1	2	3	4	Σ	Grade

6.0/4.0 VU Formale Methoden der Informatik

185.291 **October, 16 2020**

Kennzahl (study id)	Matrikelnummer (student id)	Familienname (family name)	Vorname (first name)	Gruppe (version)
				A

1.) Consider the following decision problem:

> **HALTING AFTER LINE-FLIP (HALF)**
>
> INSTANCE: A tuple (Π, I), where Π is a program that takes a string as input; I a string.
>
> QUESTION: Do there exist two consecutive lines of code in Π, such that when the two lines are flipped (i.e., the order of the two lines is reversed) in Π, the resulting program (a) is syntactically correct and (b) halts on I?

(1) By providing a suitable many-one reduction from the **HALTING** problem, prove that **HALF** is undecidable.

(2) Is **HALF** semi-decidable? Explain your answer. **(15 points)**

2.) (a) Let φ be the first-order formula

$$\forall x \forall y \left[\big((r(x,y) \land p(x)) \rightarrow p(y) \big) \land \big(r(x,y) \rightarrow (p(y) \rightarrow p(x)) \big) \right] .$$

i. Is φ valid? If yes, present a proof. If no, give a counter-example and prove that it falsifies φ.

ii. Replace r in φ by $\doteq$ (equality) resulting in ψ. Is ψ E-valid? Argue formally!

(5 points)

(b) Show the following:

$$\varphi^{EUF} \text{ is } E\text{-satisfiable iff } FC^E \wedge \mathit{flat}^E \text{ is } E\text{-satisfiable.}$$

FC^E and flat^E are obtained from φ^{EUF} by Ackermann's reduction.
(Hint: FC^E is the same for φ^{EUF} and $\neg\varphi^{EUF}$.) **(10 points)**

3.) (a) Let p be the following program:

$$
\begin{array}{l}
x := 1; \\
y := -2; \\
z := 2; \\
\textbf{while } x < N \textbf{ do} \\
\quad x := x - 2 * y - 2 * z + 1; \\
\quad y := y - 2 \\
\quad z := z + 2 \\
\textbf{od}
\end{array}
$$

Provide a formal proof of the partial correctness triple $\{N \geq 1\}\ p\ \{z = 2 * N\}$.

Note: Give an appropriate loop invariant for the **while** loop in p, to be further used in proving the partial correctness of the above Hoare triple.

(10 points)

(b) Fill in the blank such that ...

... the following Hoare triple is totally correct.

$[x \geq 2]$
while $x > 2$ **do**
  if $x = 2 * (x/2)$
    then $x := x/2$
    else $\boxed{}$
od
$[x = 2]$

... the following Hoare triple is partially but *not* totally correct.

$\{x \geq 2 \land x = 2 * (x/2) + 1\}$
while $x > 1$ **do**
  if $x = 2 * (x/2)$
    then $x := x/2$
    else $\boxed{}$
od
$\{x = 1\}$

... the following Hoare triple is *not* partially correct.

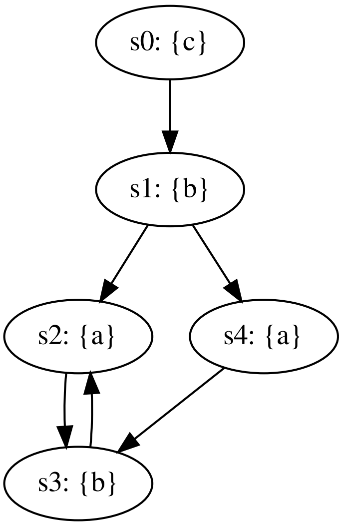
$\{x \geq 2\}$
while $x > 1$ **do**
  if $x = 2 * (x/2)$
    then $x := x/2$
    else $\boxed{}$
od
$\{x = 1\}$

(5 points)

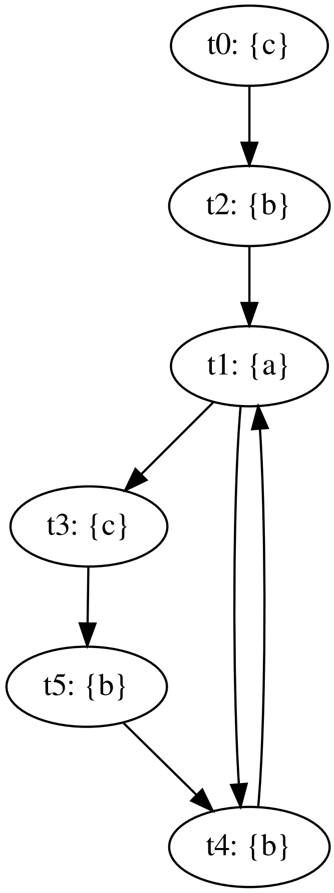
Note: Recall that / denotes integer division. Give a short informal justifications for your solutions. One or two sentences per example suffice and *no* formal proof is needed.

4.) (a) Provide a non-empty simulation relation H that witnesses $M_1 \leq M_2$, where M_1 and M_2 are shown below. The initial state of M_1 is s_0, the initial state of M_2 is t_0:

Kripke structure M_1:

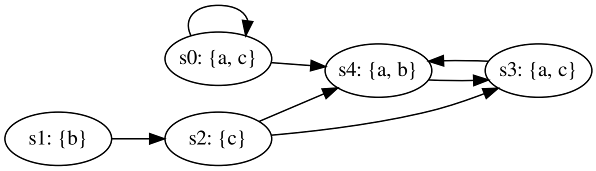


Kripke structure M_2:



(4 points)

(b) Consider the following Kripke structure M:



For each of the following formulae φ,

i. check the respective box if the formula is in CTL, LTL, and/or CTL*, and
ii. list the states s_i on which the formula φ holds; i.e. for which states s_i do we have $M, s_i \models \varphi$?

φ	CTL	LTL	CTL*	States s_i
$\mathbf{G}(a)$	☐	☐	☐	
$c\ \mathbf{U}\ b$	☐	☐	☐	
$\mathbf{AF}(a \wedge b)$	☐	☐	☐	
$\mathbf{EF}(a \wedge b)$	☐	☐	☐	
$\mathbf{X}(a)$	☐	☐	☐	

(5 points)

(c) **LTL tautologies**

Prove that the following formulas are tautologies, i.e., they hold for every Kripke structure M and every path π in M, or find a Kripke structure M and path π in M, for which the formula does not hold and justify your answer.

i. $\mathbf{X}(p \ \mathbf{U} \ q) \Leftrightarrow (\mathbf{X}p) \ \mathbf{U} \ (\mathbf{X}q)$

ii. $\mathbf{FGF}p \Leftrightarrow \mathbf{GFG}p$

(6 points)