6.0/4.0 VU Formale Methoden der Informatik
185.291 29 June 2018

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

1.) Consider the following decision problem:

> **DIFFERENT RUNTIME**
>
> INSTANCE: A tuple (Π, I_1, I_2), where Π is a program that takes a string as input, and I_1, I_2 are strings.
>
> QUESTION: Does Π hold on I_1 within a different number of computation steps than on I_2?

Remark: If a program Π neither terminates on I_1 nor on I_2, we say that Π requires the same number of computation steps (i.e., infinitly many) for I_1 and I_2.

(1) By providing a suitable reduction from the **HALTING** problem, prove undecidability of **DIFFERENT RUNTIME**.

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

2.) (a) Recall that arrays are represented functionally. For instance, $write(a, i, e)$ is denoted by $a\langle i \triangleleft e\rangle$. Similarly, $read(a, k)$ is denoted by $a[k]$. Show that the following formula $a\langle i \triangleleft e\rangle\langle j \triangleleft f\rangle[k] \doteq g \wedge j \not\doteq k \wedge i \doteq j \wedge a[k] \not\doteq g$ is $\mathcal{T}_A$-unsatisfiable. Please justify any step in your proof in detail.

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)

(12 points)

(b) Show the soundness of the following variant of the resolution rule.

$$\frac{C \vee p \vee q \quad D \vee \neg p \quad E \vee \neg q}{C \vee D \vee E}$$

(3 points)

3.) Prove that the following correctness assertion is true regarding total correctness. Use the invariant $x * m \leq n < y * m \wedge m > 0$. Describe the function computed by the program, if we consider m and n as the inputs and x as the result.

Some annotation rules you might need:

$\{F\}v := e \mapsto \{F\}v := e\{\exists v'(F[v/v'] \wedge v = e[v/v'])\}$

if e then $\{F\} \cdots$ else $\{G\} \mapsto \{(e \Rightarrow F) \wedge (\neg e \Rightarrow G)\}$if e then $\{F\} \cdots$ else $\{G\}$

$\{F\}$if e then $\cdots$ else $\mapsto \{F\}$if e then $\{F \wedge e\} \cdots$ else $\{F \wedge \neg e\}$

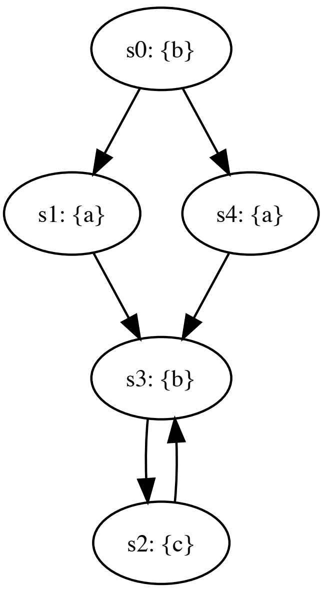
while e do $\cdots$ od $\mapsto \{\,Inv\,\}$while e do $\{\,Inv \wedge e \wedge t{=}t_0\,\} \cdots \{\,Inv \wedge (e \Rightarrow 0{\leq}t{<}t_0)\,\}od\{\,Inv \wedge \neg e\,\}$

```
{ m > 0 ∧ n ≥ 0 }
x := 0;
y := n + 1;
while x + 1 ≠ y do
    z := (x + y)/2;
    if z * m > n then
        y := z
    else
        x := z;
    fi
od
{ x * m ≤ n < (x + 1) * m }
```

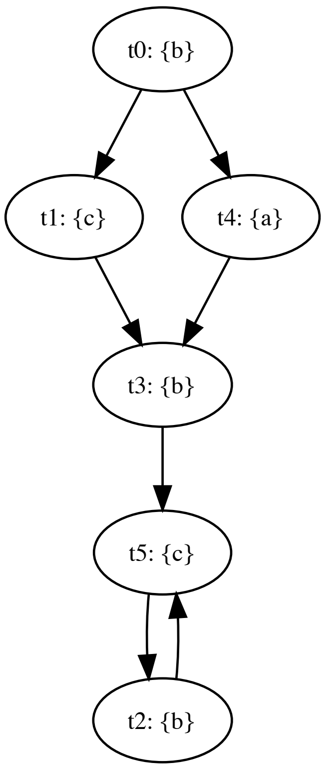
(15 points)

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:

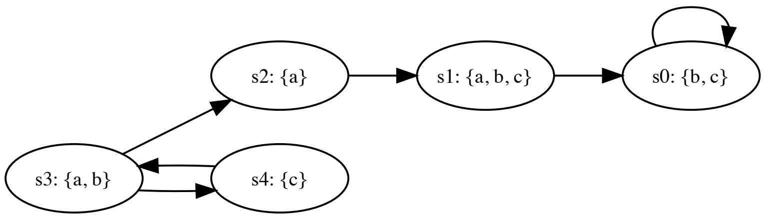


Kripke structure M_2:



(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 $M, s_i \models \varphi$?

Note that by a CTL* formula, we here mean a CTL* *state* formula *or* a CTL* *path* formula. Also recall that for an LTL formula φ we have $M, s \models \varphi$ if and only if $\pi \models \varphi$ for *all* paths in M that start at s.

φ	CTL	LTL	CTL*	States s_i
$\mathbf{G}(c)$	☐	☐	☐	
$((a)\ \mathbf{U}\ (a))$	☐	☐	☐	
$\mathbf{AAF}(a \wedge c)$	☐	☐	☐	
$\mathbf{AX}(a \wedge b)$	☐	☐	☐	
$\mathbf{E}[(b \wedge c)\ \mathbf{U}\ (c)]$	☐	☐	☐	

(5 points)

(c) **LTL tautologies**

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

i.
$$\neg(p\ \mathbf{U}\ q) \rightarrow (\neg \mathbf{G} p \vee \neg \mathbf{F} q)$$

ii.
$$\mathbf{G}(p\ \mathbf{U}\ q) \rightarrow \mathbf{G} p$$

iii.
$$\mathbf{F}(p\ \mathbf{U}\ q) \rightarrow \mathbf{F} q$$

(6 points)