Course "Formal Methods"
TEST

Roberto Sebastiani
DISI, Università di Trento, Italy

June 10^{th}, 2022

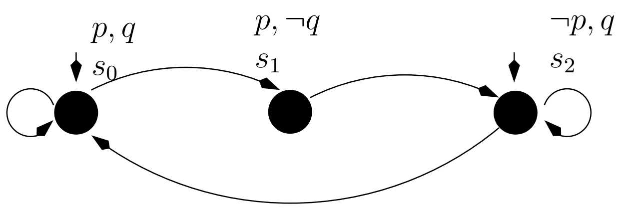
857976918

Name (please print):

Surname (please print):

1

Consider the following Kripke Model M:



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

(a) $M \models \mathbf{F}p$

(b) $M \models \mathbf{G}\neg p$

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

(d) $M \models \mathbf{G}(p \vee q)$

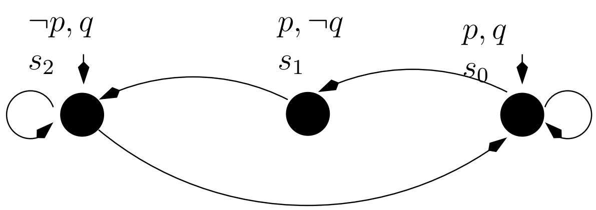
[SCORING [0...100]:

- +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) $M \models \mathbf{EG}q$

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

(c) $M \models \mathbf{AF}\neg q$

(d) $M \models (\mathbf{AGAF}\neg q)$

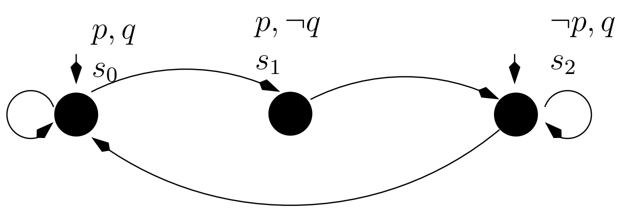
[SCORING [0...100]:

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

]

3

Consider the following *fair* Kripke Model M:



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) $M \models \mathbf{EG}q$

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

(c) $M \models \mathbf{AF}\neg q$

(d) $M \models (\mathbf{AGAF}\neg q)$

[SCORING [0...100]:

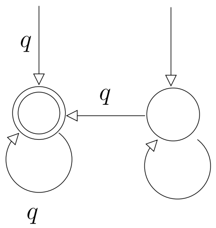
- +25pts for each correct answer
- -25pts for each incorrect answer
- 0pts for each unanswered question

]

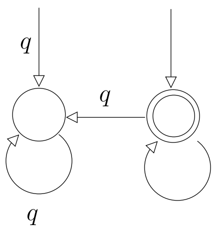
4

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

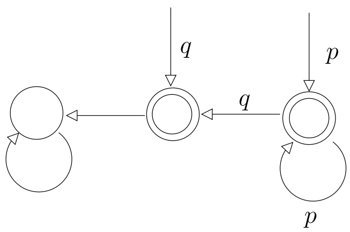
(a) The following BA represents $\mathbf{FG}q$:



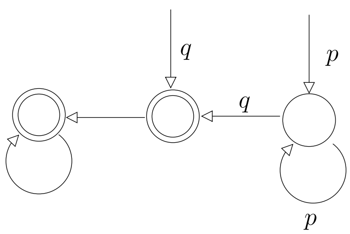
(b) The following BA represents $\mathbf{FG}q$:



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



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



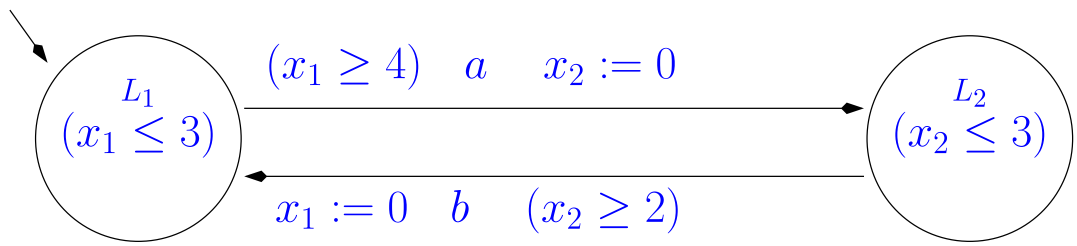
[SCORING [0...100]:

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

]

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) $s_0 = (L_1, 2.5, 3.2)$, $s_1 = (L_1, 2.5, 3.7)$

(b) $s_0 = (L_1, 4.5, 3.2)$, $s_1 = (L_1, 4.5, 3.7)$

(c) $s_0 = (L_2, 3.5, 1.4)$, $s_1 = (L_2, 3.5, 1.0)$

(d) $s_0 = (L_2, 1.7, 0.7)$, $s_1 = (L_2, 1.5, 0.1)$

[SCORING [0...100]:

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

]

6

Let

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

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:

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

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

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 $A \wedge B$

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

[SCORING: [0...100], 50 points each for questions a) and b). No penalties for wrong answers..]

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.

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

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.

(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!]

(c) the graph representing the FSM.
(Assume the notation "$v_1v_2v_3$" for labeling the states: e.g. "100" means "$v_1 = 1, v_2 = 0, v_3 = 0$".)

[SCORING: [0...100], +25pts each question (a) (c), 50pts question (b), no penalties for wrong answers.]

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 ) ;
```

1. Find a length-2 execution c_0, c_1, c_2 of M' violating the specification (notationally, represent a state as $(x, y, [z])$.)
2. Use the SAT-based refinement technique to check whether the abstract counter-example you found is spurious or not.
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.

[SCORING: [0...100], (1,3) +25pts each, (2) +50pts. No penalties for wrong answers.]