Linear temporal logic (LTL)

Let AP (atomic propositions) be a set of propositional variables. The set of LTL formulas over AP is given by:

$$\varphi ::= \text{true} \mid a \mid \varphi \wedge \psi \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi \,\mathcal{U}\, \psi$$

"next" "until"

Given a sequence $\sigma : \mathbb{N}_0 \to \mathcal{P}(AP)$, $i \in \mathbb{N}_0$, we write

$$\sigma[i..] = (\sigma(i+j))_{j \geq 0}.$$

We define "satisfaction" of a formula by a sequence:

- $\sigma \models \text{true}$
- $\sigma \models a$ iff $\sigma(0) \ni a$
- $\sigma \models \varphi \wedge \psi$ iff $\sigma \models \varphi$ and $\sigma \models \psi$
- $\sigma \models \neg\varphi$ iff $\sigma \not\models \varphi$
- $\sigma \models \bigcirc\varphi$ iff $\sigma[1..] \models \varphi$
- $\sigma \models \varphi \,\mathcal{U}\, \psi$ iff $\exists j \in \mathbb{N}_0 : \Big(\sigma[j..] \models \psi \;\wedge\; \big(\forall i \in \mathbb{N}_0 : i < j \Rightarrow \sigma[i..] \models \varphi\big) \Big)$

Example: Let $AP = \{M, T\}$, $\sigma = \big(\{M\}\{M\}\emptyset\emptyset\{T\}\emptyset\emptyset\big)^\omega$,

$\forall i \in \mathbb{N}_0 : \sigma(7i) = \sigma(7i+1) = \{M\} \wedge \sigma(7i+2) = \sigma(7i+3) = \emptyset \wedge \ldots$

Then $\sigma \models \text{true}$, $\sigma \models M$, $\sigma \models \bigcirc M$, $\sigma \not\models M \wedge T$, $\sigma \not\models \bigcirc\bigcirc M$,

$\sigma \models \bigcirc\bigcirc\bigcirc\bigcirc T$ $\big(\sigma \models \bigcirc^4 T\big)$,

$\sigma \models \text{true}\,\mathcal{U}\, T$, $\sigma \models \neg(\text{true}\,\mathcal{U}\,(T \wedge M))$,

$\sigma \models \neg(\text{true}\,\mathcal{U}\,\neg(\text{true}\,\mathcal{U}\,M))$

iff $\forall j \geq 0 : \Big(\sigma[j..] \models \text{true}\,\mathcal{U}\,M \;\vee\; \exists i < j : \sigma[i..] \not\models \text{true} \Big)$

Example: $AP = \{\text{green}, \text{yellow}, \text{red}\}$

$\sigma = \{\text{green}\}\{\text{green}\}\{\text{yellow}\}\{\text{red}\}\{\text{red}\}\{\text{red}, \text{yellow}\}\{\text{green}\}\ldots$

$\sigma \models \bigcirc\bigcirc\bigcirc\,(\text{red}\,\mathcal{U}\,(\text{red} \wedge \text{yellow}))$

$\sigma \models \bigcirc\bigcirc\bigcirc\,(\text{red}\,\mathcal{U}\,\text{green})$

$\hat{\sigma} = \{\text{red}, \text{green}\}\{\text{red}, \text{green}\}\{\text{red}, \text{yellow}\}\{\text{red}\}\{\text{red}\}\ldots$

$\hat{\sigma} \models \text{red}\,\mathcal{W}\,\text{green}$

Derived operators.

$\text{false} := \neg\text{true}$,

$\varphi \vee \psi = \neg(\neg\varphi \wedge \neg\psi)$

$\varphi \to \psi := \neg(\varphi \wedge \neg\psi)$

$\varphi \leftrightarrow \psi := (\neg\varphi \vee \psi) \wedge (\neg\psi \vee \varphi)$

$\Diamond\varphi := \text{true}\,\mathcal{U}\,\varphi$ "eventually" / Fφ "Finally"

$\Box\varphi := \neg(\text{true}\,\mathcal{U}\neg\varphi)$ "always" / Gφ "globally"

$\varphi\,W\,\psi := (\varphi\,\mathcal{U}\,\psi) \vee \Box\varphi$ "weak until"

$\varphi\,R\,\psi := \psi\,W(\varphi \wedge \psi)$ "releases"

Example: $\sigma = \{a\}\{a\}\ldots\{a\}\{a,b\}$

$\hat{\sigma} = \{a\}\{a\}\ldots\{a\}^\omega$

$\sigma \models \{b\}R\{a\}$, $\hat{\sigma} \models \{b\}R\{a\}$

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

$\varphi \equiv \psi :\Leftrightarrow \text{Words}(\varphi) = \text{Words}(\psi)$ $(\Leftrightarrow \forall \sigma \in (2^{AP})^\omega : \sigma \models \varphi \Leftrightarrow \sigma \models \psi)$

Example: Let $\sigma = (\{M\}\{M\}\emptyset\emptyset\{T\}\emptyset\emptyset)^\omega$. Then

$\sigma \models \neg\Diamond(M \wedge T)$, $\sigma \models \Box\Diamond M$ "infinitely often M"

$\sigma \models M\,W(\neg M \wedge \neg T)$, $\sigma \models$ [illegible]$(\bigcirc\bigcirc\bigcirc T)\,R\,M$

$\sigma \models M\,\mathcal{U}(M \wedge \bigcirc\bigcirc\bigcirc T)$, so $\sigma \in M\,W(M \wedge \bigcirc\bigcirc\bigcirc T)$

Prop: For all LTL formulas φ, ψ over AP the following holds:

a) $\neg\Diamond\varphi \equiv \Box\neg\varphi$

b) $\neg\Box\varphi \equiv \Diamond\neg\varphi$

c) $\neg(\varphi\,\mathcal{U}\,\psi) \equiv (\neg\psi)\,W(\neg\varphi \wedge \neg\psi)$

d) $\neg(\varphi\,\mathcal{U}\,\psi) \equiv (\neg\varphi)\,R\,(\neg\psi)$

e) $\neg(\varphi\,W\,\psi) \equiv (\varphi \wedge \neg\psi)\,\mathcal{U}\,(\neg\varphi \wedge \neg\psi)$

f) $\neg(\varphi\,R\,\psi) \equiv (\neg\varphi)\,\mathcal{U}\,\neg(\psi)$

Proof: a) Let $\sigma \in (2^{AP})^\omega$.

$\sigma \models \neg\Diamond\varphi \Leftrightarrow \sigma \models \neg(\text{true}\,\mathcal{U}\,\varphi) \Leftrightarrow \sigma \models \neg(\text{true}\,\mathcal{U}(\neg\neg\varphi))$

$\Leftrightarrow \sigma \models \Box\neg\varphi$

c) Let $\sigma \in (2^{AP})^\omega$. Will show

$\sigma \models \neg(\varphi\,\mathcal{U}\,\psi) \Leftrightarrow \sigma \models \neg\psi\,W\,(\neg\varphi \wedge \neg\psi)$

"$\Rightarrow$": Let $\sigma \not\models \varphi\,\mathcal{U}\,\psi$. Then $\forall j \geq 0$ ($\sigma[j..] \not\models \psi$ or $\exists i < j$: $\sigma[i..] \not\models \varphi$). If $\forall j \geq 0 : \sigma[j..] \not\models \psi$, then $\sigma \models \Box\neg\psi$. Otherwise there is the smallest $j \geq 0$ such that $\sigma[j..] \models \psi$. Then there is $i < j$ such that $\sigma[i..] \not\models \varphi$. Then $\forall k < i$: $\sigma[k..] \models \neg\psi$. Thus $\sigma \models \neg\psi\,\mathcal{U}\,(\neg\varphi \wedge \neg\psi)$.

"$\Leftarrow$": Let $\sigma \models \neg\psi\,\mathcal{U}\,(\neg\varphi \wedge \neg\psi)$ or $\sigma \models \Box\neg\psi$.

Case $\sigma \models \neg\psi \,\mathcal{U}\, (\neg\varphi \wedge \neg\psi)$ Then for some $j \geq 0$ we have $\sigma[j..] \models \neg\varphi \wedge \neg\psi$ and for all $i < j$ we have $\sigma[i..] \models \neg\psi$. Take the smallest such j. Let $k \geq 0$ arbitrary and $\sigma[k..] \models \psi$. Then $k > j$. Notice that $\sigma[j..] \not\models \varphi$. Thus $\forall k \geq 0: (\sigma[k..] \not\models \psi \vee \exists \hat{j} < k: \sigma[\hat{j}..] \not\models \varphi)$. So $\sigma \not\models \varphi \,\mathcal{U}\, \psi$.

Case $\sigma \models \Box\neg\psi$ Then $\sigma \models \neg(\mathrm{true}\,\mathcal{U}\,\psi)$, so $\forall j \geq 0: \sigma[j..] \not\models \psi$ or $\underbrace{\exists i < j\ \sigma[i..] \not\models \mathrm{true}}_{\text{false}}$, so $\forall j \geq 0: \sigma[j..] \not\models \psi$, so $\sigma \not\models \varphi \,\mathcal{U}\, \psi$.

b), d), e), f). Homework

Prop: $\sigma \models \varphi R \psi$ iff

$$\Big(\forall j \geq 0: \sigma[j..] \models \psi \text{ or } \exists i \geq 0. \big(\sigma[i..] \models \varphi \wedge \forall k \leq i: \sigma[k..] \models \psi\big)\Big)$$

Proof Recall $\varphi R \psi := \psi \,W\, (\varphi \wedge \psi) = (\psi \,\mathcal{U}\, (\varphi \wedge \psi) \vee \Box\psi)$

"⇒": ✓

"⇐": ✓ ∎

Def The set of positive LTL formulas over AP is given by

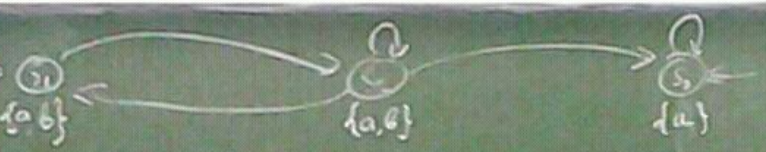
$$\varphi ::= \mathrm{true} \mid \mathrm{false} \mid a \mid \neg a \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \bigcirc\varphi \mid \varphi \,\mathcal{U}\, \varphi \mid \varphi R \varphi$$

Prop For all LTL formulas φ there is an equivalent PLTL formula of size $O(|\varphi|)$

Proof Rewrite $\neg\mathrm{true} \rightsquigarrow \mathrm{false}$, $\neg\mathrm{false} \rightsquigarrow \mathrm{true}$, $\neg\neg\varphi \rightsquigarrow \varphi$, $\neg\bigcirc\varphi \rightsquigarrow \bigcirc\neg\varphi$, $\neg(\varphi\,\mathcal{U}\,\psi) \rightsquigarrow \neg\varphi R \neg\psi$. ∎

Consider a program P with states $State$, initial states $init \subseteq State$, transition relation $\rightarrow \subseteq State^2$, w.l.o.g. $\forall s \in State\ \exists s': s \rightarrow s'$. For each $s \in State$, $a \in AP$, fix whether $a(s)$ or $\neg a(s)$. For each infinite path π in $(State, \rightarrow)$, let $trace(\pi) = \big(\{a \in AP \mid a(\pi(i))\}\big)_{i \geq 0}$. For an LTL formula φ, define $\pi \models \varphi :\Leftrightarrow trace(\pi) \models \varphi$. Let $s \in State$. Define $Paths(s) := \{\text{infinite paths } \pi \mid \pi(0) = s\}$. For an LTL formula φ, let $s \models \varphi :\Leftrightarrow \forall \pi \in Paths(s).\ \pi \models \varphi$. Let $Traces(P) = \{traces(\pi) \mid \pi(0) \in init \wedge \pi \text{ is inf.te}\}$. P satisfies an LTL formula φ if $Traces(P) \subseteq Words(\varphi)$, i.e. $\forall s \in init: s \models \varphi$.

Example:



$AP = \{a, b\}$

$s_2 \models a \wedge b$, so $s_1 \models \bigcirc(a \wedge b)$

$s_3 \not\models a \wedge b$, so $s_3 \not\models \bigcirc(a \wedge b)$

$P \not\models \bigcirc(a \wedge b)$

$P \models \Box\, a$

Example: 2-Peterson

initially $\neg Q_1 \wedge \neg Q_2 \wedge turn \in \{1,2\}$

A. $Q_1 := true$	A: $Q_2 := true$
B $turn = 1$	B: $turn = 2$
C await $\neg Q_2 \vee turn = 2$	C await $\neg Q_1 \vee turn = 1$
D $Q_1 := false$, goto A,	D $Q_2 := false$, goto A,

$AP = \{at_{1A}, at_{2A}, \ldots, at_{1D}, at_{2D}, q_1, q_2\}$

$s \models at_{ix} \iff s(pc_i) = x$ $\quad (i = 1,2)$

$s \models q_i \iff s(Q_i) = true$ $\quad (i = 1,2)$

2-Peterson satisfies $\Box\,(at_{1A} \rightarrow \neg q_1)$

$$\Box\,(at_{2A} \rightarrow \neg q_2)$$
$$\wedge\ \Box\,(at_{1D} \rightarrow \neg\, at_{2D})$$
$$\wedge\ \Box\Diamond\,(at_{1C} \wedge \bigcirc at_{1D}) \vee (at_{2C} \wedge \bigcirc at_{2D})$$
$$\wedge\ \Box\,(at_{1B} \rightarrow \Diamond\, at_{1D})$$

$$at_{1D} \rightarrow \neg\, at_{2D} \quad = \quad \neg(at_{1D} \wedge at_{2D})$$