Homework 2 Solutions

Weichao Zhou

November 8, 2017

1 Expressing Properties in LTL

(a)

$$\Phi \quad = \quad \mathbf{G}\neg(\neg p \wedge \mathbf{X}p) \tag{1}$$

(b)

$$\Phi \quad = \quad \mathbf{G}(\mathbf{F}(p \wedge \mathbf{X}\neg p) \wedge \mathbf{F}(\neg p \wedge \mathbf{X}p)) \tag{2}$$

(c)

$$\begin{aligned} \Phi &= \mathbf{G}\neg((\neg r \wedge \mathbf{X}y) \vee (\neg y \wedge \mathbf{X}g) \vee (\neg g \wedge \mathbf{X}r)) & (3) \\ &= \mathbf{G}(\neg(\neg r \wedge \mathbf{X}y) \wedge (\neg(\neg y \wedge \mathbf{X}g)) \wedge \neg(\neg g \wedge \mathbf{X}r)) & (4) \end{aligned}$$

(d)

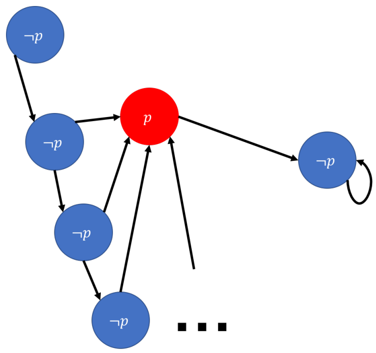
$$\Phi \quad = \quad \mathbf{G}\neg(q \wedge \neg r\mathbf{U}p) \tag{5}$$

2 LTL, CTL, CTL*

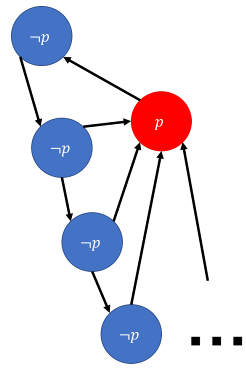
(a) $\mathbf{AFAG}p = \neg\mathbf{EGEF}\neg p$ means that there is no path satisfiying $\mathbf{GEF}\neg p$. But the infinitely cycling path through the red state on the left obviously satisfies $\mathbf{GEF}\neg p$.

(b) ($\mathbf{E}(\mathbf{GF}p)$ is stronger than $\mathbf{EG}(\mathbf{EF}p)$. In the state machine in Fig.1(a) which initiates from top left state, $\mathbf{E}(\mathbf{GF}p)$ doesn't satisfy since no path visit the red state satisfying p infinitely often. But $\mathbf{EG}(\mathbf{EF}p)$ satisfies since there is always branch transitioning from blue state to the red state satisfying p.

$\mathbf{E}(\mathbf{GF}p$ is weaker than $\mathbf{EG}(\mathbf{AF}p)$. In Fig.1(a) which initiates from top left state, $\mathbf{EG}(\mathbf{AF}p)$ doesn't satisfy since there is no such path satisfies that, every single state in the path satisfies $\mathbf{GF}p$, which means that every path initiated from this state must satisfy $\mathbf{F}p$. However, there does exist path that visit p infinitely often. Thus $\mathbf{E}(\mathbf{GF}p$ is satisfied.



(a)



(b)

Figure 1: (a) For $((\mathbf{E}(\mathbf{GF}p), \mathbf{EG}(\mathbf{EF}p))$; (b) For $((\mathbf{E}(\mathbf{GF}p), \mathbf{EG}(\mathbf{AF}p))$
;

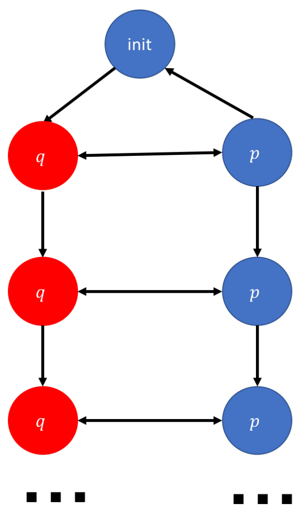


Figure 2: No state ensures $(\mathbf{AF}p)$ nor $(\mathbf{AF}q)$
;

(c) i. $(\mathbf{EF}p) \vee (\mathbf{EF}q)$ and $(\mathbf{EF}(p \vee q)$ are equavalent. ii. $(\mathbf{AF}p) \vee (\mathbf{AF}q)$ and $(\mathbf{AF}(p \vee q)$ are not equivalent. In Fig.2, no path satisfies $(\mathbf{AF}p)$ nor $(\mathbf{AF}q)$ since every p state can lead to an all q path branch and every q state can lead to an all p path branch. But the state machine satisfies $(\mathbf{AF}(p \vee q)$ for sure.

3 Simulation and SA

(a) $|S| \cdot |S'|$

(b)

$$\begin{aligned} & x_{s,s'} \Rightarrow (\exists j \in \{1,2,\ldots,k\}, x_{t,t'_j} = 1) && (6) \\ = \quad & \neg x_{s,s'} \vee (\exists j \in \{1,2,\ldots,k\}, x_{t,t'_j} = 1) && (7) \\ = \quad & \neg x_{s,s'} \vee (\bigvee_{R(s',t')} x_{t,t'}) && (8) \end{aligned}$$

If k = 0, then the CNF should be:

$$\begin{aligned} & \exists t\ R(s,t), x_{t,t'} = 0\ \forall t'\ R(s',t') \rightarrow x_{s,s'} == 0 && (9) \\ = \quad & R(s,t) \wedge (\bigwedge_{R(s',t')} \neg x_{t,t'}) \rightarrow \neg x_{s,s'} && (10) \\ = \quad & \neg(R(s,t) \wedge (\bigwedge_{R(s',t')} \neg x_{t,t'})) \vee \neg x_{s,s'} && (11) \\ = \quad & \neg R(s,t) \vee (\bigvee_{R(s',t')} x_{t,t'}) \vee \neg x_{s,s'} && (12) \end{aligned}$$

(c)

$$\begin{aligned} & \exists {s'}_0 \in {S'}_0, x_{s_0,{s'}_0} = 1 && (13) \\ = \quad & \bigvee_{k \in \{0,\ldots,|{S'}_0|-1\}} x_{s_0,{s'}_k} && (14) \end{aligned}$$

(d) (b)(c) can be turned to Horn-SAT which can be solved in linear time. For (b), since there are $|S||R||S'|$ clauses which each has $O(|R'|)$ complexity, all (b) have complexity of $O(|R'||S||R||S'|)$. For (c), there are $|S|$ clauses which complexities amount to $O(|S||S'|)$. Thus the overall CNF has complexity $O(|R'||S||R||S'|)$.

4 Symmetry Reductionh

Assume that σ is a permutation on the states of the structure, there can be multiple permutations which are all automorphisms of the structure.
$\sigma_0 = (s_0, s_1)(s_2, s_3)(s_1, s_0)(s_3, s_2)$

5 SPINing Elevators

Add one monitor and two global variables:

$byte\ mov;$
$active\ proctype\ monitor()\{$
$if\ \ ::elv?open, \_- > mov = false;$
$:: elv?close, \_- > mov = true;$
od
$\}$

- $ltl\ p\{[]!(mov == true\&\&doors\_open == true)\}$
  "$spin : \_spin\_nvr.tmp.10, Error : assertionviolated$"
  "spin: text of failed assertion: $assert(!((!((doors\_open == 0))\&\&!((mov == 0)))))$"
  The system doesn't satisfy this property. In the elevator process, elevator has to receive move signal before receiving close signal.
- $ltl\ p\{[](((iam[0] == 1||iam[1] == 1)\&\&floor! = 1)$
  $- > (<> (floor == 1\&\&(iam[0] == 1||iam[1] == 1))))\}$
  The system doesn't satisfy this property.
- $ltl\ p\{[]((<> (floor == 0))\&\&(<> (floor == 1))\&\&(<> (floor == 2))\&\&(<> (floor = 3)))\}$
  The system doesn't satisfy this property.