Universität Koblenz-Landau

FB 4 Informatik

Prof. Dr. Viorica Sofronie-Stokkermans **January 17, 2023**

Exercises for "Decision Procedures for Verification"
Exercise sheet 11

Exercise 11.1: *(4 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 formulae w.r.t. $\mathcal{T}$ using the "guessing" version of the Nelson-Oppen procedure:

(1) $\phi = (c + d \approx e \wedge f(e) \approx c + d \wedge f(f(c + d)) \not\approx e)$.
(2) $\psi = (f(c) > 0 \wedge f(d) > 0 \wedge f(c) + f(d) \approx e \wedge g(c, e) \not\approx g(d, e))$

Exercise 11.2: *(4 P)*
Let $\Sigma = (\Omega, \Pi)$ be a signature, and let $\Pi_0 \subseteq \Pi \cup \{\approx\}$.

> We say that a theory $\mathcal{T}$ is *convex* if for all atomic formulae $A_1(\overline{x}), \dots, A_n(\overline{x})$, and all atomic formulae $B_1(\overline{x}), \dots, B_k(\overline{x})$ where $B_i(\overline{x})$ is the equality $s_i \approx t_i$, with s_i, t_i terms:
>
> 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 $\mathcal{T}_\mathbb{Z}$ convex?

You will be able to solve Exercise 12.3 only after the lecture on Monday, 23.01.2023.

Exercise 11.3: *(2 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 formula 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):

$$\phi = (c + d \approx e \wedge f(e) \approx c + d \wedge f(f(c + d)) \not\approx e).$$

Please submit your solution until Tuesday, January 24, 2023 at 23:59. Joint solutions prepared by up to three persons are allowed. Please do not forget to write your name on your solution.

Submission possibilities:

- OLAT folder Homework 11