TD 9

Exercice 1

1. Si possible, dérivez les triplets de Hoare suivants en utilisant les règles d'inférence introduites dans le cours (ces règles sont rappelées au dos de cette page). On suppose l'arithetique des nombres entiers.
   (a) $\vdash \{x > 0\}$ `x:==x-1` $\{0 \leq x\}$
   (b) $\vdash \{0 \leq x \wedge x \; mod \; 5 > 5\}$ `x:==x*x` $\{x \; div \; 2 = 1\}$
   (c) $\vdash \{x \leq 0\}$ `WHILE x < 0 DO x:==x+1` $\{x = 0\}$
   (d) $\vdash \{S * Y^P = X^N\}$ `P:=P-1; S:=S*Y` $\{S * Y^P = X^N\}$
   (e) $\vdash \{x \leq -2\}$ `WHILE 0 < x*x DO x:==x+1` $\{x = 0\}$

Figure 1: Preuves Simples

(a)

$$\dfrac{x > 0 \rightarrow (0 \leqslant x[x \mapsto x - 1\,]) \qquad \dfrac{}{\vdash \{0 \leqslant x[x \mapsto x - 1\,]\}\ x:=x-1\ \{0 \leqslant x\}}\,(aff) \qquad 0 \leqslant x \rightarrow 0 \leqslant x}{\vdash \{x>0\}\ x:=x-1\ \{0 \leqslant x\}}$$

` {x > 0} x:==x-1 {0 ≤ x}

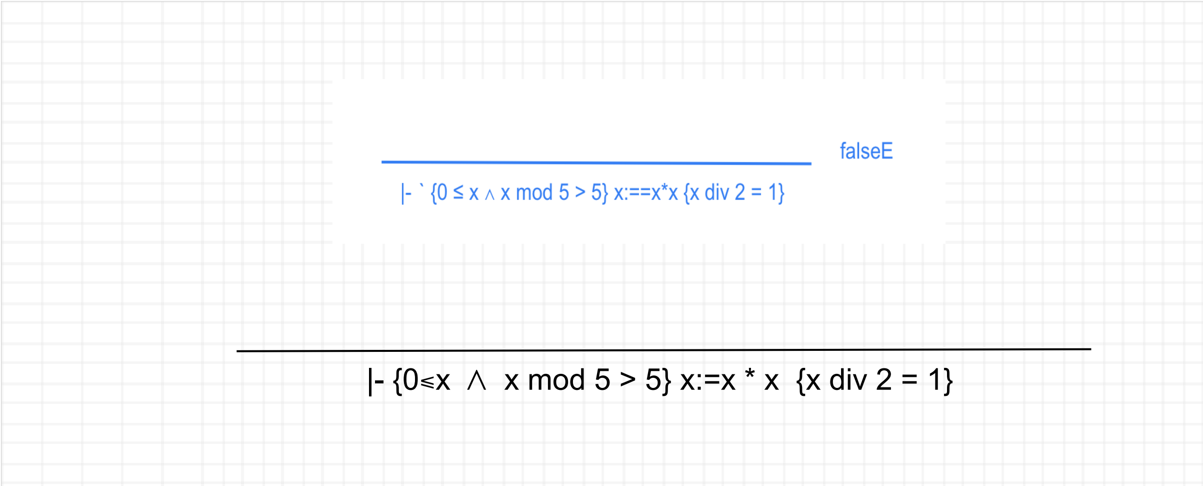
x > 0 -> (0 <= x [x -> x - 1])

equiv x > 0 -> x - 1

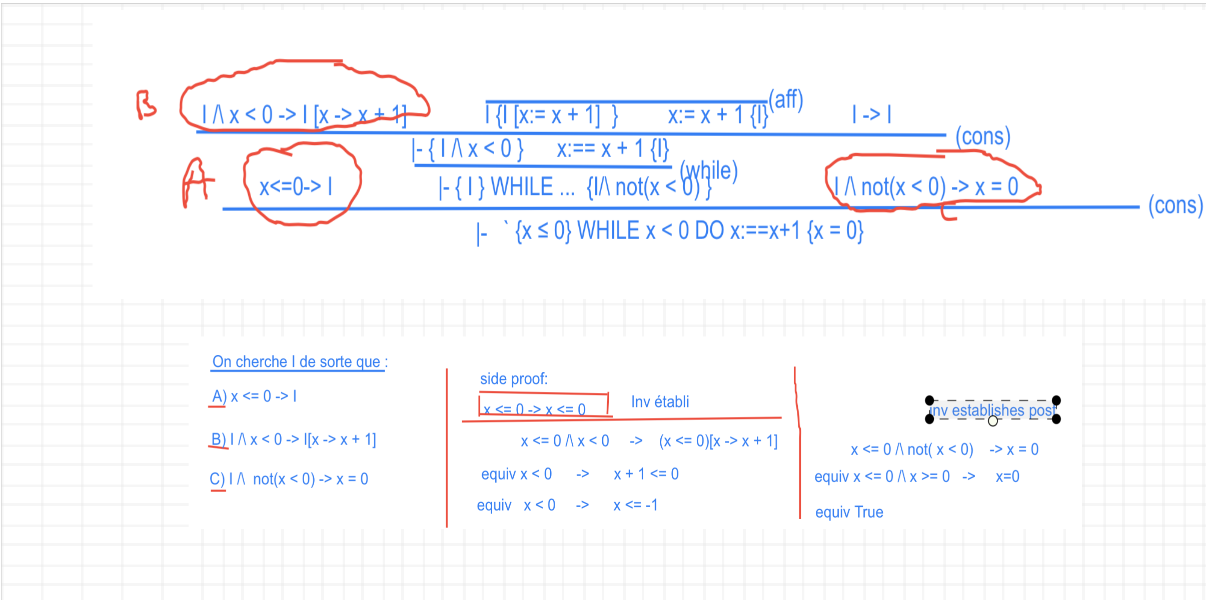
equiv x > 0 -> x >= 1

equiv True

(b)


falseE
|- ` {0 ≤ x ∧ x mod 5 > 5} x:==x*x {x div 2 = 1}
|- {0≤x ∧ x mod 5 > 5} x:=x * x {x div 2 = 1}

(c)


B
I /\ x < 0 -> I [x -> x + 1]
I {I [x:= x + 1] } x:= x + 1 {I}
(aff)
I -> I
|- { I /\ x < 0 } x:== x + 1 {I}
(cons)
A
x<=0-> I
|- { I } WHILE ... {I/\ not(x < 0) }
(while)
I /\ not(x < 0) -> x = 0
(cons)
|- ` {x ≤ 0} WHILE x < 0 DO x:==x+1 {x = 0}
On cherche I de sorte que :
A) x <= 0 -> I
B) I /\ x < 0 -> I[x -> x + 1]
C) I /\ not(x < 0) -> x = 0
side proof:
x <= 0 -> x <= 0
Inv établi
x <= 0 /\ x < 0 -> (x <= 0)[x -> x + 1]
equiv x < 0 -> x + 1 <= 0
equiv x < 0 -> x <= -1
inv establishes post
x <= 0 /\ not(x < 0) -> x = 0
equiv x <= 0 /\ x >= 0 -> x=0
equiv True

(d)

assign — assig

|- {Q[P |-> P-1]} P:=P-1 {Q} |- {Q} s:= S * Y {S * Y^P = X^P }

(sequence)

|- {S * Y^P = X^N } P:=P-1; S:=S*Y {S * Y^P = X^N }

Q equiv (S * Y^P = X^N)[S -> S * Y]
equiv S * Y * Y^P = X ^ N   OK
equiv S * Y ^ (P+1) = X ^ N

Q[P -> P - 1]
equiv S * Y^(P+1) = X ^ N[P -> P - 1]
equiv S * Y^((P-1) +1) = X^N
equiv (S * Y^P = X) = X^N)

ce qui correspond a la precondition globale....

e)

(aff)

I ∧ 0<x*x → I [x ↦ x+1] |- {I [x ↦ x+1]} x:=x+1 {I}   I → I   (cons)

|- {I ∧ 0<x*x} x:=x+1 {I}

(while)

x≤-2 → I |- {I} WHILE 0<x*x DO ... {I ∧ x*x ≥ 0}   I ∧ x*x ≥ 0 → x=

|- {x≤-2} WHILE 0<x*x DO x:=x+1 {x=2}

Hypothesis: I ≡ x≤0

Check A : x≤-2 -→ I ≡ x≤-2 -→ x≤0 ≡ True

Check B : I ∧ 0<x*x → I [x ↦ x+1]
≡ x≤0 ∧ 0<x*x -→ x+1≤ 0
≡ x≤0 ∧ 0<x*x ∧ 0 ≠ x -→ x ≤ -1
≡ True

Check C : I ∧ x*x ≥ 0 → x=0 ≡ x≤0 ∧ x*x ≥ 0 → x=0 ≡ True