DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Trabajo práctico 1: Especificación y WP

18 de septiembre de 2023 — Algoritmos y Estructuras de Datos

Alias: FKFBPRSYIXBQJXRZHLZP

Integrante	LU	Correo electrónico
Romero Laino, Mauricio	18/23	`mauricioromerolaino@gmail.com`
Chiarizia, Luciano	757/22	`chiarizialuciano@gmail.com`
Manjarín, Santiago	616/22	`santiagomanjarin111@gmail.com`
Coronel, Facundo	445/23	`coronelfacundo30@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. Predicados

Predicados generales

`pred escrutinioValido` (escrutinio: $seq\langle\mathbb{Z}\rangle$) {
$|escrutinio| \geq 2 \land noTieneNegativos(escrutinio) \land noHayEmpate(escrutinio) \land$
$sumatoriaElementos(escrutinio) > 0$
}
`pred noTieneNegativos` (secuencia: $seq\langle\mathbb{Z}\rangle$) {
$(\forall i : \mathbb{Z})(0 \leq i < |secuencia| \rightarrow_L 0 \leq secuencia[i])$
}
`pred noHayEmpate` (escrutinio : $seq\langle\mathbb{Z}\rangle$) {
$(\forall i, j : \mathbb{Z})(0 \leq i, j < |escrutinio| - 1 \rightarrow_L ((i = j) \leftrightarrow (escrutinio[i] = escrutinio[j])))$
}
`pred algunPartidoTieneMas3Porciento` (escrutinio: $seq\langle\mathbb{Z}\rangle$) {
$(\exists i : \mathbb{Z})(0 \leq i < |escrutinio| - 1 \land_L porcentaje(escrutinio[i], escrutinio) \geq 3)$
}

1.1. Predicados del ejercicio 1

`pred unicoPartido` (escrutinio : $seq\langle\mathbb{Z}\rangle$) {
$|escrutinio| = 2$
}
`pred tieneMasDel45` (partido:$\mathbb{Z}$, escrutinio:$seq\langle\mathbb{Z}\rangle$) {
$0 \leq partido < |escrutinio| - 1 \land_L porcentajePartido(escrutinio[partido], escrutinio) \geq 45$
}
`pred tieneMasDel40yDiferencia` (partido:$\mathbb{Z}$, escrutinio:$seq\langle\mathbb{Z}\rangle$) {
$0 \leq partido < |escrutinio| - 1 \land_L porcentajePartido(escrutinio[partido], escrutinio) \geq 40 \land$
$(\forall i : \mathbb{Z})((0 \leq i < |escrutinio| - 1 \land i \neq partido) \rightarrow_L$
$(porcentaje(escrutinio[partido], escrutinio) \geq (porcentaje(escrutinio[i], escrutinio) + 10)))$
}

1.2. Predicados del ejercicio 2

`pred mismaCantidadDeVotos` (escrutinio_presidencial: $seq\langle\mathbb{Z}\rangle$, escrutinio_senadores: $seq\langle\mathbb{Z}\rangle$, escrutinio_diputados: $seq\langle\mathbb{Z}\rangle$) {
$sumatoriaElementos(escrutinio\_presidencial) = sumatoriaElementos(escrutinio\_senadores) \land$
$sumatoriaElementos(escrutinio\_senadores) = sumatoriaElementos(escrutinio\_diputados) \land$
$sumatoriaElementos(escrutinio\_presidencial) = sumatoriaElementos(escrutinio\_diputados)$
}

1.3. Predicados del ejercicio 3

`pred esPartidoGanador` (partido: $\mathbb{Z}$, escrutinio: $seq\langle\mathbb{Z}\rangle$) {
$0 \leq partido < |escrutinio| - 1 \land_L (\forall k : \mathbb{Z})(0 \leq k < |escrutinio| - 1 \rightarrow_L escrutinio[partido] \geq escrutinio[k])$
}
`pred esPartidoSegundo` (partido: $\mathbb{Z}$, partidoGanador: $\mathbb{Z}$, escrutinio: $seq\langle\mathbb{Z}\rangle$) {
$0 \leq partido < |escrutinio| - 1 \land_L (\forall j : \mathbb{Z})((0 \leq j < |escrutinio| - 1 \land j \neq partidoGanador) \rightarrow_L$
$escrutinio[partido] \geq escrutinio[j])$
}

1.4. Predicados del ejercicio 4 y 5

`pred esMatrizDHondt` (matriz: $seq\langle seq\langle\mathbb{Z}\rangle\rangle$, escrutinio: $seq\langle\mathbb{Z}\rangle$, cant_bancas: $\mathbb{Z}$) {
$esMatriz(matriz) \land |matriz| > 0 \land_L |matriz[0]| = cant\_bancas \land_L$
$(\forall indexFila : \mathbb{Z})(0 \leq indexFila < |matriz| \rightarrow_L esReduccionDHondt(matriz[indexFila])) \land$
$noHayRepetidosEnMatriz(matriz) \land esPrimeraColumnaCorrecta(matriz, escrutinio)$
}
`pred esReduccionDHondt` (fila: $seq\langle\mathbb{Z}\rangle$) {
$(\forall i : \mathbb{Z})(0 \leq i < |fila| \rightarrow_L fila[i] = (fila[0]\ div\ i + 1))$
}
`pred esMatriz` (matriz: $seq\langle seq\langle\mathbb{Z}\rangle\rangle$) {
$(\forall\ indexFila : \mathbb{Z})(0 \leq indexFila < |matriz| \rightarrow_L |matriz[0]| = |matriz[indexFila]|)$
}
`pred noHayRepetidosEnMatriz` (matriz: $seq\langle seq\langle\mathbb{Z}\rangle\rangle$) {
$esMatriz(matriz) \land |matriz| > 0 \land_L$
$(\forall i, j, i', j' : \mathbb{Z})((0 \leq i, i' < |matriz| \land 0 \leq j, j' < |matriz[0]|) \rightarrow_L$
$((i = i' \land j = j') \iff (matriz[i][j] = matriz[i'][j'])))$
}
`pred esPrimeraColumnaCorrecta` (matriz: $seq\langle seq\langle\mathbb{Z}\rangle\rangle$, escrutinio: $seq\langle\mathbb{Z}\rangle$) {
$esMatriz(matriz) \land_L noHayRepetidosEnPrimeraColumna(matriz) \land$
$(\forall i : \mathbb{Z})(0 \leq i < |escrutinio| - 1 \rightarrow_L$
$((porcentaje(escrutinio[i], escrutinio) \geq 3) \iff estaEnPrimeraColumna(escrutinio[i], matriz)))$
}
`pred estaEnPrimeraColumna` (matriz: $seq\langle seq\langle\mathbb{Z}\rangle\rangle$, elemento: $\mathbb{Z}$) {
$esMatriz(matriz) \land_L (\exists i : \mathbb{Z})(0 \leq i < |matriz| \land_L elemento = matriz[i][0])$
}
`pred noHayRepetidosEnPrimeraColumna` (matriz: $seq\langle seq\langle\mathbb{Z}\rangle\rangle$) {
$esMatriz(matriz) \land_L (\forall i, j : \mathbb{Z})(0 \leq i, j < |matriz| \rightarrow_L (i = j) \iff (matriz[i][0] = matriz[j][0]))$
}
`pred noTendraRepetidosLaMatriz` (escrutinio: $seq\langle\mathbb{Z}\rangle$, cant_bancas: $\mathbb{Z}$) {
$(\forall i, j, h, h' : \mathbb{Z})$
$((0 \leq i, j < |escrutinio| - 1 \land 1 \leq h, h' \leq cant\_bancas \land_L$
$porcentaje(escrutinio[i], escrutinio) \geq 3 \land porcentaje(escrutinio[j], escrutinio) \geq 3)$
$\rightarrow_L (escrutinio[i]\ div\ h = escrutinio[j]\ div\ h' \iff i = j \land h = h'))$
}

1.5. Predicados del ejercicio 6

`pred listasCorrectas` (listas:$seq\langle seq\langle dni : \mathbb{Z}\ \ \text{x}\ \ genero : \mathbb{Z}\rangle\rangle$) {
$|listas| > 0 \land (\forall i : \mathbb{Z})(0 \leq i < |listas| \rightarrow_L (tienenDnisYGenerosValidos(listas[i]) \land sinDnisRepetidos(listas[i])))$
$\land\ noHayPersonasRepetidas(listas)$
}
`pred tienenDnisYGenerosValidos` (lista:$seq\langle dni : \mathbb{Z}\ \ \text{x}\ \ genero : \mathbb{Z}\rangle$) {
$(\forall i : \mathbb{Z})(0 \leq i < |lista| \rightarrow_L (lista[i]_0 > 0 \land (lista[i]_1 = 1 \lor lista[i]_1 = 2)))$
}
`pred sinDnisRepetidos` (partido:$seq\langle dni : \mathbb{Z}\ \ \text{x}\ \ genero : \mathbb{Z}\rangle$) {
$(\forall i, j : \mathbb{Z})((0 \leq i, j < |partido| \land_L partido[i]_0 = partido[j]_0) \rightarrow_L i = j)$
}
`pred noHayPersonasRepetidas` (listas:$seq\langle seq\langle dni : \mathbb{Z}\ \ \text{x}\ \ genero : \mathbb{Z}\rangle\rangle$) {
$\neg(\exists i, j : \mathbb{Z})(0 \leq i, j < |listas| \land_L i \neq j \land tienenUnaPersonaEnComun(listas[i], listas[j]))$
}
`pred tienenUnaPersonaEnComun` (partido1:$seq\langle dni : \mathbb{Z}\ \ \text{x}\ \ genero : \mathbb{Z}\rangle$, partido2:$seq\langle dni : \mathbb{Z}\ \ \text{x}\ \ genero : \mathbb{Z}\rangle$) {
$(\exists i, j)(0 \leq i < |partido1| \land 0 \leq j < |partido2| \land_L partido1[i]_0 = partido2[j]_0)$
}
`pred cantidadCorrecta` (n:$\mathbb{Z}$, listas:$seq\langle seq\langle dni : \mathbb{Z}\ \ \text{x}\ \ genero : \mathbb{Z}\rangle\rangle$) {
$(\forall i : \mathbb{Z})(0 \leq i < |listas| \rightarrow_L |listas[i]| = n)$
}
`pred alternanDeGenero` (listas:$seq\langle seq\langle dni : \mathbb{Z}\ \ \text{x}\ \ genero : \mathbb{Z}\rangle\rangle$) {
$(\forall i : \mathbb{Z})(0 \leq i < |listas| \rightarrow_L secuenciaDeGeneroCorrecta(listas[i]))$
}
`pred secuenciaDeGeneroCorrecta` (partido:$seq\langle dni : \mathbb{Z}\ \ \text{x}\ \ genero : \mathbb{Z}\rangle$) {
$(\forall i : \mathbb{Z})(0 \leq i < |partido| - 1 \rightarrow_L partido[i]_1 \neq partido[i + 1]_1)$
}

2. Funciones auxiliares

- `aux sumatoriaElementos` (escrutinio:$seq\langle\mathbb{Z}\rangle$) : $\mathbb{Z}$ $= \sum_{i=0}^{|escrutinio|-1} escrutinio[i]$ **;**

- `aux porcentajePartido` (votosPartido:$\mathbb{Z}$, escrutinio:$seq\langle\mathbb{Z}\rangle$) : $\mathbb{Z}$ $= \dfrac{votosPartido * 100}{sumatoriaElementos(escrutinio)}$ **;**

3. Ejercicios

3.1. Ejercicio 1

`proc` `hayBallotage` (in escrutinio: $seq\langle\mathbb{Z}\rangle$) : Bool
`requiere` $\{escrutinioValido(escrutinio)\}$
`asegura` $\{res = True \iff (\neg unicoPartido(escrutinio) \ \wedge \ \neg(\exists\ i:\mathbb{Z})(0 \le i < |escrutinio| - 1 \ \wedge_L (tieneMasDel45(i, escrutinio) \ \vee \ tieneMasDel40yDiferencia(i, escrutinio))))\}$

3.2. Ejercicio 2

`proc` `hayFraude` (in escrutinio_presidencial: $seq\langle\mathbb{Z}\rangle$, in escrutinio_senadores: $seq\langle\mathbb{Z}\rangle$, in escrutinio_diputados: $seq\langle\mathbb{Z}\rangle$) : Bool
`requiere` $\{escrutinioValido(escrutinio\_presidencial) \wedge escrutinioValido(escrutinio\_senadores) \wedge escrutinioValido(escrutinio\_diputados) \wedge |escrutinio\_senadores| \ge 3 \wedge algunPartidoTieneMas3Porciento(escrutinio\_diputados)\}$
`asegura` $\{res = True \iff \neg mismaCantidadVotos(escrutinio\_presidencial, escrutinio\_senadores, escrutinio\_diputados)\}$

3.3. Ejercicio 3

`proc` `obtenerSenadoresEnProvincia` (in escrutinio: $seq\langle\mathbb{Z}\rangle$) : $\mathbb{Z}$x $\mathbb{Z}$
`requiere` $\{escrutinioValido(escrutinio) \wedge |escrutinio| \ge 3\}$
`asegura` $\{esPartidoGanador(res_0, escrutinio) \wedge_L esPartidoSegundo(res_1, res_0, escrutinio)\}$

3.4. Ejercicio 4

`proc` `calcularDHondtEnProvincia` (in cant_bancas: $\mathbb{Z}$, in escrutinio: $seq\langle\mathbb{Z}\rangle$) : $seq\langle seq\langle\mathbb{Z}\rangle\rangle$
`requiere` $\{escrutinioValido(escrutinio) \wedge algunPartidoTieneMas3Porciento(escrutinio) \ \wedge \ 0 < cant\_bancas \ \wedge_L noTendraRepetidosLaMatriz(escrutinio, cant\_bancas)\}$
`asegura` $\{esMatrizDHondt(res, escrutinio, cant\_bancas)\}$

3.5. 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` $\{escrutinioValido(escrutinio) \wedge 0 < cant\_bancas \wedge algunPartidoTieneMas3Porciento(escrutinio) \wedge esMatrizDHondt(dHondt, escrutinio, cant\_bancas)\}$
`asegura` $\{|res| = |escrutinio| - 1 \wedge noTieneNegativos(res) \wedge sumatoriaElementos(res) = cant\_bancas \wedge_L (\forall i, j:\mathbb{Z})((0 \le i, j < |res| \wedge_L res[j] \ne 0) \rightarrow_L (escrutinio[i]\ div\ (res[i] + 1)) \le (escrutinio[j]\ div\ res[j])))\}$

3.6. Ejercicio 6

`proc` `validarListasDiputadosEnProvincia` (in cant_bancas:$\mathbb{Z}$, in listas:$seq\langle seq\langle dni:\mathbb{Z}\ \ x\ \ genero:\mathbb{Z}\rangle\rangle$) : Bool
`requiere` $\{0 < cant\_bancas \wedge listasCorrectas(listas)\}$
`asegura` $\{res = True \iff (cantidadCorrecta(cant\_bancas, listas) \wedge alternanDeGenero(listas))\}$

4. Implementaciones de los ejercicios

4.1. Ejercicio 1

```
res := True
sumaTotal := 0

primero := 0
segundo := 1

i := 0

while i < escrutinio.size():
    sumaTotal := sumaTotal + escrutinio[i]
    i := i+ 1
endwhile

i := 0

while (i<escrutinio.size()-1) do
    if (escrutinio[i]>escrutinio[primero])
        segundo := primero
        primero := i
    else
        skip
    endif
    if (escrutinio[i]>escrutinio[segundo] && escrutinio[i] != escrutinio[primero])
        segundo := i
    else
        skip
    endif

    i := i + 1
endwhile

if (escrutinio.size() == 2)
    res : = False
else
    skip
endif

if (escrutinio[primero] / sumaTotal >= 0.45) || ((escrutinio[primero] / sumaTotal >= 0.40) && ((escrutinio[primero] - escrutinio[segundo]) / sumaTotal >= 0.1)):
    res := False
else
    skip
endif
```

4.2. Ejercicio 2

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

i := 0
votosSenadores := 0
while (i < escrutinio_senadores.size()) do
    votosSenadores := votosSenadores + escrutinio_senadores[i]
    i := i + 1
endwhile

i := 0
votosDiputados := 0
while (i < escrutinio_diputados.size()) do
    votosDiputados := votosDiputados + escrutinio_diputados[i]
    i := i + 1
endwhile

res := ((votosPresidencial != votosSenadores) || (votosSenadores != votosDiputados))
```

4.3. Ejercicio 3

```
i := 0
primero := 0
segundo := 1
while (i<escrutinio.size()-1) do
    if (escrutinio[i]>escrutinio[primero])
        segundo := primero
        primero := i
    else
        skip
    endif
    if (escrutinio[i]>escrutinio[segundo] && escrutinio[i] != escrutinio[primero])
        segundo := i
    else
        skip
    endif

    i := i + 1
endwhile
res := (primero, segundo)
```

4.4. Ejercicio 6

```
res := True
i := 0

while (i < listas.size())
    if (listas[i].size() != cantidad_bancas)
        res := False
    else
        skip
    endif

    j := 0

    while (j < listas[i].size() - 1)
        if (listas[i][j][1] == listas[i][j+1][1])
            res := False
        else
            skip
        endif
        j := j + 1
    endwhile

    i := i + 1
endwhile
```

5. Correctitud de los programas

5.1. Correctitud del ejercicio 2

$Pre \equiv escrutinioValido(escrutinio\_presidencial) \wedge escrutinioValido(escrutinio\_senadores) \wedge escrutinioValido(escrutinio\_diputados) \ \wedge \ |escrutinio\_senadores| \geq 3 \ \wedge \ algunPartidoTieneMas3Porciento(escrutinio\_diputados)$

$S1 \equiv i := 0$

$S2 \equiv votosPresidencial := 0$

$P_{c1} \equiv escrutinioValido(escrutinio\_presidencial) \wedge escrutinioValido(escrutinio\_senadores) \wedge escrutinioValido(escrutinio\_diputados) \wedge |escrutinio\_senadores| \geq 3 \wedge algunPartidoTieneMas3Porciento(escrutinio\_diputados) \wedge i = 0 \wedge votosPresidencial = 0$

$S3 \equiv votosPresidencial := votosPresidencial + escrutinio\_presidencial[i]$

$S4 \equiv i := i + 1$

$Q_{c1} \equiv i = |escrutinio\_presidencial| \wedge votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

$S5 \equiv i := 0$

$S6 \equiv votosSenadores := 0$

$P_{c2} \equiv i = 0 \wedge votosSenadores = 0 \wedge votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

$S7 \equiv votosSenadores := votosSenadores + escrutinio\_senadores[i]$

$S8 \equiv i := i + 1$

$Q_{c2} \equiv i = |escrutinio\_senadores| \wedge votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$
$\wedge\, votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

$S9 \equiv i := 0$

$S10 \equiv votosDiputados := 0$

$P_{c3} \equiv i = 0 \wedge votosDiputados = 0 \wedge votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$
$\wedge\, votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

$S11 \equiv votosDiputados := votosDiputados + escrutinio\_diputados[i]$

$S12 \equiv i := i + 1$

$Q_{c3} \equiv i = |escrutinio\_diputados| \wedge votosDiputados = \sum_{j=0}^{|escrutinio\_diputados|-1} escrutinio\_diputados[j]$
$\wedge\, votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$
$\wedge\, votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

$S13 \equiv res := ((votosPresidencial \,!= votosSenadores) \,||\, (votosSenadores \,!= votosDiputados))$

$Pos \equiv res = True \iff \neg mismaCantidadVotos(escrutinio\_presidencial, escrutinio\_senadores, escrutinio\_diputados)$

Nuestro objetivo es probar que la siguiente tripla de Hoare es válida: $\{Pre\}\ S\ \{Pos\}$, con S haciendo referencia al programa completo. Esta verificación se va a realizar en 7 pasos:

1. Primero voy a probar que $\{Pre\}\ S1, S2\ \{P_{c1}\}$ es verdadero. Lo cual es equivalente a demostrar que $Pre \rightarrow wp(S1; S2, P_{c1})$.
2. En segundo lugar, quiero ver que $\{P_{c1}\}\ S3, S4\ \{Q_{c1}\}$ vale. Esto lo voy a hacer mediante Teorema del Invariante (TDI) y Teorema del variante (TDV).
3. Luego, queremos ver que vale $\{Q_{c1}\}\ S5, S6\ \{P_{c2}\}$. Lo cual es equivalente a demostrar que $Q_{c1} \rightarrow wp(S5; S6, P_{c2})$.
4. Luego, quiero ver que $\{P_{c2}\}\ S7, S8\ \{Q_{c2}\}$ vale. Esto lo voy a hacer mediante TDI y TDV.
5. Luego, queremos ver que vale $\{Q_{c2}\}\ S9, S10\ \{P_{c3}\}$. Lo cual es equivalente a demostrar que $Q_{c2} \rightarrow wp(S9; S10, P_{c3})$.
6. Luego, quiero ver que $\{P_{c3}\}\ S11, S12\ \{Q_{c3}\}$ vale. Esto lo voy a hacer mediante TDI y TDV.
7. Por último, faltaría probar la validez de $\{Q_{c3}\}\ S13\ \{Pos\}$. Lo cual es equivalente a demostrar que $Q_{c3} \rightarrow wp(S13, Pos)$.

Empecemos ...

Demostración de $\{Pre\}\ S1, S2\ \{P_{c1}\}$

Primero quiero calcular $wp(S1, wp(S2, P_{c1}))$.

Recordemos que $S1 \equiv i := 0$ y $S2 \equiv votosPresidencial := 0$

$wp(S2, P_{c1}) \equiv escrutinioValido(escrutinio\_presidencial) \wedge escrutinioValido(escrutinio\_senadores) \wedge$
$escrutinioValido(escrutinio\_diputados) \wedge |escrutinio\_senadores| \geq 3 \wedge$
$algunPartidoTieneMas3Porciento(escrutinio\_diputados)$
$\wedge\ i = 0 \wedge 0 = 0 \equiv E1$

Luego,

$wp(S1, E1) \equiv escrutinioValido(escrutinio\_presidencial) \wedge escrutinioValido(escrutinio\_senadores) \wedge$
$escrutinioValido(escrutinio\_diputados) \wedge |escrutinio\_senadores| \geq 3 \wedge$
$algunPartidoTieneMas3Porciento(escrutinio\_diputados)$
$\wedge\ 0 = 0 \wedge 0 = 0$
$\equiv escrutinioValido(escrutinio\_presidencial) \wedge escrutinioValido(escrutinio\_senadores) \wedge$
$escrutinioValido(escrutinio\_diputados) \wedge |escrutinio\_senadores| \geq 3 \wedge$
$algunPartidoTieneMas3Porciento(escrutinio\_diputados)$
$\equiv E2$

Ahora queremos ver que $Pre \rightarrow E2$

Recordemos que $Pre \equiv escrutinioValido(escrutinio\_presidencial) \wedge escrutinioValido(escrutinio\_senadores) \wedge$
$escrutinioValido(escrutinio\_diputados) \wedge |escrutinio\_senadores| \geq 3 \wedge$
$algunPartidoTieneMas3Porciento(escrutinio\_diputados)$

Podemos observar que $Pre \equiv E2$, por lo tanto podemos afirmar $Pre \rightarrow E2$ y por consecuente $\{Pre\}\ S1, S2\ \{P_c1\}$ como queriamos ver.

Demostracion de $\{P_{c1}\}\ S3, S4\ \{Q_{c1}\}$

- $P_{c1} \equiv escrutinioValido(escrutinio\_presidencial) \wedge escrutinioValido(escrutinio\_senadores) \wedge$
  $escrutinioValido(escrutinio\_diputados) \wedge |escrutinio\_senadores| \geq 3 \wedge$
  $algunPartidoTieneMas3Porciento(escrutinio\_diputados) \wedge i = 0 \wedge votosPresidencial = 0$
- $Q_{c1} \equiv i = |escrutinio\_presidencial| \wedge_L votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
- $I_{c1} \equiv 0 \leq i \leq |escrutinio\_presidencial| \wedge_L votosPresidencial = \sum_{j=0}^{i-1} escrutinio\_presidencial[j]$
- $F_{v1} \equiv |escrutinio\_presidencial| - i$

1. $P_{c1} \rightarrow I_{c1}$

   $i = 0 \wedge votosPresidencial = 0 \wedge escrutinioValido(escrutinio\_diputados) \wedge |escrutinio\_senadores| \geq 3 \wedge$
   $algunPartidoTieneMas3Porciento(escrutinio\_diputados) \rightarrow (0 \leq i \leq |escrutinio\_presidencial| \wedge_L$

$votosPresidencial = \sum_{j=0}^{i-1} escrutinio\_presidencial[j])$

Podemos ver que

- $i = 0 \rightarrow 0 \leq i \leq |escrutinio\_presidencial|$
  i = 0 es parte del subconjunto del consecuente. Por lo tanto, vale la implicación.
- $votosPresidencial = 0 \rightarrow votosPresidencial = \sum_{j=0}^{0-1} escrutinio\_presidencial[j]$
  y esto es igual a $votosPresidencial = 0 \rightarrow votosPresidencial = 0$ (el rango de la sumatoria es válido, ya que en el antecedente i=0)

2. $\{I_{c1} \wedge B_{c1}\}S3, S4\{I_{c1}\}$

   Queremos probar que $(I_{c1} \wedge B_{c1}) \rightarrow wp(S3; S4, I_{c1})$

   $wp(S3; S4, I_{c1}) \equiv wp(S3, wp(S4, I_{c1})) \equiv$

   $wp(S4, I_{c1}) \equiv def(i+1) \wedge 0 \leq i+1 \leq |escrutinio\_presidencial| \wedge_L$
   $votosPresidencial = \sum_{j=0}^{i+1-1} escrutinio\_presidencial[j]$
   $\equiv 0 \leq i+1 \leq |escrutinio\_presidencial| \wedge_L$
   $votosPresidencial = \sum_{j=0}^{i} escrutinio\_presidencial[j] \equiv E1$

   $wp(S3, E1) \equiv def(votosPresidente + escrutinio\_presidencial[i]) \wedge$
   $-1 \leq i \leq |escrutinio\_presidencial| - 1 \wedge_L$
   $votosPresidente = \sum_{j=0}^{i} escrutinio\_presidencial[j] - escrutinio\_presidencial[i]$
   $\equiv 0 \leq i < |escrutinio\_presidencial| \wedge_L$
   $-1 \leq i \leq |escrutinio\_presidencial| - 1 \wedge_L$
   $votosPresidente = \sum_{j=0}^{i-1} escrutinio\_presidencial[j]$
   $\equiv 0 \leq i < |escrutinio\_presidencial| \wedge_L$
   $votosPresidente = \sum_{j=0}^{i-1} escrutinio\_presidencial[j] \equiv E2$

   Ahora revisemos $(I_{c1} \wedge B_{c1}) \rightarrow E2$

   $0 \leq i \leq |escrutinio\_presidencial| \wedge_L i < |escrutinio\_presidencial| \wedge_L$
   $votosPresidencial = \sum_{j=0}^{i-1} escrutinio\_presidencial[j] \wedge i < |escrutinio\_presidencial| \rightarrow$
   $0 \leq i < |escrutinio\_presidencial| \wedge_L votosPresidente = \sum_{j=0}^{i-1} escrutinio\_presidencial[j]$

   a) $0 \leq i \leq |escrutinio\_presidencial| \wedge_L i < |escrutinio\_presidencial| \rightarrow 0 \leq i < |escrutinio\_presidencial|$

      Simplificamos la expresión izquierda y podemos ver que son iguales a ambos lados de la implicación

      $0 \leq i < |escrutinio\_presidencial| \rightarrow 0 \leq i < |escrutinio\_presidencial|$

   b) Tenemos la misma expresión de ambos lados de la implicación. La implicación es True trivialmente.

      $votosPresidencial = \sum_{j=0}^{i-1} escrutinio\_presidencial[j] \rightarrow votosPresidencial = \sum_{j=0}^{i-1} escrutinio\_presidencial[j]$

3. $I_{c1} \wedge \neg B_{c1} \rightarrow Q_{c1}$

   $(0 \leq i \leq |escrutinio\_presidencial| \wedge_L votosPresidencial = \sum_{j=0}^{i-1} escrutinio\_presidencial[j] \wedge$
   $|escrutinio_presidencial| \leq i) \rightarrow$
   $(i = |escrutinio\_presidencial| \wedge_L votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j])$

   Podemos ver que la intersección de las cotas para i

   $$0 \leq i \leq |escrutinio\_presidencial| \wedge |escrutinio\_presidencial| \leq i$$

   Nos termina dejando con

   $$i = |escrutinio\_presidencial|$$

   $i = |escrutinio\_presidencial| \wedge_L votosPresidencial = \sum_{j=0}^{i-1} escrutinio\_presidencial[j] \rightarrow$
   $i = |escrutinio\_presidencial| \wedge_L votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

Reemplazo el i en la sumatoria y finalmente nos queda el mismo predicado de ambos lados de la implicación.

$i = |escrutinio\_presidencial| \wedge_L votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \rightarrow$
$i = |escrutinio\_presidencial| \wedge_L votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

$$\equiv True$$

4. $\{I_{c1} \wedge B_{c1} \wedge F_{v1} = V_0\} S3, S4 \{F_{v1} < V_0\}$

   Recordemos que $F_{v1} \equiv |escrutinio\_presidencial| - i$

   Queremos probar que $(I_{c1} \wedge B_{c1} \wedge F_{v1} = V_0) \rightarrow wp(S3; S4, F_{v1})$

   Vamos a comenzar calculando $wp(S3; S4, F_{v1})$

   $wp(votosPresidencial := votosPresidencial + escrutinio\_presidencial[i]; i := i+1, |escrutinio\_presidencial| - i < V_0)$
   $\equiv wp(votosPresidencial := votosPresidencial + escrutinio\_presidencial[i], wp(i := i+1, |escrutinio\_presidencial| - i < V_0))$

   Empecemos con $wp(i := i+1, |escrutinio\_presidencial| - i < V_0)$

   $wp(i := i+1, |escrutinio\_presidencial| - i < V_0) \equiv def(i+1) \wedge |escrutinio\_presidencial| - (i+1) < V_0 \equiv E_2$

   Ahora veamos $wp(votosPresidencial := votosPresidencial + escrutinio\_presidencial[i]; E_2)$

   $wp(votosPresidencial := votosPresidencial + escrutinio\_presidencial[i]; E_2)$
   $\equiv def(votosPresidencial + escrutinio\_presidencial[i]) \wedge |escrutinio\_presidencial| - (i+1) < V_0$
   $\equiv |escrutinio\_presidencial| - i - 1 < V_0$

   Por el antecedente, tenemos que $|escrutinio\_presidencial| - i = V_0$, por lo tanto, en el consecuente podemos reemplazar ese término por V_0:

   $V_0 - 1 < V_0$, y eso vale siempre.

   Con esto probamos $\{I_{c1} \wedge B_{c1} \wedge F_{v1} = V_0\} S3, S4 \{F_{v1} < V_0\}$

5. $I_{c1} \wedge F_{v1} \leq 0 \rightarrow \neg B_{c1}$

   $I_{c1} \wedge F_{v1} \leq 0 \equiv 0 \leq i \leq |escrutinio\_presidencial| \wedge_L votosPresidencial = \sum_{j=0}^{i-1} escrutinio\_presidencial[j] \wedge$
   $|escrutinio\_presidencial| - i \leq 0 \equiv i = |escrutinio\_presidencial| \wedge votosPresidencial = \sum_{j=0}^{i-1} escrutinio\_presidencial[j]$

   $\neg B_{c1} \equiv |escrutinio\_presidencial| \leq i$

   Por hipótesis tengo que $i = |escrutinio\_presidencial|$ y reemplazando en mi consecuente me queda:
   $|escrutinio\_presidencial| \leq |escrutinio\_presidencial|$ lo cual es verdadero siempre.

   En conclusión, $I_{c1} \wedge F_{v1} \leq 0 \rightarrow \neg B_{c1}$.

Demostración de $\{Q_{c1}\}\ S5, S6\ \{P_{c2}\}$

Para demostrar esto vamos a tener que ver que $Q_{c1} \rightarrow wp(S5, wp(S6, P_{c2}))$

Recordemos que $Q_{c1} \equiv i = |escrutinio\_senadores| \wedge votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
$P_{c2} \equiv i = 0 \wedge votosSenadores = 0 \wedge_L votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
$S6 \equiv votosSenadores := 0$ y $S5 \equiv i := 0$

Ahora veamos lo que vale $wp(S5, wp(S6, P_{c2}))$

$wp(S6, P_{c2}) \equiv i = 0 \wedge 0 = 0 \wedge_L votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \equiv E1$

Ahora veamos $wp(S5, E1)$

$wp(S5, E1) \equiv 0 = 0 \wedge 0 = 0 \wedge votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
$\equiv votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \equiv E2$

Ahora queremos probar $Q_{c1} \rightarrow E2$

Podemos ver que esto vale, ya que $votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$ aparece en ambos lados de la implicación, por lo tanto, es verdadero.

Con esto probamos que $\{Q_{c1}\}\ S5, S6\ \{P_{c2}\}$

Demostración de $\{P_{c2}\}\ S7, S8\ \{Q_{c2}\}$

- $P_{c2} \equiv i = 0 \wedge_L votosSenadores = 0 \wedge votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
- $Q_{c2} \equiv i = |escrutinio\_senadores| \wedge_L votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$
$\wedge\ votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
- $I_{c1} \equiv 0 \leq i \leq |escrutinio\_senadores| \wedge_L votosSenadores = \sum_{j=0}^{i-1} escrutinio\_senadores[j] \wedge votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
- $F_{v1} \equiv |escrutinio\_senadores| - i$

1. $P_{c2} \rightarrow I_{c2}$
$(i = 0 \wedge votosSenadores = 0 \wedge votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]) \rightarrow$
$(0 \leq i \leq |escrutinio\_senadores| \wedge_L votosSenadores = \sum_{j=0}^{i-1} escrutinio\_senadores[j] \wedge$
$votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j])$

   Podemos ver que

   - $i = 0 \rightarrow 0 \leq i \leq |escrutinio\_senadores|$
   i = 0 es parte del subconjunto del consecuente. Por lo tanto vale la implicacion.
   - $votosSenadores = 0 \rightarrow votosSenadores = \sum_{j=0}^{0-1} escrutinio\_senadores[j]$
   y esto es igual a $votosSenadores = 0 \rightarrow votosSenadores = 0$ (el rango de la sumatoria es válido, ya que i=0 en el antecedente)
   - Finalmente tenemos esta tautología:
   $votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \rightarrow$
   $votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

2. $\{I_{C2} \wedge B_{C2}\} S7, S8 \{I_{C2}\}$

   Recordemos que $S7 \equiv votosSenadores := votosSenadores + escrutinio\_senadores[i]$ y $S8 \equiv i := i + 1$

   Queremos probar que $(I_{C2} \wedge B_{C2}) \rightarrow wp(S7; S8, I_{C2})$

   $wp(S7; S8, I_{C2}) \equiv wp(S7, wp(S8, I_{C2})) \equiv$

   $wp(S8, I_{C2}) \equiv def(i + 1) \wedge 0 \leq i + 1 \leq |escrutinio\_senadores| \wedge_L$
   $votosSenadores = \sum_{j=0}^{i+1-1} escrutinio\_senadores[j] \wedge$
   $votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
   $\equiv 0 \leq i + 1 \leq |escrutinio\_senadores| \wedge_L votosPresidencial = \sum_{j=0}^{i} escrutinio\_senadores[j]$
   $\wedge_L votosSenadores = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \equiv E1$

   $wp(S7, E1) \equiv def(votosSenadores + escrutinio\_senadores[i]) \wedge_L$
   $-1 \leq i \leq |escrutinio\_senadores| - 1 \wedge_L votosSenadores = \sum_{j=0}^{i} escrutinio\_senadores[j] - escrutinio\_senadores[i]$
   $\wedge\ votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
   $\equiv 0 \leq i < |escrutinio\_senadores| \ \wedge_L\ -1 \leq i \leq |escrutinio\_senadores| - 1 \ \wedge_L$
   $votosSenadores = \sum_{j=0}^{i-1} escrutinio\_senadores[j]$

$\wedge\ votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
$\equiv 0 \leq i < |escrutinio\_senadores| \wedge_L votosSenadores = \sum_{j=0}^{i-1} escrutinio\_senadores[j] \wedge$
$votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \equiv E2$

Ahora revisemos $(I_{C2} \wedge B_{C2}) \rightarrow E2$

$(0 \leq i \leq |escrutinio\_senadores| \wedge_L i < |escrutinio\_senadores| \wedge_L$
$votosSenadores = \sum_{j=0}^{i-1} escrutinio\_senadores[j] \wedge i < |escrutinio\_senadores|$
$\wedge\ votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]) \rightarrow$
$(0 \leq i < |escrutinio\_senadores| \wedge_L votosSenadores = \sum_{j=0}^{i-1} escrutinio\_senadores[j] \wedge$
$votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j])$

a) $0 \leq i \leq |escrutinio\_senadores| \wedge i < |escrutinio\_senadores| \rightarrow 0 \leq i < |escrutinio\_senadores|$

   Simplificamos la expresión izquierda y podemos ver que son iguales a ambos lados de la implicación

   $0 \leq i < |escrutinio\_senadores| \rightarrow 0 \leq i < |escrutinio\_senadores|$

b) Tenemos la misma expresión de ambos lados de la implicación. La implicación es True trivialmente.

   $votosSenadores = \sum_{j=0}^{i-1} escrutinio\_senadores[j] \rightarrow votosSenadores = \sum_{j=0}^{i-1} escrutinio\_senadores[j]$

c) Lo mismo con esta expresión:

   $votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \rightarrow$
   $votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

3. $I_{C2} \wedge \neg B_{C2} \rightarrow Q_{C2}$

   $(0 \leq i \leq |escrutinio\_senadores| \wedge_L votosSenadores = \sum_{j=0}^{i-1} escrutinio\_senadores[j] \wedge$
   $|escrutinio\_senadores| \leq i \wedge votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]) \rightarrow$
   $(i = |escrutinio\_senadores| \wedge votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \wedge$
   $votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j])$

   Podemos ver que la intersección de las cotas para i

   $$0 \leq i \leq |escrutinio\_senadores| \wedge |escrutinio\_senadores| \leq i$$

   Nos termina dejando con

   $$i = |escrutinio\_senadores|$$

   $i = |escrutinio\_senadores| \wedge_L votosSenadores = \sum_{j=0}^{i-1} escrutinio\_senadores[j] \rightarrow$
   $i = |escrutinio\_senadores| \wedge votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$

   Reemplazo el i en la sumatoria y finalmente nos queda el mismo predicado de ambos lados de la implicación.

   $i = |escrutinio\_senadores| \wedge_L votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \rightarrow$
   $i = |escrutinio\_senadores| \wedge_L votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$

   $$\equiv True$$

   Luego $votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j])$ se presenta de la misma forma en ambos lados de la implicación, por lo tanto, vale la misma.

   Con esto, probamos que vale $I_{C2} \wedge \neg B_{C2} \rightarrow Q_{C2}$

4. $\{I_{C2} \wedge B_{C2} \wedge F_{v2} = V_0\} S7, S8 \{F_{v2} < V_0\}$

   Recordemos que $F_{v2} \equiv |escrutinio\_senadores| - i$

   Queremos probar que $(I_{c2} \wedge B_{c2} \wedge F_{v2} = V_0) \rightarrow wp(S7; S8, F_{v2})$

   Vamos a comenzar calculando $wp(S7; S8, F_{v2})$

   $wp(votosSenadores := votosSenadores + escrutinio\_senadores[i]; i := i+1, |escrutinio\_senadores| - i < V_0)$
   $\equiv wp(votosSenadores := votosSenadores + escrutinio\_senadores[i], wp(i := i+1, |escrutinio\_senadores| - i < V_0))$

   Empecemos con $wp(i := i+1, |escrutinio\_senadores| - i < V_0)$

   $wp(i := i+1, |escrutinio\_senadores| - i < V_0) \equiv def(i+1) \wedge |escrutinio\_senadores| - (i+1) < V_0 \equiv E_2$

   Ahora veamos $wp(votosSenadores := votosSenadores + escrutinio\_senadores[i]; E_2)$

   $wp(votosSenadores := votosSenadores + escrutinio\_senadores[i]; E_2)$
   $\equiv def(votosSenadores + escrutinio\_senadores[i]) \wedge |escrutinio\_senadores| - (i+1) < V_0$
   $\equiv |escrutinio\_senadores| - i - 1 < V_0$

   Por el antecedente, tenemos que $|escrutinio\_senadores| - i = V_0$, por lo tanto, en el consecuente podemos reemplazar ese término por V_0:

   $V_0 - 1 < V_0$, y eso vale siempre.

   Con esto probamos $\{I_{C2} \wedge B_{C2} \wedge F_{v2} = V_0\} S11, S12 \{F_{v2} < V_0\}$

5. $I_{C2} \wedge F_{v2} \leq 0 \rightarrow \neg B_{C2}$

   $I_{C2} \wedge F_{v2} \leq 0 \equiv 0 \leq i \leq |escrutinio\_senadores| \wedge_L votosSenadores = \sum_{j=0}^{i-1} escrutinio\_senadores[j] \wedge$
   $votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \wedge |escrutinio\_senadores| - i \leq 0$
   $\equiv i = |escrutinio\_senadores| \wedge_L votosSenadores = \sum_{j=0}^{i-1} escrutinio\_senadores[j] \wedge$
   $votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

   $\neg B_{c1} \equiv |escrutinio\_senadores| \leq i$

   Por hipótesis tengo que $i = |escrutinio\_senadores|$ y reemplazando en mi consecuente me queda:
   $|escrutinio\_senadores| \leq |escrutinio\_senadores|$ lo cual es verdadero siempre.

   En conclusión, $I_{C2} \wedge F_{v2} \leq 0 \rightarrow \neg B_{C1}$.

Demostración de $\{Q_{c2}\}\ S9, S10\ \{P_{c3}\}$

Recordemos que $Q_{c2} \equiv i = |escrutinio\_senadores| \wedge_L votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$
$\wedge\, votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
$P_{c3} \equiv i = 0 \wedge_L votosDiputados = 0 \wedge votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$
$\wedge\, votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
$S9 \equiv i := 0$ y $S10 \equiv votosDiputados := 0$

Ahora queremos ver que $Q_{c2} \ \rightarrow\ wp(S9, wp(S10, P_{c3}))$

Empecemos viendo $wp(S10, P_{c3})$

$wp(S10, P_{c3}) \equiv i = 0 \wedge_L 0 = 0 \wedge votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$
$\wedge\, votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \equiv E1$

Ahora veamos $wp(S9, E1)$

$wp(S9, E1) \equiv 0 = 0 \wedge 0 = 0 \wedge votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$
$\wedge\, votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

$\equiv votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$
$\wedge\ votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \equiv E2$

Nos faltaría probar que $Q_{c2} \ \rightarrow \ E2$

Podemos ver que tanto ($votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$) como ($votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$) aparecen en ambos lados de la implicación, demostrando de esta forma que es verdadera.

Con esto probamos que $\{Q_{C3}\}\ S9, S10\ \{P_{C3}\}$

Demostración de $\{P_{C3}\}\ S11, S12\ \{Q_{C3}\}$

Primero planteo mi invariante de ciclo:
$I_{C3} \equiv 0 \leq i \leq |escrutinio\_diputados| \wedge_L \ votosDiputados = \sum_{j=0}^{i-1} escrutinio\_diputados[j] \wedge$
$votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \wedge$
$votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

Ahora planteo el variante de ciclo:
$F_{v3} \equiv |escrutinio\_diputados| - i$

Recordemos que:
$P_{c3} \equiv i = 0 \wedge_L votosDiputados = 0 \wedge votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$
$\wedge\ votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
$Q_{c3} \equiv i = |escrutinio\_diputados| \wedge_L votosDiputados = \sum_{j=0}^{|escrutinio\_diputados|-1} escrutinio\_diputados[j]$
$\wedge\ \ votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$
$\wedge\ \ votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
$S11 \equiv votosDiputados := votosDiputados + escrutinio\_diputados[i]$
$S12 \equiv i := i + 1$

$B_{c3} \equiv i < |escrutinio\_diputados|$

1. $P_{c3} \rightarrow I_{c3}$

   Esto es lo mismo que decir:

   $i = 0 \wedge_L votosDiputados = 0 \wedge votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$
   $\wedge\ votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \rightarrow$
   $0 \leq i \leq |escrutinio\_diputados| \wedge_L \ votosDiputados = \sum_{j=0}^{i-1} escrutinio\_diputados[j] \wedge$
   $votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \wedge$
   $votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

   Podemos ver que:

   - $i = 0 \rightarrow 0 \leq i \leq |escrutinio\_diputados|$
     i = 0 es parte del subconjunto del consecuente. Por lo tanto, vale la implicación.
   - $votosDiputados = 0 \rightarrow votosDiputados = \sum_{j=0}^{0-1} escrutinio\_Diputados[j]$
     y esto es igual a $votosDiputados = 0 \rightarrow votosDiputados = 0$ (el rango de la sumatoria es válido, ya que en el antecedente i=0)
   - Por otra parte, votosSenadores y votosPresidencial se presentan en ambos lados de la implicación de igual forma, por lo tanto, es válida.

2. $\{I_{c3} \wedge B_{c3}\} S11, S12 \{I_{c3}\}$

   Queremos probar que: $(I_{c3} \wedge B_{c3}) \rightarrow wp(S11; S12, I_{c1})$

$wp(S11; S12, I_{c3}) \equiv wp(S11, wp(S12, I_{c3})) \equiv$

$wp(S12, I_{c3}) \equiv def(i+1) \wedge 0 \leq i+1 \leq |escrutinio\_diputados| \wedge_L \; votosDiputados = \sum_{j=0}^{i+1-1} escrutinio\_diputados[j] \wedge$
$votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \wedge$
$votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
$\equiv 0 \leq i+1 \leq |escrutinio\_diputados| \wedge_L \; votosDiputados = \sum_{j=0}^{i} escrutinio\_diputados[j] \wedge$
$votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \wedge$
$votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \equiv E1$

$wp(S3, E1) \equiv def(votosPresidente + escrutinio\_presidencial[i]) \wedge$
$-1 \leq i \leq |escrutinio\_diputados| - 1 \wedge_L$
$votosDiputados = \sum_{j=0}^{i} escrutinio\_diputados[j] - escrutinio\_presidencial[i] \wedge$
$votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \wedge$
$votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
$\equiv 0 \leq i < |escrutinio\_diputados| \wedge_L -1 \leq i \leq |escrutinio\_diputados| - 1 \wedge_L$
$votosDiputados = \sum_{j=0}^{i-1} escrutinio\_diputados[j] \wedge$
$votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \wedge$
$votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$
$\equiv 0 \leq i < |escrutinio\_diputados| \wedge_L$
$votosDiputados = \sum_{j=0}^{i-1} escrutinio\_diputados[j] \wedge$
$votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \wedge$
$votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \equiv E2$

Ahora revisemos $(I_{c3} \wedge B_{c3}) \to E2$

$0 \leq i \leq |escrutinio\_diputados| \wedge_L \; votosDiputados = \sum_{j=0}^{i-1} escrutinio\_diputados[j] \wedge$
$votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \wedge$
$votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \wedge i < |escrutinio\_diputados| \to$
$0 \leq i < |escrutinio\_diputados| \wedge_L$
$votosDiputados = \sum_{j=0}^{i-1} escrutinio\_diputados[j] \wedge$
$votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \wedge$
$votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

a) $0 \leq i \leq |escrutinio\_diputados| \wedge i < |escrutinio\_diputados| \to 0 \leq i < |escrutinio\_diputados|$

   Simplificamos la expresión izquierda y podemos ver que son iguales a ambos lados de la implicación

   $0 \leq i < |escrutinio\_presidencial| \to 0 \leq i < |escrutinio\_presidencial|$

b) Tenemos la misma expresión de ambos lados de la implicación. La implicación es True trivialmente.

   $votosDiputados = \sum_{j=0}^{i-1} escrutinio\_diputados[j] \to votosDiputados = \sum_{j=0}^{i-1} escrutinio\_diputados[j]$

c) De la misma forma, tenemos la misma expresión de ambos lados para votosSenadores y votosPresidencial.

   $votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \to$
   $votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$

   $votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \to$
   $votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

3. $I_{c3} \wedge \neg B_{c3} \to Q_{c3}$

   Esto es equivalente a decir que:

   $(0 \leq i \leq |escrutinio\_diputados| \wedge_L \; votosDiputados = \sum_{j=0}^{i-1} escrutinio\_diputados[j] \wedge$

$votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \wedge$
$votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \wedge |escrutinio\_diputados| \leq i) \rightarrow$
$(i = |escrutinio\_diputados| \wedge votosDiputados = \sum_{j=0}^{|escrutinio\_diputados|-1} escrutinio\_diputados[j]$
$\wedge\ votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$
$\wedge\ votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

Podemos ver que la intersección de las cotas para i

$$0 \leq i \leq |escrutinio\_diputados| \wedge |escrutinio\_diputadosl| \leq i$$

Nos termina dejando con

$$i = |escrutinio\_diputados|$$

$i = |escrutinio\_diputados| \wedge_L votosDiputados = \sum_{j=0}^{i-1} escrutinio\_diputados[j] \rightarrow$
$i = |escrutinio\_diputados| \wedge votosDiputados = \sum_{j=0}^{|escrutinio\_diputados|-1} escrutinio\_diputados[j]$

Reemplazo el i en la sumatoria y finalmente nos queda el mismo predicado de ambos lados de la implicación.

$i = |escrutinio\_diputados| \wedge votosDiputados = \sum_{j=0}^{|escrutinio\_diputados|-1} escrutinio\_diputados[j] \rightarrow$
$i = |escrutinio\_diputados| \wedge votosDiputados = \sum_{j=0}^{|escrutinio\_diputados|-1} escrutinio\_diputados[j]$

$$\equiv True$$

Por otra parte, $(votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j])$
y $(votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j])$
se presentan iguales en ambos lados del implica, por lo tanto, la implicación es válida

Con esto probamos $I_{c3} \wedge \neg B_{c3} \rightarrow Q_{c3}$

4. $\{I_{C3} \wedge B_{C3} \wedge F_{v3} = V_0\} S11, S12 \{F_{v3} < V_0\}$

Recordemos que $F_{v3} \equiv |escrutinio\_diputados| - i$

Queremos probar que $(I_{C3} \wedge B_{C3} \wedge F_{v3} = V_0) \rightarrow wp(S11; S12, F_{v3})$

Vamos a comenzar calculando $wp(S11; S12, F_{v3})$

$wp(votosDiputados := votosDiputados + escrutinio\_diputados[i]; i := i + 1, |escrutinio\_diputados| - i < V_0)$
$\equiv wp(votosDiputados := votosDiputados + escrutinio\_diputados[i], wp(i := i + 1, |escrutinio\_diputados| - i < V_0))$

Empecemos con $wp(i := i + 1, |escrutinio\_diputados| - i < V_0)$

$wp(i := i + 1, |escrutinio\_diputados| - i < V_0) \equiv def(i + 1) \wedge |escrutinio\_diputados| - (i + 1) < V_0 \equiv E_2$

Ahora veamos $wp(votosDiputados := votosDiputados + escrutinio\_diputados[i]; E_2)$

$wp(votosDiputados := votosDiputados + escrutinio\_diputados[i]; E_2)$
$\equiv def(votosDiputados + escrutinio\_diputados[i]) \wedge |escrutinio\_diputados| - (i + 1) < V_0$
$\equiv |escrutinio\_diputados| - i - 1 < V_0$

Por el antecedente, tenemos que $|escrutinio\_diputados| - i = V_0$, por lo tanto, en el consecuente podemos reemplazar ese término por V_0:

$V_0 - 1 < V_0$, y eso vale siempre.

Con esto probamos $\{I_{C3} \wedge B_{C3} \wedge F_{v3} = V_0\} S11, S12 \{F_{v3} < V_0\}$

5. $I_{C3} \wedge F_{v3} \leq 0 \rightarrow \neg B_{C3}$

$I_{C3} \wedge F_{v3} \leq 0 \equiv 0 \leq i \leq |escrutinio\_diputados| \wedge_L votosDiputados = \sum_{j=0}^{i-1} escrutinio\_diputados[j] \wedge$ $|escrutinio\_senadores| - i \leq 0 \equiv i = |escrutinio\_diputados| \wedge votosDiputados = \sum_{j=0}^{i-1} escrutinio\_diputados[j] \wedge$ $votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \wedge$ $votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

$\neg B_{c1} \equiv |escrutinio\_diputados| \leq i$

Por hipótesis tengo que $i = |escrutinio\_diputados|$ y reemplazando en mi consecuente me queda: $|escrutinio\_diputados| \leq |escrutinio\_diputados|$ lo cual es verdadero siempre.

En conclusión, $I_{C3} \wedge F_{v3} \leq 0 \rightarrow \neg B_{C3}$.

Demostración de $\{Q_{c3}\}\ S13\ \{Pos\}$

Recordemos $S13 \equiv res := ((votosPresidencial\ != votosSenadores)||(votosSenadores\ != votosDiputados))$ y $Pos \equiv res = True \iff \neg mismaCantidadVotos(escrutinio\_presidencial, escrutinio\_senadores, escrutinio\_diputados)$

Podemos observar que $\neg mismaCantidadVotos(escrutinio\_presidencial, escrutinio\_senadores, escrutinio\_diputados)$
$\equiv \{sumatoriaElementos(escrutinio\_presidencial) \neq sumatoriaElementos(escrutinio\_senadores) \vee$
$sumatoriaElementos(escrutinio\_senadores) \neq sumatoriaElementos(escrutinio\_diputados) \vee$
$sumatoriaElementos(escrutinio\_presidencial) \neq sumatoriaElementos(escrutinio\_diputados)\}$
$\equiv$
$\sum_{i=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[i] \neq \sum_{i=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[i] \vee$
$\sum_{i=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[i] \neq \sum_{i=0}^{|escrutinio\_diputados|-1} escrutinio\_diputados[i] \vee$
$\sum_{i=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[i] \neq \sum_{i=0}^{|escrutinio\_diputados|-1} escrutinio\_diputados[i]$
$\equiv$ (por transitividad)
$\sum_{i=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[i] \neq \sum_{i=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[i] \vee$
$\sum_{i=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[i] \neq \sum_{i=0}^{|escrutinio\_diputados|-1} escrutinio\_diputados[i]$

Con esto podemos determinar que
$Pos \equiv res = True \iff$
$\sum_{i=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[i] \neq \sum_{i=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[i] \vee$
$\sum_{i=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[i] \neq \sum_{i=0}^{|escrutinio\_diputados|-1} escrutinio\_diputados[i]$

Ahora me interesa calcular $wp(S13, Pos)$

$wp(S13, Pos) \equiv ((votosPresidencial \neq votosSenadores) \vee (votosSenadores \neq votosDiputados)) = True \iff$
$\sum_{i=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[i] \neq \sum_{i=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[i] \vee$
$\sum_{i=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[i] \neq \sum_{i=0}^{|escrutinio\_diputados|-1} escrutinio\_diputados[i]$
$\equiv E1$

Luego queremos ver que $Q_{c3} \rightarrow E1$

Sabemos que $Q_{c3} \equiv i = |escrutinio\_diputados| \wedge_L votosDiputados = \sum_{j=0}^{|escrutinio\_diputados|-1} escrutinio\_diputados[j]$
$\wedge\ votosSenadores = \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j]$
$\wedge\ votosPresidencial = \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j]$

Para que la implicación sea válida, tenemos que demostrar que pasa cuando el antecedente es verdadero. Sabiendo esto, podemos asumir el valor que van a tomar votosPresidencial, votosSenadores y votosDiputados en el consecuente. Por lo tanto:

$E1 \equiv$
$\sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \neq \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \vee$
$\sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \neq \sum_{j=0}^{|escrutinio\_diputados|-1} escrutinio\_diputados[j] = True \iff$
$\sum_{i=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[i] \neq \sum_{i=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[i] \vee$
$\sum_{i=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[i] \neq \sum_{i=0}^{|escrutinio\_diputados|-1} escrutinio\_diputados[i]$
$\equiv \sum_{j=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[j] \neq \sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \vee$
$\sum_{j=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[j] \neq \sum_{j=0}^{|escrutinio\_diputados|-1} escrutinio\_diputados[j] \iff$

$\sum_{i=0}^{|escrutinio\_presidencial|-1} escrutinio\_presidencial[i] \neq \sum_{i=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[i] \vee$
$\sum_{i=0}^{|escrutinio\_senadores|-1} escrutinio\_senadores[i] \neq \sum_{i=0}^{|escrutinio\_diputados|-1} escrutinio\_diputados[i]$

Ahora podemos ver que esta bi implicación es una tautología, ya que tenemos los mismos predicados en ambos lados de la bi implicación, por ende la bi implicación va a ser siempre verdadera.

De igual forma, comprobamos que $Q_{c3} \rightarrow E1$ y por consiguiente, que vale $\{Q_{c3}\}\ S13\ \{Pos\}$

Conclusión: dividimos al programa en sus 7 etapas: instrucciones de asignación, ciclos y más instrucciones de asignación. Probamos la correctitud de cada parte haciendo esto:

1. $\{Pre\}\ S1, S2\ \{P_c1\}$
2. $\{P_{c1}\}\ S3, S4\ \{Q_{c1}\}$
3. $\{Q_{c1}\}\ S5, S6\ \{P_{c2}\}$
4. $\{P_{c2}\}\ S7, S8\ \{Q_{c2}\}$
5. $\{Q_{c2}\}\ S9, S10\ \{P_{c3}\}$
6. $\{P_{c3}\}\ S11, S12\ \{Q_{c3}\}$
7. $\{Q_{c3}\}\ S13\ \{Pos\}$

Por el axioma de monotonía, dicho procedimiento es equivalente a probar que $\{Pre\}\ S\ \{Pos\}$ vale. Ante todo lo planteado aquello quedó más que claro y podemos decir que dicha tripla de hoare es veraz.

5.2. Correctitud del ejercicio 3

Instrucciones:

$S1 \equiv i := 0; primero := 0; segundo := 1$

$S2 \equiv if(escrutinio[i] > escrutinio[primero])\ then\ segundo := \ primero;\ primero := \ i\ else\ skip\ endif;$

$S3 \equiv if(escrutinio[i] > escrutinio[segundo]\ \&\&\ escrutinio[i]\ ! = escrutinio[primero])\ then\ segundo := \ i\ else\ skip\ endif$

$S4 \equiv i := i + 1$

$C \equiv S2; S3; S4$

$S5 \equiv res := (primero, segundo)$

Precondiciones, poscondiciones y guardas

$Pre \equiv escrutinioValido(escrutinio) \land |escrutinio| \geq 3$

$P_c \equiv i = 0 \land primero = 0 \land segundo = 1 \land escrutinioValido(escrutinio) \land |escrutinio| \geq 3$

$Q_c \equiv i = |escrutinio| - 1 \land 0 \leq primero, segundo < |escrutinio| - 1 \land_L$
$(\forall k : \mathbb{Z})(0 \leq k < |escrutinio| - 1 \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \land_L$
$(\forall j : \mathbb{Z})((0 \leq j < |escrutinio| - 1 \land j \neq primero) \rightarrow_L escrutinio[segundo] \geq escrutinio[j]) \land escrutinioValido(escrutinio) \land$
$|escrutinio| \geq 3$

$Pos \equiv 0 \leq res_0, res_1 < |escrutinio| - 1 \land_L$
$(\forall k : \mathbb{Z})(0 \leq k < |escrutinio| - 1 \rightarrow_L escrutinio[res_0] \geq escrutinio[k]) \land_L$
$(\forall j : \mathbb{Z})((0 \leq j < |escrutinio| - 1 \land j \neq res_0) \rightarrow_L escrutinio[res_1] \geq escrutinio[j])$

$I \equiv 0 \leq i \leq |escrutinio| - 1 \land 0 \leq primero, segundo < |escrutinio| - 1 \land_L$
$(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \land_L$
$(\forall j : \mathbb{Z})((0 \leq j < i \land j \neq primero) \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$
$\land\ escrutinioValido(escrutinio) \land |escrutinio| \geq 3$

Guarda del ciclo:

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

$\neg B \equiv i \geq |escrutinio| - 1$

Guarda del primer if:

$D \equiv escrutinio[i] > escrutinio[primero]$

$\neg D \equiv escrutinio[i] \leq escrutinio[primero]$

Guarda del segundo if:

$H \equiv escrutinio[i] > escrutinio[segundo] \land escrutinio[i] \neq escrutinio[primero]$

$\neg H \equiv escrutinio[i] \leq escrutinio[segundo] \lor escrutinio[i] = escrutinio[primero]$

$I \land B \equiv 0 \leq i, primero, segundo < |escrutinio| - 1 \land_L$
$(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \land_L$
$(\forall j : \mathbb{Z})((0 \leq j < i \land j \neq primero) \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$
$\land\ escrutinioValido(escrutinio) \land |escrutinio| \geq 3$

$I \land \neg B \equiv i = |escrutinio| - 1 \land 0 \leq primero, segundo < |escrutinio| - 1 \land_L$
$(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \land_L$
$(\forall j : \mathbb{Z})((0 \leq j < i \land j \neq primero) \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$
$\land\ escrutinioValido(escrutinio) \land |escrutinio| \geq 3$

Nuestro objetivo es probar que la siguiente tripla de Hoare es válida: $\{Pre\}\ S\ \{Pos\}$. Esta verificación se va a realizar en 3 pasos:

1. Primero voy a probar que $\{Pre\}\ S1\ \{P_c\}$ es verdadero. Lo cual es equivalente a demostrar que $Pre \rightarrow wp(S1, P_c)$.
2. En segundo lugar, quiero ver que $\{P_c\}\ C\ \{Q_c\}$ vale. Esto lo voy a hacer mediante Teorema del Invariante (TDI) y Teorema del variante(TDV).
3. Por último, faltaría probar la validez de $\{Q_c\}\ S5\ \{Pos\}$

Empecemos ...

Demostración de $\{Pre\}\ S1\ \{P_c\}$

En primer lugar, calculemos la $wp(S1, P_c)$.

$wp(S1, P_c) \equiv wp(i := 0; primero := 0; segundo := 1, P_c)$

Aplico el axioma 3. Calculo la primera wp.

$wp(segundo := 1, P_c) \equiv i = 0 \wedge primero = 0 \wedge 1 = 1 \wedge escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3$
$\equiv i = 0 \wedge primero = 0 \wedge escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3 \equiv E1$

$wp(primero := 0; E1) \equiv i = 0 \wedge 0 = 0 \wedge escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3$
$\equiv i = 0 \wedge escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3 \equiv E2$

$wp(i := 0; E2) \equiv 0 = 0 \wedge escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3$
$\equiv escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3 \equiv E3$

Se puede observar que $wp(S1, P_c) \equiv E3 \equiv Pre$. Luego, $Pre \rightarrow wp(S1, P_c)$

Demostración de $\{P_c\}\ C\ \{Q_c\}$

Ahora quiero demostrar la correctitud del ciclo C. Voy a usar TDI y TDV para ver que $\{P_c\}\ C\ \{Q_c\}$ es correcto.

1. Quiero ver que $P_c \rightarrow I$

   $P_c \equiv i = 0 \wedge primero = 0 \wedge segundo = 1 \wedge escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3$

   $I \equiv 0 \leq i \leq |escrutinio| - 1 \wedge 0 \leq primero, segundo < |escrutinio| - 1 \wedge_L$
   $(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \wedge_L$
   $(\forall j : \mathbb{Z})((0 \leq j < i \wedge j \neq primero) \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$
   $\wedge\, escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3$

   Como supongo a P_c verdadero tengo que:

   - $escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3$ aparecen en ambos lados.
   - i=0: $0 \leq 0 \leq |escrutinio| - 1 \wedge_L (\forall k : \mathbb{Z})(0 \leq k < 0 \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \wedge$
     $(\forall j : \mathbb{Z})((0 \leq j < 0 \wedge j \neq primero) \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$.
     - La primera desigualdad es verdadera porque supusimos que $|escrutinio| \geq 3$.
     - Los antecedentes de ambos cuantificadores son falsos, y como estoy en una implicación tengo que esos "predicados" son verdaderos siempre.
   - primero = 0 y segundo = 1: $0 \leq 0, 1 \leq |escrutinio| - 1$. Esta desigualdad también es válida porque sé que $|escrutinio| \geq 3 \equiv |escrutinio| - 1 \geq 2$. Y $0 \leq 0, 1 < 2 \leq |escrutinio| - 1$ es verdadero.

   Se puede observar que por las pruebas anteriores I es verdadero. Luego, $P_c \rightarrow I$.

2. Para probar que $\{I \wedge B\}\ C\ \{I\}$ vale voy a demostrar qué $I \wedge B \rightarrow wp(C, I)$. Empecemos calculando la $wp(C, I)$.

   $C \equiv S2; S3; S4$

   $wp(C, I) \equiv wp(S2; S3; S4, I)$. Voy a usar el axioma 3.

   $wp(S4, I) \equiv wp(i := i + 1, I) \equiv 0 \leq i + 1 \leq |escrutinio| - 1 \wedge 0 \leq primero, segundo < |escrutinio| - 1 \wedge_L$
   $(\forall k : \mathbb{Z})(0 \leq k < i + 1 \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \wedge_L$

$(\forall j:\mathbb{Z})((0 \le j < i+1 \land j \neq primero) \rightarrow_L escrutinio[segundo] \ge escrutinio[j])$
$\land\, escrutinioValido(escrutinio) \land |escrutinio| \ge 3 \equiv F1$

Voy a tener que usar el axioma 4 porque tengo un if.

$wp(S3, F1) \equiv wp(if(escrutinio[i] > escrutinio[segundo]\ \&\&\ escrutinio[i]! = escrutinio[primero])\ then\ segundo := i\ else\ skip\ endif, F1) \equiv 0 \le i, primero, segundo < |escrutinio| \land_L ((H \land wp(segundo := i, F1)) \lor (\neg H \land wp(skip, F1)))$

$wp(segundo := i, F1) \equiv 0 \le i+1 \le |escrutinio| - 1 \land 0 \le primero, i < |escrutinio| - 1 \land_L$
$(\forall k:\mathbb{Z})(0 \le k < i+1 \rightarrow_L escrutinio[primero] \ge escrutinio[k]) \land_L$
$(\forall j:\mathbb{Z})((0 \le j < i+1 \land j \neq primero) \rightarrow_L escrutinio[i] \ge escrutinio[j])$
$\land\, escrutinioValido(escrutinio) \land |escrutinio| \ge 3$

$wp(segundo := i, F1) \land H \equiv 0 \le i+1 \le |escrutinio| - 1 \land 0 \le primero, i < |escrutinio| - 1 \land_L$
$escrutinio[i] > escrutinio[segundo] \land escrutinio[i] \neq escrutinio[primero] \land$
$(\forall k:\mathbb{Z})(0 \le k < i+1 \rightarrow_L escrutinio[primero] \ge escrutinio[k]) \land_L$
$(\forall j:\mathbb{Z})((0 \le j < i+1 \land j \neq primero) \rightarrow_L escrutinio[i] \ge escrutinio[j])$
$\land\, escrutinioValido(escrutinio) \land |escrutinio| \ge 3$

$wp(skip, F1) \equiv F1$ por segundo axioma.

$wp(skip, F1) \land \neg H \equiv 0 \le i+1 \le |escrutinio| - 1 \land 0 \le primero, segundo < |escrutinio| - 1 \land_L$
$(\forall k:\mathbb{Z})(0 \le k < i+1 \rightarrow_L escrutinio[primero] \ge escrutinio[k]) \land_L$
$(\forall j:\mathbb{Z})((0 \le j < i+1 \land j \neq primero) \rightarrow_L escrutinio[segundo] \ge escrutinio[j]) \land (escrutinio[i] \le escrutinio[segundo] \lor escrutinio[i] = escrutinio[primero])$
$\land\, escrutinioValido(escrutinio) \land |escrutinio| \ge 3$

En la conjunción veo que el primer miembro habla sobre los rangos de primero, segundo e i. Luego, usando las reglas de la lógica, puedo reescribir a $0 \le i, primero, segundo < |escrutinio| \land_L ((H \land wp(segundo := i, F1)) \lor (\neg H \land wp(skip, F1)))$ como:

$0 \le i, primero, segundo < |escrutinio| - 1\ \land$
$((escrutinio[i] > escrutinio[segundo] \land escrutinio[i] \neq escrutinio[primero] \land$
$(\forall k:\mathbb{Z})(0 \le k < i+1 \rightarrow_L escrutinio[primero] \ge escrutinio[k]) \land_L$
$(\forall j:\mathbb{Z})(0 \le j < i+1 \land j \neq primero \rightarrow_L escrutinio[i] \ge escrutinio[j]))$
$\land\, escrutinioValido(escrutinio) \land |escrutinio| \ge 3)$
$\lor((\forall k:\mathbb{Z})(0 \le k < i+1 \rightarrow_L escrutinio[primero] \ge escrutinio[k]) \land_L$
$(\forall j:\mathbb{Z})(0 \le j < i+1 \land j \neq primero \rightarrow_L escrutinio[segundo] \ge escrutinio[j]) \land (escrutinio[i] \le escrutinio[segundo] \lor escrutinio[i] = escrutinio[primero]) \land escrutinioValido(escrutinio) \land |escrutinio| \ge 3)$

Veo que $(\forall k:\mathbb{Z})$ y $escrutinioValido(escrutinio)$ y $|escrutinio| \ge 3$ aparecen iguales en ambos términos de la disyunción. Puedo volver a sacar factor común:

$0 \le i, primero, segundo < |escrutinio| - 1 \land_L escrutinioValido(escrutinio) \land |escrutinio| \ge 3 \land (\forall k:\mathbb{Z})(0 \le k < i+1 \rightarrow_L escrutinio[primero] \ge escrutinio[k]) \land$
$(((escrutinio[i] > escrutinio[segundo] \land escrutinio[i] \neq escrutinio[primero]) \land_L$
$(\forall j:\mathbb{Z})((0 \le j < i+1 \land j \neq primero) \rightarrow_L escrutinio[i] \ge escrutinio[j]))$
$\lor((escrutinio[i] \le escrutinio[segundo] \lor escrutinio[i] = escrutinio[primero]) \land (\forall j:\mathbb{Z})((0 \le j < i+1 \land j \neq primero) \rightarrow_L escrutinio[segundo] \ge escrutinio[j]))) \equiv F2$

Ahora veamos la $wp(S2, F2)$

$wp(S2, F2) \equiv wp(if(escrutinio[i] > escrutinio[primero])\ then\ (segundo := primero;\ primero := i)$
$else\ skip\ endif, F2)$
$\equiv 0 \le i, primero < |escrutinio| \land ((D \land wp(segundo := primero; primero := i, F2)) \lor (\neg D \land wp(skip, F2)))$

Voy a resolver primero $wp(segundo := primero; primero := i, F2)$.

- $wp(primero := i, F2) \equiv 0 \le i, segundo < |escrutinio| - 1 \land escrutinioValido(escrutinio) \land |escrutinio| \ge 3 \land_L (\forall k:\mathbb{Z})(0 \le k < i+1 \rightarrow_L escrutinio[i] \ge escrutinio[k]) \land$
$(((escrutinio[i] > escrutinio[segundo] \land escrutinio[i] \neq escrutinio[i]) \land_L$
$(\forall j:\mathbb{Z})((0 \le j < i+1 \land j \neq i) \rightarrow_L escrutinio[i] \ge escrutinio[j])) \lor ((escrutinio[i] \le escrutinio[segundo] \lor escrutinio[i] = escrutinio[i]) \land (\forall j:\mathbb{Z})((0 \le j < i+1 \land j \neq i) \rightarrow_L escrutinio[segundo] \ge escrutinio[j])))$

$\equiv 0 \leq i, segundo < |escrutinio| - 1 \wedge_L escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3 \wedge_L (\forall k : \mathbb{Z})(0 \leq k < i + 1 \rightarrow_L escrutinio[i] \geq escrutinio[k]) \wedge (\forall j : \mathbb{Z})((0 \leq j < i + 1 \wedge j \neq i) \rightarrow_L escrutinio[segundo] \geq escrutinio[j]) \equiv F3$

- $wp(segundo := \ primero; F3) \equiv 0 \leq i, primero < |escrutinio| - 1 \wedge_L escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3 \wedge_L (\forall k : \mathbb{Z})(0 \leq k < i+1 \rightarrow_L escrutinio[i] \geq escrutinio[k]) \wedge (\forall j : \mathbb{Z})(0 \leq j < i+1 \wedge j \neq i \rightarrow_L escrutinio[primero] \geq escrutinio[j])$

- $wp(skip, F2) \equiv F2$

- $D \wedge wp(segundo := \ primero; primero := \ i, F2) \equiv 0 \leq i, primero < |escrutinio| - 1 \wedge_L escrutinio[i] > escrutinio[primero] \wedge escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3 \wedge_L (\forall k : \mathbb{Z})(0 \leq k < i + 1 \rightarrow_L escrutinio[i] \geq escrutinio[k]) \wedge (\forall j : \mathbb{Z})((0 \leq j < i + 1 \wedge j \neq i) \rightarrow_L escrutinio[primero] \geq escrutinio[j])$

- $\neg D \wedge wp(skip, F2) \equiv 0 \leq i, primero, segundo < |escrutinio| - 1 \wedge_L escrutinio[i] \leq escrutinio[primero] \wedge escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3 \wedge (\forall k : \mathbb{Z})(0 \leq k < i + 1 \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \wedge (((escrutinio[i] > escrutinio[segundo] \wedge escrutinio[i] \neq escrutinio[primero]) \wedge_L (\forall j : \mathbb{Z})(0 \leq j < i + 1 \wedge j \neq primero \rightarrow_L escrutinio[i] \geq escrutinio[j])) \vee ((escrutinio[i] \leq escrutinio[segundo] \vee escrutinio[i] = escrutinio[primero]) \wedge (\forall j : \mathbb{Z})((0 \leq j < i + 1 \wedge j \neq primero) \rightarrow_L escrutinio[segundo] \geq escrutinio[j])))$

Quiero demostrar que: $I \wedge B \rightarrow 0 \leq i, primero < |escrutinio| \wedge_L ((D \wedge wp(segundo := \ primero; primero := i, F2)) \vee (\neg D \wedge wp(skip, F2)))$

$I \wedge B \equiv 0 \leq i, primero, segundo < |escrutinio| - 1 \wedge_L$
$(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \wedge_L$
$(\forall j : \mathbb{Z})(0 \leq j < i \wedge j \neq primero \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$
$\wedge\, escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3$

Para dicha implicación podemos notar que como $0 \leq i, primero, segundo < |escrutinio| - 1$ esto va a implicar la primera parte de la conjunción. El rango que aparece en $I \wedge B$ es más fuerte que el que aparece en el consecuente.

Ahora nos queda probar:

$I \wedge B \rightarrow (D \wedge wp(segundo := \ primero; primero := \ i, F2)) \vee (\neg D \wedge wp(skip, F2))$

Con $I \wedge B$ no puedo saber nada exacto sobre el valor de verdad de D. Pero como D es una guarda, sabemos que tiene dos posibles valores: True o False. Voy a dividir mi análisis en los dos casos y probar que si D es verdadero junto a mí $I \wedge B$ puedo implicar al resto de cosas. Y si $\neg D$ es verdadero, también voy a poder implicar el resto de cosas.

Si D es verdadero:

$D \equiv escrutinio[i] > escrutinio[primero]$

$(D \wedge wp(segundo := \ primero; primero := \ i, F2)) \vee (\neg D \wedge wp(skip, F2)) \equiv$
$wp(segundo := \ primero; primero := \ i, F2)$

Mis hipótesis son que D y que $I \wedge B$ son verdaderas. Quiero probar que:

$D \wedge I \wedge B \rightarrow wp(segundo := \ primero; primero := \ i, F2))$

$wp(segundo := \ primero; primero := \ i, F2)) \equiv 0 \leq i, primero < |escrutinio| - 1 \ \wedge_L (\forall k : \mathbb{Z})(0 \leq k < i + 1 \rightarrow_L escrutinio[i] \geq escrutinio[k]) \wedge (\forall j : \mathbb{Z})((0 \leq j < i + 1 \wedge j \neq i) \rightarrow_L escrutinio[primero] \geq escrutinio[j]) \wedge escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3$

- Sobre el rango de i y de primero ya hablamos que nuestro antecedente los implica.

- $escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3$ vale porque aparece en el invariante.

Nos interesa analizar:

$(\forall k : \mathbb{Z})(0 \leq k < i + 1 \rightarrow_L escrutinio[i] \geq escrutinio[k]) \wedge (\forall j : \mathbb{Z})((0 \leq j < i + 1 \wedge j \neq i) \rightarrow_L escrutinio[primero] \geq escrutinio[j])$

- Voy a demostrar que $(\forall k : \mathbb{Z})(0 \leq k < i+1 \rightarrow_L escrutinio[i] \geq escrutinio[k])$ es implicado por el antecedente.

Por mis hipotesis puedo deducir que como $escrutinio[i] > escrutinio[primero]$ y
$(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L escrutinio[primero] \geq escrutinio[k])$ entonces $(\forall k : \mathbb{Z})(0 \leq k < i+1 \rightarrow_L escrutinio[i] \geq escrutinio[k])$ es verdadero y es a lo que queria llegar.

- Ahora demuestro que $(\forall j : \mathbb{Z})((0 \leq j < i+1 \wedge j \neq i) \rightarrow_L escrutinio[primero] \geq escrutinio[j])$ tambien es implicado por el antecedente.

Por mis hipotesis, esto $(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L escrutinio[primero] \geq escrutinio[k])$ es verdadero. Y este predicado es equivalente a $(\forall j : \mathbb{Z})((0 \leq j < i+1 \wedge j \neq i) \rightarrow_L escrutinio[primero] \geq escrutinio[j])$. Esto es debido a que $0 \leq j < i+1 \wedge j \neq i$ se puede pensar como $0 \leq j < i$.

En conclusion, probamos que $D \wedge I \wedge B \rightarrow wp(segundo := \ primero; primero := \ i, F2))$

Si D es falso:

$\neg D \equiv escrutinio[i] \leq escrutinio[primero]$

$(D \wedge wp(segundo := \ primero; primero := \ i, F2)) \vee (\neg D \wedge wp(skip, F2)) \equiv$
$wp(skip, F2) \equiv F2$

Quiero probar esto $\neg D \wedge I \wedge B \rightarrow F2$.

$F2 \equiv 0 \leq i, primero, segundo < |escrutinio| - 1 \wedge_L escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3 \wedge$
$(\forall k : \mathbb{Z})(0 \leq k < i+1 \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \wedge$
$(((escrutinio[i] > escrutinio[segundo] \wedge escrutinio[i] \neq escrutinio[primero]) \wedge_L$
$(\forall j : \mathbb{Z})((0 \leq j < i+1 \wedge j \neq primero) \rightarrow_L escrutinio[i] \geq escrutinio[j]))$
$\vee((escrutinio[i] \leq escrutinio[segundo] \vee escrutinio[i] = escrutinio[primero]) \wedge (\forall j : \mathbb{Z})((0 \leq j < i+1 \wedge j \neq primero) \rightarrow_L escrutinio[segundo] \geq escrutinio[j])))$

- Por el antecedente vemos que $0 \leq i, primero, segundo < |escrutinio| - 1$ es verdadero porque se presenta el mismo rango para las tres variables. Notar que cuando vayamos a hacer las demostraciones, asumimos que los rangos ya fueron demostrados que son validos aca.

-$escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3$ aparecen de la misma forma en el invariante.

- Con estas dos hipotesis $(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \wedge escrutinio[primero] \geq escrutinio[i]$ puedo deducir que $(\forall k : \mathbb{Z})(0 \leq k < i+1 \rightarrow_L escrutinio[primero] \geq escrutinio[k])$ es verdadero.

Ahora me queda analizar esto:

$((escrutinio[i] > escrutinio[segundo] \wedge escrutinio[i] \neq escrutinio[primero]) \wedge_L$
$(\forall j : \mathbb{Z})((0 \leq j < i+1 \wedge j \neq primero) \rightarrow_L escrutinio[i] \geq escrutinio[j]))$
$\vee((escrutinio[i] \leq escrutinio[segundo] \vee escrutinio[i] = escrutinio[primero]) \wedge (\forall j : \mathbb{Z})((0 \leq j < i+1 \wedge j \neq primero) \rightarrow_L escrutinio[segundo] \geq escrutinio[j]))$

Podemos ver que nos queda una nueva disyunción que depende de H.

$H \equiv escrutinio[i] > escrutinio[segundo] \wedge escrutinio[i] \neq escrutinio[primero]$

$\neg H \equiv escrutinio[i] \leq escrutinio[segundo] \vee escrutinio[i] = escrutinio[primero]$

De esta forma podemos reescribir el predicado a analizar como
$(H \wedge_L (\forall j : \mathbb{Z})((0 \leq j < i+1 \wedge j \neq primero) \rightarrow_L escrutinio[i] \geq escrutinio[j])) \vee$
$(\neg H \wedge (\forall j : \mathbb{Z})((0 \leq j < i+1 \wedge j \neq primero) \rightarrow_L escrutinio[segundo] \geq escrutinio[j]))$

Para demostrar esto vamos a tener que volver a dividir en casos. La justificación del porqué es la misma que con D.

Si H es verdadero:

$(H \wedge_L (\forall j:\mathbb{Z})((0 \leq j < i+1 \wedge j \neq primero) \rightarrow_L escrutinio[i] \geq escrutinio[j]))\vee$
$(\neg H \wedge (\forall j:\mathbb{Z})((0 \leq j < i+1 \wedge j \neq primero) \rightarrow_L escrutinio[segundo] \geq escrutinio[j]))$
$\equiv (\forall j:\mathbb{Z})((0 \leq j < i+1 \wedge j \neq primero) \rightarrow_L escrutinio[i] \geq escrutinio[j]) \equiv Z1$

Quiero probar que: $(H \wedge \neg D \wedge I \wedge B) \rightarrow Z1$

Por hipotesis tengo que:
$escrutinio[i] > escrutinio[segundo] \wedge escrutinio[i] \neq escrutinio[primero] \wedge (\forall j:\mathbb{Z})((0 \leq j < i \wedge j \neq primero) \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$.
Todo esto me permite deducir que:
$(\forall j:\mathbb{Z})((0 \leq j < i+1 \wedge j \neq primero) \rightarrow_L escrutinio[i] \geq escrutinio[j])$.

Luego, $(H \wedge \neg D \wedge I \wedge B) \rightarrow Z1$

Si H es falsa:

$(H \wedge_L (\forall j:\mathbb{Z})((0 \leq j < i+1 \wedge j \neq primero) \rightarrow_L escrutinio[i] \geq escrutinio[j]))\vee$
$(\neg H \wedge (\forall j:\mathbb{Z})((0 \leq j < i+1 \wedge j \neq primero) \rightarrow_L escrutinio[segundo] \geq escrutinio[j]))$
$\equiv (\forall j:\mathbb{Z})((0 \leq j < i+1 \wedge j \neq primero) \rightarrow_L escrutinio[segundo] \geq escrutinio[j])) \equiv Z2$

$\neg H \equiv escrutinio[i] \leq escrutinio[segundo] \vee escrutinio[i] = escrutinio[primero]$

Quiero probar que $(\neg H \wedge \neg D \wedge I \wedge B) \rightarrow Z2$

Por hipótesis sé que: $(\forall j:\mathbb{Z})((0 \leq j < i \wedge j \neq primero) \rightarrow_L escrutinio[segundo] \geq escrutinio[j]) \wedge (escrutinio[i] \leq escrutinio[segundo] \vee escrutinio[i] = escrutinio[primero])$. Se puede observar que alguno de los dos términos de mi disyunción debe ser verdadero. Si $escrutinio[i] \leq escrutinio[segundo]$ es verdadero, puedo concluir que $(\forall j:\mathbb{Z})(0 \leq j < i+1 \wedge j \neq primero \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$ también lo es. Por otro lado, si $escrutinio[i] = escrutinio[primero]$ esto ocurre solo si $i = j$ porque tenemos como hipótesis que $escrutinioValido(escrutinio)$ es verdadero y en él se aclara que la secuencia no tenga elementos repetidos. Por lo tanto, si $i = primero \wedge (\forall j:\mathbb{Z})(0 \leq j < i \wedge j \neq primero \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$ podemos concluir que $(\forall j:\mathbb{Z})(0 \leq j < i+1 \wedge j \neq primero \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$ también lo es.

Luego, $(\neg H \wedge \neg D \wedge I \wedge B) \rightarrow Z2$.

Finalmente, abarcamos todos los casos posibles y llegué a qué $\neg D \wedge I \wedge B \rightarrow F2$. Y como ya probé ambos casos de D, $I \wedge B \rightarrow (D \wedge wp(segundo := \ primero; primero := \ i, F2)) \vee (\neg D \wedge wp(skip, F2))$ que es equivalente a mostrar la validez dé $\{I \wedge B\}\ C\ \{I\}$.

3. Quiero probar que $I \wedge \neg B \rightarrow Q_c$

   $I \wedge \neg B \equiv i = |escrutinio| - 1 \wedge 0 \leq primero, segundo < |escrutinio| - 1 \wedge_L$
   $(\forall k:\mathbb{Z})(0 \leq k < i \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \wedge_L$
   $(\forall j:\mathbb{Z})(0 \leq j < i \wedge j \neq primero \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$
   $\wedge\, escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3$

   $Q_c \equiv i = |escrutinio| - 1 \wedge 0 \leq primero, segundo < |escrutinio| - 1 \wedge_L$
   $(\forall k:\mathbb{Z})(0 \leq k < |escrutinio| - 1 \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \wedge_L$
   $(\forall j:\mathbb{Z})(0 \leq j < |escrutinio| - 1 \wedge j \neq primero \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$
   $\wedge\, escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3$

   Vamos a ver que si $I \wedge \neg B$ es verdadero, Q_c también lo es.

   - $i = |escrutinio| - 1 \wedge 0 \leq primero, segundo < |escrutinio| - 1 \wedge escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3$ aparece en $I \wedge \neg B$ y en Q_c.
   - Voy a usar que $i = |escrutinio| - 1 \wedge (\forall k:\mathbb{Z})(0 \leq k < i \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \equiv$ $(\forall k:\mathbb{Z})(0 \leq k < |escrutinio| - 1 \rightarrow_L escrutinio[primero] \geq escrutinio[k])$. Y esto figura en Q_c también.
   - Ahora uso que $i = |escrutinio| - 1 \wedge (\forall j:\mathbb{Z})(0 \leq j < i \wedge j \neq primero \rightarrow_L escrutinio[segundo] \geq escrutinio[j]) \equiv$ $(\forall j:\mathbb{Z})(0 \leq j < |escrutinio| - 1 \wedge j \neq primero \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$. Este también figura en Q_c.

   Luego, por las pruebas anteriores, $I \wedge \neg B \rightarrow Q_c$.

4. Ahora voy a usar el TDV. Empiezo probando que esta tripla es válida $\{I \wedge B \wedge v_0 = fv\}\ C\ \{fv < v_0\}$. Esto equivale a demostrar que $I \wedge B \wedge v_0 = fv \rightarrow wp(C, fv < v_0)$.

$fv = |escrutinio| - 1 - i$

$fv < v_0 \equiv |escrutinio| - 1 - i < v_0$

$I \wedge B \equiv 0 \leq i, primero, segundo < |escrutinio| - 1 \wedge_L P$

$P \equiv (\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \wedge_L$
$(\forall j : \mathbb{Z})(0 \leq j < i \wedge j \neq primero \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$
$\wedge\ escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3$

$I \wedge B \wedge v_0 = fv \equiv 0 \leq i, primero, segundo < |escrutinio| - 1 \wedge_L P \wedge v_0 = |escrutinio| - 1 - i$

Recordemos que $wp(C, fv < v_0) \equiv wp(S2; S3; S4, fv < v_0)$

Empiezo calculando $wp(S4, fv < v_0) \equiv wp(i := i + 1, fv < v_0) \equiv |escrutinio| - 2 - i < v_0 \equiv G1$

Ahora continuo con $wp(S2; S3, G1)$. Se puede observar que tanto en S2 como en S3 la variable i no se modifica. Tampoco la longitud del escrutinio. Luego, en G1 no reemplazo nada nunca. Esta wp sería equivalente a tener las guardas de los ifs definidas y a que valga G1.

$wp(C, fv < v_0) \equiv wp(S2; S3, G1) \equiv 0 \leq i, primero, segundo < |escrutinio| \wedge |escrutinio| - 2 - i < v_0$

Ahora probemos que $I \wedge B \wedge v_0 = fv \rightarrow wp(C, fv < v_0)$.

- Mi hipótesis $0 \leq i, primero, segundo < |escrutinio| - 1$: se puede observar que esto implica a $0 \leq i, primero, segundo < |escrutinio|$ porque es más fuerte.
- Tomando como hipótesis: $v_0 = |escrutinio| - 1 - i$, tenemos que: $|escrutinio| - 2 - i < v_0 \equiv |escrutinio| - 2 - i < |escrutinio| - 1 - i \equiv -1 < 0 \equiv True$.

Probamos que los términos de la conjunción de la wp se ven implicados por $I \wedge B \wedge v_0 = fv$.

Por lo tanto, $I \wedge B \wedge v_0 = fv \rightarrow wp(C, fv < v_0)$.

5. Quiero probar que $I \wedge fv \leq 0 \rightarrow \neg B$

   $\neg B \equiv |escrutinio| - 1 \leq i$

   $I \wedge fv \leq 0 \equiv 0 \leq i \leq |escrutinio| - 1 \wedge 0 \leq primero, segundo < |escrutinio| - 1 \wedge_L P \wedge |escrutinio| - 1 - i \leq 0 \equiv 0 \equiv 0 \leq i \leq |escrutinio| - 1 \wedge 0 \leq primero, segundo < |escrutinio| - 1 \wedge_L P \wedge |escrutinio| - 1 \leq i \equiv i = |escrutinio| - 1 \wedge 0 \leq primero, segundo < |escrutinio| - 1 \wedge_L P$

   Probemos la implicación.

   - Tomando como hipótesis: $i = |escrutinio| - 1$, tenemos que: $|escrutinio| - 1 \leq i \equiv |escrutinio| - 1 \leq |escrutinio| - 1 \equiv True$

   Luego, si $I \wedge fv \leq 0$ es verdadero, $\neg B$ también lo es.

   En conclusión, $I \wedge fv \leq 0 \rightarrow \neg B$.

Por las pruebas de los pasos 1, 2 y 3, el TDI me dice que mi ciclo es parcialmente correcto. Y con los pasos 4 y 5, por TDV sé que mi ciclo termina. En conclusión, probamos que $\{P_c\}\ C\ \{Q_c\}$ es correcto.

Demostración de $\{Q_c\}\ S5\ \{Pos\}$

Para probar que esta tripla de Hoare es verdadera probemos qué $Q_c \rightarrow wp(S5, Pos)$.

Empecemos calculando la $wp(S5, Pos)$.

$wp(S5, Pos) \equiv wp(res := (primero, segundo), Pos) \equiv 0 \leq primero, segundo < |escrutinio| - 1 \wedge_L$
$(\forall k : \mathbb{Z})(0 \leq k < |escrutinio| - 1 \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \wedge_L$
$(\forall j : \mathbb{Z})(0 \leq j < |escrutinio| - 1 \wedge j \neq primero \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$

Reemplacé todas las apariciones de res_0 por primero y las de res_1 por segundo. Recordemos el valor de Q_c.

$Q_c \equiv i = |escrutinio| - 1 \wedge 0 \leq primero, segundo < |escrutinio| - 1 \wedge_L$
$(\forall k : \mathbb{Z})(0 \leq k < |escrutinio| - 1 \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \wedge_L$
$(\forall j : \mathbb{Z})(0 \leq j < |escrutinio| - 1 \wedge j \neq primero \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$
$\wedge\ escrutinioValido(escrutinio) \wedge |escrutinio| \geq 3$

Probemos qué $Q_c \rightarrow wp(S5, Pos)$:

- $0 \leq primero, segundo < |escrutinio| - 1 \wedge_L$
  $(\forall k : \mathbb{Z})(0 \leq k < |escrutinio| - 1 \rightarrow_L escrutinio[primero] \geq escrutinio[k]) \wedge_L$
  $(\forall j : \mathbb{Z})(0 \leq j < |escrutinio| - 1 \wedge j \neq primero \rightarrow_L escrutinio[segundo] \geq escrutinio[j])$ todos estos términos de Pos aparecieron en Q_c. Por lo tanto, Q_c va a implicarlos.

Por la prueba de arriba, $Q_c \rightarrow wp(S5, Pos)$.

Conclusión: dividimos al programa en sus 3 etapas: instrucciones de asignación, ciclo y más instrucciones de asignación. Probamos la correctitud de cada parte haciendo esto:

1. $\{Pre\}\ S1\ \{P_c\} \equiv Pre \rightarrow wp(S1, P_c)$.
2. $\{P_c\}\ C\ \{Q_c\}$
3. $\{Q_c\}\ S5\ \{Pos\} \equiv Q_c \rightarrow wp(S5, Pos)$

Por el axioma de monotonía, dicho procedimiento es equivalente a probar que $\{Pre\}\ S\ \{Pos\}$ vale. Ante todo lo planteado aquello quedó más que claro y podemos decir que dicha tripla de hoare es veraz.