Theorem: Loop Invariant Theorem

Let a **while** loop with guard G be given, together with pre- and post-conditions that are predicates in the algorithm variables. Also let a predicate $I(n)$, called the **loop invariant**, be given. If the following four properties are true, then the loop is correct with respect to its pre- and post-conditions.

I. **Basis Property**: The pre-condition for the loop implies that $I(0)$ is true before the first iteration of the loop.

II. **Inductive Property**: For all integers $k \geq 0$, if the guard G and the loop invariant $I(k)$ are both true before an iteration of the loop, then $I(k + 1)$ is true after iteration of loop.

III. Eventual Falsity of Guard: After a finite number of iterations of the loop, the guard G becomes false.

IV. **Correctness of the Post-Condition**: If N is the least number of iterations after which G is false and $I(N)$ is true, then the values of the algorithm variables will be specified in the post-condition of the loop.

Proof

The loop invariant theorem follows easily from the principle of mathematical induction. Assume that $I(n)$ is a predicate that satisfies properties $I - IV$ of the loop invariant theorem. Properties I and II are the basis and inductive steps needed to prove the truth of the following statement:

<div align="center">

For all integers $n \geq 0$, if the **while** loop

iterates n times, then $I(n)$ is true.

</div>

Thus, by the principle of mathematical induction, since both I and II are true, the statement is also true.

Property III says that the guard G eventually becomes false. At that point the loop will have been iterated some number, say N, of times. Since $I(n)$ is true after the nth iteration for every $n \geq 0$, then $I(n)$ is true after the Nth iteration. That is, after the Nth iteration the guard is false and $I(N)$ is true. But this is the hypothesis of property IV, which is a if-then statement. Since statement IV is true (assumption) and its hypothesis is true (by the argument just given), it follows (by modus ponens) that its conclusion is also true. That is, the values of all algorithm variables after execution of the loop are as specified in the post-condition for the loop.