Universität Koblenz-Landau

FB 4 Informatik

Prof. Dr. Viorica Sofronie-Stokkermans

January 10, 2012

Exercises for "Decision Procedures for Verification"
Exercise sheet 10

Exercise 10.1: *(2 P)*
Let F be the following conjunction (in linear rational arithmetic):

$$\begin{array}{lrcll} F: & x_1 + x_2 + 2x_3 & = & 2 & \wedge \\ & x_1 + x_3 + \frac{1}{5} & < & 0 & \wedge \\ & x_2 - x_3 & \leq & \frac{1}{2} & \wedge \\ & x_1 + 5x_3 & \leq & 5 & \end{array}$$

Check the satisfiability of F using:

(1) the Fourier-Motzking method for quantifier elimination;
(2) the Loos-Weispfenning method for quantifier elimination.

Exercise 10.2: *(4 P)*
Let $\mathcal{T}$ be the combination of $LI(\mathbb{Q})$ (linear arithmetic over $\mathbb{Q}$) and UIF_Σ, the theory of uninterpreted function symbols in the signature $\Sigma = \{\{f/1, g/2\}, \emptyset\}$.
Check the satisfiability of the following ground formulae w.r.t. $\mathcal{T}$ using the deterministic version of the Nelson-Oppen procedure (after purifying the formulae check for entailment of equalities between shared constants and propagate the entailed equalities):

(1) $\phi_1 = (c + d \approx e \wedge f(e) \approx c + d \wedge f(f(c + d)) \not\approx e)$.
(2) $\phi_2 = (g(c+d, e) \approx f(g(c, d)) \wedge c + e \approx d \wedge e \geq 0 \wedge c \geq d \wedge g(c, c) \approx e \wedge f(e) \not\approx g(c+c, 0))$

Exercise 10.3: *(2 P)*
Let $\mathcal{T}$ be the combination of $LI(\mathbb{Z})$ (linear arithmetic over $\mathbb{Z}$) and UIF_Σ, the theory of uninterpreted function symbols in the signature $\Sigma = \{\{f/1, g/2\}, \emptyset\}$.
Check the satisfiability of the following ground formula w.r.t. $\mathcal{T}$ using the "guessing" version of the Nelson-Oppen procedure:

- $\phi = (f(c) > 0 \wedge f(d) > 0 \wedge f(c) + f(d) \approx e \wedge g(c, e) \not\approx g(d, e))$

Exercise 10.4: *(2 P)*
Let $\Sigma = (\Omega, \Pi)$ be a signature, and let $\Pi_0 \subseteq \Pi \cup \{\approx\}$.

> We say that a theory $\mathcal{T}$ is Π_0-*convex* if for all atomic formulae $A_1(\overline{x}), \dots, A_n(\overline{x})$, and all atomic formulae $B_1(\overline{x}), \dots, B_k(\overline{x})$ which start with predicate symbols in Π_0:
>
> If $\mathcal{T} \models (\bigwedge_{i=1}^{n} A_i(\overline{x})) \rightarrow (\bigvee_{j=1}^{k} B_j(\overline{x}))$ then there exists $1 \leq j \leq k$ s.t. $\mathcal{T} \models (\bigwedge_{i=1}^{n} A_i(\overline{x})) \rightarrow B_j(\overline{x})$.

Let $\mathcal{T}_{\mathbb{Z}}$ be the theory of integers having as signature $\Sigma_{\mathbb{Z}} = (\Omega, \Pi)$, where $\Omega = \{\dots, -2, -1, 0, 1, 2, \dots\} \cup \{\dots, -3\cdot, -2\cdot, 2\cdot, 3\cdot, \dots\} \cup \{+, -\}$ and $\Pi = \{\leq\}$, where:

- $\dots, -2, -1, 0, 1, 2, \dots$ are constants (intended to represent the integers)
- $\dots, -3\cdot, -2\cdot, 2\cdot, 3\cdot, \dots$ are unary functions (representing multiplication with constants)
- $+, -$ are binary functions (usual addition/subtraction)
- $\leq$ is a binary predicate.

The intended interpretation of $\mathcal{T}_{\mathbb{Z}}$ has domain $\mathbb{Z}$, and the function and predicate symbols are interpreted in the obvious way.

Show that:

- $\mathcal{T}_{\mathbb{Z}} \models [(1 \leq z \wedge z \leq 2 \wedge u \approx 1 \wedge v \approx 2) \rightarrow (z \approx u \vee z \approx v)]$
- $\mathcal{T}_{\mathbb{Z}} \not\models [(1 \leq z \wedge z \leq 2 \wedge u \approx 1 \wedge v \approx 2) \rightarrow z \approx u]$
- $\mathcal{T}_{\mathbb{Z}} \not\models [(1 \leq z \wedge z \leq 2 \wedge u \approx 1 \wedge v \approx 2) \rightarrow z \approx v]$

Is $\mathcal{T}_{\mathbb{Z}}$ $\{\approx\}$-convex? Is $\mathcal{T}_{\mathbb{Z}}$ $\{\leq\}$-convex?

Supplementary exercises.

Exercise 10.5: *(2 P)*
Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be two theories with signatures Σ_1, Σ_2. Assume that Σ_1 and Σ_2 share only constants and the equality predicate. Let ϕ be a ground formula over the signature $(\Sigma_1 \cup \Sigma_2)^c = (\Omega_1 \cup \Omega_2 \cup C, \Pi_1 \cup \Pi_2)$ (the extension of the union $\Sigma_1 \cup \Sigma_2$ with a countably infinite set C of constants). The *purification* step in the Nelson-Oppen decision procedure for satisfiability of ground formulae in the combination of $\mathcal{T}_1$ and $\mathcal{T}_2$ can be described as follows:

(Step 1) Purify all terms by replacing, in a bottom-up manner, the "alien" subterms in ϕ (i.e. terms starting with a function symbol in Σ_i occurring as arguments of a function symbol in Σ_j, $j \neq i$) with new constants (from a countably infinite set C of constants). The transformations are schematically represented as follows:

$$(\neg)P(\dots, g(..., f(t_1, \dots, t_n), ...), \dots) \quad \mapsto \quad (\neg)P(\dots, g(..., u, ...), \dots) \wedge u{\approx}t$$

where $t = f(t_1, \dots, t_n), f \in \Sigma_1, g \in \Sigma_2$ (or vice versa).

(Step 2) Purify mixed equalities and inequalities by adding additional constants and performing the following transformations (where $f \in \Sigma_1$ and $g \in \Sigma_2$ or vice versa):

$$f(s_1, \dots, s_n) \approx g(t_1, \dots, t_m) \quad \mapsto \quad u{\approx}f(s_1, \dots, s_n) \wedge u{\approx}g(t_1, \dots, t_m)$$
$$f(s_1, \dots, s_n) \not\approx g(t_1, \dots, t_m) \quad \mapsto \quad u{\approx}f(s_1, \dots, s_n) \wedge v{\approx}g(t_1, \dots, t_m) \wedge u \not\approx v$$

(Step 3) Purify mixed literals by renaming alien terms:

$$(\neg)P(\dots, s_i, \dots) \quad \mapsto \quad (\neg)P(\dots, u, \dots) \wedge u{\approx}s_i$$

if P is a predicate symbol in Σ_1 and s_i is a Σ_2^c-term (or vice versa).

After purification we obtain a conjunction $\phi_1 \wedge \phi_2$, with ϕ_i ground Σ_i^c-formula. Prove that:

- ϕ is satisfiable w.r.t. $\mathcal{T}_1 \cup \mathcal{T}_2$ if and only if $\phi_1 \wedge \phi_2$ is satisfiable w.r.t. $\mathcal{T}_1 \cup \mathcal{T}_2$.
- If ϕ is satisfiable w.r.t. $\mathcal{T}_1 \cup \mathcal{T}_2$ then ϕ_i is satisfiable w.r.t. $\mathcal{T}_i$ for $i = 1, 2$.

Exercise 10.6: *(4 P)*
Let $\mathcal{T}$ be a theory with signature $\Sigma = (\Omega, \Pi)$ and $\mathsf{Mod}(\mathcal{T})$ be its class of models.

(1) Show that if $\mathsf{Mod}(\mathcal{T})$ is closed under products then $\mathcal{T}$ is Π-convex.
(2) Assume that $\mathcal{T}$ is axiomatized by a set of Horn clauses. Show that in this case $\mathsf{Mod}(\mathcal{T})$ is closed under products. Use (1) to show that $\mathcal{T}$ is Π-convex.

Please submit your solution until Friday, January 13, 2012 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!