Formal Verification

Lecture 5: Computation Tree Logic (CTL)

Jacques Fleuriot
jdf@inf.ac.uk

¹With thanks to Bob Atkey for the diagrams.
Recap

- Previously:
  - *Linear-time* Temporal Logic

- This time:
  - A *branching-time* logic: Computation Tree Logic (CTL)
  - Syntax and Semantics
  - Comparison with LTL, CTL*
  - Model checking CTL
CTL Syntax

Assume a set $\text{Atom}$ of atom propositions.

$$
\phi, \psi ::= p \mid \neg \phi \mid \phi \land \psi \mid \phi \lor \psi \mid \phi \rightarrow \psi \\
\mid \text{AX } \phi \mid \text{EX } \phi \mid \text{AF } \phi \mid \text{EF } \phi \mid \text{AG } \phi \mid \text{EG } \phi \\
\mid \text{A}[\phi \ U \ \psi] \mid \text{E}[\phi \ U \ \psi]
$$

where $p \in \text{Atom}$.

Each temporal connective is a pair of a path quantifier:

- $\text{A}$ — for all paths
- $\text{E}$ — there exists a path

and an LTL-like temporal operator $\text{X, F, G, U}$.

Precedence (high-to-low): $(\text{AX, EX, AF, EF, AG, EG, } \neg), (\land, \lor), \rightarrow$
CTL Semantics 1: Transition Systems and Paths

(This is the same as for LTL)

Definition (Transition System)
A transition system $\mathcal{M} = \langle S, \rightarrow, L \rangle$ consists of:

- $S$ a finite set of states
- $\rightarrow \subseteq S \times S$ transition relation
- $L : S \rightarrow \mathcal{P}(\text{Atom})$ a labelling function

such that $\forall s_1 \in S. \exists s_2 \in S. s_1 \rightarrow s_2$

Definition (Path)
A path $\pi$ in a transition system $\mathcal{M} = \langle S, \rightarrow, L \rangle$ is an infinite sequence of states $s_0, s_1, \ldots$ such that $\forall i \geq 0. s_i \rightarrow s_{i+1}$.

 Paths are written as: $\pi = s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \ldots$
Satisfaction relation \( \mathcal{M}, s \models \phi \) read as

*state s in model \( \mathcal{M} \) satisfies CTL formula \( \phi \)*

We often leave \( \mathcal{M} \) implicit.

The propositional connectives:

\[
\begin{align*}
    s \models \top & \quad \text{iff} \quad p \in L(s) \\
    s \not\models \bot & \\
    s \models p & \quad \text{iff} \quad s \not\models \phi \\
    s \models \phi \land \psi & \quad \text{iff} \quad s \models \phi \text{ and } s \models \psi \\
    s \models \phi \lor \psi & \quad \text{iff} \quad s \models \phi \text{ or } s \models \psi \\
    s \models \phi \rightarrow \psi & \quad \text{iff} \quad s \models \phi \text{ implies } s \models \psi
\end{align*}
\]
CTL Semantics 2: Satisfaction Relation

The temporal connectives, assuming $\pi = s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \ldots$,

\[
\begin{align*}
s \models AX \phi & \iff \forall s'. (s \rightarrow s') \text{ implies } s' \models \phi \\
s \models EX \phi & \iff \exists s'. (s \rightarrow s') \text{ and } s' \models \phi \\
s \models AG \phi & \iff \forall \text{paths } \pi \text{ s.t. } s_0 = s. \forall i. s_i \models \phi \\
s \models EG \phi & \iff \exists \text{path } \pi \text{ s.t. } s_0 = s. \forall i. s_i \models \phi \\
s \models AF \phi & \iff \forall \text{paths } \pi \text{ s.t. } s_0 = s. \exists i. s_i \models \phi \\
s \models EF \phi & \iff \exists \text{path } \pi \text{ s.t. } s_0 = s. \exists i. s_i \models \phi \\
s \models A[\phi U \psi] & \iff \forall \text{paths } \pi \text{ s.t. } s_0 = s. \\
& \quad \exists i. s_i \models \psi \text{ and } \forall j < i. s_j \models \phi \\
s \models E[\phi U \psi] & \iff \exists \text{path } \pi \text{ s.t. } s_0 = s. \\
& \quad \exists i. s_i \models \psi \text{ and } \forall j < i. s_j \models \phi
\end{align*}
\]
For every next state, $\phi$ holds.
There exists a next state where $\phi$ holds.
For all paths, there exists a future state where $\phi$ holds.
There exists a path with a future state where $\phi$ holds.
For all paths, for all states along them, $\phi$ holds.
There exists a path such that, for all states along it, $\phi$ holds.
CTL in Pictures

For all paths, $\psi$ eventually holds, and $\phi$ holds at all states earlier.
CTL in Pictures

E[φ U ψ]

Exists path where ψ eventually holds, and φ holds at all states earlier.
Examples of CTL formulas

- $\text{EF } \phi$
  
  *there exists a future state where eventually $\phi$ is true*
Examples of CTL formulas

- **EF \( \phi \)**
  
  *there exists a future state where eventually \( \phi \) is true*

- **AG AF \( \phi \)**
  
  *for all future states, \( \phi \) will eventually hold*
Examples of CTL formulas

- EF $\phi$
  
  *there exists a future state where eventually $\phi$ is true*

- AG AF $\phi$
  
  *for all future states, $\phi$ will eventually hold*

- AG ($\phi \rightarrow$ AF $\psi$)
  
  *for all future states, if $\phi$ holds, then $\psi$ will eventually hold*
Examples of CTL formulas

- **EF $\phi$**
  
  there exists a future state where eventually $\phi$ is true

- **AG AF $\phi$**
  
  for all future states, $\phi$ will eventually hold

- **AG ($\phi \rightarrow AF \psi$)**
  
  for all future states, if $\phi$ holds, then $\psi$ will eventually hold

- **AG ($\phi \rightarrow E[\phi U \psi]$)**
  
  for all future states, if $\phi$ holds, then there is a future where $\psi$ eventually holds, and $\phi$ holds for all points in between
Examples of CTL formulas

- \(\text{EF } \phi\)
  there exists a future state where eventually \(\phi\) is true

- \(\text{AG AF } \phi\)
  for all future states, \(\phi\) will eventually hold

- \(\text{AG (} \phi \rightarrow \text{AF } \psi)\)
  for all future states, if \(\phi\) holds, then \(\psi\) will eventually hold

- \(\text{AG (} \phi \rightarrow \text{E}[\phi \text{ U } \psi])\)
  for all future states, if \(\phi\) holds, then there is a future where \(\psi\) eventually holds, and \(\phi\) holds for all points in between

- \(\text{AG (} \phi \rightarrow \text{EG } \psi)\)
  for all future states, if \(\phi\) holds then there is a future where \(\psi\) always holds
Examples of CTL formulas

- **EF \( \phi \)**
  
  "there exists a future state where eventually \( \phi \) is true"

- **AG AF \( \phi \)**
  
  "for all future states, \( \phi \) will eventually hold"

- **AG (\( \phi \rightarrow AF \psi \))**
  
  "for all future states, if \( \phi \) holds, then \( \psi \) will eventually hold"

- **AG (\( \phi \rightarrow E[\phi U \psi] \))**
  
  "for all future states, if \( \phi \) holds, then there is a future where \( \psi \) eventually holds, and \( \phi \) holds for all points in between"

- **AG (\( \phi \rightarrow EG \psi \))**
  
  "for all future states, if \( \phi \) holds then there is a future where \( \psi \) always holds"

- **EF AG \( \phi \)**
  
  "there exists a possible state in the future, from where \( \phi \) is always true"
CTL Equivalences

de Morgan dualities for the temporal connectives:

\[
\neg \text{EX } \phi \equiv \text{AX } \neg \phi \\
\neg \text{EF } \phi \equiv \text{AG } \neg \phi \\
\neg \text{EG } \phi \equiv \text{AF } \neg \phi
\]

Also have

\[
\text{AF } \phi \equiv \text{A[\top U } \phi] \\
\text{EF } \phi \equiv \text{E[\top U } \phi] \\
\text{A[}\phi \text{ U } \psi] \equiv \neg (\text{E[}\neg \psi \text{ U (}\neg \phi \land \neg \psi)) \lor \text{EG } \neg \psi)
\]

From these, one can show that the sets \{\text{AU}, \text{EU}, \text{EX}\} and \{\text{EU}, \text{EG}, \text{EX}\} are both adequate sets of temporal connectives.
Differences between LTL and CTL

LTL allows for questions of the form

- For all paths, does the LTL formula $\phi$ hold?
- Does there exist a path on which the LTL formula $\phi$ holds?
  
  *(Ask whether $\neg\phi$ holds on all paths, and ask for a counterexample)*

CTL allows mixing of path quantifiers:

- $AG (p \rightarrow EG q)$
  
  *For all paths, if p is true, then there exists a path on which q is always true.*

However, some path properties are impossible to express in CTL

LTL:  $GF p \rightarrow GF q$

CTL:  $AG AF p \rightarrow AG AF q$

\{ are not the same

Exist *fair* refinements of CTL that address this issue to some extent.

- E.g., *path quantifiers that only consider paths where something happens infinitely often.*
CTL

LTL: \( G F p \rightarrow G F q \) \\
CTL: \( AG AF p \rightarrow AG AF q \) \\
\[ \text{are not the same} \]

LTL: for all paths \( \pi \), if \( p \) holds infinitely often on \( \pi \), then \( q \) holds infinitely often on \( \pi \)

CTL: if \( p \) holds infinitely often on all paths, then \( q \) holds infinitely often on all paths

Intuitively, in CTL we cannot fix a path \( \pi \) and talk about it.

CTL* addresses this by splitting formulas into state formulas \( \phi \) and path formulas \( \alpha \):

\[
\phi ::= p \mid \neg \phi \mid \phi \land \phi \mid \phi \lor \phi \mid \phi \rightarrow \phi \\
\quad \quad \quad \quad \mid A[\alpha] \mid E[\alpha]
\]

\[
\alpha ::= \phi \mid \neg \alpha \mid \alpha \land \alpha \mid \alpha \lor \alpha \mid \alpha \rightarrow \alpha \\
\quad \quad \quad \quad \mid X \alpha \mid F \alpha \mid G \alpha \mid \alpha \ U \alpha
\]

Harder to model check.
CTL Model Checking

CTL Model Checking seeks to answer the question: *is it the case that* 

\[ \mathcal{M}, s \models \phi \]

*for all initial states* \( S_0 \subseteq S \)?

CTL Model Checking algorithms usually fix \( \mathcal{M} = \langle S, \rightarrow, L \rangle \) and \( \phi \) and compute

\[ [\phi]_{\mathcal{M}} = \{ s \in S | \mathcal{M}, s \models \phi \} \]

“the denotation of \( \phi \) in the model \( \mathcal{M} \)”

The model checking question now becomes: \( S_0 \subseteq [\phi]_{\mathcal{M}} \)?

*(The model \( \mathcal{M} \) is usually left implicit)*
Denotation Semantics for CTL

We compute \([\phi]\) recursively on the structure of \(\phi\):

\[
\begin{align*}
[\top] & = S \\
[\bot] & = \emptyset \\
[p] & = \{ s \in S \mid p \in L(s) \} \\
[\neg \phi] & = S - [\phi] \\
[\phi \land \psi] & = [\phi] \cap [\psi] \\
[\phi \lor \psi] & = [\phi] \cup [\psi] \\
[\phi \rightarrow \psi] & = (S - [\phi]) \cup [\psi]
\end{align*}
\]

Since \([\phi]\) is always a finite set, these are computable.
Denotation Semantics of the Temporal Connectives

\[
\begin{align*}
\llbracket \text{EX } \phi \rrbracket &= \text{pre}_\exists(\llbracket \phi \rrbracket) \\
\llbracket \text{AX } \phi \rrbracket &= \text{pre}_\forall(\llbracket \phi \rrbracket)
\end{align*}
\]

where

\[
\begin{align*}
\text{pre}_\exists(Y) &= \{ s \in S \mid \exists s' \in S. (s \rightarrow s') \land s' \in Y \} \\
\text{pre}_\forall(Y) &= \{ s \in S \mid \forall s' \in S. (s \rightarrow s') \rightarrow s' \in Y \}
\end{align*}
\]

these are again computable, because \( Y \) and \( S \) are finite.

But what about the rest of the temporal connectives? e.g.

\[
\llbracket \text{EF } \phi \rrbracket = \{ s \in S \mid \exists \text{ path } \pi \text{ s.t. } s_0 = s. \exists i. s_i \models \phi \}
\]

No obvious way to compute this: there are infinitely many paths \( \pi \)!
Approximating $[\text{EF } \phi]$  

Define 

\[
\begin{align*}
\text{EF}_0 \phi &= \bot \\
\text{EF}_{i+1} \phi &= \phi \lor \text{EX} \text{EF}_i \phi
\end{align*}
\]

Then 

\[
\begin{align*}
\text{EF}_1 \phi &= \phi \\
\text{EF}_2 \phi &= \phi \lor \text{EX} \phi \\
\text{EF}_3 \phi &= \phi \lor \text{EX} (\phi \lor \text{EX} \phi)
\end{align*}
\]

\[
\vdots
\]

$s \in [\text{EF}_i \phi]$ if there exists a finite path of length $i - 1$ from $s$ and $\phi$ holds at some point along that path.

For a given (fixed) model $M$, let $n = |S|$. If there is a path of length $k > n$ on which $\phi$ holds somewhere, there will also be a path of length $n$. (Proof: take the $k$-length path and repeatedly cut out segments between repeated states.)

Therefore, for all $k > n$, $[\text{EF}_k \phi] = [\text{EF}_n \phi]$
Computing $[\text{EF } \phi]$ 

By a similar argument,

$$[\text{EF } \phi] = [\text{EF}_n \phi]$$

The approximations can be computed by recursion on $i$:

$$[\text{EF}_0 \phi] = \emptyset$$

$$[\text{EF}_{i+1} \phi] = \{ \phi \} \cup \text{pre}_\exists([\text{EF}_i \phi])$$

So we have an effective way of computing $[\text{EF } \phi]$. 
Approximating $[\text{EG } \phi]$ 

Define

$$
\text{EG}_0 \phi = \top \\
\text{EG}_{i+1} \phi = \phi \land \text{EX} \text{EG}_i \phi
$$

Then

$$
\text{EG}_1 \phi = \phi \\
\text{EG}_2 \phi = \phi \land \text{EX} \phi \\
\text{EG}_3 \phi = \phi \land \text{EX} (\phi \land \text{EX} \phi) \\
...$$

$s \in [\text{EG}_i \phi]$ if there exists a finite path of length $i - 1$ from $s$ and $\phi$ holds at every point along that path.

As with $[\text{EF } \phi]$, we have for all $k > n$, $[\text{EG}_k \phi] = [\text{EG}_n \phi] = [\text{EG } \phi]$ and so we can compute $[\text{EG } \phi]$. 
Fixed point Theory

What’s happening here is that we are computing fixed points.

A set $X \subseteq S$ is a fixed point of a function $F : \mathcal{P}(S) \rightarrow \mathcal{P}(S)$ iff $F(X) = X$.

We have that

\[
\begin{align*}
[\text{EF}_n \phi] & = [\text{EF}_{n+1} \phi] \\
& = [\phi \lor \text{EX} \text{EF}_n \phi] \\
& = [\phi] \cup \text{pre}_\exists([\text{EF}_n \phi])
\end{align*}
\]

so $[\text{EF}_n]$ is a fixed point of $F(Y) = [\phi] \cup \text{pre}_\exists(Y)$.

Also, $[\text{EF} \phi]$ is a fixed point of $F$, since $[\text{EF} \phi] = [\text{EF}_n \phi]$.

More specifically, they are both the least fixed point of $F$. 
Fixed point Theorem

Let \( F : \mathcal{P}(S) \rightarrow \mathcal{P}(S) \) be a function that takes sets to sets.

- \( F \) is **monotone** iff \( X \subseteq Y \) implies \( F(X) \subseteq F(Y) \).
- Let \( F^0(X) = X \) and \( F^{i+1}(X) = F(F^i(X)) \).
- Given a collection of sets \( C \subseteq \mathcal{P}(S) \), a set \( X \in C \) is
  1. the **least** element of \( C \) if \( \forall Y \in C. \ X \subseteq Y \); and
  2. the **greatest** element of \( C \) if \( \forall Y \in C. \ Y \subseteq X \).

**Theorem (Knaster-Tarski (Special Case))**

Let \( S \) be a set with \( n \) elements and \( F : \mathcal{P}(S) \rightarrow \mathcal{P}(S) \) be a monotone function. Then

- \( F^n(\emptyset) \) is the least fixed point of \( F \); and
- \( F^n(S) \) is the greatest fixed point of \( F \).

*(Proof: see H&R, Section 3.7.1)*

This theorem justifies \( F^n(\emptyset) \) and \( F^n(S) \) being fixed points of \( F \) without the need, as before, to appeal to further details about \( F \).
Denotational semantics of temporal connectives

When \( F : \mathcal{P}(S) \rightarrow \mathcal{P}(S) \) is a monotone function, we write

- \( \mu Y. F(Y) \) for the least fixed point of \( F \); and
- \( \nu Y. F(Y) \) for the greatest fixed point of \( F \).

With this notation, we can define:

\[
\begin{align*}
[\text{EF } \phi] & = \mu Y. [\phi] \cup \text{pre}_\exists(Y) \\
[\text{EG } \phi] & = \nu Y. [\phi] \cap \text{pre}_\exists(Y) \\
[\text{AF } \phi] & = \mu Y. [\phi] \cup \text{pre}_\forall(Y) \\
[\text{AG } \phi] & = \nu Y. [\phi] \cap \text{pre}_\forall(Y) \\
[\text{E}[\phi U \psi]] & = \mu Y. [\psi] \cup ([\phi] \cap \text{pre}_\exists(Y)) \\
[\text{A}[\phi U \psi]] & = \mu Y. [\psi] \cup ([\phi] \cap \text{pre}_\forall(Y))
\end{align*}
\]

In every case, \( F \) is monotone, so the Knaster-Tarski theorem assures us that the fixed point exists, and can be computed.
The fixed point characterisations of the CTL temporal connectives justify some more equivalences between CTL formulas:

\[
\begin{align*}
\text{EF } \phi & \equiv \phi \lor \text{EX } \text{EF } \phi \\
\text{EG } \phi & \equiv \phi \land \text{EX } \text{EG } \phi \\
\text{AF } \phi & \equiv \phi \lor \text{AX } \text{AF } \phi \\
\text{AG } \phi & \equiv \phi \land \text{AX } \text{AG } \phi \\
\text{E}[\phi U \psi] & \equiv \psi \lor (\phi \land \text{EX } \text{E}[\phi U \psi]) \\
\text{A}[\phi U \psi] & \equiv \psi \lor (\phi \land \text{AX } \text{A}[\phi U \psi])
\end{align*}
\]
Summary

- CTL (H&R 3.4, 3.5, 3.6.1, 3.7)
  - CTL, Syntax and Semantics
  - Comparison with LTL, CTL*
  - Model Checking algorithm for CTL
- Next time:
  - (A taste of) The LTL Model Checking algorithm