Verificación de programas II: Teorema del Invariante

Román Gorojovsky

Algoritmos y Estructuras de Datos

4 de septiembre de 2024

Plan del día

Plan del día

- Precondición más débil de ciclos
- Teorema del Invariante
- Teorema de Terminación
- Un ejercicio de un parcial
- Correctitud de programas

Precondición más débil

Precondición más débil – Idea informal

Es la P que permite que el programa **S** funcione correctamente, pero restringiendo lo menos posible.

Principio de diseño

Ser cuidadoso con los resultados que se emiten y generoso con los parámetros que se reciben.

Axiomas

Definiciones (copiadas de la teórica)

- **Axioma 1:** $wp(\mathbf{x := E}, Q) \equiv \text{def}(E) \wedge_L Q^x_E$
- **Axioma 2:** $wp(\mathbf{skip}, Q) \equiv Q$
- **Axioma 3:** $wp(\mathbf{S1; S2}, Q) \equiv wp(\mathbf{S1}, wp(\mathbf{S2}, Q))$
- **Axioma 4:** Si $\mathbf{S} = \mathbf{if\ B\ then\ S1\ else\ S2\ endif}$, entonces

$$wp(\mathbf{S}, Q) \equiv def(B) \wedge_L \Big((B \wedge wp(\mathbf{S1}, Q)) \vee (\neg B \wedge wp(\mathbf{S2}, Q))\Big)$$

¿Qué hacemos con los ciclos?

¿Cómo calculo la WP de este programa?

proc sumar(in $s : seq\langle\mathbb{Z}\rangle) : \mathbb{Z}$

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

$Q \equiv \{res = \sum_{i=0}^{|s|-1} s[i]\}$

- A ojo

¿Qué hacemos con los ciclos?

¿Cómo calculo la WP de este programa?

proc sumar(in $s : seq\langle\mathbb{Z}\rangle) : \mathbb{Z}$

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

$Q \equiv \{res = \sum_{i=0}^{|s|-1} s[i]\}$

- A ojo $\longrightarrow WP = \{res = 0 \land i = 0\}$
- ¿Formalmente? ¿Axioma 5? Termina siendo una fórmula infinita (detalles en la teórica)
- Sólo voy a poder probar que la tripla $\{P\}$ S $\{Q\}$ es válida

Invariante de un ciclo

Dado un ciclo de la forma

```
while (B) do
        S1;
        S2;
        // ...
endwhile
```

El **Invariante** del ciclo es

- Un predicado I que se cumple:
  - Antes de "entrar" en el ciclo, es decir, antes de cada iteración
  - Al terminar cada iteración (si se cumplía B)

Teorema del Invariante

Teorema del invariante

Si existe un predicado I tal que ...

1. $P_c \Rightarrow$ I
2. $\{I \wedge B\}$ S $\{I\}$
3. $I \wedge \neg B \Rightarrow Q_c$

entonces el ciclo **while(B)** $\{$**S**$\}$ es *parcialmente correcto* respecto de la especificación (P_c, Q_c).

Teorema del Invariante

Teorema del invariante

Si existe un predicado I tal que ...

1. $P_c \Rightarrow$ I
2. $\{I \land B\}$ S $\{I\}$
3. $I \land \neg B \Rightarrow Q_c$

entonces el ciclo **while(B)** $\{$**S**$\}$ es *parcialmente correcto* respecto de la especificación (P_c, Q_c).

Más tarde vemos qué falta para que sea totalmente correcto

Ejemplo

```
proc sumar(in s : seq⟨Z⟩) : Z
res := 0
i := 0
while (i < s.size()) do
  res := res + s[i];
  i := i + 1
endwhile
```

A

$P = \{ i = 0 \wedge res = 0 \}$

$Q = \{ res = \sum_{i=0}^{|s|-1} s[i] \}$

Ej

$s = [2, 5, 7, 9]$

i: 0, 1, 2, 3 ← $|s|-1$

$I \equiv$

$0 \leq i \leq |s|$

$res = \sum_{j=0}^{i-1} s[j]$

iteraciones	i	res	
0	0	0	$0 = \sum_{i=0}^{0} s[i]$
1	1	2	2
2	2	7	$2 + 5 = \sum_{i=0}^{1} s[i]$
3	3	14	$2 + 5 + 7 = \sum_{i=0}^{2} s[i]$
4	$\boxed{4}$	23	$2 + 5 + 7 + 9$

$$I \equiv 0 \leq i \leq |s| \wedge res = \sum_{\boxed{j=0}}^{i-1} s[j]$$

$j = 0, 1, 2, \ldots i$

$$\cancel{i} \quad \sum_{\boxed{j=0}} \boxed{}$$

$j = 0, 1, 2, \ldots 8$

Ejemplo

proc sumar(in $s : seq\langle\mathbb{Z}\rangle) : \mathbb{Z}$

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

1. $P_c \Rightarrow \mathsf{I}$
2. $\{I \wedge B\}\ \mathsf{S}\ \{I\}$
3. $I \wedge \neg B \Rightarrow Q_c$

- $P_c \equiv \{res = 0 \wedge i = 0\}$
- $Q_c \equiv \{res = \sum_{i=0}^{|s|-1} s[i]\}$
- $B \equiv \{|s| - 1\}$
- $I \equiv \{0 \leq i \leq |s| \wedge res = \sum_{j=0}^{i-1} s[j]\}$

```
proc sumar(in s : seq⟨ℤ⟩) : ℤ
res := 0
i := 0
while (i < s.size()) do
  res := res + s[i];
  i := i + 1
endwhile
```

$\rightarrow$ ❶ $\underline{P_c} \Rightarrow I$

❷ $\{I \wedge B\}$ S $\{I\}$

❸ $I \wedge \neg B \Rightarrow Q_c$

1

- $P_c \equiv \{res = 0 \wedge i = 0\}$ $\Rightarrow$ $I \equiv \{0 \leq i \boxed{\leq} |s| \wedge res = \sum_{j=0}^{i-1} s[j]\}$
- $Q_c \equiv \{res = \sum_{i=0}^{|s|-1} s[i]\}$
- $B = \{ i < |s| \}$.
- $I \equiv \{0 \leq i \leq |s| \wedge res = \sum_{j=0}^{i-1} s[j]\}$

$i=0 \Rightarrow 0 \leq \overset{0}{i} \leq |s|$

$i=0 \Rightarrow 0 \leq 0 \leq |s|$

$res = 0 \wedge i=0 \Rightarrow res = \sum_{j=0}^{\overset{0-1}{i-1}} s[j] = 0$

$res=0 \wedge i=0 \Rightarrow res=0$ ✓

```
proc sumar(in s : seq⟨Z⟩) : Z

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

❶ $P_c \Rightarrow I$
→ ❷ $\{I \land B\}$ S $\{I\}$
→ ❸ $I \land \neg B \Rightarrow Q_c$

- $P_c \equiv \{res = 0 \land i = 0\}$
- $Q_c \equiv \{res = \sum_{i=0}^{|s|-1} s[i]\}$
- $B \equiv$ ~~...~~ $\{i < |s|\}$ $\rightsquigarrow$ $\neg B = i \geq |s|$
- $I \equiv \{0 \leq i \leq |s| \land res = \sum_{j=0}^{i-1} s[j]\}$

$I \land \neg B \equiv 0 \leq i \leq |s| \land res = \sum_{j=0}^{i-1} s[j] \land i \geq |s|$ $\quad$ $i = |s|$ $\quad \equiv$

$\equiv \boxed{i} = |s| \land res = \sum_{j=0}^{i-1} s[j] \equiv i = |s| \land res = \sum_{j=0}^{|s|-1} s[j]$

$I \land \neg B \Rightarrow Q_c$ ✓

```
proc sumar(in s : seq⟨Z⟩) : Z
 res := 0
 i := 0
 while (i < s.size()) do
 S1 res := res + s[i];
 S2 i := i + 1
 endwhile
```

$\underbrace{S_1; S_2}_{S}$

→ ❶ $P_c \Rightarrow I$

→ ❷ $\{I \land B\}\ S\ \{I\}$

❸ $I \land \neg B \Rightarrow Q_c$

$\{I \land B\}\ \boxed{S}\ \{I\} \equiv$

$\equiv \{I \land B\} \Rightarrow wp(S, I)$

- $P_c \equiv \{res = 0 \land i = 0\}$
- $Q_c \equiv \{res = \sum_{i=0}^{|s|-1} s[i]\}$
- $B \equiv \{i < |s|\}$
- $I \equiv \{0 \le i \le |s| \land res = \sum_{j=0}^{i-1} s[j]\}$

$\{I \land B\} \equiv \{0 \le i < |s| \land res = \sum_{j=0}^{i-1} s[j]\}$

ax3

$\{I \land B\} \Rightarrow \underline{wp(S, I)} \equiv wp(S_1; S_2, I) \equiv$

$\equiv wp(S_1, \underbrace{wp(S_2, I)}_{A})) = wp(res = res + s[i], wp(i = i+1, I))$

Ax1

Ⓐ $wp(i = i+1, I) \equiv wp(i = i+1, 0 \le i \le |s| \land res = \sum_{j=0}^{i-1} s[j]) \equiv$

$\equiv \underline{def(i+1)} \land_L 0 \le i+1 \le |s| \land res = \sum_{j=0}^{i} s[j] \equiv$

$\equiv def(i) \land def(1) \land_L 0 \le i+1 \le |s| \land res = \sum_{j=0}^{i} s[j]$

T T

Ax1

$$wp\left(res = res + s[i],\ 0 \leq i+1 \leq |s| \land res = \sum_{j=0}^{i} s[j]\right) \equiv$$

$$\equiv def(res + s[i]) \land_L 0 \leq i+1 \leq |s| \land res + s[i] = \sum_{j=0}^{i} s[j] \equiv$$

$$\equiv \underbrace{def(res)}_{T} \land def(s[i]) \land_L 0 \leq i+1 \leq |s| \land res + s[i] = \sum_{j=0}^{i} s[j] \equiv$$

$$\equiv \underbrace{def(s)}_{T} \land \underbrace{def(i)}_{T} \land 0 \leq i < |s| \land_L 0 \leq i+1 \leq |s| \land res + s[i] = \sum_{j=0}^{i} s[j] \equiv$$

$$\equiv 0 \leq i < |s| \boxed{\land_L} res + \boxed{s[i]} = \sum_{j=0}^{i} s[j] \equiv$$

$$\equiv 0 \leq i < |s| \land_L res = \sum_{j=0}^{i-1} s[j] \equiv wp(S, I)$$

$$res + s[i] = \sum_{j=0}^{i} s[j]$$

$$j = 0, 1, 2, \ldots, i-1, i$$

$$s[0] + s[1] + \ldots s[i-1] + s[i]$$

$$res = \left(\sum_{j=0}^{i} s[j]\right) - s[i]$$

$$res = \sum_{j=0}^{i-1} s[j]$$

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

$$= \{0 \leq i < |s| \wedge res = \sum_{j=0}^{i-1} s[j] \Rightarrow 0 \leq i < |s| \boxed{\wedge_L} \boxed{res = \sum_{j=0}^{i-1} s[j]}$$

- **Axioma 1:** $wp(\textbf{x := E}, Q) \equiv \mathsf{def}(E) \wedge_L Q^x_E$
- **Axioma 2:** $wp(\textbf{skip}, Q) \equiv Q$
- **Axioma 3:** $wp(\textbf{S1; S2}, Q) \equiv wp(\textbf{S1}, wp(\textbf{S2}, Q))$
- **Axioma 4:** Si **S** $=$ **if B then S1 else S2 endif**, entonces

$$\begin{aligned} wp(\textbf{S}, Q) \equiv def(B) \wedge_L \Big(& (B \wedge wp(\textbf{S1}, Q)) \vee \\ & (\neg B \wedge wp(\textbf{S2}, Q)) \Big) \end{aligned}$$

Ejemplo

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

- $P_c \equiv \{res = 0 \wedge i = 0\}$
- $Q_c \equiv \{res = \sum_{i=0}^{|s|-1} s[i]\}$
- $B \equiv \{|s| - 1\}$
- $I \equiv \{0 \leq i \leq |s| \wedge res = \sum_{j=0}^{i-1} s[j]\}$

- $P_c \Rightarrow$ I
  - $0 \leq i \leq |s| \equiv 0 \leq 0 \leq |s|$ ✓
  - $res = \sum_{j=0}^{i-1} s[j] \equiv 0 = \sum_{j=0}^{0-1} s[j] = 0$ ✓

Ejemplo

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

- $P_c \equiv \{res = 0 \wedge i = 0\}$
- $Q_c \equiv \{res = \sum_{i=0}^{|s|-1} s[i]\}$
- $B \equiv \{|s| - 1\}$
- $I \equiv \{0 \leq i \leq |s| \wedge res = \sum_{j=0}^{i-1} s[j]\}$

- $\{I \wedge B\}$ S $\{I\}$
  - $I \wedge B \equiv 0 \leq i_0 < |s| \wedge res_0 = \sum_{j=0}^{i_0-1} s[j]$
  - $i = i_0 + 1 \Rightarrow 0 \leq i_0 + 1 < |s| \rightarrow 0 \leq i \leq |s|$ ✓
  - $res = res_0 + s[i_0] \Rightarrow res = \left(\sum_{j=0}^{i_0-1} s[j]\right) + s[i_0]$
    $\rightarrow res = \sum_{j=0}^{i_0} s[j] \ \rightarrow res = \sum_{j=0}^{i-1} s[j]$ ✓

Ejemplo

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

- $P_c \equiv \{res = 0 \wedge i = 0\}$
- $Q_c \equiv \{res = \sum_{i=0}^{|s|-1} s[i]\}$
- $B \equiv \{|s| - 1\}$
- $I \equiv \{0 \leq i \leq |s| \wedge res = \sum_{j=0}^{i-1} s[j]\}$

- $\{I \wedge B\}\ \mathtt{S}\ \{I\} \leftrightarrow \{I \wedge B\} \rightarrow WP(\mathtt{S}, I)$
  - $WP(\mathtt{S}, I)$
    $\equiv WP(\mathtt{res\ :=\ res\ +\ s[i];\ i\ :=\ i\ +\ 1}, \{0 \leq i \leq |s| \wedge res = \sum_{j=0}^{i-1} s[j]\})$
    $\equiv WP\big(\mathtt{res\ :=\ res\ +\ s[i]}, WP(\mathtt{i\ :=\ i\ +\ 1}, \{0 \leq i \leq |s| \wedge res = \sum_{j=0}^{i-1} s[j]\})\big)$
    $\equiv WP(\mathtt{res\ :=\ res\ +\ s[i]}, 0 \leq i+1 \leq |s| \wedge res = \sum_{j=0}^{i} s[j])$
    $\equiv 0 \leq i+1 \leq |s| \wedge res = \sum_{j=0}^{i-1} s[j])$
  - $\{I \wedge B\} \equiv \{0 \leq |s| - 1 \wedge res = \sum_{j=0}^{i-1} s[j]\}$
  - ¿$\{I \wedge B\} \rightarrow WP(\mathtt{S}, I)$? $\checkmark$

Ejemplo

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

- $P_c \equiv \{res = 0 \land i = 0\}$
- $Q_c \equiv \{res = \sum_{i=0}^{|s|-1} s[i]\}$
- $B \equiv \{|s| - 1\}$
- $I \equiv \{0 \leq i \leq |s| \land res = \sum_{j=0}^{i-1} s[j]\}$

- $I \land \neg B \Rightarrow Q_C$
    - $I \land \neg B \equiv |s| \leq i \leq |s| \land res = \sum_{j=0}^{i-1} s[j]$
      $\equiv i = |s| \land res = \sum_{j=0}^{i-1} s[j]$
      $\equiv res = \sum_{j=0}^{|s|-1} s[j] \equiv Q_c$ ✓

Ejercicios
(Sólo la primer parte)

Práctica 3 segunda parte:

- Ejercicio 6
- Ejercicio 11.c

Ejercicios

(Sólo los tres primeros pasos)

Ejercicio 6. Dado el siguiente problema

proc sumarElementos (in s: $array < \mathbb{Z} >$) : $\mathbb{Z}$ {
    requiere $\{|s| \geq 1 \wedge |s| \textbf{ mod } 2 = 0\}$
    asegura $\{res = \sum_{j=0}^{|s|-1} s[j]\}$
}

Dar un invariante y función variante para cada una de estas posibles implementaciones

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

b)
```
res := 0
i := 0
while (i < s.size()) do
    res := res + s[s.size() − 1 − i];
    i := i + 1
endwhile
```

c)
```
res := 0
i := s.size() − 1
while (i >= 0) do
    res := res + s[i];
    i := i − 1
endwhile
```

d)
```
res := 0
i := 0
while (i > s.size() / 2) do
    res := res + s[i] + s[s.size() − 1 − i];
    i := i + 1
endwhile
```

$I \equiv \ldots i \ldots \wedge res = \sum_{i=0}^{|s|/2} s[j] + s[|s|-j-1]$

Ejercicio 6. Dado el siguiente problema

proc sumarElementos (in s: $array < \mathbb{Z} >$) : $\mathbb{Z}$ {
requiere $\{|s| \geq 1 \land |s| \text{ mod } 2 = 0\}$
asegura $\{res = \sum_{j=0}^{|s|-1} s[j]\}$
}

asegura {res = 8}

b) requiere {
```
res := 0
i := 0
while (i < s.size()) do
    res := res + s[s.size() - 1 - i];
    i := i + 1
endwhile
```
}

Pc →, Qc →

$B = \{i < |s|\} \to \neg B = \{i \geq |s|\}$

S_4 if res = 2 then res = 8

→ $wp(Qc, wp(S_4, ase))$

$P_c = \{|s| \geq 1 \land |s| \text{ mod } 2 = 0 \land res = 0 \land i = 0\}$

$Q_c = \{res = \sum_{j=0}^{|s|-1} s[j]\}$

S $[5, 2, 7, 9] \to |s| = 4$

iteración	i	res
0	0	0
1	1	$\boxed{9}$
2	2	16
3	$\boxed{3}$	18
4	4	

$9 = S[|s|-1-0] = \sum_{j=|s|-1}^{|s|-1} s[j] = \sum_{j=0}^{0} s[|s|-j-1] = S[|s|-1] = 9$

$16 = 7 + 9 = \sum_{j=|s|-2}^{|s|-1} s[j]$

$18 = 2 + 7 + 9 \to \sum_{j=|s|-3}^{|s|-1} s[j]$

$I \equiv 0 \leq i \leq |s| \land \boxed{res = \sum_{j=|s|-i}^{|s|-1} s[j]}$

reemplazo

$res = \sum_{j=0}^{i-1} s[|s|-j-1]$

❶ $P_c \Rightarrow I$

❷ $\{I \wedge B\}\ S\ \{I\}$

❸ $I \wedge \neg B \Rightarrow Q_c$

3

$$\{0 \le i \le |s| \wedge_L res = \sum_{j=0}^{i-1} s[|s|-j-1] \wedge i \geq |s|\} \equiv$$

$$\equiv \{ i = |s| \wedge_L res = \sum_{j=0}^{i-1} s[|s|-j-1] \} \equiv$$

$$\equiv \{ i = |s| \wedge_L res = \sum_{j=0}^{|s|-1} s[|s|-j-1] \} \Rightarrow \{ res = \sum_{j=0}^{|s|-1} s[j] \}$$

$$s[|s|-1] + s[|s|-2] + \dots + s[\underbrace{|s|-(|s|-1)-1}_{0}]$$

$$|s|-|s|+1-1 = 0$$

$$s[0] + \dots s[|s|-1]$$

Ejercicios
(Sólo los tres primeros pasos)

Ejercicio 11. Dados los siguientes ciclos y sus respectivas precondición (P_c) y poscondición (Q_c).

1. Proponer un invariante (I) y una función variante (f_v) para el ciclo
2. Demostrar los siguientes pasos de la demostración de correctitud del ciclo
   i) $P_c \rightarrow I$
   ii) $(I \wedge \neg B) \rightarrow Q_c$
   iii) $(I \wedge f_v \leq 0) \rightarrow \neg B$

c) $P_c \equiv \{i = |s| - 1 \wedge res = 0\}$

while $i \geq 0$ **do**
  $res := res + s[i] + 1;$
  $i := i - 1;$
end

$Q_c \equiv \{res = |s| + \sum_{j=0}^{|s|-1} s[j]\}$

Nos tomemos 15 minutos que llegamos a la mitad

(Si es que no nos tomamos el recreo antes)

¿Qué podemos demostrar hasta ahora?

- Correctitud parcial: Probando las hipótesis que vimos hasta acá sabemos que si el ciclo termina la tripla de Hoare $\{P_c\}$ S $\{Q_c\}$ es válida

¿Qué podemos demostrar hasta ahora?

- Correctitud parcial: Probando las hipótesis que vimos hasta acá sabemos que si el ciclo termina la tripla de Hoare $\{P_c\}$ S $\{Q_c\}$ es válida
- Falta probar que el ciclo efectivamente termine

¿Qué podemos demostrar hasta ahora?

- Correctitud parcial: Probando las hipótesis que vimos hasta acá sabemos que si el ciclo termina la tripla de Hoare $\{P_c\}$ S $\{Q_c\}$ es válida
- Falta probar que el ciclo efectivamente termine
- Teorema de Terminación

Teorema de Terminación

Teorema de Terminación

Si existe una función $fv : \mathbb{V} \to \mathbb{Z}$ tal que

1. $\{I \wedge B \wedge f_v = v_0\}$ S $\{f_v < v_0\}$,
2. $I \wedge f_v \leq 0 \to \neg B$,

Teorema de Terminación

Teorema de Terminación

Si existe una función $fv : \mathbb{V} \to \mathbb{Z}$ tal que

1. $\{I \wedge B \wedge f_v = v_0\}$ S $\{f_v < v_0\}$,
2. $I \wedge f_v \leq 0 \to \neg B$,

entonces la ejecución del ciclo **while B do S endwhile** siempre termina.

Teorema de Terminación

Teorema de Terminación

Si existe una función $fv : \mathbb{V} \to \mathbb{Z}$ tal que

1. $\{I \land B \land f_v = v_0\}$ S $\{f_v < v_0\}$,
2. $I \land f_v \leq 0 \to \neg B$,

entonces la ejecución del ciclo **while B do S endwhile** siempre termina.

- La función f_v se llama función variante del ciclo.

Teorema de Terminación

Teorema de Terminación

Si existe una función $fv : \mathbb{V} \rightarrow \mathbb{Z}$ tal que

1. $\{I \wedge B \wedge f_v = v_0\}$ S $\{f_v < v_0\}$,
2. $I \wedge f_v \leq 0 \rightarrow \neg B$,

entonces la ejecución del ciclo **while B do S endwhile** siempre termina.

- La función f_v se llama función variante del ciclo.
- $\mathbb{V}$ son valores que toman las variables del programa

Ejemplo

```
proc sumar(in s : seq⟨ℤ⟩) : ℤ

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

(1) $I \wedge B \rightsquigarrow fv$ decrecer

(2) $I \wedge \boxed{fv \leq 0} \rightsquigarrow \neg B$

cuando $fv \leq 0$ salgo del ciclo

$fv = |s| - i$

- $P_c \equiv \{res = 0 \wedge i = 0\}$
- $Q_c \equiv \{res = \sum_{i=0}^{|s|-1} s[i]\}$
- $B \equiv \{|s| - 1\}$
- $I \equiv \{0 \leq i \leq |s| \wedge res = \sum_{j=0}^{i-1} s[j]\}$

- $P_c \equiv \{res = 0 \wedge i = 0\}$
- $Q_c \equiv \{res = \sum_{i=0}^{|s|-1} s[i]\}$
- $B \equiv \{ i < |s| \}$
- $I \equiv \{0 \leq i \leq |s| \wedge res = \sum_{j=0}^{i-1} s[j]\}$

1. $\{I \wedge B \wedge f_v = v_0\}$ S $\{\underbrace{f_v < v_0}\}$,
2. $I \wedge f_v \leq 0 \rightarrow \boxed{\neg B}$,

$f_v = |s| - i$

(2) $\{I \wedge f_v \leq 0\} \equiv 0 \leq i \leq |s| \wedge res = \sum_{j=0}^{i-1} s[j] \wedge |s| - i \leq 0 \equiv$

$\equiv i = |s| \wedge res = \dots \rightarrow \underbrace{i \geq |s|}_{\neg B}$ $\quad |s| \geq |s| \checkmark$

(1) $\underbrace{\{I \wedge B \wedge f_v = v_0\}}_{A} \Rightarrow wp(S, f_v < v_0)$

```
while (i < s.size()) do
S1  res := res + s[i];
S2  i := i + 1
endwhile
```

$wp(S_1, wp(S_2, f_v < v_0)) \equiv$

$\equiv wp(res = res + s[i], wp(i = i+1, |s| - i < v_0)) \equiv$ ax1

$\equiv wp(res = res + s[i], |s| - (i+1) < v_0)) \equiv$ ax1

$\equiv \underbrace{0 \leq i < |s| \wedge_L |s| - i - 1 < v_0}_{B}$

$A = \{ 0 \leq i \leq |s| \wedge_L res = \sum_{j=0}^{i-1} s[j] \wedge i < |s| \wedge |s| - i = v_0 \} \equiv$

$$\equiv \{ 0 \le i < |s| \wedge_L \boxed{|s| - i = V_0} \wedge res = \dots \} \Rightarrow \{ 0 \le i < |s| \wedge_L \boxed{|s| - \underbrace{i - 1}_{2} < V_0} \}$$

$$\rightsquigarrow \quad |s| - i - 1 < |s| - i \quad \checkmark$$

Ejemplo

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

- $P_c \equiv \{res = 0 \wedge i = 0\}$
- $Q_c \equiv \{res = \sum_{i=0}^{|s|-1} s[i]\}$
- $B \equiv \{|s| - 1\}$
- $I \equiv \{0 \leq i \leq |s| \wedge res = \sum_{j=0}^{i-1} s[j]\}$
- $f_v = |s| - i$

- $\{I \wedge B \wedge f_v = v_0\}$ S $\{f_v < v_0\} \leftrightarrow$
  $\{I \wedge B \wedge f_v = v_0\} \rightarrow WP(\mathtt{S}, f_v < v_0)$
  - $WP(\mathtt{S}, f_v < v_0) \equiv WP(\mathtt{res := res + s[i]; i := i + 1}, |s| - i < v_0)$
    $\equiv WP\big(\mathtt{res := res + s[i]}, WP(\mathtt{i := i + 1}, |s| - i < v_0)\big)$
    $\equiv WP(\mathtt{res := res + s[i]}, |s| - i + 1 < v_0) \equiv |s| - i + 1 < v_0$
  - $\{I \wedge B \wedge f_v = v_0\} \equiv \{0 \leq |s| - 1 \wedge |s| - 1 = v_0 \wedge res = \sum_{j=0}^{i-1} s[j]\}$
  - $\{I \wedge B \wedge f_v = v_0\} \rightarrow WP(\mathtt{S}, f_v < v_0) \leftrightarrow |s| - i + 1 < |s| - 1 \leftrightarrow 1 < 0$ ✓

Ejemplo

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

- $P_c \equiv \{res = 0 \wedge i = 0\}$
- $Q_c \equiv \{res = \sum_{i=0}^{|s|-1} s[i]\}$
- $B \equiv \{|s| - 1\}$
- $I \equiv \{0 \leq i \leq |s| \wedge res = \sum_{j=0}^{i-1} s[j]\}$
- $f_v = |s| - i$

- $I \wedge f_v \leq 0 \rightarrow \neg B$
  - $I \wedge f_v \leq 0 \equiv 0 \leq i \leq |s| \wedge res = \sum_{j=0}^{i-1} s[j] \wedge |s| - 1 \leq 0$
    $\equiv 0 \leq i \leq |s| \wedge |s| - i \rightarrow i \leq |s| \wedge |s| \leq i$
  - $i \leq |s| \wedge |s| \leq i \leftrightarrow i = |s|$
  - $i = |s| \rightarrow \neg B$ ✓

Ejercicios

(La parte que faltaba)

Práctica 3 segunda parte:

- Ejercicio 6
- Ejercicio 11.c

Ejercicio de parcial

E4. Correctitud del ciclo [30 pts]

Dado el siguiente programa con su especificación

$P_c \equiv \{n > 0 \land n \ mod \ 2 = 0 \land i = 1 \land res = 1\}$

```
While(i <= n/2){
    res := res * i * (n+1-i);
    i := i+1;
}
```

$Q_c \equiv \{res = n!\}$

Contamos con el siguiente invariante, que sabemos que es incorrecto:

$I \equiv \{1 \leq i \leq n/2 + 1 \land res = \prod_{j=1}^{2(i-1)} j\}$

a) Señale qué axiomas del teorema del invariante no se cumplen. Justifique con palabras en forma precisa.
b) Escriba un invariante que resulte correcto.
c) Proponga una función variante y demuestre formalmente que es correcta.