Compositional Abstraction Techniques for Probabilistic Automata (PA)

Falak Sher & Joost Pieter Katoen

RWTH Aachen

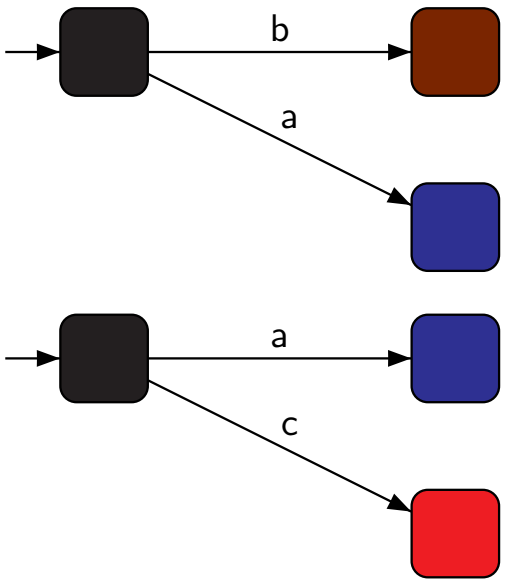
September 26, 2012

Contents

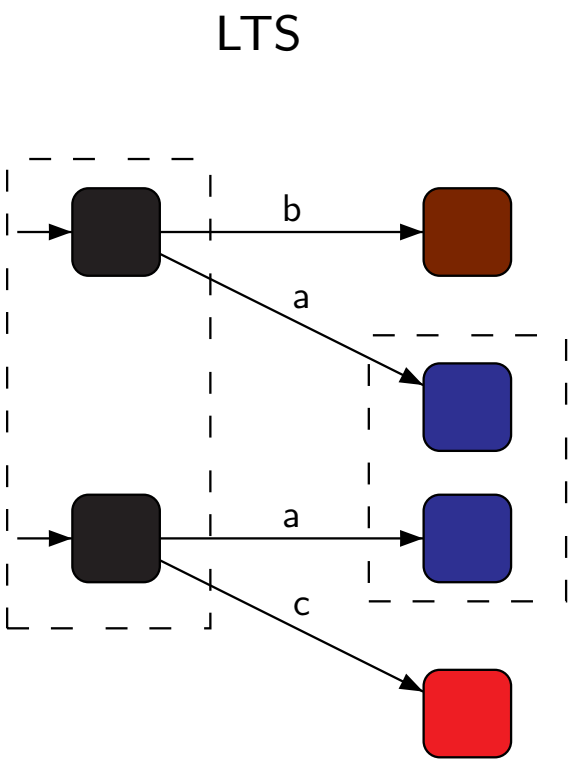
Contents

Abstraction of Labelled TS (LTS) with Modal TS (MTS)

LTS

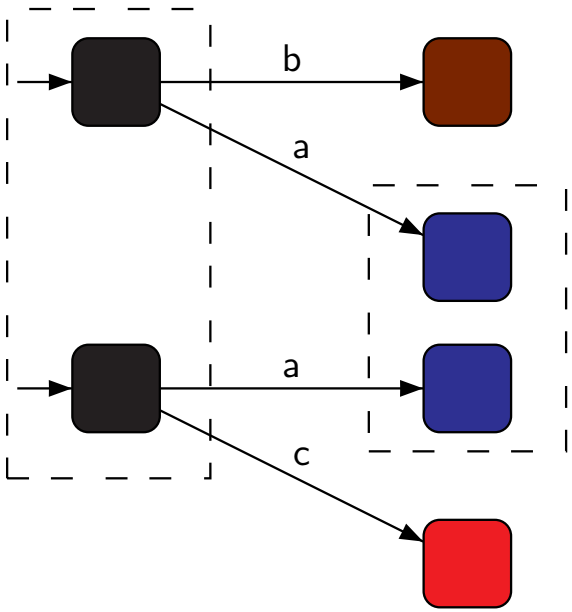


Abstraction of Labelled TS (LTS) with Modal TS (MTS)

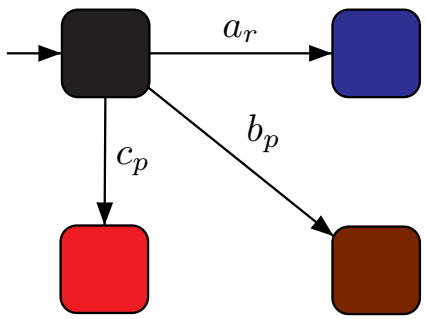


Abstraction of Labelled TS (LTS) with Modal TS (MTS)

LTS



MTS

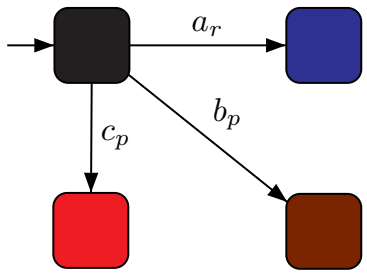


Modal Transition Systems: A Foundation for Three-Valued Program Analysis by Michael Huth, Radha Jagadeesan and David Schmidt. In: LNCS, Vol 2028. Springer (2001).

Contents

Analysis of a modal TS (MTS)

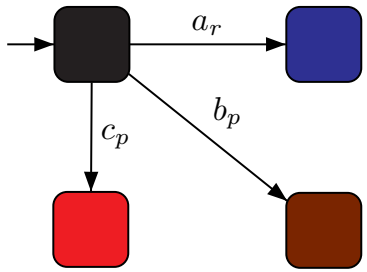
- Is it possible to reach a red state in N?



MTS

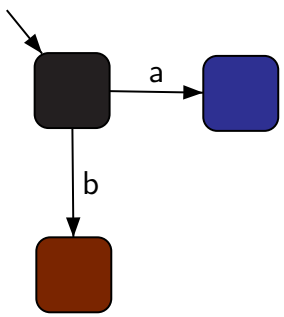
Analysis of a modal TS (MTS)

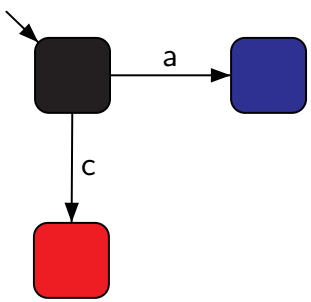
- Is it possible to reach a red state in N?

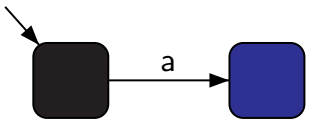


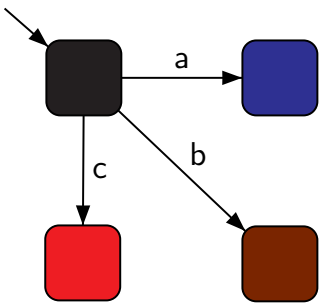
MTS

- Is it possible to reach a red state in each implementation of N?



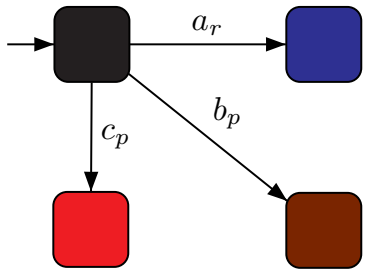






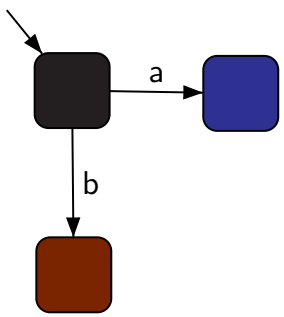
Analysis of a modal TS (MTS)

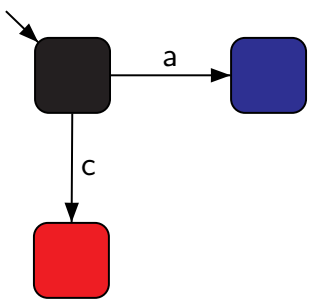
- Is it possible to reach a red state in N?

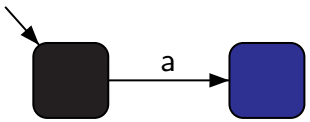


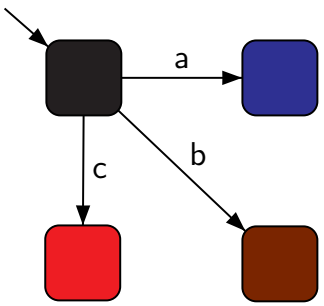
MTS

- Is it possible to reach a red state in each implementation of N?





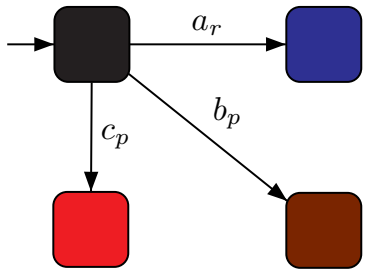




- **Don't know!!!**

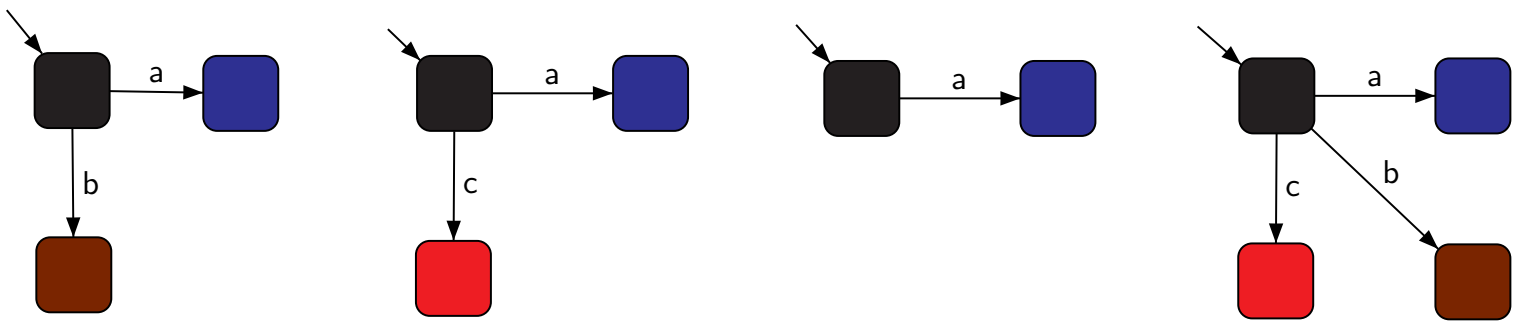
Analysis of a modal TS (MTS)

- Is it possible to reach a red state in N?



MTS

- Is it possible to reach a red state in each implementation of N?



- **Don't know!!!**
- Is it possible to reach a blue state in N?.**Yes we can!!!**

Contents

Probabilistic automata (PA)

Definition

A *PA* is a tuple $N = (S, A, \Delta, s_0)$ where:

- S is a set of states, with $s_0 \in S$
- A is a set of actions, and
- $\Delta \subseteq S \times A \times Dist(S)$ is a set of transitions.

where $Dist(S)$ is a set of distributions over S.

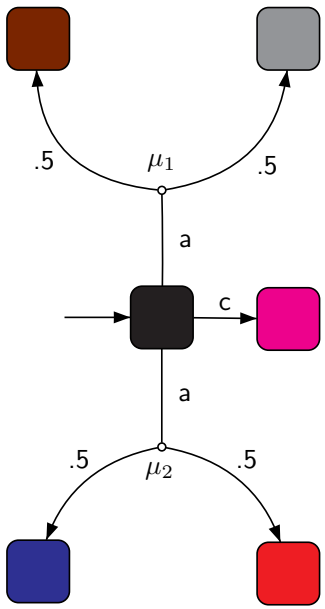
Probabilistic automata (PA)

Definition

A *PA* is a tuple $N = (S, A, \Delta, s_0)$ where:

- S is a set of states, with $s_0 \in S$
- A is a set of actions, and
- $\Delta \subseteq S \times A \times Dist(S)$ is a set of transitions.

where $Dist(S)$ is a set of distributions over S.

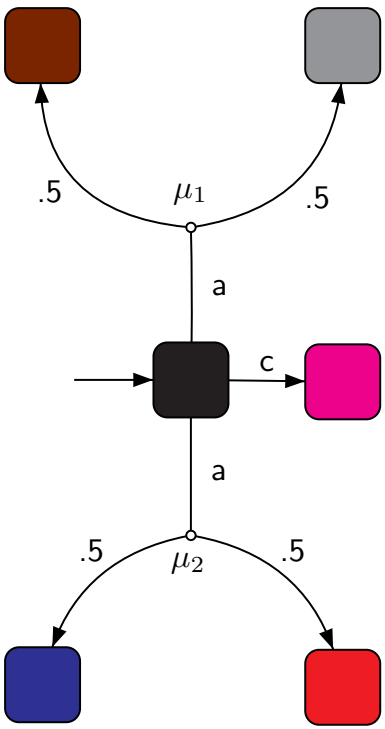


PA M_1

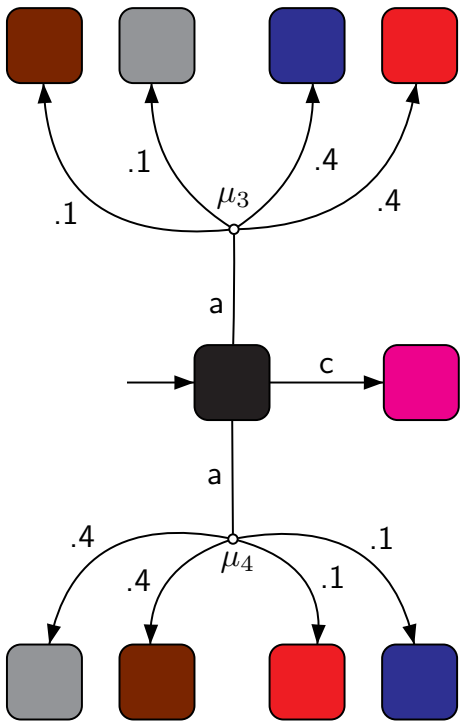
Modeling and Verification of Randomized Distributed Real-Time Systems by Roberto Segala (1995).

Contents

Abstraction of PA with modal PA (MPA)

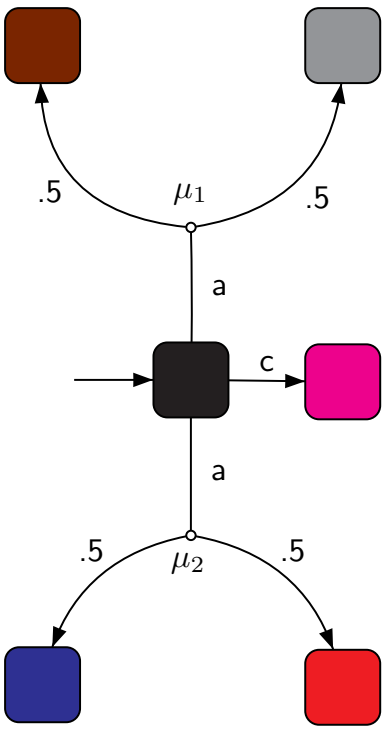


PA M_1

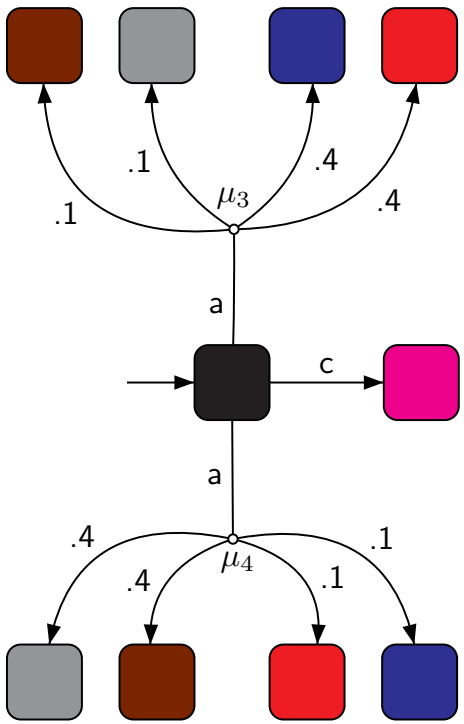


PA M_2

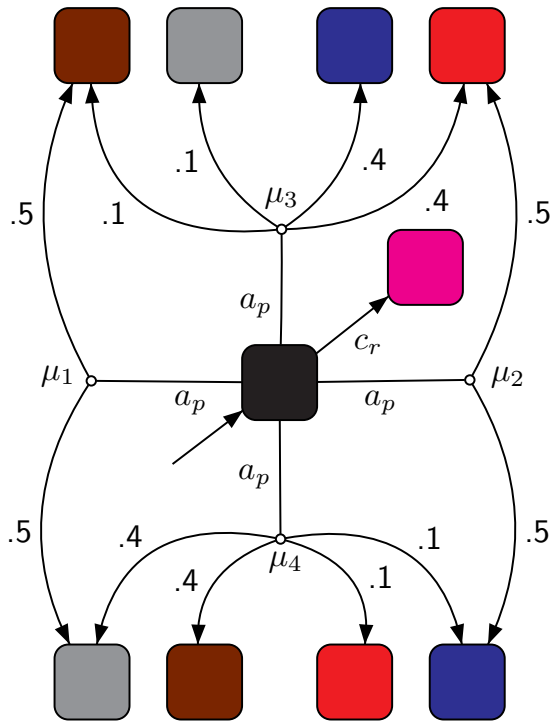
Abstraction of PA with modal PA (MPA)



PA M_1

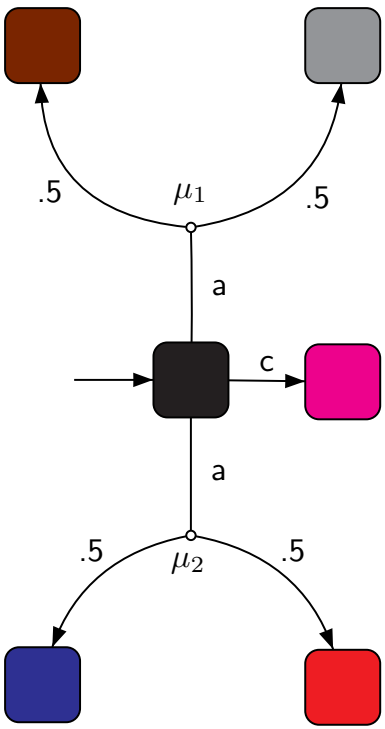


PA M_2

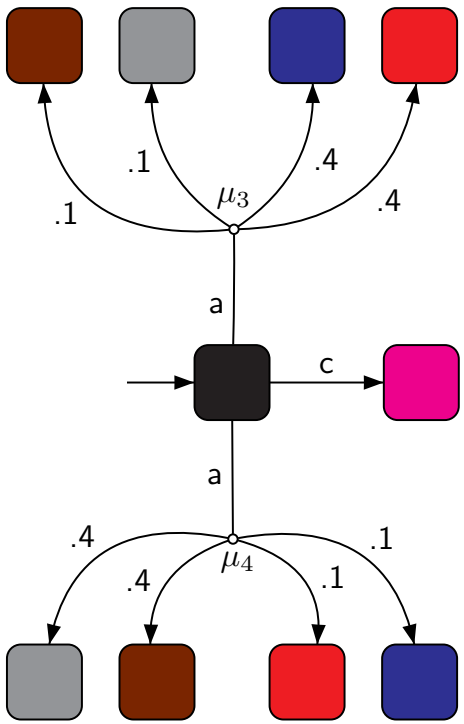


Modal PA N

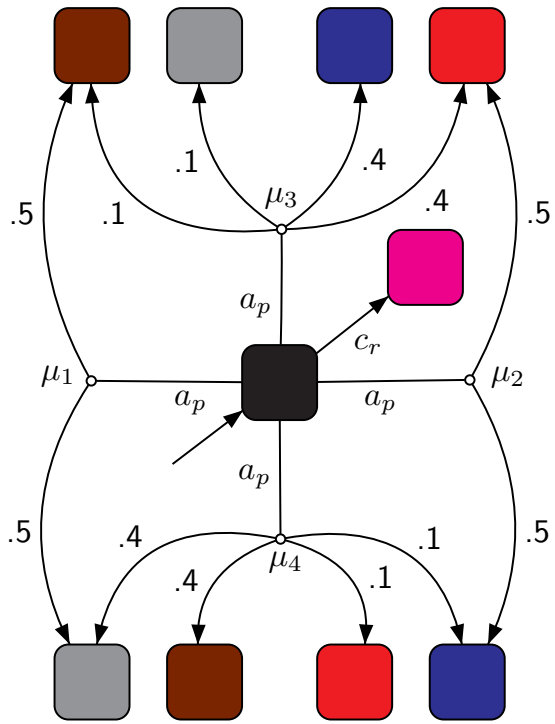
Abstraction of PA with modal PA (MPA)



PA M_1



PA M_2

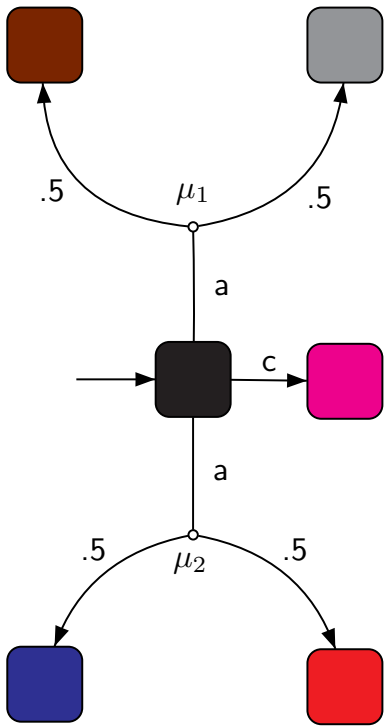


Modal PA N

Is it possible to reach a blue state with probability $\geq .1$? **Don't know!!!**.

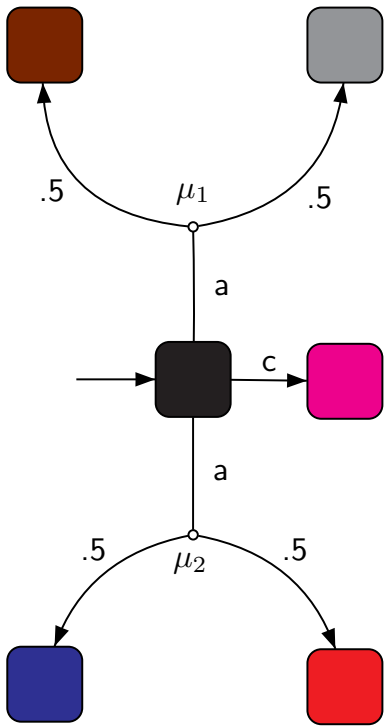
Contents

Simplification of PA



PA M_1

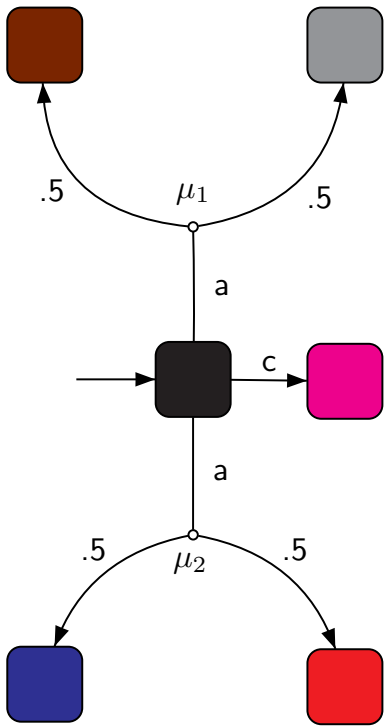
Simplification of PA



PA M_1

- Represent all combined a-transitions by one a-transition.

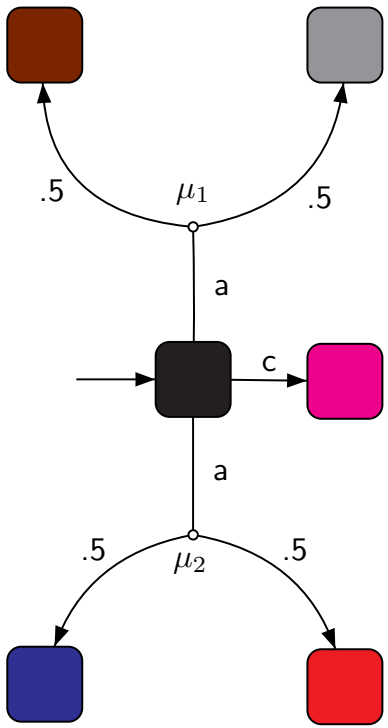
Simplification of PA



PA M_1

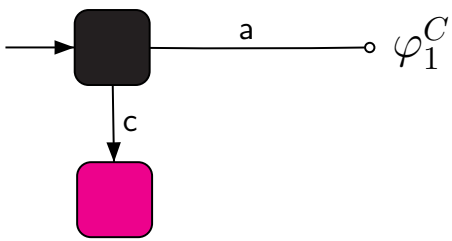
- Represent all combined a-transitions by one a-transition.
- let $\varphi_1 = \{\mu_1, \mu_2\}$ and $\varphi_1^C = \{c_1 \cdot \mu_1 \oplus c_2 \cdot \mu_2 \mid c_1 + c_2 = 1\}$

Simplification of PA



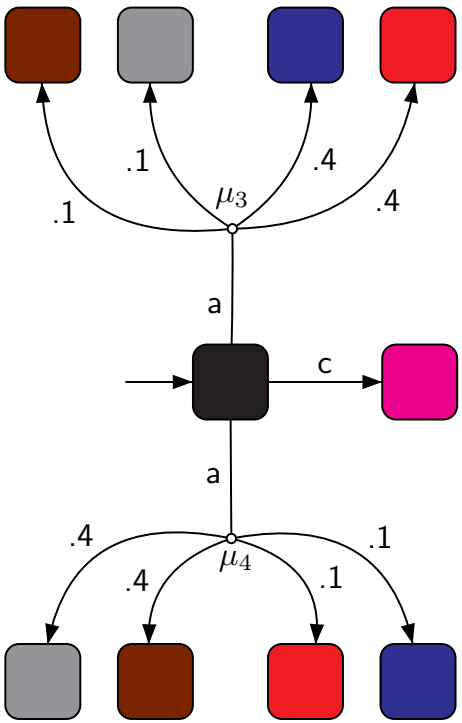
PA M_1

- Represent all combined a-transitions by one a-transition.
- let $\varphi_1 = \{\mu_1, \mu_2\}$ and $\varphi_1^C = \{c_1 \cdot \mu_1 \oplus c_2 \cdot \mu_2 \mid c_1 + c_2 = 1\}$



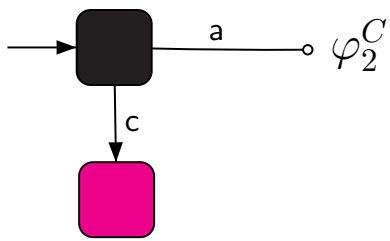
Constrained PA (CPA) N_1

Simplification of PA



PA M_2

- Represent all combined a-transitions by one a-transition.
- let $\varphi_2 = \{\mu_3, \mu_4\}$ and $\varphi_2^C = \{c_3 \cdot \mu_3 \oplus c_4 \cdot \mu_4 \mid c_3 + c_4 = 1\}$

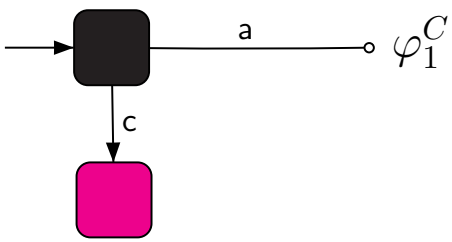


Constrained PA (CPA) N_2

Abstraction of PA with abstract PA (APA)

Abstraction of PA with abstract PA (APA)

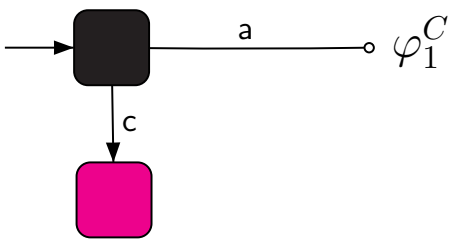
- $\mu_1 = [\![.5, .5]\!]$
- $\mu_2 = [\![.5, .5]\!]$
- $\varphi_1 = \{\mu_1, \mu_2\}$
- $\varphi_1^C = \{c_1 \cdot \mu_1 \oplus c_2 \cdot \mu_2 \mid c_1 + c_2 = 1\}$



CPA N_1

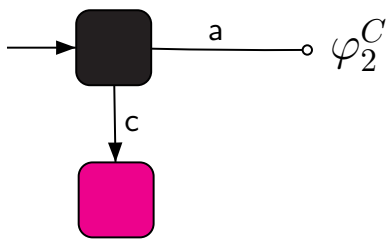
Abstraction of PA with abstract PA (APA)

- $\mu_1 = [\![.5\blacksquare, .5\blacksquare]\!]$
- $\mu_2 = [\![.5\blacksquare, .5\blacksquare]\!]$
- $\varphi_1 = \{\mu_1, \mu_2\}$
- $\varphi_1^C = \{c_1 \cdot \mu_1 \oplus c_2 \cdot \mu_2 \mid c_1 + c_2 = 1\}$



CPA N_1

- $\mu_3 = [\![.1\blacksquare, .1\blacksquare, .4\blacksquare, .4\blacksquare]\!] = .2\mu_1 \oplus .8\mu_2$
- $\mu_4 = [\![.4\blacksquare, .4\blacksquare, .1\blacksquare, .1\blacksquare]\!] = .8\mu_1 \oplus .2\mu_2$
- $\varphi_2 = \{\mu_3, \mu_4\}$
- $\varphi_2^C = \{c_3 \cdot \mu_3 \oplus c_4 \cdot \mu_4 \mid c_3 + c_4 = 1\}$

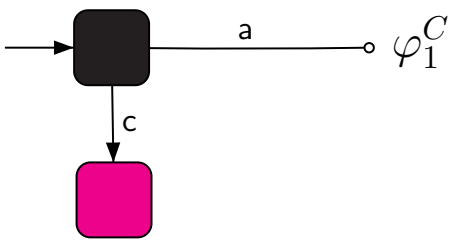


CPA N_2

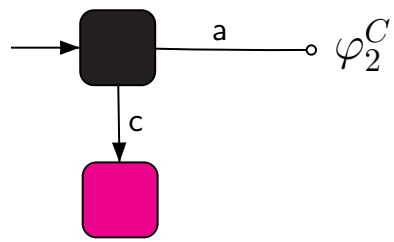
Abstraction of PA with abstract PA (APA)

- $\mu_1 = [\![.5, .5]\!]$
- $\mu_2 = [\![.5, .5]\!]$
- $\varphi_1 = \{\mu_1, \mu_2\}$
- $\varphi_1^C = \{c_1 \cdot \mu_1 \oplus c_2 \cdot \mu_2 \mid c_1 + c_2 = 1\}$

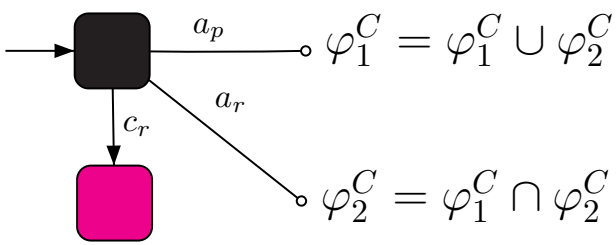
- $\mu_3 = [\![.1, .1, .4, .4]\!] = .2\mu_1 \oplus .8\mu_2$
- $\mu_4 = [\![.4, .4, .1, .1]\!] = .8\mu_1 \oplus .2\mu_2$
- $\varphi_2 = \{\mu_3, \mu_4\}$
- $\varphi_2^C = \{c_3 \cdot \mu_3 \oplus c_4 \cdot \mu_4 \mid c_3 + c_4 = 1\}$



CPA N_1



CPA N_2



APA N

Contents

Abstract Probabilistic Automata (APA)

Definition

An *APA* is a tuple $N = (S, A, \Delta_r, \Delta_p, s_0)$ where S, A and s_0 are as before, and:

- $\Delta_r \subseteq S \times A \times C(S)$ is a set of *required* transitions,
- $\Delta_p \subseteq S \times A \times C(S)$ is a set of *possible* transitions with $\Delta_r \subseteq \Delta_p$,

$C(S)$ is a set of polynomial constraints.

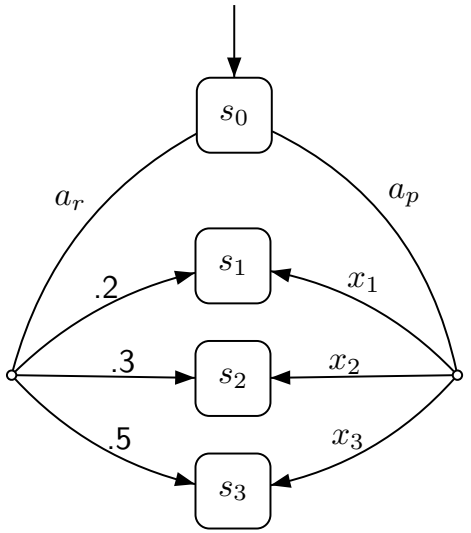
Abstract Probabilistic Automata (APA)

Definition

An *APA* is a tuple $N = (S, A, \Delta_r, \Delta_p, s_0)$ where S, A and s_0 are as before, and:

- $\Delta_r \subseteq S \times A \times C(S)$ is a set of *required* transitions,
- $\Delta_p \subseteq S \times A \times C(S)$ is a set of *possible* transitions with $\Delta_r \subseteq \Delta_p$,

$C(S)$ is a set of polynomial constraints.



$\varphi_x = (x_1 = .4 \wedge x_2 = .6) \vee x_3 = 1$

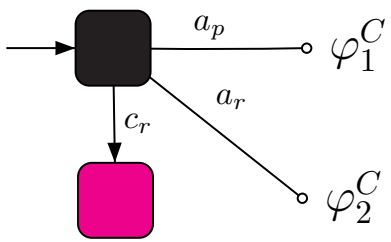
An APA

Abstract Probabilistic Automata by Benoît Delahaye, Joost-Pieter Katoen, Kim G. Larsen, Axel Legay, Mikkel L. Pedersen, Falak Sher and Andrzej Wasowski. In VMCAI . LNCS, Vol 6538. Springer (2011).

Contents

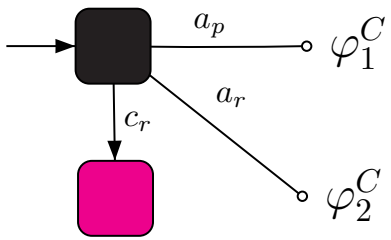
Probabilistic reachability in APA

- Is it possible to reach a blue state with probability $\geq .1$ in N?



Probabilistic reachability in APA

- Is it possible to reach a blue state with probability $\geq .1$ in N?



- Is it possible to reach a blue state with probability $\geq .1$ in each implementation of N?

Challenges in the analysis of APA

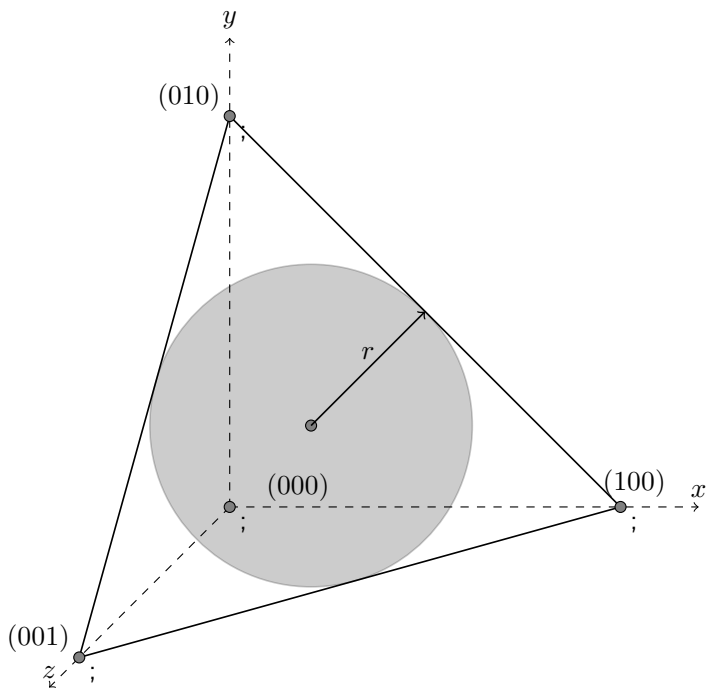
Challenges in the analysis of APA

- **Challenge:** Infinite implementations are possible because of polynomial constraint functions.

Challenges in the analysis of APA

- **Challenge:** Infinite implementations are possible because of polynomial constraint functions.

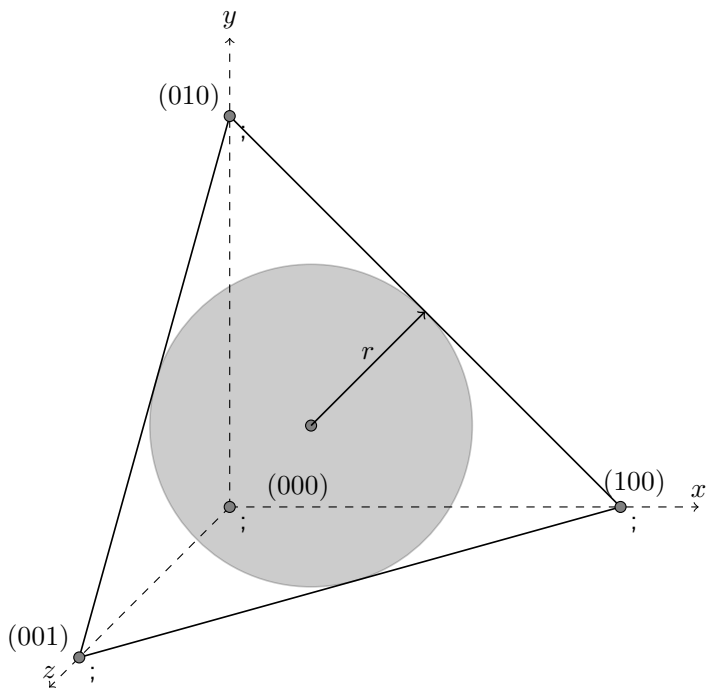
$$\varphi = (x^2 + y^2 + z^2 \leq r^2 \wedge x + y + z = 1)$$



Challenges in the analysis of APA

- **Challenge:** Infinite implementations are possible because of polynomial constraint functions.

$$\varphi = (x^2 + y^2 + z^2 \leq r^2 \wedge x + y + z = 1)$$

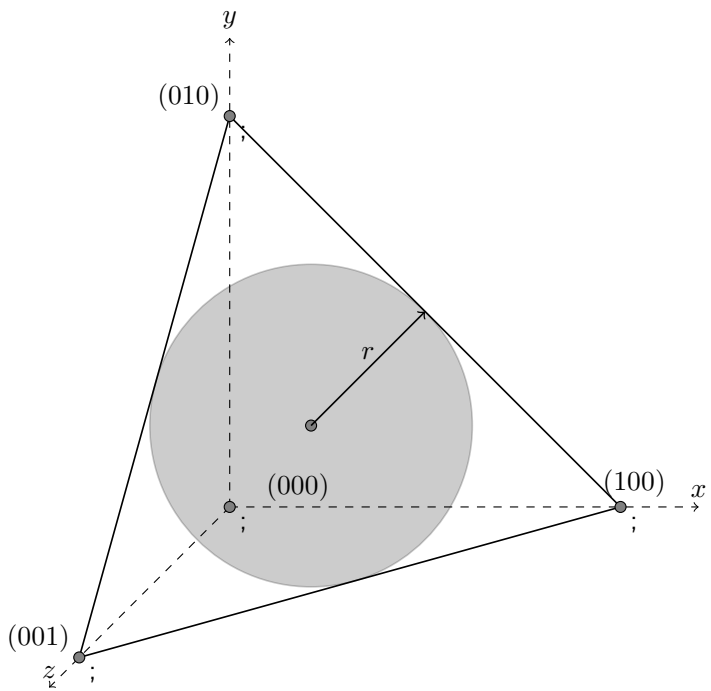


- **Two step solution:**
  - **Step 1:** Approximate polynomial constraints by linear ones.

Challenges in the analysis of APA

- **Challenge:** Infinite implementations are possible because of polynomial constraint functions.

$$\varphi = (x^2 + y^2 + z^2 \leq r^2 \wedge x + y + z = 1)$$

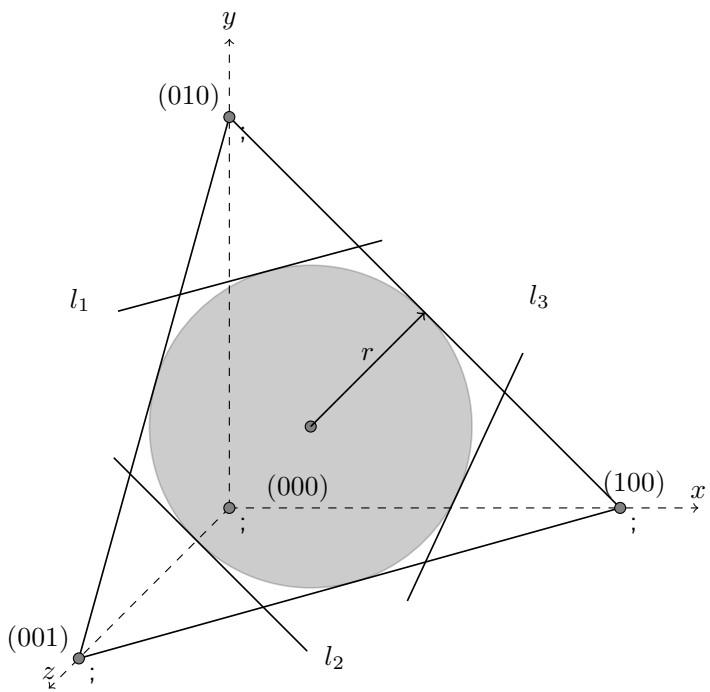


- **Two step solution:**
  - **Step 1:** Approximate polynomial constraints by linear ones.
  - **Step 2:** Exploit extreme distributions of linear constraints.

Solution: (1) Approximation of a polynomial constraint function by a linear one

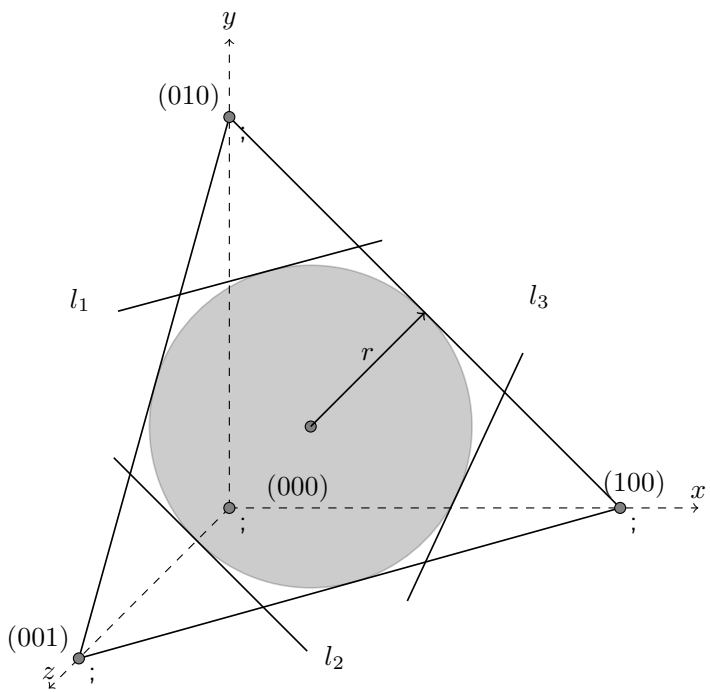
Solution: (1) Approximation of a polynomial constraint function by a linear one

Over-approximation



Solution: (1) Approximation of a polynomial constraint function by a linear one

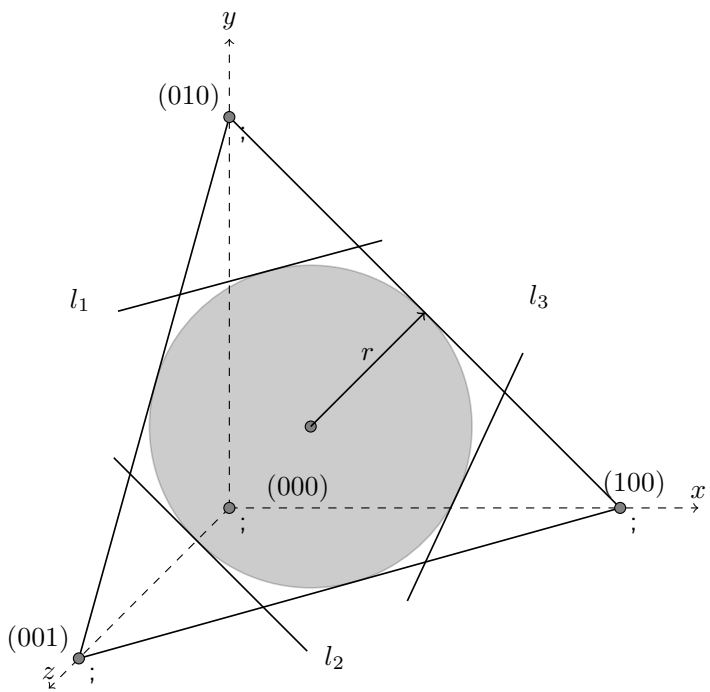
Over-approximation



- $\varphi' = \{\mu \mid \mu \text{ is enclosed by } l_1 \text{ to } l_3\}$

Solution: (1) Approximation of a polynomial constraint function by a linear one

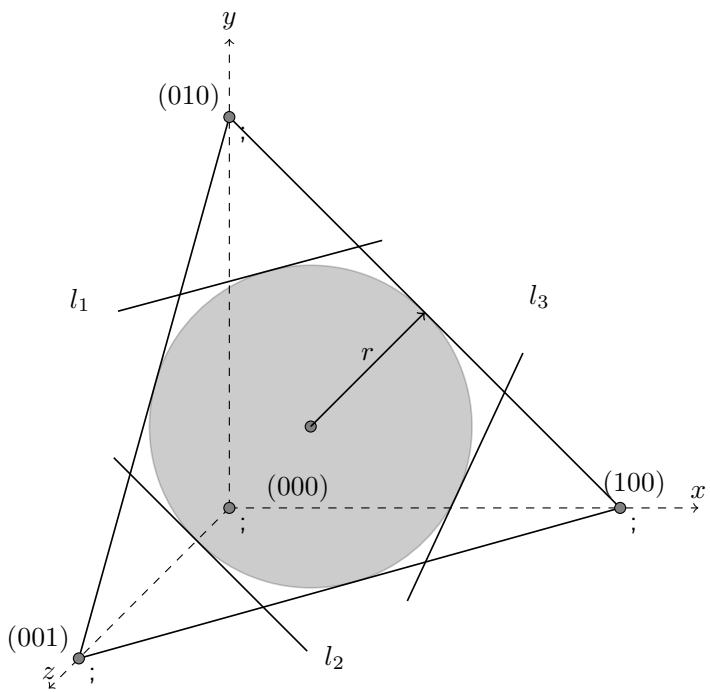
Over-approximation



- $\varphi' = \{\mu \mid \mu \text{ is enclosed by } l_1 \text{ to } l_3\}$
- $\varphi \subseteq \varphi'$

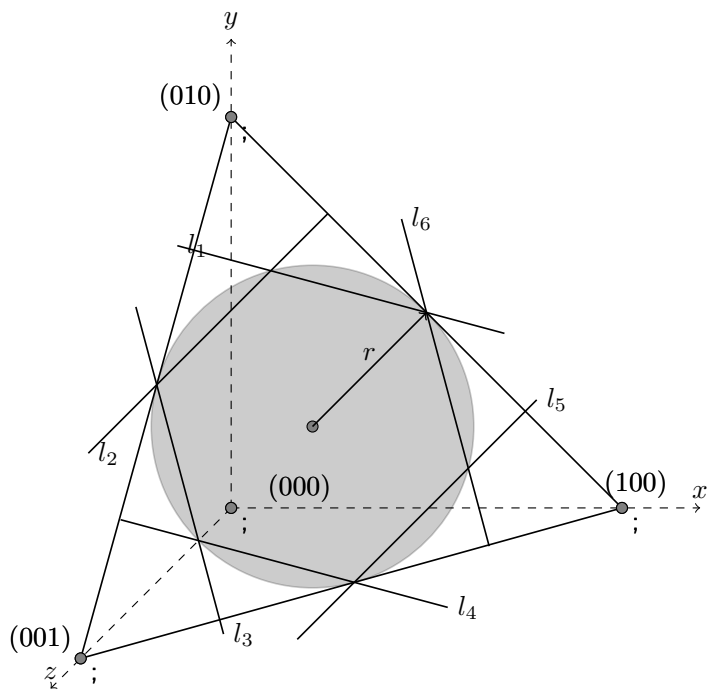
Solution: (1) Approximation of a polynomial constraint function by a linear one

Over-approximation



- $\varphi' = \{\mu \mid \mu \text{ is enclosed by } l_1 \text{ to } l_3\}$
- $\varphi \subseteq \varphi'$

Under-approximation



- $\varphi' = \{\mu \mid \mu \text{ is enclosed by } l_1 \text{ to } l_6\}$
- $\varphi \supseteq \varphi'$

Solution: (1) Effect of constraint-approximation on APA

Solution: (1) Effect of constraint-approximation on APA

Let N be an APA, then for every state s:

- if $s \xrightarrow{a}_r \varphi$, then under-approximate φ.

Solution: (1) Effect of constraint-approximation on APA

Let N be an APA, then for every state s:

- if $s \xrightarrow{a}_r \varphi$, then under-approximate φ.
- if $s \xrightarrow{a}_p \varphi$, then over-approximate φ.

Solution: (1) Effect of constraint-approximation on APA

Let N be an APA, then for every state s:

- if $s \xrightarrow{a}_r \varphi$, then under-approximate φ.
- if $s \xrightarrow{a}_p \varphi$, then over-approximate φ.

then for the resultant APA N':

Solution: (1) Effect of constraint-approximation on APA

Let N be an APA, then for every state s:

- if $s \xrightarrow{a}_r \varphi$, then under-approximate φ.
- if $s \xrightarrow{a}_p \varphi$, then over-approximate φ.

then for the resultant APA N':

- if PA M is an implementation of N, its also an implementation of N'.

Solution: (2) Exploitation of extreme distributions of linear constraints

- **Two step solution:**
  - **Step 1:** Approximate polynomial constraints by linear ones. **Done**
  - **Step 2:** Exploit extreme distributions of linear constraints.

Solution: (2) Exploitation of extreme distributions of linear constraints

- **Two step solution:**
  - **Step 1:** Approximate polynomial constraints by linear ones. **Done**
  - **Step 2:** Exploit extreme distributions of linear constraints.
- **Extreme distributions** of a linear constraint φ are the distributions of the smallest $\varphi_{extr} \subseteq \varphi$ such that $\varphi_{extr}^C = \varphi^C$.

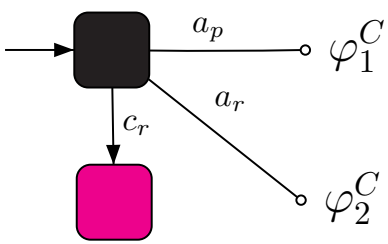
Solution: (2) Exploitation of extreme distributions of linear constraints

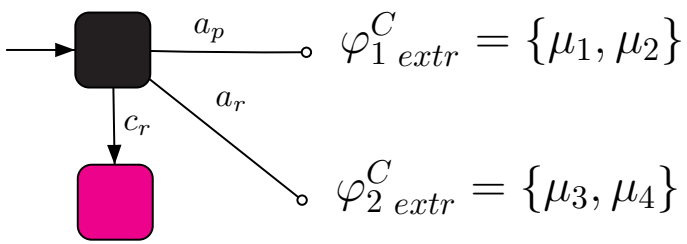
- **Two step solution:**
  - **Step 1:** Approximate polynomial constraints by linear ones. **Done**
  - **Step 2:** Exploit extreme distributions of linear constraints.
- **Extreme distributions** of a linear constraint φ are the distributions of the smallest $\varphi_{extr} \subseteq \varphi$ such that $\varphi_{extr}^C = \varphi^C$.
- Let $\varphi = \{\eta_1, \eta_2, .2 \cdot \eta_1 \oplus .8 \cdot \eta_2\}$, then $\varphi_{extr} = \{\eta_1, \eta_2\}$.

Solution: (2) Exploitation of extreme distributions of linear constraints

- **Two step solution:**
  - **Step 1:** Approximate polynomial constraints by linear ones. **Done**
  - **Step 2:** Exploit extreme distributions of linear constraints.

- **Extreme distributions** of a linear constraint φ are the distributions of the smallest $\varphi_{extr} \subseteq \varphi$ such that $\varphi_{extr}^C = \varphi^C$.
- Let $\varphi = \{\eta_1, \eta_2, .2 \cdot \eta_1 \oplus .8 \cdot \eta_2\}$, then $\varphi_{extr} = \{\eta_1, \eta_2\}$.
- For our running example:

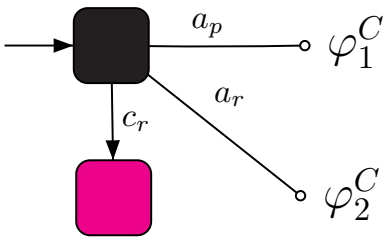




$$\varphi_1^C = \{c_1 \cdot \mu_1 \oplus c_2 \cdot \mu_2 \mid c_1 + c_2 = 1\}$$
$$\varphi_2^C = \{c_3 \cdot \mu_3 \oplus c_4 \cdot \mu_4 \mid c_3 + c_4 = 1\}$$

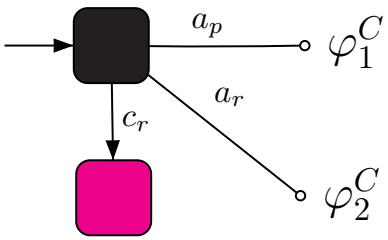
Probabilistic reachability in APA

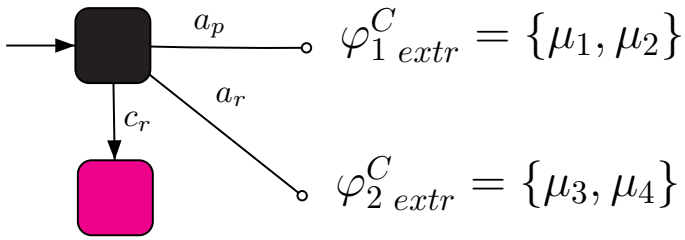
- Is it possible to reach a blue state with probability $\geq .1$ in N?



Probabilistic reachability in APA

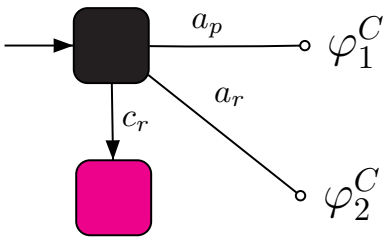
- Is it possible to reach a blue state with probability $\geq .1$ in N?

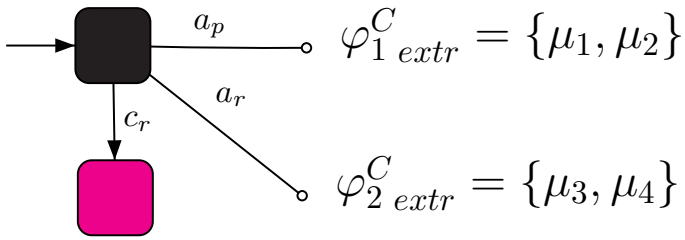




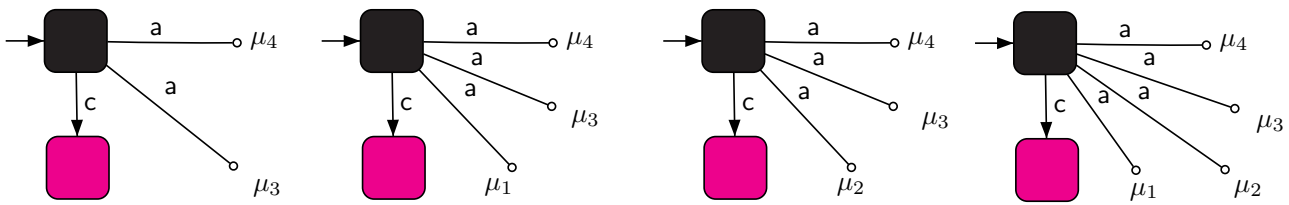
Probabilistic reachability in APA

- Is it possible to reach a blue state with probability $\geq .1$ in N?



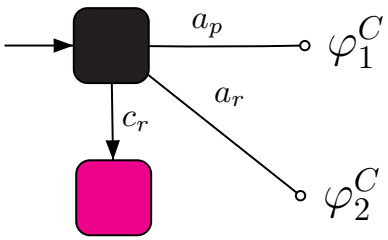


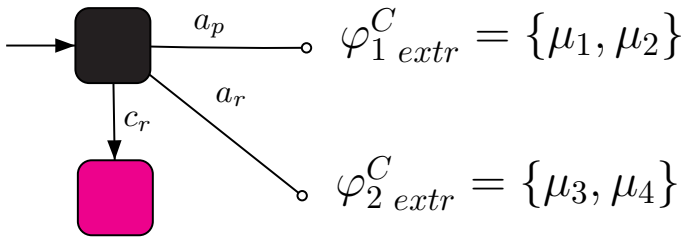
- Get all possible implementations of simplified APA:



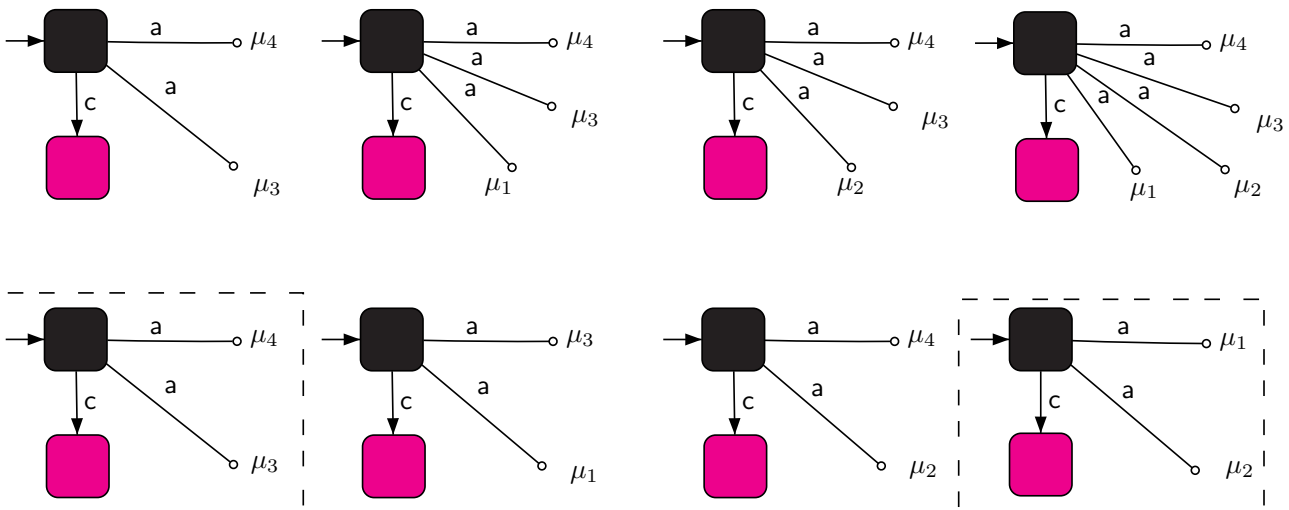
Probabilistic reachability in APA

- Is it possible to reach a blue state with probability $\geq .1$ in N?



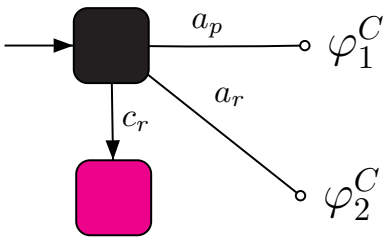


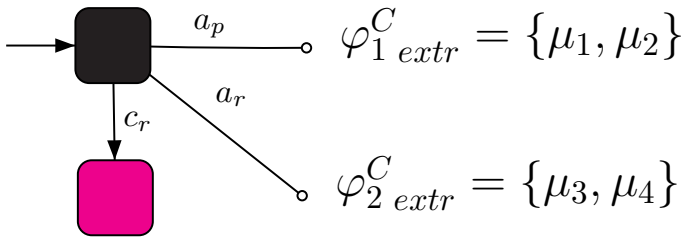
- Get all possible implementations of simplified APA:



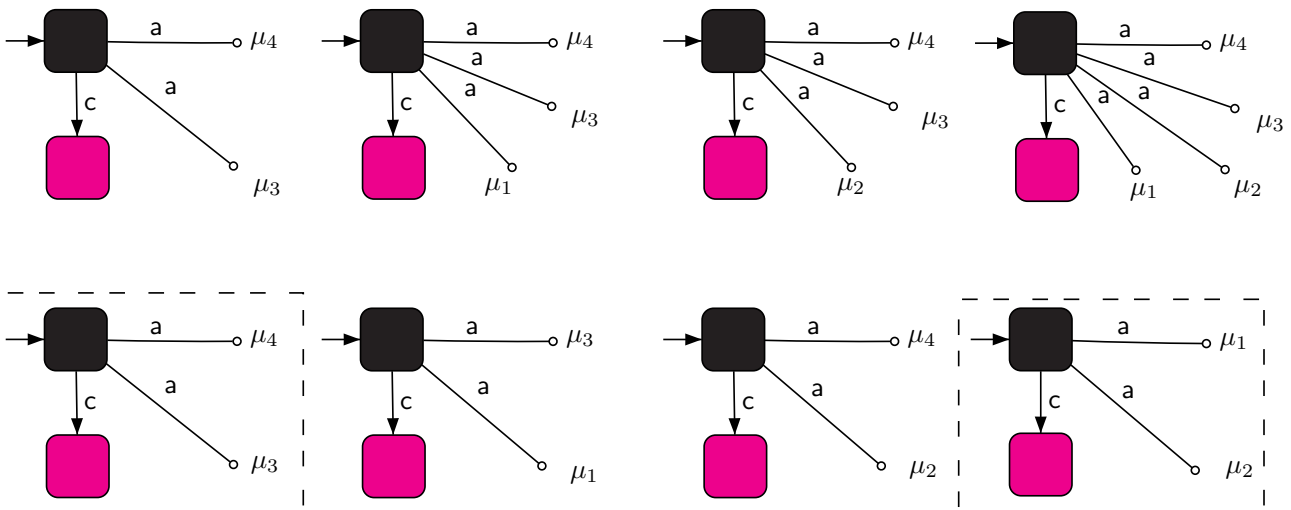
Probabilistic reachability in APA

- Is it possible to reach a blue state with probability $\geq .1$ in N?





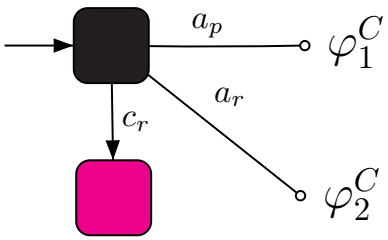
- Get all possible implementations of simplified APA:

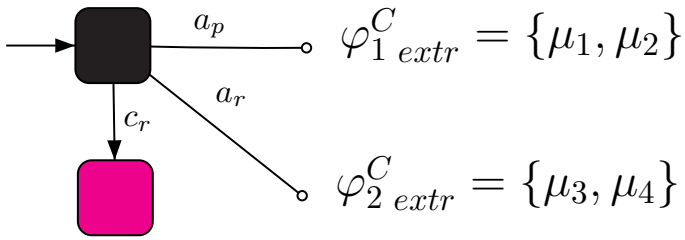


- $\mu_4(\blacksquare) = 0.1$ and $\blacksquare \xrightarrow{a} \mu_4$ is present in each implementation.

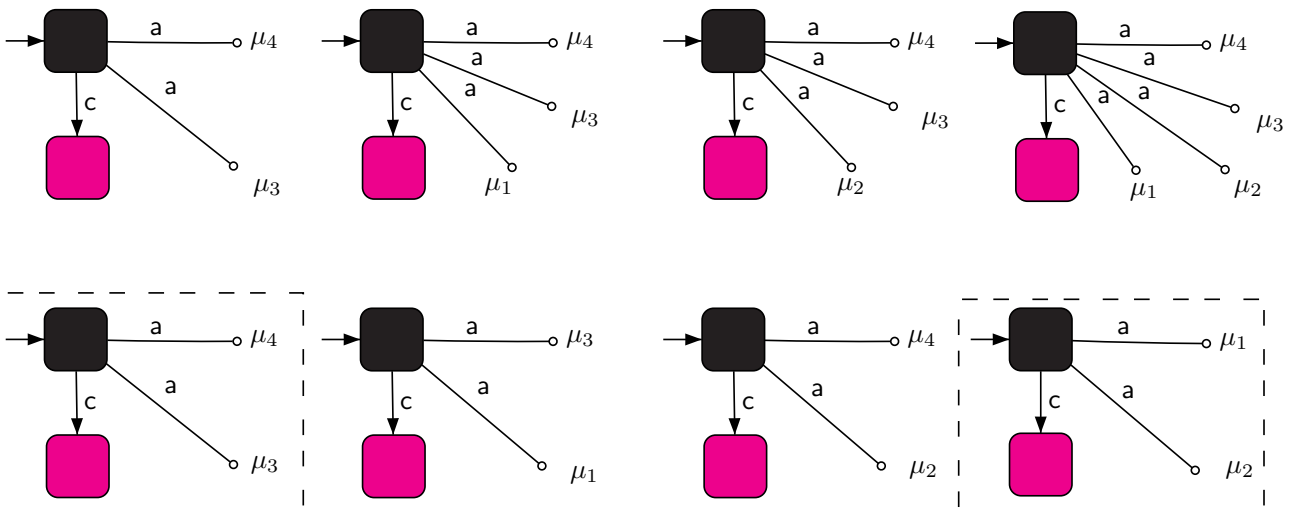
Probabilistic reachability in APA

- Is it possible to reach a blue state with probability $\geq .1$ in N?





- Get all possible implementations of simplified APA:

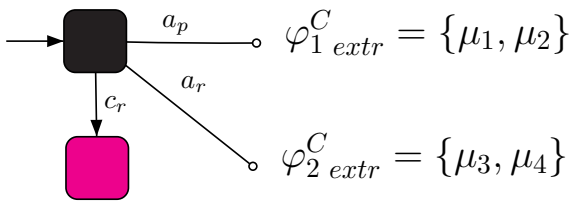


- $\mu_4(\blacksquare) = 0.1$ and $\blacksquare \xrightarrow{a} \mu_4$ is present in each implementation.
- **Yes, its possible!!!**

Lower/upper bounds of maximum reachability probabilities and extreme implementations of APA

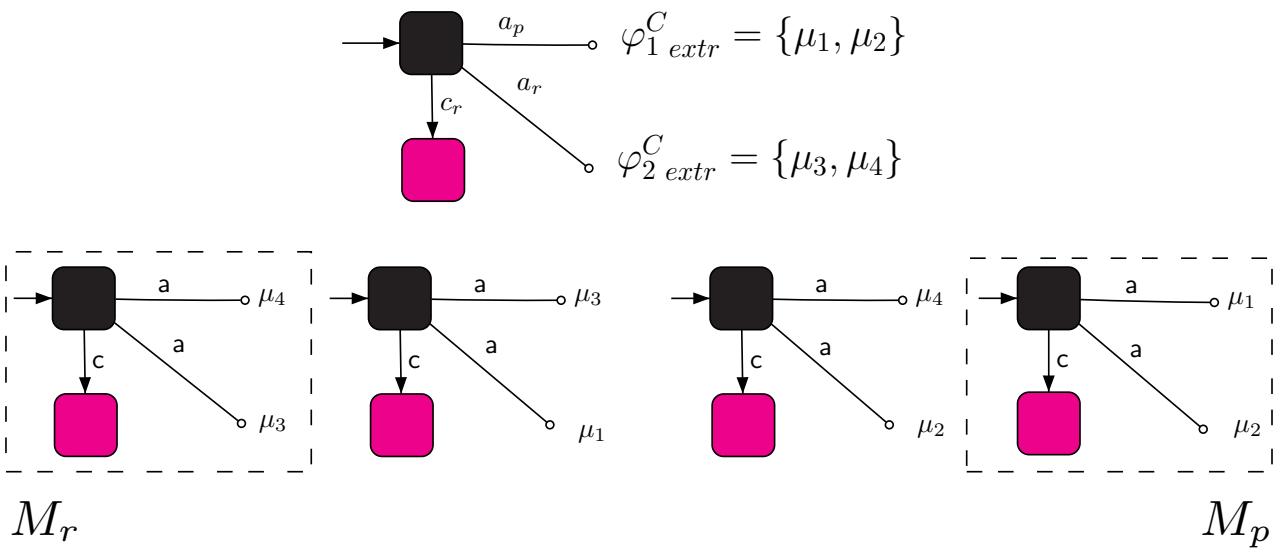
Lower/upper bounds of maximum reachability probabilities and extreme implementations of APA

- Is the maximum probability to reach a blue state between $.4$ and $.5$ in N?



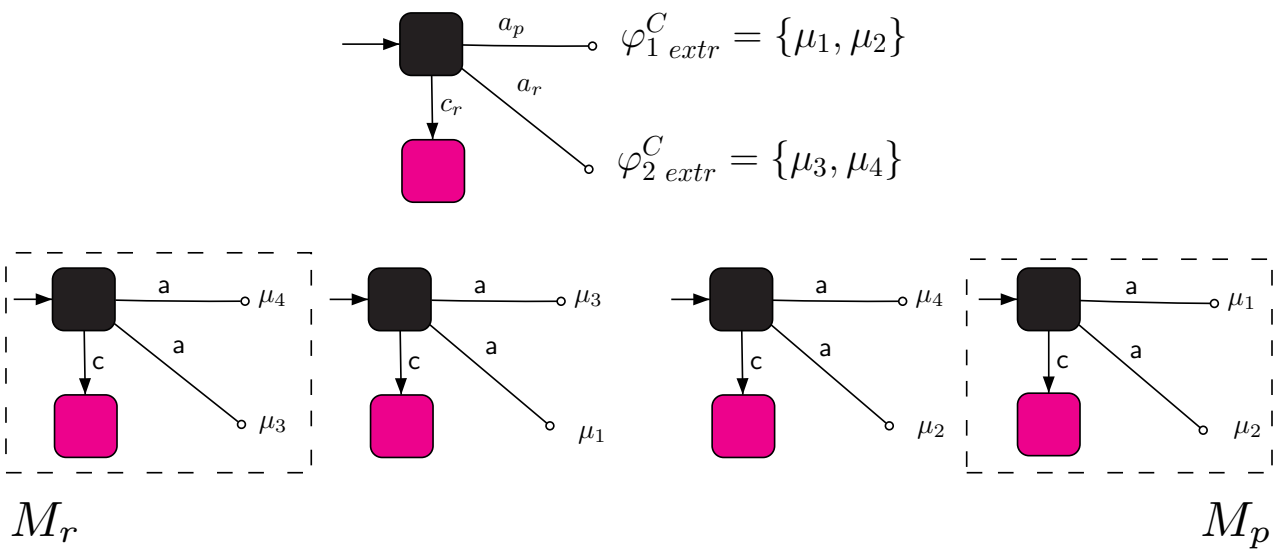
Lower/upper bounds of maximum reachability probabilities and extreme implementations of APA

- Is the maximum probability to reach a blue state between $.4$ and $.5$ in N?



Lower/upper bounds of maximum reachability probabilities and extreme implementations of APA

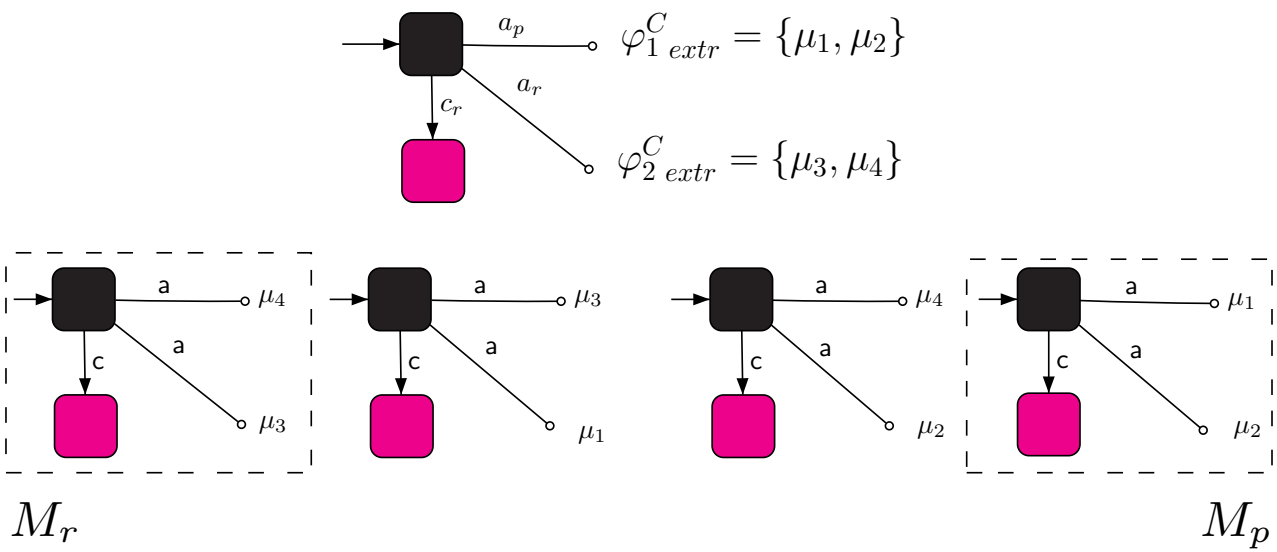
- Is the maximum probability to reach a blue state between $.4$ and $.5$ in N?



- Analysis of extreme implementations of APA N answers the above question.

Lower/upper bounds of maximum reachability probabilities and extreme implementations of APA

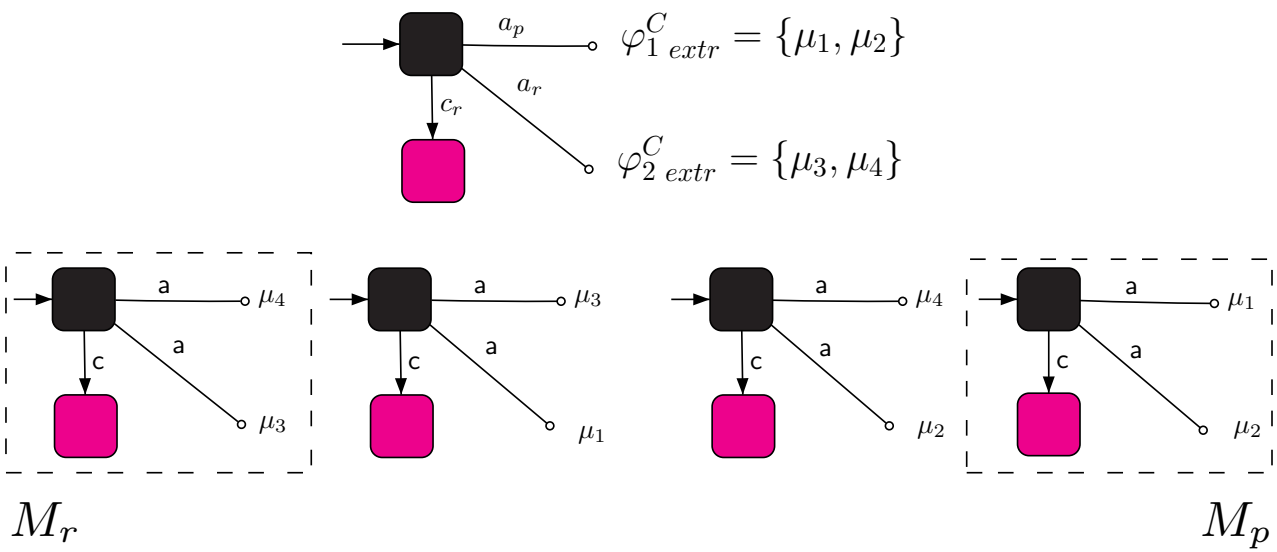
- Is the maximum probability to reach a blue state between $.4$ and $.5$ in N?



- Analysis of extreme implementations of APA N answers the above question.
- $\mu_1 = [\![.5, .5]\!]$, $\mu_2 = [\![.5, .5]\!]$,
- $\mu_3 = [\![.1, .1, .4, .4]\!]$, $\mu_4 = [\![.4, .4, .1, .1]\!]$

Lower/upper bounds of maximum reachability probabilities and extreme implementations of APA

- Is the maximum probability to reach a blue state between $.4$ and $.5$ in N?



- Analysis of extreme implementations of APA N answers the above question.
- $\mu_1 = [\![.5, .5]\!]$, $\mu_2 = [\![.5, .5]\!]$,
- $\mu_3 = [\![.1, .1, .4, .4]\!]$, $\mu_4 = [\![.4, .4, .1, .1]\!]$
- **Yes:** $\mu_3(\blacksquare) = .4$ and $\mu_2(\blacksquare) = .5$

Theorems

Theorem

Let M_r and M_p are the extreme implementations of APA N, then for a set G of goal states:

$$Pr_{max}(M_r, G) \leq Pr_{max}(N, G) \leq Pr_{max}(M_p, G)$$

Contents

Abstraction of APA

Abstraction of APA

Definition

(Multi-transition ($\mapsto$))

$s \overset{a}{\mapsto}_p \varphi'$ iff $s \overset{a}{\rightarrow}_p \varphi_1$, $s \overset{a}{\rightarrow}_p \varphi_2$,..., $s \overset{a}{\rightarrow}_p \varphi_n$ and $\varphi' = \bigvee_{i=1}^{n} \varphi_i$.

Abstraction of APA

Definition

(Multi-transition ($\mapsto$))

$s \overset{a}{\mapsto}_p \varphi'$ iff $s \overset{a}{\to}_p \varphi_1$, $s \overset{a}{\to}_p \varphi_2$,..., $s \overset{a}{\to}_p \varphi_n$ and $\varphi' = \bigvee_{i=1}^{n} \varphi_i$.

Definition

(Abstraction) For APA N, the abstraction function $\alpha : S \to S'$ induces the APA $N' = \alpha(N)$ where for all $s' \in S'$:

1. $s' \overset{a}{\to}_r \varphi'$ iff $\forall s \in \alpha^{-1}(s')$: $s \overset{a}{\to}_r \varphi$ and $\varphi' = \bigwedge_{u \in \alpha^{-1}(s') : u \overset{a}{\mapsto}_r \varphi} \alpha(\varphi)^C$,
2. $s' \overset{a}{\to}_p \varphi'$ iff $\exists s \in \alpha^{-1}(s')$: $s \overset{a}{\to}_p \varphi$ and $\varphi' = \bigvee_{u \in \alpha^{-1}(s') : u \overset{a}{\to}_p \varphi} \alpha(\varphi)$

Abstraction of APA

Definition

(Multi-transition ($\mapsto$))

$s \overset{a}{\mapsto}_p \varphi'$ iff $s \overset{a}{\to}_p \varphi_1$, $s \overset{a}{\to}_p \varphi_2$,..., $s \overset{a}{\to}_p \varphi_n$ and $\varphi' = \bigvee_{i=1}^{n} \varphi_i$.

Definition

(Abstraction) For APA N, the abstraction function $\alpha : S \to S'$ induces the APA $N' = \alpha(N)$ where for all $s' \in S'$:

1. $s' \overset{a}{\to}_r \varphi'$ iff $\forall s \in \alpha^{-1}(s')$: $s \overset{a}{\to}_r \varphi$ and $\varphi' = \bigwedge_{u \in \alpha^{-1}(s') : u \overset{a}{\mapsto}_r \varphi} \alpha(\varphi)^C$,
2. $s' \overset{a}{\to}_p \varphi'$ iff $\exists s \in \alpha^{-1}(s')$: $s \overset{a}{\to}_p \varphi$ and $\varphi' = \bigvee_{u \in \alpha^{-1}(s') : u \overset{a}{\to}_p \varphi} \alpha(\varphi)$

Theorem

$\alpha_1(N_1) \,||_{\bar{A}}\, \alpha_2(N_2) \quad = \quad (\alpha_1 \times \alpha_2)(N_1 ||_{\bar{A}} N_2)$

Refinement of APA

Refinement of APA

Definition

(Refinement ($\preceq$)) For APA N and N', a relation $R \subseteq S \times S'$ is a *refinement* relation if for every sRs':

1. $s' \overset{a}{\mapsto}_r \varphi'$ implies $s \overset{a}{\mapsto}_r \varphi$ and $\forall \mu' \in \varphi', \quad \exists \mu \in \varphi^C : \quad \mu R \mu'$.
2. $s \overset{a}{\mapsto}_p \varphi$ implies $s' \overset{a}{\mapsto}_p \varphi'$ and $\forall \mu \in \varphi, \quad \exists \mu' \in {\varphi'}^C : \quad \mu R \mu'$

Refinement of APA

Definition

(Refinement ($\preceq$)) For APA N and N', a relation $R \subseteq S \times S'$ is a *refinement* relation if for every sRs':

1. $s' \overset{a}{\mapsto}_r \varphi'$ implies $s \overset{a}{\mapsto}_r \varphi$ and $\forall \mu' \in \varphi', \quad \exists \mu \in \varphi^C : \quad \mu R \mu'$.
2. $s \overset{a}{\mapsto}_p \varphi$ implies $s' \overset{a}{\mapsto}_p \varphi'$ and $\forall \mu \in \varphi, \quad \exists \mu' \in {\varphi'}^C : \quad \mu R \mu'$

Theorem

$\preceq$ *is a pre-congruence w.r.t. parallel composition.*

Refinement of APA

Definition

(Refinement ($\preceq$)) For APA N and N', a relation $R \subseteq S \times S'$ is a *refinement* relation if for every sRs':

1. $s' \overset{a}{\mapsto}_r \varphi'$ implies $s \overset{a}{\mapsto}_r \varphi$ and $\forall \mu' \in \varphi', \quad \exists \mu \in \varphi^C : \quad \mu R \mu'$.
2. $s \overset{a}{\mapsto}_p \varphi$ implies $s' \overset{a}{\mapsto}_p \varphi'$ and $\forall \mu \in \varphi, \quad \exists \mu' \in {\varphi'}^C : \quad \mu R \mu'$

Theorem

$\preceq$ is a pre-congruence w.r.t. parallel composition.

Theorem

For APA N, $N \preceq \alpha(N)$.

Contents

Conclusion

Following are the contributions of my work for APA:

- a novel **compositional abstraction technique** that helps defining **lower/upper** bounds for **maximum** reachability probabilities,
- probabilistic reachability analysis of PA.
- a new notion of a **refinement relation** that is pre-congruence w.r.t parallel composition,

Future work

Future work includes:

- design and implementation of algorithms for abstract-refinement framework for APA.
- lifting the notion of abstraction/refinement from states to distributions.

Thanks