Universität Koblenz-Landau

FB 4 Informatik

Prof. Dr. Viorica Sofronie-Stokkermans

January 23, 2014

Exercises for "Decision Procedures for Verification"
Exercise sheet 12

In what follows we consider the theory of arrays defined in the lecture. 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 12.1: (*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 12.2: (*4 P*)
Consider the array property formula:

$$F : write(a, l, v)[k] = b[k] \wedge b[k] \neq v \wedge a[k] = v \wedge \forall i(i \neq l \rightarrow a[i] = b[i])$$

and let F_6' be the formula obtained (in the example presented in the lecture) by applying Steps 1–6 to F, after simplification.

$$\begin{aligned} F_6' : \quad & a'[k] = b[k] \wedge b[k] \neq v \wedge a[k] = v \wedge (k \neq l \rightarrow a[k] = b[k]) \\ & \wedge a[\lambda] = b[\lambda] \wedge a[l-1] = b[l-1] \wedge a[l+1] = b[l+1] \\ & \wedge a'[l] = v \wedge (k \neq l \rightarrow a[k] = a'[k]) \\ & \wedge a[\lambda] = a'[\lambda] \wedge a[l-1] = a'[l-1] \wedge a[l+1] = a'[l+1] \\ & \wedge \lambda \neq k \wedge \lambda \neq l \wedge \lambda \neq l-1 \wedge \lambda \neq l+1. \end{aligned}$$

Check the satisfiability of F_6' w.r.t. $\mathcal{T} = UIF_{\{a,b,a'\}} \cup \mathcal{T}_i \cup \mathcal{T}_e$ using one of the versions of the $DPLL(\mathcal{T})$ procedure presented in the class. For theory reasoning in $\mathcal{T}$ use the Nelson-Oppen procedure.

Exercise 12.3: (*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.

Please submit your solution until Monday, January 27, 2014 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.