Ejercicio 2 (Guía 5)

Vamos a demostrar los 5 puntos del teorema del invariante. Esto nos permite afirmar que el ciclo termina y es correcto respecto a su especificación (no demuestra que el programa entero sea correcto!). Especificación del ciclo:

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

$P_c \Rightarrow I$

Tenemos que vale P_c como hipótesis. Queremos probar que vale I. Vamos a probarlo por partes:

- Queremos ver que $0 \leq i \leq n+1$

  Sabemos que i = 0 (es información que nos da P_c). Entonces, reemplazando, lo que queremos ver es que $0 \leq 0 \leq n+1$. La primera parte, $0 \leq 0$, es una tautología. Nos resta ver si $0 \leq n+1$. Pero P_c indica también que $n \geq 0$, luego $n + i \geq 1 \geq 0$.

- Queremos ver que vale $i \ mod \ 2 = 0$

  Sabemos que i = 0, luego podemos afirmar que $i \ mod \ 2 = 0$

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

  Como $i = 0$, $\sum_{j=0}^{i-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi}) = \sum_{j=0}^{-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$. Recordemos que si el rango de una sumatoria es vacío (como en este caso), la sumatoria tiene valor 0. Luego $\sum_{j=0}^{i-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi}) = 0$. Pero además sabemos que $result = 0$ (por P_c), así que podemos afirmar que $0 = result = \sum_{j=0}^{i-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi}) = 0$

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

Queremos demostrar que vale Q_c, asumiendo que valen tanto I como $\neg B$. Es decir, queremos probar que $result = \sum_{j=0}^{n-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$.

Como sabemos que vale I, podemos afirmar $0 \leq i \leq n+1$. Además sabemos que vale $\neg B \equiv i \geq n$. Luego $n \leq i \leq n+1$. Hay dos valores de i que cumplen esa condición. Analicemos ambos casos:

- i = n

  En este caso, podemos reemplazar i por n en la parte de la sumatoria del invariante y obtenemos $result = \sum_{j=0}^{n-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$, exactamente lo que queríamos probar.

- i = n+1

  En este caso, si hacemos el mismo reemplazo llegamos a $result = \sum_{j=0}^{n}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi})$ (y esto no es a lo que queremos llegar!).

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

  Sabemos además que $i \ mod \ 2 = 0$ (información del invariante). Pero estamos en el caso en el cual $i = n+1$. Entonces podemos afirmar que si i es par, n es impar. Luego n no cumple la guarda del IF y podemos afirmar que $(\text{if } n \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi}) = 0$.

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

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

Queremos ver que vale la siguiente tripla de Hoare $\{I \wedge B\}$ ciclo $\{I\}$.
Llamemos S1 a la primer instrucción del cuerpo del ciclo, S2 a la segunda:
$S1$: `result := result + i ;`
$S2$: `i := i + 2`
Lo primero que haremos es calcular $wp(ciclo, I)$.

$$wp(S1; S2, I) \overset{Ax3}{\equiv} wp(S1, wp(S2, I)) \tag{1}$$

Antes de seguir, debemos calcular $wp(S2, I)$. Para eso usaremos el axioma 1:

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

Volviendo a (1), reemplazamos $p(S2, I)$ y nos queda:

$$wp(S1; S2, I) \overset{Ax3}{\equiv} wp(S1, wp(S2, I)) \equiv wp(S1, (0 \leq i+2 \leq n+1 \wedge i+2 \ mod \ 2 = 0 \wedge result = \sum_{j=0}^{i+1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi}))) \tag{2}$$

$\overset{Ax1}{\equiv} def(result+i) \wedge_L (0 \leq i+2 \leq n+1 \wedge i+2 \ mod \ 2 = 0 \wedge result+i = \sum_{j=0}^{i+1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi}))$
$\equiv true \wedge_L (0 \leq i+2 \leq n+1 \wedge i+2 \ mod \ 2 = 0 \wedge result+i = \sum_{j=0}^{i+1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi}))$

Una vez calculada la precondición más débil, debemos ver si $(I \wedge B)$ implican dicha precondición. Probaremos cada parte por separado:

- $0 \leq i+2 \leq n+1$

  Sabemos por I que $i > 0$, luego podemos afirmar que $0 \leq i+2$.
  Sabemos por B que $i < n$, luego (sumando 2 en ambos términos): $i+2 < n+2$, lo cual es equivalente a decir que $i+2 \leq n+1$

- $i+2 \ mod \ 2 = 0$

  Sabemos por I que $i \ mod \ 2 = 0$. Si i es par, al sumarle 2 sigue siendo par, luego $i+2 \ mod \ 2 = 0$ vale.

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

  La sumatoria puede separarse en 3 términos:
  $\sum_{j=0}^{i-1}(\text{if } j \ mod \ 2 = 0 \text{ then } j \text{ else } 0 \text{ fi}) +$
  $\text{if } i \ mod \ 2 = 0 \text{ then } i \text{ else } 0 \text{ fi} +$
  $\text{if } i+1 \ mod \ 2 = 0 \text{ then } i+1 \text{ else } 0 \text{ fi}$

  El primero de los 3 términos es igual a $result$ (lo sabemos por I).
  El segundo término es i (ya que por I sabemos que i es par).
  El tercer término es 0 (ya que por I sabemos que i es par, y por lo tanto $i+1$ es impar).

  Entonces, sumando los 3 términos nos queda: $result+i+0$, que es lo que esperábamos que valiera la sumatoria $\sum_{j=0}^{i+1}(...)$
  Como $(I \wedge B) \Rightarrow wp(ciclo, I$, podemos afirmar que el cuerpo del ciclo preserva el invariante.

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

Dado que queremos demostrar que vale una tripla de Hoare, comenzaremos calculando la precondición más débil $wp(ciclo, f_v < v_0)$.

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

Es decir, $wp(S1; S2, f_v < v_0) = n-i-2 < v_0$. Ahora debemos ver que $(I \wedge B \wedge v_0 = f_v)$ implican dicha WP. Parte de la hipótesis es que $v_0 = f_v$, es decir $v_0 = n-i$. Restando 2 a ambos lados, $n-i-2 = v_0 - 2 < v_0$.

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

Debemos mostrar que vale $\neg B$, es decir $i \geq n$.
Sabemos que $f_v \leq 0$, es decir $n-i \leq 0$, luego $n \leq i$, como queríamos demostrar.

Ejercicio 7 (Guía 5)

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
```

Especificación del ciclo:

- $P_c : i = 0 \land |s| = |r| \land r = r_0$
- $Q_c : i = |s| \land |s| = |r| \land_L (\forall j : \mathbb{Z})(0 \leq j < |s| \rightarrow_L s[j] = r[j])$
- $I : 0 \leq i \leq |s| \land |r_0| = |r| \land |s| = |r| \land_L (\forall j : \mathbb{Z})(0 \leq j < i \rightarrow_L r[j] = s[j]) \land (\forall j : \mathbb{Z})(i \leq j < |r| \rightarrow_L r[j] = r_0[j])$
- $f_v : n - i$

Sólo demostraremos corrección parcial de este ciclo.

$P_c \Rightarrow I$

Debemos demostrar que vale I sabiendo que vale P_c.

- $0 \leq i \leq |s|$
  Sabemos por P_c que $i = 0$, luego $0 \leq i$ vale. Además, $|s| \geq 0$ (porque las listas no pueden tener una cantidad negativa de elementos), luego $|s| \geq i$.
- $|r_0| = |r|$
  P_c indica que $r = r_0$. Si dos secuencias son iguales, entonces tienen la misma longitud.
- $|s|=|r|$
  P_c afirma exactamente eso
- $(\forall j : \mathbb{Z})(0 \leq j < i \rightarrow_L r[j] = s[j])$
  Dado que $i = 0$, al evaluar cualquier valor de j en $0 \leq j < i$ obtenemos False. Luego la implicación es verdadera para cualquier valor de j (es decir, para todos los valores).
- $(\forall j : \mathbb{Z})(i \leq j < |r| \rightarrow_L r[j] = r_0[j])$
  Dado que $i = 0$, esa expresión afirma que todas las posiciones de r son iguales a las de r_0. Esto es cierto pues por P_c sabemos que $r = r_0$

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

Debemos demostrar que vale Q_c sabiendo que vale $I \land \neg B$

- Por I sabemos que $i \leq |s|$, y por $\neg B$ sabemos que $i \geq |s|$. Entonces i debe ser igual a $|s|$
- Es trivial ver que vale $|s| = |r|$ ya que el invariante expresa exactamente eso
- Sabemos por I que $(\forall j : \mathbb{Z})(0 \leq j < i \rightarrow_L r[j] = s[j])$, y además sabemos que $i = |s|$. Reemplazando, el valor de i nos queda $(\forall j : \mathbb{Z})(0 \leq j < |s| \rightarrow_L r[j] = s[j])$, que es lo que queríamos ver.

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

Queremos ver que vale la siguiente tripla de Hoare $\{I \land B\}$ ciclo $\{I\}$.
Llamemos S1 a la primer instrucción del cuerpo del ciclo, S2 a la segunda:
$S1$: `r[i] := s[i] ;`
$S2$: `i := i + 1`

Empezaremos por calcular $wp(S1; S2, I)$, luego usaremos esa precondición para demostrar que vale la tripla.
$wp(S1; S2, I) \overset{Ax3}{\equiv} wp(S1, wp(S2, I))$

Calculemos entonces $wp(S2, I)$

$$\begin{aligned} wp(S2, I) &\overset{Ax1}{\equiv} def(i+1) \land_L 0 \leq i+1 \leq |s| \land |r_0| = |r| \land \\ &\quad |s| = |r| \land_L (\forall j : \mathbb{Z})(0 \leq j < i+1 \rightarrow_L r[j] = s[j]) \land (\forall j : \mathbb{Z})(i+1 \leq j < |r| \rightarrow_L r[j] = r_0[j]) \\ &\equiv 0 \leq i+1 \leq |s| \land |r_0| = |r| \land \\ &\quad |s| = |r| \land_L (\forall j : \mathbb{Z})(0 \leq j < i+1 \rightarrow_L r[j] = s[j]) \land (\forall j : \mathbb{Z})(i+1 \leq j < |r| \rightarrow_L r[j] = r_0[j]) \end{aligned}$$

Volvemos al cálculo anterior. Qué axioma usar? No hay ningún axioma para una instrucción con la forma de S1. Pero en realidad lo que estamos haciendo es una asignación. Podemos reescribirla como `r := setAt(r, i, s[i])` (también podemos escribirlo como `r := (r;i:s[i])`). Ahora sí tenemos una instrucción que permite utilizar el axioma 1.

$$\begin{aligned} wp(S1; S2, I) &\overset{Ax3}{\equiv} wp(r := setAt(r, i, s[i]), wp(S2, I)) \overset{Ax1}{\equiv} def(setAt(r, i, s[i]) \land_L wp(S2, I)^r_{setAt(r,i,s[i])} \\ &\equiv 0 \leq i < |r| \land 0 \leq i < |s| \land_L 0 \leq i+1 \leq |s| \land |r_0| = |setAt(r, i, s[i])| \land \end{aligned}$$

$|s| = |setAt(r, i, s[i])| \land_L (\forall j : \mathbb{Z})(0 \leq j < i + 1 \rightarrow_L setAt(r, i, s[i])[j] = s[j]) \land$
$(\forall j : \mathbb{Z})(i + 1 \leq j < |r| \rightarrow_L setAt(r, i, s[i])[j] = r_0[j])$

Revisemos las apariciones de setAt para ver si pueden ser reemplazadas/simplificadas:

- $|setAt(r, i, s[i])|$. Esta expresión es equivalente a $|r|$
- $setAt(r, i, s[i])[j]$. El valor de esta expresión depende del valor de i y el valor de j. Si $i = j$, la expresión evalúa a $s[i]$, en caso contrario evalúa a $r[j]$. En la primer aparición de dicha expresión, no podemos saber si $i = j$, ya que sabemos que $j < i+1$, así que tendremos que trabajar un poco más en esa parte de la expresión. La segunda aparición de $setAt$ se da cuando $i + 1 \leq j$, luego podemos afirmar que $i \neq j$. Es decir que en ese caso: $setAt(r, i, s[i])[j] = r[j]$

Entonces,
$wp(S1; S2, I) \equiv 0 \leq i < |r| \land 0 \leq i < |s| \land_L 0 \leq i + 1 \leq |s| \land |r_0| = |r| \land$
$|s| = |r| \land_L (\forall j : \mathbb{Z})(0 \leq j < i + 1 \rightarrow_L setAt(r, i, s[i])[j] = s[j]) \land$
$(\forall j : \mathbb{Z})(i + 1 \leq j < |r| \rightarrow_L r[j] = r_0[j])$

El cuantificador $(\forall j : \mathbb{Z})(0 \leq j < i + 1...$ puede reescribirse, teniendo en cuenta el rango hasta $< i$, y la expresión con $j = i$ aparte:
$wp(S1; S2, I) \equiv 0 \leq i < |r| \land 0 \leq i < |s| \land_L 0 \leq i + 1 \leq |s| \land |r_0| = |r| \land$
$|s| = |r| \land_L (\forall j : \mathbb{Z})(0 \leq j < i \rightarrow_L setAt(r, i, s[i])[j] = s[j]) \land setAt(r, i, s[i])[i] = s[i]$
$(\forall j : \mathbb{Z})(i + 1 \leq j < |r| \rightarrow_L r[j] = r_0[j])$

Ahora sí, en cada aparición de $setAt$, sabemos con certeza si $i = j$ o no:
$wp(S1; S2, I) \equiv 0 \leq i < |r| \land 0 \leq i < |s| \land_L 0 \leq i + 1 \leq |s| \land |r_0| = |r| \land$
$|s| = |r| \land_L (\forall j : \mathbb{Z})(0 \leq j < i \rightarrow_L r[j] = s[j]) \land s[i] = s[i]$
$(\forall j : \mathbb{Z})(i + 1 \leq j < |r| \rightarrow_L r[j] = r_0[j])$

Para tener en cuenta:

- $s[i] = s[i] \equiv true$
- Como $|s| = |r|$, entonces $\equiv 0 \leq i < |r| \equiv 0 \leq i < |s|$, y podemos dejar solo una de las expresiones.

$wp(S1; S2, I) \equiv 0 \leq i < |s| \land_L 0 \leq i + 1 \leq |s| \land |r_0| = |r| \land$
$|s| = |r| \land_L (\forall j : \mathbb{Z})(0 \leq j < i \rightarrow_L r[j] = s[j])$
$(\forall j : \mathbb{Z})(i + 1 \leq j < |r| \rightarrow_L r[j] = r_0[j])$

Veamos ahora que $(I \land B) \rightarrow wp(S1; S2, I)$. Usando como hipótesis $I \land B$, veamos que se cumplen todas las partes de $wp(S1; S2, I)$:

- $0 \leq i < |s|$
  Vale pues por I sabemos que $i \geq 0$, y por B sabemos que $i < |s|$
- $0 \leq i + 1 \leq |s|$
  Vale pues por I sabemos que $i \geq 0$, entonces $i + 1 \geq i \geq 0$ y por transitividad $i + 1 \geq 0$
  Además, por B sabemos que $i < |s|$, lo cual (dado que tratamos números enteros) es equivalente a $i + 1 \leq |s|$
- $|r_0| = |r|$
  Vale porque el invariante incluye esta misma expresión
- $|s| = |r|$
  Vale porque el invariante incluye esta misma expresión
- $(\forall j : \mathbb{Z})(0 \leq j < i \rightarrow_L r[j] = s[j])$
  Vale porque el invariante incluye esta misma expresión
- $(\forall j : \mathbb{Z})(i + 1 \leq j < |r| \rightarrow_L r[j] = r_0[j])$
  El invariante afirma que $r[j] = r_0[j]$ para los j que estén en el rango $rango_I = [i..|r|)$. El rango para el cual queremos ver su vale es $[i + 1..|r|)$, el cual está incluído en $rango_I$ (nuestro rango es *más chico* que $rango_I$), con lo cual podemos afirmar que $r[j] = r_0[j]$ para los j que nos interesan.