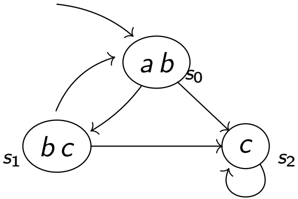
Linear Temporal Logic (LTL)

- Kripke structure:



- additional assumption: each state has at least one successor
  $\Rightarrow$ infinite processes !

- some computation paths:

  $s_0 \rightarrow s_1 \rightarrow s_0 \rightarrow s_1 \rightarrow \dots$

  $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow s_2 \rightarrow \dots$

  $s_0 \rightarrow s_2 \rightarrow s_2 \rightarrow \dots$

- LTL formulas are interpreted over *computation paths*

Syntax of LTL

Fix a set *Prop* of atomic propositions.

LTL formulas are of two kinds:

- **path formulas**:
  - $\texttt{tt}$, p where p is an atomic proposition
  - if f and g are path formulas, then so are:

$\neg f$	not f
$f \wedge g$	f and g
$\mathbf{X}\, f$	at the ne**X**t point in time, f
$\mathbf{F}\, f$	at some point in the **F**uture, f
$\mathbf{G}\, f$	**G**lobally (at all future points) f
$f\, \mathbf{U}\, g$	f **U**ntil g

- **state formulas:**

$\mathbf{A}\, f$	along **A**ll computation paths, f holds

- **binding priorities:** unary operators ; $\mathbf{U}$; $\wedge$ and $\vee$; $\rightarrow$

Semantics of LTL

Fix a Kripke structure $M = (S, R, V)$.

The semantics of LTL defines:

- when a computation path π through M satisfies a *path formula* f,

  Notation: $\pi \models f$ if π satisfies f

- when a state s of M satisfies a *state formula* ϕ.

  Notation: $s \models \phi$ if s satisfies ϕ

Meaning of Temporal Operators (Pictorially)

Let $s_0 \longrightarrow s_1 \longrightarrow s_2 \longrightarrow \ldots$ be a computation path.

$s_0 \rightarrow \ldots$	$s_0 \rightarrow \ldots$	$s_1 \rightarrow \ldots$	$\ldots$	$s_i \rightarrow \ldots$	$\ldots$
$\mathbf{X}\, f$	$\ldots$	f	$\ldots$	$\ldots$	$\ldots$
$\mathbf{F}\, f$	$\ldots$	$\ldots$	$\ldots$	f	$\ldots$
$\mathbf{G}\, f$	f	f	f	f	f
$f\, \mathbf{U}\, g$	f	f	f	g	$\ldots$

Note:

- f here is a path formula, so it is itself interpreted over *paths* !!

Semantics of LTL (Cont'd)

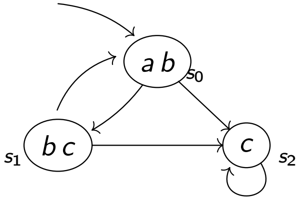
- Given $\pi = s_0 \to s_1 \to s_2 \to \ldots$, let $\pi^i = s_i \to s_{i+1} \to \ldots$.
- Now define when a path formula f holds in a path π:

$\pi \models \texttt{tt}$		
$\pi \models p$	iff	$p \in V(s_0)$
$\pi \models \neg f$	iff	$\pi \models f$ does not hold
$\pi \models f \wedge g$	iff	$\pi \models f$ and $\pi \models g$
$\pi \models \mathbf{X}\, f$	iff	$\pi^1 \models f$
$\pi \models \mathbf{F}\, f$	iff	there exists i s.t. $\pi^i \models f$
$\pi \models \mathbf{G}\, f$	iff	$\pi^i \models f$ for all $i \geq 0$
$\pi \models f\, \mathbf{U}\, g$	iff	there exists i s.t. $\pi^0 \models f, \ldots, \pi^{i-1} \models f, \pi^i \models g$

- Finally, define when a state formula $\mathbf{A}\, f$ holds *in a state* $s \in S$:

$$s \models \mathbf{A}\, f \quad \text{iff} \quad \pi \models f \quad \text{for all paths } \pi \text{ starting in } s$$

Semantics of LTL – Example



$s_0 \to s_1 \to s_0 \to s_1 \to \ldots \models \mathbf{X}\, c$

$s_0 \to s_1 \to s_0 \to s_1 \to \ldots \models \mathbf{F}\, c$

$s_0 \to s_1 \to s_0 \to s_1 \to \ldots \not\models \mathbf{G}\, c$

$s_2 \to s_2 \to s_2 \to s_2 \to \ldots \models \mathbf{G}\, c$

$s_0 \to s_1 \to s_2 \to s_2 \to \ldots \models \mathbf{F}\ \mathbf{G}\, c$

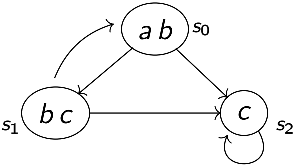
$s_0 \to s_1 \to s_2 \to s_2 \to \ldots \models b\, \mathbf{U}\, c$

$\pi \models \mathbf{G}\ \mathbf{F}\, c$ for any π

Note:

- $\pi \models \mathbf{G}\ \mathbf{F}\, f$ iff f occurs infinitely often along π.

Semantics of LTL – Example



$s_0 \models \mathbf{A}\,(a \wedge b)$
$s_0 \models \mathbf{A}\ \mathbf{X}\,c$
$s_0 \not\models \mathbf{A}\ \mathbf{X}\,(b \wedge c)$
$s_0 \models \mathbf{A}\ \mathbf{F}\,c$

$s_0 \models \mathbf{A}\ \mathbf{F}\,a$
$s_0 \models \mathbf{A}\ \mathbf{G}\,\neg(a \wedge c)$
$s_1 \not\models \mathbf{A}\ \mathbf{G}\,c$
$s_2 \models \mathbf{A}\ \mathbf{G}\,c$
$s_0 \not\models \mathbf{A}\ \mathbf{G}\ \mathbf{F}\,a$
$s_0 \models \mathbf{A}\,(\,\mathbf{G}\ \mathbf{F}\,a \rightarrow\ \mathbf{G}\ \mathbf{F}\,c)$
$s_1 \models \mathbf{A}\ (b\,\mathbf{U}\,c)$
$s_2 \models \mathbf{A}\ (b\,\mathbf{U}\,c)$
$s_0 \models \mathbf{A}\ \mathbf{X}\ (b\,\mathbf{U}\,c)$

Note:

- $s \models \mathbf{A}\ \mathbf{G}\,f$ iff f holds in all states reachable from s (including s).
- $s \models \mathbf{A}\ \mathbf{G}\ \mathbf{F}\,f$ iff f occurs infinitely often along every path from s.

Some LTL Patterns

- invariance (always): **A G** p

  "p remains invariantly true throughout every path"

- guarantee (eventually): **A F** p

  "p will eventually become true in every path"

- stability (non-progress): **A F G** p

  "there is a point in every path where p will become invariantly true"

- recurrence (progress): **A G F** p

  "if p happens to be false at any given point in a path, it is always guaranteed to become true again later"

  Same as: "p holds infinitely often"

Some LTL Patterns

- response: $\mathbf{A}\ \mathbf{G}\,(p \rightarrow\ \mathbf{F}\,q)$

  "any state satisfying p is eventually followed by a state satisfying q"

- precedence: $\mathbf{A}\ \mathbf{G}\,(p \rightarrow\ q\,\mathbf{U}\,r)$

  "from any state satisfying p, the system will continuously satisfy property q until property r becomes true"

- correlation: $\mathbf{A}\,(\ \mathbf{F}\,p \rightarrow\ \mathbf{F}\,q)$

  "if p holds at some point in the future, so does q"

Back to Mutual Exclusion

Atomic propositions:

c_0 , c_1	(critical state)
n_0 , n_1	(non-critical state)
t_0 , t_1	(trying to enter critical state)

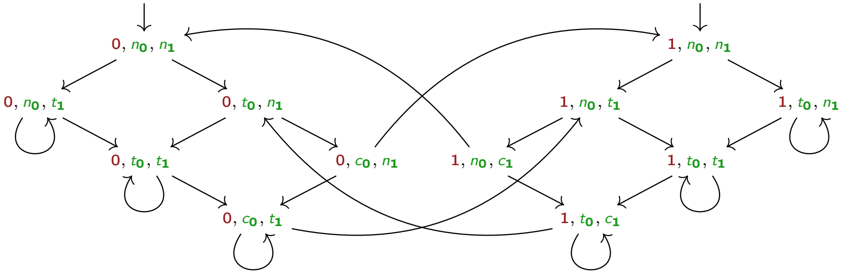
- mutual exclusion: at most one process in critical section *at any time*

  $$\mathbf{A}\ \mathbf{G}\,\neg(c_0 \land c_1)$$

- absence of starvation: *whenever* a process tries to enter its critical section, it will *eventually* do so

  $$\mathbf{A}\ \mathbf{G}\ ((t_0 \to\ \mathbf{F}\, c_0) \land (t_1 \to\ \mathbf{F}\, c_1))$$

Mutual Exclusion: Checking Correctness



- $\mathbf{A}\ \mathbf{G}\, \neg(c_0 \wedge c_1)$ ✓

  Need to check that $\neg(c_0 \wedge c_1)$ is true at all states reachable from the initial states.

- $\mathbf{A}\ \mathbf{G}\, ((t_0 \rightarrow \mathbf{F}\, c_0) \wedge (t_1 \rightarrow \mathbf{F}\, c_1))$ × ✓

  Need fairness constraints for the property to hold.