Assignment 1 — 2014

Theodore S. Norvell

6892 Due Oct 2 2014

Q0 [24] (Read all parts before attempting any.)

Suppose a is an array of numbers of length n, and x holds a number.

(a)[4] Write a contract (specification) for computing $\sum_{i \in \{0,..n\}} a(i) \times x^i$ into y.

(b)[4] Use the technique of replacing a constant by a variable to obtain an invariant.

(c)[4] Write a correct proof outline that solves the problem. (You may assume that computing x^i for any integer i is an operation in the programming language, although an expensive one.) Don't worry about efficiency at this point.

(d)[4] What is the variant?

(e)[4] Introduce a tracking variable to improve the efficiency of the algorithm. State the linking invariant that relates the new variable to the rest of the state.

(f)[4] Rewrite the proof outline from part (c) to use the tracking variable.

Q1 [16] (Read all parts before attempting any.)

(a)[4] Write a contract (specification) for computing the integer part of the square root of a natural number. (Integer part means floor, i.e., rounded down.)

(b)[4] Give a linking invariant that makes your specification equivalent to the specification

$$\{\neg A(m) \wedge A(n) \wedge m < n\} \ ? \ \{\neg A(p) \wedge A(p+1)\}$$

(c)[8] Use your linking invariant to derive a correct proof outline for the contract given in part (a) from the algorithm given in slide set 4 pages $\{5, .., 8\}$. Running time should roughly proportional to the number of bits required to represent the input. See slide set 5, for an exemplar.

I suggest doing this in three stages: first, introduce additional variables and the linking invariant; second, rewrite the algorithms so that A (at least) is no longer needed; third eliminate A and any other variables no longer needed.

Bonus [5]. Extend the solution from Q1 to find an outline that uses no multiplications.