Assignment 3: Proving Correctness in Dafny

CS 6110 – Formal Methods in System Design

March 8, 2015

Deadline: **Wednesday, Mar 25, 2015 at 11:59pm.**

The assignment consists of 5 problems (see attached Dafny sources). Your task for each problem is to prove its postcondition correct in Dafny. Apart from adding necessary annotations, do not change the source code of the assignment problems. Make sure to double-check that your preconditions are satisfiable, as we discussed in class. You do not have to prove termination. If needed, assume that input arrays are not empty.

Problem 1 [1 point]. Open `LinearSearch.dfy` in Dafny. Add preconditions and loop invariants needed to prove the postcondition and any default Dafny checks (e.g., array out of bounds). Do not change the postcondition.

Problem 2 [1 point]. Open `Abs.dfy` in Dafny. Add preconditions and loop invariants needed to prove the postcondition and any default Dafny checks (e.g., array out of bounds). Do not change the postcondition.

Problem 3 [1 point]. Open `BubbleSort.dfy` in Dafny. Add preconditions and loop invariants needed to prove the postcondition and any default Dafny checks (e.g., array out of bounds). Do not change the postcondition. This is a warm-up sorting problem since the solution is explained in great detail in the textbook (The Calculus of Computation). So you are encouraged to study the solution and read that part of the textbook. You can find a link to the free electronic version of the textbook on the course webpage.

Problem 4 [2 points]. Open `InsertionSort.dfy` in Dafny. Add preconditions and loop invariants needed to prove the postcondition and any default Dafny checks (e.g., array out of bounds). Do not change the postcondition.

Problem 5 [5 points]. Open `MergeSort.dfy` in Dafny. Add preconditions, postconditions, and loop invariants needed to prove the postcondition and any default Dafny checks (e.g., array out of bounds). Do not change the postcondition of method `MergeSort`. This is a somewhat open-ended problem since I still have not proved it myself in Dafny. I did prove it in a different verifier, and so I am confident that soon I will be able to prove it in Dafny too.

Assignment Deliverables. Email me your solutions in the form of (archived) Dafny files with missing annotations. No separate write-up is needed. Make sure you acknowledge collaboration with other students.