Formal Methods in Software Development
Exercise 7 (January 10)

Wolfgang Schreiner
Wolfgang.Schreiner@risc.jku.at

July 28, 2021

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 section for each part of the exercise with the requested deliverables and optionally any explanations or comments you would like to make;
2. the JML-annotated `.java`/`.jml` file(s) used in the exercise,
3. the proof files generated by the KeY prover (use the menu option "Save").

Email submissions are *not* accepted.

9a (70 points): A Private JML Class Specification

Take the attached source code of a class `BoundedBag` which implements a "bag" (a multiset) of integers with an upper bound on the number of different elements in the bag. Extend this source by a *private* specification in the *heavy-weight* JML format that is as expressive as possible. Pay attention to provide a suitable object invariant that describes the ranges of the variables and the contents of the arrays as accurately as possible; you also have to provide a suitable invariant for the loop in the body of the class.

Use `jml -Q` and `openjml` to check the specification (which must not yield an error). Run `escjava2 -NoCautions` and `openjmlesc` on the specification; if these tools give warnings, take them seriously[1]. Use KeY to verify the contracts of the various methods as far as possible.

The invariant related to the variable `sum` requires the use of the `\sum` quantifier which is often not so well supported by JML tools; please report your experience with `openjmlesc` and KeY with respect to this quantifier. If it lets the verification fail, you may ultimately comment out the part of the invariant involving this quantifier.

The result of this exercise contains the JML-annotated file `BoundedBag.java`, the output of `jml -Q`, `openjml`, `escjava2 -NoCautions`, and `openjmlesc` on this file, and a screenshot of the final state of KeY for the verification of each method plus an explicit statement whether the verification suceeded (if not, then try to analyze the failed verification and give your estimation, why it did not succeed).

9b (30 points): A Public JML Class Specification

Take the previously JML-annotated file `BoundedBag.java` and modify it for an appropriate *public* specification of class `BoundedBag`; this public specification is to be written into file `BoundedBag.jml` and shall be based on the abstract datatype `BagModel` which specifies an unbounded bag in the attached file `BagModel.java`.

The core idea of modeling a bounded bag (`BoundedBag`) by an unbounded bag (`BagModel`) is is that the public function `size()` in `BoundedBag` poses an upper limit on the number of different elements of the model bag; we can simply express this by an invariant. A constructor call `BoundedBag(n)` sets the limit to `n`, which has to be appropriately specified. The limit is not changed by any of the other functions, which can be specified by a corresponding constraint. A call of `add()` is only allowed, if the upper limit is not reached, which can be expressed by a corresponding precondition.

Some further hints:

- Generally the basic specification strategy is the same as shown in class for the model-based public specification of class `IntStack`.

[1] `openjmlesc` may complain about possible overflows in the variable `sum`; you may ignore these or handle them by additional preconditions and object invariants.

- Introduce in `BoundedBag.jml` a model field of type `BagModel` which receives its value from a model function `toModel()`.
- Give in `BoundedBag.jml` public specifications of the public functions using the model field and the corresponding operations on `BagModel`.
- Annotate `BoundedBag.java` by a `refines` annotation that indicates that the definition of class `BoundedBag` in this file is a refinement of the class declared in `BoundedBag.jml`. Add the keyword `also` to the private specifications of all public methods.
- Give a specification-only definition of the abstraction function `toModel` as

  ```
  /*@ public pure model BagModel toModel() {
    @   BagModel b = new BagModel();
    @   for (int i=0; i<number; i++)
    @   {
    @     b = b.add(element[i], counter[i]);
    @   }
    @   return b;
    @ }
    @*/
  ```

  Annotate this definition with a *private* behavior specification that relates the constructed `BagModel` to the current `BoundedBag` object.
- Add the private object variables to the data group of the model variable; thus whenever an assignment on the model variable in the public specification is allowed, also an assignment to the private variables in the implementation is allowed.

First use `jml -Q` to type-check `BoundedBag.jml` in a directory that contains also the file `BagModel.java` but does not contain `BoundedBag.java` (otherwise also this file will be immediately type-checked). As soon as the type-check succeeds, also add the file `BoundedBag.java` from the previous exercise to this directory and extend it as indicated above. Now use `jml -Q` again to type-check the files.

The result of the exercise contains the files `BoundedBag.jml`, `BoundedBag.java`, and also `BagModel.java`, and the output of `jml -Q`.