Universität Koblenz-Landau

FB 4 Informatik

Prof. Dr. Viorica Sofronie-Stokkermans **December 6, 2011**

Exercises for "Decision Procedures for Verification"
Exercise sheet 8

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

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

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

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

Exercise 8.2: (*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) $\phi_2 = h(c, e) \approx d \wedge g(d) \approx e \wedge g(h(c, g(d))) \not\approx e$.

Exercise 8.3: (*2 P*)
Find the definitions for the following fragments of first-order logic in the slides of the lecture:

- The Bernays-Schönfinkel class;
- The Ackermann class.

To which of these classes do the following formulae belong (note that they can be in more than one, or in none of the classes above):

(1) $\exists y \forall x \;\; ((p(x) \vee r(x, y)) \wedge q(y))$
(2) $\forall x \exists y \forall z \;\; \exists u((p(x) \vee q(y)) \wedge (q(y) \vee p(u))$
(3) $\exists y \forall x \exists z \;\; ((r(x, y) \vee r(y, z)) \wedge q(z) \wedge r(y, z))$
(4) $\exists z \forall x \forall y \exists z' \;\; ((r(x, y) \vee r(y, z)) \wedge s(z, y, z'))$

Supplementary exercises:

Exercise 8.4: *(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 $\mathcal{A} \models s = t$.

Exercise 8.5: *(7 P)*
Let $\Sigma = (\Omega, \Pi)$ be a signature and let X be a set of variables. Let I be an index set. For every $i \in I$ let $\mathcal{A}_i = (U_i, \{f_{\mathcal{A}_i}\}_{f \in \Omega}, \{p_{\mathcal{A}_i}\}_{p \in \Pi})$ be a Σ-algebra. The product of the family of Σ-algebras $\{\mathcal{A}_i\}_{i \in I}$ is the algebra $\prod_{i \in I} \mathcal{A}_i = (U, \{f_{\prod \mathcal{A}_i}\}_{f \in \Omega}, \{p_{\prod \mathcal{A}_i}\}_{p \in \Pi})$, where:

- $U = \prod_{i \in I} U_i$;
- for every $f/n \in \Omega$, $f_{\prod \mathcal{A}_i} : U^n \to U$ is defined component-wise, i.e. for every tuple $((a_i^1)_{i \in I}, \dots, (a_i^n)_{i \in I}) \in U^n$, $f_{\prod \mathcal{A}_i}((a_i^1)_{i \in I}, \dots, (a_i^n)_{i \in I}) = (f_{\mathcal{A}_i}(a_i^1, \dots, a_i^n))_{i \in I}$;
- for every $p/m \in \Pi$, $p_{\prod \mathcal{A}_i} \subseteq U^m$ is defined by:
$$((a_i^1)_{i \in I}, \dots, (a_i^m)_{i \in I}) \in p_{\prod \mathcal{A}_i} \text{ iff } (a_i^1, \dots, a_i^m) \in p_{\mathcal{A}_i} \text{ for all } i \in I.$$

(1) Let $F(x_1, \dots, x_n)$ be a conjunction of atomic formulae. Assume that for every $i \in I$ there exists a valuation $\beta_i : X \to \mathcal{A}_i$ such that $(\mathcal{A}_i, \beta_i) \models F(x_1, \dots, x_n)$. Let $\beta : X \to \prod_{i \in I} \mathcal{A}_i$ be defined by $\beta(x) = (\beta_i(x))_{i \in I}$. Prove that $(\prod_{i \in I} \mathcal{A}_i, \beta) \models F(x_1, \dots, x_n)$.

(2) Assume that I is finite and let $\{A_i(x_1, \dots, x_{n_i}) \mid i \in I\}$ be a family of atomic formulae with the property that $(\mathcal{A}_i, \beta_i) \not\models A_i(x_1, \dots, x_{n_i})$. Let $\beta : X \to \prod_{i \in I} \mathcal{A}_i$ be defined by $\beta(x) = (\beta_i(x))_{i \in I}$. Prove that: $(\prod_{i \in I} \mathcal{A}_i, \beta) \not\models \bigvee_{i \in I} A_i(x_1, \dots, x_{n_i})$.

Please submit your solution until Friday, December 9, 2011 at 17:00 by e-mail to `sofronie@uni-koblenz.de` with the keyword "Homework DP" in the subject.

Joint solutions prepared by up to two persons are allowed.
Please do not forget to write your name on your solution!