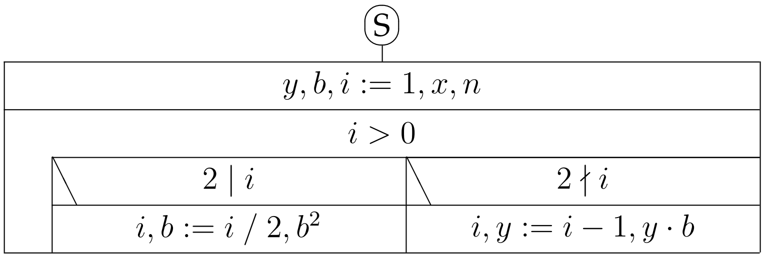
Programming theory
2nd midterm exam - sample

1. $A = (x{:}\mathbb{N}^+, n{:}\mathbb{N}, y{:}\mathbb{N}^+)$
   $B = (x'{:}\mathbb{N}, n'{:}\mathbb{N})$
   $Q = (x = x' \land n = n' \land x > 0)$
   $R = (Q \land y = x^n)$



   Let $Q' = (Q \land y = 1 \land b = x \land i = n)$ be the intermediate condition of the sequence in the loop body, $Inv = (Q \land y \cdot b^i = x^n)$ be the invariant of the loop, and $t : i$ variant function. $b{:}\mathbb{N}$ and $i{:}\mathbb{N}$ are auxiliary variables of the program S. Prove that $Q \implies wp(S, R)$ holds.

2. $A = (x{:}\mathbb{Z})$
   Write down the sequences assigned to the sates 3, 5 and 10.

   parbegin $S_1 \| S_2$ **parend**

S_1 :	S_2 :
await $x = 3$ then SKIP ta	$x := 1$

3. Prove that the following program is free from deadlock.
   $A = (a{:}\mathbb{Z}^n, b{:}\mathbb{Z}^n)$ is the base statespace, i and j are integer type of auxiliary variables.

   $i, j := 1, 1;$
   $\{a = a' \land i = 1 \land j = 1\}$
   parbegin $S_1 \| S_2$ **parend**

S_1:

$\{Inv\}$
while $i \le n$ do
$\{Inv \wedge i \le n\}$
  await $i = j$ then
    $x, i := a[i], i+1$
  ta
$\{Inv\}$
od
$\{Inv \wedge i = n+1\}$

S_2:

$\{Inv\}$
while $j \le n$ do
$\{Inv \wedge j \le n\}$
  await $i > j$ then
    $b[j], j := x, j+1$
  ta
$\{Inv\}$
od
$\{Inv \wedge j = n+1\}$

$$Inv = (a = a' \wedge 0 \le i-1 \le j \le i \le n+1 \wedge \forall k \in [1..j-1] : b[k] = a[k] \wedge (i > j \rightarrow x = a[i-1]))$$

4. Given the following problem:
   $A = (x{:}\mathbb{N}, n{:}\mathbb{N}, z{:}\mathbb{N})$
   $Pre = (x = x' \wedge n = n' \wedge x > 0)$
   $Post = (z = x'^{n'})$

   Prove the total correctness of the following (annotated) program (let us denote it by S) with respect to the given problem. You can assume that the interference freedom and deadlock freedom were alredy proven for the parallel block.

$\{x = x' \wedge n = n' \wedge x > 0\}$
$z := 1;$
$\{Inv\}$
parbegin $S_1 \| S_2$ **parend**
$\{z = x'^{n'}\}$

S_1:

$\{Inv\}$
while $n \neq 0$ do
$\{Inv \wedge n \neq 0\}$
  n,z := n−1,z·x
od
$\{z = x'^{n'} \wedge n = 0\}$

S_2:

$\{Inv\}$
while $n \neq 0$ do
$\{Inv\}$
  await even(n) then
    x,n := x·x,n/2
  ta
od
$\{z = x'^{n'} \wedge n = 0\}$

Inv denotes the invariant of the loops and is given as follows: $Inv = (z \cdot x^n = x'^{n'})$
Variant function of the loops: t: n