SHEET 12

a) Precondition → $\{n \in Z \wedge x \in Z\}$

Postcondition → $\{y = x^n\}$

b) Precondition : $\{n \in Z \wedge x \in Z\}$

$K := n$

$P := x$

$y := 1$

$\{k = n,\ P = x,\ y = 1\}$ Annotation 1

while $k > 0$ do

$\{y \times p^k = x^n,\ k \geq 0\}$ Annotation 2

if $k \bmod 2 = 0$ then

$p := p \times p$

$k := k / 2$

else

$y := y \times p$

$k := k - 1$

fi

od

Postcondition : $\{y = x^n\}$

c) Verification conditions

For assignments

$\{P\}\ V := E\ \{Q\}$

$P \to Q\ \{E/V\}$

this implies to:

$\{n \in Z \land x \in Z\}$

$k := n$

$p := x$

$y := 1$

$\{k = n, p = x, y = 1\}$

which results to

$\{n \in Z \land x \in Z\} \to \{n = n, x = x, 1 = 1\}$

For the while loop condition

$P \to R$ where

$\{P\} = \{k = n, p = x, y = 1\}$

$\{R\} = \{y \times p^k = x^n, k \geq 0\}$

this results to :

$\{K = n, P = x, Y = 1\} \rightarrow \{1 \times x^n = x^n, n \geq 0\}$

$(R \wedge \neg S) \rightarrow Q$ where

$\{R\} = \{Y \times P^k = x^n, K \geq 0\}$

$\{S\} = K > 0$

this results to :

$\{Y \times P^k = x^n, K \geq 0, K \leq 0\} \rightarrow \{Y = x^n\}$

Add conditions from $\{R \wedge S\}$ C $\{R\}$

C is the if - else statement

So :

$\{R \wedge S\} = \{Y \times P^k = x^n, K \geq 0, K > 0\}$

This is a precondition now

P

$\{R\} = \{Y \times P^k = x^n, K \geq 0\}$

This is a postcondition now

Q

We bump into another if condition now

- $\{P \wedge S\}\ C_1\ \{Q\}$

$$\{y \times p^k = x^n,\ k \geq 0,\ k > 0,\ (k \bmod 2 = 0)\}$$

$$p := p \times p$$

$$k := k / 2$$

Do the assignment too:

$$\{y \times p^k = x^n,\ k \geq 0,\ k > 0,\ (k \bmod 2 = 0)\}$$

$$\rightarrow$$

$$\{\frac{k}{2} \geq 0,\ y \times (p \times p)^{k/2} = x^n\}$$

- $\{P \wedge \neg S\}\ C_2\ \{Q\}$

$$\{y \times p^k = x^n,\ k \geq 0,\ k > 0,\ k \bmod 2 = 1\}$$

$$y := y \times p$$

$$k := k - 1$$

$$\rightarrow$$

$$\{k - 1 \geq 0,\ (y \times p) \times p^{k-1} = x^n\}$$

d) Proving the partial correctness verification conditions

- $\{n \in Z \wedge x \in Z\} \rightarrow \{n = n, x = x, 1 = 1\}$

This is true as n and x are both integers and the outcome is also true

- $\{k = n, P = x, y = 1\} \rightarrow \{1 \times x^n = x^n, n \geq 0\}$

We have : $1 \times x^n = x^n$

so : $x^n = x^n$

$n \geq 0 \rightarrow$ n is derived from k, as $k \geq 0$, n also satisfies this

- $\{y \times p^k = x^n, k \geq 0, k \leq 0\} \rightarrow \{y = x^n\}$

We have : $k \geq 0$ and $k \leq 0$

so the only thing that satisfies this is $k = 0$

$\Downarrow$

$$y \times p^k = x^n$$

$$y \times p^0 = x^n$$

$$y = x^n$$

- $\{ y \times p^k = x^n,\ k \geq 0,\ k > 0,\ (k \bmod 2 = 0) \}$

$\rightarrow$

$\{ \frac{k}{2} \geq 0,\ y \times (p \times p)^{\frac{k}{2}} = x^n \}$

$k \geq 0 \xrightarrow{\text{divide by } 2} \frac{k}{2} \geq 0$

Also: $y \times (p \times p)^{\frac{k}{2}} = x^n$

$y \times p^{\frac{k}{2} + \frac{k}{2}} = x^n$

$y \times p^k = x^n$

- $\{ y \times p^k = x^n,\ k \geq 0,\ k > 0,\ k \bmod 2 = 1 \}$

$\rightarrow$

$\{ k - 1 \geq 0,\ y \times p \times p^{k-1} = x^n \}$

We have: $k \geq 0$

$k > 0$

$k \bmod 2 = 1$

So we can say $k = 1$

$k - 1 \geq 0$

$1 - 1 \geq 0$

$0 \geq 0 \rightarrow$ this is true

Also:
$$y \times p \times p^{k-1} = x^n$$
$$y \times p^{1+k-1} = x^n$$
$$y \times p^k = x^n$$

e) We need to put an additional annotation to show that the while loop is terminating

K is the variable of the loop, hence:

$E = [k] \rightarrow$ put in the beginning

$[k] \rightarrow$ put after the loop

f) Updating verification conditions

$P \rightarrow R$ (shown before)

$R \wedge \neg S \rightarrow Q$ (shown before)

$R \wedge S \rightarrow E \geq 0$

$\downarrow$

$\{y \times p^k = x^n, k \geq 0, k > 0\} \rightarrow E \geq 0$

$\rightarrow k \geq 0$

The precondition and the postcondition change for the if-else statement

$$\{R \wedge S \wedge (E = m)\} = \{Y \times P^k = x^n, k \geq 0, k > 0, k = m\}$$

precondition

$$\{R \wedge (E < m)\} = \{Y \times P^k = x^n, k \geq 0, k < m\}$$

postcondition

- $\{P \wedge S\}\ C_1\ \{Q\}$

$$\{Y \times P^k = x^n, k \geq 0, k > 0, k = m, k \bmod 2 = 0\}$$

$$P := P \times P$$

$$K := K / 2$$

$$\{\frac{K}{2} \geq 0, Y \times (P \times P)^{\frac{K}{2}} = x^n, \frac{K}{2} < m\}$$

• $\{P \wedge \neg S\}\ C_2\ \{Q\}$

$$\{y \times p^k = x^n,\ k \geq 0,\ k > 0,\ k = m\}$$

$$y := y \times p$$

$$k := k - 1$$

$$\rightarrow$$

$$\{(k-1) < m,\ y \times p \times p^{k-1} = x^n\}$$

9) Proving the total correctness verification conditions

• $\{y \times p^k = x^n,\ k \geq 0,\ k > 0\} \rightarrow k \geq 0$

We see that the condition on the left side satisfy the one on the right side

• $\{y \times p^k = x^n,\ k \geq 0,\ k > 0,\ k = m,\ k \bmod 2 = 0\}$

$$\rightarrow$$

$$\left\{\frac{k}{2} \geq 0,\ y \times (p \times p)^{k/2} = x^n,\ \frac{k}{2} < m\right\}$$

$k/2 \geq 0$ (already proven)

$y \times (p \times p)^{k/2} = x^n$ (already proven)

We have : $k = m$

So : $\frac{k}{2} < m$

$\frac{m}{2} < m \rightarrow$ this is true

- $\{ Y \times P^{k} = x^{n} , k \geq 0 , k > 0 , k = m \}$

$\rightarrow$

$\{ (k-1) < m , Y \times P \times P^{k-1} = x^{n} \}$

$Y \times P \times P^{k-1} = x^{n}$ (already proven)

We have : $k = m$

So : $k - 1 < m$

$m - 1 < m \rightarrow$ this is true