Linear Temporal Logic (propositional)

Syntax $\varphi ::= \text{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi$ logical connectives

$\mid \bigcirc\varphi \mid \varphi_1 \,\mathsf{U}\, \varphi_2$ temporal modalities

redundant if $AP \neq \emptyset$ (true); $a \in AP$; U: right associative

Obs false, $\vee$, $\rightarrow$, $\leftrightarrow$, $\oplus$ obtained as usual eg

$$\varphi_1 \oplus \varphi_2 \overset{\text{def}}{=} (\varphi_1 \wedge \neg\varphi_2) \vee (\neg\varphi_1 \wedge \varphi_2)$$

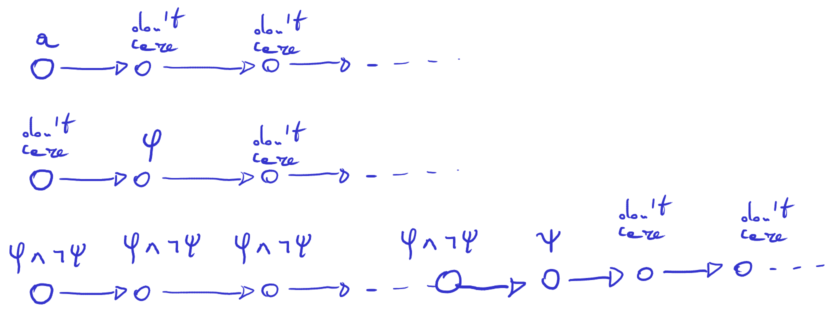
Intuitive semantics

An LTL f.la expresses a property of an infinite "path"
(i.e. the models of an LTL f.la are infinite sequences of 2^{AP} (= states))

$a \leadsto$

$\bigcirc\varphi \leadsto$

$\varphi \,\mathsf{U}\, \psi \leadsto$



Formal Semantics

Let $\sigma \in (2^{AP})^\omega$ and $\sigma = A_0 \ldots A_i A_{i+1} \ldots$ then $\begin{cases} \sigma @ i = A_i A_{i+1} \ldots \\ \sigma[i] = A_i \end{cases}$

$\sigma \in (2^{AP})^\omega$ models $\varphi \in LTL$ if $\sigma \models \varphi$ can be derived from the following statements

$\sigma \models \text{true}$

$\sigma \models a$ iff $a \in \sigma[0]$ $(\equiv \sigma[0] \models a)$

$\sigma \models \varphi \wedge \psi$ iff $\sigma \models \varphi$ and $\sigma \models \psi$

$\sigma \models \neg\varphi$ iff $\sigma \not\models \varphi$

$\sigma \models \bigcirc\varphi$ iff $\sigma @ 1 \models \varphi$

$\sigma \models \varphi \,\mathsf{U}\, \psi$ iff $\exists_{j \geq 0} : \sigma @ j \models \psi \wedge \forall_{0 \leq i < j} : \sigma @ i \models \varphi$

Some important derived modalities

"eventually" $\Diamond$

$\Diamond \varphi \equiv \text{true} \ U \varphi$

$\equiv \neg \Box \neg \varphi$

"always" $\Box$

$\Box \varphi \equiv \varphi \ U \text{false}$

$\equiv \neg \Diamond \neg \varphi$

Exercise Define "infinitely often". A: $\Box \Diamond \varphi$

"eventually forever" $\Diamond \Box \varphi$

Exercise Which of the following equivalences are correct:

$\varphi = \text{true}$

- ✗ a) $\Box(\varphi \to \Diamond \psi) \equiv \varphi \ U (\psi \wedge \neg \varphi)$
- ✗ b) $\circ \Diamond \varphi \equiv \Diamond \circ \varphi$
- ✓ c) $\Box \varphi \wedge \circ \Diamond \varphi \equiv \Box \varphi$
- ✗ d) $\Diamond(\varphi \wedge \psi) \equiv \Diamond \varphi \wedge \Diamond \psi$
- ✓ e) $\Box(\varphi \wedge \psi) \equiv \Box \varphi \wedge \Box \psi$
- ✓ f) $\Box \Box (\psi \to \varphi) \equiv \neg \Diamond (\neg \varphi \wedge \psi)$

$\Box \Box \varphi = \Box \varphi$

Exercise Give an LTL f.la expressing safety & liveness of the mutual exclusion problem

$$\Box \bigwedge_{1 \le h \ne k \le n} (\neg c_h \vee \neg c_k)$$ safety

$$\bigwedge_{1 \le h \le n} \Box \Diamond c_h$$ liveness

$$\bigwedge_{1 \le h \le n} \Box (w_h \to \Diamond c_h)$$ liveness

Exercise Express the fairness conditions as LTL f.lae

φ, ψ propositional f.lae on AP

unconditional $\quad \Box\Diamond\varphi$

strong $\quad \Box\Diamond\varphi \rightarrow \Box\Diamond\psi$

weak $\quad \Diamond\Box\varphi \rightarrow \Box\Diamond\psi$

LTL sem. over TS

$\text{Words}(\varphi) = \{ \sigma \in (2^{AP})^\omega \mid \sigma \models \varphi \}$

π infinite path fragment of TS

$$\pi \models \varphi \iff \text{trace}(\pi) \models \varphi \iff \text{trace}(\pi) \in \text{Words}(\varphi)$$

$s \in S$

$$s \models \varphi \iff \forall \pi \in \text{Path}(s) : \pi \models \varphi$$

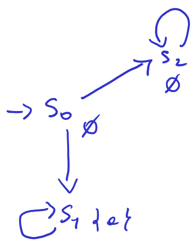
$$TS \models \varphi \iff \forall s \in I : s \models \varphi$$
$$\iff TS \models \text{Words}(\varphi)$$

$\text{Words}(\neg\varphi) = (2^{AP})^\omega \setminus \text{Words}(\varphi) \quad \Rightarrow \quad \pi \models \varphi \iff \pi \not\models \neg\varphi$

However negation is weird:

Exercise show that $TS \not\models \varphi \not\Leftrightarrow TS \models \neg\varphi$

$\Leftarrow$ holds, but $\not\Rightarrow$



$TS \not\models \Diamond a \qquad s_0\, s_2^\omega$

$TS \not\models \neg \Diamond a \qquad s_0\, s_1^\omega$

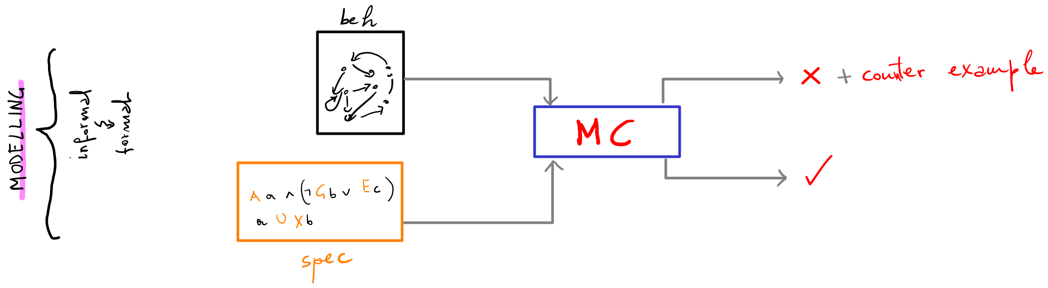
$\equiv \Box \neg a$

Model Checking LTL (brief note)

Basic Algorithm (Vardi, Wolper 1986)

LTL f.la

$$TS \models \varphi \iff Traces(TS) \subseteq Words(\varphi)$$
$$\iff Traces(TS) \cap \left((2^{AP})^{\omega} \setminus Words(\varphi)\right) = \emptyset$$
$$\iff Traces(TS) \cap Words(\neg\varphi) = \emptyset$$



thm: φ LTL f.la $\Rightarrow$ φ ω-regular
$\Updownarrow$
$\exists$ NBA "accepts" φ

Input: finite TS & LTL f.la φ
Output: "yes" if $TS \models \varphi$, otherwise c. ex.

$\mathcal{A}_{\neg\varphi} :=$ NBA s.t. $\mathcal{L}(\mathcal{A}_{\neg\varphi}) = Words(\neg\varphi)$

$\mathcal{A} := TS \times \mathcal{A}_{\neg\varphi}$

state explosion

if $\exists \pi \in paths(TS \times \mathcal{A}_{\neg\varphi}) : \mathcal{A}$ accepts π
  then return an expressive (bad) prefix of π
  else return "yes"
fi

there is a reachable accepting state on a cicle!
$\Updownarrow$
emptiness of NBA is decidable

The actual process is more complicated, but we do not look at the details.

E.g. Account for fairness
- f.la : $\varphi_{fair} \longrightarrow \varphi$
- alg : look only fair executions

more efficient