu'(s_1')}{\sum_{s' \in S_i'} \mu'(s')} \sum_{s_1 \in S_i} \mu(s_1) \\ &= \mu'(s_1'),\end{aligned}$$

since by probabilistic bisimulation $\sum_{s_1 \in S_i} \mu(s_1) = \sum_{s' \in S_i'} \mu'(s')$.

(c) Assume that $\delta(s_1)(s_1') > 0$. Then $s_1 \in S_i$ and $s_1' \in S_i'$ for some $i \in \{1, \ldots, n\}$, and hence $s_1 \mathcal{R}_b s_1'$. Then $s_1 \mathcal{R} s_1'$.

3. By $\mathcal{R}_b$, we have $V(s) = V'(s')$, and therefore $V(s) \in \{V'(s')\} = \widetilde{V'}(s')$.

Finally, $\mathcal{R}$ is a satisfaction relation such that $s_0 \mathcal{R} s_0'$, thus $P \models \widetilde{P'}$.

• $P \simeq P' \Leftarrow P \models \widetilde{P'}$: Let $P = (S, A, L, AP, V, s_0)$ and $P' = (S', A, L', AP, V', s_0')$ be PAs and let $\widetilde{P'} = (S', A, \tilde{L'}, AP, \tilde{V'}, s_0')$ be the lifting of P'. Suppose that $P \models \widetilde{P'}$. We prove that $P \simeq P'$.

Let $(S_1, \ldots, S_n)$ and $(S_1', \ldots, S_n')$ be the partitions of S and S' given by Lemma 48. Let $\mathcal{R}_b \subseteq S \times S'$ be the relation such that $s \mathcal{R}_b s'$ if and only if $\exists i \in \{1, \ldots, n\} : s \in S_i \wedge s' \in S_i'$. We prove that $\mathcal{R}_b$ is a probabilistic bisimulation relation. Consider the partitions above. It holds by construction that

- for all $i \in \{1, \ldots, n\}$, and for all $s_1 \in S_i$ and $s_2 \in S_i'$, it holds that $(s_1, s_2) \in \mathcal{R}$, and
- for all $i \in \{1, \ldots, n\}$ and for all $j \in \{1, \ldots, n\}$ such that $i \neq j$ and for all $s_1 \in S_i$ and $s_2 \in S_j'$ it holds that $(s_1, s_2) \notin \mathcal{R}$.

Let $s \in S$ and $s' \in S'$ such that $s \mathcal{R}_b s'$. Remark that, by Lemma 48, either $s \mathcal{R} s'$ or there exists $k \in \mathbb{N}$, $s_1, \ldots, s_k \in S_i$ and $s_1', \ldots, s_k' \in S_i'$ such that

$$\begin{array}{lll} s \mathcal{R} s_1' & s_1 \mathcal{R} s_1' & \wedge \\ s_1 \mathcal{R} s_2' & s_2 \mathcal{R} s_2' & \wedge \\ & & \vdots \\ & s_k \mathcal{R} s' & \end{array}$$

- By Lemma 48 and $\mathcal{R}$, we have $V(s) = V(s')$.
- Let $a \in A$ and $\mu \in Dist(S)$ such that $L(s, a, \mu) = \top$.

– If $(s, s') \in \mathcal{R}$, then by $\mathcal{R}$ there exists $\varphi' \in C(S')$ such that $\widetilde{L'}(s', a, \varphi') = \top$ and $\exists \mu' \in Sat(\varphi') : \mu \Subset_{\mathcal{R}} \mu'$; let δ be the witnessing correspondence function. By construction of $\widetilde{P'}$, we have that $Sat(\varphi') = \{\mu'\}$ and $L'(s', a, \mu') = \top$. By construction of the partitions it holds, for all $j \in \{1, \ldots, n\}$ and all $s_1 \in S_j$, that $\delta(s_1)(s'_1) = 0$ if $s'_1 \notin S'_j$. As a consequence, if $s_1 \in S_j$ and $\mu(s_1) > 0$, then it holds by $\mathcal{R}$ that $\sum_{s'_1 \in S'_j} \delta(s_1)(s'_1) = 1$. Let $j \in \{1, \ldots, n\}$.

$$\begin{aligned}
\sum_{s'_1 \in S'_j} \mu'(s'_1) &= \sum_{s'_1 \in S'_j} \sum_{s_1 \in S} \mu(s_1)\delta(s_1)(s'_1) \\
&= \sum_{s'_1 \in S'_j} \sum_{s_1 \in S_j} \mu(s_1)\delta(s_1)(s'_1) \\
&= \sum_{s_1 \in S_j} \mu(s_1) \sum_{s'_1 \in S'_j} \delta(s_1)(s'_1) \\
&= \sum_{s_1 \in S_j} \mu(s_1).
\end{aligned}$$

We conclude that s and s' are indeed probabilistically bisimilar.

– If $(s, s') \notin \mathcal{R}$, then there exists $k \in \mathbb{N}$, $s_1, \ldots, s_k \in S_i$ and $s'_1, \ldots, s'_k \in S'_i$ such that

$$\begin{array}{cc}
s \,\mathcal{R}\, s'_1 & s_1 \,\mathcal{R}\, s'_1 \quad \wedge \\
s_1 \,\mathcal{R}\, s'_2 & s_2 \,\mathcal{R}\, s'_2 \quad \wedge \\
 & \vdots \\
 & s_k \,\mathcal{R}\, s'
\end{array}$$

As above, for states $v \in S_i$ and $v' \in S'_i$ such that $v \,\mathcal{R}\, v'$ we have that, for all $\mu_v \in Dist(S)$ such that $L(v, a, \mu_v) = \top$, there exists $\mu'_v \in Dist(S')$ such that $L'(v', a, \mu'_v) = \top$ and all for all $j \in \{1, \ldots, n\}$, $\sum_{s_1 \in S_j} \mu_v(s_1) = \sum_{s'_1 \in S'_j} \mu'_v(s'_1)$.

Moreover, for all $\mu'_v \in Dist(S')$ such that $L'(s', a, \mu'_v) = \top$, we have that $\widetilde{L'}(v', a, \varphi'_v) = \top$ with $Sat(\varphi'_v) = \{\mu'\}$. Thus, by $\mathcal{R}$, there exists $\mu_v \in Dist(S)$ such that $L(v, a, \mu_v) = \top$ and $\mu_v \Subset \mu'_v$. As above, we obtain that for all $j \in \{1, \ldots, n\}$, $\sum_{s_1 \in S_j} \mu_v(s_1) = \sum_{s'_1 \in S'_j} \mu'_v(s'_1)$.

By transitivity, we conclude that there exists $\mu' \in Dist(S')$ such that $L'(s', a, \mu') = \top$ and all for all $j \in \{1, \ldots, n\}$, $\sum_{s_1 \in S_j} \mu(s_1) = \sum_{s'_1 \in S'_j} \mu'(s'_1)$.

- Let $a \in A$ and $\mu' \in Dist(S')$ such that $L'(s', a, \mu') = \top$. Then, by construction of $\widetilde{P'}$, we have that $\widetilde{L'}(s', a, \varphi') = \top$ with $Sat(\varphi') = \{\mu'\}$.

  – If $(s, s') \in \mathcal{R}$, then by $\mathcal{R}$ there exists $\mu \in Dist(S)$ such that $L(s, a, \mu) = \top$ and $\mu \Subset_{\mathcal{R}} \mu'$. As above, we can conclude that for all $j \in \{1, \ldots, n\}$, we have $\sum_{s_1 \in S_j} \mu(s_1) = \sum_{s'_1 \in S'_j} \mu'(s'_1)$.

  – If $(s, s') \notin \mathcal{R}$, there exists $k \in \mathbb{N}$, $s_1, \ldots, s_k \in S_i$ and $s'_1, \ldots, s'_k \in S'_i$ such

that

$$\begin{array}{lll} s\,\mathcal{R}\,s'_1 & s_1\,\mathcal{R}\,s'_1 & \wedge \\ s_1\,\mathcal{R}\,s'_2 & s_2\,\mathcal{R}\,s'_2 & \wedge \\ & & \vdots \\ & s_k\,\mathcal{R}\,s' & \end{array}$$

As above, by transitivity, we prove that there exists $\mu \in Dist(S)$ such that $L(s,a,\mu) = \top$ and for all $j \in \{1,\ldots,n\}$, we have $\sum_{s_1 \in S_j} \mu(s_1) = \sum_{s'_1 \in S'_j} \mu'(s'_1)$.

We conclude that $\mathcal{R}_b$ is a probabilistic bisimulation relation, thus $P \simeq P'$. □

Appendix B.2. Detailed proof for Lemma 21

Let P be a PA and let N be an APA. We prove the following: $P \models N \iff \widetilde{P} \preceq N$.

Proof. We prove the two directions separately.

• $P \models N \Rightarrow \widetilde{P} \preceq N$: Let $P = (S, A, L, AP, V, s_0)$ be a PA and let $N = (S', A, L', AP, V', s'_0)$ be an APA such that $P \models N$ with relation $\mathcal{R}_s$. Let $\widetilde{P} = (S, A, \tilde{L}, AP, \tilde{V}, s_0)$ be the lifting of P. Let $\mathcal{R} \subseteq S \times S'$ be the relation such that $s\,\mathcal{R}\,s'$ iff $s\,\mathcal{R}_s\,s'$. We prove that $\mathcal{R}$ is a refinement relation such that $\widetilde{P} \preceq N$.

Let $s \in S$ and $s' \in S'$ such that $s\,\mathcal{R}\,s'$. We show that $\mathcal{R}$ satisfies the axioms of a weak refinement relation.

1. Let $a \in A$ and $\varphi' \in C(S')$ such that $L'(s', a, \varphi') = \top$. By $\mathcal{R}_s$, there exists $\mu \in Dist(S)$ and $\mu' \in Sat(\varphi')$ such that $L(s,a,\mu) = \top$ and $\mu \Subset_{\mathcal{R}_s} \mu'$. By construction of $\widetilde{P}$, there exists $\varphi \in C(S)$ such that $\widetilde{L}(s,a,\varphi) = \top$ and $Sat(\varphi) = \{\mu\}$. Let δ_s be the correspondence function witnessing $\mu \Subset^{\delta_s}_{\mathcal{R}_s} \mu'$. Since $\mathcal{R} = \mathcal{R}_s$, it also holds that $\mu \Subset^{\delta_s}_{\mathcal{R}} \mu'$. Thus there exists $\varphi \in C(S)$ such that $L(s,a,\varphi = \top)$ and for all $\mu \in Sat(\varphi)$, there exists $\mu' \in Sat(\varphi')$ such that $\mu \Subset_{\mathcal{R}} \mu'$.
2. Let $a \in A$ and $\varphi \in C(S)$ such that $\widetilde{L}(s,a,\varphi) \neq \bot$. By construction of $\widetilde{P}$, there exists $\mu \in Dist(S)$ such that $L(s,a,\mu) = \top$ and $Sat(\varphi) = \{\mu\}$. By $\mathcal{R}_s$, there exists $\varphi' \in C(S')$ such that $L'(s', a, \varphi') \neq \bot$ and $\mu' \in Sat(\varphi')$ such that $\mu \Subset_{\mathcal{R}_s} \mu'$. As above, it also holds that $\mu \Subset_{\mathcal{R}} \mu'$. Thus there exists $\varphi' \in C(S')$ such that $L'(s', a, \varphi') \geq ?$ and for all $\mu \in Sat(\varphi)$, there exists $\mu' \in Sat(\varphi')$ such that $\mu \Subset_{\mathcal{R}} \mu'$.
3. Since $\widetilde{V}(s) = \{V(s)\}$ and $V(s) \in V'(s')$ by $\mathcal{R}_s$, it holds that $\widetilde{V}(s) \subseteq V'(s')$.

Thus $\mathcal{R}$ is a weak refinement relation. Moreover, by construction, $s_0\,\mathcal{R}\,s'_0$. Thus we conclude that $\widetilde{P} \preceq N$.

• $P \models N \Leftarrow \widetilde{P} \preceq N$: Let $P = (S, A, L, AP, V, s_0)$ be a PA, let $\widetilde{P} = (S, A, \tilde{L}, AP, \tilde{V}, s_0)$ be the lifting of P and let $N = (S', A, L', AP, V', s'_0)$ be an APA such that $\widetilde{P} \preceq N$ with relation $\mathcal{R}_r$. Let $\mathcal{R} \subseteq S \times S'$ be the relation such that $s\,\mathcal{R}\,s'$ iff $s\,\mathcal{R}_r\,s'$. We prove that $\mathcal{R}$ is a satisfaction relation such that $P \models N$.

Let $s \in S$ and $s' \in S'$ such that $s\,\mathcal{R}\,s'$. We show that $\mathcal{R}$ satisfies the axioms of a satisfaction relation.

1. Let $a \in A$ and $\varphi' \in C(S')$ such that $L'(s', a, \varphi') = \top$. By $\mathcal{R}_r$, there exists $\varphi \in C(S)$ such that $\widetilde{L}(s,a,\varphi) = \top$ and for all $\mu \in Sat(\varphi)$, there exists $\mu' \in Sat(\varphi')$ such that $\mu \Subset_{\mathcal{R}_r} \mu'$. By construction of $\widetilde{P}$, there exists $\mu \in Dist(S)$ such that

$L(s,a,\mu) = \top$ and $Sat(\varphi) = \{\mu\}$. Consider the distribution $\mu' \in Sat(\varphi')$ such that $\mu \Subset_{\mathcal{R}_r} \mu'$ given by $\mathcal{R}_r$. Since $\mathcal{R}_r = \mathcal{R}$, it also holds that $\mu \Subset_{\mathcal{R}} \mu'$. Thus there exists $\mu \in Dist(S)$ such that $L(s,a,\mu) = \top$ and there exists $\mu' \in Sat(\varphi')$ such that $\mu \Subset_{\mathcal{R}} \mu'$.

2. Let $a \in A$ and $\mu \in Dist(S)$ such that $L(s,a,\mu) = \top$. By construction of $\widetilde{P}$, there exists $\varphi \in C(S)$ such that $\widetilde{L}(s,a,\varphi) = \top$ and $Sat(\varphi) = \{\mu\}$. Thus, by $\mathcal{R}_r$, there exists $\varphi' \in C(S')$ such that $L'(s',a,\varphi') \neq \bot$ and $\mu' \in Sat(\varphi')$ such that $\mu \Subset_{\mathcal{R}_r} \mu'$. Since $\mathcal{R}_r = \mathcal{R}$, it also holds that $\mu \Subset_{\mathcal{R}} \mu'$. Thus there exists $\varphi' \in C(S')$ such that $L'(s',a,\varphi') \geq ?$ and $\mu' \in Sat(\varphi')$ such that $\mu \Subset_{\mathcal{R}} \mu'$.
3. Since $\widetilde{V}(s) = \{V(s)\}$ and $\widetilde{V}(s) \subseteq V'(s')$, it holds that $V(s) \in V'(s')$.

Thus $\mathcal{R}$ is a satisfaction relation. Moreover, by construction, $s_0 \,\mathcal{R}\, s'_0$. As a consequence, we conclude that $P \models N$.

□

Appendix C. Detailed proof for Lemma 24

We prove that, for any APA N and abstraction function α, it holds that $N \preceq_S \alpha(N)$.

Proof. Let $N = (S, A, L, AP, V, s_0)$ be an APA and let $\alpha : S \to S'$ be an abstraction function. Consider the state abstraction $\alpha(N) = (S', A, L', AP, V', \alpha(s_0))$. Let $\mathcal{R} \subseteq S \times S'$ be the relation such that $s \,\mathcal{R}\, s'$ iff $s' = \alpha(s)$. We prove that $\mathcal{R}$ is a strong refinement relation.

Let $s \in S$ and $s' \in S'$ such that $s \,\mathcal{R}\, s'$. By construction, we thus have $s \in \gamma(s')$. We show that $\mathcal{R}$ satisfies the axioms of a strong refinement relation.

1. Let $a \in A$ and $\varphi' \in C(S')$ such that $L'(s',a,\varphi') = \top$. This implies, by definition of abstraction, that there exists $\varphi \in C(S)$, such that $L(s,a,\varphi) = \top$ and

$$Sat(\varphi') = \alpha\left(\bigcup_{(s,\varphi^*) \in \gamma(s') \times C(S) : L(s,a,\varphi^*) = \top} Sat(\varphi^*)\right)$$

   Define $\delta : S \to (S' \to [0,1])$ such that $\delta(u)(v) = 1$ if $\alpha(u) = v$, and 0 otherwise. We now show that for all distribution $\mu \in Sat(\varphi)$, there exists $\mu' \in Sat(\varphi')$ such that $\mu \Subset^{\delta}_{\mathcal{R}} \mu'$.
   Let $\mu \in Sat(\varphi)$ and let $\mu' \in Dist(S')$ such that $\mu'(s'') = \alpha(\mu)(s'')$ for all $s'' \in S'$. Clearly, $\mu' \in Sat(\varphi')$.
   (a) Let $u \in S$ such that $\mu(u) > 0$. By construction, $\delta(u)$ is a distribution on S'.
   (b) Let $v \in S'$.

$$\begin{aligned}\sum_{u \in S} \mu(u)\delta(u)(v) &= \sum_{u \text{ st. } \alpha(u) = v} \mu(u) \\ &= \sum_{u \in \gamma(v)} \mu(u) = \alpha(\mu)(v) = \mu'(v),\end{aligned}$$

   (c) Let $u \in S$ and $v \in S'$ such that $\delta(u)(v) > 0$. By construction, we thus have $\alpha(u) = v$, and finally $u \,\mathcal{R}\, v$.

2. Let $a \in A$ and $\varphi \in C(S)$ such that $L(s,a,\varphi) \neq \bot$. By construction of $\alpha(N)$, then there are two cases. Either (1) there exists $\varphi' \in C(S')$ such that $L'(s',a,\varphi') =?$ and
$$Sat(\varphi') = \alpha\left(\bigcup_{(s,\varphi^*)\in\gamma(s')\times C(S):L(s,a,\varphi^*)\neq\bot} Sat(\varphi^*)\right)$$
or (2) there is no constraint φ'' such that $L'(s',a,\varphi'') =?$, which means that $L(s,a,\varphi) = \top$ and there exists $\varphi' \in C(S')$ such that $L'(s',a,\varphi') = \top$ and
$$Sat(\varphi') = \alpha\left(\bigcup_{(s,\varphi^*)\in\gamma(s')\times C(S):L(s,a,\varphi^*)=\top} Sat(\varphi^*)\right)$$
Let $\delta : S \to (S' \to [0,1])$ be the correspondence function defined as above.
Let $\mu \in Sat(\varphi)$ and consider $\mu' \in Dist(S')$ such that $\mu'(s'') = \alpha(\mu)(s'')$ for all $s'' \in S'$. Clearly, in both cases, we have $\mu' \in Sat(\varphi')$. Define $\delta : S \to (S' \to [0,1])$ as $\delta(u)(v) = 1$, if $\alpha(u) = v$, and 0 otherwise. We now show that $\mu \Subset^{\delta}_{\mathcal{R}} \mu'$.
   (a) Let $u \in S$ such that $\mu(u) > 0$. Clearly, $\delta(u)$ is a distribution on S'.
   (b) Let $v \in S'$.
$$\begin{aligned}\sum_{u\in S} \mu(u)\delta(u)(v) &= \sum_{u \text{ st. } \alpha(u)=v} \mu(u) \\ &= \sum_{u\in\gamma(v)} \mu(u) = \mu'(v),\end{aligned}$$
   by definition of an abstraction of a distribution.
   (c) Assume that $\delta(u)(v) > 0$. Then $\alpha(u) = v$, and $u \,\mathcal{R}\, v$.
3. By Definition 23, it is easy to see that $V(s) \subseteq V'(s')$.

By construction, we have $s_0 \,\mathcal{R}\, \alpha(s_0)$, so we conclude that $\mathcal{R}$ is a strong refinement relation and $N \preceq_S \alpha(N)$. □

Appendix D. Detailed proof for Lemma 26

We prove that, for any APA N, it holds that $N \preceq_S \chi(N)$.

Proof. Let $N = (S, A, L, AP, V, s_0)$ be an APA and let $\chi(N) = (S, A, L', AP, V, s_0)$ be the constraint-abstraction of N. Let $\mathcal{R} = S \times S$ be the identity relation. We prove that $\mathcal{R}$ is a strong refinement relation.

Let $s, s' \in S$ such that $s \,\mathcal{R}\, s'$. Notice that this is implies that $s = s'$. We show that $\mathcal{R}$ satisfies the axioms of a strong refinement relation.

1. Let $a \in A$ and $\varphi_I \in C(S)$ such that $L'(s',a,\varphi_I) = \top$. This implies, by Definition 25, that there exists $\varphi \in C(S)$, such that $L(s,a,\varphi) = \top$ and $Sat(\varphi_I) = \{\mu' \in Dist(S) | \bigwedge_{s'\in S} \mu'(s') \in I^{\varphi}_{s'}\}$ with $\{I^{\varphi}_{s'} | s' \in S\}$ the smallest closed intervals such that $\forall \mu \in Sat(\varphi) : \bigwedge_{s'\in S} \mu(s') \in I^{\varphi}_{s'}$.
   Let δ be the identity correspondence function.
   Let $\mu \in Sat(\varphi)$. By definition of φ_I, it is trivial that $\mu \in Sat(\varphi_I)$ and $\mu \Subset^{\delta}_{\mathcal{R}} \mu$.

2. Let $a \in A$ and $\varphi \in C(S)$ such that $L(s,a,\varphi) \geq ?$. This implies, by Definition 25, that there exists $\varphi_I \in C(S)$, such that $L(s',a,\varphi_I) = L(s,a,\varphi)$ and $Sat(\varphi_I) = \{\mu' \in Dist(S) | \bigwedge_{s' \in S} \mu'(s') \in I^{\varphi}_{s'}\}$ with $\{I^{\varphi}_{s'} | s' \in S\}$ the smallest closed intervals such that $\forall \mu \in Sat(\varphi) : \bigwedge_{s' \in S} \mu(s') \in I^{\varphi}_{s'}$.
   Let δ be the identity correspondence function.
   Let $\mu \in Sat(\varphi)$. Again, it is trivial that $\mu \in Sat(\varphi_I)$ and $\mu \Subset^{\delta}_{\mathcal{R}} \mu$.
3. By Definition 25, since $s = s'$, we have $V(s) \subseteq V(s')$.

By construction, as the initial states are equal, we have $s_0 \,\mathcal{R}\, s_0$, so we conclude that $\mathcal{R}$ is a strong refinement relation and $N \preceq_S \chi(N)$.

□

Appendix E. Detailed proof for Theorem 30

We prove that for or any APA N, it holds that $[\![N]\!] = [\![\beta(N)]\!]$, and $[\![N]\!] = [\![\beta^*(N)]\!]$.

Proof. Let $N = (S, A, L, AP, V, s_0)$ be an APA. Let T be the set of inconsistent states of N and let $\beta(N)$ be the corresponding APA using the pruning operator of Definition 29. The result is trivial if $\beta(N)$ is empty. Otherwise, suppose that $\beta(N) = (S', A, L', AP, V', s_0)$, and let $P = (Q, A, L_P, AP, V_P, q_0)$ be a PA. We prove that $P \models N \iff P \models \beta(N)$. If this holds, then, by applying β until a fixpoint is reached, it holds that $[\![N]\!] = [\![\beta^*(N)]\!]$.

• $P \models N \Rightarrow P \models \beta(N)$: Suppose that $P \models N$, and let $\mathcal{R} \subseteq Q \times S$ be the corresponding satisfaction relation. Define the relation $\mathcal{R}' \subseteq Q \times S'$ such that for all $s \in S'$, $q \,\mathcal{R}'\, s$ iff $q \,\mathcal{R}\, s$. We prove that $\mathcal{R}'$ is a satisfaction relation. Let $q \in Q$ and $s \in S'$ such that $q \,\mathcal{R}'\, s$. We show that $\mathcal{R}'$ satisfies the axioms of a satisfaction relation.

1. Let $a \in A$ and $\varphi \in C(S')$ such that $L'(s,a,\varphi) = \top$. By definition of L', we have that $\overline{\varphi}^{s,a} \neq \emptyset$ and $\sqcup_{\overline{\varphi} \in \overline{\varphi}^{s,a}} L(s,a,\overline{\varphi}) = \top$. As a consequence, there exists $\overline{\varphi} \in C(S)$ such that $L(s,a,\overline{\varphi}) = T$ and $\mu \in Sat(\varphi)$ iff there exists $\overline{\mu} \in Sat(\overline{\varphi})$ such that $\overline{\mu}(s') = \mu(s')$ for all $s' \in S'$ and $\overline{\mu}(t) = 0$ for all $t \in T$.
   By $\mathcal{R}$, there exists $\varrho \in Dist(Q)$ such that $L_P(q,a,\varrho) = \top$ and there exists $\overline{\mu} \in Sat(\overline{\varphi})$ such that $\varrho \Subset_{\mathcal{R}} \overline{\mu}$. Let $s' \in S$ and suppose that $\overline{\mu}(s') > 0$. Let δ be the correspondence function such that $\varrho \Subset^{\delta}_{\mathcal{R}} \overline{\mu}$. By definition, there must exist $q' \in Q$ such that $\varrho(q') > 0$ and $\delta(q')(s') > 0$. By the definition of $\mathcal{R}$, this means that s' is not inconsistent. As a consequence, for all $t \in T$, we have $\overline{\mu}(t) = 0$ (1). Moreover, $\delta(q')(s') > 0$ also implies that s' is consistent. Thus, for all $q' \in Q$ and $t \in T$, we have that $\delta(q')(t) = 0$ (2).
   Let $\mu \in Dist(S')$ such that for all $s' \in S'$, $\mu(s') = \overline{\mu}(s')$. By (1), μ is indeed a distribution. Moreover, we have by construction that $\mu \in Sat(\varphi)$. Let $\delta' : Q \to (S' \to [0,1])$ such that for all $q' \in Q$ and $s' \in S$, $\delta'(q')(s') = \delta(q')(s')$. By (2), we have that δ' is a correspondence function, and
   (a) For all $q' \in Q$, if $\varrho(q') > 0$, then, by $\mathcal{R}$, $\delta(q')$ is a distribution on S. Thus, by (2), δ' is a distribution on S'.
   (b) For all $s' \in S'$,

$$\begin{aligned}\sum_{q' \in Q} \varrho(q')\delta'(q')(s') &= \sum_{q' \in Q} \varrho(q')\delta(q')(s') \\ &= \overline{\mu}(s') = \mu(s').\end{aligned}$$

(c) Whenever $\delta'(s')(q') > 0$, we have by definition $\delta(q')(s') > 0$. Thus, by $\mathcal{R}$, $q' \mathcal{R} s'$, and finally $q' \mathcal{R}' s'$.

Finally, we have that $\varrho \Subset^{\delta'}_{\mathcal{R}'} \mu$.

2. Let $a \in A$ and $\varrho \in Dist(Q)$ such that $L_P(q, a, \varrho) = \top$. By $\mathcal{R}$, there exists $\overline{\varphi} \in C(S)$ and $\overline{\mu} \in Sat(\overline{\varphi})$ such that $L(s, a, \overline{\varphi}) \neq \bot$ and $\varrho \Subset_{\mathcal{R}} \overline{\mu}$. Let $\varphi \in C(S')$ be the constraint such that $\mu^* \in Sat(\varphi)$ iff there exists $\mu^{*\prime} \in Sat(\overline{\varphi})$ such that, for all $s' \in S'$, $\mu^*(s') = \mu^*(s')$ and for all $t \in T$, $\mu^*(t) = 0$.

Let δ be the associated correspondence function. Let $s' \in S$ and suppose that $\overline{\mu}(s') > 0$. By definition, there must exist $q' \in Q$ such that $\varrho(q') > 0$ and $\delta(q')(s') > 0$. By the definition of $\mathcal{R}$, this means that s' is not inconsistent. As a consequence, for all $t \in T$, we have $\overline{\mu}(t) = 0$ (1). Moreover, $\delta(q')(s') > 0$ also implies that s' is consistent. Thus, for all $q' \in Q$ and $t \in T$, we have that $\delta(q')(t) = 0$ (2).

Let $\varphi \in C(S')$ such that $\mu \in Sat(\varphi)$ iff there exists $\mu' \in Sat(\overline{\varphi})$ such that, for all $s' \in S'$, $\mu(s') = \mu'(s')$ and for all $t \in T$, $\mu'(t) = 0$. By construction, we have $\overline{\varphi} \in \overline{\varphi}^{s,a}$. Thus, $L'(s, a, \varphi) \neq \bot$.

Moreover, let $\mu \in Dist(S')$ be the distribution such that for all $s' \in S'$, $\mu(s') = \overline{\mu}(s')$. By (1), μ is indeed a distribution. By construction, we have that $\mu \in Sat(\varphi)$. Let $\delta' : Q \to (S' \to [0, 1])$ such that for all $q' \in Q$ and $s' \in S$, $\delta'(q')(s') = \delta(q')(s')$. By (2), we have that δ' is a correspondence function, and

(a) For all $q' \in Q$, if $\varrho(q') > 0$, then, by $\mathcal{R}$, $\delta(q')$ is a distribution on S. Thus, by (2), δ' is a distribution on S'.

(b) For all $s' \in S'$,

$$\begin{aligned} \sum_{q' \in Q} \varrho(q')\delta'(q')(s') &= \sum_{q' \in Q} \varrho(q')\delta(q')(s') \\ &= \overline{\mu}(s') = \mu(s'). \end{aligned}$$

(c) Whenever $\delta'(s')(q') > 0$, we have by definition $\delta(q')(s') > 0$. Thus, by $\mathcal{R}$, $q' \mathcal{R} s'$, and finally $q' \mathcal{R}' s'$.

Finally, we have that $\varrho \Subset^{\delta'}_{\mathcal{R}'} \mu$.

3. By $\mathcal{R}$, we have that $V(q) \in V(s') = V'(s')$.

Finally, $\mathcal{R}'$ is a satisfaction relation. Moreover, we have by definition that $q_0 \mathcal{R}' s_0$, thus $P \models \beta(N)$.

• $P \models N \Leftarrow P \models \beta(N)$: Suppose that $P \models \beta(N)$, and let $\mathcal{R}' \subseteq Q \times S'$ be the corresponding satisfaction relation. Define $\mathcal{R} \subseteq Q \times S$ such that for all $q \in Q$ and $s \in S$, $q \mathcal{R} s$ iff $s \in S'$ and $q \mathcal{R}' s'$. By construction, $\mathcal{R}$ is a satisfaction relation and $q_0 \mathcal{R} s_0$. Thus $P \models N$.

□

Appendix F. Detailed proof for Theorem 32

Let N_1, N_2, and N_3 be consistent APAs sharing action and atomic proposition sets. We prove that

- $\beta^*(N_1 \wedge N_2) \preceq_W N_1$ and $\beta^*(N_1 \wedge N_2) \preceq_W N_2$.
- If $N_3 \preceq_W N_1$ and $N_3 \preceq_W N_2$, then $N_3 \preceq_W \beta^*(N_1 \wedge N_2)$.

Proof. Let $N_1 = (S_1, A, L_1, AP, V_1, s_0)$ and $N_2 = (S_2, A, L_2, AP, V_2, s_0^2)$ and $N_3 = (S_3, A, L_3, AP, V_3, s_0^3)$ be three APAs. Let $N_1 \wedge N_2 = (S_1 \times S_2, A, \tilde{L}, AP, \tilde{V}, (s_0, s_0^2))$ be the conjunction of N_1 and N_2 defined as in Definition 31. We prove the claims separately.

• $\beta^*(N_1 \wedge N_2) \preceq_W N_1$: Obviously, if $N_1 \wedge N_2$ is fully inconsistent, then $\beta^*(N_1 \wedge N_2)$ is empty and refines N_1 with the empty refinement relation. Suppose now that $\beta^*(N_1 \wedge N_2) = (S^\wedge, A, L^\wedge, AP, V^\wedge, (s_0, s_0^2))$, with $S^\wedge \subseteq S_1 \times S_2$, not empty. Define the relation $\mathcal{R} \subseteq S^\wedge \times S_1$ such that for all $(s, s') \in S^\wedge$ and $t \in S_1$, $(s, s')\,\mathcal{R}\,t$ iff $s = t$. We prove that $\mathcal{R}$ is a weak weak refinement relation. Let $(s, s') \in S^\wedge$ such that $(s, s')\,\mathcal{R}\,s$. We show that $\mathcal{R}$ satisfies the axioms of a weak weak refinement relation.

1. let $a \in A$ and $\varphi \in C(S_1)$ such that $L_1(s, a, \varphi) = \top$. Since $(s, s') \in S^\wedge$, we have that $a \in \mathsf{May}(s')$. Let $\tilde{\varphi} \in C(S_1 \times S_2)$ such that $\tilde{\mu} \in Sat(\tilde{\varphi})$ iff
   - the distribution $\mu : r \to \sum_{r' \in S_2} \tilde{\mu}((r, r'))$ is in $Sat(\varphi)$, and
   - there exists a distribution $\varphi' \in C(S_2)$ such that $L_2(s', a, \varphi') \neq \bot$ and the distribution $\mu' : r' \to \sum_{r \in S_1} \tilde{\mu}((r, r'))$ is in $Sat(\varphi')$.

   By definition of $N_1 \wedge N_2$, we have that $\tilde{L}((s, s'), a, \tilde{\varphi}) = \top$. Consider now $\varphi^\wedge \in C(S^\wedge)$ the constraint such that $\mu^\wedge \in Sat(\varphi^\wedge)$ iff there exists $\tilde{\mu} \in Sat(\tilde{\varphi})$ such that $\forall r \in S^\wedge, \mu^\wedge(r) = \tilde{\mu}(r)$ and $\forall r \in S_1 \times S_2 \setminus S^\wedge, \tilde{\mu}(r) = 0$. According to the definition of pruning, we know that $L^\wedge((s, s'), a, \varphi^\wedge) = \sqcup_{\psi \in \overline{\varphi^\wedge}^{(s,s'),a}} \tilde{L}((s, s'), a, \psi)$.
   Since $\tilde{\varphi} \in \overline{\varphi^\wedge}^{(s,s'),a}$, it holds that $L^\wedge((s, s'), a, \varphi^\wedge) = \top$.
   Thus there exists $\varphi^\wedge \in C(S^\wedge)$ such that $L^\wedge((s, s'), a, \varphi^\wedge) = \top$. Moreover, define the correspondence function $\delta : S^\wedge \to (S_1 \to [0, 1])$ such that $\delta((r, r'))(r'') = 1$ iff $r'' = r$. Let $\mu^\wedge \in Sat(\varphi^\wedge)$, $\tilde{\mu}$ the corresponding distribution in $Sat(\tilde{\varphi})$, and μ the distribution such that $\mu : r \in S_1 \mapsto \sum_{r' \in S_2} \tilde{\mu}((r, r'))$. By definition, μ is in $Sat(\varphi)$. We now prove that $\mu^\wedge \Subset^\delta_{\mathcal{R}} \mu$.
   - For all $(r, r') \in S^\wedge$, $\delta((r, r'))$ is a distribution on S_1 by definition.
   - Let $r \in S_1$.

$$\begin{aligned}\sum_{(r,r'') \in S^\wedge} \mu^\wedge((r', r''))\delta((r', r''))(r) &= \sum_{r' \in S_2 \mid (r,r') \in S^\wedge} \mu^\wedge((r, r')) \\ &= \sum_{r' \in S_2 \mid (r,r') \in S^\wedge} \tilde{\mu}((r, r')) \\ &= \sum_{r' \in S_2} \tilde{\mu}((r, r')) \\ &= \mu(r)\end{aligned}$$

   - Finally, if $\delta((r, r'))(r'') > 0$, then $r = r''$ and $(r, r')\,\mathcal{R}\,r$ by definition.

   Thus $\mu^\wedge \Subset^\delta_{\mathcal{R}} \mu$.
2. Let $a \in A$ and $\varphi^\wedge \in C(S^\wedge)$ such that $L^\wedge((s, s'), a, \varphi^\wedge) \neq \bot$. By definition of $L^\wedge$, there exists $\tilde{\varphi} \in \overline{\varphi^\wedge}^{t,a}$. Thus, $\tilde{L}((s, s'), a, \tilde{\varphi} \neq \bot$ in $N_1 \wedge N_2$, and a distribution $\mu^\wedge$ satisfies $\varphi^\wedge$ iff there exists a distribution $\tilde{\mu} \in Sat(\tilde{\varphi})$ such that $\mu^\wedge(r) = \tilde{\mu}(r)$ for all $r \in S^\wedge$ and $\tilde{\mu}(r) = 0$ for all $r \in S_1 \times S_2 \setminus S^\wedge$. Since $S^\wedge$ contains only consistent states, there exists $\mu^\wedge \in Sat(\varphi^\wedge)$. Let $\tilde{\mu} \in Sat(\tilde{\varphi})$ be a corresponding distribution in $\tilde{\varphi}$. There are 3 cases.

- If $a \notin \mathsf{Must}(s)$ and $a \notin \mathsf{Must}(s')$, then by definition of $\tilde{L}$, there must exist $\varphi \in C(S_1)$ and $\varphi' \in C(S_2)$ such that $L_1(s,a,\varphi) \neq \bot$ and $L_2(s',a,\varphi') \neq \bot$. Moreover, $\tilde{\varrho} \in Sat(\tilde{\varphi})$ iff the distributions $\varrho : r \in S_1 \mapsto \sum_{r' \in S_2} \tilde{\varrho}((r,r'))$ and $\varrho' : r' \in S_2 \mapsto \sum_{r \in S_1} \tilde{\varrho}((r,r'))$ are respectively in $Sat(\varphi)$ and in $Sat(\varphi')$.

  Since $\tilde{\mu} \in Sat(\tilde{\varphi})$, let μ and μ' be the corresponding distributions in $Sat(\varphi)$ and $Sat(\varphi')$. Define the correspondence function $\delta : S^\wedge \to (S_1 \to [0,1])$ such that $\delta((r,r'))(r'') = 1$ iff $r'' = r$. As above, we can prove that $\mu^\wedge \Subset^\delta_{\mathcal{R}} \mu$.

- Otherwise, suppose that $a \in \mathsf{Must}(s)$ and there exists $\varphi \in C(S_1)$ such that $\tilde{\varphi}$ is such that $\tilde{\varrho} \in Sat(\tilde{\varphi})$ iff
  - the distribution $\varrho : r \to \sum_{r' \in S_2} \tilde{\varrho}((r,r'))$ is in $Sat(\varphi)$, and
  - there exists a distribution $\varphi' \in C(S_2)$ such that $L_2(s',a,\varphi') \neq \bot$ and the distribution $\varrho' : r' \to \sum_{r \in S_1} \tilde{\varrho}((r,r'))$ is in $Sat(\varphi')$.

  Since $\tilde{\mu} \in Sat(\tilde{\varphi})$, let $\varphi' \in C(S_2)$ be the corresponding constraint on S_2 such that $L_2(s',a,\varphi') \neq \bot$. Let μ and μ' be the corresponding distributions in $Sat(\varphi)$ and $Sat(\varphi')$. Define the correspondence function $\delta : S^\wedge \to (S_1 \to [0,1])$ such that $\delta((r,r'))(r'') = 1$ iff $r'' = r$. As above, we can prove that $\mu^\wedge \Subset^\delta_{\mathcal{R}} \mu$.

- Finally, suppose that $a \in \mathsf{Must}(s')$ and there exists $\varphi' \in C(S_2)$ such that $\tilde{\varphi}$ is such that $\tilde{\varrho} \in Sat(\tilde{\varphi})$ iff
  - there exists a distribution $\varphi \in C(S_1)$ such that $L_1(s,a,\varphi) \neq \bot$ and the distribution $\varrho : r \to \sum_{r' \in S_2} \tilde{\varrho}((r,r'))$ is in $Sat(\varphi)$, and
  - the distribution $\varrho' : r' \to \sum_{r \in S_1} \tilde{\varrho}((r,r'))$ is in $Sat(\varphi')$.

  Since $\tilde{\mu} \in Sat(\tilde{\varphi})$, let $\varphi \in C(S_1)$ be the corresponding constraint on S_1 such that $L_1(s,a,\varphi) \neq \bot$. Let μ and μ' be the corresponding distributions in $Sat(\varphi)$ and $Sat(\varphi')$. Define the correspondence function $\delta : S^\wedge \to (S_1 \to [0,1])$ such that $\delta((r,r'))(r'') = 1$ iff $r'' = r$. As above, we can prove that $\mu^\wedge \Subset^\delta_{\mathcal{R}} \mu$.

Finally, in any case, there exists $\varphi \in C(S_1)$ such that $L_1(s,a,\varphi) \neq \bot$ and there exists $\mu \in Sat(\varphi)$ such that $\mu^\wedge \Subset_{\mathcal{R}} \mu$.

3. By definition, $V^\wedge((s,s')) = \tilde{V}((s,s')) = V_1(s) \cap V_2(s') \subseteq V_1(s)$.

Finally, $\mathcal{R}$ is a weak weak refinement relation, and we have $\beta^*(N_1 \wedge N_2) \preceq_W N_1$.

• $\beta^*(N_1 \wedge N_2) \preceq_W N_2$: This result is obtained using a similar proof as above.

• if $N_3 \preceq_W N_1$ and $N_3 \preceq_W N_2$, then $N_3 \preceq_W \beta^*(N_1 \wedge N_2)$: Let $\mathcal{R}_1 \subseteq S_3 \times S_1$ and $\mathcal{R}_2 \subseteq S_3 \times S_2$ be the weak weak refinement relations such that $N_3 \preceq N_1$ and $N_3 \preceq N_2$. Obviously, if $N_1 \wedge N_2$ is fully inconsistent, then $\beta^*(N_1 \wedge N_2)$ is empty. In this case, there are no consistent APAs refining both N_1 and N_2. As a consequence, N_3 is inconsistent, which violates the hypothesis. Suppose now that $\beta^*(N_1 \wedge N_2) = (S^\wedge, A, L^\wedge, AP, V^\wedge, (s_0, s_0^2))$, with $S^\wedge \subseteq S_1 \times S_2$, is not empty. Define the relation $\mathcal{R}^\wedge \subseteq S_3 \times S^\wedge$ such that $s'' \,\mathcal{R}^\wedge (s,s') \in S^\wedge$ iff $s'' \,\mathcal{R}\, s \in S_1$ and $s'' \,\mathcal{R}'\, s' \in S_2$. We prove that $\mathcal{R}^\wedge$ is a weak weak refinement relation.

Let $s \in S_1, s' \in S_2$ and $s'' \in S_3$ such that $s'' \,\mathcal{R}^\wedge (s,s')$. We show that $\mathcal{R}^\wedge$ satisfies the axioms of a weak weak refinement relation.

1. Let $a \in A$ and $\varphi^\wedge \in C(S^\wedge)$ such that $L^\wedge((s,s'),a,\varphi^\wedge) = \top$. By definition, we have $\tilde{L}((s,s'),a,\tilde{\varphi}) = \top$ with $\tilde{\varphi} \in C(S_1 \times S_2)$ such that $\mu^\wedge \in Sat(\varphi^\wedge)$ iff there exists $\tilde{\mu} \in Sat(\tilde{\varphi})$ such that $\mu^\wedge(r) = \tilde{\mu}(r)$ for all $r \in S^\wedge$ and $\tilde{\mu}(r) = 0$ for all $r \in S_1 \times S_2 \setminus S^\wedge$. There are 2 cases.

   - Suppose that $a \in \mathsf{Must}(s)$ and there exists $\varphi \in C(S_1)$ such that $L_1(s,a,\varphi) = \top$, and $\tilde{\varrho} \in Sat(\tilde{\varphi})$ iff
     - the distribution $\varrho : r \to \sum_{r' \in S_2} \tilde{\varrho}((r,r'))$ is in $Sat(\varphi)$, and
     - there exists a distribution $\varphi' \in C(S_2)$ such that $L_2(s',a,\varphi') \neq \bot$ and the distribution $\varrho' : r' \to \sum_{r \in S_1} \tilde{\varrho}((r,r'))$ is in $Sat(\varphi')$.

     Since $L_1(s,a,\varphi) = \top$ and $s'' \mathcal{R}_1 s$, there exist $\varphi'' \in C(S_3)$ such that $L_3(s'',a,\varphi'') = \top$ and $\forall \mu'' \in Sat(\varphi''), \exists \mu \in Sat(\varphi)$, such that $\mu'' \Subset_{\mathcal{R}_1} \mu$ (1).

     Since $L_3(s'',a,\varphi'') = \top$ and $s'' \mathcal{R}_2 s'$, we have that $\forall \mu'' \in Sat(\varphi'')$, there exist $\varphi' \in C(S_2)$ such that $L_2(s',a,\varphi') \neq \bot$ and $\mu' \in Sat(\varphi')$ such that $\mu'' \Subset_{\mathcal{R}_2} \varrho'$ (2).

     Let $\mu'' \in Sat(\varphi'')$. By (1) and (2), there exists $\mu \in Sat(\varphi)$, $\varphi' \in C(S_2)$ such that $L_2(s',a\varphi') \neq \bot$ and $\mu' \in Sat(\varphi')$ such that $\mu'' \Subset_{\mathcal{R}_1} \mu$ and $\mu'' \Subset_{\mathcal{R}_2} \mu'$. Since (s,s') and s'' are consistent, remark that for all (r,r') in $S_1 \times S_2 \setminus S^\wedge$, we cannot have $s'' \mathcal{R}_1 r$ and we cannot have $s'' \mathcal{R}_2 r'$ (3).

     We now build $\mu^\wedge \in Sat(\varphi^\wedge)$ such that $\mu'' \Subset_{\mathcal{R}^\wedge} \mu^\wedge$.

     Let δ and δ' be the correspondence functions such that $\mu'' \Subset^{\delta}_{\mathcal{R}_1} \mu$ and $\mu'' \Subset^{\delta'}_{\mathcal{R}_2} \mu'$. Define the correspondence function $\delta'' : S_3 \to (S^\wedge \to [0,1])$ such that for all $r'' \in S_3$ and $(r,r') \in S^\wedge$, $\delta''(r'')((r,r')) = \delta(r'')(r)\delta'(r'')(r')$. We build $\mu^\wedge$ and prove that $\mu'' \Subset^{\delta''}_{\mathcal{R}^\wedge} \mu^\wedge$.

     - For all $r'' \in S_3$, if $\mu''(r'') > 0$, both $\delta(r'')$ and $\delta'(r'')$ are distributions. By (3), we know that for all $(r,r') \in S_1 \times S_2 \setminus S^\wedge$, $\delta(r'')(r) = \delta'(r'')(r') = 0$. As a consequence, $\delta''(r'')$ is a distribution on $S^\wedge$.
     - Define $\mu^\wedge(r,r') = \sum_{r'' \in S_3} \mu''(r'')\delta''(r'')((r,r'))$. We prove that $\mu^\wedge \in Sat(\varphi^\wedge)$,
       * Let $r' \in S_2$, we have

$$\begin{aligned}
&\sum_{r \in S_1 \mid (r,r') \in S^\wedge} \mu^\wedge(r,r') \\
&\qquad = \sum_{r \in S_1 \mid (r,r') \in S^\wedge} \sum_{r'' \in S_3} \mu''(r'')\delta''(r'')((r,r')) \\
&\qquad = \sum_{r \in S_1 \mid (r,r') \in S^\wedge} \sum_{r'' \in S_3} \mu''(r'')\delta(r'')(r)\delta'(r'')(r') \\
&\qquad = \sum_{r'' \in S_3} \mu''(r'')\delta'(r'')(r') \sum_{r \in S_1 \mid (r,r') \in S^\wedge} \delta(r'')(r) \\
&\qquad = \sum_{r'' \in S_3} \mu''(r'')\delta'(r'')(r') \\
&\qquad = \mu'(r') \text{ by definition.}
\end{aligned}$$

* Let $r \in S_1$, we have

$$\begin{aligned}
&\sum_{r' \in S_2 \mid (r,r') \in S^\wedge} \mu^\wedge(r,r') \\
&\qquad = \sum_{r' \in S_2 \mid (r,r') \in S^\wedge} \sum_{r'' \in S_3} \mu''(r'')\delta''(r'')((r,r')) \\
&\qquad = \sum_{r' \in S_2 \mid (r,r') \in S^\wedge} \sum_{r'' \in S_3} \mu''(r'')\delta(r'')(r)\delta'(r'')(r') \\
&\qquad = \sum_{r'' \in S_3} \mu''(r'')\delta(r'')(r) \sum_{r' \in S_2 \mid (r,r') \in S^\wedge} \delta'(r'')(r') \\
&\qquad = \sum_{r'' \in S_3} \mu''(r'')\delta(r'')(r) \\
&\qquad = \mu(r) \text{ by definition.}
\end{aligned}$$

Thus we have that

· the distribution $\varrho : r \to \sum_{r' \in S_2} \mu^\wedge((r,r'))$ is in $Sat(\varphi)$, and

· the distribution $\varrho' : r' \to \sum_{r \in S_1} \mu^\wedge((r,r'))$ is in $Sat(\varphi')$.

As a consequence, $\mu^\wedge \in Sat(\varphi^\wedge)$ by definition of $\varphi^\wedge$.

– If $\delta''(r'')((r,r')) > 0$, then by definition $\delta(r'')(r) > 0$ and $\delta'(r'')(r') > 0$. As a consequence, $r'' \mathcal{R}_1 r$ and $r'' \mathcal{R}_2 r'$, thus $r'' \mathcal{R}^\wedge (r,r')$.

Finally, $\mu'' \Subset_{\mathcal{R}^\wedge} \mu^\wedge$ and $\mu^\wedge \in Sat(\varphi^\wedge)$.

- Suppose that $a \in \mathsf{Must}(s')$ and there exists $\varphi' \in C(S_2)$ such that $L_2(s', a, \varphi') = \top$, and $\tilde{\varrho} \in Sat(\tilde{\varphi})$ iff
  – there exists a distribution $\varphi \in C(S_1)$ such that $L_1(s,a,\varphi) \neq \bot$ and the distribution $\varrho : r \to \sum_{r' \in S_2} \tilde{\varrho}((r,r'))$ is in $Sat(\varphi)$, and
  – the distribution $\varrho' : r' \to \sum_{r \in S_1} \tilde{\varrho}((r,r'))$ is in $Sat(\varphi')$.

  This case is strictly symmetric to the one presented above, so there also exists $\varphi'' \in C(S_3)$ such that $L_3(s'', a, \varphi'') = \top$ and for all $\mu'' \in Sat(\varphi'')$, there exists $\mu^\wedge \in Sat(\varphi^\wedge)$ such that $\mu'' \Subset_{\mathcal{R}^\wedge} \mu^\wedge$.

2. Let $a \in A$ and $\varphi'' \in C(S_3)$ such that $L_3(s'', a, \varphi'') \neq \bot$. Let $\mu'' \in Sat(\varphi'')$. Since $s'' \mathcal{R}_1 s$ and $s'' \mathcal{R}_2 s'$, there must exist $\varphi \in C(S_1)$, $\mu \in Sat(\varphi)$, $\varphi' \in C(S_2)$ and $\mu' \in Sat(\varphi')$ such that $L_1(s,a,\varphi) \neq \bot$, $L_2(s', a, \varphi') \neq \bot$, $\mu'' \Subset_{\mathcal{R}_1} \mu$ and $\mu'' \Subset_{\mathcal{R}_2} \mu'$. As a consequence, $\tilde{L}((s,s'), a, \tilde{\varphi}) \neq \bot$, with $\tilde{\varphi} \in C(S_1 \times S_2)$ such that $\tilde{\varrho} \in Sat(\tilde{\varphi})$ iff the distributions $\varrho : r \in S_1 \mapsto \sum_{r' \in S_2} \tilde{\varrho}((r,r'))$ and $\varrho' : r' \in S_2 \mapsto \sum_{r \in S_1} \tilde{\varrho}((r,r'))$ are respectively in $Sat(\varphi)$ and in $Sat(\varphi')$. Moreover, since s'' and (s,s') are consistent, there exists $\varphi^\wedge \in C(S^\wedge)$ such that $L^\wedge((s,s'), a, \varphi^\wedge) \neq \bot$ and $\varrho^\wedge \in Sat(\varphi^\wedge)$ iff there exists $\tilde{\varrho} \in Sat(\tilde{\varphi})$ such that $\varrho^\wedge(r,r') = \tilde{\varrho}(r,r')$ for all $(r,r') \in S^\wedge$ and $\tilde{\varrho}(r,r') = 0$ for all $(r,r') \in S_1 \times S_2 \setminus S^\wedge$. Let δ and δ' the correspondence functions such that $\mu'' \Subset^{\delta}_{\mathcal{R}_1} \mu$ and $\mu'' \Subset^{\delta'}_{\mathcal{R}_2} \mu'$. Since s'' and (s,s') are consistent, we know that (1) for all $(r,r') \in S_1 \times S_2 \setminus S^\wedge$, we have $\mu(r) = \mu'(r') = 0$ and (2) for all $r'' \in S_3$ and $(r,r') \in S_1 \times S_2 \setminus S^\wedge$, we cannot have $r'' \mathcal{R}_1 r$ and we cannot have $r'' \mathcal{R}_2 r'$.
Define the correspondence function $\delta'' : S_3 \to (S^\wedge \to [0,1])$ such that for all $r'' \in S_3$ and $(r,r') \in S^\wedge$, $\delta''(r'')((r,r')) = \delta(r'')(r)\delta'(r'')(r')$. We now build $\mu^\wedge$ such that $\mu'' \Subset^{\delta''}_{\mathcal{R}^\wedge} \mu^\wedge$ and prove that $\mu^\wedge \in Sat(\varphi^\wedge)$.

- For all $r'' \in S_3$, if $\mu''(r'') > 0$, both $\delta(r'')$ and $\delta'(r'')$ are distributions. By (2), we know that for all $(r, r') \in S_1 \times S_2 \setminus S^\wedge$, $\delta(r'')(r) = \delta'(r'')(r') = 0$. As a consequence, $\delta''(r'')$ is a distribution on $S^\wedge$.
- Define $\mu^\wedge(r, r') = \sum_{r'' \in S_3} \mu''(r'')\delta''(r'')((r, r'))$. As above, we can prove that $\mu^\wedge \in Sat(\varphi^\wedge)$.
- If $\delta''(r'')((r, r')) > 0$, then by definition $\delta(r'')(r) > 0$ and $\delta'(r'')(r') > 0$. As a consequence, $r'' \mathcal{R}_1 r$ and $r'' \mathcal{R}_2 r'$, thus $r'' \mathcal{R}^\wedge (r, r')$.

Finally, there exists $\varphi^\wedge \in C(S^\wedge)$ such that $L^\wedge((s, s'), a, \varphi^\wedge) \neq \bot$ and $\mu^\wedge \in Sat(\varphi^\wedge)$ such that $\mu'' \Subset_{\mathcal{R}^\wedge} \mu^\wedge$.

3. Since $s'' \mathcal{R}_1 s$ and $s'' \mathcal{R}_2 s'$, we have $V_3(s'') \subseteq V_1(s) \cap V_2(s') = V^\wedge((s, s'))$. Finally, $\mathcal{R}^\wedge$ is a weak weak refinement relation between N_3 and $\beta^*(N_1 \wedge N_2)$. Moreover, we know that $s_0^3 \mathcal{R}_1 s_0$, $s_0^3 \mathcal{R}_2 s_0^2$, and (s_0, s_0^2) is consistent. As a consequence $s_0^3 \mathcal{R}^\wedge (s_0, s_0^2)$ and $N_3 \preceq \beta^*(N_1 \wedge N_2)$.

□

Appendix G. Detailed proof for Theorem 35

Given a synchronization set $\overline{A}$, we prove that all notions of refinement are a pre-congruence with respect to the parallel composition operator $\|_{\overline{A}}$ defined above, i.e. if $N_1 \ltimes N_1'$ and $N_2 \ltimes N_2'$, then $N_1 \|_{\overline{A}} N_2 \ltimes N_1' \|_{\overline{A}} N_2'$, for $\ltimes \in \{\preceq_T, \preceq_W, \preceq, \preceq_S\}$.

Proof. We provide the proof for $\ltimes = \preceq$. The other proofs are similar.

Let $N_1 = (S_1, A_1, L_1, AP_1, V_1, s_0^1)$, $N_2 = (S_2, A_2, L_2, AP_2, V_2, s_0^2)$, $N_1' = (S_1', A_1, L_1', AP_1, V_1', s_0^{1'})$ and $N_2' = (S_2', A_2, L_2', AP_2, V_2', s_0^{2'})$ be APAs such that $AP_1 \cap AP_2 = \emptyset$. Let $\overline{A} \subseteq A_1 \cap A_2$. Assume that $N_1 \preceq N_1'$ and $N_2 \preceq N_2'$ with weak refinement relations $\mathcal{R}_1$ and $\mathcal{R}_2$, respectively. Let $N_1 \|_{\overline{A}} N_2 = (S_1 \times S_2, A_1 \cup A_2, L, AP_1 \cup AP_2, V, (s_0^1, s_0^2))$ and $N_1' \|_{\overline{A}} N_2' = (S_1' \times S_2', A_1 \cup A_2, L', AP_1 \cup AP_2, V, (s_0^{1'}, s_0^{2'}))$.

Let $\mathcal{R} \subseteq (S_1 \times S_2) \times (S_1' \times S_2')$ be the relation such that $(s_1, s_2) \mathcal{R} (s_1', s_2')$ iff $s_1 \mathcal{R}_1 s_1'$ and $s_2 \mathcal{R}_2 s_2'$. We now show that $\mathcal{R}$ is a weak refinement relation such that $N_1 \|_{\overline{A}} N_2 \preceq N_1' \|_{\overline{A}} N_2'$.

Assume that $(s_1, s_2) \mathcal{R} (s_1', s_2')$. We show that $\mathcal{R}$ satisfies the axioms of a weak refinement relation.

1. Let $a \in A_1 \cup A_2$ and $\varphi' \in C(S_1' \times S_2')$ such that $L'((s_1', s_2'), a, \varphi') = \top$. There are three cases:
   - If $a \in \overline{A}$, then there exists $\varphi_1' \in C(S_1')$ and $\varphi_2' \in C(S_2')$ such that $L_1'(s_1', a, \varphi_1') = L_2'(s_2', a, \varphi_2') = \top$ and $\mu' \in Sat(\varphi')$ iff there exists $\mu_1' \in Sat(\varphi_1')$ and $\mu_2' \in Sat(\varphi_2')$ such that $\mu' = \mu_1' \mu_2'$. Since $s_1 \mathcal{R}_1 s_1'$ and $s_2 \mathcal{R}_2 s_2'$, there exists $\varphi_1 \in C(S_1)$ and $\varphi_2 \in C(S_2)$ with $L_1(s_1, a, \varphi_1) = L_2(s_2, a, \varphi_2) = \top$ and $\forall \mu_1 \in Sat(\varphi_1), \exists \mu_1' \in Sat(\varphi_1') : \mu_1 \Subset_{\mathcal{R}_1} \mu_1'$ and $\forall \mu_2 \in Sat(\varphi_2), \exists \mu_2' \in Sat(\varphi_2') : \mu_2 \Subset_{\mathcal{R}_2} \mu_2'$.

     Define $\varphi \in C(S_1 \times S_2)$ such that $Sat(\varphi) = Sat(\varphi_1) Sat(\varphi_2)$. By definition of $N_1 \|_{\overline{A}} N_2$, we have $L((s_1, s_2), a, \varphi) = \top$. Let $\mu \in Sat(\varphi)$. Then there exist $\mu_1 \in Sat(\varphi_1)$ and $\mu_2 \in Sat(\varphi_2)$ such that $\mu = \mu_1 \mu_2$. Since $s_1 \mathcal{R}_1 s_1'$ and $s_2 \mathcal{R}_2 s_2'$, there exist $\mu_1' \in Sat(\varphi_1')$, $\mu_2' \in Sat(\varphi_2')$ and correspondence functions $\delta_1 : S_1 \to (S_1' \to [0, 1])$ and $\delta_2 : S_2 \to (S_2' \to [0, 1])$, such that $\mu_1 \Subset_{\mathcal{R}_1}^{\delta_1} \mu_1'$ and $\mu_2 \Subset_{\mathcal{R}_2}^{\delta_2} \mu_2'$.

Define the correspondence function $\delta : (S_1 \times S_2) \to ((S_1' \times S_2') \to [0,1])$ as $\delta(u,v)(u',v') = \delta_1(u)(u')\delta_2(v)(v')$. Consider the distribution μ' such that $\mu' = \mu_1'\mu_2'$. By construction, $\mu' \in Sat(\varphi')$. We now prove that $\mu \Subset^{\delta}_{\mathcal{R}} \mu'$:

(a) Assume that for $(u,v) \in S_1 \times S_2$, $\mu(u,v) > 0$. Then we have

$$\begin{aligned}\sum_{(u',v') \in S_1' \times S_2'} \delta(u,v)(u',v') &= \sum_{u' \in S_1'} \sum_{v' \in S_2'} \delta_1(u)(u')\delta_2(v)(v') \\ &= \left(\sum_{u' \in S_1'} \delta_1(u)(u')\right)\left(\sum_{v' \in S_2'} \delta_2(v)(v')\right) \\ &= 1.\end{aligned}$$

Thus $\delta(u,v)$ is a distribution on $S_1' \times S_2'$.

(b) Let $(u',v') \in S_1' \times S_2'$.

$$\begin{aligned}\sum_{(u,v) \in S_1 \times S_2} \mu(u,v)\delta(u,v)(u',v') &= \sum_{u \in S_1} \sum_{v \in S_2} \mu_1(u)\mu_2(v) \\ &\qquad \delta_1(u,u')\delta_2(v,v') \\ &= \left(\sum_{u \in S_1} \mu_1(u)\delta_1(u)(u')\right) \\ &\qquad \left(\sum_{v \in S_2} \mu_2(v)\delta_2(v)(v')\right) \\ &= \mu_1'(u')\mu_2'(v') = \mu'(u',v').\end{aligned}$$

(c) Assume that $\delta(u,v)(u',v') > 0$. Then $\delta_1(u)(u') > 0$ and $\delta_2(v)(v') > 0$, and since $N_1 \preceq N_1'$ and $N_2 \preceq N_2'$, $u \,\mathcal{R}_1\, u'$ and $v \,\mathcal{R}_2\, v'$. Thus, by definition of $\mathcal{R}$, we have $(u,v)\,\mathcal{R}(u',v')$.

- If $a \in A_1 \setminus \overline{A}$, then there exists $\varphi_1' \in C(S_1')$ such that $L_1'(s_1', a, \varphi_1') = \top$. Since $s_1 \,\mathcal{R}_1\, s_1'$, there exists $\varphi_1 \in C(S_1)$ with $L_1(s_1, a, \varphi_1) = \top$ and $\forall \mu_1 \in Sat(\varphi_1), \exists \mu_1' \in Sat(\varphi_1')$ such that $\mu_1 \Subset_{\mathcal{R}_1} \mu_1'$.

  Define $\varphi \in C(S_1 \times S_2)$ such that $\mu \in Sat(\varphi)$ iff for all $u \in S_1$ and $v \neq s_2, \mu(u,v) = 0$ and the distribution $\mu_1 : t \mapsto \mu(t,s_2)$ is in $Sat(\varphi_1)$. By definition of $N_1 \|_{\overline{A}} N_2$, we have $L((s_1,s_2),a,\varphi) = \top$. Let $\mu \in Sat(\varphi)$. Then there exists a $\mu_1 \in Sat(\varphi_1)$ such that μ_1 can be written as $t \mapsto \mu(t,s_2)$ and furthermore there exists $\mu_1' \in Sat(\varphi_1')$ and a correspondence function $\delta_1 : S_1 \to (S_1' \to [0,1])$ such that $\mu_1 \Subset^{\delta_1}_{\mathcal{R}_1} \mu_1'$.

  Define the correspondence function $\delta : (S_1 \times S_2) \to ((S_1' \times S_2') \to [0,1])$ as $\delta(u,v)(u',v') = \delta(u)(u')$ if $v = s_2$ and $v' = s_2'$, and 0 otherwise. Consider the distribution μ' over $S_1' \times S_2'$ such that for all $u' \in S_1'$ and $v' \neq s_2'$, $\mu'(u',v') = 0$ and for all $u' \in S_1'$ $\mu'(u',s_2') = \mu_1'(u')$. By construction, $\mu' \in Sat(\varphi')$. We now prove that $\mu \Subset^{\delta}_{\mathcal{R}} \mu'$:

  (a) Assume that for $(u,v) \in S_1 \times S_2$, $\mu(u,v) > 0$. Then we have

$$\begin{aligned}\sum_{(u',v') \in S_1' \times S_2'} \delta(u,v)(u',v') &= \sum_{u' \in S_1'} \sum_{v' \in S_2'} \delta_1(u)(u') \\ &= \sum_{u' \in S_1'} \delta_1(u)(u') = 1.\end{aligned}$$

Thus $\delta(u,v)$ is a distribution on $S_1' \times S_2'$.

(b) Let $(u',v') \in S_1' \times S_2'$, with $v' \neq s_2'$.

$$\begin{aligned}\sum_{(u,v)\in S_1\times S_2} \mu(u,v)\delta(u,v)(u',v') &= \sum_{u\in S_1}\sum_{v\in S_2}\mu(u,v)0\\ &= 0\\ &= \mu'(u',v'),\end{aligned}$$

Let $u' \in S_1'$, we have

$$\begin{aligned}\sum_{(u,v)\in S_1\times S_2} \mu(u,v)\delta(u,v)(u',s_2') &= \sum_{u\in S_1}\sum_{v=s_2}\mu(u,v)\delta(u,v)(u',s_2')\\ &= \sum_{u\in S_1}\mu_1(u)\delta_1(u,u')\\ &= \mu'(u',v').\end{aligned}$$

(c) Assume that $\delta(u,v)(u',v') > 0$. By definition of δ, we have $\delta_1(u)(u') > 0$ and $v = s_2, v' = s_2'$. By definition of δ_1, we thus have $u \,\mathcal{R}_1\, u'$. Since $s_2 \,\mathcal{R}_2\, s_2'$ by assumption, we finally have $(u,v)\,\mathcal{R}(u',v')$.

- If $a \in A_2 \setminus \overline{A}$, the proof is similar.

2. Let $a \in A_1 \cup A_2$ and $\varphi \in C(S_1 \times S_2)$ such that $L((s_1,s_2),a,\varphi) \neq \bot$. There are three cases:

   - If $a \in \overline{A}$, then there exists $\varphi_1 \in C(S_1)$ and $\varphi_2 \in C(S_2)$ such that $L_1(s_1,a,\varphi_1) \neq \bot$, $L_2(s_2,a,\varphi_2) \neq \bot$, and $\mu \in Sat(\varphi)$ iff there exist $\mu_1 \in Sat(\varphi_1)$ and $\mu_2 \in Sat(\varphi_2)$ such that $\mu = \mu_1\mu_2$. Since $s_1 \,\mathcal{R}_1\, s_1'$ and $s_2 \,\mathcal{R}_2\, s_2'$, there exists $\varphi_1' \in C(S_1')$ and $\varphi_2' \in C(S_2')$ with $L_1'(s_1',a,\varphi_1') \neq \bot$, $L_2'(s_2',a,\varphi_2') \neq \bot$, and $\forall \mu_1 \in Sat(\varphi_1), \exists \mu_1' \in Sat(\varphi_1') : \mu_1 \Subset_{\mathcal{R}_1} \mu_1'$ and $\forall \mu_2 \in Sat(\varphi_2), \exists \mu_2' \in Sat(\varphi_2') : \mu_2 \Subset_{\mathcal{R}_2} \mu_2'$.
     Define $\varphi' \in C(S_1' \times S_2')$ such that $Sat(\varphi') = Sat(\varphi_1')Sat(\varphi_2')$. By definition of $N_1' \|_{\overline{A}} N_2'$, we have $L'((s_1',s_2'),a,\varphi') \neq \bot$. Let $\mu \in Sat(\varphi)$. By definition of φ, there exist $\mu_1 \in Sat(\varphi_1)$ and $\mu_2 \in Sat(\varphi_2)$ such that $\mu = \mu_1\mu_2$. Furthermore, since $s_1 \,\mathcal{R}_1\, s_1'$ and $s_2 \,\mathcal{R}_2\, s_2'$, there exist $\mu_1' \in Sat(\varphi_1')$, $\mu_2' \in Sat(\varphi_2')$ and two correspondence functions $\delta_1 : S_1 \to (S_1' \to [0,1])$ and $\delta_2 : S_2 \to (S_2' \to [0,1])$ such that $\mu_1 \Subset^{\delta_1}_{\mathcal{R}_1} \mu_1'$ and $\mu_2 \Subset^{\delta_2}_{\mathcal{R}_2} \mu_2'$.
     Define the correspondence function $\delta : (S_1 \times S_2) \to ((S_1' \times S_2') \to [0,1])$ such that, for all u,u',v,v', $\delta(u,v)(u',v') = \delta_1(u)(u')\delta_2(v)(v')$. By the same calculations as above, we know that the distribution μ' over $S_1' \times S_2'$ constructed as $\mu' = \mu_1'\mu_2'$ is in $Sat(\varphi')$ and gives that $\mu \Subset^{\delta}_{\mathcal{R}} \mu'$.
   - If $a \in A_1 \setminus \overline{A}$, then there exists $\varphi_1 \in C(S_1)$ such that $L_1(s_1,a,\varphi_1) \neq \bot$. Since $s_1 \,\mathcal{R}_1\, s_1'$, there exists $\varphi_1' \in C(S_1')$ with $L_1'(s_1',a,\varphi_1') \neq \bot$ and $\forall \mu_1 \in Sat(\varphi_1), \exists \mu_1' \in Sat(\varphi_1') : \mu_1 \Subset_{\mathcal{R}_1} \mu_1'$.
     Define $\varphi' \in C(S_1' \times S_2')$ such that $\mu' \in Sat(\varphi')$ iff for all $u' \in S_1'$ and $v' \neq s_2', \mu(u',v') = 0$ and the distribution $\mu_1' : t \mapsto \mu(t,s_2')$ is in $Sat(\varphi_1')$. By definition of $N_1' \|_{\overline{A}} N_2'$, we have $L'((s_1',s_2'),a,\varphi') \neq \bot$. Let $\mu \in Sat(\varphi)$. Let μ_1 be the distribution on S_1 such that for all $t \in S_1$, $\mu_1(t) = \mu(t,s_2)$. By definition, $\mu_1 \in Sat(\varphi_1)$. Let $\mu_1' \in Sat(\varphi_1')$ and a correspondence function $\delta_1 : S_1 \to (S_1' \to [0,1])$ such that $\mu_1 \Subset^{\delta_1}_{\mathcal{R}_1} \mu_1'$.

Define the correspondence function $\delta : (S_1 \times S_2) \to ((S_1' \times S_2') \to [0,1])$ such that for all u, u', v, v', $\delta(u,v)(u',v') = \delta_1(u)(u')$ if $v = s_2$ and $v' = s_2'$, and 0 otherwise. By the same calculations as above, we know that the distribution $\mu' \in Sat(\varphi')$ such that for all $u' \in S_1'$ and $v' \neq s_2'$, $\mu'(u',v') = 0$ and for all $u' \in S_1'$, $\mu_1' = \mu'(u', s_2')$, gives that $\mu \Subset_{\mathcal{R}}^{\delta} \mu'$.

- If $a \in A_2 \setminus \overline{A}$, the proof is similar.

3. For atomic propositions we have that, $V((s_1,s_2)) = V_1(s_1) \cup V_2(s_2)$ and $V'((s_1',s_2')) = \{B = B_1 \cup B_2 \mid B_1 \in V_1'(s_1') \text{ and } B_2 \in V_2'(s_2')\}$. Since $S_1 \mathcal{R}_1 s_1'$ and $s_2 \mathcal{R}_2 s_2'$, we know by definition that $V_1(s_1) \in V_1'(s_1')$ and $V_2(s_2) \in V_2'(s_2')$. Considering $B_1 = V_1(s_1)$ and $B_2 = V_2(s_2)$, we thus have that $V((s_1,s_2)) \in V'((s_1',s_2'))$.

By observing that $(s_0^1, s_0^2)\,\mathcal{R}(s_0^{1\prime}, s_0^{2\prime})$, since $s_0^1 \mathcal{R}_1 s_0^{1\prime}$ and $s_0^2 \mathcal{R}_2 s_0^{2\prime}$, we conclude that $\mathcal{R}$ is a weak refinement relation. □

Appendix H. Detailed proof for Theorem 39

Let N be an APA in single valuation normal form. We prove that $N \preceq_S \varrho(N)$.

Proof. Let $N = (S, A, L, AP, V, s_0)$ be a (consistent) APA in single valuation normal form. Let $\varrho(N) = (S', A, L', AP, V', \{s_0\})$ be the determinisation of N defined as in Definition 38. We prove that $N \preceq_S \varrho(N)$.

Let $\mathcal{R} \subseteq S \times S'$ be the relation such that $s \mathcal{R} Q \iff s \in Q$. We prove that $\mathcal{R}$ is a strong refinement relation. Let s, Q such that $s \mathcal{R} Q$. We show that $\mathcal{R}$ satisfies the axioms of a strong refinement relation.

1. Let $a \in A$ and $\varphi' \in C(S')$ such that $L'(Q,a,\varphi') = \top$. By construction of φ', we have that $\forall q \in Q, \exists \varphi_q \in C(S)$ such that $L(q,a,\varphi_q) = \top$.
   Since $s \in Q$, there exists φ_s such that $L(s,a,\varphi_s) = \top$.
   Define the correspondence function $\delta : S \to (S' \to [0,1])$ such that $\delta(s')(Q') = 1$ if $Q' \in \mathsf{Reach}(Q,a)$ and $s' \in Q'$. Otherwise, $\delta(s')(Q') = 0$.
   We now prove that for all $\mu \in Sat(\varphi_s)$, there exists $\mu' \in Sat(\varphi')$ such that $\mu \Subset_{\mathcal{R}}^{\delta} \mu'$. Let $\mu \in Sat(\varphi_s)$.
   - Let $s' \in S$ such that $\mu(s') > 0$. As a consequence, by definition of Reach, there exists a single $Q' \in S'$ such that $s' \in Q'$. Thus $\delta(s')(Q') = 1$ and for all $Q'' \neq Q'$, we have $\delta(s')(Q'') = 0$. Thus δ defines a distribution on S'.
   - Define $\mu' : S' \to [0,1]$ such that $\mu'(Q') = \sum_{s' \in S} \mu(s')\delta(s')(Q')$. By def of δ, we have that (1) for all $Q' \notin \mathsf{Reach}(Q,a)$, $\mu'(Q') = 0$; (2) there exists $q \in Q$, $\varphi \in C(S)$ and $\mu \in Sat(\varphi)$ (namely s, φ_s and μ) such that $L(q,a,\varphi) \neq \bot$ and for all $Q' \in \mathsf{Reach}(Q,a)$, $\mu'(Q') = \sum_{q' \in Q'} \mu(q')$. Thus $\mu' \in Sat(\varphi')$ by construction.
   - Let s', Q' such that $\delta(s')(Q') > 0$. By construction of δ, we have $s' \in Q'$, thus $s' \mathcal{R} Q'$.

   As a consequence, there exists $\mu' \in Sat(\varphi')$ such that $\mu \Subset_{\mathcal{R}}^{\delta} \mu'$.
2. Let $a \in A$ and $\varphi \in C(S)$ such that $L(s,a,\varphi) \neq \bot$. By construction of $\varrho(N)$, there exists $\varphi' \in C(S')$ such that $L'(Q,a,\varphi') \neq \bot$. φ' is defined as follows: $\mu' \in Sat(\varphi')$ iff (1) $\forall Q' \notin \mathsf{Reach}(Q,a)$, we have $\mu'(Q') = 0$, and (2) there exists $q \in Q$, $\varphi_q \in C(S)$ and $\mu_q \in Sat(\varphi_q)$ such that $L(q,a,\varphi_q) \neq \bot$ and $\forall Q' \in \mathsf{Reach}(Q,a)$, $\mu'(Q') = \sum_{q' \in Q'} \mu_q(q')$.

Define the correspondence function $\delta : S \to S' \to [0,1])$ such that $\delta(s')(Q') = 1$ if $Q' \in \mathsf{Reach}(Q,a)$ and $s' \in Q'$. Otherwise, $\delta(s')(Q') = 0$.
We now prove that for all $\mu \in Sat(\varphi)$, there exists $\mu' \in Sat(\varphi')$ such that $\mu \in^{\delta}_{\mathcal{R}} \mu'$. Let $\mu \in Sat(\varphi)$. and let $\mu' : S' \to [0,1]$ be the distribution such that $\mu'(Q') = \sum_{s' \in S} \mu(s')\delta(s')(Q')$. We prove that $\mu \in^{\delta}_{\mathcal{R}} \mu'$ and $\mu' \in Sat(\varphi')$.

- Let $s' \in S$ such that $\mu(s') > 0$. As a consequence, by definition of Reach, there exists a single $Q' \in S'$ such that $s' \in Q'$. Thus $\delta(s')(Q') = 1$ and for all $Q'' \neq Q'$, we have $\delta(s')(Q'') = 0$. Thus δ defines a distribution on S'.
- Define $\mu' : S' \to [0,1]$ such that $\mu'(Q') = \sum_{s' \in S} \mu(s')\delta(s')(Q')$. By def of δ, we have that (1) for all $Q' \notin \mathsf{Reach}(Q,a)$, $\mu'(Q') = 0$; (2) there exists $q \in Q$, $\varphi_q \in C(S)$ and $\mu_q \in Sat(\varphi_q)$ (namely s, φ and μ) such that $L(q,a,\varphi_q) \neq \bot$ and for all $Q' \in \mathsf{Reach}(Q,a)$, $\mu'(Q') = \sum_{q' \in Q'} \mu_q(q')$. Thus $\mu' \in Sat(\varphi')$ by construction.
- Let s', Q' such that $\delta(s')(Q') > 0$. By construction of δ, we have $s' \in Q'$, thus $s' \,\mathcal{R}\, Q'$.

As a consequence, there exists $\mu' \in Sat(\varphi')$ such that $\mu \in_{\mathcal{R}} \mu'$.

3. By construction of $\varrho(N)$, we have that $V(s) = V'(Q)$.

Finally, $\mathcal{R}$ is a strong refinement relation. Moreover, we have that $s_0 \in \{s_0\}$, thus $s_0 \,\mathcal{R}\{s_0\}$ and $N \preceq_S \varrho(N)$. □

Appendix I. Detailed proof for Theorem 42

Let $N = (S, A, L, AP, V, s_0)$ be a deterministic APA in single valuation normal form and such that $AP \cap A = \emptyset$. We prove that the CMC $\widehat{N}$ is such that, for all MC M, $M \models_{\mathrm{MC}} N \iff M \models \widehat{N}$.

Proof. We prove the two directions separately.

• $M \models_{\mathrm{MC}} N \Rightarrow M \models_{\mathrm{CMC}} \widehat{N}$: Let $M = (Q, \pi, A_M, V_M, q_0)$ be a Markov Chain. We first prove that if $M \models_{\mathrm{MC}} N$, then $M \models_{\mathrm{CMC}} \widehat{N}$. Suppose that there exists a PA $P = (S_P, A, L_P, AP, V_P, s_0^P)$ such that M satisfies P and $P \models N$. Let $\widehat{N} = (\widehat{Q}, \psi, \widehat{A}, \widehat{V}, \widehat{q_0})$ be the transformation of N following Definition 41.

By the satisfaction relation between M and P, we obtain that $A_M = A \cup AP$ and $Q = Q_N \cup Q_D$. Let $\mathcal{R}^{MC} \subseteq Q_D \times S_P$ be the satisfaction relation witnessing that M satisfies P. Let $\mathcal{R}^{\mathrm{PA}} \subseteq S_P \times S$ be the satisfaction relation witnessing $P \models N$. Consider the relation $\mathcal{R} \subseteq Q \times \widehat{Q}$ such that

- $q \,\mathcal{R}(s, \epsilon)$ iff there exists $p \in S_p$ such that $q \,\mathcal{R}^{MC}\, p$ and $p \,\mathcal{R}^{\mathrm{PA}}\, s$, and
- for all $a \in A$, $q \,\mathcal{R}(s,a)$ iff there exists $q' \in Q$ such that
  - $\pi(q')(q) > 0$,
  - $V_M(q) = V_M(q') \cup \{a\}$, and
  - $q' \,\mathcal{R}(s, \epsilon)$.

We now prove that $\mathcal{R}$ is a satisfaction relation for CMCs.

First consider $q \in Q$ and $s \in S$ such that $q \,\mathcal{R}(s, \epsilon)$. By definition, there exists $p \in S_P$ such that $q \,\mathcal{R}^{MC}\, p$ and $p \,\mathcal{R}^{\mathrm{PA}}\, s$. We show that, in this case, $\mathcal{R}$ satisfies the axioms of a satisfaction relation for CMCs.

1. By $\mathcal{R}^{MC}$, we have that $V_M(q) = V_P(p)$. By $\mathcal{R}^{\text{PA}}$, we know that $V_P(p) \in V(s)$. Since $\widehat{V}((s,\epsilon)) = V(s)$, we have, $V_M(q) \in \widehat{V}((s,\epsilon))$.
2. Let δ be a correspondence function such that, for all $q' \in Q$, $s' \in S$ and $a \in A$, $\delta(q')((s',a)) = 1$ if $s' = s$, $\pi(q)(q') > 0$ and $V_M(q') = V_M(q) \cup \{a\}$ and 0 otherwise.
   - Let $q' \in Q$ such that $\pi(q)(q') > 0$. By $\mathcal{R}^{MC}$, there exists $a \in A$ and a distribution ϱ over S_P such that $V_M(q') = V(p) \cup \{a\}$, $L_P(p,a,\varrho) = \top$ and $\pi(q') \Subset_{\mathcal{R}^{MC}} \varrho$. Thus, we have $\pi(q)(q') > 0$ and $V_M(q') = V_M(q) \cup \{a\}$. As a consequence, $\delta(q')((s,a)) = 1$, and for all $(s',b) \neq (s,a)$, $\delta(q')((s',b)) = 0$. Finally, $\delta(q')$ defines a distribution on $\widehat{Q}$.
   - Let $\gamma = \pi(q)\delta$. We prove that γ satisfies $\psi((s,\epsilon))$:
     - By definition of δ, for all $q' \in Q$, we have $\delta(q')((s,\epsilon)) = 0$. As a consequence,
     $$\gamma((s,\epsilon)) = \sum_{q' \in Q} \pi(q)(q')\delta(q')((s,\epsilon)) = 0.$$
     - By definition of δ, we also have that for all $q' \in Q$, $s' \in S$ with $s' \neq s$ and $b \in A \cup \{\epsilon\}$, $\delta(q')((s',b)) = 0$. As a consequence,
     $$\forall s' \neq s, b \in A \cup \{\epsilon\},\ \gamma((s',b)) = \sum_{q' \in Q} \pi(q)(q')\delta(q')((s',b)) = 0.$$
     - Let $a \in \mathsf{Must}(s)$, and $\varphi \in C(S)$ such that $L(s,a,\varphi) = \top$. By $\mathcal{R}^{AP}$, we have that there exists a distribution ϱ over S_P such that $L_P(p,a,\varrho) = \top$ and there exists $\mu \in Sat(\varphi)$ such that $\varrho \Subset_{\mathcal{R}^{AP}} \mu$. Thus, by $\mathcal{R}^{MC}$, we have that there exists $q' \in Q$ such that $V_M(q') = V_P(p) \cup \{a\} = V_M(q) \cup \{a\}$, $\pi(q)(q') > 0$ and $\pi(q') \Subset_{\mathcal{R}^{MC}} \varrho$. By definition of δ, we have that $\delta(q')((s,a)) > 0$. As a consequence,
     $$\gamma((s,a)) = \sum_{q'' \in Q} \pi(q)(q'')\delta(q'')((s,a)) > 0.$$
     - Let $a \notin \mathsf{May}(s)$, i.e. such that for all $\varphi \in C(S)$, we have $L(s,a,\varphi) = \bot$. Suppose that $\gamma((s,a)) > 0$. By definition of γ, there must exist $q' \in Q$ such that $\pi(q)(q') > 0$ and $\delta(q')((s,a)) > 0$. By definition of δ, we thus have $V_M(q') = V_M(q) \cup \{a\} = V_P(p) \cup \{a\}$. Moreover, by $\mathcal{R}^{MC}$, there exists a distribution ϱ such that $L_P(p,a,\varrho) = \top$ and $\pi(q') \Subset_{\mathcal{R}^{MC}} \varrho$. Thus, by $\mathcal{R}^{\text{PA}}$, there must exist $\varphi \in C(S)$ such that $L(s,a,\varphi) \neq \bot$, which is a contradiction. As a consequence, we have
     $$\gamma((s,a)) = 0.$$

     Finally, we have that γ satisfies $\psi((s,\epsilon))$.
   - Let $q' \in Q$ and $(s',a) \in \widehat{Q}$ such that $\delta(q')((s',a)) > 0$. By definition of δ, we have that $\pi(q)(q') > 0$, $a \neq \epsilon$, $V_M(q') = V_M(q) \cup \{a\}$ and $s' = s$. Since $q\,\mathcal{R}(s,\epsilon)$, we have, by definition of $\mathcal{R}$, that $q'\,\mathcal{R}(s,a)$.

Let $q \in Q$, $s \in S$ and $a \in A$ such that $q\,\mathcal{R}(s,a)$. By definition, there exists $q' \in Q$ such that $\pi(q')(q) > 0$, $V_M(q) = V_M(q') \cup \{a\}$ and $q'\,\mathcal{R}(s,\epsilon)$. We show that, also in this case, $\mathcal{R}$ satisfies the axioms of a satisfaction relation for CMCs.

1. Since $q' \mathcal{R}(s,\epsilon)$, we know that there exists $p \in S_P$ such that $q' \mathcal{R}^{MC} p$ and $p \mathcal{R}^{\mathrm{PA}} s$. Thus, we have $V_M(q') = V_P(p) \in V(s)$. Moreover, by definition of $\widehat{N}$, we have that $\widehat{V}((s,a)) = \{B \cup \{a\} \mid B \in V(s)\}$. Since $V_M(q) = V_M(q') \cup \{a\}$ and $V_M(q') \in V(s)$, we have that $V_M(q) \in \widehat{V}((s,a))$.
2. Since $q' \mathcal{R}^{MC} p$ and $\pi(q')(q) > 0$, there exists a distribution ϱ over S_P such that $L_P(p,a,\varrho) = \top$ and there exists a correspondence function δ^{MC} such that $\pi(q) \in^{\delta^{MC}}_{\mathcal{R}^{MC}} \varrho$. Moreover, since $p \mathcal{R}^{\mathrm{PA}} s$, there exists $\varphi \in C(S)$ such that $L(s,a,\varphi) \neq \bot$, and there exist $\mu \in Sat(\varphi)$ and a correspondence function δ^{PA} such that $\varrho \in^{\delta^{\mathrm{PA}}}_{\mathcal{R}^{\mathrm{PA}}} \mu$.
   Define the correspondence function $\delta : Q \to (\widehat{Q} \to [0,1])$ such that for all $q'' \in Q$ and $s'' \in S$,

$$\forall b \in A,\ \delta(q'')((s'',b)) = 0, \text{ and}$$
$$\delta(q'')((s'',\epsilon)) = \sum_{p'' \in P} \delta^{MC}(q'')(p'')\delta^{\mathrm{PA}}(p'')(s'').$$

   - Let $q'' \in Q$ such that $\pi(q)(q'') > 0$. By $\mathcal{R}^{MC}$, we know that $\delta^{MC}(q'')$ is a distribution over S_P. Let now $p'' \in S_P$ such that $\delta^{MC}(q'')(p'') > 0$. By $\mathcal{R}^{MC}$, we know that $\varrho(p'') = \sum_{u \in Q} \pi(q,u)\delta^{MC}(u)(p'') > 0$. As a consequence, by $\mathcal{R}^{\mathrm{PA}}$, we know that $\delta^{\mathrm{PA}}(p'')$ is a distribution over S. As a consequence, we have that $\delta(q'')$ is a distribution over $\widehat{Q}$.
   - Let $\gamma = \pi(q)\delta$. We prove that γ satisfies $\psi((s,a))$.
     - By definition of δ, we have that for all $s'' \in S$ and $b \in A$,

$$\gamma((s'',b)) = \sum_{q'' \in Q} \pi(q)(q'')\delta(q'')((s'',b)) = 0.$$

     - Let $\gamma' : s'' \mapsto \gamma((s'',\epsilon))$. Let $s'' \in S$. By definition, we have

$$\begin{aligned}
\gamma'(s'') &= \gamma((s'',\epsilon)) \\
&= \sum_{q'' \in Q} \pi(q)(q'')\delta(q'')((s'',\epsilon)) \\
&= \sum_{q'' \in Q} \pi(q)(q'') \sum_{p'' \in S_P} \delta^{MC}(q'')(p'')\delta^{\mathrm{PA}}(p'')(s'') \\
&= \sum_{p'' \in S_P} \left(\sum_{q'' \in Q} \pi(q)(q'')\delta^{MC}(q'')(p'') \right) \delta^{\mathrm{PA}}(p'')(s'') \\
&= \sum_{p'' \in S_P} \varrho(p'')\delta^{\mathrm{PA}}(p'')(s'') \ \text{ By definition of } \delta^{MC} \\
&= \mu(s'') \ \text{ By definition of } \delta^{\mathrm{PA}}
\end{aligned}$$

       Finally, we have $\gamma' = \mu$. Since, by definition, $\mu \in Sat(\varphi)$, we have that there exists $\varphi \in C(S)$ such that $L(s,a,\varphi) \neq \bot$ and $\gamma' \in Sat(\varphi)$. Thus γ satisfies $\psi((s,a))$.
     - Let $q'' \in Q$ and $(s'',b) \in \widehat{Q}$ such that $\delta(q'')((s'',b)) > 0$. By definition of δ, $b = \epsilon$ and there must exist $p'' \in S_P$ such that (1) $\delta^{MC}(q'')(p'') > 0$ and (2) $\delta^{\mathrm{PA}}(p'')(s'') > 0$. By (1), we have $q'' \mathcal{R}^{MC} p''$ and by (2),

we have $p'' \mathcal{R}^{\mathrm{PA}} s''$. As a consequence, by definition of $\mathcal{R}$, we have $q'' \mathcal{R}(s'', \epsilon)$.

Thus $\mathcal{R}$ is a satisfaction relation for CMCs. Moreover, we have that $q_0 \mathcal{R}(s_0, \epsilon)$, which gives that $M \models_{\mathrm{CMC}} \widehat{N}$.

• $M \models_{\mathrm{MC}} N \Leftarrow M \models_{\mathrm{CMC}} \widehat{N}$: Let $M = (Q, \pi, A_M, V_M, q_0)$ be a Markov Chain. We prove that if $M \models_{\mathrm{CMC}} \widehat{N}$, then $M \models_{\mathrm{MC}} N$, i.e. there exists a PA P such that M satisfies P and $P \models N$. Let $\widehat{N} = (\widehat{Q}, \psi, \widehat{A}, \widehat{V}, \widehat{q_0})$ be the transformation of N following Definition 41.
Let $\mathcal{R}$ be the satisfaction relation for CMCs witnessing that $M \models_{\mathrm{CMC}} \widehat{N}$. First observe that, by $\mathcal{R}$, the Markov chain M satisfies the following properties: Let $Q_D = \{q \in Q \mid \exists s \in S,\ q \mathcal{R}(s, \epsilon)\}$ and $Q_N = \{q \in Q \mid \exists s \in S, a \in A,\ q \mathcal{R}(s, a)\}$, we have

- $Q_D \cap Q_N = \emptyset$ because of their valuations and $\mathcal{R}$,
- $\forall q, q' \in Q_D$, $\pi(q)(q') = 0$ and $\forall q, q' \in Q_N$, $\pi(q)(q') = 0$,
- $q_0 \in Q_D$, and
- $A_M = A \cup AP$.

Define the PA $P = (S_P, A, L_P, AP, V_P, s_0^P)$ such that $S_P = Q_D$, with $s_0^P = q_0$, V_P is such that for all $q \in Q_D$, $V_P(q) = V_M(q)$, and L_P is such that for all $s \in S_P$, $a \in A$ and for all distribution ϱ over S_P, $L(s, a, \varrho) = \top$ iff there exists $q' \in Q_N$ such that

- $\pi(q)(q') > 0$,
- $V(q') = V(q) \cup \{a\}$, and
- $\varrho = \pi(q')$.

By construction, it is trivial that M satisfies P using the identity relation on Q_D.
We now prove that $P \models N$. Let $\mathcal{R}^{\mathrm{PA}} \subseteq S_P \times S$ the relation such that $p \mathcal{R}^{\mathrm{PA}} s$ iff $p \mathcal{R}(s, \epsilon)$. We now prove that $\mathcal{R}^{\mathrm{PA}}$ is a satisfaction relation for APA.

Let $q \in S_P$ and $s \in S$ such that $q \mathcal{R}^{\mathrm{PA}} s$. We show that $\mathcal{R}^{\mathrm{PA}}$ satisfies the axioms of a satisfaction relation for APAs.

1. Let $a \in A$ and $\varphi \in C(S)$ such that $L(s, a, \varphi) = \top$. By construction, we have that a distribution γ over $\widehat{Q}$ satisfies $\psi((s, \epsilon))$ if $\gamma((s, a)) > 0$.
   Since $q \mathcal{R}(s, \epsilon)$, we have that there exists a correspondence function $\delta : Q \to (\widehat{N} \to [0, 1])$ such that $\pi(q)\delta$ satisfies $\psi((s, \epsilon))$. As a consequence, there must exist $q' \in Q$ such that $\pi(q)(q') > 0$ and $\delta(q')((s, a)) > 0$. By $\mathcal{R}$ again, we have that $V_M(q') = V_M(q) \cup \{a\} = V_M(s) \cup \{a\}$.
   As a consequence, in P, we have that $L_P(q, a, \varrho) = \top$ with $\varrho = \pi(q')$. Moreover, since $\delta(q')((s, a)) > 0$, we have that $q' \mathcal{R}(s, a)$. Thus, there exists a correspondence function $\delta' : Q \to (\widehat{Q} \to [0, 1])$ such that $\pi(q')\delta'$ satisfies $\psi((s, a))$, i.e. the distribution $\gamma' : s' \in S \mapsto [\pi(q')\delta'](s', \epsilon)$ is such that there exists φ' such that $L(s, a, \varphi') \neq \bot$ and $\gamma' \in Sat(\varphi')$. By determinism of N, we have $\varphi = \varphi'$. Let δ^{PA} be the correspondence function between P and S such that for all $p' \in S_P$ and $s' \in S$, $\delta^{\mathrm{PA}}(p')(s') = \delta'(p')((s', \epsilon))$. By construction of $\psi((s, a))$, we have that for all $p' \in S_P$, $b \in A$ and $s' \in S$, $\delta'(p')((s', b)) = 0$. Thus, δ^{PA} is a correct correspondence function by construction.
   Moreover, we have that $\varrho\delta^{\mathrm{PA}} \in Sat(\varphi)$, and, for all p', s' such that $\delta^{\mathrm{PA}}(p')(s') > 0$, we have that $\delta'(p')((s', \epsilon)) > 0$. So, by $\mathcal{R}$, we have $p' \mathcal{R}(s', \epsilon)$, and thus $p' \mathcal{R}^{\mathrm{PA}} s'$.
   Finally, we have that there exists ϱ such that $L_P(q, a, \varrho) = \top$, and there exists $\gamma' = \varrho\delta^{\mathrm{PA}} \in Sat(\varphi)$ such that $\varrho \Subset_{\mathcal{R}^{\mathrm{PA}}}^{\delta^{\mathrm{PA}}} \gamma'$.

2. Let $a \in A$ and $\varrho \in Dist(S_P)$ such that $L_P(q, a, \varrho) = \top$. By construction, there exists $q' \in Q_N$ such that $\pi(q)(q') > 0$, $V_M(q') = V_M(q) \cup \{a\}$ and $\varrho = \pi(q')$.
   Since $q \mathcal{R}(s, \epsilon)$, we have that there exists δ such that $\pi(q)\delta$ satisfies $\psi((s, \epsilon))$. Since $\pi(q)(q') > 0$, $delta(q')$ defines a distribution over $\widehat{Q}$. As a consequence, there exists $(s', b) \in \widehat{Q}$ such that $\delta(q')((s', b)) > 0$. Since $\pi(q)\delta$ satisfies $\psi((s, \epsilon))$, we have that $(s', b) = (s, a)$.
   Thus $\delta(q')((s, a)) > 0$, and, by definition of δ, we have that $q' \mathcal{R}(s, a)$. As a consequence, there exists a correspondence function δ' such that $\pi(q')\delta'$ satisfies $\psi((s, a))$, i.e. the distribution $\gamma' : s' \in S \mapsto [\pi(q')\delta'](s', \epsilon)$ is such that there exists φ such that $L(s, a, \varphi) \neq \bot$ and $\gamma' \in Sat(\varphi)$. Let δ^{PA} be the correspondence function between P and S such that for all $p' \in S_P$ and $s' \in S$, $\delta^{\mathrm{PA}}(p')(s') = \delta'(p')((s', \epsilon))$. By construction of $\psi((s, a))$, we have that for all $p' \in S_P$, $b \in A$ and $s' \in S$, $\delta'(p')((s', b)) = 0$. Thus, δ^{PA} is a correct correspondence function by construction.
   Moreover, we have that $\varrho\delta^{\mathrm{PA}} \in Sat(\varphi)$, and, for all p', s' such that $\delta^{\mathrm{PA}}(p')(s') > 0$, we have that $\delta'(p')((s', \epsilon)) > 0$. So, by $\mathcal{R}$, we have $p' \mathcal{R}(s', \epsilon)$, and thus $p' \mathcal{R}^{\mathrm{PA}} s'$.
   Finally, there exists $\varphi \in C(S)$ such that $L(s, a, \varphi) \neq \bot$ and there exists $\gamma' = \varrho\delta^{\mathrm{PA}}$ in $Sat(\varphi)$ such that $\varrho \Subset^{\delta^{\mathrm{PA}}}_{\mathcal{R}^{\mathrm{PA}}} \gamma'$.
3. By construction, we have $V_P(q) = V_M(q)$. By $\mathcal{R}$, we have $V_M(q) \in \widehat{V}((s, \epsilon)) = V(s)$. Thus $V_P(q) \in V(s)$.

Finally, $\mathcal{R}^{\mathrm{PA}}$ is indeed a satisfaction relation.

By construction, we have that $s_0^P \mathcal{R}^{\mathrm{PA}} s_0$, thus $P \models N$. As a consequence, we have that there exists a PA P such that M satisfies P and $P \models N$. Thus $M \models_{\mathrm{MC}} N$. □