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.
    \( \forall \neg (\text{not}), \land (\text{and}), \lor (\text{or}), \rightarrow (\text{imply}), \leftrightarrow (\text{equivalent}). \)
  – Ex.: \((\neg A \lor B) \leftrightarrow C\)

• Truth of formulas are evaluated bottom-up.
Natural Deduction

• \( f, g \implies f \land g \)
• \( f \land g \implies f, g \)
\( \forall \neg \neg f \implies f \)
• \( f, f \rightarrow g \implies g \)
• \( f \rightarrow g, \neg g \implies \neg f \)
• Question: \( f \rightarrow g \rightarrow h \iff f \rightarrow h \)?
Predicate Logic

• Need richer language constructs.
  – For all, there exist some, etc.

• Predicates enclose propositions with those constructs.
  – $S(Andy) = Andy$ is a student.

\[
\forall \ \forall x \ S(x) \\
\forall \ \exists x \ S(x) \\
\forall \ \forall x \ (S(x) \land T(x)) = \forall x \ S(x) \land \forall x \ T(x) \\
\forall \ \exists x \ (S(x) \lor T(x)) = \exists x \ S(x) \lor \exists x \ T(x)
\]
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)

• $AF\ p$

$AF\ p$ is true
Examples (cont’d)

• $AX \ p$

$AX \ p$ is true
Examples (cont’d)

• $A(p \ U \ q)$

$A(p \ U \ q)$ is true
Some CTL Formulas

• It is possible to reach a state where \textit{start} but \textit{ready} does not hold.
  \[ EF (start \land \neg \text{ready}) \]

• It is always true that if a \textit{request} occurs, it will be eventually \textit{acknowledged}.
  \[ AG (request \rightarrow AF \text{ acknowledged} ) \]

• It is always true that if a \textit{request} occurs, it will hold until it is \textit{acknowledged}.
  \[ AG (request \rightarrow A (request U \text{ acknowledged} )) \]
Standard Abbreviation

- $A(f) = \neg E(\neg f)$
- $G(f) = \neg F(\neg f)$
- $F(f) = (\text{true } U f)$
More on CTL Formulas

• $AX\ p = \neg EX\ \neg p$
• $AG\ p = \neg EF\ \neg p$
• $AF\ p = \neg EG\ \neg p$
• $A\ (p\ U\ q) = (\neg EG\ \neg q) \land (\neg E\ (\neg q\ U\ \neg p\ \land\ \neg q))$
• 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 $M, s \not\models f$.
  - $M, s \models f \lor g$ iff $M, s \models f$ or $M, s \models g$.
  - $M, s \models f \land g$ iff $M, s \models f$ and $M, s \models g$.
  - $M, s \models \text{AX} f$ iff for all $s_1$ such that $R(s, s_1)$ and $M, s_1 \models f$.
  - $M, s \models \text{EX} f$ iff for some $s_1$ such that $R(s, s_1)$ and $M, s_1 \models f$. 
CTL Model Checking (cont'd)

- Given a $M$ and a CTL formula $f, g, M, s \models f$
  - $M, s \models AG f$ 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 $i = 0, 1, 2, \ldots$
  - $M, s \models EG f$ 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 $i = 0, 1, 2, \ldots$
  - $M, s \models AF f$ 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 $i = 0, 1, 2, \ldots$
  - $M, s \models EF f$ 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 $f, g$, $M, s \models f$
  
  - $M, s \models A[f \mathbin{U} g]$ iff for all paths $s_0 \rightarrow s_1 \rightarrow s_2 \ldots$ such that $s = s_0$ and $M, s_i \models g$ for some $i = 0, 1, 2, \ldots$ and for all $0 \leq k \leq i$ $M, s_k \models g$.

  - $M, s \models E[f \mathbin{U} g]$ iff for some paths $s_0 \rightarrow s_1 \rightarrow s_2 \ldots$ such that $s = s_0$ and $M, s_i \models g$ for some $i = 0, 1, 2, \ldots$ and for all $0 \leq k \leq i$ $M, s_k \models g$. 
Linear Time Logic

• Computation is a set of paths.
  – Infinite sequences of states.

• LTL formulas:
  – atomic propositions, \texttt{true}, \texttt{false};
  – $\neg f, f \land g, f \lor g, f \rightarrow g$ where $f$ and $g$ are LTL formulas;
  – $Xf, Ff, Gf, f \mathbf{U} g, f \mathbf{W} g, f \mathbf{R} g$ where $f$ and $g$ are LTL formulas.

• LTL formulas are evaluated over all the computation paths.
Semantics of LTL

• Let \( \pi \) 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 \( \pi \not\models f \)
  
  - \( \pi \models f \land g \) iff \( \pi \models f \) and \( \pi \models g \)
  
  - \( \pi \models f \lor g \) iff \( \pi \models f \) or \( \pi \models g \)
  
  - \( \pi \models Xf \) iff \( \pi^1 \models f \)
  
  - \( \pi \models Gf \) iff \( \pi^i \models f \) for all \( i \geq 0 \).
Semantics of LTL (cont'd)

- Let $\pi$ be a path, $p$ an atomic formula, and $f$ and $g$ are LTL formulas,
  - $\pi \models Ff$ iff $\pi^i \models f$ for some $i \geq 0$
  - $\pi \models f U g$ iff $\pi^i \models g$ for a $i \geq 0$ and $\pi^j \models f$ for all $0 \leq j < i$.
  - $\pi \models f W g$ 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 $k \geq 0$.
  - $\pi \models f R g$ 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 $\neg (\neg f \ U \neg g)$
LTL Model Checking

• Given a model $M$, and a LTL formula $f$, $M, s \models f$ if $\pi \models f$ for all path $\pi$ starting from $s$.

• If $\pi \models f$ for all paths $\pi$ starting from all initial states, then $M \models f$. 
LTL Semantics Example

\[
M, s_0 \models p \land q
\]
\[
M, s_0 \models X r
\]
\[
M, s_0 \models G \neg (p \land r)
\]
\[
M, s_0 \models G (F p)
\]
A Sufficient Set of LTL Formulas

- \( Gf \equiv \neg F \neg f \)
- \( \neg Xf \equiv X \neg f \)
- \( f R g \equiv \neg (\neg f \ U \neg g) \)
- \( f U g \equiv f \ W \ g \land Fg \)
- \( Ff \equiv \text{true} \ U f \)
- \( \{ U, X \}, \{ R, X \}, \text{ or } \{ W, X \} \) is surfficient.
- \( F(f \lor g) \equiv Ff \lor Fg \)
- \( G(f \land g) \equiv Gf \land Gg \)