Temporal Logic
- Branching-time logic (1/2)

Moonzoo Kim
CS Division of EECS Dept.
KAIST

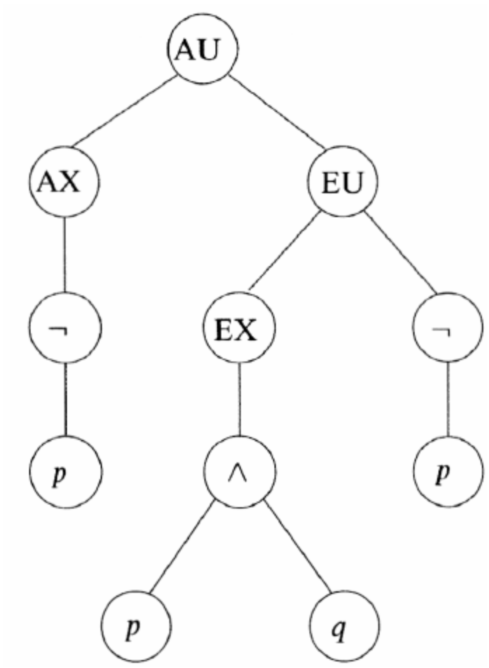
moonzoo@cs.kaist.ac.kr
http://pswlab.kaist.ac.kr/courses/cs402-07

LTL vs. CTL

- LTL implicitly quantifies universally over paths
  - a state of a system satisfies an LTL formula if all paths from the given state satisfy it
  - properties which use both universal and existential path quantifiers cannot in general be model checked using LTL.
    - property ϕ which use only universal path quantifiers can be checked using LTL by checking $\neg\phi$
- Branching-time logic solve this limitation by quantifying paths explicitly
  - There is a reachable state satisfying q: EF q
    - Note that we can check this property by checking LTL formula ϕ=G $\neg$q
      - If ϕ is true, the property is false. If ϕ is false, the property is true
  - From all reachable states satisfying p, it is possible to maintain p continuously until reaching a state satisfying q: AG (p $\rightarrow$ E (p U q))
  - Whenever a state satisfying p is reached, the system can exhibit q continuously forevermore: AG (p $\rightarrow$ EG q)
  - There is a reachable state from which all reachable states satisfy p: EF AG p

Syntax of Computation Tree Logic (CTL)

- Def 3.12 $\phi = \bot \mid \top \mid p \mid \neg \phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \rightarrow \phi \mid$ AX ϕ | EX ϕ | AF ϕ | EF ϕ | AG ϕ | EG ϕ | A (ϕ U ϕ) | E (ϕ U ϕ)
  - A: along all paths
  - E: along at least one path
- Precedence
  - AG, EG, AF, EF,AX, EX, $\wedge$, $\vee$, $\rightarrow$, AU, EU
- Note that the following formulas are not well-formed CTL formulas
  - EF G r
  - A $\neg$G $\neg$ p
  - F (r U q)
  - EF (r U q)
  - AEF r
  - A ((r U q) $\wedge$ (p U r))



A [(AX ¬p) U (E [(EX p∧q) U ¬p)]]

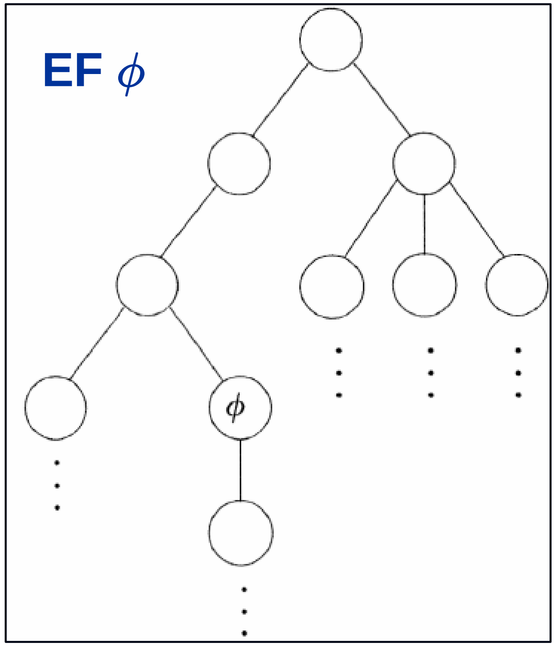
Semantics of CTL (1/2)

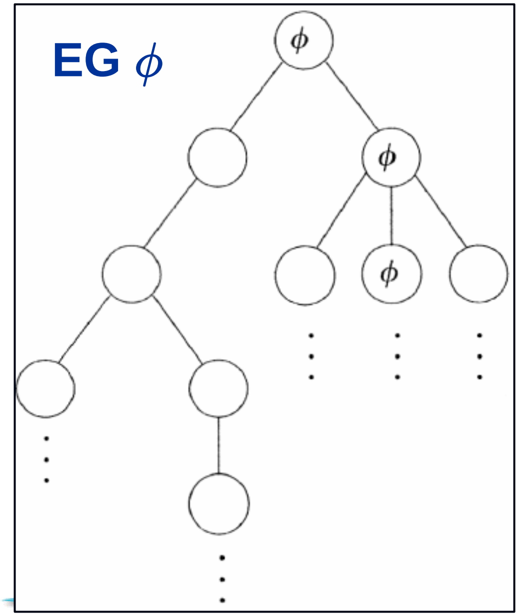
- Def 3.15 Let $\mathcal{M}$ = (S, $\rightarrow$, L) be a model for CTL, s in S, ϕ a CTL formula. The relation $\mathcal{M}$,s $\vDash \phi$ is defined by structural induction on ϕ. We omit $\mathcal{M}$ if context is clear.
  - $\mathcal{M}$,s $\vDash \top$ and $\mathcal{M}$,s $\nvDash \bot$
  - $\mathcal{M}$,s $\vDash$ p iff p $\in$ L(s)
  - $\mathcal{M}$,s $\vDash \neg \phi$ iff $\mathcal{M}$,s $\nvDash \phi$
  - $\mathcal{M}$,s $\vDash \phi_1 \wedge \phi_2$ iff $\mathcal{M}$,s $\vDash \phi_1$ and $\mathcal{M}$,s $\vDash \phi_2$
  - $\mathcal{M}$,s $\vDash \phi_1 \vee \phi_2$ iff $\mathcal{M}$,s $\vDash \phi_1$ or $\mathcal{M}$,s $\vDash \phi_2$
  - $\mathcal{M}$,s $\vDash \phi_1 \rightarrow \phi_2$ iff $\mathcal{M}$,s $\nvDash \phi_1$ or $\mathcal{M}$,s $\vDash \phi_2$
  - $\mathcal{M}$,s $\vDash$ AX ϕ iff for all s_1 s.t. s $\rightarrow$ s_1 we have $\mathcal{M}$, $s_1 \vDash \phi$. Thus AX says "in every next state"
  - $\mathcal{M}$,s $\vDash$ EX ϕ iff for some s_1 s.t. s $\rightarrow$ s_1 we have $\mathcal{M}$, $s_1 \vDash \phi$. Thus EX says "in some next state"
  - $\mathcal{M}$,s $\vDash$ AX ϕ iff for all s_1 s.t. s $\rightarrow$ s_1 we have $\mathcal{M}$, $s_1 \vDash \phi$. Thus AX says "in every next state"
  - $\mathcal{M}$,s $\vDash$ EX ϕ iff for some s_1 s.t. s $\rightarrow$ s_1 we have $\mathcal{M}$, $s_1 \vDash \phi$. Thus EX says "in some next state"

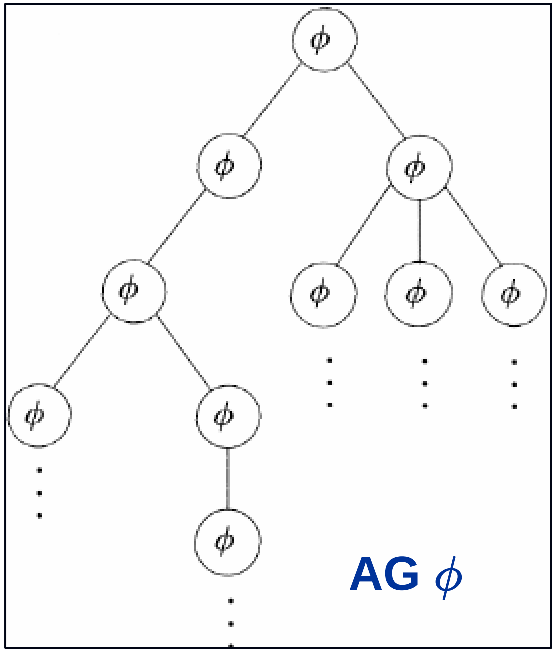
Semantics of CTL (2/2)

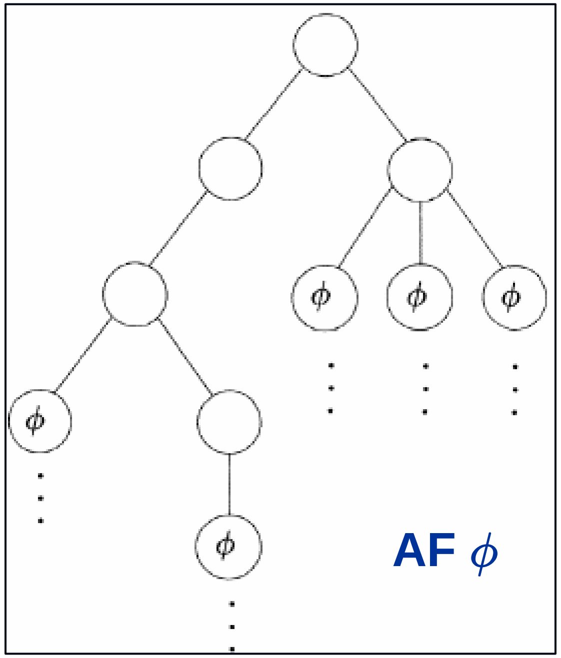
- Def 3.15 Let $\mathcal{M} = (S, \rightarrow, L)$ be a model for CTL, s in S, ϕ a CTL formula. The relation $\mathcal{M}, s \vDash \phi$ is defined by structural induction on ϕ. We omit $\mathcal{M}$ if context is clear.
  - $\mathcal{M}, s \vDash$ AG ϕ iff for all paths $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \ldots$ where s_1 equals s, and all s_i along the path, we have $\mathcal{M}, s_i \vDash \phi$.
  - $\mathcal{M}, s \vDash$ EG ϕ iff there is a path $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \ldots$ where s_1 equals s, and all s_i along the path, we have $\mathcal{M}, s_i \vDash \phi$.
  - $\mathcal{M}, s \vDash$ AF ϕ iff for all paths $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \ldots$ where s_1 equals s, and there is some s_i s.t. $\mathcal{M}, s_i \vDash \phi$.
  - $\mathcal{M}, s \vDash$ EF ϕ iff there is a path $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \ldots$ where s_1 equals s, and there is some s_i s.t. $\mathcal{M}, s_i \vDash \phi$.
  - $\mathcal{M}, s \vDash$ A $[\phi_1$ U $\phi_2]$ iff for all paths $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \ldots$ where s_1 equals s, that path satisfies ϕ_1 U ϕ_2
  - $\mathcal{M}, s \vDash$ E $[\phi_1$ U $\phi_2]$ iff there is a path $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \ldots$ where s_1 equals s, that path satisfies ϕ_1 U ϕ_2

Example (1/2)









Example (2/2)

- $\mathcal{M}, s_0 \vDash p \wedge q$, $\mathcal{M}, s_0 \vDash \neg r$, $\mathcal{M}, s_0 \vDash \top$
- $\mathcal{M}, s_0 \vDash \text{EX}\ (q \wedge r)$
- $\mathcal{M}, s_0 \vDash \neg \text{AX}(q \wedge r)$
- $\mathcal{M}, s_0 \vDash \neg \text{EF}(p \wedge r)$
- $\mathcal{M}, s_2 \vDash \text{EG}\ r$
- $\mathcal{M}, s_0 \vDash \text{AF}\ r$
- $\mathcal{M}, s_0 \vDash \text{E}\ [(p \wedge q)\ \text{U}\ r]$
- $\mathcal{M}, s_0 \vDash \text{A}\ [p\ \text{U}\ r]$
- $\mathcal{M}, s_0 \vDash \text{AG}\ (p \vee q \vee r \rightarrow \text{EF EG}\ r)$