Métodos Formales en Ingeniería del Software

Práctica 5: Verificación Formal

Juan José Méndez Torrero
i42metoj@uco.es

Universidad de Córdoba

29 de abril de 2019

Índice

1. Ejercicio 1

Demostrar que los siguientes códigos son correctos

1. $\{x > 0\} \quad y := x + 1 \quad \{y > 1\}$

   Postcondición:

   $$\{y > 1\}_y^{x+1} \rightarrow \{x + 1 > 1\} \rightarrow \{x > 1 - 1\} \rightarrow \{x > 0\}$$

   El código se puede decir que es correcto al llegar a la precondición a través de la postcondición.

2. $\{\} \quad y := x; \quad y := x + x + y \quad \{y = 3 * x\}$

   Postcondición:

   $$\{y = 3{*}x\}_y^{x+x+y} \rightarrow \{x{+}x{+}y = 3{*}x\} \rightarrow \{y = 3{*}x{-}2{*}x\}_y^x \rightarrow \{x = 3{*}x{-}2{*}x\} \rightarrow \{0 = 3{*}x{-}3{*}x\} \rightarrow \{0 = 0\}$$

   El código se puede decir que es correcto al llegar a la precondición a través de la postcondición.

3. $\{x > 1\} \quad a := 1; \quad y := x; \quad y := y - a \quad \{y > 0 \ \wedge \ x > y\}$

   Postcondición:

   $$\{y > 0 \ \wedge \ x > y\}_y^{y-a} \rightarrow \{y - a > 0 \ \wedge \ x > y - a\}_y^x \rightarrow \{x - a > 0 \ \wedge \ x > x - a\}_a^1 \rightarrow$$

   $$\{x{-}1 > 0 \wedge x > x{-}1\} \rightarrow \{x > 1 \wedge 1 > x{-}x\} \rightarrow \{x > 1 \wedge 1 > 0\} \rightarrow \{x > 1 > 0\} \rightarrow \{x > 1\}$$

   El código se puede decir que es correcto al llegar a la precondición a través de la postcondición.

2. Ejercicio 2

Demostrar que el siguiente código es correcto.

$$\{x = A, \ y = B\}$$

$$x := 0$$

$$y := x + y$$

$$\{x = 0, \ y = B\}$$

¿Qué ocurre si intercambiamos el orden de las sentencias de asignación?

- **Postcondición:**

  $$\{x = 0, \ y = B\}_y^{x+y} \rightarrow \{x = 0, \ x + y = B\} \rightarrow \{x = 0, \ y = B - x\}_x^0 \rightarrow \{\{\}, \ y = B\}$$

  Como vemos, desde la postcondición hemos llegado a la precondición, ya que en el conjunto $\{\}$ está incluido $x = A$, con lo que podemos decir que este código es correcto. En el caso de intercambiar las sentencias, a partir de la postcondición no seríamos capaces de llegar a la precondición, con lo que el código no sería correcto. El razonamiento es el siguiente:

  $$\{x = 0, \ y = B\}_x^0 \rightarrow \{0 = 0, \ y = B\}_y^{x+y} \rightarrow \{\{\}, \ x + y = B\}$$

3. Ejercicio 3

Probar la corrección del siguiente fragmento de código.

```
{}
 a:= x+1
 IF (a — 1 = 0) THEN
    y:= 1
 ELSE
    y:= a
 END
{y = x+1}
```

Lo que primero vamos a hallar son los posibles estados a los que se podría llegar a través de la condición:

$$\{a := x + 1 \ \wedge \ (a = 1)\} \ y := 1 \ \{y = x + 1\}$$
$$\{a := x + 1 \ \wedge \ (a \neq 1)\} \ y := a \ \{y = x + 1\}$$

A continuación, analizaremos los dos casos anteriores y comprobar que a través de las postcondición, podemos llegar a la precondición.

- $\{a := x + 1 \ \wedge \ (a = 1)\} \ y := 1 \ \{y = x + 1\}$:

  $$\{y = x + 1\}_y^1 \rightarrow \{x = 0\} \rightarrow \{a := 1\}$$

  Como vemos, hemos llegado a la precondición, con lo que por ahora, podemos decir que el código está correcto.

- $\{a := x + 1 \ \wedge \ (a \neq 1)\} \ y := a \ \{y = x + 1\}$:

  $$\{y = x + 1\}_y^a \rightarrow \{a = x + 1\} \rightarrow \{a := a \wedge (a \neq 1)\} \rightarrow \{(a \neq 1)\}$$

  Finalmente, podemos decir que el código es correcto ya que tanto el primero como el segundo estado son capaces de llegar de la postcondición a la precondición.

4. Ejercicio 4

Verifica formalmente la función factorial que calcula el factorial de un número. Razona tu respuesta.

```
entero función factorial (E entero:n)
{n=N ≥ 0}
var
   entero: k,f
inicio
 k:= 0
 f:= 1
 mientras k<n hacer  {n=N≥0 ∧ k≤n ∧ f=k!}
    k:= k + 1
    f:= f * k
 fin_mientras

 {f = N!}
 devolver f
 fin_función
 Función de cota → t= n-k
```

Para verificar este código, tendremos que hacer uso de la regla de composición secuencial, para poder así dividir el código en dos bloques para finalmente verificarlos por separado. Los dos bloques a analizar son los siguientes:

1. **Bloque 1:**
   $\{n = N \ \geq \ 0\}$
   $k \leftarrow 0$
   $f \leftarrow 1$
   $\{n = N \geq 0 \ \wedge k \leq n \ \wedge \ f = k!\}$
2. **Bloque 2:**
   $\{n = N \geq 0 \ \wedge k \leq n \ \wedge \ f = k!\}$
   mientras $k < n$ **hacer**
   $k \leftarrow k + 1$
   $f \leftarrow f * k$
   fin_mientras
   $\{f = N!\}$

Una vez divididos los dos bloques, comenzaremos demostrando el primero bloque.

Demostración bloque 1:

Aplicando los axiomas de la asignación llegamos al siguiente razonamiento:

$\{n = N \geq 0 \ \wedge 0 = 0 \ \wedge \ 1 = 1\}$
$k \leftarrow 0$
$\{n = N \geq 0 \ \wedge 0 = k \ \wedge \ 1 = 1!\}$

$f \leftarrow 1$
$\{n = N \geq 0 \ \wedge 0 = k \ \wedge \ f = 1!\}$

Como vemos, las especificaciones son correctas, ahora, verificaremos la especificación aplicando la regla de la consecuencia.

$n = N > 0 \rightarrow n = N \geq 0 \ \wedge \ 0 = 0 = 0 \ \wedge \ 1 = 1$

Al tener incluido el antecedente en el consecuente y tener igualdades cuyo valor son verdades absolutas, la especificación se considera correcta.

Demostración bloque 2:

A diferencia que con el primer bloque, en este caso hay que especificar un bucle, con lo que para realizar su especificación vamos a tener que utilizar la siguiente invariante:

$$I \ \equiv \ n = N \ \geq \ 0 \ \wedge \ k \leq \ n \ \wedge \ f = k!$$

1. Como sabemos, P es la precondición e I la invariante, con lo que tenemos que: $P \Rightarrow I$

   $n = N \geq 0 \ \wedge \ k = 0 \ \wedge \ f = 1 \Rightarrow n = N \geq 0 \ \wedge \ k \leq n \ \wedge \ f = k!$

   $n = N \geq 0 \Rightarrow n = N \geq 0$

   $n = N \geq 0 \ \wedge \ k = 0 \Rightarrow k \leq n$

   $k = 0 \ \wedge \ f = 1 \Rightarrow f = k!$

   Como en lógica si el antecedente es cierto, el consecuente también lo es, podremos decir que esto es cierto.

2. $I \ \wedge \ \neg B \Rightarrow Q$

   $n = N \geq 0 \ \wedge \ k \leq n \ \wedge \ f = k! \ \wedge \ \neg(k < n) \Rightarrow f = N!$

   $k \leq n \ \wedge \ \neg(k < n) \Rightarrow k \leq n \ \wedge \ k \geq n$

   $k \leq n \ \wedge \ k \geq n \Rightarrow k = n$

   $n = N \geq 0 \ \wedge \ k = n \ \wedge \ f = k! \ \Rightarrow \ f = N!$

   Esta implicación es cierta ya que se cumple el consecuente.

3. $\{I \ \wedge \ B\}S\{I\}$

   $\{n = N \geq 0 \ \wedge \ k \leq n \ \wedge \ f = k! \ \wedge \ k < n\}$

   $k \leftarrow k + 1$

   $f \leftarrow f * k$

   $\{n = N \geq 0 \ \wedge \ k \leq n \ \wedge \ f = k!\}$

   A continuación se aplicarán las reglas de composición secuencial y de asignación:

   $\{n = N \geq 0 \ \wedge \ k + 1 \leq n \ \wedge \ f * (k + 1) = (k + 1)!\}$

   $k \leftarrow k + 1$

   $\{n = N \geq 0 \ \wedge \ k \leq n \ \wedge \ f * k = k!\}$

   $f \leftarrow f * k$

   $\{n = N \geq 0 \ \wedge \ k \leq n \ \wedge \ f = k!\}$

   Esta especificación es verdadera, con lo que podríamos decir que es correcta. Seguidamente, aplicaremos la regla de la consecuencia:

   $n = N \geq 0 \ \wedge \ k \leq n \ \wedge \ f = k! \ \wedge \ k < n \Rightarrow n = N \geq 0 \ \wedge \ k + 1 \leq n \ \wedge \ f * (k + 1) = (k + 1)!$

$n = N \geq 0 \Rightarrow n = N \geq 0$

$k \leq n \ \wedge \ k < n \Rightarrow k < n$

$k < n$ por lo que $k + 1 \leq n$. En el caso de que $f = k!$ sea cierto, al multiplicar por $(k + 1)$ se tiene:

$f * (k + 1) = k! * (k + 1) \Rightarrow f * (k + 1) = (k + 1)!$

Hasta ahora, la especificación es correcta. Seguidamente, para que sea completamente correcta hay que comprobar la corrección total.

Como hemos visto, todas las verificaciones realizadas sobre el segundo bloque son ciertas, con lo que podremos decir que el segundo bloque es correcto.

Teniendo que $t = n - k$

1. $I \ \wedge \ B \Rightarrow t > 0$

   $\{n = N \ \wedge \ n \geq 0 \ \wedge \ k \leq n \ \wedge \ f = k! \ \wedge \ k < n \Rightarrow \{n - k > 0\}\}$

   $k \leq n \ \wedge \ k < n \Rightarrow k < n$

   $k < n \Rightarrow n - k > 0$

   Por lo que la implicación es cierta.

2. $\{I \ \wedge \ B \ \wedge \ t = T\} S \{t < T\}$

   $\{n = N \ \wedge \ n \geq 0 \ \wedge \ k \leq n \ \wedge \ f = k! \ \wedge \ k < n \ \wedge \ (n - k) = T$

   Aplicando el axioma de la asignación a ambas instrucciones:

   $\{n - (k + 1) < T\}$

   $k \leftarrow k + 1$

   $\{(n - k) < T\}$

   $f \leftarrow f * k$

   $\{n - k < T\}$

   De aquí obtenemos que las dos especificaciones son correctas. A continuación les aplicaremos la regla de composición secuencial:

   $\{n - (k + 1) < T\}$

   $k \leftarrow k + 1$

   $f \leftarrow f * k$

   $\{n - k < T\}$

   La especificación sigue siendo correcta, por lo que ahora deberíamos de aplicar la regla de la consecuencia, llegando a lo siguiente:

   $n = N \geq 0 \ \wedge \ k \leq n \ \wedge \ f = k! \ \wedge \ k < n \ \wedge \ (n - k) = T \Rightarrow n - (k + 1) < T$

   $k \leq n \ \wedge \ k < n \Rightarrow k < n$

   $k < n \ \wedge \ (n - k) = T \Rightarrow n - (k + 1) < T$

   Puesto que $n(k + 1) = (n - k) - 1 = T - 1$, como $\forall x \ xzx \ + \ 1$, entonces $T - 1 < T$

Una vez hecho esto, vemos que este código para calcular el factorial de un número es correcto.

5. Ejercicio 5

Verifica formalmente la función potencia de un número. Razona tu respuesta.

```
entero función potencia (E entero:x, E entero:y)
{x = A ∧ y=B ∧ y ≥ 0}
var
   entero: r
inicio
   r:=1
mientras y > 0 hacer      {y ≥ 0 ∧ r*x^y=A^B}
   si impar(y) entonces
      y := y -1
      r := r*x
   si_no
      y := ⌊y/2)⌋
      x := x*x
   fin_si
fin_mientras
{r=A^B}
devolver r
fin_funcion
Función de cota → t= y
```

Como vemos, para esta función tendremos que hacer como en el ejercicio anterior, es decir, primero verificar la asignación y después verificar el bucle. La asignación se verificaría de la siguiente manera:

$$\{x = A \ \wedge \ y = B \ \wedge y \geq 0\}$$

$$r := 1$$

$$\{x = A \ \wedge \ y = B \ \wedge y \geq 0 \ \wedge \ r \geq 1\}$$

Visto esto, comprobamos que la verificación es inmediata. Seguidamente, vamos a verificar el bucle *mientras*. Para ello, vamos a dividir el bucle en dos bloques.

- **Corrección parcial:**

  1. $P \Rightarrow I$
     $\{x = A \ \wedge \ y = B \ \wedge y \geq 0 \ \wedge \ r := 1\} \Rightarrow \{y \geq 0 \ \wedge \ r * x^y = A^B\}$
     $\{x = A \ \wedge \ y = B \ \wedge y \geq 0 \ \wedge \ r := 1\} \rightarrow \{x^y = A^y \ \wedge \ y = B \ \wedge \ y \geq 0 \ \wedge \ r := 1\}$
     $\{x^y = A^y \ \wedge \ y = B \ \wedge y \geq 0 \ \wedge \ r := 1\} \rightarrow \{r * x^y = A^B \ \wedge \ y = B \ \wedge \ y \geq 0 \ \wedge \ r := 1\}$
     Como podemos observar, al añadir las condiciones $y = B$ y $r = 1$ hacemos que la precondición sea más restrictiva.
  2. $I \ \wedge \ \neg B \Rightarrow Q$
     $\{y \geq 0 \ \wedge \ r * x^y = A^B \ \wedge \ \neg(y > 0)\} \Rightarrow \{r = A^B\}$
     $\{y \geq 0 \ \wedge \ r * x^y = A^B \ \wedge \ y \leq 0\} \rightarrow \{y = 0 \ \wedge \ r * x^y = A^B\} \rightarrow \{y = 0 \ \wedge \ r * x^0 = A^B\}$
     $\{y = 0 \ \wedge \ r * x^0 = A^B\} \rightarrow \{y = 0 \ \wedge \ r = A^B\}$
     Al añadir una condición para y, la precondición se hace más restrictiva.
  3. $\{I \ \wedge \ B\}S\{I\}$
     Ahora, tendremos que comprobar la sentencia condicional, la cual se volverá a dividir en dos bloques:

a) $\{P \ \wedge \ B\}S_1\{Q\}$
$y \geq 0 \ \wedge \ r * x^y = A^B \ \wedge \ y > 0 \ \wedge \ impar(y)$
$y := y - 1$
$\{y \geq 0 \ \wedge \ r * x * x^y = A^B\}_y^{y-1}$
$r := r * x$
$\{y \geq 0 \ \wedge \ r * x^y = A^B\}_r^{r*x}$
La precondición es más restrictiva ya que añadimos una condición para $y.(r*x*x^y = A^B \rightarrow r * x^y = A^B)$

b) $\{P \ \wedge \ \neg B\}S_2\{Q\}$
$\{y \geq 0 \ \wedge \ r * x^y = A^B \ \wedge \ y > 0 \ \wedge \ \neg impar(y)\}$
$\{y \geq 0 \ \wedge \ r * (x * x)^{\frac{y}{2}} = A^B\}$
$y := \frac{y}{2}$
$\{y \geq 0 \ \wedge \ r * (x * x)^y = A^B\}_y^{\frac{y}{2}}$
$x := x * x$
$\{y \geq 0 \ \wedge \ r * x^y = A^B\}_x^{x*x}$
Como finalmente tenemos la siguiente implicación $r * (x * x)^{\frac{y}{2}} = A^B \rightarrow r * x^y = A^B$, podemos decir que es cierta.

Al final, hemos conseguido verificar tanto el bucle como la asignación, quedando la corrección parcial terminada.

- **Corrección total:**

Teniendo que $t = y$:

1. $\{I \ \wedge \ B\} \Rightarrow t > 0$
$\{y \geq 0 \ \wedge \ r * x^y = A^B \ \wedge \ y > 0\} \Rightarrow y > 0$
$\{y \geq 0 \ \wedge \ r * x^y = A^B \ \wedge y > 0\} \rightarrow \{y > 0 \ \wedge \ r * x^y = A^B\}$
Con esto demostramos que la implicación es cierta.
2. $\{I \ \wedge \ B \ \wedge \ t = T\}S\{t < T\}$
Seguidamente, comprobamos la sentencia condicional doble:

a) $\{P \ \wedge \ B\}S_1\{Q\}$
$\{y \geq 0 \ \wedge \ r * x^y = A^B \ \wedge \ y > 0 \ \wedge \ y = T \ \wedge \ impar(y)\}$
$\{y - 1 < T\}$
$y := y - 1$
$\{y < T\}_y^{y-1}$
$r := r * x$
$\{y < T\}_r^{r*x}$
Al tener que $y = T \rightarrow y - 1 = T - 1 \rightarrow T - 1 < T \rightarrow y - 1 < T$, este condicional queda demostrado.

b) $\{P \ \wedge \neg B\}S_2\{Q\}$
$\{y \geq 0 \ \wedge \ r * x^y = A^B \ \wedge \ y > 0 \ \wedge \ y = T \ \wedge \ \neg impar(y)\}$
$\{\frac{y}{2} < T\}$
$y := \frac{y}{2}$
$\{y < T\}_y^{\frac{y}{2}}$
$x := x * x$
$\{y < T\}_x^{x*x}$
Gracias a que $y = T \rightarrow \frac{y}{2} = \frac{T}{2} \rightarrow \frac{T}{2} < T \rightarrow \frac{y}{2} < T$ decimos que la implicación se ha cumplido.

Para finalizar, una vez verificadas la condición doble y el bucle, concluimos la corrección total quedando verificada la función para calcular la potencia de un número.