CS181u Applied Logic & Automated Reasoning

Lecture 7

Transition Systems

Linear Temporal Logic
Next Few Weeks:

Linear Temporal Logic (LTL)
We will assign symbols for expressing temporal system requirements like *always* ($G$), *eventually* ($F$), *next* ($X$), *until* ($U$), and a few more. We will give a formal and unambiguous semantics to these symbols.

Transition Systems
We will learn a formal system of specifying transition systems (which we often depict as a transition diagram).

Concurrency Concepts
Safety, liveness, mutual exclusion, ...

Temporal Logic Software
Symbolic Model Verifier (NuSMV)
Next Few Weeks:

Linear Temporal Logic (LTL)
We will assign symbols for expressing temporal system requirements like always ($G$), eventually ($F$), next ($X$), until ($U$), and a few more. We will give a formal and unambiguous semantics to these symbols.

Transition Systems
We will learn a formal system of specifying transition systems (which we often depict as a transition diagram).

Concurrency Concepts
Safety, liveness, mutual exclusion, …

Temporal Logic Software
Symbolic Model Verifier (NuSMV)
Remember the big picture

Reactive System Code satisfies $\models$ Requirements

Transition System satisfies $\models$ Temporal Logic Formula $\phi$

Model Checking
Actual specifications are subtler than a trip to the grocery store. Programmers may want to write a program that notarizes and time-stamps documents in the order in which they’re received (a useful tool in, say, a patent office). In this case the specification would need to explain that the counter **always increases** (so that a document received later always has a higher number than a document received earlier) and that the program will **never leak the key** it uses to sign the documents.

Kathleen Fisher: Director of the Information Innovation Office at DARPA and former professor of Computer Science at Tufts.
Many important properties have a temporal component.

The light eventually turns green.

The door eventually opens.

Two processes are never in the critical section at the same time.
We will give meaning to temporal logic formulas with respect to transition systems. So, let’s talk about transition systems first.
Transition system for $P_0 \parallel P_1$ from in-class activity.
Transition Systems

A *transition system* \( \mathcal{M} = (S, I, \rightarrow, L) \) is a set of *states* \( S \) and a set of *initial states* \( I \), along with a *transition relation* \( \rightarrow \) and *labelling function* \( L \).

The transition relation \( \rightarrow \) is equivalent to a set of directed graph edges, with the states as nodes.

For example, \( ((n_0, n_1, 0, F, F), (n_0, w_1, 0, F, T)) \in \rightarrow \)

Alternatively, we can write \( (n_0, n_1, 0, F, F) \rightarrow (n_0, w_1, 0, F, T) \).

**Important assumption:** no dead states. Every state has an outgoing transition, even if only to itself.
Transition Systems, execution paths

A path in a transition system $\mathcal{M} = (S, I, \rightarrow, L)$ is an infinite sequence of states $s_1, s_2, s_3, \ldots$ such that $s_1 \in I$ and for every $i \geq 1$, $s_i \rightarrow s_{i+1}$
Transition Systems, execution paths

A path in a transition system $\mathcal{M} = (S, I, \rightarrow, L)$ is an infinite sequence of states $s_1, s_2, s_3, \ldots$ such that $s_1 \in I$ and for every $i \geq 1$, $s_i \rightarrow s_{i+1}$

For example, one path from our two-process mutual exclusion transition diagram:

$((n_0, n_1, 0, F, F), (n_0, w_1, 0, F, T), (n_0, c_1, 0, F, T))^{\omega}$
Transition Systems, execution paths

A path in a transition system $\mathcal{M} = (S, I, \rightarrow, L)$ is an infinite sequence of states $s_1, s_2, s_3, \ldots$ such that $s_1 \in I$ and for every $i \geq 1$, $s_i \rightarrow s_{i+1}$.

For example, one path from our two-process mutual exclusion transition diagram:

$((n_0, n_1, 0, F, F), (n_0, w_1, 0, F, T), (n_0, c_1, 0, F, T))^\omega$

We will use the symbol $\pi$ for paths.

We write $\pi = s_1, s_2, s_3 \ldots$

We write $\pi^i$ to indicate the $i$th suffix of $\pi$.

E.g. $\pi^3 = s_3, s_4, s_5 \ldots$
Transition System Example

\[ S = \{0, 1, 2\} \quad I = \{0\} \quad AP = \{p, q, r\} \]
\[ \rightarrow = \{(0, 1), (1, 0), (0, 2), (1, 2)\} \]
\[ L(0) = \{p, q\} \quad L(1) = \{q, r\} \quad L(2) = \{r\} \]
Transition System Example

\[ S = \{0, 1, 2\} \quad I = \{0\} \quad AP = \{p, q, r\} \]
\[ \rightarrow = \{(0, 1), (1, 0), (0, 2), (1, 2)\} \]
\[ L(0) = \{p, q\} \quad L(1) = \{q, r\} \quad L(2) = \{r\} \]
Syntax of Linear Temporal Logic Formulas

Suppose $\alpha$ and $\beta$ are LTL formulas. Suppose $p_i$ is a propositional atom. Then the following are all LTL formulas.

\[
\top \\
\bot
\]
Syntax of Linear Temporal Logic Formulas

Suppose $\alpha$ and $\beta$ are LTL formulas. Suppose $p_i$ is a propositional atom. Then the following are all LTL formulas.

$\top$

$\bot$

$p_i$
Syntax of Linear Temporal Logic Formulas

Suppose $\alpha$ and $\beta$ are LTL formulas.
Suppose $p_i$ is a propositional atom.
Then the following are all LTL formulas.

- $\top$
- $\bot$
- $p_i$
- $\neg \alpha$
- $\alpha \lor \beta$
- $\alpha \land \beta$
- $\alpha \rightarrow \beta$
Syntax of Linear Temporal Logic Formulas

Suppose $\alpha$ and $\beta$ are LTL formulas.
Suppose $p_i$ is a propositional atom.
Then the following are all LTL formulas.

$\top$
$\bot$
$p_i$
$\neg \alpha$
$\alpha \lor \beta$
$\alpha \land \beta$
$\alpha \rightarrow \beta$
$G\alpha$
$F\alpha$
$X\alpha$
$\alpha U \beta$
$\alpha R \beta$
$\alpha W \beta$
Syntax of Linear Temporal Logic Formulas

Suppose \( \alpha \) and \( \beta \) are LTL formulas.
Suppose \( p_i \) is a propositional atom.
Then the following are all LTL formulas.

\[
\begin{align*}
\top & \\
\bot & \\
p_i & \\
\neg \alpha & \\
\alpha \lor \beta & \\
\alpha \land \beta & \\
\alpha \rightarrow \beta & \\
G \alpha & \\
F \alpha & \\
X \alpha & \\
\alpha U \beta & \\
\alpha R \beta & \\
\alpha W \beta & \\
\end{align*}
\]

Today’s focus
Semantics of Linear Temporal Logic Formulas

Suppose $\pi$ is a path and $p$ and $q$ are LTL formulas.

We write $\pi \models \phi$ to mean that a path satisfies an LTL formula $\phi$. 
Semantics of Linear Temporal Logic Formulas

Suppose \( \pi \) is a path and \( p \) and \( q \) are LTL formulas.

We write \( \pi \models \phi \) to mean that a path satisfies an LTL formula \( \phi \)

\[ \pi \models p \quad \text{iff} \quad p \in L(s_1) \land p \in AP \quad p \text{ holds now} \]
Semantics of Linear Temporal Logic Formulas

Suppose $\pi$ is a path and $p$ and $q$ are LTL formulas.

We write $\pi \models \phi$ to mean that a path satisfies an LTL formula $\phi$

$\pi \models p$ iff $p \in L(s_1) \land p \in AP$ $p$ holds now

$\pi \models \neg p$ iff $\pi \not\models p$ $\neg p$ holds now
Semantics of Linear Temporal Logic Formulas

Suppose $\pi$ is a path and $p$ and $q$ are LTL formulas.

We write $\pi \models \phi$ to mean that a path satisfies an LTL formula $\phi$.

- $\pi \models p$ iff $p \in L(s_1) \land p \in AP$ (p holds now)
- $\pi \models \neg p$ iff $\pi \not\models p$ (\neg p holds now)
- $\pi \models p \land q$ iff $\pi \models p \land \pi \models q$ (p and q hold now)
- $\pi \models p \lor q$ iff $\pi \models p \lor \pi \models q$ (p or q hold now)
Semantics of Linear Temporal Logic Formulas

Suppose $\pi$ is a path and $p$ and $q$ are LTL formulas.

We write $\pi \models \phi$ to mean that a path satisfies an LTL formula $\phi$.

- $\pi \models p$ iff $p \in L(s_1) \land p \in AP$  \hspace{1cm} \text{$p$ holds now}
- $\pi \models \neg p$ iff $\pi \not\models p$  \hspace{1cm} \text{$\neg p$ holds now}
- $\pi \models p \land q$ iff $\pi \models p \land \pi \models q$  \hspace{1cm} \text{$p$ and $q$ hold now}
- $\pi \models p \lor q$ iff $\pi \models p \lor \pi \models q$  \hspace{1cm} \text{$p$ or $q$ hold now}
- $\pi \models Xp$ iff $\pi^2 \models p$  \hspace{1cm} \text{$p$ holds next}
Semantics of Linear Temporal Logic Formulas

Suppose $\pi$ is a path and $p$ and $q$ are LTL formulas.

We write $\pi \models \phi$ to mean that a path satisfies an LTL formula $\phi$.

- $\pi \models p$ iff $p \in L(s_1) \land p \in AP$ (p holds now)
- $\pi \models \neg p$ iff $\pi \not\models p$ (\neg p holds now)
- $\pi \models p \land q$ iff $\pi \models p \land \pi \models q$ (p and q hold now)
- $\pi \models p \lor q$ iff $\pi \models p \lor \pi \models q$ (p or q hold now)
- $\pi \models Xp$ iff $\pi^2 \models p$ (p holds next)
- $\pi \models Gp$ iff $\forall i \geq 1 \ \pi^i \models p$ (p holds always)
Semantics of Linear Temporal Logic Formulas

Suppose $\pi$ is a path and $p$ and $q$ are LTL formulas.

We write $\pi \models \phi$ to mean that a path satisfies an LTL formula $\phi$

\[
\begin{align*}
\pi \models p & \text{ iff } p \in L(s_1) \land p \in AP \\
\pi \models \neg p & \text{ iff } \pi \not\models p \\
\pi \models p \land q & \text{ iff } \pi \models p \land \pi \models q \\
\pi \models p \lor q & \text{ iff } \pi \models p \lor \pi \models q \\
\pi \models Xp & \text{ iff } \pi^2 \models p \\
\pi \models Gp & \text{ iff } \forall i \geq 1 \quad \pi^i \models p \\
\pi \models Fp & \text{ iff } \exists i \geq 1 \quad \pi^i \models p
\end{align*}
\]

$p$ holds now

$\neg p$ holds now

$p$ and $q$ hold now

$p$ or $q$ hold now

$p$ holds next

$p$ holds always

$p$ holds eventually
Semantics of Linear Temporal Logic Formulas

Suppose $\pi$ is a path and $p$ and $q$ are LTL formulas. We write $\pi \models \phi$ to mean that a path satisfies an LTL formula $\phi$

$\pi \models p$ iff $p \in L(s_1) \land p \in AP$ \hspace{1cm} $p$ holds now

$\pi \models \neg p$ iff $\pi \not\models p$ \hspace{1cm} $\neg p$ holds now

$\pi \models p \land q$ iff $\pi \models p \land \pi \models q$ \hspace{1cm} $p$ and $q$ hold now

$\pi \models p \lor q$ iff $\pi \models p \lor \pi \models q$ \hspace{1cm} $p$ or $q$ hold now

$\pi \models Xp$ iff $\pi^2 \models p$ \hspace{1cm} $p$ holds next

$\pi \models Gp$ iff $\forall i \geq 1 \hspace{1cm} \pi^i \models p$ \hspace{1cm} $p$ holds always

$\pi \models Fp$ iff $\exists i \geq 1 \hspace{1cm} \pi^i \models p$ \hspace{1cm} $p$ holds eventually

$\pi \models pUq$ iff $\exists i \geq 1 \hspace{1cm} \pi^i \models q \land \forall 1 \leq j < i \hspace{1cm} \pi^j \models p$ \hspace{1cm} $p$ holds until $q$ holds
We just defined what it means for a path to satisfy a property, $\pi \models \phi$. 
We just defined what it means for a path to satisfy a property, $\pi \models \phi$.

Now, let’s define what it means for a transition system to satisfy a property, $M \models \phi$. 
We just defined what it means for a path to satisfy a property, $\pi \models \phi$.

Now, let's define what it means for a transition system to satisfy a property, $M \models \phi$.

We say that transition system $M$ satisfies property $\phi$ if for every path $\pi$ of $M$, $\pi \models \phi$. 
Semantics of Linear Temporal Logic Formulas

We just defined what it means for a path to satisfy a property, $\pi \models \phi$.

Now, let’s define what it means for a transition system to satisfy a property, $\mathcal{M} \models \phi$.

We say that transition system $\mathcal{M}$ satisfies property $\phi$ if for every path $\pi$ of $\mathcal{M}$, $\pi \models \phi$.

$LTL \text{ Model Checking}$
Semantics of Linear Temporal Logic Formulas

LTL Model Checking

\[ M \models \phi \iff \forall \pi \ [\pi \models \phi] \]
Semantics of Linear Temporal Logic Formulas

LTL Model Checking

$\mathcal{M} \models \phi \iff \forall \pi \ [\pi \models \phi]$

$\mathcal{M} \not\models \phi \iff \exists \pi \ [\pi \models \neg \phi]$

Counterexample path!
Some exercises

Does $G$ distribute over $\lor$?

\[ G(p \lor q) \equiv Gp \lor Gq \]?
Some exercises

Does $G$ distribute over $\lor$?

$$G(p \lor q) \equiv Gp \lor Gq$$

Does $G$ distribute over $\land$?

$$G(p \land q) \equiv Gp \land Gq$$
Some exercises

Does $G$ distribute over $\lor$?

\[ G(p \lor q) \equiv Gp \lor Gq \ ? \]

Does $G$ distribute over $\land$?

\[ G(p \land q) \equiv Gp \land Gq \ ? \]

Does $F$ distribute over $\lor$?

\[ F(p \lor q) \equiv Fp \lor Fq \ ? \]

Does $F$ distribute over $\land$?

\[ F(p \land q) \equiv Fp \land Fq \ ? \]
Some exercises

Does $G$ distribute over $\lor$?

$G(p \lor q) \equiv Gp \lor Gq$ ?

Does $G$ distribute over $\land$?

$G(p \land q) \equiv Gp \land Gq$ ?

Does $F$ distribute over $\lor$?

$F(p \lor q) \equiv Fp \lor Fq$ ?

Does $F$ distribute over $\land$?

$F(p \land q) \equiv Fp \land Fq$ ?

Do $U$ and $X$ have any distributive properties?

$X(p \lor q) \equiv \ldots$ \hspace{1cm} $(p \land q)U(r \land t) \equiv \ldots$
Some exercises

Do $G$ and $F$ commute?

$$FGp \equiv GFp$$
Some exercises

Do $G$ and $F$ commute?

$$FGp \equiv GFp \ ?$$

$FGp \ M \text{ converges to } p$

$GFp \ \text{infinitely often } p$
Transition System Example

Do these properties hold?
Transition System Example

Do these properties hold?

\[ \mathcal{M} \models p \land q \]
Transition System Example

Do these properties hold?

\[ \mathcal{M} \models p \land q \]

\[ \mathcal{M} \models \neg r \]
Transition System Example

Do these properties hold?

\( \mathcal{M} \models p \land q \)
\( \mathcal{M} \models \neg r \)
\( \mathcal{M} \models Xr \)
Transition System Example

Do these properties hold?

\[ M \models p \land q \]
\[ M \models \neg r \]
\[ M \models Xr \]
\[ M \models X(q \land r) \]
Transition System Example

Do these properties hold?

\[ M \models p \land q \]
\[ M \models \neg r \]
\[ M \models Xr \]
\[ M \models X(q \land r) \]
\[ M \models G\neg(p \land r) \]
Transition System Example

Do these properties hold?

\[ M \models p \land q \]
\[ M \models \neg r \]
\[ M \models Xr \]
\[ M \models X(q \land r) \]
\[ M \models \neg(p \land r) \]
\[ M \models GFp \]
Transition System Example

Do these properties hold?

\[ M \models p \land q \]

\[ M \models \neg r \]

\[ M \models Xr \]

\[ M \models X(q \land r) \]

\[ M \models \neg(p \land r) \]

\[ M \models GFp \]

\[ M \models F(\neg q \land r) \Rightarrow FGr \]
Transition System Example

Do these properties hold?

\[ \mathcal{M} \models p \land q \]

\[ \mathcal{M} \models \neg r \]

\[ \mathcal{M} \models Xr \]

\[ \mathcal{M} \models X(q \land r) \]

\[ \mathcal{M} \models G\neg(p \land r) \]

\[ \mathcal{M} \models GFp \]

\[ \mathcal{M} \models F(\neg q \land r) \Rightarrow FGr \]

\[ \mathcal{M} \models GFp \Rightarrow GFr \]
Transition System Example

Do these properties hold?

\[ M \models p \land q \]
\[ M \models \neg r \]
\[ M \models Xr \]
\[ M \models X(q \land r) \]
\[ M \models G\neg(p \land r) \]
\[ M \models GFp \]
\[ M \models F(\neg q \land r) \Rightarrow FGr \]
\[ M \models GFp \Rightarrow GFr \]
\[ M \models GFr \Rightarrow GFp \]
Linear Temporal Logic (LTL)
We will assign symbols for expressing temporal system requirements like *always* \((G)\), *eventually* \((F)\), *next* \((X)\), *until* \((U)\), and a few more. We will give a formal and unambiguous semantics to these symbols.

Transition Systems
We will learn a formal system of specifying transition systems (which we often depict as a transition diagram).

Concurrency Concepts
Safety, liveness, mutual exclusion, …

Verification Software
Symbolic Model Verifier (NuSMV)
Linear Temporal Logic (LTL)
We will assign symbols for expressing temporal system requirements like always \((G)\), eventually \((F)\), next \((X)\), until \((U)\), and a few more. We will give a formal and unambiguous semantics to these symbols.

Transition Systems
We will learn a formal system of specifying transition systems (which we often depict as a transition diagram).

Concurrency Concepts
Safety, liveness, mutual exclusion, …

Verification Software
Symbolic Model Verifier (NuSMV)