UNOBIELISTIC MODEL CHECKING

THE AUTOMATA-THEORETIC APPROACH

Moshe Y. Vardi

RICE UNIVERSITY
$w$-Automata

$A = (\Sigma, S, S_0, \delta, \lambda)$

$\Sigma$: alphabet
$S$: states
$S_0 \subseteq S$: initial states
$\delta: S \times \Sigma^* \rightarrow 2^S$: transition function
$\lambda$: acceptance condition

Input: $a_0, a_1, a_2, \ldots$

Run: $D_0, D_1, D_2, \ldots$

$D_0 \in S_0, \ D_i \rightarrow \lambda \delta(D_i, a_i)$$

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

Büchi: $\alpha \leq 5$

Rabin, Streett: $\alpha \leq 2^5 \times 2^5$

i.e., $\{(L_i, R_i) \ldots (L_k, R_k)\}$

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

Rabin acceptance:

$\exists (L_i, R_i) \in \mathcal{E}$ s.t. $\lim(r) \cap L \neq \emptyset$

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

Streett acceptance:

$\forall (L_i, R_i) \in \mathcal{E}: \lim(r) \cap L \neq \emptyset \Rightarrow \lim(r) \cap R \neq \emptyset$

Fairness
\[ L(A) = (0^* 1)^w \]

Büchi: \{2\}

Rabin: (\{25, \emptyset\})

Streett: (\{8, 2\}, \{25\})
System: $M$ - behaviors

Specification: $\gamma$ - correct behaviors

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

all behaviors are correct

T. F. A. E.:
1. $L(M) \subseteq L(\gamma)$
2. $L(M) \cap \overline{L(\gamma)} = \emptyset$
3. $L(M \times \overline{\gamma}) = \emptyset$

↑

Emptiness Problem
Linear Temporal Logic

- PTL: X, U, F, G
- ETL: automata connectives
- MTL: X, M

PTL ⊆ ETL = MTL

Theorem: [J. + Wolper]

There is an algorithm that constructs for a given LTL formula ϕ a Büchi automaton Aϕ of size \( \exp(\text{im}(\#\#\#\#)) \) s.t.
\[ L(CA(\phi)) = \text{models}(\phi). \]

Complementation: \( A\overline{\phi} = A(\neg\phi) \)
\text{GFP:} \hspace{1cm} \text{FGP:}

\text{nondeterministic!}
NONEMPTINESS

$$A = (\varepsilon, S, S_0, P, a)$$

Graph: $$G_A = (S, E_A)$$

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

Nonemptiness Test:

- Büchi: there is a reachable ssc that intersects $$a$$
- Rabin: for some $$(L, R)$$ there is a reachable ssc inside $$S - R$$ that intersects $$L$$
Streett non-emptiness

[Emerson – Lei, 1985]

Iterate:

1. Decompose \( G_A \) into maximal SSCs.

2. For a component \( Q \) and pair \( (L, R) \) of \( \mathcal{E} \), if \( Q \cap L \neq \emptyset \) and \( Q \cap R = \emptyset \), delete states in \( Q \).

Check: \( L(A) \neq \emptyset \) iff a reachable SCC survives.

Complexity: Quadratic
**Probabilistic Programs**

\[ M = (W, P) \] - Markov chain

- \( W \): states
- \( P : W^2 \rightarrow [0,1] \): transition probabilities
  \[ \sum_{w \in W} P(0, w) = 1 \]

**Sequence space:** \((W^w, B, \mu)\)

- \( W^w \): infinite sequences
- \( B \): Borel field
- \( \mu \): measure on \( B \)

**Specification:** \( A = (W, S, S_0, P, \alpha) \)

- Prob. universality: \( \mu(\mathcal{L}(A)) = 1 \)
- Prob. emptiness: \( \mu(\mathcal{L}(A)) = 0 \)
Borel Field

- Cylinder \( (u_0, u_1, \ldots, u_{m-1}) \) = 
  \[ \{ \mathbf{w} \in \mathcal{W}^m : \mathbf{p}[0, \ldots, m-1] = \langle u_0, \ldots, u_{m-1} \rangle \} \]

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

- Borel field: closure under countable unions and comp.
Determinization

Determinism: \(|P(\delta, a)| \leq 1\)
\(|\text{Sol}| = 1\)

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

\[ L(A) = L(A^d) \, \text{(alt., } L(A) = \omega - L(A^d) \text{)} \]

(co-determinization)

Acceptance condition: Streett or Rabin

Müller, 1965: \(2^{||A||}\) - incorrect
McNaughton, 1966: \(2^{||A||}\)
FGP:

\[ \begin{array}{c}
\begin{array}{c}
\text{Rabin: } (\exists 123, \exists 45) \\
\text{Streit: } (\exists 15, \phi)
\end{array}
\end{array} \]
**Product Construction**

\[ M = (W, P) \]

\[ A = (W, S, \delta_0, \rho, \alpha) \text{ deterministic} \]

\[ M \times A = (W \times S, P \times P, W \times \alpha) \]

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

\[ W \times \{ (L_1, R_1), \ldots, (L_k, R_k) \} S = \]

\[ \{ (W \times L_1, W \times R_1), \ldots, (W \times L_k, W \times R_k) \} \]

**Lemma:**

\[ m_k(L(A)) > 0 \iff M \times A (\text{sat}(w \times X)) > 0 \]

limit satisfying, \( \forall \)
Ergodic Analysis

\[ M = (W, P, \alpha) : \text{chain} \]

\[ G_m = (W, E_m) : \text{graph} \]

\[ E_m = \{ (u, v) : P(u, v) > 0 \} \]

Ergodic set: terminal scc of \( G_m \) (scc closed under \( E_m \))

Lemma: \( M_m(\text{sat}(\alpha)) > 0 \) if and only if some ergodic set \( Q \)
“satisfies” \( \alpha \), e.g., \( V(LR) \in Q \), if \( Q \not= \emptyset \) then \( Q \cap R \not= \emptyset \)
(strengthen condition)

Note: Probabilities irrelevant!
Automata-Theoretic Perspective

\[ M = ( \mathcal{W}, P, \delta) \]

\[ A_M = (\exists a \in \mathcal{W}, \mathcal{W}_0, \mathcal{P}_\psi, \alpha \cup \beta) \]

\[ \mathcal{W}_0: \text{initial states} \quad P(u) > 0 \]

\[ \mathcal{P}_\psi(u, a) = \exists u: P(u, u) > 0 \]

\[ \beta = \{ \exists u \exists \tilde{u}: P(u, \tilde{u}) > 0 \} \]

Lemma: \[ M_\psi (\text{sat} L) > 0 \quad \text{iff} \quad L(M_\psi) \neq \emptyset \]

Intuition: Probabilistic behavior

\[ \equiv \] State Fairness
**Verification**

\[ M : \text{ Program} \]
\[ A : \text{ specification (automaton)} \]

1. \[ A \rightarrow A^d \text{ (exponential)} \]
2. \[ M, A^d \rightarrow M \times A^d \text{ (polynomial)} \]
3. ergodic analysis (polynomial for prob. nonemptiness)

**Complexity:** poly. in \text{NMA} \\
exp. in \text{NALL}

Ok!

Lower Bound: PSPACE-hard
VERIFICATION II

M: Program
φ: Specification (PCTL)

1. \( \phi \mapsto A_φ \) (Exponential)
2. \( A_φ \mapsto A_φ^d \) (Exponential)
3. \( A_φ \mapsto M \times A_φ \) (Polynomial)
4. Ergodic analysis (Polynomial)

Complexity: Poly in \( \mathbb{N} \)
2 exp. in \( \mathbb{N} \)

Improvement: [CY’95]
Exp. in \( \mathbb{N} \)
REACTIVE PROBABILISTIC PROGRAMS

Reactive Markov chain:
\[ M = (W, N, P) \]

\( W \): states
\( N \): nondeterministic states
\( W \cdot N \): probabilistic states
\( P \): transition probabilities

History: V. '85 (concurrent Markov chains)

Hart-Sharir-Pnueli '83: interleaved Markov chains

Derman '70: Markov Decision Processes
SCHEDULERS

Schedule $T$ = Adversary = Environment

$T : W^* W \rightarrow W$

$T(\alpha u) = v \Rightarrow p(y, v) > 0$

$M, T \mapsto M_T : Markov$ Chain

$M_T = (W^*, P_T)$

$P_T(\alpha u, xuv) = \begin{cases} 1 & \text{if } \alpha u \in EN \land T(\alpha u) = v \\ 0 & \text{if } \alpha u \in EN \land T(\alpha u) \neq v \\ p(y, v) & \text{if } u \in EN \end{cases}$
**VERIFICATION**

**M:** Reactive Prob. Program  
**σ:** Specification

**Correctness:**

∀ scheduler ξ, $M_{\xi}(\sigma) = 1$

**Intuition:** $\sigma$ almost surely holds regardless of the environment's behavior.

**Dually:** ∃ scheduler ξ s.t. $M_{\xi}(\overline{\sigma}) > 0$
**PRODUCT CONSTRUCTION**

\[ M = (W, N, P) \]

\[ A = (W, S, D_0, P, \alpha) \quad \text{deterministic} \]

\[ M, A \rightarrow M \times A = \text{reactive chain} \]

\[ (W \times S, N \times S, P \times P, W \times \alpha) \]

**Lemma:**

\[ \exists T \quad M^T \vdash (L(A) > 0) \quad \text{iff} \]

\[ \exists T \quad M^{\alpha(A)}_T (\text{sat}(W \times \alpha)) > 0 \]
Ergodic Analysis

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

$G_m = (W, Em)$

$Em = \{(u, v): p(u, v) > 0\}$

Ergodic set: SCC of $G_m$ closed under probabilistic transitions, i.e., under $Em \cap (W \times W \times W)$

Lemma: $\exists \exists : M_m_2(sat(x)) > 0$ iff some ergodic set $Q$ "satisfies" $x$.

Intuition: System has to be fair, environment does not
Automata-Theoretic Perspective

$M = (W, N, P, D)$

$A_M = (\{a, b, c\}, W, W_0, P_0, D_U \beta)$

$P_0(u, a) = \frac{3}{2} v: P(4, v) > 0$

$\beta = \{\{a\}, \{c\}\}: u \in W - N, P(4, u) > 0$

Lemma: $\exists x \mu_M(x) > 0$ if and only if $L(A_M) \neq \emptyset$

Again: Probabilistic behavior

$\equiv$ State Fairness
**FAIRNESS**

Intuition: restrict to "well-behaved" schedulers

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

Generally: Streett condition f

Fair scheduler: Fairness holds w.r.t. Prob. 1

Correctness: spec holds w.r.t. Prob. 1

w.r.t. all fair schedulers

Algorithm: just another Streett condition.
VERIFICATION

M: program

(q, A: specification

1. A \rightarrow A^d \quad (\text{exponential})
   (q_1 \rightarrow A_{eq} \rightarrow A^d \quad (2 \text{ exponential})

2. M, A_d \rightarrow M \times A_d \quad (\text{polynomial})

3. ergodic analysis \quad (\text{polynomial})

Complexity: poly. in \text{IMUI}
QXP. in \text{UIAI}
2QXP. in \text{UIAI}

Matching e.b.: \text{[CY'95]}
Mystery

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

But:

$M$: Probabilistic program
$\varphi$: PTL specification

Problem: $M \models \varphi$

Automata-theoretic: $2^{\exp\text{ in } n}$

Cy'95: $\exp\text{ in } 114n$

Is there an automata-theoretic explanation?
**ALTERNATION**

Non determinism: \( \exists \) choice

Co-mondeterminism: \( \forall \) choices

**Alternation:** \( \exists + \forall \)

\( \exists \) choice: \( p(\exists x.a) = \{ t, t_2 \} \)

\( p(\exists x.a) = t, v t_2 \)

\( \forall \) choice: \( p(\forall a) = \{ b_1, t_2 \} \)

\( p(\forall a) = b_1 \vee t_2 \)

**Alternation:** \( p(\exists x.a) = (b_1 \wedge t_2) \vee (t_3 \wedge t_4) \)
Theorem:
There is an algorithm that constructs for a given PTL formula \( \phi \) an alternating Büchi automaton \( A^a_\phi \) of size linear in \( \|\phi\| \) s.t.
\[
L(A^a_\phi) = \text{models}(\phi).
\]

Example:
\[
\rho(\psi U \psi, a) = \rho(\psi, a) \lor \\
(\rho(\psi, a) \land (\psi U \psi))
\]
Weak Alternating Automata

Weakness: The 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: \( A^q \) is weak!

Conjecture: Probabilistic non-emptiness for WAA is exponential.

Note: Naive alg. is \( 2^{p \cdot n} \) exponential.
Lemma: [Miyano-Hayashi, 1984]

There is an algorithm that constructs for a given WAS $A$ a nondeterministic automaton $A^m$ of size $2^{O(||A||)}$ s.t. $L(A) = L(A^m)$.

Naive Algorithm:
1. $A \overset{\exp}{\rightarrow} A^m$
2. $A^m \overset{\exp}{\rightarrow} A^d$
3. $M, A^d \overset{\text{Poly}}{\rightarrow} M \times A^d$
4. Ergodic analysis (Poly)
How standard is the problem?

1. Theory vs. practice: How bad is unit testing at your work.

2. Point that 8x80 from question turning for little or none ever happens!

3. The obvious does to dismiss. The language has to be logically closed? 

4. What does \((puq)uv\) mean? 

5. Are genuine fragments of practical complexity of MTL?