Formal Verification

Lecture 2: Linear Temporal Logic

Jacques Fleuriot
jdf@inf.ed.ac.uk

Recap

- Previously:
  - Model Checking, and an informal introduction to LTL
- This time: Linear Temporal Logic
  - Syntax
  - Semantics
  - Equivalences

LTL – Syntax

LTL = Linear(-time) Temporal Logic

Assume some set *Atom* of atomic propositions

Syntax of LTL formulas ϕ:

$$\phi ::= p \mid \neg\phi \mid \phi \vee \phi \mid \phi \wedge \phi \mid \phi \rightarrow \phi \mid \mathbf{X}\phi \mid \mathbf{F}\phi \mid \mathbf{G}\phi \mid \phi\mathbf{U}\phi$$

where $p \in Atom$.

Pronunciation:

- $\mathbf{X}\phi$ – neXt ϕ
- $\mathbf{F}\phi$ – Future ϕ
- $\mathbf{G}\phi$ – Globally ϕ
- $\phi\mathbf{U}\psi$ – ϕ Until ψ

Other common connectives: **W** (weak until), **R** (release).

Precedence high-to-low: $(\mathbf{X}, \mathbf{F}, \mathbf{G}, \neg)$, $(\mathbf{U})$, $(\wedge, \vee)$, $\rightarrow$.

- E.g. Write $\mathbf{F}p \wedge \mathbf{G}q \rightarrow p\,\mathbf{U}\,r$ instead of $((\mathbf{F}p) \wedge (\mathbf{G}q)) \rightarrow (p\,\mathbf{U}\,r)$.

LTL – Informal Semantics

LTL formulas are evaluated at a position i along a path π through the system (a path is a sequence of states connected by transitions)

- An atomic p holds if p is true the state at position i.
- The propositional connectives $\neg, \wedge, \vee, \rightarrow$ have their usual meanings.
- Meaning of LTL connectives:
  - $\mathbf{X}\phi$ holds if ϕ holds at the next position;
  - $\mathbf{F}\phi$ holds if there exists a future position where ϕ holds;
  - $\mathbf{G}\phi$ holds if, for all future positions, ϕ holds;
  - $\phi\mathbf{U}\psi$ holds if there is a future position where ψ holds, and ϕ holds for all positions prior to that.
  - $\phi\mathbf{R}\psi$ holds if there is a future position where ϕ becomes true, and ψ holds for all positions prior to and including that i.e. ϕ 'releases' ψ.
    - It is equivalent to $\neg(\neg\phi\mathbf{U}\neg\psi)$.
    - Thus $\mathbf{R}$ is the dual of $\mathbf{U}$.

This will be made more formal in the next few slides.

LTL – Formal Semantics: Transition Systems and Paths

Definition (Transition System)

A *transition system* (or model) $\mathcal{M} = \langle S, \rightarrow, L\rangle$ consists of:

$$\begin{array}{cl} S & \text{a finite set of states} \\ \rightarrow \subseteq S \times S & \text{transition relation} \\ L : S \rightarrow \mathcal{P}(Atom) & \text{a labelling function} \end{array}$$

such that $\forall s_1 \in S.\ \exists s_2 \in S.\ s_1 \rightarrow s_2$

Note: $Atom$ is a fixed set of atomic propositions, $\mathcal{P}(Atom)$ is the powerset of $Atom$.

Thus, $L(s)$ is just the set of atomic propositions that is true in state s.

Definition (Path)

A *path* π in a transition system $\mathcal{M} = \langle S, \rightarrow, L\rangle$ is an infinite sequence of states $s_0, s_1, \ldots$ such that $\forall i \geq 0.\ s_i \rightarrow s_{i+1}$.

Paths are written as: $\pi = s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \ldots$

LTL – Formal Semantics: Satisfaction by Path

Satisfaction: $\pi \models^i \phi$ – "path at position i satisfies formula ϕ"

$$
\begin{array}{ll}
\pi \models^i \top & \\
\pi \not\models^i \bot & \\
\pi \models^i p & \text{iff } p \in L(s_i) \\
\pi \models^i \neg\phi & \text{iff } \pi \not\models^i \phi \\
\pi \models^i \phi \wedge \psi & \text{iff } \pi \models^i \phi \text{ and } \pi \models^i \psi \\
\pi \models^i \phi \vee \psi & \text{iff } \pi \models^i \phi \text{ or } \pi \models^i \psi \\
\pi \models^i \phi \rightarrow \psi & \text{iff } \pi \models^i \phi \text{ implies } \pi \models^i \psi \\
\pi \models^i \mathbf{X}\, \phi & \text{iff } \pi \models^{i+1} \phi \\
\pi \models^i \mathbf{F}\, \phi & \text{iff } \exists j \geq i.\ \pi \models^j \phi \\
\pi \models^i \mathbf{G}\, \phi & \text{iff } \forall j \geq i.\ \pi \models^j \phi \\
\pi \models^i \phi_1\ \mathbf{U}\ \phi_2 & \text{iff } \exists j \geq i.\ \pi \models^j \phi_2 \text{ and } \forall k \in \{i..j-1\}.\ \pi \models^k \phi_1 \\
\pi \models^i \phi_1\ \mathbf{R}\ \phi_2 & \text{iff } (\forall j \geq i.\ \pi \models^j \phi_2) \text{ or} \\
& \quad (\exists j \geq i.\ \pi \models^j \phi_1 \text{ and } \forall k \in \{i..j\}.\ \pi \models^k \phi_2)
\end{array}
$$

LTL – Formal Semantics: Alternative Satisfaction by Path

Alternatively, we can define $\pi \models \phi$ using the notion of ith suffix $\pi^i = s_i \to s_{i+1} \to \ldots$ of a path $\pi = s_0 \to s_1 \to \ldots$.

For example, the alternative definition of satisfaction for G would be:

$$\pi \models \mathbf{G}\,\phi \qquad \text{iff} \qquad \forall j \geq 0.\ \pi^j \models \phi$$

instead of

$$\pi \models^0 \mathbf{G}\,\phi \qquad \text{iff} \qquad \forall j \geq 0.\ \pi \models^j \phi$$

Satisfaction in terms of $\models$ for the other connectives is left as an exercise.

- $\pi \models^i \phi$ is better for understanding, and needed for past-time operators.
- $\pi \models \phi$ is needed for the semantics of branching-time logics, like CTL.

LTL Semantics: Satisfaction by a Model

For a model $\mathcal{M}$, we write

$$\mathcal{M}, s \models \phi$$

if, for **every** execution path $\pi \in \mathcal{M}$ starting at state s, we have

$$\pi \models^0 \phi$$

A Taste of LTL – Examples

1. $\pi \models^i \mathbf{G}\ \mathit{invariant}$

   invariant is true for all future positions

   $\forall j \geq i.\ \pi \models^j \mathit{invariant}$

   $\forall j \geq i.\ \mathit{invariant} \in L(s_j)$

A Taste of LTL – Examples

1. $\pi \models^i \mathbf{G}\ \mathit{invariant}$

   invariant is true for all future positions

   $\forall j \geq i.\ \pi \models^j \mathit{invariant}$

   $\forall j \geq i.\ \mathit{invariant} \in L(s_j)$

2. $\pi \models^i \mathbf{G}\ \neg(\mathit{read} \wedge \mathit{write})$

   In all future positions, it is not the case that *read* and *write*

   $\forall j \geq i.\ \mathit{read} \notin L(s_j) \vee \mathit{write} \notin L(s_j)$

A Taste of LTL – Examples

1. $\pi \models^i \mathbf{G}\ invariant$

   invariant is true for all future positions

   $\forall j \geq i.\ \pi \models^j invariant$

   $\forall j \geq i.\ invariant \in L(s_j)$

2. $\pi \models^i \mathbf{G}\ \neg(read \wedge write)$

   In all future positions, it is not the case that *read* and *write*

   $\forall j \geq i.\ read \notin L(s_j) \vee write \notin L(s_j)$

3. $\pi \models^i \mathbf{G}(request \rightarrow \mathbf{F}grant)$

   At every position in the future, a *request* implies that there exists a future point where *grant* holds.

   $\forall j \geq i.\ request \in L(s_j)$ implies $\exists k \geq j.\ grant \in L(s_k)$.

A Taste of LTL – Examples

1. $\pi \models^i \mathbf{G}\ \mathit{invariant}$

   invariant is true for all future positions

   $\forall j \geq i.\ \pi \models^j \mathit{invariant}$

   $\forall j \geq i.\ \mathit{invariant} \in L(s_j)$

2. $\pi \models^i \mathbf{G}\ \neg(\mathit{read} \wedge \mathit{write})$

   In all future positions, it is not the case that *read* and *write*

   $\forall j \geq i.\ \mathit{read} \notin L(s_j) \vee \mathit{write} \notin L(s_j)$

3. $\pi \models^i \mathbf{G}(\mathit{request} \rightarrow \mathbf{F}\mathit{grant})$

   At every position in the future, a *request* implies that there exists a future point where *grant* holds.

   $\forall j \geq i.\ \mathit{request} \in L(s_j)$ implies $\exists k \geq j.\ \mathit{grant} \in L(s_k)$.

4. $\pi \models^i \mathbf{G}(\mathit{request} \rightarrow (\mathit{request}\ \mathbf{U}\ \mathit{grant}))$

   At every position in the future, a *request* implies that there exists a future point where *grant* holds, and *request* holds up until that point.

   $\forall j \geq i.\ \mathit{request} \in L(s_j)$ implies

   $\exists k \geq j.\ \mathit{grant} \in L(s_k)$ and $\forall l \in \{j, k-1\}.\ \mathit{request} \in L(s_l)$.

LTL Equivalences 1

$$\phi \equiv \psi \quad \doteq \quad \forall \mathcal{M}. \forall \pi \in \mathcal{M}. \forall i.\, \pi \models^i \phi \leftrightarrow \pi \models^i \psi$$

LTL Equivalences 1

$$\phi \equiv \psi \quad \doteq \quad \forall \mathcal{M}. \forall \pi \in \mathcal{M}. \forall i.\, \pi \models^i \phi \leftrightarrow \pi \models^i \psi$$

Dualities from Propositional Logic:

$$\neg(\phi \wedge \psi) \equiv \neg\phi \vee \neg\psi \qquad \neg(\phi \vee \psi) \equiv \neg\phi \wedge \neg\psi$$

LTL Equivalences 1

$$\phi \equiv \psi \quad \doteq \quad \forall \mathcal{M}. \forall \pi \in \mathcal{M}. \forall i.\, \pi \models^i \phi \leftrightarrow \pi \models^i \psi$$

Dualities from Propositional Logic:

$$\neg(\phi \wedge \psi) \equiv \neg\phi \vee \neg\psi \qquad \neg(\phi \vee \psi) \equiv \neg\phi \wedge \neg\psi$$

Dualities from LTL:

$$\neg \mathbf{X}\phi \equiv \mathbf{X}\neg\phi \qquad \neg \mathbf{G}\phi \equiv \mathbf{F}\neg\phi \qquad \neg \mathbf{F}\phi \equiv \mathbf{G}\neg\phi$$

$$\neg(\phi \;\mathbf{U}\; \psi) \equiv \neg\phi \;\mathbf{R}\; \neg\psi \qquad \neg(\phi \;\mathbf{R}\; \psi) \equiv \neg\phi \;\mathbf{U}\; \neg\psi$$

LTL Equivalences 1

$$\phi \equiv \psi \quad \doteq \quad \forall \mathcal{M}. \forall \pi \in \mathcal{M}. \forall i.\, \pi \models^i \phi \leftrightarrow \pi \models^i \psi$$

Dualities from Propositional Logic:

$$\neg(\phi \wedge \psi) \equiv \neg\phi \vee \neg\psi \qquad \neg(\phi \vee \psi) \equiv \neg\phi \wedge \neg\psi$$

Dualities from LTL:

$$\neg\mathbf{X}\phi \equiv \mathbf{X}\neg\phi \qquad \neg\mathbf{G}\phi \equiv \mathbf{F}\neg\phi \qquad \neg\mathbf{F}\phi \equiv \mathbf{G}\neg\phi$$

$$\neg(\phi\ \mathbf{U}\ \psi) \equiv \neg\phi\ \mathbf{R}\ \neg\psi \qquad \neg(\phi\ \mathbf{R}\ \psi) \equiv \neg\phi\ \mathbf{U}\ \neg\psi$$

Distributive laws:

$$\mathbf{G}(\phi \wedge \psi) \equiv \mathbf{G}\phi \wedge \mathbf{G}\psi \qquad \mathbf{F}(\phi \vee \psi) \equiv \mathbf{F}\phi \vee \mathbf{F}\psi$$

LTL Equivalences 2

Inter-definitions:

$$\mathbf{F}\phi \equiv \neg\mathbf{G}\neg\phi \qquad \mathbf{G}\phi \equiv \neg\mathbf{F}\neg\phi \qquad \mathbf{F}\phi \equiv \top \ \mathbf{U}\ \phi \qquad \mathbf{G}\phi \equiv \bot \ \mathbf{R}\ \phi$$

LTL Equivalences 2

Inter-definitions:

$$\mathbf{F}\phi \equiv \neg\mathbf{G}\neg\phi \qquad \mathbf{G}\phi \equiv \neg\mathbf{F}\neg\phi \qquad \mathbf{F}\phi \equiv \top\ \mathbf{U}\ \phi \qquad \mathbf{G}\phi \equiv \bot\ \mathbf{R}\ \phi$$

Idempotency:

$$\mathbf{FF}\phi \equiv \mathbf{F}\phi \qquad \mathbf{GG}\phi \equiv \mathbf{G}\phi$$

LTL Equivalences 2

Inter-definitions:

$$\mathbf{F}\phi \equiv \neg\mathbf{G}\neg\phi \qquad \mathbf{G}\phi \equiv \neg\mathbf{F}\neg\phi \qquad \mathbf{F}\phi \equiv \top\ \mathbf{U}\ \phi \qquad \mathbf{G}\phi \equiv \bot\ \mathbf{R}\ \phi$$

Idempotency:

$$\mathbf{FF}\phi \equiv \mathbf{F}\phi \qquad \mathbf{GG}\phi \equiv \mathbf{G}\phi$$

Weak and strong until:

$$\phi\ \mathbf{W}\ \psi \equiv \phi\ \mathbf{U}\ \psi \vee \mathbf{G}\phi \qquad \phi\ \mathbf{U}\ \psi \equiv \phi\ \mathbf{W}\ \psi \wedge \mathbf{F}\psi$$

LTL Equivalences 2

Inter-definitions:

$$\mathbf{F}\phi \equiv \neg\mathbf{G}\neg\phi \qquad \mathbf{G}\phi \equiv \neg\mathbf{F}\neg\phi \qquad \mathbf{F}\phi \equiv \top\ \mathbf{U}\ \phi \qquad \mathbf{G}\phi \equiv \bot\ \mathbf{R}\ \phi$$

Idempotency:

$$\mathbf{FF}\phi \equiv \mathbf{F}\phi \qquad \mathbf{GG}\phi \equiv \mathbf{G}\phi$$

Weak and strong until:

$$\phi\ \mathbf{W}\ \psi \equiv \phi\ \mathbf{U}\ \psi \lor \mathbf{G}\phi \qquad \phi\ \mathbf{U}\ \psi \equiv \phi\ \mathbf{W}\ \psi \land \mathbf{F}\psi$$

Some more surprising equivalences:

$$\mathbf{GFG}\phi \equiv \mathbf{FG}\phi \qquad \mathbf{FGF}\phi \equiv \mathbf{GF}\phi \qquad \mathbf{G}(\mathbf{F}\phi \lor \mathbf{F}\psi) \equiv \mathbf{GF}\phi \lor \mathbf{GF}\psi$$

Summary

- Introduction to Model Checking (H&R 3.2)
  - Semantics of LTL
- Next time:
  - Introduction to NuSMV