DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Práctica 5

1er cuatrimestre 2022 — Algoritmos y Estructuras de Datos 1

Integrante	LU	Correo electrónico
Yago Pajariño	546/21	ypajarino@dc.uba.ar

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

Índice

5. Práctica 5

5.1. Ejercicio 1

5.1.A. Pregunta i

- $P_c \equiv \{i = 0; result = 0\}$
- $Q_c \equiv \{result = \sum_{j=0}^{|s|-1} s[j]\}$

5.1.B. Pregunta ii

Falla $\{I \wedge B\}S\{I\}$ en la última iteración, pues al finalizar esta, $i = |s|$

5.1.C. Pregunta iii

Falla $P_c \implies I$ pues si el límite de la sumatoria es i, la misma se inicializa con $result = s[0]$.

5.1.D. Pregunta iv

Falla $\{I \wedge B\}S\{I\}$ en la última iteración, pues se indefine $s[i]$ en la última iteración.

5.1.E. Pregunta v

Defino y/o recuerdo,

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

Para probar la correctitud del ciclo tengo que demostrar que valen:

(a) $P_c \implies I$

(b) $\{I \wedge B\}S\{I\}$

(c) $(I \wedge \neg B) \implies Q_c$

Demostración (a)

$i = 0 \implies 0 \leq i \leq |s|$ pues $|s| \geq 0$

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

Demostración (c)

$$\begin{aligned}(I \wedge \neg B) &\equiv \{0 \leq i \leq |s| \wedge_L result = \sum_{j=0}^{i-1} s[j] \wedge i \geq |s|\} \\ &\equiv \{i = |s| \wedge_L result = \sum_{j=0}^{i-1} s[j]\}\end{aligned}$$

Pero $i = |s| \implies result = \sum_{j=0}^{|s|-1} s[j] \equiv Q_c$

Demostración (b)

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

$$
\begin{aligned}
wp(S, I) &\equiv wp(result := result + s[i], wp(i := i+1, I)) \\
&\equiv wp(result := result + s[i], def(i+1) \wedge_L (0 \leq i+1 \leq |s| \wedge_L result = \sum_{j=0}^{i+1-1} s[j])) \\
&\equiv wp(result := result + s[i], (0 \leq i+1 \leq |s| \wedge_L result = \sum_{j=0}^{i+1-1} s[j])) \\
&\equiv def(result + s[i]) \wedge_L (0 \leq i+1 \leq |s| \wedge_L result + s[i] = \sum_{j=0}^{i+1-1} s[j]) \\
&\equiv 0 \leq i < |s| \wedge_L (0 \leq i+1 \leq |s| \wedge_L result + s[i] = \sum_{j=0}^{i+1-1} s[j]) \\
&\equiv 0 \leq i < |s| \wedge_L result + s[i] = \sum_{j=0}^{i} s[j]
\end{aligned}
$$

Por $(I \wedge B)$ se que $0 \leq i < |s|$ y $result + s[i] = \sum_{j=0}^{i} s[j] \iff result = \sum_{j=0}^{i-1} s[j]$

Luego el ciclo es parcialmente correcto.

5.1.F. Pregunta vi

Defino $fv = |s| - i$

Para probar que el ciclo termina tengo que demostrar que,

(a) $\{I \wedge B \wedge fv = v_0\}S\{fv < v_0\}$

(b) $(I \wedge fv \leq 0) \implies \neg B$

Demostración (b)

$fv \leq 0 \iff |s| - i \leq 0 \iff |s| \leq i \equiv i \geq |s|$

$\neg B \equiv \neg(i < |s|) \equiv i \geq |s|$

Demostración (a)

Tengo que probar que $(I \wedge B \wedge fv = v_0) \implies wp(S, fv < v_0)$

$$
\begin{aligned}
wp(S, fv < v_0) &\equiv wp(result := result + s[i], wp(i := i+1, fv < v_0)) \\
&\equiv wp(result := result + s[i], def(i+1) \wedge_L |s| - (i+1) < v_0) \\
&\equiv wp(result := result + s[i], |s| - (i+1) < v_0) \\
&\equiv \{def(result + s[i]) \wedge_L |s| - (i+1) < v_0\} \\
&\equiv \{0 \leq i < |s| \wedge_L |s| - (i+1) < v_0\}
\end{aligned}
$$

Pero,

- $0 \leq i < |s|$ vale por $(I \wedge B)$
- $|s| - i - 1 < v_0 \iff |s| - i - 1 < |s| - i \iff -1 < 0$

Por lo tanto el ciclo es correcto y finaliza.

5.2. Ejercicio 2

Defino,

- $P_c \equiv \{result = 0 \land i = 0\}$
- $Q_c \equiv \{i = n + n \bmod 2 \land result = \sum_{j=0}^{n-1} \textsf{if } j \bmod 2 = 0 \textsf{ then } j \textsf{ else } 0 \textsf{ fi}\}$
- $I \equiv 0 \leq i \leq n + 1 \land i \bmod 2 = 0 \land result = \sum_{j=0}^{i-1} \textsf{if } j \bmod 2 = 0 \textsf{ then } j \textsf{ else } 0 \textsf{ fi}$
- $B \equiv i < n$

Para probar la correctitud del ciclo tengo que demostrar que valen:

(a) $P_c \implies I$

(b) $\{I \land B\}S\{I\}$

(c) $(I \land \neg B) \implies Q_c$

Demostración (a)

Se que $result = 0$ y que $i = 0$

Quiero probar que:

- $0 \leq i \leq n + 1$. Vale pues $n \geq 0$ e $i = 0$
- $i \bmod 2 = 0$. Vale pues $0 \bmod 2 = 0$
- $result = \sum_{j=0}^{i-1} \textsf{if } j \bmod 2 = 0 \textsf{ then } j \textsf{ else } 0 \textsf{ fi}$

Con $i = 0 \implies \sum_{j=0}^{0-1} \textsf{if } j \bmod 2 = 0 \textsf{ then } j \textsf{ else } 0 \textsf{ fi} = 0 = result$

Luego $P_c \implies I$ como se quería probar.

Demostración (c)

$$(I \land \neg B) \equiv \{0 \leq i \leq n + 1 \land i \geq n \land i \bmod 2 = 0 \land result = \sum_{j=0}^{i-1} \textsf{if } j \bmod 2 = 0 \textsf{ then } j \textsf{ else } 0 \textsf{ fi}\}$$

Luego se que $n \leq i \leq n + 1 \iff i = n \lor i = n + 1$

Separo en casos par e impar,

- n par $\implies i = n + n \bmod 2 = n$
- n impar $\implies i = n + n \bmod 2 = n + 1$

Y con los valores de i hallados,

- $i = n \implies result = \sum_{j=0}^{n-1} \textsf{if } j \bmod 2 = 0 \textsf{ then } j \textsf{ else } 0 \textsf{ fi}$
- $i = n + 1 \implies result = \sum_{j=0}^{n} \textsf{if } j \bmod 2 = 0 \textsf{ then } j \textsf{ else } 0 \textsf{ fi} = \sum_{j=0}^{n-1} \textsf{if } j \bmod 2 = 0 \textsf{ then } j \textsf{ else } 0 \textsf{ fi} + 0$

Luego $(I \land \neg B) \implies Q_c$ como se quería probar.

Demostración (b)

$\{I \land B\}S\{I\} \iff (I \land B) \implies wp(S, I)$

Luego,

$$\begin{aligned}
wp(S,I) &\equiv wp(result := result+1, wp(i := i+2, I)) \\
&\equiv wp(result := result+1, (0 \leq i+2 \leq n+1 \wedge i+2 \text{ mód } 2 = 0 \wedge result = \sum_{j=0}^{i+2-1} \textsf{if } j \text{ mód } 2 = 0 \textsf{ then } j \textsf{ else } 0 \textsf{ fi})) \\
&\equiv def(result+1) \wedge_L (0 \leq i+2 \leq n+1 \wedge i+2 \text{ mód } 2 = 0 \wedge result+1 = \sum_{j=0}^{i+2-1} \textsf{if } j \text{ mód } 2 = 0 \textsf{ then } j \textsf{ else } 0 \textsf{ fi}) \\
&\equiv \{0 \leq i+2 \leq n+1 \wedge i \text{ mód } 2 = 0 \wedge result+i = \sum_{j=0}^{i+1} \textsf{if } j \text{ mód } 2 = 0 \textsf{ then } j \textsf{ else } 0 \textsf{ fi}\}
\end{aligned}$$

Queda ver que $(I \wedge B) \implies wp(S,I)$

Entonces, $(I \wedge B) \equiv 0 \leq i \leq n+1 \wedge i < n \wedge i \text{ mód } 2 = 0 \wedge result = \sum_{j=0}^{i-1} \textsf{if } j \text{ mód } 2 = 0 \textsf{ then } j \textsf{ else } 0 \textsf{ fi}$

Y quiero probar,

- $0 \leq i+2$. Vale pues por I, $0 \leq i$
- $i+2 \leq n+1$. Vale pues $i < n \iff i+1 \leq n \iff i+2 \leq n+1$
- $i \text{ mód } 2 = 0$. Vale por I
- $result = \sum_{j=0}^{i-1} \textsf{if } j \text{ mód } 2 = 0 \textsf{ then } j \textsf{ else } 0 \textsf{ fi}$

La última condicion vale pues la sumatoria entre $0 \leq j \leq i-1$ vale por I, dado que i es par, el i-ésimo termino de la sumatoria es igual a i y el $i+1$ es cero.

Por lo tanto el ciclo es parcialmente correcto respecto a su especificación.

Para probar finalización del ciclo tengo que probar:

(a) $\{I \wedge B \wedge f_v = v_0\} S \{f_v < v_0\}$

(b) $(I \wedge f_v \leq 0) \implies \neg B$

Sea $f_v = n - i$

Demostración (b)

$n - i \leq 0 \iff n - i + i \leq i \iff n \leq i \equiv \neg B$

Demostración (a)

$\{I \wedge B \wedge f_v = v_0\} S \{f_v < v_0\} \iff (I \wedge B \wedge f_v = v_0) \implies wp(S, f_v < v_0)$

$$\begin{aligned}
wp(S, f_v < v_0) &\equiv wp(result := result+1, wp(i := i+2, f_v < v_0)) \\
&\equiv wp(result := result+1, n-(i+2) < v_0) \\
&\equiv \{n-(i+2) < v_0\} \\
&\equiv \{n-i-2 < v_0\}
\end{aligned}$$

Pero $f_v = v_0 \implies n - i = v_0 \implies n - i - 2 = v_0 - 2 < v_0 \iff -2 < 0$

Luego el ciclo finaliza y por lo tanto es correcto respecto a su especificación.

5.3. Ejercicio 3

5.3.A. Pregunta i

```
int result = 1;
int i = 0;
while ( i < n ) {
    result = result * m;
    i = i + 1;
}
```

Defino,

- $P_C \equiv \{result = 1 \wedge i = 0\}$
- $Q_C \equiv \{result = m^n\}$
- $I \equiv \{0 \leq i \leq n \wedge result = m^i\}$
- $B \equiv \{i < n\}$

Para probar la correctitud del ciclo tengo que demostrar que valen:

(a) $P_c \implies I$

(b) $\{I \wedge B\}S\{I\}$

(c) $(I \wedge \neg B) \implies Q_c$

Demostración (a)

$i = 0 \implies 0 \leq i$ y por $Pre : n \geq 0 \implies i \leq n$

$i = 0 \implies m^0 = 1 = result$

Demostración (c)

$(I \wedge \neg B) \equiv \{0 \leq i \leq n \wedge result = m^i \wedge i \geq n\}$

Luego se que $(I \wedge \neg B) \implies i = n \implies result = m^n \equiv Post$

Demostración (b)

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

Luego,

$$\begin{aligned}
wp(S, I) &\equiv wp(result = result * m, wp(i = i + 1, I)) \\
&\equiv wp(result = result * m, def(i + 1) \wedge_L 0 \leq i + 1 \leq n \wedge result = m^{i+1}) \\
&\equiv wp(result = result * m, 0 \leq i + 1 \leq n \wedge result = m^{i+1}) \\
&\equiv def(result * m) \wedge_L 0 \leq i + 1 \leq n \wedge result * m = m^{i+1} \\
&\equiv 0 \leq i + 1 \leq n \wedge result * m = m^{i+1}
\end{aligned}$$

$0 \leq i \leq n \wedge i < n \implies 0 \leq i < n \implies \leq i + 1 \wedge i < n \implies i + 1 \leq n$

$result = m^i \iff resutl * m = m^i * m \iff result * m = m^{i+1}$

Por lo tanto queda probado que el ciclo es parcialmente correcto.

Para probar finalización del ciclo tengo que probar:

(a) $\{I \wedge B \wedge f_v = v_0\}S\{f_v < v_0\}$

(b) $(I \wedge f_v \leq 0) \implies \neg B$

Sea $f_v = n - i$

Demostración (b)

$(I \wedge f_v \leq 0) \equiv \{0 \leq i \leq n \wedge result = m^i \wedge n - i \leq 0\}$

Pero, $n - i \leq 0 \implies n \leq i \implies i \geq n \equiv \neg B$

Demostración (a)

$\{I \wedge B \wedge f_v = v_0\}S\{f_v < v_0\} \iff (I \wedge B \wedge f_v = v_0) \implies wp(S, f_v < v_0)$

$$\begin{aligned}
wp(S, f_v < v_0) &\equiv wp(result = result * m, wp(i = i+1, n - i < v_0)) \\
&\equiv wp(result = result * m, def(i+1) \wedge_L n - (i+1) < v_0) \\
&\equiv wp(result = result * m, n - (i+1) < v_0) \\
&\equiv \{def(result * m) \wedge_L n - (i+1) < v_0\} \\
&\equiv \{n - (i+1) < v_0\}
\end{aligned}$$

Pero, $n - i = v_0 \implies n - i - 1 < v_0 \iff v_0 - 1 < v_0 \iff -1 < 0$

Por lo tanto el ciclo finaliza. Y el programa es correcto respecto a su especificación.

5.3.B. Pregunta ii

Falla la demostración de $\{I \wedge B\}S\{I\}$

5.3.C. Pregunta iii

Es correcto, solo hay que probar de nuevo los puntos (2) y (4) de la demostración.

5.3.D. Pregunta iv

Se puede pedir $n \geq 2$ en la precondición.

5.4. Ejercicio 4

5.4.A. Pregunta i

```
int i = 1;
int result = 0;
while (i <= n) {
    if (n % i == 0) {
        result = result + 1;
    }
    i = i + 1;
}
```

5.4.B. Pregunta ii

El invariante propuesto falla en la última iteración, hay que cambiarlo por
$\{1 \leq i \leq n \wedge result = \sum_{j=1}^{i} \textsf{if } n \bmod j = 1 \textsf{ then } j \textsf{ else } 0 \textsf{ fi}\}$

5.5. Ejercicio 5

5.5.A. Pregunta i

```
int result = 0;
int j = 0;
while (j < s.size()) {
    if (j % 2 == 1) {
        result = result + s[j];
    }
    j = j+1;
}
```

5.5.B. Pregunta ii

Defino,

- $P_C \equiv \{result = 0 \land j = 0\}$
- $Q_C \equiv \{result = \sum_{i=0}^{|s|-1} \text{if } i \text{ mód } 2 = 1 \text{ then } s[i] \text{ else } 0 \text{ fi}\}$
- $I \equiv \{0 \leq j \leq |s| \land result = \sum_{i=0}^{j-1} \text{if } i \text{ mód } 2 = 1 \text{ then } s[i] \text{ else } 0 \text{ fi}\}$
- $B \equiv \{j < |s|\}$
- $f_v = |s| - j$

Para probar la correctitud del ciclo tengo que demostrar que valen:

(a) $P_c \implies I$

(b) $\{I \land B\}S\{I\}$

(c) $(I \land \neg B) \implies Q_c$

(d) $\{I \land B \land f_v = v_0\}S\{f_v < v_0\}$

(e) $(I \land f_v \leq 0) \implies \neg B$

Demostración (a)

$j = 0 \implies 0 \leq j \leq |s|$

$j = 0 \implies \sum_{i=0}^{j-1} \text{if } i \text{ mód } 2 = 1 \text{ then } s[i] \text{ else } 0 \text{ fi} = 0 = result$

Demostración (c)

$0 \leq j \leq |s| \land j \geq |s| \implies j = |s| \implies result = \sum_{i=0}^{|s|-1} \text{if } i \text{ mód } 2 = 1 \text{ then } s[i] \text{ else } 0 \text{ fi} \equiv Q_c$

Demostración (b)

$\{I \land B\}S\{I\} \iff (I \land B) \implies wp(S, I)$

Luego,

$$\begin{aligned}
wp(S, I) &\equiv wp(if(...), wp(j = j + 1, I)) \\
&\equiv wp(if(...), def(j+1) \wedge_L (0 \leq j+1 \leq |s| \wedge result = \sum_{i=0}^{j+1-1} \text{if } i \text{ mód } 2 = 1 \text{ then } s[i] \text{ else } 0 \text{ fi})) \\
&\equiv wp(if(...), (0 \leq j+1 \leq |s| \wedge result = \sum_{i=0}^{j} \text{if } i \text{ mód } 2 = 1 \text{ then } s[i] \text{ else } 0 \text{ fi})) \\
&\equiv (j \text{ mód } 2 = 1 \wedge wp(result = result + 1, (0 \leq j+1 \leq |s| \wedge result = \sum_{i=0}^{j} \text{if } i \text{ mód } 2 = 1 \text{ then } s[i] \text{ else } 0 \text{ fi}))) \vee \\
&\quad (j \text{ mód } 2 = 0 \wedge wp(skip, (0 \leq j+1 \leq |s| \wedge result = \sum_{i=0}^{j} \text{if } i \text{ mód } 2 = 1 \text{ then } s[i] \text{ else } 0 \text{ fi}))) \\
&\equiv (j \text{ mód } 2 = 1 \wedge (0 \leq j+1 \leq |s| \wedge result + 1 = \sum_{i=0}^{j} \text{if } i \text{ mód } 2 = 1 \text{ then } s[i] \text{ else } 0 \text{ fi})) \vee \\
&\quad (j \text{ mód } 2 = 0 \wedge (0 \leq j+1 \leq |s| \wedge result = \sum_{i=0}^{j} \text{if } i \text{ mód } 2 = 1 \text{ then } s[i] \text{ else } 0 \text{ fi}))
\end{aligned}$$

Por $(I \wedge B)$ vale que $0 \leq j+1 \leq |s|$ en ambas ramas del if.

Ambas sumatorias valen pues dependiendo de la paridad de j, se suma 1 a la sumatoria. Y la sumatoria entre $0 \leq j \leq |s|$ vale por I

Demostración (e)

$|s| - j < 0 \implies j \geq |s| \equiv \neq B$

Demostración (d)

$\{I \wedge B \wedge f_v = v_0\} S \{f_v < v_0\} \iff (I \wedge B \wedge f_v = v_0) \implies wp(S, f_v < v_0)$

$$\begin{aligned}
wp(S, f_v < v_0) &\equiv wp(if(...), wp(j = j+1, f_v < v_0)) \\
&\equiv wp(if(...), def(j+1) \wedge_L |s| - (j+1) < v_0) \\
&\equiv wp(if(...), |s| - (j+1) < v_0) \\
&\equiv (j \text{ mód } 2 = 1 \wedge |s| - (j+1) < v_0) \vee ((j \text{ mód } 2 \neq 1 \wedge |s| - (j+1) < v_0)) \\
&\equiv \{|s| - (j+1) < v_0\}
\end{aligned}$$

Luego $|s| - j - 1 < v_0 \iff v_0 - 1 < v_0 \iff -1 < 0$

Por lo tanto el ciclo es correcto.

5.6. Ejercicio 6

5.6.A. Pregunta i

- $P_c \equiv \{i = 0 \wedge j = 1\}$
- $Q_c \equiv Post$

5.6.B. Pregunta ii

Defino,

- $P_C \equiv \{i = 0 \wedge j = 1\}$
- $Q_C \equiv Post$

- $I \equiv \{(0 \leq i < |s| \land 1 \leq j \leq |s|) \land_L (\forall k : \mathbb{Z})(0 \leq k < j \longrightarrow_L s[k] \leq s[i])\}$
- $B \equiv \{j < |s|\}$

Para probar la correctitud parcial del ciclo tengo que demostrar que valen:

(a) $P_c \implies I$

(b) $\{I \land B\}S\{I\}$

(c) $(I \land \neg B) \implies Q_c$

Demostración (a)

$i = 0 \land j = 1 \implies 0 \leq 0 \leq |s| \land 1 \leq 1 \leq |s| \land k = 0 \implies s[0] = s[0]$

Demostración (c)

$1 \leq j \leq |s| \land j \geq |s| \implies j = |s| \implies (\forall k : \mathbb{Z})(0 \leq k \leq |s| \longrightarrow_L s[k] \leq s[i]) \equiv Q_C$

Demostración (b)

$\{I \land B\}S\{I\} \iff (I \land B) \implies wp(C, I)$

$$
\begin{aligned}
wp(C, I) &\equiv wp(iff(...), wp(j = j + 1, I)) \\
&\equiv wp(if(...), def(j+1) \land_L (0 \leq i < |s| \land 1 \leq j+1 \leq |s|) \land_L (\forall k : \mathbb{Z})(0 \leq k < j+1 \longrightarrow_L s[k] \leq s[i])) \\
&\equiv wp(if(...), (0 \leq i < |s| \land 1 \leq j+1 \leq |s|) \land_L (\forall k : \mathbb{Z})(0 \leq k < j+1 \longrightarrow_L s[k] \leq s[i])) \\
&\equiv def(s[j] > s[i]) \land_L (s[j] > s[i] \land wp(i = j, (0 \leq i < |s| \land 1 \leq j+1 \leq |s|) \land_L (\forall k : \mathbb{Z})(0 \leq k < j+1 \longrightarrow_L s[k] \leq s[i])) \lor \\
&\qquad (s[j] \leq s[i] \land wp(skip, (0 \leq i < |s| \land 1 \leq j+1 \leq |s|) \land_L (\forall k : \mathbb{Z})(0 \leq k < j+1 \longrightarrow_L s[k] \leq s[i])))) \\
&\equiv 0 \leq j < |s| \land 0 \leq i < |s| \land_L (s[j] > s[i] \land (0 \leq j < |s| \land 1 \leq j+1 \leq |s|) \land_L (\forall k : \mathbb{Z})(0 \leq k < j+1 \longrightarrow_L s[k] \leq s[j])) \lor \\
&\qquad (s[j] \leq s[i] \land (0 \leq i < |s| \land 1 \leq j+1 \leq |s|) \land_L (\forall k : \mathbb{Z})(0 \leq k < j+1 \longrightarrow_L s[k] \leq s[i]))
\end{aligned}
$$

5.6.C. Pregunta ii

$f_v = |s| - j - 1$

TODO la demostración de finalización.

5.7. Ejercicio 7

5.7.A. Pregunta i

- $P_c \equiv i = 0 \land |r| = |s|$
- $Q_c \equiv Post$

5.7.B. Pregunta ii

Defino,

- $P_C \equiv \{i = 0 \land |r| = |s|\}$
- $Q_C \equiv Post$
- $I \equiv \{0 \leq i \leq |s| \land |s| = |r| \land (\forall j : \mathbb{Z})(0 \leq j < i \longrightarrow_L s[j] = r[j])\}$
- $B \equiv \{i < |s|\}$

Para probar la correctitud parcial del ciclo tengo que demostrar que valen:

(a) $P_c \implies I$

(b) $\{I \wedge B\}S\{I\}$

(c) $(I \wedge \neg B) \implies Q_c$

Demostración (a)

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

$|s| = |r| \implies |s| = |r|$

$i = 0 \implies (\forall j : \mathbb{Z})(0 \leq j < 0 \longrightarrow_L s[j] = r[j])$ pero $0 \leq j < 0 \equiv False$

Demostración (c)

$(I \wedge \neg B) \equiv 0 \leq i \leq |s| \wedge |s| = |r| \wedge (\forall j : \mathbb{Z})(0 \leq j < i \longrightarrow_L s[j] = r[j]) \wedge i \geq |s|$

Pero, $0 \leq i \leq |s| \wedge i \geq |s| \implies i = |s|$

Luego, $i = 0 \implies |s| = |r| \wedge (\forall j : \mathbb{Z})(0 \leq j < |s| \longrightarrow_L s[j] = r[j]) \equiv Q_c$

Demostración (b)

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

$$\begin{aligned} wp(S, I) &\equiv wp(r[i] = s[i], wp(i = i + 1, I)) \\ &\equiv wp(r[i] = s[i], def(i + 1) \wedge_L 0 \leq i + 1 \leq |s| \wedge |s| = |r| \wedge (\forall j : \mathbb{Z})(0 \leq j < i + 1 \longrightarrow_L s[j] = r[j])) \\ &\equiv wp(r = setAt(r, i, s[i]), 0 \leq i + 1 \leq |s| \wedge |s| = |r| \wedge (\forall j : \mathbb{Z})(0 \leq j < i + 1 \longrightarrow_L s[j] = r[j])) \\ &\equiv 0 \leq i < |s| \wedge_L |s| = |r| \wedge (\forall j : \mathbb{Z})(0 \leq j < i \longrightarrow_L s[j] = r[j])) \end{aligned}$$

Es facil ver que por $I \wedge B$ valen los tres elementos de la conjunción.

Luego el ciclo es parcialmente correcto.

5.7.C. Pregunta iii

Defino $f_v = |s| - i$

Para probar finalización del ciclo tengo que probar:

(a) $\{I \wedge B \wedge f_v = v_0\}S\{f_v < v_0\}$

(b) $(I \wedge f_v \leq 0) \implies \neg B$

Demostración (b)

$(I \wedge f_v \leq 0) \implies |s| - i \leq 0 \implies i \geq |s| \equiv \neg B$

Demostración (a)

$\{I \wedge B \wedge f_v = v_0\}S\{f_v < v_0\} \iff (I \wedge B \wedge f_v = v_0) \implies wp(S, f_v < v_0)$

$$\begin{aligned} wp(S, I) &\equiv wp(r[i] = s[i], wp(i = i + 1, |s| - i < v_0)) \\ &\equiv wp(r[i] = s[i], |s| - (i + 1) < v_0) \\ &\equiv |s| - (i + 1) < v_0 \end{aligned}$$

Pero $f_v = v_0 \implies v_0 - 1 < v_0 \iff -1 < 0$

Así queda probado que el ciclo finaliza.

5.8. Ejercicio 8

5.8.A. Pregunta i

- $P_c \equiv \{i = d\}$
- $q_c \equiv Post$

5.8.B. Pregunta ii

Defino,

- $P_C \equiv \{i = d\}$
- $Q_C \equiv Post$
- $I \equiv \{d \leq i \leq |s| \wedge |s| = |s_0| \wedge_L (\forall j : \mathbb{Z})(0 \leq j < d \longrightarrow_L s[j] = s_0[j]) \wedge (\forall j : \mathbb{Z})(d \leq j < |s| \longrightarrow_L s[j] = e)\}$
- $B \equiv \{i < |s|\}$

Para probar la correctitud parcial del ciclo tengo que demostrar que valen:

(a) $P_c \implies I$

(b) $\{I \wedge B\}S\{I\}$

(c) $(I \wedge \neg B) \implies Q_c$

TODO. Hecho en clase 20/04/2022.

5.9. Ejercicio 9

5.9.A. Pregunta i

Defino,

- $P_C \equiv \{|s| \bmod 2 = 0 \wedge i = |s| - 1 \wedge suma = 0\}$
- $Q_C \equiv \{|s| \bmod 2 = 0 \wedge i = |s|/2 - 1 \wedge_L suma = \sum_{j=0}^{|s|/2-1} s[j]\}$
- $I \equiv \{|s|/2 - 1 \leq i \leq |s| - 1 \wedge |s| \bmod 2 = 0 \wedge suma = \sum_{j=0}^{|s|-2-i}\}$
- $B \equiv \{i \geq |s|/2\}$

Para probar la correctitud parcial del ciclo tengo que demostrar que valen:

(a) $P_c \implies I$

(b) $\{I \wedge B\}S\{I\}$

(c) $(I \wedge \neg B) \implies Q_c$

5.9.B. Pregunta ii

$f_v = i - |s|/2 - 1$

5.9.C. Pregunta iii

TODO

5.10. Ejercicio 10

5.10.A. Pregunta i

```
int i = 0;
while (i < s.size()) {
    if (s[i] == a) {
        s[i] = b;
    }
    i = i+1;
}
```

5.10.B. Pregunta ii

- $P_c \equiv i = 0 \land |s| = |s_0|$
- $Q_c \equiv Post$

5.10.C. Pregunta iii

Defino,

- $P_C \equiv \{i = 0 \land |s| = |s_0|\}$
- $Q_C \equiv Post$
- $I \equiv \{|s| = |s_0| \land 0 \leq i \leq |s| \land (\forall j : \mathbb{Z})((0 \leq j < i \land_L s_0[j] = a) \longrightarrow_L s[j] = b) \land (\forall j : \mathbb{Z})((0 \leq j < i \land_L s_0[j] \neq a) \longrightarrow_L s[j] = s_0[j])\}$
- $B \equiv \{i < |s|\}$

Para probar la correctitud parcial del ciclo tengo que demostrar que valen:

(a) $P_c \implies I$

(b) $\{I \land B\}S\{I\}$

(c) $(I \land \neg B) \implies Q_c$

Demostración (a)

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

Ambos $\forall$ son verdaderos pues $i = 0$ implica antecedente falso y por lo tanto implicación verdadera.

Demostración (c)

$(I \land \neg B) \implies 0 \leq i \leq |s| \land i \geq |s| \implies i = |s| \implies$ ambos $\forall$ igual que en $Post$

Demostración (b)

$\{I \land B\}S\{I\} \iff (I \land B) \implies wp(S, I)$

$$
\begin{aligned}
wp(S, I) &\equiv wp((if(...), wp(i = i + 1, I))) \\
&\equiv wp((if(...), I(i + 1))) \\
&\equiv def(i < |s|) \land_L (i < |s| \land wp(s = setAt(s, i, b), I(i + 1))) \lor (i \geq |s| \land wp(skip, I(i + 1))) \\
&\equiv (i < |s| \land 0 \leq i < |s| \land_L |s| = |s_0| \land 0 \leq i + 1 \leq |s| \land (\forall j : \mathbb{Z})((0 \leq j < i + 1 \land_L s_0[j] = a) \longrightarrow_L setAt(s, i, b)[j] = b) \land \\
&\qquad (\forall j : \mathbb{Z})((0 \leq j < i + 1 \land_L s_0[j] \neq a) \longrightarrow_L setAt(s, i, b)[j] = s_0[j])) \lor \\
&\quad (i \geq |s| \land |s| = |s_0| \land 0 \leq i + 1 \leq |s| \land (\forall j : \mathbb{Z})((0 \leq j < i + 1 \land_L s_0[j] = a) \longrightarrow_L s[j] = b) \land \\
&\qquad (\forall j : \mathbb{Z})((0 \leq j < i + 1 \land_L s_0[j] \neq a) \longrightarrow_L s[j] = s_0[j]))
\end{aligned}
$$

Y usando $I \land B$ hay que probar cada termino de la conjunción.

5.10.D. Pregunta iv

$f_v = |s| - i$

5.11. Ejercicio 11

Tengo que probar que vale la tripla de Hoare $\{Pre\}S\{Post\}$

La estrategia en la demostración en programas completos que tienen un ciclo es dividir en tres:

1. $Pre \implies wp(A, P_c)$
2. $\{P_c\}C\{Q_c\}$
3. $Q_c \implies wp(B, Q_c)$

Con,

- A: código antes del ciclo
- C: ciclo
- B: código después del ciclo

Por lo tanto tengo que probar,

(a) $wp(S_4, Post)$

(b) $wp(C, (a))$

(c) $wp(S_2, (b))$

(d) $wp(S_1, (c))$

Demostración (a)

$$\begin{aligned} wp(S_4, Post) \equiv def(j) \wedge_L j = -1 &\implies (\forall j : \mathbb{Z})(0 \leq j < |s| \longrightarrow_L s[j] \neq e) \wedge \\ j \neq -1 &\implies (0 \leq j < |s| \wedge_L s[j] = e) \end{aligned}$$

Esto es lo que uso como Pre para probar el ciclo usando el teorema del invariante.

Demostración (b)

Defino,

- $P_c \equiv i = |s| - 1 \wedge j = -1$
- $Q_c \equiv (a)$
- $I \equiv -1 \leq i \leq |s| - 1 \wedge j = -1 \implies (\forall j : \mathbb{Z})(i \leq j < |s| \longrightarrow_L s[j] \neq e) \wedge j \neq -1 \implies (i < j < |s| \wedge_L s[j] = e)$
- $B \equiv i \geq 0$

Para probar la correctitud parcial del ciclo tengo que demostrar que valen:

(a) $P_c \implies I$

(b) $\{I \wedge B\}S\{I\}$

(c) $(I \wedge \neg B) \implies Q_c$

Demostración (b.a)

Se que $i = |s| - 1 \wedge j = -1$. Luego valen,

- $-1 \leq i \leq |s| - 1$
- $j = -1 \implies (\forall j : \mathbb{Z})(i \leq j < |s| \longrightarrow_L s[j] \neq e)$
- $j \neq -1 \implies$ (...) pues el antecedente es falso.

Demostración (b.c)

Por $(I \wedge \neg B)$ se que $i = -1$ luego valen ambos casos $j = -1 \wedge j \neq -1$

Demostración (b.b)

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

$$\begin{aligned}
wp(S, I) &\equiv wp(if(...), wp(i = i-1, I)) \\
&\equiv wp(if(...), def(i-1) \wedge_L I(i-1)) \\
&\equiv def(s[i] = e) \wedge_L (s[i] = e \wedge wp(j = i, I(i-1))) \vee (s[i] \neq e \wedge wp(skip, I(i-1))) \\
&\equiv 0 \leq i < |s| \wedge_L (s[i] = e \wedge I(i = i-1)(j = i)) \vee (s[i] \neq e \wedge I(i-1)) \\
&\equiv 0 \leq i < |s| \wedge_L (s[i] = e \wedge -1 \leq i-1 \leq |s|-1 \wedge \\
& i = -1 \implies (\forall j : \mathbb{Z})(i-1 \leq j < |s| \longrightarrow_L s[j] \neq e) \wedge \\
& i \neq -1 \implies (i-1 < i < |s| \wedge_L s[i] = e)) \vee \\
& (s[i] \neq e \wedge -1 \leq i-1 \leq |s|-1 \wedge \\
& j = -1 \implies (\forall j : \mathbb{Z})(i-1 \leq j < |s| \longrightarrow_L s[j] \neq e) \wedge \\
& j \neq -1 \implies (i-1 < j < |s| \wedge_L s[j] = e))
\end{aligned}$$

Queda probar que $(I \wedge B) \implies wp(S, I)$ calculada

Ahora pruebo terminación del ciclo

Defino $f_v = i + 1$

Para probar finalización del ciclo tengo que probar:

(a) $\{I \wedge B \wedge f_v = v_0\}S\{f_v < v_0\}$

(b) $(I \wedge f_v \leq 0) \implies \neg B$

Luego, $\{I \wedge B \wedge f_v = v_0\}S\{f_v < v_0\} \iff (I \wedge B \wedge f_v = v_0) \implies wp(S, f_v < v_0)$

$$\begin{aligned}
wp(S, f_v < v_0) &\equiv wp(if(...), wp(i = i-1, f_v < v_0)) \\
&\equiv wp(if(...), i-1+1 < v_0) \\
&\equiv def(s[i] = e) \wedge_L (s[i] = e \wedge wp(j = i, i-1+1 < v_0)) \vee (s[i] \neq e \wedge i-1+1 < v_0) \\
&\equiv 0 \leq i < |s| \wedge_L i-1+1 < v_0
\end{aligned}$$

Luego por $f_v = v_0 \implies i+1 = v_0 \implies i-1+1 < v_0 \equiv v_0 - 1 < v_0 \iff -1 < 0$

Además, $f_v \leq 0 \implies i+1 \leq 0 \implies i \leq -1 \iff i < 0 \equiv \neg B$

Luego el ciclo es correcto y finaliza. Por monotonía queda probar que $Pre \implies wp(S_1, S_2; P_c)$

$$\begin{aligned}
wp(S_1, S_2; P_c) &\equiv wp(S_1, wp(S_2, P_c)) \\
&\equiv wp(i = |s|-1, wp(j = -1, P_c)) \\
&\equiv wp(i = |s|-1, i = |s|-1 \wedge -1 = -1) \\
&\equiv wp(i = |s|-1, i = |s|-1) \\
&\equiv def(|s|-1) \wedge_L |s|-1 = |s|-1 \\
&\equiv True
\end{aligned}$$

Queda ver que $Pre \implies True \iff True \implies True$ que es verdadero y por lo tanto el programa es correcto respecto a su especificación.

5.12. Ejercicio 12

Divido la demostración en:

(a) Codigo antes del ciclo $Pre \implies wp(A, P_c)$

(b) Demostración de correctitud del ciclo usando el teorema del invariante

(c) Código posterior al ciclo $Q_c \implies wp(C, Post)$

Demostración (c)

Calculo,

$$\begin{aligned} wp(if(...), Post) &\equiv def(j \neq -1) \wedge_L (j \neq -1 \wedge wp(r = True, Post)) \vee \\ &\qquad\qquad\qquad\qquad (j = -1 \wedge wp(r = false, Post)) \\ &\equiv (j \neq -1 \wedge wp(r = True, Post)) \vee \\ &\quad\ (j = -1 \wedge wp(r = false, Post)) \\ &\equiv (j \neq -1 \wedge true = true \iff ((\exists k : \mathbb{Z})(0 \leq k < |s| \wedge_L s[k] = e))) \vee \\ &\quad\ (j = -1 \wedge false = true \iff ((\exists k : \mathbb{Z})(0 \leq k < |s| \wedge_L s[k] \neq e))) \end{aligned}$$

Demostración (b)

Defino,

- $P_c \equiv i = 0 \wedge j = -1$
- $Q_c \equiv (c)$
- $I \equiv 0 \leq i \leq |s| \wedge (j \neq -1 \implies (\exists k : \mathbb{Z})(0 \leq k < i \wedge_L s[k] = e)) \wedge (j = -1 \implies (\exists k : \mathbb{Z})(0 \leq k < i \wedge_L s[k] \neq e))$
- $B \equiv i \geq |s|$

Para probar la correctitud parcial del ciclo tengo que demostrar que valen:

(a) $P_c \implies I$

(b) $\{I \wedge B\} S \{I\}$

(c) $(I \wedge \neg B) \implies Q_c$

Demostración (b.a)

Se que $i = 0 \wedge j = -1$ luego $0 \leq 0 \leq |s|$ es verdadero, la implicación de $j \neq -1$ es verdadera, la implicación de $j = -1$ es verdadera pues el antecedente del $\exists$ es falso.

Demostración (b.c)

$(I \wedge \neg B) \implies i = |s|$ y por lo tanto para este valor de i, las dos ramas del invariante son iguales a las de Q_c

Demostración (b.b)

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

TODO

5.13. Ejercicio 13

TODO

5.14. Ejercicio 14

TODO

5.15. Ejercicio 15

TODO