2) Derivar:

Const M : Int;

Var a: array [0, M) of Int;

r: Bool;

$\{M \geq 0\}$

S

$Q: \{r = \langle \forall i : 0 \leq i \leq M : (\Sigma j : 0 \leq j < i : a.j) \leq \langle N j : 0 \leq j < i : a.j \geq 0 \rangle \rangle\}$

Planteo un bucle con una invariantización SO primero

$\{M \geq 0\}$

SO

$\{I\}$

do b ->

S

od

$\{I\}$

$\{Q\}$

Planteo el invariante:

$\{r = \langle \forall i : 0 \leq i \leq n : (\Sigma j : 0 \leq j < i : a.j) \leq \langle N j : 0 \leq j < i : a.j \geq 0 \rangle \rangle\} \wedge 0 \leq n \leq M$

Busco una guarda tal que $I \wedge \neg b \Rightarrow Q$

- Propongo $b \equiv M > n$
- tenemos $\neg b \wedge 0 \leq n \leq M \equiv M \leq n \wedge 0 \leq n \leq M = n = M$
- si reemplazamos n por M (Leibniz), queda probada la postcondición Q.

• Planteo la cota $t = M - m$

Tenemos $I \Rightarrow m \leq M \Rightarrow T \geq 0$

• Derivo el cuerpo del ciclo.

- Propongo una asignación
- Propongo incrementar m en 1 en la asignación

$\{I \wedge b \wedge t = T\}$

$S; m := E, m+1$

$\{I \wedge t < T\}$

$= \{$Simplifico + obligación de prueba$\}$

$\Gamma = \langle \forall i : 0 \leq i \leq M : \langle \Sigma j : 0 \leq j < i : a.j \rangle \leq \langle N j : 0 \leq j < i : a.j \rangle \rangle \wedge 0 \leq m \leq M \wedge M - m = T$

$\Rightarrow$

$E = \underbrace{\langle \forall i : 0 \leq i \leq m+1 : \langle \Sigma j : 0 \leq j < i : a.j \rangle \leq \langle N j : 0 \leq j < i : a.j \rangle \rangle}_{h} \wedge \underbrace{0 \leq m+1 \leq M}_{P}$

• Prueba de a parte usando la hipótesis (Hip)

$Hip \Rightarrow m < M \Leftrightarrow m+1 < M+1 \Rightarrow m+1 \leq M \equiv P$

• Para probar h parto el rango en $i = m+1 \vee 0 \leq i \leq m$

• Uso rango virtual para escribir menos • Hipótesis

$E = \langle \Sigma j : 0 \leq j < m+1 : a.j \rangle \leq \langle N j : 0 \leq j < m+1 : a.j \rangle \wedge \Gamma$

$= \{$Partición de rango y análisis por casos$\}$

$E = \langle \Sigma j : 0 \leq j < m : a.j \rangle + a.m \leq \langle N j : 0 \leq j < m : a.j \geq 0 \rangle + (a.m \geq 0 \rightarrow 1, a.m < 0 \rightarrow 0) \wedge \Gamma$

• Debido al análisis por casos, propongo un condicional el cual asigna un valor distinto a Γ según el caso:

```
if a.m ≥ 0 -> Γ := E1
[] a.m < 0 -> Γ := E2
```

- Vemos que las guardas son exhaustivas y siempre se cumple alguna.
- Vemos que ambos temas son válidos

$I \wedge M > m \wedge a.m \geq 0$
$\Rightarrow$
$E1 = \langle \Sigma j : 0 \leq j < m : a.j \rangle + a.m \leq \langle N j : 0 \leq j < m : a.j \geq 0 \rangle + 1 \wedge \Gamma$

$\wedge$
$I \wedge M > m \wedge a.m < 0$
$\Rightarrow$
$E2 = \langle \Sigma j : 0 \leq j < m : a.j \rangle + a.m \leq \langle N j : 0 \leq j < m : a.j \geq 0 \rangle \wedge \Gamma$

- Propongo fortalecer el invariante con $s = \langle \Sigma j : 0 \leq j < m : a.j \rangle$
$c = \langle N j : 0 \leq j < m : a.j \geq 0 \rangle$

Tenemos: $E1 = s + a.m \leq c + 1 \wedge \Gamma$
$E2 = s + a.m \leq c \wedge \Gamma$

Entonces, si agregamos al cuerpo la asignación de s y c para mantener los condicionales el invariante, luego de hacer los mismos pasos, puedo demostrar los temas:

$\{I \wedge M > m \wedge a.m \geq 0\}$ $\wedge$ $\{I \wedge M > m \wedge a.m \geq 0\}$
$s, c := s, c$ $\wedge$ $s, c := s, c$
$\{I\}$ $\{I\}$
$= \{$Obligaciones de prueba, Punto los rangos y aplico hipótesis (s y c)

$I \wedge M > m \wedge a.m \geq 0$	$I \wedge M > m \wedge a.m < 0$
$\Rightarrow$	$\Rightarrow$
$S = s + b.m \wedge C = c + 1$	$S = s + a.m \wedge C = c$

Tenemos entonces el cuerpo del bucle:

$\{I \wedge M > m \wedge M - n = T\}$

if $a.n \geq 0 \rightarrow$

$r, s, c, m := s + a.n \leq c+1 \wedge r,\ s + a.n,\ c+1,\ m+1$

[] $a.n < 0 \rightarrow$

$r, s, c, n := s + a.n \leq c \wedge r,\ s + a.n,\ c,\ n+1$

$\{I \wedge M > n \wedge M - m = T\}$

Queda ahora derivar la inicialización:

$\{M \geq 0\}$

$r, s, c, n := R, S, C, F$

$\{I\}$

$= \{$Obligación de prueba$\}$

$M \geq 0$

$\Rightarrow$

$R = \langle \forall i : 0 \leq i \leq m : \langle \Sigma j : 0 \leq j < i : a.j \rangle \leq \langle N j : 0 \leq j < i : a.j \geq 0 \rangle \rangle \wedge S = \langle \Sigma j : 0 \leq j < m : a.j \rangle \wedge$

$C = \langle N j : 0 \leq j < m : a.j \geq 0 \rangle \wedge 0 \leq F \leq M$

$\Leftarrow \{$Propongo $R = True,\ S = 0,\ C = 0,\ F = 0\}$

$= \{$Rangos vacíos de todos los cuantificadores de la expresión$\}$

$True = True \wedge 0 = 0 \wedge 0 = 0 \wedge 0 \leq 0 \leq M$

$= \{$Reflexividad + $0 \leq M\}$

$True$

Respuesta:

$\{0 \leq M\}$

$r, s, c, m := True, 0, 0, 0;$

do $M > m \rightarrow$

if $a.m \geq 0 \rightarrow$

$r, s, c, m := r \wedge s + am \leq c+1,\ s + a.m,\ c+1,\ m+1$

$[]\ a.m < 0$

$r, s, c, m := r \wedge s + a.m \leq c,\ s + a.m,\ c,\ m+1$

od

$\{Q\}$