Tarea 2

Tony Santiago Montes Buitrago - 202014562
Juan Carlos Marin Morales - 202013973

Departamento de Ingeniería de Sistemas y Computación, Universidad de los Andes

30 de agosto de 2021

Punto 1. Calcular la precondición más débil Q en los siguientes casos

I $\{Q\}$ x := x∗x∗x − 5 x∗x $\{x{>}0\}$

$wp(x := x * x * x - 5x * x | x > 0)$
$\equiv$ ⟨Axioma de Asignación⟩

$(x > 0)[x := x * x * x - 5x * x]$

$\equiv$ ⟨Definición de Sustitución⟩

$x^3 - 5x^2 > 0$

$\equiv$ ⟨Aritmética - factorización⟩

$x^2 \cdot (x - 5) > 0$

$\equiv$ ⟨Aritmética - x^2 siempre es positivo⟩

$x - 5 > 0$

$\equiv$ ⟨Aritmética - sumar 5 a ambos lados⟩

$x > 5$

□

II $\{Q\}$ x := x+1 $\{x^3 + 3x^2 + x > 0\}$

$wp(x := x + 1 | x^3 + 3x^2 + x > 0)$
$\equiv$ ⟨Axioma de Asignación, Definición de Sustitución⟩

$(x + 1)^3 + 3(x + 1)^2 + (x + 1) > 0$

$\equiv$ ⟨Aritmética - operar paréntesis⟩

$x^3 + 3x^2 + 3x + 1 + 3x^2 + 6x + 3 + x + 1 > 0$

$\equiv$ ⟨Aritmética - términos semejantes⟩

$x^3 + 6x^2 + 10x + 5 > 0$

$\equiv$ ⟨Aritmética - factor común polinomio⟩

$(x + 1) \cdot (x^2 + 5x + 5) > 0$

$\equiv$ ⟨Aritmética - trinomio de la forma $x^2 + bx + c$⟩

$\frac{1}{4} \cdot (x+1) \cdot (2x - \sqrt{5} + 5) \cdot (2x + \sqrt{5} + 5) > 0$

$\equiv$ $\langle$Aritmética - orden de los números: $\frac{1}{4} > 0\rangle$

$(x+1) \cdot (2x - \sqrt{5} + 5) \cdot (2x + \sqrt{5} + 5) > 0$

$\equiv$ $\langle$Aritmética - disyunción de 4 posibles soluciones$\rangle$

$$\left(x > -1 \land x > \frac{\sqrt{5}-5}{2} \land x > \frac{-\sqrt{5}-5}{2}\right) \lor \left(x > -1 \land x < \frac{\sqrt{5}-5}{2} \land x < \frac{-\sqrt{5}-5}{2}\right) \lor$$
$$\left(x < -1 \land x < \frac{\sqrt{5}-5}{2} \land x > \frac{-\sqrt{5}-5}{2}\right) \lor \left(x < -1 \land x > \frac{\sqrt{5}-5}{2} \land x < \frac{-\sqrt{5}-5}{2}\right)$$

$\equiv$ $\langle$Representación de desigualdades como rangos, Intersección de rangos $(\land)\rangle$

$$x \in (-1, \infty) \lor x \in \varnothing \lor x \in \left(\frac{-\sqrt{5}-5}{2}, \frac{\sqrt{5}-5}{2}\right) \lor x \in \varnothing$$

$\equiv$ $\langle$Unión de conjuntos $(\lor)\rangle$

$$x \in \left\{\left(\frac{-\sqrt{5}-5}{2}, \frac{\sqrt{5}-5}{2}\right) \cup (-1, \infty)\right\}$$

$\square$

III $\{Q\}$ x := x **mod** 4 $\{x = x \ mod \ 4\}$

$wp(x := x \texttt{ mod } 4 | x = x \texttt{ mod } 4)$

$\equiv$ $\langle$Axioma de Asignación, Definición de Sustitución$\rangle$

$x \texttt{ mod } 4 = (x \texttt{ mod } 4) \texttt{ mod } 4$

$\equiv$ $\langle$Sustitución $[y := x \texttt{ mod } 4]$, en donde $0 \leq y < 4$ por definición de módulo$\rangle$

$(y = y \texttt{ mod } 4)$

$\equiv$ $\langle$Para todo número entre 0 y d, su módulo d es el mismo número. $0 \leq y < 4 \Rightarrow (y \texttt{ mod } 4 = y)\rangle$

`true`

$\square$

IV $\{Q\}$ x, y := x+1, y−1 $\{x>y\}$

$wp(x, y := x+1, y-1 | x > y)$

$\equiv$ $\langle$Axioma de Asignación x2, Definición de Sustitución x2$\rangle$

$x + 1 > y - 1$

$\equiv$ $\langle$Aritmética - restar 1 a ambos lados$\rangle$

$x > y - 2$

$\square$

V $\{Q\}$ x , y := y+1, x−1 $\{y>5\}$

$wp(x, y := y + 1, x - 1|y > 5)$
$\equiv$ ⟨Axioma de Asignación x2, Definición de Sustitución x2⟩

$x - 1 > 5$

$\equiv$ ⟨Aritmética - sumar 1 a ambos lados⟩

$x > 6$

□

VI $\{Q\}$ x := x+1; y := y−1 $\{x>y\}$

$wp(x := x + 1; y := y - 1|x > y)$
$\equiv$ ⟨Axioma de Asignación x2⟩

$((x > y)[y := y - 1])[x := x + 1]$

$\equiv$ ⟨Definición de Sustitución $[y := y - 1]$⟩

$(x > y - 1)[x := x + 1]$

$\equiv$ ⟨Definición de Sustitución $[x := x + 1]$⟩

$x + 1 > y - 1$

$\equiv$ ⟨Aritmética - restar 1 a ambos lados⟩

$x > y - 2$

□

VII $\{Q\}$ x := y+1; y := x−1 $\{x>y\}$

$wp(x := y + 1; y := x - 1|x > y)$
$\equiv$ ⟨Axioma de Asignación x2⟩

$((x > y)[y := x - 1])[x := y + 1]$

$\equiv$ ⟨Definición de Sustitución $[y := x - 1]$⟩

$(x > x - 1)[x := y + 1]$

$\equiv$ ⟨Definición de Sustitución $[x := y + 1]$⟩

$y + 1 > y + 1 - 1$

$\equiv$ ⟨Aritmética - restar y a ambos lados⟩

$1 > 0$

$\equiv$ ⟨Aritmética - orden de los números⟩

`true`

□

Punto 2. Verificar la corrección del siguiente programa

```
var x, y : real

{true}

x,y := y*y, x*x;

if x ≥ y → x := x − y
 [] y ≥ x → y := y − x
fi

{x ≥ 0 ∧ y ≥ 0}
```

1. Cálculo de la precondición más débil:

$wp(S|R)$

$\equiv$ ⟨Axioma de asignación⟩

$wp(IF|R)[x, y := y * y, x * x]$

$\equiv$ ⟨Axioma de IF⟩

$(\exists i|1 \leq i \leq n : B_i) \wedge (\forall i|1 \leq i \leq n : \{Q \wedge B_i\}S_i\{R\})[x, y := y * y, x * x]$

$\equiv$ ⟨Definición de $\exists$ y $\forall$⟩

$((x \geq y \vee y \geq x) \wedge (\texttt{true} \wedge x \geq y \Rightarrow wp(x := x - y|x \geq 0 \wedge y \geq 0))\wedge$

$(\texttt{true} \wedge y \geq x \Rightarrow wp(y := y - x|x \geq 0 \wedge y \geq 0)))[x, y := y * y, x * x]$

$\equiv$ ⟨Axioma de asignación, Definición de sustitución⟩

$((x \geq y \vee y \geq x) \wedge (\texttt{true} \wedge x \geq y \Rightarrow x - y \geq 0 \wedge y \geq 0)\wedge$

$(\texttt{true} \wedge y \geq x \Rightarrow x \geq 0 \wedge y - x \geq 0))[x, y := y * y, x * x]$

$\equiv$ ⟨Definición de sustitución⟩

$(y^2 \geq x^2 \vee x^2 \geq y^2) \wedge (\texttt{true} \wedge y^2 \geq x^2 \Rightarrow y^2 - x^2 \geq 0 \wedge x^2 \geq 0)\wedge$

$(\texttt{true} \wedge x^2 \geq y^2 \Rightarrow y^2 \geq 0 \wedge x^2 - y^2 \geq 0)$

$\equiv$ ⟨Orden total de los números⟩

$\texttt{true} \wedge (\texttt{true} \wedge y^2 \geq x^2 \Rightarrow y^2 - x^2 \geq 0 \wedge x^2 \geq 0) \wedge (\texttt{true} \wedge x^2 \geq y^2 \Rightarrow y^2 \geq 0 \wedge x^2 - y^2 \geq 0)$

$\equiv$ ⟨Identidad del $\wedge$ x3⟩

$(y^2 \geq x^2 \Rightarrow y^2 - x^2 \geq 0 \wedge x^2 \geq 0) \wedge (x^2 \geq y^2 \Rightarrow y^2 \geq 0 \wedge x^2 - y^2 \geq 0)$

$\equiv$ ⟨Aritmética - suma y resta en las desigualdades⟩

$(y^2 \geq x^2 \Rightarrow y^2 \geq x^2 \wedge x^2 \geq 0) \wedge (x^2 \geq y^2 \Rightarrow y^2 \geq 0 \wedge x^2 \geq y^2)$

$\equiv$ ⟨Aritmética - todo real elevado al cuadrado es ≥ 0 x2, Identidad del $\wedge$ x2⟩

$(y^2 \geq x^2 \Rightarrow y^2 \geq x^2) \wedge (x^2 \geq y^2 \Rightarrow x^2 \geq y^2)$

$\equiv$ ⟨Reflexividad del $\Rightarrow$ x2, Identidad del $\wedge$⟩

`true`

□

2. Verificación del programa:

$\{Q\}S\{R\}$

$\equiv$ ⟨Definición de verificación de un programa⟩

$Q \Rightarrow wp(S|R)$

$\equiv$ ⟨Sustitución de Q y $wp(S|R)$⟩

`true` $\Rightarrow$ `true`

$\equiv$ ⟨`true` a la derecha del $\Rightarrow$⟩

`true`

□

Punto 3. Verificar la corrección del siguiente programa. Utilizar la variable r como cota. ¿Qué hace el programa?

```
var a,b,q,r : nat

{b > 0}

q,r := 0,a;

{b > 0 ∧ a = q * b + r}
do r ≥ b → q,r := q + 1, r − b
od

{a = q * b + r ∧ r < b}
```

• ¿Qué hace el programa?: Ejecuta el procedimiento de división de $\frac{a}{b}$ en donde q termina siendo el cociente y r el residuo.

Verificación de Ciclos:

1. Verificar {Q} INIC {P}.

$\{Q\}INIC\{P\}$

$\equiv$ ⟨Sustitución de Q, $INIC$, P⟩

$\{b > 0\}q, r := 0, a\{b > 0 \wedge a = q * b + r\}$

$\equiv$ $\langle$Definición de verificación de un programa$\rangle$

$b > 0 \Rightarrow wp(q, r := 0, a | b > 0 \wedge a = q * b + r)$

$\equiv$ $\langle$Axioma de asignación, Definición de sustitución$\rangle$

$b > 0 \Rightarrow b > 0 \wedge a = 0 * b + a$

$\equiv$ $\langle$Aritmética - Identidad del producto (0)$\rangle$

$b > 0 \Rightarrow b > 0 \wedge a = a$

$\equiv$ $\langle$Iguales a ambos lados del =, Identidad del $\wedge\rangle$

$b > 0 \Rightarrow b > 0$

$\equiv$ $\langle$Reflexividad del $\Rightarrow\rangle$

`true`

$\square$

2. Verificar $(P \wedge \neg BC \Rightarrow R)$

$P \wedge \neg BC \Rightarrow R$

$\equiv$ $\langle$Sustitución de P, BC y $R\rangle$

$b > 0 \wedge a = q * b + r \wedge \neg(r \geq b) \Rightarrow a = q * b + r \wedge r < b$

$\equiv$ $\langle$Negación de $\geq\rangle$

$b > 0 \wedge a = q * b + r \wedge r < b \Rightarrow a = q * b + r \wedge r < b$

Dem: Por hipótesis

Hip 1: $b > 0$

Hip 2: $a = q * b + r$

Hip 3: $r < b$

A Demostrar: $a = q * b + r \wedge r < b$

`true`

$\equiv$ $\langle$Hipótesis 2$\rangle$

$a = q * b + r$

$\equiv$ $\langle$Identidad del $\wedge\rangle$

$a = q * b + r \wedge \texttt{true}$

$\equiv$ $\langle$Hipótesis 3$\rangle$

$a = q * b + r \wedge r < b$

$\square$

3. Verificar $(\forall i | 1 \leq i \leq n : \{P \wedge B_i\} S_i \{P\})$

$(\forall i | 1 \leq i \leq n : \{P \wedge B_i\} S_i \{P\})$
$\equiv$ $\langle$Definición de $\forall$ - Única guarda, Sustitución P, B_1, S_1 y $P\rangle$

$\{b > 0 \wedge a = q * b + r \wedge r \geq b\} q, r := q + 1, r - b \{b > 0 \wedge a = q * b + r\}$

$\equiv$ $\langle$Definición de verificación de un programa$\rangle$

$b > 0 \wedge a = q * b + r \wedge r \geq b \Rightarrow wp(q, r := q + 1, r - b | b > 0 \wedge a = q * b + r)$

$\equiv$ $\langle$Axioma de asignación, Definición de Sustitución$\rangle$

$b > 0 \wedge a = q * b + r \wedge r \geq b \Rightarrow b > 0 \wedge a = (q + 1) * b + r - b$

$\equiv$ $\langle$Aritmética$\rangle$

$b > 0 \wedge a = q * b + r \wedge r \geq b \Rightarrow b > 0 \wedge a = q * b + b + r - b$

$\equiv$ $\langle$Aritmética$\rangle$

$b > 0 \wedge a = q * b + r \wedge r \geq b \Rightarrow b > 0 \wedge a = q * b + r$

Dem: Por hipótesis

Hip 1: $b > 0$

Hip 2: $a = q * b + r$

Hip 3: $r \geq b$

A Demostrar: $b > 0 \wedge a = q * b + r$

`true`
$\equiv$ $\langle$Hipótesis 1$\rangle$

$b > 0$

$\equiv$ $\langle$Identidad del $\wedge\rangle$

$b > 0 \wedge \texttt{true}$

$\equiv$ $\langle$Hipótesis 2$\rangle$

$b > 0 \wedge a = q * b + r$

$\square$

4. Verificar $(P \wedge BC) \Rightarrow t > 0$

$(P \wedge BC) \Rightarrow t > 0$
$\equiv$ $\langle$Sustitución P y BC, Sustitución de cota $t = r\rangle$

$b > 0 \wedge a = q * b + r \wedge r \geq b \Rightarrow r > 0$

Dem: Por hipótesis

Hip 1: $b > 0$

Hip 2: $a = q * b + r$

Hip 3: $r \geq b$

A Demostrar: $r > 0$

`true`

$\equiv$ $\langle$Hipótesis 3$\rangle$

$r \geq b$

$\equiv$ $\langle$Identidad del $\wedge\rangle$

$r \geq b \wedge \texttt{true}$

$\equiv$ $\langle$Hipótesis 1$\rangle$

$r \geq b \wedge b > 0$

$\equiv$ $\langle$Transitividad del $>$, Orden de los números$\rangle$

$r \geq 0 + 1$

$\equiv$ $\langle$Definición del $\geq\rangle$

$r > 0 \vee r = 1$

$\Rightarrow$ $\langle$Debilitamiento$\rangle$

$r > 0$

$\square$

5. Verificar $(\forall i | 1 \leq i \leq n : \{P \wedge B_i \wedge t = C\} S_i \{t < C\})$

$(\forall i | 1 \leq i \leq n : \{P \wedge B_i \wedge t = C\} S_i \{t < C\})$

$\equiv$ $\langle$Definición de $\forall$ - Única guarda, Sustitución P, B_1, S_1, Sustitución de cota $t = r\rangle$

$\{b > 0 \wedge a = q * b + r \wedge r \geq b \wedge r = C\} q, r := q + 1, r - b \{r < C\}$

$\equiv$ $\langle$Definición de verificación de un programa$\rangle$

$b > 0 \wedge a = q * b + r \wedge r \geq b \wedge r = C \Rightarrow wp(q, r := q + 1, r - b | r < C)$

$\equiv$ $\langle$Axioma de asignación, Definición de Sustitución$\rangle$

$b > 0 \wedge a = q * b + r \wedge r \geq b \wedge r = C \Rightarrow r - b < C$

Dem: Por hipótesis

Hip 1: $b > 0$

Hip 2: $a = q * b + r$

Hip 3: $r \geq b$

Hip 4: $r = C$

A Demostrar: $r - b < C$

En este caso se inicia por lo que se quiere demostrar

$r - b < C$

$\equiv \quad \langle$Hipótesis 4$\rangle$

$C - b < C$

$\equiv \quad \langle$Aritmética - restar C a ambos lados$\rangle$

$-b < 0$

$\equiv \quad \langle$Aritmética - multiplicar -1 a ambos lados$\rangle$

$b > 0$

$\equiv \quad \langle$Hipótesis 1$\rangle$

`true`

$\square$

Punto 4. Verificar la corrección del siguiente programa que dado un número N calcula dos números tales que su multiplicación da N. ¿Qué variable puede servir como cota? ¿El programa genera siempre los mismos números?

• ¿Que variable puede servir como cota?: La variable p puede servir como cota, ya que esta es la que determina cuando se sale del ciclo dada la variación de su valor

• ¿El programa genera siempre los mismos números?: Puede que no genere siempre los mismos números, ya que si ambas guardas del condicional se llegan a cumplir se accede a una de estas aleatoriamente.

```
var p,x,y,N : nat

{N > 0}

p,x,y:= N−1,1,1

{x > 0 ∧ y > 0 ∧ p ≥ 0 ∧ N = x ∗ y + p∧ (p mod x = 0 ∨ p mod y = 0)}
do p ≠ 0 →
      if p mod x = 0 → y, p := y + 1, p − x
      [] p mod y = 0 → x, p := x + 1, p − y
      fi
od

{x ∗ y = N}
```

Verificación de Ciclos:

1. Verificar {Q} INIC {P}.

$\{Q\}INIC\{P\}$

$\equiv \quad \langle$Definicion de Q, $INIC$, $P\rangle$

$\{N > 0\}p, x, y := N - 1, 1, 1\{x > 0 \land y > 0 \land p \geq 0 \land N = x * y + p \land (p \texttt{ mod } x = 0 \lor p \texttt{ mod } y = 0)\}$

$\equiv$ $\langle$Definición de verificación de un programa$\rangle$

$N > 0 \Rightarrow (x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + p \wedge (p \texttt{ mod } x = 0 \vee p \texttt{ mod } y = 0))[p, x, y := N - 1, 1, 1]$

$\equiv$ $\langle$Sustitución$\rangle$

$N > 0 \Rightarrow 1 > 0 \wedge 1 > 0 \wedge N - 1 \geq 0 \wedge N = 1 * 1 + N - 1 \wedge (N - 1 \texttt{ mod } 1 = 0 \vee N - 1 \texttt{ mod } 1 = 0))$

$\equiv$ $\langle$Orden Total de enteros,$a \texttt{ mod } 1 = 0$ para todo a, Identidad del $\wedge\rangle$

$N > 0 \Rightarrow N - 1 \geq 0 \wedge N = 1 * 1 + N - 1$

$\equiv$ $\langle$Aritmética - pasar el $+1$ a restar$\rangle$

$N > 0 \Rightarrow N - 1 \geq 0 \wedge N - 1 = N - 1$

$\equiv$ $\langle$Iguales a ambos lados del $=$, Identidad del $\wedge\rangle$

$N > 0 \Rightarrow N - 1 \geq 0$

$\equiv$ $\langle$Aritmética$\rangle$

$N > 0 \Rightarrow N \geq 1$

$\equiv$ $\langle$Orden de los enteros$\rangle$

`true`

$\square$

2. Verificar $P \wedge \neg BC \Rightarrow R$.

$P \wedge \neg BC \Rightarrow R$

$\equiv$ $\langle$Sustitución de P, BC y $R\rangle$

$x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + p \wedge (p \texttt{ mod } x = 0 \vee p \texttt{ mod } y = 0) \wedge \neg(p \neq 0) \Rightarrow x * y = N$

$\equiv$ $\langle$Definición de $\neq\rangle$

$x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + p \wedge (p \texttt{ mod } x = 0 \vee p \texttt{ mod } y = 0) \wedge p = 0 \Rightarrow x * y = N$

$\equiv$ $\langle$Sustitución de iguales por iguales $p := 0\rangle$

$x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + 0 \wedge (p \texttt{ mod } x = 0 \vee p \texttt{ mod } y = 0) \wedge p = 0 \Rightarrow x * y = N$

$\equiv$ $\langle$Debilitamiento$\rangle$

$N = x * y + 0 \Rightarrow x * y = N$

$\equiv$ $\langle$Aritmética (Modulo de la suma), Reordenando los iguales$\rangle$

$N = x * y \Rightarrow N = x * y$

$\equiv$ $\langle a \Rightarrow a \equiv \texttt{true}\rangle$

`true`

$\square$

3. Verificar $(\forall i | 1 \leq i \leq n : \{P \wedge B_i\} S_i \{P\})$

Dado que la invariante es muy extensa; se realiza la siguiente anotación para simplificar los pasos:

$P \equiv (x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + p \wedge (p \texttt{ mod } x = 0 \vee p \texttt{ mod } y = 0))$

$(\forall i | 1 \leq i \leq n : \{P \wedge B_i\} S_i \{P\})$

$\equiv$ $\langle$Unica Guarda$\rangle$

$\{x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + p \wedge (p \texttt{ mod } x = 0 \vee p \texttt{ mod } y = 0) \wedge p \neq 0\}$

```
if p  mod  x = 0 → y,p := y+1, p−x
[] p  mod  y = 0 → x,p := x+1, p−y
fi
```

$\{x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + p \wedge (p \texttt{ mod } x = 0 \vee p \texttt{ mod } y = 0)\}$

$\equiv$ $\langle$Verificación Para Condicionales$\rangle$

3.1 Verificar $Q \Rightarrow B_1 \vee B_2$

$Q \Rightarrow B_1 \vee B_2$

$\equiv$ $\langle$Definición de la tripla$\rangle$

$x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + p \wedge (p \texttt{ mod } x = 0 \vee p \texttt{ mod } y = 0) \wedge p \neq 0 \Rightarrow (p \texttt{ mod } x = 0 \vee p \texttt{ mod } y = 0)$

$\equiv$ $\langle$Debilitamiento$\rangle$

$(p \texttt{ mod } x = 0 \vee p \texttt{ mod } y = 0) \Rightarrow (p \texttt{ mod } x = 0 \vee p \texttt{ mod } y = 0)$

$\equiv$ $\langle$Reflexividad del $\Rightarrow\rangle$

`true`

$\square$

3.2 Verificar $(\forall i | 1 \leq i \leq n : \{P \wedge p \neq 0 \wedge B_i\} S_i \{P\}))$

3.2.1 $\{P \wedge p \neq 0 \wedge p \texttt{ mod } x = 0\} y, p := y + 1, p - x \{P\})$

$\{P \wedge p \neq 0 \wedge p \texttt{ mod } x = 0\} y, p := y + 1, p - x \{P\})$

$\equiv$ $\langle$Corrección con wp$\rangle$

$P \wedge p \neq 0 \wedge p \texttt{ mod } x = 0 \Rightarrow (x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + p \wedge$

$(p \texttt{ mod } x = 0 \vee p \texttt{ mod } y = 0))[y, p := y + 1, p - x]$

$\equiv$ $\langle$Sustitución$\rangle$

$P \wedge p \neq 0 \wedge p \texttt{ mod } x = 0 \Rightarrow (x > 0 \wedge y + 1 > 0 \wedge p - x \geq 0 \wedge N = x * (y + 1) + (p - x) \wedge$

$((p - x) \texttt{ mod } x = 0 \vee (p - x) \texttt{ mod } y + 1 = 0))$

$\equiv$ $\langle x > 0 \Rightarrow x > 0$, Por orden de enteros $y > 0 \Rightarrow y + 1 > 0, \wedge - Identidad\rangle$

$P \wedge p \neq 0 \wedge p \texttt{ mod } x = 0 \Rightarrow (p - x \geq 0 \wedge N = x * (y + 1) + (p - x) \wedge ((p - x) \texttt{ mod } x = 0 \vee (p - x) \texttt{ mod } y + 1 = 0))$

$\equiv$ $\langle p \texttt{ mod } x = 0 \Rightarrow p \pm x \texttt{ mod } x = 0, \wedge - Identidad\rangle$

$P \wedge p \neq 0 \wedge p \texttt{ mod } x = 0 \Rightarrow (p - x \geq 0 \wedge N = x * (y + 1) + (p - x))$

$\equiv$ $\langle$Aritmética$\rangle$

$P \wedge p \neq 0 \wedge p \ \texttt{mod} \ x = 0 \Rightarrow (p - x \geq 0 \wedge N = x * y + x + p - x)$

$\equiv \quad \langle \text{Aritmética} \rangle$

$P \wedge p \neq 0 \wedge p \ \texttt{mod} \ x = 0 \Rightarrow (p - x \geq 0 \wedge N = x * y + p)$

$\equiv \quad \langle N = x * y + p \Rightarrow N = x * y + p, \wedge - Identidad \rangle$

$x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + p \wedge (p \ \texttt{mod} \ x = 0 \vee p \ \texttt{mod} \ y = 0) \wedge p \neq 0 \wedge p \ \texttt{mod} \ x = 0 \Rightarrow p - x \geq 0$

$\equiv \quad \langle p \ \texttt{mod} \ x = 0 \Rightarrow p \geq x \vee p = 0, p \neq 0, p \geq x \Rightarrow p - x \geq 0 \rangle$

$x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + p \wedge (p \ \texttt{mod} \ x = 0 \vee p \ \texttt{mod} \ y = 0) \wedge p \neq 0 \wedge p \ \texttt{mod} \ x = 0 \Rightarrow \texttt{true}$

$\equiv \quad \langle \texttt{true}$ a la derecha del $\Rightarrow \rangle$

`true`

□

3.2.2 $\{P \wedge p \neq 0 \wedge p \ \texttt{mod} \ y = 0\} x, p := x + 1, p - y \{P\})$

$\{P \wedge p \neq 0 \wedge p \ \texttt{mod} \ y = 0\} x, p := x + 1, p - y \{P\})$

$\equiv \quad \langle \text{Corrección con wp} \rangle$

$P \wedge p \neq 0 \wedge p \ \texttt{mod} \ y = 0 \Rightarrow (x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + p \wedge$

$(p \ \texttt{mod} \ x = 0 \vee p \ \texttt{mod} \ y = 0))[y, p : x + 1, p - y]$

$\equiv \quad \langle \text{Sustitución} \rangle$

$P \wedge p \neq 0 \wedge p \ \texttt{mod} \ y = 0 \Rightarrow (x + 1 > 0 \wedge y > 0 \wedge p - y \geq 0 \wedge N = (x + 1) * y + (p - y) \wedge$

$((p - y) \ \texttt{mod} \ x + 1 = 0 \vee (p - y) \ \texttt{mod} \ y = 0))$

$\equiv \quad \langle y > 0 \Rightarrow y > 0,$ Por orden de enteros $x > 0 \Rightarrow x + 1 > 0, \wedge - Identidad \rangle$

$P \wedge p \neq 0 \wedge p \ \texttt{mod} \ y = 0 \Rightarrow (p - y \geq 0 \wedge N = (x + 1) * y + (p - y) \wedge ((p - y) \ \texttt{mod} \ x + 1 = 0 \vee (p - y) \ \texttt{mod} \ y = 0))$

$\equiv \quad \langle p \ \texttt{mod} \ y = 0 \Rightarrow p \pm y \ \texttt{mod} \ y = 0, \wedge - Identidad \rangle$

$P \wedge p \neq 0 \wedge p \ \texttt{mod} \ y = 0 \Rightarrow (p - y \geq 0 \wedge N = (x + 1) * y + (p - y))$

$\equiv \quad \langle \text{Aritmética} \rangle$

$P \wedge p \neq 0 \wedge p \ \texttt{mod} \ y = 0 \Rightarrow (p - y \geq 0 \wedge N = x * y + y + p - y)$

$\equiv \quad \langle \text{Aritmética} \rangle$

$P \wedge p \neq 0 \wedge p \ \texttt{mod} \ y = 0 \Rightarrow (p - y \geq 0 \wedge N = x * y + p)$

$\equiv \quad \langle N = x * y + p \Rightarrow N = x * y + p, \wedge - Identidad \rangle$

$x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + p \wedge (p \ \texttt{mod} \ x = 0 \vee p \ \texttt{mod} \ y = 0) \wedge p \neq 0 \wedge p \ \texttt{mod} \ y = 0 \Rightarrow p - y \geq 0$

$\equiv \quad \langle p \ \texttt{mod} \ y = 0 \Rightarrow p \geq y \vee p = 0, p \neq 0, p \geq y \Rightarrow p - y \geq 0 \rangle$

$x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + p \wedge (p \ \texttt{mod} \ x = 0 \vee p \ \texttt{mod} \ y = 0) \wedge p \neq 0 \wedge p \ \texttt{mod} \ y = 0 \Rightarrow \texttt{true}$

$\equiv \quad \langle \texttt{true}$ a la derecha del $\Rightarrow \rangle$

`true`

$\square$

4. Verificar $(P \wedge BC) \Rightarrow t > 0$, Usando como cota la variable p.

$(P \wedge BC) \Rightarrow t > 0$
$\equiv \quad \langle$Definición de P, BC y t$\rangle$

$x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + p \wedge (p \ \texttt{mod} \ x = 0 \vee p \ \texttt{mod} \ y = 0) \wedge p \neq 0 \Rightarrow p > 0$

$\equiv \quad \langle p \neq 0 \wedge p \geq 0 \equiv p > 0 \rangle$

$x > 0 \wedge y > 0 \wedge N = x * y + p \wedge (p \ \texttt{mod} \ x = 0 \vee p \ \texttt{mod} \ y = 0) \wedge p > 0 \Rightarrow p > 0$

$\equiv \quad \langle$Debilitamiento$\rangle$

$p > 0 \Rightarrow p > 0$

$\equiv \quad \langle$Reflexividad del $\Rightarrow\rangle$

`true`

$\square$

5. Verificar $(\forall i | 1 \leq i \leq n : \{P \wedge B_i \wedge t = C\} S_i \{t < C\})$

Dado que la invariante es muy extensa; se realiza la siguiente anotación para simplificar los pasos:

$P \equiv (x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + p \wedge (p \ \texttt{mod} \ x = 0 \vee p \ \texttt{mod} \ y = 0))$

$(\forall i | 1 \leq i \leq n : \{P \wedge B_i \wedge t = C\} S_i \{t < C\})$
$\equiv \quad \langle$Definición con la única guarda$\rangle$

$\{P \wedge p \neq 0 \wedge p = C\}$
```
if p  mod  x = 0 → y,p := y+1, p−x
 [] p  mod  y = 0 → x,p := x+1, p−y
fi
```
$\{p < C\}$

$\equiv \quad \langle$Verificación de Condicionales$\rangle$
5.1 $x > 0 \wedge y > 0 \wedge p \geq 0 \wedge N = x * y + p \wedge (p \ \texttt{mod} \ x = 0 \vee p \ \texttt{mod} \ y = 0) \wedge p \neq 0 \wedge p = C \Rightarrow (p \ \texttt{mod} \ x = 0 \vee p \ \texttt{mod} \ y = 0)$
$\equiv \quad \langle$Debilitamiento$\rangle$
$(p \ \texttt{mod} \ x = 0 \vee p \ \texttt{mod} \ y = 0) \Rightarrow (p \ \texttt{mod} \ x = 0 \vee p \ \texttt{mod} \ y = 0)$

$\equiv \quad \langle$Reflexividad del $\Rightarrow\rangle$

`true`

$\square$

5.2 $(\forall i | 1 \leq i \leq n : \{P \wedge p \neq 0 \wedge p = C \wedge B_i\} S_i \{p < C\})$

5.2.1 $(\{P \wedge p \neq 0 \wedge p = C \wedge p \ \texttt{mod} \ x = 0\} y, p := y + 1, p - x \{p < C\})$

$(\{P \wedge p \neq 0 \wedge p = C \wedge p \texttt{ mod } x = 0\}y, p := y+1, p-x\{p < C\})$

$\equiv$ $\langle$Verificacion con wp$\rangle$

$P \wedge p \neq 0 \wedge p = C \wedge p \texttt{ mod } x = 0 \Rightarrow (p < C)[y, p := y+1, p-x]$

$\equiv$ $\langle$Sustitucion$\rangle$

$P \wedge p \neq 0 \wedge p = C \wedge p \texttt{ mod } x = 0 \Rightarrow p - x < C$

$\equiv$ $\langle$Debilitamiento$\rangle$

$x > 0 \wedge p = C \Rightarrow p - x < C$

$\equiv$ $\langle$Al x ser $>$0, al restarle algo a p, sera menor que antes$\rangle$

`true`

$\square$

5.2.2 $(\{P \wedge p \neq 0 \wedge p = C \wedge p \texttt{ mod } y = 0\}x, p := x+1, p-y\{p < C\})$

$(\{P \wedge p \neq 0 \wedge p = C \wedge p \texttt{ mod } y = 0\}x, p := x+1, p-y\{p < C\})$

$\equiv$ $\langle$Verificacion con wp$\rangle$

$P \wedge p \neq 0 \wedge p = C \wedge p \texttt{ mod } y = 0 \Rightarrow (p < C)[x, p := x+1, p-y]$

$\equiv$ $\langle$Sustitucion$\rangle$

$P \wedge p \neq 0 \wedge p = C \wedge p \texttt{ mod } y = 0 \Rightarrow p - y < C$

$\equiv$ $\langle$Debilitamiento$\rangle$

$y > 0 \wedge p = C \Rightarrow p - y < C$

$\equiv$ $\langle$Al y ser $>$0, al restarle x a p, p sera menor que antes$\rangle$

`true`

$\square$

Punto 5. Verificar la corrección del siguiente programa que calcula el índice de un arreglo no vacío de números naturales en el que se encuentra el máximo

```
var n, i, r : nat
var a : array [0,N) of nat

{N>0}

i,r := 1,0

{0 ≤ r < i ≤ N ∧ (∀k|0 ≤ k < i : a[k] ≤ a[r])}
do  i < N ∧ a[i] ≥ a[r] → r,i := i,i+1
 [] i < N ∧ a[i] ≤ a[r] → i := i+1
od
```

$\{0 \leq r < N \wedge (\forall k | 0 \leq k < N : a[k] \leq a[r])\}$

Verificación de Ciclos:

1. Verificar {Q} INIC {P}.

$\{N > 0\} i, r := 1, 0 \{0 \leq r < i \leq N \wedge (\forall k | 0 \leq k < i : a[k] \leq a[r])\}$

$\equiv$ $\langle$Verificacion con Wp$\rangle$

$N > 0 \Rightarrow (0 \leq r < i \leq N \wedge (\forall k | 0 \leq k < i : a[k] \leq a[r]))[i, r := 1, 0]$

$\equiv$ $\langle$Sustitución$\rangle$

$N > 0 \Rightarrow (0 \leq 0 < 1 \leq N \wedge (\forall k | 0 \leq k < 1 : a[k] \leq a[0]))$

$\equiv$ $\langle$Orden de enteros y $N > 0$$\rangle$

$N > 0 \Rightarrow (\texttt{true} \wedge (\forall k | 0 \leq k < 1 : a[k] \leq a[0]))$

$\equiv$ $\langle$Punto fijo$\rangle$

$N > 0 \Rightarrow a[0] \leq a[0]$

$\equiv$ $\langle$Mismo elemento$\rangle$

`true`

$\square$

2. Verificar $P \wedge \neg BC \Rightarrow R$.

Dado que la invariante es muy extensa; se realiza la siguiente anotación para simplificar los pasos:

$P \equiv 0 \leq r < i \leq N \wedge (\forall k | 0 \leq k < i : a[k] \leq a[r])$

$P \wedge \neg BC \Rightarrow R$

$\equiv$ $\langle$Definición de P, BC y R$\rangle$

$P \wedge \neg((i < N \wedge a[i] \geq a[r]) \vee (i < N \wedge a[i] \leq a[r])) \Rightarrow 0 \leq r < N \wedge (\forall k | 0 \leq k < N : a[k] \leq a[r])$

$\equiv$ $\langle r < i \Rightarrow r < N$ Según la invariante$\rangle$

$P \wedge \neg((i < N \wedge a[i] \geq a[r]) \vee (i < N \wedge a[i] \leq a[r])) \Rightarrow \texttt{true} \wedge (\forall k | 0 \leq k < N : a[k] \leq a[r])$

$\equiv$ $\langle$De Morgan, varias veces$\rangle$

$P \wedge (\neg(i < N) \vee \neg(a[i] \geq a[r])) \wedge (\neg(i < N) \vee \neg(a[i] \leq a[r])) \Rightarrow \texttt{true} \wedge (\forall k | 0 \leq k < N : a[k] \leq a[r])$

$\equiv$ $\langle$Distributividad$\rangle$

$P \wedge (\neg(i < N) \vee (\neg(a[i] \geq a[r]) \wedge \neg(a[i] \leq a[r])) \Rightarrow \texttt{true} \wedge (\forall k | 0 \leq k < N : a[k] \leq a[r])$

$\equiv$ $\langle$Negacion de desigualdades$\rangle$

$P \wedge ((i \geq N) \vee ((a[i] < a[r]) \wedge (a[i] > a[r])) \Rightarrow \texttt{true} \wedge (\forall k | 0 \leq k < N : a[k] \leq a[r])$

$\equiv$ $\langle$Orden de enteros, $\vee$-Identidad$\rangle$

$P \wedge i \geq N \Rightarrow \texttt{true} \wedge (\forall k | 0 \leq k < N : a[k] \leq a[r])$

$\equiv \quad \langle \text{Debilitamiento} \rangle$

$i \leq N \wedge (\forall k | 0 \leq k < i : a[k] \leq a[r]) \wedge i \geq N \Rightarrow (\forall k | 0 \leq k < N : a[k] \leq a[r])$

$\equiv \quad \langle i \leq N \wedge \ i \geq N \Rightarrow i = N \rangle$

$(\forall k | 0 \leq k < i : a[k] \leq a[r]) \wedge i = N \Rightarrow (\forall k | 0 \leq k < N : a[k] \leq a[r])$

$\equiv \quad \langle \text{Sustitucion de iguales} \rangle$

$(\forall k | 0 \leq k < N : a[k] \leq a[r]) \Rightarrow (\forall k | 0 \leq k < N : a[k] \leq a[r])$

$\equiv \quad \langle \text{Reflexividad del } \Rightarrow \rangle$

`true`

$\square$

3. Verificar $(\forall i | 1 \leq i \leq n : \{P \wedge B_i\} S_i \{P\})$

Dado que la invariante es muy extensa; se realiza la siguiente anotación para simplificar los pasos:

$P \equiv 0 \leq r < i \leq N \wedge (\forall k | 0 \leq k < i : a[k] \leq a[r])$

3.1 $\{P \wedge i < N \wedge a[i] \geq a[r]\} r, i := i, i+1 \{P\}$

$\{P \wedge i < N \wedge a[i] \geq a[r]\} r, i := i, i+1 \{P\}$

$\equiv \quad \langle \text{Verificación con wp} \rangle$

$P \wedge i < N \wedge a[i] \geq a[r] \Rightarrow (P)[r, i := i, i+1]$

$\equiv \quad \langle \text{Sustitución} \rangle$

$P \wedge i < N \wedge a[i] \geq a[r] \Rightarrow 0 \leq i < i+1 \leq N \wedge (\forall k | 0 \leq k < i+1 : a[k] \leq a[i])$

$\equiv \quad \langle \text{Orden de enteros, } \wedge\text{-Identidad} \rangle$

$0 \leq r < i \leq N \wedge (\forall k | 0 \leq k < i : a[k] \leq a[r]) \wedge i < N \wedge a[i] \geq a[r] \Rightarrow (\forall k | 0 \leq k < i+1 : a[k] \leq a[i])$

$\equiv \quad \langle \text{Debilitamiento} \rangle$

$(\forall k | 0 \leq k < i : a[k] \leq a[r]) \wedge a[i] \geq a[r] \Rightarrow (\forall k | 0 \leq k < i+1 : a[k] \leq a[i])$

$\equiv \quad \langle \text{Partir rango por derecha} \rangle$

$(\forall k | 0 \leq k < i : a[k] \leq a[r]) \wedge a[i] \geq a[r] \Rightarrow (\forall k | 0 \leq k < i : a[k] \leq a[i]) \wedge a[i] \leq a[i]$

$\equiv \quad \langle \text{Mismo elemento} \rangle$

$(\forall k | 0 \leq k < i : a[k] \leq a[r]) \wedge a[i] \geq a[r] \Rightarrow (\forall k | 0 \leq k < i : a[k] \leq a[i])$

$\leq \quad \langle a[i] \geq a[r], \text{ Debilitamiento} \rangle$

$(\forall k | 0 \leq k < i : a[k] \leq a[i]) \Rightarrow (\forall k | 0 \leq k < i : a[k] \leq a[i])$

$\equiv \quad \langle \text{Reflexividad del } \Rightarrow \rangle$

`true`

$\square$

3.2 $\{P \wedge i < N \wedge a[i] \leq a[r]\} i := i+1 \{P\}$

$\{P \wedge i < N \wedge a[i] \leq a[r]\} i := i+1 \{P\}$

$\equiv$ $\langle$Verificacion con WP$\rangle$

$P \wedge i < N \wedge a[i] \leq a[r] \Rightarrow (0 \leq r < i \leq N \wedge (\forall k | 0 \leq k < i : a[k] \leq a[r]))[i := i+1]$

$\equiv$ $\langle$Sustitucion$\rangle$

$P \wedge i < N \wedge a[i] \leq a[r] \Rightarrow 0 \leq r < i+1 \leq N \wedge (\forall k | 0 \leq k < i+1 : a[k] \leq a[r])$

$\equiv$ $\langle i < N \Rightarrow i+1 \leq N$, Transitividad del $<$, $\wedge$-Identidad$\rangle$

$P \wedge i < N \wedge a[i] \leq a[r] \Rightarrow (\forall k | 0 \leq k < i+1 : a[k] \leq a[r])$

$\equiv$ $\langle$Partir rango por derecha, debilitamiento$\rangle$

$(\forall k | 0 \leq k < i : a[k] \leq a[r]) \wedge a[i] \leq a[r] \Rightarrow (\forall k | 0 \leq k < i : a[k] \leq a[r]) \wedge a[i] \leq a[r]$

$\equiv$ $\langle$Reflexividad del $\Rightarrow\rangle$

`true`

$\square$

4.Verificar $(P \wedge BC) \Rightarrow t > 0$, Usando como cota la funcion t = N-i

Dado que la invariante es muy extensa; se realiza la siguiente anotación para simplificar los pasos:

$P \equiv 0 \leq r < i \leq N \wedge (\forall k | 0 \leq k < i : a[k] \leq a[r])$

$(P \wedge BC) \Rightarrow t > 0$

$\equiv$ $\langle$Definicion de P, BC y t$\rangle$

$P \wedge ((i < N \wedge a[i] \geq a[r]) \vee (i < N \wedge a[i] \leq a[r])) \Rightarrow N - i > 0$

$\equiv$ $\langle$Distributividad $\wedge/\vee\rangle$

$P \wedge i < N \wedge (a[i] \geq a[r] \vee a[i] \leq a[r]) \Rightarrow N - i > 0$

$\equiv$ $\langle$Debilitamiento$\rangle$

$i < N \Rightarrow N - i > 0$

$\equiv$ $\langle$Aritmetica$\rangle$

$0 < N - i \Rightarrow N - i > 0$

$\equiv$ $\langle$Reorganizando desigualdades$\rangle$

$N - i > 0 \Rightarrow N - i > 0$

$\equiv$ $\langle$Reflexividad del $\Rightarrow\rangle$

`true`

$\square$

5. Verificar $(\forall i | 1 \leq i \leq n : \{P \wedge B_i \wedge t = C\} S_i \{t < C\})$

Dado que la invariante es muy extensa; se realiza la siguiente anotación para simplificar los pasos:

$P \equiv 0 \leq r < i \leq N \wedge (\forall k | 0 \leq k < i : a[k] \leq a[r])$

5.1 $\{P \wedge i < N \wedge a[i] \geq a[r] \wedge N - i = C\} r, i := i, i+1 \{N - i < C\}$
$\equiv$ $\langle$Verificacion con WP$\rangle$
$P \wedge i < N \wedge a[i] \geq a[r] \wedge N - i = C \Rightarrow (N - i < C)[r, i := i, i+1]$

$\equiv$ $\langle$Sustitucion$\rangle$

$P \wedge i < N \wedge a[i] \geq a[r] \wedge N - i = C \Rightarrow N - (i+1) < C$

$\equiv$ $\langle$Aritmetica$\rangle$

$P \wedge i < N \wedge a[i] \geq a[r] \wedge N - i = C \Rightarrow N - i - 1 < C$

$\equiv$ $\langle a - 1 < a \rangle$

$P \wedge i < N \wedge a[i] \geq a[r] \wedge N - i = C \Rightarrow$ `true`

$\equiv$ $\langle$`true` a la derecha del $\Rightarrow\rangle$

`true`

$\square$

5.2 $\{P \wedge i < N \wedge a[i] \leq a[r] \wedge N - i = C\} i := i+1 \{N - i < C\}$
$\equiv$ $\langle$Verificacion con WP$\rangle$
$P \wedge i < N \wedge a[i] \leq a[r] \wedge N - i = C \Rightarrow (N - i < C)[i := i+1]$

$\equiv$ $\langle$Sustitucion$\rangle$

$P \wedge i < N \wedge a[i] \leq a[r] \wedge N - i = C \Rightarrow N - (i+1) < C$

$\equiv$ $\langle$Aritmetica$\rangle$

$P \wedge i < N \wedge a[i] \leq a[r] \wedge N - i = C \Rightarrow N - i - 1 < C$

$\equiv$ $\langle a - 1 < a \rangle$

$P \wedge i < N \wedge a[i] \leq a[r] \wedge N - i = C \Rightarrow$ `true`

$\equiv$ $\langle$`true` a la derecha del $\Rightarrow\rangle$

`true`

$\square$