6.0/4.0 VU Formale Methoden der Informatik (185.291)

February 1, 2013

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

1.) Consider the following problem:

> **FIND-INPUT**
>
> INSTANCE: A pair (Π_1, Π_2) of programs such that:
>
> - Π_1 takes a *string* as input and outputs a string, and
> - Π_2 takes an *integer* as input and outputs a string.
>
> It is guaranteed that Π_1 and Π_2 terminate on any input.
>
> QUESTION: Does there exist a string S and an integer n such that $\Pi_1(S) = \Pi_2(n)$? Here $\Pi_1(S)$ is the string returned by Π_1 on the string S, and $\Pi_2(n)$ is the string returned by Π_2 on the integer n.

Prove that the problem **FIND-INPUT** is semi-decidable. For this, describe a procedure that shows the semi-decidability of the problem (i.e. a semi-decision procedure for **FIND-INPUT**) and argue that it is correct.

(15 points)

2.) (a) The removal of Boolean variables from an E-formula is defined as follows:

Definition. Let φ^E be any E-formula with Boolean variables $b_1, \ldots, b_n$. Construct an E-formula ψ^E without any Boolean variable by replacing each b_i by $v_{b_{i,1}} \doteq v_{b_{i,2}}$ where $v_{b_{i,1}}$, $v_{b_{i,2}}$ are two new term variables (identifiers).

Prove that φ^E is E-satisfiable iff ψ^E is E-satisfiable. **(10 points)**

(b) Transform the EUF-formula φ^{EUF} below to an E-formula φ^E using Ackermann's reduction. Note that φ^{EUF} contains an uninterpreted predicate, which requires special treatment first.

$$\varphi^{EUF}: \quad F(F(x_1)) \doteq G(x_2, G(x_1, x_3, x_4), F(x_2)) \rightarrow p(x_1, y).$$

(5 points)

3.) (a) We use $[x]$ to denote the function associated with the syntactic entity x, where x may be a program, an expression, or one of the pre-defined operators. Investigate for each of the three cases, whether $[x] = [y]$ implies $x = y$ for arbitrary programs/expressions/operators x and y. If yes, give an argument for it, if not, give a counterexample. Note that these are three separate questions. What about the converse: Does $x = y$ necessarily imply $[x] = [y]$? **(5 points)**

(b) Show that the following correctness assertion is totally correct. Describe the function computed by the program; assume x and y to be the inputs and z the output of the program.

Depending on how you choose the variant, use one of the following annotation rules:

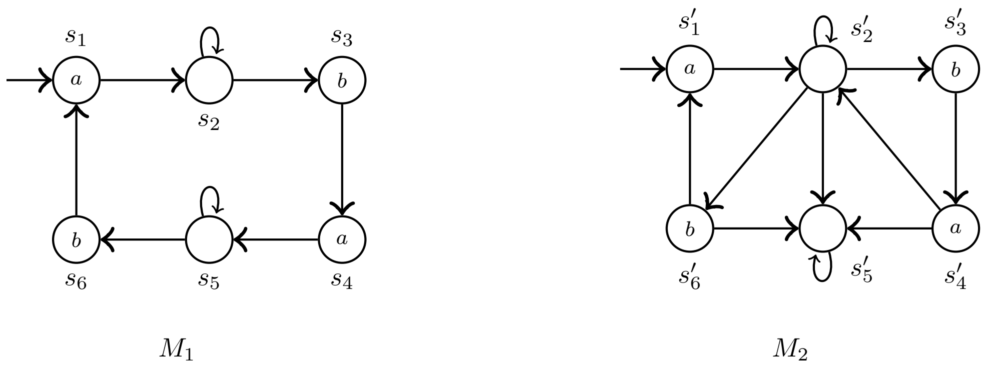
$\mathsf{while}\ e\ \mathsf{do} \cdots \mathsf{od} \mapsto \{\, Inv \,\}\mathsf{while}\ e\ \mathsf{do}\ \{\, Inv \wedge e \wedge t{=}t_0 \,\} \cdots \{\, Inv \wedge 0{\le}t{<}t_0 \,\}\mathsf{od}\{\, Inv \wedge \neg e \,\}$

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

$\{\, 1\colon x \geq 1 \wedge y \geq 2 \,\}$
$u := y;$
$z := 0;$
$\{\, Inv\colon u = y^{z+1} \wedge u \leq x * y \wedge y > 0 \,\}$
while $u \leq x$ do
    $u := u * y;$
    $z := z + 1$
od
$\{\, 2\colon y^z \leq x < y^{z+1} \,\}$

(10 points)

4.) Simulation.



(a) Show that M_2 simulates M_1, i.e., that $M_1 \leq M_2$.

(6 points)

(b) For Kripke structures M_1 and M_2 given above, provide an $\mathsf{ECTL}^\star$ formula φ such that $M_1 \not\models \varphi$ but $M_2 \models \varphi$. Justify why $M_1 \not\models \varphi$ and $M_2 \models \varphi$ holds, respectively.

(6 points)

(c) Show that the following theorem holds.

> **Theorem.**
> If $M_1 \leq M_2$ holds, then for all $\mathsf{ECTL}^\star$ formulas φ holds that if $M_1 \models \varphi$, then $M_2 \models \varphi$.

Hint: You can use the following theorem from the lecture:

> **Theorem.**
> If $M_1 \leq M_2$ holds, then for all $\mathsf{ACTL}^\star$ formulas φ holds that if $M_2 \models \varphi$, then $M_1 \models \varphi$.

(3 points)