Course “Formal Methods”
TEST

Roberto Sebastiani
DISI, Università di Trento, Italy

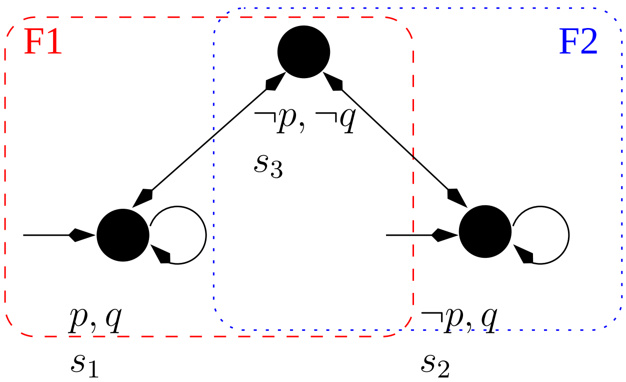
June 7^{th}, 2018

769857918

[COPY WITH SOLUTIONS]

1

Consider the following <u>*fair*</u> Kripke Model M:



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

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

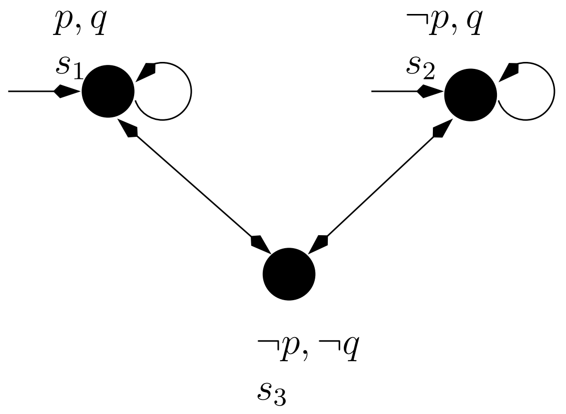
(b) $M \models \mathbf{FG}p$
[Solution: false]

(c) $M \models q$
[Solution: true]

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

2

Consider the following Kripke Model M:



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

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

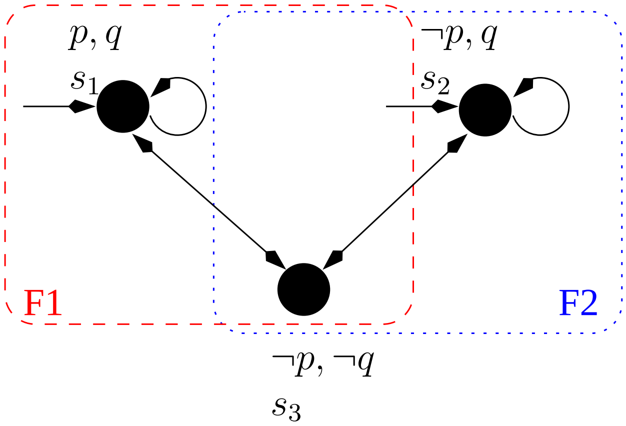
(b) $M \models \mathbf{EFEG}p$
[Solution: true]

(c) $M \models (\mathbf{AGAF}p \wedge \mathbf{AGAF}\neg p \wedge \mathbf{AGAF}\neg q) \to q$
[Solution: true]

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

3

Consider the following *fair* Kripke Model M:



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

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

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

(c) $M \models q$
[Solution: true]

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

4

Let φ be a generic Boolean formula. Let:

- φ_{tree} be the result of converting φ into Negative Normal Form, using a tree representation.
- φ_{dag} be the result of converting φ into Negative Normal Form, using a DAG representation.

Let $|\varphi|$, $|\varphi_{tree}|$, and $|\varphi_{dag}|$ denote the size of φ, φ_{tree}, and φ_{dag} respectively.

For each of the following sentences, say if it is true or false.

(a) $|\varphi_{tree}|$ is in worst-case exponential in size wrt. $|\varphi|$
[Solution: True. (Its size may blow exponentially on the number of "$\leftrightarrow$"s in φ.)]

(b) $|\varphi_{dag}|$ is in worst-case exponential in size wrt. $|\varphi|$
[Solution: False. (The sharing of the nodes avoids the exponential blowup in size, so that $|\varphi_{dag}|$ is at most twice as big as $|\varphi|$.)]

(c) If φ is in the form

$$\neg \bigvee_{j=1}^{N} \bigwedge_{i=1}^{K} l_{ij}$$

s.t. l_{ij}'s are Boolean literals, then $|\varphi_{tree}|$ is exponential in size wrt. $|\varphi|$
[Solution: False. In fact there are no $\leftrightarrow$'s in φ.]

(d) If φ is in the form

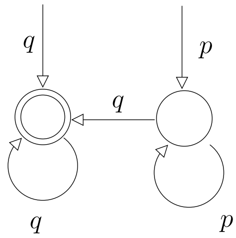
$$(\bigwedge_{j=1}^{N} (l_{j1} \leftrightarrow l_{j2})) \leftrightarrow (\bigwedge_{i=1}^{K} (l_{i1} \leftrightarrow l_{i2}))$$

s.t. l_{ij}'s are Boolean literals, then $|\varphi_{dag}|$ is linear in size wrt. $|\varphi|$
[Solution: True. Due to node sharing, $|\varphi_{dag}|$ is always linear, regardless the occurrences of $\leftrightarrow$'s.]

5

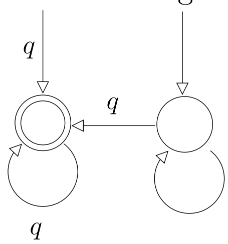
For each of the following facts about Buchi automata, say if it true or false.

(a) The following BA represents the LTL formula $p\mathbf{U}q$.



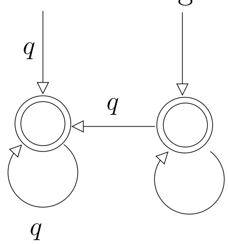
[Solution: No]

(b) The following BA represents the LTL formula $\mathbf{FG}q$.



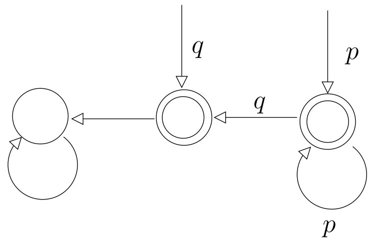
[Solution: Yes]

(c) The following BA represents the LTL formula $\mathbf{FG}q$.



[Solution: No]

(d) The following BA represents the LTL formula $p\mathbf{U}q$.



[Solution: No]

6

In a counter-example-guided-abstraction-refinement model checking process using localization reduction, variables $x_3, x_4, x_5, x_6, x_7, x_8$ are made invisible.

Suppose the process has identified a spurious counterexample with an abstract failure state [00], two ground deadend states d_1, d_2 and two ground bad states b_1, b_2 as described in the following table:

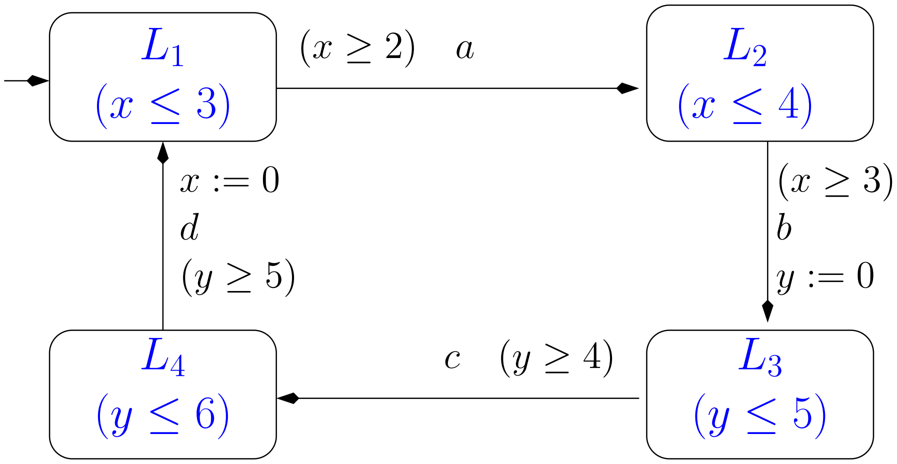
	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
d_1	0	0	0	0	0	1	1	1
d_2	0	0	0	1	1	1	1	0
b_1	0	0	1	1	1	1	0	1
b_2	0	0	0	1	0	0	0	0

Identify a minimum-size subset of invisible variables which must be made visible in the next abstraction to avoid the above failure. Briefly explain why.

[Solution: The minimum-size subset is $\{x_7\}$. In fact, if x_7 is made visible, then both d_1, d_2 are made different from both b_1, b_2.]

7

Consider the following timed automaton.



(a) What is the maximum amount of time units which can pass from two consecutive events b? Briefly explain why.
[Solution: $6 + 4 = 10$. You need at most 6 from b to d and at most 4 to pass from d to b.]

(b) What is the minimum amount of time units which can pass from two consecutive events b? Briefly explain why.
[Solution: $5 + 3 = 8$. You need at least 5 from b to d and at least 3 to pass from d to b.]

(c) What is the maximum amount of time which can pass from event c and the subsequent event d? Briefly explain why.
[Solution: $6 - 4 = 2$. c can happen when $y \geq 4$ and d can happen when $y \leq 6$.]

(d) What is the minimum amount of time which can pass from event a and the subsequent event b? Briefly explain why.
[Solution: $3 - 3 = 0$. a can happen when $x \leq 3$ and b can happen when $x \geq 3$.]

8

Consider the following LTL formula:

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

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: No. In fact, every initial state T_φ should belong to $(sat(p\mathbf{U}q) \cap sat(\mathbf{F}r))$ as defined above, which is not the case of S_3.]

(*d*) S_1 verifies all accepting conditions of T_φ.
[Solution: Yes. In fact, since there are two positive until-subformulas $p\mathbf{U}q$ and $\mathbf{F}r$, so that to verify the first accepting condition it should belong to $sat(\neg(p\mathbf{U}q)) \cup sat(q)$, for the secomnd it should belong to $sat(\neg(\mathbf{F}r)) \cup sat(r)$, which is the case of S_1.]

9

Let

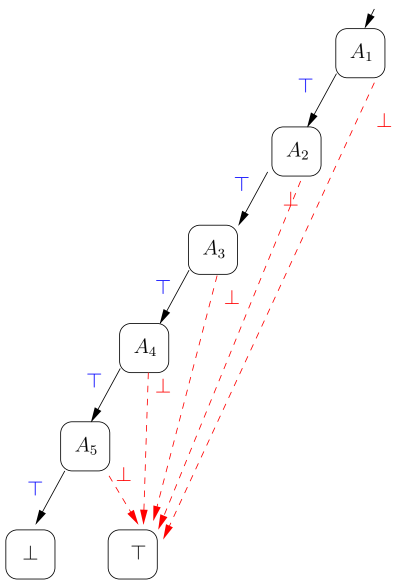
$$\varphi \stackrel{\text{def}}{=} \neg \left(\begin{array}{rrl} & (\quad A_1) & \wedge \\ (\quad A_1 \rightarrow & A_2) & \wedge \\ (\quad A_2 \rightarrow & A_3) & \wedge \\ (\quad A_3 \rightarrow & A_4) & \wedge \\ (\quad A_4 \rightarrow & A_5) & \wedge \end{array} \right)$$

Using the variable ordering:

$$" \quad A_1 \quad A_2, \quad A_3, \quad A_4, \quad A_5",$$

draw the OBDD corresponding to the formula φ

[Solution: It corresponds to the following OBDD:



(Notice also that the formula is equivalent to $\neg(\quad A_1 \wedge \quad A_2 \wedge \quad A_3 \wedge \quad A_4 \wedge \quad A_5))$
]

10

Given a symbolic representation of a finite state machine M, expressed in terms of the following two Boolean formulas: $I(x, y) \stackrel{\text{def}}{=} (x \wedge y)$, $T(x, y, x', y') \stackrel{\text{def}}{=} ((x' \leftrightarrow (x \leftrightarrow y) \wedge (y' \leftrightarrow (\neg x \leftrightarrow y))$, and given the LTL property: $\varphi \stackrel{\text{def}}{=} \neg\mathbf{G}(x \vee y)$,

(a) Write a Boolean formula whose models (if any) represent length-2 executions of M violating φ.

[Solution: The question corresponds to the Bounded Model Checking problem $M \models_2 \mathbf{E}\,\mathbf{G} f$ s.t. $f(x, y) \stackrel{\text{def}}{=} (x \vee y)$. Thus we have:

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

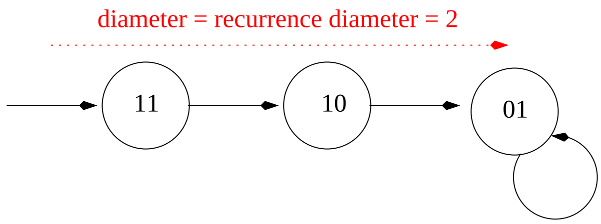
]

(b) Is there a solution? If yes, find the corresponding execution. If not, explain why. [The answer must be based on the Boolean formula, not on the graphical representation of the FSM.]

[Solution: yes, because the formula is satisfiable. In fact, the first two rows force the assignment $\{x_0, y_0, x_1, \neg y_1, \neg x_2, y_2\}$ which satisfies the whiole formula, –in particular, it satisfies the third loopback— corresponding to the cyclic execution path: $\underbrace{(1,1)}_{s_0} \rightarrow \underbrace{(1,0)}_{s_1} \rightarrow \underbrace{(0,1)}_{s_2} \leftrightarrow \underbrace{(0,1)}_{s_2}$.]

(c) What are the diameter and the recurrence diameter of this system?

[Solution:



]

(d) From your answers to questions (b) and (c) you can conclude that:

(i) $M \models \neg\mathbf{G}(x \vee y)$

(ii) $M \not\models \neg\mathbf{G}(x \vee y)$

(iii) you can conclude nothing.

[Solution: (ii) $M \not\models \neg\mathbf{G}(x \vee y)$, since we have found a counter-example.]