Programming theory - practice #10

1. Problem: Decide whether a given positive integer is prime number or not.

   $A = (x{:}\mathbb{N}^+, l{:}\mathbb{L})$
   $B = (x'{:}\mathbb{N}^+)$
   $Q = (x = x' \wedge x > 1)$
   $R = (Q \wedge l = (\forall j \in [2..x-1] \colon j \nmid x))$
   The statespace of the program is $(x{:}\mathbb{N}^+, k{:}\mathbb{N}^+, l{:}\mathbb{L})$.

   S

$k, l := 2, true$	
	Q'
$k \neq x$	
$\quad l := l \wedge k \nmid x$	
	Q''
$\quad k := k + 1$	

   Let $Q' = (Q \wedge k = 2 \wedge l = true)$ be the intermediate condition of the sequence, and $t : x - k$ be the variant function.
   $Inv = (Q \wedge l = (\forall j \in [2..k-1] \colon j \nmid x) \wedge k \in [2..x])$
   The body of the loop is a sequence. Let $Q'' = (Q \wedge l = (\forall j \in [2..k] \colon j \nmid x) \wedge k + 1 \in [2..x] \wedge x - k = t_0)$ be the intermediate condition of the loop body.
   Prove that program S solves the problem.

2. Problem: Calculate the nth Fibonacci number.

   $A = (n{:}\mathbb{N}, s{:}\mathbb{N})$
   $B = (n'{:}\mathbb{N})$
   $Q = (n = n' \wedge n > 2)$
   $R = (Q \wedge s = Fib(n))$
   where

$$Fib(n) = \begin{cases} 0 & \text{if} \quad n = 1 \\ 1 & \text{if} \quad n = 2 \\ Fib(n-1) + Fib(n-2) & \text{if} \quad n > 2 \end{cases}$$

   The statespace of the program is $(n{:}\mathbb{N}, s{:}\mathbb{N}, z{:}\mathbb{N}, i{:}\mathbb{N})$.

   S

$i, s, z := 3, 1, 0$	
	Q'
$i \leq n$	
$\quad i, s, z := i + 1, s + z, s$	

Let $Q' = (Q \wedge i = 3 \wedge s = 1 \wedge z = 0)$ be the intermediate condition of the sequence, and $t : n + 1 - i$ be the variant function.
$Inv = (Q \wedge s = Fib(i-1) \wedge z = Fib(i-2) \wedge i \in [3..n+1])$ is the loop invariant.
Prove that program S solves the problem.

3. Problem: Given an array containing integer numbers. Increment every element of the array by 1.

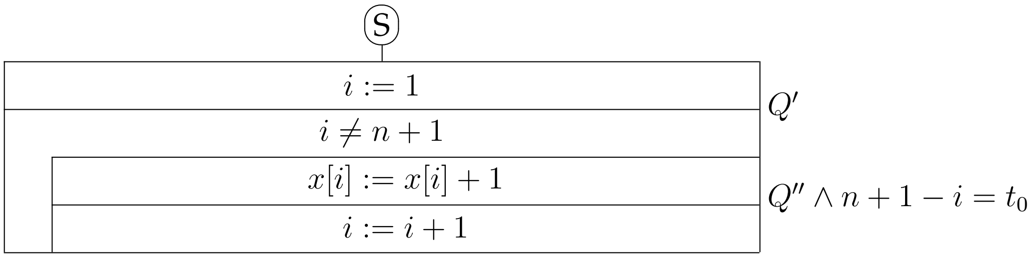
   $A = (x{:}\mathbb{Z}^n)$

   $B = (x'{:}\mathbb{Z}^n)$

   $Q = (x = x')$

   $R = (\forall k \in [1..n]\colon x[k] = x'[k] + 1)$

   The statespace of the program is $(x{:}\mathbb{Z}^n, i{:}\mathbb{N})$.

   Let $Q' = (Q \wedge i = 1)$ be the intermediate condition of the sequence, and $t : n + 1 - i$ be the variant function.
   $Inv = (\forall k \in [1..i-1]\colon x[k] = x'[k] + 1 \wedge i \in [1..n+1] \wedge \forall k \in [i..n]\colon x[k] = x'[k])$
   The body of the loop is a sequence. Let $Q'' \wedge n+1-i = t_0$ be the intermediate condition of the loop body, where $Q'' = Inv^{i \leftarrow i+1}$.
   Prove that program S solves the problem.

4. Problem: Given an array containing integer numbers. We can assume that the array contains at least one negative number. Find the index of the first negative element of the array.

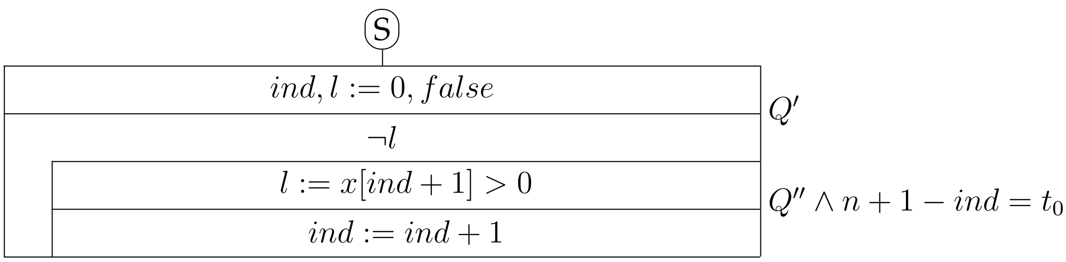
   $A = (x{:}\mathbb{Z}^n, ind{:}\mathbb{N})$

   $B = (x'{:}\mathbb{Z}^n)$

   $Q = (x = x' \wedge \exists j \in [1..n]\colon x[j] < 0)$

   $R = (Q \wedge ind \in [1..n] \wedge x[ind] < 0 \wedge \forall k \in [1..ind-1]\colon x[k] \geq 0)$

   The statespace of the program is $(x{:}\mathbb{Z}^n, ind{:}\mathbb{N}, l{:}\mathbb{L})$.

Let $Q' = (Q \land ind = 0 \land l = false)$ be the intermediate condition of the sequence, and $t : n + 1 - ind$ be the variant function.
$Inv = (Q \land ind \in [0..n] \land \forall j \in [1..ind - 1]\colon x[j] \geq 0 \land l = (\exists j \in [1..ind]\colon x[j] < 0))$
The body of the loop is a sequence. Let $Q'' \land n + 1 - ind = t_0$ be the intermediate condition of the loop body, where $Q'' = Inv^{ind \leftarrow ind+1}$.
Prove that program S solves the problem.

5. Problem: Determine the greatest common divisor of two positive integers.

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

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

   $Q = (x = x' \land y = y')$

   $R = (Q \land d \mid x \land d \mid y \land \forall k \in [d + 1..min(x, y)]\colon \neg(k \mid x \land k \mid y))$

   The statespace of the program is $(x{:}\mathbb{N}^+, y{:}\mathbb{N}^+, d{:}\mathbb{N}^+)$.

   S

$d := min(x, y)$	Q'
$\neg(d \mid x \land d \mid y)$	
$\quad d := d - 1$	

   Let $Q' = (Q \land d = min(x, y))$ be the intermediate condition of the sequence, and $t : d$ be the variant function.
   $Inv = (Q \land \forall k \in [d + 1..min(x, y)]\colon \neg(k \mid x \land k \mid y))$
   Prove that program S solves the problem.

6. Problem: Determine the largest integer that is less than the square root of a given natural number.

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

   $B = (x'{:}\mathbb{N})$

   $Q = (x = x')$

   $R = (Q \land y^2 \leqslant x < (y + 1)^2)$

   The statespace of the program is $(x{:}\mathbb{N}, y{:}\mathbb{N}, a{:}\mathbb{N}, b{:}\mathbb{N})$.

   S

$y, a, b := 0, 1, 1$	Q'
$a \leq x$	
$\quad b := b + 2$	Q''
$\quad y, a := y + 1, a + b$	

Let $Q' = (Q \land \land y = 0 \land a = 1 \land b = 1)$ be the intermediate condition of the sequence, and $t : x - a + 8$ be the variant function.
$Inv = (Q \land y^2 \leqslant x \land a = (y+1)^2 \land b = 2y+1)$ is the loop invariant.
The body of the loop is a sequence. Let $Q'' = (Q \land (y+1)^2 \leqslant x \land a + b = (y+2)^2 \land b = 2y + 3 \land x - a + 8 = t_0)$ be the intermediate condition of the loop body.
Prove that program S solves the problem.