Manuel Kauers
RISC-Linz

Hagenberg, December 20, 2002

Formal Specification of Abstract Datatypes

Exercise 1: Loose Specifications

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

$\varnothing\colon \to set$	*the empty set*
$\mathit{Insert}\colon set \times el \to set$	*adds an element to a set*
$\mathit{Delete}\colon set \times el \to set$	*removes an element from a set*
$\cup\colon set \times set \to set$	*set union*
$\in\colon el \times set \to bool$	*element predicate*

Hint: Some of the equations that must hold are, for $s\colon set$, $n, m\colon el$

$$\mathit{Insert}(\mathit{Insert}(s,n),n) = \mathit{Insert}(s,n)$$
$$\mathit{Insert}(\mathit{Insert}(s,n),m) = \mathit{Insert}(\mathit{Insert}(s,m),n).$$

Let sp be defined as follows:

loose spec sp

sorts: $bool, el, set$

operators:
$\mathit{True}\colon \to bool$
$\mathit{False}\colon \to bool$
$\varnothing\colon \to set$
$\mathit{Insert}\colon set \times el \to set$
$\mathit{Delete}\colon set \times el \to set$
$\_ \cup \_\colon set \times set \to set$
$\_ \in \_\colon el \times set \to bool$

generated sorts: $bool, set$

constructors:
$\mathit{True}\colon \to bool$
$\mathit{False}\colon \to bool$
$\varnothing\colon \to set$
$\mathit{Insert}\colon set \times el \to set$

variables:
$s, s_1, s_2\colon set$
$e, m, n\colon el$

axioms:
$\mathit{False} \neq \mathit{True}$
$\mathit{Insert}(\mathit{Insert}(s,n),n) = \mathit{Insert}(s,n)$
$\mathit{Insert}(\mathit{Insert}(s,n),m) = \mathit{Insert}(\mathit{Insert}(s,m),n)$
$\varnothing \cup s = s$
$\mathit{Insert}(s_1,e) \cup s_2 = \mathit{Insert}(s_1 \cup s_2, e)$
$\mathit{Delete}(\varnothing, e) = \varnothing$
$\mathit{Delete}(\mathit{Insert}(s,e),e) = \mathit{Delete}(s,e)$
$\mathit{Insert}(s_1,e) \neq \mathit{Delete}(s_2,e)$
$m \neq n \Rightarrow \mathit{Delete}(\mathit{Insert}(s,m),n) = \mathit{Insert}(\mathit{Delete}(s,n),m)$
$(e \in s) = \mathit{True} \Leftrightarrow s = \mathit{Insert}(s,e)$
$(e \in s) = \mathit{False} \Leftrightarrow s = \mathit{Delete}(s,e)$

end spec.

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*

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

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.*

Consider the algebra S which is defined as follows:

$$\begin{aligned} S(bool) &:= \{\text{true}, \text{false}\} \\ S(set) &:= \text{The set of all finite sets with elements of type } el \\ S(el) &:= \text{An arbitrary set} \\ S(True) &:= \text{true} \\ S(False) &:= \text{false} \\ S(\varnothing) &:= \varnothing \\ S(Insert)(s,e) &:= s \cup \{e\} \\ S(Delete)(s,e) &:= s \setminus \{e\} \\ S(\cup)(s_1,s_2) &:= s_1 \cup s_2 \\ S(\in)(e,s) &:= \begin{cases} \text{true} & \text{if } e \in s \\ \text{false} & \text{otherwise} \end{cases} \end{aligned}$$

We show that S is a model of sp and that every other model of sp is isomorphic to S.

First, S is a model of sp: We have to check that for all sets, elements and boolean values, all axioms of sp are satisfied. So, consider the axioms of sp.

For the purely equational axioms, i.e. for all but the last two axiom, there is nothing to prove. We simply state the claims and refer to Zermelo Fraenkel or something similar for rigorous proofs of the corresponding properties of sets.

$$\begin{aligned} & S(False) \neq S(True) \\ \Leftrightarrow \quad & \text{false} \neq \text{true} \quad \checkmark \\ & S(Insert(Insert(s,n),n)) = S(Insert(s,n)) \\ \Leftrightarrow \quad & (S(s) \cup \{S(n)\}) \cup \{S(n)\} = S(s) \cup \{S(n)\} \quad \checkmark \\ & S(Insert(Insert(s,n),m)) = S(Insert(Insert(s,m),n)) \\ \Leftrightarrow \quad & (S(s) \cup \{S(n)\}) \cup \{S(m)\} = (S(s) \cup \{S(m)\}) \cup \{S(m)\} \quad \checkmark \end{aligned}$$

$$
\begin{array}{rrcl}
& S(\varnothing \cup s) &=& S(s) \\
\Leftrightarrow & \varnothing \cup S(s) &=& S(s) \quad \checkmark \\
& S(\mathit{Insert}(s_1, e) \cup s_2) &=& S(\mathit{Insert}(s_1 \cup s_2, e)) \\
\Leftrightarrow & (S(s_1) \cup \{S(e)\}) \cup S(s_2) &=& (S(s_1) \cup S(s_2)) \cup \{S(e)\} \quad \checkmark \\
& S(\mathit{Delete}(\varnothing, e)) &=& S(\varnothing) \\
\Leftrightarrow & \varnothing \setminus \{S(e)\} &=& \varnothing \quad \checkmark \\
& S(\mathit{Delete}(\mathit{Insert}(s, e), e)) &=& S(\mathit{Delete}(s, e)) \\
\Leftrightarrow & (S(s) \cup \{S(e)\}) \setminus \{e\} &=& S(s) \setminus \{S(e)\} \quad \checkmark \\
& S(\mathit{Insert}(s_1, e)) &\neq& S(\mathit{Delete}(s_2, e)) \\
\Leftrightarrow & S(s_1) \cup \{S(e)\} &\neq& S(s_2) \setminus \{S(e)\} \quad \checkmark
\end{array}
$$

It remains to show that also the last three axiom

$$
\begin{aligned}
& m \neq n \Rightarrow \mathit{Delete}(\mathit{Insert}(s, m), n) = \mathit{Insert}(\mathit{Delete}(s, n), m) \\
& (e \in s) = \mathit{True} \Leftrightarrow s = \mathit{Insert}(s, e) \\
& (e \in s) = \mathit{False} \Leftrightarrow s = \mathit{Delete}(s, e)
\end{aligned}
$$

As for the first of them, we have to check

$$
S(m) \neq S(n) \Rightarrow (S(s) \cup \{S(m)\}) \setminus \{S(n)\} = (S(s) \setminus \{S(n)\}) \cup \{S(m)\} \quad \checkmark.
$$

As for the next one, we have to check

$$
S(e) \in S(s) \Leftrightarrow S(s) = S(s) \cup \{S(e)\} \quad \checkmark.
$$

As for the last one, we have to check

$$
S(e) \in S(s) \Leftrightarrow S(s) = S(s) \setminus \{S(e)\} \quad \checkmark.
$$

Summarizing, we have "shown" that S is a model of *sp*.

It remains to show that each other model A of *sp* is isomorphic to S. We show this by providing an isomorphism between S and A. Let $h\colon S \to A$ be defined by

$$
\begin{aligned}
h(\text{true}) &:= A(\mathit{True}) \\
h(\text{false}) &:= A(\mathit{False}) \\
h(\varnothing) &:= A(\varnothing) \\
h(\{S(a_1), \ldots, S(a_r)\}) &:= A(\mathit{Insert}(\ldots \mathit{Insert}(\mathit{Insert}(\varnothing, a_1), a_2) \ldots, a_r)).
\end{aligned}
$$

For the *bool* type the isomorphism property is immediate by use of the axiom $\mathit{False} \neq \mathit{True}$. In what follows, we therefore restrict ourselves to the *set* type.

First, we show that h is well defined, injective, and surjective.

- h is well defined, because A is a model of *sp* by assumption and so it satisfies the axioms of *sp*. We conclude

  $$
  \begin{aligned}
  & A(\mathit{Insert}(\ldots \mathit{Insert}(\mathit{Insert}(\varnothing, a_1), a_2), \ldots, a_r)) \\
  = {} & A(\mathit{Insert}(\ldots \mathit{Insert}(\mathit{Insert}(\varnothing, a_{\pi(1)}), a_{\pi(2)}), \ldots, a_{\pi(r)}))
  \end{aligned}
  $$

  for any permutation $\pi \in S_r$.

- h is surjective. To show: $h(S(set)) = A(set)$. First, it is immediate that $h(S(set)) \subseteq A(set)$: Write

$$s := \{a_1, a_2, \ldots, a_r\} \in S(set)$$

as

$$s = \{a_1\} \cup \{a_2\} \cup \cdots \cup \{a_r\}.$$

Then

$$h(s) = A(\mathit{Insert}(\ldots \mathit{Insert}(\mathit{Insert}(\varnothing, h(a_1)), h(a_2)) \ldots, h(a_r))) \in A(set).$$

As for the other inclusion, it suffices to show that every term $t\colon set$ has a representation of the form that appears in the definition of h. Consider the map

$$\Phi\colon T_\Sigma \to T_\Sigma$$

which is recursively defined by

$$\begin{aligned}
\Phi(\varnothing) &:= \varnothing, \\
\Phi(\mathit{Insert}(t,m)) &:= \begin{cases} \Phi(t) & \text{if } m \text{ is subterm of } \Phi(t) \\ \mathit{Insert}(\Phi(t), m) & \text{else} \end{cases} \\
\Phi(\varnothing \cup t) &:= \Phi(t) \\
\Phi(\mathit{Insert}(t_1, e) \cup t_2) &:= \mathit{Insert}(\Phi(t_1 \cup t_2), e) \\
\Phi(\mathit{Delete}(t_1, e) \cup t_2) &:= \Phi(\Phi(\mathit{Delete}(t_1, e)) \cup t_2) \\
\Phi((t_1 \cup t_2) \cup t_3) &:= \Phi(\Phi(t_1 \cup t_2) \cup t_3) \\
\Phi(\mathit{Delete}(\varnothing), n) &:= \varnothing \\
\Phi(\mathit{Delete}(\mathit{Delete}(t,m), n)) &:= \Phi(\mathit{Delete}(\Phi(\mathit{Delete}(t,m)), n)), \\
\Phi(\mathit{Delete}(\mathit{Insert}(t,m), n)) &:= \begin{cases} \Phi(t) & m = n \\ \Phi(\mathit{Insert}(t,m)) & m \neq n \end{cases} \\
\Phi(\mathit{Delete}(t_1 \cup t_2), n) &:= \Phi(\mathit{Delete}(\Phi(t_1 \cup t_2), n))
\end{aligned}$$

By structural induction, it is easy to see that $M \models \Phi(t) = t$ for every model M and every term t. Furthermore, iterated application of Φ will always terminate and finally give a term of the desired form.

set is generated, which means that every element of $A(set)$ can be expressed by some term t. Also, we know that every term t has an equivalent term $\tilde{t} = \Phi^n(t)$ of the form which appears in the definition of h, and hence $A(t) = h(s)$ for some $s \in S(set)$ which can be read of the term $\tilde{t}$.

- h is injective: Assume there are terms a, b such that $S(a) \neq S(b)$. Without loss of generality, we can assume the existence of an element $S(e) \in S(a) \setminus S(b)$ (exchange roles of a and b if necessary). We know that $S(e) \in S(a)$ and $S(e) \notin S(b)$, i.e. $S(e \in a) = \text{true}$ und $S(e \in b) = \text{false}$. By the according axioms of sp, we can conclude

$$a = \mathit{Insert}(a, e), \qquad b = \mathit{Delete}(b, e).$$

Since A is a model, we also know that

$$A(a) = A(\mathit{Insert}(a, e)), \qquad A(b) = A(\mathit{Delete}(b, e))$$

and hence

$$A(a) = A(Insert(a, e)) \neq A(Delete(b, e)) = A(b)$$

so $A(a) \neq A(b)$ which was to prove.

Now, we know that h is a bijection between $S(set)$ and $A(set)$. It remains to show that it is also a homomorphism.

For the constant term $\varnothing$, the claim is immediate by the definition of h. For *Insert* and *Delete* terms we show the claim by computation. Note that each step is justified by the axioms of sp, the definition of h, and/or the definition of semantics. Take a set $s = \{s_1, \ldots, s_r\}$ and an element a. Then

$$\begin{aligned}
h(S(Insert)(s, a)) &= h(s \cup \{a\}) \\
&= h(\{s_1, \ldots, s_r, a\}) \\
&= A(Insert(Insert(\ldots Insert(\varnothing, s_1) \ldots, s_r), a)) \\
&= A(Insert)(A(Insert(\ldots Insert(\varnothing, s_1) \ldots, s_r)), A(a)) \\
&= A(Insert)(h(s), h(a)).
\end{aligned}$$

$$h(S(Delete)(s, a)) = h(s \setminus \{a\})$$

Case 1. $a \notin s$. Then

$$\begin{aligned}
h(s \setminus \{a\}) &= h(s) \\
&= h(\{s_1, \ldots, s_r\}) \\
&= A(Insert(\ldots Insert(\varnothing, s_1) \ldots, s_r)) \\
&= A(Delete(Insert(\ldots Insert(\varnothing, s_1) \ldots, s_r), a)) \\
&= A(Delete)(A(Insert(\ldots Insert(\varnothing, s_1) \ldots, s_r)), A(a)) \\
&= A(Delete)(h(s), h(a)).
\end{aligned}$$

Case 2. $a \in s$. W.l.o.g. $a = s_r$. Then

$$\begin{aligned}
h(s \setminus \{a\}) &= h(\{s_1, \ldots, s_{r-1}\}) \\
&= A(Insert(\ldots Insert(\varnothing, s_1) \ldots, s_{r-1})) \\
&= A(Delete(Insert(\ldots Insert(\varnothing, s_1) \ldots, s_r), s_r)) \\
&= A(Delete)(A(Insert(\ldots Insert(\varnothing, s_1) \ldots, s_r)), A(a)) \\
&= A(Delete)(h(s), h(a)).
\end{aligned}$$

It remains to consider the union. Take two sets $s = \{s_1, \ldots, s_r\}$ and a set t. We proceed by induction on the size of t. In the base case, we have

$$\begin{aligned}
h(S(\cup)(t, s)) &= h(S(\cup)(\varnothing, s)) \\
&= h(s) \\
&= A(Insert(\ldots Insert(\varnothing, s_1) \ldots, s_r)) \\
&= A(\varnothing \cup Insert(\ldots Insert(\varnothing, s_1) \ldots, s_r)) \\
&= A(\cup)(A(\varnothing), A(Insert(\ldots Insert(\varnothing, s_1) \ldots, s_r))) \\
&= A(\cup)(h(\varnothing), h(s)).
\end{aligned}$$

As for the induction step, assume that the claim holds for all sets $t = \{t_1, \ldots, t_m\}$ of size $m \geq 0$, and prove that it still holds for $t \cup \{t_{m+1}\}$ where $t_{m+1} \notin t$.

$$
\begin{aligned}
h(S(\cup)(t \cup \{t_{m+1}\}, s)) &= h(\{t_1, \ldots, t_{m+1}, s_1, \ldots, s_r\}) \\
&= h(\{t_1, \ldots, t_m, s_1, \ldots, s_r\} \cup \{t_{m+1}\}) \\
&= A(\mathit{Insert})(h(\{t_1, \ldots, t_m, s_1, \ldots, s_r\}), h(t_{m+1})) \\
&= A(\mathit{Insert})(h(t \cup s), h(t_{m+1})) \\
&= A(\mathit{Insert})(A(\cup)(h(t), h(s)), h(t_{m+1})) \\
&= A(\mathit{Insert}(\mathit{Insert}(\ldots \mathit{Insert}(\varnothing, t_1) \ldots, t_m) \cup \\
&\qquad\qquad \mathit{Insert}(\ldots \mathit{Insert}(\varnothing, s_1) \ldots, s_r), t_{m+1})) \\
&= A(\mathit{Insert}(\ldots \mathit{Insert}(\varnothing, t_1) \ldots, t_{m+1}) \cup \\
&\qquad \mathit{Insert}(\ldots \mathit{Insert}(\varnothing, s_1) \ldots, s_r)) \\
&= A(\cup)(\mathit{Insert}(\ldots \mathit{Insert}(\varnothing, t_1) \ldots, t_{m+1}), \\
&\qquad\quad \mathit{Insert}(\ldots \mathit{Insert}(\varnothing, s_1) \ldots, s_r)) \\
&= A(\cup)(h(\{t_1, \ldots, t_{m+1}\}), h(\{s_1, \ldots, s_r\})) \\
&= A(\cup)(h(t \cup \{t_{m+1}\}), h(s)).
\end{aligned}
$$

We have now proven that h is compatible with all the operations of sp, so h is a homomorphism. And since we proved before that h is also bijective, we finally know that h is an isomorphism. This shows that S is isomorphic to A and since A was an arbitrary model of sp, all models are isomorphic to S. This means that S is strictly adequate *quod erat demonstrandum.*

3. Let $e\colon el$ and $s, t\colon set$ be arbitrary. Prove

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

To show this, use induction as a proof method.

We assume that the lecturer had a different specification in mind when he designed this exercise, because for our axiom system, it makes no sense to attack the first claim by induction. Using the last axiom on page 1, we find that

$$(e \in \mathit{Delete}(s, e)) = \mathit{False}$$

is equivalent to

$$\mathit{Delete}(s, e) = \mathit{Delete}(s, e),$$

i.e. there is nothing to prove.

Also for the second claim, there is a much easier way than induction. Let A be a generated model of sp. Let $s\colon set$ and $e\colon el$ be arbitrary terms with $A(e \in s) = A(\mathit{True})$, and let $t\colon set$. Then,

$$
\begin{aligned}
& & A(e \in s) &= A(\mathit{True}) \\
&\Rightarrow & A(\mathit{Insert}(s, e)) &= A(s) \\
&\Rightarrow & A(\mathit{Insert}(s, e) \cup t) &= A(s \cup t) \\
&\Rightarrow & A(\mathit{Insert}(s \cup t, e)) &= A(s \cup t) \\
&\Rightarrow & A(e \in s \cup t) &= A(\mathit{True}).
\end{aligned}
$$

We dare to hand this in as a solution because every proof (without induction) can be viewed as a special induction proof in which the induction step makes no use of the induction hypothesis.