p-Automata: New Foundations for Discrete-Time Probabilistic Verification

Michael Huth, Nir Piterman, and Daniel Wagner

RWTH Aachen University
11 March 2010
Aachen, Germany
Outline of talk

Motivation
Markov Chains and PCTL
Weak Stochastic Games
p-Automata
Acceptance Games
Expressiveness
Simulation
Conclusion
Motivation
Abstraction in Probabilistic Model Checking

- Probabilistic model checking increasingly important, widely used technique
- Advanced model-checking tools exist, e.g. PRISM (Oxford) and MRMC (Aachen)
- Scalability of analysis critical in many application domains
- Abstraction believed to be critical for scalability
- Effective abstraction techniques for probabilistic model checking: still an open research problem
Automata-Based Verification

Automaton $A$ accepts as its language $\mathcal{L}(A)$ set of models $M$. This approach supports important techniques:

- specifications and models have meaning-preserving representations as automata
- model checking reduces to acceptance of automata input
- satisfiability reduces to emptiness checks of automata
- automata closed under Boolean operations
- simulation under-approximates language containment
- uniform, strong framework for sound abstraction of branching-time properties
Aim of this talk

Develop automata-based approach to probabilistic verification:

- supports all aforementioned techniques
- models: countable, discrete-time, labeled Markov chains
- specifications: subsume Probabilistic Computation Tree Logic (PCTL) [Hansson & Jonsson 1994]
- p-automata are themselves probabilistic specifications
Related work

- Automata for co-algebras [Venema 2006] have corresponding logic with finite-model property: hence they cannot express path modalities of PCTL.

These don’t support all aforementioned techniques.
Markov Chains and PCTL
Models

Countable, discrete-time, labeled Markov chain $M$:

- set of atomic propositions $\mathbb{AP}$
- $S$ countable set of locations
- $P : S \times S \to [0, 1]$ stochastic matrix with $\sum_{s' \in S} P(s, s') = 1$ for all $s \in S$
- location $s^{\text{in}} \in S$ designated initial one
- $L : S \to 2^{\mathbb{AP}}$ labeling function
  $L(s) =$ set of propositions true in location $s$
- $P(s, s') =$ probability that $M$, when in location $s$, transitions to location $s'$ in one discrete time step
Example

- Three locations $s_0$ (initial), $s_1$, and $s_2$
- Two atomic propositions $a$ and $b$; e.g. $a$ true only at $s_0$
- Probability distribution $P(s_0, \cdot)$ uniform over all locations
- Sink state $s_2$ has implicit probability 1 self-loop
- $\{s_2\}$ terminal, maximal strongly connected component
PCTL Syntax

\[ \phi, \psi ::= \begin{align*}
\text{PCTL formulas} & \quad \alpha ::= \\
\text{Atom} & \quad \text{Next} \\
\text{Conjunction} & \quad \text{Until} \\
\text{Disjunction} & \quad \text{Weak Until} \\
\text{Path Probability} & \quad \phi \wedge \psi \\
\phi \vee \psi \\
[\alpha] \triangledown p
\end{align*} \]

- \( a \in AP, \ k \in \mathbb{N} \cup \{\infty\}, \ p \in [0, 1], \triangledown \in \{>, \geq\} \)
- full PCTL has this Greater Than Negation Normal Form
PCTL Semantics

\[ \|a\| = \{s \in S \mid a \in L(s)\} \quad \|\neg a\| = \{s \in S \mid a \notin L(s)\} \]
\[ \|\phi \land \psi\| = \|\phi\| \cap \|\psi\| \quad \|\phi \lor \psi\| = \|\phi\| \cup \|\psi\| \]
\[ \| [\alpha] \triangleright p \| = \{s \in S \mid \text{Prob}_M(s, \alpha) \triangleright p\} \]

- paths: sequences \(s_0 s_1 \ldots\) with \(P(s_i, s_{i+1}) > 0\)
- \(s_0 s_1 \ldots \models X \phi\) iff \(s_1 \in \|\phi\|_M\)
- \(s_0 s_1 \ldots \models \phi U \leq^k \psi\) iff there is \(l \in \mathbb{N}\) such that \(l \leq k\), \(s_l \in \|\psi\|_M\) and for all \(0 \leq j < l\) we have \(s_j \in \|\phi\|_M\)
- \(s_0 s_1 \ldots \models \phi W \leq^k \psi\) iff for all \(l \in \mathbb{N}\) such that \(0 \leq l \leq k\), either \(s_l \in \|\phi\|_M\) or there is \(0 \leq j \leq l\) with \(s_j \in \|\psi\|_M\)
Example

- Convention: write U for $U_{\leq \infty}$ and W for $W_{\leq \infty}$
- $s_0 \in \llbracket (a \lor b) U (\neg a \land \neg b) \rrbracket_{\geq 1} \|_M$ since measure of paths beginning at $s_0$ and satisfying $(a \lor b) U (\neg a \land \neg b)$ is 1
- $s_0 \in \llbracket a U b \rrbracket_{\geq 0.5} \|_M$ as infinite path $s_0s_0\ldots$ has measure 0
Weak Stochastic Games
Stochastic game

Tuple $G = ((V, E), (V_0, V_1, V_p), \kappa, \alpha)$ where

- $(V, E)$ directed graph
- $(V_0, V_1, V_p)$ partitions $V$ into Player 0, Player 1, and probabilistic configurations
- for each $v \in V_p$: $\kappa(v)$ probability distribution on $E(v) = \{ v' \mid (v, v') \in E \}$ with $(v, v') \in E$ iff $\kappa(v)(v') \neq 0$
- $\alpha \subseteq V$ winning condition
Weakness

- **Weak** Stochastic game $G$: all its maximal, strongly connected components (SCC) $V'$ in $(V, E)$ satisfy
  \[ V' \subseteq \alpha \text{ or } V' \cap \alpha = \{\} \]

- **Weak Game** $G$: weak stochastic game without probabilistic configurations: $V_p = \{\}$.

- Markov chain: representable as weak stochastic game with $V_0 = V_1 = \{\}$ and $\alpha = V$. 
Plays and their wins

- Plays from $v_0$ are sequences $v_0 \, v_1 \ldots$ of configurations
  - $v_i \in V_0$: Player 0 chooses $v_{i+1}$ with $(v_i, v_{i+1}) \in E$
  - $v_i \in V_1$: Player 1 chooses $v_{i+1}$ with $(v_i, v_{i+1}) \in E$
  - $v_i \in V_p$: distribution $\kappa(v_i)$ chooses $v_{i+1}$ at random

- WLOG: plays are infinite as Player 0 and Player 1 configurations don’t deadlock.

- Play won by
  - player 0 if all configurations in some suffix of play are in $\alpha$
  - Otherwise: player 1 wins play
Strategies and game values

- (pure memoryless) strategy $\sigma \in \Sigma$ for Player 0: function $\sigma : V_0 \rightarrow V$ with $(v, \sigma(v)) \in E$ for all $v \in V_0$
- strategy $\pi \in \Pi$ for Player 1: similar function $\pi : V_1 \rightarrow V$
- each pair $(\sigma, \pi) \in \Sigma \times \Pi$ determines Markov chain $M^{\sigma, \pi}$: all paths in $G$ consistent with $\sigma$ and $\pi$
- $\text{val}_{\sigma, \pi}^{\sigma}(v)$ measure of paths from $v$ Player 0 wins in $M^{\sigma, \pi}$
- $\text{val}_0(v) = \sup_{\sigma \in \Sigma} \inf_{\pi \in \Pi} \text{val}_{\sigma, \pi}^{\sigma}(v)$: game value for player 0 at $v$
- $\text{val}_1(v) = \sup_{\pi \in \Pi} \inf_{\sigma \in \Sigma}(1 - \text{val}_{\sigma, \pi}^{\sigma}(v))$ game value for player 1 at $v$
- strategies that achieve these values are optimal
A Weak Stochastic Game

\[ \alpha = \{ v_2, v_5, v_7, v_8 \} \]

- game values for player 0 are 1 at \( v_2, v_5, v_7, v_8 \); 0 at \( v_4 \) and \( v_6 \); 0.4 at \( v_3 \); 0.52 at \( v_1 \); and 0.46 at \( v_0 \)
Determinacy and algorithms

- Stochastic games $G$ are determined: for all $v \in V$
  \[ \text{val}_0(v) = 1 - \text{val}_1(v) \]

- Let $G$ be finite:
  - $\text{val}_0(v)$ computable in NP & coNP
  - optimal strategies exist for both players
  - If $G$ is weak, then $\text{val}_0(v) \in \{0, 1\}$ and is linear-time computable
p-Automata
A p-automaton $A$ is tuple

$$\langle \Sigma, Q, \delta, \varphi^{\text{in}}, \alpha \rangle$$

- $\Sigma$ finite input alphabet
- $Q$ set of states (not necessarily finite)
- $\delta : Q \times \Sigma \to \mathcal{B}^+(Q \cup \llbracket Q \rrbracket)$ transition function
- $\varphi^{\text{in}} \in \mathcal{B}^+(Q \cup \llbracket Q \rrbracket)$ initial condition
- $\alpha \subseteq Q$ acceptance condition
Guiding Intuition

- p-automata reuse ideas from alternating tree automata
- Need ability to quantify over probabilities of path sets
- Do this for regular path sets, not just for one time step.
- Need mechanism for decomposing probabilities and witnessing path sets.
- Value space $B^+(Q \cup \llbracket Q \rrbracket)$ for transitions informed by that
Definition of $B^+(Q \cup [Q])$

- $B^+(T)$ set of positive Boolean formulas generated from elements $t \in T$:

  \[
  \varphi ::= t \mid \text{ff} \mid \text{tt} \mid \varphi \lor \varphi \mid \varphi \land \varphi
  \]

- Term set $[Q]$ defined through:

  \[
  [Q]_\succ = \{[q] \times p \mid q \in Q, \times \in \{\geq, >\}, p \in [0, 1]\}
  
  [Q]^* = \{(t_1, \ldots, t_n) \mid n \in \mathbb{N}, \forall i: t_i \in [Q]_\succ\}
  
  [Q]^{\prec} = \{\prec(t_1, \ldots, t_n) \mid n \in \mathbb{N}, \forall i: t_i \in [Q]_\succ\}
  
  [Q] = [Q]^* \cup [Q]^{\prec}
  \]
Intuition behind $B^+(Q \cup [Q])$

- meaning of Boolean connectives as for alternating automata

- $\lbrack q \rbrack_{\triangleright p}$ holds in location $s$ if: measure of paths that begin in $s$ and satisfy $q$ is $\blacklozenge p$

- $\ast(\lbrack q_1 \rbrack_{> p_1}, \lbrack q_2 \rbrack_{\geq p_2})$ means
  - $q_1$ and $q_2$ hold with probability greater than $p_1$ and greater than or equal to $p_2$, respectively
  - and sets supplying these probabilities are disjoint

- $\forall(\lbrack q_1 \rbrack_{\geq p_1}, \lbrack q_2 \rbrack_{\geq p_2})$ has dual meaning
Example

\[ A = \langle 2^{\{a,b\}} , \{ q_1, q_2 \} , \delta , \llbracket q_1 \rrbracket \geq 0.5 , \{ q_2 \} \rangle \]

\[ \delta(q_1, \{a, b\}) = \delta(q_1, \{a\}) = q_1 \lor \llbracket q_2 \rrbracket \geq 0.5 \]
\[ \delta(q_2, \{b\}) = \delta(q_2, \{a, b\}) = \llbracket q_2 \rrbracket \geq 0.5 \]
\[ \delta(q_1, \{\}) = \delta(q_1, \{b\}) = \delta(q_2, \{\}) = \delta(q_2, \{a\}) = \text{ff} \]

- \( q_2 \) encodes recursive property \( \phi = \text{“b holds at location presently read by } q_2 \text{, and } \phi \text{ holds with probability } \geq 0.5 \text{ in next locations”} \)
- \( q_1 \) asserts it is possible to get to a location that satisfies \( q_2 \) along a path that satisfies \( a \)
- initial condition \( \llbracket q_1 \rrbracket \geq 0.5 \) encodes that set of paths satisfying “\( a \cup \phi \)” has probability at least 0.5
Acceptance Games
Constraints for solvability of acceptance games

- p-automata can express recursive, probabilistic, regular path sets
- can do this also using $\ast$ and $\Downarrow$ operator
- such properties may potentially be inconsistent, making the acceptance game insolvable
- **current solution**: constrain $A$, through its graph $G_A$
- partition graph $G_A$ into maximal, strongly connected components (SCC)
- each SCC determines a weak stochastic or weak game
- solve these games bottom-up
Structure of acceptance game for $M \in \mathcal{L}(A)$

- Most configurations of these weak (stochastic) games in $S \times (Q \cup \{\text{cl}_p(\delta(q, \phi)) \mid q \in Q, \phi \in 2^{\text{AP}}\})$
  where $\text{cl}_p(\eta)$ set of Boolean subformulas of $\eta$
- Initial configuration $(s^{\text{in}}, \varphi^{\text{in}})$ occurs as configuration in exactly one of these games
- $A$ accepts $M$ iff game value of $(s^{\text{in}}, \varphi^{\text{in}})$ in that game is $1$
Graph $G_A = \langle Q', \rightarrow, \rightarrow_b, \rightarrow_u \rangle$ of p-Automaton $A$

$Q' = Q \cup \text{cl}_p(\delta(Q, \Sigma))$

$\rightarrow = \{((\varphi_1 \land \varphi_2, \varphi_i), (\varphi_1 \lor \varphi_2, \varphi_i) | \varphi_i \in Q' \setminus Q \} \cup$

$\{((q, \delta(q, \sigma)) | q \in Q, \sigma \in \Sigma\}$

$\rightarrow_u = \{((\varphi \land q, q), (q \land \varphi, q), (\varphi \lor q, q), (q \lor \varphi, q) | \varphi \in Q', q \in Q\}$

$\rightarrow_b = \{((\varphi, q) | \varphi \in \llbracket Q \rrbracket \text{ and } q \in \text{gs}(\varphi)\}$

- $\text{gs}(\varphi)$ set of guarded states of $\varphi$: all $q' \in Q$ occurring in some term in $\varphi$
- $\rightarrow_b$ set of bounded transitions
- $\rightarrow_u$ set of unbounded transitions
- $\rightarrow$ set of simple transitions
- mark $(\varphi, q) \in \rightarrow_b$ with $\ast$ (resp. with $\checkmark$) if some $\llbracket q' \rrbracket_{\Box^p}$ occurs in $\varphi$ within scope of a $\ast$ (resp. $\checkmark$)
Example $G_A$

\[ A = \langle 2\{a,b\}, \{q_1, q_2\}, \delta, \lceil q_1 \rceil \geq 0.5, \{q_2\} \rangle \]

\[ \delta(q_1, \{a, b\}) = \delta(q_1, \{a\}) = q_1 \lor \lceil q_2 \rceil \geq 0.5 \]
\[ \delta(q_2, \{b\}) = \delta(q_2, \{a, b\}) = \lceil q_2 \rceil \geq 0.5 \]
\[ \delta(q_1, \{\} ) = \delta(q_1, \{b\}) = \delta(q_2, \{\} ) = \delta(q_2, \{a\}) = \text{ff} \]
Uniform Weak p-Automata

- p-automaton $A$ **uniform** if:
  - cycles in $G_A$ have transitions only in $\rightarrow \cup \rightarrow_b$ or only in $\rightarrow \cup \rightarrow_u$
  - cycles in $\langle Q, \rightarrow \cup \rightarrow_b \rangle$ have markings $\{\}$, $\{\ast\}$ or $\{\bigstar\}$, not $\{\ast, \bigstar\}$.
  - preorder that encodes reachability in $\rightarrow \cup \rightarrow_b \cup \rightarrow_u$, induces finitely many equivalence classes $\left(\langle q \rangle\right)$.

- (not necessarily uniform) p-automaton $A$ **weak** if for all $q \in Q$, either $\left(\langle q \rangle\right) \cap Q \subseteq \alpha$ or $\left(\langle q \rangle\right) \cap \alpha = \{\}$.

- acceptance game for $M \in \mathcal{L}(A)$ well-defined for uniform weak p-automata

- acceptance game exponential in size of input $M$ and size of automaton $A$
Uniform Weak p-automaton $A$

\[
\delta(q_1, \{a, b\}) = \delta(q_1, \{a\}) = q_1 \lor \llbracket q_2 \rrbracket \geq 0.5 \\
\delta(q_2, \{b\}) = \delta(q_2, \{a, b\}) = \llbracket q_2 \rrbracket \geq 0.5 \\
\delta(q_1, \{\} ) = \delta(q_1, \{b\}) = \delta(q_2, \{\} ) = \delta(q_2, \{a\} ) = \text{ff}
\]

- **A uniform:** $\text{SCC}((q_1)) = \{q_1, q_1 \lor \llbracket q_2 \rrbracket \geq 0.5\}$ no bounded transitions, $\text{SCC}((q_2)) = \{q_2, \llbracket q_2 \rrbracket \geq 0.5\}$ no unbounded transitions, $\text{SCC}(\llbracket q_1 \rrbracket \geq 0.5) = \llbracket q_1 \rrbracket \geq 0.5$ trivial

- **A weak:** $\alpha = \{q_2\}$.
Expressiveness
Dual of $A = \langle \Sigma, Q, \delta, \varphi^{\text{in}}, \alpha \rangle$:

$M \in \mathcal{L}(\text{dual}(A))$ iff $M \notin \mathcal{L}(A)$

$$\text{dual}(A) = \langle \Sigma, \overline{Q}, \overline{\delta}, \text{dual}(\varphi^{\text{in}}), Q \setminus \alpha \rangle$$

- $\overline{Q} = \{q \mid q \in Q\}$ and $\overline{\delta}(q, \sigma) = \text{dual}(\delta(q, \sigma))$

| $\text{dual}(\varphi_1 \lor \varphi_2)$ | $\text{dual}(\varphi_1) \ast \text{dual}(\varphi_2)$ |
| $\text{dual}(\varphi_1 \land \varphi_2)$ | $\text{dual}(\varphi_1) \lor \text{dual}(\varphi_2)$ |
| $\text{dual}(\varphi_1 \lor \varphi_2)$ | $\text{dual}(\varphi_1) \land \text{dual}(\varphi_2)$ |
| $\text{dual}(q)$ | $\overline{q}$ |
| $\text{dual}(\overline{q})$ | $q$ |
| $\text{dual}(\ulcorner q \urcorner \trianglesingleleft p)$ | $\ulcorner \overline{q} \urcorner_{\text{dual}(\trianglesingleleft p)}$ |
| $\text{dual}(\geq p)$ | $> 1 - p$ |
| $\text{dual}(> p)$ | $\geq 1 - p$ |
Let input alphabet $\Sigma$ be $2^{\text{AP}}$.

- Set of languages accepted by p-automata with $\Sigma$ is closed under Boolean operations
- Language containment of p-automata with $\Sigma$ reduces to language emptiness of such p-automata, and vice versa
- For p-automaton $A = \langle 2^{\text{AP}}, Q, \delta, \varphi^{\text{in}}, \alpha \rangle$ and probabilistically bisimilar Markov chains $M_1, M_2$ over $\text{AP}$:
  $$M_1 \in \mathcal{L}(A) \text{ iff } M_2 \in \mathcal{L}(A)$$
Representing Markov chains

Convert Markov chain $M = (S, P, L, s^{in})$ into p-automaton

$$A_M = \langle 2^{AP}, Q, \delta, \varphi^{in}, \alpha \rangle$$

- $\mathcal{L}(A_M)$ set of Markov chains bisimilar to $M$
- conversion uses linear order on each successor set:

- $Q = \{(s, s') \in S \times S \mid P(s, s') > 0\}$
- $\delta((s, s'), L(s)) = *([([s', s'']) \geq_{P(s', s'')} \mid P(s', s'') > 0)]$
- $\delta((s, s'), \sigma) = \text{ff} \quad \text{if} \ \sigma \neq L(s)$
- $\varphi^{in} = *([([s^{in}, s']) \geq_{P(s^{in}, s')} \mid P(s^{in}, s) > 0)]$
- $\alpha = Q$

- Only bounded transitions and $*$ operator, so uniform weak

Michael Huth, Nir Piterman, and Daniel Wagner
p-Automata: New Foundations for Discrete-Time Probabilistic Verification
Representing PCTL formulas

Convert PCTL formula $\phi$ over $\text{AP}$ into p-automaton

$$A_\phi = \langle 2^{\text{AP}}, \text{cl}_t(\phi) \cup \text{AP}, \rho_x, \rho_\epsilon(\phi), F \rangle$$

- $\mathcal{L}(A_\phi)$ exactly Markov chains satisfying $\phi$
- resembles translation from CTL to alternating tree automata:
  - $\text{cl}_t(\phi)$ set of temporal subformulas of $\phi$
  - $F$ consists of $\text{AP}$ and all $\psi$ of $\text{cl}_t(\phi)$ not of form $\psi_1 \cup \psi_2$
- function $\rho_x$: unfolds fixed points, replaces PCTL $[]$ with $\llbracket\llbracket$
- function $\rho_\epsilon$: for initial state, replaces $[]$ with $\llbracket\llbracket$
Example for $\varphi = [a \cup [X b]_{>0.5}]_{\geq 0.3}$

$$A_\varphi = \langle 2^{\{a,b\}}, \text{cl}_t(\varphi) \cup \{a, b\}, \rho_x, \rho_\epsilon(\varphi), F \rangle$$

- $\text{cl}_t(\varphi) = \{a \cup [X b]_{>0.5}, X b\}$
- $\rho_\epsilon(\varphi) = (a \land [a \cup [X b]_{>0.5}]_{\geq 0.3}) \lor [X b]_{>0.5}$
- $F = \{X b, a, b\}$
- $\rho_x(X b) = b$
- $\rho_x(a \cup [X b]_{>0.5}) = (a \land a \cup [X b]_{>0.5}) \lor [X b]_{>0.5}$
p-Automata Are More Expressive

- p-automata more expressive than Markov chains (trivial)
- Routine (counting argument) to show that p-automata are more expressive than PCTL formulas
- Would like to capture a fixed-point logic that corresponds to p-automata (not yet done, don’t yet know how)
Simulation
Under-approximating language containment

- decidability status of $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ not known at present
- seek “efficient” simulation $A \leq B$ between p-automata such that $A \leq B$ implies $\mathcal{L}(A) \subseteq \mathcal{L}(B)$
- we developed such a simulation notion that borrows from
  - fair simulation
  - simulation for alternating word automata
  - probabilistic bisimulation
  - and from our acceptance games $M \in \mathcal{L}(A)$

- For $A$ and $B$ finite, or for $A$ representing some Markov chain, the above under-approximation holds
Conclusion
What We Did

- presented notion of p-automaton $A$ which accepts or rejects an entire Markov chain $M$ as input
- reduced acceptance games for $M \in \mathcal{L}(A)$ to solving a weak stochastic game, at most exponential in size of automaton and Markov chain
- showed p-automata to be closed under Boolean operations, their languages to be closed under bisimulation
- represented both Markov chains and PCTL formulas as p-automata
- developed notion of simulation that “efficiently” under-approximates language inclusion
What We Want To Do

- Decidability of non-emptiness for **qualitative** p-automata? (Only thresholds > 0 and ≥ 1.)
- Decidability of non-emptiness for **full** p-automata?
- Determinism and non-determinism for p-automata?
- How to define and solve acceptance game for non-uniform p-automata?
- p-automata as acceptors of Markov decision processes?
- Retrofit existing tools with support for p-automata?
- How to use p-automata for CEGAR?
Thank You for Your Kind Attention

Questions?