



J. Hoenicke
J. Christ

04.12.2012

Hand in solutions via email to
`christj@informatik.uni-freiburg.de`
until 11.12.2012 (only Java sources and
PDFs accepted)

Tutorials for “Formal methods for Java” Exercise sheet 7

Exercise 1: Universe Type System

On the lecture’s webpage you find an implementation of a heap. The heap is realized by an array, and every element in the heap stores its position in the heap. A method to **enqueue** new elements into the heap, and a method to **remove** an element from the heap are provided. The *Universe Type System* is used to guard the invariant that every element in the heap knows its current position. Unfortunately, this does not work. Explain the problem(s) and discuss why they cannot be solved with this type system.

Exercise 2: Pack/Unpack

Use the *pack/unpack* mechanism to guard the invariant. Change the implementation and verify it with ESC/Java 2. Your solutions are allowed to contain warnings for possible exceptions due to `compareTo` calls.

Hint: To get rid of all warnings you have to tell ESC/Java 2 that the `elems` arrays are not shared between different heaps, i.e., you need an invariant of the form

```
//@ invariant (\forall Heap h; ; h == this || h.elems != elems);
```

Note that this invariant is independent of *pack/unpack* as it is a class invariant and not an object invariant.