Introduction to Software Verification

Orna Grumberg

Lectures Material
winter 2015-16
Lecture 5
Model of a system
Kripke structure / transition system

Labeled by **atomic propositions AP**
(critical section, variable value...)

Reactive Systems
Kripke Structure $M=(S, R, L, S_0)$

Given $\mathcal{AP}$ - finite set of atomic proposition

- $S$ - (finite) set of states
- $R \subseteq S \times S$ - total transition relation
  - For every $s \in S$ there exists $s' \in S$ such that $(s, s') \in R$. Totality means that every path is infinite
- $L : S \rightarrow 2^{\mathcal{AP}}$ - labeling function that associates every state with the atomic propositions true in that state
- $S_0 \subseteq S$ - set of initial states (optional)
\[ \pi = s_0, s_1, \ldots \text{ is a path in } M \text{ from a state } s \text{ if} \]

- \( s = s_0 \) and

- \( R(s_i, s_{i+1}) \) for every \( i \in \mathbb{N} \)

\[ \pi^i - \text{ the suffix of } \pi \text{ starting at } s_i \]
Temporal Logics

Express properties of event orderings in time

• **Linear Time**
  - Every moment has a unique successor
  - Infinite sequences (words)
  - Linear Time Temporal Logic (LTL)

• **Branching Time**
  - Every moment has several successors
  - Infinite tree
  - Computation Tree Logic (CTL)
Propositional Temporal Logic

$AP$ - a set of atomic propositions, $p \in AP$

Temporal operators:

- $Xp$

- $Gp$

- $Fp$

- $pUq$

Path quantifiers: $A$ for all path

$E$ there exists a path
Temporal logics

We present 3 (propositional) temporal logics:
• $CTL^*$
• $CTL$
• $LTL$

$CTL$ and $LTL$ can be described as sub-logics of $CTL^*$
CTL* - syntax

CTL* is defined using two types of formulas:
• State formulas - interpreted over a state
• Path formulas - interpreted over a path
CTL*

State formulas:
• \( p \in \mathcal{AP} \)
• \( \neg g_1, g_1 \lor g_2, g_1 \land g_2 \) where \( g_1, g_2 \) are state formulas
• \( Ef, Af \) where \( f \) is a path formula

Path formulas:
• Every state formula \( g \) is a path formula
• \( \neg f_1, f_1 \lor f_2, f_1 \land f_2, Xf_1, Gf_1, Ff_1, f_1 U f_2 \) where \( f_1, f_2 \) are path formulas

CTL* - set of all state formulas
CTL* - semantics

CTL* formulas are interpreted over:
• A Kripke structure $M$
• A state $s$ in $M$

Since state formulas are defined based on path formulas, we also give semantics to path formulas
• Over $M$ and a path $\pi$ in $M$
Semantics of CTL*

$$\pi = s_0, s_1, \ldots$$ is a path in $$M$$ if $$R(s_i, s_{i+1})$$ for every $$i$$.

$$\pi^i$$ - the suffix of $$\pi$$ starting at $$s_i$$.

State formulas:
- $$M, s \models p \iff p \in L(s)$$
- $$M, s \models \neg g \iff M, s \not\models g$$
- $$M, s \models g_1 \lor g_2 \iff M, s \models g_1 \text{ or } M, s \models g_2$$
- $$M, s \models Ef \iff$$ there is a path $$\pi$$ from $$s$$ s.t. $$M, \pi \models f$$
- $$M, s \models Af \iff$$ for every path $$\pi$$ from $$s$$, $$M, \pi \models f$$
Semantics of CTL*

\[ \pi = s_0, s_1, \ldots \text{ is a path in } M \text{ if } R(s_i, s_{i+1}) \text{ for every } i. \]

\[ \pi^i \text{ - the suffix of } \pi \text{ starting at } s_i. \]

Path formulas:

- \( M, \pi \models g, \) where \( g \) is a state formula \( \iff M, s_0 \models g \)

\[ \text{Diagram:} \]

1. Start at \( s_0 \)
2. Move along the path \( s_0, s_1, \ldots \)
3. Reach state \( s_i \)
4. \( \models g \)
Semantics of CTL*

π = s₀, s₁, … is a path in M if R(sᵢ, sᵢ₊₁) for every i.

πᵢ - the suffix of π starting at sᵢ.

Path formulas:
• M, π ⊨ g, where g is a state formula ⇔ M, s₀ ⊨ g
• M, π ⊨ Xf ⇔ M, π¹ ⊨ f
Semantics of CTL*

\[ \pi = s_0, s_1, \ldots \] is a path in \( M \) if \( R(s_i, s_{i+1}) \) for every \( i \).

\( \pi^i \) - the suffix of \( \pi \) starting at \( s_i \).

Path formulas:

- \( M, \pi \vDash g \), where \( g \) is a state formula \( \iff M, s_0 \vDash g \)
- \( M, \pi \vDash Xf \iff M, \pi^1 \vDash f \)
- \( M, \pi \vDash Gf \iff \) for every \( k \geq 0, M, \pi^k \vDash f \)
Semantics of CTL*

\( \pi = s_0, s_1, \ldots \) is a path in \( M \) if \( R(s_i, s_{i+1}) \) for every \( i \).
\( \pi^i \) - the suffix of \( \pi \) starting at \( s_i \).

Path formulas:
- \( M, \pi \models g \), where \( g \) is a state formula \( \iff M, s_0 \models g \)
- \( M, \pi \models Xf \) \( \iff M, \pi^1 \models f \)
- \( M, \pi \models Gf \) \( \iff \) for every \( k \geq 0 \), \( M, \pi^k \models f \)
- \( M, \pi \models Ff \) \( \iff \) there exists \( k \geq 0 \), s.t. \( M, \pi^k \models f \)
Semantics of CTL*

\[ \pi = s_0, s_1, \ldots \text{ is a path in } M \text{ if } R(s_i, s_{i+1}) \text{ for every } i. \]

\( \pi^i \) - the suffix of \( \pi \) starting at \( s_i \).

\[ \begin{align*}
M, \pi & \models \mathbf{g}, \text{ where } \mathbf{g} \text{ is a state formula} \iff M, s_0 \models \mathbf{g} \\
M, \pi & \models \mathbf{Xf} \iff M, \pi_1 \models \mathbf{f} \\
M, \pi & \models \mathbf{Gf} \iff \text{for every } k \geq 0, M, \pi^k \models \mathbf{f} \\
M, \pi & \models \mathbf{Ff} \iff \text{there exists } k \geq 0, \text{ s.t. } M, \pi^k \models \mathbf{f} \\
M, \pi & \models \mathbf{f_1 U f_2} \iff \text{there exists } k \geq 0, \text{ s.t. } M, \pi^k \models \mathbf{f_2} \\
& \quad \text{and for every } 0 \leq j < k, M, \pi^j \models \mathbf{f_1} 
\end{align*} \]
Semantics of CTL*

$\pi = s_0, s_1, \ldots$ is a path in $M$ if $R(s_i, s_{i+1})$ for every $i$.
$\pi^i$ - the suffix of $\pi$ starting at $s_i$.

Path formulas:

- $M, \pi \vDash g$, where $g$ is a state formula $\iff M, s_0 \vDash g$
- $M, \pi \vDash Xf \iff M, \pi^1 \vDash f$
- $M, \pi \vDash Gf \iff$ for every $k \geq 0$, $M, \pi^k \vDash f$
- $M, \pi \vDash Ff \iff$ there exists $k \geq 0$, s.t. $M, \pi^k \vDash f$
- $M, \pi \vDash f_1 \mathsf{U} f_2 \iff$ there exists $k \geq 0$, s.t. $M, \pi^k \vDash f_2$
  and for every $0 \leq j < k$, $M, \pi^j \vDash f_1$
Semantics of Path Formulas

If $p,q$ are state formulas then:

- $Xp$
- $Gp$
- $Fp$
- $pUq$

But in the general case, they can be path formulas.
Semantics of CTL*

\[ M \models g \iff \text{for every initial state } s: M, s \models g \]
Examples
LTL/CTL/CTL*

**LTL** - state formulas of the form $A\psi$
- $\psi$ - path formula, contains **no** path quantifiers
- interpreted over infinite computation paths

**CTL** - state formulas where path quantifiers and temporal operators appear in pairs:
- $AG, AU, AF, AX, EG, EU, EF, EX$
- interpreted over infinite computation trees

**CTL*** - Allows any combination of temporal operators and path quantifiers. Includes both LTL and CTL
LTL

State formulas:
• \( \mathcal{A}f \) where \( f \) is a path formula

Path formulas:
• \( p \in \mathcal{AP} \)
• \( \neg f_1, f_1 \lor f_2, f_1 \land f_2, Xf_1, Gf_1, Ff_1, f_1 U f_2 \) where \( f_1, f_2 \) are path formulas

LTL - set of all state formulas
CTL

CTL - set of all state formulas

• \( p \in AP \)

• \( \neg g_1, g_1 \lor g_2, g_1 \land g_2 \)

• \( AX g_1, AG g_1, AF g_1, A g_1 U g_2 \)

• \( EX g_1, EG g_1, EF g_1, E g_1 U g_2 \)

where \( g_1, g_2 \) are state formulas
Semantics of CTL

Recall: path $\pi = s_0, s_1, \ldots$

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

- $M,s \models \varphi_1 \lor \varphi_2 \iff M,s \models \varphi_1$ or $M,s \models \varphi_2$

- $M,s \models EX \varphi \iff$ there is $s'$ s.t. $R(s,s')$ and $M,s' \models \varphi$

- $M,s \models EG \varphi \iff$ there is a path $\pi$ from $s$, s.t. for every $i \geq 0$, $M,s_i \models \varphi$
Semantics of CTL

- $M, s \models E[\varphi_1 U \varphi_2] \iff$ there is a path $\pi$ from $s$ and there is $k \geq 0$ s.t. $M, s_k \models \varphi_2$ and for every $k > i \geq 0$, $M, s_i \models \varphi_1$

- $M, s \models AG \varphi \iff$ for every path $\pi$ from $s$ and for every $i \geq 0$, $M, s_i \models \varphi$

- $M, s \models AF \varphi \iff$ for every path $\pi$ from $s$ there exists $i \geq 0$ s.t. $M, s_i \models \varphi$
Illustration of CTL Semantics

**EFp:**
```
exists reachable state s.t.
```

**AFp:**
```
```

**EGp:**
```
```

**AGp:**
```
“all reachable states....”
Examples (LTL)

1. $AG \neg (\text{start} \land \neg \text{ready})$
2. $AG (\text{req} \rightarrow \text{F ack})$
3. $A \text{ GF enabled}$
4. $A \text{ FG deadlock}$
5. $A (\text{GF enabled} \rightarrow \text{GF running})$

Cannot express existential properties: “from any state the system can...”
Examples (CTL)

1. EF (start ∧¬ready)
2. AG (req → AF ack)
3. AG (AF enabled)
4. AF (AG deadlock)
5. AG (EF restart)
6. AG (non_critical → EX trying)
7. AG (try → A[try U succeed])
Equivalence

• **Path formulas** $\psi_1, \psi_2$ are equivalent if:
  For every $M$ and path $\pi$
  \[ M, \pi \models \psi_1 \iff M, \pi \models \psi_2 \]

• **State formulas** $\varphi_1, \varphi_2$ are equivalent if:
  For every $M$ and state $s$
  \[ M, s \models \varphi_1 \iff M, s \models \varphi_2 \]
Expressiveness

¬, ∨, X, U, E suffice to express all CTL*:
• Ff ≡ true U f
• Gf ≡ ¬F (¬f)
• Af ≡ ¬E (¬f)

In CTL: EX, EG, EU are sufficient

• A [pUq] ≡ (¬EG ¬q) ∧ ¬E[¬q U (¬p ∧ ¬q)]
LTL vs. CTL

• **A (FG p)** has no equivalent in CTL
  “in all paths, p globally holds from some point on”

• Failed attempts:
  **AFAGP** : “in every path there is a point from which all reachable states satisfy p.”

All paths satisfy FGp
- $s_0,s_0,s_0,...$
- $s_0,s_0,...s_0,s_1,s_2,s_2,s_2...$

But first one does not sat FAGp
LTL vs. CTL

• **A (FG p)** has no equivalent in CTL
  "in all paths, p globally holds from some point on"

• What about **AFEGP**?
  "in every path there is a point from which there is a path where p globally holds"

All paths satisfy FEGp
- since $s_1$ sat EGp
But $s_0, s_1, s_0, s_1, s_0, s_1, ...$ does not sat FGp
LTL vs. CTL

• **AG (EFp)** has no equivalent in LTL
  - “all reachable states can reach \( p \)”

• Failed attempt:
  \( \text{AGFp} \) : “in all paths, \( p \) holds infinitely many times.”

All reachable states \((s_0, s_1)\) satisfy EFp

But \( s_0, s_0, s_0, ... \) does not satisfy GFp
LTL and CTL vs. CTL*

- E (GFp) has no equivalent in LTL or CTL