Algorithms for Model Checking (2IW55)

Lecture 4

Symbolic Model Checking: Fairness and Counterexamples

Chapter 6.3, 6.4.

Tim Willemse
(timw@win.tue.nl)
http://www.win.tue.nl/~timw
HG 6.81

Outline

Symbolic Model Checking

Fair Symbolic Model Checking

Counterexamples and Witnesses

- Witnesses for E [U]
- Witnesses for fair E G

Exercise

Symbolic Model Checking

In summary, symbolic model checking:

- Recursively processes subformulae
- Represent the set of states satisfying a subformula by OBDDs
- Treats temporal operators by fixed point computations
- Relies on efficient implementation of equivalence test, and $\wedge, \vee, \neg$ and $\exists$ connectives on OBDDs.

Symbolic Model Checking

Fix a Kripke Structure $M = \langle S, R, L \rangle$.

The temporal operators of CTL are characterised by fixed points:

- $\mathsf{E}\,\mathsf{F}\, g = \mu Z.g \vee \mathsf{E}\,\mathsf{X}\, Z$
- $\mathsf{E}\,\mathsf{G}\, f = \nu Z.f \wedge \mathsf{E}\,\mathsf{X}\, Z$
- $\mathsf{E}\,[f\, \mathsf{U}\, g] = \mu Z.g \vee (f \wedge \mathsf{E}\,\mathsf{X}\, Z)$

- Least Fixed Points: start iteration at **false** ($\emptyset$)
- Greatest Fixed Points: start iteration at **true** (S)

Intuition:

- Eventually .... least fixed points
- Globally .... greatest fixed points

Symbolic Model Checking

CTL model checking with Fixed Points

Function $\textsc{check}(f)$ takes a formula f and returns the set of states where f holds: $\{s \mid s \models f\}$ (given a fixed Kripke Structure $M = \langle S, R, L \rangle$).

$\textsc{check}(p)$	$\{s \mid p \in L(s)\}$
$\textsc{check}(\neg f)$	$S \setminus \textsc{check}(f)$
$\textsc{check}(f \vee g)$	$\textsc{check}(f) \cup \textsc{check}(g)$
$\textsc{check}(\mathsf{E}\,\mathsf{X}\, f)$	$Pre_R(\textsc{check}(f))$
$\textsc{check}(\mathsf{E}\,[f\ \mathsf{U}\ g])$	$\textsc{lfp}\left(Z \mapsto \textsc{check}(g) \cup (\textsc{check}(f) \cap Pre_R(Z))\right)$
$\textsc{check}(\mathsf{E}\,\mathsf{G}\, f)$	$\textsc{gfp}\left(Z \mapsto \textsc{check}(f) \cap Pre_R(Z)\right)$

Recall: $Pre_R(Z) = \{s \in S \mid \exists t \in Z. s\ R\ t\}$

Outline

Symbolic Model Checking

Fair Symbolic Model Checking

Counterexamples and Witnesses
- Witnesses for E [U]
- Witnesses for fair E G

Exercise

Fair Symbolic Model Checking

Fix a fair Kripke Structure $M = \langle S, R, L, \{F_1, \ldots, F_n\} \rangle$

Recall that a fair path infinitely often hits some state from each fairness constraint F_i

- First, note that in fair CTL (with $\models_F$),

$$\mathsf{E}\,\mathsf{G}\,f \equiv f \wedge \bigwedge_{k=1}^{n} \mathsf{E}\,\mathsf{X}\,\mathsf{E}\,[f\,\mathsf{U}\,(F_k \wedge \mathsf{E}\,\mathsf{G}\,f)] \qquad \text{(prove } \subseteq \text{ and } \supseteq\text{)}$$

- Next, if

$$Z \equiv f \wedge \bigwedge_{k=1}^{n} \mathsf{E}\,\mathsf{X}\,\mathsf{E}\,[f\,\mathsf{U}\,(F_k \wedge Z)]$$

  Then $Z \subseteq \mathsf{E}\,\mathsf{G}\,f$ (construct a path cycling through $F_1, \ldots, F_n$)

- Hence, we found:

$$\mathsf{E}\,\mathsf{G}\,f \equiv \nu Z. f \wedge \bigwedge_{k=1}^{n} \mathsf{E}\,\mathsf{X}\,\mathsf{E}\,[f\,\mathsf{U}\,(F_k \wedge Z)]$$

Fair Symbolic Model Checking

The equivalence

$$\mathsf{E\,G}\, f \equiv \nu Z. f \wedge \bigwedge_{k=1}^{n} \mathsf{E\,X\,E}\,[f\ \mathsf{U}\ (F_k \wedge Z)]$$

leads to the following algorithm:

$\text{CHECK}_F(\mathsf{E\,G}\ f)$	$\text{GFP}\big(Z \mapsto \text{CHECK}(f \wedge \bigwedge_{k=1}^{n} \mathsf{E\,X}\,(\mathsf{E}\,[f\ \mathsf{U}\ (F_k \wedge Z)]))\big)$

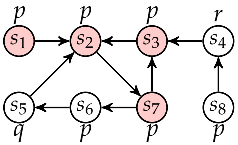
So, in the greatest fixed point computation for $\mathsf{E\,G}$, we perform nested least fixed point computations to compute $\mathsf{E}\,[\ \mathsf{U}\ ]$.

Next, we can compute an OBDD $fair := \text{CHECK}_F(\mathsf{E\,G}\ \mathsf{true})$. The remaining temporal operators can then be encoded as follows:

$\text{CHECK}_F(\mathsf{E\,X}\ f)$	$\text{CHECK}(\mathsf{E\,X}\ (f \wedge fair))$
$\text{CHECK}_F(\mathsf{E}\,[f\ \mathsf{U}\ g])$	$\text{CHECK}(\mathsf{E}\,[f\ \mathsf{U}\ (g \wedge fair)])$

Fair Symbolic Model Checking

Example



- To check: E G p
- Fairness constraint: $\neg r$
- Compute: $\nu Z.\text{CHECK}(p \wedge \mathsf{E\,X}\,(\mathsf{E}\,[p\ \mathsf{U}\ (\neg r \wedge Z)]))$
- Set $\phi(Z) = \text{LFP}(Y \mapsto (\text{CHECK}(\neg r) \cap Z) \cup (\text{CHECK}(p) \cap \text{PRE}_R(Y)))$

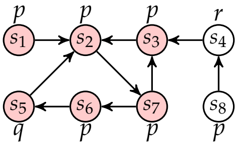
$$
\begin{aligned}
Z_0 &= S \\
Z_1 &= \text{CHECK}(p) \cap \text{PRE}_R(\phi(S)) = \{s_1, s_2, s_3, s_6, s_7\} \\
Z_2 &= \text{CHECK}(p) \cap \text{PRE}_R(\{s_1, s_2, s_3, s_6, s_7\}) \\
&= \{s_1, s_2, s_3, s_7\} \\
Z_3 &= \text{CHECK}(p) \cap \text{PRE}_R(\{s_1, s_2, s_3, s_7\}) \\
&= \{s_1, s_2, s_3, s_7\}
\end{aligned}
$$

$Z_2 = Z_3$, so this is the greatest fixed point.

Fair Symbolic Model Checking

Example

- To check: $\mathsf{E}\,[p\ \mathsf{U}\ q]$
- Fairness constraint: $\neg r$
- Compute $fair := \text{CHECK}_F(\mathsf{E\,G\,true})$ (= S)
- Compute: $\mu Z.(q \wedge fair) \vee (p \wedge \mathsf{E\,X}\ Z)$ (with LFP)



$$
\begin{aligned}
Z_0 &= \mathsf{false} = \emptyset \\
Z_1 &= q \vee (p \wedge \mathsf{E\,X}\ Z_0) = \{s_5\} \\
Z_2 &= q \vee (p \wedge \mathsf{E\,X}\ Z_1) = \{s_5, s_6\} \\
Z_3 &= q \vee (p \wedge \mathsf{E\,X}\ Z_2) = \{s_5, s_6, s_7\} \\
Z_4 &= q \vee (p \wedge \mathsf{E\,X}\ Z_3) = \{s_2, s_5, s_6, s_7\} \\
Z_5 &= q \vee (p \wedge \mathsf{E\,X}\ Z_4) = \{s_1, s_2, s_3, s_5, s_6, s_7\} \\
Z_6 &= q \vee (p \wedge \mathsf{E\,X}\ Z_5) = \{s_1, s_2, s_3, s_5, s_6, s_7\}
\end{aligned}
$$

$Z_5 = Z_6$, so this is the least fixed point.

Outline

Symbolic Model Checking

Fair Symbolic Model Checking

Counterexamples and Witnesses

- Witnesses for E [U]
- Witnesses for fair E G

Exercise

Counterexamples and Witnesses

- Motivation:
  - In practice, a model checker is often used as an extended debugger
  - If a bug is found, the model checker should provide a particular trace, which shows it
- A formula with a universal path quantifier has a counterexample consisting of one trace
- A formula with an existential path quantifier has a witness consisting of one trace
- Due to the dualities in CTL, we only have to consider:
  - a finite trace witnessing $\mathsf{E}\,[f\ \mathsf{U}\ g]$
  - an infinite trace witnessing $\mathsf{E}\,\mathsf{G}\,f$; for finite systems, the latter is a so-called lasso, consisting of a prefix and a loop
- For fair counter examples we require that the loop contains a state from each fairness constraint

Counterexamples and Witnesses – Witnesses for E [U]

- $\mathsf{E}\,[f\,\mathsf{U}\,g] = \mu Z.\, g \vee (f \wedge \mathsf{E}\,\mathsf{X}\, Z)$
- Unfolding the recursion, we get:

$$\begin{array}{rcl} Z_0 & = & \mathsf{false} \\ Z_1 & = & g \\ Z_2 & = & g \vee (f \wedge \mathsf{E}\,\mathsf{X}\, g) \\ Z_3 & = & g \vee (f \wedge \mathsf{E}\,\mathsf{X}\,(g \vee (f \wedge \mathsf{E}\,\mathsf{X}\, g))) \end{array}$$

- So, the fixed point computation corresponds to a backward reachability analysis
- Z_i contains those states that can reach g in at most $i-1$ steps (and f holds in between).
- Assume $s_0 \models \mathsf{E}\,[f\,\mathsf{U}\,g]$. To find a minimal witness from state s_0, we start in the smallest N such that $s_0 \in Z_N$.
- For $i \in 1, \ldots, N-1$, we define s_i to be a state in Z_{N-i} satisfying $s_{i-1}\; R\; s_i$.

Counterexamples and Witnesses – Witnesses for fair E G

- We want an initial path to a cycle on which each fairness constraint $\{F_1, \ldots, F_n\}$ occurs (i.e. the cycle must contain at least one state from all F_i).
- $\mathsf{E}\,\mathsf{G}\, f = \nu Z. f \wedge \bigwedge_{k=1}^{n} \mathsf{E}\,\mathsf{X}\ \mathsf{E}\,[f\ \mathsf{U}\ (F_k \wedge Z)]$
- Unfolding the recursion, we get:

$$\begin{aligned} Z_0 &= \mathsf{true} \\ &\ldots \\ Z_L &= f \wedge \bigwedge_{k=1}^{n} \mathsf{E}\,\mathsf{X}\ \mathsf{E}\,[f\ \mathsf{U}\ (F_k \wedge Z_{L-1})] \end{aligned}$$

- Let $Z := Z_L = Z_{L-1} = \mathsf{E}\,\mathsf{G}\, f$ be the fixed point
- To compute Z, we compute for each k $(1 \leq k \leq n)$, $\mathsf{E}\,[f\ \mathsf{U}\ (F_k \wedge Z)]$ using backward reachability. So, we have for each k the approximations: $Q_0^k \subseteq Q_1^k \subseteq Q_2^k \subseteq \ldots \subseteq Q_{j_k}^k$
- From the $\mathsf{E}\,[\ \mathsf{U}\ ]$ case, recall that Q_i^k contains those states that can reach $F_k \wedge Z$ in at most i steps

Counterexamples and Witnesses – Witnesses for fair E G

- Assume $s_0 \models_F \mathsf{E\,G}\, f$, hence, $s_0 \in Z$
- We will now inductively construct a path $s_0 \rightarrow^* s_1 \rightarrow^* \ldots \rightarrow^* s_n$, such that:
  - f holds along the whole path
  - $s_k \in Z \wedge F_k$ (for $1 \leq k \leq n$)
- Observe: by induction $s_{k-1} \models Z$, so, by definition of Z: $s_{k-1} \models \mathsf{E\,X\;E}\,[f\,\mathsf{U}\,(Z \wedge F_k)]$
- For $1 \leq k \leq n$ do:
  1. Determine the minimal M such that s_{k-1} has a successor $t_0^k \in Q_M^k$.
  2. Construct (as the witness for $\mathsf{E}\,[\;\mathsf{U}\;]$):

     $$s_{k-1} \rightarrow t_0^k \rightarrow \cdots \rightarrow t_M^k \in Z \wedge F_k$$

  3. Define $s_k := t_M^k$.
- heuristic improvement: Visit the F_k in a different order: continue with the closest F_k that has not yet been visited.

Counterexamples and Witnesses – Witnesses for fair E G

- Finally, we must close the loop, but this is not always possible: Check if $s_n \models \mathsf{EX}\ \mathsf{E}\,[f\ \mathsf{U}\ \{s_1\}]$.
- If so: the $\mathsf{E}\,[\ \mathsf{U}\ ]$-witness closes the loop
- If not: the cycle cannot be closed. Hence:
  - The sequence so far $s_0 \to \cdots \to s_n$ is in the prefix of the lasso, not yet on the loop.
  - Restart the whole procedure of the previous slide, now starting in $s_n \in Z$.
- Eventually, this process must terminate:
  - We only restart if s_n cannot reach s_1
  - so we moved to the next Strongly Connected Component
  - The SCC graph cannot contain cycles
- Optimisation: By precomputing $\mathsf{E}\,[f\ \mathsf{U}\ \{s_1\}]$, one can detect earlier that closing the cycle will not be possible.

Outline

Symbolic Model Checking

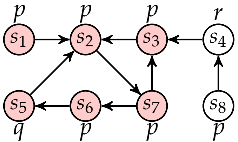
Fair Symbolic Model Checking

Counterexamples and Witnesses
- Witnesses for E [U]
- Witnesses for fair E G

Exercise

Exercise

Example



- Check that $s_1 \models_F \mathsf{E\,G}\,(p \vee q)$
- Fairness constraint: $\neg r$ and q
- Construct a witness for $s_1 \models_F \mathsf{E\,G}\,(p \vee q)$