Total Correctness

Total Correctness =
Partial Correctness + Termination

Termination must be proved only
for "while" loops

Often proof of termination is easier
but not always!

A FAMOUS EXAMPLE

```
{x >= 1}
while (x>1) {
    if (x%2 == 0)
        x = x/2;
    else
        x = 3*x+1;
}
{x = 1}
```

Partial Correctness: trivial! Termination???

Total Correctness for loops

We need to prove that the loop will terminate. To do so we should find a variant function `v` such that:

- `v` is an upper bound on the number of loops
- Initially `v` evaluates to a positive finite integer

$$\{Inv \wedge C\} \Rightarrow v > 0$$

- The value of the variant function decreases each time the loop executes (here V is a constant)

$$\{ Inv \wedge C \wedge v=V \} \text{ loop } \{v < V\}$$

Loop exit is guarenteed since sooner or later v becomes $\leq 0 \Rightarrow C$ must be false!

Guessing v

- `v=(N-i)` if loop always adds a constant to i.
- `v=(i)` if loop subtracts a constant from i.
  - `v` $\leq$ `0` at loop exit
- Other loops
  - Find an expression that is an upper bound on the number of iterations left in the loop.

EXERCISES OF SESSION ONE

Ex.1

- Square root of a positive integer.

```
{x > 0}
if (x == 1) sqrt := 1
else
      i:=1;
      z:=1;
      while ( z ≤ x )
            i++;
            z:=i*i;
      sqrt := i-1;
{sqrt²≤ x < (sqrt + 1)² }
```

Ex.1

- Termination proof obligations:

1. Choose a variant `v`.
2. Show that it is initially positive:

    `{Inv ∧ C} => v > 0`

3. Show that it is decreasing:

    `{Inv ∧ C ∧ "v"} S {Inv ∧ "v'"}`

    `v' < v`

$v(\cdot) = v$ $\qquad\qquad$ $v(\cdot) = v'$

Ex.1

- Termination proof obligations:

1. Choose a variant $\mathtt{v}$.

Ex.1

- Termination proof obligations:

1. Choose a variant v.

```
while ( z ≤ x )
            i++;
            z:=i*i;
```

Ex.1

- Termination proof obligations:

1. Choose a variant v.

```
while ( z ≤ x )
            i++;
            z:=i*i;
```

$$v(x, i) = x - (i-1)^2$$

Ex.1

- Termination proof obligations:

2. Show that it is initially positive:

```
{Inv ∧ C} => v > 0
```

Ex.1

- Termination proof obligations:

2. Show that it is initially positive:

$$\{Inv \wedge C\} \Rightarrow v > 0$$

$Inv = \{z = i^2 \wedge (i-1)^2 \leq x\}$

$C = \{z \leq x\}$

$\{z = i^2 \wedge (i-1)^2 \leq x \wedge z \leq x\} \Rightarrow \{x - (i-1)^2 > 0\}$

Ex.1

- Termination proof obligations:

2. Show that it is initially positive:

$$\{Inv \wedge C\} \Rightarrow v > 0$$

$Inv = \{z = i^2 \wedge (i-1)^2 \leq x\}$

$C = \{z \leq x\}$

$\{z = i^2 \wedge (i-1)^2 \leq x \wedge z \leq x\} \Rightarrow \{x - (i-1)^2 > 0\}$

$\{(i-1)^2 \leq x \wedge i^2 \leq x\} \Rightarrow \{x > (i-1)^2\}$

Ex.1

- Termination proof obligations:

2. Show that it is initially positive:

$$\{Inv \wedge C\} \Rightarrow v > 0$$

$Inv = \{z = i^2 \wedge (i-1)^2 \le x\}$

$C = \{z \le x\}$

$\{z = i^2 \wedge (i-1)^2 \le x \wedge z \le x\} \Rightarrow \{x - (i-1)^2 > 0\}$

$\{(i-1)^2 \le x \wedge i^2 \le x\} \Rightarrow \{x > (i-1)^2\}$

$\{i^2 \le x\} \Rightarrow \{x > (i-1)^2\}$

Ex.1

- Termination proof obligations:

3. Show that it is decreasing:

$$\{\texttt{Inv} \wedge \texttt{C} \wedge \texttt{v}\}\ \texttt{i++;z:=i*i;}\{\texttt{Inv} \wedge \texttt{v}_{\texttt{new}}\}$$

$$\texttt{v}_{\texttt{new}} < \texttt{v}$$

Ex.1

- Termination proof obligations:

3. Show that it is decreasing:

$$\{Inv \land C \land v\}\ i{+}{+};z{:=}i{*}i;\{Inv \land v_{new}\}$$

$$v_{new} < v$$

$\{z = i^2 \land (i-1)^2 \leq x \land z \leq x \ \land v\}\ i{+}{+};z{:=}i{*}i;\ \{z = i^2 \land (i-1)^2 \leq x \land v_{new}\}$

Ex.1

- Termination proof obligations:

3. Show that it is decreasing:

$$\{Inv \wedge C \wedge v\}\ i{+}{+};z{:=}i*i;\{Inv \wedge v_{new}\}$$

$$v_{new} < v$$

$\{z = i^2 \wedge (i-1)^2 \leq x \wedge z \leq x \wedge v\}$ `i++;z:=i*i;` $\{z = i^2 \wedge (i-1)^2 \leq x \wedge v_{new}\}$

$v \rightarrow v(x_{old}, i_{old}) = x_{old} - (i_{old}-1)^2$

$v_{new} \rightarrow v(x_{new}, i_{new}) = x_{new} - (i_{new}-1)^2$

Ex.1

- Termination proof obligations:

3. Show that it is decreasing:

$$\{Inv \wedge C \wedge v\}\ i{+}{+};z{:=}i{*}i;\{Inv \wedge v_{new}\}$$

$$v_{new} < v$$

$\{z = i^2 \wedge (i-1)^2 \leq x \wedge z \leq x \wedge v\}\ i{+}{+};z{:=}i{*}i;\ \{z = i^2 \wedge (i-1)^2 \leq x \wedge v_{new}\}$

$v \to v(x_{old}\ ,\ i_{old}) = x_{old} - (i_{old}-1)^2$

$v_{new} \to v(x_{new}\ ,\ i_{new}) = x_{old} - (i_{old}+1-1)^2$

Ex.1

- Termination proof obligations:

3. Show that it is decreasing:

$$\{Inv \wedge C \wedge v\}\ i{+}{+};z:=i*i;\{Inv \wedge v_{new}\}$$

$$v_{new} < v$$

$\{z = i^2 \wedge (i-1)^2 \leq x \wedge z \leq x \wedge v\}$ `i++;z:=i*i;` $\{z = i^2 \wedge (i-1)^2 \leq x \wedge v_{new}\}$

$v \rightarrow v(x_{old}, i_{old}) = x_{old} - (i_{old}-1)^2$

$v_{new} \rightarrow v(x_{new}, i_{new}) = x_{old} - (i_{old})^2$

Ex.1

- Termination proof obligations:

3. Show that it is decreasing:

$$\{Inv \wedge C \wedge v\}\ i{+}{+};z{:=}i{*}i;\{Inv \wedge v_{new}\}$$

$$v_{new} < v$$

$\{z = i^2 \wedge (i-1)^2 \le x \wedge z \le x \wedge v\}$ i++;z:=i*i; $\{z = i^2 \wedge (i-1)^2 \le x \wedge v_{new}\}$

$v \to v(x_{old}, i_{old}) = x_{old} - (i_{old}-1)^2$

$v_{new} \to v(x_{new}, i_{new}) = x_{old} - (i_{old})^2$

We already know that $x_{old} - (i_{old}-1)^2 > 0$

Ex.1

- Termination proof obligations:

3. Show that it is decreasing:

$$\{Inv \wedge C \wedge v\}\ i{+}{+};z:=i*i;\{Inv \wedge v_{new}\}$$

$$v_{new} < v$$

$\{z = i^2 \wedge (i-1)^2 \le x \wedge z \le x \wedge v\}\ i{+}{+};z:=i*i;\ \{z = i^2 \wedge (i-1)^2 \le x \wedge v_{new}\}$

$$\left.\begin{array}{l} v \rightarrow v(x_{old}, i_{old}) = x_{old} - (i_{old}-1)^2 \\ v_{new} \rightarrow v(x_{new}, i_{new}) = x_{old} - (i_{old})^2 \\ \text{We already know that } x_{old} - (i_{old}-1)^2 > 0 \end{array}\right\}$$

Ex.1

- Termination proof obligations:

3. Show that it is decreasing:

$$\{\texttt{Inv} \wedge \texttt{C} \wedge \texttt{v}\}\ \texttt{i++;z:=i*i;}\{\texttt{Inv} \wedge \texttt{v}_{\texttt{new}}\}$$

$$\texttt{v}_{\texttt{new}} < \texttt{v}$$

$\{z = i^2 \wedge (i-1)^2 \le x \wedge z \le x \wedge v\}$ `i++;z:=i*i;` $\{z = i^2 \wedge (i-1)^2 \le x \wedge v_{new}\}$

$$\left.\begin{array}{l} v \to v(x_{old}\ ,\ i_{old}) = x_{old} - (i_{old}-1)^2 \\ v_{new} \to v(x_{new}\ ,\ i_{new}) = x_{old} - (i_{old})^2 \\ \text{We already know that } x_{old} - (i_{old}-1)^2 > 0 \end{array}\right\}\quad v_{new} < v$$

Ex.2

- Least common multiple of two positive integers.

```
{x,y > 0}
Z := 1
While (z % x != 0 ∨ z % y != 0 )
      z ++;
{z%x=0 ∧ z%y=0 ∧ ∀i(1≤i<z =>i%x!=0 ∨ i%y!=0)}
```

Ex.2

- Termination proof obligations:

1. Choose a variant v.

Ex.2

- Termination proof obligations:

1. Choose a variant v.

```
While (z % x != 0 ∨ z % y != 0 )
      z ++;
```

Ex.2

- Termination proof obligations:

1. Choose a variant `v`.

```
While (z % x != 0 ∨ z % y != 0 )
     z ++;
```

```
v(x , y , z) = xy - z
```

Ex.2

- Termination proof obligations:

2. Show that it is initially positive:

$$\{Inv \wedge C\} \Rightarrow v > 0$$

Ex.2

- Termination proof obligations:

2. Show that it is initially positive:

$$\{Inv \wedge C\} \Rightarrow v > 0$$

```
Inv = {∀i(1≤i<z =>i%x!=0 ∨ i%y!=0)}
C = {z % x != 0 ∨ z % y != 0 }
v(x , y , z) = xy - z
```

Ex.2

- Termination proof obligations:

2. Show that it is initially positive:

$$\{Inv \wedge C\} \Rightarrow v > 0$$

```
Inv = {∀i(1≤i<z =>i%x!=0 ∨ i%y!=0)}
C = {z % x != 0 ∨ z % y != 0 }
v(x , y , z) = xy - z
```

```
{∀i(1≤i<z =>i%x!=0 ∨ i%y!=0) ∧ z % x != 0 ∨ z % y !=
0} => {xy – z > 0}
```

Ex.2

- Termination proof obligations:

2. Show that it is initially positive:

$$\{Inv \wedge C\} \Rightarrow v > 0$$

```
Inv = {∀i(1≤i<z =>i%x!=0 ∨ i%y!=0)}
C = {z % x != 0 ∨ z % y != 0 }
v(x , y , z) = xy - z
```

```
{∀i(1≤i≤z =>i%x!=0 ∨ i%y!=0)} => {xy – z > 0}
```

Ex.2

- Termination proof obligations:

2. Show that it is initially positive:

$$\{Inv \land C\} \Rightarrow v > 0$$

Inv = {∀i(1≤i<z =>i%x!=0 ∨ i%y!=0)}

C = {z % x != 0 ∨ z % y != 0 }

v(x , y , z) = xy - z

$$\{\forall i(1 \le i \le z \Rightarrow \underbrace{i\%x!=0}_{i \neq x} \lor \underbrace{i\%y!=0}_{i \neq y})\} \Rightarrow \{xy - z > 0\}$$

Ex.2

- Termination proof obligations:

2. Show that it is initially positive:

$$\{Inv \wedge C\} \Rightarrow v > 0$$

$Inv = \{\forall i(1 \le i < z \Rightarrow i\%x != 0 \vee i\%y != 0)\}$

$C = \{z \% x != 0 \vee z \% y != 0\}$

$v(x, y, z) = xy - z$

$$\{\forall i(1 \le i \le z \Rightarrow \underbrace{i\%x != 0}_{i < x} \vee \underbrace{i\%y != 0}_{i < y})\} \Rightarrow \{xy - z > 0\}$$

Ex.2

- Termination proof obligations:

2. Show that it is initially positive:

```
{Inv ∧ C} => v > 0
```

```
Inv = {∀i(1≤i<z =>i%x!=0 ∨ i%y!=0)}
C = {z % x != 0 ∨ z % y != 0 }
v(x , y , z) = xy - z
```

```
{∀i(1≤i≤z =>i%x!=0 ∨ i%y!=0)} => {xy – z > 0}
```

```
i < xy
```

Ex.2

- Termination proof obligations:

2. Show that it is initially positive:

$$\{Inv \land C\} \Rightarrow v > 0$$

Inv = $\{\forall i(1 \le i < z \Rightarrow i\%x != 0 \lor i\%y != 0)\}$

C = $\{z \% x != 0 \lor z \% y != 0\}$

$v(x, y, z) = xy - z$

$$\{\forall i(1 \le i \le z \Rightarrow i\%x != 0 \lor i\%y != 0)\} \Rightarrow \{xy - z > 0\}$$

$i = z \Rightarrow z < xy$

Ex.2

- Termination proof obligations:

3. Show that it is decreasing:

$$\{\mathtt{Inv} \wedge \mathtt{C} \wedge \mathtt{v}\}\ \mathtt{z\ ++;}\ \{\mathtt{Inv} \wedge \mathtt{v}_{\mathtt{new}}\}$$

$$\mathtt{v}_{\mathtt{new}} < \mathtt{v}$$

Ex.2

- Termination proof obligations:

3. Show that it is decreasing:

$$\{Inv \wedge C \wedge v\}\ z\ {+}{+};\ \{Inv \wedge v_{new}\}$$

$$v_{new} < v$$

$\{\forall i(1 \le i < z \Rightarrow i\%x != 0 \vee i\%y != 0) \wedge z \% x != 0 \vee z \% y != 0\}\ z\ {+}{+};\ \{\forall i(1 \le i < z \Rightarrow i\%x != 0 \vee i\%y != 0)\}$

Ex.2

- Termination proof obligations:

3. Show that it is decreasing:

$$\{Inv \land C \land v\}\ z\ {+}{+};\ \{Inv \land v_{new}\}$$

$$v_{new} < v$$

$\{\forall i(1 \le i < z \Rightarrow i\%x != 0 \lor i\%y != 0) \land z \% x != 0 \lor z \% y != 0\}\ z\ {+}{+};\ \{\forall i(1 \le i < z \Rightarrow i\%x != 0 \lor i\%y != 0)\}$

$v \to v(x_{old}, y_{old}, z_{old}) = x_{old}y_{old} - z_{old}$

$v_{new} \to v(x_{new}, y_{new}, z_{new}) = x_{new}y_{new} - z_{new}$

Ex.2

- Termination proof obligations:

3. Show that it is decreasing:

$$\{Inv \wedge C \wedge v\}\ z\ {+}{+};\ \{Inv \wedge v_{new}\}$$

$$v_{new} < v$$

{∀i(1≤i<z =>i%x!=0 ∨ i%y!=0) ∧ z % x != 0 ∨ z % y != 0 } z ++; {∀i(1≤i<z =>i%x!=0 ∨ i%y!=0)}

$v \rightarrow v(x\ ,\ y,\ z_{old}) = xy - z_{old}$

$v_{new} \rightarrow v(x\ ,\ y,\ z_{new}) = xy - z_{new}$

Ex.2

- Termination proof obligations:

3. Show that it is decreasing:

$$\{\mathtt{Inv} \wedge \mathtt{C} \wedge \mathtt{v}\}\ \mathtt{z\ ++;}\ \{\mathtt{Inv} \wedge \mathtt{v_{new}}\}$$

$$\mathtt{v_{new}} < \mathtt{v}$$

{∀i(1≤i<z =>i%x!=0 ∨ i%y!=0) ∧ z % x != 0 ∨ z % y != 0 } z ++; {∀i(1≤i<z =>i%x!=0 ∨ i%y!=0)}

$\mathtt{v} \rightarrow \mathtt{v}(x, y, z_{old}) = xy - z_{old}$

$\mathtt{v_{new}} \rightarrow \mathtt{v}(x, y, z_{new}) = xy - (z_{old} + 1)$

Ex.2

- Termination proof obligations:

3. Show that it is decreasing:

$$\{Inv \wedge C \wedge v\}\ z{+}{+};\ \{Inv \wedge v_{new}\}$$

$$v_{new} < v$$

$\{\forall i(1 \le i < z \Rightarrow i\%x != 0 \vee i\%y != 0) \wedge z \% x != 0 \vee z \% y != 0\}\ z{+}{+};\ \{\forall i(1 \le i < z \Rightarrow i\%x != 0 \vee i\%y != 0)\}$

$$\left.\begin{array}{l} v \rightarrow v(x, y, z_{old}) = xy - z_{old} \\ v_{new} \rightarrow v(x, y, z_{new}) = xy - (z_{old} + 1) \end{array}\right\} v_{new} = v - 1$$

Ex.2

- Termination proof obligations:

3. Show that it is decreasing:

$$\{Inv \wedge C \wedge v\}\ z{+}{+};\ \{Inv \wedge v_{new}\}$$

$$v_{new} < v$$

{∀i(1≤i<z =>i%x!=0 ∨ i%y!=0) ∧ z % x != 0 ∨ z % y != 0 } z ++; {∀i(1≤i<z =>i%x!=0 ∨ i%y!=0)}

$$\left.\begin{array}{l} v \rightarrow v(x\ ,\ y,\ z_{old}) = xy - z_{old} \\ v_{new} \rightarrow v(x\ ,\ y,\ z_{new}) = xy - (z_{old} + 1) \end{array}\right\}\ v_{new} < v$$