Universität Koblenz-Landau

FB 4 Informatik

Prof. Dr. Viorica Sofronie-Stokkermans **January 31, 2012**

Exercises for "Decision Procedures for Verification"
Exercise sheet 13

In what follows we consider the fragment of the theory of pointers introduced by McPeak and Necula, which was defined in the lecture as follows:

> The language used has two sorts (a pointer sort p and a scalar sort s). Sets Σ_p and Σ_s of pointer resp. scalar fields are given. They can be modeled by functions of sort $\mathsf{p} \rightarrow \mathsf{p}$ and $\mathsf{p} \rightarrow \mathsf{s}$, respectively. A constant null of sort p exists. The only predicate of sort p is equality between pointers; predicates of scalar sort can have any arity. In this language one can define pointer (dis)equalities and arbitrary scalar constraints.
>
> We consider sets of clauses of the form $\forall p \;\; \mathcal{E} \vee \mathcal{C}$ where:
>
> - $\mathcal{E}$ contains disjunctions of pointer equalities (no negative literals allowed);
> - $\mathcal{C}$ contains scalar constraints (sets of both positive and negative literals);
> - it is assumed that for all terms $f_1(f_2(\dots f_n(p)))$ occurring in the body of an axiom, the axiom also contains the disjunction $p = \mathsf{null} \vee f_n(p) = \mathsf{null} \vee \dots \vee f_2(\dots(f_n(p))) = \mathsf{null}$. (This has the rôle of excluding null pointer errors.)
>
> If $f_1, \dots, f_n$ are pointer or scalar fields, $f_1(f_2(\dots f_n(p)))$ will also be written $p.f_n. \dots .f_2.f_1$.

Exercise 13.1: *(5 P)*
Which of the sets of formulae below are (equivalent to formulae) in the fragment of the theory of pointers defined above and which are not?
Justify your answer. (The universally quantified variables p are sort p).

(1) The axiom $\forall p(p \neq \mathsf{null} \rightarrow p.a \neq \mathsf{null})$, where a is a pointer field.

The following axioms (specifying tree shapes) where left and right are pointer fields and kind is a scalar field, and $L \neq R$.

(2) $\forall p((p \neq \mathsf{null} \wedge p.\mathsf{left} \neq \mathsf{null}) \rightarrow (p.\mathsf{left.inv} = p \wedge p.\mathsf{left.kind} = L))$
$\forall p.((p \neq \mathsf{null} \wedge p.\mathsf{right} \neq \mathsf{null}) \rightarrow (p.\mathsf{right.inv} = p \wedge p.\mathsf{right.kind} = R))$

(3) $\forall p((p \neq \mathsf{null} \wedge p.\mathsf{left} \neq \mathsf{null}) \rightarrow (p.\mathsf{left.inv} = p \wedge p.\mathsf{left.kind} \neq R))$
$\forall p((p \neq \mathsf{null} \wedge p.\mathsf{right} \neq \mathsf{null}) \rightarrow (p.\mathsf{right.inv} = p \wedge p.\mathsf{right.kind} \neq L))$
$\forall p(p \neq \mathsf{null} \rightarrow (p.\mathsf{kind} = L \vee p.\mathsf{kind} = R))$

(4) $\forall p(p.\mathsf{left} \neq \mathsf{null} \rightarrow (p.\mathsf{left}.\mathsf{inv} = p \wedge p.\mathsf{left}.\mathsf{kind} = L))$

(5) $\forall p.(p \neq \mathsf{null} \rightarrow (p.\mathsf{right}.\mathsf{inv} = p \wedge p.\mathsf{right}.\mathsf{kind} = R))$

Please submit your solution until Friday, February 3, 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!