6.0/4.0 VU Formale Methoden der Informatik

185.291 WS2011/SS 2012 29 June 2012

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

1.) We want to prove the *NP-hardness* of **SUBSET SUM**. Your task is to give a polynomial time reduction R from **PARTITION** (which is *NP-complete*) to **SUBSET SUM**. Additionally, prove the "$\Leftarrow$" direction in the proof of correctness of the reduction, i.e., let x denote an arbitrary instance of the PARTITION problem and let $R(x)$ denote the corresponding instance of the SUBSET SUM problem. You have to prove the following statement: if $R(x)$ is a positive instance of **SUBSET SUM**, then x is a positive instance of **PARTITION**.

The definiton of these two problems is given below:

PARTITION:
Instance: A finite set of n positive integers $P = \{p_1, p_2, \dots, p_n\}$.
Question: Can the set P be partitioned into two subsets P_1, P_2 such that the sum of the numbers in P_1 equals the sum of the numbers in P_2?

SUBSET SUM:
Instance: A finite set of integer numbers $S = \{a_1, a_2, \dots, a_n\}$ and an integer number t.
Question: Does there exist a subset $S' \subseteq S$, s.t. the sum of the elements in S' is equal to t, i.e., $\left(\sum_{a_i \in S'} a_i\right) = t$? **(15 points)**

2.) (a) Let φ^E be the following equality logic formula:

$$(x_5 = x_6 \vee x_4 \neq x_5) \wedge x_4 \neq x_6 \wedge x_4 = x_2 \wedge x_2 = x_3 \wedge (x_3 \neq x_1 \vee x_4 = x_1)$$

Apply the *Sparse Method* to obtain an equisatisfiable propositional formula: Apply simplification/preprocessing to obtain an equi-satisfiable φ^E_S; draw the nonpolar equality graph $G^E_{NP}(\varphi^E_S)$; make $G^E_{NP}(\varphi^E_S)$ chordal; compute the propositional skeleton $e(\varphi^E_S)$ and transitivity constraints B_t; and give the resulting propositional formula. **(6 points)**

(b) Given a set $\mathcal{C}$ of clauses, a conflict graph G with respect to $\mathcal{C}$, and some clause D. Prove the following:
If D was learned from G following the first-UIP scheme, then the following formula is valid:

$$\left(\bigwedge_{C \in \mathcal{C}} C\right) \rightarrow D$$

(9 points)

3.) (a) Show that the following version of the 'logical consequence'-rule is not sound, by means of a counter-example; argue that it is a counter-example.

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

(A rule being sound means: "Whenever all premises are true, the conclusion is also true.") **(5 points)**

(b) Show that the following correctness assertion is totally correct. Describe the function computed by the program if we consider n as its input and a as its output.
Hint: Use the annotation rule

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

$\{\, \boldsymbol{n \geq 1} \,\}$
$a \leftarrow 0;$
$b \leftarrow 2;$
$\{\, \boldsymbol{Inv\colon b = 2^{a+1} \wedge 0 < b \leq 2n} \,\}$
while $b \leq n$ do
    $a \leftarrow a + 1;$
    $b \leftarrow b + b$
od;
$\{\, \boldsymbol{2^a \leq n < 2^{a+1}} \,\}$

(10 points)

4.) Computation Tree Logic.

Let AP be a set of propositional symbols, and $AP' \subseteq AP$ be a subset of AP.

We recall the definition of ACTL formulae over AP:

- $p \in AP$ and $\neg p \in AP$ are ACTL formulae,
- if φ and ψ are ACTL formulae, then $\varphi \wedge \psi$, $\varphi \vee \psi$, $\mathbf{AX}\,\varphi$, $\mathbf{AG}\,\varphi$, and $\mathbf{A}\,[\varphi\,\mathbf{U}\,\psi]$ are ACTL formulae.

Let $M = (S, I, R, L)$ and $M' = (S', I', R', L')$ be two Kripke structures related as follows:

- $S = S'$, $I = I'$, $R = R'$, and
- $L'(s) = L(s) \cap AP'$, where $s \in S$.

Let $\hat{M} = (\hat{S}, \hat{I}, \hat{R}, \hat{L})$ be a Kripke structure related to M' as follows:

- $\hat{S} = 2^{AP'}$, i.e., a state $\hat{s} \in \hat{S}$ is a subset of AP',
- $\hat{I} = \{\hat{s} \in \hat{S} \mid \exists s \in I'.\ L'(s) = \hat{s}\}$, i.e., a state $\hat{s} \in \hat{S}$ is an initial state of $\hat{M}$ if there is an initial state $s \in I'$ such that s is labeled with $\hat{s}$.
- $\hat{R} = \{(\hat{s}, \hat{t}) \in \hat{S} \times \hat{S} \mid \exists s, t \in S.\ \hat{s} = L'(s) \wedge \hat{t} = L'(t) \wedge (s, t) \in R'\}$, i.e., for each transition $(\hat{s}, \hat{t}) \in \hat{R}$ there are states $s, t \in S'$ such that there is a transition from s to t and s is labeled with $\hat{s}$ and t is labeled with $\hat{t}$,
- $\hat{L}(\hat{s}) = \hat{s}$ for all $\hat{s} \in \hat{S}$, i.e., each state $\hat{s} \in \hat{S}$ is labeled with the atomic propositions it contains.

(a) Prove that for any $ACTL$ formula φ over propositions from AP' the following holds:

$$M \models \varphi \text{ if and only if } M' \models \varphi$$

Hint: Use the semantics of ACTL. You can either use an induction on the structure of the formula (structural induction) or an induction on the formula length.

(5 points)

(b) Prove that for any ACTL formula φ over propositions from AP' the following holds:

$$\text{If } \hat{M} \models \varphi, \text{ then } M' \models \varphi$$

Hint: You can use the following theorem from the lecture:
Let M_1 and M_2 be Kripke structures such that $M_1 \preceq M_2$. Let φ be an $ACTL^*$ formula. If $M_2 \models \varphi$, then $M_1 \models \varphi$.

(10 points)