15-414 Bug Catching: Model Checking

Soonho Kong
soonhok@cs.cmu.edu

10 Oct 2011
Model Checking
Model Checking

What is “Model”? 
Kripke Structure is a triple $\langle S, R, L \rangle$, where

- $S$ is the set of states
- $R \subseteq S \times S$ is the transition relation (left-total), and
- $L : S \rightarrow \mathcal{P}(AP)$ gives the set of atomic propositions $\text{true}$ in each state
Model Checking

What to Check?
Model Checking Problem

Find all states $s$ such that $M$ has property $f$ at state $s$.

$M, s \models f$

Kripke Structure  
state  
Property  
(Temporal Logic Formula)
Model Checking Problem

Find all states $s$ such that $M$ has property $f$ at state $s$.

$M, s \models f$

Kripke Structure

state

Property
(Temporal Logic Formula)

EX $q$
Model Checking Problem

Find all states $s$ such that $M$ has property $f$ at state $s$.

\[ M, s \models f \]

Kripke Structure  

\[ s_0 \rightarrow p \rightarrow p, q \rightarrow s_1 \]

\[ s_2 \rightarrow q \rightarrow s_3 \]

\[ s_0 \rightarrow p \]

\[ \text{Property (Temporal Logic Formula)} \]

\[ \text{EX } q \]
Model Checking Problem

Find all states $s$ such that $M$ has property $f$ at state $s$.

$M, s \models f$

Kripke Structure  state  Property
(Temporal Logic Formula)

EX $q$
Model Checking Problem

Find all states $s$ such that $M$ has property $f$ at state $s$.

$M, s \models f$

Kripke Structure

state

Property (Temporal Logic Formula)

EX $q$
Model Checking Problem

Find all states $s$ such that $M$ has property $f$ at state $s$.

$M, s \models f$

Kripke Structure

state

Property

(Temporal Logic Formula)

EX $q$
Model Checking

What’s Temporal Logic (esp, CTL*)?
The Logic CTL*

The computation tree logic CTL* combines both branching-time and linear-time operators.

In this logic a *path quantifier* can prefix an assertion composed of arbitrary combinations of the usual linear-time operators.

1. Path quantifier:
   
   \( A \) - “for every path”

   \( E \) - “there exists a path”

2. Linear-time operators:
   
   \( X \ p \) - \( p \) holds next time

   \( F \ p \) - \( p \) holds sometime in the future

   \( G \ p \) - \( p \) holds globally in the future

   \( p \ U \ q \) - \( p \) holds until \( q \) holds
Semantics of State Formulas

For a state formula $f$, the notation

$$M, s \models f$$

means that $f$ holds at state $s$ in the Kripke structure $M$. It’s inductively defined as follows:

$$M, s \models p \iff p \in L(s)$$

$$M, s \models \neg f \iff M, s \not\models f$$

$$M, s \models f_1 \lor f_2 \iff M, s \models f_1 \text{ or } M, s \models f_2$$
Semantics of State Formulas

For a state formula $f$, the notation

$$M, s \models f$$

means that $f$ holds at state $s$ in the Kripke structure $M$. It’s inductively defined as follows:

$$s \models E(g) \iff \text{there exists a path } \pi \text{ starting with } s \text{ such that } \pi \models g.$$
Semantics of State Formulas

For a state formula $f$, the notation $\mathcal{M}, s \models f$ means that $f$ holds at state $s$ in the Kripke structure $\mathcal{M}$. It’s inductively defined as follows:

$$s \models A(g) \iff \text{For all path } \pi \text{ starting with } s, \text{ we have } \pi \models g.$$
Semantics of Path Formulas

For a path formula $f$, the notation

$$M, \pi \models f$$

means that $f$ holds along path $\pi$ in the Kripke structure $M$. It's inductively defined as follows:

$$M, \pi \models f \iff s \text{ is the first state of } \pi \text{ and } s \models f.$$
Semantics of Path Formulas

For a path formula $f$, the notation

$$ M, \pi \models f $$

means that $f$ holds along path $\pi$ in the Kripke structure $M$. It's inductively defined as follows:

$$ M, \pi \models Xf \iff M, \pi^1 \models f $$
Semantics of Path Formulas

For a path formula \( f \), the notation

\[
M, \pi \models f
\]

means that \( f \) holds along path \( \pi \) in the Kripke structure \( M \). It's inductively defined as follows:

\[
M, \pi \models \mathbf{X}f \iff M, \pi^1 \models f
\]

\[\pi^0 \rightarrow \text{green circles} \rightarrow \text{circles} \rightarrow \ldots\]

\[
M, \pi^1 \models f
\]
Semantics of Path Formulas

For a path formula $f$, the notation

$$ M, \pi \models f $$

means that $f$ holds along path $\pi$ in the Kripke structure $M$. It’s inductively defined as follows:

$$ M, \pi \models Gf \iff \text{for all } i \geq 0, \pi^i \models f $$
Semantics of Path Formulas

For a path formula $f$, the notation

$$ M, \pi \models f $$

means that $f$ holds along path $\pi$ in the Kripke structure $M$. It’s inductively defined as follows:

$$ M, \pi \models G f \iff \text{for all } i \geq 0, \pi^i \models f $$

$$ \pi^0 \rightarrow \pi^1 \rightarrow \pi^2 \rightarrow \pi^3 \rightarrow \ldots $$
Semantics of Path Formulas

For a path formula $f$, the notation

$$M, \pi \models f$$

means that $f$ holds along path $\pi$ in the Kripke structure $M$. It's inductively defined as follows:

$$M, \pi \models Ff \iff \text{there exists } i \geq 0, \pi^i \models f$$
Semantics of Path Formulas

For a path formula \( f \), the notation

\[
M, \pi \models f
\]

means that \( f \) holds along path \( \pi \) in the Kripke structure \( M \). It’s inductively defined as follows:

\[
M, \pi \models F f \iff \text{there exists } i \geq 0, \pi^i \models f
\]
Semantics of Path Formulas

For a path formula $f$, the notation

$$M, \pi \models f$$

means that $f$ holds along path $\pi$ in the Kripke structure $M$. It’s inductively defined as follows:

$$M, \pi \models f_1 U f_2 \iff \text{there exists } k \geq 0 \text{ such that } M, \pi^k \models f_2$$

and for all $0 \leq j < k$, $M, \pi^j \models f_1$
Semantics of Path Formulas

For a path formula $f$, the notation

$$M, \pi \models f$$

means that $f$ holds along path $\pi$ in the Kripke structure $M$. It’s inductively defined as follows:

$$M, \pi \models f_1 U f_2 \iff \text{there exists } k \geq 0 \text{ such that } M, \pi^k \models f_2$$

and for all $0 \leq j < k$, $M, \pi^j \models f_1$
Model Checking Problem

Find all states $s$ such that $M$ has property $f$ at state $s$.

$M, s \models f$

Kripke Structure  state  Property (Temporal Logic Formula)

How to Solve it?
Model Checking Problem

Find all states \( s \) such that \( M \) has property \( f \) at state \( s \).

\[
M, s \models f
\]

Kripke Structure \quad \text{state} \quad \text{Property (Temporal Logic Formula)}

Fixed-Point Computation, using the following Identity!

\[
\begin{align*}
AF \ f_1 &= \text{lfp} \ Z(f_1 \lor AX \ Z) \\
EF \ f_1 &= \text{lfp} \ Z(f_1 \lor EX \ Z) \\
AG \ f_1 &= \text{gfp} \ Z(f_1 \land AX \ Z) \\
EG \ f_1 &= \text{gfp} \ Z(f_1 \land EX \ Z) \\
A[f_1 \mathbin{U} f_2] &= \text{lfp} \ Z(f_2 \lor (f_1 \land AX \ Z)) \\
E[f_1 \mathbin{U} f_2] &= \text{lfp} \ Z(f_2 \lor (f_1 \land EX \ Z))
\end{align*}
\]
This example is from the textbook (page 65)

\[ E[pUq] = \text{lfp}\ Z.q \lor (p \land \text{EX} \ Z) \]