Topics in Concurrency

Lectures 6

Glynn Winskel

20 February 2019

CTL: Computation tree logic

A logic based on paths

$$A \quad ::= \quad At \mid A_0 \wedge A_1 \mid A_0 \vee A_1 \mid \neg A \mid T \mid F \mid$$
$$\mathrm{EX}\ A \mid \mathrm{EG}\ A \mid \mathrm{E}[A_0\ \mathrm{U}\ A_1]$$

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 $\pi_i \to \pi_{i+1}$ for all i.

$s \models \mathrm{EX}\ A$	iff	Exists a path from s along which the neXt state satisfies A
$s \models \mathrm{EG}\ A$	iff	Exists a path from s along which Globally each state satisfies A
$s \models \mathrm{E}[A\ \mathrm{U}\ B]$	iff	Exists a path from s along which A holds Until B holds

Derived assertions

$$
\begin{aligned}
\mathrm{AX}\ B &\equiv \neg\mathrm{EX}\ \neg B \\
\mathrm{EF}\ B &\equiv \mathrm{E}[\ T\ \mathrm{U}\ B\ ] \\
\mathrm{AG}\ B &\equiv \neg\mathrm{EF}\ \neg B \\
\mathrm{AF}\ B &\equiv \neg\mathrm{EG}\ \neg B \\
\mathrm{A}[B\ \mathrm{U}\ C] &\equiv \neg\mathrm{E}[\neg C\ \mathrm{U}\ \neg B \wedge \neg C] \wedge \neg\mathrm{EG}\ \neg C
\end{aligned}
$$

The *U*ntil operator is strict

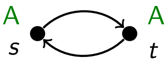
From CTL to μ

Want a modal-μ assertion equivalent to EG A.

Begin by writing a fixed point equation:

$$X = \varphi(X) \quad \text{where} \quad \varphi(X) = A \wedge ([-]F \vee \langle - \rangle X)$$

Least or greatest fixed point? Consider:



$$\mu X . A \wedge ([-]F \vee \langle - \rangle X) = \emptyset$$
$$\nu X . A \wedge ([-]F \vee \langle - \rangle X) = \{s, t\}$$

Alternatively, consider the approximants for finite-state systems.

A translation into modal-μ

$$
\begin{aligned}
\mathsf{EX}\ a &\equiv \langle - \rangle A \\
\mathsf{EG}\ a &\equiv \nu Y. A \wedge ([-]F \vee \langle - \rangle Y) \\
\mathsf{E}[a\ \mathsf{U}\ b] &\equiv \mu Z. B \vee (A \wedge \langle - \rangle Z)
\end{aligned}
$$

Based on this, we get a translation of CTL into the modal-μ calculus.

Proposition

$$s \vDash \nu Y.A \wedge ([-]F \vee \langle - \rangle Y)$$

in a finite-state transition system iff
there exists a path π from s such that $\pi_i \vDash A$ for all i.

Proof:
Take $\varphi(Y) \stackrel{\text{def}}{=} A \wedge ([-]F \vee \langle - \rangle Y)$.

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

since φ is monotonic and $\bigcap$-continuous due to the set of states being finite.
By induction, for $n \geq 1$

$s \vDash \varphi^n(T)$	iff	there is a path of length $\leq n$ from s along which all states satisfy A and the final state has no outward transition
	or	there is a path of length n from s along which all states satisfy A 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 maxmial A path of length $\leq k$ from s
	or	there exists a necessarily looping A path of length k from s

□

Model checking modal-μ

Assume processes are finite-state

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

$$p \in \nu X.\varphi(X) \iff p \in \varphi(\nu X.\{p\} \vee \varphi(X))$$

Modal-μ for model checking

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

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

Semantics identifies assertions with subsets of states:

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

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

$$
\begin{aligned}
& U \subseteq \nu X.\varphi(X) \\
\iff \quad & U \subseteq \varphi(\nu X.(U \cup \varphi(X)))
\end{aligned}
$$

In particular,

$$
\begin{aligned}
& p \in \nu X.\varphi(X) \\
\iff \quad & p \in \varphi(\nu X.(\{p\} \cup \varphi(X))).
\end{aligned}
$$

Model checking algorithm

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

$$
\begin{array}{lcll}
p \vdash U & \longrightarrow & \text{true} & \text{if } p \in U \\
p \vdash U & \longrightarrow & \text{false} & \text{if } p \notin U \\
p \vdash T & \longrightarrow & \text{true} & \\
p \vdash F & \longrightarrow & \text{false} & \\
p \vdash \neg B & \longrightarrow & \text{not}(p \vdash B) & \\
p \vdash A \wedge B & \longrightarrow & p \vdash A \quad \text{and} \quad p \vdash B & \\
p \vdash A \vee B & \longrightarrow & p \vdash A \quad \text{or} \quad p \vdash B & \\
p \vdash \langle a \rangle B & \longrightarrow & q_1 \vdash B \text{ or } \ldots \text{ or } q_n \vdash B & \\
 & & \qquad \{q_1, \ldots, q_n\} = \{q \mid p \xrightarrow{a} q\} & \\
p \vdash \nu X\{\vec{r}\}.B & \longrightarrow & \text{true} & \text{if } p \in \{\vec{r}\} \\
p \vdash \nu X\{\vec{r}\}.B & \longrightarrow & p \vdash B[\nu X\{p, \vec{r}\}.B/X] & \text{if } p \notin \{\vec{r}\}
\end{array}
$$

Can use any sensible reduction technique for not, or and and.

Examples

Define the pure CCS process

$$P \stackrel{\text{def}}{=} a.(a.\mathbf{nil} + a.P)$$

Check

$$P \vdash \nu X.\langle a \rangle X$$

and check

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

Note:

$$\mu Y.[-]F \vee \langle - \rangle Y \equiv \neg \nu Y.\neg([-]F \vee \langle - \rangle \neg Y))$$

Well-founded induction

A binary relation $\prec$ on a set A is well-founded iff there are no infinite descending chains

$$\cdots \prec a_n \prec \cdots \prec a_1 \prec a_0$$

The principle of well-founded induction:
Let $\prec$ be a well-founded relation on a set A. Let P be a property on A. Then

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

iff

$$\forall a \in A.\ ((\forall b \prec a.\ P(b)) \implies P(a))$$

Correctness and termination of the algorithm

Write $(p \vDash A) = \mathrm{true}$ 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 $t \in \{\mathrm{true}, \mathrm{false}\}$,

$$(p \vdash A) \to^* t \quad \Longleftrightarrow \quad (p \vDash A) = t$$

Proof sketch

For assertions A and A', take

$$A' \prec A \iff \begin{array}{ll} & A' \text{ is a proper subassertion of } A \\ \text{or} & A \equiv \nu X\{\vec{r}\}B \;\;\& \\ \exists p & A' \equiv \nu X\{\vec{r}, p\}B \;\;\&\;\; p \notin \vec{r} \end{array}$$

Want, for all closed assertions A,

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

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

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

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