6.0/4.0 VU Formale Methoden der Informatik

185.291 December, 5 2014

Kennzahl (study id)	Matrikelnummer (student id)	Familienname (family name)	Vorname (first name)	Gruppe (version)
				A

1.) Consider the following problem:

> **BOTH-HALT**
>
> INSTANCE: A triple (Π_1, Π_2, I), where I is a string and Π_1, Π_2 are programs that take a string as input.
>
> QUESTION: Is it true that Π_1 halts on I and Π_2 halts on I?

Provide a reduction from **BOTH-HALT** to **HALTING**. Argue formally that your reduction is correct.

(15 points)

2.) (a) Prove or refute the following EUF-formula φ^{EUF}:

$$F(F(F(a))) \doteq F(a) \wedge F(F(a)) \doteq a \rightarrow F(a) \doteq a$$

In case φ^{EUF} is valid, give a proof. Otherwise give a counterexample, i.e., an EUF-interpretation I which falsifies φ^{EUF}. Argue formally that φ^{EUF} is false under I. **(10 points)**

(b) Apply Ackermann's reduction to the following EUF-formula ψ:

$$p(a, F(b)) \wedge F(F(c)) \doteq G(G(b)) \rightarrow p(a, c)$$

Hint: Treat uninterpreted predicates correctly. **(4 points)**

(c) Let φ be a formula, let I be an interpretation for φ, and let M be a model of φ. Explain what I and M have in common. Explain the difference between a model and an interpretation. Is it possible that I is equal to M? **(1 point)**

3.) (a) Show that the axioms $\{\, G[v/e] \,\}\ v := e\ \{\, G \,\}$ and $\{\, F \,\}\ v := e\ \{\, \exists v'\, (F[v/v'] \wedge v = e[v/v']) \,\}$ are equivalent, i.e., that a complete calculus needs only one of the axioms. **(7 points)**

(b) Show that the following program terminates, if we assume that $b = (c+1)^3 \wedge 0 \leq c^3 \leq a$ is a loop invariant.

Remember the annotation rule

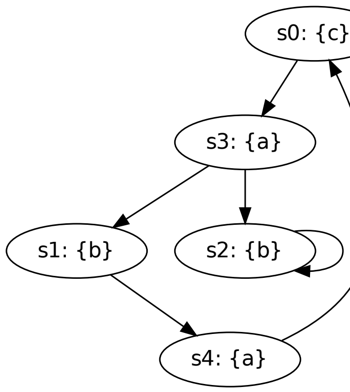
$\mathsf{while}\ e\ \mathsf{do} \cdots \mathsf{od} \mapsto \{\, Inv \,\}\mathsf{while}\ e\ \mathsf{do}\ \{\, Inv \wedge e \wedge t{=}t_0 \,\} \cdots \{\, Inv \wedge (e \rightarrow 0{\leq}t{<}t_0) \,\}\mathsf{od}\{\, Inv \wedge \neg e \,\}$

```
b := 1; c := 0;
while b ≤ a do
   d := 3 * c + 6;
   c := c + 1;
   b := b + c * d + 1
od
```

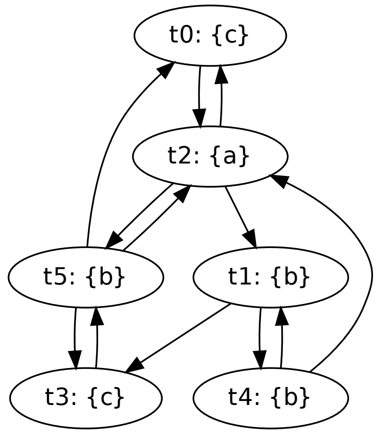
(8 points)

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 (M_1 on the left, M_2 on the right), 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) State a Kripke Structure which statisfies all of the following 4 formulae:

i. $\mathbf{GF}\neg b$

ii. $\mathbf{GF}\neg a$

iii. $\mathbf{GF}(a \wedge b)$

iv. $\mathbf{G}(a\mathbf{U}b)$

(4 points)

(c) State two Kripke structures A and B such that B simulates A and A simulates B but A and B are *not* bisimilar, i.e. $A \leq B$ and $B \leq A$ but not $A \equiv B$. Argue why in your example A and B are not bisimilar.

(7 points)

DEFINITIONS

Let $M_1 = (S_1, I_1, R_1, L_1)$ and $M_2 = (S_2, I_2, R_2, L_2)$ be two Kripke structures.

Simulation

A relation $H \subseteq S_1 \times S_2$ is a simulation relation if for each $(s, s') \in H$ holds:

- $L_1(s) = L_2(s')$, and
- for each $(s, t) \in R_1$ there is a $(s', t') \in R_2$ such that $(t, t') \in H$.

M_2 *simulates* M_1 (denoted as $M_1 \leq M_2$), if there is a simulation relation $H \subseteq S_1 \times S_2$ *such that*

- for each initial state $s \in I_1$ there is an initial state $s' \in I_2$ with $(s, s') \in H$.

We say that H *witnesses the similarity of* M_1 *and* M_2 in case H is a simulation relation from M_1 to M_2 that satisfies the condition stated above.

Bisimulation

A relation $H' \subseteq S_1 \times S_2$ is a *bisimulation relation* if for each $(s, s') \in H'$ holds:

- $L_1(s) = L_2(s')$, and
- for each $(s, t) \in R_1$ there is a $(s', t') \in R_2$ such that $(t, t') \in H'$, and
- for each $(s', t') \in R_2$ there is a $(s, t) \in R_1$ such that $(t, t') \in H'$.

M_1 and M_2 are bisimilar (denoted as $M_1 \equiv M_2$) if there is a bisimulation relation $H' \subseteq S_1 \times S_2$ *such that*

- for each initial state $s \in I_1$ there is an initial state $s' \in I_2$ with $(s, s') \in H'$, and
- for each initial state $s' \in I_2$ there is an initial state $s \in I_1$ with $(s, s') \in H'$.