Temporal Logic

Hao Zheng
Dept. of Computer Science & Eng.
Univ. of South Florida

Propositional Logic

- A proposition = statement that is true/false
  - Ex.: 5+5 = 10, today is Tuesday, etc
- Proposition formulas are constructed:
  - True/false, atomic propositions are formulas;
  - Formulas connected are still formulas.

    $\forall \neg$ (not), $\wedge$ (and), $\vee$ (or), $\rightarrow$ (imply), $\leftrightarrow$ (equivalent).
  - Ex.: $(\neg A \vee B) \leftrightarrow C$
- Truth of formulas are evaluated bottom-up.

Natural Deduction

- $f, g \Rightarrow f \wedge g$
- $f \wedge g \Rightarrow f, g$

$\forall \neg\neg f \Rightarrow f$

- $f, f \rightarrow g \Rightarrow g$
- $f \rightarrow g, \neg g \Rightarrow \neg f$
- Question: $f \rightarrow g \rightarrow h \Leftrightarrow f \rightarrow h$ **?**

Predicate Logic

- Need richer language constructs.
  - For all, there exist some, etc.
- Predicates enclose propositions with those constructs.
  - S(Andy) = Andy is *a* student.

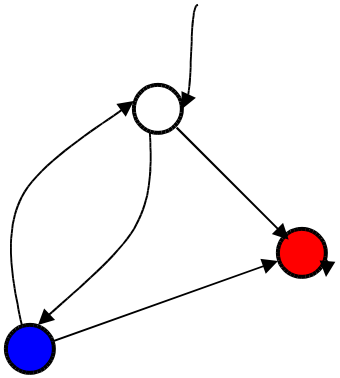
$\forall\ \forall x\ S(x)$

$\forall\ \exists x\ S(x)$

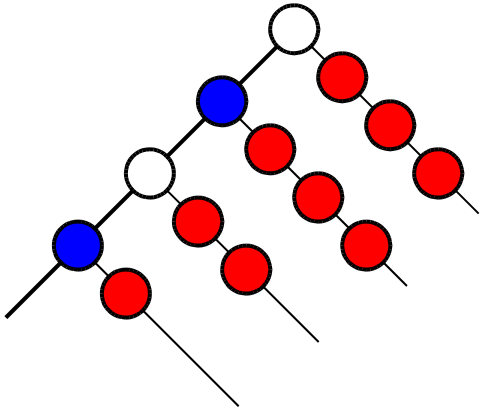
$\forall\ \forall x\ (S(x) \wedge T(x)) = \forall x\ S(x) \wedge \forall x\ T(x))$

$\forall\ \exists x\ (S(x) \vee T(x)) = \exists x\ S(x) \vee \exists x\ T(x))$

Model of Computation



State transition graph
Kripke Structure



Model of Computation (cont'd)

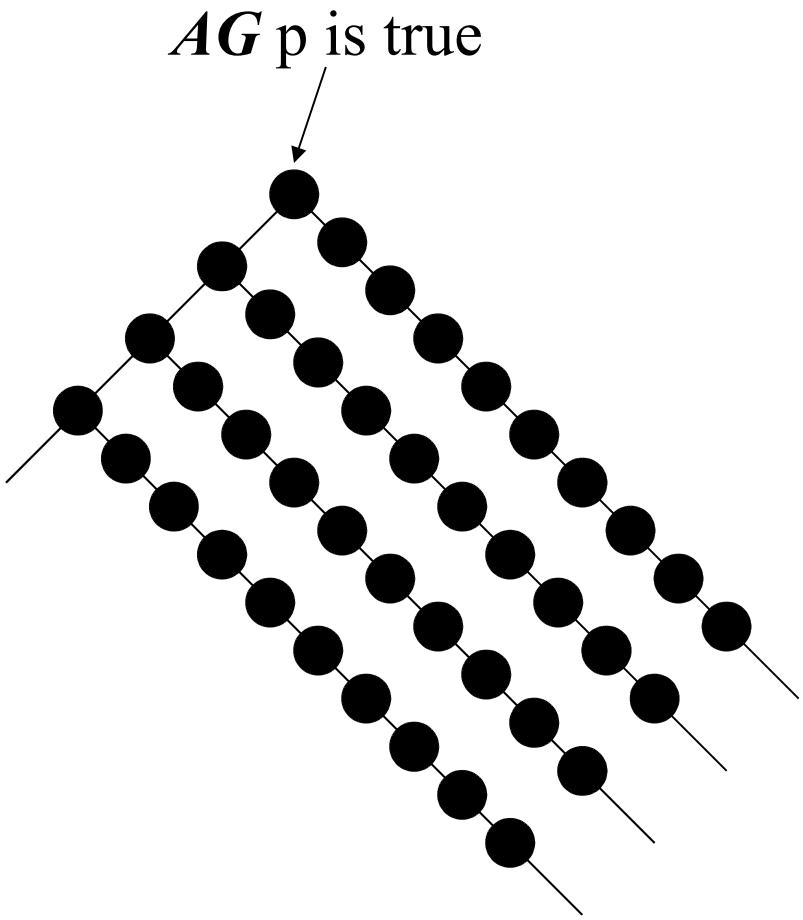
- Kripke Structure $M = (S, R, L, I)$
  - S: finite set of states;
  - $R \subseteq S \times S$: transition relations;
  - L: labeling functions;
  - $I \subseteq S$: Initial states.
- A path = an infinite sequence of states.
  - $\pi = s_0, s_1, s_2, \ldots$
  - Suffix $\pi^1 = s_1, s_2, \ldots$

Computational Tree Logic

- Path qualifiers:
  - ***A***: for every computation path
  - ***E***: for some computation paths
- Temporal qualifiers: ***G, F, X,*** and ***U***.
- Basic Operators: ***AG***, ***AF, AX,*** ***A***(p ***U*** q), ***EG***, ***EF, EX, E***(p ***U*** q),

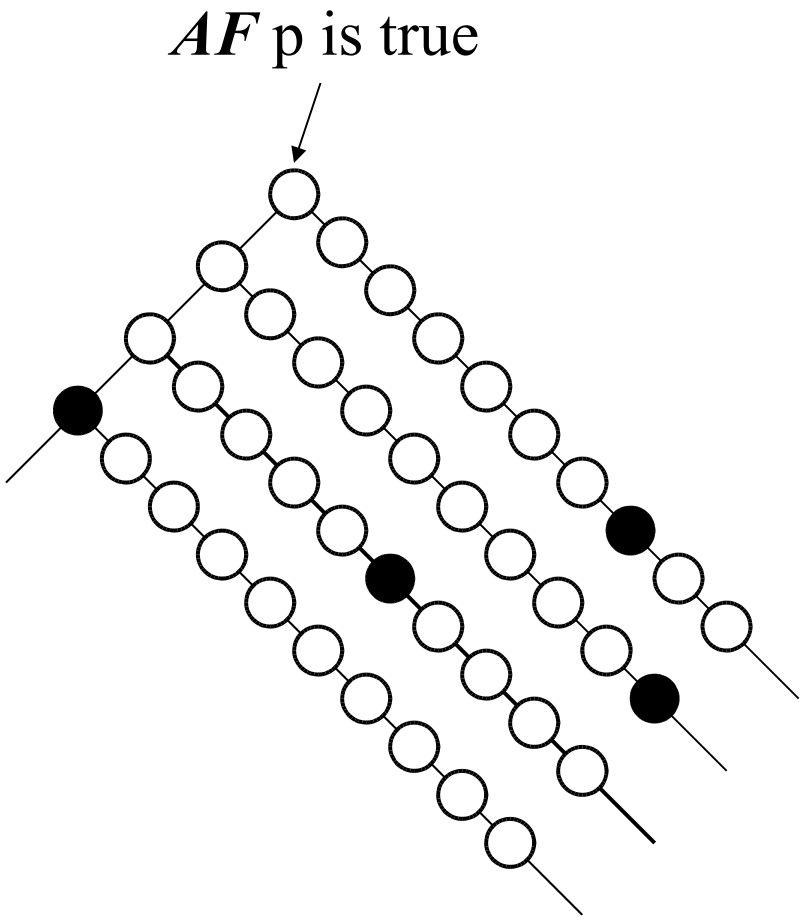
Examples

- ***AG*** p



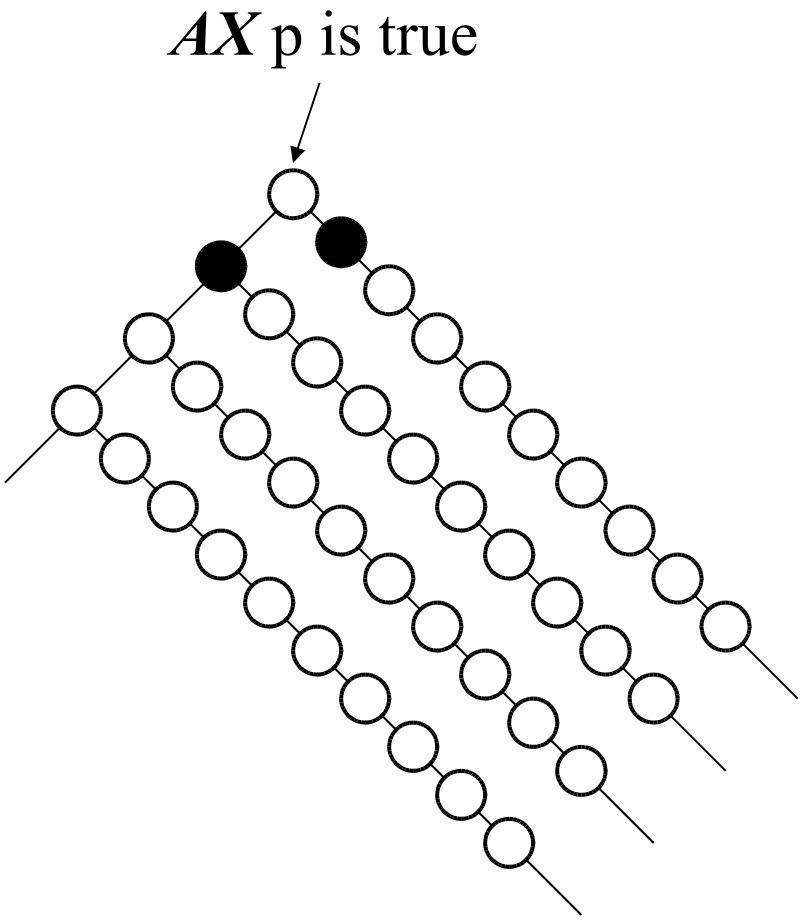
Examples (cont'd)

- ***AF*** p



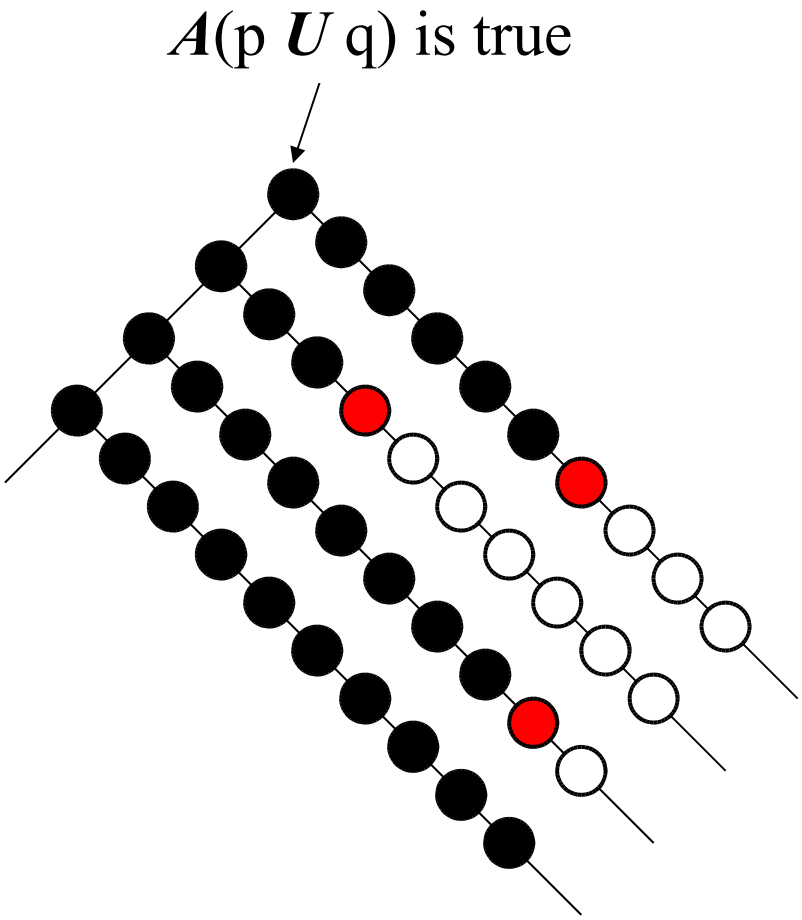
Examples (cont'd)

- ***AX*** p



Examples (cont'd)

- $A(p\ U\ q)$



Some CTL Formulas

- It is possible to reach a state where *start* but *ready* does not hold.
  - $\boldsymbol{EF}\ (start \wedge \neg ready)$
- It is always true that if a *request* occurs, it will be eventually *acknowledged*.
  - $\boldsymbol{AG}\ (request \rightarrow \boldsymbol{AF}\ acknowledged\ )$
- It is always true that if a *request* occurs, it will hold until it is *acknowledged*.
  - $\boldsymbol{AG}\ (request \rightarrow \boldsymbol{A}\ (request\ \boldsymbol{U}\ acknowledged\ ))$

Standard Abbreviation

- $\boldsymbol{A}$ (f) = $\neg\boldsymbol{E}$ ($\neg$f)
- $\boldsymbol{G}$ (f) = $\neg\boldsymbol{F}$ ($\neg$f)
- $\boldsymbol{F}$ (f) = (true $\boldsymbol{U}$ f)

More on CTL Formulas

- $\boldsymbol{AX}\ p = \neg \boldsymbol{EX} \neg p$
- $\boldsymbol{AG}\ p = \neg \boldsymbol{EF} \neg p$
- $\boldsymbol{AF}\ p = \neg \boldsymbol{EG} \neg p$
- $\boldsymbol{A}\ (p\ \boldsymbol{U}\ q) = (\neg \boldsymbol{EG} \neg q) \wedge (\neg \boldsymbol{E}\ (\neg q\ U \neg p \wedge \neg q))$
- All CTL formulas can be expressed using
  - ***EX, E(U), EG.***

CTL Model Checking

- Given a M and a CTL formula f, g, $M, s \models f$
  - $M, s \models f$ iff f is atomic proposition and $f \in L(s)$.
  - $M, s \models \neg f$ iff $M, s \not\models f$.
  - $M, s \models f \vee g$ iff $M, s \models f$ or $M, s \models g$
  - $M, s \models f \wedge g$ iff $M, s \models f$ and $M, s \models g$
  - $M, s \models \mathbf{AX} f$ iff for <u>all</u> s_1 such that $R(s, s_1)$ and $M, s_1 \models f$
  - $M, s \models \mathbf{EX} f$ iff for <u>some</u> s_1 such that $R(s, s_1)$ and $M, s_1 \models f$

CTL Model Checking (cont'd)

- Given a M and a CTL formula f, g, $M, s \models f$
  - $M, s \models \mathbf{AG}\, f$ iff for all paths $s_0 \rightarrow s_1 \rightarrow s_2 \ldots$ such that $s = s_0$ and $M, s_i \models f$ for all $i = 0, 1, 2, \ldots$
  - $M, s \models \mathbf{EG}\, f$ iff for some paths $s_0 \rightarrow s_1 \rightarrow s_2 \ldots$ such that $s = s_0$ and $M, s_i \models f$ for all $i = 0, 1, 2, \ldots$
  - $M, s \models \mathbf{AF}\, f$ iff for all paths $s_0 \rightarrow s_1 \rightarrow s_2 \ldots$ such that $s = s_0$ and $M, s_i \models f$ for some $i = 0, 1, 2, \ldots$
  - $M, s \models \mathbf{EF}\, f$ iff for some paths $s_0 \rightarrow s_1 \rightarrow s_2 \ldots$ such that $s = s_0$ and $M, s_i \models f$ for some $i = 0, 1, 2, \ldots$

CTL Model Checking (cont'd)

- Given a M and a CTL formula f, g, $M, s \models f$
  - $M, s \models \mathbf{A}[f\ \mathbf{U}\ g]$ iff for <u>all</u> paths $s_0 \rightarrow s_1 \rightarrow s_2 \ldots$ such that $s=s_0$ and $M, s_i \models g$ for <u>some</u> $i = 0, 1, 2, \ldots$ and for all $0 \leq k \leq i$ $M, s_k \models g$.
  - $M, s \models \mathbf{E}[f\ \mathbf{U}\ g]$ iff for <u>some</u> paths $s_0 \rightarrow s_1 \rightarrow s_2 \ldots$ such that $s=s_0$ and $M, s_i \models g$ for <u>some</u> $i = 0, 1, 2, \ldots$ and for all $0 \leq k \leq i$ $M, s_k \models g$.

Linear Time Logic

- Computation is a set of paths.
  - Infinite seqences of states.
- LTL formulas:
  - atomic propositions, **true**, **false;**
  - $\neg f, f \wedge g, f \vee g, f \rightarrow g$ where f and g are LTL formulas;
  - $\mathbf{X}f$, $\mathbf{F}f$, $\mathbf{G}f$, $f\ \mathbf{U}\ g$, $f\ \mathbf{W}\ g$, $f\ \mathbf{R}\ g$ where f and g are LTL formulas.
- LTL formulas are evaluated over all the compatation paths.

Semantics of LTL

- Let π be a path, p an atomic formula, and f and g are LTL formulas,
  - $\pi \models$ **true**
  - $\pi \not\models$ **false**
  - $\pi \models p$ iff $p \in L(s_0)$
  - $\pi \models \neg f$ iff $\pi \not\models f$
  - $\pi \models f \wedge g$ iff $\pi \models f$ and $\pi \models g$
  - $\pi \models f \vee g$ iff $\pi \models f$ or $\pi \models g$
  - $\pi \models \mathbf{X}f$ iff $\pi^1 \models f$
  - $\pi \models \mathbf{G}f$ iff $\pi^i \models f$ for all $i \geq 0$.

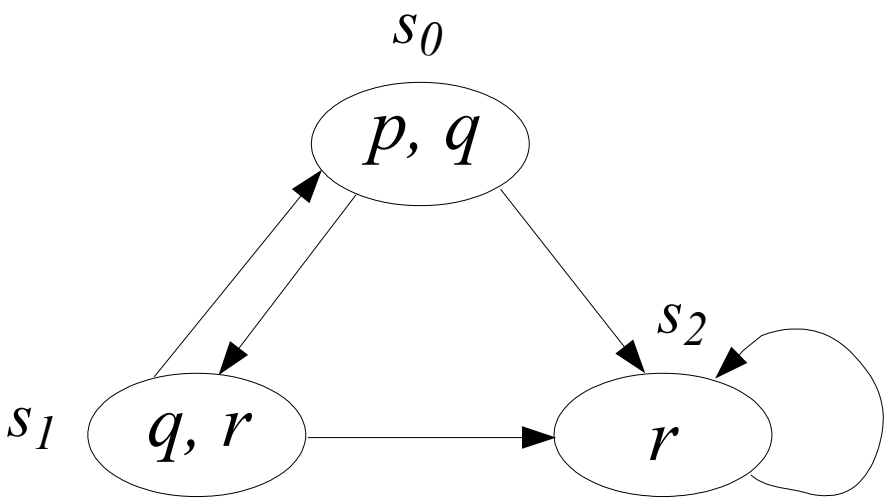
Semantics of LTL (cont'd)

- Let π be a path, p an atomic formula, and f and g are LTL formulas,
  - $\pi \models \mathbf{F}f$ iff $\pi^1 \models f$ for some $i \geq 0$
  - $\pi \models f \mathbf{U} g$ iff $\pi^i \models g$ for a $i \geq 0$ and $\pi^j \models f$ for all $0 \leq j < i$.
  - $\pi \models f \mathbf{W} g$ iff either $\pi^i \models g$ for a $i \geq 0$ and $\pi^j \models f$ for all $0 \leq j < i$, or $\pi^k \models$ f for all $k \geq 0$.
  - $\pi \models f \mathbf{R} g$ iff either $\pi^i \models f$ for a $i \geq 0$ and $\pi^j \models g$ for all $0 \leq j \leq i$, or $\pi^k \models g$ for all $k \geq 0$.
    - equivalent to $\neg(\neg f \ \mathbf{U} \ \neg g)$

LTL Model Checking

- Given a model M, and a LTL formula f, $M, s \models f$ if $\pi \models f$ for all path π starting from s.
-
- If $\pi \models f$ for all paths π starting from all initial states, then $M \models f$.

LTL Semantics Example



$M, s_0 \models p \wedge q$

$M, s_0 \models \mathbf{X}\, r$

$M, s_0 \models \mathbf{G} \neg (p \wedge r)$

$M, s_0 \models \mathbf{G}\, (\mathbf{F}\, p)$

A Sufficient Set of LTL Formulas

- $\mathbf{G}f \equiv \neg\mathbf{F}\neg f$
- $\neg\mathbf{X}f \equiv \mathbf{X}\neg f$
- $f\ \mathbf{R}\ g \equiv \neg(\neg f\ \mathbf{U}\ \neg g)$
- $f\ \mathbf{U}\ g \equiv f\ \mathbf{W}\ g \wedge \mathbf{F}g$
- $\mathbf{F}f \equiv \mathbf{true}\ \mathbf{U}\ f$
- $\{\mathbf{U}, \mathbf{X}\}$, $\{\mathbf{R}, \mathbf{X}\}$, or $\{\mathbf{W}, \mathbf{X}\}$ is surrficient.
- $\mathbf{F}(f \vee g) \equiv \mathbf{F}f\ \vee \mathbf{F}g$
- $\mathbf{G}(f \wedge g) \equiv \mathbf{G}f\ \wedge \mathbf{G}g$