Assignment 0

Theodore S. Norvell

6892 Due 2016 Oct 4th.

Q0 Square root.

(a) [10] List all the conditions that must be shown to be universally true in order to show that the following proof outline is partially correct. Assume all state variables hold integers

$\{n \geq 0\}$
$p := 0$
$r := n + 1$
$\left\{0 \leq p < r \leq n + 1 \wedge p^2 \leq n < r^2\right\}$
while $p + 1 \neq r$ do
  $q := \left\lfloor \frac{p+r}{2} \right\rfloor$
  $\left\{0 \leq p < q < r \leq n + 1 \wedge p^2 \leq n < r^2\right\}$
  if $q * q \leq n$ then
    $p := q$
  else
    $r := q$
  end if
end while
$\{p \leq \sqrt{n} < p + 1\}$

(b) [5] Propose a variant for the loop. Explain what must be shown about the variant.

Q1 Sorting

(a) [10] We want to sort the items of an array. Write out a precondition and a postcondition that specify this problem. (Hint: you may want to define some predicates.)

(b) [5] Consider the selection sort algorithm, which works by repeatedly selecting the smallest item in the right part of an array, moving it to the left end of that part and then moving the boundary between the left part and the right part to the right.

Design and draw a picture of the invariant for this algorithm.

(c) [10] Write out the invariant as a mathematical statement.

(d) [10] Write a proof outline for the algorithm. Be sure to state an invariant and a variant for all loops.

Q2

Define the function $c : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ as follows

$$\begin{aligned} c(n, 0) &= 1, \text{ for all } n \in \mathbb{N} \\ c(n, n) &= 1, \text{ for all } n \in \mathbb{N} \\ c(n, r) &= c(n-1, r-1) + c(n-1, r), \text{ for all } r, n \in \mathbb{N} \text{ such that } 0 < r < n \end{aligned}$$

In the algorithm below, m is a matrix of size at least $n+1$ by $n+1$.

$\{r \leq n\}$
$i := 0$
$j := 0$
$m(0,0) := 1$
$\{I\}$
while $i < n \vee j < r$ do
    if $j = i$ then
        $i := i + 1$
        $j := 0$
        $m(i,j) := 1$
    else
        $j := j + 1$
        if $i = j$ then
            $m(i,j) := 1$
        else
            $m(i,j) := m(i-1, j-1) + m(i-1, j)$
        end if
    end if
end while
$\{m(n,r) = c(n,r)\}$

(a) [10] State an invariant that could be used to verify this algorithm.

(b) [5] An optimization is to only fill in the matrix up to and including column r. How would the invariant change? How would the algorithm change?