

NSWI101: System Behaviour Models and Verification

Lab 02

Jan Kofroň; Klára Pernicová



FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

Department of
Distributed and
Dependable
Systems



For AP – set of atomic propositions (Boolean variables, constants, predicates),
Kripke structure $M = (S, I, R, L)$ over AP is four-tuple:

- S – finite set of states
- $I \subseteq S$ – set of initial states
- $R \subseteq S \times S$ – transition relation such that R is left-total (for each state s there is a transition originating in it)
- $L : S \rightarrow 2^{AP}$ – labelling function

Draw a Kripke structure for the following program:

$x := 3;$

$x := x + 2;$

$x := 7;$

LTL semantics

1. $M, \pi \models p \quad \Leftrightarrow \quad p \in L(\pi_0)$
2. $M, \pi \models \neg\varphi \quad \Leftrightarrow \quad \neg(M, \pi \models \varphi)$
3. $M, \pi \models \varphi_1 \vee \varphi_2 \quad \Leftrightarrow \quad M, \pi \models \varphi_1 \vee M, \pi \models \varphi_2$
4. $M, \pi \models \varphi_1 \wedge \varphi_2 \quad \Leftrightarrow \quad M, \pi \models \varphi_1 \wedge M, \pi \models \varphi_2$
5. $M, \pi \models \mathbf{X}\varphi \quad \Leftrightarrow \quad M, \pi^1 \models \varphi$
6. $M, \pi \models \mathbf{F}\varphi \quad \Leftrightarrow \quad \exists i \geq 0 : M, \pi^i \models \varphi$
7. $M, \pi \models \mathbf{G}\varphi \quad \Leftrightarrow \quad \forall i \geq 0 : M, \pi^i \models \varphi$
8. $M, \pi \models \varphi_1 \mathbf{U} \varphi_2 \quad \Leftrightarrow \quad \exists i \geq 0 : M, \pi^i \models \varphi_2 \wedge \forall j : 0 \leq j < i \implies M, \pi^j \models \varphi_1$
9. $M, \pi \models \varphi_1 \mathbf{R} \varphi_2 \quad \Leftrightarrow \quad M, \pi \models (\mathbf{G} \varphi_2) \vee (\varphi_2 \mathbf{U} (\varphi_1 \wedge \varphi_2))$

Draw a path for each one.

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

1. $G p$ and $F G p$
2. $G p$ and $G F p$
3. $F p$ and $F G p$
4. $F p$ and $G F p$
5. $p \cup q$ and $G q \vee (F q \wedge G p)$

Is any of these formulae implied by another one?

Normal form of LTL formulae

Property formula φ is transformed into *normal form*:

- Only $\top$, atomic propositions, $\neg$, $\wedge$, and X and U operators
- Assume $\varphi \neq \top$, otherwise trivial

Application of rewrite rules:

- $F p = \top U p$
- $G p = \neg F \neg p$
- $p R q = \neg(\neg p U \neg q)$
- $\neg X p = X \neg p$
- De Morgan Boolean equivalences

1. Show that the rewrite rules are correct.
2. Transform the following formulae into normal form:

2.1 $p \vee q$

2.2 $\neg X G p$

2.3 $(F p) R (X q)$

For LTL formula f in normal form, $\text{closure}(\varphi)$ contains all its subformulae and their negations

E.g.: for $\varphi = a \cup (\neg a \wedge b)$, $\text{closure}(\varphi) = \{a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), \varphi, \neg\varphi\}$

$\text{closure}(\varphi)$ is closure of sub-formulae of φ under negation

- We identify $\neg\neg\psi$ with ψ

Find the closure for the following formulae:

1. $p \wedge q$
2. $X(p \wedge \neg q)$
3. $p R q$

Elementary set

1. B is *consistent* with respect to propositional logic, i.e., for all $\varphi_1 \wedge \varphi_2, \psi \in \text{closure}(\varphi)$:
 - $\varphi_1 \wedge \varphi_2 \in B \iff \varphi_1 \in B \text{ and } \varphi_2 \in B$
 - $\psi \in B \implies \neg\psi \notin B$
 - $\top \in \text{closure}(\varphi) \implies \top \in B$
2. B is *locally consistent* with respect to the until operator, i.e., for all $\varphi_1 \cup \varphi_2 \in \text{closure}(\varphi)$:
 - $\varphi_2 \in B \implies \varphi_1 \cup \varphi_2 \in B$
 - $\varphi_1 \cup \varphi_2 \in B \text{ and } \varphi_2 \notin B \implies \varphi_1 \in B$
3. B is *maximal*, i.e., for all $\psi \in \text{closure}(\varphi)$:
 - $\psi \notin B \implies \neg\psi \in B$

Find at least one elementary set for the following formulae:

1. $p \wedge q$
2. $X(p \wedge \neg q)$
3. $p R q$

GNBA $\mathcal{G}_\varphi$ for LTL φ

Let φ be LTL formula over AP . Then $\mathcal{G}_\varphi = (Q, 2^{AP}, \Delta, Q_0, F)$, where:

- Q is set of all elementary sets of $B \subseteq \text{closure}(\varphi)$
- AP is set of atomic propositions
- $Q_0 = \{B \in Q \mid \varphi \in B\}$
- $F = \{F_{\varphi_1 \cup \varphi_2} \mid \varphi_1 \cup \varphi_2 \in \text{closure}(\varphi)\}$ where

$$F_{\varphi_1 \cup \varphi_2} = \{B \in Q \mid \varphi_1 \cup \varphi_2 \notin B \text{ or } \varphi_2 \in B\}$$
- Δ : transition (B, A, B') is defined iff:
 - $A = B \cap AP$, and
 - for every $X\psi \in \text{closure}(\varphi) : X\psi \in B \Leftrightarrow \psi \in B'$, and
 - for every $\varphi_1 \cup \varphi_2 \in \text{closure}(\varphi) :$

$$\varphi_1 \cup \varphi_2 \in B \Leftrightarrow (\varphi_2 \in B \vee (\varphi_1 \in B \wedge \varphi_1 \cup \varphi_2 \in B')).$$

Draw the GNBA for the following formulae and find some accepting and non-accepting runs:

1. Xp
2. $\neg Xp$
3. $a \cup b$

Procedure:

1. Property formula F negated
2. Creating Büchi automaton $A_{\neg F}$ accepting exactly language of $\neg F$
3. Converting Kripke structure to Büchi automaton A_M
4. Creating product automaton $A = A_{\neg F} \times A_M$ accepting intersection of languages
5. Checking for emptiness of language accepted by A

Product of Büchi automata

Intersection: $A' = (Q', \Sigma, \Delta_1 \cup \Delta_2, I', F')$

- $Q' = Q_A \times Q_B \times \{1, 2\}$
- $\Delta_1 = \{((q_A, q_B, 1), a, (q'_A, q'_B, i)) \mid (q_A, a, q'_A) \in \Delta_A \wedge (q_B, a, q'_B) \in \Delta_B \text{ and if } q_A \in F_A \text{ then } i = 2 \text{ else } i = 1\}$
- $\Delta_2 = \{((q_A, q_B, 2), a, (q'_A, q'_B, i)) \mid (q_A, a, q'_A) \in \Delta_A \wedge (q_B, a, q'_B) \in \Delta_B \text{ and if } q_B \in F_B \text{ then } i = 1 \text{ else } i = 2\}$
- $I' = I_A \times I_B \times \{1\}$
- $F' = \{(q_A, q_B, 2) \mid q_B \in F_B\}$

Check whether the following Kripke structure satisfies the properties:

1. $F a$
2. $a \cup b$

