Introduction to Software Verification

Orna Grumberg

Lectures Material
winter 2015-16
Explicit Model Checking for CTL
Kripke Structure $M=(S,R,L,S_0)$

Labeled by atomic propositions $AP$
(critical section, variable value...)
CTL Model Checking $M \models f$

- Define label(s) which will collect the set of subformulas of $f$ which are true in $s$

- For each $s$, the model checking algorithm gradually add formulas to label(s):

- The Model Checking algorithm works iteratively on subformulas of $f$, from simpler subformulas to more complex ones
Model Checking \( M |\models f \) (cont.)

- The algorithm checks subformula \( g \) of \( f \) only after all subformulas of \( g \) have already been checked

- For subformula \( g \), the algorithm adds \( g \) to label(s) for every state that satisfies \( g \)
Model Checking $M \models f$ (cont.)

- At the end of checking $g$, the following holds: For every $s \in S$
  - $g \in \text{label}(s) \iff M,s \models g$
Model Checking Atomic Propositions

- For atomic proposition $p \in AP$:
  
  \[ p \in \text{label}(s) \iff p \in L(s) \]

  Held by alg  Defined by M

How do we handle more complex formulas?

Observation:

- Sufficient to handle $\neg$, $\lor$, EX, EU, EG
Model Checking $g = EG f_1$

• A Strongly Connected Component (SCC) in a graph is a subgraph $C$ s.t. every node in $C$ is reachable from any other node in $C$ via nodes in $C$

• An SCC $C$ is maximal (MSCC) if it is not contained in any other SCC in the graph
• $C$ is nontrivial if it contains at least one edge. Otherwise, it is trivial

Tarjan has a linear algorithm in $O(|S| + |R|)$ for finding all MSCCs in a graph, including the trivial SCCs.
**Model Checking** $g = EG f_1$

Why using maximal SCCs?

*Complexity concerns:*

There are up to $2^{|S|}$ non-maximal SCCs in $M$.

Number of **maximal SCCs** is at most $|S|$

- Disjoint
- Overall number of states is $|S|$
Model Checking $g = \text{EG} \; f_1$

Reduced structure for $M$ and $f_1$:
Remove from $M$ all states s.t. $f_1 \notin \text{label}(s)$

Resulting model: $M' = (S', R', L')$
\begin{itemize}
  \item $S' = \{ s \mid M, s \models f_1 \}$
  \item $R' = (S' \times S') \cap R$
  \item $L'(s') = L(s')$ for every $s' \in S'$
\end{itemize}

Theorem: $M, s \models \text{EG} \; f_1$ iff
1. $s \in S'$ and
2. There is a path in $M'$ from $s$ to some state in a nontrivial strongly connected component of $M'$
**Model Checking $g = EG f_1$**

procedure `CheckEG (f_1)`

\[ S' := \{ s \mid f_1 \in \text{label}(s) \} \]

\[ \text{MSCC} := \{ C \mid C \text{ is a nontrivial MSCC of } M' \} \]

\[ T := \bigcup_{C \in \text{MSCC}} \{ s \mid s \in C \} \]

For all \( s \in T \) do \( \text{label}(s) := \text{label}(s) \cup \{ EG f_1 \} \)

while \( T \neq \emptyset \) do

\[ \text{choose } s \in T; \quad T := T \setminus \{ s \}; \]

for all \( t \in S' \) s.t. \( R(t, s) \) do

\[ \text{if } EG f_1 \notin \text{label}(t) \text{ then} \]

\[ \text{label}(t) := \text{label}(t) \cup \{ EG f_1 \}; \]

\[ T := T \cup \{ t \} \]

end for all

end while
• Computing MSCCs: using Tarjan’s algorithm.
• Complexity: $O(|S'| + |R'|) = O(|M'|)$
Complexity for EG $f_1$

- Computing $M'$: $O(|S| + |R|)$
- Computing MSCCs using Tarjan’s algorithm: $O(|S'| + |R'|)$
- Labeling all states in MSCCs: $O(|S'|)$
- Backward traversal: $O(|S'| + |R'|)$

Overall: $O(|S| + |R|) = O(M)$
Theorem: $M,s \models EG f_1$ iff

1. $s \in S'$ and
2. There is a path in $M'$ from $s$ to some state in a nontrivial, maximal strongly connected component of $M'$

Proof:
Model Checking Complexity

- Each subformula requires $O(|M|)$
- Number of subformulas: $O(|f|)$
- Total: $O(|M| \times |f|)$
Microwave Example
Property

- $AG (\text{start} \rightarrow \text{AF Heat})$
- $EF (\neg \text{Heat})$
- $E (\text{true} U (\text{start} \land \text{EG} \neg \text{Heat}))$

Instead of writing the formulas in label(s) for each s,
Use $S(f)$ to denote set of states s.t. $f \in \text{label(s)}$
\[ \neg E \ (\text{true} \ U \ (\text{start} \land \ EG \ \neg \text{Heat})) \]

\[ S(\text{Start}) : \{2,5,6,7\} \]
\[ S(\neg \text{Heat}) : \{1,2,3,5,6\} \]
\[ S(EG \neg \text{Heat}) : \{1,2,3,5\} \]
\(!E (\text{true } U (\text{start } \land \text{EG } \neg \text{Heat})) \)

\[ S(\text{Start}): \{2,5,6,7\} \]
\[ S(\neg \text{Heat}): \{1,2,3,5,6\} \]
\[ S(\text{EG } \neg \text{Heat}): \{1,2,3,5\} \]

\[ S(\text{Start } \land \text{EG } \neg \text{Heat}): \{2,5\} \]
\[ S(\text{EU}): \{1,2,3,4,5,6,7\} \]
\[ S(\text{f}): \emptyset \]
Explicit Model Checking for Fair CTL
Motivation
Fair CTL ($\text{CTL}^F$)

- Same syntax as CTL
- Different semantics

$\text{CTL}^F$ formulas are interpreted over fair Kripke structures
Fair Kripke Structures

Fair Kripke structure $M = (S, S_0, R, L, F)$

- $S, S_0, R, L$ - as before
- $F \subseteq 2^S$ is a set of fairness constraints

- $F = \{ P_1, \ldots, P_k \}$ where
  - $P_i \subseteq S$
  - $P_i$ is a CTL formula
Fairness

Fair paths:

• $\pi = s_0, s_1, s_2, \ldots$
• $\text{inf}(\pi) = \{ s \mid s = s_i \text{ for infinitely many } i \}$

$\pi$ is fair if for every $P \in F$, $\text{inf}(\pi) \cap P \neq \emptyset$
Semantics of Fair CTL

• $M,s \models_F \text{EX } \psi \iff$ there exists a fair path
  $\pi = s_0,s_1,...$ from $s$ such that $M, s_1 \models_F \psi$

• $M,s \models_F \text{AX } \psi \iff$ for every fair path
  $\pi = s_0,s_1,...$ from $s$, $M, s_1 \models_F \psi$

• Similarly for $\text{EG}$, $\text{AG}$, $\text{EU}$, $\text{AU}$,...
Model checking Fair CTL

• Needs to consider only fair paths

• \( g \in \text{label}(s) \iff M,s \models_F g \)
Reminder: Model Checking $g = EG f_1$
without fairness

Observation:
• $s |= EG f_1$
  iff
• $s$ is the start of a path where all states satisfy $f_1$
  iff
• $s$ has a finite path to a Strongly Connected Component (SCC), where all states satisfy $f_1$
Model Checking $g = \text{EG} f_1$

with fairness

Observation:

• $s \equiv F \text{EG} f_1$
  iff

• $s$ is the start of a fair path where all states satisfy $f_1$
  iff

• $s$ has a finite path to a Fair Strongly Connected Component (FSCC), where all states satisfy $f_1$
\( M, s \models_E G f_1 \)

**Strongly connected component \( C \) is fair iff**
for every \( P \in F, C \cap P \neq \emptyset \)

**Reduced structure:**
Remove from \( M \) all states s.t. \( f_1 \not\in \text{label}(s) \).

**Resulting model:** \( M' = (S', R', L', F') \)
- \( S' = \{ s \mid M, s \models_f f_1 \} \)
- \( R', L' \) defined as before
- \( F' = \{ P_i \cap S' \mid P_i \in F \} \)
Theorem: \( M,s \models_{F} EG f_1 \) iff

1. \( s \in S' \) and
2. There is a path in \( M' \) from \( s \) to some state \( t \) in a nontrivial maximal fair strongly connected component of \( M' \)

Proof: similar to theorem for EG without fairness
\( M, s \models_{F} EG f_1 \)

**procedure** `CheckFairEG (f_1)`

\[ S' := \{ s \mid f_1 \in label(s) \} \]

\[ SCC := \{ C \mid C \text{ is a nontrivial fair SCC of } M' \} \]

\[ T := \bigcup_{C \in SCC} \{ s \mid s \in C \} \]

**For all** \( s \in T \) **do** \( label(s) := label(s) \cup \{ EG f_1 \} \)

**while** \( T \neq \emptyset \) **do**

\[ \text{choose } s \in T ; \ T := T \setminus \{s\} ; \]

**for all** \( t \in S' \) **s.t.** \( R(t,s) \) **do**

\[ \text{if } EG f_1 \notin label(t) \text{ then} \]

\[ label(t) := label(t) \cup \{ EG f_1 \}; \]

\[ T := T \cup \{t\} \]

**end for all**

**end while**

*Complexity increases to* \( O((|S| + |R|) \cdot |F|) \)
Model Checking other Fair CTL Formulas

- Add atomic proposition \texttt{fair} to all states that satisfy $M,s \models F \text{EG true}$

- $M,s \models F \text{EX } f_1$ iff $M,s \models \text{EX } (f_1 \land \text{fair})$

- $M,s \models F \text{E } [f_1 \cup f_2]$ iff $M,s \models E \ [f_1 \cup (f_2 \land \text{fair})]$

Overall complexity: $O(|f| \cdot (|S| + |R|) \cdot |F|)$
$M, s \models \mathit{FGa}$ with $F = \{ \{1,2\}, \{1,5\} \}$

$F' = \{ \{1\} \}$

$\mathit{MSCC} = \{ \{1\}, \{3,4\}, \{6\} \}$

$\mathit{FMSCC} = \emptyset$

Set of states satisfying $E_F \mathit{Ga}$ is empty
Model Checking other Fair CTL Formulas

• Add a new atomic proposition *fair* to all states which are a start of a fair path
• $\text{fair} \in \text{label(s)} \iff M, s \models F \text{EG } \text{true}$

$M, s \models F \text{EX } f_1$ iff $M, s \models \text{EX } (f_1 \land \text{fair})$

$M, s \models F \text{E } [f_1 \text{ U } f_2]$ iff $M, s \models E [f_1 \text{ U } (f_2 \land \text{fair})]$

*Overall complexity: $O(|f| \cdot (|S| + |R|) \cdot |F|)$*
Computing $S_{\text{fair}}$ with $F=\{\{1,2\}, \{1,5\}\}$

MSCC = \{\{0\}, \{1\}, \{2,3,4,5\}, \{6\}\}

FMSCC = \{\{2,3,4,5\}\}

$S_{\text{fair}} = \{2,3,4,5\} \cup \{0,1\}$
$M, s \models F \ E(aUc)$ with $F=\{ \{1,2\}, \{1,5\} \}$

$S_{fair} = \{0,1,2,3,4,5\}$

$E_F(aUc) \equiv E(aU(c \land fair)) = \varnothing$

$S_a = \{1,3,4,6\} \quad S_c = \{0,3,6\}$

$S_{fair \land c} = \{0,3\}$

$S_\varnothing = \{0,3,4\}$
Microwave Example

Fairness:
Start \land \text{Close} \land \neg \text{Error}
\( \neg E (\text{true } U (\text{start } \land EG \neg \text{Heat})) \)
\[ \neg E \ (\text{true} \ U \ (\text{start} \land EG \ \neg \text{Heat})) \]

All states belong to the same nontrivial fair SCC

\[ \Rightarrow \text{All states labeled fair} \]
\[ \neg E \ (\text{true} \cup (\text{start} \land \neg \text{EG} \ - \text{Heat})) \]

\[ S(\text{Start}) : \{2,5,6,7\} \]
\[ S(\neg \text{Heat}) : \{1,2,3,5,6\} \]
\[ S(\neg \text{EG} \ - \text{Heat}) : \emptyset \]

Not fair
\( \neg E (true \cup (start \land EG \neg Heat)) \)

- \( S(Start) : \{2,5,6,7\} \)
- \( S(\neg Heat) : \{1,2,3,5,6\} \)
- \( S(EG \neg Heat) : \emptyset \)
- \( S(Start \land EG \neg Heat) : \emptyset \)
- \( S(EU) : \emptyset \)
- \( S(f) : \{1,2,3,4,5,6,7\} \)