Formal Methods in Software Development
Exercise 5 (December 10)

Wolfgang Schreiner
Wolfgang.Schreiner@risc.jku.at

November 20, 2012

The result is to be submitted by the deadline stated above *via the Moodle interface* of the course as a *.zip or .tgz* file which contains

1. a PDF file with
   - a cover page with the course title, your name, Matrikelnummer, and email address,
   - a (nicely formatted) copy of the *.java/.theory* file(s) used in the exercise,
   - the deliverables requested in the description of the exercise,
   - for each program method, a screenshot of the "Analysis" view of the RISC ProgramExplorer with the specification/implementation of the method and the (expanded) tree of all (non-optional) tasks generated from the method,
   - for each program method, a screenshot of the corresponding "Semantics" view and an informal interpretation of the method semantics;
   - for each task an explicit statement whether the goal of the task was achieved or not and, if yes, how (fully automatic proof, immediate completion after starting an interactive proof, complete or incomplete interactive proof),
   - for each truly interactive proof, a screenshot of the corresponding "Verify" view with the proof tree,
   - optionally any explanations or comments you would like to make;
2. the *.java/.theory* file(s) used in the exercise,
3. the task directory (*.PETASKS**) generated by the RISC ProgramExplorer.

Email submissions are *not* accepted.

Exercise 5: Overwriting an Array

Use the RISC ProgramExplorer to specify the following program, reason about its behavior, and verify its correctness with respect to its specification:

```
class Exercise5
{
  // overwrites every occurrence of 'x' in 'a' by 'y'
  // returns true iff some element was overwritten
  public static boolean overwrite(int[] a, int x, int y)
  {
    boolean result = false;
    int n = a.length;
    int i = 0;
    while (i < n)
    {
      if (a[i] == x)
      {
        a[i] = y;
        result = true;
      }
      i = i+1;
    }
    return result;
  }
}
```

Create a separate directory in which you place the file *Exercise5.java*, `cd` to this directory, and start `ProgramExplorer&` from there. The task directory *.PETASKS** is then generated as a subdirectory of this directory.

Then perform the following tasks:

1. (25P) Specify the method by an appropriate contract (clauses `requires`, `assignable`, and `ensures`).

   You have to specify the requirement and the effect on the array (do not forget any side conditions as non-null status and length in pre/post-state) and you have to specify the result value of the function. In the first part, a formula like

   `(FORALL(j:NAT): j < (VAR a).length => IF ... ELSE ... ENDIF)`

   may become handy.

2. (25P) Annotate the loop with an appropriate invariant and termination term (clauses `invariant` and `decreases`).

   In the invariant, start with that part of the precondition that is still true and then focus on your knowledge about the values of `result`, `n`, `i` and `a`.

3. (25P) Investigate the computed semantics of the method, in particular the method's state relation and termination condition in order to judge the adequacy of your annotations. Give an informal interpretation of the semantics and your detailed explanation whether respectively why it seems adequate.

   Take the interpretation and explanation serious; not only will they be judged for the credit of this part of the exercise, they will also help you to detect errors that would be hard to find in the later proofs. In particular, a description in just two sentences will not do to get full credit. At least, interpret the semantics of the loop body, the semantics of the loop, and the semantics of the method body.

4. (25P) Verify all (non-optional) tasks generated from the method. Only few of them should require interactive proofs; most of these can probably be performed just by application of `scatter` and `auto`.

   The only complex case should be the proof at the invariant is preserved; here it is wise to first perform a `decompose` and then a `split` corresponding to the two branches in the loop body (if you immediately performed a `scatter`, you would have to make a `split` in each of the resulting proof obligations which would considerably blow up the proof).