1	2	3	4	Σ

6.0/4.0 VU Formale Methoden der Informatik (185.291)

June 9, 2020

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

1.) Consider the following decision problem:

> **HALTING AFTER LINE-REMOVAL (HALR)**
>
> INSTANCE: A tuple (Π, I), where Π is a program that takes a string as input; I a string.
>
> QUESTION: Does there exist a line of code in Π, such that when the line is removed from 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 **HALR** is undecidable.

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

2.) We consider a slightly restricted and simplified form M of the Ackermann-Péter function, which we discussed in the exercise part.

Algorithm 1: The function M

Input: x, y, two *positive* integers
Output: The computed positive integer value for x, y

if $x == 1$ **then**
  return $2y$;
else if $y == 1$ **then**
  return x;
else return $\mathrm{M}(x-1, \mathrm{M}(x, y-1))$;

(a) Let $\mathbb{N}$ denote the natural numbers *without* 0. Use well-founded induction to show

$$\forall x \, \forall y \, \big((x \in \mathbb{N} \wedge y \in \mathbb{N}) \rightarrow \mathrm{M}(x, y) \geq 2y\big).$$

(11 points)

(b) Suppose $\texttt{M}_\texttt{C}$ is an implementation of M in the `C` programming language with x and y of type unsigned integers of size 32 bit (i.e., of type `uint32_t`). Is

$$\mathrm{M}(x', y') = \texttt{M}_\texttt{C}(x', y')$$

true for all integers x', y' satisfying $1 \leq x', y' \leq$ `UINT32_MAX`, where `UINT32_MAX` is the largest value for a variable of type `uint32_t`?

If so, then prove this fact. Otherwise provide a counterexample with an exact explanation of what is computed and what is happening. **(4 points)**

(15 points)

3.) Let p be the following IMP program:

$$
\begin{array}{l}
\textbf{while } y < 10 \textbf{ do} \\
\quad x := x + z + 1; \\
\quad z := z + 2; \\
\quad y := y + 1 \\
\textbf{od}
\end{array}
$$

where x, y, z are program variables. For each Hoare triple below, prove/disprove its total correctness. If the Hoare triple is correct, prove its total correctness by providing a formal proof. If the Hoare triple is not correct, provide a counterexample.

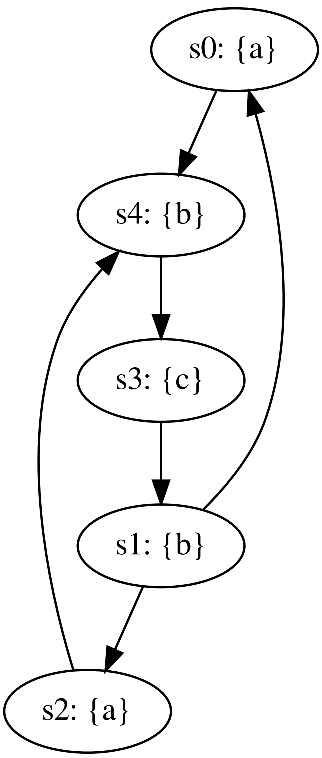
(3a) Hoare triple: $[x = 0 \wedge y = 0 \wedge z = 0]\ p\ [x = 100]$.

(3b) Hoare triple: $[x = 0 \wedge y = 20 \wedge z = 0]\ p\ [x = 100]$.

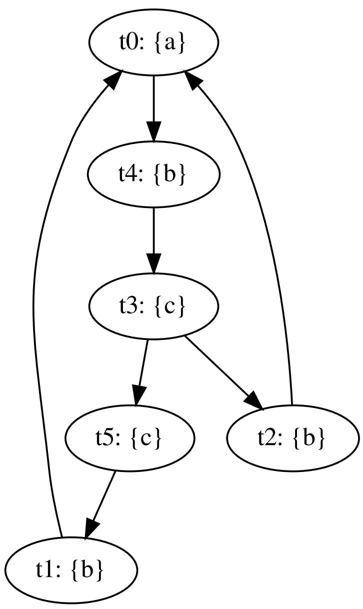
(15 points)

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:

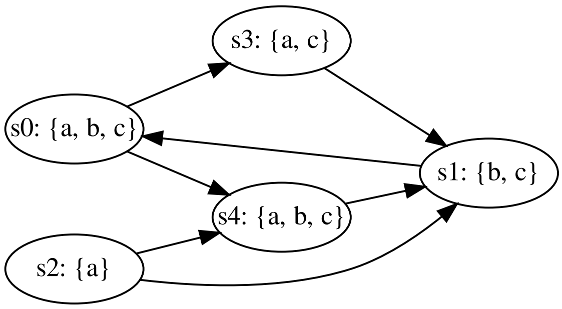


Kripke structure M_2:



(5 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
$\mathbf{X}(a \wedge b)$	☐	☐	☐	
$\mathbf{AX}(b)$	☐	☐	☐	
$\mathbf{EG}(a)$	☐	☐	☐	
$\mathbf{EX}(a \wedge b)$	☐	☐	☐	
$\mathbf{E}[(a \wedge b \wedge c)\ \mathbf{U}\ (c)]$	☐	☐	☐	

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

ii. $((\mathbf{F}p) \Rightarrow q) \Rightarrow (p \Rightarrow \mathbf{F}q)$

(5 points)

Grading scheme: 0–29 nicht genügend, 30–35 genügend, 36–41 befriedigend, 42–47 gut, 48–60 sehr gut