University of Massachusetts Lowell — Comp 3010: Organization of Programming Languages

Assignment 9

DUE: Sunday, Dec 8, 2024, 11:59PM

Collaboration Policy: You may collaborate with others but must submit work that is your own. Submissions of collaborators should be different and each submission must demonstrate your own work. Please refer to the collaboration policy on the course page in Blackboard.

Submission instructions: Please submit your homework via GradeScope. Some points to note:

- If you collaborate with your classmates, please note who they are when you submit your answers.
- **Submit your file with the name "min.dfy" in Gradescope.**

1 Minimal Element of an Array (50 points)

In this hw, you will verify the functions using Dafny. Use the following resources:

- `https://dafny.org/dafny/OnlineTutorial/guide` for invariants
- `https://dafny.org/latest/OnlineTutorial/ValueTypes` for sets, sequences and multisets.

Consider the signature of a Dafny method that finds the minimal element of the input array.

```
method find_min(a:array<int>) returns (m:int)
```

The above method returns the minimum element of the input array. **Note:** it does not return the index of the minimum value. If the input array is null, return 0. For example, if $a = [2, 6, 3]$, then $m = 2$.

Your job is to write pre- and post-conditions as well as verify the body of the method against the specification.

(a) Provide the pre- and post-conditions satisfying the following conditions.

   i. a could be NULL;

   ii. a may contain duplicates (e.g., $a = [1, 2, 2]$);

   iii. the value returned should be the minimum of all elements of the given array (e.g., if $a = [1, 2, 2]$ then $m \leq 1$ and $m \leq 2$).

(b) Complete the body of the `find_min` such that it verifies against the specification.

(c) Using comments, explain each pre- and post-condition in the specification as well as any of the invariants used.

2 Bonus Question (10 points)

In the above question, strengthen the post-condition to satisfy the following additional condition (i.e., in-addition to the ones already given):

(a) conditions i to iii in the above question, and

(b) the post-condition should not type check when the return value does not belong to the input array (e.g., if $a = [1, 2]$ then $m = 1$ or $m = 2$).

You will get a shout-out in the class if you have the solution for this question.