Course "Formal Methods"
TEST

Roberto Sebastiani
DISI, Università di Trento, Italy

June 7^{th}, 2018

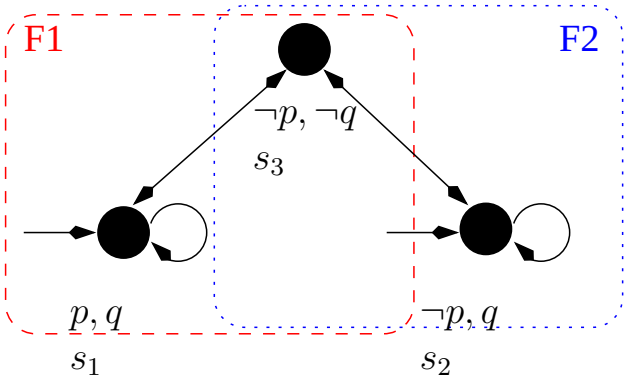
769857918

Name (please print):

Surname (please print):

1

Consider the following *fair* Kripke Model M:



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

(*a*) $M \models \mathbf{GF}\neg p$

(*b*) $M \models \mathbf{FG}p$

(*c*) $M \models q$

(*d*) $M \models (p\mathbf{U}\neg q)$

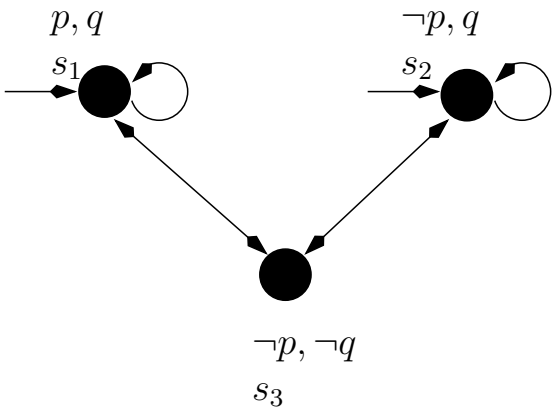
[SCORING [0...100]:

- +25pts for each correct answer
- -25pts for each incorrect answer
- 0pts for each unanswered question

]

2

Consider the following Kripke Model M:



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

(a) $M \models \mathbf{AGAF}\neg p$

(b) $M \models \mathbf{EFEG}p$

(c) $M \models (\mathbf{AGAF}p \wedge \mathbf{AGAF}\neg p \wedge \mathbf{AGAF}\neg q) \rightarrow q$

(d) $M \models \mathbf{E}(p\mathbf{U}\neg q)$

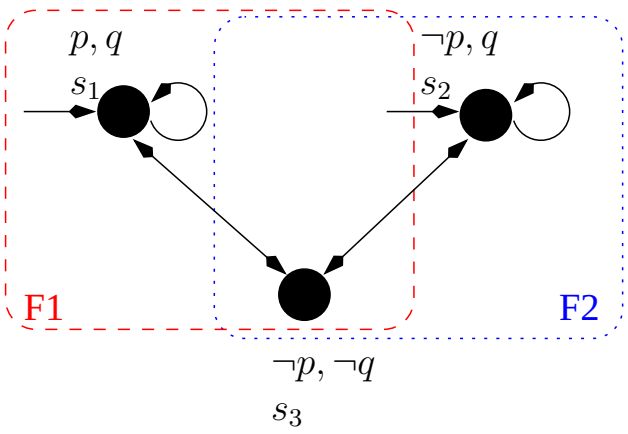
[SCORING [0...100]:

- +25pts for each correct answer
- -25pts for each incorrect answer
- 0pts for each unanswered question

]

3

Consider the following *fair* Kripke Model M:



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

(*a*) $M \models \mathbf{AGAF}\neg p$

(*b*) $M \models \mathbf{EFEG}p$

(*c*) $M \models q$

(*d*) $M \models \mathbf{E}(p\mathbf{U}\neg q)$

[SCORING [0...100]:

- +25pts for each correct answer
- -25pts for each incorrect answer
- 0pts for each unanswered question

]

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. $|\varphi|$

(b) $|\varphi_{dag}|$ is in worst-case exponential in size wrt. $|\varphi|$

(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. $|\varphi|$

(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. $|\varphi|$

[SCORING [0...100]:

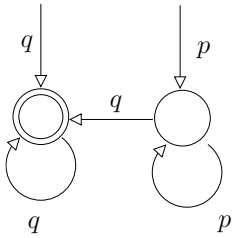
- +25pts for each correct answer
- -25pts for each incorrect answer
- 0pts for each unanswered question

]

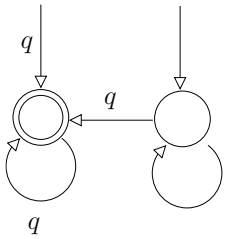
5

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

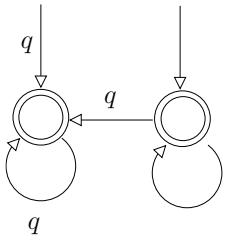
(a) The following BA represents the LTL formula $p\mathbf{U}q$.



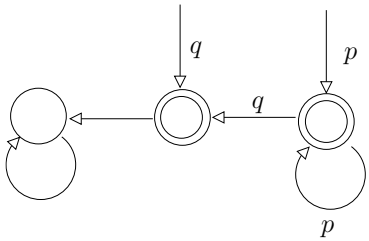
(b) The following BA represents the LTL formula $\mathbf{FG}q$.



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



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



[SCORING [0...100]:

- +25pts for each correct answer
- -25pts for each incorrect answer
- 0pts for each unanswered question

]

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:

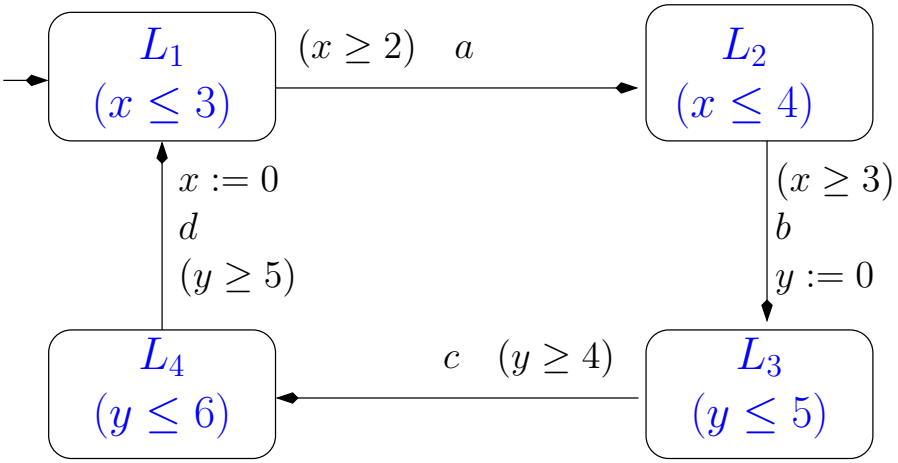
	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
d_1	0	0	0	0	0	1	1	1
d_2	0	0	0	1	1	1	1	0
b_1	0	0	1	1	1	1	0	1
b_2	0	0	0	1	0	0	0	0

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.

[SCORING: [0...100], 100 pts iff the solution is correct, minimum an properly explained. .]

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.

(b) What is the minimum amount of time units which can pass from two consecutive events b? Briefly explain why.

(c) What is the maximum amount of time which can pass from event c and the subsequent event d? Briefly explain why.

(d) What is the minimum amount of time which can pass from event a and the subsequent event b? Briefly explain why.

[SCORING: [0...100], 25 pts for each correct answer, no penalties for wrong answers..]

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.

(*a*) S_2 is a successor of S_1 in T_φ.
(*b*) S_3 is a successor of S_2 in T_φ.
(*c*) S_3 is an initial state of T_φ.
(*d*) S_1 verifies all accepting conditions of T_φ.

[SCORING [0...100]:

- +25pts for each correct answer
- -25pts for each incorrect answer
- 0pts for each unanswered question

]

[SCORING: [0...100], 25 pts for each correct answer. No penalties for wrong answers.]

9

Let

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

Using the variable ordering:

$$\text{"} \quad A_1 \quad A_2, \quad A_3, \quad A_4, \quad A_5\text{"},$$

draw the OBDD corresponding to the formula φ

[SCORING: [0...100], 100 pts for a correct answer. No penalties for a wrong answer..]

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.

(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.]

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

(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.

[SCORING: [0...100], +25pts for each correct answer. No penalties for wrong answers.]