

Formal Specification of Abstract Datatypes

Wolfgang Schreiner
RISC-Linz

10. Dezember 2002

Exercise 1 (Loose Specs): Deadline January 16

1. Design a loose specification with constructors, say sp , for the algebra of sets containing among others the following operations:

\emptyset	$:\rightarrow set$	the empty set
$Insert$	$: set \times el \rightarrow set$	adds an element to a set
$Delete$	$: set \times el \rightarrow set$	removes an element from a set
\cup	$: set \times set \rightarrow set$	set union
\in	$: el \times set \rightarrow bool$	element predicate

Hint: some of the equations that most hold are, for $s : set, n, m : el$,

$$\begin{aligned}Insert(Insert(s, n), n) &= Insert(s, n) \\Insert(Insert(s, n), m) &= Insert(Insert(s, m), n)\end{aligned}$$

2. Prove that sp is strictly adequate.

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

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

Proof sketch (please elaborate in detail): 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. This amounts to showing that (i) S is a model of the axioms of sp and that (ii) every model A of the axioms of sp is isomorphic to S . To show the second, use induction as demonstrated in class.

3. Let $e : el, s, t : set$ be arbitrary. Prove:

$$\begin{aligned}\mathcal{M}(sp) \models (e \in Delete(s, e)) &= False \\ \mathcal{M}(sp) \models (e \in s) = True &\Rightarrow (e \in s \cup t) = True\end{aligned}$$

To show this, use induction as a proof method.

Exercise 2 (Initial Specs): Deadline January 30

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 March 3

Design a constructive version of the specification of sets developed in Exercise 1 and implement it in CafeOBJ (on the basis of the existing “Bool” specification).

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