Formal Specification of Abstract Datatypes
Exercises 2+3 (May 3+24)

Wolfgang Schreiner
Wolfgang.Schreiner@risc.uni-linz.ac.at

April 15, 2010

The result for each exercise is to be submitted by the deadline stated above via the Moodle interface as a .zip or .tgz file which contains

- a PDF file with
  - a cover page with the title of the course, your name, Matrikelnummer, and email-address,
  - the content required by the exercise (specification, source, proof),
- (if required) the CafeOBJ (.mod) file(s) of the specifications.

Exercise 2: Loose Specifiction of Integers

Assume you are given a strictly adequate specification of the classical algebra of Boolean values by a sort *bool* with free constructors $\mathit{True} :\to \mathit{bool}$, $\mathit{False} :\to \mathit{bool}$ and the logical operations $\mathit{not} : \mathit{bool} \to \mathit{bool}$, $\mathit{and} : \mathit{bool} \times \mathit{bool} \to \mathit{bool}$, $\mathit{or} : \mathit{bool} \times \mathit{bool} \to \mathit{bool}$.

Furthermore, assume you are also given a strictly adequate specification of the classical algebra of natural numbers by a sort *nat* with free constructors $0_n :\to \mathit{nat}$ and $\mathit{succ}_n : \mathit{nat} \to \mathit{nat}$, constant $1_n :\to \mathit{nat}$, and operations $-_n : \mathit{nat} \to \mathit{nat}$ ($x -_n y = 0$ for $x \leq y$), $+_n : \mathit{nat} \times \mathit{nat} \to \mathit{nat}$, $*_n : \mathit{nat} \times \mathit{nat} \to \mathit{nat}$, $=_n$: $\mathit{nat} \times \mathit{nat} \to \mathit{bool}$, $<_n$: $\mathit{nat} \times \mathit{nat} \to \mathit{bool}$.

With the help of these sorts and operations, write in a logic of your choice (please state explicitly which one you coose) a loose specification (potentially with constructors) of a sort *int* with constants $0_i :\to \mathit{int}$, $1_i :\to \mathit{int}$ and operations $-_i : \mathit{int} \to \mathit{int}$, $+_i : \mathit{int} \times \mathit{int} \to \mathit{int}$, $*_i : \mathit{int} \times \mathit{int} \to \mathit{int}$, $=_i$: $\mathit{int} \times \mathit{int} \to \mathit{bool}$, $<_i$: $\mathit{nat} \times \mathit{nat} \to \mathit{bool}$. This specification shall be strictly adequate with respect to the classical algebra of integer numbers.

For writing the specification, think how you can construct a representation of the integer numbers as "natural numbers with a sign" (be aware of the special case zero) and define corresponding constructors. Based on this representation, write (potentially recursive) definitions of the other constants and operations.

Also develop an executable version of this specification in CafeOBJ (i.e. a tight module `module! MYINT {...}` based on the existing modules `BOOL` and `NAT`) and test it with a couple of sample reductions. In particular, check whether

$$-_i(0_i) =_i 1_i +_i -_i(1_i)$$

reduces to *true* (deliver the corresponding output).

Exercise 3: Strict Adequacy of Specification

Prove that above specification of the integers is strictly adequate, i.e. that every algebra satisfying this specification is isomorphic to the "classical" integer algebra with carrier $\mathbb{Z}$ (you only need to show the homomorphism condition for the operations 0_i, 1_i, $+_i$, and $=_i$).

For performing the proof, you have to define (as shown in class) a unique term representation for every element of $\mathbb{Z}$ (including 0).