Appendix to Chapter 2 of [Manber]: Proving a Loop Invariant

Consider the following variant of Euclid's algorithm for computing the greatest common divisor of two positive integers.

Algorithm myEuclid (m, n);
begin
    // assume that $m > 0 \wedge n > 0$
    $x := m$;
    $y := n$;
    while $x \neq 0 \wedge y \neq 0$ **do**
        if $x < y$ **then** swap(x,y);
        $x := x - y$;
    od
    ...
end

where swap(x,y) exchanges the values of x and y.

Let $Inv(m, n, x, y)$ denote the assertion:

$$x \geq 0 \wedge y \geq 0 \wedge (x \neq 0 \vee y \neq 0) \wedge \gcd(x, y) = \gcd(m, n).$$

(Note: by convention, $\gcd(0, z) = \gcd(z, 0) = z$ for $z > 0$.)

Claim: $Inv(m, n, x, y)$ is a loop invariant of the while loop, assuming that $m, n > 0$. (The invariant is sufficient to deduce that, when the while loop terminates, x or y whichever is nonzero stores the value of $\gcd(m, n)$.)

Proof: The proof is by induction on the number of times the loop body is executed. More specifically, we show that (1) the assertion is true when the flow of control reaches the loop for the first time and (2) given that the assertion is true and the loop condition holds, the assertion will remain true after the next iteration (i.e., after the loop body is executed once more).

(1) When the flow of control reaches the loop for the first time, $x = m$ and $y = n$, with $m > 0$ and $n > 0$. Obviously, $x \geq 0$, $y \geq 0$, $x \neq 0 \vee y \neq 0$, and $\gcd(x, y) = \gcd(m, n)$ and therefore the assertion $Inv(m, n, x, y)$ holds.

(2) Assume that $Inv(m, n, x, y)$ is true at the start of the next iteration and the loop condition $(x \neq 0 \wedge y \neq 0)$ holds. We need to show that $Inv(m', n', x', y')$ also holds, where m', n', x', and y' denote respectively the new values of m, n, x, and y after the next iteration of the while loop

(m, n, x, and y themselves denote the current values of these variables at the start of the next iteration).

From the loop body, we deduce the following relationship (assuming that the loop condition holds):

$$\begin{array}{ll} & ((x < y) \rightarrow (x' = y - x) \wedge (y' = x)) \\ \wedge & ((x \geq y) \rightarrow (x' = x - y) \wedge (y' = y)) \\ \wedge & m' = m \\ \wedge & n' = n \end{array}$$

There are two cases to consider: when $x < y$ and when $x \geq y$. We prove the first case; the second case can be proven similarly.

Suppose $x < y$. $x' = y - x > 0$ and hence $x' \geq 0$; also, $y' = x \geq 0$ (from the induction hypothesis). These also imply that $x' \neq 0 \vee y' \neq 0$. $\gcd(x', y') = \gcd(y - x, x) = \gcd(y, x) = \gcd(x, y)$, which from the induction hypothesis equals $\gcd(m, n) = \gcd(m', n')$, and therefore $\gcd(x', y') = \gcd(m', n')$. Therefore, $Inv(m', n', x', y')$ holds and this concludes the proof.