NSWI101: System Behaviour Models and Verification

Lab 02 – LTL model checking

Jan Kofroň

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

Department of
Distributed and
Dependable
Systems
D3S

Linear Temporal Logic (LTL)

- Captures properties of particular *runs* – executions
- Does not capture *possible futures* – branching
- Frequently used for expressing system properties

LTL SYNTAX

LTL syntax defined inductively, similarly to propositional logic:

Let *AP* be a finite set of Boolean variables (atomic propositions).
The set of LTL formulae over *AP* is defined as:

- If $p \in AP$ then p is LTL formula.
- If φ and ψ are LTL formulae then
  $\neg\varphi$, $\varphi \vee \psi$, $\varphi \wedge \psi$, $\mathrm{X}\,\varphi$, $\varphi\,\mathrm{U}\,\psi$, $\mathrm{F}\,\varphi$, $\varphi\,\mathrm{R}\,\psi$, and $\mathrm{G}\,\varphi$ are LTL formulae.

Negation, disjunction, X, and U are fundamental operators, others can be derived.

LTL SEMANTICS

Path in Kripke structure is infinite sequence $\pi = \pi_0, \pi_1, \pi_2, \ldots$ where for all $\forall i > 0.(\pi_i, \pi_{i+1}) \in R$

Let $M = (S, I, R, L)$ be Kripke structure and $\pi = \pi_0, \pi_1, \pi_2, \ldots$ be an infinite path in M. For an integer $i \geq 0$, π^i stands for i-th suffix of π: $\pi^i = \pi_i, \pi_{i+1}, \pi_{i+2}, \ldots$

Let M be Kripke structure, φ be LTL formula, π be path in M and s be state of M.

$M, \pi \models \varphi$: Path π from M satisfies φ
$M, s \models \varphi$: State s from M satisfies φ

- $M, s \models \varphi \leftrightarrow \forall \pi . \pi_0 = s : M, \pi \models \varphi$

LTL SEMANTICS

$$M, \pi \models p \quad \leftrightarrow \quad p \in L(\pi_0)$$

$$M, \pi \models \neg\varphi \quad \leftrightarrow \quad \neg(M, \pi \models \varphi)$$

$$M, \pi \models \varphi_1 \lor \varphi_2 \quad \leftrightarrow \quad M, \pi \models \varphi_1 \lor M, \pi \models \varphi_2$$

$$M, \pi \models \varphi_1 \land \varphi_2 \quad \leftrightarrow \quad M, \pi \models \varphi_1 \land M, \pi \models \varphi_2$$

$$M, \pi \models \mathrm{X}\,\varphi \quad \leftrightarrow \quad M, \pi^1 \models \varphi$$

$$M, \pi \models \mathrm{F}\,\varphi \quad \leftrightarrow \quad \exists i \geq 0 . M, \pi^i \models \varphi$$

$$M, \pi \models \mathrm{G}\,\varphi \quad \leftrightarrow \quad \forall i \geq 0 . M, \pi^i \models \varphi$$

$$M, \pi \models \varphi_1 \,\mathrm{U}\, \varphi_2 \quad \leftrightarrow \quad \exists i \geq 0 . M, \pi^i \models \varphi_2 \land \forall j . 0 \leq j < i \implies M, \pi^j \models \varphi_1$$

$$M, \pi \models \varphi_1 \,\mathrm{R}\, \varphi_2 \quad \leftrightarrow \quad (\mathrm{G}\,\varphi_2) \lor (\varphi_2 \,\mathrm{U}\, (\varphi_1 \land \varphi_2))$$

LTL EXERCISES

Decide and prove or disprove equivalence of following pairs of LTL formulae:

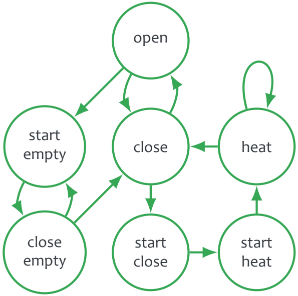
- $\mathrm{G}\,p : \mathrm{F}\,\mathrm{G}\,p$
- $\mathrm{G}\,p : \mathrm{G}\,\mathrm{F}\,p$
- $\mathrm{F}\,p : \mathrm{F}\,\mathrm{G}\,p$
- $\mathrm{F}\,p : \mathrm{G}\,\mathrm{F}\,p$
- $p\,\mathrm{U}\,q : \mathrm{G}\,q \vee (\mathrm{F}\,q \wedge \mathrm{G}\,p)$

Is any of these formulae implied by another one?

LTL EXERCISES

- Assume model of Alternating Bit Protocol (last lab)
- What properties could be verified?
- Express them in LTL!

Assume following model of microwave oven:



- What properties could be verified?
- Express them in LTL.
- Would you enhance the model somehow?