Proof of Correctness:

A Simple Example

- Problem: Store in s the sum of array $b[0..10]$
- Program

```
i := 1;
s := b[0];
while (i < 11)
    s := s + b[i];
    i := i + 1;
end-while
```

Establish Pre- and Post-Conditions

pre: true

```
i := 1;
s := b[0];
while (i < 11)
    s := s + b[i];
    i := i + 1;
end-while
```

post: $s = \sum_{k=0}^{10} b[k]$

Loop Invariant

- A constant (unchanging) predicate (constraint or fact)
- Unaffected by the group of mathematical operations under consideration
- In the programming context, an operation is an iteration of the loop

Establishing a Loop Invariant

- Define a predicate I that shows the logical relationship between i, s, and b:

  $$I\colon\ 1 \leq i \leq 11 \wedge s = \sum_{k=0}^{i-1} b[k]$$

- Show that I is true before the loop and after each iteration of the loop (so that it is true upon completion)

- If I is true in all these places, with the falsity of the guard, we can show that the program post-condition holds

Another way of saying this ...

pre: true

```
i := 1;
s := b[0];
```

I

```
while (i < 11)
    s := s + b[i];
    i := i + 1;
```

I

```
end-while
```

$i \geq 11 \wedge I \Rightarrow$ post: $s = \sum_{k=0}^{10} b[k]$

Reasoning Steps

1. Show that I is true before the loop
2. Show that each iteration of the loop leaves I true
   - I is true before and after each iteration of the loop and upon termination
3. Show that the truth of I and the falsity of the guard (i.e., $i \geq 11$) imply the post-condition

Show I is True Before the Loop

- Before the loop, we have:

```
i := 1; s := b[0];
```

- Do these affect the loop invariant I?

$$1 \leq i \leq 11 \wedge s = \sum_{k=0}^{i-1} b[k]$$

$$\equiv$$

$$1 \leq 1 \leq 11 \wedge b[0] = \sum_{k=0}^{1-1} b[k]$$

$$\equiv$$

$$\text{true} \wedge b[0] = \sum_{k=0}^{0} b[k]$$

$$\equiv$$

$$\text{true} \wedge b[0] = b[0] \equiv \text{true}$$

Show I is True After Each Loop Iteration

- Inside loop we have

```
s = s + b[i]
i := i + 1
```

- Do these affect the loop invariant I?

$$1 \leq i \leq 11 \wedge s = \sum_{k=0}^{i-1} b[k]$$

Substitute new values for i and s

Show I is True After Each Loop Iteration (continued)

$$1 \leq i+1 \leq 11 \wedge s + b[i] = \sum_{k=0}^{(i+1)-1} b[k]$$

$$\equiv$$

$$0 \leq i < 11 \wedge s + b[i] = \sum_{k=0}^{i} b[k]$$

$$\equiv$$

$$0 \leq i < 11 \wedge s + b[i] = (\sum_{k=0}^{i-1} b[k] + b[i])$$

$$\equiv 0 \leq i < 11 \wedge s = \sum_{k=0}^{i-1} b[k]$$

Upon Loop Termination

- $I \wedge i \geq 11 \Rightarrow$ post-condition?
- We know $i = 11$, thus

  $$1 \leq 11 \leq 11 \wedge s = \sum_{k=0}^{11-1} b[k]$$

  $$\equiv$$

  $$\text{true} \wedge s = \sum_{k=0}^{10} b[k]$$