Jochen Hoenicke
Tanja Schindler

07.01.2020
submit until 14.01.2020, 14:15

Tutorials for Decision Procedures
Exercise Sheet 10

Exercise 1: Quantifier-free T_{A} 4 Points

Apply the decision procedure for quantifier-free T_A to decide satisfiability of the following Σ_{A}-formulae:

(a) $a\langle i \triangleleft e\rangle[j] = e \wedge i \neq j$

(b) $a\langle i \triangleleft e\rangle[j] = f \wedge i = j \wedge e \neq f$

(c) $a\langle i \triangleleft e\rangle\langle j \triangleleft f\rangle[i] = g \wedge e \neq g$

(d) $a\langle i \triangleleft e\rangle\langle j \triangleleft f\rangle[i] = g \wedge e \neq g \wedge i \neq j$

Exercise 2: Array Property Fragment of $T_{\mathsf{A}}^{\mathbb{Z}}$ 4 Points

Check *unsatisfiability* of the formulae

(a) $\mathit{sorted}(a, \ell, u) \wedge \mathit{contains}(a, \ell, u, v) \wedge v > a[u]$

(b) $\mathit{sorted}(a, \ell, u) \wedge \neg \mathit{partitioned}(a, \ell, k, k, u)$

where *contains*, *sorted* and *partitioned* are defined as usual:

$$\begin{aligned}
\mathit{contains}(a, \ell, u, v): &\quad \exists i.\ \ell \leq i \leq u \wedge a[i] = v \\
\mathit{sorted}(a, \ell, u): &\quad \forall i, j.\ \ell \leq i \leq j \leq u \ \rightarrow\ a[i] \leq a[j] \\
\mathit{partitioned}(a, \ell_1, u_1, \ell_2, u_2): &\quad \forall i, j.\ \ell_1 \leq i \leq u_1 \wedge \ell_2 \leq j \leq u_2 \ \rightarrow\ a[i] \leq a[j]
\end{aligned}$$

You don't have to write down all clauses, only the ones needed to show unsatisfiability.

Exercise 3: Correctness of Decision Procedure for $T_{\mathsf{A}}^{\mathbb{Z}}$ 4 Points

Let I and J' be interpretations with $\alpha_{J'}[\bar{i}] = \bar{v}$ and $\alpha_{J'}[x] = \alpha_I[x]$ for all symbols except $\cdot[\cdot]$ and the variables $\bar{i}$. In particular $\alpha_{J'}[t] = \alpha_I[t]$ for all $t \in \mathcal{I}$.
Prove for $F[\bar{i}] : \mathit{expr} \leq \mathit{expr}$ that $J' \models F[\bar{i}] \ \rightarrow\ F[\mathit{proj}_I(\bar{v})]$. The expression *expr* is either one of the universal variables i_k or it is a *pexpr* contained in $\mathcal{I}$. You can use that $\mathit{proj}_I(v) \in \mathcal{I}$ and that

either $\alpha_I[\mathit{proj}_I(v)] \leq v$ and $\alpha_I[t'] \leq \alpha_I[\mathit{proj}_I(v)]$ for all $t' \in \mathcal{I}$ with $\alpha_I[t'] \leq v$
or $v < \alpha_I[\mathit{proj}_I(v)]$ and $\alpha_I[\mathit{proj}_I(v)] \leq \alpha_I[t']$ for all $t' \in \mathcal{I}$.