1	2	3	4	5	Σ	Grade

6.0/4.0 VU Formale Methoden der Informatik

185.291 October, 18 2019

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

1.) Consider the following decision problem:

> **REACHING LINE in LESS STEPS (RLLS)**
>
> INSTANCE: A tuple $(\Pi_1, \Pi_2, I, n_1, n_2)$, where Π_1, Π_2 are programs that take a string as input, I a string, and n_1, n_2 integers.
>
> QUESTION: Does Π_1 when applied to I reach line n_1 (of the source code of Π_1) in strictly less computation steps than Π_2 when applied to I reaches line n_2 (of the source code of Π_2)?

Remark: If neither Π_1 reaches line n_1 nor Π_2 reaches line n_2, we have a negative instance of RLLS.

(1) By providing a suitable many-one reduction from the **HALTING** problem, prove that **REACHING LINE in LESS STEPS** is undecidable.

(2) Is **REACHING LINE in LESS STEPS** semi-decidable? Explain your answer. **(15 points)**

2.) (a) Consider φ: $a[i] \doteq e \rightarrow a\langle i \lhd e\rangle \doteq a$. If φ is $\mathcal{T}_A^{=}$-valid then provide a proof using the semantic argument method from the lecture. If φ is not $\mathcal{T}_A^{=}$-valid then provide a counter-example. Besides the equality axioms, you have the following ones for arrays.

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

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

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

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

Please be precise. In a proof indicate exactly why proof lines follow from some other(s). If you use derived rules you have to prove them. Recall that a counter-example has to satisfy all axioms and falsifies φ.

(11 points)

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

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 $[y \geq 0]\ p\ [x = 5 * y + 2]$ is valid with respect to total correctness, where p is the following program:

$$
\begin{array}{l}
c := y; \\
x := 2; \\
\textbf{while } c > 0 \textbf{ do} \\
\quad x := x + 5; \\
\quad c := c - 1 \\
\textbf{od}
\end{array}
$$

(11 points)

(b) Let q be the program

$$
\begin{array}{l}
r := 0; a := x; b := y; \\
\textbf{while } (a \geq 0 \vee b \geq 0) \textbf{ do} \\
\quad \textbf{if } a \geq b \\
\quad \textbf{then } r := r + 1; a := a - 1 \\
\quad \textbf{else } r := r + 1; b := b - 1 \\
\textbf{od}.
\end{array}
$$

Prove that the Hoare triple $\{true\}\ c\ \{r = x + y\}$ is invalid.

Hint: Provide a counterexample, i.e., a state that does not satisfy the correctness assertion.

(2 points)

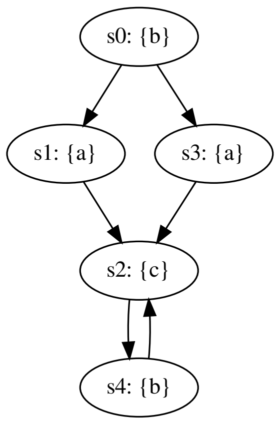
(c) Let q be the program from exercise 3b. State the weakest precondition P such that the triple $\{P\}\ q\ \{r = x + y\}$ is valid.

You are *not* required to prove that P is the weakest precondition.

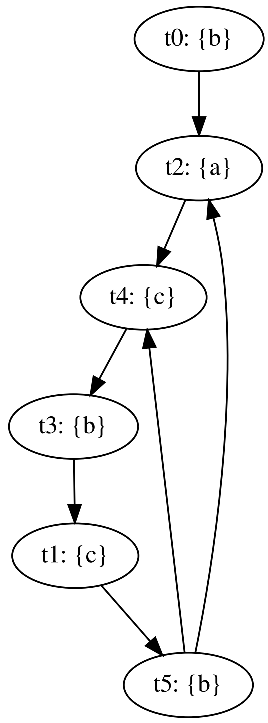
(2 points)

4.) (a) Provide a 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:

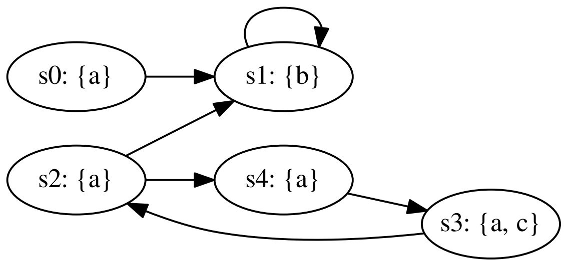


Kripke structure M_2:



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

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

ii.
$$\mathbf{F}(\mathbf{F}p \wedge \mathbf{G}q) \Leftarrow \mathbf{F}p \wedge \mathbf{F}\mathbf{G}q$$

(5 points)

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