Refinement and Difference for Probabilistic Automata

Benoît Delahaye Uli Fahrenberg Kim Larsen Axel Legay

IRISA/INRIA Rennes, France

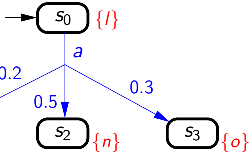
Aalborg University, Denmark

QEST 2013

Probabilistic Automata

$$P = (S, A, L, AP, V, s_0)$$

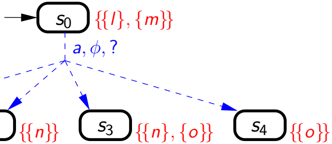
- states S, s_0 initial state,
- $L : S \times A \times Dist(S) \to \{\bot, \top\}$ is a two-valued transition function,
- A is a set of actions,
- AP is a set of atomic propositions, $V : S \to 2^{AP}$,



Abstract Probabilistic Automata

$$N = (S, A, L, AP, V, S_0)$$

- states S, $S_0 \subseteq S$ initial states,
- $L : S \times A \times \mathbf{C(S)} \to \{\bot, ?, \top\}$ is a **three-valued** transition function,
- A is a set of actions,
- AP is a set of atomic propositions, $V : S \to \mathbf{2^{2^{AP}}}$,



$$\mu \in Sat(\phi) \iff (\mu(s_1) + \mu(s_2) \geq 0.7) \wedge (\mu(s_3) + \mu(s_4) \geq 0.2)$$

Satisfaction / 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 APA. A relation $R \subseteq S_1 \times S_2$ is a refinement relation if and only if, for all $(s_1, s_2) \in R$, we have $V_1(s_1) \subseteq V_2(s_2)$ and

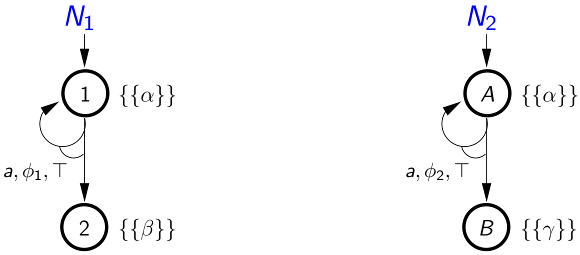
- $\forall a \in A$, $\forall \phi_2 \in C(S_2)$, if $L_2(s_2, a, \phi_2) = \top$, then $\exists \phi_1 \in C(S_1) : L_1(s_1, a, \phi_1) = \top$ and $\forall \mu_1 \in Sat(\phi_1)$, $\exists \mu_2 \in Sat(\phi_2)$ such that $\mu_1 \leqslant_R \mu_2$,
- $\forall a \in A$, $\forall \phi_1 \in C(S_1)$, if $L_1(s_1, a, \phi_1) \neq \bot$, then $\exists \phi_2 \in C(S_2)$ such that $L_2(s_2, a, \phi_2) \neq \bot$ and $\forall \mu_1 \in Sat(\phi_1)$, $\exists \mu_2 \in Sat(\phi_2)$ such that $\mu_1 \leqslant_R \mu_2$.

We say that N_1 refines N_2, denoted $N_1 \preceq N_2$, if there exists a refinement relation R such that $\forall s_0^1 \in S_0^1, \exists s_0^2 \in S_0^2 : (s_0^1, s_0^2) \in R$. Since any PA P is also an APA, we say that P *satisfies* N (or equivalently P *implements* N), denoted $P \models N$, iff $P \preceq N$.

Difference

- For APA N, $[\![N]\!]$ = set of all PA implementations of N
- Goal: given APA N_1, N_2, find specification N so that $[\![N]\!] = [\![N_1]\!] \setminus [\![N_2]\!]$

Problem: Exact Difference Does Not Exist



$\mu \in Sat(\phi_1) \iff (\mu(1) = 1) \vee (\mu(2) = 1)$

$\mu \in Sat(\phi_2) \iff (\mu(A) = 1) \vee (\mu(B) = 1)$

$[\![N_1]\!] \setminus [\![N_2]\!] =$ all PAs that can loop on valuation α with probability 1 and finish with β

$\Rightarrow$ Not Regular

Overapproximation

Assumptions:

- *Deterministic* APA in single valuation normal form
- APA N_1 and N_2 such that $N_1 \npreceq N_2$

Algorithm:

1. Compute maximal refinement relation R
2. Use R to build the difference

Overapproximation

Definition

$N_1 \setminus^* N_2 = (S, A, L, AP, V, S_0)$ with

- $S = S_1 \times (S_2 \cup \{\bot\}) \times (A \cup \{\epsilon\})$
- $V(s_1, s_2, a) = V(s_1)$ for all s_2 and a
- $S_0 = \{(s_0^1, s_0^2, f) : f \in B(s_0^1, s_0^2)\}$

Property: always $[\![N_1]\!] \setminus [\![N_2]\!] \subseteq [\![N_1 \setminus^* N_2]\!]$, but not always equality

Overapproximation

Definition

$N_1 \setminus^* N_2 = (S, A, L, AP, V, S_0)$ with

- $S = S_1 \times (S_2 \cup \{\bot\}) \times (A \cup \{\epsilon\})$
- $V(s_1, s_2, a) = V(s_1)$ for all s_2 and a
- $S_0 = \{(s_0^1, s_0^2, f) : f \in B(s_0^1, s_0^2)\}$

Property: always $[\![N_1]\!] \setminus [\![N_2]\!] \subseteq [\![N_1 \setminus^* N_2]\!]$, but not always equality

Overapproximation

Definition

$N_1 \setminus^* N_2 = (S, A, L, AP, V, S_0)$ with

- $S = S_1 \times (S_2 \cup \{\bot\}) \times (A \cup \{\epsilon\})$
  - $\bot$: Satisfaction to N_2 already broken previously
- $V(s_1, s_2, a) = V(s_1)$ for all s_2 and a
- $S_0 = \{(s_0^1, s_0^2, f) : f \in B(s_0^1, s_0^2)\}$

Property: always $[\![N_1]\!] \setminus [\![N_2]\!] \subseteq [\![N_1 \setminus^* N_2]\!]$, but not always equality

Overapproximation

Definition

$N_1 \setminus^* N_2 = (S, A, L, AP, V, S_0)$ with

- $S = S_1 \times (S_2 \cup \{\bot\}) \times (A \cup \{\epsilon\})$
  - $\bot$: Satisfaction to N_2 already broken previously
  - ϵ: Satisfaction to N_2 broken in this step
- $V(s_1, s_2, a) = V(s_1)$ for all s_2 and a
- $S_0 = \{(s_0^1, s_0^2, f) : f \in B(s_0^1, s_0^2)\}$

Property: always $[\![N_1]\!] \setminus [\![N_2]\!] \subseteq [\![N_1 \setminus^* N_2]\!]$, but not always equality

Underapproximation

- for any $K \in \mathbb{N}$, define $N_1 \setminus^K N_2$, basically like $N_1 \setminus^* N_2$ but with loops K-fold unfolded
- gives underapproximation: always $[\![N_1]\!] \setminus [\![N_2]\!] \supseteq [\![N_1 \setminus^K N_2]\!]$, but not always equality

How Good Are the Approximations?

- have approximations $[\![N_1 \setminus^K N_2]\!] \subseteq [\![N_1]\!] \setminus [\![N_2]\!] \subseteq [\![N_1 \setminus^* N_2]\!]$ for all $K \in \mathbb{N}$
- (for deterministic APA N_1, N_2 in single valuation normal form)
- but how good are these approximations?
- Use distances to answer this question

Distances

$$d(s_1, s_2) = \max \begin{cases} \max\limits_{\{a,\phi_1 : L_1(s_1,a,\phi_1) \neq \bot\}} \min\limits_{\{\phi_2 : L_2(s_2,a,\phi_2) \neq \bot\}} \lambda D_{N_1,N_2}(\phi_1, \phi_2, d) \\ \max\limits_{\{a,\phi_2 : L_2(s_2,a,\phi_2) = \top\}} \min\limits_{\{\phi_1 : L_1(s_1,a,\phi_1) = \top\}} \lambda D_{N_1,N_2}(\phi_1, \phi_2, d) \end{cases}$$

$$D_{N_1,N_2}(\phi_1, \phi_2, d) = \sup_{\mu_1 \in Sat(\phi_1)} \left[\inf_{\mu_2 \in Sat(\phi_2)} \left(\inf_{\delta : \mu_1 \leqslant^\delta \mu_2} \sum_{(s_1,s_2) \in S_1 \times S_2} \mu_1(s_1) \delta(s_1, s_2) d(s_1, s_2) \right) \right]$$

- discounted, accumulating distance

Properties

- for all $K \in \mathbb{N}$, $[\![N_1 \setminus^K N_2]\!] \subseteq [\![N_1]\!] \setminus [\![N_2]\!] \subseteq [\![N_1 \setminus^* N_2]\!]$
- for all $K \in \mathbb{N}$, $N_1 \setminus^K N_2 \preceq N_1 \setminus^{K+1} N_2$
- for all $P \in [\![N_1]\!] \setminus [\![N_2]\!]$ there is $K \in \mathbb{N}$ for which $P \models N_1 \setminus^K N_2$
- the sequence $([\![N_1 \setminus^K N_2]\!])_{K \in \mathbb{N}}$ converges in the distance d, and $\lim_{K \to \infty} d([\![N_1]\!] \setminus [\![N_2]\!], [\![N_1 \setminus^K N_2]\!]) = 0$.
- $d([\![N_1 \setminus^* N_2]\!], [\![N_1]\!] \setminus [\![N_2]\!]) = 0$