Correctness of While Loops

Correctness of While loops

Example

1. $z \leftarrow 0$
2. $w \leftarrow y$
3. while $w \neq 0$ do
4. $\quad z \leftarrow z + x$
5. $\quad w \leftarrow w - 1$

Values at variables immediately after ith iteration of the loop: $w = y - i, z = xi$
Convention: immediately after iteration 0 means immediately before the first iteration

Method1
Let $P(i) =$ if the while loop is executed at least i times, then immediately after the ith iteration, $w = y - i$ and $z = xi$

Lemma1 Let $x, y \in \mathbb{Z}^+. \forall i \in \mathbb{N}. P(i)$
Proof Let w_i and z_i denote the value of w, z immediately after the ith iteration
Initially, $w_0 = y = y - 0, z_0 = x = x_0$ from line 1 and 2
$P(0)$
Let $i \geq 0$ and assume $P(i)$, then $w_i = y - i$ and $z_i = xi$
From line 4 and 5, $z_{i+1} = z_i + x = xi + x = x(i + 1), w_{i+1} = w_i - 1 = y - (i + 1)$
$P(n)$ IMPLIES $P(n + 1)$

Corollary2 Let $x, y \in \mathbb{Z}$ If the algorithm runs and halts, then when it halts $z = xy$
Proof Suppose the loop halts immediately after ith iteration, from the termination condition of the loop in line 3, $w_i = 0$. From lemma1, $w_i = y - i = 0, i = y$ and $z_i = xy$

Definition A loop invariant is a predicate about the program variables that is true each time a particular place in the loop is reached. Often, we consider the beginning or the end of the loop.

Method2
Because $w = y - i$ and $z = xi$, it implies $z = x(y - w), z = xy$ which only involves program variables

Lemma3 $z = x(y - w)$ is the loop invariant
Proof initially, from line 1, known $w = y, z = x(y - w) = x0 = 0$
Consider an arbitrary iteration of the loop, let w' and z' denote the value of w and z at the beginning of the iteration, let w'' and z'' be the value at the end of the iteration.
Suppose the claim is true at the beginning of the iteration, i.e. $z' = x(y - w')$
From line 4 and 5, $w'' = w' + 1, \ z'' = z' + x = x(y - w') + x = x(y - (w' - 1)) = x(y - w'')$
Thus the claim is true at the end of the iteration
By induction, $z = x(y - w)$ after every iteration.

Corollary4
Proof From the termination condition in line3, $w = 0$.
By lemma, $z = x(y - 0) = xy$

Termination: show the loop terminates is the same as show some quantity in natural numbers decreases each time through the loop.
Lemma if $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ and the algorithm is ran, it eventually halts
Discussion w is initialized as $y \in \mathbb{N}$, each iteration of the loop w is decreased by 1, so it's a smaller natural number.
Iteration eventually reaches 0, this is the exist condition of the loop, hence the loop and the algorithm estimates

Proof To obtain a contradiction, suppose loop doesn't terminate
Let w_i be the value of w immediately after ith iteration, each iteration at the loop w is decreasing by 1, so $w_{i+1} < w_i$. Since the loop doesn't terminate, $w_i \neq 0$.
Thus, if $w_i \in \mathbb{N}, w_{i+1} \in \mathbb{N}$,
Since $w_0 = y \in \mathbb{N}$, it follows by induction of $w_0, w_1, \ldots$ is a sequence of natural number.
By the well ordering principle, the set of sequence has a smallest element.
But $w + 1 < w_i$, this contradicts with the definition of w, thus the loop terminates