CSC240 Winter 2024 Quiz 7

due March 15, 2024

Consider the following algorithm DIV that, given positive integers a and b, computes the quotient q and remainder r of a divided by b:

```
DIV(a, b):
1   p ← 1
2   s ← b
3   while s ≤ a do
4         s ← 2 × s
5         p ← 2 × p
6   q ← 0
7   r ← a
8   while s ≠ b do
9         s ← s div 2
10        p ← p div 2
11        if r ≥ s then
12          r ← r − s
13          q ← q + p
```

1. Write a precise statement of what it means for this algorithm to be correct.

   Solution.

   The algorithm is correct (totally correct) if it is both partially correct and terminates.

   Precondition: a and b are positive integers.

   Postcondition: q and r are integers such that $a = qb + r$ and $0 \leq r < b$. Also, a and b are not changed.

   Moreover, for the algorithm to be partially correct, we need the postcondition to be true whenever the algorithm terminates.

2. Write a loop invariant for both while loops that relates s and p. You do not have to prove that it is a loop invariant.

   Solution.

   Loop Invariant for both while loops: $s = p \times b$.

3. Prove that $a = qb + r$ is a loop invariant for the second while loop. **Solution.**

   Proof. Initially from lines 6 and 7 we can see that $a = 0 \times b + a = q \times b + r$, the loop invariant holds.

   Consider an arbitrary iteration of the loop,

Let q', r' be the values of q and r at the beginning of the iteration, and let q'', r'' be the values of q and r at the end of the iteration.

Suppose the invairant is true at the beginning of the iteration, on line 12 and 13, since by question 2 we have $s = p \times b$, substitute $p \times b$ into line 12's s and we will see that $r'' = r' - p \times b$ and on line 13 $q'' = q' + p$.

Combine together we have $q''b + r'' = (q' + p)b + (r' - p \times b) = q'b + r' = a$, the loop invariant holds.

Therefore by induction we have that $a = qb + r$ is a loop invariant for the second while loop.

□