Topics in Concurrency Lecture 9

Jonathan Hayman

3 February 2016

CTL: Computation tree logic

A logic based on paths

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

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*.

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

 $AX B \equiv \neg EX \neg B$ $EF B \equiv E[T \cup B]$ $AG B \equiv \neg EF \neg B$ $AF B \equiv \neg EG \neg B$ $A[B \cup C] \equiv \neg E[\neg C \cup \neg B \land \neg C] \land \neg EG \neg C$

The Until operator is strict

Begin by writing a fixed point equation:

 $X = \varphi(X)$ where $\varphi(X) = A \land ([-]F \lor \langle - \rangle X)$

Least or greatest fixed point? Consider:



Begin by writing a fixed point equation:

 $X = \varphi(X)$ where $\varphi(X) = A \land ([-]F \lor \langle - \rangle X)$

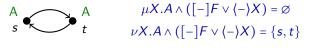
Least or greatest fixed point? Consider:



Begin by writing a fixed point equation:

 $X = \varphi(X)$ where $\varphi(X) = A \land ([-]F \lor \langle - \rangle X)$

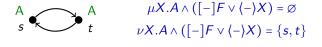
Least or greatest fixed point? Consider:



Begin by writing a fixed point equation:

 $X = \varphi(X)$ where $\varphi(X) = A \land ([-]F \lor \langle - \rangle X)$

Least or greatest fixed point? Consider:



Alternatively, consider the approximants for finite-state systems.

A translation into modal- μ

$$EX a \equiv \langle - \rangle A$$

$$EG a \equiv \nu Y \cdot A \land ([-]F \lor \langle - \rangle Y)$$

$$E[a \cup b] \equiv \mu Z \cdot B \lor (A \land \langle - \rangle Z)$$

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

Proposition

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

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 $\varphi(Y) \stackrel{\text{def}}{=} A \land ([-]F \lor \langle - \rangle Y).$ $\nu Y.\varphi(Y) = \bigcap_{n \in \omega} \varphi^n(T) \text{ where } T \supseteq \varphi(T) \supseteq \cdots$

since φ is monotonic and $\bigcap\mbox{-continuous}$ due to the set of states being finite.

By induction, for $n \ge 1$

- $s \models \varphi^n(T)$ iff there is a path of length $\le n$ 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 sor 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]

Assume processes are finite-state

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

$$p \in \nu X. \varphi(X) \iff p \in \varphi(\nu X. \qquad \varphi(X))$$

Assume processes are finite-state

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

$$p \in \nu X.\varphi(X) \Longleftrightarrow p \in \varphi(\nu X.\{p\} \lor \varphi(X))$$

Modal- μ for model checking

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

$$A ::= \bigcup |T|F| \neg A |A \land B|A \lor B |\langle a \rangle A |\langle - \rangle A |\nu X \qquad .A$$

Semantics identifies assertions with subsets of states:

- U is an arbitrary subset of states
- T = S
- *F* = Ø

•
$$\neg A = S \setminus A$$

•
$$A \wedge B = A \cap B$$

•
$$A \lor B = A \cup B$$

•
$$\langle a \rangle A = \{ p \in S \mid \exists q. p \xrightarrow{a} q \land q \in A \}$$

• $\langle - \rangle A = \{ p \in S \mid \exists q, a. p \xrightarrow{a} q \land q \in A \}$
• $\nu X \{ p_1, \dots, p_n \} . A = \bigcup \{ U \subseteq S \mid U \subseteq A \}$

Modal- μ for model checking

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

 $A ::= \bigcup |T| F |\neg A | A \land B | A \lor B | \langle a \rangle A | \langle - \rangle A | \nu X \{p_1, \dots, p_n\}.A$

Semantics identifies assertions with subsets of states:

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

Modal- μ for model checking

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

 $A ::= \bigcup |T| F |\neg A | A \land B | A \lor B | \langle a \rangle A | \langle - \rangle A | \nu X \{p_1, \dots, p_n\}.A$

Semantics identifies assertions with subsets of states:

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

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

Lemma

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

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 $\{U, V, \ldots\}$:

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

Define the pure CCS process

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

Check

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

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

```
\forall a \in A. P(a) iff
```

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

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}, \text{false}\},\$

$$(p \vdash A) \rightarrow^* t \iff (p \vDash A) = t$$

Proof sketch

For assertions A and A', take

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

Want, for all closed assertions A,

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

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

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

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