Abstract Probabilistic Automata*

Benoît Delahaye[1], Joost-Pieter Katoen[2], Kim G. Larsen[3], Axel Legay[1], Mikkel L. Pedersen[3], Falak Sher[2], and Andrzej Wąsowski[4]

[1] INRIA/IRISA, Rennes, France
[2] RWTH Aachen University, Software Modeling and Verification Group, Germany
[3] Aalborg University, Denmark
[4] 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.

1 Introduction

Probabilistic Automata (PAs) constitute a mathematical framework for the specification and analysis of non-deterministic probabilistic systems. They have been developed by Segala [22] to model and analyze asynchronous, concurrent systems with discrete probabilistic choice 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 [21]. PAs are recognized as an adequate formalism for randomized distributed algorithms and fault tolerant systems. They are used as semantic model for formalisms such as probabilistic process algebra [19] and a probabilistic variant of Harel's statecharts [11]. An input-output version of PAs is the basis of PIOA and variants thereof [7, 5]. PAs have been enriched with notions such as weak and strong (bi)simulations [22], decision algorithms for these notions [6] and a statistical testing theory [8]. This paper brings two new contributions to the field of probabilistic automata: the theories of *abstraction* and of *specification*.

Abstraction is pivotal to combating the state 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

* Work partially funded by VKR Centre of Excellence — MT-LAB. Part of the work was performed during Wąsowski's stay at INRIA/Rennes.

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, 10, 14]. To abstract from action transitions, we introduce *may* and *must* modalities in the spirit of modal transition systems [17]. 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 shall be viewed as a combination of both Modal Automata [18] and Constraint Markov Chains (CMC) [3] that are abstractions for transition systems and Markov Chains, respectively.

We also propose the first specification theory for PAs, 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 [9]. To the best of our knowledge, the theory of APAs is the first specification theory for PAs in 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. One of our main 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 [12, 2, 10].

Our last contribution is to propose an *abstraction-based* methodology that allows to simplify the behavior of APAs with respect to the refinement relation – such an operation is crucial to avoid state-space explosion. We show that our abstraction preserves weak refinement, and that weak refinement is a precongruence with respect to parallel composition. These results provide the key ingredients to allow *compositional* abstraction of PAs.

Organisation of the paper. In Section 2, we introduce the concepts of APAs and a satisfaction relation with respect to PAs. We also propose a methodology to decide whether an APA is consistent. Refinement relations and abstraction of APAs are discussed in Section 3. Other compositional reasoning operators such as conjunction and composition as well as their relation with abstraction are presented in Section 4. Section 5 discusses the relation between CMCs and APAs and proposes a class of deterministic APAs for which strong and weak refinements coincide with inclusion of sets of implementations. Finally, Section 6 concludes the paper and proposes directions for future research. Due to space limitation, proofs and larger examples are reported in the appendix.

2 Specifications and Implementations

We now introduce the main models of the paper: first *Probabilistic Automata*, and then the new abstraction—*Abstract Probabilistic Automata*.

Implementations. A PA [22] resembles a non-deterministic automaton, but its transitions target probability distributions over states instead of single states. Hence, PAs can be seen as a combination of Markov Chains and non-deterministic automata or as Markov Decision Processes allowing non-determinism.

Definition 1. (Probabilistic automata) *A* probabilistic automaton *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 *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 valuations, and*
- V*:* $S \to 2^{AP}$ *is a state-labeling function.*

Here $\mathbb{B}_2 = \{\bot, \top\}$, with $\bot < \top$. $L(s, a, \mu)$ identifies the *transition* of the automaton: $\top$ indicates its presence and $\bot$ indicates its absence. 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. A *Markov Chain* (MC) is a PA, where, for each $s \in S$, there exists exactly one triple (s, a, μ) such that $L(s, a, \mu) = \top$.

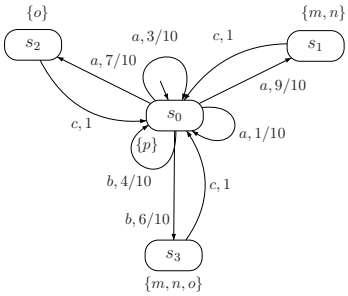


Fig. 1: An example PA

Example 1. Figure 1 presents a PA with $L(s_0, a, \mu) = \top$, where $\mu(s_0) = 3/10$ and $\mu(s_2) = 7/10$. We adopt a notational convention that represents $L(s_0, a, \mu) = \top$ by a set of arrows with tails located close to each other on the boundary of s_0, and heads targeting the states in the support of μ.

In state s_0, a non-deterministic choice takes places on action a between the distributions μ and μ' with $\mu'(s_0) = 1/10$ and $\mu'(s_1) = 9/10$.

Specifications. A Constraint Markov Chain (CMC) [3] is a MC equipped with a constraint on the next-state probabilities from any state. Roughly speaking, an implementation for a CMC is thus a MC, whose next-state probability distribution satisfies the constraint associated with each state. Let $Sat(\varphi)$ denote the set of distributions that satisfy constraint function φ, and $C(S)$ the set of constraint functions defined on state space S.

A *Modal Automaton* [16, 17] 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 needs not be.

An *Abstract Probabilistic Automaton* (APA) is an abstraction that represents a possibly infinite set of PAs. APAs combine Modal Automata and CMCs – the abstractions for labelled transition systems and Markov Chains, respectively.

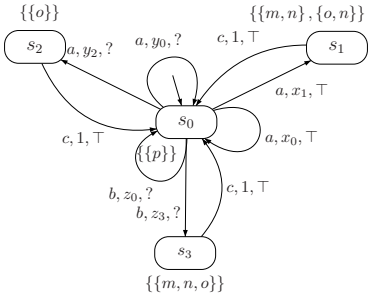
Definition 2. *An* abstract PA *is a tuple* (S, A, L, AP, V, s_0) *such that:*

- S, A, AP *and* s_0 *are defined as before*
- $L : S \times A \times C(S) \longrightarrow \mathbb{B}_3$ *is a* three-*valued state-constraint function, and*
- $V : S \longrightarrow 2^{2^{AP}}$ *maps a state onto a set of admissible valuations.*

Here, $\mathbb{B}_3 = \{\bot, ?, \top\}$ denotes a *complete lattice* with the following ordering $\bot < ? < \top$ and meet ($\sqcap$) and join ($\sqcup$) operators. A CMC is thus an APA, where for each $s \in S$, there exists exactly one triple (s, a, φ) such that $L(s, a, \mu) = \top$, while an *Interval Markov Chain* (IMC) [12] is a CMC whose constraints are disjunctions of intervals. 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 of a constraint function, respectively. We could have limited ourselves to constraints denoting unions of intervals of probability values. However, as we shall soon see, polynomial constraints are needed to support *both* conjunction *and* parallel composition. Like for CMCs, states of an APA are labeled with a set of subsets of atomic propositions. A single set of propositions represents properties that should be satisfied by an implementation state. A powerset models a disjunctive choice of properties. Later, we shall see that any APA 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 AP.

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

Example 2. Consider the APA N given in Figure 2. State s_0 has three outgoing transitions: a *must* a-transition (s_0, a, φ_x), a *may* a-transition (s_0, a, φ_y), and a *may* b-transition (s_0, b, φ_z). Due to the constraint, each of these transitions can cover several transitions in a concrete implementation PA. As an example, the a-transition $(s_0, a, (1/10, 9/10, 0, 0))$ of the PA given in Figure 1 is satisfying the *must* a-transition (s_0, a, φ_x).



$\varphi_x \equiv x_1 \geq 0.9 \wedge x_0 + x_1 = 1$
$\varphi_y \equiv y_2 \leq 0.8 \wedge y_0 + y_2 = 1$
$\varphi_z \equiv z_3 \geq 0.5 \wedge z_0 + z_3 = 1$

Fig. 2: An example APA

In the rest of the paper we distinguish deterministic APAs. The distinction will be of particular importance when comparing APAs in Section 3.1. In APAs, the non-determinism can arise due to sets of valuations in states, or due to actions that label transitions:

Definition 3 (Deterministic APA). *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* $L(s,a,\varphi) \neq \bot$*:*

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

N is deterministic iff it is both action-deterministic and valuation-deterministic.

Satisfaction. We relate APA specifications to PAs implementing them, by extending the definitions of satisfaction introduced in [12]. We start with the following definition that relates distributions between set of states. We use $Dist(S)$ to denote a set of *probability distributions* on the finite set S in the usual way.

Definition 4. **($\Subset_R^\delta$)** *Let S and S' be non-empty 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 as $\mu \Subset_R^\delta \mu'$, iff*

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

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

We are now ready to define the satisfaction relation between PAs and APAs.

Definition 5. (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 *iff, for any $(s,s') \in R$, the following conditions hold:*

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

We say that P satisfies N, denoted $P \models N$, iff 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 iff any must-transition of N is matched by a must-transition of P that agrees on 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 all implementations of N is given by $[\![N]\!] = \{P \mid P \models N\}$.

Example 3. The relation $R = \{(s_0,s_0), (s_1,s_1), (s_2,s_2), (s_3,s_3)\}$ is a satisfaction relation between the PA P given in Figure 1 and the APA N of Figure 2.

Consistency. An APA N is *consistent* iff it admits at least one implementation. 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 also consistent, i.e. has at least one implementation. 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 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). See Appendix C for details.

Theorem 1. *For any APA N, it holds:* $[\![N]\!] = [\![\beta(N)]\!]$.

As the set of states of N is finite, the fixed point computation will always terminate. By the above theorem, we have that $[\![N]\!] = [\![\beta^*(N)]\!]$.

3 Abstraction and Refinement

In this section we introduce *Refinement* that allows to compare APAs. We also propose an *abstraction-based* methodology that permits to simplify the behavior of APAs with respect to the refinement relation.

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 6. (Thorough refinement) *Let $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A, L', AP, V', s'_0)$ be APAs. We say that 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 [1]). 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 two syntactical refinements. These relations extend two well known refinement relations for CMCs and IMCs by combining them with the refinement defined on modal automata. We start with the strong refinement.

Definition 7. (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 iff, for all $(s, s') \in R$, the following conditions hold:*

1. $\forall a \in A. \forall \varphi' \in C(S'). L'(s', a, \varphi') = \top \implies \exists \varphi \in C(S). L(s, a, \varphi) = \top$ *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. $\forall a \in A. \forall \varphi \in C(S). L(s, a, \varphi) \neq \bot \implies \exists \varphi' \in C(S'). L'(s', a, \varphi') \neq \bot$ *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* $N \preceq_S N'$, *iff there exists a strong refinement relation relating* s_0 *and* s'_0.

Observe that strong refinement imposes a "fixed-in-advance" δ in the simulation relation between distributions. This assumption is lifted with the definition of *weak refinement*:

Definition 8. (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 iff, for all* $(s, s') \in R$, *the following conditions hold:*

1. $\forall a \in A. \forall \varphi' \in C(S'). L'(s', a, \varphi') = \top \implies \exists \varphi \in C(S). L(s, a, \varphi) = \top$ *and* $\forall \mu \in Sat(\varphi). \exists \mu' \in Sat(\varphi')$ *with* $\mu \Subset_R \mu'$,
2. $\forall a \in A. \forall \varphi \in C(S). L(s, a, \varphi) \neq \bot \implies \exists \varphi' \in C(S'). L'(s', a, \varphi') \neq \bot$ *and* $\forall \mu \in Sat(\varphi). \exists \mu' \in Sat(\varphi')$ *with* $\mu \Subset_R \mu'$, *and*
3. $V(s) \subseteq V'(s')$.

We say that N *weakly refines* N', *denoted* $N \preceq N'$, *iff there exists a 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 and strong refinements for APAs can be obtained by combining existing fixed-point algorithms for CMCs [4] and Modal Automata [18]. 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 [4]. Both strong and weak refinement imply inclusion of sets of implementations. However, the converse is not true. The following theorem classifies the refinement relations.

Theorem 2. *Thorough refinement is strictly finer than weak refinement, and weak refinement is strictly finer than strong refinement.*

Proof. We present a sketch of the proof and refer to Appendix F.1 for details. By definition, we have that $\preceq_S$ implies $\preceq$. By observing the definition of satisfaction relation, one can easily deduce that $\preceq_S$ and $\preceq$ imply $\preceq_T$. Consider now the APAs N_1 and N_2 given in Figure 3. It is easy to see that $N_1 \preceq N_2$. However, we have that $N_1 \not\preceq_S N_2$. Informally, one can see that State s'_3 and State s'_4 of N_2 both correspond to State s_3 of N_1. Thus, the probability mass x_3 of going to state s_3 in N_1 has to be distributed on s'_3 and s'_4 in order to match probabilities y_3 and

(a) N_1 (b) N_2

Fig. 3: APAs N_1 and N_2 such that $N_1 \preceq N_2$, but not $N_1 \preceq_S N_2$.

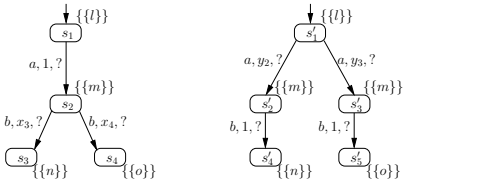
y_4. The latter shall be achieved with the correspondence function δ that defines the refinement relation. The crucial point is that this correspondence function will depend on the exact value of x_3, thus δ cannot be precomputed and we have that $\preceq$, but not $\preceq_S$ holds.

Similarly, $\preceq$ does not imply $\preceq_T$. Consider the APAs N_3 and N_4 given in Figure 4. It is easy to see that $\preceq_T$ holds between N_3 and N_4. However, State s_2 of N_3 cannot refine State s'_2 or s'_3. Indeed, State s_2 has more implementations than s'_2 and s'_3 taken separately. □

We have just seen that thorough refinement is strictly finer than strong and weak refinement. In Section 5, we will propose a class of deterministic APAs on which the three relations coincide.

3.2 Abstraction

This section covers the abstraction of APA. The rationale is to partition the state space, i.e., group (disjoint) sets of states by 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 $s' \in S'$.



(a) N_3 (b) N_4

Fig. 4: APAs N_3 and N_4

Abstraction is lifted to sets of states, or sets of distributions in a pointwise manner. It follows that $\varphi' = \alpha(\varphi)$ iff $Sat(\varphi') = \alpha(Sat(\varphi))$. The abstraction of the product of constraint functions φ and φ' is given as $\alpha(\varphi \cdot \varphi') = \alpha(\varphi) \cdot \alpha(\varphi')$. These ingredients provide the basis to define the abstraction of an APA.

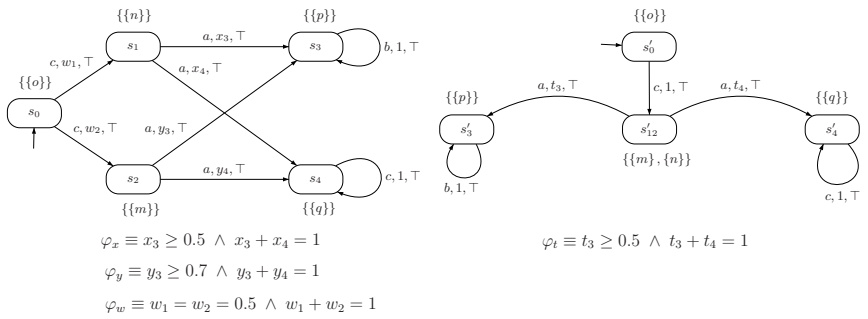


Fig. 5: The APA N (left) is abstracted by the APA N' (right), i.e. $N' = \alpha(N)$

Definition 9. (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 $\varphi' \in C(S')$:*

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

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

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 the total behavior. Item (b) asserts that a may a-transition emanating from s' represents the total behaviour of all transitions (s, a, φ) for $s \in \gamma(s')$, if not all states in $\gamma(s')$ have a must a-transition, and there is a a-transition on modality different from $\bot$. 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.

Lemma 1. *For any APA N, $\alpha(N)$ is an APA.*

Example 4. Consider the APA $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A, L', AP, V', s'_0)$ depicted in Fig. 5. Let the abstraction function $\alpha : S \to S'$ be given by $\alpha(s_0) = s'_0$, $\alpha(s_1) = s'_{12} = \alpha(s_2)$, $\alpha(s_3) = s'_3$ and $\alpha(s_4) = s'_4$. Both states s_1 and s_2 in N have a must a-transition. These are abstracted in N' by a single must a-transition satisfied by distributions in the union of satisfaction sets of φ_x and φ_y.

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

Theorem 3. *For any APA N and abstraction function α, $N \preceq \alpha(N)$.*

4 Compositional Reasoning

APAs can serve as a specification theory for systems with both non-deterministic and stochastic behaviors. Any good specification theory shall be equiped with a *conjunction operation* that allows to combine multiple requirements into a single specification, and a *composition operation* that allows specifications to be combined structurally. Studying these two operations for APAs is the subject of this section.

4.1 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, conjunction allows to compute the intersection of sets of implementations. In this paper, conjunction will be defined for action-deterministic APAs with the same action alphabet. The generalization to non-deterministic APAs with dissimilar alphabets, which is already known to be complex for the case of Modal Automata [20], is postponed for future work. The conjunction operation is a mix between the corresponding operation for modal automata and CMCs.

Definition 10 (Conjunction). *Let $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A, L', AP, V', s'_0)$ be action-deterministic APAs sharing actions sets and atomic propositions sets. The conjunction of N and N' is the APA $N \wedge N' = (S \times S', A, \tilde{L}, AP, \tilde{V}, (s_0, s'_0))$ such that*

- *$\tilde{L}$ is defined as follows. For all $a \in A$ and $(s, s') \in S \times S'$,*
  - *If there exists $\varphi \in C(S)$ such that $L(s, a, \varphi) = \top$ and for all $\varphi' \in C(S')$, we have $L'(s', a, \varphi') = \bot$, or if there exists $\varphi' \in C(S')$ such that $L'(s', a, \varphi') = \top$ and for all $\varphi \in C(S)$, we have $L(s, a, \varphi) = \bot$, then $\tilde{L}((s, s'), a, \mathit{false}) = \top$.*
  - *Else, if either for all $\varphi \in C(S)$, we have $L(s, a, \varphi) = \bot$ or for all $\varphi' \in C(S')$, we have $L'(s', a, \varphi') = \bot$, then for all $\tilde{\varphi} \in C(S \times S')$, $\tilde{L}((s, s'), a, \tilde{\varphi}) = \bot$.*
  - *Otherwise, for all $\varphi \in C(S)$ and $\varphi' \in C(S')$ such that $L(s, a, \varphi) \neq \bot$ and $L'(s', a, \varphi') \neq \bot$), define $\tilde{L}((s, s'), a, \tilde{\varphi}) = L(s, a, \varphi) \sqcup L'(s', a, \varphi')$ with $\tilde{\varphi}$ the new constraint in $C(S \times S')$ such that $\tilde{\mu} \in Sat(\tilde{\varphi})$ iff*
    - *the distribution $\mu : t \to \sum_{t' \in S'} \tilde{\mu}((t, t'))$ is in $Sat(\varphi)$, and*
    - *the distribution $\mu' : t' \to \sum_{t \in S} \tilde{\mu}((t, t'))$ is in $Sat(\varphi')$.*
  - *Finally, for all other $\tilde{\varphi}' \in C(S \times S')$, let $\tilde{L}((s, s'), a, \tilde{\varphi}') = \bot$.*
- *$\tilde{V}((s, s')) = V(s) \cap V'(s')$.*

Observe that the conjunction of two action-deterministic APAs is an action-deterministic APA. The conjunction operation may introduce inconsistent states. Hence, any conjunction operation has to be followed by a pruning operation. Finally, observe that the conjunction of two APAs with interval constraints is not necessarily an APA with interval constraints, but could be an APA whose constraints are systems of linear inequalities (see Appendix B for an example).

The following theorem states that the pruned conjunction of two action-deterministic APAs matches their greatest lower bound with respect to refinement.

Theorem 4. *Let N, N', and N'' be action-deterministic consistent APAs. It holds that $\beta^*(N \wedge N') \preceq N$ and, if $N'' \preceq N$ and $N'' \preceq N'$, then $N'' \preceq \beta^*(N \wedge N')$.*

4.2 Parallel composition

We now propose a composition operation that allows to combine two APAs. We then show how composition and abstraction can collaborate to avoid state-space explosion.

In our theory, the composition operation is parametrized with a set of synchronization actions. This set allows to specify on which actions the two specifications should collaborate and on which actions they can behave individually. The composition of two must transitions is a must transition, but composing a must with a may leads to a may transition.

Definition 11 (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' w.r.t. synchronization set $\bar{A} \subseteq A \cap A'$, written as $N \|_{\bar{A}} N'$, is given as $N \|_{\bar{A}} N' = (S \times S', A \cup A', \tilde{L}, AP \cup AP', \tilde{V}, (s_0, s'_0))$ where*

- *$\tilde{L}$ is defined as follows:*
  - *For all $(s, s') \in S \times S'$, $a \in \bar{A}$, if there exists $\varphi \in C(S)$ and $\varphi' \in C(S')$, such that $L(s, a, \varphi) \neq \bot$ and $L'(s', a, \varphi') \neq \bot$, define $\tilde{L}((s, s'), a, \tilde{\varphi}) = L(s, a, \varphi) \sqcap L'(s', a, \varphi')$ with $\tilde{\varphi}$ the new constraint in $C(S \times S')$ such that $\tilde{\mu} \in Sat(\tilde{\varphi})$ iff there exists $\mu \in Sat(\varphi)$ and $\mu' \in Sat(\varphi')$ such that $\tilde{\mu}(u, v) = \mu(u) \cdot \mu'(v)$ for all $u \in S$ and $v \in S'$.*
    If either for all $\varphi \in C(S)$, we have $L(s, a, \varphi) = \bot$, or $\forall \varphi' \in C(S')$, we have $L'(s', a, \varphi') = \bot$ then for all $\tilde{\varphi} \in C(S \times S')$, $\tilde{L}((s, s'), a, \tilde{\varphi}) = \bot$.
  - *For all $(s, s') \in S \times S'$, $a \in A \setminus \bar{A}$, and for all $\varphi \in C(S)$, define $L((s, s'), a, \tilde{\varphi}) = L(s, a, \varphi)$ with $\tilde{\varphi}$ the new constraint in $C(S \times S')$ such that $\tilde{\mu} \in Sat(\tilde{\varphi})$ iff for all $u \in S$ and $v \neq s'$, $\tilde{\mu}(u, v) = 0$ and the distribution $\mu : t \mapsto \tilde{\mu}(t, s')$ is in $Sat(\varphi)$.*
  - *For all $(s, s') \in S \times S'$, $a \in A' \setminus \bar{A}$, and for all $\varphi' \in C(S')$, define $L((s, s'), a, \tilde{\varphi'}) = L'(s', a, \varphi')$ with $\tilde{\varphi'}$ the new constraint in $C(S \times S')$ such that $\tilde{\mu'} \in Sat(\tilde{\varphi'})$ iff for all $u \neq s$ and $v \in S'$, $\tilde{\mu'}(u, v) = 0$ and the distribution $\mu' : t' \mapsto \tilde{\mu'}(s, t')$ 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 both dissimilar alphabets and non-deterministic APAs. Since PAs are a restriction of APAs, their compositions is defined in the same way. By inspecting Definition 11, 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 closed under all compositional design operations.

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

Theorem 5. *Given a synchronization set $\bar{A}$, the parallel composition operator $\|_{\bar{A}}$ defined above is a precongruence with respect to weak refinement.*

The fact that abstraction preserves weak refinement (cf. Theorem 3), and that weak refinement is a pre-congruence w.r.t. parallel composition, enables us to apply abstraction in a component-wise manner. That is to say, rather than first generating (the typically large PA) $M\|_{\bar{A}}N$, and then applying abstraction, it allows for first applying abstraction, yielding $\alpha_1(M)$ and $\alpha_2(N)$, respectively, and then constructing $\alpha_1(M)\|_{\bar{A}}\alpha_2(N)$. Possibly a further abstraction of $\alpha_1(M)\|_{\bar{A}}\alpha_2(N)$ 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 6. *Let M and N be APA, $\bar{A}$ a synchronization set, and α_1, α_2 be abstraction functions, then:*

$$\alpha_1(M) \,\|_{\bar{A}}\, \alpha_2(N) = (\alpha_1 \times \alpha_2)(M \,\|_{\bar{A}}\, N) \qquad \textit{up to isomorphism}$$

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

5 Completeness and Relation with CMCs

In this section, we propose a class of APAs on which thorough and strong refinements coincide. For doing so, we will compare the expressiveness power of APAs and CMCs, showing that APAs can also act as a specification theory for MCs. We now introduce an important definition that will be used through the rest of the section.

Definition 12. *We say that an APA $N = (S, A, L, AP, V, s_0)$ is in a single valuation normal form iff all its admissible valuations sets are singletons, i.e. for all $s \in S$, we have $|V(s)| = 1$.*

It is worth mentioning that any APA with a single valuation in the initial state can be turned into an APA in single valuation normal form that accepts the same set of implementations (see Appendix D for such a transformation that preserves determinism).

Some results on CMCs. We recap the definitions of MCs and CMCs. Informally, a MC is a PA with a single probability distribution per state.

Definition 13 (Markov Chain). *$P = \langle Q, q_0, \pi, A, V\rangle$ is a* Markov Chain *if Q is a set of states containing the initial state q_0, A is a set of atomic propositions, $V : Q \to 2^A$ is a state valuation, and $\pi : Q \to (Q \to [0,1])$ is a probability transition function: $\sum_{q' \in Q} \pi(q)(q') = 1$ for all $q \in Q$.*

We now formally introduce CMC, our abstraction theory for MCs.

Definition 14 (Constraint Markov Chain). *A* Constraint Markov Chain *is a tuple $C = \langle Q, q_0, \psi, AP, V\rangle$ where Q is a finite set of states, $q_0 \in Q$ is the initial state, $\psi : Q \to (Dist(Q) \to \{0,1\})$ is a constraint function, AP is a set of atomic propositions and $V : Q \to 2^{2^{AP}}$ is a state labeling function.*

For each state $q \in Q$, the constraint function ψ is such that, for all distribution π on Q, $\psi(q)(\pi) = 1$ iff the distribution π is allowed in state q.

We say that a CMC C is deterministic iff for all states $q, q', q'' \in Q$, if there exists $\pi' \in Dist(Q)$ such that $(\psi(q)(\pi') \wedge (\pi'(q') \neq 0))$ and $\pi'' \in Dist(Q)$ such that $(\psi(q)(\pi'') \wedge (\pi''(q'') \neq 0))$, then we have that $V(q') \cap V(q'') = \emptyset$. 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. We will use the following result.

Theorem 7 ([3]). *For deterministic CMCs in single valuation normal form, strong refinement coincides with thorough and weak refinement.*

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 relation between PAs and APAs to conclude.

Definition 15. *Let $P = (S, A, L, AP, V, s_0)$ be a PA with $A \cap AP = \emptyset$. Let $M = \langle Q, q_0, \pi, A_M, V_M\rangle$ 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 iff whenever $q \,\mathcal{R}\, s$, we have*

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

We say that M satisfies P iff 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 $M \models_{MC} N$, iff there exists a PA P such that M satisfies P and P satisfies N.

Expressivity Completeness. In the previous section, we have proposed a satisfaction relation for MCs with respect to APAs. We now propose the following theorem that relates the expressive power of CMCs and APAs.

Theorem 8. *Let $N = (S, A, L, AP, V, s_0)$ be a deterministic APA in single valuation normal form and such that $AP \cap A = \emptyset$. There exists a deterministic CMC $\widehat{N}$ in single valuation normal form such that for all MC M, $M \models_{MC} N \iff M \models \widehat{N}$.*

We have just shown that for all APA N, there exists a CMC $\widehat{N}$ such that $[\![N]\!]_{MC} = [\![\widehat{N}]\!]$. The reverse of the theorem also holds up to a syntactical transformation that preserves sets of implementations (see Appendix E for details). This result together with Theorem 7 leads to the following important result.

Theorem 9. *For deterministic APAs with single valuations in the initial state, strong refinement coincides with thorough and weak refinement.*

6 Conclusion

This paper presents a novel abstraction for PAs and proposes the first specification theory for them. In addition, the paper also studies the relation between abstraction and compositional design in combating the state-space explosion problem.

There are various directions for future research. The first of them being 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 should also consider a continuous-timed extension of our model inspired by [15].

References

1. Benes, N., Kretínský, J., Larsen, K. G., Srba, J.: Checking thorough refinement on modal transition systems is exptime-complete. In: *ICTAC*. Springer (2009) 112–126
2. Caillaud, B., Delahaye, B., Larsen, K. G., Legay, A., Pedersen, M. L., Wasowski, A.: Decision Problems for Interval Markov Chains. http://www.cs.aau.dk/∼mikkelp/doc/IMCpaper.pdf (2010) Research report.
3. Caillaud, B., Delahaye, B., Larsen, K. G., Legay, A., Pedersen, M. L., Wąsowski, A.: Compositional design methodology with constraint Markov chains. In: *QEST*. IEEE (2010)

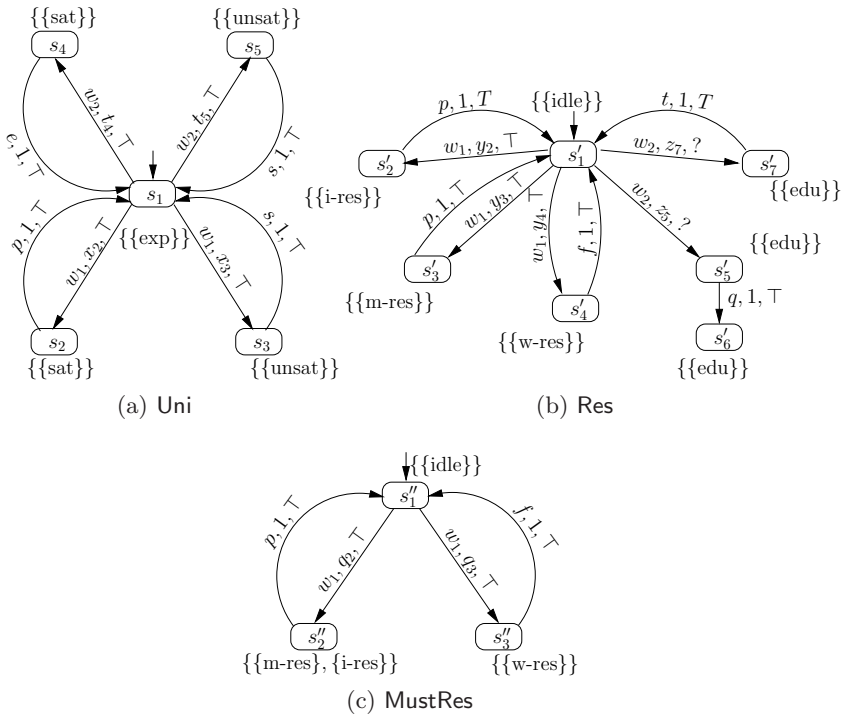
4. Caillaud, B., Delahaye, B., Larsen, K. G., Legay, A., Pedersen, M. L., Wąsowski, A.: Compositional design methodology with constraint Markov chains. In: *Submitted to TCS*. Elsevier (2010)
5. Canetti, R., Cheung, L., Kaynar, D. K., Liskov, M., Lynch, N. A., Pereira, O., Segala, R.: Analyzing security protocols using time-bounded task-pioas. *Discrete Event Dynamic Systems* **18** (2008) 111–159
6. Cattani, S., Segala, R.: Decision algorithms for probabilistic bisimulation. In: *CONCUR. LNCS*, Vol. 2421. Springer (2002) 371–385
7. Cheung, L., Lynch, N. A., Segala, R., Vaandrager, F. W.: Switched pioa: Parallel composition via distributed scheduling. *TCS* **365** (2006) 83–108
8. Cheung, L., Stoelinga, M., Vaandrager, F. W.: A testing scenario for probabilistic processes. *J. ACM* **54** (2007)
9. de Alfaro, L., Henzinger, T. A.: Interface-based design. In: *Engineering Theories of Software-intensive Systems. NATO Science Series: Mathematics, Physics, and Chemistry*, Vol. 195. Springer (2005) 83–104
10. Fecher, H., Leucker, M., Wolf, V.: Don't know in probabilistic systems. In: *Model Checking Software. LNCS*, Vol. 3925. Springer (2006) 71–88
11. Jansen, D. N., Hermanns, H., Katoen, J.-P.: A probabilistic extension of uml statecharts. In: *FTRTFT. LNCS*, Vol. 2469. Springer (2002) 355–374
12. Jonsson, B., Larsen, K. G.: Specification and refinement of probabilistic processes. In: *LICS*. IEEE (1991) 266–277
13. Jonsson, B., Larsen, K. G.: Specification and refinement of probabilistic processes. In: *LICS*. IEEE (1991) 266–277
14. Katoen, J.-P., Klink, D., Leucker, M., Wolf, V.: Three-valued abstraction for continuous-time Markov chains. In: *CAV. LNCS*, Vol. 4590. Springer (2007) 316–329
15. Katoen, J.-P., Klink, D., Neuhäußer, M. R.: Compositional abstraction for stochastic systems. In: *FORMATS. LNCS*, Vol. 5813. Springer (2009) 195–211
16. Larsen, K., Nyman, U., Wąsowski, A.: Modal I/O automata for interface and product line theories. In: *Programming Languages and Systems*. Springer (2007)
17. Larsen, K. G., Thomsen, B.: A modal process logic. In: *LICS*. IEEE (1988) 203–210
18. Larsen, K. G.: Modal specifications. In: *AVMFSS*. Springer (1989) 232–246
19. Parma, A., Segala, R.: Axiomatization of trace semantics for stochastic nondeterministic processes. In: *QEST*. IEEE (2004) 294–303
20. Raclet, J.-B., Badouel, E., Benveniste, A., Caillaud, B., Legay, A., Passerone, R.: Modal interfaces: unifying interface automata and modal specifications. In: *EMSOFT*. ACM (2009) 87–96
21. Segala, R.: Probability and nondeterminism in operational models of concurrency. In: *CONCUR. LNCS*, Vol. 4173. Springer (2006) 64–78
22. Segala, R., Lynch, N. A.: Probabilistic simulations for probabilistic processes. *NJC* **2** (1995) 250–273

A Example

In this example we will illustrate the concepts of conjunction and parallel composition, and demonstrate the need for general constraint functions. We also direct the attention to section B.

Example 5. In Figure 6a and Figure 6b specifications modeling a university (Uni) and a researcher (Res) are shown. The shared action set $A = \{w_1, w_2, s, p, f, q, e, t\}$ denotes the actions work1, work2, stress, paper, failure, quit, exam, and teach. Constraint on probabilities are shown in Equation 1.

Uni expects both types of work to be done symbolized by the transition on w_1 and w_2 with $\top$ modality. When research is done (w_1), with a low probability, an employee will get stress, but much more likely a paper will be produced. With education (w_2), stress is slightly more likely, but will more likely yield an exam. Res may educate students (w_2), which involves a risk of quitting, but must research (w_1). Research can be done in three manners; intensive (i-res), moderate (m-res), and weak (w-res), all as state valuations. Doing weak research involves a risk of failing due to rejectance or other causes.



(a) Uni (b) Res

(c) MustRes

Fig. 6: Three specifications over action set A

$$
\begin{aligned}
&\varphi_x \equiv 0 \leq x_2 \leq 1 \wedge 0 \leq x_3 \leq 0.1 \wedge x_2 + x_3 = 1 \\
&\varphi_t \equiv 0 \leq t_4 \leq 1 \wedge 0 \leq t_5 \leq 0.3 \wedge t_4 + t_5 = 1 \\
&\varphi_y \equiv 0 \leq y_2 \leq 0.5 \wedge 0.2 \leq y_3 \leq 0.7 \wedge 0 \leq y_4 \leq 0.5 \wedge y_2 + y_3 + y_4 = 1 \\
&\varphi_z \equiv 0.02 \leq z_5 \leq 0.07 \wedge 0.95 \leq z_7 \leq 0.99 \wedge z_5 + z_7 = 1 \\
&\varphi_q \equiv 0.4 \leq q_2 \leq 0.8 \wedge 0 \leq q_3 \leq 1 \wedge q_2 + q_3 = 1.
\end{aligned} \tag{1}
$$

The overall specification of Res and Uni running in parallel, is that Res is under no circumstances allowed to quit the job, which could be modeled as a single loop on all actions other than quit with ? modality. That is, Uni and Res composed in parallel must obey this rule or, said differently, the parallel composition must *refine* this overall specification.

The parallel composition Uni and Res, synchronizing on w_1, w_2, e, and p, Figure 8, will still allow Res to quit. The figure is slightly abbreviated to avoid clutter; The valuation on (s_1, s_1') is $\{\{\text{exp}, \text{idle}\}\}$, and the same pattern applies for all other states. Transition modalities are $\top$ every except $\tilde{L}((s_1, s_1'), w_2, \varphi_p) =$?. State (s_1, s_1') is replicated to avoid long arcs. A transition denoted with a single letter, say q, is shorthand for $q, 1, T$. The constraint functions are:

$$
\begin{aligned}
\varphi_r &\equiv \exists \mu \in Sat(\varphi_x) \exists \mu' \in Sat(\varphi_y) \forall (i,j) : r_{ij} = \mu(s_i) \cdot \mu'(s_j') \\
\varphi_p &\equiv \exists \mu \in Sat(\varphi_t) \exists \mu' \in Sat(\varphi_z) \forall (i,j) : p_{ij} = \mu(s_i) \cdot \mu'(s_j')
\end{aligned}
$$

Notice, that constructing the parallel composition yields products of probabilities, which is why we consider general constraint functions.

A behavioural specification (MustRes) (on action set A) is given in Figure 6c. It specifies that a researcher must do moderate or intensive research with a probability between 0.4 and 0.8. Conjoining Res with MustRes will yield Figure 8 with constraint function in Figure 2

$$
\begin{aligned}
\varphi_v \equiv 0 \leq v_{22} \leq 0.5 \wedge 0.2 \leq v_{32} \leq 0.7 \wedge 0 \leq v_{43} \leq 0.5 \wedge \\
0.4 \leq v_{22} + v_{32} \leq 0.8 \wedge v_{22} + v_{32} + v_{43} = 1
\end{aligned} \tag{2}
$$

Notice that this constraint function, because of $0.4 \leq v_{22} + v_{32} \leq 0.8$, can not be expressed using only intervals for each variable.

The parallel composition of the conjoined specifications and Uni is obtained by removing the right part of Figure 7, since this part is deemed inconsistent after conjunction and removed by setting $\tilde{L}((s_1, s_1'), w_2, \varphi_p) = \bot$. This parallel composition does not allow the quit action, and satisfies the requirements.

B Appendix for General Constraints

In this section we will illustrate the need for general constraint functions. The examples that will be presented are extensions of examples introduced in [3].

Parallel composition

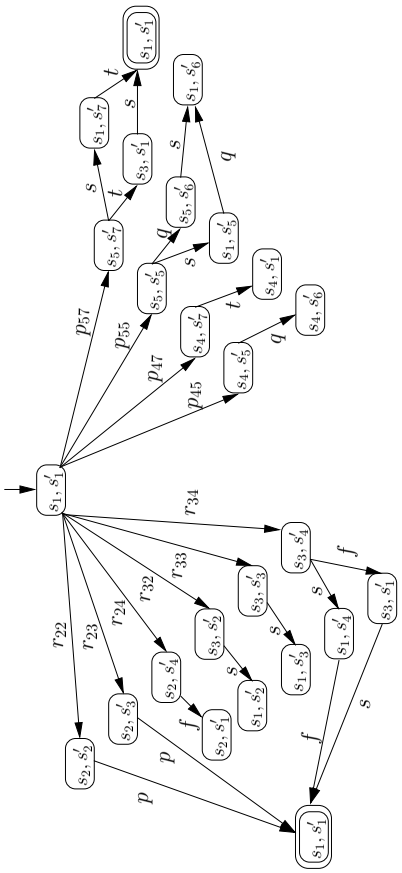


Fig. 7: Parallel composition of Uni and Res with $\bar{A} = \{w_1, w_2, e, p\}$

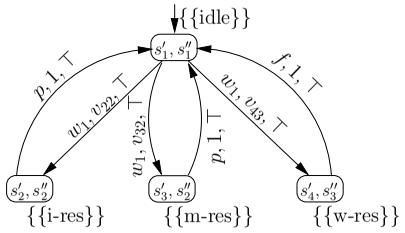
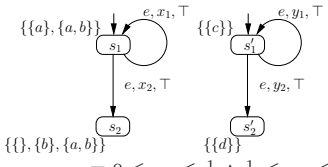
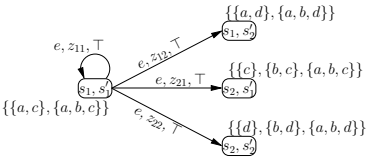


Fig. 8: Conjoining specifications in Figure 6b and Figure 6c



$\varphi_x \equiv 0 \leq x_1 \leq \frac{1}{2} \wedge \frac{1}{3} \leq x_2 \leq 1 \wedge$
$x_1 + x_2 = 1$
$\varphi_y \equiv \frac{1}{2} \leq y_1 \leq 1 \wedge 0 \leq y_2 \leq \frac{2}{3} \wedge$
$y_1 + y_2 = 1$

(a) Two APAs with interval constraints



(b) The parallel composition synchronizing on $\{e\}$

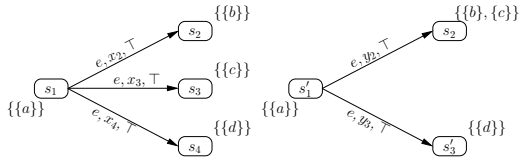
Fig. 9: Two APAs with interval constraints

Consider the two APAs in Figure 9a sharing the action set $A = \{e\}$ and the set of atomic propositions $AP = \{a, b, c, d\}$.

A naive (and wrong) solution to φ_z is $z_{11} \in [0, 1/2]$, $z_{12} \in [0, 1/3]$, $z_{21} \in [1/6, 1]$, and $z_{22} \in [0, 2/3]$. Indeed $z_{11} = 0$, $z_{12} = 1/3$, $z_{21} = 1/3$, and $z_{22} = 1/3$ is in the polytope defined by the intervals, but no implementation of the parallel composition exists for these values, since $z_{11} = 0$ implies $x_1 = 0$, and therefore $z_{12} = 0$.

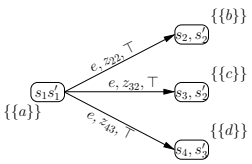
Conjunction

Consider the two APAs in Figure 10a sharing the action set $A = \{e\}$ and the set of atomic propositions $AP = \{a, b, c, d\}$.



$\varphi_x \equiv 0 \leq x_2 \leq \frac{1}{2} \wedge 0.2 \leq x_3 \leq 0.7 \wedge$
$0 \leq x_4 \leq \frac{1}{2} \wedge x_2 + x_3 + x_4 = 1$
$\varphi_y \equiv 0.4 \leq y_2 \leq 0.8 \wedge 0 \leq y_3 \leq 1 \wedge$
$y_2 + y_3 = 1$

(a) Two APAs with interval constraints



(b) The conjunction

Fig. 10: Two APAs with interval constraints

According to Definition 10, $\varphi_z \equiv 0 \leq z_{22} \leq 0.5 \wedge 0.2 \leq z_{32} \leq 0.7 \wedge 0 \leq z_{43} \leq 0.5 \wedge 0.4 \leq z_{22} + z_{32} \leq 0.8 \wedge z_{22} + z_{32} + z_{43} = 1$. Because of $0.4 \leq z_{22} + z_{32} \leq 0.8$, this constraint function can not be expressed as a interval over each variable.

C Appendix for Pruning

It is possible that not all states of an APA N are consistent; however, this does not imply that N is inconsistent. We employ *pruning* to remove inconsistent states of an APA while not reducing its set of implementations.

Definition 16. *Given APA $N = (S, A, L, AP, V, s_0)$, a dummy state $\lambda \notin S$, and $T \subseteq S$ a set of inconsistent states, let $\nu : S \to \{\lambda\} \cup S \backslash T$ be defined by $\nu(s) = \lambda$ if $s \in T$, and $\nu(s) = s$ otherwise.*

Thus, ν maps any inconsistent state in T to the dummy state λ, and is the identity function otherwise.

Definition 17. (Pruning) *Let $N = (S, A, L, AP, V, s_0)$ be an APA with $\lambda \notin S$ and $T \subseteq S$ the set of inconsistent states in N. Let $\nu : S \to \{\lambda\} \cup S \setminus T$ be defined as above. Let β be a pruning function that induces the following: If $\nu(s_0) = \lambda$, then let $\beta(N)$ be the empty APA. Else, let $\beta(N)$ be the APA $\beta(N) = (S', A, L', AP, V', s_0)$ such that $S' = S \setminus T$, and for all $s \in S'$, $a \in A$, $p \in AP$ and $\varphi \in C(S')$,*

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

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

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

All states in T are mapped onto λ and are removed from APA N. The APA $\beta(N)$ that results after 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.

The following is a proof of Theorem 1, that states, that 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 17. The result is trivial if $\beta(N)$ is empty. Else, 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 $P \models N \iff P \models \beta(N)$.

$\Rightarrow$: 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 $q \,\mathcal{R}'\, s$.

1. Let $a \in A$ and $\varphi \in C(S')$ such that $L'(s, a, \varphi) = \top$. By def of L', we have that $\bar{\varphi}^{s,a} \neq \emptyset$ and $\sqcup_{\bar{\varphi} \in \bar{\varphi}^{s,a}} L(s, a, \bar{\varphi}) = \top$. As a consequence, there exists $\bar{\varphi} \in C(S)$ such that $L(s, a, \bar{\varphi}) = T$ and $\mu \in Sat(\varphi)$ iff there exists $\bar{\mu} \in Sat(\bar{\varphi})$ such that $\bar{\mu}(s') = \mu(s')$ for all $s' \in S'$ and $\bar{\mu}(t) = 0$ for all $t \in T$.
   By $\mathcal{R}$, there exists $\rho \in Dist(Q)$ such that $L_P(q, a, \rho) = \top$ and there exists $\bar{\mu} \in Sat(\bar{\varphi})$ such that $\rho \Subset_{\mathcal{R}} \bar{\mu}$. Let $s' \in S$ and suppose that $\bar{\mu}(s') > 0$. Let δ be the correspondence function such that $\rho \Subset^{\delta}_{\mathcal{R}} \bar{\mu}$. By definition, there must exist $q' \in Q$ such that $\rho(q') > 0$ 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 $\bar{\mu}(t) = 0$ (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 $s' \in S'$, $\mu(s') = \bar{\mu}(s')$. 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 $\rho(q') > 0$, then, by $\mathcal{R}$, $\delta(q')$ is a distribution on S. Thus, by (2), δ' is a distribution on S'.
   (b) For all $s' \in S'$,

$$\begin{aligned}\sum_{q' \in Q} \rho(q') \cdot \delta'(q', s') &= \sum_{q' \in Q'} \rho(q') \cdot \delta(q', s') \\ &= \mu(\bar{s'}) = \mu(s').\end{aligned}$$

   (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 $\rho \Subset^{\delta'}_{\mathcal{R}'} \mu$.
2. Let $a \in A$ and $\rho \in Dist(Q)$ such that $L_P(q, a, \rho) = \top$. By $\mathcal{R}$, there exists $\bar{\varphi} \in C(S)$ and $\bar{\mu} \in Sat(\bar{\varphi})$ such that $L(s, a, \bar{\varphi}) \neq \bot$ and $\rho \Subset_{\mathcal{R}} \bar{\mu}$. Let δ be the associated correspondence function. Let $s' \in S$ and suppose that $\bar{\mu}(s') > 0$. By definition, there must exist $q' \in Q$ such that $\rho(q') > 0$ 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 $\bar{\mu}(t) = 0$ (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 $\mu' \in Sat(\bar{\varphi})$ such that, for all $s' \in S'$, $\mu(s') = \mu'(s')$ and for all $t \in T$, $\mu'(t) = 0$. By construction, we have $\bar{\varphi} \in \bar{\varphi}^{s,a}$. Thus, $L'(s, a, \varphi) \neq \bot$.
   Moreover, let $\mu \in Dist(S')$ be the distribution such that for all $s' \in S'$, $\mu(s') = \bar{\mu}(s')$. 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 $\rho(q') > 0$, then, by $\mathcal{R}$, $\delta(q')$ is a distribution on S. Thus, by (2), δ' is a distribution on S'.
(b) For all $s' \in S'$,

$$\sum_{q' \in Q} \rho(q') \cdot \delta'(q', s') = \sum_{q' \in Q'} \rho(q') \cdot \delta(q', s') = \bar{\mu}(s') = \mu(s').$$

(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 $\rho \in^{\delta'}_{\mathcal{R}'} \mu$.

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 $P \models \beta(N)$.

$\Leftarrow$: 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 $P \models N$.

D Appendix for Single Valuation Normal Form

Definition 18. *Let $N = (S, A, L, AP, V, s_0)$ be an APA. If there exists a function $\mathcal{N} : S \to 2^{S'}$ such that*

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

and, 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 $s' \in \mathcal{N}(s)$, let $L'(s', a, \varphi') = L(s, a, \varphi)$ for $\varphi' \in C(S')$ such that $Sat(\varphi') = \{\mu' \in Dist(S') | \mu : s \mapsto \sum_{u \in \mathcal{N}(s)} \mu'(u) \in Sat(\varphi)\}$.*

Clearly, $\mathcal{N}(N)$ is an APA.

Theorem 10. *Let $N = (S, A, L, AP, V, s_0)$ be an APA with a single valuation in the initial state. It holds that $[\![N]\!] = [\![\mathcal{N}(N)]\!]$.*

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 $\mathcal{N} : S \to 2^{S'}$.

$\subseteq$ Let $P = (S_P, A, L_P, AP, V_P, s_0^P)$ be any PA such that $P \in [\![N]\!]$ with satisfaction relation $\mathcal{R} \subseteq S_P \times S$ with $s_0^P \,\mathcal{R}\, s_0$. We show that $P \in [\![\mathcal{N}(N)]\!]$, implying that $[\![N]\!] \subseteq [\![\mathcal{N}(N)]\!]$. We define the relation $\mathcal{R}' \subseteq S_P \times S'$ such that $p \,\mathcal{R}'\, s' \iff V_P(p) \in V'(s') \wedge p \,\mathcal{R}\, \mathcal{N}^{-1}(s')$ and show that it is a satisfaction relation relating s_0^P and s_0'.

Let $p \in S_P$ and $s' \in S'$ be such that $p \,\mathcal{R}'\, s'$:

1. Let $a \in A$ and $\varphi' \in C(S')$, and assume that $L'(s', a, \varphi') = \top$. By definition of $\mathcal{N}(N)$, this must-transition exist, since there exists a transition $L(\mathcal{N}^{-1}(s'), a, \varphi) = \top$ for some $\varphi \in C(S)$. Then, since $P \models N$, there exists $\mu_P \in Dist(S_P)$ such that $L_P(p, a, \mu_P) = \top$ and $\exists \mu \in Sat(\varphi) : \mu_P \Subset_{\mathcal{R}} \mu$. We will now show that $\exists \mu' \in Sat(\varphi') : \mu_P \Subset_{\mathcal{R}'} \mu'$. Let $\delta : S_P \to (S \to [0,1])$ be the correspondence matrix witnessing $\mu_P \Subset_{\mathcal{R}} \mu$. We construct $\delta' : S_P \to (S' \to [0,1])$ as $\delta'(q)(t) = \delta(q)(\mathcal{N}^{-1}(t))$ if $V_P(q) \in V'(t)$, and 0 else. The distribution $\mu' \in Sat(\varphi')$ is defined as a distribution that satifies $\mu(s) = s \mapsto \sum_{u \in \mathcal{N}(s)} \mu'(u)$.
   (a) Take $p' \in S_P$ such that $\mu_P(p') > 0$. We see, since for each $t' \in S$ st. $\delta(q)(t') > 0$, there exists precisely one $t \in S'$ st. $\delta'(q)(t) = \delta(q)(t')$, that
   $$\sum_{s'' \in S'} \delta'(p')(s'') = \sum_{s \in S} \delta(p')(s) = 1.$$
   (b) Let $s'' \in S'$
   $$\begin{aligned}\sum_{p' \in S_P} \mu_P(p') \cdot \delta'(p')(s'') &= \sum_{p' \in S_P : V_P(p') \in V'(s'')} \mu_P(p') \cdot \delta(p')(\mathcal{N}^{-1}(s'')) \\ &= \mu(\mathcal{N}^{-1}(s'')) = \sum_{u \in \mathcal{N}(\mathcal{N}^{-1}(s''))} \mu'(u) \\ &= \mu'(s'').\end{aligned}$$
   (c) Assume that $\delta'(p')(s'') > 0$. Then we know that $V_P(p') \in V'(s'')$ and $\delta(p')(\mathcal{N}^{-1}(s''))$. By the latter, we know that $p' \,\mathcal{R}\, \mathcal{N}^{-1}(s'')$, and therefore $p' \,\mathcal{R}'\, s''$.
2. Let $a \in A$ and $\mu_P \in Dist(S_P)$, and assume that $L_P(p, a, \mu_P) = \top$. Since $P \models N$, there exists $\varphi \in C(S)$ such that $L(\mathcal{N}^{-1}(s'), a, \varphi) \neq \bot$ and $\exists \mu \in Sat(\varphi) : \mu_P \Subset_{\mathcal{R}} \mu$. By definition of $\mathcal{N}(N)$, there exists $\varphi' \in C(S')$ such that $L(s', a, \varphi') = L(\mathcal{N}^{-1}(s'), a, \varphi)$ and $Sat(\varphi') = \{\mu' \in Dist(S') | \mu : s \mapsto \sum_{u \in \mathcal{N}(s)} \mu'(u) \in Sat(\varphi)\}$. We will now show that $\exists \mu' \in Sat(\varphi') : \mu_P \Subset_{\mathcal{R}'} \mu'$. Let $\delta : S_P \to (S \to [0,1])$ be the correspondence matrix witnessing $\mu_P \Subset_{\mathcal{R}} \mu$. We construct $\delta' : S_P \to (S' \to [0,1])$ as $\delta'(q)(t) = \delta(q)(\mathcal{N}^{-1}(t))$ if $V_P(q) \in V'(t)$, and 0 else. The distribution $\mu' \in Sat(\varphi')$ is defined as a distribution that satifies $\mu(s) = s \mapsto \sum_{u \in \mathcal{N}(s)} \mu'(u)$. Using the same reasoning as above, we can deduce that $\mu_P \Subset^{\delta'}_{\mathcal{R}'} \mu'$.
3. By construction of $\mathcal{R}'$, we know that $V_P(p) \in V'(s')$.

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

$\supseteq$ 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 $P \in [\![N]\!]$, implying that $[\![N]\!] \supseteq [\![\mathcal{N}(N)]\!]$. We define the relation $\mathcal{R} \subseteq S_P \times S$ such that $p \,\mathcal{R}\, s \iff \exists s' \in \mathcal{N}(s) : p \,\mathcal{R}'\, s'$ and show that it is a satisfaction relation relating s_0^P and s_0.

Let $p \in S_P$ and $s \in S$ be such that $p \,\mathcal{R}\, s$:

1. Let $a \in A$ and $\varphi \in C(S)$, and assume that $L(s, a, \varphi) = \top$. There exists $s' \in \mathcal{N}(s) : p \,\mathcal{R}'\, s'$, and therefore, by definition of $\mathcal{N}(s)$, there exists a $\varphi \in C(S')$ st. $L'(s', a, \varphi) = \top$. Since $P \models \mathcal{N}(N)$, there exists $\mu_P \in Dist(S_P)$ such that $L_P(p, a, \mu_P) = \top$ and $\exists \mu' \in Sat(\varphi') : \mu_P \Subset_{\mathcal{R}'} \mu'$. We will now show that $\exists \mu \in Sat(\varphi) : \mu_P \Subset_{\mathcal{R}} \mu$. Let $\delta' : S_P \to (S' \to [0,1])$ be the correspondence matrix witnessing $\mu_P \Subset_{\mathcal{R}'} \mu'$. We construct $\delta : S_P \to (S \to [0,1])$ as $\delta(q)(t) = \sum_{t' \in \mathcal{N}(t)} \delta'(q)(t')$. The distribution $\mu \in Sat(\varphi)$ is defined as the distribution that satifies $\mu(s) = s \mapsto \sum_{u \in \mathcal{N}(s)} \mu'(u)$.
   (a) Take $p' \in S_P$ such that $\mu_P(p') > 0$. Clearly, since $S' = \cup_{s \in S} \mathcal{N}(s)$,
   $$\sum_{s'' \in S} \delta(p')(s'') = \sum_{s'' \in S} \sum_{t' \in \mathcal{N}(s'')} \delta'(p')(t') = 1.$$
   (b) Let $s'' \in S'$
   $$\begin{aligned}\sum_{p' \in S_P} \mu_P(p') \cdot \delta(p')(s'') &= \sum_{p' \in S_P} \mu_P(p') \cdot \sum_{t' \in \mathcal{N}(s'')} \delta'(p')(t') \\ &= \sum_{t' \in \mathcal{N}(s'')} \sum_{p' \in S_P} \mu_P(p') \cdot \delta'(p')(t') \\ &= \sum_{t' \in \mathcal{N}(s'')} \mu'(t') = \mu(s'').\end{aligned}$$
   (c) Assume $\delta(p')(s'') > 0$. Then there exists $t' \in \mathcal{N}(s'')$ such that $\delta'(p')(t') > 0$ and therefore $p' \,\mathcal{R}'\, t'$ which implies $p' \,\mathcal{R}\, s''$.
2. Let $a \in A$ and $\mu_P \in Dist(S_P)$, and assume that $L_P(p, a, \mu_P) = \top$. There exists $s' \in \mathcal{N}(s) : p \,\mathcal{R}'\, s'$, and since $P \models \mathcal{N}(N)$, there exists $\varphi' \in C(S')$ such that $L'(s', a, \varphi') \neq \bot$ and $\exists \mu' \in Sat(\varphi') : \mu_P \Subset_{\mathcal{R}'} \mu'$. By definition of $\mathcal{N}(N)$, there exists $\varphi \in C(S)$ such that $L(s, a, \varphi) = L'(s', a, \varphi')$ and $Sat(\varphi') = \{\mu' \in Dist(S') | \mu : s \mapsto \sum_{u \in \mathcal{N}(s)} \mu'(u) \in Sat(\varphi)\}$. We will now show that $\exists \mu \in Sat(\varphi) : \mu_P \Subset_{\mathcal{R}} \mu$. Let $\delta' : S_P \to (S' \to [0,1])$ be the correspondence matrix witnessing $\mu_P \Subset_{\mathcal{R}'} \mu'$. We construct $\delta : S_P \to (S \to [0,1])$ as $\delta(q)(t) = \sum_{t' \in \mathcal{N}(t)} \delta'(q)(t')$. The distribution $\mu \in Sat(\varphi)$ is defined as the distribution that satifies $\mu(s) = s \mapsto \sum_{u \in \mathcal{N}(s)} \mu'(u)$. Using the same reasoning as above, we can deduce that $\mu_P \Subset^{\delta}_{\mathcal{R}} \mu$.
3. Since there exists $s' \in \mathcal{N}(s) : p \,\mathcal{R}'\, s'$, we know that $V_P(p) \in V'(s')$. By definition $V(s) = \cup_{s'' \in \mathcal{N}(s)} V'(s)$, so it is clear that $V_P(p) \in V(s)$.

We conclude that $s_0^P \,\mathcal{R}\, s_0$, since $p \,\mathcal{R}'\, s_0'$ and $s_0' \in \mathcal{N}(s_0)$).

By mutual inclusion, we conclude that $[\![N]\!] = [\![\mathcal{N}(N)]\!]$.

E Appendix for Completeness

In this section, we describe a syntactic transformation f on CMCs, preserving sets of implementations, such that the reverse of Theorem 8 holds. This transformation consists in duplicating all the states of a given CMC C in order to simulate a non-deterministic choice.

Definition 19. *Let $C = \langle Q, q_0, \psi, AP, V\rangle$ be a CMC. Let Γ be a fresh variable ($\gamma \notin AP$). Define the CMC $f(C) = \langle Q', q'_0, \psi', AP \cup \{\Gamma\}, V'\rangle$ such that $Q' = Q_N \cup Q_D$, with Q_N and Q_D two copies of Q. If $q \in Q$, denote q_N and q_D the copies of q belonging to Q_N and Q_D respectively. Let $q'_0 = (q_0)_D$ and define ψ' such that*

- *for all $q_D \in Q_D$, and $\pi \in Dist(Q')$, $\psi'(q_D)(\pi) = 1$ iff $\pi(q_N) = 1$, and*
- *for all $q_N \in Q_N$ and $\pi \in Dist(Q')$, $\psi'(q_N)(\pi) = 1$ iff*
  1. *for all $q'_N \in Q_N$, we have $\pi(q'_N) = 0$, and*
  2. *the distribution $\pi' : q' \in Q \mapsto \pi(q'_D)$ over Q is such that $\psi(q)(\pi') = 1$.*

Finally, let $V'(q_D) = V(q)$ and $V'(q_N) = V(q) \cup \{gamma\}$ for all $q \in Q$.

Since Markov chains are restrictions of CMCs, the same transformation can be defined on Markov Chains.

The following theorem states that this transformation preserves implementation.

Theorem 11. *Let M be a MC and C be a CMC. We have $M \models C \iff f(M) \models f(C)$.*

The proof of this theorem is straightforward and left to the reader.

By introducing non-deterministic choices in the original CMCs, the transformation f enables us to turn any CMC into an APA that will have the same set of implementations. This is formalized in the following theorem.

Theorem 12. *Let C be a CMC. There exists an APA $\widetilde{C}$ such that, for all MC M, we have $M \models C \iff f(M) \models_{MC} \widetilde{C}$.*

Proof. We define the transformation from CMCs to APAs $C \mapsto \widetilde{C}$ and leave the rest of the proof to the reader.

Let $C = \langle Q, q_0, \psi, AP, V\rangle$ be a CMC. Let Γ be a fresh variable ($\Gamma \notin AP$). Define the APA $\widetilde{C} = (\widetilde{Q}, \{\Gamma\}, L, AP, \widetilde{V}, \widetilde{q_0})$ such that

- $\widetilde{Q} = Q$,
- $\widetilde{q_0} = q_0$,
- $\widetilde{V} : \widetilde{q} \in \widetilde{Q} \mapsto V(q)$, and
- L is such that for all $\widetilde{q} \in \widetilde{Q}$, $L(\widetilde{q}, \Gamma, \varphi) = \top$ with $\varphi \in C(\widetilde{Q})$ such that for all $\pi \in Dist(\widetilde{Q})$, $\pi \in Sat(\varphi)$ iff the distribution $\pi' : q' \in Q \mapsto \pi(\widetilde{q'})$ over Q is such that $\psi(q)(\pi') = 1$.

F Proofs

F.1 Proof of Theorem 2

Refinement relations can be ordered as follows: thorough refinement is strictly finer than weak refinement, and weak refinement is strictly finer than strong refinement.

– It directly follows from the definitions (by a swap of quantifiers) that strong refinement implies weak refinement. We prove that 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 with $AP = AP'$ and $A = A'$. If $N \preceq N'$, then $N \preceq_T N'$.

Proof. Assume that $N \preceq N'$. Then there exists a weak refinement relation $\mathcal{R}' \subseteq S \times S'$ such that $s_0 \,\mathcal{R}'\, s_0'$. Let $P = (S_P, A_P, L_P, AP_P, V_P, s_0^P)$ such that $P \models N$; if $[\![N]\!] = \emptyset$, the theorem is true. Else, there exists a satisfaction relation $\mathcal{R}'' \subseteq S_P \times S$ such that $s_0^P \,\mathcal{R}''\, s_0$.
We now propose a relation $\mathcal{R} \subseteq S_P \times S'$, such that $u \,\mathcal{R}\, w$ iff $\exists v \in S : u \,\mathcal{R}''\, v \wedge v \,\mathcal{R}'\, w$. We now show that $\mathcal{R}$ is a satisfaction relation.
Assume that $u \,\mathcal{R}\, w$ and let $v \in S$ be a state such that $u \,\mathcal{R}''\, v$ and $v \,\mathcal{R}'\, w$.

1. Let $a \in A'$ and $\varphi' \in C(S')$, and assume that $L'(w, a, \varphi') = \top$: By refinement of N and N', there exists $\varphi \in C(S)$ such that $L(v, a, \varphi) = \top$ and $\forall \mu \in Sat(\varphi), \exists \mu' \in Sat(\varphi')$ with $\mu \Subset_{R'} \mu'$. Moreover, by satisfaction of P and N there exists $\mu_P \in Dist(S_P)$ such that $L_P(u, a, \mu) = \top$ 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 $\delta'' : S \to (S' \to [0,1])$ and $\delta' : S_P \to (S \to [0,1])$ be correspondence functions witnessing $\mu_P \Subset_{R''} \mu_S$ and $\mu_S \Subset_{R'} \mu'$, respectively. We now construct the correspondence function $\delta : S_P \to (S' \to [0,1])$ by $\delta(s)(t) = \sum_{r \in S} \delta''(s)(r) \cdot \delta'(r)(t)$ and prove that $\mu_P \Subset_{\mathcal{R}}^{\delta} \mu'$:
   (a) Let $s \in P$ such that $\mu_P(s) > 0$.

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

   (b) Let $t \in S'$.

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

(c) Assume that $\delta(s)(t) > 0$. Then, there exists $r \in S$ such that $\delta''(s)(r) > 0$ and $\delta'(r)(t) > 0$. The implies that $s \,\mathcal{R}''\, r$ and $r \,\mathcal{R}'\, t$ and by definition of $\mathcal{R}$, $s \,\mathcal{R}\, t$.

2. Let $a \in A$ and $\mu_P \in Dist(S_P)$ and assume that $L_P(u, a, \mu) \geq ?$ Then, by satisfaction of P and N, there exists $\varphi \in C(S)$ such that $L(v, a, \varphi) \geq ?$ and $\exists \mu_S \in Sat(\varphi)$ with $\mu_P \Subset_{R''} \mu$. Moreover, by refinement of N and N' there exists $\varphi' \in C(S')$ such that $L'(w, a, \varphi') \geq ?$ and $\forall \mu \in Sat(\varphi), \exists \mu' \in Sat(\varphi')$ with $\mu \Subset_{R'} \mu'$.
   Choose $\mu_S \in Dist(S)$ such that $\mu_P \Subset_{R''} \mu_S$ and choose $\mu' \in Dist(S')$ such that $\mu_S \Subset_{R'} \mu'$. Let $\delta'' : S \to (S' \to [0, 1])$ and $\delta' : S_P \to (S \to [0, 1])$ be correspondence functions witnessing $\mu_P \Subset_{R''} \mu_S$ and $\mu_S \Subset_{R'} \mu'$, respectively. We now construct the correspondence function $\delta : S_P \to (S' \to [0, 1])$ by $\delta(s)(t) = \sum_{r \in S} \delta''(s)(r) \cdot \delta'(r)(t)$. Using the same reasoning as above, we can deduce that $\mu_P \Subset^{\delta}_{\mathcal{R}} \mu'$.
3. By definition 5, 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 $N \preceq_T N'$.

– We now show that there exists APAs N_1 and N_2, such that $N_1 \preceq N_2$, but $N_1 \not\preceq_S N_2$.

Proof. Consider the APAs N_1 and N_2 given in Figure 3.

- $N_1 \preceq N_2$: We prove 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 starting by proving $s_1 \,\mathcal{R}\, s_1'$; the others pairs are trivially related since the have no outgoing transitions and their valuations correspond.
  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

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

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

  $$\begin{aligned}
  \sum_{s \in S} \mu(s) \cdot \delta(s)(s_3') &= \mu(s_3) \cdot \frac{0.7 - \mu(s_2)}{\mu(s_3)} = 0.7 - \mu(s_2), \\
  \sum_{s \in S} \mu(s) \cdot \delta(s)(s_4') &= \mu(s_3) \cdot \left(1 - \frac{0.7 - \mu(s_2)}{\mu(s_3)}\right) \\
  &= \mu(s_3) - 0.7 + \mu(s_2).
  \end{aligned}$$

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 $\mu \Subset_R^\delta \mu'$. Similarly, 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 $\{\{l\}\} \subseteq \{\{l\}\}$.

- $N_1 \not\preceq_S N_2$: 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 not influenced by the value of $\mu(s_2)$). Consider the following two distributions over S, μ_1 and μ_2 given by

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

It must hold both, that $\exists \mu'_1 \in Dist(S') \forall s' \in S' : \sum_{s \in S} \mu_1(s) \cdot \delta(s)(s') = \mu'_1(s')$ and $\exists \mu'_2 \in Dist(S') \forall s' \in S' : \sum_{s \in S} \mu_2(s) \cdot \delta(s)(s') = \mu'_2(s')$. But the first case implies requires $\gamma = 1$, and the second case requires $\gamma = 0$, which shows that there can not exists a strong refinement relation, since the correspondence function can not be fixed in advance.

– Finally, we show that there exists APAs N_3 and N_4, such that $N_3 \preceq_T N_4$, but $N_3 \not\preceq N_4$.

Proof. Consider the APAs N_3 and N_4 given in Figure 4.

- $N_3 \preceq_T N_4$: Any PA satisfying N_3 will also satisfy N_4.
- $N_3 \not\preceq N_4$: Consider the pair (s_2, s'_2). For this pair to be member of a weak refinement relation $\mathcal{R}$. $Sat(\varphi_x)$ consists of the distribution μ_1 and μ_2 that give probability 1 to s_3 and s_4, respectively. A correspondence function δ such that $\mu_2 \Subset_{\mathcal{R}}^\delta \mu'_2$, where μ'_2 is the distribution assigning probability 1 to s'_4, can not exist, since such a δ will satisfy that $\delta(s_4)(s'_4) = 1$. This pair can not be related, since $\{\{o\}\} \not\subseteq \{\{n\}\}$. The same applies for the pair (s_2, s'_3). This implies, that N_3 can not weakly refine N_4.

F.2 Proof of Theorem 3

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

Assume that $s \,\mathcal{R}\, s'$ for $s \in S$ and $s' \in S'$. Notice, that this is implies that $s \in \gamma(s')$.

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

$\top$. Let $\mu \in Sat(\varphi)$ and construct $\mu' \in Dist(S')$ as $\mu'(s'') = \alpha(\mu)(s'')$ for all $s'' \in S'$. Clearly, $\mu' \in Sat(\varphi')$.
Define $\delta : S \to (S' \to [0,1])$ as $\delta(u)(v) = 1$, if $\alpha(u) = v$, and 0 else. 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 $v \in S'$.

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

by definition of an abstraction of a distribution.
(c) Assume that $\delta(u)(v) > 0$. Then $\alpha(u) = v$, and $u \,\mathcal{R}\, v$.

2. Let $a \in A$ and $\varphi \in C(S)$, and assume that $L(s,a,\varphi) \geq ?$
   (a) If $L(s,a,\varphi) = \top$ and $\forall s_1 \in \gamma(s') \exists \varphi_1 \in C(S) : L(s_1,a,\varphi_1) = \top$, we have that $\varphi' \in C(S')$ defined as in case (a) of Definition 9 yields that $L'(s',a,\varphi') = \top$.
   Again define $\mu' \in Dist(S')$ as the distribution defined by $\mu'(s'') = \alpha(\mu)(s'')$ for all $s'' \in S'$ and some $\mu \in Sat(\varphi)$, and by the same reasoning as above, $\mu \Subset_{\mathcal{R}'} \mu'$.
   (b) If $L(s,a,\varphi) = \top$ and $\exists s_1 \in \gamma(s') \exists \varphi_1 \in C(S) : L(s_1,a,\varphi_1) \neq \bot$, we have that $\varphi' \in C(S')$ defined as in case (b) of Definition 9 yields that $L'(s',a,\varphi') = ?$.
   Again define $\mu' \in Dist(S')$ as the distribution defined by $\mu'(s'') = \alpha(\mu)(s'')$ for all $s'' \in S'$ and some $\mu \in Sat(\varphi)$, and by the same reasoning as above, $\mu \Subset_{\mathcal{R}'} \mu'$.
   (c) If $L(s,a,\varphi) = \top$ and $\forall s_1 \in \gamma(s') : s_1 \neq s, \forall \varphi_1 \in C(S) : L(s_1,a,\varphi_1) = \bot$, we have that $\varphi' \in C(S')$ defined as in case (b) of Definition 9 yields that $L'(s',a,\varphi') = ?$.
   Again define $\mu' \in Dist(S')$ as the distribution defined by $\mu'(s'') = \alpha(\mu)(s'')$ for all $s'' \in S'$ and some $\mu \in Sat(\varphi)$, and by the same reasoning as above, $\mu \Subset_{\mathcal{R}'} \mu'$.
   (d) If $L(s,a,\varphi) = ?$: Similar to the above case.
3. By Definition 9, it is easy to see that $V(s) \subseteq V'(s')$.

Trivially, the initial states s_0 and $\alpha(s_0)$ are related, so we conclude that $\mathcal{R}$ is a weak refinement relation.

F.3 Proof of Theorem 4

Let N, N', and N'' be action-deterministic consistent APAs. It holds that $\beta^*(N \wedge N') \preceq N$, $\beta^*(N \wedge N') \preceq N'$, and, if $N'' \preceq N$ and $N'' \preceq N'$, then $N'' \preceq \beta^*(N \wedge N')$.

Proof. Let $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A, L', AP, V', s'_0)$ and $N'' = (S'', A, L'', AP, V'', s''_0)$ be three APAs. Let $N \wedge N' = (S \times S', A, \tilde{L}, AP, \tilde{V}, (s_0, s'_0))$ be the conjunction of N and N' defined as above.

(1) We first show that $\beta^*(N \wedge N') \preceq_S N$. Obviously, if $N \wedge N'$ is fully inconsistent, then $\beta^*(N \wedge N')$ is empty and refines N with the empty refinement relation. Suppose now that $\beta^*(N \wedge N') = (T, A, L^T, AP, V^T, (s_0, s'_0))$, with $T \subseteq S \times S'$, is not empty. Define the relation $\mathcal{R} \subseteq T \times S$ such that for all $s, t \in S$ and $s' \in S'$, $(s, s') \mathcal{R} t$ iff $s = t$. We show that $\mathcal{R}$ is a (strong) refinement relation. Let $(s, s') \in T$ such that $(s, s') \mathcal{R} s$.

1. Let $a \in A$ and $\varphi \in C(S)$ such that $L(s, a, \varphi) = \top$. Since $(s, s') \in T$, we know that there exists $\varphi' \in C(S')$ such that $L'(s', a, \varphi') \neq \bot$. Thus define $\tilde{\varphi} \in C(S \times S')$ such that $\tilde{\mu} \in Sat(\tilde{\varphi})$ iff
   - the distribution $\mu : s \in S \mapsto \sum_{s' \in S'} \tilde{\mu}((s, s'))$ is in $Sat(\varphi)$, and
   - the distribution $\mu' : s' \in S' \mapsto \sum_{s \in S} \tilde{\mu}((s, s'))$ is in $Sat(\varphi')$.

   By definition of $N \wedge N'$, we have that $\tilde{L}((s, s'), a, \tilde{\varphi}) = \top$. Consider now $\varphi^T \in C(T)$ the constraint such that $\mu^T \in Sat(\varphi^T)$ iff there exists $\tilde{\mu} \in Sat(\tilde{\varphi})$ such that $\forall t \in T, \mu^T(t) = \tilde{\mu}(t)$ and $\forall t \in S \setminus T, \tilde{\mu}(t) = 0$. According to the definition of pruning, we know that $L^T((s, s'), a, \varphi^T) = \sqcup_{\psi \in \bar{\varphi^T}^{(s,s'),a}} \tilde{L}((s, s'), a, \psi)$.
   Since $\tilde{\varphi} \in \bar{\varphi^T}^{(s,s'),a}$, it holds that $L^T((s, s'), a, \varphi^T) = \top$.
   Thus there exists $\varphi^T \in C(T)$ such that $L^T((s, s'), a, \varphi^T) = \top$. Then, define the correspondence function $\delta : T \to (S \to [0, 1])$ such that $\delta((t, t'), t'') = 1$ iff $t'' = t$. Let $\mu^T \in Sat(\varphi^T)$, $\tilde{\mu}$ the corresponding distribution in $Sat(\tilde{\varphi})$, and μ the distribution such that $\mu : t \in S \mapsto \sum_{t' \in S'} \tilde{\mu}((t, t'))$. By definition, μ is in $Sat(\varphi)$. We now show that $\mu^T \Subset^{\delta}_{\mathcal{R}} \mu$.
   - For all $(t, t') \in T$, $\delta((t, t'))$ is a distribution on S by definition.
   - Let $t \in S$.

$$\begin{aligned}
\sum_{(t,t'') \in T} \mu^T((t', t'')) \cdot \delta((t', t''), t) &= \sum_{t' \in S' | (t,t') \in T} \mu^T((t, t')) \quad \text{(By Def of } \delta\text{)} \\
&= \sum_{t' \in S' | (t,t') \in T} \tilde{\mu}((t, t')) \quad \text{(By Def of } \mu^T\text{)} \\
&= \sum_{t' \in S'} \tilde{\mu}((t, t')) \quad \text{(By Def of } \mu^T\text{)} \\
&= \mu(t) \quad \text{(By Def of } \mu\text{)}
\end{aligned}$$

   - Finally, if $\delta((t, t'), t'') > 0$, then $t = t''$ and $(t, t') \mathcal{R} t$ by definition.

   Thus $\mu^T \Subset^{\delta}_{\mathcal{R}} \mu$.
2. Let $a \in A$ and $\varphi^T \in C(T)$ such that $L^T((s, s'), a, \varphi^T) \neq \bot$. By definition of L^T, there exists $\tilde{\varphi} \in \bar{\varphi^T}^{t,a}$. Thus, $\tilde{L}((s, s'), a, \tilde{\varphi} \neq \bot$ in $N \wedge N'$, and a distribution μ^T satisfies φ^T iff there exists a distribution $\tilde{\mu} \in Sat(\tilde{\varphi})$ such that $\mu^T(t) = \tilde{\mu}(t)$ for all $t \in T$ and $\tilde{mu}(t) = 0$ for all $t \in S \times S' \setminus T$. Since T contains only consistent states, there exists $\mu^T \in Sat(\varphi^T)$. Let $\tilde{\mu} \in Sat(\tilde{\varphi})$

be a corresponding distribution in $\tilde{\varphi}$. By definition of $\tilde{L}$, there must exist $\varphi \in C(S)$ and $\varphi' \in C(S')$ such that $L(s,a,\varphi) \neq \bot$ and $L'(s',a,\varphi') \neq \bot$. Moreover, $\tilde{\rho} \in Sat(\tilde{\varphi})$ iff the distributions $\rho : t \in S \mapsto \sum_{t' \in S'} \tilde{\rho}((t,t'))$ and $\rho' : t' \in S' \mapsto \sum_{t \in S} \tilde{\rho}((t,t'))$ 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 $\delta : T \to (S \to [0,1])$ such that $\delta((t,t'),t'') = 1$ iff $t'' = t$. We now show that $\mu^T \Subset^{\delta}_{\mathcal{R}} \mu$.

- For all $(t,t') \in T$, $\delta((t,t'))$ is a distribution on S by definition.
- Let $t \in S$.

$$\begin{aligned}\sum_{(t,t'') \in T} \mu^T((t',t'')) \cdot \delta((t',t''),t) &= \sum_{t' \in S' | (t,t') \in T} \mu^T((t,t')) \quad \text{(By Def of } \delta\text{)} \\ &= \sum_{t' \in S' | (t,t') \in T} \tilde{\mu}((t,t')) \quad \text{(By Def of } \mu^T\text{)} \\ &= \sum_{t' \in S'} \tilde{\mu}((t,t')) \quad \text{(By Def of } \mu^T\text{)} \\ &= \mu(t) \quad \text{(By Def of } \mu\text{)}\end{aligned}$$

- Finally, if $\delta((t,t'),t'') > 0$, then $t = t''$ and $(t,t')\,\mathcal{R}\,t$ by definition.

Thus $\mu^T \Subset^{\delta}_{\mathcal{R}} \mu$.
Finally, there exists $\varphi \in C(S)$ such that $L(s,a,\varphi) \neq \bot$ and there exists a correspondence function δ such that for all $\mu^T \in Sat(\varphi^T)$, there exists $\mu \in Sat(\varphi)$ such that $\mu^T \Subset^{\delta}_{\mathcal{R}} \mu$.

3. By definition, $V^T((s,s')) = \tilde{V}((s,s')) = V(s) \cap V'(s') \subseteq V(s)$.

Finally, $\mathcal{R}$ is a (strong) refinement relation, and we have $\beta^*(N \wedge N') \preceq_S N$.

(2) By a similar proof, we obtain that $\beta^*(N \wedge N') \preceq_S N'$.

(3) We finally prove that if $N'' \preceq N$ and $N'' \preceq N'$, then $N'' \preceq \beta^*(N \wedge N')$.

Let $\mathcal{R} \subseteq S'' \times S$ and $\mathcal{R}' \subseteq S'' \times S'$ be the refinement relations such that $N'' \preceq N$ and $N'' \preceq N'$. Obviously, if $N \wedge N'$ is fully inconsistent, then $\beta^*(N \wedge N')$ is empty. In this case, there are no consistent APAs refining both N and N'. As a consequence, N'' is inconsistent, which violates the hypothesis. Suppose now that $\beta^*(N \wedge N') = (T, A, L^T, AP, V^T, (s_0, s'_0))$, with $T \subseteq S \times S'$, is not empty. Define the relation $\mathcal{R}^T \subseteq S'' \times T$ such that $s''\,\mathcal{R}^T(s,s') \in T$ iff $s''\,\mathcal{R}\,s \in S$ and $s''\,\mathcal{R}'\,s' \in S'$. We prove that $\mathcal{R}^T$ is a (weak) refinement relation.

Let $s \in S, s' \in S'$ and $s'' \in S''$ such that $s''\,\mathcal{R}^T(s,s')$.

1. Let $a \in A$ and $\varphi^T \in C(T)$ such that $L^T((s,s'),a,\varphi^T) = \top$. By definition, we have $\tilde{L}((s,s'),a,\tilde{\varphi}) = \top$ with $\tilde{\varphi} \in C(S \times S')$ such that $\mu^T \in Sat(\varphi^T)$ iff there exists $\tilde{\mu} \in Sat(\tilde{\varphi})$ such that $\mu^T(t) = \tilde{\mu}(t)$ for all $t \in T$ and $\tilde{\mu}(t) = 0$ for all $t \in S \times S' \setminus T$.
   By definition of $\tilde{L}$, there must exist $\varphi \in C(S)$ and $\varphi' \in C(S')$ such that either $L(s,a,\varphi) = \top$ and $L'(s',a,\varphi') \neq \bot$ or $L(s,a,\varphi) \neq \bot$ and $L'(s',a,\varphi') = \top$. Suppose the former holds. Since $L(s,a,\varphi) = \top$ and $s''\,\mathcal{R}\,s$, 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 $\mu'' \Subset_{\mathcal{R}} \mu$ (1).
Since $L''(s'', a, \varphi'') = \top$ and $s'' \mathcal{R}' s'$, there exists $\rho' \in C(S')$ such that $L'(s', a, \rho') \neq \bot$ and for all $\mu'' \in Sat(\varphi'')$, there exists $\mu' \in Sat(\rho')$ such that $\mu'' \Subset_{\mathcal{R}'} \mu'$ (2). **By action-determinism of N', we have** $\rho' = \varphi'$.
Let $\mu'' \in Sat(\varphi'')$. By (1) and (2), there exists $\mu \in Sat(\varphi)$ and $\mu' \in Sat(\varphi')$ such that $\mu'' \Subset_{\mathcal{R}} \mu$ and $\mu'' \Subset_{\mathcal{R}'} \mu'$. Since (s, s') and s'' are consistent, remark that for all t, t' in $S \times S' \setminus T$, we cannot have $s'' \mathcal{R} t$ and we cannot have $s'' \mathcal{R} t'$ (3).
We now build $\mu^T \in Sat(\varphi^T)$ such that $\mu \Subset_{\mathcal{R}''} \mu^T$. Let μ^T be the distribution on T such that for all $(t, t') \in T$, $\mu^T((t, t')) = \mu(t) \cdot \mu'(t')$. Again, since (s, s') and s'' are consistent, we have that $\forall (t, t') \in S \times S' \setminus T$, $\mu(t) = \mu'(t') = 0$. Thus μ^T is indeed a distribution, and by definition of $\tilde{\varphi}$ and φ^T, we have that $\mu^T \in Sat(\varphi^T)$. Let δ and δ' be the correspondance functions such that $\mu'' \Subset^{\delta}_{\mathcal{R}} \mu$ and $\mu'' \Subset^{\delta'}_{\mathcal{R}'} \mu'$. Define the correspondance function $\delta'' : S'' \to (T \to [0, 1])$ such that for all $t'' \in S''$ and $(t, t') \in T$, $\delta''(t'', (t, t')) = \delta(t'', t) \cdot \delta'(t'', t')$. We now prove that $\mu'' \Subset^{\delta''}_{\mathcal{R}''} \mu^T$.

- For all $t'' \in S''$, if $\mu''(t'') > 0$, both $\delta(t'')$ and $\delta'(t'')$ are distributions. By (3), we know that for all $(t, t') \in S \times S' \setminus T$, $\delta(t'', t) = \delta'(t'', t') = 0$. As a consequence, $\delta''(t'')$ is a distribution on T.
- Define $\rho^T(t, t') = \sum_{t'' \in S''} \mu''(t'') \cdot \delta''(t'', (t, t'))$. We prove that, for all $(t, t') \in T$, we have $\rho^T(t, t') = \mu^T(t, t')$.
  - Let $t' \in S'$, we have

$$\begin{aligned}
\sum_{t \in S | (t,t') \in T} \rho(t, t') &= \sum_{t \in S | (t,t') \in T} \sum_{t'' \in S''} \mu''(t'') \cdot \delta''(t'', (t, t')) \\
&= \sum_{t \in S | (t,t') \in T} \sum_{t'' \in S''} \mu''(t'') \cdot \delta(t'', t) \cdot \delta'(t'', t') \\
&= \sum_{t'' \in S''} \mu''(t'') \cdot \delta'(t'', t') \cdot \sum_{t \in S | (t,t') \in T} \delta(t'', t) \\
&= \sum_{t'' \in S''} \mu''(t'') \cdot \delta'(t'', t') \\
&= \mu'(t') \text{ by definition.}
\end{aligned}$$

  - Let $t \in S$, we have

$$\begin{aligned}
\sum_{t' \in S' | (t,t') \in T} \rho(t, t') &= \sum_{t' \in S' | (t,t') \in T} \sum_{t'' \in S''} \mu''(t'') \cdot \delta''(t'', (t, t')) \\
&= \sum_{t' \in S | (t,t') \in T} \sum_{t'' \in S''} \mu''(t'') \cdot \delta(t'', t) \cdot \delta'(t'', t') \\
&= \sum_{t'' \in S''} \mu''(t'') \cdot \delta(t'', t) \cdot \sum_{t' \in S' | (t,t') \in T} \delta'(t'', t') \\
&= \sum_{t'' \in S''} \mu''(t'') \cdot \delta(t'', t) \\
&= \mu(t) \text{ by definition.}
\end{aligned}$$

Thus we have that for all $(t,t') \in T$, $\rho = \mu^T$.

As a consequence, for all $(t,t') \in T$, $\sum_{t'' \in S''} \mu''(t'') \cdot \delta''(t'',(t,t')) = \mu^T(t,t')$.

- If $\delta''(t'',(t,t')) > 0$, then by definition $\delta(t'',t) > 0$ and $\delta'(t'',t') > 0$. As a consequence, $t'' \mathcal{R}\, t$ and $t'' \mathcal{R}'\, t'$, thus $t'' \mathcal{R}''(t,t')$.

Finally, $\mu'' \Subset_{\mathcal{R}''} \mu^T$.

2. Let $a \in A$ and $\varphi'' \in C(S'')$ such that $L''(s'',a,\varphi'') \neq \bot$. Since $s'' \mathcal{R}\, s$ and $s'' \mathcal{R}'\, s'$, there must exist $\varphi \in C(S)$ and $\varphi' \in C(S')$ such that both $L(s,a,\varphi) \neq \bot$ and $L'(s',a,\varphi') \neq \bot$. As a consequence, $\tilde{L}((s,s'),a,\tilde{\varphi}) \neq \bot$, with $\tilde{\varphi} \in C(S \times S')$ such that $\tilde{\rho} \in Sat(\tilde{\varphi})$ iff the distributions $\rho : t \in S \mapsto \sum_{t' \in S'} \tilde{\rho}((t,t'))$ and $\rho' : t' \in S' \mapsto \sum_{t \in S} \tilde{\rho}((t,t'))$ are respectively in $Sat(\varphi)$ and in $Sat(\varphi')$. Moreover, since s'' and (s,s') are consistent, there exists $\varphi^T \in C(T)$ such that $L^T((s,s'),a,\varphi^T) \neq \bot$ and $\rho^T \in Sat(\varphi^T)$ iff there exists $\tilde{\rho} \in Sat(\tilde{\varphi})$ such that $\rho^T(t,t') = \tilde{\rho}(t,t')$ for all $(t,t') \in T$ and $\tilde{\rho}(t,t') = 0$ for all $(t,t') \in S \times S' \setminus T$.

Let $\mu'' \in Sat(\varphi'')$. We prove that there exists $\mu^T \in Sat(\varphi^T)$ such that $\mu'' \Subset_{\mathcal{R}''} \mu^T$. By definition of φ and φ', we know that there exist $\mu \in Sat(\varphi)$ and $\mu' \in Sat(\varphi')$ such that $\mu'' \Subset_{\mathcal{R}} \mu$ and $\mu'' \Subset_{\mathcal{R}'} \mu'$. Let δ and δ' the correspondance functions such that $\mu'' \Subset^{\delta}_{\mathcal{R}} \mu$ and $\mu'' \Subset^{\delta'}_{\mathcal{R}'} \mu'$. Let $\tilde{\mu}$ the distribution on $S \times S'$ such that for all $(t,t') \in S \times S'$, $\tilde{mu}(t,t') = \mu(t) \cdot \mu'(t')$. By definition, we have that $\tilde{\mu} \in Sat(\tilde{\varphi})$. Moreover, since s'' and (s,s') are consistent, we know that (1) for all $(t,t') \in S \times S' \setminus T$, we have $\mu(t) = \mu'(t') = 0$ and (2) for all $t'' \in S''$ and $(t,t') \in S \times S' \setminus T$, we cannot have $t'' \mathcal{R}\, t$ and we cannot have $t'' \mathcal{R}'\, t'$. Define μ^T the distribution on T such that for all $(t,t') \in T$, $\mu^T(t,t') = \tilde{\mu}(t,t')$. By (1), μ^T is indeed a distribution, and $\mu^T \in Sat(\varphi^T)$. Define the correspondance function $\delta'' : S'' \to (T \to [0,1])$ such that for all $t'' \in S''$ and $(t,t') \in T$, $\delta''(t'',(t,t')) = \delta(t'',t) \cdot \delta'(t'',t')$. We now prove that $\mu'' \Subset^{\delta''}_{\mathcal{R}''} \mu^T$.

- For all $t'' \in S''$, if $\mu''(t'') > 0$, both $\delta(t'')$ and $\delta'(t'')$ are distributions. By (2), we know that for all $(t,t') \in S \times S' \setminus T$, $\delta(t'',t) = \delta'(t'',t') = 0$. As a consequence, $\delta''(t'')$ is a distribution on T.
- Define $\rho^T(t,t') = \sum_{t'' \in S''} \mu''(t'') \cdot \delta''(t'',(t,t'))$. We prove that, for all $(t,t') \in T$, we have $\rho^T(t,t') = \mu^T(t,t')$.
  - Let $t' \in S'$, we have

$$\begin{aligned}
\sum_{t \in S | (t,t') \in T} \rho(t,t') &= \sum_{t \in S | (t,t') \in T} \sum_{t'' \in S''} \mu''(t'') \cdot \delta''(t'',(t,t')) \\
&= \sum_{t \in S | (t,t') \in T} \sum_{t'' \in S''} \mu''(t'') \cdot \delta(t'',t) \cdot \delta'(t'',t') \\
&= \sum_{t'' \in S''} \mu''(t'') \cdot \delta'(t'',t') \cdot \sum_{t \in S | (t,t') \in T} \delta(t'',t) \\
&= \sum_{t'' \in S''} \mu''(t'') \cdot \delta'(t'',t') \\
&= \mu'(t') \text{ by definition.}
\end{aligned}$$

- Let $t \in S$, we have

$$\begin{aligned}\sum_{t' \in S' | (t,t') \in T} \rho(t,t') &= \sum_{t' \in S' | (t,t') \in T} \sum_{t'' \in S''} \mu''(t'') \cdot \delta''(t'', (t,t')) \\ &= \sum_{t' \in S | (t,t') \in T} \sum_{t'' \in S''} \mu''(t'') \cdot \delta(t'', t) \cdot \delta'(t'', t') \\ &= \sum_{t'' \in S''} \mu''(t'') \cdot \delta(t'', t) \cdot \sum_{t' \in S' | (t,t') \in T} \delta'(t'', t') \\ &= \sum_{t'' \in S''} \mu''(t'') \cdot \delta(t'', t) \\ &= \mu(t) \text{ by definition.}\end{aligned}$$

  Thus we have that for all $(t,t') \in T$, $\rho = \mu^T$.

  As a consequence, for all $(t,t') \in T$, $\sum_{t'' \in S''} \mu''(t'') \cdot \delta''(t'', (t,t')) = \mu^T(t,t')$.

  – If $\delta''(t'', (t,t')) > 0$, then by definition $\delta(t'', t) > 0$ and $\delta'(t'', t') > 0$. As a consequence, $t'' \mathcal{R} t$ and $t'' \mathcal{R}' t'$, thus $t'' \mathcal{R}''(t,t')$.

  Finally, $\mu'' \Subset_{\mathcal{R}''} \mu^T$.

3. Since $s'' \mathcal{R} s$, we know that $V''(s'') \subseteq V(s)$. Moreover, since $s'' \mathcal{R}' s'$, we also have $V''(s'') \subseteq V'(s')$. As a consequence, we obviously have $V''(s'') \subseteq V(s) \cap V'(s') = V^T((s,s'))$.

   Finally, $\mathcal{R}''$ is indeed a (weak) refinement relation between N'' and $\beta^*(N \wedge N')$. Moreover, we know that $s''_0 \mathcal{R} s_0$, $s''_0 \mathcal{R} s'_0$, and (s_0, s'_0) is consistent. As a consequence $s''_0 \mathcal{R}''(s_0, s'_0)$ and $N'' \preceq \beta^*(N \wedge N')$.

F.4 Proof of Theorem 5

Let $N_i = (S_i, A_i, L_i, AP_i, V_i, s_0^i)$ and $N'_i = (S'_i, A'_i, L'_i, AP'_i, V'_i, s_0^{i'})$ be APAs with for $i = 1, 2$ with $AP_1 \cap AP_2 = \emptyset$ and $AP'_1 \cap AP'_2 = \emptyset$. Let $\bar{A} \subseteq (A_1 \cap A_2) \bigcap (A_{1'} \cap A'_2)$. If $N_1 \preceq N_{1'}$ and $N_2 \preceq N'_2$, then we have $N_1 \| _{\bar{A}} N_2 \preceq N'_1 \| _{\bar{A}} N'_2$. Consequently, for PAs P and P', if $P \models N_1$ and $P' \models N_2$, then $P \| _{\bar{A}} P' \models N_1 \| _{\bar{A}} N_2$.

Proof. 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 $N_1 \| _{\bar{A}} N_2 = (S_1 \times S_2, A_1 \cup A_2, L, AP_1 \cup AP_2, V, (s_0^1, s_0^2))$ and $N'_1 \| _{\bar{A}} N'_2 = (S'_1 \times S'_2, A'_1 \cup A'_2, L', AP'_1 \cup AP'_2, V, (s_0^{1'}, s_0^{2'}))$.

Define the relation $\mathcal{R} \subseteq (S_1 \times S_2) \times (S'_1 \times S'_2)$ 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 $N_1 \| _{\bar{A}} N_2 \preceq N'_1 \| _{\bar{A}} N'_2$.

Assume that $(s_1, s_2) \mathcal{R} (s'_1, s'_2)$.

– Let $a \in A'_1 \cup A'_2$ and $\varphi' \in C(S'_1 \times S'_2)$ such that $L'((s'_1, s'_2), a, \varphi') = \top$. There are three cases:
  - If $a \in \bar{A}$, 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 $\mu' = \mu'_1 \cdot \mu'_2$. 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 $Sat(\varphi) = Sat(\varphi_1) \cdot Sat(\varphi_2)$. By definition of $N_1 \|_{\bar{A}} N_2$, 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 $\mu = \mu_1 \cdot \mu_2$. 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 $\mu' = \mu_1' \cdot \mu_2'$. By construction, $\mu' \in Sat(\varphi')$. We now prove that $\mu \Subset^{\delta}_{\mathcal{R}} \mu'$:

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

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

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

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

3. 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 $a \in A_1' \setminus \bar{A}$: 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 $N_1 \|_{\bar{A}} N_2$, 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 else. 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 $\mu \Subset^{\delta}_{\mathcal{R}} \mu'$:

1. 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 $S'_1 \times S'_2$.
2. Let $(u',v') \in S'_1 \times S'_2$, with $v' \neq s'_2$.

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

   Let $u' \in S'_1$, we have

$$\begin{aligned}\sum_{(u,v) \in S_1 \times S_2} \mu(u,v) \cdot \delta(u,v)(u',s'_2) &= \sum_{u \in S_1} \sum_{v = s_2} \mu(u,v) \cdot \delta(u,v)(u',s'_2) \\ &= \sum_{u \in S_1} \mu_1(u) \cdot \delta_1(u,u') \\ &= \mu'(u',v').\end{aligned}$$

   3. 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 $a \in A'_2 \setminus \bar{A}$, the proof is similar.

– 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 $a \in \bar{A}$, then there exists $\varphi_1 \in C(S_1)$ and $\varphi_2 \in C(S_2)$ such that $L_1(s_1,a,\varphi_1) \geq ?$, $L_2(s_2,a,\varphi_2) \geq ?$, and $\mu \in Sat(\varphi)$ iff there exist $\mu_1 \in Sat(\varphi_1)$ and $\mu_2 \in Sat(\varphi_2)$ such that $\mu = \mu_1 \cdot \mu_2$. 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 $L'_1(s'_1,a,\varphi'_1) \geq ?$, $L'_2(s'_2,a,\varphi'_2) \geq ?$, 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 $Sat(\varphi') = Sat(\varphi'_1) \cdot Sat(\varphi'_2)$. By definition of $N'_1 \|_{\bar{A}} N'_2$, we have $L'((s'_1, s'_2), a, \varphi') \geq ?$. 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 $\mu = \mu_1 \cdot \mu_2$. 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, that the distribution μ' o, $S'_1 \times S'_2$ constructed as $\mu' = \mu'_1 \cdot \mu'_2$ is in $Sat(\varphi')$ and gives that $\mu \Subset^{\delta}_{\mathcal{R}} \mu'$.

- If $a \in A'_1 \setminus \bar{A}$, then there exists $\varphi_1 \in C(S_1)$ such that $L_1(s_1, a, \varphi_1) \geq ?$. Since $s_1 \mathcal{R}_1 s'_1$, there exists $\varphi'_1 \in C(S'_1)$ with $L'_1(s'_1, a, \varphi'_1) \geq ?$ 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 $N'_1 \|_{\bar{A}} N'_2$, we have $L'((s'_1, s'_2), a, \varphi') \geq ?$. 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', $\delta(u,v)(u',v') = \delta(u)(u')$ if $v = s_2$ and $v' = s'_2$, and 0 else. 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 $a \in A'_2 \setminus \bar{A}$, the proof is similar.

– 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 $(s^1_0, s^2_0)\, \mathcal{R}(s^{1'}_0, s^{2'}_0)$, since $s^1_0 \mathcal{R}_1 s^{1'}_0$ and $s^2_0 \mathcal{R}_2 s^{2'}_0$, we conclude that $\mathcal{R}$ is a weak refinement relation.

F.5 Proof of Theorem 6

Proof. Let $M = (S, A, L, AP, V, s_0)$ and $N = (S'', A'', L'', AP'', V'', s''_0)$ be APAs and let $\bar{A} \subseteq A \cap A''$ be a synchronization set such that the parallel composition of M and N is given as $M \|_{\bar{A}} N = (S \times S'', A \cup A'', \tilde{L}, AP \cup AP'', \tilde{V}, (s_0, s''_0))$.

Let $\alpha_1 : S \to S'$ and $\alpha_2 : S'' \to S'''$. Let $\alpha_1(M) = (S', A, L', AP, V', \alpha(s_0))$, $\alpha_2(N) = (S''', A'', L''', AP'', V''', \alpha(s''_0))$ and $(\alpha_1 \times \alpha_2)(M \|_{\bar{A}} N) = (S' \times S''', A \cup A'', \tilde{L}', AP \cup AP'', \tilde{V}', (\alpha(s_0), \alpha(s''_0)))$ be the induced APA. Let $\alpha_1(M) \|_{\bar{A}} \alpha_2(N) = (S' \times S''', A \cup A'', \tilde{L}'', AP \cup AP'', \tilde{V}'', (\alpha(s_0), \alpha(s''_0)))$

Notice that the signatures of $\alpha_1(M) \|_{\bar{A}} \alpha_2(N)$ and $(\alpha_1 \times \alpha_2)(M \|_{\bar{A}} N)$ only differs on constraint function and valuation function. We establish the result, by

proving that for all $(s', s''') \in S' \times S'''$, $a \in A \cup A''$, and $\varphi \in C(S' \times S''')$, that $\tilde{V}'(s', s''') = \tilde{V}''(s', s''')$ 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 $\alpha_1(M) \|_{\bar{A}} \alpha_2(N)$ 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 $a \in \bar{A}$ 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

$$Sat(\tilde{\varphi}') = (\alpha_1 \times \alpha_2) \left(\bigcup_{\substack{(s,s'') \in (\gamma_1 \times \gamma_2)(s', s'''), \\ \exists \varphi_{M\|N} \in C(S \times S''): L((s,s''), a, \varphi_{M\|N}) = \top}} Sat(\varphi) \right). \quad (3)$$

  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. $\mu_{M\|N}(u, v) = \mu_M(u) \cdot \mu_N(v)$ 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,

$$Sat(\varphi_{\alpha_1(M)}) = \alpha_1(\bigcup\nolimits_{s \in \gamma_1(s'), \exists \varphi_M \in C(S): L(s,a,\varphi_M) = \top} Sat(\varphi_M)) \quad (4)$$

$$Sat(\varphi_{\alpha_2(N)}) = \alpha_2(\bigcup\nolimits_{s'' \in \gamma_1(s'''), \exists \varphi_N \in C(S): L(s'',a,\varphi_N) = \top} Sat(\varphi_N))$$

  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. $\mu_{\alpha_1(M)\|\alpha_2(N)}(u, v) = \mu_{\alpha_1(M)}(u) \cdot \mu_{\alpha_2(N)}(v)$ 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 $a \notin \bar{A}$ (wlog. $a \in A \setminus \bar{A}$) 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 3.
  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 4. 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 $\tilde{L}'((s', s'''), a, \tilde{\varphi}') =?$.

F.6 Proof of Theorem 8

We first propose the following tranformation from APA to CMC.

Definition 20. *Let $N = (S, A, L, AP, V, s_0)$ be a deterministic APA such that $AP \cap A = \emptyset$. Let ϵ be a fresh variable. The CMC corresponding to N is $\widehat{N} = \langle \widehat{Q}, \widehat{q_0}, \psi, \widehat{A}, \widehat{V} \rangle$, 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*
- ψ *is such that*
  - *For all* $(s, \epsilon) \in \widehat{Q}$, $\psi((s, \epsilon))(\pi) = 1$ *iff*

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

  - *For all* $a \in A$ *and* $(s, a) \in \widehat{Q}$, $\psi((s, a))(\pi) = 1$ *iff (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* $\pi' \in Sat(\varphi)$.

The proof consists of two parts:

1. Let $N = (S, A, L, AP, V, s_0)$ be a deterministic APA such that $AP \cap A = \emptyset$. Let $\widehat{N}$ be the CMC corresponding to N using the transformation presented in Definition 20. We have the following: For all MC M, $M \models_{MC} N \iff M \models \widehat{N}$.
2. Let $N = (S, A, L, AP, V, s_0)$ be an APA. If N is deterministic and in single valuation normal form, then we have that $\widehat{N}$ is a deterministic CMC in single valuation normal form.

For point 2, it is required to have both actions and valuations determinism on the original APA in order to have determinism on the CMC. The rest of the proof is obvious. What remains is to present the proof of point 1.

Proof. $\Rightarrow$**:** Let $M = \langle Q, q_0, \pi, A_M, V_M \rangle$ be a Markov Chain. We first prove that if $M \models_{MC} N$, then $M \models \widehat{N}$. 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 $\widehat{N} = \langle \widehat{Q}, \widehat{q_0}, \psi, \widehat{A}, \widehat{V} \rangle$ be the transformation of N following Definition 20.

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 $\mathcal{R}^{PA} \subseteq S_P \times S$ be the satisfaction relation witnessing $P \models M$. 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 $p \,\mathcal{R}^{PA}\, s$, 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 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 $p \,\mathcal{R}^{PA}\, s$.

- By $\mathcal{R}^{MC}$, we have that $V_M(q) = V_P(p)$. By $\mathcal{R}^{PA}$, we know that $V_P(p) \in V(s)$. Since $\widehat{V}((s, \epsilon)) = V(s)$, we have, $V_M(q) \in \widehat{V}((s, \epsilon))$.
- Let δ be a correspondance 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 else.
  - 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 $V_M(q') = V(p) \cup \{a\}$, $L_P(p, a, \rho) = \top$ and $\pi(q') \Subset_{\mathcal{R}^{MC}} \rho$. 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 $\gamma = \pi(q) \times \delta$. 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,

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

∗ 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,

$$\forall s' \neq s, b \in A \cup \{\epsilon\},\ \gamma((s', b)) = \sum_{q' \in Q} \pi(q)(q') \cdot \delta(q', (s', b)) = 0.$$

∗ 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 $L_P(p, a, \rho) = \top$ and there exists $\mu \in Sat(\varphi)$ such that $\rho \Subset_{\mathcal{R}^{AP}} \mu$. 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 $\pi(q') \Subset_{\mathcal{R}^{MC}} \rho$. By definition of δ, we have that $\delta(q', (s, a)) > 0$. As a consequence,

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

∗ 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 $L_P(p, a, \rho) = \top$ and $\pi(q') \Subset_{\mathcal{R}^{MC}} \rho$. Thus, by $\mathcal{R}^{PA}$, 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 $q'\,\mathcal{R}(s, \epsilon)$.

– Since $q'\,\mathcal{R}(s, \epsilon)$, we know that there exists $p \in S_P$ such that $q'\,\mathcal{R}^{MC}\,p$ and $p\,\mathcal{R}^{PA}\,s$. 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 $V_M(q) \in \widehat{V}((s, a))$.
– Since $q'\,\mathcal{R}^{MC}\,p$ and $\pi(q')(q) > 0$, there exists a distribution ρ over S_P such that $L_P(p, a, \rho) = \top$ and there exists a correspondance function δ^{MC} such that $\pi(q) \Subset^{\delta^{MC}}_{\mathcal{R}^{MC}} \rho$. Moreover, since $p\,\mathcal{R}^{PA}\,s$, there exists $\varphi \in C(S)$ such that $L(s, a, \varphi) \neq \bot$, and there exist $\mu \in Sat(\varphi)$ and a correspondance fucntion δ^{PA} such that $\rho \Subset^{\delta^{PA}}_{\mathcal{R}^{PA}} \mu$.

Define the correspondance function $\delta : Q \to (\widehat{Q} \to [0,1])$ such that for all $q'' \in Q$ and $s'' \in S$,

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

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

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

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

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

    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) $\delta^{PA}(p'', s'') > 0$. By (1), we have $q'' \,\mathcal{R}^{MC}\, p''$ and by (2), we have $p'' \,\mathcal{R}^{PA}\, s''$. 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 trivially have that $q_0 \,\mathcal{R}(s_0, \epsilon)$, which gives that $M \models_{MC} \widehat{N}$.

$\Leftarrow$: Let $M = \langle Q, q_0, \pi, A_M, V_M \rangle$ be a Markov Chain. We prove that if $M \models \widehat{N}$, then $M \models_{MC} N$, i.e. there exists a PA P such that M satisfies P and $P \models N$. Let $\widehat{N} = \langle \widehat{Q}, \widehat{q_0}, \psi, \widehat{A}, \widehat{V} \rangle$ be the transformation of N following Definition 20.
Let $\mathcal{R}$ be the satisfaction relation for CMCs witnessing that $M \models \widehat{N}$. 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, $L(s, a, \rho) = \top$ iff there exists $q' \in Q_N$ such that

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

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

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 correspondance function $\delta : Q \to (\widehat{N} \to [0, 1])$ such that $\pi(q) \times \delta$ 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 $L_P(q, a, \rho) = \top$ with $\rho = \pi(q')$. Moreover, since $\delta(q', (s, a)) > 0$, we have that $q'\,\mathcal{R}(s, a)$. Thus, there exists a correspondance function $\delta' : Q \to (\widehat{Q} \to [0, 1])$ such that $\pi(q') \times \delta'$ satisfies $\psi((s, a))$, i.e. the distribution $\gamma' : s' \in S \mapsto [\pi(q') \times \delta'](s', \epsilon)$ 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 correspondance function between P and S such that for all $p' \in S_P$ and $s' \in S$, $\delta^{PA}(p', s') = \delta'(p', (s', \epsilon))$. 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 correspondance function by construction.
   Moreover, we have that $\rho \times \delta^{PA} \in Sat(\varphi)$, and, for all p', s' such that $\delta^{PA}(p', s') > 0$, we have that $\delta'(p', (s', \epsilon)) > 0$. So, by $\mathcal{R}$, we have $p'\,\mathcal{R}(s', \epsilon)$, and thus $p'\,\mathcal{R}^{PA}\,s'$.

Finally, we have that there exists ρ such that $L_P(q,a,\rho) = \top$, and there exists $\gamma' = \rho \times \delta^{PA} \in Sat(\varphi)$ such that $\rho \Subset^{\delta^{PA}}_{\mathcal{R}^{PA}} \gamma'$.

2. Let $a \in A$ and $\rho \in Dist(S_P)$ such that $L_P(q,a,\rho) = \top$. By construction, there exists $q' \in Q_N$ such that $\pi(q)(q') > 0$, $V_M(q') = V_M(q) \cup \{a\}$ and $\rho = \pi(q')$.
   Since $q\,\mathcal{R}(s,\epsilon)$, we have that there exists δ such that $\pi(q) \times \delta$ 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 $\pi(q) \times \delta$ 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 $\pi(q') \times \delta'$ satisfies $\psi((s,a))$, i.e. the distribution $\gamma' : s' \in S \mapsto [\pi(q') \times \delta'](s',\epsilon)$ is such that there exists φ such that $L(s,a,\varphi) \neq \bot$ and $\gamma' \in Sat(\varphi)$. Let δ^{PA} be the correspondance function between P and S such that for all $p' \in S_P$ and $s' \in S$, $\delta^{PA}(p',s') = \delta'(p',(s',\epsilon))$. 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 correspondance function by construction.
   Moreover, we have that $\rho \times \delta^{PA} \in Sat(\varphi)$, and, for all p', s' such that $\delta^{PA}(p',s') > 0$, we have that $\delta'(p',(s',\epsilon)) > 0$. So, by $\mathcal{R}$, we have $p'\,\mathcal{R}(s',\epsilon)$, and thus $p'\,\mathcal{R}^{PA}\,s'$.
   Finally, there exists $\varphi \in C(S)$ such that $L(s,a,\varphi) \neq \bot$ and there exists $\gamma' = \rho \times \delta^{PA}$ in $Sat(\varphi)$ such that $\rho \Subset^{\delta^{PA}}_{\mathcal{R}^{PA}} \gamma'$.
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, $\mathcal{R}^{PA}$ is indeed a satisfaction relation. Since we trivially have that $s_0^P\,\mathcal{R}^{PA}\,s_0$, 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 $M \models_{MC} N$.

F.7 Proof of Theorem 9

Let $N = (S, A, L, AP, V, s_0)$ and $N' = (S', A, L', AP, V', s'_0)$ be two deterministic APA in single valuation normal form. Suppose also that N and N' are pruned, i.e. that they do not have any inconsistent state. We have that $[\![N]\!] \subseteq [\![N']\!]$ iff $N \preceq_S N'$.

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.
$\Leftarrow$: As already stated in Theorem F.1, if $N \preceq_S N'$, then $[\![N]\!] \subseteq [\![N']\!]$.
$\Rightarrow$: Suppose that $[\![N]\!] \subseteq [\![N']\!]$. We prove that $N \preceq_S N'$.
Let $\widehat{N} = \langle \widehat{Q}, \widehat{q_0}, \psi, \widehat{A}, \widehat{V} \rangle$ and $\widehat{N'} = \langle \widehat{Q'}, \widehat{q'_0}, \psi', \widehat{A}, \widehat{V'} \rangle$ be the CMCs equivalent to N and N' obtained by the transformation proposed in Definition 20. By Definition 15, we have that $[\![N]\!]_{MC} \subseteq [\![N']\!]_{MC}$. As a consequence, by Theorem 8, we have that $[\![\widehat{N}]\!] \subseteq [\![\widehat{N'}]\!]$. Since $\widehat{N}$ and $\widehat{N'}$ are deterministic CMCs in single valuation normal form, we have, by Theorem 18 of [3], that $\widehat{N} \preceq \widehat{N'}$ with a strong refinement relation between CMCs.

Let $\widehat{\mathcal{R}}$ be the strong refinement relation between CMCs such that $\widehat{N} \preceq \widehat{N'}$. 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 $s \,\mathcal{R}\, t$.

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 correspondance function $\widehat{\delta}$ such that for all distribution π satisfying $\psi((s,\epsilon))$ we have that $\pi' = \pi \times \widehat{\delta}$ 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 $\pi((s,a)) > 0$. Again, since π satisfies ψ, we have $a \in \mathsf{May}(s)$. Thus there exists $\varphi \in C(S)$ such that $L(s,a,\varphi) \neq \bot$.
   Moreover, we have that $(s,a)\widehat{\mathcal{R}}(t,a)$. Let $\widehat{\delta'}$ be the associated correspondance 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 $\rho' = \mu' \times \widehat{\delta'}$ satisfies $\psi'((t,a))$. As a consequence, the distribution $\rho \in Dist(S')$ such that $\rho(t') = \rho'((t',\epsilon))$ for all t' is such that there exists φ'' such that $L'(t,a,\varphi'') \neq \bot$ and $\rho \in Sat(\varphi'')$. **By action-determinism of** N', we have that $\varphi'' = \varphi'$.
   Let δ be the correspondance function such that $\delta(s',t') = \widehat{\delta'}((s',\epsilon),(t',\epsilon))$. We prove that $\mu \Subset^{\delta}_{\mathcal{R}} \rho$.
   (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 $\rho' = \mu' \times \widehat{\delta'}$ satisfies $\psi'((t,a))$, we have that for all $t' \in T$ and $b \in A$, $\rho'((t',b)) = 0$. 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 $\rho' = \mu' \times \widehat{\delta'}$. 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 $\rho = \mu \times \delta$. As a consequence, we have that for all $t' \in S'$,
   $$\sum_{s' \in S} \mu(s') \cdot \delta(s',t') = \rho(t').$$
   (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 $s' \,\mathcal{R}\, t'$.
   Finally, we have that $\mu \Subset^{\delta}_{\mathcal{R}} \rho$.
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 correspondance function $\widehat{\delta}$ such that for all distribution π satisfying $\psi((s,\epsilon))$ we have that $\pi' = \pi \times \widehat{\delta}$ 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 reccursion axiom, we have $b = a$. Let $\pi' = \pi \times \widehat{\delta}$,

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 $L'(t, a, \varphi') \neq \bot$.

Moreover, we have that $(s, a)\widehat{\mathcal{R}}(t, a)$. Let $\widehat{\delta'}$ be the associated correspondance 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 $\rho' = \mu' \times \widehat{\delta'}$ satisfies $\psi'((t, a))$. As a consequence, the distribution $\rho \in Dist(S')$ such that $\rho(t') = \rho'((t', \epsilon))$ for all t' is such that there exists φ'' such that $L'(t, a, \varphi'') \neq \bot$ and $\rho \in Sat(\varphi'')$. **By action-determinism of** N', we have that $\varphi'' = \varphi'$.

Let δ be the correspondance function such that $\delta(s', t') = \widehat{\delta'}((s', \epsilon), (t', \epsilon))$. We prove that $\mu \Subset^{\delta}_{\mathcal{R}} \rho$.

(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 $\rho' = \mu' \times \widehat{\delta'}$ satisfies $\psi'((t, a))$, we have that for all $t' \in T$ and $b \in A$, $\rho'((t', b)) = 0$. 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 $\rho' = \mu' \times \widehat{\delta'}$. 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 $\rho = \mu \times \delta$. As a consequence, we have that for all $t' \in S'$,

$$\sum_{s' \in S} \mu(s') \cdot \delta(s', t') = \rho(t').$$

(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 $s' \,\mathcal{R}\, t'$.

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

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 $N \preceq_S N'$.