Ejercicios Práctico 7

1)a)Section Name

Primero realicemos la especificacion del programa:

$$\{P : N \geq 0\}$$
$$S$$
$$\{Q : x^3 + x \geq N \wedge \langle \forall i : 0 \leq i < x : i^3 + i < N \rangle\}$$

Teniendo en cuenta la tecnica de tomar el termino de una conjuncion, tenemos que:

$$B \equiv x^3 + x < N$$
$$I \equiv \langle \forall i : 0 \leq i < x : i^3 + i < N \rangle$$

Estructura del programa:

$$\{N \geq 0\}$$
$$S_0$$
$$\{\langle \forall i : 0 \leq i < x : i^3 + i < N \rangle\}$$
$$do\ x^3 + x < N \rightarrow$$
$$\quad \{\langle \forall i : 0 \leq i < x : i^3 + i < N \rangle \wedge x^3 + x < N\}$$
$$\quad S_1$$
$$\quad \{\langle \forall i : 0 \leq i < x : i^3 + i < N \rangle\}$$
$$od$$
$$\{x^3 + x \geq N \wedge \langle \forall i : 0 \leq i < x : i^3 + i < N \rangle\}$$

Primero derivemos S_0:

$$\{N \geq 0\}$$
$$S_0$$
$$\{\langle \forall i : 0 \leq i < x : i^3 + i < N \rangle\}$$

En la hipotesis no aparece x así que tenemos que encontrar alguna x de la forma

$x := E$. Para ello asumimos la hipotesis y realizamos la wp:

$$
\begin{aligned}
&wp.(x := E).(\langle \forall i : 0 \leq i < x : i^3 + i < N\rangle)\\
&\equiv \{\text{Def wp asignacion}\}\\
&\langle \forall i : 0 \leq i < E : i^3 + i < N\rangle\\
&\equiv \{\text{Elijo } E = 0\}\\
&\langle \forall i : 0 \leq i < 0 : i^3 + i < N\rangle\\
&\equiv \{\text{Rango vacio}\}\\
&True
\end{aligned}
$$

Por ende tenemos que $S_0 \equiv x := 0$.

Ahora derivemos el cuerpo del bucle:

$$
\begin{aligned}
&\{\langle \forall i : 0 \leq i < x : i^3 + i < N\rangle \wedge x^3 + x < N\}\\
&S_1\\
&\{\langle \forall i : 0 \leq i < x : i^3 + i < N\rangle\}
\end{aligned}
$$

Probemos con $x := x + 1$. Supongamos la precondicion y veamos la wp:

$$
\begin{aligned}
&wp.(x := x+1).(\langle \forall i : 0 \leq i < x : i^3 + i < N\rangle)\\
&\equiv \{\text{Def wp asignacion}\}\\
&\langle \forall i : 0 \leq i < x+1 : i^3 + i < N\rangle\\
&\equiv \{\text{Aritmetica}\}\\
&\langle \forall i : 0 \leq i \leq x : i^3 + i < N\rangle\\
&\equiv \{\text{Aritmetica}\}\\
&\langle \forall i : 0 \leq i < x \vee i = x : i^3 + i < N\rangle\\
&\equiv \{\text{Particion de rango y rango unitario}\}\\
&\langle \forall i : 0 \leq i < x : i^3 + i < N\rangle \wedge x^3 + x < N\\
&\equiv \{\text{Por primer termino de la suposicion}\}\\
&True \wedge x^3 + x < N\\
&\equiv \{\text{Por segundo termino de la suposicion}\}\\
&True \wedge True\\
&\equiv \{\text{Logica}\}\\
&True
\end{aligned}
$$

Por ende, tenemos que $S_1 \equiv x := x + 1$.

Resultado final:

$$
\begin{array}{l}
\{N \geq 0\} \\
x := 0 \\
\{\langle \forall i : 0 \leq i < x : i^3 + i < N \rangle\} \\
do\ x^3 + x < N \rightarrow \\
\quad \{\langle \forall i : 0 \leq i < x : i^3 + i < N \rangle \wedge x^3 + x < N\} \\
\quad x := x + 1 \\
\quad \{\langle \forall i : 0 \leq i < x : i^3 + i < N \rangle\} \\
od \\
\{x^3 + x \geq N \wedge \langle \forall i : 0 \leq i < x : i^3 + i < N \rangle\}
\end{array}
$$

2) Estructura del programa:

$$
\begin{array}{l}
\{N \geq 0\} \\
S_0 \\
\{I\} \\
do\ B \rightarrow \\
\quad \{I \wedge B\} \\
\quad S_1 \\
\quad \{I\} \\
od \\
\{s = \langle \Sigma i : 0 \leq i < N : A.i \rangle\}
\end{array}
$$

Determinamos el invariante: Para determinar el invariante hacemos uso de la tecnica de reemplazo de constante por variable, obteniendo lo siguiente:

$$I : s = \langle \Sigma i : 0 \leq i < k : A.i \rangle \wedge 0 \leq k \leq N$$

Veamos si $P \Rightarrow I$:

$$
\begin{array}{l}
\{P : N \geq 0\} \\
S_0 \\
\{I : s = \langle \Sigma i : 0 \leq i < k : A.i \rangle \wedge 0 \leq k \leq N\}
\end{array}
$$

S_0 no puede ser skip ya que s no aparece en la precondicion. Probemos encontrar un S_0 de la forma $s, k := E, F$ suponiendo la precondicion y viendo la wp de la asignacion:

$$
\begin{aligned}
&P \Rightarrow wp.(s,k := E,F).(s = \langle \Sigma i : 0 \leq i < k : A.i \rangle \wedge 0 \leq k \leq N)\\
&\equiv \{\text{Suponemos P}\}\\
&wp.(s,k := E,F).(s = \langle \Sigma i : 0 \leq i < k : A.i \rangle \wedge 0 \leq k \leq N)\\
&\equiv \{\text{Def wp asignacion}\}\\
&E = \langle \Sigma i : 0 \leq i \leq F : A.i \rangle \wedge 0 \leq F \leq N\\
&\equiv \{\text{Elijo F=0}\}\\
&E = \langle \Sigma i : 0 \leq i \leq 0 : A.i \rangle \wedge 0 \leq 0 \leq N\\
&\equiv \{\text{Por suposicion } N \geq 0\}\\
&E = \langle \Sigma i : 0 \leq i \leq 0 : A.i \rangle\\
&\equiv \{\text{Rango vacio}\}\\
&E = 0\\
&\equiv \{\text{Elijo E=0}\}\\
&0 = 0\\
&\equiv \{\text{Logica}\}\\
&True
\end{aligned}
$$

Por ende tenemos que $S_0 \equiv s, k := 0, 0$.

Finalizacion: Veamos si se cumple $I \wedge \neg B \Rightarrow Q$:

$$
\begin{aligned}
&(s = \langle \Sigma i : 0 \leq i < k : A.i \rangle \wedge 0 \leq k \leq N) \wedge \neg(k \neq N)\\
&\Rightarrow s = \langle \Sigma i : 0 \leq i \leq N : A.i \rangle\\
&\equiv \{\text{Logica}\}\\
&(s = \langle \Sigma i : 0 \leq i < k : A.i \rangle \wedge 0 \leq k \leq N) \wedge k = N\\
&\Rightarrow s = \langle \Sigma i : 0 \leq i < N : A.i \rangle\\
&\equiv \{\text{Suponemos precedente y demostramos consecuente}\}\\
&s = \langle \Sigma i : 0 \leq i < N : A.i \rangle\\
&\equiv \{\text{Por suposicion } k = N\}\\
&s = \langle \Sigma i : 0 \leq i < k : A.i \rangle\\
&\equiv \{\text{Por suposicion de s}\}\\
&True
\end{aligned}
$$

Por ende, obtuvimos que $B \equiv k \neq N$

Programa hasta ahora:

$$
\begin{array}{l}
\{N \geq 0\} \\
s, k := 0, 0 \\
\{I : s = \langle \Sigma i : 0 \leq i < k : A.i \rangle \wedge 0 \leq k \leq N\} \\
do\ k \neq N \rightarrow \\
\quad \{I \wedge B\} \\
\quad S_1 \\
\quad \{I\} \\
od \\
\{s = \langle \Sigma i : 0 \leq i < N : A.i \rangle\}
\end{array}
$$

Cota candidata: $N - k$

Cuerpo del bucle:

$$
\begin{array}{l}
\{I \wedge B\} \\
S_1 \\
\{I\}
\end{array}
$$

Veamos si podemos encontrar un S_1 de la forma $s, k := E, k + 1$, para ello supongamos $I \wedge (k \neq N)$ y veamos la wp:

$wp.(s, k := E, k+1).(s = \langle \Sigma i : 0 \leq i < k : A.i \rangle \wedge 0 \leq k \leq N)$
$\equiv$ {Def wp asignacion}
$(E = \langle \Sigma i : 0 \leq i < (k+1) : A.i \rangle \wedge 0 \leq (k+1) \leq N)$
$\equiv$ {Aritmetica}
$(E = \langle \Sigma i : 0 \leq i < (k+1) : A.i \rangle \wedge 0 \leq (k+1) \leq N)$
$\equiv$ {Aritmetica}
$(E = \langle \Sigma i : 0 \leq i < k \vee i = k : A.i \rangle \wedge 0 \leq (k+1) \leq N)$
$\equiv$ {Suposicion $k \neq N \wedge 0 \leq k \leq N$}
$(E = \langle \Sigma i : 0 \leq i < k \vee i = k : A.i \rangle$
$\equiv$ {Particion de rango y rango unitario}
$(E = \langle \Sigma i : 0 \leq i < k : A.i \rangle + A.k$
$\equiv$ {Por suposicion s}
$E = s + A.k$
$\equiv$ {Elegimos $E = s + A.k$}
$s + A.k = s + A.k$
$\equiv$ {Logica}
$True$

Demostracion de que la cota es positiva:

$s = \langle \Sigma i : 0 \leq i < k : A.i \rangle \wedge 0 \leq k \leq N \wedge k \neq N$
$\Rightarrow N - k \geq 0$
$\equiv$ {Asumimos precedente y demostramos consecuente}
$N - k \geq 0$
$\equiv$ {Aritmetica}
$N \geq k$
$\equiv$ {Suposicion $0 \leq k \leq N \wedge k \neq N$}
$True$

Demostracion de que la cota disminiye:

$$
\begin{aligned}
&\{s = \langle \Sigma i : 0 \leq i < k : A.i \rangle \wedge 0 \leq k \leq N \wedge k \neq N \wedge N - k = T\} \\
&s, k := s + A.k, k + 1 \\
&\{N - k < T\} \\
&\equiv \{\text{Suponemos antecedente y demostramos consecuente}\} \\
&wp.(s, k := s + A.k, k + 1).(N - k < T) \\
&\equiv \{\text{Def wp asignacion}\} \\
&N - (k + 1) < T \\
&\equiv \{\text{Aritmetica}\} \\
&N - k - 1 < T \\
&\equiv \{\text{Suposicion } N - k = T\} \\
&N - k - 1 < N - k \\
&\equiv \{\text{Logica}\} \\
&True
\end{aligned}
$$

3)

Especificacion:

$$
\begin{aligned}
&Var a : array[0, N) of Int; \\
&\{N \geq 0\} \\
&S_0 \\
&\{r = \langle \forall i : 0 \leq i < N : A.i \geq 0 \rangle\}
\end{aligned}
$$

Determinemos el invariante utilizando la tecnica de reemplazar una constante por una variable:

$$I : r = \langle \forall i : 0 \leq i < k : A.i \geq 0 \rangle \wedge 0 \leq k \leq N$$

Estructura del programa:

$$\{N \geq 0\}$$
$$S_0$$
$$\{I\}$$
$$do\ B \rightarrow$$
$$\quad \{I \wedge B\}$$
$$\quad S_1$$
$$\quad \{I\}$$
$$od$$
$$\{\langle \forall i : 0 \leq i < N : A.i \geq 0 \rangle\}$$

Inicializacion:

$$\{N \geq 0\}$$
$$S_0$$
$$\{I : r = \langle \forall i : 0 \leq i < k : A.i \geq 0 \rangle \wedge 0 \leq k \leq N\}$$

Busquemos algun S_0 de la forma $r, k := E, F$, para ello supongamos la hipotesis($N \geq 0$) y veamos la wp:

$$wp.(r, k := E, F).(r = \quad \langle \forall i : 0 \leq i < k : A.i \geq 0 \rangle \wedge 0 \leq k \leq N)$$
$$\equiv \{\text{Def wp asignacion}\}$$
$$(E = \quad \langle \forall i : 0 \leq i < F : A.i \geq 0 \rangle \wedge 0 \leq F \leq N)$$
$$\equiv \{\text{Elijo F=0}\}$$
$$(E = \quad \langle \forall i : 0 \leq i < 0 : A.i \geq 0 \rangle \wedge 0 \leq 0 \leq N)$$
$$\equiv \{\text{Por suposicion } N \geq 0\}$$
$$(E = \quad \langle \forall i : 0 \leq i < 0 : A.i \geq 0 \rangle$$
$$\equiv \{\text{Rango vacio}\}$$
$$E = True$$
$$\equiv \{\text{Elijo E=True}\}$$
$$True = True$$
$$\equiv \{\text{Logica}\}$$
$$True$$

Por ende, tenemos que $S_0 \equiv r, k := True, 0$

Finalizacion: Para demostrar $I \wedge \neg B \Rightarrow Q$ elegimos un $B \equiv k \neq N$:

$$
\begin{aligned}
& r = \quad \langle \forall i : 0 \leq i < k : A.i \geq 0 \rangle \wedge 0 \leq k \leq N \wedge \neg(k \neq N) \\
& \Rightarrow \langle \forall i : 0 \leq i < N : A.i \geq 0 \rangle \\
& \equiv \{\text{Logica}\} \\
& r = \quad \langle \forall i : 0 \leq i < k : A.i \geq 0 \rangle \wedge 0 \leq k \leq N \wedge k = N \\
& \Rightarrow \langle \forall i : 0 \leq i < N : A.i \geq 0 \rangle \\
& \equiv \{\text{Suponemos antecedente y demostramos consecuente}\} \\
& \langle \forall i : 0 \leq i < N : A.i \geq 0 \rangle \\
& \equiv \{\text{Por suposicion } k = N\} \\
& \langle \forall i : 0 \leq i < k : A.i \geq 0 \rangle \\
& \equiv \{\text{Por suposicion } r\} \\
& True
\end{aligned}
$$

Programa hasta ahora:

$$
\begin{aligned}
& \{N \geq 0\} \\
& r, k := True, 0 \\
& \{I\} \\
& do\ k \neq N \rightarrow \\
& \quad \{I \wedge B\} \\
& \quad S_1 \\
& \quad \{I\} \\
& od \\
& \{\langle \forall i : 0 \leq i < N : A.i \geq 0 \rangle\}
\end{aligned}
$$

Elegimos cota candidata: $t = N - k$

Cuerpo del bucle: Busquemos algun S_1 de la forma $r, k := E, k + 1$, para ello asumamos $r = \langle \forall i : 0 \leq i < k : A.i \geq 0 \rangle \wedge 0 \leq k \leq N \wedge k \neq N$ y veamos la wp:

$wp.(r, k := E, k+1).(r = \quad \langle \forall i : 0 \leq i < k : A.i \geq 0 \rangle \wedge 0 \leq k \leq N)$
$\equiv$ {Def wp asignacion}
$E = \langle \forall i : 0 \leq i < (k+1) : A.i \geq 0 \rangle \wedge 0 \leq (k+1) \leq N$
$\equiv$ {Aritmetica}
$E = \langle \forall i : 0 \leq i < k \vee i = k : A.i \geq 0 \rangle \wedge 0 \leq (k+1) \leq N$
$\equiv$ {Por supocicion $0 \leq k \leq N \wedge k \neq N$}
$E = \langle \forall i : 0 \leq i < k \vee i = k : A.i \geq 0 \rangle \wedge True$
$\equiv$ {Particion de rango y rango unitario}
$E = \langle \forall i : 0 \leq i < k : A.i \geq 0 \rangle \wedge A.k \geq 0$
$\equiv$ {Por suposicion r}
$E = r \wedge A.k \geq 0$
$\equiv$ {Elijo $E = r \wedge A.k \geq 0$}
$r \wedge A.k \geq 0 = r \wedge A.k \geq 0$
$\equiv$ {Logica}
$True$

Por ende $S_1 \equiv r, k := r \wedge A.k \geq 0, k+1$

Demostracion de que la cota es positiva:

$r = \langle \forall i : 0 \leq i < k : A.i \geq 0 \rangle \wedge 0 \leq k \leq N \wedge k \neq N$
$\Rightarrow N - k \geq 0$
$\equiv$ {Suponemos antecedente y demostramos consecuente}
$N - k \geq 0$
$\equiv$ {Aritmetica}
$N \geq k$
$\equiv$ {Por suposicion $k \neq N$}
$N > k$
$\equiv$ {Por suposicion $0 \leq k \leq N$}
$True$

Demotracion de que la cota disminuye:

$\{r = \langle \forall i : 0 \leq i < k : A.i \geq 0 \rangle \wedge 0 \leq k \leq N \wedge k \neq N \wedge N - k = T\}$
$r, k := r \wedge A.k \geq 0, k + 1$
$\{N - k < T\}$
$\equiv$ {Asumamos la precondicion y veamos la wp}
$wp.(r, k := r \wedge A.k \geq 0, k + 1).(N - k < T)$
$\equiv$ {Def wp asignacion}
$N - (k + 1) < T$
$\equiv$ {Supocicion $N - k = T$}
$N - (k + 1) < N - k$
$\equiv$ {Aritmetica}
$N - k - 1 < N - k$
$\equiv$ {Logica}
$True$