Algoritmos y Estructuras de Datos I
Segundo Cuatrimestre 2021

Guía Práctica 5
Demostración de corrección de ciclos en SmallLang

Departamento de Computación
Facultad de Ciencias Exactas y Natu
Universidad de Buenos Aires

Teorema del invariante: corrección de ciclos

Ejercicio 9. ★ Sea el siguiente ciclo con su correspondiente precondición y postcondición:

```
while (i >= |s| / 2) do
  S1: suma := suma + s[|s|−1−i];
  S2: i := i − 1;
endwhile
```

$$P_c : \{|s|\ mod\ 2 = 0 \wedge i = |s| - 1 \wedge suma = 0\}$$

$$Q_c : \{|s|\ mod\ 2 = 0 \wedge i = |s|/2 - 1\ \wedge_L\ suma = \sum_{j=0}^{|s|/2-1} s[j]\}$$

a) Especificar un invariante de ciclo que permita demostrar que el ciclo cumple la postcondición.

b) Especificar una función variante que permita demostrar que el ciclo termina.

c) Demostrar formalmente la corrección y terminación del ciclo usando el Teorema del invariante.

Solución

$$I : \{|s|\ mod\ 2 = 0 \wedge |s| > i \geq |s|/2 - 1\ \wedge_L suma = \sum_{j=0}^{|s|-2-i} s[j]\}$$

Justificación:

a) $|s|\ mod\ 2 = 0$: porque tengo que garantizar que no cambia en todo el ciclo.

b) $|s| > i \geq |s|/2 - 1$: porque es la condición que valdrá justo al finalizar el ciclo y antes.

c) $suma = \sum_{j=0}^{|s|-2-i} s[j]$: porque la sumatoria va "atrasada".

Veamos ahora que se cumplen las condiciones para probar que correctitud parcial:

$P_c \implies I$**:** Obviamente $|s|\ mod\ 2 = 0$. Como $i = |s| - 1$ claramente $|s| > i \geq |s|/2 - 1$ porque $|s| \geq |s|/2$.

Finalmente, $suma = \sum_{j=0}^{|s|-2-(|s|-1)} s[j] = \sum_{j=0}^{-1} s[j] = 0$.

$\{I \wedge B\} S_c \{I\}$: Para comprobar esto hay que calcular $I \wedge B \longrightarrow wp(S1, wp(S2, I))$.

Aplicando el axioma 1 tenemos que:

$wp(S2, I) = def(i-1) \wedge_L I^i_{i-1} =$

$True \wedge_L |s|\ mod\ 2 = 0 \wedge |s| > i-1 \geq |s|/2 - 1\ \wedge_L suma = \sum_{j=0}^{|s|-2-(i-1)} s[j] =$

$|s|\ mod\ 2 = 0 \wedge |s| \geq i \geq |s|/2\ \wedge_L suma = \sum_{j=0}^{|s|-i-1} s[j] \equiv E2$

$wp(S1, E2) = def(suma + s[|s|-1-i]) \wedge_L$

$|s|\ mod\ 2 = 0 \wedge |s| \geq i \geq |s|/2\ \wedge_L suma + s[|s|-1-i] = \sum_{j=0}^{|s|-i-1} s[j] =$

$0 \leq i < |s| \wedge_L |s|\ mod\ 2 = 0 \wedge |s| \geq i \geq |s|/2\ \wedge_L suma + s[|s|-1-i] = \sum_{j=0}^{|s|-i-1} s[j] =$

$|s|\ mod\ 2 = 0 \wedge |s| > i \geq |s|/2 \wedge_L suma + s[|s|-1-i] = \sum_{j=0}^{|s|-i-2} s[j] + s[|s|-1-i] =$

$|s|\ mod\ 2 = 0 \wedge |s| > i \geq |s|/2 \wedge_L suma = \sum_{j=0}^{|s|-i-2} s[j]$

Claramente $I \wedge B$ implican esta última expresión.

$I \wedge \neg B \Longrightarrow Q_c$: Claramente cuando termina el ciclo $|s| > i \geq |s|/2 - 1$ y $i < |s|/2$. Entonces $i = |s|/2 - 1$. Por lo tanto las dos primeras condiciones del Q_c se cumplen. De acuerdo al invariante la sumatoria valdrá:

$$suma = \sum_{j=0}^{|s|-2-(|s|/2-1)} s[j] =$$

$$\sum_{j=0}^{|s|-|s|/2-1)} s[j] =$$

Puesto que sabemos que $|s|\ mod\ 2 = 0$ entonces $|s| - |s|/2 = |s|/2$ y reemplazando en la ecuación anterior encontramos lo buscado.

Ahora para demostrar terminación debemos proponer una función variante. Tomemos $f_v = (i - |s|/2) + 1$. Veamos que las dos condiciones de terminación se cumplen:

$\{I \wedge B \wedge f_v = V_0\} S_c \{f_v < V_0\}$: Para comprobar esto hay que calcular:

$I \wedge B \wedge f_v = V_0 \longrightarrow wp(S1, wp(S2, \{(i - |s|/2) + 1 < V_0\}))$.

Aplicando el axioma 1 tenemos que:

$wp(S2, (i - |s|/2) + 1 < V_0) = def(i-1) \wedge_L \{(i - |s|/2) + 1 < V_0\}^i_{i-1} =$

$True \wedge_L (i - 1 - |s|/2) + 1) < V_0 = (i - |s|/2) < V_0 \equiv E2$

$wp(S1, E2) = def(suma + s[|s|-1-i]) \wedge_L (i - |s|/2) < V_0$

$0 \leq i < |s| \wedge_L (i - |s|/2) < V_0$

Claramente $f_v = V_0 = (i - |s|/2) + 1$ implican esta última expresión.

$I \wedge f_v \leq 0 \Longrightarrow \neg B$: Si $(i - |s|/2) + 1 \leq 0$ y que $i \geq |s|/2 - 1$ resulta que $i = |s|/2 - 1$. Esto implica que $i < |s|/2$.