Lecture 18

LTL model checking for DTMCs and MDPs

Dr. Dave Parker

Department of Computer Science
University of Oxford
Overview

- **Recall**
  - deterministic $\omega$-automata (DBA or DRA) and DTMCs

- **LTL model checking for DTMCs**
  - measurability
  - complexity
  - PCTL* model checking for DTMCs

- **LTL model checking for MDPs**
Recall – DBA and DRA

• Deterministic Büchi automata (DBA)
  – \((Q, \Sigma, \delta, q_0, F)\)
  – accepting run must visit some state in \(F\) infinitely often
  – less expressive than nondeterministic Büchi automata (NBA)

• Deterministic Rabin automata (DRA)
  – \((Q, \Sigma, \delta, q_0, \text{Acc})\)
  – \(\text{Acc} = \{ (L_i, K_i) \mid 1 \leq i \leq k \}\)
  – for some pair \((L_i, K_i)\), the states in \(L_i\) must be visited finitely often and (some of) the states in \(K_i\) visited infinitely often
  – equally expressive as NBA
  – (i.e. all \(\omega\)-regular properties; and hence all LTL formulae)
Product DTMC for a DBA

- For DTMC $D$ and DBA $A$

\[
\text{Prob}^{D}(s, A) = \text{Prob}^{D \otimes A}( (s, q_s), \text{GF accept})
\]

- where $q_s = \delta(q_0, L(s))$

- Hence:

\[
\text{Prob}^{D}(s, A) = \text{Prob}^{D \otimes A}( (s, q_s), F T_{\text{GF accept}})
\]

- where $T_{\text{GF accept}}$ is the union of all BSCCs $T$ in $D \otimes A$ with $T \cap \text{Sat (accept)} \neq \emptyset$

- Reduces to computing BSCCs and reachability probabilities
Product DTMC for a DRA

- For DTMC $D$ and DRA $A$

$$\text{Prob}^D(s, A) = \text{Prob}^{D \otimes A}((s, q_s), \bigvee_{1 \leq i \leq k} (\text{FG } \neg l_i \land \text{GF } k_i))$$

- where $q_s = \delta(q_0, L(s))$

- Hence:

$$\text{Prob}^D(s, A) = \text{Prob}^{D \otimes A}((s, q_s), F T_{\text{Acc}})$$

- where $T_{\text{Acc}}$ is the union of all accepting BSCCs in $D \otimes A$

- an accepting BSCC $T$ of $D \otimes A$ is such that, for some $1 \leq i \leq k$:
  - $q \models \neg l_i$ for all $(s, q) \in T$ and $q \models k_i$ for some $(s, q) \in T$
  - i.e. $T \cap (S \times L_i) = \emptyset$ and $T \cap (S \times K_i) \neq \emptyset$

- Reduces to computing BSCCs and reachability probabilities
LTL model checking for DTMCs

• Model check LTL specification $P_{\neg p}[\psi]$ against DTMC $D$

• 1. Generate a deterministic Rabin automaton (DRA) for $\psi$
   – build nondeterministic Büchi automaton (NBA) for $\psi$ [VW94]
   – convert the NBA to a DRA [Saf88]

• 2. Construct product DTMC $D \otimes A$

• 3. Identify accepting BSCCs of $D \otimes A$

• 4. Compute probability of reaching accepting BSCCs
   – from all states of the $D \otimes A$

• 5. Compare probability for $(s, q_s)$ against $p$ for each $s$

• Qualitative LTL model checking – no probabilities needed
Example 3 (Lec 17) revisited

- Model check $P_{>0.2} [ \text{FG a} ]$

- Result:
  - $\text{Prob}(\text{FG a}) = [0.125, 0.5, 1, 0, 0, 1]$
  - $\text{Sat}(P_{>0.2} [ \text{FG a} ]) = \{ s_1, s_2, s_5 \}$
Measurability of $\omega$–regular properties

• For any $\omega$–regular property $\psi$
  – the set of $\psi$–satisfying paths in any DTMC $D$ is measurable

• Hence, the same applies to
  – any regular safety property
  – any LTL formula

• Proof sketch
  – any $\omega$–regular property can be represented by a DRA $A$
  – we can construct $D \otimes A$, in which there is a direct mapping from
    any path $\omega$ in $D$ to a path $\omega'$ in $D \otimes A$
  – $\omega \models \psi$ iff $\omega' \models \bigvee_{1 \leq i \leq k} \left( \text{FG } \neg l_i \land \text{GF } k_i \right)$
  – GF $\Phi$ and FG $\Phi$ are measurable (see lecture 3)
  – $\land$ and $\lor$ = intersection/union (which preserve measurability)
Complexity

- **Complexity of model checking LTL formula $\psi$ on DTMC $D$**
  - is doubly exponential in $|\psi|$ and polynomial in $|D|$ (for the algorithm presented in these lectures)
- **Converting LTL formula $\psi$ to DRA $A$**
  - for some LTL formulae of size $n$, size of smallest DRA is $2^{2n}$
- **BSCC computation**
  - Tarjan algorithm – linear in model size (states/transitions)
- **Probabilistic reachability**
  - linear equations – cubic in (product) model size
- **In total: $O(poly(|D|,|A|))$**
- **In practice: $|\psi|$ is small and $|D|$ is large**
- **Complexity can be reduced to single exponential in $|\psi|$**
  - see e.g. [CY88,CY95]
PCTL* model checking

- **PCTL* syntax:**
  
  - $\phi ::= \text{true} \mid a \mid \phi \land \phi \mid \neg \phi \mid P_{\sim p} [ \psi ]$
  
  - $\psi ::= \phi \mid \psi \land \psi \mid \neg \psi \mid X \psi \mid \psi U \psi$

- **Example:**
  
  - $P_{>p} [ \text{GF ( send } \to \ P_{>0} [ \text{ F ack } ] ) ]$

- **PCTL* model checking algorithm**
  
  - bottom-up traversal of parse tree for formula (like PCTL)
  
  - to model check $P_{\sim p} [ \psi ]$:
    
    - replace maximal state subformulae with atomic propositions
    
    - (state subformulae already model checked recursively)
    
    - modified formula $\psi$ is now an LTL formula
    
    - which can be model checked as for LTL
Recall – end components in MDPs

- End components of MDPs are the analogue of BSCCs in DTMCs.
- An end component is a strongly connected sub-MDP.
- A sub-MDP comprises a subset of states and a subset of the actions/distributions available in those states, which is closed under probabilistic branching.

Note:
- Action labels omitted.
- Probabilities omitted where $=1$. 
Recall – end components in MDPs

- End components of MDPs are the analogue of BSCCs in DTMCs

- For every end component, there is an adversary which, with probability 1, forces the MDP to remain in the end component, and visit all its states infinitely often

- Under every adversary $\sigma$, with probability 1, the set of states visited infinitely often forms an end component
Recall – long-run properties of MDPs

• Maximum probabilities
  – \( p_{\text{max}}(s, GF a) = p_{\text{max}}(s, F T_{GFa}) \)
    • where \( T_{GFa} \) is the union of sets \( T \) for all end components
      \((T,\text{Steps}')\) with \( T \cap \text{Sat}(a) \neq \emptyset \)

  – \( p_{\text{max}}(s, FG a) = p_{\text{max}}(s, F T_{FGa}) \)
    • where \( T_{FGa} \) is the union of sets \( T \) for all end components
      \((T,\text{Steps}')\) with \( T \subseteq \text{Sat}(a) \)

• Minimum probabilities
  – need to compute from maximum probabilities...
  – \( p_{\text{min}}(s, GF a) = 1 - p_{\text{max}}(s, FG \neg a) \)
  – \( p_{\text{min}}(s, FG a) = 1 - p_{\text{max}}(s, GF \neg a) \)
Automata–based properties for MDPs

- For an MDP $M$ and automaton $A$ over alphabet $2^{AP}$
  - consider probability of “satisfying” language $L(A) \subseteq (2^{AP})^\omega$
  - $\text{Prob}^M,\sigma(s, A) = \Pr_{s}^{M,\sigma}\{ \omega \in \text{Path}^M,\sigma(s) \mid \text{trace}(\omega) \in L(A) \}$
  - $p_{\text{max}}^M(s, A) = \sup_{\sigma \in \text{Adv}} \text{Prob}^M,\sigma(s, A)$
  - $p_{\text{min}}^M(s, A) = \inf_{\sigma \in \text{Adv}} \text{Prob}^M,\sigma(s, A)$

- Might need minimum or maximum probabilities
  - e.g. $s \models P_{\geq 0.99} [ \psi_{\text{good}} ] \iff p_{\text{min}}^M(s, \psi_{\text{good}}) \geq 0.99$
  - e.g. $s \models P_{\leq 0.05} [ \psi_{\text{bad}} ] \iff p_{\text{max}}^M(s, \psi_{\text{bad}}) \leq 0.05$

- But, $\psi$–regular properties are closed under negation
  - as are the automata that represent them
  - so can always consider maximum probabilities…
  - $p_{\text{max}}^M(s, \psi_{\text{bad}})$ or $1 - p_{\text{max}}^M(s, \neg \psi_{\text{good}})$
LTL model checking for MDPs

- Model check LTL specification $P \neg p [ \psi ]$ against MDP $M$

  - 1. Convert problem to one needing maximum probabilities
    - e.g. convert $P_{>p} [ \psi ]$ to $P_{<1-p} [ \neg \psi ]$
  
  - 2. Generate a DRA for $\psi$ (or $\neg \psi$)
    - build nondeterministic Büchi automaton (NBA) for $\psi$ [VW94]
    - convert the NBA to a DRA [Saf88]
  
  - 3. Construct product MDP $M \otimes A$
  
  - 4. Identify accepting end components (ECs) of $M \otimes A$
  
  - 5. Compute max. probability of reaching accepting ECs
    - from all states of the $D \otimes A$
  
  - 6. Compare probability for $(s, q_s)$ against $p$ for each $s$
Product MDP for a DRA

- For a MDP $M = (S, s_{init}, \text{Steps}, L)$
- and a (total) DRA $A = (Q, \Sigma, \delta, q_0, \text{Acc})$
  - where $\text{Acc} = \{ (L_i, K_i) \mid 1 \leq i \leq k \}$

- The product MDP $M \otimes A$ is:
  - the MDP $(S \times Q, (s_{init}, q_{init}), \text{Steps}', L')$ where:
    $q_{init} = \delta(q_0, L(s_{init}))$
    $\text{Steps}'(s,q) = \{ \mu^q \mid \mu \in \text{Step}(s) \}$
    $\mu^q(s',q') = \begin{cases} 
      \mu(s') & \text{if } q' = \delta(q, L(s)) \\
      0 & \text{otherwise}
    \end{cases}$

$l_i \in L'(s,q) \text{ if } q \in L_i \text{ and } k_i \in L'(s,q) \text{ if } q \in K_i$
(i.e. state sets of acceptance condition used as labels)
Product MDP for a DRA

• For MDP \( M \) and DRA \( A \)

\[
p_{\text{max}}^M(s, A) = p_{\text{max}}^{M \otimes A}((s, q_s), \bigvee_{1 \leq i \leq k} (\text{FG } \neg l_i \land \text{GF } k_i))
\]

– where \( q_s = \delta(q_0, L(s)) \)

• Hence:

\[
p_{\text{max}}^M(s, A) = p_{\text{max}}^{M \otimes A}((s, q_s), \text{F } T_{\text{Acc}})
\]

– where \( T_{\text{Acc}} \) is the union of all sets \( T \) for accepting end components \((T, \text{Steps'})\) in \( D \otimes A \)

– an accepting end components is such that, for some \( 1 \leq i \leq k \):
  • \((s, q) \models \neg l_i \) for all \((s, q) \in T \) and \((s, q) \models k_i \) for some \((s, q) \in T \)
  • i.e. \( T \cap (S \times L_i) = \emptyset \) and \( T \cap (S \times K_i) \neq \emptyset \)
MDPs – Example 1

- **Model check** $P_{<0.8} [ G \neg b \land GF \ a ]$

  - **Result:**
    - $p_{\text{max}}(G \neg b \land GF \ a) = [0.7, 0, 1, 1]$
    - $\text{Sat}(P_{<0.8} [ G \neg b \land GF \ a ]) = \{ s_0, s_1 \}$

DRA (in fact DBA):

Acc = \{(\emptyset, \{q_1\})\}
• **Model check** $P_{>0} [ G \neg b \land GF a ]$
  
  $- p_{\text{min}}(s, G \neg b \land GF a) = 1 - p_{\text{max}}(s, \neg(G \neg b \land GF a))$
  
  $= 1 - p_{\text{max}}(s, F b \lor FG \neg a))$

  
  **Result:** $p_{\text{min}}(G \neg b \land GF a) = [0, 0, 0, 1]$

  $- \text{Sat}(P_{>0} [ G \neg b \land GF a ]) = \{s_3\}$
LTL model checking for MDPs

- **Maximal end components**
  - can optimise LTL model checking using maximal end components (there may be exponentially many ECs)

- **Qualitative LTL model checking**
  - no numerical computation: use Prob1E, Prob0A algorithms

- **Complexity of model checking LTL formula $\psi$ on MDP $M$**
  - is doubly exponential in $|\psi|$ and polynomial in $|M|$  
  - unlike DTMCs, this cannot be improved upon

- **PCTL* model checking**
  - LTL model checking can be adapted to PCTL*, as for DTMCs

- **Optimal adversaries for LTL formulae**
  - memoryless adversary always exists for $p_{\text{max}}(s, \text{GF} \ a)$ and for $p_{\text{max}}(s, \text{FG} \ a)$ but not for arbitrary LTL formulae
Summing up…

- **Deterministic $\omega$–automata (DBA or DRA) and DTMCs**
  - probability of language acceptance reduces to probabilistic reachability of set of accepting BSCCs in product DTMC

- **LTL model checking for DTMCs**
  - via construction of DRA for LTL formula
  - complexity: (doubly) exponential in the size of the LTL formula and polynomial in the size of the DTMC
  - measurability of any $\omega$–regular property on a DTMC

- **PCTL* model checking for DTMCs**
  - combination of PCTL and LTL model checking algorithms

- **LTL model checking for MDPs**
  - max. probabilities of reaching accepting end components
  - min. probabilities through negation and max. probabilities