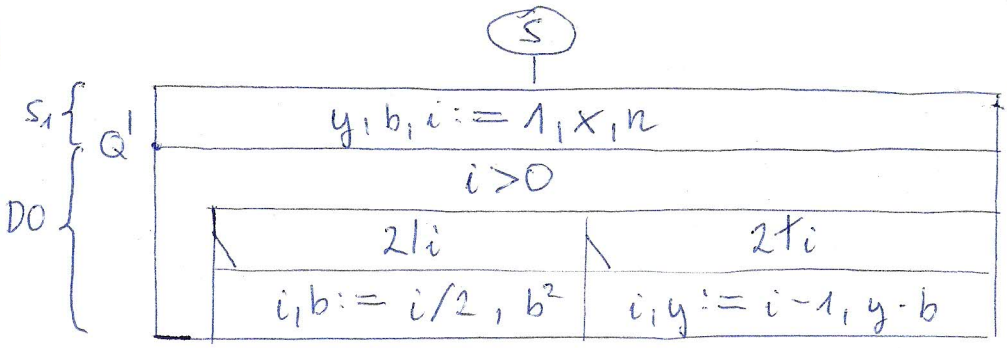
$A = (x : \mathbb{N}^+, n : \mathbb{N}, y : \mathbb{N})$

$B = (x' : \mathbb{N}^+, n' : \mathbb{N})$

$Q = (x = x' \wedge n = n')$

$R = (Q \wedge y = x^n)$



$i : \mathbb{N}$ and $b : \mathbb{N}^+$ are auxiliary variables

$Q' = (Q \wedge y = 1 \wedge b = x \wedge i = n)$

$Inv = (Q \wedge y \cdot b^i = x^n)$

$t : i$

We want to prove the total correctness formula in order to prove that S solves the problem:

$Q \Rightarrow wp(S, R)$

Now, S is a sequence. Let us apply the verification rule of sequence. Instead of proving $Q \Rightarrow wp(S, R)$, it is enough to prove two others:

I) $Q \Rightarrow wp(S_1, Q')$

II) $Q' \Rightarrow wp(DO, R)$

$S = (S_1 ; DO)$ is a sequence, Q' is the intermediate condition

I) $Q \Rightarrow wp(\underbrace{y, b, i := 1, x, n}_{\text{program}}, \underbrace{Q'}_{\text{logical function}})$

$wp(y, b, i := 1, x, n, Q') = Q'^{\,y \leftarrow 1, b \leftarrow x, i \leftarrow n} =$

$(Q \wedge y = 1 \wedge b = x \wedge i = n)^{y \leftarrow 1, b \leftarrow x, i \leftarrow n} =$

$(Q \wedge 1 = 1 \wedge x = x \wedge n = n) = Q$

$Q \Rightarrow Q$ ✓ this is true

II) $Q' \Rightarrow wp(DO, R)$

We prove this by using the verification rule of loop, and proving 5 other conditions. We want to prove that DO loop takes us from Q' to R. (Not from Q to R.)

1. $Q' \Rightarrow Inv$

$Q' \Rightarrow Inv$ means: for any state where Q' is true, Inv is also true. We do not need to prove that Inv is always true. In fact, Inv is not always true; but in case Q' is true then Inv is also true.