Formal Specification of Abstract Datatypes

Wolfgang Schreiner
RISC-Linz

7. Dezember 2000

Exercise 1 (Loose Specs): Deadline January 11

Elaborate Exercise 6.2-5 (attached).

Hint for (ii): the abstract datatype "set" is defined as set $:= \{a : a \approx S\}$ where S is the sp-algebra for which e.g. holds:

$$
\begin{array}{l}
S(set) := \text{the set of all } el-\text{sets} \\
S(Insert)(s,x) := s \cup \{x\} \\
S(Delete)(s,x) := s - \{x\} \\
S(\cup)(s_1,s_2) := s_1 \cup s_2 \\
S(\in)(x,s) := \begin{cases} \text{true, if } x \in s \\ \text{false, otherwise} \end{cases}
\end{array}
$$

To show that sp is strictly adequate, it suffices to show that every element of set is an element of $\mathcal{M}(sp)$ and vice versa.

For proving (ii) and (iii), use induction as a proof method.

Exercise 2 (Initial Specs): Deadline January 25

Consider the classical algebra of integers containing the operations 0, $Succ$, $Pred$, $+$, $-$, $*$, $\leq$.

1. Design an initial specification for the abstract datatype "integer".
2. Show that this specification is adequate using the proof technique of characteristic term algebras.
   Hint: define $C(int) := \{Succ^n(0) : n \geq 0\} \cup \{Pred^n(0) : n \geq 1\}$.

Exercise 3 (CafeOBJ): Deadline February 1

Design constructive versions of the specifications of sets and integers developed in the previous exercises and implement them in CafeOBJ (on the basis of the existing “Bool” specification).

Include the program listing and screen outputs of several sample simplifications in your report.