Formal Methods in software development

a.a.2017/2018

Prof. Anna Labella

Temporal logic

Let us want to express the following properties

$\forall x\ ((file(x) \wedge requested(x)) \Rightarrow \exists y\ (y \geq a\ \wedge print(x,y))$

$\forall y\ (y \geq a\ \ \Rightarrow works(x))$

The constant *a* as well as the variable *y*, of type "time"

If a file is requested to be printed, *eventually* it will be printed

After an amount *a* of time, *x* will begin to work

Temporal logic

One could use typed variables and first order logic
making a distinction between temporal and dominion references

Or one can use modal operators

$$\forall x \, ((file(x) \wedge requested(x)) \Rightarrow \mathsf{F}\, print(x))$$

$$\mathsf{G}\, works(x))$$

F means *eventually*
G means *always*

Some hypotheses on temporal structure

Discrete/ Continuous

Linear / Branching

Linear time temporal logic: LTL (syntax)

- φ::=T $|\bot$ | p | $(\neg\varphi)$ | $(\varphi\wedge\varphi)$ | $(\varphi\vee\varphi)$ | $(\varphi\rightarrow\varphi)$ | $(X\varphi)$ | $(F\varphi)$ | $(G\varphi)$ | $(X\varphi)$ | $(\varphi\ U\ \varphi)$ | $(\varphi\ W\ \varphi)$
- F "eventually"
- G "always"
- X "next step"
- U "until"
- W "until possibly"

LTL: syntax

Warning: Operators not connectives

They bind more tightly than connectives

Exercises

Draw parse trees for the LTL formulas:

(a) $\mathrm{F}\, p \wedge \mathrm{G}\, q \rightarrow p\, \mathrm{W}\, r$

(b) $\mathrm{F}\,(p \rightarrow \mathrm{G}\, r) \vee \neg q\, \mathrm{U}\, p$

(c) $p\, \mathrm{W}\, (q\, \mathrm{W}\, r)$

(d) $\mathrm{G}\,\mathrm{F}\, p \rightarrow \mathrm{F}\,(q \vee s)$

LTL: satisfiability

Suppose $\mathcal{M} = (S, \rightarrow, L)$ is a model, $s \in S$, and ϕ an LTL formula.

We write $\mathcal{M}, s \vDash \phi$ if, for every execution path π of $\mathcal{M}$ starting at s, we have $\pi \vDash \phi$.

We write $\mathcal{M} \vDash \phi$ if, for every execution path π of $\mathcal{M}$ we have $\pi \vDash \phi$.

LTL: semantics

We are dealing with a path intended as an infinite series of states

$\mathcal{M}, s \models \varphi$ if the path starting from s satisfys φ

States or paths? States are starting points of paths

suffixes of paths are still paths

LTL: semantics (satisfaction)

1. $\pi \vDash \top$
2. $\pi \nvDash \bot$
3. $\pi \vDash p$ iff $p \in L(s_1)$
4. $\pi \vDash \neg\phi$ iff $\pi \nvDash \phi$
5. $\pi \vDash \phi_1 \wedge \phi_2$ iff $\pi \vDash \phi_1$ and $\pi \vDash \phi_2$
6. $\pi \vDash \phi_1 \vee \phi_2$ iff $\pi \vDash \phi_1$ or $\pi \vDash \phi_2$
7. $\pi \vDash \phi_1 \rightarrow \phi_2$ iff $\pi \vDash \phi_2$ whenever $\pi \vDash \phi_1$
8. $\pi \vDash \mathrm{X}\,\phi$ iff $\pi^2 \vDash \phi$
9. $\pi \vDash \mathrm{G}\,\phi$ iff, for all $i \geq 1$, $\pi^i \vDash \phi$
10. $\pi \vDash \mathrm{F}\,\phi$ iff there is some $i \geq 1$ such that $\pi^i \vDash \phi$
11. $\pi \vDash \phi\,\mathrm{U}\,\psi$ iff there is some $i \geq 1$ such that $\pi^i \vDash \psi$ and for all $j = 1, \ldots, i-1$ we have $\pi^j \vDash \phi$
12. $\pi \vDash \phi\,\mathrm{W}\,\psi$ iff either there is some $i \geq 1$ such that $\pi^i \vDash \psi$ and for all $j = 1, \ldots, i-1$ we have $\pi^j \vDash \phi$; or for all $k \geq 1$ we have $\pi^k \vDash \phi$

Semantics

- $\pi \models \varphi$

π O-----O-----O-----O-----O

φ, φ' φ ...

Semantics of G and F

- Semantics of G: $\pi \models G\ p$

π O-----O-----O-----O-----O----

p *p* *p* *p* *p*

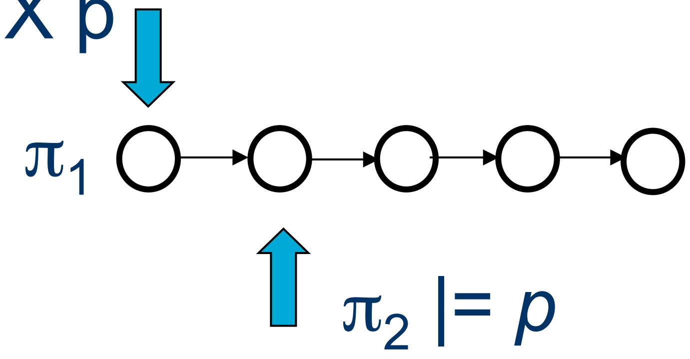
- Semantics of F: $\pi \models F\ p$

π O-----O-----O-----O-----O----

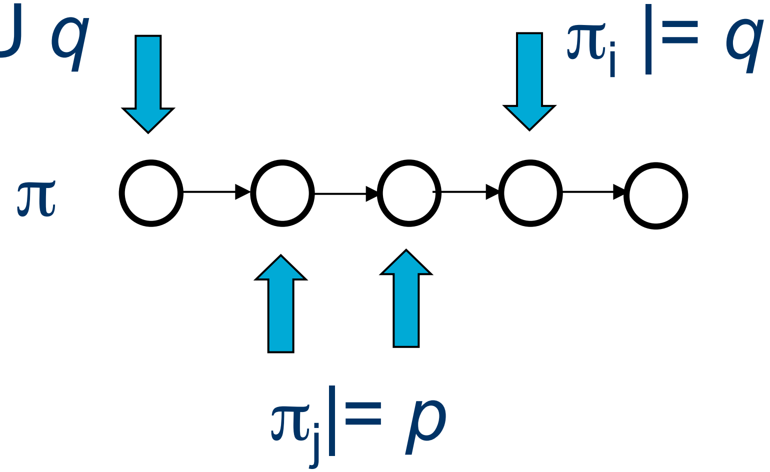
p

Semantics of X and U

- Semantics of X: $\pi_1 \models X\, p$



- Semantics of U: $\pi \models p\ U\ q$



Semantics

- a modal formula can be true or false in a path

e.g. in this trace: O-----O-----O-----O-----O------…..

pq $p\neg q$ $p\neg q$ pq pq …

- $p \vee \neg q$ true: is true in the first state of the trace
- $X\neg q$ true, because q is false in the second state
- XXq false, because q is false in the *third* state
- Gp true, because p is true in all states
- Gq false, because q is not true in all states (it is true only in some states)

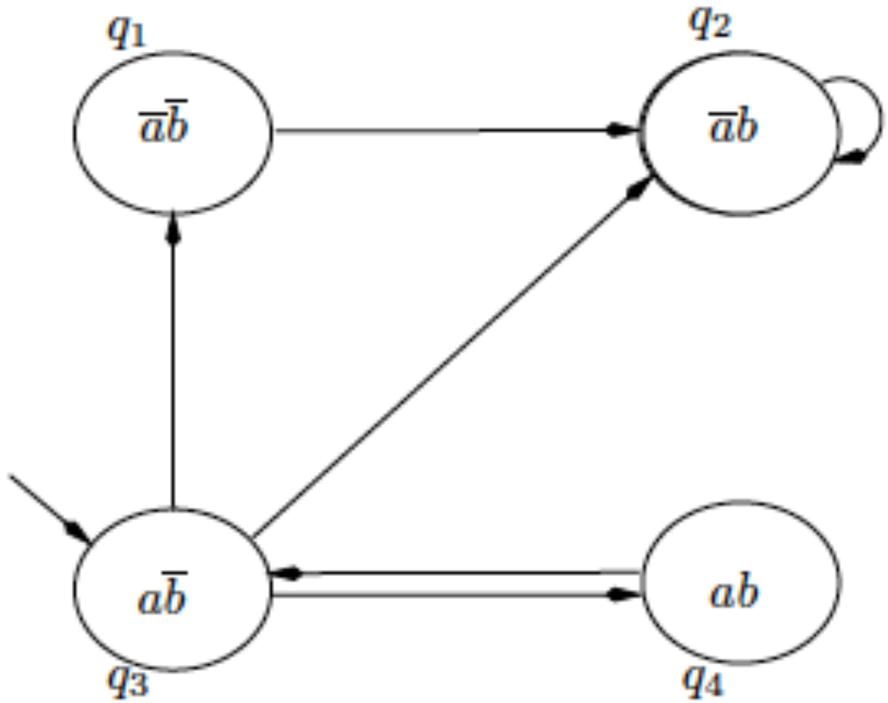
Semantics

in the same trace: O-----O-----O-----O-----O------…..

$pq \quad p\neg q \quad p\neg q \quad pq \quad pq \quad \ldots$

- *GFq* true: for all states of the sequence, there is some future point where *q* is true
- *pU¬q* true: *p* is true until *¬q* becomes true; (in the first state *p* is true, then *¬q* becomes true)
- *qUXXq* true: in the first state *q* is true, in the second state *XXq* is true (because *q* is true two states later)
- *G(pUXXq)* not straightforward to check: all states have to be checked for *qUXXq* in turn, check *XXq* in all states

Exercises



For each of the formulas ϕ:

(a) $\mathrm{G}\, a$

(b) $a \,\mathrm{U}\, b$

(c) $a \,\mathrm{U}\, \mathrm{X}\,(a \wedge \neg b)$

(d) $\mathrm{X}\, \neg b \wedge \mathrm{G}\,(\neg a \vee \neg b)$

(e) $\mathrm{X}\,(a \wedge b) \wedge \mathrm{F}\,(\neg a \wedge \neg b)$

(i) Find a path from the initial state q_3 which satisfies ϕ.

(ii) Determine whether $\mathcal{M}, q_3 \vDash \phi$.

LTL: equivalences

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

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

$$\phi\,\mathbf{U}\,\psi \equiv \phi\,\mathbf{W}\,\psi \wedge \mathbf{F}\,\psi\,.$$

$$\phi\,\mathbf{W}\,\psi \equiv \phi\,\mathbf{U}\,\psi \vee \mathbf{G}\,\phi.$$

LTL: what does hold (exercises)

$G(\varphi \to \psi) \to (G\varphi \to G\psi)$

$G\varphi \to \varphi$

$\varphi \to F\varphi$

$G\varphi \to X\varphi$

$X\varphi \to F\varphi$

$G\varphi \to F\varphi$

$X(\varphi \wedge \psi) \cong X\varphi \wedge X\psi$

LTL: reductions

(transitivity on paths)

$G\ \varphi \rightarrow GG\varphi$

while

$GG\ \varphi \rightarrow G\varphi$ is always valid

LTL

An internal induction rule w.r.t. time

$$\frac{\varphi \rightarrow X\varphi \qquad G(\varphi \rightarrow X\varphi)}{(\varphi \rightarrow G\varphi)}$$

LTL: definability

- $F\ \varphi \cong T\ U\ \varphi$ "eventually"
- $G\ \varphi \cong \varphi\ W\ \bot$ "always"
- $\varphi U \psi \cong (\varphi W \psi) \wedge (F\psi)$ "until"
- $\varphi W \psi \cong (\varphi U \psi) \vee (G\varphi)$ "until possibly"

LTL

"next" operator

- X is completely orthogonal to the other connectives. That is to say, its presence doesn't help in defining any of the other ones in terms of each other. Moreover, X cannot be derived from any combination of the others.

- Each of the sets $\{U, X\}$, $\{R, X\}$, $\{W, X\}$ is adequate.

Exercises

2. Consider the sentence $\phi \stackrel{\text{def}}{=} \forall x\, \exists y\, \exists z\, (P(x,y) \land P(z,y) \land (P(x,z) \to P(z,x)))$. Which of the following models satisfies ϕ?
   (a) The model $\mathcal{M}$ consists of the set of natural numbers with $P^{\mathcal{M}} \stackrel{\text{def}}{=} \{(m,n) \mid m < n\}$.
   (b) The model $\mathcal{M}'$ consists of the set of natural numbers with $P^{\mathcal{M}'} \stackrel{\text{def}}{=} \{(m, 2*m) \mid m \text{ natural number}\}$.
   (c) The model $\mathcal{M}''$ consists of the set of natural numbers with $P^{\mathcal{M}''} \stackrel{\text{def}}{=} \{(m,n) \mid m < n+1\}$.
3. Let P be a predicate with two arguments. Find a model which satisfies the sentence $\forall x\, \neg P(x,x)$; also find one which doesn't.