1	2	3	4	Σ

6.0/4.0 VU Formale Methoden der Informatik (185.291)

June 28, 2019

Kennz. (study id)	Matrikelnummer (student id)	Nachname (surname)	Vorname (first name)

1.) Consider the following decision problem:

> **EXACTLY-ONE-HALTS (EOH)**
>
> INSTANCE: A tuple (Π_1, Π_2, I), where Π_1, Π_2 are programs that take a string as input, and I is a string.
> QUESTION: Does either Π_1 halt on I or Π_2 halt on I (but not both halt on I)?

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

(10 points)

(b) Is **EXACTLY-ONE-HALTS** semi-decidable? Explain your answer.

(5 points)

2.) (a) Consider $\mathcal{T}_{PA}^{+}$, which is Peano arithmetic with the axioms

$\forall x\ \neg(x + 1 \doteq 0)$	(zero)
$\forall x\ \forall y\ (x + 1 \doteq y + 1 \to x \doteq y)$	(successor)
$F[0] \wedge (\forall x\ (F[x] \to F[x + 1])) \to \forall x\ F[x]$	(induction)
$\forall x\ (x + 0 \doteq x)$	(plus zero)
$\forall x\ \forall y\ (x + (y + 1) \doteq (x + y) + 1)$	(plus successor)
$\forall x\ (x \cdot 0 \doteq 0)$	(times zero)
$\forall x\ \forall y\ (x \cdot (y + 1) \doteq (x \cdot y) + x)$	(time successor)

together with the following additional axioms:

$\forall x\ (x^0 \doteq 1)$	(exp zero)
$\forall x\ \forall y\ (x^{y+1} \doteq x^y \cdot x)$	(exp succ)
$\forall x\ \forall z\ (exp_3(x, 0, z) \doteq z)$	(exp_3 zero)
$\forall x\ \forall y\ \forall z\ (exp_3(x, y + 1, z) \doteq exp_3(x, y, x \cdot z))$	(exp_3 succ)

Show by induction that $\varphi\colon \forall x \forall y\ (exp_3(x, y, 1) \doteq x^y \cdot 1)$ is $\mathcal{T}_{PA}^{+}$-valid. Use the semantic argument method from the lecture to formally prove the formula in the base case and in the step case. In order to sImplify the proof, you may use the formulas $(L)\colon \forall x\ (1 \cdot x \doteq x)$ and $(A)\colon \forall x \forall y \forall z\ (x \cdot (y \cdot z) \doteq (x \cdot y) \cdot z)$ as additional lemmas.

Please be precise and indicate exactly why proof lines follow from some other(s). Moreover, recall that equality handling is performed using equality axioms.

Hint: You need to prove a stronger formula from which φ follows.

(12 points)

(b) Apply the Ackermann reduction to the formula

$$\varphi^{EUF} : F(F(x_1)) \doteq G(x_2, G(x_1, x_3, x_4), F(x_2)) \to p(x_1, y)$$

and obtain the validity-equivalent formula φ^{E}. **(3 points)**

3.) Note that all programs within this exercise are programs over the integers, that is, every program variable can only take integer values.

(a) Show that the Hoare triple $\{a \geq 0 \wedge b \geq 0\}\ p\ \{a - b * c - d = 0\}$ is valid with respect to partial correctness where p is the following program:

$c := 0;$
$d := a;$
while $b \leq d$ **do**
  $d := d - b;$
  $c := c + 1;$
od

(8 points)

(b) Is the Hoare triple from Exercise 3a totally correct? If yes, provide a variant, otherwise provide a counterexample. In both cases, justify your answer!

(2 points)

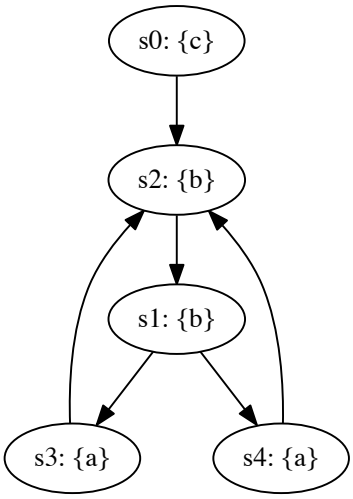
(c) Let p be a program and let $A, B \in \text{Assn}$. Is the following Hoare rule sound/admissible? If yes, provide a proof. Otherwise, provide a counterexample and argue why it is a counterexample.

$$\frac{\{A\}\ \textbf{skip};\ p\ \{B\}}{\{A\}\ p\ \{B\}}$$

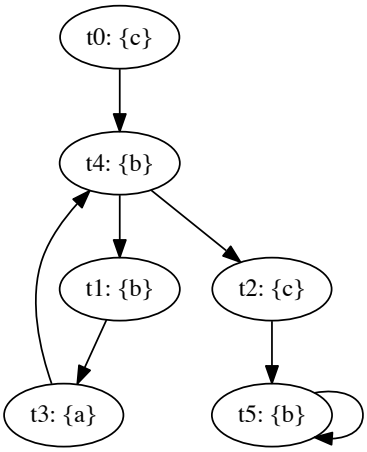
(5 points)

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:

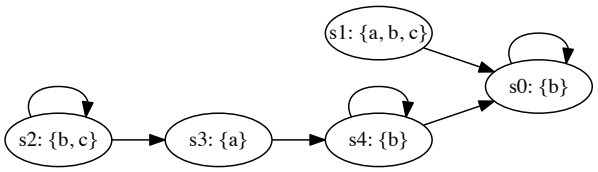


Kripke structure M_2:



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

(5 points)

(c) **LTL tautologies**

Provide a Kripke structure, which satisfies all of the following CTL* formulas:

$$\neg q$$
$$\mathbf{AG}p \Rightarrow q$$
$$\mathbf{EF}p$$
$$\mathbf{EFG}\neg p$$

(6 points)

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