

# Topics in Concurrency

## Lecture 7

Jonathan Hayman

27 February 2015

# CTL: Computation tree logic

A logic based on paths

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

A **path** from state  $s$  is a maximal sequence of states

$$\pi = (\pi_0, \pi_1, \dots, \pi_i \dots)$$

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

$s \models EX A$       iff    **E**xists a path from  $s$  along which the **neXt** state satisfies  $A$

$s \models EG A$       iff    **E**xists a path from  $s$  along which **G**lobally each state satisfies  $A$

$s \models E[A U B]$     iff    **E**xists a path from  $s$  along which  $A$  holds **U**ntil  $B$  holds

## Derived assertions

$$AX B \equiv \neg EX \neg B$$

$$EF B \equiv E[T U B]$$

$$AG B \equiv \neg EF \neg B$$

$$AF B \equiv \neg EG \neg B$$

$$A[B U C] \equiv \neg E[\neg C U \neg B \wedge \neg C] \wedge \neg EG \neg C$$

The *U*ntil operator is **strict**

## From CTL to $\mu$

Want a modal- $\mu$  assertion equivalent to EG A.

# From CTL to $\mu$

Want a modal- $\mu$  assertion equivalent to  $EG A$ .

Begin by writing a fixed point equation:

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

Least or greatest fixed point? Consider:



# From CTL to $\mu$

Want a modal- $\mu$  assertion equivalent to  $EG A$ .

Begin by writing a fixed point equation:

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

Least or greatest fixed point? Consider:



$$\mu X. A \wedge ([-]F \vee \langle - \rangle X) = \emptyset$$

# From CTL to $\mu$

Want a modal- $\mu$  assertion equivalent to  $EG A$ .

Begin by writing a fixed point equation:

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

Least or greatest fixed point? Consider:



$$\mu X. A \wedge ([-]F \vee \langle - \rangle X) = \emptyset$$

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

# From CTL to $\mu$

Want a modal- $\mu$  assertion equivalent to  $EG A$ .

Begin by writing a fixed point equation:

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

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- $\mu$

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

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

## Proposition

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

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

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

since  $\varphi$  is monotonic and  $\bigcap$ -continuous due to the set of states being finite.

By induction, for  $n \geq 1$

- $s \models \varphi^n(T)$  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  $\nu Y.\varphi(Y) = \varphi^k(T)$ .

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

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  $s$



# Model checking modal- $\mu$

Assume processes are finite-state

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

# Model checking modal- $\mu$

Assume processes are finite-state

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

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

# Model checking modal- $\mu$

Assume processes are finite-state

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

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

# Modal- $\mu$ for model checking

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

$$A ::= U \mid T \mid F \mid \neg A \mid A \wedge B \mid A \vee B \mid \langle a \rangle A \mid \langle - \rangle A \mid \nu X \quad .A$$

Semantics identifies assertions with subsets of states:

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

$$A[U/X]\}$$

# Modal- $\mu$ for model checking

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

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

Semantics identifies assertions with subsets of states:

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



# Modal- $\mu$ for model checking

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

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

Semantics identifies assertions with subsets of states:

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

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

$$\nu X.A = \nu X \{\}.A$$

# The reduction lemma

## Lemma

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

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

In particular,

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

# Model checking algorithm

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

$p \vdash U$	$\longrightarrow$	true	if $p \in U$
$p \vdash \neg U$	$\longrightarrow$	false	if $p \notin U$
$p \vdash T$	$\longrightarrow$	true	
$p \vdash F$	$\longrightarrow$	false	
$p \vdash \neg B$	$\longrightarrow$	not( $p \vdash B$ )	
$p \vdash A \wedge B$	$\longrightarrow$	$p \vdash A$ and $p \vdash B$	
$p \vdash A \vee B$	$\longrightarrow$	$p \vdash A$ or $p \vdash B$	
$p \vdash \langle a \rangle B$	$\longrightarrow$	$q_1 \vdash B$ or ... or $q_n \vdash B$	
		$\{q_1, \dots, q_n\} = \{q \mid p \rightarrow aq\}$	
$p \vdash \nu X \{\vec{r}\}.B$	$\longrightarrow$	true	if $p \in \{\vec{r}\}$
$p \vdash \nu X \{\vec{r}\}.B$	$\longrightarrow$	$p \vdash B[\nu X \{\vec{r}\}.B/X]$	if $p \notin \{\vec{r}\}$