Theory of Hybrid Systems
Prof. Dr. Erika Ábrahám
RWTH Aachen University, Informatik 2 · D-52056 Aachen · GERMANY
http://ths.rwth-aachen.de/

Modeling and Analysis of Hybrid Systems

Series 1

Exercise 1

Please match each following LTL formulae φ_i to one of the given execution paths π_j, such that $\pi_j \models \varphi_i$ for all $i \leq i, j \leq 6$ and such that each φ_i is assigned a different path. (*Note: You can assume that the paths continue infinitely in the pattern of the last 2 nodes.*)

$\varphi_1 :\ true\, \mathcal{U} \mathcal{X} a$

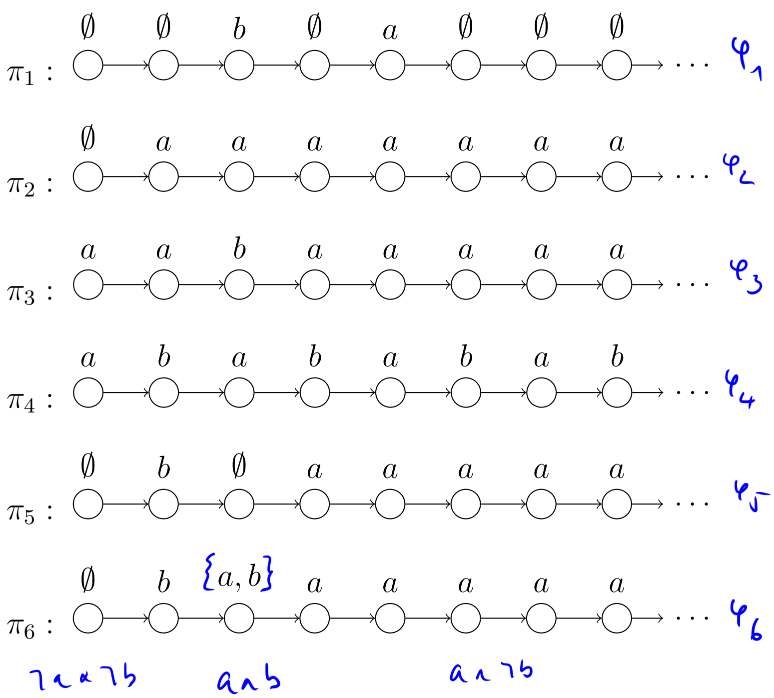
$\varphi_2 :\ \mathcal{G} \mathcal{X} a$

$\varphi_3 :\ a\, \mathcal{U} b$

$\varphi_4 :\ a \wedge \mathcal{X} b$

$\varphi_5 :\ \mathcal{F} \mathcal{G} a$

$\varphi_6 :\ (\mathcal{X} b) \mathcal{U} a$



φ_1 : true $\mathcal{U}$ ($\mathcal{X}$ a) π : $\cancel{1}, \cancel{2}, \cancel{3}, \cancel{4}, \cancel{5}, \cancel{6}$

φ_2 : $\mathcal{G} \mathcal{X}$ a π : $\cancel{2}$

φ_3 : a $\mathcal{U}$ b π : $\cancel{3}, \cancel{4}$

φ_4 : a $\wedge$ ($\mathcal{X}$ b) π : $\cancel{4}$

φ_5 : $\mathcal{F} \mathcal{G}$ a π : $\cancel{2}, \cancel{3}, \cancel{4}, \cancel{6}$

φ_6 : ($\mathcal{X}$ b) $\mathcal{U}$ a π : $\cancel{6}$

Solution:

$\varphi_1 \models \pi_1, \ldots, \pi_6$

$\varphi_2 \models \pi_2$

$\varphi_3 \models \pi_3, \pi_4$

$\varphi_4 \models \pi_4$

$\varphi_5 \models \pi_2, \pi_3, \pi_5, \pi_6$

$\varphi_6 \models \pi_3, \pi_4, \pi_6$

$\Rightarrow \varphi_i \models \pi_i, i \in \{1, \ldots, 6\}$.

Exercise 2

Consider an *elevator* that services 4 *floors* numbered 0 through 3. There is an elevator *door* at each floor with a call-button and an indicator light that signals whether or not the call-button has been pushed. If the light is on then we say that the corresponding floor is *requested*. The request is *served* (and the corresponding light is switched off) when the elevator stays at the given floor and the floor door is open.

Present a set of atomic propositions - try to minimize the number of them - that are needed to describe the following properties of the elevator system as LTL formulae and give the corresponding LTL formulae:

$G \bigwedge_{i=0}^{3} (req_i \to F(at_i \wedge open_i))$

(a) The doors are "safe", i.e., a floor door is never open if the elevator is not staying there. $AG(\bigwedge_{i=0}^{3} \bigwedge_{j=0,\, j\neq i}^{3} (at_i \to \neg open_j))$

(b) Any requested floor will eventually be served. $\bigwedge_{i=0}^{3} AG(req_i \to AF(at_i \wedge open_i))$

(c) Again and again the elevator stays at floor 0. $GF\, at_0$ $AGAF\, at_0$

(d) If the top floor is requested then the elevator does ~~not~~ stop on any other floor before the top floor is served. $AG(req_3 \to AXA(\bigwedge_{i=0}^{2} \neg at_i)\ U\ (at_3 \wedge open_3))$

$\neg at_0 \wedge \neg at_1 \wedge \neg at_2$

(e) Eventually there will be a last request, i.e., there is a time point after which no floor is requested any more.

$FG \bigwedge_{i=0}^{3} \neg req_i$

Is it also possible to give a CTL formula for each of the properties above?

Solution: We define the following atomic propositions.

e_i	the elevator stays on the i-th floor
d_i	the door on the i-th floor is open
r_i	there is a request on the i-th floor

The LTL formulae for the properties above are given as below.

(a) $\Phi_a = \mathcal{G}(\bigwedge_{i=0,1,2,3}(\neg e_i \rightarrow \neg d_i))$

(b) $\Phi_b = \mathcal{G}(\bigwedge_{i=0,1,2,3}(r_i \rightarrow \mathcal{F}(e_i \wedge d_i)))$

(c) $\Phi_c = \mathcal{G}\mathcal{F}\ e_0$

(d) $\Phi_d = \mathcal{G}(r_3 \rightarrow \mathcal{X}((\bigwedge_{i=0,1,2} \neg e_i)\ \mathcal{U}\ (e_3 \wedge d_3)))$

(e) $\Phi_e = \mathcal{F}\mathcal{G}(\bigwedge_{i=0,1,2,3}(\neg r_i))$

We also give the CTL formulae for the properties.

(a) $\Psi_a = A\mathcal{G}(\bigwedge_{i=0,1,2,3}(\neg e_i \rightarrow \neg d_i))$

(b) $\Psi_b = A\mathcal{G}(\bigwedge_{i=0,1,2,3}(r_i \rightarrow A\mathcal{F}(e_i \wedge d_i)))$

(c) $\Psi_c = A\mathcal{G}A\mathcal{F}\ e_0$

(d) $\Psi_d = A\mathcal{G}(r_3 \rightarrow A\mathcal{X}A((\bigwedge_{i=0,1,2} \neg e_i)\ \mathcal{U}\ (e_3 \wedge d_3)))$

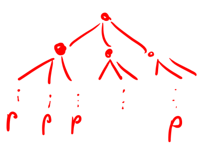
(e) Not possible.

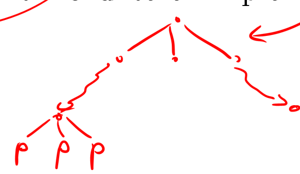
Exercise 3

The LTL formulae $\mathcal{X}\mathcal{F}p$ and $\mathcal{F}\mathcal{X}p$ are equivalent, since we have the following formal proof: For any *path* $\pi : s_0 s_1 \cdots$ of an $\mathcal{LSTS}$ $\mathcal{L}$,

$$\begin{aligned}
&\mathcal{L}, \pi \models \mathcal{X}\mathcal{F}p \\
\Leftrightarrow\ &\pi^1 = s_1 s_2 \cdots \models \mathcal{F}p \\
\Leftrightarrow\ &\exists i \geq 1. s_i \models p \\
\Leftrightarrow\ &\exists i \geq 1. s_{i-1} \models \mathcal{X}p \\
\Leftrightarrow\ &\exists i \geq 0. s_i \models \mathcal{X}p \\
\Leftrightarrow\ &\pi \models \mathcal{F}\mathcal{X}p
\end{aligned}$$

Is it also the case for the CTL formulae $A\mathcal{X}A\mathcal{F}p$ and $A\mathcal{F}A\mathcal{X}p$? If so, please give a formal proof. Otherwise please present a counterexample.





Solution: The CTL formulae $A\mathcal{X}A\mathcal{F}p$ and $A\mathcal{F}A\mathcal{X}p$ are not equivalent. We give the following counterexample (see Figure 1). All paths starting in the initial state satisfy

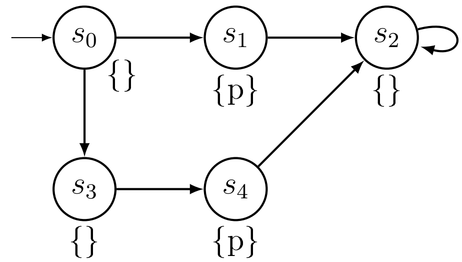


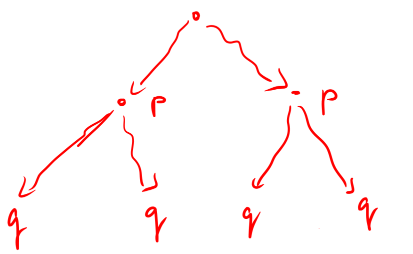
Figure 1: The transition system *TS*

the formula $A\mathcal{X}A\mathcal{F}p$, whereas the formula $A\mathcal{F}A\mathcal{X}p$ is not satisfied in the initial state. The second formula essentially states that for all paths there exists one state, from which all next states satisfy p. This formula holds for the state s_3 and for the state s_1 but does not hold in state s_0, as not all successors of this state satisfy p.

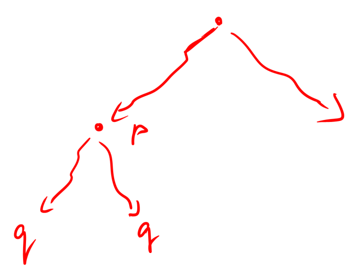
Exercise 4

We only consider $\mathcal{LSTS}$s with infinite runs. Assume $p, q \in$ AP. Are the CTL formula φ_{CTL} : $A\mathcal{G}(p \rightarrow A\mathcal{F}q)$ and the LTL formula φ_{LTL} : $\mathcal{G}(p \rightarrow \mathcal{F}q)$ *equivalent* (i.e., $\mathcal{LSTS}, \sigma \models \varphi_{CTL} \Leftrightarrow \sigma \models \varphi_{LTL}$ for all states σ of $\mathcal{LSTS}$)?
(Note: LTL formulae can also be used to describe the properties of states.)

$AG(p \rightarrow AFq)$



$G(p \rightarrow Fq)$



Solution: Let $\pi(s)$ contain those infinite paths of $\mathcal{LSTS}$ that start in s and $\pi(s, s')$ contain those finite paths starting in s and ending in s'.

The CTL formula $A\mathcal{G}(p \to A\mathcal{F}q)$ is equivalent to the LTL formula $\mathcal{G}(p \to \mathcal{F}q)$, since

$\mathcal{LSTS}, s_0 \models_{LTL} \mathcal{G}(p \to \mathcal{F}q)$

$\Leftrightarrow$For all paths $\pi = s_0, s_1, \ldots : \mathcal{LSTS}, \pi \models_{LTL} \mathcal{G}(p \to \mathcal{F}q)$

$\Leftrightarrow$For all paths $\pi = s_0, s_1, \ldots$ and for all $i \geq 0$: If $\mathcal{LSTS}, \pi(i) \models p$ then there exists a $j \geq i$ such that $\mathcal{LSTS}, \pi(j) \models q$

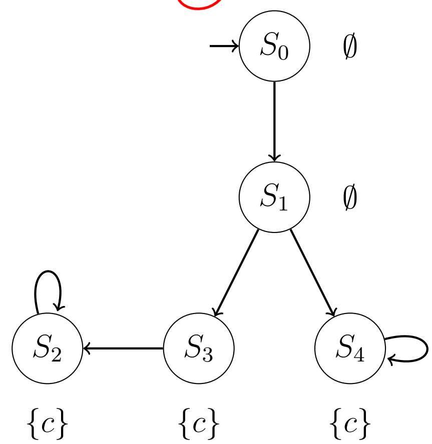
$\Leftrightarrow$For all paths $\pi = s_0, \ldots, s$ where $\mathcal{LSTS}, s \models p$ then for all paths π' starting in s there exists a $j \geq 0$ such that $\mathcal{LSTS}, \pi'(j) \models q$

$\Leftrightarrow$For all paths $\pi = s_0, s_1, \ldots, s_i, \ldots$ with $s_i \models p$ then $\mathcal{LSTS}, \pi(s_i) \models A\mathcal{F}q$

$\Leftrightarrow\mathcal{LSTS}, s_0 \models AG(p \to AFq)$.

Exercise 5

Assume the following transition system TS: LSTS



$EF\,\underbrace{AG\,\underline{c}}_{\varphi_1}$

Decide whether $TS \models \Phi$ where $\Phi = \boxed{E\mathcal{F}A\mathcal{G}c}$. Please sketch the main steps of the CTL model-checking algorithm.

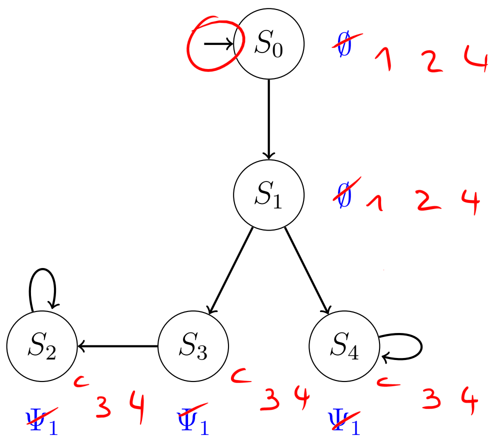
Solution: In the lecture, we only taught the model-checking algorithm for the operators $\neg$, $\wedge$, $E(\cdot\,\mathcal{U}\,\cdot)$ and $A(\cdot\,\mathcal{U}\,\cdot)$. Therefore, we need to rewrite the formula Φ as follows:

$$\Phi = E\mathcal{F}\,A\mathcal{G}\,c = E(true\,\mathcal{U}\,(A\mathcal{G}\,c)) = E(true\,\mathcal{U}\,(\neg\,E\mathcal{F}\,\neg c)) = \underbrace{E(true\,\mathcal{U}\,\underbrace{(\neg\,\underbrace{E(true\,\mathcal{U}\,\underbrace{\neg c}_{1})}_{2})}_{3})}_{4}$$

syntactic sugar

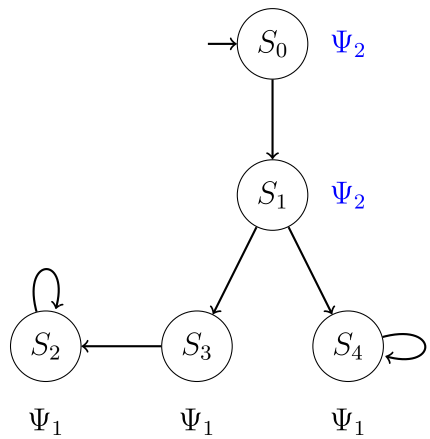
We present the main steps of checking $TS \models \Phi$.

$\Psi_1 = c$



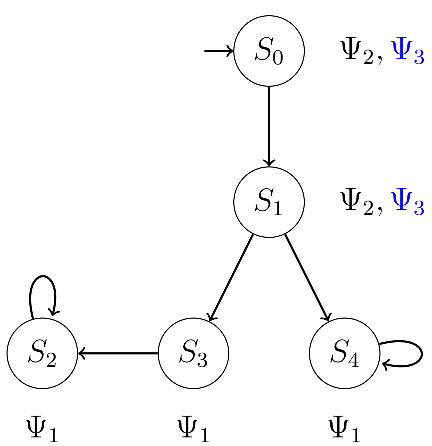
Step 1

$\Psi_2 = \neg\Psi_1$



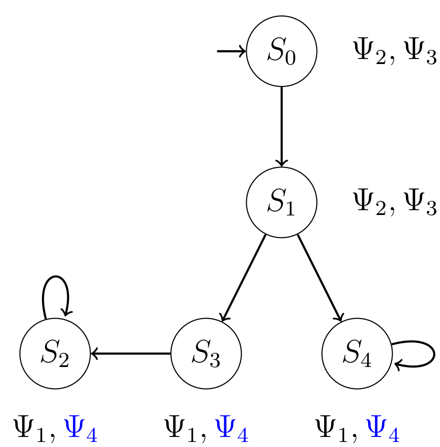
Step 2

$\Psi_3 = E(true\,\mathcal{U}\,\Psi_2)$



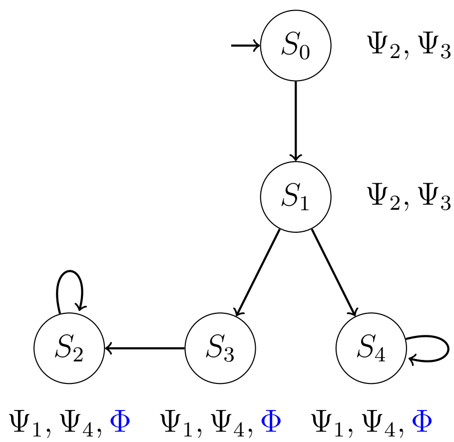
Step 3

$\Psi_4 = \neg\Psi_3$



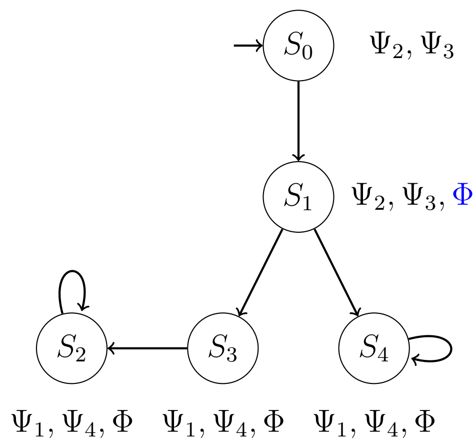
Step 4

$\Phi = E(true\ \mathcal{U}\ \Psi_4)$



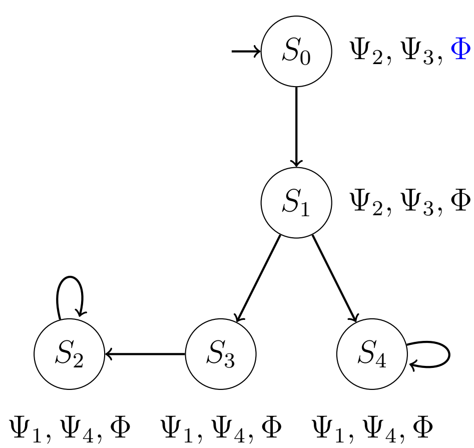
Step 5

$\Phi = E(true\ \mathcal{U}\ \Psi_4)$



Step 6

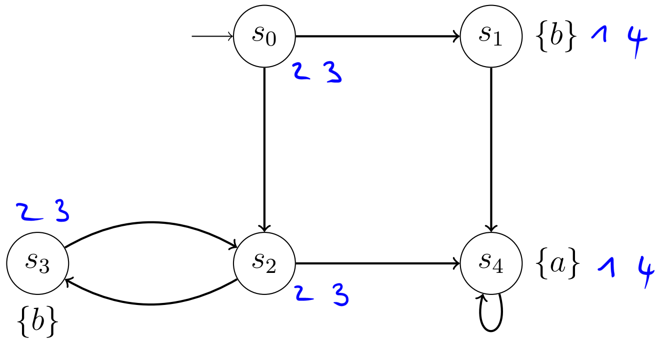
$\Phi = E(true\ \mathcal{U}\ \Psi_4)$



Step 7

Exercise 6

Assume the following transition system ~~TS~~: LSTS



Decide whether $TS \models \Phi$ where $\Phi = \boxed{\mathcal{A}\mathcal{G}\mathcal{A}\mathcal{F}a}$. Please sketch the main steps of the CTL model-checking algorithm. *(Note: To eliminate syntactic sugar, you can use $\mathcal{A}\mathcal{F}\varphi \equiv \mathcal{A}true\,\mathcal{U}\,\varphi$ and $\mathcal{A}\mathcal{G}\varphi \equiv \neg\mathcal{E}\mathcal{F}\neg\varphi$.)*

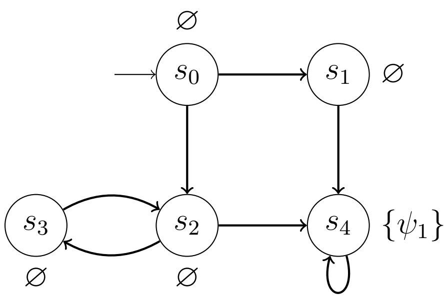
$AGAFa = \neg EF \neg (AFa)$

$\underbrace{\neg \underbrace{E\, true\, \mathcal{U} \underbrace{\neg (\underbrace{A\, true\, \mathcal{U}\, a}_{1})}_{2}}_{3}}_{4}$

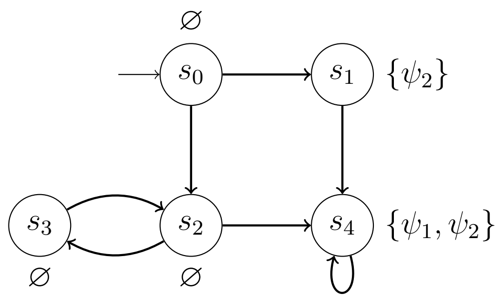
Solution:

First of all, we eliminate the syntactic sugar operators:

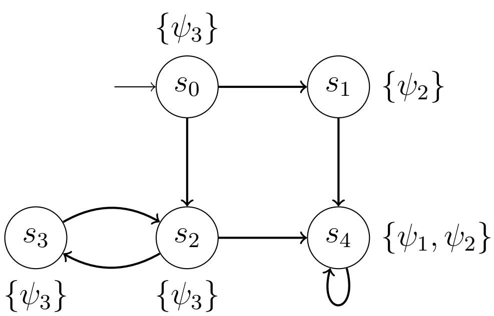
$$\Phi = A\mathcal{G}A\mathcal{F}a = A\mathcal{G}A(true\,\mathcal{U}a) = \neg E\mathcal{F}\neg(A(true\,\mathcal{U}a)))$$



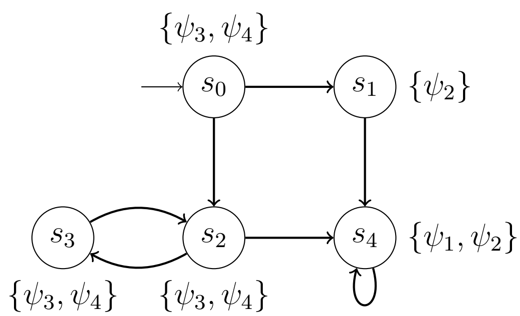
(a) Step 1: $\psi_1 = a$



(b) Step 2: $\psi_2 = A\ true\,\mathcal{U}\ \psi_1$



(a) Step 3: $\psi_3 = \neg\psi_2$



(b) Step 4: $\psi_4 = E\mathcal{F}\psi_3$

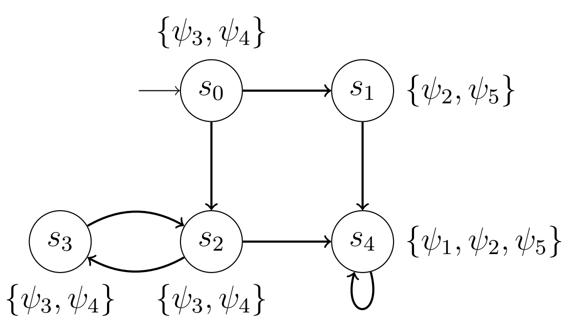
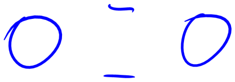
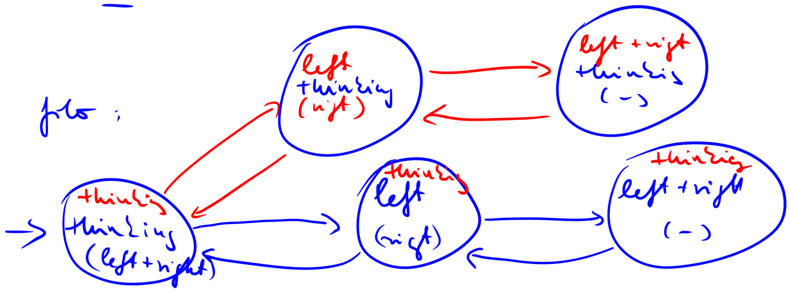


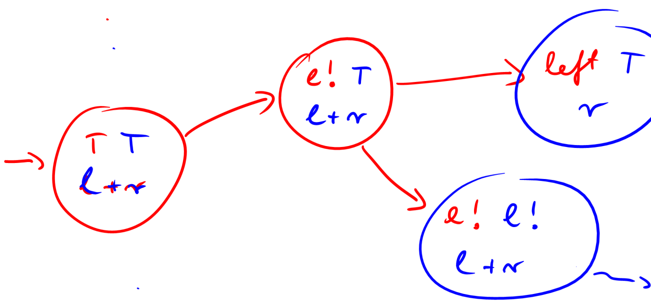
Figure 4: Step 5: $\Phi = \psi_5 = \neg\psi_4$



1 filo:



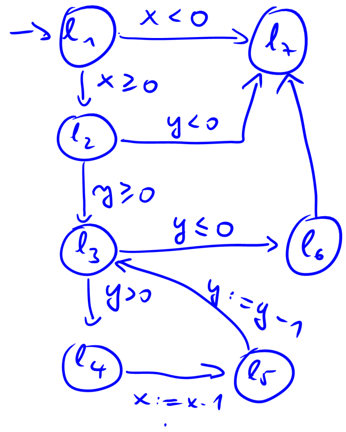
no deadlock



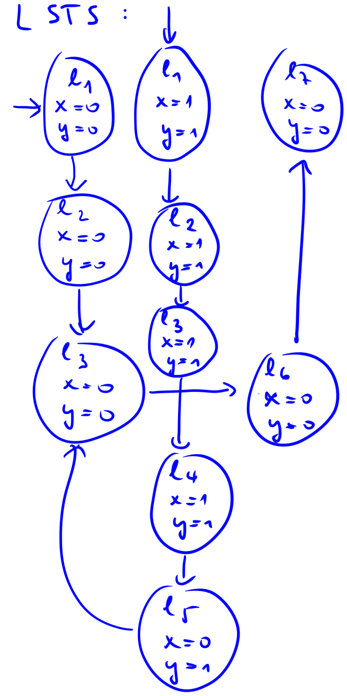
deadlock

```
m ( int x , int y ) {
ℓ1:  if  x < 0  return 0 ;  ℓ7
ℓ2   if  y < 0  return 0 ;  ℓ7
ℓ3   while ( y > 0 ) {
  ℓ4   x := x - 1 ;
  ℓ5   y := y - 1 ;  }
ℓ6   return x
ℓ7
```

LTS :



LSTS :



$\neg(x < 0) \equiv x \geq 0$