Verification

Lecture 16

Bernd Finkbeiner

UNIVERSITÄT
DES
SAARLANDES

Plan for today

- LTL bounded model checking
- Expressiveness of LTL vs. CTL

REVIEW: Bounded model checking

Search for counterexamples of bounded length

There exists a counterexample of length k to the invariant AG p iff the following formula is satisfiable:

$$f_I(\vec{v}_0) \wedge f_{\rightarrow}(\vec{v}_0, \vec{v}_1) \wedge f_{\rightarrow}(\vec{v}_1, \vec{v}_2) \wedge \ldots f_{\rightarrow}(\vec{v}_{k-2}, \vec{v}_{k-1}) \wedge (\neg p_0 \vee \neg p_1 \vee \ldots \vee \neg p_{k-1})$$

Bounded LTL model checking

Automata-based approach:

- Translate LTL formula $\neg\varphi$ to Büchi automaton
- Build product with transition system
- Encode all paths that start in initial state and are k steps long
- Require that path contains loop with accepting state

$$f_I(\vec{v}_0) \;\wedge\; \bigwedge_{i=0}^{k-2} f_{\to}(\vec{v}_i, \vec{v}_{i+1}) \;\wedge\; \bigvee_{i=0}^{k-1} \Big((\vec{v}_i = \vec{v}_k) \wedge \bigvee_{j=i}^{k-1} f_F(\vec{v}_j) \Big)$$

Formula size: $O(k \cdot |TS| \cdot 2^{|\varphi|})$

Fixpoint-based translation

$$\psi_{TS} \wedge \psi_{loop} \wedge [\psi]_0$$

- $\psi_{TS} = f_I(\vec{v}_0) \ \wedge \ \bigwedge_{i=0}^{k-2} f_{\rightarrow}(\vec{v}_i, \vec{v}_{i+1})$
- ψ_{loop}: loop constraint, ensures the existence of exactly one loop
- $[\varphi]_0$: fixpoint formula, ensures that LTL formula holds

Formula size: $O(k \cdot (|TS| + |\varphi|))$

Loop constraint

- $\psi_{loop} = AtLeastOneLoop \wedge AtMostOneLoop$
- $AtLeastOneLoop = \bigwedge_{i=0}^{k-2} (l_i \Rightarrow (\vec{v}_i = \vec{v}_{k-1})) \ \wedge \bigvee_{i=0}^{k-2} l_i$
- $AtMostOneLoop = \bigwedge_{i=0}^{k-2} (SmallerExists_i \Rightarrow \neg l_i)$
- $\text{SmallerExists}_0 = \mathit{false}$
- $\text{SmallerExists}_{i+1} = \text{SmallerExists}_i \vee l_i$ for $0 \leq i < k-1$.

Fixpoint formula

Let φ be in PNF.

- $[p]_i = p_i$ for $i < k - 1$
  $[p]_i = \bigvee_{j=0}^{k-2}(l_j \wedge p_j)$ for $i = k - 1$
- $[\neg p]_i = \neg p_i$ for $i < k - 1$
  $[\neg p]_i = \bigvee_{j=0}^{k-2}(l_j \wedge \neg p_j)$ for $i = k - 1$
- $[\bigcirc \varphi']_i = [\varphi']_{i+1}$ for $i < k - 2$
  $[\bigcirc \varphi']_i = \bigvee_{j=0}^{k-2}(l_j \wedge [\varphi'])$ for $i = k - 2$
- $[\varphi_1 \text{ U } \varphi_2]_i = [\varphi_2]_i \vee ([\varphi_1]_i \wedge [\varphi_1 \text{ U } \varphi_2]_{i+1})$ for $i < k - 1$
  $[\varphi_1 \text{ U } \varphi_2]_i = \bigvee_{j=0}^{k-2}(l_j \wedge \langle \varphi_1 \text{ U } \varphi_2 \rangle_j)$ for $i = k - 1$
- $[\varphi_1 \text{ R } \varphi_2]_i = [\varphi_2]_i \wedge ([\varphi_1]_i \vee [\varphi_1 \text{ R } \varphi_2]_{i+1})$ for $i < k - 1$
  $[\varphi_1 \text{ R } \varphi_2]_i = \bigvee_{j=0}^{k-2}(l_j \wedge \langle \varphi_1 \text{ R } \varphi_2 \rangle_j)$ for $i = k - 1$
- $\langle \varphi_1 \text{ U } \varphi_2 \rangle_i = [\varphi_2]_i \vee ([\varphi_1]_i \wedge \langle \varphi_1 \text{ U } \varphi_2 \rangle_{i+1}$ for $i < k - 1$
  $\langle \varphi_1 \text{ U } \varphi_2 \rangle_i = \mathit{false}$ for $i = k - 1$
- $\langle \varphi_1 \text{ R } \varphi_2 \rangle_i = [\varphi_2]_i \wedge ([\varphi_1]_i \vee \langle \varphi_1 \text{ R } \varphi_2 \rangle_{i+1}$ for $i < k - 1$
  $\langle \varphi_1 \text{ R } \varphi_2 \rangle_i = \mathit{true}$ for $i = k - 1$

The Completeness Threshold

The bound k is increased incrementally until

- a counterexample is found, or
- the problem becomes intractable due to the complexity of the SAT problem
- k reaches a precomputed threshold that guarantees that there is no counterexample

→ this threshold is called the completeness threshold CL.

The completeness threshold

- Computing *CL* is as hard as model checking
- Idea: Compute an overapproximation of *CL* based on the graph structure

Basic notions:

- Diameter D: Longest shortest path between any two reachable states
- Recurrence diameter RD: Longest loop-free path between any two reachable states
- Initialized diameter D^I: Longest shortest path between some initial state and some reachable state
- Initialized recurrence diameter RD^I: Longest loop-free path between some initial state and some reachable state

Completeness thresholds

- For $\Box\, p$ properties, $CT \leq D^l$.
- For $\Diamond\, p$ properties, $CT \leq RD^l + 1$.
- For general LTL properties, $CT \leq \min(RD^l + 1, D^l + D)$
  (where D, D^l, RD, RD^l refer to the product graph)

Complexity

- k chosen as $\min(RD^l + 1, D^l + D)$ is exponential in number of state variables
- Size of SAT instance is $O(k \cdot (|TS| + |\varphi|))$
- SAT is solved in exponential time

$\Rightarrow$ double exponential in number of state variables
(Compare: BDD-based model checking is single-exponential)

- In practice, bounded model checking is very successful
- Finds shallow errors fast
- In practice, RD, D are often not exponential

Expressiveness of LTL vs. CTL

Equivalence of LTL and CTL formulas

CTL-formula Φ and LTL-formula φ (both over *AP*) are equivalent, denoted $\Phi \equiv \varphi$, if for any transition system *TS* (over *AP*):

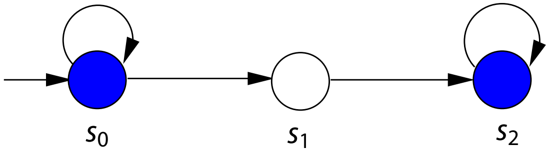
$$TS \models \Phi \quad \text{if and only if} \quad TS \models \varphi$$

Examples (1)

CTL-formula $\mathsf{A\,G\,A\,F}\,a$ and LTL-formula $\mathsf{G\,F}\,a$ are equivalent.

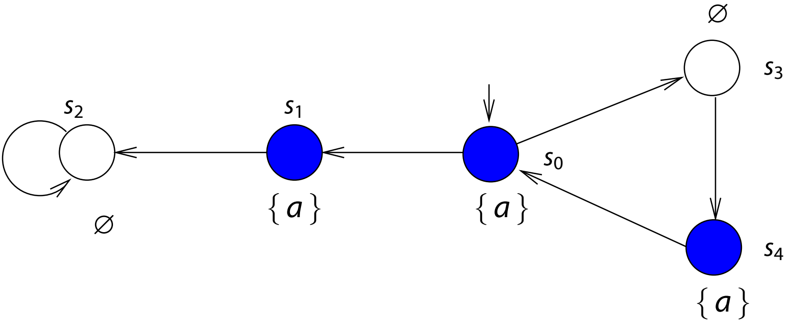
Examples (2)

AF AG a is not equivalent to F G a



Examples (3)

F $(a \wedge \mathrm{X}\, a)$ is not equivalent to AF $(a \wedge \mathrm{AX}\, a)$



LTL and CTL are incomparable

- Some LTL-formulas cannot be expressed in CTL, e.g.,
  - $\mathrm{F}\,\mathrm{G}\,a$
  - $\mathrm{F}\,(a \wedge \mathrm{X}\,a)$
- Some CTL-formulas cannot be expressed in LTL, e.g.,
  - $\mathrm{AF}\,\mathrm{AG}\,a$
  - $\mathrm{AF}\,(a \wedge \mathrm{AX}\,a)$
  - $\mathrm{AG}\,\mathrm{EF}\,a$

$\Rightarrow$ Cannot be expressed = there does not exist an equivalent formula

Example

$\boxed{\text{The CTL-formula AG EF } a \text{ cannot be expressed in LTL}}$

Comparing LTL and CTL

Let Φ be a CTL-formula, and φ the LTL-formula obtained by eliminating all path quantifiers in Φ. Then: [Clarke & Draghicescu]

$\Phi \equiv \varphi$ or there does not exist any LTL-formula that is equivalent to Φ

Comparing LTL and CTL

$\boxed{\text{The LTL-formula FG } a \text{ cannot be expressed in CTL}}$