6.0/4.0 VU Formale Methoden der Informatik (185.291)

January 26, 2018

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

1.) Consider the following decision problem:

> **HALTING IN LESS STEPS**
>
> INSTANCE: A tuple (Π_1, Π_2, I), where Π_1, Π_2 are programs that take a string as input, and I a string.
>
> QUESTION: Does Π_1 hold on I in strictly less computation steps than Π_2 does on I?

Remark: If a program Π terminates on an input I and a program Π' does not terminate on I, we say that Π holds on I in strictly less computation steps than Π'. In case both programs do not terminate, it is not the case that Π holds on I in strictly less computation steps than Π' on I.

(1) By providing a suitable reduction from the **HALTING** problem, prove that **HALTING IN LESS STEPS** is undecidable.

(2) Is **HALTING IN LESS STEPS** semi-decidable? Explain your answer. **(15 points)**

2.) (a) Show that $a[i] \doteq e \rightarrow a\langle i \triangleleft e\rangle \doteq a$ is $\mathcal{T}_A^{=}$-valid.

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)

(12 points)

(b) Answer the questions about the CDCL algorithm and justify your answers in detail.

i. Suppose that CDCL is applied to solve a propositional formula φ in CNF, and a clause C is learned. Does $\varphi \equiv \varphi \wedge C$ hold?

ii. Consider a run of CDCL on a given CNF F, and suppose that the run has terminated. What is the current decision level in CDCL at the time when CDCL terminates?

(3 points)

3.) Consider the following modified while-rule:

$$\frac{\{\, Inv \wedge e \,\}\, p \,\{\, Inv \,\}}{\{\, Inv \wedge e \,\}\, \textsf{while}\ e\ \textsf{do}\ p\ \textsf{od}\, \{\, Inv \wedge \neg e \,\}} \; \text{mw}$$

(a) Show that this rule is admissible regarding partial correctness. **(5 points)**

(b) Show that the Hoare calculus for partial correctness is no longer complete, if we replace the regular while-rule by the modified one. **(10 points)**

A rule $\frac{X_1 \cdots X_n}{\{F\}\,p\,\{G\}}$ is *admissible regarding partial correctness*, if the conclusion $\{F\}\,p\,\{G\}$ is partially correct whenever all premises $X_1, \ldots, X_n$ are valid formulas/partially correct assertions.

Hoare calculus for partial correctness:

$$\{F\}\,\mathsf{skip}\,\{F\}$$

$$\{F\}\,\mathsf{abort}\,\{G\}$$

$$\{F[v/e]\}\,v := e\,\{F\}$$

$$\frac{\{F\}\,p\,\{G\} \quad \{G\}\,q\,\{H\}}{\{F\}\,p;q\,\{H\}}$$

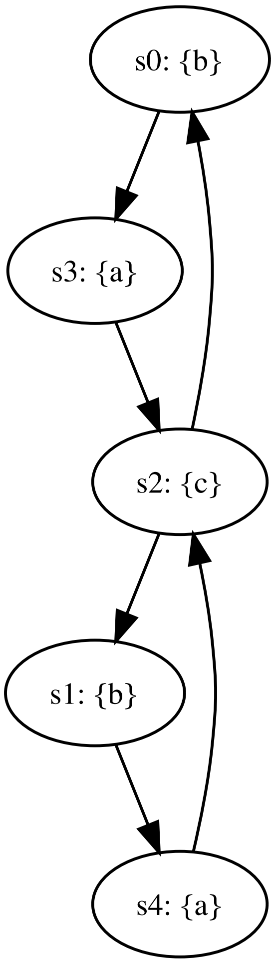
$$\frac{\{F \wedge e\}\,p\,\{G\} \quad \{F \wedge \neg e\}\,q\,\{G\}}{\{F\}\,\mathsf{if}\ e\ \mathsf{then}\ p\ \mathsf{else}\ q\ \mathsf{fi}\,\{G\}}$$

$$\frac{\{Inv \wedge e\}\,p\,\{Inv\}}{\{Inv\}\,\mathsf{while}\ e\ \mathsf{do}\ p\ \mathsf{od}\,\{Inv \wedge \neg e\}}$$

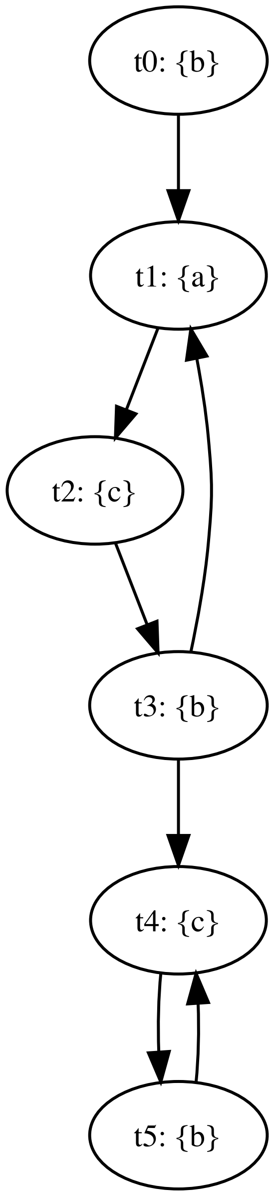
$$\frac{F \Rightarrow F' \quad \{F'\}\,p\,\{G'\} \quad G' \Rightarrow G}{\{F\}\,p\,\{G\}}$$

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:

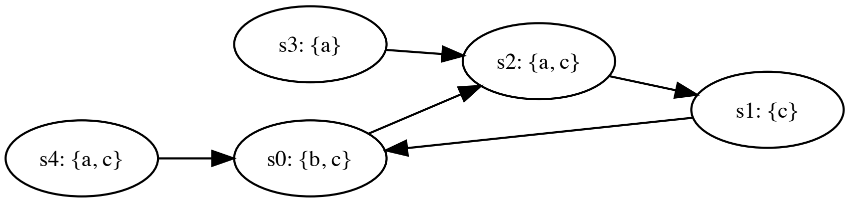


Kripke structure M_2:



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

(5 points)

(c) Consider the LTL formulas $\mathbf{GF}(p\mathbf{U}q)$ and $\mathbf{GF}q$. Prove that they are equivalent or give an example showing that they are not equivalent.

(6 points)