Lecture 35
Bounded Model Checking
Instructor: Hossein Hojjat

November 29, 2017
Observation

- LTL model checking requires checking all paths
- On the other hand: a counterexample to LTL formula \( \phi \) corresponds to the question if there exists a witness for \( \neg \phi \)
- A counterexample for \( G \phi \) is a finite prefix of a path in which \( F\neg \phi \) holds
  
  ![Diagram for G phi]

- A counterexample for \( F \phi \) is a finite prefix of a path that is a lasso in which \( G\neg \phi \) holds
  
  ![Diagram for F phi]

- Finite paths may say something about infinite behaviors
Bounded Model Checking (BMC) performs only on the basis of finite bounded prefixes of paths of the system.

Unroll the transition relation up to certain fixed bound \( k \) and search for violations of the property within that bound.

Transform this search to a Boolean satisfiability problem and solve it using a SAT solver.

Mostly incomplete in practice:

- validity of a formula can often not be proven.
Motivating Example: Two-bit Counter

Does the safety property $G\neg(x \land y)$ hold in the initial state?

Boolean Variables: $x$, $y$

- Represent initial states and the transition relation as Boolean formulas
Motivating Example: Two-bit Counter

Does the safety property $G\neg(x \land y)$ hold in the initial state?

Boolean Variables: $x, y$

Initial State: $I(x, y) = \neg x \land \neg y$

- Represent initial states and the transition relation as Boolean formulas
Motivating Example: Two-bit Counter

Does the safety property $G\neg(x \land y)$ hold in the initial state?

- Represent initial states and the transition relation as Boolean formulas

**Initial States:**

- **00**
- **11**
- **01**
- **10**

**Transition Relation:**

$$R(x, y, x', y') = \left( x' = (x \neq y) \land y' = \neg y \right)$$

**Boolean Variables:** $x$, $y$

**Initial State:** $I(x, y) = \neg x \land \neg y$
Motivating Example: Two-bit Counter

Does the safety property $G \neg (x \land y)$ hold in the initial state?

Boolean Variables: $x$, $y$

Initial State: $I(x, y) = \neg x \land \neg y$

Transition Relation:

\[
R(x, y, x', y') = \left( x' = (x \neq y) \land y' = \neg y \right)
\]

- Represent initial states and the transition relation as Boolean formulas
- Unroll the transition relation up to a bound $k$ starting from the initial states

\[
\neg x_0 \land \neg y_0 \land \left( x_1 = (x_0 \neq y_0) \land y_1 = \neg y_0 \right) \land \left( x_2 = (x_1 \neq y_1) \land y_2 = \neg y_1 \right) \land \left( x_3 = (x_2 \neq y_2) \land y_3 = \neg y_2 \right)
\]

UNSAT for $k = 0$
Motivating Example: Two-bit Counter

Does the safety property $G\neg(x \land y)$ hold in the initial state?

Boolean Variables: $x$, $y$

Initial State: $I(x, y) = \neg x \land \neg y$

Transition Relation:

$$R(x, y, x', y') = \left( x' = (x \neq y) \land y' = \neg y \right)$$

- Represent initial states and the transition relation as Boolean formulas
- Unroll the transition relation up to a bound $k$ starting from the initial states

$$\neg x_0 \land \neg y_0 \land \left( x_1 = (x_0 \neq y_0) \land y_1 = \neg y_0 \right) \land \left( x_2 = (x_1 \neq y_1) \land y_2 = \neg y_1 \right) \land \left( x_3 = (x_2 \neq y_2) \land y_3 = \neg y_2 \right) \land \left( x_0 \land y_0 \right) \lor \left( x_1 \land y_1 \right) \lor \left( x_2 \land y_2 \right)$$

UNSAT for $k = 1$
Motivating Example: Two-bit Counter

Does the safety property $G\neg(x \land y)$ hold in the initial state?

Boolean Variables: $x$, $y$
Initial State: $I(x, y) = \neg x \land \neg y$
Transition Relation:
$R(x, y, x', y') = \left( x' = (x \neq y) \land y' = \neg y \right)$

- Represent initial states and the transition relation as Boolean formulas
- Unroll the transition relation up to a bound $k$ starting from the initial states

$(\neg x_0 \land \neg y_0) \land \left( \begin{array}{l} x_1 = (x_0 \neq y_0) \land y_1 = \neg y_0 \\ \land \\ x_2 = (x_1 \neq y_1) \land y_2 = \neg y_1 \\ \land \\ x_3 = (x_2 \neq y_2) \land y_3 = \neg y_2 \end{array} \right) \land \left( \begin{array}{c} (x_0 \land y_0) \\ \lor \\ (x_1 \land y_1) \\ \lor \\ (x_2 \land y_2) \end{array} \right)$

UNSAT for $k = 2$
Motivating Example: Two-bit Counter

Does the safety property $G\neg(x \land y)$ hold in the initial state?

- Boolean Variables: $x$, $y$
- Initial State: $I(x, y) = \neg x \land \neg y$
- Transition Relation:
  $R(x, y, x', y') = \left(x' = (x \neq y) \land y' = \neg y\right)$

- Represent initial states and the transition relation as Boolean formulas
- Unroll the transition relation up to a bound $k$ starting from the initial states

$$\begin{align*}
(x_0 \land y_0) & \\
(x_1 \neq y_1) & \land y_1 = \neg y_0 \\
(x_2 \neq y_2) & \land y_2 = \neg y_1 \\
(x_3 \neq y_3) & \land y_3 = \neg y_2 \\
(x_0 \land y_0) & \\
(x_1 \land y_1) & \\
(x_2 \land y_2) & \\
(x_3 \land y_3) & \\
\end{align*}$$

SAT for $k = 3$
Motivating Example: Two-bit Counter

Does the safety property $F(x \land y)$ hold in the initial state?

Boolean Variables: $x, y$

Initial State: $I(x, y) = \neg x \land \neg y$

$R(x, y, x', y') = \left( x' = (x \neq y) \land y' = \neg y \right) \lor \left( x' = x \land y' = y \land x \land \neg y \right)$
Motivating Example: Two-bit Counter

Does the safety property $F(x \land y)$ hold in the initial state?

Boolean Variables: $x$, $y$

Initial State: $I(x, y) = \neg x \land \neg y$

$R(x, y, x', y') = (x' = (x \neq y) \land y' = \neg y) \lor (x' = x \land y' = y \land x \land \neg y)$

$I(x_0, y_0) \land R(x_0, y_0, x_1, y_1) \land R(x_1, y_1, x_2, y_2) \land \bigvee_{i=0}^{2} \neg (x_i \land y_i) \land \text{loop}$

where

$\text{loop} = R(x_2, y_2, x_3, y_3) \land$

$(x_3 = x_0 \land y_3 = y_0) \lor (x_3 = x_1 \land y_3 = y_1) \lor (x_3 = x_2 \land y_3 = y_2)$

SAT: satisfying assignment gives counterexample to the liveness property
• Given: transition system $M$, temporal logic formula $\phi$ and user-supplied bound $k$
• Construct propositional formula that is satisfiable iff $\phi$ is valid along a path of length $k$
• Initialized Paths of length $k$:

$$\left[M\right]_k = I(s_0) \land \bigwedge_{i=0}^{k-1} R(s_i, s_{i+1})$$

• $G \phi$ means $\phi$ must hold in every state along any path of length $k$

$$\left[M\right]_k \land \bigvee_{i=0}^{k} \neg \phi_i$$

• If satisfiable, satisfying assignment gives:
  • Witness for $F \neg \phi$
  • Counterexample to the safety property $G\phi$
How big should $k$ be?

- For every model $M$ and LTL property $\phi$ there exists $k$ s.t.
  \[ M \models_k \phi \rightarrow M \models \phi \]
- The minimal such $k$ is the Completeness Threshold (CT)
How big should $k$ be?

- Diameter $d$ = longest shortest path from an initial state to any other reachable state
- Recurrence Diameter $rd$ = longest loop-free path
- $rd \geq d$

$d = 2$

$rd = 3$
How big should $k$ be?

- Theorem: for $G\phi$ properties $CT = d$

![Diagram with $s_0$ arbitrary path and $\neg \phi$]
How big should $k$ be?

- Theorem: for $F\phi$ properties $CT = rd$

![Diagram of a model with states and transitions]

Open Problem: The value of $CT$ for general Linear Temporal Logic properties is unknown

See e.g.
“Linear Completeness Thresholds for Bounded Model Checking” (CAV’11)