Correctness of loops (method of loop invariants)

```
while (G) {
    // body
    // can't jump out early
}
```
Loop invariant

- Predicate over the set of integers

1. true before the first iteration $P(0)$

2. For each iteration, if it is true before, then it is true after.

3. If the loop finishes after finite steps, then the truth of the invariant ensures the truth of the post-cond.
Given: a while loop
a guard $G$
an invariant $I(n)$

If the following are true,
then the loop is correct

I. Basis $I(o)$ is true

II. Induction
\[ \forall k \geq 0, k \in \mathbb{Z} \]
if $G \land I(k)$ then $I(k+1)$

III. Eventual falsity of $G$

IV. Correctness of the post condition
product \ m \cdot x

Pre-cond: \ m \text{ is a non-\text{neg} int,}
\ x \text{ is real, } i = 0 \text{ and}
\ product = 0

\text{while ( } i \neq m \text{)}
\hspace{1cm} \text{product} := \text{product} + x
\hspace{1cm} i := i + 1
\hspace{1cm} \text{end while}

Postcondition: \ product = m \cdot x

Loop invariant: \ I(n): \ i = n
\hspace{1cm} \text{and product} = n \cdot x
I. Basis I(0)

Show $i = 0$ and product = 0·X
true from precondition.

II. Induction: if $I(k) \land G$ then $I(k+1)$

Suppose $I(k)$ and $G$ are true
for some $k$, prior to an
iteration of the loop

Show $I(k+1)$ is true after that
iteration.

$I(k)$ is true so $i = k$
and product = $k \cdot X$

$G$ is true so $i \neq m$

Since $G$ is true, statement 1
is executed.

product_new = product_old + X
and product_old = $k \cdot X$

so $product\_new = k \cdot X + X$
sub. ind. hyp

$= (k+1) \cdot X$

Also stat. 2 is executed
so $i\_new = i\_old + 1$

and $i\_old = k$

so $i\_new = k + 1$

So $I(k+1)$ is true.
III  Eventual falsity of the Guard.

\[ G : \ i \neq m \]

\[ m \] is a non-neg. int

from I and II

for all \( n \geq 0 \) if the loop

is iterated \( n \) times \( \text{then} \)

\[ i = n \text{ and product} = n \cdot x \]

So after \( m \) iterations \( i = m \).

So \( G \) is false

IV  Correctness of the post condition

post-cond: \( \text{product} = m \cdot x \)

after execution of the loop

\( G \) is false after \( m \) iterations

(from III)

and \( I(m) \) was true

so \( \text{product} = m \cdot x \)

\( \text{QED} \)
<table>
<thead>
<tr>
<th>Pre-cond</th>
<th>i = 0</th>
<th>product = 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>I(0)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>I(1)</td>
<td>1</td>
<td>X</td>
</tr>
<tr>
<td>I(2)</td>
<td>2</td>
<td>2.X</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I(m)</td>
<td>m</td>
<td>m.X</td>
</tr>
</tbody>
</table>

Post-cond