Course “Formal Methods”
TEST

Roberto Sebastiani
DISI, Università di Trento, Italy

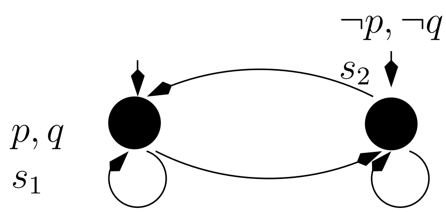
September 6^{th}, 2018

769857918

[COPY WITH SOLUTIONS]

1

Consider the following Kripke Model M:



For each of the following facts, say if it is true or false in CTL*.
[Solution: Recall that an LTL formula φ represents the same property as the CTL* formula $\mathbf{A}\varphi$.]

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

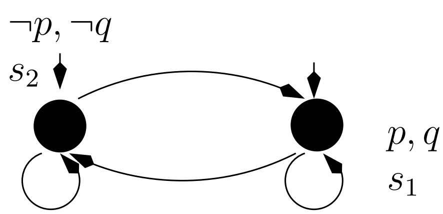
(b) $M \models \mathbf{A}(\mathbf{GF}p)$
[Solution: false]

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

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

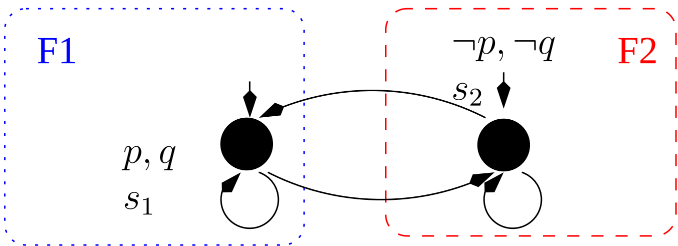
(b) $M \models \mathbf{AF}\neg p$
[Solution: false]

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

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

3

Consider the following fair Kripke Model M:



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

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

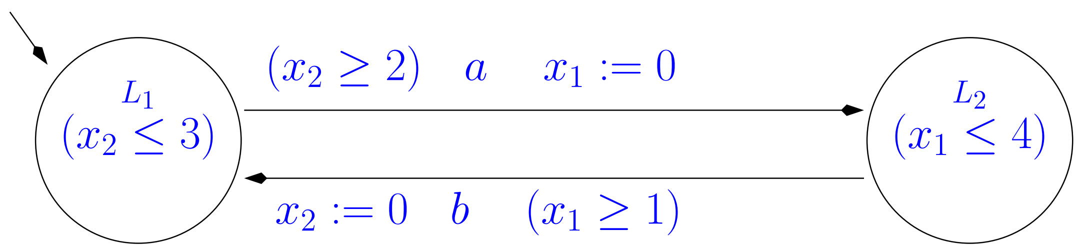
(b) $M \models \mathbf{AF}\neg p$
[Solution: true]

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

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

4

Consider the following timed automaton A:



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 $(Location, x_1, x_2)$.)

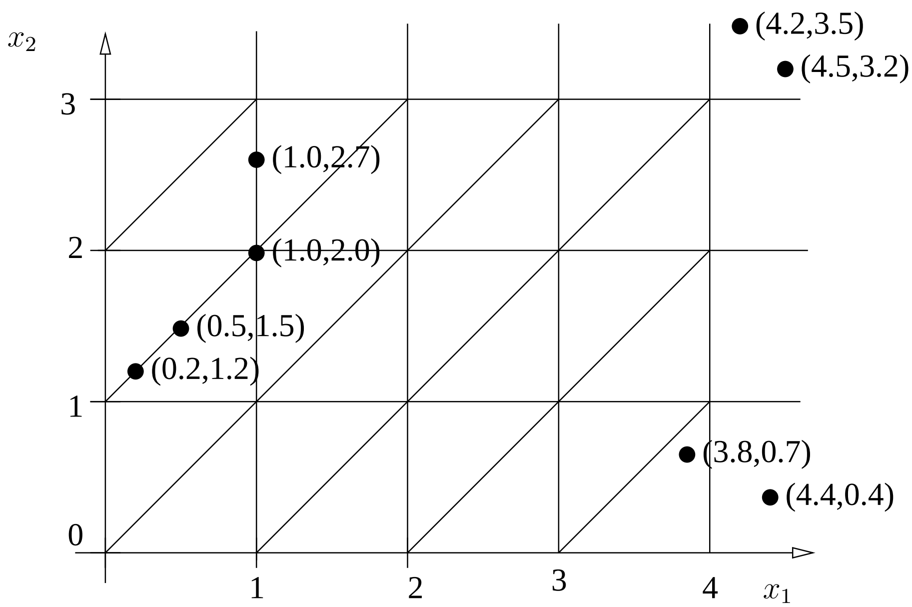
(a) $s_0 = (L_1, 4.2, 3.5)$, $s_1 = (L_1, 4.5, 3.2)$
[Solution: yes]

(b) $s_0 = (L_1, 1.0, 2.0)$, $s_1 = (L_1, 1.0, 2.7)$
[Solution: no]

(c) $s_0 = (L_2, 0.2, 1.2)$, $s_1 = (L_2, 0.5, 1.5)$
[Solution: yes]

(d) $s_0 = (L_2, 3.8, 0.7)$, $s_1 = (L_2, 4.4, 0.4)$
[Solution: no]

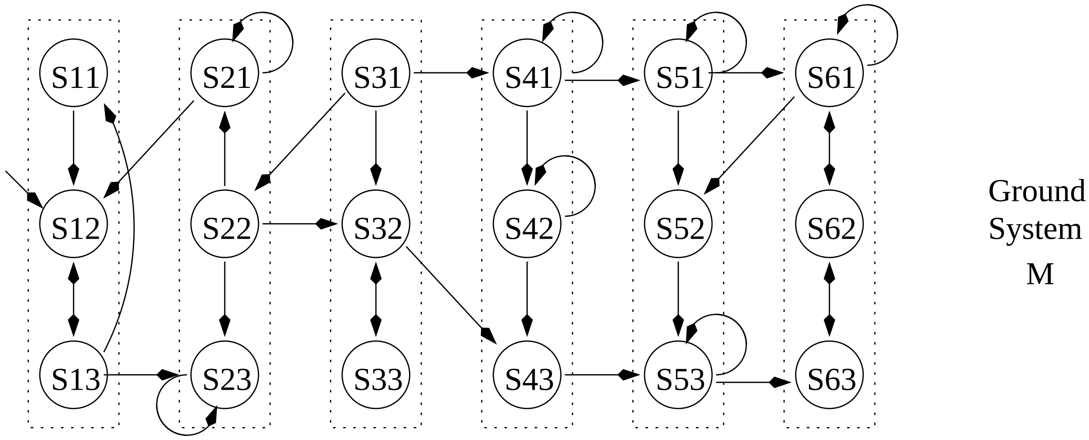
[Solution: The regions of R(A) are partitioned as follows:

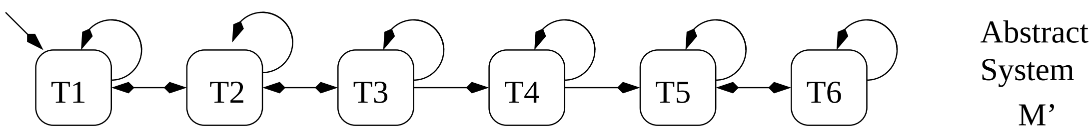


]

5

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





and the abstraction $\alpha : M \longmapsto M'$ which, for every $j \in \{1, ..., 6\}$, maps $Sj1, Sj2, Sj3$ into Tj.

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

(a) M simulates M'.
[Solution: False. E.g.,: if M is in $S23$, M' is in $T2$ and M' switches to $T3$, there is no transition in M from $S23$ to any state $S3i$, $i \in \{1, 2, 3\}$.]

(b) M' simulates M.
[Solution: true]

(c) If φ is an LTL formula and $M' \models \varphi$, then $M \models \varphi$
[Solution: true]

(d) If φ is an LTL formula and $M \models \varphi$, then $M' \models \varphi$
[Solution: false]

6

Consider the following transition relation inside a NuXMV program:

```
(...)
TRANS
(b0 -> next(b0)) & (b1 -> next(b1)) & (b2 -> next(b2)) & (b3 -> next(b3))
(...)
```

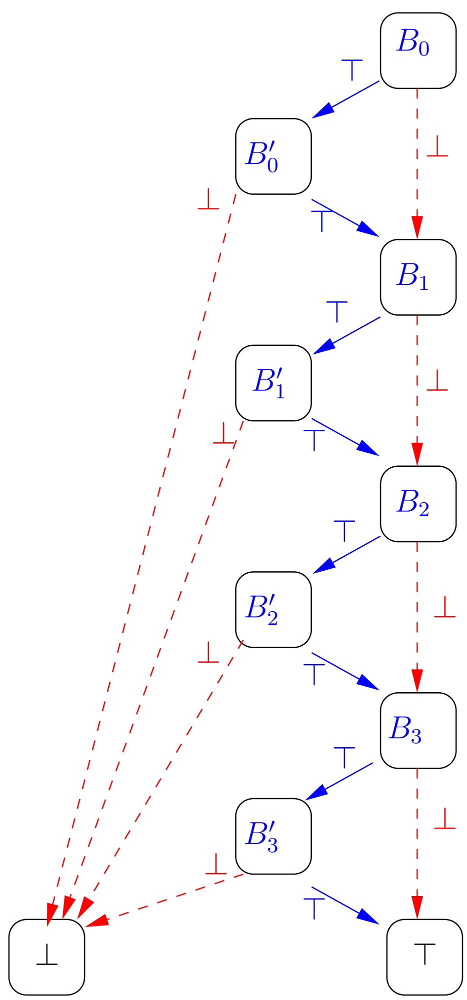
Adopting a suitable variable ordering of your choice, draw the OBDD representing such transition relation.

Use the following notation: B_i for `bi` and B_i' for `next(bi)`, for every $i \in [0, ...3]$.

[Solution: The transition relation corresponds to the Boolean formula

$$(B_0 \to B_0') \wedge (B_1 \to B_1') \wedge (B_2 \to B_2') \wedge (B_3 \to B_3')$$

The obvious choice of variable ordering is $\{B_0, B_0', B_1, B_1', B_2, B_2', B_3, B_3'\}$, and the corresponding OBDD is:



]

7

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;
}
```

]

8

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(y) <-> x)) & (next(x) <-> (y))
LTLSPEC G ! (x <-> y)
```

1. Write a Boolean formula corresponding to the Bounded Model Checking problem with k = 2., and say if it is satisfiable.

   [Solution: The question corresponds to the Bounded Model Checking problem

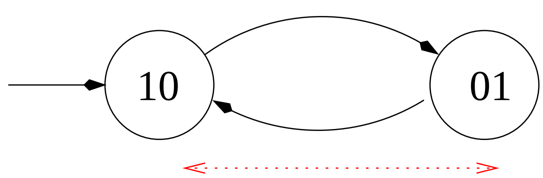
   $$M \models_2 \mathbf{E}\,\mathbf{F} f$$

   s.t. $f(x, y) \stackrel{\text{def}}{=} (x \leftrightarrow y)$. Thus we have:

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

   The formula is not satisfiable: the first three conjuncts force the assignment $\{x_0, \neg y_0, \neg x_1, y_1, x_2, \neg y_2\}$ which falsifies all three disjuncts.]

2. What are the diameter and the recurrence diameter of this system?

   [Solution: diameter = recurrence diameter = 1]

3. *From the previous answers* (and only from them!) we can conclude:

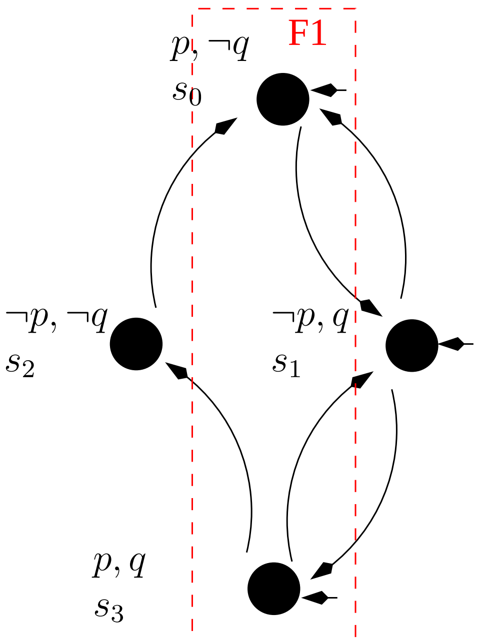
   (a) that $M \models \varphi$;
   (b) that $M \not\models \varphi$;
   (c) nothing.

   Briefly explain your choice.

   [Solution: a) $M \models \varphi$. In fact, there is no counter-example of length up to k s.t. $k > diameter(M)$.
   ]

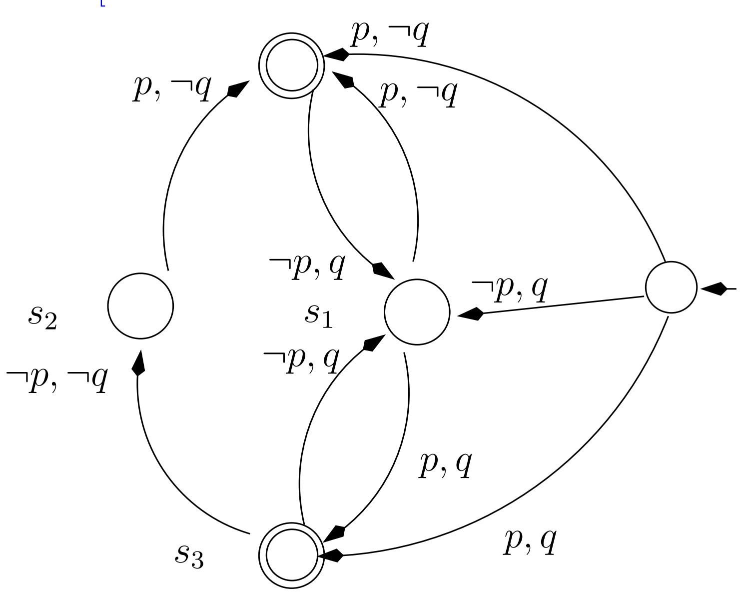
9

Consider the following fair Kripke model M:



Convert it into an equivalent Buchi automaton.

[Solution:



]

10

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

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

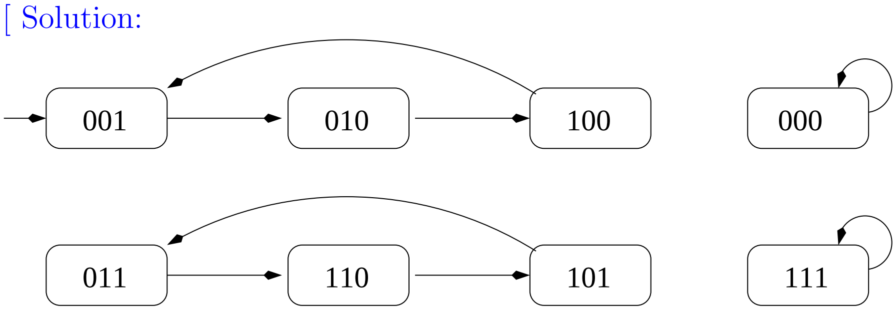
and consider the property $P \stackrel{\text{def}}{=} (v_1 \wedge \neg v_2 \wedge \neg v_3)$. Write:

(*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 $(\neg v_1 \wedge \neg v_2 \wedge v_3)$, $T(v_1, v_2, v_3, v_1', v_2', v_3')$ is $(v_1' \leftrightarrow v_2) \wedge (v_2' \leftrightarrow v_3) \wedge (v_3' \leftrightarrow v_1)$]

(*b*) the graph representing the FSM.
(Assume the notation "$v_1v_2v_3$" for labeling the states: e.g. "101" means "$v_1 = 1, v_2 = 0, v_3 = 1$".)

[Solution:



]

(*c*) the Boolean formula representing symbolically $\mathbf{EX}P$. [The formula must be computed symbolically, not simply inferred from the graph of the previous question!]

[Solution:

$$
\begin{aligned}
\mathbf{EX}(P) &= \exists v_1', v_2', v_3'.(T(v_1, v_2, v_3, v_1', v_2', v_3') \wedge P(v_1', v_2', v_3')) \\
&= \exists v_1', v_2', v_3'.((v_1' \leftrightarrow v_2) \wedge (v_2' \leftrightarrow v_3) \wedge (v_3' \leftrightarrow v_1) \wedge (v_1' \wedge \neg v_2' \wedge \neg v_3')) \\
&= \exists v_1', v_2', v_3'.((v_2 \wedge \neg v_3 \wedge \neg v_1) \wedge (v_1' \wedge \neg v_2' \wedge \neg v_3')) \\
&= \bot \vee \bot \vee \overbrace{(v_2 \wedge \neg v_3 \wedge \neg v_1)}^{v_1'=\top, v_2'=v_3'=\bot} \vee \bot \vee \bot \vee \bot \vee \bot \vee \bot \\
&= (v_2 \wedge \neg v_3 \wedge \neg v_1)
\end{aligned}
$$

.]