Universität Koblenz-Landau

FB 4 Informatik

Prof. Dr. Viorica Sofronie-Stokkermans

December 28, 2018

Exercises for "Decision Procedures for Verification"
Exercise sheet 8

Exercise 8.1: (*2 P*)
Let ϕ be the following (ground) formula:

$$f(f(c)) \approx f(c) \wedge f(f(c)) \approx f(d) \wedge d \not\approx f(c).$$

(1) Compute $FLAT(\phi)$ (the formula obtained by recursively replacing, in a bottom-up fashion, any term of the form $f(c')$, where c' is a constant, with a new constant).

(2) Compute $FC(\phi)$ (the set of functional consistency axioms associated with the flattening above):

$$FC(\phi) = \{c_1 \approx c_2 \rightarrow d_1 \approx d_2 \mid d_i \text{ is introduced as an abbreviation for } f(c_i)\}.$$

(3) Check whether $FLAT(\phi) \wedge FC(\phi)$ is satisfiable.

(4) Is ϕ is satisfiable? Justify your answer.

Exercise 8.2: (*6 P*)
Check the satisfiability of the following ground formulae using the algorithm based on congruence closure presented in the lecture on Thursday, 20.12.2018 (set of slides presented on 17.12 and 20.12.2018).

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

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

Supplementary exercise:

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 $R = \{(v_{s_i}, v_{t_i}) \mid i \in \{1, \ldots, n\}\}$, 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 Wednesday, January 9, 2018 at 12:00. 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.