Linear Temporal Logic

MCS-19

Syntax

$$\varphi ::= \text{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi_1 \, \mathsf{U} \, \varphi_2$$

a ranges over AP. "next" "until"

Unary operators bind tighter than binary ones; U associates to the right.

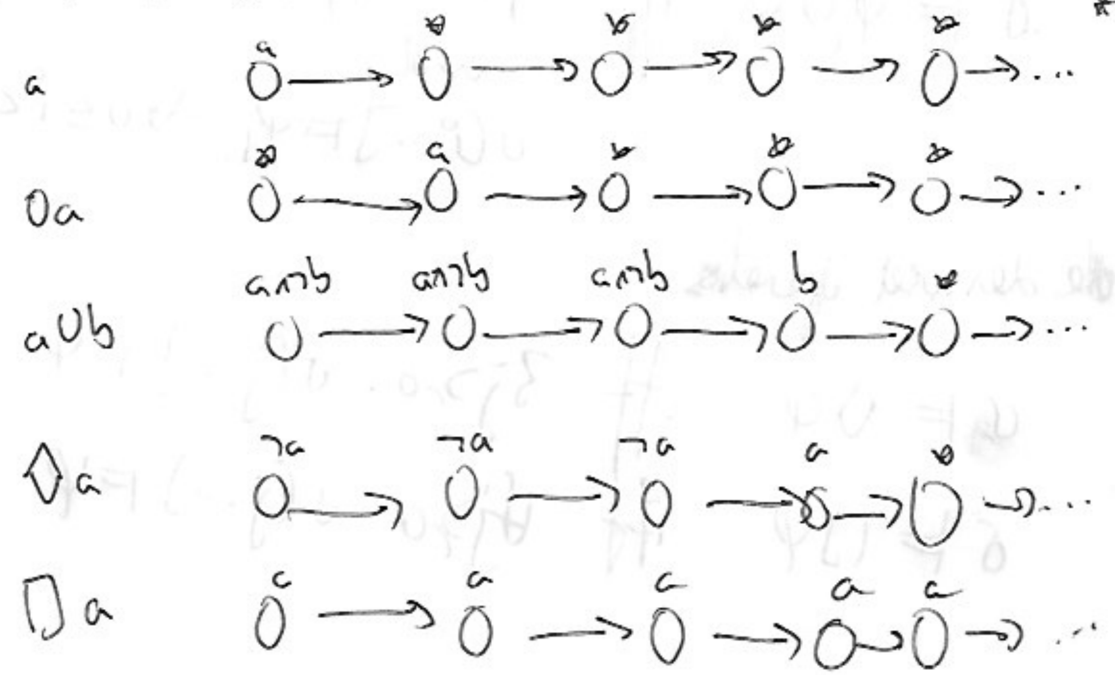
Derived operators

$\Diamond\varphi \triangleq \text{true} \, \mathsf{U} \, \varphi$ "φ will eventually be true in the future"

$\Box\varphi \triangleq \neg\Diamond\neg\varphi$ "φ holds from now on forever"

Intuitive semantics

$*$ = arbitrary



Semantics

φ LTL formula over AP. The LT property induced by φ is:

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

where $\models \subseteq (2^{AP})^\omega \times LTL$ is the smallest relation satisfying: $\sigma = A_0 A_1 A_2 \ldots$

$\sigma \models true$

$\sigma \models a$ iff $a \in A_0$

$\sigma \models \varphi_1 \wedge \varphi_2$ iff $\sigma \models \varphi_1$ and $\sigma \models \varphi_2$

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

$\sigma \models \bigcirc\varphi$ iff $\sigma[1..] = A_1 A_2 A_3 \ldots \models \varphi$

$\sigma \models \varphi_1 \cup \varphi_2$ iff $\exists j \geq 0.\ \sigma[j..] \models \varphi_2$ and $\sigma[i\ldots] \models \varphi_1,\ \forall 0 \leq i < j$

For the derived operators

$\sigma \models \Diamond\varphi$ iff $\exists j \geq 0.\ \sigma[j\ldots] \models \varphi$

$\sigma \models \Box\varphi$ iff $\forall j \geq 0.\ \sigma[j..] \models \varphi$

Combinations

"infinitely often φ"

$$\sigma \models \Box\Diamond\varphi \text{ iff } \overset{\infty}{\exists} j.\ \sigma[j..] \models \varphi$$

$$\sigma \models \Diamond\Box\varphi \text{ iff } \overset{\infty}{\forall} j.\ \sigma[j...] \models \varphi$$

"eventually forever φ"

where

$\overset{\infty}{\exists} j$ means $\forall i \geq 0. \exists j \geq i.$ "for infinitely many $j \in \mathbb{N}$"

$\overset{\infty}{\forall} j$ means $\exists i \geq 0. \forall j \geq i.$ "for almost all $j \in \mathbb{N}$".

Eg. (Properties for mutual exclusion)

P_1, P_2 concurrent processes.

$wait_i \to P_i$ waiting to enter CS

$crit_i \to P_i$ in CS.

$\Box(\neg crit_1 \vee \neg crit_2)$

Always, at least one of the two processes is not in its critical section.
(safety property).

$\Box\Diamond crit_1 \wedge \Box\Diamond crit_2$

Each process is infinitely often in its critical section. (liveness property).

$(\Box\Diamond wait_1 \Rightarrow \Box\Diamond crit_1) \wedge (\Box\Diamond wait_2 \Rightarrow \Box\Diamond crit_2)$

Every waiting process will eventually enter its critical section (starvation freedom)

$\Box((y=0) \rightarrow crit_1 \vee crit_2)$

whenever y has the value 0, then one of the processes is in its CS.

Def. 5.7 [Semantics of LTL over Paths and States]
Let $TS = (S, Act, \rightarrow, I, AP, L)$ be a TS without terminal states. and let φ be an LTL formula over AP:

- π finite path fragment of TS

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

- $s \in S$ state

$$s \models \varphi \quad \text{iff} \quad (\forall \pi \in Paths(s).\ \pi \models \varphi)$$

- TS satisfies φ

$$TS \models \varphi \quad \text{iff} \quad Traces(TS) \subseteq Words(\varphi).$$

Ex MCS-21

$AP = \{a,b\}$ Transition system over AP

$TS \models \Box a$ (all traces of TS are words of the form $A_0 A_1 \ldots$ with $a \in A_i \ \forall i \geq 0$)

$s_1 \models \bigcirc(a \wedge b)$ (s_2 is the only successor of s_1 and $s_2 \models a \wedge b$)

$s_2 \not\models \bigcirc(a \wedge b)$

$s_3 \not\models \bigcirc(a \wedge b)$ ($s_3 \in Post(s_3)$ and $s_3 \not\models a \wedge b$)

$TS \not\models \bigcirc(a \wedge b)$ (since s_3 is an initial state and $s_3 \not\models \bigcirc(a \wedge b)$)

$TS \models \Box(\neg b \rightarrow \Box(a \wedge \neg b))$? Yes

$TS \models b \, U (a \wedge \neg b)$? No $(s_1 s_2)^\omega$

Remarks

For paths it holds that

$$\pi \models \varphi \text{ iff } \pi \not\models \neg\varphi$$