Universität Koblenz-Landau

FB 4 Informatik

Prof. Dr. Viorica Sofronie-Stokkermans

December 12, 2013

Exercises for "Decision Procedures for Verification"
Exercise sheet 8

Exercise 8.1: (*6 P*)
Check the satisfiability of the following ground formulae using the algorithm based on congruence closure presented in the lecture.

(1) $\phi_1 = f(f(c)) \approx f(c) \wedge f(f(c)) \approx f(d) \wedge d \not\approx f(c)$.

(2) $\phi_2 = f(f(c)) \approx f(c) \wedge f(c) \approx d \wedge f(d) \not\approx f(f(c))$.

(3) $\phi_3 = h(c, e) \approx d \wedge g(d) \approx e \wedge g(h(c, g(d))) \not\approx e$.

Exercise 8.2: (*4 P*)
Check the satisfiability of the following formulae in (positive) difference logic w.r.t. $\mathbb{Q}$.

(1) $\phi_1 = x - y \leq 3 \;\wedge\; y - z \leq 2 \;\wedge\; x - z \leq 1 \;\wedge\; x - u \leq -3$.

(2) $\phi_2 = x - y \leq 3 \;\wedge\; y - z \leq 2 \;\wedge\; x - z \leq 1 \;\wedge\; x - u \leq -3 \;\wedge u - x \leq 1$.

(3) $\phi_3 = x - y \leq 3 \;\wedge\; y - z \leq 2 \;\wedge\; x - z \leq 1 \;\wedge\; x - u \leq -3 \;\wedge\; u - z \leq 3 \;\wedge\; z - x \leq 1$.

(Note that all graphs have the same sets of nodes, and ϕ_2 and ϕ_3 are obtained from ϕ_1 by adding some constraints.)

Hint: It is sufficient to check the existence of negative cycles in $G(\phi_i)$ by looking at the graphs; in this assignment you do not have to use the Bellman-Ford algorithm for this.

Supplementary exercises:

Exercise 8.3: (*3 P*)
Prove the $\Rightarrow$ part in the correctness proof of the algorithm for checking the validity of a conjunction of literals in UIF, under the assumption that an algorithm for computing the congruence closure of a set R of pairs of vertices in a graph G exists.

Let $\phi := \bigwedge_{i=1}^{n} s_i \approx t_i \wedge \bigwedge_{j=1}^{m} s'_j \not\approx t'_j$ be a ground formula. Let $G = (V, E)$ be the labelled directed graph constructed from ϕ as in the description of the congruence closure algorithm based on Union/Find. Let $R = \{(v_{s_i}, v_{t_i}) \mid i \in \{1, \dots, n\}\}$, and let R^c be the congruence closure of R.

(1) $\mathcal{A}$ is a Σ-structure such that $\mathcal{A} \models \phi$. Prove that $[v_s]_{R^c} = [v_t]_{R^c}$ implies that $\mathcal{A} \models s = t$.
(2) Assume that ϕ is satisfiable. Prove that $[v_{s'_j}]_{R^c} \neq [v_{t'_j}]_{R^c}$.

Hint: Use the fact that if $[v_s]_{R^c} = [v_t]_{R^c}$ then there is a derivation for $(v_s, v_t) \in R^c$ in the calculus defined before; use induction on the length of derivation to show that $\mathcal{A} \models s = t$.

Please submit your solution until Monday, December 16, 2013 at 16:00. Joint solutions prepared by up to three persons are allowed. Please do not forget to write your name on your solution.

Submission possibilities:

- By e-mail to `sofronie@uni-koblenz.de` with the keyword "Homework DP" in the subject.
- Put it in the box in front of Room B 222.