6.0/4.0 VU Formale Methoden der Informatik

185.291 WS 2012 3 May 2013

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

1.) Consider the following problem:

> **ECO-VERTEX-COVER (EVC)**
>
> INSTANCE: Undirected graph $G = (V, E)$.
>
> QUESTION: Does there exist a set N, where $N \subseteq V$, such that: for all edges $[a, b] \in E$, we have $|\{a, b\} \cap N| = 1$, i.e. exactly one of a, b is in N?

We provide next a reduction from **EVC** to **2-SAT**. Let $G = (V, E)$ be an arbitrary undirected graph (i.e. an arbitrary instance of **EVC**), where $V = \{v_1, \ldots, v_n\}$. For the reduction we use propositional variables $x_1, \ldots, x_n$. Then the instance φ_G of **2-SAT** resulting from G is defined as follows:

$$\varphi_G = \bigwedge_{[v_i,v_j]\in E} (x_i \vee x_j) \wedge (\neg x_i \vee \neg x_j).$$

Task: Prove the "$\Leftarrow$" direction in the proof of correctness of the reduction, i.e. prove the following statement: if φ_G is a positive instance of **2-SAT**, then G is a positive instance of **EVC**.

Note: For any property that you use in your proof, make it perfectly clear why this property holds (e.g., "by the problem reduction", "by the assumption X", "by the definition X", etc.)

(15 points)

2.) (a) A SAT solver is given the following set of clauses:

$c_1 = (\neg a \vee b \vee e)$ $c_2 = (c \vee \neg e)$ $c_3 = (\neg a \vee \neg c \vee \neg d)$
$c_4 = (\neg b \vee \neg d)$ $c_5 = (\neg b \vee \neg e \vee f)$

i. Draw an implication graph starting with decisions $a = 1@1$, $b = 0@2$ and apply BCP with the clauses above.

ii. Extract a satisfying assignment σ from the implication graph. Is σ a partial or a complete assignment?

(4 points)

(b) In the lecture, we discussed reasoning under different theories. Here we are concerned with LISP-like lists and the theory $\mathcal{T}^E_{cons} = \mathcal{T}_{cons} \cup \mathcal{T}_E$. In a verification attempt of some program, we have to prove the following:

Given a non-atomic list ℓ, we construct a new list by changing $car(\ell)$ by another list b. If $car(\ell) \doteq b$ then ℓ and the new list are equal.

We formalize the above statement as follows:

$$\varphi: \quad \left[\neg atom(\ell) \wedge car(\ell) \doteq b\right] \rightarrow \ell \doteq cons\,(b, cdr\,(\ell))$$

Task: Prove the statement $\mathcal{T}^E_{cons}$-valid, i.e., show that $\mathcal{T}^E_{cons} \models \varphi$.

Hint: The following axioms might be helpful:

(1) Substitution axioms (functional congruence) for *cons*:

$$\forall x_1 \forall x_2 \forall y_1 \forall y_2\, [(x_1 \doteq x_2 \wedge y_1 \doteq y_2) \rightarrow cons(x_1, y_1) \doteq cons(x_2, y_2)]$$

(2) Construction:

$$\forall x\, [\neg atom(x) \rightarrow x \doteq cons(car(x), cdr(x))]$$

(3) Equality axioms:

$$\forall x\,(x \doteq x) \qquad \text{(Reflexivity)}$$
$$\forall x \forall y\,(x \doteq y \rightarrow y \doteq x) \qquad \text{(Symmetry)}$$
$$\forall x \forall y \forall z\,[(x \doteq y \wedge y \doteq z) \rightarrow x \doteq z] \qquad \text{(Transitivity)}$$

(11 points)

3.) Let p be the program $\mathsf{while}\ i > j\ \mathsf{do}\ i := j/2;\ j := i - 2\ \mathsf{od}$. For each of the four correctness assertions $\{\,\phi\,\}\,p\,\{\,\text{true}\,\}$, $\{\,\phi\,\}\,p\,\{\,\text{false}\,\}$, $\{\,\text{true}\,\}\,p\,\{\,\phi\,\}$, and $\{\,\text{false}\,\}\,p\,\{\,\phi\,\}$ find formulas ϕ **that are neither equivalent to true nor to false** such that the assertion is partially correct, partially but not totally correct, totally correct, or totally but not partially correct. In total, these may be up to 16 formulas. Note that in some cases the required formula ϕ may not exist; mark the entry in the table below correspondingly.

$p \equiv \mathsf{while}\ i > j\ \mathsf{do}\ i := j/2;\ j := i - 2\ \mathsf{od}$

	partially correct	partially but not totally correct	totally correct	totally but not partially correct
$\{\,\phi\,\}\,p\,\{\,\text{true}\,\}$				
$\{\,\phi\,\}\,p\,\{\,\text{false}\,\}$				
$\{\,\text{true}\,\}\,p\,\{\,\phi\,\}$				
$\{\,\text{false}\,\}\,p\,\{\,\phi\,\}$				

(15 points)

4.) Model Checking

(a) Consider the two **CTL** formulas $\mathsf{AGAF}p$ and $\mathsf{AFAG}p$. Give a Kripke structure that distinguishes these two formulas, i.e., give a Kripke structure for which one formula is true and the other formula is not. Justify your answer. **(4 points)**

(b) Show that the following theorem holds.

Theorem.
Consider two Kripke structures $M_1 = (S_1, I_1, R_1, L_1)$ and $M_2 = (S_2, I_2, R_2, L_2)$ such that M_1 is simulated by M_2, i.e., $M_1 \leq M_2$.
Prove that for every path $s_0 s_1 \dots s_k$ of M_1 starting with $s_0 \in I_1$ there exists a corresponding path $t_0 t_1 \dots t_k$ of M_2 with the following properties:

i. It holds that $t_0 \in I_2$.

ii. For every $i \geq 0$ it holds that $L_1(s_i) = L_2(t_i)$.

Hint: Recall the definition of simulation from the lectures and use induction on the length of a path:
M_2 simulates M_1 (in signs $M_1 \leq M_2$) iff there is a *simulation relation* $H \subseteq S_1 \times S_2$ with the following properties satisfied for every pair $(s_1, s_2) \in H$:

i. Labels coincide: $L_1(s_1) = L_2(s_2)$.

ii. For every transition $(s_1, t_1) \in R_1$ there is a matching transition $(s_2, t_2) \in R_2$ with $(t_1, t_2) \in H$.

iii. For every initial state $s_1 \in I_1$ there is a corresponding initial state $s_2 \in I_2$ such that $(s_1, s_2) \in H$.

(5 points)

(c) Give an algorithm that computes those states s of a given Kripke structure $M = (S, T, L)$ for which $M, s \models \mathsf{EFAG}p$ holds. **(6 points)**

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