Witnesses and Counterexamples for CTL
CS 720
Fall 2016

Peter A Fejer

December 7, 2016

Table of contents

Definitions

- A witness for a CTL path formula φ in a transition system T is an indication of a path π in T such that $\pi \models \varphi$.
- A counterexample for a CTL path formula φ in a transition system T is an indication of a path π in T such that $\pi \not\models \varphi$.

$\bigcirc\Phi$

- A witness for $\bigcirc\Phi$ in T is a pair (s, s') with $s \in I$, $s' \in Post(s)$ and $s' \models \Phi$.
- A counterexample for $\bigcirc\Phi$ in T is a pair (s, s') with $s \in I$, $s' \in Post(s)$ and $s' \not\models \Phi$.
- Both witnesses and counterexamples are found by analyzing $Post(I)$ after model checking Φ.

$\Phi U \Psi$ Witnesses

- A witness for $\Phi U \Psi$ is an initial path fragment $s_0, s_1, \ldots, s_n$ with $s_n \models \Psi$ and $s_i \models \Phi$ for $0 \leq i < n$.
- The witness is found by a backwards search starting at $Sat(\Phi)$.

$\Phi U \Psi$ Counterexamples

- A counterexample to $\Phi U \Psi$ is an initial path fragment indicating a path π with either
  1. $\pi \models \Box(\Phi \wedge \neg\Psi)$, or
  2. $\pi \models (\Phi \wedge \neg\Psi) U (\neg\Phi \wedge \neg\Psi)$
- A counterexample showing (1) is an initial path fragment $s_0 s_1 \ldots s_{n-1} s_n s'_1 \ldots s'_r$ with $s_n = s'_r$ and each s_i and s'_j satisfies $\Phi \wedge \neg\Psi$.
- A counterexample demonstrating (2) is an initial path fragment $s_0 s_1 \ldots s_{n-1} s_n$ where $s_n \models \neg\Phi \wedge \neg\Psi$ and $s_i \models \Phi \wedge \neg\Psi$ for $0 \leq i < n$.

$\Phi U \Psi$ Finding Counterexamples

Counterexamples are found by analyzing $G = (S, E)$ where

$$E = \{(s, s') | s' \in Post(s) \text{ and } s \models \Phi \wedge \neg\Psi\}.$$

A path starting from $s_0 \in I$ and leading to a nontrivial SCC of G yields a counterexample of the first kind, while a path in G from an initial state s_0 to a trivial SCC $C = \{s'\}$ with $s' \models \neg\Phi \wedge \neg\Psi$ yields a counterexample of the second kind.

$\Box\Phi$

1. A counterexample to $\Box\Phi$ is an initial path fragment $s_0 s_1 \ldots s_n$ with $s_i \models \Phi$ for $0 \leq i < n$ and $s_n \not\models \Phi$.
2. Found by backwards search from states where Φ is false.
3. Witness to $\Box\Phi$ is initial path fragment of the form $s_0 s_1 \ldots s_n s'_1 \ldots s'_r$ with $s_n = s'_r$ where $s_i \models \Phi$ for $0 \leq i \leq n$ and $s'_i \models \Phi$ for $1 \leq i \leq r$.
4. Found by a cycle search in $G = (S, E)$ where $E = \{(s, s') | s' \in Post(s) \text{ and } s \models \Phi\}$.

$\bigcirc a$

1. A fair witness for $\bigcirc a$ is a witness for $\bigcirc(a \wedge a_{fair})$.
2. A fair counterexample for $\bigcirc a$ is a counterexample to $\bigcirc(a_{fair} \rightarrow a)$.

aUa'

1. A fair witness to aUa' is a witness to $aU(a' \wedge a_{fair})$.
2. A fair counterexample for aUa' is either a witness to $(a \wedge \neg a')U(\neg a \wedge \neg a' \wedge a_{fair})$ or a fair witness to $\Box(a \wedge \neg a')$.

$\Box a$

1. A fair counterexample to $\Box a$ is an initial path fragment $s_0 s_1 \ldots s_n$ with $s_n \models \neg a \wedge a_{fair}$ and $s_i \models a$ for $0 \leq i < n$.
2. Let $sfair = \bigwedge_{1 \leq i \leq k} (\Box \Diamond a_i \rightarrow \Box \Diamond b_i)$
3. A fair witness to $\Box a$ is an initial path fragment $s_0 s_1 \ldots s_n s'_1 \ldots s'_r$ with $s_n = s'_r$ such that
   - $s_i \models a$ for $0 \leq i \leq n$.
   - $s'_i \models a$ for $1 \leq i \leq r$.
   - For all i, $1 \leq i \leq k$, either $Sat(a_i) \cap \{s'_1, \ldots, s'_r\} = \emptyset$ or $Sat(b_i) \cap \{s'_1, \ldots, s'_r\} \neq \emptyset$.
4. Found by analyzing SCCs of $G[a]$.