Linear Temporal Logic[1]

Paul Jackson
Paul.Jackson@ed.ac.uk

University of Edinburgh

Formal Verification
Autumn 2023

[1] Including contributions by Jacques Fleuriot and Bob Atkey

LTL Syntax

Syntax of LTL formulas ϕ:

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

where $p \in$ Atom and Atom is a set of atomic propositions

Temporal operators are

X	NeXt	$\bigcirc$
G	Globally	$\Box$
F	Future	$\Diamond$
U	Until	

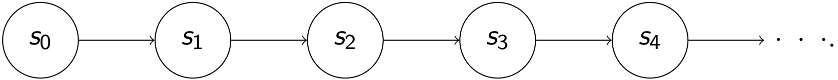
Other temporal operators include **W**(Weak until) and **R**(Release)

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

- So $\mathbf{F}\,p \wedge \mathbf{G}\,q \Rightarrow \neg p\,\mathbf{U}\,r$ means $((\mathbf{F}\,p) \wedge (\mathbf{G}\,q)) \Rightarrow ((\neg p)\,\mathbf{U}\,r)$

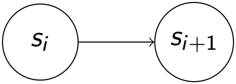
Meaning of LTL Operators

LTL Operators are considered either to hold or not hold at each position on an execution path



of a transition-system model.

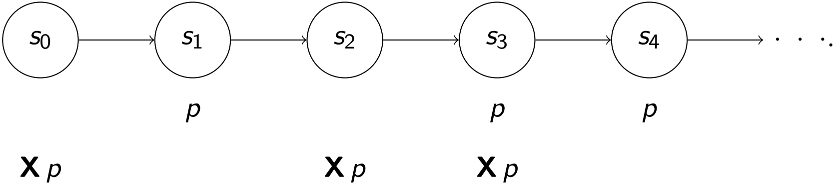
Here, the s_i are the successive states of the path, and



indicates a transition in one step from state s_i to state s_{i+1}.

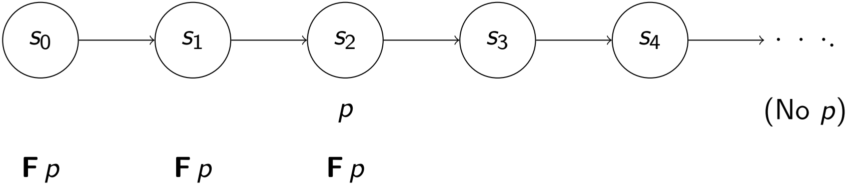
X – Next

X ϕ holds at a position if ϕ holds at the next position



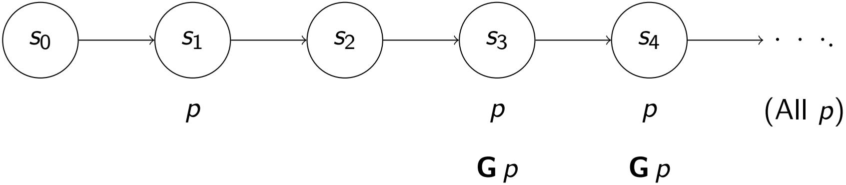
F – Future

F ϕ holds at a position if ϕ holds at some future position (including the current position)



G – Globally

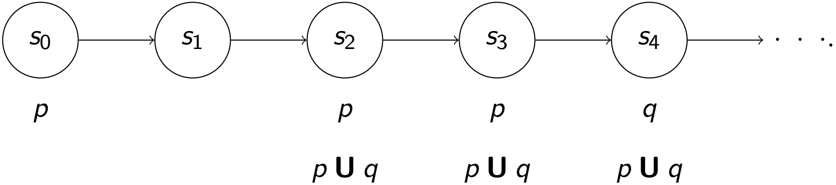
G ϕ holds at a position if ϕ holds at all positions in the future (including the current position)



U – Until

ϕ **U** ψ holds at some position if

1. ψ holds at some future position (including current position), and
2. ϕ holds at all positions from current position up to just before where ψ holds



LTL Formula Examples

1. $\mathbf{G}\,\mathrm{invar}$
   'invar' is always true (is an invariant)

2. $\mathbf{G}\,\neg(\mathrm{read} \wedge \mathrm{write})$
   'read' and 'write' are never asserted at the same time

3. $\mathbf{G}\,(\mathrm{request} \Rightarrow \mathbf{F}\,\mathrm{grant})$
   If 'request' is asserted, then eventually 'grant' is asserted

4. $\mathbf{G}\,(\mathrm{request} \Rightarrow (\mathrm{request}\,\mathbf{U}\,\mathrm{grant}))$
   If 'request' is asserted, then eventually 'grant' is asserted, and, up until then, 'request' continues to be asserted

More LTL Formula Examples

5. $\mathbf{F}\,(\text{open} \wedge \mathbf{X}\,\mathbf{F}\,\text{close})$
   At some time in the future ‘open’ is asserted, and then at some time further, at least one step further, ‘close’ is asserted

6. $\mathbf{G}\,\mathbf{F}$ enabled
   ‘enable’ is infinitely-often asserted

7. $\mathbf{F}\,\mathbf{G}$ stable
   'stable’ is eventually always asserted

LTL Semantics 1: Transition Systems and Paths

Definition (Transition System)

A transition system $\mathcal{M} = \langle S, \rightarrow, L, I \rangle$ consists of

S			set of states
$\rightarrow$	$\subseteq$	$S \times S$	transition relation
L	$:$	$S \rightarrow \mathcal{P}(\mathrm{Atom})$	labelling function
I	$\subseteq$	S	set of initial states (*sometimes*)

such that $\forall s. \exists t. \ s \rightarrow t$.

Definition (Path)

A path π in a model $\mathcal{M} = \langle S, \rightarrow, L, I \rangle$ is an infinite sequence of states $s_0, s_1, \ldots$ such that $s_0 \in I$ and $\forall i \geq 0. \ s_i \rightarrow s_{i+1}$.
We write the path as $s_0 \rightarrow s_1 \rightarrow \ldots$.

LTL Semantics 2: Satisfaction by Path

Satisfaction relation $\pi \models^i \phi$ read as

"path π at position i satisfies LTL formula ϕ".

$\pi \models^i \top$		
$\pi \not\models^i \bot$		
$\pi \models^i p$	iff	$p \in L(s_i)$
$\pi \models^i \neg\phi$	iff	$\pi \not\models^i \phi$
$\pi \models^i \phi \wedge \psi$	iff	$\pi \models^i \phi$ and $\pi \models^i \psi$
$\pi \models^i \phi \vee \psi$	iff	$\pi \models^i \phi$ or $\pi \models^i \psi$
$\pi \models^i \phi \Rightarrow \psi$	iff	$\pi \models^i \phi$ implies $\pi \models^i \psi$
$\pi \models^i \mathbf{X}\,\phi$	iff	$\pi \models^{i+1} \phi$
$\pi \models^i \mathbf{F}\,\phi$	iff	$\exists j \geq i.\ \pi \models^j \phi$
$\pi \models^i \mathbf{G}\,\phi$	iff	$\forall j \geq i.\ \pi \models^j \phi$
$\pi \models^i \phi\,\mathbf{U}\,\psi$	iff	$\exists j \geq i.\ \pi \models^j \psi$ and $\forall k \in \{i..j-1\}.\ \pi \models^k \phi$

LTL Semantics 3: Alternative Satisfaction by Path

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

E.g. write

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

instead of

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

- $\pi \models^i \phi$ better for understanding and needed for past time operators.
- $\pi \models \phi$ needed for semantics of CTL branching-time temporal logic.

LTL Semantics 4: Satisfaction by Model

We write

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

if, for every execution path π of model $\mathcal{M}$ starting at state s, we have

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

.

We write

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

if, for every state s in the set of initial states of model $\mathcal{M}$, we have $\mathcal{M}, s \models \phi$.

Understanding Formulas

Expand formulas by using semantics: e.g.

$$\pi \models^0 \mathbf{F}\,\mathbf{G}\ \text{stable} \ \equiv\ \exists i \geq 0.\ \forall j \geq i.\ \text{stable} \in L(s_j)$$

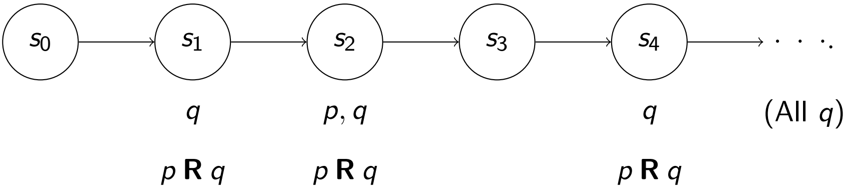
Exercise: expand the rest of the example formulas a few slides back.

R – Release

ϕ **R** ψ holds at a position, if either

1. ψ holds for ever from that position onwards, or
2.
   a. ϕ holds at some future position, and
   b. ψ holds from the current position to up to and including when ϕ holds

ϕ releases ψ

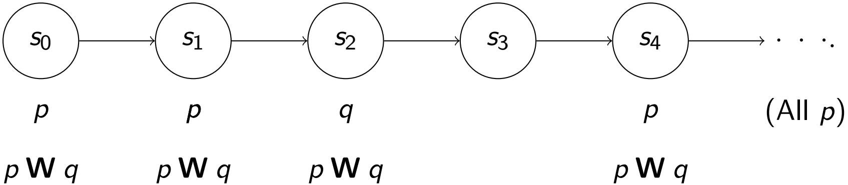


$$\pi \models^i \phi \, \mathbf{R} \, \psi \quad \text{iff} \quad (\forall j \geq i.\ \pi \models^j \psi) \text{ or}$$
$$\exists k \geq i.\ \pi \models^k \phi \text{ and } \forall j \in \{i..k\}.\ \pi \models^j \psi$$

W – Weak Until

$\phi\,\mathbf{W}\,\psi$ holds at a position, if either

1. $\phi\,\mathbf{U}\,\psi$ holds there, or
2. $\mathbf{G}\,\phi$ holds there



$$\pi \models^i \phi\,\mathbf{W}\,\psi \quad \text{iff} \quad \begin{array}{l} (\forall j \geq i.\ \pi \models^j \phi) \text{ or} \\ \exists k \geq i.\ \pi \models^k \psi \text{ and } \forall j \in \{i..k-1\}.\ \pi \models^j \phi \end{array}$$

LTL Equivalences 1

$$\phi \;\equiv\; \psi \quad \doteq \quad \forall \mathcal{M}.\, \forall \pi \in \mathcal{M}. \quad \pi \models^{0} \phi \;\longleftrightarrow\; \pi \models^{0} \psi$$

Elimination of implication

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

Dualities in 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 2

Dualities in LTL

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

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

Inter-definitions

$$\mathbf{F}\,\phi \;\equiv\; \neg\mathbf{G}\,\neg\phi \qquad \mathbf{G}\,\phi \;\equiv\; \neg\mathbf{F}\,\neg\phi$$

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

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 3

Idempotency

$$\mathbf{F}\,\mathbf{F}\,\phi \;\equiv\; \mathbf{F}\,\phi \qquad \mathbf{G}\,\mathbf{G}\,\phi \;\equiv\; \mathbf{G}\,\phi$$

Weak and strong Until

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

Some more suprising equivalences

$$\mathbf{G}\,\mathbf{F}\,\mathbf{G}\,\phi \;\equiv\; \mathbf{F}\,\mathbf{G}\,\phi \qquad \mathbf{F}\,\mathbf{G}\,\mathbf{F}\,\phi \;\equiv\; \mathbf{G}\,\mathbf{F}\,\phi$$

$$\mathbf{G}\,(\mathbf{F}\,\phi \vee \mathbf{F}\,\psi) \;\equiv\; \mathbf{G}\,\mathbf{F}\,\phi \vee \mathbf{G}\,\mathbf{F}\,\psi$$

Past-time LTL Operators

$$\pi \models^i \mathbf{Y}\,\phi \quad \text{iff} \quad i > 0 \text{ and } \pi \models^{i-1} \phi$$

$$\pi \models^i \mathbf{Z}\,\phi \quad \text{iff} \quad i = 0 \text{ or } \pi \models^{i-1} \phi$$

$$\pi \models^i \mathbf{F}^-\,\phi \quad \text{iff} \quad \exists j \in \{0..i\}.\ \pi \models^j \phi$$

$$\pi \models^i \mathbf{G}^-\,\phi \quad \text{iff} \quad \forall j \in \{0..i\}.\ \pi \models^j \phi$$

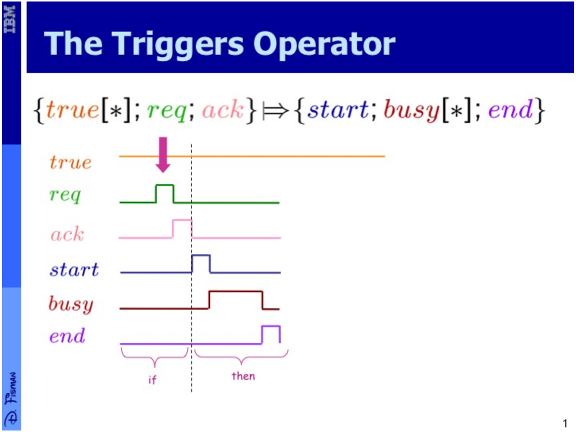
Interval LTL Operators

$$\pi \models^i \mathbf{F}_{[a,b]}\,\phi \quad \text{iff} \quad \exists j \in \{i + a \;..\; i + b\}.\ \pi \models^j \phi$$

$$\pi \models^i \mathbf{G}_{[a,b]}\,\phi \quad \text{iff} \quad \forall j \in \{i + a \;..\; i + b\}.\ \pi \models^j \phi$$

where $a, b \in \mathbb{N}$

PSL – Property Specification Language



Extends expressive power of LTL to that of omega-regular languages

SystemVerilog Assertions are similar.