

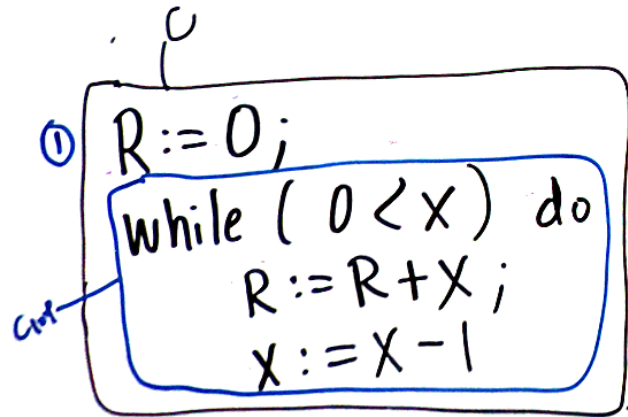
① $R := 0;$
while ($0 < X$) do
 $R := R + X;$
 $X := X - 1$



① $R := 0;$
while ($0 < X$) do
 $R := R + X;$
 $X := X - 1$

Prop. $\forall \sigma, \sigma', n. \sigma(X) = n \wedge$
 $\langle \sigma, c \rangle \Downarrow \sigma' \Rightarrow$
 $\sigma'(R) = \sum_{i=1}^n i$

Proof.



Prop. $P(n) \equiv \forall \sigma, \sigma'. \sigma(X) = n \wedge$
 $\forall n. P(n). \quad \langle \sigma, c \rangle \Downarrow \sigma' \Rightarrow$
 $\sigma'(R) = \sum_{i=1}^n i$

Proof.
 By induction on n .

Base case
 $n = 0$

Assume $\sigma(X) = n$
 $\langle \sigma, c \rangle \Downarrow \sigma'$
To show $\sigma'(R) = \sum_{i=1}^n i = 0$

From $\langle \sigma, c \rangle \Downarrow \sigma'$ we know seq. was used.

① $\langle \sigma, R := 0 \rangle \Downarrow \sigma_1$

② $\langle \sigma_1, C_{loop} \rangle \Downarrow \sigma'$

From ①, we know Assign.

so $\sigma_1 = \sigma[R \mapsto 0]$

From

① $R := 0;$
 While ($0 < X$) do
 $R := R + X;$
 $X := X - 1$

Prop. $P(n) \equiv \forall \sigma, \sigma'. \sigma(X) = n \wedge$
 $\forall n. P(n). \langle \sigma, c \rangle \Downarrow \sigma' \Rightarrow$
 $\sigma'(R) = \sum_{i=1}^n i$

Proof.
 By induction on n .

$\sigma' = \sigma'$
 $= \sigma[R \mapsto 0].$
 $\sigma'(R) = 0 \checkmark$

Base case
 $n = 0$

Assume $\sigma(X) = 0$
 $\langle \sigma, c \rangle \Downarrow \sigma'$
To show $\sigma'(R) = \sum_{i=1}^n i = 0$

From $\langle \sigma, c \rangle \Downarrow \sigma'$ we know seq. was used.

① $\langle \sigma, R := 0 \rangle \Downarrow \sigma_1$

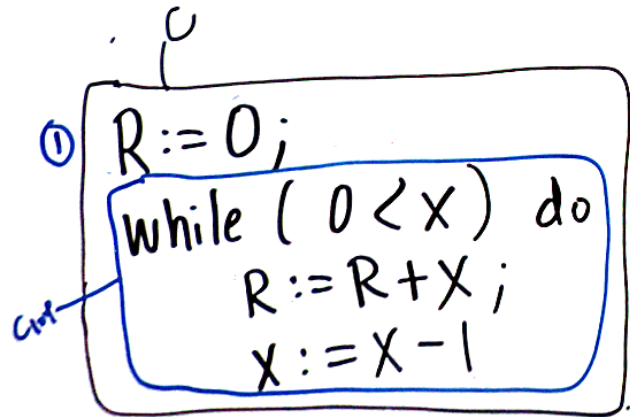
② $\langle \sigma_1, c_{loop} \rangle \Downarrow \sigma'$

From ①, we know Assign.

so $\sigma_1 = \sigma[R \mapsto 0]$

Observe $\langle \sigma_1, 0 < X \rangle \Downarrow \text{false}$.

From ② we know while-F was used.



Prop. $P(n) \equiv \forall \sigma, \sigma'. \sigma(X) = n \wedge$
 $\forall n. P(n). \langle \sigma, c \rangle \Downarrow \sigma' \Rightarrow$
 $\sigma'(R) = \sum_{i=1}^n i$

Proof.
 By induction on n .

Inductive case

$n = m + 1$
 Assume $\sigma(X) = n$
 ① $\langle \sigma, c \rangle \Downarrow \sigma'$

From ①, Seq was used.

② $\langle \sigma, R := 0 \rangle \Downarrow \sigma_1 = \sigma(R \mapsto 0)$

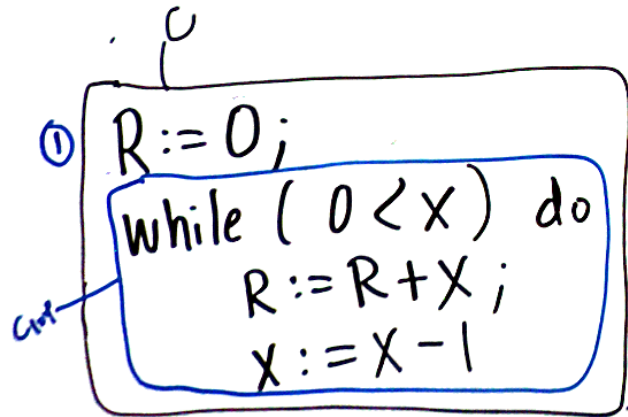
③ $\langle \sigma_1, c_{loop} \rangle \Downarrow \sigma'$

Observe $\langle \sigma_1, 0 < X \rangle \Downarrow \text{true}$.

From ③, While-T was used.

$\langle \sigma_1, c \rangle \Downarrow \sigma_2$

$\langle \sigma_2, c_{loop} \rangle \Downarrow \sigma'$



Prop. $P(n) \equiv \forall \sigma, \sigma'. \sigma(X) = n \wedge$
 $\forall n. P(n). \langle \sigma, c \rangle \Downarrow \sigma' \Rightarrow$
 $\sigma'(R) = \sum_{i=1}^n i$

Proof.
 By induction on n .

Inductive case

$n = m + 1$
 Assume $\sigma(X) = n$
 ① $\langle \sigma, c \rangle \Downarrow \sigma'$

From ①, Seq was used.

② $\langle \sigma, R := 0 \rangle \Downarrow \sigma_1 = \sigma(R \mapsto 0)$

③ $\langle \sigma_1, c_{loop} \rangle \Downarrow \sigma'$

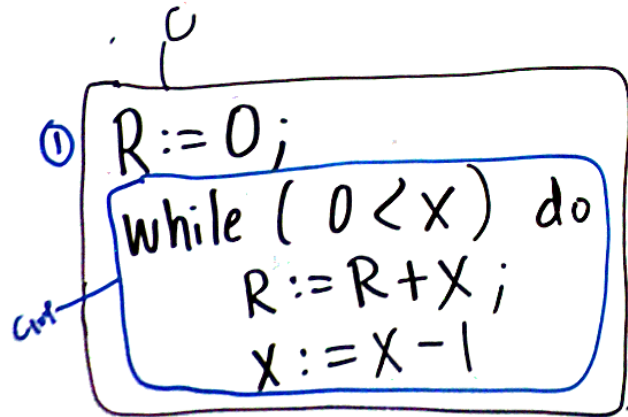
Observe $\langle \sigma_1, 0 < X \rangle \Downarrow \text{true}$.

From ③, While-T was used.

④ $\langle \sigma_1, R := R + X; X := X - 1 \rangle \Downarrow \sigma_2$

⑤ $\langle \sigma_2, c_{loop} \rangle \Downarrow \sigma'$

Observe $\sigma_2(X) = m$.



Inductive case

$$n = m + 1$$

Assume $\sigma(X) = n$

$$\textcircled{1} \langle \sigma, c \rangle \Downarrow \sigma'$$

From $\textcircled{1}$, Seq was used.

$$\textcircled{2} \langle \sigma, R := 0 \rangle \Downarrow \sigma_1 = \sigma(R \mapsto 0)$$

$$\textcircled{3} \langle \sigma_1, c_{loop} \rangle \Downarrow \sigma'$$

Observe $\langle \sigma_1, 0 < X \rangle \Downarrow \text{true}$.

From $\textcircled{3}$, While-T was used.

$$\textcircled{4} \langle \sigma_1, R := R + X; X := X - 1 \rangle \Downarrow \sigma_2$$

$$\textcircled{5} \langle \sigma_2, c_{loop} \rangle \Downarrow \sigma'$$

Observe $\sigma_2(X) = m$.

Prop. $P(n) \equiv \forall \sigma, \sigma'. \sigma(X) = n \wedge \sigma(R) = m$

$\forall n. P(n).$

$$\langle \sigma, c_{loop} \rangle \Downarrow \sigma' \Rightarrow$$

$$\sigma'(R) = \sum_{i=1}^n i$$

Proof.

By induction on n .

① $R := 0;$
 While ($0 < X$) do
 $R := R + X;$
 $X := X - 1$

Prop. $P(n) \equiv \forall \sigma, \sigma'. \sigma(X) = n \wedge \sigma(R) = m$

$\forall n. P(n).$

$$\langle \sigma, c_{loop} \rangle \Downarrow \sigma' \Rightarrow \sigma'(R) = m + \sum_{i=1}^n i.$$

Proof.

By induction on n .

Inductive case

$$n = m + 1$$

Assume $\sigma(X) = n$

$$\textcircled{1} \langle \sigma, c \rangle \Downarrow \sigma'$$

From $\textcircled{1}$, Seq was used.

$$\textcircled{2} \langle \sigma, R := 0 \rangle \Downarrow \sigma_1 = \sigma(R \mapsto 0)$$

$$\textcircled{3} \langle \sigma_1, c_{loop} \rangle \Downarrow \sigma'$$

Observe $\langle \sigma_1, 0 < X \rangle \Downarrow \text{true}$.

From $\textcircled{3}$, While-T was used.

$$\textcircled{4} \langle \sigma_1, R := R + X; X := X - 1 \rangle \Downarrow \sigma_2$$

$$\textcircled{5} \langle \sigma_2, c_{loop} \rangle \Downarrow \sigma'$$

Observe $\sigma_2(X) = m$.

① $R := 0;$
 conf $\text{while } (0 < X) \text{ do}$
 $R := R + X;$
 $X := X - 1$

Prop. $P(n) \equiv \forall \sigma, \sigma'. \sigma(X) = n \wedge \sigma(R) = m$

$\forall n. P(n).$

$\langle \sigma, c_{loop} \rangle \Downarrow \sigma' \Rightarrow$

$$\sigma'(R) = m + \sum_{i=1}^n i.$$

Proof.

By induction on n .

Base case

$n = 0$

Assume $\sigma(X) = 0$

$\sigma(R) = m$

① $\langle \sigma, c_{loop} \rangle \Downarrow \sigma'$

Observe $\langle \sigma, 0 < X \rangle \Downarrow \text{false}$

From ① while \leftarrow F.

$\sigma = \sigma'$

$$\sigma'(R) = m = m + \sum_{i=1}^0 i \quad \checkmark$$

① $R := 0;$
 While ($0 < X$) do
 $R := R + X;$
 $X := X - 1$

Prop. $P(n) \equiv \forall \sigma, \sigma'. \sigma(X) = n \wedge \sigma(R) = m$
 $\forall n. P(n). \langle \sigma, c_{loop} \rangle \Downarrow \sigma' \Rightarrow \sigma'(R) = m + \sum_{i=1}^n i.$

Proof.

By induction on n .

Inductive case

$$n = n' + 1$$

Assume $\sigma(X) = n$
 $\sigma(R) = m$

① $\langle \sigma, c_{loop} \rangle \Downarrow \sigma'$

Observe $\langle \sigma, 0 < X \rangle \Downarrow \text{true}$.

From ① while-T was used.

② $\langle \sigma, R := R + X, X := X - 1 \rangle \Downarrow \sigma_1$

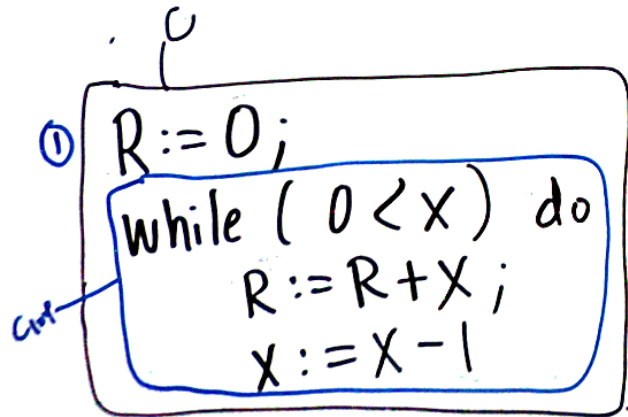
③ $\langle \sigma_1, c_{loop} \rangle \Downarrow \sigma'$

From ②, Seq, Assign (lhs).

$\sigma_1 = \sigma[R \mapsto m+n, X \mapsto n']$

Applying IH n' .

$$\sigma'(R) = m+n + \sum_{i=1}^{n'} i = m + \sum_{i=1}^n i \quad \checkmark$$



Prop. $P(D). \forall \sigma, \sigma', n. \sigma(X) = n \wedge \sigma(R) = m$

$\forall D. P(D). \text{DIT} \langle \sigma, c_{loop} \rangle \Downarrow \sigma' \Rightarrow$
 $\sigma'(R) = m + \sum_{i=1}^n i.$

Proof.

By induction on derivation of D.

Inductive case

$$n = n' + 1$$

Assume $\sigma(X) = n$
 $\sigma(R) = m$

① $\langle \sigma, c_{loop} \rangle \Downarrow \sigma'$

Observe $\langle \sigma, 0 < X \rangle \Downarrow \text{true}$.

From ① while-T was used.

② $\langle \sigma, R := R + X, X := X - 1 \rangle \Downarrow \sigma_1$

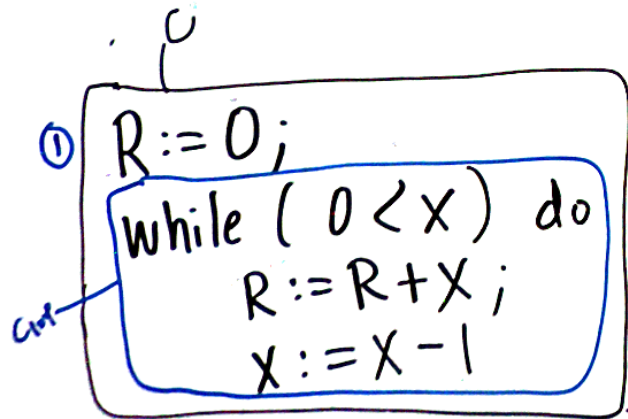
③ $\langle \sigma_1, c_{loop} \rangle \Downarrow \sigma'$

From ②, Seq, Assign (Seq).

$\sigma_1 = \sigma[R \mapsto m+n, X \mapsto n']$

Applying IH n' .

$$\sigma'(R) = m+n + \sum_{i=1}^{n'} i = m + \sum_{i=1}^n i \quad \checkmark$$



Prop. $P(D). \forall \sigma, \sigma', n. \sigma(X) = n \wedge \sigma(R) = m$

$\forall D. P(D). \text{DIT} \langle \sigma, c_{loop} \rangle \Downarrow \sigma' \Rightarrow$
 $\sigma'(R) = m + \sum_{i=1}^n i.$

Proof.

By induction on derivation of D.

Case Skip

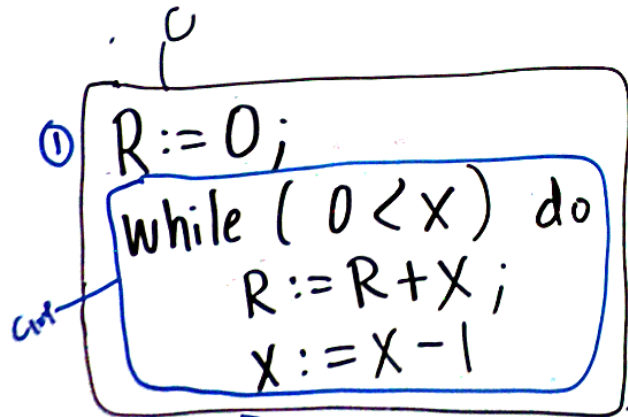
$c = \text{skip}.$

Assume $\sigma(x) = n$
 $\sigma(R) = m$

$\text{DIT} \langle \sigma, c_{loop} \rangle \Downarrow \sigma'$

$c = \text{while}(\dots) \text{ do } \dots$

~~X~~



Prop. ① $P(D). \forall \sigma, \sigma', n. \sigma(X) = n \wedge \sigma(R) = m$
 $\forall D. P(D). D \Vdash \langle \sigma, c_{loop} \rangle \Downarrow \sigma' \Rightarrow$
 $\sigma'(R) = m + \sum_{i=1}^n i.$

Proof.

By induction on derivation of D.

Case While-F

$\sigma = \sigma'$
 $\langle \sigma, 0 < X \rangle \Downarrow \text{false.}$
 \vdots

Case While-T

$\langle \sigma, 0 < X \rangle \Downarrow \text{true}$
 $\langle \sigma, R := R + X; X := X - 1 \rangle \Downarrow \sigma_1$
 $D, \Vdash \langle \sigma_1, c_{loop} \rangle \Downarrow \sigma'$
 \vdots