Topics in Concurrency
Lectures 6

Glynn Winskel

20 February 2019
CTL: Computation tree logic

A logic based on paths

\[
A ::= At \mid A_0 \land A_1 \mid A_0 \lor A_1 \mid \neg A \mid T \mid F \mid \ EX \ A \mid EG \ A \mid E[A_0 \ U \ A_1]
\]

A path from state \( s \) is a maximal sequence of states

\[
\pi = (\pi_0, \pi_1, \ldots, \pi_i \ldots)
\]

such that \( s = \pi_0 \) and \( \pi_i \rightarrow \pi_{i+1} \) for all \( i \).

\[
\begin{align*}
\ s \models EX \ A & \iff \text{Exists a path from } s \text{ along which the next state satisfies } A \\
\ s \models EG \ A & \iff \text{Exists a path from } s \text{ along which globally each state satisfies } A \\
\ s \models E[A \ U \ B] & \iff \text{Exists a path from } s \text{ along which } A \text{ holds Until } B \text{ holds}
\end{align*}
\]
Derived assertions

\[
\begin{align*}
AX \ B & \equiv \neg EX \neg B \\
EF \ B & \equiv \ E[ T \ U \ B] \\
AG \ B & \equiv \neg EF \neg B \\
AF \ B & \equiv \neg EG \neg B \\
A[ B \ U \ C] & \equiv \neg E[ \neg C \ U \neg B \land \neg C] \land \neg EG \neg C
\end{align*}
\]

The \textit{Until} operator is \textbf{strict}
Want a modal-$\mu$ assertion equivalent to EG $A$.

Begin by writing a fixed point equation:

$$X = \varphi(X) \quad \text{where} \quad \varphi(X) = A \land ([\neg]F \lor \langle \rangle X)$$

Least or greatest fixed point? Consider:

$$\mu X.A \land ([\neg]F \lor \langle \rangle X) = \emptyset$$

$$\nu X.A \land ([\neg]F \lor \langle \rangle X) = \{s, t\}$$

Alternatively, consider the approximants for finite-state systems.
A translation into modal-$\mu$

\[
\begin{align*}
\text{EX } a & \equiv \langle-\rangle A \\
\text{EG } a & \equiv \nu Y. A \land (\lnot F \lor \langle-\rangle Y) \\
E[a U b] & \equiv \mu Z. B \lor (A \land \langle-\rangle Z)
\end{align*}
\]

Based on this, we get a translation of CTL into the modal-$\mu$ calculus.
Proposition

\[ s \models \nu Y. A \land (\lnot F \lor \lnot Y) \]

in a finite-state transition system iff
there exists a path \( \pi \) from \( s \) such that \( \pi_i \models A \) for all \( i \).

Proof:
Take \( \varphi(Y) \equiv A \land (\lnot F \lor \lnot Y) \).

\[
\nu Y. \varphi(Y) = \bigcap_{n \in \omega} \varphi^n(T) \quad \text{where} \quad T \supseteq \varphi(T) \supseteq \ldots
\]

since \( \varphi \) is monotonic and \( \cap \)-continuous due to the set of states being finite.
By induction, for \( n \geq 1 \)
\[
s \models \varphi^n(T) \quad \text{iff} \quad \text{there is a path of length } \leq n \text{ from } s \text{ along which all states satisfy } A \text{ and the final state has no outward transition}
\]
or
\[
\text{there is a path of length } n \text{ from } s \text{ along which all states satisfy } A \text{ and the final state has some outward transition}
\]
Assuming the number of states is $k$, we have

$$\varphi^k(T) = \varphi^{k+1}(T)$$

and hence $\nu Y.\varphi(Y) = \varphi^k(T)$.

$s \models \nu Y.\varphi(Y)$ \iff $s \models \varphi^k(T)$

\iff there exists a maximal $A$ path of length $\leq k$ from $s$

or there exists a necessarily looping $A$ path of length $k$ from $s$
Assume processes are finite-state

- Brute force (+ optimizations) computes each fixed point
- Local model checking [Larsen, Stirling and Walker, Winskel]

"Silly idea" Reduction Lemma

\[ p \in \nu X. \varphi(X) \iff p \in \varphi(\nu X.\{p\} \lor \varphi(X)) \]
Modal-$\mu$ for model checking

Extend the syntax with defined basic assertions and adapt the fixed point operator:

$$A ::= U \mid T \mid F \mid \neg A \mid A \land B \mid A \lor B \mid \langle a \rangle A \mid \langle \neg \rangle A \mid \nu X\{p_1, \ldots, p_n\}.A$$

Semantics identifies assertions with subsets of states:

- $U$ is an arbitrary subset of states
- $T = S$
- $F = \emptyset$
- $\neg A = S \setminus A$
- $A \land B = A \cap B$
- $A \lor B = A \cup B$
- $\langle a \rangle A = \{p \in S \mid \exists q. p \xrightarrow{a} q \land q \in A\}$
- $\langle \neg \rangle A = \{p \in S \mid \exists q, a. p \xrightarrow{a} q \land q \in A\}$
- $\nu X\{p_1, \ldots, p_n\}.A = \bigcup\{U \subseteq S \mid U \subseteq \{p_1, \ldots, p_n\} \cup A[U/X]\}$

As before, $\mu X.A \equiv \neg \nu X.\neg A[\neg X/X]$ and now

$$\nu X.A = \nu X\{\}.A$$
The reduction lemma

**Lemma**

Let $\varphi : \mathcal{P}(S) \to \mathcal{P}(S)$ be monotonic. For all $U \subseteq S$,

$$U \subseteq \nu X. \varphi(X) \iff U \subseteq \varphi(\nu X.(U \cup \varphi(X)))$$

In particular,

$$p \in \nu X. \varphi(X) \iff p \in \varphi(\nu X.({p} \cup \varphi(X))).$$
Model checking algorithm

Given a transition system and a set of basic assertions \( \{U, V, \ldots\} \):

- \( p \vdash U \) \quad \rightarrow \quad \text{true} \quad \text{if} \ p \in U
- \( p \vdash U \) \quad \rightarrow \quad \text{false} \quad \text{if} \ p \notin U
- \( p \vdash T \) \quad \rightarrow \quad \text{true}
- \( p \vdash F \) \quad \rightarrow \quad \text{false}
- \( p \vdash \neg B \) \quad \rightarrow \quad \text{not}(p \vdash B)
- \( p \vdash A \land B \) \quad \rightarrow \quad p \vdash A \quad \text{and} \quad p \vdash B
- \( p \vdash A \lor B \) \quad \rightarrow \quad p \vdash A \quad \text{or} \quad p \vdash B
- \( p \vdash \langle a \rangle B \) \quad \rightarrow \quad q_1 \vdash B \quad \text{or} \quad \ldots \quad \text{or} \quad q_n \vdash B

\[
\{q_1, \ldots, q_n\} = \{q \mid p \xrightarrow{a} q\}
\]

- \( p \vdash \nu X\{\tilde{r}\}.B \) \quad \rightarrow \quad \text{true} \quad \text{if} \ p \in \{\tilde{r}\}
- \( p \vdash \nu X\{\tilde{r}\}.B \) \quad \rightarrow \quad p \vdash B[\nu X\{p, \tilde{r}\}.B/X] \quad \text{if} \ p \notin \{\tilde{r}\}

Can use any sensible reduction technique for \text{not, or and and.}
Examples

Define the pure CCS process

\[ P \overset{\text{def}}{=} a.(a.\text{nil} + a.P) \]

Check

\[ P \vdash \nu X.(a)X \]

and check

\[ P \vdash \mu Y.[-]F \lor \langle \rangle Y \]

Note:

\[ \mu Y.[-]F \lor \langle \rangle Y \equiv \neg \nu Y.\neg([-]F \lor \langle \rangle \neg Y)) \]
A binary relation $<$ on a set $A$ is well-founded iff there are no infinite descending chains

$$\cdots < a_n < \cdots < a_1 < a_0$$

**The principle of well-founded induction:**

Let $<$ be a well-founded relation on a set $A$. Let $P$ be a property on $A$. Then

$$\forall a \in A. \ P(a)$$

iff

$$\forall a \in A. \ ((\forall b < a. \ P(b)) \implies P(a))$$
Correctness and termination of the algorithm

Write \((p \models A) = \text{true}\) iff \(p\) is in the set of states determined by \(A\).

**Theorem**

Let \(p \in \mathcal{P}\) be a finite-state process and \(A\) be a closed assertion. For any truth value \(t \in \{\text{true, false}\}\),

\[
(p \models A) \rightarrow^* t \iff (p \models A) = t
\]
Proof sketch

For assertions $A$ and $A'$, take

$$A' \text{ is a proper subassertion of } A \iff A' < A \quad \text{or} \quad A \equiv \nu X \{\bar{r}\} B \quad \&\quad \exists p \quad A' \equiv \nu X \{\bar{r}, p\} B \quad \& \quad p \notin \bar{r}$$

Want, for all closed assertions $A$,

$$Q(A) \iff \forall q \in \mathcal{P}. \forall t. (q \vdash A) \rightarrow^* t \iff (q \models A) = t$$

We show the following stronger property on open assertions by well-founded induction:

$$Q^+(A) \iff \forall \text{closed substitutions for free variables} \quad B_1/X_1, \ldots, B_n/X_n:\quad Q(B_1) \& \ldots \& Q(B_n) \implies Q(A[B_1/X_1, \ldots, B_n/X_n])$$

The proof (presented in the lecture notes) centrally depends on the reduction lemma.