Development of Safety Critical Systems(Sichere Software) winter term 18
Martin Leucker, Grigory Markin, Felix Lange November 29, 2018

Exercise Sheet 4 (Solution)

Task 4.1 Linear-time temporal logic

Specify the following properties of linear executions using LTL

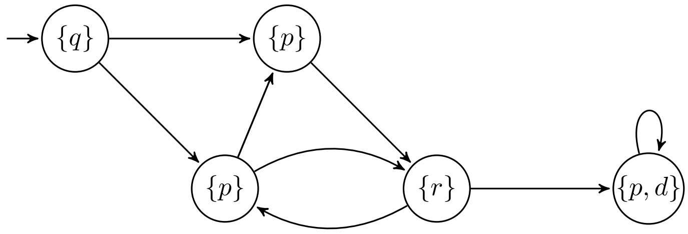
- "p holds in the third position."
- "p never holds."
- "p holds before the third position or it never holds."
- "p holds from the beginning until q holds."
- "p holds from the beginning until q holds and q has to hold sometime."
- "p holds at most, as long as q holds."
- $\{w \in \Sigma^\omega \mid \forall_{i \in \mathbb{N}} \{p, q\} \subseteq w_i\}$
- $\{w \in \Sigma^\omega \mid \exists_{i \in \mathbb{N}} \{p, q\} \subseteq w_i\}$
- Σ^ω
- $\emptyset$

Solution

- $\mathrm{X}\,\mathrm{X}\,p$
- $\mathrm{G}\,\neg p$
- $p \vee \mathrm{X}\,p \vee \mathrm{G}\,\neg p$
- $p \,\mathrm{W}\, q$
- $p \,\mathrm{U}\, q$
- $p \,\mathrm{U}\, \neg q$
- $\mathrm{G}(p \wedge q)$
- $\mathrm{F}(p \wedge q)$
- $true$
- $false$

Task 4.2 Labeled Transition System

Consider the following labeled transition system.



Which of the following properties hold in *all* executions of the transition system ?

- p
- $\mathrm{F}\, d$
- $\neg\, \mathrm{F}\, d$
- $\mathrm{G}\, \mathrm{F}\, p$
- $\mathrm{F}\, \mathrm{G}(p\, \mathrm{U}\, q)$
- $q\, \mathrm{U} \neg(p\, \mathrm{U}\, d)$
- $\mathrm{G}(p \rightarrow \mathrm{X}\, \mathrm{F}\, p)$
- $\mathrm{X}\, \mathrm{X}\, \mathrm{X}\, p$

Solution

- No
- No (There exists a cycle without d)
- No ($\neg\, \mathrm{F}\, d \equiv \mathrm{G}\, \neg d$)
- Yes (in the loop at the last state p always hold)
- No (after p is reached, there is no way to go back to q)
- Yes (all paths after q towards d go through r)
- Yes (if p does not hold, that's fine, but after p holds, there is always some position where p holds again)
- No (e.g. qpr)

Task 4.3 Symbolic Encoding

Consider the labeled transition system from the previous Task.

- How many variables do we need to encode the transition system in propositional logic ?
- Define the set of propositional variables V and describe the set of initial states and the transition relation by propositional formulas I and T respectively.
- Consider LTL properties from the previous task that do not hold for the considered transition system. Find for every the properties the lowest bound k (if there exists one) that is enough to falsify the property using the Bounded Model Checking algorithm.

Solution

- We have 5 states, i.e. we need at least 3 propositional variables. It's enough to encode 2^3 states.
- For the sake of clarity, we encode every state by a separate variable (from left to right, starting from the first row): $S = \{s_0, s_1, s_2, s_3, s_4\}$. Variables for atomic propositions: $AP = \{p, q, r, d\}$. Finally, the set of variables is defined as $V = S \cup AP$.
- Initial states: $I(V) = s_0 \wedge q \wedge \bigwedge_{v \in V \setminus \{s_0, q\}} \neg v$
- Let:
  - $T_{s_0 \rightarrow s_1}(V, V') = s_0 \wedge s_1' \wedge p' \wedge \bigwedge_{v \in V' \setminus \{s_1', p'\}} \neg v'$
  - $T_{s_0 \rightarrow s_2}(V, V') = s_0 \wedge s_2' \wedge p' \wedge \bigwedge_{v \in V' \setminus \{s_2', p'\}} \neg v'$
  - $T_{s_1 \rightarrow s_3}(V, V') = s_1 \wedge s_3' \wedge r' \wedge \bigwedge_{v \in V' \setminus \{s_3', r'\}} \neg v'$

- $T_{s_2 \to s_1}(V, V') = s_2 \wedge s'_1 \wedge p' \wedge \bigwedge_{v \in V' \setminus \{s'_1, p'\}} \neg v'$
- $T_{s_2 \to s_3}(V, V') = s_2 \wedge s'_3 \wedge r' \wedge \bigwedge_{v \in V' \setminus \{s'_3, r'\}} \neg v'$
- $T_{s_3 \to s_2}(V, V') = s_3 \wedge s'_2 \wedge p' \wedge \bigwedge_{v \in V' \setminus \{s'_2, p'\}} \neg v'$
- $T_{s_3 \to s_4}(V, V') = s_3 \wedge s'_4 \wedge p' \wedge d' \wedge \bigwedge_{v \in V' \setminus \{s'_4, p', d'\}} \neg v'$
- $T_{s_4 \to s_4}(V, V') = s_4 \wedge s'_4 \wedge p' \wedge d' \wedge \bigwedge_{v \in V' \setminus \{s'_4, p', d'\}} \neg v'$

- Then transition relation is defined as:

$$\begin{aligned} T(V, V') = & T_{s_0 \to s_1}(V, V') \vee T_{s_0 \to s_2}(V, V') \vee \\ & T_{s_1 \to s_3}(V, V') \vee T_{s_2 \to s_1}(V, V') \vee \\ & T_{s_2 \to s_3}(V, V') \vee T_{s_3 \to s_2}(V, V') \vee \\ & T_{s_3 \to s_4}(V, V') \vee T_{s_4 \to s_4}(V, V') \end{aligned}$$

- Following properties from the previous task does not hold:
  - p
  - $\mathrm{F}\, d$
  - $\neg \mathrm{F}\, d$
  - $\mathrm{F}\,\mathrm{G}(p \,\mathrm{U}\, q)$
  - $\mathrm{X}\,\mathrm{X}\,\mathrm{X}\, p$
- Bounds to falsify properties using BMC (NOTE: we need to negate every property and show that negated property holds within first k steps):
  - $k = 0$ ($\neg p$ is true in the initial state)
  - $k = INF$ ($\neg \mathrm{F}\, d \equiv \mathrm{G}\, \neg d$ cannot be fulfilled, because we never know if in the next states d could hold (without loop recognition))
  - $k = 3$ ($\neg\neg \mathrm{F}\, d \equiv \mathrm{F}\, d$ is true after $\{q\}, \{p\}, \{r\}, \{p, d\}$)
  - $k = INF$ ($\neg \mathrm{F}\,\mathrm{G}(p \,\mathrm{U}\, q) \equiv \mathrm{G}\,\mathrm{F}\,\neg(p \,\mathrm{U}\, q)$) we need loop recognition to show that $p \,\mathrm{U}\, q$ never holds)
  - $k = 3$ ($\mathrm{X}\,\mathrm{X}\,\mathrm{X}\, p$ is true after $\{q\}, \{p\}, \{p\}, \{r\}$).