Demostraciones de corrección: Condicionales y Teorema del invariante

Algoritmos y Estructuras de Datos I

Clase práctica 5 - Teorema del invariante

Corrección

- $P_c \Rightarrow I$
- $(I \wedge \neg B) \Rightarrow Q_c$
- $\{I \wedge B\}$ ciclo $\{I\}$

Terminación

- $\{(I \wedge B \wedge v_0 = f_v)\}$ ciclo $\{fv < v_0\}$
- $(I \wedge f_v \leq 0) \Rightarrow \neg B$

Guía 5. Ejercicio 2

Dadas la especificación y la implementación del problema `sumarParesHastaN`, escribir la precondición y la postcondición del ciclo, y demostrar formalmente su corrección.

`proc sumarParesHastaN` (in n: $\mathbb{Z}$, out result: $\mathbb{Z}$) {
`Pre` $\{n \geq 0\}$
`Post` $\{result = \sum_{j=0}^{n-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})\}$
}

```
result := 0;
i := 0;
while (i < n) do
  result := result + i;
  i := i + 2
endwhile
```

$$I \equiv 0 \leq i \leq n+1 \wedge i \ mod \ 2 \ = \ 0 \wedge result = \sum_{j=0}^{i-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$$

Guía 5. Ejercicio 2

```
result := 0;
i := 0;
while (i < n) do
  result := result + i;
  i := i + 2
endwhile
```

- $P_c : n \geq 0 \wedge result = 0 \wedge i = 0$
- $Q_c : result = \sum_{j=0}^{n-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$
- $I : 0 \leq i \leq n+1 \wedge i \ mod \ 2 \ = \ 0 \wedge$ $result = \sum_{j=0}^{i-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$
- $fv : n - i$

$P_c \Rightarrow I$

- Datos que puedo usar: P_c
  - $n \geq 0$
  - $result = 0$
  - $i = 0$
- Quiero probar: I
  - $0 \leq i \leq n+1$
  - $i \ mod \ 2 \ = \ 0$
  - $result = \sum_{j=0}^{i-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$

  - $0 \leq i \leq n+1$ Vale, porque $i = 0$ y $n \geq 0$
  - $i \ mod \ 2 \ = \ 0$ Vale, porque $i = 0$
  - $result = \sum_{j=0}^{i-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$ Vale porque $result = 0$ y la sumatoria tiene el rango vacío

$(I \wedge \neg B) \Rightarrow Q_c$

- Datos que puedo usar: $I \wedge \neg B$
  - $0 \leq i \leq n+1$
  - $i \ mod \ 2 \ = \ 0$
  - $result = \sum_{j=0}^{i-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$
  - $i \geq n$
- Quiero probar: Q_c
  - $result = \sum_{j=0}^{n-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$

$n \leq i \leq n+1$

- i = n
- i = n + 1

- i = n

$$result = \sum_{j=0}^{i-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$$

$$result = \sum_{j=0}^{n-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$$

$(I \wedge \neg B) \Rightarrow Q_c$

- i = n + 1

$$result = \sum_{j=0}^{i-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$$

$$result = \sum_{j=0}^{(n+1)-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$$

$$result = \sum_{j=0}^{n}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$$

$$result = \sum_{j=0}^{n-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi}) + (\text{if } n \ mod \ 2 = 0 \text{ then } n \text{ else } 0 \text{ fi})$$

$$result = \sum_{j=0}^{n-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi}) + 0$$

porque $i \ mod \ 2 = 0$

$\{I \wedge B\}$ ciclo $\{I\}$

- Ciclo:

  $S1$ `result := result + i ;`

  $S2$ `i := i + 2`
- $(I \wedge B) \Rightarrow wp(ciclo, I)$

$\{I \land B\}$ ciclo $\{I\}$

$wp(S1; S2, I) \overset{Ax3}{\equiv} wp(S1, wp(S2, I))$

$wp(S2, I) \overset{Ax1}{\equiv} def(i+2) \land_L I^i_{i+2}$
$\equiv true \land_L (0 \leq i+2 \leq n+1 \land i+2 \ mod \ 2 = 0 \land$
$result = \sum_{j=0}^{i+2-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi}))$
$\equiv (0 \leq i+2 \leq n+1 \land i+2 \ mod \ 2 = 0 \land$
$result = \sum_{j=0}^{i+1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi}))$
$\equiv wp(S1, (0 \leq i+2 \leq n+1 \land i+2 \ mod \ 2 = 0 \land$
$result = \sum_{j=0}^{i+1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})))$
$\overset{Ax1}{\equiv} def(result + i) \land_L$
$(0 \leq i+2 \leq n+1 \land i+2 \ mod \ 2 = 0 \land$
$result + i = \sum_{j=0}^{i+1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi}))$
$\equiv true \land_L (0 \leq i+2 \leq n+1 \land i+2 \ mod \ 2 = 0 \land$
$result + i = \sum_{j=0}^{i+1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi}))$

$\{I \land B\}$ ciclo $\{I\}$

- Datos que puedo usar: $I \land B$
  - $0 \leq i \leq n+1$
  - $i \ mod \ 2 \ = \ 0$
  - $result = \sum_{j=0}^{i-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$
  - $i < n$
- Quiero probar: $wp(ciclo, I)$
  - $0 \leq i+2 \leq n+1$
  - $i+2 \ mod \ 2 = 0$
  - $result + i = \sum_{j=0}^{i+1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$

  - $0 \leq i+2 \leq n+1$ Vale porque $0 \leq i \leq n+1$
  - $i+2 \ mod \ 2 = 0$ Vale porque $i \ mod \ 2 \ = \ 0$
  - $result + i = \sum_{j=0}^{i+1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$

$= \sum_{j=0}^{i-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi}) +$ result
$\text{if } i \ mod \ 2 = 0 \text{ then } i \text{ else } 0 \text{ fi} +$ i
$\text{if } i+1 \ mod \ 2 = 0 \text{ then } i+1 \text{ else } 0 \text{ fi}$ 0

$(I \land f_v \leq 0) \Rightarrow \neg B$

- $\neg B$, es decir $i \geq n$.

Sabemos que $f_v \leq 0$, y $f_v = n - i$
$\Rightarrow n - i \leq 0$
$\Rightarrow n \leq i$

$\{(I \land B \land v_0 = f_v)\}$ ciclo $\{fv < v_0\}$

$wp(S1; S2, f_v < v_0) \overset{Ax3}{\equiv} wp(S1, wp(S2, n - i < v_0))$
$\overset{Ax1}{\equiv} wp(S1, true \land_L n - (i+2) < v_0)$
$\overset{Ax3}{\equiv} true \land_L (true \land_L n - (i+2) < v_0)$
$\equiv n - (i+2) < v_0$
$\equiv n - i - 2 < v_0$

$f_v = v_0$
$n - i = v_0$
$n - i - 2 = v_0 - 2 < v_0$

Guía 5. Ejercicio 7

proc `copiarSecuencia` (in s: $seq\langle\mathbb{Z}\rangle$, inout r: $seq\langle\mathbb{Z}\rangle$) {
  Pre $\{|s| = |r| \wedge r = r_0\}$
  Post $\{|s| = |r| \wedge_L (\forall j : \mathbb{Z})(0 \leq j < |s| \rightarrow_L s[j] = r[j])\}$
}

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

a) Escribir la precondición y la postcondición del ciclo.

b) Proponer un invariante y demostrar que el ciclo es parcialmente correcto.

c) Proponer una función variante que permita demostrar que el ciclo termina.