Universität Koblenz-Landau

FB 4 Informatik

Prof. Dr. Viorica Sofronie-Stokkermans **January 30, 2019**

Exercises for "Decision Procedures for Verification"
Exercise sheet 12

Exercise 12.1: *(2 P)*
Let $\mathcal{T} = LI(\mathbb{Q})$, and let $Q := x \geq 1, R := x \leq y, P := x + x \leq 2$. Use a DPLL($\mathcal{T}$) method to check the satisfiability w.r.t. $\mathcal{T}$ of the following set of clauses:

$$\begin{array}{ll} (C_1) & \neg R \vee P \\ (C_2) & \neg Q \vee \neg P \\ (C_4) & R \vee P \end{array}$$

Exercise 12.2: *(2 P)*
Let $\mathcal{T} = LI(\mathbb{Q})$, and let $Q := x \leq 1, R := x \leq y, P := x + x \leq 2$. Use a DPLL($\mathcal{T}$) method to check the satisfiability w.r.t. $\mathcal{T}$ of the following set of clauses:

$$\begin{array}{ll} (C_1) & \neg R \vee P \\ (C_2) & \neg Q \vee \neg P \\ (C_4) & R \vee P \end{array}$$

Exercise 12.3: *(4p P)*
Let $\mathcal{T} = LI(\mathbb{Q})$, and let $Q := y \leq 1, R := x \leq y, P := y + y \leq 2, S := x \geq 1$. Use a DPLL($\mathcal{T}$) method to check the satisfiability w.r.t. $\mathcal{T}$ of the following set of clauses:

$$\begin{array}{ll} (1) & \neg R \vee P \\ (2) & \neg Q \vee \neg P \\ (3) & R \vee P \\ (4) & S \end{array}$$

For checking the satisfiability of conjunctions of inequalities in $LI(\mathbb{Q})$ use the Fourier-Motzkin method.

In what follows we consider the theory of arrays which will be defined in the lecture from 4.02.2019. We assume that the theory of indices $\mathcal{T}_i$ is $LI(\mathbb{Z})$, and the theory of elements $\mathcal{T}_e$ is $LI(\mathbb{Q})$.

Exercise 12.4: (*2 P*)
Which of the formulae below are (equivalent to formulae) in the array property fragment and which are not?
Justify your answer. (The universally quantified variables i, j are sort index; the indices k, l which are not universally quantified are considered to be constants of sort index)

(1) $\forall i \; (a[i+1] > a[i])$

(2) $\forall i \; (i < a[k] \rightarrow a[i] = a[k])$

(3) $\forall i, j \; (l_1 \leq i \leq u_1 < l_2 \leq j \leq u_2 \rightarrow a[i] \leq a[j]$

(3) $\forall i, j \; (l_1 < i \leq u_1 < l_2 \leq j \leq u_2 \rightarrow a[i] \leq a[j]$.

Exercise 12.5: (*4 P*)
Consider the following array property formula:

$$F : \forall i \; (l \leq i \leq u \rightarrow a[i] = b[i]) \wedge \neg \forall i \; (l \leq i \leq u + 1 \rightarrow \mathsf{write}(a, u+1, b[u+1])[i] = b[i])$$

Apply to the formula F the Steps 1–6 of the transformation procedure for formulae in the array property fragment presented in the lecture from Monday, 4.02.2019.

Supplementary exercises:

Exercise 12.6: (*5 P*)
We say that a theory $\mathcal{T}$ is *stably infinite* if for every quantifier-free formula ϕ, ϕ is satisfiable in $\mathcal{T}$ iff ϕ is satisfiable in a (countably) infinite model of $\mathcal{T}$.
Let $\mathcal{T}_1, \mathcal{T}_2$ be stably infinite theories with disjoint signatures. Prove that their combination $\mathcal{T}_1 \cup \mathcal{T}_2$ is stably infinite.

Please submit your solution until Wednesday, February 6, 2019 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.