1	2	3	4	Σ

6.0/4.0 VU Formale Methoden der Informatik (185.291)

March 15, 2019

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

1.) Consider the following decision problem:

> **AT-MOST-ONE-HALTS (AMOH)**
>
> 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 $\Pi_1(I)$ halt, $\Pi_2(I)$ halt, or none of the two halt?

(a) By providing a suitable many-one reduction from the **CO-HALTING** problem, prove that **AT-MOST-ONE-HALTS** is undecidable. Recall that **CO-HALTING** is given as follows

> **CO-HALTING**
> INSTANCE: A (source code of a) program Π, an input string I.
> QUESTION: Does $\Pi(I)$ run forever (i.e., does Π not terminate on I)?

(10 points)

(b) Recall that **CO-HALTING** is not even semi-decidable. Given a reduction from **CO-HALTING** to **AT-MOST-ONE-HALTS**, what can we say about semi-decidability of **AT-MOST-ONE-HALTS**?

(5 points)

2.) (a) Show that $a[i] \doteq e \rightarrow a\langle i \triangleleft e \rangle \doteq a$ is $\mathcal{T}_A^{=}$-valid using the semantic argument method from the lecture. Besides the equality axioms, you have the following ones for the arrays.

i. $\forall a, i, j \; \big(i \doteq j \rightarrow a[i] \doteq a[j]\big)$ (array congruence)

ii. $\forall a, v, i, j \; \big(i \doteq j \rightarrow a\langle i \triangleleft v \rangle[j] \doteq v\big)$ (read-over-write 1)

iii. $\forall a, v, i, j \; \big(i \not\doteq j \rightarrow a\langle i \triangleleft v \rangle[j] \doteq a[j]\big)$ (read-over-write 2)

iv. $\forall a, b \, \big(\forall j \; \big(a[j] \doteq b[j]\big) \leftrightarrow a \doteq b\big)$ (extensionality)

Please be precise and indicate exactly why proof lines follow from some other(s).

(11 points)

(b) First define the concept of a $\mathcal{T}$-interpretation. Then use it to define the following:

i. the $\mathcal{T}$-satisfiability of a formula;

ii. the $\mathcal{T}$-validity of a formula.

Additionally define the completeness of a theory $\mathcal{T}$. **(4 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 $\{n > 0\}\ p\ \{a = n * n\}$ is valid with respect to partial correctness where p is the following program:

$a := 0;$

$b := 0;$

while $b \neq n$ **do**

  $a := a + 2 * b + 1;$

  $b := b + 1;$

od

(10 points)

(b) Let p be the program from exercise 3a. Is the Hoare triple $[true]\ p\ [a = n * n]$ valid with respect to total correctness? If yes, prove its validity using the Hoare calculus. Otherwise, provide a counterexample, that is, a state that does not satisfy the correctness assertion.

(2 points)

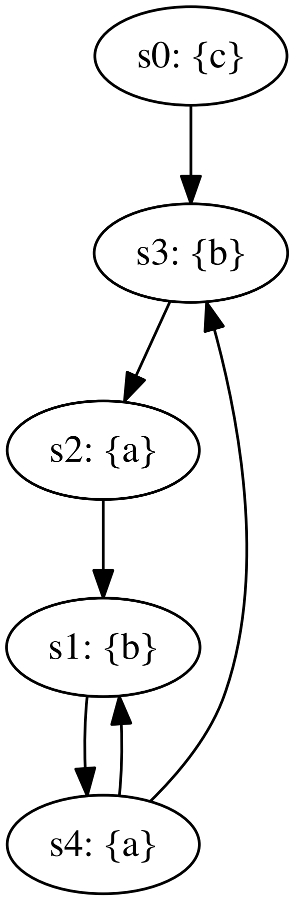
(c) Is the following Hoare triple valid with respect to total correctness? If yes, prove its validity using the Hoare calculus. Otherwise, provide a counterexample, that is, a state that does not satisfy the correctness assertion.

$$[n \geq 0]\ \mathbf{if}\ n > 0\ \mathbf{then}\ m := 2 * n\ \mathbf{else\ abort\ endif}\ [m = 2 * n]$$

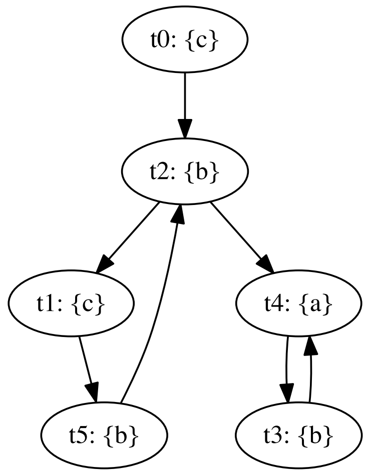
(3 points)

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:

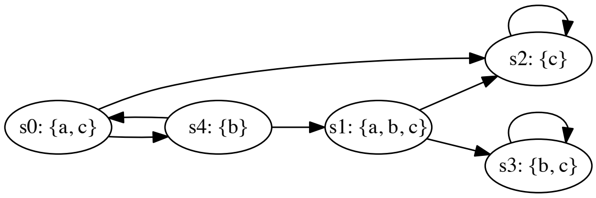


Kripke structure M_2:



(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
$\mathbf{G}(c)$	☐	☐	☐	
$\mathbf{F}(a)$	☐	☐	☐	
$\mathbf{AF}(b)$	☐	☐	☐	
$\mathbf{EX}(a \wedge b)$	☐	☐	☐	
$\mathbf{E}[(a \wedge b)\ \mathbf{U}\ (a)]$	☐	☐	☐	

(5 points)

(c) **LTL tautologies**

Prove or disprove (e.g. by providing a counter-example) the following LTL formulas:

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

ii. $\mathbf{GF}p \Rightarrow \mathbf{G}(\neg p\ \mathbf{U}\ p)$

(6 points)

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