Course “Formal Methods” TEST

Roberto Sebastiani
DISI, Università di Trento, Italy

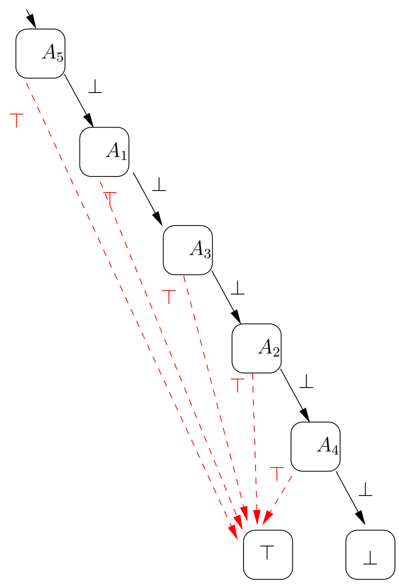
June 17^{th}, 2021

769857918

[COPY WITH SOLUTIONS]

1

Given the following OBDD, with the ordering $\{\ A_5,\ \ A_1,\ \ A_3,\ \ A_2,\ \ A_4\}$,



for each of the following Boolean formulas, say whether the OBDD represents it or not.

(*a*) $(\neg A_5 \rightarrow (\neg A_1 \rightarrow (\neg A_3 \rightarrow (\neg A_2 \rightarrow \ \ A_4))))$
[Solution: true]

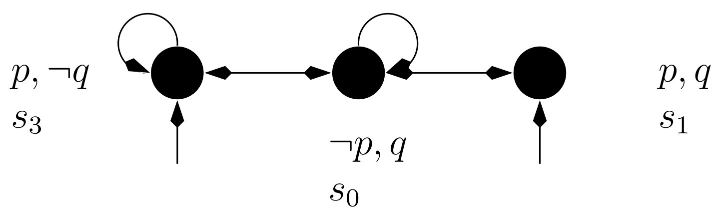
(*b*) $(\ \ A_2 \vee \ \ A_1 \vee \ \ A_5 \vee \ \ A_3 \vee \ \ A_4)$
[Solution: true]

(*c*) $(\ \ A_3 \wedge \ \ A_5 \wedge \ \ A_4 \wedge \ \ A_1 \wedge \ \ A_2)$
[Solution: false]

(*d*) $(\ \ A_5 \rightarrow (\ \ A_1 \rightarrow (\ \ A_3 \rightarrow (\ \ A_2 \rightarrow \neg A_4))))$
[Solution: false]

2

Consider the following Kripke Model M:



For each of the following facts, say if it is true or false in LTL.

(a) $M \models \mathbf{GF}p$
[Solution: false]

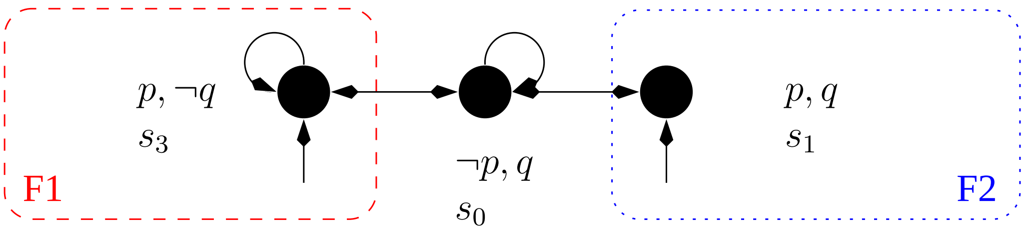
(b) $M \models \mathbf{FG}\neg p$
[Solution: false]

(c) $M \models p\mathbf{U}q$
[Solution: false]

(d) $M \models (\mathbf{GF}\neg p \land \mathbf{GF}\neg q) \rightarrow p$
[Solution: true]

3

Consider the following fair Kripke Model M:



For each of the following facts, say if it is true or false in LTL.

(a) $M \models \mathbf{GF}p$
[Solution: true]

(b) $M \models \mathbf{FG}\neg p$
[Solution: false]

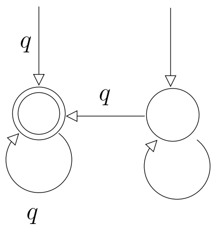
(c) $M \models p\mathbf{U}q$
[Solution: true]

(d) $M \models (\mathbf{GF}\neg p \wedge \mathbf{GF}\neg q) \rightarrow p$
[Solution: true]

4

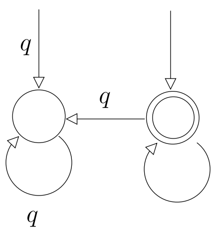
For each of the following fact regarding Buchi automata, say if it true or false.

(a) The following BA represents $\mathbf{FG}q$:



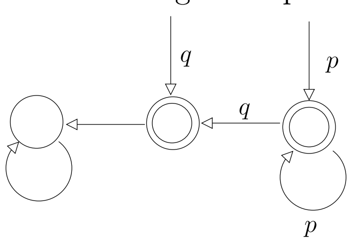
[Solution: Yes.]

(b) The following BA represents $\mathbf{FG}q$:



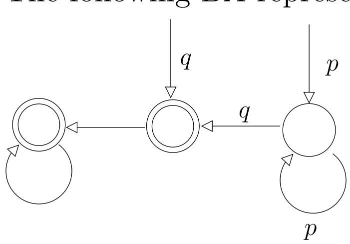
[Solution: No, it accepts every execution.]

(c) The following BA represents $p\mathbf{U}q$:



[Solution: No, it accepts $\mathbf{G}p$]

(d) The following BA represents $p\mathbf{U}q$:



[Solution: Yes]

5

Consider the following pair of ground and abstract machines M and M':

M:

```
MODULE main
VAR
  v1 : boolean;
  v2 : boolean;
  v3 : boolean;
ASSIGN
  init(v1) := FALSE;
  init(v2) := TRUE;
  init(v3) := FALSE;
TRANS
  (next(v1) <-> v2) &
  (next(v2) <-> v3) &
  (next(v3) <-> v1)
```

M':

```
MODULE main
VAR
  v1 : boolean;
  v2 : boolean;
  v3 : boolean;
ASSIGN
  init(v1) := FALSE;
  init(v2) := TRUE;

TRANS
  (next(v1) <-> v2) &
  (next(v2) <-> v3)
```

For each of the following facts, say which is true and which is false.

(*a*) M' simulates M.
[Solution: True]

(*b*) M simulates M'.
[Solution: False. E.g.: M can execute the path $(01[1]) \longmapsto (11[1]) \longmapsto ...$, which cannot be simulated by M'.]

(*c*) For every Boolean property φ on `v1,v2`, if $M' \models \mathbf{G}\varphi$, then $M \models \mathbf{G}\varphi$,
[Solution: True]

(*d*) For every Boolean property φ on `v1,v2`, if $M \models \mathbf{G}\varphi$, then $M' \models \mathbf{G}\varphi$,
[Solution: False. E.g., `G (!v1 | !v2)` (see example above).]

6

Consider the following piece of a much bigger formula, which has been fed to a CDCL SAT solver:

$$\begin{array}{l}
c_1 : \neg A_9 \vee \quad A_{12} \vee \neg A_1 \\
c_2 : \quad A_9 \vee \neg A_7 \vee \neg A_3 \\
c_3 : \neg A_{11} \vee \quad A_5 \vee \quad A_2 \\
c_4 : \neg A_{10} \vee \neg A_{12} \vee \quad A_{11} \\
c_5 : \neg A_{11} \vee \quad A_6 \vee \quad A_4 \\
c_6 : \neg A_9 \vee \quad A_{10} \vee \neg A_1 \\
c_7 : \quad A_9 \vee \quad A_8 \vee \neg A_3 \\
c_8 : \neg A_5 \vee \neg A_6 \\
c_9 : \quad A_7 \vee \neg A_8 \vee \quad A_{13} \\
...
\end{array}$$

Suppose the solver has decided, in order, the following literals (possibly interleaved by others not occurring in the above clauses):
$\{..., \quad A_1, ...\neg A_2, ...\neg A_4, ... \quad A_3, ...\neg A_{13}, ..., \quad A_9\}$

(a) List the sequence of unit-propagations following after the last decision, each literal tagged (in square brackets) by its antecedent clause

[Solution:

$$\begin{array}{ll}
A_{12} & [c_1] \\
A_{10} & [c_6] \\
A_{11} & [c_4] \\
A_5 & [c_3] \\
A_6 & [c_5] \\
\multicolumn{2}{c}{conflict\ on\ c_8}
\end{array}$$

]

(b) Derive the conflict clause via conflict analysis by means of the 1st-UIP technique

[Solution:

$$\dfrac{\neg A_{11} \vee \quad A_5 \vee \quad A_2 \qquad \dfrac{\neg A_{11} \vee \quad A_6 \vee \quad A_4 \qquad \overbrace{\neg A_5 \vee \neg A_6}^{Conflicting\ cl.}}{\neg A_{11} \vee \neg A_5 \vee \quad A_4}\ (\ A_6)}{\underbrace{\neg A_{11}}_{1st\ UIP} \vee \quad A_2 \vee \quad A_4}\ (\ A_5)$$

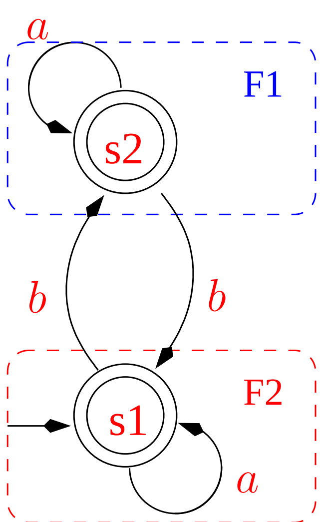
]

(c) Using the 1st-UIP backjumping strategy, update the list of literals above after the backjumping step and the unit-propagation of the UIP

[Solution: $\{..., \quad A_1, ...\neg A_2, ...\neg A_4, \neg A_{11}\}$]

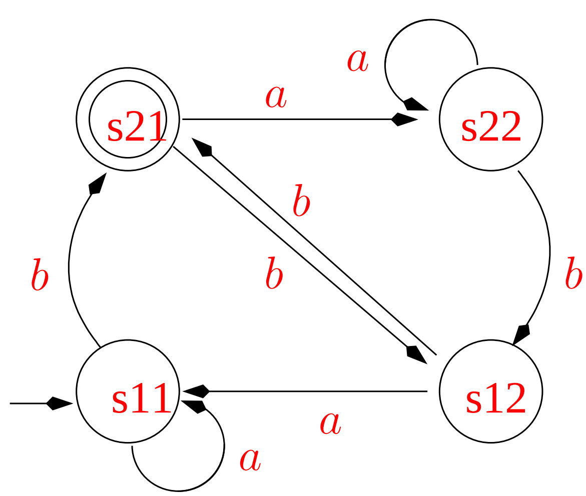
7

Given the following generalized Büchi automaton $A \stackrel{\text{def}}{=} \langle Q, \Sigma, \delta, I, FT \rangle$, $\{a, b\}$ being labels, with two sets of accepting states $FT \stackrel{\text{def}}{=} \{F1, F2\}$ s.t. $F1 \stackrel{\text{def}}{=} \{s2\}, F2 \stackrel{\text{def}}{=} \{s1\}$:



convert it into an equivalent plain Büchi automaton.

[Solution: The result is:



]

8

Consider the following LTL formula:

$$\varphi \stackrel{\text{def}}{=} (\mathbf{F}r) \rightarrow (p\mathbf{U}q)$$

and the following three states of the construction of the tableau T_φ of φ:

$S_1 : \langle\ q,\ \ p, \neg\mathbf{X}(p\mathbf{U}q),\ \ r,\ \ \mathbf{XF}r\rangle$

$S_2 : \langle \neg q,\ \ p,\ \ \mathbf{X}(p\mathbf{U}q),\ \ r, \neg\mathbf{XF}r\rangle$

$S_3 : \langle\ q, \neg p, \neg\mathbf{X}(p\mathbf{U}q), \neg r, \neg\mathbf{XF}r\rangle$

For each of the following statements, say if it is true or false.
[Solution: recall that

- $sat(p\mathbf{U}q) \stackrel{\text{def}}{=} sat(q) \cup (sat(p) \cap sat(\ \mathbf{X}(p\mathbf{U}q)))$
- $sat(\mathbf{F}r) \stackrel{\text{def}}{=} sat(r) \cup sat(\mathbf{XF}r)$

Thus
$S_1 \in sat(p\mathbf{U}q)$, $S_1 \in sat(\mathbf{F}r)$,
$S_2 \in sat(p\mathbf{U}q)$, $S_2 \in sat(\mathbf{F}r)$,
$S_3 \in sat(p\mathbf{U}q)$, $S_3 \notin sat(\mathbf{F}r)$.]

(a) S_2 is a successor of S_1 in T_φ.
[Solution: No. In fact, every successor of S_1 should not belong to $sat(p\mathbf{U}q)$.]

(b) S_3 is a successor of S_2 in T_φ.
[Solution: Yes. In fact, every successor of S_2 should belong to $sat(p\mathbf{U}q)$ and should not belong to $sat(\mathbf{F}r)$ as defined above, which is the case of S_3.]

(c) S_3 is an initial state of T_φ.
[Solution: Yes. In fact, every initial state T_φ should belong to $(S \setminus sat(\mathbf{F}r)) \cup sat(p\mathbf{U}q)$ as defined above, which is the case of S_3.]

(d) S_2 is an accepting state of T_φ.
[Solution: No. Since there is only one (relevant) positive $\mathbf{U}$-subformula in φ, we have only one group of accepting states, these which belong to $sat(\neg(p\mathbf{U}q)) \cup sat(q)$. S_2 does not belong to it, because it belongs to $sat(p\mathbf{U}q)$ and not to $sat(q)$.]

9

Given the following LTL Model Checking problem $M \models \varphi$ expressed in NuXMV input language:

```
MODULE main
VAR x : boolean; y : boolean;
INIT (!x & !y)
TRANS (next(x) <-> !x) & (next(y) <-> (x<->y))

LTLSPEC G (x<->y)
```

1. Write a Boolean formula corresponding to the Bounded Model Checking problem with $k = 2$.

   [Solution: We have $I(x, y) \stackrel{\text{def}}{=} (\neg x \wedge \neg y)$, $R(x, y, x', y') \stackrel{\text{def}}{=} (x' \leftrightarrow \neg x) \wedge (y' \leftrightarrow (x \leftrightarrow y))$, and $\neg\varphi \stackrel{\text{def}}{=} \mathbf{F}\neg(x \leftrightarrow y)$. Thus the resulting formula is:

$$
\begin{array}{lcl}
(\neg x_0 \wedge \neg y_0) & \wedge & // \ I(x_0, y_0) \wedge \\
(x_1 \leftrightarrow \neg x_0) \wedge (y_1 \leftrightarrow (x_0 \leftrightarrow y_0)) & \wedge & // \ R(x_0, y_0, x_1, y_1) \wedge \\
(x_2 \leftrightarrow \neg x_1) \wedge (y_2 \leftrightarrow (x_1 \leftrightarrow y_1)) & \wedge & // \ R(x_1, y_1, x_2, y_2) \wedge \\
(\neg(x_0 \leftrightarrow y_0) & \vee & // \ (f(x_0, y_0, z_0) \vee \\
\ \neg(x_1 \leftrightarrow y_1) & \vee & // \ \ f(x_1, y_1, z_1) \vee \\
\ \neg(x_2 \leftrightarrow y_2)) & & // \ \ f(x_2, y_2, z_2))
\end{array}
$$

   ]

2. Is there a solution? If yes, find the corresponding execution.

   [Solution: Yes. $\{x_0 = y_0 = \bot, x_1 = y_1 = \top, x_2 = \bot, y_2 = \top\}$ satisfies the formula. This corrsponds to the execution: $(0, 0) \longrightarrow (1, 1) \longrightarrow (0, 1)$. (States are resapresented as (x_i, y_i).)]

3. From the answers of questions 1) and 2) we can deduce

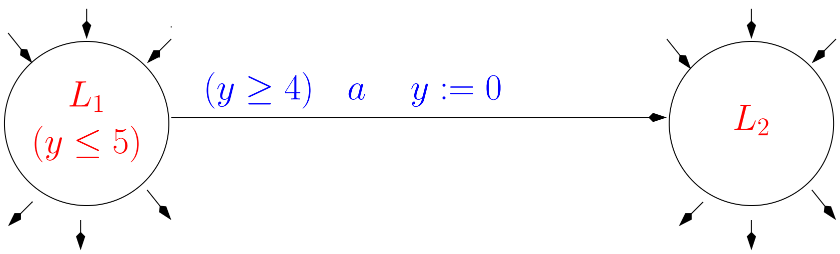
   (a) that $M \models \varphi$. [Solution: No]

   (b) that $M \not\models \varphi$. [Solution: Yes, because a counter-model of length 2 is produced.]

   (c) nothing. [Solution: No]

10

Consider the following switch e in a timed automaton:

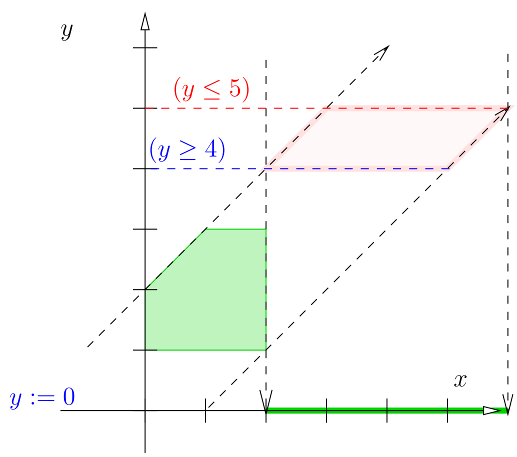


and consider the zone $Z1 \stackrel{\text{def}}{=} \langle L_1, \varphi \rangle$ s.t

$$\varphi \stackrel{\text{def}}{=} (x \geq 0) \wedge (x \leq 2) \wedge (y \geq 1) \wedge (y \leq 3) \wedge (y - x \leq 2).$$

Compute $succ(\varphi, e)$, displaying the process in a cartesian graph.

[Solution: The behaviour of $succ(\varphi, e)$ is displayed in the following diagram:



from which the solution is $succ(\varphi, e) = (x \geq 2) \wedge (x \leq 6) \wedge (y = 0)$.]