Trabajo Práctico

Especificacion

Algoritmos y Estructura de Datos 1

Misión_Java

Integrante	LU	Correo electrónico
Livia, Mario	642/23	marioalelivia@gmail.com
Schenone, Ariel	431/22	ariel8sche@gmail.com
Pacheco, Thomas	190/22	thomasextrem0408@gmail.com
Perotti, Franco	548/23	francoperotti52@gmail.com

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2610 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (++54 +11) 4576-3300
http://www.exactas.uba.ar

1. Consideraciones

-El ultimo elemento de la lista de escrutinio son los votos en blanco.
-Un DNI válido es aquel que sea mayor a 0.
-No hay repetidos en el escrutinio.
-Aceptamos repetidos en la matriz DHondt.
-Si había dos o más cocientes iguales en la matriz D´Hondt, se le otorgará la banca al partido que recibió más votos totales.

2. Ejercicios

2.1. Ejercicio 1

`proc hayBallotage` (in escrutinio: $seq\langle\mathbb{Z}\rangle$) : Bool
`requiere` $\{escrutinioValido(escrutinio)\}$
`asegura` $\{res = \text{true} \leftrightarrow (nadieSupera40Porciento(escrutinio) \ \vee \ (noHayDiferencia10(escrutinio) \wedge nadieSupera45Porciento(escrutinio))\}$
`pred escrutinioValido` (escrutinio: $seq\langle\mathbb{Z}\rangle$) {
$todosDistintos(escrutinio) \ \wedge \ todosPositivos(escrutinio) \wedge \ |escrutinio| > 2$
}
`pred todosDistintos` (s: $seq\langle\mathbb{Z}\rangle$) {
$(\forall k, j : \mathbb{Z})(0 \leq k, j < |s| - 1 \ \wedge \ k \neq j \ \longrightarrow_L \ s[k] \neq s[j])$
}
`pred todosPositivos` (s: $seq\langle\mathbb{Z}\rangle$) {
$(\forall i : \mathbb{Z})(0 \leq i < |s| \ \longrightarrow_L \ s[i] \geq \ 0)$
}
`pred nadieSupera45Porciento` (escrutinio: $seq\langle\mathbb{Z}\rangle$) {
$\{(\forall id : \mathbb{Z})(0 \leq id < |escrutinio| - 1 \ \wedge_L \ (escrutinio[id] \ / \ sumaDeVotos(escrutinio)) < 0{,}45)$

}
`pred nadieSupera40Porciento` (escrutinio: $seq\langle\mathbb{Z}\rangle$) {
$\{(\forall id : \mathbb{Z})(0 \leq id < |escrutinio| - 1 \ \wedge_L \ ((escrutinio[id] \ / \ sumaDeVotos(escrutinio)) < 0{,}40)$

}
`pred noHayDiferencia10` (escrutinio: $seq\langle\mathbb{Z}\rangle$) {
$\neg(\exists x, y : \mathbb{Z})((x \in escrutinio \ \wedge \ y \in escrutinio \ \wedge \ x \neq y) \ \wedge_L \ (\forall z : \mathbb{Z})(z \in escrutinio \ \wedge \ x \neq z \longrightarrow_L z < y < x) \wedge ((x-y) \ / \ sumaDeVotos(escrutinio)) \ > 0,10) \wedge_L (x \neq escrutinio[|escrutinio|-1] \wedge y \ \neq \ escrutinio[|escrutinio| - 1]))$
}
`aux sumaDeVotos` (escrutinio: $seq\langle\mathbb{Z}\rangle$) : $\mathbb{Z} \ = \sum_{id=0}^{|escrutinio|-1} \ escrutinio[i]$;

2.2. Ejercicio 2

`proc hayFraude` (in escrutinio_presidencial: $seq\langle\mathbb{Z}\rangle$, in escrutinio_diputados: $seq\langle\mathbb{Z}\rangle$, in escrutinio_senadores: $seq\langle\mathbb{Z}\rangle$) : Bool
`requiere` $\{escrutinioValido(escrutinio\_presidencial) \ \wedge \ escrutinioValido(escrutinio\_diputados) \ \wedge \ escrutinioValido(escrutinio\_senadores) \ \wedge \ |escrutinio\_presidencial| = |escrutinio\_diputados| = |escrutinio\_senadores|\}$
`asegura` $\{res = \text{true} \leftrightarrow ((sumaDeVotos(escrutinio\_presidencial) \neq sumaDeVotos(escrutinio\_diputados)) \vee (sumaDeVotos(escrutinio\_presidencial) \neq sumaDeVotos(escrutinio\_senadores)))\}$

2.3. Ejercicio 3

`proc obtenerSenadoresEnProvincia` (in escrutinio: $seq\langle\mathbb{Z}\rangle$) : $\mathbb{Z}\times\mathbb{Z}$
`requiere` $\{escrutinioValido(escrutinio)\}$

asegura $\{0 \leq res_0, res_1 < |escrutinio| - 1 \wedge_L (\forall id : \mathbb{Z})(0 \leq id < |escrutinio| - 1 \longrightarrow_L escrutinio[id] \leq escrutinio[res_0]) \wedge (\forall id : \mathbb{Z})(0 \leq id < |escrutinio| - 1 \wedge_L escrutinio[id] \neq escrutinio[res_0] \longrightarrow_L escrutinio[id] \leq escrutinio[res_1])\}$

2.4. Ejercicio 4

proc `calcularDHondtEnProvincia` (in cantidad_bancas: $\mathbb{Z}$, in escrutinio: $seq\langle\mathbb{Z}\rangle$) : $seq\langle seq\langle\mathbb{Z}\rangle\rangle$

requiere $\{escrutinioValido(escrutinio) \wedge cant\_bancas > 0\}$

asegura $\{|res| = |escrutinio| - 1 \wedge_L (\forall id : \mathbb{Z})(0 \leq id < |res| \longrightarrow_L |res[id]| = cant\_bancas \wedge sonCocientes(res[id], escrutinio, id))\}$

pred `soloCocientesOrdenados` (in fila:$seq\langle\mathbb{Z}\rangle$, in cant_bancas:$\mathbb{Z}$, in votos: $\mathbb{Z}$) {
$(\forall i\mathbb{Z})(0 \leq i < |fila| - 1 \longrightarrow_L fila[i] \leq fila[i+1]) \wedge (\forall j : \mathbb{Z})(0 \leq j < |fila| \longrightarrow_L fila[j] = votosdiv1 + j)$
}

pred `sonCocientes` (in fila:$seq\langle\mathbb{Z}\rangle$, in escrutinio: $seq\langle\mathbb{Z}\rangle$, in id:$\mathbb{Z}$) {
$(\forall i : \mathbb{Z})(0 \leq i < |fila| \longrightarrow_L fila[i] = (escrutinio[id]\ div\ i + 1))$
}

2.5. Ejercicio 5

proc `obtenerDiputadosEnProvincia` (in cant_bancas: $\mathbb{Z}$, in escrutinio: $seq\langle\mathbb{Z}\rangle$, in dHondt: $seq\langle seq\langle\mathbb{Z}\rangle\rangle$) : $seq\langle\mathbb{Z}\rangle$

requiere $\{cant\_bancas > 0 \wedge dHondtValido(dHondt, cantidad\_bancas) \wedge algunoSupera3\%(escrutinio) \wedge escrutinioValido(escrutinio)\}$

t := i asegura $\{|res| = |dHondt| \wedge (\forall id : \mathbb{Z})(0 \leq id < |dHondt|) \longrightarrow_L (res[i] = ganaNBancos(dHondt[i], dHondt, escrutinio, id, cant\_bancas))\}$

aux `ganaNBancas` (fila:$seq\langle\mathbb{Z}\rangle$, dHondt:$seq\langle seq\langle\mathbb{Z}\rangle\rangle$, escrutinio:$seq\langle\mathbb{Z}\rangle$, id:$\mathbb{Z}$ cantidad_bancas: $\mathbb{Z}$) : $\mathbb{Z}$ = $\sum_{k=0}^{|fila|-1} if\ (cantidadMayores(fila[k], dHondt, id) < cantidad\_bancas \wedge fila[0]/sumaDeVotos(escrutinio) > 0,03)\ then\ 1\ else\ 0\ fi$;

aux `cantidadMayores` (cociente:$\mathbb{Z}$, dHondt:$seq\langle seq\langle\mathbb{Z}\rangle\rangle$, id:$\mathbb{Z}$) : $\mathbb{Z}$ = $\sum_{k=0}^{|dHondt|-1} \sum_{j=0}^{|dHondt[k]|-1} if\ (cociente < dHondt[k][j] \vee (cociente = dHondt[k][j] \wedge dHondt[id][0] < dHond[k][0]))\ then\ 1\ else\ 0\ fi$;

pred `dHondtValido` (s:$seq\langle\mathbb{Z}\rangle$, n : $\mathbb{Z}$) {
$|dHondt| = |escrutinio| - 1 \wedge_L (\forall id : \mathbb{Z})(0 \leq id < |dHondt| \longrightarrow_L$
$|dHondt[id]| = cant\_bancas \wedge sonCocientes(dHondt[id], escrutinio, id)$
}

pred `algunoSupera3%` (in escrutinio:$seq\langle\mathbb{Z}\rangle$) {
$(\exists id : \mathbb{Z})(0 \leq id < |escrutinio| \wedge_L (escrutinio[id] / sumaDeVotos[escrutinio]) > 0,03)$
}

2.6. Ejercicio 6

proc `validarListaDiputadosEnProvincia` (in cantidad_bancas: $\mathbb{Z}$, in listas: $seq\langle seq\langle DNI : \mathbb{Z} \times Genero : \mathbb{Z}\rangle\rangle$) : Bool

requiere $\{listaValida(listas) \wedge cantidad\_bancas > 0\}$

asegura $\{res = \text{true} \leftrightarrow ((\forall sub : seq\langle\mathbb{Z} \times \mathbb{Z}\rangle)((sub \in listas \wedge |sub| = cantidad\_bancas) \longrightarrow_L hayAlternancia(sub) \wedge todosElementosDistintos(sub))\}$

pred `listaValida` (in listas: $seq\langle seq\langle\mathbb{Z} \times \mathbb{Z}\rangle\rangle$) {
$|lista| > 0 \wedge soloHombreYMujer(lista) \wedge dniValido(lista)$
}

pred `hayAlternancia` (in lista: $seq\langle\mathbb{Z} \times \mathbb{Z}\rangle$) {
$(\forall id : \mathbb{Z})(0 \leq id < |lista| - 1 \longrightarrow_L lista[id]_1 \neq lista[id+1]_1)$
}

pred `soloHombreYMujer` (in lista: $seq\langle\mathbb{Z} \times \mathbb{Z}\rangle$) {
$(\forall i, j : \mathbb{Z})((0 \leq i < |l| \wedge_L 0 \leq j < |l[i]|) \longrightarrow_L ((lista[i][j])_1 == 0 \vee (lista[i][j])_1 == 1))$

}

`pred dniValido` (in lista: $seq\langle \mathbb{Z} \times \mathbb{Z} \rangle$) {

$(\forall persona : \mathbb{Z})(0 \leq persona < |lista| - 1 \longrightarrow_L lista[persona]_1 > 0)$

}

`pred todosElementosDistintos` (s: $seq\langle seq\langle \mathbb{Z} \times \mathbb{Z} \rangle\rangle$) {

$(\forall k, j : \mathbb{Z})(\forall i, t : \mathbb{Z})(0 \leq k, j < |s| \ \wedge \ 0 \leq i, t < |escrutinio[0]| \ \wedge \ i \neq t \ \longrightarrow_L \ s[k][t]_0 \neq s[j][i]_0)$

}

3. Programas

3.1. Programa 1

hayBallotage

```
votosTotales:=0
i:=0
while (i < escrutinio.size()−1) do
    votosTotales := votosTotales + escrutinio[i]
    i:= i+1)
endwhile
primero := 0
segundo := 0
i := 0
while (i < escrutinio.size()−1) do
    if (escrutinio[i] >= primero) then
        segundo := primero
        primero:= escrutinio[i]
    else
        skip
    endif
    if (escrutinio[i] >= segundo) then
        segundo := escrutinio[i]
    else
        skip
    endif
    i: = i+1
endwhile
res := False
if (((primero / votosTotales) < 0,40) || (((primero / votosTotales) < 0,45) && (((primeros − segundos) / votosTotales) < 0,1)) then
    res := True
else
    skip
endif
```

3.2. Programa 2

sumaDeVotos(escrutinio)

```
res := 0
i := 0
while (i < escrutinio.size( )) do
    res := res + escrutinio[i]
    i := i+1
endwhile
```

hayFraude(escrutinio_ presidencial, escrutinio_ diputados, escrutinio_ senadores)

```
votosTotalesPre := sumaDeVotos(escrutinio_presidencial)
votosTotalesDip := sumaDeVotos(escrutinio_diputados)
votosTotalesSen := sumaDeVotos(escrutinio_senadores)
```

```
if (votosTotalesPre != votosTotalesDip) || (votosTotalesPre != votosTotalesSen) then
    res := true
else
    res := false
endif
```

3.3. Programa 3

```
obtenerSenadoresEnProvincia
i := 1
j := 0
while i < escrutinio.size()-1 do
    if (escrutinio[j] < escrutinio[i]) then
            j := i
    else
            skip
    endif
    i := i+1
endwhile
i := 1
k := 0
while i < escrutinio.size()-1 do
    if (escrutinio[k] < escrutinio[i] && escrutinio[i]!=escrutinio[j]) then
            k := i
    else
            skip
    endif
    i := i+1
endwhile
res0 := j
res1 := k
```

3.4. Programa 6

```
validarListaDiputados
res := True
i := 0
j:=0
while i < listas.size( ) do
    while j < listas.size( )-1 do
        if (listas[i][j][1]==listas[i][j+1][1]) then
            res := False
        else
            skip
        endif
        j := j+1
    endwhile
    i := i+1
endwhile


i := 0
j := 0
res := true
while i < listas.size( ) do
    while j < listas[0].size( ) do
        t := i
        k := j+1
        MismoPartido := true
```

```
        while t < listas.size( ) do
            if (MismoPartido = False) then
                k := 0
            else
                MismoPartido := False
            endif
            while k < listas[0].size( ) do
                if (lista[i][j][0] = lista[t][k][0]) then
                    res := False
                else
                    skip
                endif
                k:=k+1
            endwhile
            t:=t+1
        endwhile
        j:=j+1
    endwhile
    i=i+1
endwhile
```

4. Correctitud

4.1. Correctitud programa 2

El planteo es el siguiente:

```
{P}
    S1
    S2
    S3
{Q_0}
{P_if}
    S4
{Q}
```

Reemplazos sintácticos:
- SDV = auxiliar definida en la especificación sumaDeVotos
- es = escrutinio
Empiezo de abajo hacia arriba:
Tengo que asegurar que Pif (Precondicion del If) implique Q (Postcondicion del programa completo) es decir, Pif ⇒ wp(S4,Q).

$Pif \equiv votosTotalesPre = SDV(es\_presidencial) \wedge VotosTotalesDip = SDV(es\_diputados)) \wedge (VotosTotalesSen) = SDV(es\_senadores))$

$Q \equiv res = True \leftrightarrow (SDV(es\_presidencial \neq SDV(es\_diputados) \vee SDV(es\_presidencial) \neq SDV(es\_senadores))$

$S4 \equiv If\ (sumaVotosPresidencial \neq sumaVotosDiputados \vee sumaVotosPresidencial \neq sumaVotosSeandores)\ Then\ (res := true)\ Else\ (res := false)\ Fi$

$B \equiv\ (votosTotalesPre \neq votosTotalesDip\ \vee\ votosTotalesPre \neq votosTotalesSen)$

Pif $\implies$ wp(S4, Q)

Calculo wp(S4,Q)

$\equiv def(B) \wedge_L ((B \wedge wp(res := true, Q) \vee (\neg B \wedge wp(res := false, Q)))$

$\equiv (B \wedge (true = true \leftrightarrow (SDV(es\_presidencial) \neq SDV(es\_diputados) \vee SDV(es\_presidencial) \neq SDV(es\_senadores)))) \vee (\neg B \wedge (false = true \leftrightarrow (SDV(es\_presidencial) \neq SDV(es\_diputados) \vee SDV(es\_presidencial) \neq SDV(es\_senadores))))$

$\equiv (B \wedge (true \leftrightarrow (SDV(es\_presidencial) \neq SDV(es\_diputados) \vee SDV(es\_presidencial) \neq SDV(es\_senadores)))) \vee (\neg B \wedge (false \leftrightarrow (SDV(es\_presidencial) \neq SDV(es\_diputados) \vee SDV(es\_presidencial) \neq SDV(es\_senadores))))$

$\equiv \; (B \wedge (SDV(es\_presidencial) \neq SDV(es\_diputados) \vee SDV(es\_presidencial) \neq SDV(es\_senadores))) \vee (\neg B \wedge \neg(SDV(es\_presidencial) \neq SDV(es\_diputados) \vee SDV(es\_presidencial) \neq SDV(es\_senadores)))$

$\equiv \; (B \wedge (SDV(es\_presidencial) \neq SDV(es\_diputados) \vee SDV(es\_presidencial) \neq SDV(es\_senadores))) \vee (\neg B \;\wedge\; (SDV(es\_presidencial) = SDV(es\_diputados) \wedge SDV(es\_presidencial) = SDV(es\_senadores)))$

Cambio B por su definición

$\equiv \; ((votosTotalesPre \neq votosTotalesDip \vee votosTotalesPre \neq votosTotalesSen) \wedge (SDV(es\_presidencial) \neq SDV(es\_diputados) \vee SDV(es\_presidencial) \neq SDV(es\_senadores))) \vee ((votosTotalesPre = votosTotalesDip \vee votosTotalesPre = votosTotalesSen) \wedge (SDV(es\_presidencial) = SDV(es\_diputados) \wedge SDV(es\_presidencial) = SDV(es\_senadores)))))$

Ahora nos queda por ver que Pif $\implies$ wp(S4,Q)

Asumimos que Pif es verdadero ($Pif \equiv votosTotalesPre = SDV(es\_presidencial) \;\wedge\; VotosTotalesDip = SDV(es\_diputados)) \;\wedge\; (VotosTotalesSen) = SDV(es\_senadores)))$, entonces reemplazo y tengo que:

$\equiv \; (SDV(es\_presidencial) \neq SDV(es\_diputados) \;\vee\; (SDV(es\_presidencial) \neq SDV(es\_senadores)) \;\wedge\; (SDV(es\_presidencial) \neq SDV(es\_diputados)) \vee (SDV(es\_presidencial) \neq SDV(es\_senadores)) \vee (SDV(es\_presidencial) SDV(es\_diputados)) \wedge SDV(es\_presidencial) = SDV(es\_senadores) \wedge (SDV(es\_presidencial) = SDV(es\_diputados) \wedge SDV(es\_presidencial) = SDV(es\_senadores)$

En la fórmula anterior tengo algo de la forma $(P \wedge P) \vee (\neg P \wedge \neg P)$ que es equivalente a $P \vee \neg P$

$\equiv \; (SDV(es\_presidencial) \neq SDV(es\_diputados) \;\vee\; (SDV(es\_presidencial) \neq SDV(es\_senadores)) \;\vee\; (SDV(es\_presidencial) = SDV(es\_diputados)) \;\wedge\; SDV(es\_presidencial) = SDV(es\_senadores))$

Veo que ahora tengo algo de la forma P $\vee$ $\neg$P, que es equivalente a True

$\equiv True$

Por lo tanto Pif $\implies$ $wp(S4, Q)$

$\mathbf{Q_0} \implies$ Pif

Ahora hay que probar que $Q_0 \implies Pif$

$Q_0 \equiv Pif$

Por lo tanto la implicación es trivialmente verdadera

P $\implies$ wp(S1;S2;S3, $\mathbf{Q_0}$)

Queda por probar que P $\implies$ wp(S1;S2;S3, Q_0)

Por definición tenemos que:

$wp(S1; S2; S3, P) \equiv wp(S1, wp(S2, wp(S3, Q_0)))$

Calculo primero wp(S3,Q_0)

wp(S3,Q_0) $\equiv$ $wp(votosTotalesSen := sumaDeVotos(es\_senadores),\, votosTotalesPre = SDV(es\_presidencial) \wedge VotosTotalesDip = SDV(es\_diputados)) \;\wedge\; (VotosTotalesSen) = SDV(es\_senadores)))$

$\equiv \forall r.(r = \sum_{j=0}^{|es\_senadores|-1} es\_senadores[j]) \implies (votosTotalesPre = SDV(es\_presidencial) \wedge votosTotalesDip = SDV(es\_diputados) \wedge r = SDV(es\_senadores))$

Como hay un único r posible, reemplazo:

$\equiv (votosTotalesPre = SDV(es\_presidencial) \wedge votosTotalesDip = SDV(es\_diputados) \wedge \sum_{j=0}^{|es\_senadores|-1} es\_senadores[j] =$ SDV(es_senadores))

Como por definición SDV(es_senadores) $= \sum_{j=0}^{|es\_senadores|-1} es\_senadores[j]$ tengo que:

$\equiv (votosTotalesPre = SDV(es\_presidencial) \ \wedge \ votosTotalesDip = SDV(es\_diputados) \ \wedge \ True)$
$\equiv (votosTotalesPre = SDV(es\_presidencial) \ \wedge \ votosTotalesDip = SDV(es\_diputados))$
$\equiv E_0$

Ahora calculo wp(S2,E_0)

wp(S2,E_0) $\equiv wp(votosTotalesDip := sumaDeVotos(es\_dip),\ votosTotalesPre = SDV(es\_presidencial) \wedge VotosTotalesDip = SDV(es\_diputados))$

$\equiv \forall r.(r = \sum_{j=0}^{|es\_dip|-1} es\_diputados[j]) \implies (votosTotalesPre = SDV(es\_presidencial) \wedge r = SDV(es\_diputados))$

Como hay un único r posible, reemplazo:

$\equiv (votosTotalesPre = SDV(es\_presidencial) \ \wedge \ \sum_{j=0}^{|es\_diputados|-1} es\_diputados[j] =$ SDV(es_diputados))

Como por definición SDV(es_diputados) $= \sum_{j=0}^{|es\_diputados|-1} es\_diputados[j]$ tengo que:

$\equiv (votosTotalesPre = SDV(es\_presidencial) \ \wedge \ True)$
$\equiv (votosTotalesPre = SDV(es\_presidencial))$
$\equiv E_1$

Ahora calculo wp(S1,E_1)

wp(S1,E_1) $\equiv wp(votosTotalesPre := sumaDeVotos(es\_presidencial),\ votosTotalesPre = SDV(es\_presidencial))$

$\equiv \forall r.(r = \sum_{j=0}^{|es\_presidencial|-1} es\_presidencial[j]) \implies r = SDV(es\_presidencial))$

Como hay un único r posible, reemplazo:

$\equiv \sum_{j=0}^{|es\_presidencial|-1} es\_presidencial[j]) =$ SDV(es_presidencial)

Como por definición SDV(es_presidencial) $= \sum_{j=0}^{|es\_presidencial|-1} es\_presidencial[j]$ tengo que:

$\equiv \ True$

En conclusión, la wp(S1;S2;S3,Q_0)$\equiv$ True

Por lo tanto P $\implies$ Q_0 es trivialmente verdadera, probando asi la tripla de Hoare

Nos falta probar que el programa sumaDeVotos es correcto:

$Pc \ \equiv \ res := 0 \ \wedge \ i := 0 \ \wedge \ |escrutinio| > 2$
$Qc \ \equiv \ res := \sum_{i=0}^{|escrutinio|-1} \ escrutinio[i]$
$I \ \equiv \ 0 \leq i \leq |escrutinio| \ \wedge_L \ res := \sum_{j=0}^{i-1} \ escrutinio[j] \ \wedge \ |escrutinio| > 2$
$B \ \equiv \ i < |escrutinio|$

Teorema del invariante

Pc $\implies$ I

$\equiv \ res = 0 \ \wedge \ i = 0 \ \wedge \ |escrutinio| > 2 \Rightarrow \ 0 \leq i \leq |escrutinio| \ \wedge_L \ res := \sum_{j=0}^{i-1}$ escrutinio[j] $\wedge \ |escrutinio| > 2$

$\equiv \ 0 = \sum_{j=0}^{0-1}$ escrutinio[j] $\wedge \ 0 \leq 0 \leq |escrutinio| \ (|escrutinio| > 2)$
$\equiv \ 0 = 0 \ \wedge \ True$
$\equiv \ True$

(I $\wedge \neg$ B) $\implies$ Qc

(I $\wedge \neg B) \equiv i = |escrutinio| \wedge_L res = \sum_{j=0}^{i-1}$ escrutinio[j] $\wedge |escrutinio| > 2$
$\equiv i = |escrutinio| \wedge_L res = \sum_{j=0}^{i-1}$ escrutinio[j] $\wedge |escrutinio| > 2 \Rightarrow res := \sum_{j=0}^{|escrutinio|-1}$ escrutinio[j]
$\equiv i = |escrutinio| \wedge_L res = \sum_{j=0}^{i-1}$ escrutinio[j] $\wedge |escrutinio| > 2 \Rightarrow res = \sum_{j=0}^{i-1}$ escrutinio[j]
$\equiv True$

{ I $\wedge$ B } S { I }

$\equiv (I \wedge B) \Rightarrow wp(S, Qc)$

(I $\wedge B) \equiv 0 \leq i < |escrutinio| \wedge_L res = \sum_{j=0}^{i-1} escrutinio[j] \wedge |escrutinio| > 2$

$wp(S, Q_c) \equiv wp(res := res + escrutinio[i], wp(i := i + 1, I))$

Calculamos wp(i:=i+1, I)

wp(i:=i+1, $0 \leq i \leq |escrutinio| \wedge_L res = \sum_{j=0}^{i-1} escrutinio[j] \wedge |escrutinio| > 2)$

$\equiv 0 \leq i + 1 \leq |escrutinio| \wedge_L res = \sum_{j=0}^{i+1-1} escrutinio[j] \wedge |escrutinio| > 2$

$\equiv$ -1 $\leq i \leq |escrutinio| - 1 \wedge_L res = \sum_{j=0}^{i} escrutinio[j] \wedge |escrutinio| > 2$

Ahora calculamos wp(res:=res+escrutinio[i], $-1 \leq i \leq |escrutinio| - 1 \wedge_L res = \sum_{j=0}^{i} escrutinio[j] \wedge |escrutinio| > 2)$

$\equiv def(res := res+escrutinio[i]) \wedge_L$ -1 $\leq i \leq |escrutinio|-1 \wedge_L res+escrutinio[i] = \sum_{j=0}^{i} escrutinio[j] \wedge |escrutinio| > 2$

$\equiv 0 \leq i < |escrutinio| \wedge_L -1 \leq i \leq |escrutinio| - 1 \wedge_L res + escrutinio[i] = \sum_{j=0}^{i} escrutinio[j] \wedge |escrutinio| > 2$

$\equiv 0 \leq i < |escrutinio| \wedge_L res = \sum_{j=0}^{i} escrutinio[j] - escrutinio[i] \wedge |escrutinio| > 2$

$\equiv 0 \leq i < |escrutinio| \wedge_L res = \sum_{j=0}^{i-1} escrutinio[j] \wedge |escrutinio| > 2$

Ahora (I $\wedge$ B) tiene que implicar lo anterior

$0 \leq i < |escrutinio| \wedge_L res = \sum_{j=0}^{i-1} escrutinio[j] \wedge |escrutinio| > 2 \implies 0 \leq i < |escrutinio| \wedge_L res = \sum_{j=0}^{i-1} escrutinio[j] \wedge |escrutinio| > 2$

Tenemos algo de la forma P $\implies$ P, y eso es True, por lo tanto.

$\equiv True$

Asi queda demostrado el teorema del invariante, y su parcial correctitud

Teorema de la función variante

Definimos a la función variante como:

fv $\equiv |escrutinio| - i$

{ I $\wedge$ B $\wedge$ v_0 = vf } S { fv < v_0 }

$\equiv wp(S, fv < v_0)$

$\equiv wp(res := res + escrutinio[i], wp(i := i+1, fv < \mathrm{v}_0))$

Calculo wp(i := i+1, fv $< v_0$)

wp(i := i+1, fv $< v_0$)

$\equiv |escrutinio| - (i+1) \ < \mathrm{v}_0$

$\equiv |escrutinio| - i - 1 \ < \ |escrutinio| - i$

$\equiv -1 < 0 \equiv True$

Ahora calculo wp(res := res + escrutinio[i], True), asumimos que (I $\wedge$ B) es verdadero, entonces:

I $\wedge$ B $\wedge$ v_0 = vf $\implies True \equiv True$

(I $\wedge$ fv ≤ 0) $\implies$ ¬ B

I $\wedge \ fv \ \leq \ 0 \ \equiv \ I \ \wedge \ |escrutinio| - i \ \leq \ 0 \ \equiv \ I \ \wedge \ |escrutinio| \ \leq \ i$

$\neg B \ \equiv \ i \geq |escrutinio|$

I $\wedge \ |escrutinio| \ \leq \ i \implies i \geq |escrutinio| \equiv True$

Como se probo que {I $\wedge B\}S\{fv < \mathrm{v}_0\}$ y (I $\wedge \ fv \ \leq \ 0) \implies \neg B$, y a su vez se probo el teorema del invariante, queda demostrado la correctitud del programa.

4.2. Correctitud del programa 3

el planteo es el siguiente:

```
{P}
{P_0}
i:= 1
j:= 0
{Q_0}

{P_1}
ciclo1
{Q_1}

{P_2}
i:= 1
k:= 0
{Q_2}

{P_3}
ciclo_2
{Q_3}

{P_4}
res[0] = j
res[1] = k
{Q}
```

Primero, tengo que probar que $\mathrm{P}_4 \implies wp(res[0] := j, wp(res[1] := k, Q))$
Recuerdo :
$Q \equiv 0 \leq res_0, \mathrm{res}_1$ ¡$|escrutinio|$-1 $\wedge_L (\forall id : \mathbb{Z})(0 \leq id < |escrutinio| - 1 \longrightarrow_L escrutinio[id] \leq escrutinio[res_0])$
$\wedge (\forall id : \mathbb{Z})(0 \leq id < |escrutinio| - 1 \wedge_L escrutinio[id] \neq escrutinio[res_0] \longrightarrow_L escrutinio[id] \leq escrutinio[res_1])$

ahora si calculo wp(res[0]:= j, wp(res[1]:= k,Q)):
como las instrucciones son simples, realiazo todo en un solo paso:
wp(res[0]:= j, wp(res[1]:= k,Q)) $\equiv 0 \leq j,k < |escrutinio| - 1 \ \wedge_L (\forall id : \mathbb{Z})(0 \leq id < |escrutinio| - 1 \ \longrightarrow_L escrutinio[id] \leq escrutinio[j]) \ \wedge \ (\forall id : \mathbb{Z})(0 \leq id < |escrutinio| - 1 \wedge_L escrutinio[id] \neq escrutinio[j] \ \longrightarrow_L escrutinio[id] \leq escrutinio[k])$

Defino P$_4$ $\equiv$ $wp(res[0] := j, \ wp(res[1] := k, Q))$, *por lo que* $P_4 \implies wp(res[0] := j, wp(res[1] := k, Q))$ *se cumple trivialmente.*

A continuación, tengo que probar que se cumple $\{P_4\}$ ciclo_2 $\{Q_3\}$ y que $Q_3 \implies P_4$

Segundo Ciclo
reemplazos sintácticos:
- **id** = t

B$_c$ $\equiv i < |escrutinio| - 1$

P$_3$ $\equiv k = 0 \ \wedge \ i = 1 \ \wedge \ 0 \leq j < |escrutinio| - 1 \wedge_L (\forall t : \mathbb{Z})(0 \leq t < |escrutinio| - 1 \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \ \wedge \ |escrutinio| > 2$

A $\equiv 0 \leq j < |escrutinio| - 1$

B $\equiv (\forall t : \mathbb{Z})(0 \leq t < |escrutinio| - 1 \longrightarrow_L escrutinio[j] \geq escrutinio[t])$

Q$_3$ $\equiv 0 \leq k < |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < |escrutinio| - 1 \ \wedge \ escrutinio[t] \neq escrutinio[j] \longrightarrow_L escrutinio[k] \geq escrutinio[t]) \ \wedge \ escrutinio[k] \neq escrutinio[j] \wedge \ B$

I $\equiv 0 \leq k < i \ \wedge_L \ 0 \leq i \leq |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \wedge escrutinio[t] < escrutinio[j] \longrightarrow_L escrutinio[k] \geq escrutinio[t]) \ \wedge \ A \ \wedge \ B$

P$_3$ $\implies$ **I**

$\equiv k = 0 \ \wedge \ i = 1 \ \wedge \ 0 \leq j < |escrutinio| - 1 \wedge_L \ B \ \wedge \ A \ \implies \ 0 \leq k < i \ \wedge_L \ 0 \leq i \leq |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \wedge escrutinio[t] < escrutinio[j] \longrightarrow_L escrutinio[k] \geq escrutinio[t]) \ \wedge \ escrutinio[k] < escrutinio[j] \ \wedge \ A \ \wedge \ B$

Reemplazo $k = 0 \wedge$ i=1

$0 \leq 0 < 1 \ \wedge_L \ 0 \leq 1 \leq |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < 0 \wedge escrutinio[t] < escrutinio[j] \longrightarrow_L escrutinio[k] \geq escrutinio[t]) \ \wedge \ A \ \wedge \ B$

$\equiv True \ \wedge_L \ |escrutinio| \geq \ 2 \ \wedge_L \ True \ \wedge \ A \ \wedge \ B$

$|escrutinio| > 2$ implica a $|escrutinio| \geq$2, a su vez A y B implica en ambos lados, por lo tanto Pc $\implies$ I

(I $\wedge$ ¬ **B)** $\implies$ **Q**$_3$

I $\wedge$ ¬ B $\equiv 0 \leq k < i \ \wedge_L \ i = |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \wedge escrutinio[t] < escrutinio[j] \longrightarrow_L escrutinio[k] \geq escrutinio[t]) \ \wedge \ escrutinio[k] < escrutinio[j] \ \wedge \ A \ \wedge \ B$

I $\wedge$ ¬ B) $\implies$ Q$_3$

$\equiv 0 \leq k < i \wedge_L i = |escrutinio| - 1 \wedge_L (\forall t : \mathbb{Z})(0 \leq t < i \wedge escrutinio[t] < escrutinio[j] \longrightarrow_L escrutinio[k] \geq escrutinio[t]) \ \wedge \ escrutinio[k] < escrutinio[j] \ \wedge \ A \ \wedge \ B \ \implies \ 0 \leq j,k < |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < |escrutinio| - 1 \ \wedge \ escrutinio[t] \neq escrutinio[j] \longrightarrow_L escrutinio[k] \geq escrutinio[t]) \ \wedge \ escrutinio[k] \neq escrutinio[j] \ \wedge \ A \ \wedge \ B$

{I $\wedge$ B} S {I}

$\equiv I \wedge$ B $\implies wp(if......fi, wp(i := i + 1, I))$

$\mathbf{I} \equiv 0 \leq i < |escrutinio| - 1 \ \wedge\ 0 \leq k < i \ \wedge\ 0 \leq j < |escrutinio| - 1 \ \wedge\ (\forall t : \mathbb{Z})(0 \leq t < i \ \wedge\ escrutinio[t] \neq escrutinio[j] \implies escrutinio[k] \geq escrutinio[t]) \ \wedge\ (\forall x : \mathbb{Z})(0 \leq x < |escrutinio| - 1 \longrightarrow_L escrutinio[j] \geq escrutinio[x])$

$\mathbf{B}_c \equiv i < |escrutinio| - 1$

$\mathbf{B}_i f \equiv escrutinio[k] < escrutinio[i] \ \wedge\ escrutinio[i] < escrutinio[j]$

calculo wp(i:= i+1,I)

$\equiv -1 \leq i \leq |escrutinio| - 2 \ \wedge\ 0 \leq k \leq i \ \wedge\ 0 \leq j < |escrutinio| - 1 \ \wedge\ (\forall t : \mathbb{Z})(0 \leq t \leq i \ \wedge j \neq t \implies escrutinio[k] \leq escrutinio[t]) \ \wedge\ (\forall x : \mathbb{Z})(0 \leq x < |escrutinio| - 1 \longrightarrow_L escrutinio[j] \geq escrutinio[x]) \ \equiv\ E0$

Usamos un formula equivalente a
A $\implies$ def(B$_i f$) $\wedge_L$ ((B$_i f$ $\wedge_L$ wp1) $\vee$ ($\neg$ B$_i f$ $\wedge_L$ wp2)
$\equiv$
((A $\wedge$ B$_i f$ $\wedge$ def(B$_i f$)) $\implies$ wp1) $\wedge$ ((A $\wedge$ $\neg$B $_i f$ $\wedge$ def(B$_i f$)) $\implies$ wp2)

I $\wedge$ B$_c$ $\wedge$ B$_i f$ $\implies wp(k := i, E_0)$

I $\wedge$ B$_c$ $\wedge$ B$_i f$ $\equiv 0 \leq i < |escrutinio| - 1 \ \wedge\ 0 \leq k < i \ \wedge\ 0 \leq j < |escrutinio| - 1 \ \wedge\ (\forall t : \mathbb{Z})(0 \leq t < i \wedge escrutinio[t] \neq escrutinio[j] \implies escrutinio[k] \geq escrutinio[t]) \wedge (\forall x : \mathbb{Z})(0 \leq x < |escrutinio| - 1 \longrightarrow_L escrutinio[j] \geq escrutinio[x]) \ \wedge\ (escrutinio[k] < escrutinio[i] \ \wedge\ escrutinio[i] < escrutinio[j])$

wp(k:=i,E$_0$) $\equiv -1 \leq i \leq |escrutinio| - 2 \ \wedge\ 0 \leq i \leq i \ \wedge\ 0 \leq j < |escrutinio| - 1 \ \wedge\ (\forall t : \mathbb{Z})(0 \leq t < i \ \wedge\ escrutinio[t] \neq escrutinio[j] \implies escrutinio[i] \geq escrutinio[t])$

$\equiv 0 \leq i \leq |escrutinio| - 2 \wedge 0 \leq j < |escrutinio| - 1 \wedge (\forall t : \mathbb{Z})(0 \leq t < i \wedge escrutinio[t] \neq escrutinio[j] \implies escrutinio[i] \geq escrutinio[t]) \ \wedge\ (\forall x : \mathbb{Z})(0 \leq x < |escrutinio| - 1 \longrightarrow_L escrutinio[j] \geq escrutinio[x])$

Ahora veo I $\wedge$ B$_c$ $\wedge$ B$_i f$ $\implies wp(k := i, E_0)$

$0 \leq i < |escrutinio| - 1 \ \wedge\ 0 \leq k < i \ \wedge\ 0 \leq j < |escrutinio| - 1 \ \wedge\ (\forall t : \mathbb{Z})(0 \leq t < i \ \wedge\ escrutinio[t] \neq escrutinio[j] \implies escrutinio[k] \geq escrutinio[t]) \ \wedge\ (escrutinio[k] < escrutinio[i] \ \wedge\ escrutinio[i] < escrutinio[j]) \implies 0 \leq i \leq |escrutinio| - 2 \wedge 0 \leq j < |escrutinio| - 1 \wedge (\forall t : \mathbb{Z})(0 \leq t < i \wedge escrutinio[t] \neq escrutinio[j] \implies escrutinio[i] \geq escrutinio[t])$

Como escrutinio[k] $<$ escrutinio[i] $\wedge$ escrutinio[k] $\geq$ escrutinio[t] $\implies$ escrutinio[i] $\geq$ escrutinio[t]

$\equiv True$

I $\wedge$ B$_c$ $\wedge$ $\neg$B$_i f$ $\equiv 0 \leq i < |escrutinio| - 1 \ \wedge\ 0 \leq k < i \ \wedge\ 0 \leq j < |escrutinio| - 1 \ \wedge\ (\forall t : \mathbb{Z})(0 \leq t < i \wedge escrutinio[t] \neq escrutinio[j] \implies escrutinio[k] \geq escrutinio[t]) \wedge (\forall x : \mathbb{Z})(0 \leq x < |escrutinio| - 1 \longrightarrow_L escrutinio[j] \geq escrutinio[x]) \ \wedge\ (escrutinio[k] \geq escrutinio[i] \ \wedge\ escrutinio[i] \geq escrutinio[j])$

wp(skip,E$_0$) $\equiv -1 \leq i \leq |escrutinio| - 2 \ \wedge\ 0 \leq k \leq i \ \wedge\ 0 \leq j < |escrutinio| - 1 \ \wedge\ (\forall t : \mathbb{Z})(0 \leq t \leq i \ \wedge escrutinio[j] \neq escrutinio[t] \implies escrutinio[k] \leq escrutinio[t]) \ \wedge\ (\forall x : \mathbb{Z})(0 \leq x < |escrutinio| - 1 \longrightarrow_L escrutinio[j] \geq escrutinio[x])$

Ahora veo I $\wedge$ B$_c$ $\wedge$ $\neg$B$_i f$ $\implies$ wp(skip,E0)

$0 \leq i < |escrutinio| - 1 \ \wedge\ 0 \leq k < i \ \wedge\ 0 \leq j < |escrutinio| - 1 \ \wedge\ (\forall t : \mathbb{Z})(0 \leq t < i \ \wedge\ escrutinio[t] \neq escrutinio[j] \implies escrutinio[k] \geq escrutinio[t]) \ \wedge\ (\forall x : \mathbb{Z})(0 \leq x < |escrutinio| - 1 \longrightarrow_L escrutinio[j] \geq escrutinio[x]) \wedge (escrutinio[k] \geq escrutinio[i] \ \wedge\ escrutinio[i] \geq escrutinio[j]) \implies -1 \leq i \leq |escrutinio| - 2 \ \wedge\ 0 \leq k \leq i \ \wedge\ 0 \leq j < |escrutinio| - 1 \ \wedge\ (\forall t : \mathbb{Z})(0 \leq t \leq i \ \wedge escrutinio[j] \neq escrutinio[t] \implies escrutinio[k] \leq escrutinio[t]) \ \wedge\ (\forall x : \mathbb{Z})(0 \leq x < |escrutinio| - 1 \longrightarrow_L escrutinio[j] \geq escrutinio[x])$

Todo se implica

$\equiv True$

$((\mathrm{A} \wedge \mathrm{B}_i f \wedge \mathrm{def}(\mathrm{B}_i f)) \implies \mathrm{wp1}) \;\wedge\; ((\mathrm{A} \wedge \neg \mathrm{B}\ _i f \wedge \mathrm{def}(\mathrm{B}_i f)) \implies \mathrm{wp2})$

$\mathrm{True} \wedge True \equiv True$

Teorema de la función variante del ciclo 2

$(\mathbf{I} \wedge \mathbf{fv} \leq \mathbf{0}) \implies \neg\ \mathbf{B}_c$

Defino la función variante como:

$\mathbf{fv} \equiv |escrutinio| - i - 1$

Voy a utilizar el rango de i del I y no(B) para implicar, las demás partes del I implican por restricción

$(\mathbf{I} \wedge \mathbf{fv} \leq 0)\ 0 \leq i \leq |escrutinio| - 1 \;\wedge_L\; |escrutinio| - i - 1 \leq 0$

Despejo escrutinio del yluego derecho y uno con la parte izquierda para hacer la implicación

$\equiv\; 0 \leq i \leq |escrutinio| - 1 \;\wedge_L\; |escrutinio| - 1 \leq i$

$\equiv\; i \;= |escrutinio| - 1 \rightarrow\; i \geq |escrutinio| - 1$

Por lo tanto la implicación es verdadera

$\{\ \mathbf{I} \wedge \mathbf{B}_c \wedge \mathbf{fv{=}v0}\ \}\ \mathbf{S}\ \{\ \mathbf{fv} < \mathbf{v}_0\ \}$

Empiezo haciendo la wp(i:=i+1,$|escrutinio|$**-i-1<v0)**

wp(i :=i+1,$|escrutinio|$**-i-1** $<$ $\mathbf{v}_0$)

$\equiv\; def(i := i + 1) \;\wedge_L\; |escrutinio| - i - 2 < v0$

$\equiv\; |escrutinio| - i - 2 < v0$

wp(If escrutinio[j]<escrutinio[i] $\wedge escrutinio[i] < escrutinio[j]\ then\ S1\ elseskip\ fi, wp(i := i + 1, fv < v0))$

como fv<v0 no varía dentro del IF, lo unico que importa son las restricciones de rango de la guarda del IF, puedo terminar concluyendo que:

$\equiv\; |escrutinio| - i - 2 < v0 \;\wedge\; 0 \leq i \leq |escrutinio| \;\wedge_L\; 0 \leq j \leq |escrutinio| \;\wedge_L\; 0 \leq k \leq |escrutinio|$

Uno los rangos de I y lo uno con la guarda de Bc y fv=v0 e implico con lo de arriba. Recordación A es el rango de j
$\mathbf{0} \leq k < i \;\wedge_L\; A \;\wedge_L\; 0 \leq i < |escrutinio| - 1 \;\wedge_L\; |escrutinio| - i - 1 = v0 \implies |escrutinio| - i - 2 < v0 \;\wedge\; 0 \leq i \leq |escrutinio| \;\wedge_L\; 0 \leq j \leq |escrutinio| \;\wedge_L\; 0 \leq k \leq |escrutinio|$

los rangos del antecedente implican al consecuente, vamos a analizar v0

$|escrutinio|$**-i-1** $=$ **v0** $\rightarrow\; |escrutinio| - i - 2 < v0$

$\equiv\; |escrutinio| - i - 2 < |escrutinio| - i - 1$

$\equiv\; 0 < 1$
Luego, se puede concluir que el ciclo termina.

Finalemente sabemos que se cumple $\{P_3\}$ **ciclo_2** $\{Q_3\}$
y que también, trivialmente $Q_3 \implies P_4$

Ahora se tiene que probar que:
$\{P_2\}\ i := 1; k := 0\{Q_2\}\ y\ que\ Q_2 \implies P_3$

$\mathbf{P}_2 \equiv 0 \leq j < |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge \ |escrutinio| > 2$

$\mathbf{Q}_2 \equiv P_3 \equiv k = 0 \ \wedge \ i = 1 \ \wedge \ 0 \leq j < |escrutinio| - 1 \wedge_L (\forall t : \mathbb{Z})(0 \leq t < |escrutinio| - 1 \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \ \wedge \ |escrutinio| > 2$

Calculo wp(i:=1 wp(k:=0,Q$_2$))

wp(i:=1, wp(k:=0,Q$_2$)) $\equiv 0 \leq j < |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge |escrutinio| > 2$

Luego, trivialmente P$_2$ $\implies wp(i := 1, \ wp(k := 0, Q_2)$
Valiendo así la tripla de Hoare
Y también Q$_2$ $\implies P_3$

Primer Ciclo
Ahora se tiene que probar que vale:
{P_1} ciclo1 {Q_1} y que vale que Q_1 $\implies P\_2$
Teorema del Invariante del primer ciclo

$\mathbf{P}_1 \equiv i = 1 \wedge j = 0 \wedge |escrutinio| > 2$

$\mathbf{Q}_1 \equiv 0 \leq j < |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge |escrutinio| > 2$

$\mathbf{B}_c \equiv i < |escrutinio| - 1$

$\mathbf{I} \equiv 0 \leq j < i \ \wedge_L \ 0 \leq i \leq |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge |escrutinio| > 2$

Vale trivialemente $Q_1 \implies P_2$

$\mathbf{P}_1 \implies \mathbf{I}$

$\equiv i = 1 \wedge j = 0 \wedge |escrutinio| > 2 \implies 0 \leq j < i \ \wedge_L \ 0 \leq i \leq |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge |escrutinio| > 2$

Reemplazo i=1 y j=0

$\equiv i = 1 \wedge j = 0 \wedge |escrutinio| > 2 \implies 0 \leq 0 < 1 \ \wedge_L \ 0 \leq 1 \leq |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < 1 \longrightarrow_L escrutinio[0] \geq escrutinio[t])$
$\equiv i = 1 \wedge j = 0 \wedge |escrutinio| > 2 \implies True \ \wedge_L \ True \ \wedge_L \ t = 0 \longrightarrow_L escrutinio[0] \geq escrutinio[t])$
$\equiv i = 1 \wedge j = 0 \wedge |escrutinio| > 2 \implies True \ \wedge_L \ True \ \wedge_L \ t = 0 \longrightarrow_L escrutinio[0] \geq escrutinio[0]$
$\equiv i = 1 \wedge j = 0 \wedge |escrutinio| > 2 \implies True \ \wedge_L \ True \ \wedge_L \ t = 0 \longrightarrow_L True$
$\equiv i = 1 \wedge j = 0 \wedge |escrutinio| > 2 \implies True$
$\equiv True$

$(\mathbf{I} \wedge \neg \mathbf{B}) \implies \mathbf{Q}_1$

$\mathbf{I} \wedge \neg \mathbf{B} \equiv 0 \leq j < i \ \wedge_L \ i = |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \ \wedge |escrutinio| > 2$

Ahora veo que $(\mathbf{I} \wedge \neg \mathbf{B}) \implies \mathbf{Q}_1$

$\equiv 0 \leq j < i \wedge_L i = |escrutinio| - 1 \wedge_L (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge |escrutinio| > 2 \implies 0 \leq j < |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \ \wedge |escrutinio| > 2$

Reemplazo i = $|escrutinio|$**-1**

$\equiv 0 \leq j < |escrutinio| - 1 \wedge_L i = |escrutinio| - 1 \wedge_L (\forall t : \mathbb{Z})(0 \leq t < |escrutinio| - 1 \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \ \wedge |escrutinio| > 2 \implies 0 \leq j < |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < |escrutinio| - 1 \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \ \wedge |escrutinio| > 2$

Implica todo

$\equiv True$

{ **I** $\wedge$ **B** } **S** { **I** }

$\equiv (I \wedge \mathbf{B}) \implies wp(S, I))$

wp(i:=i+1,I)

$\equiv 0 \leq j < i+1 \ \wedge_L \ 0 \leq i+1 \leq |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i+1 \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge |escrutinio| > 2$

$\equiv 0 \leq j \leq i \ \wedge_L \ -1 \leq i \leq |escrutinio| - 2 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t \leq i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge |escrutinio| > 2 \equiv E_0$

wp(if escrutinio[j] $<$ escrutinio[i] then j:=i else skip fi,E$_0$)

$\equiv def(escrutinio[j] < escrutinio[i]) \wedge_L ((escrutinio[j] < escrutinio[i] \wedge_L wp(j := i, E_0)) \vee (escrutinio[j] \geq$ **escrutinio[i]**$) \ \wedge_L \ wp(skip, E_0))$

Usamos un formula equivalente a
A $\implies$ def(B$_i f$) $\wedge_L$ ((B$_i f$ $\wedge_L$ wp1) $\vee$ ($\neg$ B$_i f$ $\wedge_L$ wp2)
$\equiv$
((A $\wedge$ B$_i f$ $\wedge$ def(B$_i f$)) $\implies$ wp1) $\wedge$ ((A $\wedge$ $\neg$B $_i f$ $\wedge$ def(B$_i f$)) $\implies$ wp2)

((I $\wedge$ B$_c$) $\wedge$ B$_i f$ $\wedge$ def(B$_i f$)) $\implies$ wp(j:=i,E$_0$))

(I $\wedge$ B$_c$) $\wedge$ B$_i f$ $\equiv 0 \leq j < i \ \wedge_L \ 0 \leq i < |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge$ **escrutinio[j]** $<$ **escrutinio[i]** $\wedge |escrutinio| > 2$

wp(j:=i, E$_0$)

$\equiv 0 \leq i \leq i \ \wedge_L \ -1 \leq i \leq |escrutinio| - 2 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t \leq i \longrightarrow_L escrutinio[i] \geq escrutinio[t]) \wedge |escrutinio| > 2$

$\equiv 0 \leq i \leq |escrutinio| - 2 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t \leq i \longrightarrow_L escrutinio[i] \geq escrutinio[t]) \wedge |escrutinio| > 2$

$\equiv 0 \leq i \leq |escrutinio| - 2 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[i] \geq escrutinio[t]) \wedge escrutinio[i] \geq escrutinio[i] \wedge |escrutinio| > 2$

$\equiv 0 \leq i \leq |escrutinio| - 2 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[i] \geq escrutinio[t]) \wedge |escrutinio| > 2$

Ahora veo que (I $\wedge$ B$_c$ $\wedge$ B$_i f$ $\wedge$ def(B$_i f$)) $\implies$ wp(j:=i,E$_0$))

$\mathbf{0} \leq j < i \ \wedge_L \ 0 \leq i < |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge$ **escrutinio[j]** $<$ **escrutinio[i]** $\wedge |escrutinio| > 2 \implies 0 \leq i \leq |escrutinio| - 2 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[i] \geq escrutinio[t]) \wedge |escrutinio| > 2$

Implica todo

$\equiv True$

((I $\wedge$ B$_c$) $\wedge$ $\neg$B$_i f$ $\wedge$ def(B$_i f$)) $\implies$ wp(skip,E$_0$))

((I $\wedge$ B$_c$) $\wedge$ $\neg$B$_i f$) $\equiv 0 \leq j < i \ \wedge_L i = |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge escrutinio[j] \geq escrutinio[i] \wedge |escrutinio| > 2$

wp(skip, E$_0$) $\equiv 0 \leq j \leq i \ \wedge_L \ -1 \leq i \leq |escrutinio| - 2 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t \leq i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge |escrutinio| > 2$

Ahora veo que $((\mathbf{I} \wedge \mathbf{B}_c) \wedge \neg \mathbf{B}_i f \wedge \mathbf{def}(\mathbf{B}_i f)) \implies \mathbf{wp(skip,E_0)})$

$\equiv 0 \leq j < i \ \wedge_L \ i = |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge escrutinio[j] \geq escrutinio[i] \wedge |escrutinio| > 2 \implies 0 \leq j \leq i \wedge_L -1 \leq i \leq |escrutinio| - 2 \wedge_L (\forall t : \mathbb{Z})(0 \leq t \leq i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge |escrutinio| > 2$

Se implica todo

$\equiv True$

Con esto se demuestra su parcial correctitud

Teorema de la función variante

$(\mathbf{I} \wedge \mathbf{fv} \leq \mathbf{0}) \implies \neg \mathbf{B}$

Defino la función variante como:

$\mathbf{fv} \equiv |escrutinio| - i - 1$

$(\mathbf{I} \wedge \mathbf{fv} \leq 0) \equiv 0 \leq j < i \ \wedge_L \ 0 \leq i \leq |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \ \wedge \ |escrutinio| - i - 1 \leq 0 \ \wedge |escrutinio| > 2$

$\neg \mathbf{B} \equiv i \geq |escrutinio| - 1$

$\equiv 0 \leq j < i \ \wedge_L \ 0 \leq i \leq |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \ \wedge |escrutinio| - i - 1 \leq 0 \implies i \geq |escrutinio| - 1 \ \wedge |escrutinio| > 2$

$\equiv 0 \leq j < i \ \wedge_L \ 0 \leq i \leq |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \ \wedge |escrutinio| - 1 \leq i \implies i \geq |escrutinio| - 1 \ \wedge |escrutinio| > 2$

$\equiv 0 \leq j < i \ \wedge_L i = |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge \implies i \geq |escrutinio| - 1 \ \wedge |escrutinio| > 2$

$\mathbf{i} = |escrutinio|\mathbf{-1} \implies \mathbf{i} \geq |escrutinio|\mathbf{-1}$

$\equiv True$

$\{ \ \mathbf{I} \wedge \mathbf{B} \wedge \mathbf{v_0} = \mathbf{vf} \ \} \ \mathbf{S} \ \{ \ \mathbf{fv} < \mathbf{v_0} \ \}$

$\mathbf{I} \wedge \mathbf{B} \wedge \mathbf{v_0} = \mathbf{vf} \equiv 0 \leq j < i \ \wedge_L \ 0 \leq i < |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge |escrutinio| - i - 1 \ \wedge |escrutinio| > 2$

$\mathbf{wp(i :=i+1,}|escrutinio|\mathbf{-i-1} < \mathbf{v_0})$
$\equiv \ def(i := i + 1) \ \wedge_L \ |escrutinio| - i - 2 < v0$

$\mathbf{wp(If\ escrutinio[j]} < \mathbf{escrutinio[i]\ then\ S1\ else\ skip\ fi\ ,\ wp(i :=i+1,fv} < \mathbf{v_0}))$

$\equiv \ 0 \leq j < |escrutinio| - 1 \ \wedge_L \ 0 \leq i < |escrutinio| - 1 \ \wedge_L [(escrutinio[j] < escrutinio[i] \ \wedge_L \ |escrutinio| - i - 2 < v_0) \ \vee \ (escrutinio[j] \geq escrutinio[i] \wedge |escrutinio| - i - 2 < v_0)]$

$\equiv 0 \leq j < |escrutinio| - 1 \ \wedge_L \ 0 \leq i < |escrutinio| - 1 \ \wedge \ |escrutinio| - i - 2 < v_0 \ \wedge (escrutinio[j] < escrutinio[i] \vee escrutinio[j] \geq escrutinio[i])$

$\equiv 0 \leq j < |escrutinio| - 1 \ \wedge_L \ 0 \leq i < |escrutinio| - 1 \ \wedge \ |escrutinio| - i - 2 < v_0 \ \wedge True$

$\equiv 0 \leq j < |escrutinio| - 1 \ \wedge_L \ 0 \leq i < |escrutinio| - 1 \ \wedge \ |escrutinio| - i - 2 < v_0$

Ahora quiero ver que $\mathbf{I} \wedge \mathbf{B} \wedge \mathbf{v_0} = \mathbf{vf} \implies \mathbf{wp(S,fv} < \mathbf{v_0})$

$\mathbf{0} \leq j < i \ \wedge_L \ 0 \leq i < |escrutinio| - 1 \ \wedge_L \ (\forall t : \mathbb{Z})(0 \leq t < i \longrightarrow_L escrutinio[j] \geq escrutinio[t]) \wedge |escrutinio| - i - 1 \ \wedge |escrutinio| > 2 \implies 0 \leq j < |escrutinio| - 1 \ \wedge_L \ 0 \leq i < |escrutinio| - 1 \ \wedge |escrutinio| - i - 2 < v_0$

$\equiv |escrutinio| - i - 1 \implies |escrutinio| - i - 2$

$\equiv v_0 \geq fv$

Como se probo que {I $\wedge$ B $\wedge$ $\mathbf{v_0}$ = vf} S {fv $< v_0$} y (I $\wedge\ fv \leq 0) \implies \neg B$) y a su vez se probo el teorema del invariante, queda demostrado la correctitud del programa.

Por lo tanto vale a tripla de Hoare
Ahora toca probar que vale:

{$\mathbf{P_0}$} i:=1, j:=0 {$\mathbf{Q_0}$} y que vale $\mathbf{Q_0} \implies \mathbf{P_1}$

$\mathbf{Q_0} \equiv i = 1 \wedge j = 0 \wedge |escrutinio| > 2$

$\mathbf{P_0} \equiv |escrutinio| > 2$

calculo la wp(i:=1, wp(j:=0,Q)):

wp(i:=1, wp(j:=0,Q)) $\equiv |escrutinio| > 2$

Se ve que vale $\mathbf{P_0} \implies$ wp(i:=1, wp(j:=0,Q) y que también $\mathbf{Q_0} \implies \mathbf{P_1}$, como se quería.

Por último, vamos a demostrar que se cumple P $\implies \mathbf{P_0}$

Si recordamos de la especificación, P es:

TodosDistintos(escrutinio) $\wedge$ todosPositivos(escrutinio) $\wedge$ $|escrutinio| > \mathbf{2}$

Y $\mathbf{P_0}$:

$\mathbf{P_0} \equiv |escrutinio| > 2$

Si hacemos P $\implies \mathbf{P_0}$

Vemos que vale trivialmente.

Luego de lo expuesto, por monotonía, vale que:

P $\implies$ wp(programa completo,Q) y por lo tanto, el programa es correcto respecto a la especificación.