Refinement and Difference for Probabilistic Automata

Benoit Delahaye, Uli Fahrenberg, Kim Guldstrand Larsen, Axel Legay

REFINEMENT AND DIFFERENCE FOR PROBABILISTIC AUTOMATA

BENOÎT DELAHAYE, ULI FAHRENBERG, KIM G. LARSEN, AND AXEL LEGAY

Université de Nantes, France

Inria / IRISA Rennes, France

Aalborg University, Denmark

Inria / IRISA Rennes, France

Abstract. This paper studies a difference operator for stochastic systems whose specifications are represented by Abstract Probabilistic Automata (APAs). In the case refinement fails between two specifications, the target of this operator is to produce a specification APA that represents all witness PAs of this failure. Our contribution is an algorithm that permits to approximate the difference of two deterministic APAs with arbitrary precision. Our technique relies on new quantitative notions of distances between APAs used to assess convergence of the approximations, as well as on an in-depth inspection of the refinement relation for APAs. The procedure is effective and not more complex than refinement checking.

1. Introduction

Probabilistic automata as promoted by Segala and Lynch [43] are a widely-used formalism for modeling systems with probabilistic behavior. These include randomized security and communication protocols, distributed systems, biological processes and many other applications. Probabilistic model checking [5, 29, 47] is then used to analyze and verify the behavior of such systems. Given the prevalence of applications of such systems, probabilistic model checking is a field of great interest. However, and similarly to the situation for non-probabilistic model checking, probabilistic model checking suffers from *state space explosion*, which hinders its applicability considerably.

One generally successful technique for combating state space explosion is the use of *compositional* techniques, where a (probabilistic) system is model checked by verifying its components one by one. This compositionality can be obtained by *decomposition*, that is, to check whether a given system satisfies a property, the system is automatically

2012 ACM Subject Classification: Mathematics of computing—Markov processes; Theory of computation—Probabilistic computation.

Key words and phrases: Probabilistic automaton, difference, distance, specification theory.

This is an extended version of the paper [17] which has been presented at the 10th International Conference on Quantitative Evaluation of SysTems (QEST 2013) in Buenos Aires, Argentina. Compared to [17], and in addition to a number of small changes and improvements, proofs of the main statements and a new section on counter-example generation have been added to the paper.

LOGICAL METHODS
IN COMPUTER SCIENCE DOI:10.2168/LMCS-???

decomposed into components which are then verified. Several attempts at such automatic decomposition techniques have been made [13,34], but in general, this approach has not been very successful [12].

As an alternative to the standard model checking approaches using logical specifications, e.g. LTL, MITL or PCTL [3,26,39], automata-based specification theories have been proposed, such as Input/Output Automata [37], Interface Automata [14], and Modal Specifications [8,35, 40]. These support composition *at specification level*; hence a model which naturally consists of a composition of several components can be verified by model checking each component on its own, against its own specification. The overall model will then automatically satisfy the composition of the component specifications. Remark that this solves the decomposition problem mentioned above: instead of trying to automatically decompose a system for verification, specification theories make it possible to verify the system without constructing it in the first place.

Moreover, specification theories naturally support *stepwise refinement* of specifications, i.e. iterative implementation of specifications, and *quotient*, i.e. the synthesis of missing component specifications given an overall specification and a partial implementation. Hence they allow both logical and compositional reasoning at the same time, which makes them well-suited for compositional verification.

For probabilistic systems, such automata-based specification theories have been first introduced in [31], in the form of Interval Markov Chains. The focus there is only on refinement however; to be able to consider also composition and conjunction, we have in [10] proposed Constraint Markov Chains (CMCs) as a natural generalization which uses general constraints instead of intervals for next-state probabilities.

In [18], we have extended this specification theory to probabilistic automata, which combine stochastic and non-deterministic behaviors. These *Abstract Probabilistic Automata* (APA) combine modal specifications and CMCs. Our specification theory using APA should be viewed as an alternative to classical PCTL [26], probabilistic I/O automata [38] and stochastic extensions of CSP [27]. Like these, its purpose is model checking of probabilistic properties, but unlike the alternatives, APA support compositionality at specification level.

In the context of refinement of specifications, it is important that informative debugging information is given in case refinement fails. More concretely, given APAs N_1, N_2 for which N_1 does not refine N_2, we would like to know *why* refinement fails, and if possible, *where* in the state spaces of N_1 and N_2 there is a problem. We hence need to be able to compare APAs at the semantic level, i.e. to capture the *difference between their sets of implementations* and to relate it to structural differences of the APAs. This is what we attempt in this paper: given two APAs N_1 and N_2, to generate another APA N such that the set of implementations of N is the differences between the sets of implementations of N_1 and of N_2.

As a second contribution, we introduce a notion of *distance* between APAs which measures how far away one APA is from refining a second one. This distance, adapted from our work in [8,23], is *accumulating* and *discounted*, so that differences between APAs accumulate along executions, but in a way so that differences further in the future are discounted, i.e. have less influence on the result than had they occurred earlier.

Both difference and distances are important tools to compare APAs which are not in refinement. During an iterative development process, one usually wishes to successively replace specifications by more refined ones, but due to external circumstances such as, for example, cost of implementation, it may happen that a specification needs to be replaced by one which is not a refinement of the old one. This is especially important when models

incorporate quantitative information, such as for APAs; the reason for the failed refinement might simply be some changes in probability constraints, for example due to measurement updates. In this case, it is important to assess precisely *how much* the new specification differs from the old one. Both the distance between the new and old specifications, as well as their precise difference, can aid in this assessment.

Unfortunately, because APAs are finite-state structures, the difference between two APAs cannot always itself be represented by an APA. Instead of extending the formalism, we propose to *approximate* the difference for a subclass of APAs. We introduce both over- and under-approximations of the difference of two *deterministic* APAs. We construct a sequence of under-approximations which converges to the exact difference, hence eventually capturing all PAs in $[\![N_1]\!] \setminus [\![N_2]\!]$, and a fixed over-approximation which may capture also PAs which are not in the exact difference, but whose distance to the exact difference is zero: hence any superfluous PAs which are captured by the over-approximation are infinitesimally close to the real difference. Taken together, these approximations hence solve the problem of assessing the precise difference between deterministic APAs in case of failing refinement.

For completeness, we show as a last contribution how our algorithms can be refined into a procedure that computes a single counter-example to a failed refinement.

We restrict ourselves to the subclass of deterministic APAs, as it permits syntactic reasoning to decide and compute refinement. Indeed, for deterministic APAs, syntactic refinement coincides with semantic refinement [18], hence allowing for efficient procedures. Note that although the class of APAs we consider is called "deterministic", it still offers non-determinism in the sense that one can choose between different actions in a given state.

Related work. This paper embeds into a series of articles on APA as a specification theory [17–21]. In [18] we introduce deterministic APA, generalizing earlier work on interval-based abstractions of probabilistic systems [24, 31, 32], and define notions of refinement, logical composition, and structural composition. We also introduce a notion of *compositional abstraction* for APA. In [19] we extend this setting to non-deterministic APA and give a notion of (over-approximating) determinization. In [21] we introduce the tool APAC which implements most of these operations and hence can be used for compositional design and verification of probabilistic systems.

The journal paper [20] sums up and streamlines the contributions of [18, 19, 21]. One interesting detail in the theory of APA is that there are several types of *syntactic refinement* of APA. In [20], these are called *strong* refinement, *weak* refinement, and *weak weak* refinement, respectively; all are motivated by similar notions for CMCs [10]. For *deterministic* APAs, these refinements agree, and they also coincide with thorough refinement (i.e. inclusion of implementation sets). The distance and difference we introduce in the present paper complement the refinement and abstraction from [20], in the sense that our distance between APAs is a quantitative generalization of APA refinement, and our difference structurally characterizes refinement failure.

Compositional abstraction of APA is also considered in [44], but with the additional feature that transitions with the same action (i.e. non-deterministic choices) can be combined into so-called *multi-transitions*. The refinement in [44] is thus even weaker than the weak weak refinement of [20]; for deterministic APA however, they agree.

Differences between automata-based specifications have not been considered much in the literature. [41] develops a notion of *pseudo-merge* between modal specifications which keeps track of inconsistencies between specifications; here, the inconsistent states can be

seen as a form of difference. Distances between probabilistic systems have been introduced in [15, 22, 46] and other works, and distances between modal specifications in [6–8]; here, we combine these notions to introduce distances between APAs.

The originality of our present work is the ability to measure how far away one probabilistic specification is from being a refinement of another, using distances and our new difference operator. Both are important in assessing precisely how much one APA differs from another.

Acknowledgment. The authors wish to thank Joost-Pieter Katoen for interesting discussions and insightful comments on the subject of this work, and a number of anonymous referees for useful comments and improvements.

2. Background

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

Definition 1. A probabilistic automaton (PA) [43] is a tuple (S, A, L, AP, V, s_0), where S is a finite set of states with the initial state $s_0 \in S$, A is a finite set of actions, $L\colon S \times A \times \mathit{Dist}(S) \to \mathbb{B}_2$ is a (two-valued) transition function, AP is a finite set of atomic propositions and $V\colon S \to 2^{AP}$ is a state-labeling function.

Consider a state s, an action a, and a probability distribution μ. The value of $L(s, a, \mu)$ is set to $\top$ in case there exists a transition from s under action a to a distribution μ on successor states. In other cases, we have $L(s, a, \mu) = \bot$. We now introduce Abstract Probabilistic Automata (APA) [18], that is a specification theory for PAs. For a finite set S, we let $C(S)$ denote the set of constraints over discrete probability distributions on S. Each element $\varphi \in C(S)$ describes a set of distributions: $\mathit{Sat}(\varphi) \subseteq \mathit{Dist}(S)$. Let $\mathbb{B}_3 = \{\top, ?, \bot\}$. APAs are formally defined as follows.

Definition 2. An APA [18] is a tuple (S, A, L, AP, V, S_0), where S is a finite set of states, $S_0 \subseteq S$ is a set of initial states, A is a finite set of actions, and AP is a finite set of atomic propositions. $L : S \times A \times C(S) \to \mathbb{B}_3$ is a *three*-valued distribution-constraint function, and $V : S \to 2^{2^{AP}}$ maps each state in S to a set of admissible labelings.

APAs play the role of specifications in our framework. An APA transition abstracts transitions of certain unknown PAs, called its implementations. Given a state s, an action a, and a constraint φ, the value of $L(s, a, \varphi)$ gives the modality of the transition. More precisely, the value $\top$ means that transitions under a must exist in the PA to some distribution in $\mathit{Sat}(\varphi)$; ? means that these transitions are allowed to exist; $\bot$ means that such transitions must not exist. We will sometimes view L as a *partial* function, with the convention that a lack of value for a given argument is equivalent to the $\bot$ value. The function V labels each state with a subset of the power set of AP, which models a disjunctive choice of possible combinations of atomic propositions.

We say that an APA $N = (S, A, L, AP, V, S_0)$ is in *Single Valuation Normal Form* (SVNF) if the valuation function V assigns at most one valuation to all states, i.e. $\forall s \in S, |V(s)| \leq 1$. From [18], we know that every APA can be turned into an APA in SVNF with the same set of implementations. An APA is *deterministic* [18] if (1) there is at most one outgoing transition for each action in all states, (2) two states with overlapping atomic propositions can never be reached with the same transition, and (3) there is only one initial state.

Note that every PA is an APA in SVNF where all constraints represent a single distribution. As a consequence, all the definitions we present for APAs in the following can be directly extended to PAs.

Let $N = (S, A, L, AP, V, \{s_0\})$ be an APA in SVNF and let $v \subseteq AP$. Given a state $s \in S$ and an action $a \in A$, we will use the notation $\mathsf{succ}_{s,a}(v)$ to represent the set of potential a-successors of s that have v as their valuation. Formally, $\mathsf{succ}_{s,a}(v) = \{s' \in S \mid V(s') = \{v\}, \exists \varphi \in C(S), \mu \in Sat(\varphi) : L(s,a,\varphi) \neq \bot, \mu(s') > 0\}$. When clear from the context, we may use $\mathsf{succ}_{s,a}(s')$ instead of $\mathsf{succ}_{s,a}(V(s'))$. Remark that when N is deterministic, we have $|\mathsf{succ}_{s,a}(v)| \leq 1$ for all s, a, v.

3. Refinement and Distances between APAs

We recall the notion of refinement between APAs. Roughly speaking, refinement guarantees that if A_1 refines A_2, then the set of implementations of A_1 is included in the one of A_2.

Definition 3. Let S and S' be non-empty sets and $\mu \in \mathit{Dist}(S)$, $\mu' \in \mathit{Dist}(S')$. We say that μ is *simulated* by μ' with respect to a relation $\mathcal{R} \subseteq S \times S'$ and a *correspondence function* $\delta : S \to (S' \to [0,1])$ [18] if

(1) for all $s \in S$ with $\mu(s) > 0$, $\delta(s)$ 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) whenever $\delta(s)(s') > 0$, then $(s, s') \in \mathcal{R}$.

We write $\mu \Subset^{\delta}_{\mathcal{R}} \mu'$ if μ is simulated by μ' with respect to $\mathcal{R}$ and δ, $\mu \Subset_{\mathcal{R}} \mu'$ if there exists δ with $\mu \Subset^{\delta}_{\mathcal{R}} \mu'$, and $\mu \Subset^{\delta} \mu'$ for $\mu \Subset^{\delta}_{S \times S'} \mu'$.

Definition 4. Let $N_1 = (S_1, A, L_1, AP, V_1, S_0^1)$ and $N_2 = (S_2, A, L_2, AP, V_2, S_0^2)$ be APAs. A relation $\mathcal{R} \subseteq S_1 \times S_2$ is a *refinement* relation [18] if, for all $(s_1, s_2) \in \mathcal{R}$, we have $V_1(s_1) \subseteq V_2(s_2)$ and

(1) $\forall a \in A$, $\forall \varphi_2 \in C(S_2)$, if $L_2(s_2, a, \varphi_2) = \top$, then $\exists \varphi_1 \in C(S_1) : L_1(s_1, a, \varphi_1) = \top$ and $\forall \mu_1 \in Sat(\varphi_1)$, $\exists \mu_2 \in Sat(\varphi_2)$ such that $\mu_1 \Subset_{\mathcal{R}} \mu_2$,
(2) $\forall a \in A$, $\forall \varphi_1 \in C(S_1)$, if $L_1(s_1, a, \varphi_1) \neq \bot$, then $\exists \varphi_2 \in C(S_2)$ such that $L_2(s_2, a, \varphi_2) \neq \bot$ and $\forall \mu_1 \in Sat(\varphi_1)$, $\exists \mu_2 \in Sat(\varphi_2)$ such that $\mu_1 \Subset_{\mathcal{R}} \mu_2$.

We say that N_1 refines N_2, denoted $N_1 \preceq N_2$, if there exists a refinement relation such that $\forall s_0^1 \in S_0^1 : \exists s_0^2 \in S_0^2 : (s_0^1, s_0^2) \in \mathcal{R}$. Since any PA P is also an APA, we say that P *satisfies* N (or equivalently P *implements* N), denoted $P \models N$, if $P \preceq N$. In the following, a refinement relation between a PA and an APA is called a *satisfaction* relation. In [18], it is shown that for deterministic APAs N_1, N_2, we have $N_1 \preceq N_2 \iff [\![N_1]\!] \subseteq [\![N_2]\!]$, where $[\![N_i]\!]$ denotes the set of implementations of APA N_i. Hence for deterministic APAs, the difference $[\![N_1]\!] \setminus [\![N_2]\!]$ is non-empty iff $N_1 \not\preceq N_2$. This equivalence breaks for non-deterministic APAs [18], whence we develop our theory only for deterministic APAs.

To show a convergence theorem about our difference construction in Sect. 4.3 below, we need a relaxed notion of refinement which takes into account that APAs are a *quantitative* formalism. Indeed, refinement as of Def. 4 is a purely qualitative relation; if both $N_2 \not\preceq N_1$ and $N_3 \not\preceq N_1$, then there are no criteria to compare N_2 and N_3 with respect to N_1, saying which one is the closest to N_1. We provide such a relaxed notion by generalizing refinement to a *discounted distance* which provides precisely such criteria. In Sect. 4.3, we will show how those distances can be used to show that increasingly precise difference approximations between APAs converge to the real difference.

In order to simplify notation, the definitions presented below are dedicated to APAs in SVNF. They can however be easily extended to account for general APAs. The next definition shows how a distance between states is lifted to a distance between constraints.

Definition 5. Let $d : S_1 \times S_2 \to \mathbb{R}^+$ and $\varphi_1 \in C(S_1)$, $\varphi_2 \in C(S_2)$ be constraints in N_1 and N_2. Define the distance D_{N_1,N_2} between φ_1 and φ_2 as follows:

$$D_{N_1,N_2}(\varphi_1,\varphi_2,d) = \sup_{\mu_1 \in Sat(\varphi_1)} \inf_{\mu_2 \in Sat(\varphi_2)} \inf_{\delta : \mu_1 \Subset^{\delta} \mu_2} \sum_{(s_1,s_2)\in S_1\times S_2} \mu_1(s_1)\delta(s_1)(s_2)d(s_1,s_2)$$

Note the analogy of this definition to the one of the *Hausdorff* distance between (closed) subsets of a metric space: Any distribution μ_1 in $Sat(\varphi_1)$ is sought matched with a distribution μ_2 in $Sat(\varphi_2)$ which mimics it as closely as possible, where the quality of a match is measured by existence of a correspondence function δ which minimizes the distance between points reached from s_1 and s_2 weighted by their probability.

For the definition of d below, we say that states $s_1 \in S_1$, $s_2 \in S_2$ are *not compatible* if

(1) $V_1(s_1) \neq V_2(s_2)$,
(2) there exists $a \in A$ and $\varphi_1 \in C(S_1)$ such that $L_1(s_1,a,\varphi_1) \neq \bot$ and for all $\varphi_2 \in C(S_2), L_2(s_2,a,\varphi_2) = \bot$, or
(3) there exists $a \in A$ and $\varphi_2 \in C(S_2)$ such that $L_2(s_2,a,\varphi_2) = \top$ and for all $\varphi_1 \in C(S_1), L_1(s_1,a,\varphi_1) \neq \top$.

For compatible states, their distance is similar to the accumulating branching distance on modal transition systems as introduced in [8, 23], adapted to our formalism. In the rest of the paper, the real constant $0 < \lambda < 1$ represents a discount factor. Formally, $d : S_1 \times S_2 \to [0,1]$ is the least fixed point to the following system of equations:

$$d(s_1,s_2) = \begin{cases} 1 \text{ if } s_1 \text{ is not compatible with } s_2 \\ \max \begin{cases} \max\limits_{a,\varphi_1 : L_1(s_1,a,\varphi_1)\neq\bot} \min\limits_{\varphi_2 : L_2(s_2,a,\varphi_2)\neq\bot} \lambda D_{N_1,N_2}(\varphi_1,\varphi_2,d) \\ \max\limits_{a,\varphi_2 : L_2(s_2,a,\varphi_2)=\top} \min\limits_{\varphi_1 : L_1(s_1,a,\varphi_1)=\top} \lambda D_{N_1,N_2}(\varphi_1,\varphi_2,d) \end{cases} \text{otherwise} \end{cases} \tag{3.1}$$

Since the above system of linear equations defines a *contraction*, the existence and uniqueness of its least fixed point is ensured, cf. [36]. The intuition here is that $d(s_1,s_2)$ compares not only the probability constraints at s_1 and s_2, but also (recursively) the constraints at all states reachable from s_1 and s_2, weighted by their probability. Each step is discounted by λ, hence steps further in the future contribute less to the distance.

The above definition intuitively extends to PAs, which allows us to propose the two following notions of distance:

Definition 6. Let $N_1 = (S_1, A, L_1, AP, V_1, S_0^1)$ and $N_2 = (S_2, A, L_2, AP, V_2, S_0^2)$ be APAs in SVNF. The *syntactic* and *thorough* distances between N_1 and N_2 are defined as follows:

- syntactic distance: $d(N_1,N_2) = \max_{s_0^1 \in S_0^1} \big(\min_{s_0^2 \in S_0^2} d(s_0^1, s_0^2) \big)$.
- thorough distance: $d_t(N_1,N_2) = \sup_{P_1 \in [\![N_1]\!]} \big(\inf_{P_2 \in [\![N_2]\!]} d(P_1,P_2) \big)$.

Note that the notion of thorough distance defined above intuitively extends to sets of PAs: given two sets of PAs $\mathbb{S}_1$, $\mathbb{S}_2$, we have $d_t(\mathbb{S}_1,\mathbb{S}_2) = \sup_{P_1 \in \mathbb{S}_1} \big(\inf_{P_2 \in \mathbb{S}_2} d(P_1,P_2) \big)$.

We also remark that $N_1 \preceq N_2$ implies $d(N_1,N_2) = 0$. It can be shown, cf. [45], that both d and d_t are *asymmetric pseudometrics* (or *hemimetrics*), i.e. satisfying $d(N_1,N_1) = 0$ and $d(N_1,N_2) + d(N_2,N_3) \geq d(N_1,N_3)$ for all APAs N_1, N_2, N_3 (and similarly for d_t). The

fact that they are only pseudometrics, i.e. that $d(N_1, N_2) = 0$ does not imply $N_1 = N_2$, will play a role in our convergence arguments later.

The following proposition shows that the thorough distance is bounded above by the syntactic distance. Hence we can bound distances between (sets of) implementations by the syntactic distance between their specifications.

Proposition 1. For all APAs N_1 and N_2 in SVNF, it holds that $d_t(N_1, N_2) \leq d(N_1, N_2)$.

Proof. For a distribution μ_1 and a constraint φ_2, we denote by

$$\mathsf{RD}(\mu_1, \varphi_2) := \{\delta : \mu_1 \Subset^{\delta} \mu_2 \mid \mu_2 \in Sat(\varphi_2)\}$$

the set of all correspondence functions between μ_1 and distributions satisfying φ_2.

If $d(N_1, N_2) = 1$, we have nothing to prove. Otherwise, write $N_i = (S_i, A, L_i, AP, V_i, S_0^i)$ for $i = 1, 2$, and let $P_1 = (S_1', A, L_1', AP, V_1', \bar{S}_0^1) \in [\![N_1]\!]$ and $\eta > 0$; we need to expose $P_2 \in [\![N_2]\!]$ for which $d(P_1, P_2) \leq d(N_1, N_2) + \eta$. Note that by the triangle inequality, $d(P_1, N_2) \leq d(P_1, N_1) + d(N_1, N_2) \leq d(N_1, N_2)$. Define $P_2 = (S_2, A, L_2', AP, V_2, S_0^2)$, with L_2' given as follows:

For all $s_1' \in S_1'$, $a \in A$, $\mu_1 \in Dist(S_1')$ for which $L_1'(s_1', a, \mu_1) = \top$ and for all $s_2 \in S_2$, $\varepsilon < 1$ with $\varepsilon := d(s_1', s_2) < 1$: We must have $\varphi_2 \in Dist(S_2)$ such that $L_2(s_2, a, \varphi_2) \neq \bot$ and

$$\inf_{\delta \in \mathsf{RD}(\mu_1, \varphi_2)} \sum_{(t_1', t_2) \in S_1' \times S_2} \mu_1(t_1')\delta(t_1', t_2)d(t_1', t_2) \leq \lambda^{-1}\varepsilon\,,$$

so there must exist a correspondence function $\delta \in \mathsf{RD}(\mu_1, \varphi_2)$ for which

$$\sum_{(t_1', t_2) \in S_1' \times S_2} \mu_1(t_1')\delta(t_1', t_2)d(t_1', t_2) \leq \lambda^{-1}\varepsilon + \lambda^{-1}\eta.$$

We let $\mu_2(s) = \sum_{s_1' \in S_1} \mu_1(s_1')\delta(s_1', s)$ and set $L_2'(s_2, a, \mu_2) = \top$ in P_2.

Similarly, for all $s_2 \in S_2$, $a \in A$, $\varphi_2 \in C(S_2)$ for which $L_2(s_2, a, \varphi_2) = \top$ and for all $s_1' \in S_1'$ with $\varepsilon := d(s_1', s_2) < 1$: We must have $\mu_1 \in Dist(S_1')$ for which $L_1'(s_1', a, \mu_1) = \top$ and

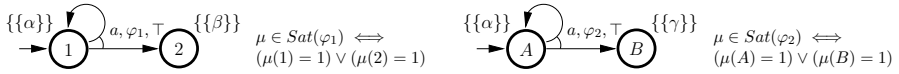
$$\inf_{\delta \in \mathsf{RD}(\mu_1, \varphi_2)} \sum_{(t_1', t_2) \in S_1' \times S_2} \mu_1(t_1')\delta(t_1', t_2)d(t_1', t_2) \leq \lambda^{-1}\varepsilon\,,$$

so there is $\delta \in \mathsf{RD}(\mu_1, \varphi_2)$ with

$$\sum_{(t_1', t_2) \in S_1' \times S_2} \mu_1(t_1')\delta(t_1', t_2)d(t_1', t_2) \leq \lambda^{-1}\varepsilon + \lambda^{-1}\eta.$$

Let again $\mu_2(s) = \sum_{s_1' \in S_1} \mu_1(s_1')\delta(s_1', s)$, and set $L_2'(s_2, a, \mu_2) = \top$ in P_2.

It is easy to see that $P_2 \in [\![N_2]\!]$: by construction of P_2, the identity relation $\{(s_2, s_2) \mid s_2 \in S_2\}$ provides a refinement $P_2 \preceq N_2$. To show that $d(P_1, P_2) \leq d(N_1, N_2) + \eta$, we define a function $d' : S_1' \times S_2 \to [0, 1]$ by $d'(s_1', s_2) = d(s_1', s_2) + \eta$ and show that d' is a pre-fixed



(A) APA N_1 (B) APA N_2

FIGURE 1. APAs N_1 and N_2 such that $[\![N_1]\!] \setminus [\![N_2]\!]$ cannot be represented using a finite-state APA.

point to (3.1). Indeed, for s_1' and s_2 compatible, we have

$$\begin{aligned} d'(s_1', s_2) &= d(s_1', s_2) + \eta \\ &= \max \begin{cases} \max\limits_{a,\mu_1 : L_1'(s_1',a,\mu_1)=\top} \min\limits_{\varphi_2 : L_2(s_2,a,\varphi_2)\neq\bot} \lambda D_{P_1,N_2}(\mu_1, \varphi_2, d) + \eta \\ \max\limits_{a,\varphi_2 : L_2(s_2,a,\varphi_2)=\top} \min\limits_{\mu_1 : L_1'(s_1',a,\mu_1)=\top} \lambda D_{P_1,N_2}(\mu_1, \varphi_2, d) + \eta \end{cases} \\ &= \max \begin{cases} \max\limits_{a,\mu_1 : L_1'(s_1',a,\mu_1)=\top} \min\limits_{\mu_2 : L_2'(s_2,a,\mu_2)=\top} \lambda D_{P_1,P_2}(\mu_1, \mu_2, d) + \eta \\ \max\limits_{a,\mu_2 : L_2'(s_2,a,\mu_2)=\top} \min\limits_{\mu_1 : L_1'(s_1',a,\mu_1)=\top} \lambda D_{P_1,P_2}(\mu_1, \mu_2, d) + \eta \,, \end{cases} \end{aligned}$$

due to the construction of P_2 and the fact that the $\sup_{\mu_1 \in Sat(\mu_1)}$ is trivial in the formula for $D_{P_1,N_2}(\mu_1, \varphi_2, d)$,

$$\geq \max \begin{cases} \max\limits_{a,\mu_1 : L_1'(s_1',a,\mu_1)=\top} \min\limits_{\mu_2 : L_2'(s_2,a,\mu_2)=\top} \lambda D_{P_1,P_2}(\mu_1, \mu_2, d') \\ \max\limits_{a,\mu_2 : L_2'(s_2,a,\mu_2)=\top} \min\limits_{\mu_1 : L_1'(s_1',a,\mu_1)=\top} \lambda D_{P_1,P_2}(\mu_1, \mu_2, d') \,, \end{cases}$$

where the last inequality is a consequence of

$$\begin{aligned} \lambda D_{P_1,P_2}(\mu_1, \mu_2, d') &= \lambda \sum_{t_1', t_2} \mu_1(t_1') \delta(t_1', t_2)(d(t_1', t_2) + \eta) \\ &= \lambda \sum_{t_1', t_2} \mu_1(t_1') \delta(t_1', t_2) d(t_1', t_2) + \lambda\eta. \end{aligned}$$

□

4. Difference Operators for Deterministic APAs

The difference $N_1 \setminus N_2$ of two APAs N_1, N_2 is meant to be a syntactic representation of *all counterexamples*, i.e. all PAs P for which $P \in [\![N_1]\!]$ but $P \notin [\![N_2]\!]$.

We first observe that such a set may not be representable by an APA. Consider the APAs N_1 and N_2 given in Figures 1a and 1b, where $\alpha \neq \beta \neq \gamma$. Note that both N_1 and N_2 are deterministic and in SVNF. Consider the difference of their sets of implementations. It is easy to see that this set contains all PAs that can finitely loop on valuation α and then move into a state with valuation β. Since there is no bound on the number of steps spent in the loop, there is no finite-state APA that can represent this set of implementations.

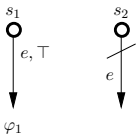
By the above example, there is no hope of finding a general construction that permits to represent the exact difference of two APAs as an APA. In the rest of this section, we thus

propose to *approximate* it using APAs. We first introduce some notations and then propose constructions for over-approximating and under-approximating the exact difference.

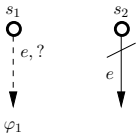
4.1. **Notation.** Let $N_i = (S_i, A, L_i, AP, V_i, \{s_0^i\})$, $i = 1, 2$, be deterministic APAs in SVNF. Because N_1 and N_2 are deterministic, we know that the difference $[\![N_1]\!] \setminus [\![N_2]\!]$ is non-empty if and only if $N_1 \not\preceq N_2$. So let us assume that $N_1 \not\preceq N_2$, and let $\mathcal{R}$ be a maximal refinement relation between N_1 and N_2. Since $N_1 \not\preceq N_2$, we know that $(s_0^1, s_0^2) \notin \mathcal{R}$. Given $(s_1, s_2) \in S_1 \times S_2$, we can distinguish between the following cases:

(1) $(s_1, s_2) \in \mathcal{R}$,
(2) $V_1(s_1) \neq V_2(s_2)$, or
(3) $(s_1, s_2) \notin \mathcal{R}$ and $V_1(s_1) = V_2(s_2)$, and

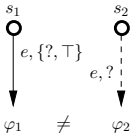
(a) there exists $e \in A$ and $\varphi_1 \in C(S_1)$ such that $L_1(s_1, e, \varphi_1) = \top$ and $\forall \varphi_2 \in C(S_2) : L_2(s_2, e, \varphi_2) = \bot$,



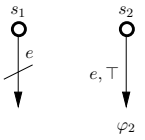
(b) there exists $e \in A$ and $\varphi_1 \in C(S_1)$ such that $L_1(s_1, e, \varphi_1) = ?$ and $\forall \varphi_2 \in C(S_2) : L_2(s_2, e, \varphi_2) = \bot$,



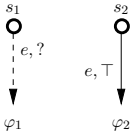
(c) there exists $e \in A$ and $\varphi_1 \in C(S_1)$ such that $L_1(s_1, e, \varphi_1) \geq ?$ and $\exists \varphi_2 \in C(S_2) : L_2(s_2, e, \varphi_2) = ?, \exists \mu \in Sat(\varphi_1)$ such that $\forall \mu' \in Sat(\varphi_2) : \mu \not\preceq_{\mathcal{R}} \mu'$,



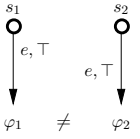
(d) there exists $e \in A$ and $\varphi_2 \in C(S_2)$ such that $L_2(s_2, e, \varphi_2) = \top$ and $\forall \varphi_1 \in C(S_1) : L_1(s_1, e, \varphi_1) = \bot$,



(e) there exists $e \in A$ and $\varphi_2 \in C(S_2)$ such that $L_2(s_2, e, \varphi_2) = \top$ and $\exists \varphi_1 \in C(S_1) : L_1(s_1, e, \varphi_1) = ?$,



(f) there exists $e \in A$ and $\varphi_2 \in C(S_2)$ such that $L_2(s_2, e, \varphi_2) = \top$, $\exists \varphi_1 \in C(S_1) : L_1(s_1, e, \varphi_1) = \top$ and $\exists \mu \in Sat(\varphi_1)$ such that $\forall \mu' \in Sat(\varphi_2) : \mu \not\preceq_{\mathcal{R}} \mu'$.



Remark that because of the determinism and SVNF of APAs N_1 and N_2, cases 1, 2 and 3 cannot happen at the same time. Moreover, although the cases in 3 can happen simultaneously, they cannot be "triggered" by the same action. In order to keep track of these "concurrent" situations, we define the following sets.

Given a pair of states (s_1, s_2), let $B_a(s_1, s_2)$ be the set of actions in A such that case 3.a above holds. If there is no such action, then $B_a(s_1, s_2) = \emptyset$. Similarly, we define $B_b(s_1, s_2), B_c(s_1, s_2), B_d(s_1, s_2), B_e(s_1, s_2)$ and $B_f(s_1, s_2)$ to be the sets of actions such that case 3.b, c, d, e and 3.f holds, respectively. Given a set $X \subseteq \{a, b, c, d, e, f\}$, let $B_X(s_1, s_2) = \cup_{x \in X} B_x(s_1, s_2)$. In addition, let $B(s_1, s_2) = B_{\{a,b,c,d,e,f\}}(s_1, s_2)$.

4.2. **Over-Approximating Difference.** We now propose a construction $\setminus^*$ that over-approximates the difference between deterministic APAs in SVNF in the following sense: given two such APAs $N_1 = (S_1, A, L_1, AP, V_1, \{s_0^1\})$ and $N_2 = (S_2, A, L_2, AP, V_2, \{s_0^2\})$ such that $N_1 \not\preceq N_2$, we have $[\![N_1]\!] \setminus [\![N_2]\!] \subseteq [\![N_1 \setminus^* N_2]\!]$. We first observe that if $V_1(s_0^1) \neq V_2(s_0^2)$, i.e. (s_0^1, s_0^2) in case 2, then $[\![N_1]\!] \cap [\![N_2]\!] = \emptyset$. In such case, we define $N_1 \setminus^* N_2$ as N_1. Otherwise, we build on the reasons for which refinement fails between N_1 and N_2. Note that the assumption that $N_1 \not\preceq N_2$ implies that the pair (s_0^1, s_0^2) can never be in any refinement relation, hence in case 1. We first give an informal intuition of how the construction works and then define it formally.

In our construction, states in $N_1 \setminus^* N_2$ will be elements of $S_1 \times (S_2 \cup \{\bot\}) \times (A \cup \{\varepsilon\})$. Our objective is to ensure that any implementation of our constructed APA will satisfy N_1 and not N_2. In (s_1, s_2, e), states s_1 and s_2 keep track of executions of N_1 and N_2. Action e is the action of N_1 that will be used to break satisfaction with respect to N_2, i.e. the action that will be the cause for which any implementation of (s_1, s_2, e) cannot satisfy N_2. Since satisfaction is defined recursively, the breaking is not necessarily immediate and can be postponed to successors. $\bot$ is used to represent states that can only be reached after breaking the satisfaction relation to N_2. In these states, we do not need to keep track of the corresponding execution in N_2, thus only focus on satisfying N_1. States of the form (s_1, s_2, ε) with $s_2 \neq \bot$ are states where the satisfaction is broken by a distribution that does not match constraints in N_2 (cases 3.c and 3.f). In order to invalidate these constraints, we still need to keep track of the corresponding execution in N_2, hence the use of ε instead of $\bot$.

The transitions in our construction will match the different cases shown in the previous section, ensuring that in each state, either the relation is broken immediately or reported to at least one successor. Since there can be several ways of breaking the relation in state (s_0^1, s_0^2), each corresponding to an action $e \in B(s_0^1, s_0^2)$, the APA $N_1 \setminus^* N_2$ will have one initial state for each of them. Formally, if (s_0^1, s_0^2) is in case 3, we define the over-approximation of the difference of N_1 and N_2 as follows.

Definition 7. Let $N_1 \setminus^* N_2 = (S, A, L, AP, V, S_0)$, where $S = S_1 \times (S_2 \cup \{\bot\}) \times (A \cup \{\varepsilon\})$, $V(s_1, s_2, a) = V(s_1)$ for all s_2 and a, $S_0 = \{(s_0^1, s_0^2, f) \mid f \in B(s_0^1, s_0^2)\}$, and L is defined by:

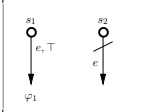
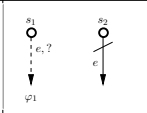
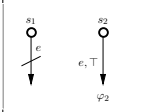
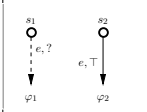
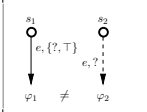
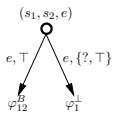
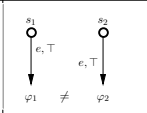
- If $s_2 = \bot$ or $e = \varepsilon$ or (s_1, s_2) in case 1 or 2, then for all $a \in A$ and $\varphi \in C(S_1)$ such that $L_1(s_1, a, \varphi) \neq \bot$, let $L((s_1, s_2, e), a, \varphi^\bot) = L_1(s_1, a, \varphi)$, with $\varphi^\bot$ defined below. For all other $b \in A$ and $\varphi \in C(S)$, let $L((s_1, s_2, e), b, \varphi) = \bot$.
- Else, we have (s_1, s_2) in case 3 and $B(s_1, s_2) \neq \emptyset$ by construction. The definition of L is given in Table 1, with the constraints $\varphi^\bot$ and φ_{12}^B defined hereafter.

Given $\varphi \in C(S_1)$, $\varphi^\bot \in C(S)$ is defined as follows: $\mu \in Sat(\varphi^\bot)$ iff $\forall s_1 \in S_1, \forall s_2 \neq \bot, \forall b \neq \varepsilon, \mu(s_1, s_2, b) = 0$ and the distribution $(\mu \downarrow_1 : s_1 \mapsto \mu(s_1, \bot, \varepsilon))$ is in $Sat(\varphi)$.

Given a state $(s_1, s_2, e) \in S$ with $s_2 \neq \bot$ and $e \neq \varepsilon$ and two constraints $\varphi_1 \in C(S_1)$, $\varphi_2 \in C(S_2)$ such that $L_1(s_1, e, \varphi_1) \neq \bot$ and $L_2(s_2, e, \varphi_2) \neq \bot$, the constraint $\varphi_{12}^B \in C(S)$ is defined as follows: $\mu \in Sat(\varphi_{12}^B)$ iff

(1) for all $(s_1', s_2', c) \in S$, we have $\mu(s_1', s_2', c) > 0 \Rightarrow s_2' = \bot$ if $\mathsf{succ}_{s_2,e}(s_1') = \emptyset$ and $s_2' = \mathsf{succ}_{s_2,e}(s_1')$ otherwise, and $c \in B(s_1', s_2') \cup \{\varepsilon\}$,
(2) the distribution $\mu_1 : s_1' \mapsto \sum_{c \in A \cup \{\varepsilon\}, s_2' \in S_2 \cup \{\bot\}} \mu(s_1', s_2', c)$ satisfies φ_1, and
(3) one of the following holds:
   (a) there exists $(s_1', \bot, c)$ such that $\mu(s_1', \bot, c) > 0$,
   (b) the distribution $\mu_2 : s_2' \mapsto \sum_{c \in A \cup \{\varepsilon\}, s_1' \in S_1} \mu(s_1', s_2', c)$ does not satisfy φ_2, or
   (c) there exists $s_1' \in S_1$, $s_2' \in S_2$ and $c \neq \varepsilon$ such that $\mu(s_1', s_2', c) > 0$.

TABLE 1. Definition of the transition function L in $N_1 \setminus^* N_2$.

$e \in$	N_1, N_2	$N_1 \setminus^* N_2$	Formal Definition of L
$B_a(s_1, s_2)$			For all $a \neq e \in A$ and $\varphi \in C(S_1)$ such that $L_1(s_1, a, \varphi) \neq \bot$, let $L((s_1, s_2, e), a, \varphi^{\bot}) = L_1(s_1, a, \varphi)$. In addition, let $L((s_1, s_2, e), e, \varphi_1^{\bot}) = \top$. For all other $b \in A$ and $\varphi \in C(S)$, let $L((s_1, s_2, e), b, \varphi) = \bot$.
$B_b(s_1, s_2)$			
$B_d(s_1, s_2)$			For all $a \in A$ and $\varphi \in C(S_1)$ such that $L_1(s_1, a, \varphi) \neq \bot$, let $L((s_1, s_2, e), a, \varphi^{\bot}) = L_1(s_1, a, \varphi)$. For all other $b \in A$ and $\varphi \in C(S)$, let $L((s_1, s_2, e), b, \varphi) = \bot$.
$B_e(s_1, s_2)$			For all $a \neq e \in A$ and $\varphi \in C(S_1)$ such that $L_1(s_1, a, \varphi) \neq \bot$, let $L((s_1, s_2, e), a, \varphi^{\bot}) = L_1(s_1, a, \varphi)$. In addition, let $L((s_1, s_2, e), e, \varphi_{12}^{B}) = ?$. For all other $b \in A$ and $\varphi \in C(S)$, let $L((s_1, s_2, e), b, \varphi) = \bot$.
$B_c(s_1, s_2)$			For all $a \in A$ and $\varphi \in C(S_1)$ such that $L_1(s_1, a, \varphi) \neq \bot$ (including e and φ_1), let $L((s_1, s_2, e), a, \varphi^{\bot}) = L_1(s_1, a, \varphi)$. In addition, let $L((s_1, s_2, e), e, \varphi_{12}^{B}) = \top$. For all other $b \in A$ and $\varphi \in C(S)$, let $L((s_1, s_2, e), b, \varphi) = \bot$.
$B_f(s_1, s_2)$			

Informally, distributions in φ_{12}^{B} must (1) follow the corresponding execution is N_1 and N_2 if possible, (2) satisfy φ_1 and (3), (a) reach a state in N_1 that cannot be matched in N_2, (b) break the constraint φ_2, or (c) report breaking the relation to at least one successor state.

The following theorem shows that $N_1 \setminus^* N_2$ is, as intended, an over-approximation of the difference of N_1 and N_2 in terms of sets of implementations.

Theorem 2. For all deterministic APAs N_1 and N_2 in SVNF such that $N_1 \not\preceq N_2$, we have $[\![N_1]\!] \setminus [\![N_2]\!] \subseteq [\![N_1 \setminus^* N_2]\!]$.

Proof. Let $N_1 = (S_1, A, L_1, AP, V_1, \{s_0^1\})$ and $N_2 = (S_2, A, L_2, AP, V_2, \{s_0^2\})$ be deterministic APAs in SVNF such that $N_1 \not\preceq N_2$. Let $\mathcal{R}$ be the maximal refinement relation between N_1 and N_2. Let $P = (S_P, A, L_P, AP, V_P, s_0^P)$ be a PA such that $P \models N_1$ and $P \not\models N_2$. We prove that $P \models N_1 \setminus^* N_2$. Let $\mathcal{R}_1 \subseteq S_P \times S_1$ be the relation witnessing $P \models N_1$ and let $\mathcal{R}_2$ be the maximal satisfaction relation in $S_P \times S_2$. By construction, $(s_0^P, s_2) \notin \mathcal{R}_2$.

If $V_1(s_0^1) \neq V_2(s_0^2)$, then by construction $N_1 \setminus^* N_2 = N_1$ and thus $P \models N_1 \setminus^* N_2$. Else, we have (s_0^1, s_0^2) in case 3, thus $N_1 \setminus^* N_2 = (S, A, L, AP, V, S_0)$ is defined as in Section 4.2. By construction, we also have (s_0^P, s_0^2) in case 3, thus there must exist $f \in B(s_0^P, s_0^2)$. Remark that by construction, we must have $B(s_0^P, s_0^2) \subseteq B(s_0^1, s_0^2)$. We will prove that $P \models N_1 \setminus^* N_2$.

Define the following relation $\mathcal{R}^{\setminus} \subseteq S_P \times S$:

$$p \,\mathcal{R}^{\setminus}(s_1, s_2, e) \iff \begin{cases} & (p \,\mathcal{R}_1\, s_1) \text{ and } (s_2 = \bot) \text{ and } (e = \varepsilon) \\ \text{or} & (p \,\mathcal{R}_1\, s_1) \text{ and } (p, s_2) \text{ in case 1 or 2 and and } (e = \varepsilon) \\ \text{or} & (p \,\mathcal{R}_1\, s_1) \text{ and } (p, s_2) \text{ in case 3 and } (e \in B(p, s_2)) \end{cases}$$

We now prove that $\mathcal{R}^{\setminus}$ is a satisfaction relation. Let $(p,(s_1,s_2,e)) \in \mathcal{R}^{\setminus}$.

If $s_2 = \bot$ or $e = \varepsilon$, then since $p\,\mathcal{R}_1\,s_1$, $\mathcal{R}^{\setminus}$ satisfies the axioms of a satisfaction relation by construction. Else we have $s_2 \in S_2$ and $e \neq \varepsilon$, thus, by definition of $\mathcal{R}^{\setminus}$, we know that (p,s_2) is in case 3.

- By construction, we have $V_P(p) \in V_1(s_1) = V((s_1,s_2,e))$.
- Let $a \in A$ and $\mu_P \in Dist(S_P)$ such that $L_P(p,a,\mu_P) = \top$. There are several cases.
  - If $a \neq e$, then since $p\,\mathcal{R}_1\,s_1$, there exists $\varphi_1 \in C(S_1)$ such that $L_1(s_1,a,\varphi_1) \neq \bot$ and there exists $\mu_1 \in Sat(\varphi_1)$ such that $\mu_P \Subset_{\mathcal{R}^{\setminus}} \mu_1$. By construction, we have $L((s_1,s_2,e),a,\varphi_1^{\perp}) \neq \bot$ and there obviously exists $\mu \in Sat(\varphi_1^{\perp})$ such that $\mu_P \Subset_{\mathcal{R}^{\setminus}} \mu$.
  - If $a = e \in B_a(p,s_2)$, then, as above, there exists a constraint $\varphi \in C(S)$ such that $L((s_1,s_2,e),a,\varphi) \neq \bot$ and there exists $\mu \in Sat(\varphi)$ such that $\mu_P \Subset_{\mathcal{R}^{\setminus}} \mu$. Remark that $B_a(s_1,s_2) \subseteq B_a(p,s_2) \subseteq B_a(s_1,s_2) \cup B_b(s_1,s_2)$.
  - Else, we necessarily have $a = e \in B_c(p,s_2) \cup B_f(p,s_2)$. Remark that, by construction, $B_c(p,s_2) \subseteq B_c(s_1,s_2)$ and $B_f(p,s_2) \subseteq B_f(s_1,s_2)$. Since $p\,\mathcal{R}_1\,s_1$, there exists $\varphi_1 \in C(S_1)$ such that $L_1(s_1,e,\varphi_1) \neq \bot$ and there exists $\mu_1 \in Sat(\varphi_1)$ and a correspondence function $\delta_1 : S_P \to (S_1 \to [0,1])$ such that $\mu_P \Subset^{\delta_1}_{\mathcal{R}_1} \mu_1$.
    Moreover, by construction of $N_1 \setminus^* N_2$, we know that the constraint φ^B_{12} such that $\mu \in Sat(\varphi^B_{12})$ iff. (1) for all $(s'_1,s'_2,c) \in S$, we have $\mu(s'_1,s'_2,c) > 0 \Rightarrow s'_2 = \bot$ if $\mathsf{succ}_{s_2,e}(s'_1) = \emptyset$ and $s'_2 = \mathsf{succ}_{s_2,e}(s'_1)$ otherwise, and $c \in B(s'_1,s'_2) \cup \{\varepsilon\}$, (2) the distribution $\mu_1 : s'_1 \mapsto \sum_{c \in A \cup \{\varepsilon\}, s'_2 \in S_2 \cup \{\bot\}} \mu(s'_1,s'_2,c)$ satisfies φ_1, and (3) either (b) the distribution $\mu_2 : s'_2 \mapsto \sum_{c \in A \cup \{\varepsilon\}, s'_1 \in S_1} \mu(s'_1,s'_2,c)$ does not satisfy φ_2, or (c) there exists $s'_1 \in S_1$, $s'_2 \in S_2$ and $c \neq \varepsilon$ such that $\mu(s'_1,s'_2,c) > 0$ is such that $L((s_1,s_2,e),e,\varphi^B_{12}) = \top$.
    We now prove that there exists $\mu \in Sat(\varphi^B_{12})$ such that $\mu_P \Subset_{\mathcal{R}^{\setminus}} \mu$. Consider the function $\delta^{\setminus} : S_P \to (S \to [0,1])$ defined as follows: Let $p' \in S_P$ such that $\mu_P(p') > 0$ and let $s'_1 = \mathsf{succ}_{s_1,e}(p')$, which exists by $\mathcal{R}_1$.
    - If $\mathsf{succ}_{s_2,e}(p') = \emptyset$, then $\delta^{\setminus}(p')(s'_1,\bot,\varepsilon) = 1$.
    - Else, let $s'_2 = \mathsf{succ}_{s_2,e}(p')$. Then,
      - if $(p',s'_2) \in \mathcal{R}_2$, then $\delta^{\setminus}(p')(s'_1,s'_2,\varepsilon) = 1$.
      - Else, (p',s'_2) is in case 3 and $B(p',s'_2) \neq \emptyset$. In this case, let $c \in B(p',s'_2)$ and define $\delta^{\setminus}(p',(s'_1,s'_2,c)) = 1$. For all other $c' \in B(p',s'_2)$, define $\delta^{\setminus}(p',(s'_1,s'_2,c)) = 0$.

    Remark that for all $p' \in S_P$ such that $\mu_P(p') > 0$, there exists a unique $s' \in S'$ such that $\delta^{\setminus}(p')(s') = 1$. Thus $\delta^{\setminus}$ is a correspondence function.
    We now prove that $\mu = \mu_P\delta^{\setminus} \in Sat(\varphi^B_{12})$.
    (1) Let $(s'_1,s'_2,c) \in S$ such that $\mu(s'_1,s'_2,c) > 0$. By construction, there exists $p' \in S_P$ such that $\mu_P(p') > 0$ and $\delta^{\setminus}(p')(s'_1,s'_2,c) > 0$. Moreover, $c \in B(s'_1,s'_2) \cup \{\varepsilon\}$, and $s'_2 = \bot$ if $\mathsf{succ}_{s_2,e}(s'_1) = \emptyset$ and $s'_2 = \mathsf{succ}_{s_2,e}(s'_1)$ otherwise.
    (2) Consider the distribution $\mu'_1 : s'_1 \mapsto \sum_{c \in A \cup \{\varepsilon\}, s'_2 \in S_2 \cup \{\bot\}} \mu(s'_1,s'_2,c)$. By determinism (See Lemma 28 in [10]), we have that $\delta_1(p')(s'_1) = 1 \iff s'_1 = (succ)_{s_1,e}(p')$. As a consequence, we have that $\mu'_1 = \mu_1 \in Sat(\varphi_1)$.

(3) Assume that for all $p' \in S_P$ such that $\mu_P(p') > 0$, we have $\mathsf{succ}_{s_2,e}(p') \neq \emptyset$ (the other case being trivial). Consider the distribution $\mu_2 : s_2' \mapsto \sum_{c \in A \cup \{\varepsilon\}, s_1' \in S_1} \mu(s_1', s_2', c)$ and let $\delta_2 : S_P \to (S_2 \to [0,1])$ be such that $\delta_2(p')(s_2') = 1 \iff s_2' = \mathsf{succ}_{s_2,e}(p')$. By construction, δ_2 is a correspondence function and $\mu_2 = \mu_P \delta_2$. Since $e \in B_c(p, s_2) \cup B_f(p, s_2)$, we have that $\mu_P \not\Subset_{\mathcal{R}_2} \mu_2$. If $\mu_2 \notin Sat(\varphi_2)$, then we have $\mu \in Sat(\varphi_{12}^B)$. Else, there must exist $p' \in S_P$ and $s_2' \in S_2$ such that $\mu_P(p') > 0$, $\delta_2(p')(s_2') > 0$ and $(p', s_2') \notin \mathcal{R}_2$. As a consequence, (p', s_2') is in case 3 and there exists $c \neq \varepsilon$ such that $\delta^{\setminus}(p')(s_1', s_2', c) > 0$, thus $\mu(s_1', s_2', c) > 0$. As a consequence, $\mu \in Sat(\varphi_{12}^B)$.

We thus conclude that there exists $\mu \in Sat(\varphi_{12}^B)$ such that $\mu_P \Subset_{\mathcal{R}^{\setminus}} \mu$.

Finally, in all cases, there exists $\varphi \in C(S)$ such that $L((s_1, s_2, e), a, \varphi) \neq \bot$ and there exists $\mu \in Sat(\varphi)$ such that $\mu_P \Subset_{\mathcal{R}^{\setminus}} \mu$.

- Let $a \in A$ and $\varphi \in C(S)$ such that $L((s_1, s_2, e), a, \varphi) = \top$. As above, there are several cases.
  - If $a \neq e$, then, by construction of $N_1 \setminus^* N_2$, there must exists $\varphi_1 \in C(S_1)$ such that $L_1(s_1, a, \varphi_1) = \top$. The rest of the proof is then as above.
  - If $a = e \in B_a(p, s_2)$, then there exists $\mu_P \in Dist(S_P)$ such that $L_P(p, e, \mu_P) = \top$. The rest of the proof is then as above. Recall that $B_a(s_1, s_2) \subseteq B_a(p, s_2) \subseteq B_a(s_1, s_2) \cup B_b(s_1, s_2)$.
  - Else, we necessarily have $a = e \in B_c(p, s_2) \cup B_f(p, s_2)$. Recall that, by construction, $B_c(p, s_2) \subseteq B_c(s_1, s_2)$ and $B_f(p, s_2) \subseteq B_f(s_1, s_2)$. Thus, there exists $\mu_P \in Dist(S_P)$ and $\varphi_2 \in C(S_2)$ such that $L_2(s_2, e, \varphi_2) \neq \bot$ and $\forall \mu_2 \in Sat(\varphi_2), \mu_P \not\Subset_{\mathcal{R}_2} \mu_2$. Since $e \in B_c(s_1, s_2) \cup B_f(s_1, s_2)$, there also exist $\varphi_1 \in C(S_1)$ such that $L_1(s_1, e, \varphi_1) \neq \bot$. By determinism, φ_1 and φ_2 are unique. The rest of the proof follows as above.

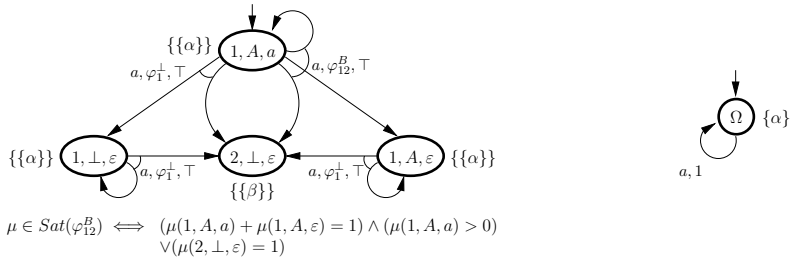
  Thus, in all cases, there exists $\mu_P \in Dist(S_P)$ such that $L_P(p, a, \mu_P) = \top$ and there exists $\mu \in Sat(\varphi)$ such that $\mu_P \Subset_{\mathcal{R}^{\setminus}} \mu$.

Finally, $\mathcal{R}^{\setminus}$ is a satisfaction relation. Moreover, we have $s_0^P \, \mathcal{R}_1 \, s_0^1$, (s_0^P, s_0^2) in case 3 and $f \in B(s_0^P, s_0^2)$ by construction, thus $s_0^P \, \mathcal{R}^{\setminus}(s_0^1, s_0^2, f) \in S_0$. We thus conclude that $P \models N_1 \setminus^* N_2$. □

The reverse inclusion unfortunately does not hold. Intuitively, as explained in the construction of the constraint φ_{12}^B above, one can postpone the breaking of the satisfaction relation for N_2 to the next state (condition (3.c)). This assumption is necessary in order to produce an APA representing *all* counterexamples. However, when there are cycles in the execution of $N_1 \setminus^* N_2$, then we may postpone forever, thus allowing for implementations that will ultimately satisfy N_2. This is illustrated in the following example.

Example 1. Consider the APAs N_1 and N_2 given in Fig. 1. Their over-approximating difference $N_1 \setminus^* N_2$ is given in Fig. 2a. One can see that the PA P in Fig. 2b satisfies both $N_1 \setminus^* N_2$ and N_2.

We will later see in Corollary 7 that even though $N_1 \setminus^* N_2$ may be capturing too many counterexamples, the *distance* between $N_1 \setminus^* N_2$ and the real set of counterexamples $[\![N_1]\!] \setminus [\![N_2]\!]$ is zero. This means that the two sets are infinitesimally close to each other, so in this sense, and with respect to this distance, $N_1 \setminus^* N_2$ is a *best possible* over-approximation.



(A) $N_1 \setminus^* N_2$ (B) P

FIGURE 2. Over-approximating difference $N_1 \setminus^* N_2$ of APAs N_1 and N_2 from Figure 1 and PA P such that $P \models N_1 \setminus^* N_2$ and $P \models N_2$.

4.3. **Under-Approximating Difference.** We now propose a construction that instead *under-estimates* the difference between APAs. This construction resembles the over-approximation presented in the previous section, the main difference being that in the under-approximation, states are indexed with integers which represent the maximal depth of the unfolding of counterexamples. The construction is as follows.

Let $N_1 = (S_1, A, L_1, AP, V_1, \{s_0^1\})$ and $N_2 = (S_2, A, L_2, AP, V_2, \{s_0^2\})$ be two deterministic APAs in SVNF such that $N_1 \not\preceq N_2$. Let $K \in \mathbb{N}$ be the parameter of our construction. As in Section 4.2, if $V_1(s_0^1) \neq V_2(s_0^2)$, i.e. (s_0^1, s_0^2) in case 2, then $[\![N_1]\!] \cap [\![N_2]\!] = \emptyset$. In this case, we define $N_1 \setminus^K N_2$ as N_1. Otherwise, the under-approximation is defined as follows.

Definition 8. Let $N_1 \setminus^K N_2 = (S, A, L, AP, V, S_0^K)$, where $S = S_1 \times (S_2 \cup \{\bot\}) \times (A \cup \{\varepsilon\}) \times \{1, \dots, K\}$, $V(s_1, s_2, a, k) = V(s_1)$ for all s_2, a, $k < K$, $S_0^K = \{(s_0^1, s_0^2, f, K) \mid f \in B(s_0^1, s_0^2)\}$, and L is defined by:

- If $s_2 = \bot$ or $e = \varepsilon$ or (s_1, s_2) in case 1 or 2, then for all $a \in A$ and $\varphi \in C(S_1)$ such that $L_1(s_1, a, \varphi) \neq \bot$, let $L((s_1, s_2, e, k), a, \varphi^\bot) = L_1(s_1, a, \varphi)$, with $\varphi^\bot$ defined below. For all other $b \in A$ and $\varphi \in C(S)$, let $L((s_1, s_2, e, k), b, \varphi) = \bot$.
- Else we have (s_1, s_2) in case 3 and $B(s_1, s_2) \neq \emptyset$ by construction. The definition of L is given in Table 2. The constraints $\varphi^\bot$ and $\varphi_{12}^{B,k}$ are defined hereafter.

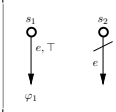
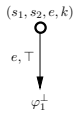
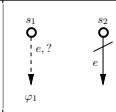
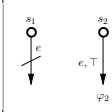
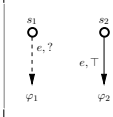
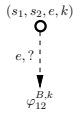
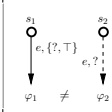
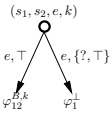
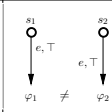
Given a constraint $\varphi \in C(S_1)$, the constraint $\varphi^\bot \in C(S)$ is defined as follows: $\mu \in Sat(\varphi^\bot)$ iff $\forall s_1 \in S_1, \forall s_2 \neq \bot, \forall b \neq \varepsilon, \forall k \neq 1, \mu(s_1, s_2, b, k) = 0$ and the distribution $(\mu \downarrow_1 : s_1 \mapsto \mu(s_1, \bot, \varepsilon, 1))$ is in $Sat(\varphi)$.

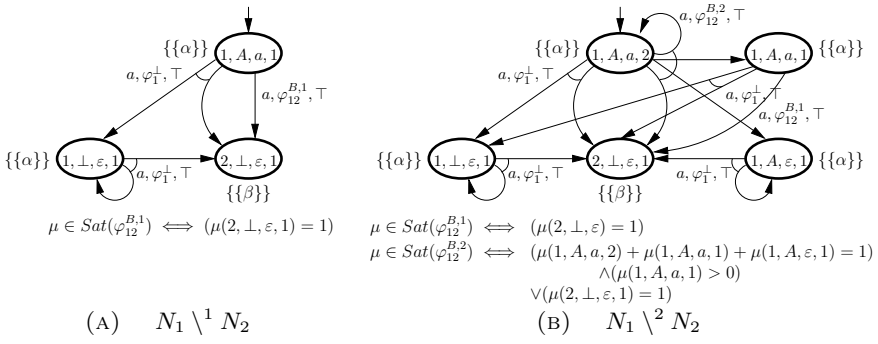
Given a state $(s_1, s_2, e, k) \in S$ with $s_2 \neq \bot$ and $e \neq \varepsilon$ and two constraints $\varphi_1 \in C(S_1)$ and $\varphi_2 \in C(S_2)$ such that $L_1(s_1, e, \varphi_1) \neq \bot$ and $L_2(s_2, e, \varphi_2) \neq \bot$, the constraint $\varphi_{12}^{B,k} \in C(S)$ is defined as follows: $\mu \in Sat(\varphi_{12}^{B,k})$ iff

(1) for all $(s_1', s_2', c, k') \in S$, if $\mu(s_1', s_2', c, k') > 0$, then $c \in B(s_1', s_2') \cup \{\varepsilon\}$ and either $\mathsf{succ}_{s_2,e}(s_1') = \emptyset$, $s_2' = \bot$ and $k' = 1$, or $s_2' = \mathsf{succ}_{s_2,e}(s_1')$,
(2) the distribution $\mu_1 : s_1' \mapsto \sum_{c \in A \cup \{\varepsilon\}, s_2' \in S_2 \cup \{\bot\}, k' \geq 1} \mu(s_1', s_2', c, k')$ satisfies φ_1, and
(3) one of the following holds:
   (a) there exists $(s_1', \bot, c, 1)$ such that $\mu(s_1', \bot, c, 1) > 0$,
   (b) the distribution $\mu_2 : s_2' \mapsto \sum_{c \in A \cup \{\varepsilon\}, s_1' \in S_1, k' \geq 1} \mu(s_1', s_2', c, k')$ does not satisfy φ_2, or
   (c) $k \neq 1$ and there exists $s_1' \in S_1$, $s_2' \in S_2$, $c \neq \varepsilon$ and $k' < k$ such that $\mu(s_1', s_2', c, k') > 0$.

The construction is illustrated in Figure 3.

TABLE 2. Definition of the transition function L in $N_1 \setminus^K N_2$.

$e \in$	N_1, N_2	$N_1 \setminus^K N_2$	Formal Definition of L
$B_a(s_1, s_2)$			For all $a \neq e \in A$ and $\varphi \in C(S_1)$ such that $L_1(s_1, a, \varphi) \neq \bot$, let $L((s_1, s_2, e, k), a, \varphi^{\bot}) = L_1(s_1, a, \varphi)$. In addition, let $L((s_1, s_2, e, k), e, \varphi_1^{\bot}) = \top$. For all other $b \in A$ and $\varphi \in C(S)$, let $L((s_1, s_2, e, k), b, \varphi) = \bot$.
$B_b(s_1, s_2)$			
$B_d(s_1, s_2)$			For all $a \in A$ and $\varphi \in C(S_1)$ such that $L_1(s_1, a, \varphi) \neq \bot$, let $L((s_1, s_2, e, k), a, \varphi^{\bot}) = L_1(s_1, a, \varphi)$. For all other $b \in A$ and $\varphi \in C(S)$, let $L((s_1, s_2, e, k), b, \varphi) = \bot$.
$B_e(s_1, s_2)$			For all $a \neq e \in A$ and $\varphi \in C(S_1)$ such that $L_1(s_1, a, \varphi) \neq \bot$, let $L((s_1, s_2, e, k), a, \varphi^{\bot}) = L_1(s_1, a, \varphi)$. In addition, let $L((s_1, s_2, e, k), e, \varphi_{12}^{B,k}) = ?$. For all other $b \in A$ and $\varphi \in C(S)$, let $L((s_1, s_2, e, k), b, \varphi) = \bot$.
$B_c(s_1, s_2)$			For all $a \in A$ and $\varphi \in C(S_1)$ such that $L_1(s_1, a, \varphi) \neq \bot$ (including e and φ_1), let $L((s_1, s_2, e, k), a, \varphi^{\bot}) = L_1(s_1, a, \varphi)$. In addition, let $L((s_1, s_2, e, k), e, \varphi_{12}^{B,k}) = \top$. For all other $b \in A$ and $\varphi \in C(S)$, let $L((s_1, s_2, e, k), b, \varphi) = \bot$.
$B_f(s_1, s_2)$			



(A) $N_1 \setminus^1 N_2$ (B) $N_1 \setminus^2 N_2$

FIGURE 3. Under-approximations at level 1 and 2 of the difference of APAs N_1 and N_2 from Figure 1.

4.4. **Properties.** We already saw in Theorem 2 that $N_1 \setminus^* N_2$ is a correct over-approximation of the difference of N_1 by N_2 in terms of sets of implementations. The next theorem shows that, similarly, all $N_1 \setminus^K N_2$ are correct under-approximations. Moreover, increasing the value of K improves the level of approximation, and eventually all PAs in $[\![N_1]\!] \setminus [\![N_2]\!]$ are caught. (Hence in a set-theoretic sense, $\lim_{K \to \infty} [\![N_1 \setminus^K N_2]\!] = [\![N_1]\!] \setminus [\![N_2]\!]$.)

Theorem 3. For all deterministic APAs N_1 and N_2 in SVNF such that $N_1 \not\preceq N_2$:

(1) for all $K \in \mathbb{N}$, we have $N_1 \setminus^K N_2 \preceq N_1 \setminus^{K+1} N_2$,
(2) for all $K \in \mathbb{N}$, $[\![N_1 \setminus^K N_2]\!] \subseteq [\![N_1]\!] \setminus [\![N_2]\!]$, and
(3) for all PA $P \in [\![N_1]\!] \setminus [\![N_2]\!]$, there exists $K \in \mathbb{N}$ such that $P \in [\![N_1 \setminus^K N_2]\!]$.

Note that item 3 implies that for all PA $P \in [\![N_1]\!] \setminus [\![N_2]\!]$, there is a finite specification capturing $[\![N_1]\!] \setminus [\![N_2]\!]$ "up to" P. The proof of the theorem is similar to the one of Theorem 2 (if somewhat more complicated) and available in appendix.

Using our distance defined in Section 3, we can make the above convergence result more precise. We first need a lemma comparing $N_1 \setminus^{K_1} N_2$ with $N_1 \setminus^{K_2} N_2$ for $K_1 \leq K_2$.

Lemma 4. Let $N_1 = (S_1, A, L_1, AP, V_1, \{s_0^1\})$ and $N_2 = (S_2, A, L_2, AP, V_2, \{s_0^2\})$ be two deterministic APAs in SVNF such that $N_1 \not\preceq N_2$. Let $1 \leq K_1 \leq K_2$ be integers. Then $d(N_1 \setminus^{K_2} N_2, N_1 \setminus^{K_1} N_2) \leq \lambda^{K_1}$.

Proof. Let $N_1 \setminus^{K_i} N_2 = N^i = (S^i, A, L^i, AP, V^i, T_0^i)$. We first remark that for all $(s_1, s_2, e) \in S_1 \times (S_2 \cup \bot) \times (A \cup \varepsilon)$ and for all $k \leq K_1$, the distance between the states $(s_1, s_2, e, k)^1 \in S^1$ and $(s_1, s_2, e, k)^2 \in S^2$ is 0. Indeed, if k is the same in both states, then they are identical by construction.

We now prove by induction on $1 \leq k_1 \leq K_1$ and $k_1 \leq k_2 \leq K_2$ that

$$d((s_1, s_2, e, k_2)^2, (s_1, s_2, e, k_1)^1) \leq \lambda^{k_1} :$$

- **Base case:** $k_1 = 1$**.** By construction, $t_1 = (s_1, s_2, e, k_1)^1$ and $t_2 = (s_1, s_2, e, k_2)^2$ have the same outgoing transitions. The only distinction is in the constraints $\varphi_{12}^{B,1}$ and φ_{12}^{B,k_2} when $e \in B_{\{c,e,f\}}(s_1, s_2)$. Thus, t_1 and t_2 are compatible, and

$$d(t_2, t_1) = \max \begin{cases} \max\limits_{a,\varphi' : L^2(t_2,a,\varphi') \neq \bot} \min\limits_{\varphi : L^1(t_1,a,\varphi) \neq \bot} \lambda D_{N^2,N^1}(\varphi', \varphi, d) \\ \max\limits_{a,\varphi : L^1(t_1,a,\varphi) = \top} \min\limits_{\varphi' : L^2(t_2,a,\varphi') = \top} \lambda D_{N^2,N^1}(\varphi', \varphi, d) \end{cases}$$

  Moreover, we know by construction that $D_{N^2,N^1}(\varphi', \varphi, d) \leq 1$ for all φ' and φ. As a consequence, $d(t_2, t_1) \leq \lambda = \lambda^{k_1}$.
- **Induction.** Let $t_1 = (s_1, s_2, e, k_1)^1$ and $t_2 = (s_1, s_2, e, k_2)^2$, with $1 < k_1 \leq k_2$. Again, if $e \notin B_c(s_1, s_2) \cup B_e(s_1, s_2) \cup B_f(s_1, s_2)$, then t_1 and t_2 are identical by construction and the result holds. Otherwise, the pair of constraints for which the distance is maximal will be constraints $\varphi_{12}^{B,k_1} \in C(S^1)$ and $\varphi_{12}^{B,k_2} \in C(S^2)$. Assume that $d((s_1, s_2, e, k_2')^2, (s_1, s_2, e, k_1')^1) \leq \lambda^{k_1'}$ for all $k_1' < k_1$ and $k_1' \leq k_2' \leq K_2$. By definition, we have

$$D_{N^2,N^1}(\varphi_{12}^{B,k_2}, \varphi_{12}^{B,k_1}, d) = \sup_{\mu_2 \in Sat(\varphi_{12}^{B,k_2})} \inf_{\delta \in \mathsf{RD}(\mu_2, \varphi_{12}^{B,k_1})} \sum_{t_2', t_1' \in S^2 \times S^1} \mu_2(t_2') \delta(t_2', t_1') d(t_2', t_1')$$

Consider the function $\delta : S^2 \times S^1 \to [0,1]$ such that

$$\delta((s_1', s_2', f, k_2'), (s_1'', s_2'', f', k_1')) = \begin{cases} 1 & \text{if } s_1' = s_1'' \wedge s_2' = s_2'' \wedge f' = f \\ & \qquad \wedge k_1' = k_2' \wedge k_2' < k_1 \\ 1 & \text{if } s_1' = s_1'' \wedge s_2' = s_2'' \wedge f' = f \\ & \qquad \wedge k_1' = k_1 - 1 \wedge k_1 \leq k_2' \\ 0 & \text{otherwise} \end{cases}$$

Let $\mu_2 \in Sat(\varphi_{12}^{B,k_2})$. One can verify that $\delta \in \mathsf{RD}(\mu_2, \varphi_{12}^{B,k_1})$ as follows:

(1) Let $t_2' = (s_1', s_2', f, k_2')$ be such that $\mu_2(t_2') > 0$. By definition, we always have $\sum_{t_1' \in S^1} \delta(t_2', t_1') = 1$.

(2) δ preserves all the conditions for satisfying φ_{12}^{B,k_2}. In particular, all states $t_2' = (s_1', s_2', f, k_2')^2$ such that $k_2' < k_2$ are redistributed to states $(s_1', s_2', f, k_1')^1$ with $k_1' < k_1$. As a consequence, the distribution $\mu_1 : t_1' \mapsto \sum_{t_2' \in S^2} \mu_2(t_2')\delta(t_2', t_1')$ satisfies φ_{12}^{B,k_1}.

As a consequence, for all $\mu_2 \in Sat(\varphi_{12}^{B,k_2})$, we have

$$\begin{aligned} &\inf_{\delta \in \mathsf{RD}(\mu_2, \varphi_{12}^{B,k_1})} \sum_{t_2', t_1' \in S^2 \times S^1} \mu_2(t_2')\delta(t_2', t_1')d(t_2', t_1') \\ &\quad \leq \sum_{\substack{(s_1', s_2', f, k_2') \in S^2 \\ k_2' < k_1}} \mu_2(s_1', s_2', f, k_2')d((s_1', s_2', f, k_2')^2, (s_1', s_2', f, k_2')^1) \\ &\qquad + \sum_{\substack{(s_1', s_2', f, k_2') \in S^2 \\ k_1 \leq k_2'}} \mu_2(s_1', s_2', f, k_2')d((s_1', s_2', f, k_2')^2, (s_1', s_2', f, k_1 - 1)^1) \\ &\quad \leq \sum_{\substack{(s_1', s_2', f, k_2') \in S^2 \\ k_1 \leq k_2'}} \mu_2(s_1', s_2', f, k_2')d((s_1', s_2', f, k_2')^2, (s_1', s_2', f, k_1 - 1)^1) \\ &\quad \leq \sum_{\substack{(s_1', s_2', f, k_2') \in S^2 \\ k_1 \leq k_2'}} \mu_2(s_1', s_2', f, k_2')\lambda^{k_1 - 1} \leq \lambda^{k_1 - 1} \end{aligned}$$

(the next-to-last step by induction).

Since this is true for all $\mu_2 \in Sat(\varphi_{12}^{B,k_2})$, we have $D_{N^2,N^1}(\varphi_{12}^{B,k_2}, \varphi_{12}^{B,k_1}, d) \leq \lambda^{k_1 - 1}$.

Finally, we have $d(t_2, t_1) \leq \lambda\lambda^{k_1 - 1} = \lambda^k$, which proves the induction.

For any state $t_0^2 = (s_0^1, s_0^2, e, K_2) \in T_0^2$, there exists a state $t_0^1 = (s_0^1, s_0^2, e, K_1) \in T_0^1$ such that $d(t_0^2, t_0^1) \leq \lambda^{K_1}$. As a consequence, we have $d(N_1 \setminus^{K_2} N_2, N_1 \setminus^{K_1} N_2) \leq \lambda^{K_1}$. □

The next proposition then shows that the speed of convergence is exponential in K; hence in practice, K will typically not need to be very large.

Proposition 5. Let N_1 and N_2 be two deterministic APAs in SVNF such that $N_1 \not\preceq N_2$, and let $K \in \mathbb{N}$. Then $d_t([\![N_1]\!] \setminus [\![N_2]\!], [\![N_1 \setminus^K N_2]\!]) \leq \lambda^K(1 - \lambda)^{-1}$.

Proof. By Lemma 4, we know that $d(N_1 \setminus^{L+1} N_2, N_1 \setminus^{L} N_2) \leq \lambda^L$ for each L, hence also $d_t([\![N_1 \setminus^{L+1} N_2]\!], [\![N_1 \setminus^{L} N_2]\!]) \leq \lambda^L$ for each L by Proposition 1. Applying the triangle inequality and continuity of d_t, we see that

$$\begin{aligned} d_t([\![N_1]\!] \setminus [\![N_2]\!], [\![N_1 \setminus^K N_2]\!]) &\leq d_t([\![N_1]\!] \setminus [\![N_2]\!], [\![N_1 \setminus^{K+1} N_2]\!]) \\ &\quad + d_t([\![N_1 \setminus^{K+1} N_2]\!], [\![N_1 \setminus^K N_2]\!]) \\ &\leq \lim_{i\to\infty} d_t([\![N_1]\!] \setminus [\![N_2]\!], [\![N_1 \setminus^{K+i} N_2]\!]) \\ &\quad + \sum_{i=0}^{\infty} d_t([\![N_1 \setminus^{K+i+1} N_2]\!], [\![N_1 \setminus^{K+i} N_2]\!]) \\ &\leq \sum_{i=0}^{\infty} \lambda^{K+i} = \frac{\lambda^K}{1-\lambda} \end{aligned}$$

□

For the actual application on hand however, the particular accumulating distance d we have introduced in Section 3 may have limited interest, especially considering that one has to fix a discounting factor for actually calculating it. What is more interesting are results of a *topological* nature which abstract away from the particular distance used and apply to all distances which are *topologically equivalent* to d. The results we present below are of this nature.

It can be shown, cf. [45], that accumulating distances for different choices of λ are topologically equivalent (indeed, even Lipschitz equivalent), hence the particular choice of discounting factor is not important. Also some other system distances are Lipschitz equivalent to the accumulating one, in particular the so-called *point-wise* and *maximum-lead* ones, see again [45].

Theorem 6. Let N_1 and N_2 be two deterministic APAs in SVNF such that $N_1 \not\preceq N_2$.

(1) The sequence $(N_1 \setminus^K N_2)_{K\in\mathbb{N}}$ converges in the distance d, and $\lim_{K\to\infty} d(N_1 \setminus^* N_2, N_1 \setminus^K N_2) = 0$.
(2) The sequence $([\![N_1 \setminus^K N_2]\!])_{K\in\mathbb{N}}$ converges in the distance d_t, and $\lim_{K\to\infty} d_t([\![N_1]\!] \setminus [\![N_2]\!], [\![N_1 \setminus^K N_2]\!]) = 0$.

Proof. Let $N_1 = (S_1, A, L_1, AP, V_1, \{s_0^1\})$ and $N_2 = (S_2, A, L_2, AP, V_2, \{s_0^2\})$ be two deterministic APAs in SVNF such that $N_1 \not\preceq N_2$.

1. The proof of the convergence of both sequences $(N_1 \setminus^K N_2)_K$ and $([\![N_1 \setminus^K N_2]\!])_K$ is done as follows. Let $\varepsilon > 0$. Since $\lambda < 1$, there exists $K \in \mathbb{N}$ such that $\lambda^K < \varepsilon$. As a consequence, by Lemma 4, we have that for all $K \leq K_1 \leq K_2$,

$$d(N_1 \setminus^{K_2} N_2, N_1 \setminus^{K_1} N_2) \leq \lambda^{K_1} \leq \lambda^K < \varepsilon.$$

The sequence $(N_1 \setminus^K N_2)_K$ is thus *bi-Cauchy* (i.e. both forward-Cauchy and backwards-Cauchy) in the sense of [9]. Hence, because of Proposition 1, the sequence (of sets of PA) $([\![N_1 \setminus^K N_2]\!])_K$ is also bi-Cauchy. The other two items show that they converge.

2. Theorem 3 shows that the sequence $([\![N_1 \setminus^K N_2]\!])_K$ converges in a set-theoretic sense (as a direct limit), and that $\lim_{K\to\infty} [\![N_1 \setminus^K N_2]\!] = [\![N_1]\!] \setminus [\![N_2]\!]$. Hence $d_t([\![N_1]\!] \setminus [\![N_2]\!], \lim_{K\to\infty} [\![N_1 \setminus^K N_2]\!]) = 0$, and by continuity of d_t, $\lim_{K\to\infty} d_t([\![N_1]\!] \setminus [\![N_2]\!], [\![N_1 \setminus^K N_2]\!]) = 0$.

3. Finally, we prove that $\lim_{K\to\infty} d(N_1 \setminus^* N_2, N_1 \setminus^K N_2) = 0$. This proof is very similar to the proof of Lemma 4 above: we can show that the distance between $N_1 \setminus^* N_2$ and $N_1 \setminus^K N_2$ is bounded as follows:

$$d(N_1 \setminus^* N_2, N_1 \setminus^K N_2) \leq \lambda^K$$

Let $N_1 \setminus^K N_2 = N^K = (S^K, A, L^K, AP, V^K, T_0^K)$, $N_1 \setminus^* N_2 = N^* = (S^*, A, L^*, AP, V^*, T_0^*)$. We start by proving by induction on $1 \leq k \leq K$ that for all $(s_1, s_2, e) \in S_1 \times (S_2 \cup \bot) \times (A \cup \varepsilon)$, we have $d((s_1, s_2, e)^*, (s_1, s_2, e, k)) \leq \lambda^k$. The only difference with the proof of Lemma 4 is in the choice of the function $\delta : S^* \times S^K \to [0, 1]$ in the induction part. Here, we choose δ as follows:

$$\delta((s_1', s_2', f), (s_1'', s_2'', f', k')) = \begin{cases} 1 & \text{if } s_1' = s_1'' \wedge s_2' = s_2'' \wedge f' = f \wedge k' = k - 1 \\ 0 & \text{otherwise} \end{cases}$$

The rest of the proof is identical, and we obtain that for all $1 \leq k \leq K$ and for all $(s_1, s_2, e) \in S_1 \times (S_2 \cup \bot) \times (A \cup \varepsilon)$, we have $d((s_1, s_2, e)^*, (s_1, s_2, e, k)) \leq \lambda^k$. In particular, this is also true for initial states. As a consequence, for all states $t_0^* = (s_0^2, s_0^1, e) \in T_0^*$, there exists a state $t_0^K = (s_0^1, s_0^2, e, K) \in T_0^K$ such that $d(t_0^*, t_0^K) \leq \lambda^K$, hence we have $d(N_1 \setminus^* N_2, N_1 \setminus^K N_2) \leq \lambda^K$, so that $\lim_{K\to\infty} d(N_1 \setminus^* N_2, N_1 \setminus^K N_2) = 0$. □

Recall that as d and d_t are not metrics, but only (asymmetric) pseudometrics (i.e. hemimetrics), the above sequences may have more than one limit; hence the particular formulation. The theorem's statements are topological, as they only allude to convergence of sequences and distance 0; topologically equivalent distances obey precisely the property of having the same convergence behavior and the same kernel, cf. [1].

The next corollary, which is easily proven from the above theorem by noticing that its first part implies that also $\lim_{K\to\infty} d_t([\![N_1 \setminus^* N_2]\!], [\![N_1 \setminus^K N_2]\!]) = 0$, shows what we mentioned already at the end of Section 4.2: with respect to the distance d, $N_1 \setminus^* N_2$ is a best possible over-approximation of $[\![N_1]\!] \setminus [\![N_2]\!]$.

Corollary 7. Let N_1 and N_2 be two deterministic APAs in SVNF such that $N_1 \not\preceq N_2$. Then $d_t([\![N_1 \setminus^* N_2]\!], [\![N_1]\!] \setminus [\![N_2]\!]) = 0$.

Again, as d_t is not a metric, the distance being zero does not imply that the sets $[\![N_1 \setminus^* N_2]\!]$ and $[\![N_1]\!] \setminus [\![N_2]\!]$ are equal; it merely means that they are *indistinguishable* by the distance d_t, or infinitesimally close to each other.

5. Counter-Example Generation

Here we show how some techniques similar to the ones we have introduced can be used to generate *one* counterexample to a failed refinement $N_1 \not\preceq N_2$. Note that when we compute the approximating differences $N_1 \setminus^* N_2$ and $N_1 \setminus^K N_2$, we are in principle generating (approximations to) the set of *all* counterexamples, hence what we do in Section 4 is much more general than what we will present below. Generating only *one* counterexample may still be interesting however, as it is somewhat easier than computing the differences $N_1 \setminus^* N_2$, $N_1 \setminus^K N_2$ and is all that is needed in a CEGAR approach.

First remark that Definition 4 can be trivially turned into an algorithm for checking refinement. Let $N_1 = (S_1, A, L_1, AP, V_1, \{s_0^1\})$ and $N_2 = (S_2, A, L_2, AP, V_2, \{s_0^2\})$ be two deterministic APAs in SVNF. Consider the initial relation $\mathcal{R}_0 = S_1 \times S_2$. Compute $\mathcal{R}_{k+1}$ by removing all pairs of states not satisfying Definition 4 for $\mathcal{R}_k$. The sequence $(\mathcal{R}_n)_{n\in\mathbb{N}}$ is then strictly decreasing and converges to a fixed point within a finite number of steps

$K \leq |S_1 \times S_2|$. This fixed point $\mathcal{R}_K$ coincides with the maximal refinement relation $\mathcal{R}$ between N_1 and N_2. Let the index of this fixed point be denoted with $\mathsf{Ind}(\mathcal{R}) = K$; hence $\mathsf{Ind}_{\mathcal{R}}(s_1, s_2) = \min(\max(\{k \mid (s_1, s_2) \in \mathcal{R}_k\}), K)$.

We now observe that if a pair of states (s_1, s_2) is removed from the relation $\mathcal{R}$ by case 3, then we need to keep track of the actions that lead to this removal in order to use them in our counterexample. Whenever a pair of states is in cases 3.a, 3.b, 3.d or 3.e, we have that $\mathsf{Ind}_{\mathcal{R}}(s_1, s_2) = 0$ and the counterexample can be easily produced by allowing or disallowing the corresponding transitions from N_1 and N_2. Cases 3.c and 3.f play a different role: due to the fact that they exploit distributions, they are the only cases in which refinement can be broken by using its *recursive* axiom. In these cases, producing a counterexample can be done in two ways: either by using a distribution that does not satisfy the constraints in N_2 (if such a distribution exists, then $\mathsf{Ind}_{\mathcal{R}}(s_1, s_2) = 0$), or by using a distribution that reaches a pair of states $(s_1', s_2') \notin \mathcal{R}$. When $0 < \mathsf{Ind}_{\mathcal{R}}(s_1, s_2) < \mathsf{Ind}(\mathcal{R})$, only the latter is possible. This recursive construction has disadvantages: it allows us to produce loops that may lead to incorrect counterexamples. In order to prevent these loops, we propose to use only those distributions that decrease the value of Ind in this particular case. The set $\mathsf{Break}(s_1, s_2)$ defined hereafter allows us to distinguish the actions for which the value of Ind decreases, hence ensuring (by Lemma 8 below) the correctness of our counterexample construction. Let $(s_1, s_2) \in S_1 \times S_2$ be such that $V_1(s_1) = V_2(s_2)$ and $\mathsf{Ind}_{\mathcal{R}}(s_1, s_2) = k < \mathsf{Ind}(\mathcal{R})$. We define

$$\begin{aligned}\mathsf{Break}(s_1, s_2) = \{a \in A \mid a \in B_{a,b,d,e}(s_1, s_2),\ &\text{or} \\ &\exists \varphi_1 \in C(S_1), \varphi_2 \in C(S_2), \mu_1 \in Sat(\varphi_1) : \\ &L_1(s_1, a, \varphi_1) \neq \bot, L_2(s_2, a, \varphi_2) \neq \bot, \forall \mu_2 \in Sat(\varphi_2) : \mu_1 \not\in_{\mathcal{R}_k} \mu_2\}\end{aligned}$$

Remark that the conditions for Break above are exactly the conditions for removing a pair of states (s_1, s_2) at step k of the algorithm for computing $\mathcal{R}$ defined above. Under the assumption that $V_1(s_1) \subseteq V_2(s_2)$ and $\mathsf{Ind}_{\mathcal{R}}(s_1, s_2) = k < \mathsf{Ind}(\mathcal{R})$, we can be sure that the set $\mathsf{Break}(s_1, s_2)$ is not empty. Moreover, we have the following lemma.

Lemma 8. For all pairs of states (s_1, s_2) in case 3 and for all actions $e \in (B_c(s_1, s_2) \cup B_f(s_1, s_2)) \cap \mathsf{Break}(s_1, s_2)$, there exist constraints φ_1 and φ_2 such that $L_1(s_1, e, \varphi_1) \neq \bot$ and $L_2(s_2, e, \varphi_2) \neq \bot$ and a distribution $\mu_1 \in Sat(\varphi_1)$ such that

(1) $\exists s_1' \in S_1$ such that $\mu_1(s_1') > 0$ and $\mathsf{succ}_{s_2,e}(s_1') = \emptyset$,
(2) $\mu_1^2 : \left(s_2' \mapsto \sum_{\{s_1' \in S_1 \mid s_2' = \mathsf{succ}_{s_2,e}(s_1')\}} \mu_1(s_1')\right) \notin Sat(\varphi_2)$, or
(3) $\exists s_1' \in S_1, s_2' \in S_2$ such that $\mu_1(s_1') > 0, s_2' = \mathsf{succ}_{s_2,e}(s_1')$ and $\mathsf{Ind}_{\mathcal{R}}(s_1', s_2') < \mathsf{Ind}_{\mathcal{R}}(s_1, s_2)$.

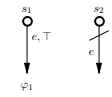
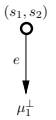
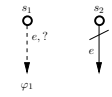
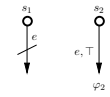
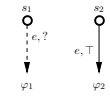
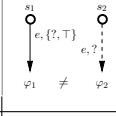
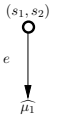
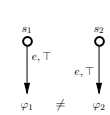
Proof. Let $\mathcal{R}$ be the maximal refinement relation between N_1 and N_2 and let $(s_1, s_2) \in S_1 \times S_2$ such that (s_1, s_2) is in case 3, i.e. $(s_1, s_2) \notin \mathcal{R}$ and $V_1(s_1) = V_2(s_2)$. Let $e \in A$ such that $e \in (B_c(s_1, s_2) \cup B_f(s_1, s_2)) \cap \mathsf{Break}(s_1, s_2)$.

Since $e \in B_c(s_1, s_2) \cup B_f(s_1, s_2)$, there exists $\varphi_1 \in C(S_1)$ and $\varphi_2 \in C(S_2)$ such that either $L_2(s_2, e, \varphi_2) = \top$ and $L_1(s_1, e, \varphi_1) = \top$ or $L_2(s_2, e, \varphi_2) = ?$ and $L_1(s_1, e, \varphi_1) \neq \bot$. As a consequence, since $e \in \mathsf{Break}(s_1, s_2)$, we have that

$$\exists \mu_1 \in Sat(\varphi_1), \forall \mu_2 \in Sat(\varphi_2), \mu_1 \not\in_{\mathcal{R}_k} \mu_2. \tag{5.1}$$

Let K be the smallest index such that $\mathcal{R}_K = \mathcal{R}$. By construction, we know that $\mathsf{Ind}_{\mathcal{R}}(s_1, s_2) = k < K$, i.e. $(s_1, s_2) \in \mathcal{R}_k$ and $(s_1, s_2) \notin \mathcal{R}_{k+1}$. Consider the distribution μ_1 given by (5.1) above. We have that $\forall \mu_2 \in Sat(\varphi_2) : \forall$ corresp. $\delta : \mu_1 \not\in^{\delta}_{\mathcal{R}_k} \mu_2$. Consider the

TABLE 3. Definition of the transition function L in P.

$e \in$	N_1, N_2	P	Formal Definition of L
$B_a(s_1, s_2)$			Let $\varphi_1 \in C(S_1)$ such that $L_1(s_1, e, \varphi_1) \neq \bot$ and let μ_1 be an arbitrary distribution in $Sat(\varphi_1)$. Define $L((s_1, s_2), e, \mu_1^{\bot}) = \top$.
$B_b(s_1, s_2)$			
$B_d(s_1, s_2)$			For all $\mu \in Dist(S)$, let $L((s_1, s_2), e, \mu) = \bot$.
$B_e(s_1, s_2)$			
$B_c(s_1, s_2)$			Let $\varphi_1 \in C(S_1)$ and $\varphi_2 \in C(S_2)$ such that $L_1(s_1, e, \varphi_1) \neq \bot$ and $L_2(s_2, e, \varphi_2) \neq \bot$. • If $e \in \mathsf{Break}(s_1, s_2)$, then let μ_1 be the distribution given in Lemma 8. • Else, let μ_1 be an arbitrary distribution in $Sat(\varphi_1)$ such that $\forall \mu_2 \in Sat(\varphi_2), \mu_1 \notin_{\mathcal{R}} \mu_2$. In both cases, let $L((s_1, s_2), e, \widehat{\mu_1}) = \top$.
$B_f(s_1, s_2)$			

function δ such that $\delta(s_1', s_2') = 1$ if $s_2' = \mathsf{succ}_{s_2,e}(s_1')$ and 0 otherwise. There are several cases.

- If there exists $s_1' \in S_1$ such that $\mu_1(s_1') > 0$ and $\mathsf{succ}_{s_2,e}(s_1') = \emptyset$, then the lemma is proven.
- Else, δ is a correspondence function. Since $\forall \mu_2 \in Sat(\varphi_2), \mu_1 \notin_{\mathcal{R}_k} \mu_2$, we know that either (1) $\mu_2 : s_2' \mapsto \sum_{s_1' \in S_1} \mu_1(s_1')\delta(s_1', s_2')$ does not satisfy φ_2, or (2) there exists s_1' and s_2' such that $\mu_1(s_1') > 0$, $\delta(s_1', s_2') > 0$ and $(s_1', s_2') \notin \mathcal{R}_k$.
  (1) Assume that $\mu_2 : s_2' \mapsto \sum_{s_1' \in S_1} \mu_1(s_1')\delta(s_1', s_2')$ does not satisfy φ_2. Remark that the function μ_1^2 from Lemma 8 is equal to μ_2 defined above. As a consequence, $\mu_1^2 \notin \varphi_2$.
  (2) Otherwise, assume that there exists s_1' and s_2' such that $\mu_1(s_1') > 0$, $\delta(s_1', s_2') > 0$ and $(s_1', s_2') \notin \mathcal{R}_k$. Since $(s_1', s_2') \notin \mathcal{R}_k$, we have that $\mathsf{Ind}_{\mathcal{R}}(s_1', s_2') < k$. As a consequence, there exists $s_1' \in S_1, s_2' \in S_2$ such that $\mu_1(s_1') > 0, s_2' = \mathsf{succ}_{s_2,e}(s_1')$ and $\mathsf{Ind}_{\mathcal{R}}(s_1', s_2') < \mathsf{Ind}_{\mathcal{R}}(s_1, s_2)$. □

In other words, the above lemma ensures that a pair (s_1', s_2') such that $\mathsf{Ind}_{\mathcal{R}}(s_1', s_2') = 0$ can be reached within a bounded number of transitions for all pairs of states (s_1, s_2) in case 3. As explained above, this is a prerequisite for the correctness of the counterexample construction defined hereafter.

We now propose a construction to build counterexamples. Let $N_1 = (S_1, A, L_1, AP, V_1, \{s_0^1\})$ and $N_2 = (S_2, A, L_2, AP, V_2, \{s_0^2\})$ be deterministic APAs in SVNF such that $N_1 \not\preceq N_2$. Let $\mathcal{R}$ be the maximal refinement relation between N_1 and N_2.

Definition 9. The counterexample $P = (S, A, L, AP, V, s_0)$ is computed as follows:

- $S = S_1 \times (S_2 \cup \{\bot\})$, $s_0 = (s_0^1, s_0^2)$,
- $V(s_1, s_2) = v \in 2^{AP}$ such that $V_1(s_1) = \{v\}$ for all $(s_1, s_2) \in S$, and
- L is defined as follows. Let $(s_1, s_2) \in S$.
  - If (s_1, s_2) in case 1 or 2 or $s_2 = \bot$, then for all $a \in A$ and $\varphi_1 \in C(S_1)$ such that $L_1(s_1, a, \varphi_1) = \top$, let μ_1 be an arbitrary distribution in $Sat(\varphi_1)$ and let $L((s_1, s_2), a, \mu_1^\bot) = \top$ with $\mu_1^\bot \in Dist(S)$ such that $\mu_1^\bot(s_1', s_2') = \mu_1(s_1')$ if $s_2' = \bot$ and 0 otherwise.
  - Else, (s_1, s_2) is in case 3 and $B(s_1, s_2) \neq \emptyset$. For all $a \in A \setminus B(s_1, s_2)$ and $\varphi_1 \in C(S_1)$ such that $L_1(s_1, a, \varphi_1) = \top$, let μ_1 be an arbitrary distribution in $Sat(\varphi_1)$ and let $L((s_1, s_2), a, \mu_1^\bot) = \top$, with $\mu_1^\bot$ defined as above.
    In addition, for all $e \in B(s_1, s_2)$, let $L((s_1, s_2), e, .)$ be defined as in Table 3. In the table, given constraints $\varphi_1 \in C(S_1)$ and $\varphi_2 \in C(S_2)$ such that $L_1(s_1, e, \varphi_1) \neq \bot$ and $L_2(s_2, e, \varphi_2) \neq \bot$, and a distribution $\mu_1 \in Sat(\varphi_1)$, the distribution $\widehat{\mu_1} \in Dist(S)$ is defined as follows: $\widehat{\mu_1}(s_1', s_2') = \mu_1(s_1)$ if $s_2' = \mathsf{succ}_{s_2,e}(s_1')$ or $\mathsf{succ}_{s_2,e}(s_1') = \emptyset$ and $s_2' = \bot$, and 0 otherwise.

Theorem 9. The counterexample PA P defined above is such that $P \models N_1$ and $P \not\models N_2$.

The proof of the theorem is similar to the one of Theorem 2 and available in appendix.

6. Conclusion

We have in this paper added an important aspect to the specification theory of Abstract Probabilistic Automata, in that we have shown how to exhaustively characterize the *difference* between two deterministic specifications. In a stepwise refinement methodology, difference is an important tool to gauge refinement failures.

We have also introduced a notion of *discounted distance* between specifications which can be used as another measure for how far one specification is from being a refinement of another. Using this distance, we were able to show that our sequence of under-approximations converges, semantically, to the real difference of sets of implementations, and that our over-approximation is infinitesimally close to the real difference.

There are many different ways to measure distances between implementations and specifications, allowing to put the focus on either transient or steady-state behavior. In this paper we have chosen one specific discounted distance, placing the focus on transient behavior. Apart from the fact that this can indeed be a useful distance in practice, we remark that the convergence results about our under- and over-approximations are topological in nature and hence apply with respect to all distances which are topologically equivalent to the specific one used here, typically discounted distances. Although the results presented in the paper do not hold in general for the accumulating (undiscounted) distance, there are other notions of distances that are more relevant for steady-state behavior, e.g. limit-average. Whether our results hold in this setting remains future work.

We also remark that we have shown that it is not more difficult to compute the difference of two APAs than to check for their refinement. Hence if a refinement failure is detected (for example by using the methods in the APAC tool [21]), it is not difficult to also compute the difference for assessing the reason for refinement failure. For the class of APAs with polynomial constraints, which is the one implemented in APAC, refinement checking can be

done in time quadratic in the number of states and doubly-exponential in the number of constraints [20]; in APAC, the Z3 solver [16] is used for operations on constraints.

One limitation of our approach is the use of *deterministic* APAs. Even though deterministic specifications are generally considered to suffice from a modeling point of view [35], non-determinism may be introduced for example when composing specifications. Indeed, our constructions themselves introduce non-determinism: for deterministic APAs N_1, N_2, both $N_1 \setminus^* N_2$ and $N_1 \setminus^K N_2$ may be non-deterministic. Hence it is of interest to extend our approach to non-deterministic specifications. The problem here is, however, that for non-deterministic specifications, the relation between refinement and inclusion of sets of implementations $N_1 \preceq N_2 \iff [\![N_1]\!] \subseteq [\![N_2]\!]$ breaks: we may well have $N_1 \not\preceq N_2$ but $[\![N_1]\!] \subseteq [\![N_2]\!]$, cf. [18]. So the technique we have used in this paper to compute differences will not work for non-deterministic APAs, and techniques based on *thorough refinement* will have to be used.

As a last note, we wish to compare our approach of difference between APA specifications with the use of *counterexamples* in probabilistic model checking. Counterexample generation is studied in a number of papers [2,4,11,25,28,30,33,42,48,49], typically with the purpose of embedding it into a procedure of counterexample guided abstraction refinement (CEGAR). The focus typically is on generation of *one* particular counterexample to refinement, which can then be used to adapt the abstraction accordingly.

In contrast, although we propose a construction for building single counter-examples, our main focus is on computing APA difference, i.e. generating a representation of *all counterexamples*. Our goal is not to refine abstractions at *system* level, using counterexamples, but to assess *specifications*. This is, then, the reason why we want to compute all counterexamples instead of only one. Our work is hence supplementary and orthogonal to the CEGAR-type use of counterexamples: CEGAR procedures can be used also to refine APA specifications, but only our difference can assess the precise distinction between specifications.

References

[1] Charalambos D. Aliprantis and Kim C. Border. *Infinite Dimensional Analysis: A Hitchhiker's Guide*. Springer, 3rd edition, 2007.

[2] Husain Aljazzar and Stefan Leue. Directed explicit state-space search in the generation of counterexamples for stochastic model checking. *IEEE Trans. Software Eng.*, 36(1):37–60, 2010.

[3] Rajeev Alur, Tomás Feder, and Thomas A. Henzinger. The benefits of relaxing punctuality. *J. ACM*, 43(1):116–146, 1996.

[4] Miguel E. Andrés, Pedro R. D'Argenio, and Peter van Rossum. Significant diagnostic counterexamples in probabilistic model checking. In Hana Chockler and Alan J. Hu, editors, *HVC*, volume 5394 of *Lecture Notes Comput. Sci.*, pages 129–148. Springer, 2008.

[5] Christel Baier and Joost-Pieter Katoen. *Principles of Model Checking*. MIT Press, 2008.

[6] Sebastian S. Bauer, Uli Fahrenberg, Line Juhl, Kim G. Larsen, Axel Legay, and Claus Thrane. Quantitative refinement for weighted modal transition systems. In Filip Murlak and Piotr Sankowski, editors, *MFCS*, volume 6907 of *Lecture Notes Comput. Sci.*, pages 60–71. Springer, 2011.

[7] Sebastian S. Bauer, Uli Fahrenberg, Line Juhl, Kim G. Larsen, Axel Legay, and Claus Thrane. Weighted modal transition systems. *Formal Methods in System Design*, 42(2):193–220, 2013.

[8] Sebastian S. Bauer, Uli Fahrenberg, Axel Legay, and Claus Thrane. General quantitative specification theories with modalities. In Edward A. Hirsch, Juhani Karhumäki, Arto Lepistö, and Michail Prilutskii, editors, *CSR*, volume 7353 of *Lecture Notes Comput. Sci.*, pages 18–30. Springer, 2012.

[9] Marcello M. Bonsangue, Franck van Breugel, and Jan J. M. M. Rutten. Generalized metric spaces: Completion, topology, and powerdomains via the Yoneda embedding. *Theor. Comput. Sci.*, 193(1-2):1–51, 1998.

[10] Benoît Caillaud, Benoît Delahaye, Kim G. Larsen, Axel Legay, Mikkel L. Pedersen, and Andrzej Wąsowski. Constraint Markov chains. *Theor. Comput. Sci.*, 412(34):4373–4404, 2011.
[11] Rohit Chadha and Mahesh Viswanathan. A counterexample-guided abstraction-refinement framework for Markov decision processes. *ACM Trans. Comput. Log.*, 12(1):1, 2010.
[12] Jamieson M. Cobleigh, George S. Avrunin, and Lori A. Clarke. Breaking up is hard to do: An evaluation of automated assume-guarantee reasoning. *ACM Trans. Softw. Eng. Methodol.*, 17(2), 2008.
[13] Jamieson M. Cobleigh, Dimitra Giannakopoulou, and Corina S. Pasareanu. Learning assumptions for compositional verification. In Hubert Garavel and John Hatcliff, editors, *TACAS*, volume 2619 of *Lecture Notes Comput. Sci.*, pages 331–346. Springer, 2003.
[14] Luca de Alfaro and Thomas A. Henzinger. Interface automata. In *ESEC / SIGSOFT FSE*, pages 109–120. ACM, 2001.
[15] Luca de Alfaro, Rupak Majumdar, Vishwanath Raman, and Mariëlle Stoelinga. Game relations and metrics. In *LICS*, pages 99–108. IEEE Computer Society, 2007.
[16] Leonardo Mendonça de Moura and Nikolaj Bjørner. Z3: An efficient SMT solver. In C. R. Ramakrishnan and Jakob Rehof, editors, *TACAS*, volume 4963 of *Lecture Notes Comput. Sci.*, pages 337–340. Springer, 2008.
[17] Benoît Delahaye, Uli Fahrenberg, Kim G. Larsen, and Axel Legay. Refinement and difference for probabilistic automata. In Kaustubh R. Joshi, Markus Siegle, Mariëlle Stoelinga, and Pedro R. D'Argenio, editors, *QEST*, volume 8054 of *Lecture Notes Comput. Sci.*, pages 22–38. Springer, 2013.
[18] Benoît Delahaye, Joost-Pieter Katoen, Kim G. Larsen, Axel Legay, Mikkel L. Pedersen, Falak Sher, and Andrzej Wąsowski. Abstract probabilistic automata. In *VMCAI*, volume 6538 of *Lecture Notes Comput. Sci.*, pages 324–339. Springer, 2011.
[19] Benoît Delahaye, Joost-Pieter Katoen, Kim G. Larsen, Axel Legay, Mikkel L. Pedersen, Falak Sher, and Andrzej Wąsowski. New results on abstract probabilistic automata. In Benoît Caillaud, Josep Carmona, and Kunihiko Hiraishi, editors, *ACSD*, pages 118–127. IEEE, 2011.
[20] Benoît Delahaye, Joost-Pieter Katoen, Kim G. Larsen, Axel Legay, Mikkel L. Pedersen, Falak Sher, and Andrzej Wąsowski. Abstract probabilistic automata. *Inf. Comp.*, 232:66–116, 2013.
[21] Benoît Delahaye, Kim G. Larsen, Axel Legay, Mikkel L. Pedersen, and Andrzej Wąsowski. APAC: A tool for reasoning about abstract probabilistic automata. In *QEST*, pages 151–152. IEEE, 2011.
[22] Josee Desharnais, Vineet Gupta, Radha Jagadeesan, and Prakash Panangaden. Metrics for labelled Markov processes. *Theor. Comput. Sci.*, 318(3):323–354, 2004.
[23] Uli Fahrenberg, Axel Legay, and Claus Thrane. The quantitative linear-time–branching-time spectrum. In Supratik Chakraborty and Amit Kumar, editors, *FSTTCS*, volume 13 of *LIPIcs*, pages 103–114. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2011.
[24] Harald Fecher, Martin Leucker, and Verena Wolf. Don't know in probabilistic systems. In *SPIN*, volume 3925 of *Lecture Notes Comput. Sci.*, pages 71–88. Springer, 2006.
[25] Tingting Han, Joost-Pieter Katoen, and Berteun Damman. Counterexample generation in probabilistic model checking. *IEEE Trans. Software Eng.*, 35(2):241–257, 2009.
[26] Hans Hansson and Bengt Jonsson. A logic for reasoning about time and reliability. *Formal Asp. Comput.*, 6(5):512–535, 1994.
[27] Holger Hermanns, Ulrich Herzog, and Joost-Pieter Katoen. Process algebra for performance evaluation. *Theor. Comput. Sci.*, 274(1-2):43–87, 2002.
[28] Holger Hermanns, Björn Wachter, and Lijun Zhang. Probabilistic CEGAR. In Aarti Gupta and Sharad Malik, editors, *CAV*, volume 5123 of *Lecture Notes Comput. Sci.*, pages 162–175. Springer, 2008.
[29] Andrew Hinton, Marta Z. Kwiatkowska, Gethin Norman, and David Parker. PRISM: A tool for automatic verification of probabilistic systems. In *TACAS*, volume 3920 of *Lecture Notes Comput. Sci.*, pages 441–444. Springer, 2006.
[30] Nils Jansen, Erika Ábrahám, Jens Katelaan, Ralf Wimmer, Joost-Pieter Katoen, and Bernd Becker. Hierarchical counterexamples for discrete-time Markov chains. In Tevfik Bultan and Pao-Ann Hsiung, editors, *ATVA*, volume 6996 of *Lecture Notes Comput. Sci.*, pages 443–452. Springer, 2011.
[31] Bengt Jonsson and Kim G. Larsen. Specification and refinement of probabilistic processes. In *LICS*, pages 266–277. IEEE, 1991.
[32] Joost-Pieter Katoen, Daniel Klink, Martin Leucker, and Verena Wolf. Three-valued abstraction for continuous-time Markov chains. In *CAV*, volume 4590 of *Lecture Notes Comput. Sci.*, pages 311–324. Springer, 2007.

[33] Anvesh Komuravelli, Corina S. Pasareanu, and Edmund M. Clarke. Assume-guarantee abstraction refinement for probabilistic systems. In P. Madhusudan and Sanjit A. Seshia, editors, *CAV*, volume 7358 of *Lecture Notes Comput. Sci.*, pages 310–326. Springer, 2012.

[34] Marta Z. Kwiatkowska, Gethin Norman, David Parker, and Hongyang Qu. Assume-guarantee verification for probabilistic systems. In *TACAS*, volume 6015 of *Lecture Notes Comput. Sci.*, pages 23–37. Springer, 2010.

[35] Kim G. Larsen. Modal specifications. In Joseph Sifakis, editor, *Automatic Verification Methods for Finite State Systems*, volume 407 of *Lecture Notes Comput. Sci.*, pages 232–246. Springer, 1989.

[36] Kim G. Larsen, Uli Fahrenberg, and Claus Thrane. Metrics for weighted transition systems: Axiomatization and complexity. *Theor. Comput. Sci.*, 412(28):3358–3369, 2011.

[37] Nancy Lynch and Mark R. Tuttle. An introduction to Input/Output automata. *CWI*, 2(3), 1989.

[38] Nancy A. Lynch. *Distributed Algorithms*. Morgan Kaufmann, 1996.

[39] Zohar Manna and Amir Pnueli. *The Temporal Logic of Reactive and Concurrent Systems*. Springer, 1992.

[40] Jean-Baptiste Raclet. *Quotient de spécifications pour la réutilisation de composants*. PhD thesis, Université de Rennes I, December 2007. (In French).

[41] Mathieu Sassolas, Marsha Chechik, and Sebastián Uchitel. Exploring inconsistencies between modal transition systems. *Software and System Modeling*, 10(1):117–142, 2011.

[42] Matthias Schmalz, Daniele Varacca, and Hagen Völzer. Counterexamples in probabilistic LTL model checking for Markov chains. In Mario Bravetti and Gianluigi Zavattaro, editors, *CONCUR*, volume 5710 of *Lecture Notes Comput. Sci.*, pages 587–602. Springer, 2009.

[43] Roberto Segala and Nancy A. Lynch. Probabilistic simulations for probabilistic processes. In Bengt Jonsson and Joachim Parrow, editors, *CONCUR*, volume 836 of *Lecture Notes Comput. Sci.*, pages 481–496. Springer, 1994.

[44] Falak Sher and Joost-Pieter Katoen. Compositional abstraction techniques for probabilistic automata. In Jos C. M. Baeten, Thomas Ball, and Frank S. de Boer, editors, *IFIP TCS*, volume 7604 of *Lecture Notes Comput. Sci.*, pages 325–341. Springer, 2012.

[45] Claus Thrane, Uli Fahrenberg, and Kim G. Larsen. Quantitative analysis of weighted transition systems. *J. Logic Algeb. Prog.*, 79(7):689–703, 2010.

[46] Franck van Breugel, Michael W. Mislove, Joël Ouaknine, and James Worrell. An intrinsic characterization of approximate probabilistic bisimilarity. In Andrew D. Gordon, editor, *FoSSaCS*, volume 2620 of *Lecture Notes Comput. Sci.*, pages 200–215. Springer, 2003.

[47] Moshe Y. Vardi. Automatic verification of probabilistic concurrent finite-state programs. In *FOCS*, pages 327–338. IEEE, 1985.

[48] Ralf Wimmer, Bettina Braitling, and Bernd Becker. Counterexample generation for discrete-time Markov chains using bounded model checking. In Neil D. Jones and Markus Müller-Olm, editors, *VMCAI*, volume 5403 of *Lecture Notes Comput. Sci.*, pages 366–380. Springer, 2009.

[49] Ralf Wimmer, Nils Jansen, Erika Ábrahám, Bernd Becker, and Joost-Pieter Katoen. Minimal critical subsystems for discrete-time Markov models. In Cormac Flanagan and Barbara König, editors, *TACAS*, volume 7214 of *Lecture Notes Comput. Sci.*, pages 299–314. Springer, 2012.

Appendix: Proof of Theorem 3

Proof of Theorem 3. For the first claim, consider the relation $\mathcal{R} \subseteq (S_1 \times (S_2 \cup \{\bot\}) \times (A \cup \{\varepsilon\}) \times \{1, \dots, K\}) \times (S_1 \times (S_2 \cup \{\bot\}) \times (A \cup \{\varepsilon\}) \times \{1, \dots, K+1\})$ such that $\mathcal{R} = \{((s_0^1, s_0^2, e, K), (s_0^1, s_0^2, e, K+1)) \mid e \in B(s_0^1, s_0^2)\} \cup \mathcal{R}_{\mathsf{id}}$, where $\mathcal{R}_{\mathsf{id}}$ denotes the identity relation. One can verify that, by construction, $\mathcal{R}$ is a refinement relation witnessing $N_1 \setminus^K N_2 \preceq N_1 \setminus^{K+1} N_2$.

Let $N_1 = (S_1, A, L_1, AP, V_1, \{s_0^1\})$ and $N_2 = (S_2, A, L_2, AP, V_2, \{s_0^2\})$ be deterministic APAs in single valuation normal form such that $N_1 \not\preceq N_2$. Let $\mathcal{R}$ be the maximal refinement relation between N_1 and N_2.

1. We first prove that for all $K \in \mathbb{N}$, $[\![N_1 \setminus^K N_2]\!] \subseteq [\![N_1]\!] \setminus [\![N_2]\!]$. If $V_1(s_0^1) \neq V_2(s_0^2)$, then for all $K \in \mathbb{N}$, we have $N_1 \setminus^K N_2 = N_1$ and the result holds.

Otherwise, assume that (s_0^1, s_0^2) is in case 3 and let $K \in \mathbb{N}$. We have $N_1 \setminus^K N_2 = (S, A, L, AP, V, S_0^K)$ defined as in Section 4.3. Let $P = (S_P, A, L_P, AP, V_P, s_0^P)$ be a PA such that $P \models N_1 \setminus^K N_2$. Let $\mathcal{R}^\setminus \subseteq S_P \times S$ be the associated satisfaction relation and let $f \in B(s_0^1, s_0^2)$ be such that $s_0^P \, \mathcal{R}^\setminus (s_0^1, s_0^2, f, K)$. We show that $P \models N_1$ and $P \not\models N_2$.

We start by proving that $P \models N_1$. Consider the relation $\mathcal{R}_1 \subseteq S_P \times S_1$ such that $p \, \mathcal{R}_1 \, s_1 \iff \exists s_2 \in (S_2 \cup \{\bot\}), \exists e \in (A \cup \{\varepsilon\}), \exists n \leq K$ s.t. $p \, \mathcal{R}^\setminus (s_1, s_2, e, n)$. We prove that $\mathcal{R}_1$ is a satisfaction relation. Let p, s_1, s_2, e, n such that $p \, \mathcal{R}_1 \, s_1$ and $p \, \mathcal{R}^\setminus (s_1, s_2, e, n)$.

- By construction, we have $V_P(p) \in V((s_1, s_2, e, n)) = V_1(s_1)$.
- Let $a \in A$ and $\mu_P \in Dist(S_P)$ be such that $L_P(p, a, \mu_P) = \top$. By $\mathcal{R}^\setminus$, there exists $\varphi \in C(S)$ such that $L((s_1, s_2, e, n), a, \varphi) \neq \bot$ and there exists $\mu \in Sat(\varphi)$ such that $\mu_P \Subset_{\mathcal{R}^\setminus} \mu$.

  If $s_2 = \bot$ or $e = \varepsilon$ or $a \neq e$, then by construction of $N_1 \setminus^K N_2$, there exists $\varphi_1 \in C(S_1)$ such that $\varphi = \varphi_1^\bot$ and $L_1(s_1, a, \varphi_1) \neq \bot$. As a consequence, the distribution $\mu \downarrow_1 \colon s_1' \mapsto \mu(s_1', \bot, \varepsilon, 1)$ is in $Sat(\varphi_1)$ and it follows that $\mu_P \Subset_{\mathcal{R}_1} \mu \downarrow_1$.

  Otherwise, assume that $s_2 \in S_2$, $e \in A$ and $a = e$. There are several cases.
  - If $e \in B_a(s_1, s_2) \cup B_b(s_1, s_2)$, then by construction of $N_1 \setminus^K N_2$, there exists $\varphi_1 \in C(S_1)$ such that $L_1(s_1, e, \varphi_1) \neq \bot$ and $\varphi = \varphi_1^\bot$. As above, we thus have $\mu_P \Subset_{\mathcal{R}_1} \mu \downarrow_1$.
  - Else, if $e \in B_e(s_1, s_2)$, then there exists $\varphi_1 \in C(S_1)$ and $\varphi_2 \in C(S_2)$ such that $L_1(s_1, e, \varphi_1) =?$ and $L_2(s_2, e, \varphi_2) = \top$. Moreover, φ is of the form φ_{12}^B, and $\mu' \in Sat(\varphi_{12}^B)$ implies that the distribution μ_1' such that $\mu_1' : s_1' \mapsto \sum_{c \in A \cup \{\varepsilon\}, s_2' \in S_2 \cup \{\bot\}, k' \geq 1} \mu(s_1', s_2', c, k')$ satisfies φ_1. Thus, the distribution $\mu_1 : s_1' \mapsto \sum_{c \in A \cup \{\varepsilon\}, s_2' \in S_2 \cup \{\bot\}, k' \geq 1} \mu(s_1', s_2', c, k')$ satisfies φ_1. Let $\delta_1 : S_P \to (S_1 \to [0,1])$ be such that $\delta_1(p')(s_1') = 1$ if $\mu_P(p') > 0$ and $s_1' = \mathsf{succ}_{s_1, e}(p')$ and 0 otherwise. By construction, δ_1 is a correspondence function and we have $\mu_P \delta_1 = \mu_1$. Thus there exists $\mu_1 \in Sat(\varphi_1)$ such that $\mu_P \Subset_{\mathcal{R}_1} \mu_1$.
  - Finally, if $e \in B_c(s_1, s_2) \cup B_f(s_1, s_2)$, then there exists $\varphi_1 \in C(S_1)$ such that $L(s_1, e, \varphi_1) \neq \bot$, and either $\varphi = \varphi_1^\bot$ or $\varphi = \varphi_{12}^B$ as in the case above. In both cases, as proven before, there exists $\mu_1 \in Sat(\varphi_1)$ such that $\mu_P \Subset_{\mathcal{R}_1} \mu_1$.
- Let $a \in A$ and $\varphi_1 \in C(S_1)$ such that $L_1(s_1, a, \varphi_1) = \top$.

  If $s_2 = \bot$ or $e = \varepsilon$ or $a \neq e$, then by construction of $N_1 \setminus^K N_2$, the constraint $\varphi_1^\bot$ is such that $L((s_1, s_2, e, n), a, \varphi_1^\bot) = \top$. As a consequence, there exists a distribution $\mu_P \in Dist(S_P)$ such that $L_P(p, a, \mu_P) = \top$ and there exists $\mu \in Sat(\varphi_1^\bot)$ such

that $\mu_P \Subset_{\mathcal{R}^\setminus} \mu$. Moreover, by construction of $\varphi_1^\perp$, the distribution $\mu \downarrow_1 : s_1' \mapsto \mu(s_1', \perp, \varepsilon, 1)$ is in $Sat(\varphi_1)$ and it follows that $\mu_P \Subset_{\mathcal{R}_1} \mu \downarrow_1$.

Otherwise, assume that $s_2 \in S_2$, $e \in A$ and $a = e$. Since $L_1(s_1, a, \varphi_1) = \top$, (s_1, s_2) can only be in cases $3.a, 3.c$ or $3.f$. As a consequence, $e \in B_a(s_1, s_2) \cup B_c(s_1, s_2) \cup B_f(s_1, s_2)$. By construction, in all of these cases, we have $L((s_1, s_2, e, n), a, \varphi_1^\perp) = \top$. Thus, there exists a distribution $\mu_P \in Dist(S_P)$ such that $L_P(p, a, \mu_P) = \top$ and there exists $\mu \in Sat(\varphi_1^\perp)$ such that $\mu_P \Subset_{\mathcal{R}^\setminus} \mu$. As above, it follows that $\mu_P \Subset_{\mathcal{R}_1} \mu \downarrow_1$.

Finally, $\mathcal{R}_1$ is a satisfaction relation. Moreover, by hypothesis, we have $s_0^P \, \mathcal{R}^\setminus(s_0^1, s_0^2, f, K)$, thus $s_0^P \, \mathcal{R}_1 \, s_0^1$ and $P \models N_1$.

We now prove that $P \not\models N_2$. Assume the contrary and let $\mathcal{R}_2 \subseteq S_P \times S_2$ be the smallest satisfaction relation witnessing $P \models N_2$ (i.e. containing only reachable states). We prove the following by induction on the value of n, for $1 \leq n \leq K$: $\forall p \in S_P, s_2 \in S_2$, if there exists $s_1 \in S_1$ and $e \in A$ such that $p \, \mathcal{R}^\setminus(s_1, s_2, e, n)$, then $(p, s_2) \notin \mathcal{R}_2$.

- **Base Case ($n = 1$).** Let p, s_1, s_2, e such that $p \, \mathcal{R}^\setminus(s_1, s_2, e, 1)$. If $e \in B_a(s_1, s_2) \cup B_b(s_1, s_2) \cup B_d(s_1, s_2)$, then by construction there is an e transition in either P or N_2 that cannot be matched by the other. Thus $(p, s_2) \notin \mathcal{R}_2$. The same is verified if $e \in B_e(s_1, s_2)$ and there is no distribution $\mu_P \in Dist(S_P)$ such that $L_P(p, e, \mu_P) = \top$.

  Otherwise, $e \in B_e(s_1, s_2) \cup B_c(s_1, s_2) \cup B_f(s_1, s_2)$ and there exists $\mu_P \in Dist(S_P)$ such that $L_P(p, e, \mu_P) = \top$. Let $\varphi_1 \in C(S_1)$ and $\varphi_2 \in C(S_2)$ be the corresponding constraints in N_1 and N_2. Consider the corresponding constraint $\varphi_{12}^{B,1} \in C(S)$. By $\mathcal{R}^\setminus$, there exists $\mu \in Sat(\varphi_{12}^{B,1})$ such that $\mu_P \Subset_{\mathcal{R}^\setminus} \mu$. By construction of $\varphi_{12}^{B,1}$, we know that either (3.a) there exists $(s_1', \perp, \varepsilon, 1)$ such that $\mu(s_1', \perp, \varepsilon, 1) > 0$ or (3.b) the distribution $\mu_2 : s_2' \mapsto \sum_{c \in A \cup \{\varepsilon\}, s_1' \in S_1, k' \geq 1} \mu(s_1', s_2', c, k')$ does not satisfy φ_2. If there exists $(s_1', \perp, \varepsilon, 1)$ such that $\mu(s_1', \perp, \varepsilon, 1) > 0$, then there exists $p' \in S_P$ such that $\mu_P(p') > 0$ and $\mathsf{succ}_{s_2,e}(p') = \emptyset$. Thus there cannot exists $\mu_2' \in Sat(\varphi_2)$ such that $\mu_P \Subset_{\mathcal{R}_2} \mu_2'$. Otherwise, by determinism of N_2, we know that the only possible correspondence function for μ_P and $\mathcal{R}_2$ is $\delta_2 : S_P \to (S_2 \to [0, 1])$ such that $\delta_2(p')(s_2') = 1$ if $s_2' = \mathsf{succ}_{s_2,e}(p')$ and 0 otherwise. By construction, we have $\mu_P \delta_2 = \mu_2$ and thus there is no distribution $\mu_2' \in Sat(\varphi_2)$ such that $\mu_P \Subset_{\mathcal{R}_2} \mu_2'$. Consequently, $(p, s_2) \notin \mathcal{R}_2$.
- **Induction.** Let $1 < n \leq K$ and assume that for all $k < n$, for all $p' \in S_P, s_2' \in S_2$, whenever there exists $s_1' \in S_1$ and $e \in A$ such that $p' \, \mathcal{R}^\setminus(s_1', s_2', e, k)$, we have $(p', s_2') \notin \mathcal{R}_2$. Let p, s_1, s_2, e such that $p \, \mathcal{R}^\setminus(s_1, s_2, e, n)$. If $e \in B_a(s_1, s_2) \cup B_b(s_1, s_2) \cup B_d(s_1, s_2)$, then by construction there is an e transition in either P or N_2 that cannot be matched by the other. Thus $(p, s_2) \notin \mathcal{R}_2$. The same is verified if $e \in B_e(s_1, s_2)$ and there is no distribution $\mu_P \in Dist(S_P)$ such that $L_P(p, e, \mu_P) = \top$. Else, $e \in B_e(s_1, s_2) \cup B_c(s_1, s_2) \cup B_f(s_1, s_2)$ and there exists $\mu_P \in Dist(S_P)$ such that $L_P(p, e, \mu_P) = \top$. Let $\varphi_1 \in C(S_1)$ and $\varphi_2 \in C(S_2)$ be the corresponding constraints in N_1 and N_2.

  Consider the corresponding constraint $\varphi_{12}^{B,n} \in C(S)$. By $\mathcal{R}^\setminus$, there exists $\mu \in Sat(\varphi_{12}^{B,n})$ such that $\mu_P \Subset_{\mathcal{R}^\setminus} \mu$. By construction of $\varphi_{12}^{B,n}$, we know that either (3.a) there exists $(s_1', \perp, c, 1)$ such that $\mu(s_1', \perp, c, 1) > 0$ or (3.b) the distribution $\mu_2 : s_2' \mapsto \sum_{c \in A \cup \{\varepsilon\}, s_1' \in S_1, k' \geq 1} \mu(s_1', s_2', c, k')$ does not satisfy φ_2, or (3.c) there exists $s_1' \in S_1$, $s_2' \in S_2$, $c \neq \varepsilon$ and $k < n$ such that $\mu(s_1', s_2', c, k) > 0$. If case (3.a) or

(3.b) holds, then as in the base case, there is no distribution $\mu_2' \in Sat(\varphi_2)$ such that $\mu_P \Subset_{\mathcal{R}_2} \mu_2'$. Otherwise, if (3.c) holds, then there exists $p' \in S_P$ such that $\mu_P(p') > 0$ and $p' \,\mathcal{R}^{\setminus}(s_1', s_2', c, k)$. By induction, we thus know that $(p', s_2') \notin \mathcal{R}_2$ and by construction and determinism of N_2, we have that $\mathsf{succ}_{s_2,e}(p') = \{s_2'\}$. Thus there is no distribution $\mu_2' \in Sat(\varphi_2)$ such that $\mu_P \Subset_{\mathcal{R}_2} \mu_2'$. Consequently, $(p, s_2) \notin \mathcal{R}_2$.

By hypothesis, we have $s_0^P \,\mathcal{R}^{\setminus}(s_0^1, s_0^2, f, K)$. As a consequence, we have that $(s_0^P, s_0^2) \notin \mathcal{R}_2$, implying that $P \not\models N_2$.

2. We now prove that for all PA $P \in [\![N_1]\!] \setminus [\![N_2]\!]$, there exists $K \in \mathbb{N}$ such that $P \in [\![N_1 \setminus^K N_2]\!]$. If $V_1(s_0^1) \neq V_2(s_0^2)$, then for all $K \in \mathbb{N}$, we have $N_1 \setminus^K N_2 = N_1$ and the result holds.

Otherwise, assume that (s_0^1, s_0^2) is in case 3. Let $P = (S_P, A, L_P, AP, V_P, s_0^P)$ be a PA such that $P \models N_1$ and $P \not\models N_2$. Let $\mathcal{R}_1$ be the satisfaction relation witnessing $P \models N_1$ and $\mathcal{R}_2$ be the maximal satisfaction relation between P and N_2. Assume that $\mathcal{R}_2$ is computed as described in Section 5. Let $\mathsf{Ind}_{\mathcal{R}_2}$ be the associated index function and let K be the minimal index such that $\mathcal{R}_{2K} = \mathcal{R}_2$. We show that $P \models N_1 \setminus^K N_2$. Let $N_1 \setminus^K N_2 = (S, A, L, AP, V, S_0)$ be defined as in Section 4.3.

Let $\mathcal{R}^{\setminus} \subseteq S_P \times S_2$ be the relation such that

$$p \,\mathcal{R}^{\setminus}(s_1, s_2, e, k) \iff \begin{cases} (p \,\mathcal{R}_1 \, s_1) \text{ and } (s_2 = \bot) \text{ and } (e = \varepsilon) \text{ and } (k = 1) \\ \text{or} \begin{cases} (p \,\mathcal{R}_1 \, s_1) \text{ and } (p, s_2) \text{ in case 1 or 2 and } (e = \varepsilon) \\ \qquad\qquad \text{and } (k = 1) \end{cases} \\ \text{or} \begin{cases} (p \,\mathcal{R}_1 \, s_1) \text{ and } (p, s_2) \text{ in case 3 and } (e \in \mathsf{Break}(p, s_2)) \\ \qquad\qquad \text{and } (k = \mathsf{Ind}_{\mathcal{R}_2}(p, s_2) + 1) \end{cases} \end{cases}$$

Remark that whenever (p, s_2) is in case 3, we know that $\mathsf{Ind}_{\mathcal{R}_2}(p, s_2) < K$, thus $\mathsf{Ind}_{\mathcal{R}_2}(p, s_2) + 1 \leq K$.

We prove that $\mathcal{R}^{\setminus}$ is a satisfaction relation. Let $p \,\mathcal{R}^{\setminus}(s_1, s_2, e, k)$. If $s_2 = \bot$ or $e = \varepsilon$, then since $p \,\mathcal{R}_1 \, s_1$, $\mathcal{R}^{\setminus}$ satisfies the axioms of a satisfaction relation by construction.

Else we have $s_2 \in S_2$ and $e \neq \varepsilon$, thus, by definition of $\mathcal{R}^{\setminus}$, we know that (p, s_2) is in case 3. The rest of the proof is almost identical to the proof of Theorem 2. In the following, we report to this proof and only highlight the differences.

- By construction, we have $V_P(p) \in V_1(s_1) = V((s_1, s_2, e, k))$.
- Let $a \in A$ and $\mu_P \in Dist(S_P)$ such that $L_P(p, a, \mu_P) = \top$. There are several cases.
  - If $a \neq e$, or $a = e \in B_a(p, s_2)$, the proof is identical to the proof of Theorem 2.
  - Else, we necessarily have $a = e \in B_c(p, s_2) \cup B_f(p, s_2)$. Remark that, by construction, $B_c(p, s_2) \subseteq B_c(s_1, s_2)$ and $B_f(p, s_2) \subseteq B_f(s_1, s_2)$. Since $p \,\mathcal{R}_1 \, s_1$, there exists $\varphi_1 \in C(S_1)$ such that $L_1(s_1, e, \varphi_1) \neq \bot$ and there exists $\mu_1 \in Sat(\varphi_1)$ and a correspondence function $\delta_1 : S_P \to (S_1 \to [0, 1])$ such that $\mu_P \Subset^{\delta_1}_{\mathcal{R}_1} \mu_1$.

    Moreover, by construction of $N_1 \setminus^K N_2$, we know that the constraint $\varphi_{12}^{B,k}$ is such that $L((s_1, s_2, e, k), e, \varphi_{12}^{B,k}) = \top$.

    We now prove that there exists $\mu \in Sat(\varphi_{12}^{B,k})$ such that $\mu_P \Subset_{\mathcal{R}^{\setminus}} \mu$. Consider the function $\delta : S_P \to (S \to [0, 1])$ defined as follows: Let $p' \in S_P$ such that $\mu_P(p') > 0$ and let $s_1' = \mathsf{succ}_{s_1,e}(p')$, which exists by $\mathcal{R}_1$.
    - If $\mathsf{succ}_{s_2,e}(p') = \emptyset$, then $\delta(p')(s_1', \bot, \varepsilon, 1) = 1$.
    - Else, let $s_2' = \mathsf{succ}_{s_2,e}(p')$. Then,
      - if $(p', s_2') \in \mathcal{R}_2$, then $\delta(p')(s_1', s_2', \varepsilon, 1) = 1$.

· Else, (p', s'_2) is in case 3 and $\mathsf{Break}(p', s'_2) \neq \emptyset$. In this case, let $c \in \mathsf{Break}(p', s'_2)$ and define $\delta(p', (s'_1, s'_2, c, \mathsf{Ind}_{\mathcal{R}_2}(p', s'_2) + 1)) = 1$. For all other $c' \in A$ and $1 \leq k' \leq K$, define $\delta(p', (s'_1, s'_2, c', k')) = 0$.

Remark that for all $p' \in S_P$ such that $\mu_P(p') > 0$, there exists a unique $s' \in S'$ such that $\delta(p')(s') = 1$. Thus δ is a correspondence function.

We now prove that $\mu = \mu_P \delta \in Sat(\varphi_{12}^{B,k})$.

(1) Let $(s'_1, s'_2, c, k') \in S$ such that $\mu(s'_1, s'_2, c, k') > 0$. By construction, there exists $p' \in S_P$ such that $\mu_P(p') > 0$ and $\delta(p')(s'_1, s'_2, c, k') > 0$. Moreover, $c \in B(s'_1, s'_2) \cup \{\varepsilon\}$, $s'_2 = \perp$ if $\mathsf{succ}_{s_2,e}(s'_1) = \emptyset$ and $s'_2 = \mathsf{succ}_{s_2,e}(s'_1)$ otherwise.

(2) Consider the distribution $\mu'_1 : s'_1 \mapsto \sum_{c \in A \cup \{\varepsilon\}, s'_2 \in S_2 \cup \{\perp\}, k' \geq 1} \mu(s'_1, s'_2, c, k')$. By determinism (See Lemma 28 in [10]), we have that $\delta_1(p')(s'_1) = 1 \iff s'_1 = (succ)_{s_1,e}(p')$. As a consequence, we have that $\mu'_1 = \mu\delta_1 = \mu_1 \in Sat(\varphi_1)$.

(3) Depending on k, there are 2 cases.

∗ If $k > 1$, assume that for all $p' \in S_P$ such that $\mu_P(p') > 0$, we have $\mathsf{succ}_{s_2,e}(p') \neq \emptyset$ (the other case being trivial). Since $c \in (B_c(p, s_2) \cup B_f(p, s_2)) \cap \mathsf{Break}(p, s_2)$ by $\mathcal{R}^{\setminus}$, we can apply Lemma 8. As a consequence, either (2) $\mu_1^2 : \left(s'_2 \mapsto \sum_{p' \in P | s'_2 = \mathsf{succ}_{s_2,e}(p')} \mu_P(p')\right)$ does not satisfy φ_2, or (3) there exists $p' \in S_P$ and $s'_2 \in S_2$ such that $\mu_P(p') > 0$, $s'_2 = \mathsf{succ}_{s_2,e}(p')$ and $\mathsf{Ind}_{\mathcal{R}_2}(p', s'_2) < \mathsf{Ind}_{\mathcal{R}_2}(p, s_2)$.
In the first case (2), consider the distribution μ_2 defined as follows:

$$\mu_2 : s'_2 \mapsto \sum_{c \in A \cup \{\varepsilon\}, s'_1 \in S_1, k' \geq 1} \mu(s'_1, s'_2, c, k').$$

We have the following: for all $s'_2 \in S_2$,

$$\begin{aligned}
\mu_2(s'_2) &= \sum_{c \in A \cup \{\varepsilon\}, s'_1 \in S_1, k' \geq 1} \mu(s'_1, s'_2, c, k') \\
&= \sum_{c \in A \cup \{\varepsilon\}, s'_1 \in S_1, k' \geq 1} \sum_{p' \in S_P} \mu_P(p')\delta(p')((s'_1, s'_2, c, k')) \\
&= \sum_{p' \in S_P} \mu_P(p') \sum_{c \in A \cup \{\varepsilon\}, s'_1 \in S_1, k' \geq 1} \delta(p')((s'_1, s'_2, c, k')) \\
&= \sum_{p' \in S_P | s'_2 = \mathsf{succ}_{s_2,e}(p')} \mu_P(p')\delta(p')((\mathsf{succ}_{s_1,e}(p'), s'_2, c, \\
&\qquad\qquad \mathsf{Ind}_{\mathcal{R}_2}(p', s'_2))) \\
&\qquad \text{for } c \in \mathsf{Break}(p', s'_2) \text{ fixed as above} \\
&= \sum_{p' \in S_P | s'_2 = \mathsf{succ}_{s_2,e}(p')} \mu_P(p') = \mu_1^2(s'_2)
\end{aligned}$$

As a consequence, $\mu_2 \notin Sat(\varphi_2)$ and $\mu \in Sat(\varphi_{12}^{B,k})$.
In the second case (3), we have $\delta(p')((s'_1, s'_2, c, k')) > 0$ for $s'_1 = \mathsf{succ}_{s_1,e}(p')$, $c \in \mathsf{Break}(p', s'_2)$ fixed above, and $k' = \mathsf{Ind}_{\mathcal{R}_2}(p', s'_2) + 1 < \mathsf{Ind}_{\mathcal{R}_2}(p, s_2) + 1 = k$. As a consequence, we thus have $\mu(s'_1, s'_2, c, k') > 0$ for $k' < k$ and $c \neq \varepsilon$, thus $\mu \in Sat(\varphi_{12}^{B,k})$.

* On the other hand, if $k = 1$, then $\mathsf{Ind}_{\mathcal{R}_2}(p, s_2) = 0$ and either (1) there exists $p' \in S_P$ such that $\mu_P(p') > 0$ and $\mathsf{succ}_{s_2,e}(p') = \emptyset$, or (2) the distribution $\mu_1^2 : \big(s_2' \mapsto \sum_{p' \in P | s_2' = \mathsf{succ}_{s_2,e}(p')} \mu_P(p')\big) \notin \varphi_2$. In both cases, as above, we can prove that $\mu \in Sat(\varphi 12^{B,k}$.

In both cases, we have $\mu \in Sat(\varphi_{12}^{B,k})$.

We thus conclude that there exists $\mu \in Sat(\varphi_{12}^{B,k})$ such that $\mu_P \Subset_{\mathcal{R}^\setminus} \mu$.

- Let $a \in A$ and $\varphi \in C(S)$ such that $L((s_1, s_2, e), a, \varphi) = \top$. As in the proof of Theorem 2, there are several cases that all boil down to the same arguments as above.

Finally, $\mathcal{R}^\setminus$ is a satisfaction relation: Let $c \in \mathsf{Break}_{\mathcal{R}_2}(s_0^P, s_0^2)$ and consider the relation $\mathcal{R}^{\setminus\prime} = \mathcal{R}^\setminus \cup \{(s_0^P, (s_0^1, s_0^2, c, K))\}$. Due to the fact that $K \geq \mathsf{Ind}_{\mathcal{R}_2}(s_0^P, s_0^2)$, one can verify that the pair $(s_0^P, (s_0^1, s_0^2, c, K))$ also satisfies the axioms of a satisfaction relation. The proof is identical to the one presented above. As a consequence, $\mathcal{R}^{\setminus\prime}$ is also a satisfaction relation. Moreover, we now have that $(s_0^P, (s_0^1, s_0^2, c, K)) \in \mathcal{R}^{\setminus\prime}$, with $(s_0^1, s_0^2, c, K) \in S_0$, thus $P \models N_1 \setminus^K N_2$. □

Appendix: Proof of Theorem 9

Proof of Theorem 9. Let $N_1 = (S_1, A, L_1, AP, V_1, \{s_0^1\})$ and $N_2 = (S_2, A, L_2, AP, V_2, \{s_0^2\})$ be deterministic APAs in SVNF such that $N_1 \not\preceq N_2$. Let $P = (S, A, L, AP, V, s_0)$ be the counterexample defined as above. We prove that $P \models N_1$ and $P \not\models N_2$.

$P \models N_1$. Consider the relation $\mathcal{R}_s \subseteq S \times S_1$ such that $(s_1, s_2)\, \mathcal{R}_s\, s_1'$ iff $s_1 = s_1'$. We prove that $\mathcal{R}_s$ is a satisfaction relation. Let $t = (s_1, s_2) \in S$ and consider $(t, s_1) \in \mathcal{R}_s$.

- By construction, we have $V(s_1, s_2) \subseteq V_1(s_1)$.
- Let $a \in A$ and $\varphi_1 \in C(S_1$ such that $L_1(s_1, a, \varphi_1) = \top$. There are several cases.
  - If (s_1, s_2) in case 1 or 2 or $s_2 = \bot$, then by construction there exists $\mu_1^\perp \in Dist(S)$ such that $L((s_1, s_2), a, \mu_1^\perp) = \top$. By construction, we have that there exists $\mu_1 \in Sat(\varphi_1)$ such that $\mu_1^\perp \Subset_{\mathcal{R}_s} \mu_1$.
  - Else, (s_1, s_2) is in case 3 and $B(s_1, s_2) \neq \emptyset$. If $a \notin B(s_1, s_2)$, the result follows as above. Else, either $a \in B_a(s_1, s_2) \cup B_b(s_1, s_2)$ and the result follows again by construction, or $a \in B_c(s_1, s_2) \cup B_f(s_1, s_2)$. In this case, there exists a distribution $\widehat{\mu_1} \in Dist(S)$ such that $L((s_1, s_2), a, \widehat{\mu_1}) = \top$. By construction, $\widehat{\mu_1}$ is defined as follows:

$$\widehat{\mu_1}(s_1', s_2') = \begin{cases} \mu_1(s_1) & \text{if } s_2' = \mathsf{succ}_{s_2,e}(s_1') \\ & \quad \text{or } \mathsf{succ}_{s_2,e}(s_1') = \emptyset \text{ and } s_2' = \bot \\ 0 & \text{otherwise} \end{cases},$$

    where μ_1 is either the distribution given by Lemma 8 if $a \in \mathsf{Break}(s_1, s_2)$ or an arbitrary distribution in $Sat(\varphi_1)$. In both cases, $\mu_1 \in Sat(\varphi_1)$. Consider the function $\delta : S \times S_1 \to [0, 1]$ such that $\delta((s_1', s_2'), s_1'') = 1$ if $s_1' = s_1''$ and 0 otherwise. Using standard techniques, on can verify that δ is a correspondence function and that $\widehat{\mu_1} \Subset_{\mathcal{R}_s} \mu_1$.
- Let $a \in A$ and $\mu \in Dist(S)$ such that $L((s_1, s_2), a, \mu) = \top$. By construction of P, there must exists $\varphi_1 \in C(S_1)$ such that $L_1(s_1, a, \varphi_1) \neq \bot$ and μ is either of the form $\mu_1^\perp$ or $\widehat{\mu_1}$ for some $\mu_1 \in Sat(\varphi_1)$. As above, we can prove that in all cases, $\mu \Subset_{\mathcal{R}_s} \mu_1$.

Finally $\mathcal{R}_s$ is a satisfaction relation. Moreover, we have $((s_0^1, s_0^2), s_0^1) \in \mathcal{R}_s$, thus $P \models N_1$.

$\mathbf{P \not\models N_2}$. Let $\mathcal{R}_s \subseteq S \times S_2$ be the maximal satisfaction relation between P and N_2, and assume that $\mathcal{R}_s$ is not empty. Let $\mathcal{R} \subseteq S_1 \times S_2$ be the maximal refinement relation between N_1 and N_2 and let K be the smallest index such that $\mathcal{R}_K = \mathcal{R}$. We prove that for all $(s_1, s_2) \in S_1 \times S_2$, if $\mathsf{Ind}_{\mathcal{R}}(s_1, s_2) < K$, then $((s_1, s_2), s_2) \notin \mathcal{R}_s$. The proof is done by induction on $k = \mathsf{Ind}_{\mathcal{R}}(s_1, s_2)$. Let $(s_1, s_2) \in S_1 \times S_2$.

- **Base case.** If $\mathsf{Ind}_{\mathcal{R}}(s_1, s_2) = 0$, then there are several cases.
  - If (s_1, s_2) in case 2, i.e. $V_1(s_1) \neq V_2(s_2)$. In this case, we know that $V((s_1, s_2)) \in V_1(s_1)$. Thus, by SVNF of N_1 and N_2, we have that $V((s_1, s_2)) \notin V_2(s_2)$ and $((s_1, s_2), s_2) \notin \mathcal{R}_s$.
  - Else, if (s_1, s_2) in cases 3.a or 3.b, then there exists $a \in A$ and $\mu_1^{\perp} \in Dist(S)$ such that $L((s_1, s_2), a, \mu_1^{\perp}) = \top$ and $\forall \varphi_2 \in C(S_2)$, we have $L_2(s_2, a, \varphi_2) = \bot$. As a consequence, $((s_1, s_2), s_2) \notin \mathcal{R}_s$.
  - Else, if (s_1, s_2) in cases 3.d or 3.d, then there exists $a \in A$ and $\varphi_2 \in C(S_2)$ such that $L_2(s_2, a, \varphi_2) = \top$ and for all $\mu \in Dist(S)$, we have $L((s_1, s_2), a, \mu) = \bot$. As a consequence, $((s_1, s_2), s_2) \notin \mathcal{R}_s$.
  - Finally, if (s_1, s_2) in cases 3.c or 3.f, there exists $e \in (B_c(s_1, s_2) \cup B_f(s_1, s_2)) \cap \mathsf{Break}(s_1, s_2)$. By Lemma 8, there exists constraints φ_1 and φ_2 such that $L_1(s_1, e, \varphi_1) \neq \bot$ and $L_2(s_2, e, \varphi_2) \neq \bot$ and a distribution $\mu_1 \in Sat(\varphi_1)$ such that either
    (I) $\exists s_1' \in S_1$ such that $\mu_1(s_1') > 0$ and $\mathsf{succ}_{s_2,e}(s_1') = \emptyset$,
    (II) $\mu_1^2 : \left(s_2' \mapsto \sum_{\{s_1' \in S_1 | s_2' = \mathsf{succ}_{s_2,e}(s_1')\}} \mu_1(s_1')\right) \notin Sat(\varphi_2)$, or
    (III) $\exists s_1' \in S_1, s_2' \in S_2$ such that $\mu_1(s_1') > 0, s_2' = \mathsf{succ}_{s_2,e}(s_1')$ and $\mathsf{Ind}_{\mathcal{R}}(s_1', s_2') < \mathsf{Ind}_{\mathcal{R}}(s_1, s_2)$.
    By construction, we have that $L((s_1, s_2), e, \widehat{\mu_1}) = \top$ for μ_1 given above. Since $\mathsf{Ind}_{\mathcal{R}}(s_1, s_2) = 0$, case (III) above is not possible. From cases (I) and (II), we can deduce that for all $\mu_2 \in Sat(\varphi_2)$, we have $\widehat{\mu_1} \not\in_{\mathcal{R}_s} \mu_2$. Moreover, by determinism of N_2, φ_2 is the only constraint such that $L_2(s_2, e, \varphi_2) \neq \bot$. As a consequence, $((s_1, s_2), s_2) \notin \mathcal{R}_s$.
- **Inductive step.** Let $0 < k < K$ and assume that for all $k' < k$ and for all $(s_1', s_2) \in \S_1 \times S_2$, if $\mathsf{Ind}_{\mathcal{R}}(s_1, s_2) = k'$, then $((s_1, s_2), s_2) \notin \mathcal{R}_s$. Assume that $\mathsf{Ind}_{\mathcal{R}}(s_1, s_2) = k$. There are two cases.
  - If (s_1, s_2) in cases 2, 3.a, 3.b, 3.d or 3.d, the same reasoning applies as for the base case. We thus deduce that $((s_1, s_2), s_2) \notin \mathcal{R}_s$.
  - Otherwise, if (s_1, s_2) in cases 3.c or 3.f, then, as above, there exists $e \in (B_c(s_1, s_2) \cup B_f(s_1, s_2)) \cap \mathsf{Break}(s_1, s_2)$. By Lemma 8, there exists constraints φ_1 and φ_2 such that $L_1(s_1, e, \varphi_1) \neq \bot$ and $L_2(s_2, e, \varphi_2) \neq \bot$ and a distribution $\mu_1 \in Sat(\varphi_1)$ such that either
    (I) $\exists s_1' \in S_1$ such that $\mu_1(s_1') > 0$ and $\mathsf{succ}_{s_2,e}(s_1') = \emptyset$,
    (II) $\mu_1^2 : \left(s_2' \mapsto \sum_{\{s_1' \in S_1 | s_2' = \mathsf{succ}_{s_2,e}(s_1')\}} \mu_1(s_1')\right) \notin Sat(\varphi_2)$, or
    (III) $\exists s_1' \in S_1, s_2' \in S_2$ such that $\mu_1(s_1') > 0, s_2' = \mathsf{succ}_{s_2,e}(s_1')$ and $\mathsf{Ind}_{\mathcal{R}}(s_1', s_2') < \mathsf{Ind}_{\mathcal{R}}(s_1, s_2)$.
    By construction, we have that $L((s_1, s_2), e, \widehat{\mu_1}) = \top$ for μ_1 given above. As above, if cases (I) or (II) apply, then we can deduce that $((s_1, s_2), s_2) \notin \mathcal{R}_s$. If case (III) applies, then there exists $(s_1', s_2') \in S$ such that $\widehat{\mu_1}(s_1', s_2') > 0$,

$s'_2 = \mathsf{succ}_{s_2,e}(s'_1)$ and $\mathsf{Ind}_{\mathcal{R}}(s'_1, s'_2) < \mathsf{Ind}_{\mathcal{R}}(s_1, s_2)$. Since $s'_2 = \mathsf{succ}_{s_2,e}(s'_1)$, then, by determinism of N_2, all correspondence functions δ will be such that $\delta((s'_1, s'_2), s'_2) = 1$. However, we have that $\mathsf{Ind}_{\mathcal{R}}(s'_1, s'_2) < k$, thus by induction $((s'_1, s'_2), s'_2) \notin \mathcal{R}_s$. As a consequence, we have that for all $\mu_2 \in Sat(\varphi_2)$, we have $\widehat{\mu_1} \not\in_{\mathcal{R}_s} \mu_2$. We can thus deduce that $((s_1, s_2), s_2) \notin \mathcal{R}_s$.

Finally, we know that $\mathsf{Ind}_{\mathcal{R}}(s^1_0, s^2_0) < k$. As a consequence, we have $((s^1_0, s^2_0), s^2_0) \notin \mathcal{R}_s$ and thus $P \not\models N_2$. □