Exercise Set 5.5

Exercises 1–5 contain a while loop and a predicate. In each case show that if the predicate is true before entry to the loop, then it is also true after exit from the loop.

1. loop: **while** ($m \geq 0$ and $m \leq 100$)

   $m := m + 1$

   $n := n - 1$

   end while

   predicate: $m + n = 100$

2. loop: **while** ($m \geq 0$ and $m \leq 100$)

   $m := m + 4$

   $n := n - 2$

   end while

   predicate: $m + n$ is odd

3. loop: **while** ($m \geq 0$ and $m \leq 100$)

   $m := 3 \cdot m$

   $n := 5 \cdot n$

   end while

   predicate: $m^3 > n^2$

4. loop: **while** ($n \geq 0$ and $n \leq 100$)

   $n := n + 1$

   end while

   predicate: $2^n < (n + 2)!$

5. loop: **while** ($n \geq 3$ and $n \leq 100$)

   $n := n + 1$

   end while

   predicate: $2n + 1 \leq 2^n$

Exercises 6–9 each contain a while loop annotated with a pre- and a post-condition and also a loop invariant. In each case, use the loop invariant theorem to prove the correctness of the loop with respect to the pre- and post-conditions.

6. *[Pre-condition: m is a nonnegative integer, x is a real number, $i = 0$, and exp = 1.]*

   while ($i \neq m$)

   1. $exp := exp \cdot x$
   2. $i := i + 1$

   end while

   [Post-condition: $exp = x^m$]
   loop invariant: $I(n)$ is "exp $= x^n$ and $i = n$."

7. *[Pre-condition: largest $= A[1]$ and $i = 1$]*

   while ($i \neq m$)

   1. $i := i + 1$
   2. **if** $A[i] >$ largest **then** largest $:= A[i]$

   end while

   [Post-condition: largest = maximum value of $A[1], A[2], \ldots, A[m]$]

loop invariant: $I(n)$ is "largest = maximum value of $A[1], A[2], \ldots, A[n+1]$ and $i = n+1$."

8. *[Pre-condition: sum = A[1] and i = 1]*

while $(i \neq m)$
  1. $i := i + 1$
  2. sum: = sum + A[i]
end while

[Post-condition: sum = $A[1] + A[2] + \cdots + A[m]$]

loop invariant: $I(n)$ is "$i = n+1$ and $sum = A[1] + A[2] + \cdots + A[n+1]$."

9. *[Pre-condition: a = A and A is a positive integer.]*

while $(a > 0)$
  1. $a := a - 2$
end while

[Post-condition: $a = 0$ if A is even and $a = -1$ if A is odd.]
loop invariant: $I(n)$ is "Both a and A are even integers or both are odd integers and $a \geq -1$."

***H* ✶ 10.** Prove correctness of the **while** loop of Algorithm 4.8.3 (in exercise 24 of Exercise Set 4.8) with respect to the following pre- and post-conditions:

Pre-condition: A and B are positive integers, $a = A$, and $b = B$.

Post-condition: One of a or b is zero and the other is nonzero. Whichever is nonzero equals $\gcd(A, B)$.

Use the loop invariant

$I(n)$ "(1) a and b are nonnegative integers with $\gcd(a, b) = \gcd(A, B)$.
(2) at most one of a and b equals 0,
(3) $0 \leq a + b \leq A + B - n$."

11. The following **while** loop implements a way to multiply two numbers that was developed by the ancient Egyptians.

[Pre-condition: A and B are positive integers, $x = A$, $y = B$, and product = 0.]

while $(y \neq 0)$
  $r := y \ mod \ 2$
  if $r = 0$
    then do $x := 2 \cdot x$
      $y := y \ div \ 2$
    end do
  if $r = 1$
    then do $product := product + x$
      $y := y - 1$
    end do
end while

[Post-condition: product = $A \cdot B$]

Prove the correctness of this loop with respect to its pre- and post-conditions by using the loop invariant

$$I(n): \text{"}xy + product = A \cdot B\text{."}$$

✶ 12. The following sentence could be added to the loop invariant for the Euclidean algorithm:

There exist integers u, v, s, and t such that
$a = uA + vB$ and $b = sA + tB$. 5.5.12

a. Show that this sentence is a loop invariant for

while $(b \neq 0)$
  $r := a \ mod \ b$
  $a := b$
  $b := r$
end while

b. Show that if initially $a = A$ and $b = B$, then sentence (5.5.12) is true before the first iteration of the loop.

c. Explain how the correctness proof for the Euclidean algorithm together with the results of (a) and (b) above allow you to conclude that given any integers A and B with $A > B \geq 0$, there exist integers u and v so that $\gcd(A, B) = uA + vB$.

d. By actually calculating u, v, s, and t at each stage of execution of the Euclidean algorithm, find integers u and v so that $\gcd(330, 156) = 330u + 156v$.