Course “Formal Methods” TEST

Roberto Sebastiani
DISI, Università di Trento, Italy

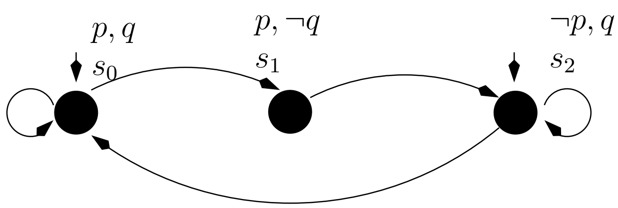
June 10^{th}, 2022

857976918

[COPY WITH SOLUTIONS]

1

Consider the following Kripke Model M:



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

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

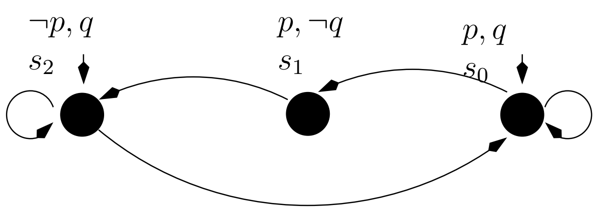
(b) $M \models \mathbf{G}\neg p$
[Solution: false]

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

(d) $M \models \mathbf{G}(p \vee q)$
[Solution: true]

2

Consider the following Kripke Model M:



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

(a) $M \models \mathbf{EG}q$
[Solution: true]

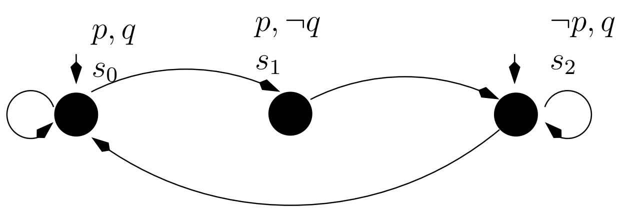
(b) $M \models \mathbf{AF}p$
[Solution: false]

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

(d) $M \models (\mathbf{AGAF}\neg q)$
[Solution: false]

3

Consider the following *fair* Kripke Model M:



where the fairness properties are expressed by the following LTL formulas: $\mathbf{GF}\neg q$, $\mathbf{GF}\neg p$.

For each of the following facts, say if it is true or false in CTL.
cacchio: p $\neg p$ q $\neg q$

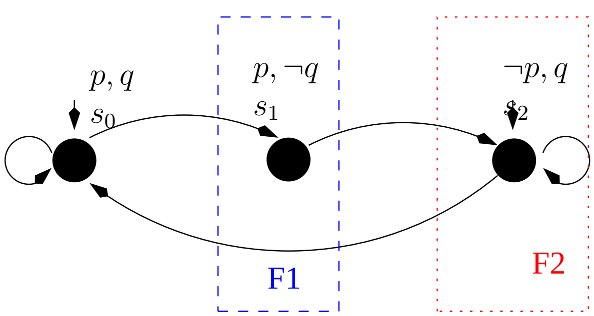
(a) $M \models \mathbf{EG}q$
[Solution: false]

(b) $M \models \mathbf{AF}p$
[Solution: true]

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

(d) $M \models (\mathbf{AGAF}\neg q)$
[Solution: true]

[Solution: In fact, the graphical representation of M is:

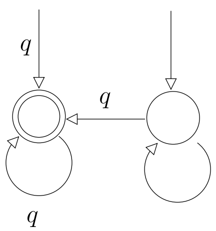


so that the paths in the form $...[s_0]^\omega$ and $...[s_2]^\omega$ are not fair paths (that is, no infinite loops in s_0 or in s_2).]

4

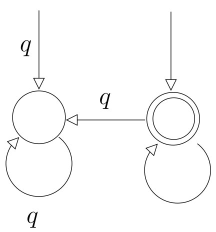
For each of the following fact regarding Buchi automata, say if it true or false.

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



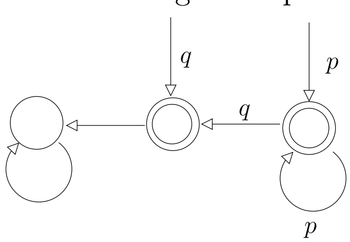
[Solution: True.]

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



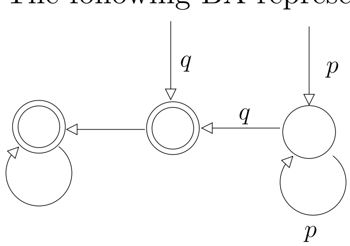
[Solution: False. It accepts every execution.]

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



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

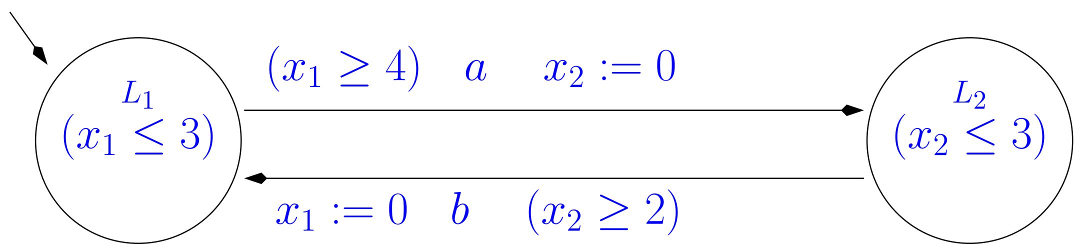
(d) The following BA represents $p\mathbf{U}q$:



[Solution: True]

5

Consider the following timed automaton A, x_1 and x_2 being clocks:



Considere the correponding Region automaton R(A). For each of the following pairs of states of A, say if the two states belong to the same region. (States are represented as $(Location, x_1, x_2)$.)

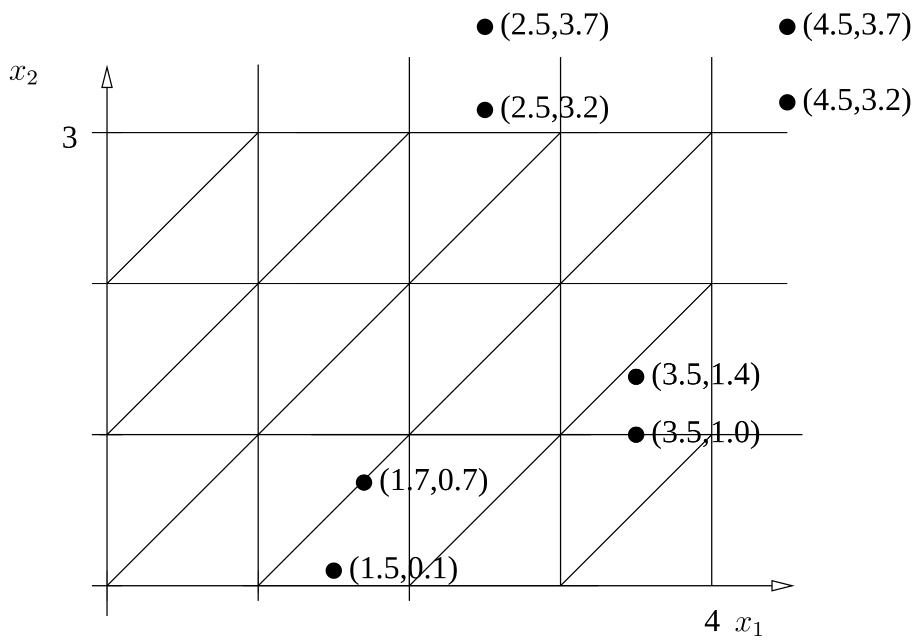
(a) $s_0 = (L_1, 2.5, 3.2)$, $s_1 = (L_1, 2.5, 3.7)$
[Solution: true]

(b) $s_0 = (L_1, 4.5, 3.2)$, $s_1 = (L_1, 4.5, 3.7)$
[Solution: true]

(c) $s_0 = (L_2, 3.5, 1.4)$, $s_1 = (L_2, 3.5, 1.0)$
[Solution: false]

(d) $s_0 = (L_2, 1.7, 0.7)$, $s_1 = (L_2, 1.5, 0.1)$
[Solution: false]

[Solution: The regions of R(A) are partitioned as follows:



]

6

Let

$$\varphi \stackrel{\text{def}}{=} (\;\; A_2 \leftrightarrow \left(\begin{array}{ll} (\;\; A_3 \vee \;\; A_6 \vee \;\; A_8) & \wedge \\ (\;\; A_5 \vee \;\; A_7 \vee \;\; A_8) & \wedge \\ (\neg A_4 \vee \neg A_6 \vee \neg A_8) & \wedge \\ (\neg A_6 \vee \;\; A_7 \vee \neg A_8) & \wedge \\ (\neg A_3 \vee \;\; A_6 \vee \;\; A_9) & \wedge \\ (\neg A_6 \vee \neg A_8 \vee \neg A_9) & \wedge \\ (\;\; A_3 \vee \;\; A_4 \vee \neg A_5) & \wedge \\ (\;\; A_5 \vee \;\; A_8 \vee \neg A_9) & \wedge \\ (\neg A_3 \vee \neg A_8 \vee \neg A_4) & \wedge \\ (\;\; A_6 \vee \;\; A_4 \vee \neg A_7) & \wedge \\ (\;\; A_5 \vee \;\; A_8 \vee \neg A_1) & \wedge \\ (\neg A_4 \vee \neg A_7 \vee \neg A_9) & \end{array} \right)).$$

Using the variable ordering:

$$\text{"} \;\; A_1, \;\; A_3, \;\; A_4, \;\; A_5, \;\; A_6, \;\; A_7, \;\; A_8, \;\; A_9\text{"},$$

draw the OBDD corresponding to the formula φ' defined as:

$$\varphi' \stackrel{\text{def}}{=} \exists \;\; A_2.\varphi.$$

[Solution: Trivial, because φ is in the form "($\;A_2 \leftrightarrow \psi$)", Thus:

$$\begin{array}{lll} \varphi' \stackrel{\text{def}}{=} & \exists \;\; A_2.(\;\; A_2 \leftrightarrow \psi) & \\ = & ((\;\; A_2 \leftrightarrow \psi)[\;\; A_2 := \top]) & \vee \;\; ((\;\; A_2 \leftrightarrow \psi)[\;\; A_2 := \bot]) \\ = & \psi & \vee \;\; \neg\psi \\ = & \top & \end{array}$$

which corresponds to the following OBDD:

$$\boxed{\top}$$

]

7

Consider the following pair of SMT($\mathcal{LRA}$) sets of literals:

$$\begin{array}{lcl} A & \stackrel{\text{def}}{=} & \{(0 \le -3x_1 - 5x_2 + 1), (0 \le x_1 + x_2)\} \\ B & \stackrel{\text{def}}{=} & \{(0 \le 3x_3 - 2x_1 - 3), (0 \le x_1 - 2x_3 + 1)\}. \end{array}$$

(a) Write a proof P of $\mathcal{LRA}$-unsatisfiablity of $A \wedge B$

[Solution: A proof of unsatisfiability P for $A \wedge B$ is the following:

$$\dfrac{\dfrac{(0 \le -3x_1 - 5x_2 + 1) \quad (0 \le x_1 + x_2)}{\textsc{Comb} \ \ (0 \le 2x_1 + 1) \ \textit{with c. 1 and 5}} \quad \dfrac{(0 \le 3x_3 - 2x_1 - 3) \quad (0 \le x_1 - 2x_3 + 1)}{\textsc{Comb} \ \ (0 \le -x_1 - 3) \ \textit{with c. 2 and 3}}}{\textsc{Comb} \ \ (0 \le -5) \ \textit{with c. 1 and 2}}$$

]

(b) From such a proof, compute a $\mathcal{LRA}$-interpolant for $\langle A, B\rangle$ using McMillan's technique.

[Solution: An interpolant $\langle A, B\rangle$ is the following:

$$\dfrac{\dfrac{(0 \le -3x_1 - 5x_2 + 1) \quad (0 \le x_1 + x_2)}{\textsc{Comb} \ \ (0 \le 2x_1 + 1) \ \textit{with c. 1 and 5}} \quad \dfrac{(0 \le 0) \quad (0 \le 0)}{\textsc{Comb} \ \ (0 \le 0) \ \textit{with c. 2 and 3}}}{\textsc{Comb} \ \ (0 \le 2x_1 + 1) \ \textit{with c. 1 and 2}}$$

Thus, the interpolant obtained is $(0 \le 2x_1 + 1)$.]

8

Given the function

OBDD $Preimage$(**OBDD** X)

which computes symbolically the preimage of a set of states X wrt. the transition relation of the Kripke model, write the pseudo-code of the function:

OBDD $CheckEU$(**OBDD** X_1, X_2)

computing symbolically the (OBDD representing) the denotation of $\mathbf{E}[\varphi_1 \mathbf{U} \varphi_2]$, X_1, X_2 being the OBDDs representing the denotation of φ_1 and φ_2.
[Solution:

```
OBDD CheckEU(OBDD X1, X2)
    Y' := X2;
    repeat
        Y := Y';
        Y' := X2 ∨ (X1 ∧ Preimage(Y));
    until (Y ↔ Y');
return Y;
}
```

]

9

Given the following finite state machine expressed in NuSMV input language:

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

Write:

(*a*) the Boolean formulas $I(v_1, v_2, v_3)$ and $T(v_1, v_2, v_3, v_1', v_2', v_3')$ representing respectively the initial states and the transition relation of M.

[Solution: $I(v_1, v_2, v_3)$ is $(v_1 \wedge \neg v_2)$, $T(v_1, v_2, v_3, v_1', v_2', v_3')$ is $(v_1' \leftrightarrow v_2) \wedge (v_2' \leftrightarrow v_3) \wedge (v_3' \leftrightarrow v_1)$]

(*b*) the Boolean formula representing symbolically the set of states which are reached after exactly one step. [The formula must be computed symbolically, not simply inferred from the graph of the next question!]

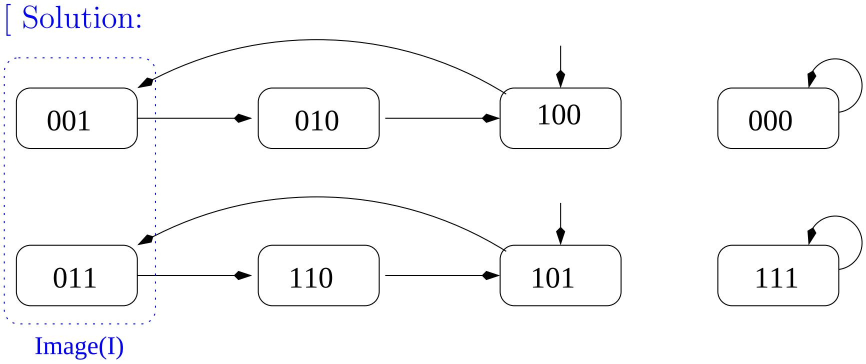
[Solution: The formula is the forward image of the initial states. [For better readability, here we represent it in terms of current variables v_i and next variables v_i' rather than of step-indexed variables $v_i^{(0)}$ and $v_i^{(1)}$]

$$\begin{array}{rcl}
Image(I) & = & \exists v_1, v_2, v_3.(T(v_1, v_2, v_3, v_1', v_2', v_3') \wedge I(v_1, v_2, v_3)) \\
& = & \exists v_1, v_2, v_3.((v_1' \leftrightarrow v_2) \wedge (v_2' \leftrightarrow v_3) \wedge (v_3' \leftrightarrow v_1) \wedge (v_1 \wedge \neg v_2)) \\
& = & \exists v_1, v_2, v_3.((\neg v_1') \wedge (v_2' \leftrightarrow v_3) \wedge (v_3') \wedge (v_1 \wedge \neg v_2)) \\
& = & \bot \vee \bot \vee \overbrace{(\neg v_1' \wedge \neg v_2' \wedge v_3')}^{v_1=\top, v_2=\bot, v_3=\bot} \vee \overbrace{(\neg v_1' \wedge v_2' \wedge v_3')}^{v_1=\top, v_2=\bot, v_3=\top} \bot \vee \bot \vee \bot \vee \bot \\
& = & (\neg v_1' \wedge \neg v_2' \wedge v_3') \vee (\neg v_1' \wedge v_2' \wedge v_3') \\
& = & (\neg v_1' \wedge v_3')
\end{array}$$

.]

(*c*) the graph representing the FSM.
(Assume the notation "$v_1 v_2 v_3$" for labeling the states: e.g. "100" means "$v_1 = 1, v_2 = 0, v_3 = 0$".)

[Solution:



]

10

Consider the following ground and abstract machines M and M', and the abstraction $\alpha : M \longmapsto M'$:

M:

```
MODULE main
VAR
x:boolean; y:boolean; z:boolean;
INIT (x & y & z)
TRANS
((next(x)<->y)&(next(y)<->z)&(next(z)<->x))
LTLSPEC   G (x | y ) ;
```

M':

```
MODULE main
VAR
x:boolean; y:boolean; z:boolean;
INIT (x & y)
TRANS
((next(x)<->y)&(next(y)<->z))
LTLSPEC   G (x | y ) ;
```

[Solution: Notice that the abstraction α makes the variable `z` invisible.]

1. Find a length-2 execution c_0, c_1, c_2 of M' violating the specification (notationally, represent a state as $(x, y, [z])$.)

   [Solution: $(1, 1, [0]) \Longrightarrow (1, 0, [0]) \Longrightarrow (0, 0, [0])$]

2. Use the SAT-based refinement technique to check whether the abstract counter-example you found is spurious or not.

   [Solution: We generate the following formula and feed it to a SAT solver:

$$\begin{array}{lcl}
(x_0 \wedge y_0 \wedge z_0) & \wedge & // \; I(x_0, y_0, z_0) \wedge \\
((x_1 \leftrightarrow y_0) \wedge (y_1 \leftrightarrow z_0) \wedge (z_1 \leftrightarrow x_0)) & \wedge & // \; T(x_0, y_0, z_0, x_1, y_1, z_1) \wedge \\
((x_2 \leftrightarrow y_1) \wedge (y_2 \leftrightarrow z_1) \wedge (z_2 \leftrightarrow x_1)) & \wedge & // \; T(x_1, y_1, z_1, x_2, y_2, z_2) \wedge \\
(\; x_0 \wedge \; y_0) & \wedge & // \; (visible(s_0) = c_0) \wedge \\
(\; x_1 \wedge \neg y_1) & \wedge & // \; (visible(s_1) = c_1) \wedge \\
(\neg x_2 \wedge \neg y_2) & & // \; (visible(s_2) = c_2)
\end{array}$$

   The formula is trivially unsatisfiable, since the first three rows force assigning all variables to true, which contradicts the last two rows.]

3. From the answers to questions 1. and 2. we can conclude that:

   (a) M verifies the LTL property
   (b) M does not verify the LTL property
   (c) we can conclude nothing.

   [Solution: (c). In fact we have found a spurious counter-example.
   ]