PROBABILISTIC MODEL CHECKING: THE AUTOMATA-THEORETIC APPROACH

MOSHE Y. VARDI

RICE UNIVERSITY

ω- Automata

$A = (\Sigma, S, S_0, \rho, \alpha)$

Σ : alphabet
S : states
$S_0 \subseteq S$: initial states
$\rho : S \times \Sigma \to 2^S$: transition function
α : acceptance condition

Input : $a_0, a_1, a_2 \ldots$
Run : $s_0, s_1, s_2 \ldots$

$s_0 \in S_0, \quad s_{i+1} \in \rho(s_i, a_i)$

Limit : $\lim(r)$ - recurrent states of r

Acceptance Conditions

Büchi: $\alpha \subseteq S$

Rabin, Streett: $\alpha \subseteq 2^S \times 2^S$

i.e., $\{(L_1, R_1) \dots (L_k, R_k)\}$

Büchi acceptance: $\lim(r) \cap \alpha \neq \emptyset$

Rabin acceptance:

$\exists (L, R) \in \alpha$ s.t. $\lim(r) \cap L \neq \emptyset$

$\lim(r) \cap R = \emptyset$

Streett acceptance:

$\forall (L, R) \in \alpha$: $\lim(r) \cap L \neq \emptyset \Longrightarrow$

$\lim(r) \cap R \neq \emptyset$

Fairness

A:

$$L(A) = (0^* 1)^\omega$$

Büchi: $\{2\}$

Rabin: $(\{2\}, \emptyset)$

Streett: $(\{1,2\}, \{2\})$

VERIFICATION

System: M - behaviors

Specification: σ - correct behaviors

Correctness: $L(M) \subseteq L(\sigma)$

all behaviors are correct

T. F. A. E.:

1. $L(M) \subseteq L(\sigma)$
2. $L(M) \cap \overline{L(\sigma)} = \phi$
3. $L(M \times \overline{\sigma}) = \phi$

Complementation

Emptiness Problem

Linear Temporal Logic

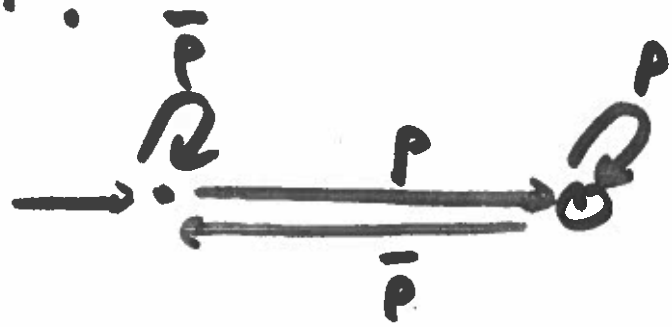
- PTL: X, U, F, G
- ETL: automata connectives
- μTL: X, μ

$$PTL < ETL = \mu TL$$

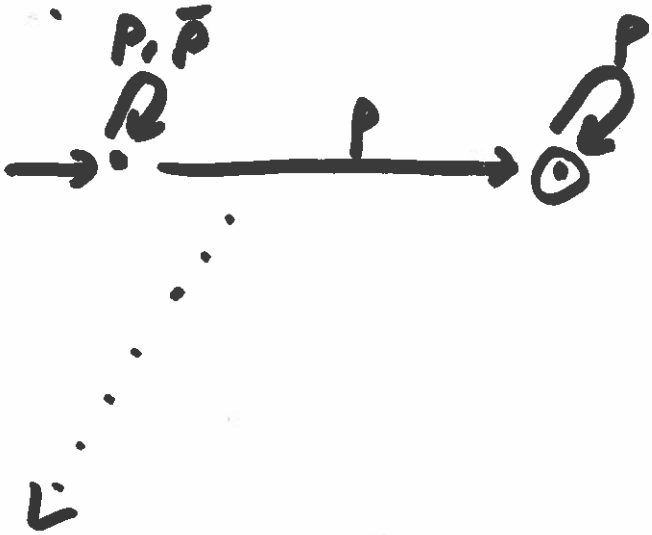
Theorem: [V. + Wolper]
There is an algorithm that constructs for a given LTL formula φ a Büchi auto. A_φ of size exp. in $\|\varphi\|$ s.t. $L(A_\varphi) = models(\varphi)$.

Complementation: $\overline{A_\varphi} = A_{\neg\varphi}$

GFp:



FGp:



nondeterministic!

NONEMPTINESS

$A = (\Sigma, S, S_0, \rho, \alpha)$

Graph: $G_A = (S, E_A)$

$E_A = \{(s, t) : t \in \rho(s, a), a \in \Sigma\}$

Nonemptiness Test:

- Büchi: there is a reachable SSC that intersects α
- Rabin: for some $(L, R) \in \alpha$ there is a reachable SSC inside $S - R$ that intersects L

Streett nonemptiness

[Emerson - Lei, 1985]

Iterate:

1. Decompose G_A into maximal SSCs.

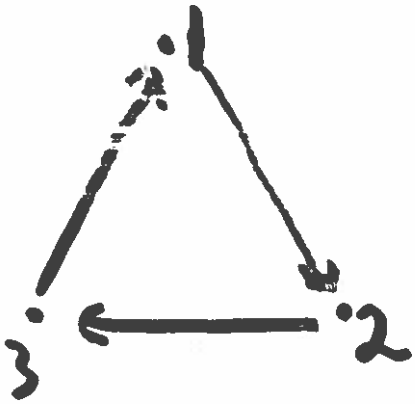
2. For a component Q and pair $(L,R) \in \alpha$, if $Q \cap L \neq \emptyset$ and $Q \cap R = \emptyset$, delete states in L

check: $L(A) \neq \emptyset$ iff a reachab SCC survives.

complexity: quadratic

X

X



$(\{1,2\},\{4\})$

PROBABILISTIC PROGRAMS

$M = (W, P)$ - Markov chain

W: states

$P : W^2 \longrightarrow [0,1]$ transition probabilities

$$\sum_{t \in W} P(s,t) = 1$$

Sequence space: (W^ω, B, μ)

W^ω: infinite sequences

B : Borel field

μ : measure on B

Specification: $A = (W, S, S_0, \rho, \alpha)$

Prob. Universality: $\mu(L(A)) = 1$

Prob. emptiness: $\mu(L(A)) = 0$

BOREL FIELD

- $\text{cylinder}(u_0, u_1 \ldots u_{m-1}) =$
  $\{\rho \in W^\omega : \rho[0, \ldots m-1] = \langle u_0 \ldots u_{m-1} \rangle\}$

- $\text{Prob}(\text{cylinder}(u_0 \ldots u_{m-1})) =$
  $\prod_{i=1}^{m-1} P(u_{i-1}, u_i)$

- Borel field: closure under countable unions and comp.

Determinization

Determinism: $|\rho(s,a)| \leq 1$
$|S_0| = 1$

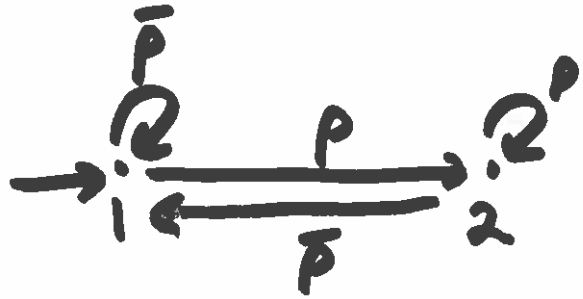
Theorem: [Safra, 1989]
There is an algorithm that constructs for a given ω-auto. A a deterministic automaton A^d of size $2^{O(\|A\| \cdot \log \|A\|)}$ s.t.

$L(A) = L(A^d)$ (alt., $L(A) = W^\omega - L(A^d)$)
(co-determinization)

Acceptance condition: Streett or Rabin

Müller, 1965: $2^{\|A\|}$ - incorrect
McNaughton, 1966: $2^{2^{\|A\|}}$

FG_p:



Rabin: $(\{1,2\}, \{1\})$

Streett: $(\{1\}, \phi)$

Product Construction

$M = (W, P)$

$A = (W, S, s_0, \rho, \alpha)$ deterministic

$M \times A = (W \times S, P \times \rho, W \times \alpha)$

$$P \times \rho((u, s), (v, t)) = \begin{cases} P(u, v) & \text{if } \rho(s, u) = t \\ 0 & \text{otherwise} \end{cases}$$

$W \times \{(L_1, R_1) \ldots (L_k, R_k)\} =$

$\{(W \times L_1, W \times R_1) \ldots (W \times L_k, W \times R_k)$

Lemma:

$\mu_M(L(A)) > 0$ iff $\mu_{M \times A}(sat(W \times \alpha)) > 0$

limit satisfying $W \times$

Ergodic Analysis

$M = (W, P, \alpha)$: chain

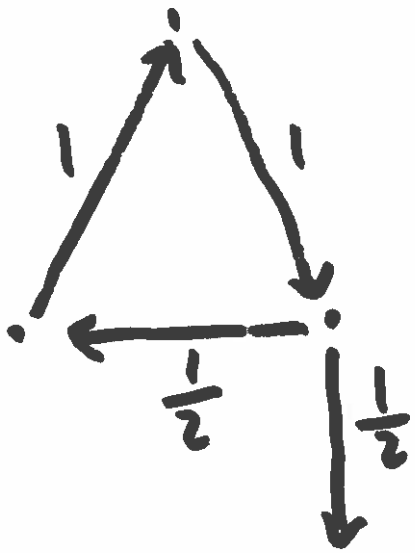
$G_M = (W, E_M)$: graph

$E_M = \{(u,v) : P(u,v) > 0\}$

Ergodic set: terminal SCC of G_M (SCC closed under E_M)

Lemma: $\mu_M(sat(\alpha)) > 0$ iff some ergodic set Q "satisfies" α, e.g., $\forall (L,R) \in \alpha$, if $Q \cap L \neq \phi$ then $Q \cap R \neq \phi$.
(Streett condition)

Note: Probabilities irrelevant!


1
1
$\frac{1}{2}$
$\frac{1}{2}$

Automata-Theoretic Perspective

$M = (W, P, \alpha)$

$A_M = (\{a\}, W, W_0, \rho_P, \alpha \cup \beta)$

W_0: initial states $P(u) > 0$

$\rho_P(u, a) = \{v : P(u, v) > 0\}$

$\beta = \{(\{u\}, \{v\}) : P(u, v) > 0\}$.

Lemma: $\mu_M(sat(\alpha)) > 0$ iff

$$L(A_M) \neq \emptyset$$

Intuition: probabilistic behavior

$\equiv$

state fairness

VERIFICATION I

M : Program

A : Specification (automaton)

1. $A \xmapsto{\text{co-det.}} A^d$ (exponential)

2. $M, A^d \xmapsto{\times} M \times A^d$ (polynomial)

3. ergodic analysis (polynomial) for prob. nonemptiness

<u>Complexity:</u> poly. in $\|M\|$

exp. in $\|A\|$

Ok!

Lower Bound: PSPACE-hard

VERIFICATION II

M: program

φ: specification (PTL)

1. $\varphi \longmapsto A_{\neg\varphi}$ (exponential)
2. $A_\varphi \overset{\text{det.}}{\longmapsto} A^d_\varphi$ (exponential)
3. $M, A^d_\varphi \overset{\times}{\longmapsto} M \times A^d_\varphi$ (polynomial)
4. ergodic analysis (polynomial)

Complexity: poly in $\|M\|$

2 exp. in $\|\varphi\|$

Improvement: [CY'95]

exp. in $\|\varphi\|$

REACTIVE PROBABILISTIC PROGRAMS

Reactive Markov chain:

$M = (W, N, P)$

W: states

N: nondeterministic states

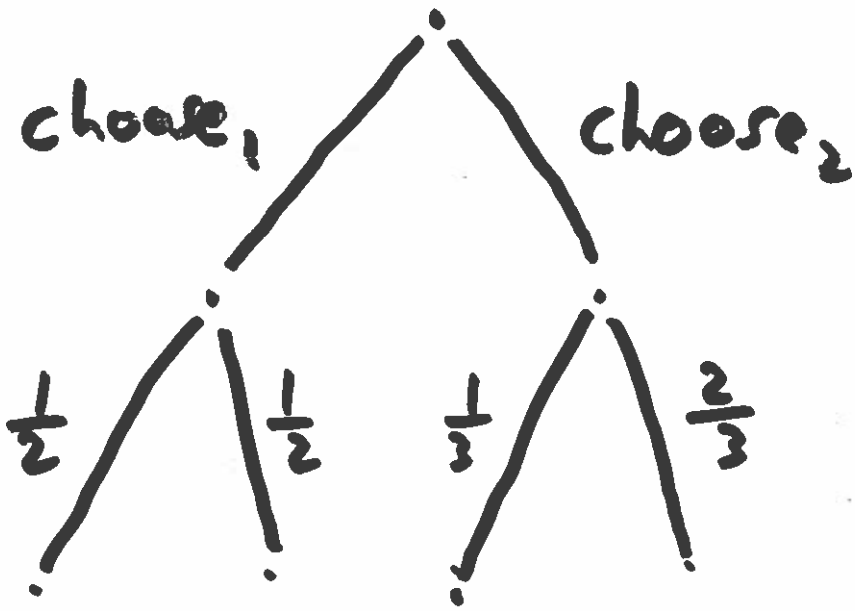
$W - N$: probabilistic states

P: transition probabilities

History: V. '85 (concurrent Markov chains)

Hart-Sharir-Pnueli '83: interleaved Markov chains

Derman '70: Markov Decision Processes


choose$_1$
choose$_2$
$\frac{1}{2}$
$\frac{1}{2}$
$\frac{1}{3}$
$\frac{2}{3}$

SCHEDULERS

Scheduler = Adversary = Environment

$\tau : W^* N \to W$

$\tau(\alpha u) = v \implies P(u,v) > 0$

$\mathcal{M}, \tau \longmapsto \mathcal{M}_\tau$: Markov chain

$\mathcal{M}_\tau = (W^*, P_\tau)$

$$P_\tau(\alpha u, \alpha u v) = \begin{cases} 1 & u \in N \quad \tau(\alpha u) = v \\ 0 & u \in N \quad \tau(\alpha u) \neq v \\ P(u,v) & u \in N \end{cases}$$

VERIFICATION

M: reactive prob. program

σ: specification

Correctness:

$\forall$ scheduler τ, $\mu_{M_\tau}(\sigma) = 1$

Intuition: σ almost surely holds regardless of the environment's behavior.

Dually: $\exists$ scheduler τ s.t. $\mu_{M_\tau}(\bar{\sigma}) > 0$?

PRODUCT CONSTRUCTION

$\mathcal{M} = (W, N, P)$

$A = (W, S, \Delta_0, \rho, \alpha)$ deterministic

$\mathcal{M}, A \longmapsto \mathcal{M} \times A =$ reactive chain
$(W \times S, N \times S, P \times \rho, W \times \alpha)$

<u>Lemma:</u>

$\exists \tau \quad \mu_{\mathcal{M}_\tau}(L(A) > 0)$ iff

$\exists \tau \quad \mu_{(\mathcal{M} \times A)_\tau}(\mathrm{sat}(W \times \alpha)) > 0$

Ergodic Analysis

$M = (W, N, P, \alpha)$: reactive chain

$G_M = (W, E_M)$

$E_M = \{(u, v) : P(u, v) > 0\}$

Ergodic set: SCC of G_M closed under probabilistic transitions, i.e. under $E_M \cap (W-N \times W-N)$

Lemma: $\exists \tau \; \mu_{M_\tau}(sat(\alpha)) > 0$ iff some ergodic set Q "satisfies" α.

Intuition: system has to be fair, Environment does not

Automata-Theoretic Perspective

$M = (W, N, P, \alpha)$

$A_M = (\{a\}, W, W_0, \rho_P, \alpha \cup \beta)$

$\rho_P(u, a) = \{v : P(u, v) > 0\}$

$\beta = \{(\{u\}, \{v\}) : u \in W - N, P(u, v) > 0\}$

Lemma: $\exists \tau . \mu_{M_\tau}(sat(\alpha)) > 0$ iff

$$L(A_M) \neq \phi$$

Again: Probabilistic behavior

$\equiv$

state fairness

FAIRNESS

Intuition: restrict to "well-behaved" schedulers

Example: if a transition is enabled i.o. then it is scheduled i.o.

Generally: streett condition f

Fair scheduler: Fairness holds w. Prob. 1

Correctness: spec holds w. Prob. 1 wrt all fair schedulers

Algorithm: just another streett condition

VERIFICATION

M: program

φ, A: specification

1. $A \mapsto A^d$ (exponential)

   $\varphi \mapsto A_{\neg\varphi} \mapsto A^d$ (2 exponential)

2. $M, A^d \mapsto M \times A^d$ (polynomial)

3. ergodic analysis (polynomial)

Complexity: poly. in $\|M\|$

exp. in $\|A\|$

2 exp. in $\|\varphi\|$

Matching l.b.: [CY'95]

MYSTERY

My motto: "Anything you can do, I can do better with automata."

But:

M: probabilistic program

φ: PTL specification

Problem: $M \overset{?}{\models} \varphi$

Automata-theoretic: 2 exp. in $\|\varphi\|$

CY'95: exp in $\|\varphi\|$

Is there an automata-theoretic explanation?

ALTERNATION

Nondeterminism: $\exists$ choice

Co-nondeterminism: $\forall$ choices

Alternation: $\exists + \forall$

$\exists$ choice: $\rho(q, a) = \{t_1, t_2\}$

$$\Downarrow$$

$$\rho(q, a) = t_1 \vee t_2$$

$\forall$ choice: $\rho(q, a) = \{t_1, t_2\}$

$$\Downarrow$$

$$\rho(q, a) = t_1 \wedge t_2$$

Alternation: $\rho(q, a) = (t_1 \wedge t_2) \vee (t_3 \wedge t_4)$

PTL and ALTERNATION

Theorem:

There is an algorithm that constructs for a given PTL formula φ an alternating Büchi automaton A^a_φ of size linear in $\|\varphi\|$ s.t. $L(A^a_\varphi) = models(\varphi)$.

Example:

$$\rho(\varphi \cup \psi, a) = \rho(\psi, a) \vee (\rho(\varphi, a) \wedge (\varphi \cup \psi))$$

Weak Alternating Automata

Weakness:
- state set is partitioned into blocks
- every branch of a run tree gets stuck in a block
- every block is either accepting or rejecting

Fact: A^a_φ is weak!

Conjecture: probabilistic non-emptiness for WAA is exponential.

Note: Naive alg. is 2 exponential

<u>Lemma:</u> [Miyano - Hayashi, 1984]

There is an algorithm that constructs for a given WAA A a nondeterministic auto. A^n of size $2^{O(\|A\|)}$ s.t.

$L(A) = L(A^n)$.

Naive Algorithm:

1. $A \xmapsto{\text{exp}} A^n$
2. $A^n \xmapsto{\text{exp}} A^d$
3. $M, A^d \xmapsto{\text{poly}} M \times A^d$
4. ergodic analysis (Poly)

How summarize the problem?

1. Theory vs. practice: Automata theory provides a unifying framework. How bad is forgetting it?

2. Fourth alternation quantification forgetification never happens!

3. The logicians to branching language to be logically "closed"? The demise:

4. What does $((p \cup q) \cup r) \cup t$ mean?

5. Open questions: complexity of MTL fragments?