

Formal Methods in Software Engineering

Exercise 7 (December 22)

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

November 11, 2008

The result 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,
 - for each exercise, a section with the number and name of the exercise, the JML-annotated Java code, a copy of the output of an `escjava2` check of that code, and a screen shot of the KeY prover when the proof has been completed (respectively with an open state if you could not complete the proof),
 - an explicit statement where you say whether you could complete the KeY proof or not (and how many states have remained open) and optionally any explanations or comments you would like to make;
- the JML-annotated Java files developed in the exercise,
- the proof files generated by the KeY prover (use the menu option “Save”).

7a (50 points): JML specification and KeY Proof

Consider the function `replace` in class `Exercise7a` (put the attached source file into a subdirectory `exercises` and check/verify it with the parent directory as the current working directory).

Write for this function a JML header specifications that is as expressive as possible and provide the loop with a suitable invariant and termination term (but no assignable clause yet). In the loop invariant use the dummy variable `olda` rather than the term `\old(a)` to refer to the old value of `a`.

Type-check the specification with `jml -Q` (which must not give an error) and then statically check it with `escjava2`. If this gives a warning, reconsider your specification (perhaps you have made an error, but perhaps the warning is also superfluous).

If you are confident with your specification, provide the loop also with an assignable clause and verify the specification with the KeY prover (both the verification conditions for the assignable clause and for the postcondition of the method body). If your specifications are correct, the proofs should run through with repeated applications of “Run” and “Simplify”. If you cannot complete the proof, reconsider your specification.

7b (50 points): JML specification and KeY Proof

Proceed as for Exercise 7a with the function `partition` in class `Exercise7b` (for this task it is not necessary to use the dummy variable).