Course "Formal Methods"
or
Joint Courses "Automated Reasoning & Formal Verification"
TEST

Roberto Sebastiani
DISI, Università di Trento, Italy

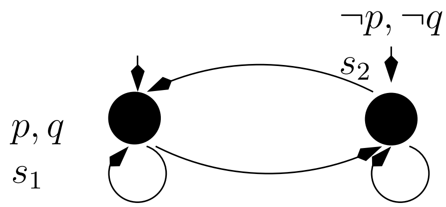
July 7^{th}, 2022

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 CTL*.
[Solution: Recall that an LTL formula φ represents the same property as the CTL* formula $\mathbf{A}\varphi$.]

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

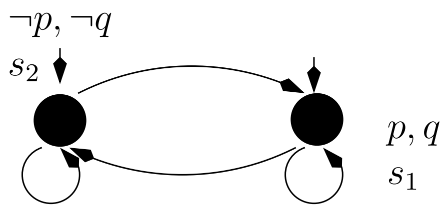
(b) $M \models \mathbf{A}(\mathbf{GF}p)$
[Solution: false]

(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]

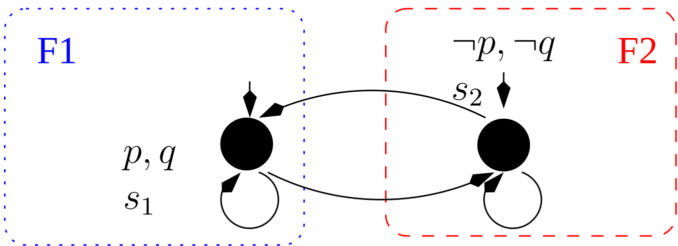
(b) $M \models \mathbf{AF}\neg p$
[Solution: false]

(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 CDCL SAT solving. For each of the following sentences, say if it is true or false.

(a) Let φ be the CNF input Boolean formula, and C denote a generic clause learned during the process. Then $\varphi \models C$.

[Solution: True]

(b) During the CDCL SAT solving process, the formula may contain an exponential number of learned clauses.

[Solution: False. Clauses are discharged according to their activity to avoid exponential blowups.]

(c) Let C be a conflict clause learned using the original backjumping&learning strategy. Then C contains at least one literal whose negation was unit-propagated in the current branch.

[Solution: False. In the decision criterion used by original CDCL solvers, C contains only decision literals.]

(d) Let C be a conflict clause learned using the state-of-the-art backjumping&learning strategy. Then C contains at most one literal whose negation was unit-propagated in the current branch.

[Solution: False. In the 1st-UIP criterion used by state-of-the-art CDCL solvers, C contains at most one literal whose negation was unit-propagated *at the last decision level* in the current branch.]

5

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

M:

```
MODULE main
VAR
  v1 : boolean;
  v2 : boolean;
  v3 : boolean;
ASSIGN
  init(v1) := TRUE;
  init(v2) := TRUE;

TRANS
  (next(v1) <-> v2) &
  (next(v2) <-> v3)
```

M':

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

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

(a) M simulates M'.
[Solution: True]

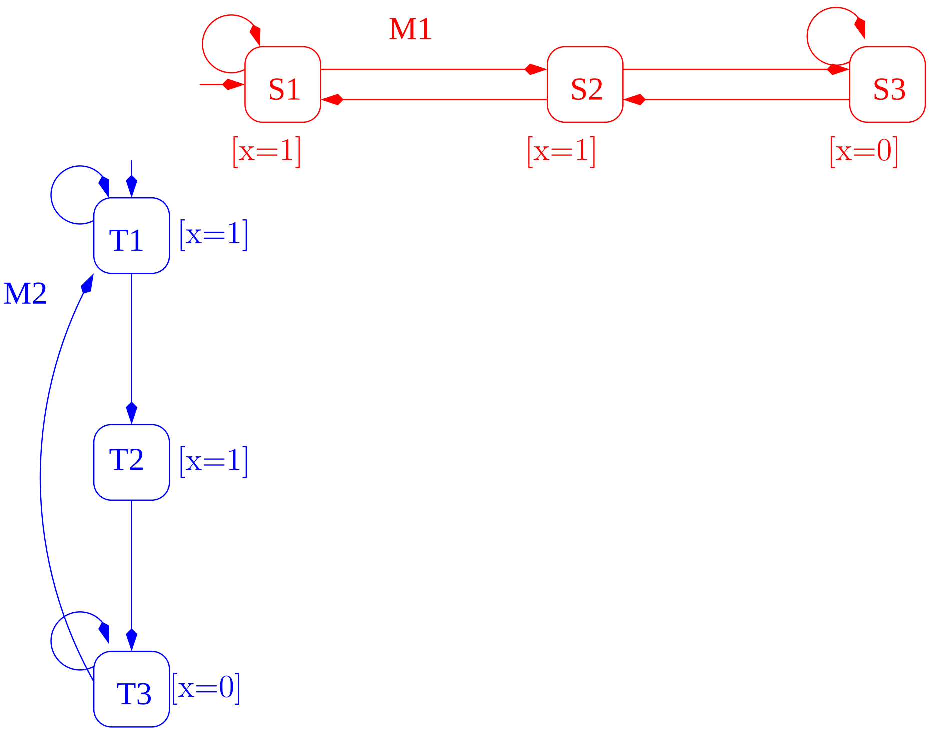
(b) M' simulates M.
[Solution: False. E.g.: M can execute the path $(11[1]) \longmapsto (11[0]) \longmapsto (10[1]) \longmapsto ...$, which cannot be simulated by M'.]

(c) for every Boolean property φ on `v1,v2`, if $M \models \mathbf{AG}\varphi$, then $M' \models \mathbf{AG}\varphi$,
[Solution: True]

(d) for every Boolean property φ on `v1,v2`, if $M \models \mathbf{EF}\varphi$, then $M' \models \mathbf{EF}\varphi$,
[Solution: False. E.g., `EF (v1 & !v2)` (see example above).]

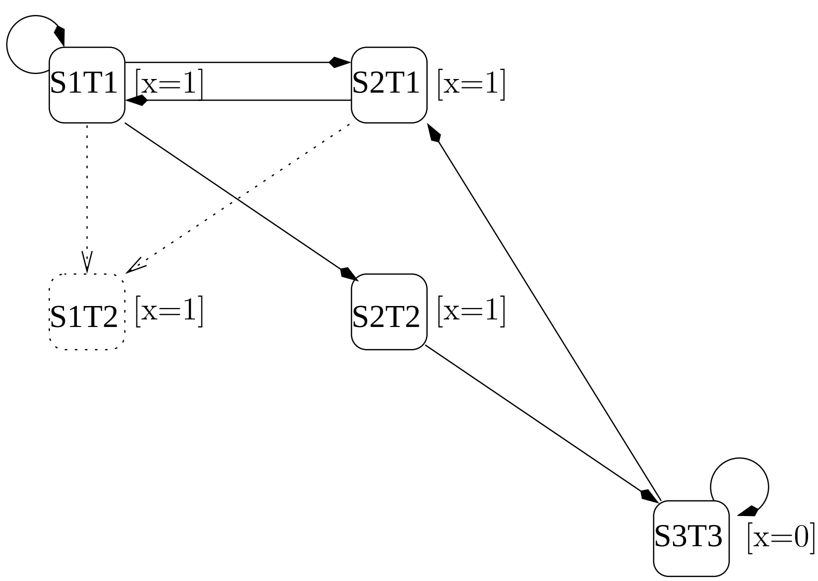
6

Consider the following two Kripke models $M1$ and $M2$, which share the variable x:



Compute and draw the graph of the synchronous product of $M1$ and $M2$.
Note: unreachable and deadend states should be removed.

[Solution:



]

7

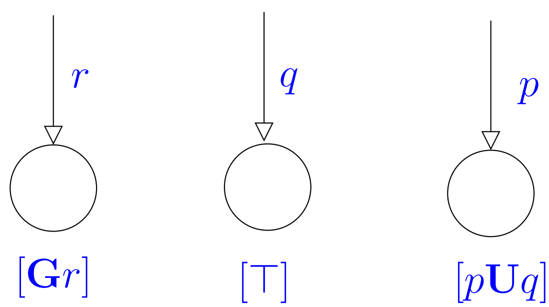
Consider the LTL formula $\varphi \stackrel{\text{def}}{=} (\neg p\mathbf{R}\neg q) \rightarrow \mathbf{G}r$

(a) rewrite φ into Negative Normal Form

[Solution: $(\neg p\mathbf{R}\neg q) \rightarrow \mathbf{G}r \Longrightarrow \neg(\neg p\mathbf{R}\neg q) \vee \mathbf{G}r \Longrightarrow (p\mathbf{U}q) \vee \mathbf{G}r$]

(b) find the initial states of a corresponding Generalized Büchi Automaton (for each state, define the labels of the incoming arcs and the "next" section.)

[Solution: Applying tableaux rules we obtain: $q \vee (p \wedge \mathbf{X}(p\mathbf{U}q)) \vee (r \wedge \mathbf{X}\mathbf{G}r)$, which is already in disjunctive normal form. This corresponds to the following three initial states:



]

(c) How many distinct sets of accepting states will the final Generalized Büchi Automaton have?

[Solution: One, since there is one "$\mathbf{U}$" subformulas occurring positively in φ.]

8

Let M be a **fair** Kripke model, which is represented symbolically by the OBDDs I, T, $FT \stackrel{\text{def}}{=} \{F_1, ..., F_k\}$ (which for simplicity we assume to be global variables), representing respectively the initial states, the transition relation and the fairness properties.

We assume it is given an implementation of the standard symbolic CTL Model Checking functions:

OBDD Check_EX(**OBDD** X)
OBDD Check_EG(**OBDD** X)
OBDD Check_EU(**OBDD** X,Y)

Write the pseudo-code of the fair symbolic CTL Model Checking function:

OBDD Check_FairEG(**OBDD** X)

which handles the **EG** operator.

[Solution: Emerson-lei Algorithm:

```
OBDD Check_FairEG(OBDD X) {
   Z':= X;
   repeat
      Z:= Z';
      for each F_i in FT
         Y:= Check_EU(Z,F_i∧Z);
         Z':= Z' ∧ Check_EX(Y));
      end for;
   until (Z' ↔ Z);
   return Z;
}
```

]

9

Given the following LTL Model Checking problem $M \models \varphi$ expressed in NuSMV input language:

```
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 | z) ;
```

1. Write the Boolean formulas describing the k-induction encoding of the problem, with k = 1.

   [Solution: The LTL property is in the form "$\mathbf{G}Good(x, y, z)$", hence, applying k-induction:

$$\begin{array}{rlcl} \varphi_{Base} \stackrel{\text{def}}{=} & (\neg x_0 \wedge \neg y_0 \wedge z_0) & \wedge & // \; I(x_0, y_0, z_0) \wedge \\ & \neg(x_0 \vee y_0 \vee z_0) & & // \; \neg Good(x_0, y_0, z_0) \end{array}$$

$$\begin{array}{rlcl} \varphi_{Ind1} \stackrel{\text{def}}{=} & (x_i \vee y_i \vee z_i) & \wedge & // \; Good(x_i, y_i, z_i) \wedge \\ & ((x_{i+1} \leftrightarrow y_i) \wedge (y_{i+1} \leftrightarrow z_i) \wedge (z_{i+1} \leftrightarrow x_i)) & \wedge & // \; T(x_i, y_i, z_i, x_{i+1}, y_{i+1}, z_{i+1}) \wedge \\ & \neg(x_{i+1} \vee y_{i+1} \vee z_{i+1}) & \wedge & // \; \neg Good(x_{i+1}, y_{i+1}, z_{i+1}) \wedge \end{array}$$

   ]

2. Say if they are satisfiable or not. If yes, show a model. If not, explain why. [Solution:

   - φ_{Base} is not satisfiable. In fact, the second row forces the assignments $\neg x_0, \neg y_0, \neg z_0$, which makes the first row false.
   - φ_{Ind1} is not satisfiable. In fact, the third row forces the assignments $\neg x_{i+1}, \neg y_{i+1}, \neg z_{i+1}$, from which the second row forces the assignments $\neg x_i, \neg y_i, \neg z_i$, which makes the first row false.

   ]

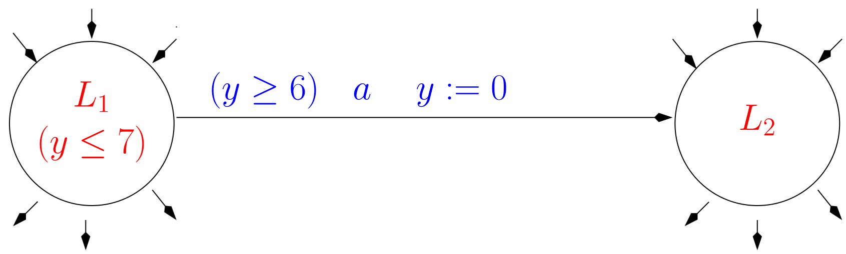
3. From the previous answers we can conclude:

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

   [Solution: a) $M \models \varphi$. In fact, we have proved it in one induction step.
   ]

10

Consider the following switch e in a timed automaton:

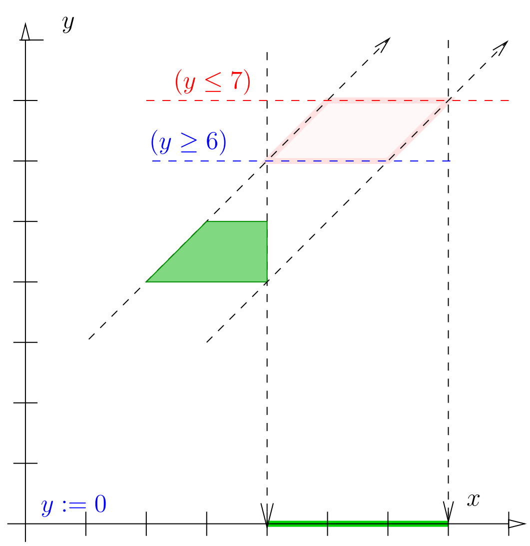


and consider the zone $Z1 \stackrel{\text{def}}{=} \langle L_1, \varphi \rangle$ s.t

$$\varphi \stackrel{\text{def}}{=} (x \geq 2) \wedge (x \leq 4) \wedge (y \geq 4) \wedge (y \leq 5) \wedge (y - x \leq 2).$$

Compute $succ(\varphi, e)$, displaying the process in a cartesian graph.

[Solution: The behaviour of $succ(\varphi, e)$ is displayed in the following diagram:



from which the solution is $succ(\varphi, e) = (x \geq 4) \wedge (x \leq 7) \wedge (y = 0)$.]