Universidad de Cádiz

Metodología de la Programación

Ingeniería Técnica en Informática de Gestión

Ingeniería Técnica en Informática de Sistema

Departamento de Lenguajes y Sistemas Informáticos

TEMA 2 – TEORÍA

VERIFICACIÓN DE ALGORITMOS

Ejercicios resueltos

Ejercicio.- Demuestra que la siguiente especificación es correcta. Razona detalladamente la respuesta.

$\{n=N\geq 0\}$
i←0
k←0
mientras i ≤ n
    k←k+i
    i←i+1
fin mientras
k←k*2
$\left\{k=\sum_{\alpha=1}^{N} 2*\alpha\right\}$

1er Bloque: i←0, k←0

2º Bloque: mientras i ≤ n … fin mientras

3er Bloque: k←k*2

Para poder verificar este fragmento de pseudocódigo comprobamos si cumple dicha especificación. Para ello, se aplica la regla de composición secuencial y se divide la especificación en los tres bloques que se indican con las líneas que aparecen a la derecha de la especificación y que se han numerado con 1, 2 y 3. Es necesario incluir dos asertos intermedios, uno que actúe a su vez de postcondición de las dos instrucciones de asignación y de precondición del bucle mientras y otro aserto que sea, a la vez, postcondición del bucle mientras y precondición de la última instrucción del fragmento, una instrucción de asignación.

El primer aserto lo podemos obtener anotando las instrucciones de asignación:

$\{n=N\geq 0\}$
i←0
k←0
$\{n=N\geq 0 \wedge i=0 \wedge k=0\}$

Y el segundo, podemos obtenerlo aplicando el axioma de asignación:

$\left\{2*k=\sum_{\alpha=1}^{N} 2*\alpha\right\}$
k←k*2
$\left\{k=\sum_{\alpha=1}^{N} 2*\alpha\right\}$

Luego añadiendo los asertos intermedios, la especificación a demostrar sería:

{n=N≥0}
i←0
k←0
{ N≥0 ∧ i=0 ∧ k=0}
mientras i ≤ n
    k←k+i
    i←i+1
fin mientras

$$\left\{2 * k = \sum_{\alpha=1}^{N} 2 * \alpha\right\}$$

k←k*2

$$\left\{k = \sum_{\alpha=1}^{N} 2 * \alpha\right\}$$

3^er^ Bloque) La última instrucción de asignación queda demostrada al haberse aplicado el axioma de asignación. Por tanto, la especificación

$$\left\{2 * k = \sum_{\alpha=1}^{N} 2 * \alpha\right\}$$

k←k*2

$$\left\{k = \sum_{\alpha=1}^{N} 2 * \alpha\right\}$$

es correcta.

Veamos a continuación la demostración de los dos primeros bloques.

1^er^ Bloque)

{n=N≥0}
i←0
k←0
{n=N≥0 ∧ i=0 ∧ k=0}

Aplicando la regla inferencia de la composición secuencial y la regla de inferencia de la asignación, obtenemos la siguiente especificación correcta:

{n=N≥0 ∧ 0=0 ∧ 0=0}
i←0
{n=N≥0 ∧ i=0 ∧ 0=0}
k←0
{n=N≥0 ∧ i=0 ∧ k=0}

Cómo, el predicado n=N≥0 ⇒ n=N≥0 ∧ 0=0 ∧ 0=0 es trivialmente cierto al ser 0=0 una tautología, entonces la especificación que representa el primer bloque es correcta.

2º Bloque) Quedaría por demostrar la especificación para el bucle mientras:

{n=N≥0 ∧ i=0 ∧ k=0}
mientras i ≤ n
  k←k+i
  i←i+1
fin mientras

$$\left\{2*k=\sum_{\alpha=1}^{N}2*\alpha\right\}$$

Para ello, proponemos el siguiente invariante: $k=\sum_{\alpha=1}^{i-1}\alpha \wedge i\leq(n+1)\wedge n=N\geq 0$

a) P⇒ I

n=N≥0 ∧ i=0 ∧ k=0 ⇒ $k=\sum_{\alpha=1}^{i-1}\alpha \wedge i\leq(n+1)\wedge n=N\geq 0$

Si n=N≥0 entonces n=N≥0
Si n=N≥0 ∧ i=0 entonces i≤(n+1), es decir, 0≤(n+1)
Si i=0 ∧ k=0 entonces $k=\sum_{\alpha=1}^{i-1}\alpha \quad\equiv\quad 0=\sum_{\alpha=1}^{0-1}\alpha$

Si el antecedente es cierto entonces el consecuente también lo es, siendo cierto el predicado.

b) I ∧¬B ⇒ Q

$$k=\sum_{\alpha=1}^{i-1}\alpha \wedge i\leq(n+1)\wedge n=N\geq 0\wedge\neg(i\leq n)\Rightarrow 2*k=\sum_{\alpha=1}^{N}2*\alpha$$

Si i≤(n+1) ∧ ¬(i≤n) entonces i≤(n+1) ∧ i>n por tanto i=n+1
Si i=n+1 ∧ n=N≥0 entonces i=N+1, por tanto, sustituyendo en el antecedente i por su valor N+1 se obtiene $2*k=\sum_{\alpha=1}^{(N+1)-1}2*\alpha$ es decir $2*k=\sum_{\alpha=1}^{N}2*\alpha$, por tanto se cumple el consecuente. El predicado es cierto.

c) {I ∧B} S {I}

$$\left\{k=\sum_{\alpha=1}^{i-1}\alpha \wedge i\leq(n+1)\wedge n=N\geq 0\wedge i\leq n\right\}$$

  k←k+i
  i←i+1

$$\left\{k=\sum_{\alpha=1}^{i-1}\alpha \wedge i\leq(n+1)\wedge n=N\geq 0\right\}$$

Para demostrar esta especificación, aplicamos la regla de inferencia de la composición secuencial y el axioma de asignación, obteniendo que la siguiente especificación es correcta:

$$\left\{ k+i=\sum_{\alpha=1}^{i}\alpha \wedge i+1 \le (n+1) \wedge n=N \ge 0 \right\}$$

k←k+i

$$\left\{ k=\sum_{\alpha=1}^{i}\alpha \wedge i+1 \le (n+1) \wedge n=N \ge 0 \right\}$$

i←i+1

$$\left\{ k=\sum_{\alpha=1}^{i-1}\alpha \wedge i \le (n+1) \wedge n=N \ge 0 \right\}$$

Aplicando la primera regla de consecuencia, quedaría por demostrar:

$$k=\sum_{\alpha=1}^{i-1}\alpha \wedge i \le (n+1) \wedge n=N \ge 0 \wedge i \le n \quad \Rightarrow \quad k+i=\sum_{\alpha=1}^{i}\alpha \wedge i+1 \le (n+1) \wedge n=N \ge 0$$

Si i≤n entonces i+1≤(n+1)

Si n=N≥0 entonces n=N≥0, trivialmente cierto.

Si a la expresión $k=\sum_{\alpha=1}^{i-1}\alpha$, le sumamos a ambos miembros la variable i obtenemos $k+i=\sum_{\alpha=1}^{i-1}\alpha+i=\sum_{\alpha=1}^{i}\alpha$, por tanto esa implicación es cierta.

Todas las condiciones de verificación generadas por a), b) y c) son ciertas, por tanto, la especificación del 2º bloque es parcialmente correcta.

Al ser correctas las especificaciones del 1er, 2º y 3er bloques la especificación

{n=N≥0}
i←0
k←0
mientras i ≤ n
        k←k+i
        i←i+1
fin mientras
k←k*2

$$\left\{ k=\sum_{\alpha=1}^{N}2*\alpha \right\}$$

es parcialmente correcta.

Para demostrar que es totalmente correcta, tendremos que demostrar que son ciertas las condiciones de verificación generadas por:

d) $I \wedge B \Rightarrow t>0$
e) y las generadas por $\{ I \wedge B \wedge t=T\} S \{t<T\}$

Para ello, se asocia al bucle una función *t* monótona decreciente acotada, demostrando que tras un número finito de repeticiones se alcanza el límite y el bucle termina. En este caso podría considerarse t=n+1-i

d) $I \wedge B \Rightarrow t>0$

$$k=\sum_{\alpha=1}^{i-1}\alpha \wedge i \le (n+1) \wedge n=N \ge 0 \wedge i \le n \;\Rightarrow\; t=n+1-i>0$$

Si $i \le (n+1) \wedge i \le n$ entonces $i \le n$
Si $i \le n \wedge n=N \ge 0$ entonces $t=n+1-i>0$
La condición de verificación es cierta.

e) $\{ I \wedge B \wedge t=T\} S \{t<T\}$

$$\left\{k=\sum_{\alpha=1}^{i-1}\alpha \wedge i \le (n+1) \wedge n=N \ge 0 \wedge i \le n \wedge n+1-i=T\right\}$$

k←k+i
i←i+1
$\{n+1-i<T\}$

Para demostrar esta especificación, aplicamos la regla de composición secuencial y la regla de inferencia de la asignación, y obtenemos que la especificación:

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

es una especificación correcta.

Quedaría por demostrar que

$$k=\sum_{\alpha=1}^{i-1}\alpha \wedge i \le (n+1) \wedge n=N \ge 0 \wedge i \le n \wedge n+1-i=T \;\Rightarrow\; n+1-(i+1)<T$$

Si $i \le n \wedge n=N \ge 0 \wedge n+1-i=T$ entonces n+1-i-1=T-1 siendo T-1<T , por tanto es un predicado cierto.

Todas las condiciones de verificación generadas son ciertas, luego la especificación es totalmente correcta.

(Ejercicio número 9 del guión de prácticas número 2)
Ejercicio.- Demuestra que la siguiente especificación es correcta. Razona detalladamente la respuesta.

$\{A\neq 0 \wedge n \geq 0\}$
x ← 1
si n≠0 **entonces**
  i ← 0
  mientras i < n **hacer**
    x ←A*x
    i←i+1
  fin_mientras
fin_si
$\{x=A^n\}$

Esta especificación será correcta si todas las condiciones de verificación que se generan son ciertas. Se aplica la regla de composición secuencial, utilizando un aserto intermedio adecuado se divide la especificación en dos, de forma que dicho aserto será la postcondición de la instrucción de asignación y la precondición del bucle mientras.

1) Anotando la instrucción de asignación, obtenemos la siguiente postcondición:
$\{A\neq 0 \wedge n \geq 0\}$
x ← 1
$\{A\neq 0 \wedge n \geq 0 \wedge x=1\}$

Aplicando el axioma de asignación, se obtiene la siguiente especificación correcta:
$\{A\neq 0 \wedge n \geq 0 \wedge 1=1\}$
x ← 1
$\{A\neq 0 \wedge n \geq 0 \wedge x=1\}$

Aplicando la primera regla de consecuencia, se obtiene una única condición de verificación:

$$A\neq 0 \wedge n \geq 0 \Rightarrow A\neq 0 \wedge n \geq 0 \wedge 1=1$$

que es cierta, al ser 1=1 una tautología.

(Recordamos que aplicar el axioma de asignación y la primera regla de consecuencia es aplicar la regla de inferencia de la asignación).

2) $\{A\neq 0 \wedge n \geq 0 \wedge x=1\}$
si n≠0 **entonces**
  i ← 0
  mientras i < n **hacer**
    x ←A*x
    i←i+1
  fin_mientras
fin_si
$\{x=A^n\}$

Aplicando el esquema de selección, obtenemos las condiciones de verificación siguientes:

2.1) $P \wedge \neg B \Rightarrow Q$

$A \neq 0 \wedge n \geq 0 \wedge x=1 \wedge \neg (n \neq 0) \Rightarrow x=A^n$

Si $\neg (n \neq 0) \Rightarrow n=0$

Si $A \neq 0 \wedge n=0 \wedge x=1$ entonces $x= A^n=A^0=1$

Por tanto el predicado $A \neq 0 \wedge n \geq 0 \wedge x=1 \wedge \neg (n \neq 0) \Rightarrow x=A^n$ es cierto.

2.2) Y las generadas por $\{P \wedge B\}$ S $\{Q\}$

$\{A \neq 0 \wedge n \geq 0 \wedge x=1 \wedge n \neq 0\}$
  $i \leftarrow 0$
  mientras $i < n$ **hacer**
    $x \leftarrow A*x$
    $i \leftarrow i+1$
  fin_mientras
$\{x=A^n\}$

Para demostrar esta especificación se aplica la regla de composición, obteniendo dos especificaciones:

$\{A \neq 0 \wedge n \geq 0 \wedge x=1 \wedge n \neq 0\}$
  $i \leftarrow 0$
$\{A \neq 0 \wedge n \geq 0 \wedge x=1 \wedge n \neq 0 \wedge i=0\}$

que por la regla de inferencia de la asignación obtenemos el predicado:

$$A \neq 0 \wedge n \geq 0 \wedge x=1 \wedge n \neq 0 \Rightarrow A \neq 0 \wedge n \geq 0 \wedge x=1 \wedge n \neq 0 \wedge 0=0$$

que es trivialmente cierto.

Y la especificación:

$\{A \neq 0 \wedge n \geq 0 \wedge x=1 \wedge n \neq 0 \wedge i=0\}$
mientras $i < n$ **hacer**
  $x \leftarrow A*x$
  $i \leftarrow i+1$
fin_mientras
$\{x=A^n\}$

Para demostrar la corrección parcial de esta especificación, buscamos un invariante del bucle, se puede proponer como invariante: $x=A^i \wedge i \leq n$

$\{A \neq 0 \wedge n \geq 0 \wedge x=1 \wedge n \neq 0 \wedge i=0\}$
mientras $i < n$ **hacer** $\{x=A^i \wedge i \leq n\}$
  $x \leftarrow A*x$
  $i \leftarrow i+1$
fin_mientras
$\{x=A^n\}$

Las condiciones de verificación generadas son:

a) $P \Rightarrow I$

$$A \neq 0 \wedge n \geq 0 \wedge x=1 \wedge n \neq 0 \wedge i=0 \Rightarrow x=A^i \wedge i \leq n$$

Si $n \geq 0 \wedge n \neq 0 \wedge i=0$ entonces $i \leq n$

Si $A \neq 0 \wedge x=1 \wedge i=0$ entonces $x=A^i = A^0=1$

Por tanto, el predicado $A \neq 0 \wedge n \geq 0 \wedge x=1 \wedge n \neq 0 \wedge i=0 \Rightarrow x=A^i \wedge i \leq n$ es cierto.

b) $I \wedge \neg B \Rightarrow Q$

$$x=A^i \wedge i \leq n \wedge \neg(i<n) \Rightarrow x=A^n$$

Si $i \leq n \wedge \neg(i<n)$ entonces $i \leq n \wedge i \geq n$ es decir, que $i=n$

Si $x=A^i \wedge i=n$ entonces $x=A^n$

Por tanto, la condición de verificación es cierta.

c) Y las generadas por $\{I \wedge B\}\ S\ \{I\}$

$\{x=A^i \wedge i \leq n \wedge i<n\}$

$x \leftarrow A*x$

$i \leftarrow i+1$

$\{x=A^i \wedge i \leq n\}$

Aplicando el esquema de composición secuencial y el axioma de asignación, obtenemos la siguiente especificación correcta:

$\{A*x=A^{i+1} \wedge (i+1) \leq n\}$

$x \leftarrow A*x$

$\{x=A^{i+1} \wedge (i+1) \leq n\}$

$i \leftarrow i+1$

$\{x=A^i \wedge i \leq n\}$

Sólo nos quedaría probar el predicado:

$$x=A^i \wedge i \leq n \wedge i<n \Rightarrow A*x=A^{i+1} \wedge (i+1) \leq n$$

Si $x=A^i$ entonces si se multiplican ambos miembros por A, obtendríamos $A*x=A^i*A=A^{i+1}$

Si $i \leq n \wedge i<n$ entonces $i<n$, es decir que $(i+1) \leq n$.

Todas las condiciones de verificación generadas con ciertas luego la especificación es parcialmente correcta.

Para demostrar que es totalmente correcta, tendremos que demostrar que son ciertas las condiciones de verificación generadas por:

d) $I \wedge B \Rightarrow t>0$

e) y las generadas por $\{I \wedge B \wedge t=T\} S \{t<T\}$

Para ello, se asocia al bucle una función *t* monótona decreciente acotada, demostrando que tras un número finito de repeticiones se alcanza el límite y el bucle termina. En este caso podría considerarse $t=n-i$

d) $I \wedge B \Rightarrow t>0$

$x=A^i \wedge i \le n \wedge i<n \Rightarrow n-i>0$

Si $i<n$ entonces $n-i>0$. La condición de verificación es cierta.

e) $\{I \wedge B \wedge t=T\} S \{t<T\}$

$\{x=A^i \wedge i \le n \wedge i<n \wedge n-i=T\}$
x ←A*x
i←i+1
$\{n-i<T\}$

Para demostrar esta especificación, aplicamos la regla de composición secuencial y la regla de inferencia de la asignación, y obtenemos que la especificación:

$\{n-(i+1)<T\}$
x ←A*x
$\{n-(i+1)<T\}$
i←i+1
$\{n-i<T\}$

es una especificación correcta.

Quedaría por demostrar que
$x=A^i \wedge i \le n \wedge i<n \wedge n-i=T \Rightarrow n-(i+1)<T$

Si $i<n \wedge n-i=T$ entonces $n-(i+1)= n-i-1<T$, por tanto es un predicado cierto.

Todas las condiciones de verificación generadas son ciertas, luego la especificación

$\{A \neq 0 \wedge n \geq 0\}$
x ← 1
si n≠0 **entonces**
    i ← 0
    mientras i < n **hacer**
        x ←A*x
        i←i+1
    fin_mientras
fin_si
$\{x=A^n\}$

es totalmente correcta.

(Ejercicio número 10 del guión de prácticas número 2)
Ejercicio.- Demuestra que la siguiente especificación es correcta. Razona detalladamente la respuesta.

{ $n=A\geq 0 \wedge x=0$ }
mientras $(x+1)^2 \leq n$ **hacer**
  $x \leftarrow x+1$
fin_mientras
{ $x = \lfloor \sqrt{A} \rfloor$ }

En primer lugar, va a resultar más sencillo si reformulamos la postcondición y la sustituimos por un aserto equivalente:

$$x = \lfloor \sqrt{A} \rfloor \quad \Leftrightarrow \quad x \leq \lfloor \sqrt{A} \rfloor < x+1 \quad \Leftrightarrow \quad x^2 \leq A < (x+1)^2$$

Por lo que tendríamos que verificar la siguiente especificación:

{ $n=A\geq 0 \wedge x=0$ }
mientras $(x+1)^2 \leq n$ **hacer**
  $x \leftarrow x+1$
fin_mientras
{ $x^2 \leq A < (x+1)^2$ }

Directamente nos encontramos con un bucle, por lo que tenemos que aplicar la regla de inferencia de la composición iterativa y debemos buscar el invariante.

Para encontrar un invariante que nos sirva para la demostración podemos hacer el seguimiento del algoritmo con uno o varios ejemplos con valores concretos, anotar el valor que toman las variables (estado de cómputo) antes de entrar en el bucle y al final de cada iteración, y buscar relaciones entre el valor de las variables.

Además de realizar el seguimiento de la ejecución del bucle, también podemos fijarnos en que a la salida del bucle se debe poder verificar la postcondición, formalmente: $I \wedge\neg B \Rightarrow Q$. En este caso concreto, se traduciría en que

$$I \wedge\neg((x+1)^2 \leq n) \quad \Rightarrow \quad x^2 \leq A < (x+1)^2$$
$$I \wedge (x+1)^2 > n \quad \Rightarrow \quad x^2 \leq A \wedge A < (x+1)^2$$

teniendo en cuenta que n=A, con $(x+1)^2 > n \Rightarrow A < (x+1)^2$, pero faltaría demostrar la primera parte de la postcondición ($x^2 \leq A$), que tendría que demostrarse a partir de lo que hubiese en el invariante.

En concreto, vamos a proponer el invariante $I \equiv x^2 \leq n \wedge n=A$, donde los dos primeros componentes hemos visto que serían útiles para demostrar $I \wedge\neg B \Rightarrow Q$.

Las condiciones de verificación generadas son:

a) $P\Rightarrow I$

$$n=A\geq 0 \wedge x=0 \Rightarrow x^2 \leq n \wedge n=A$$

$x=0 \Rightarrow x^2=0$, junto con $n \geq 0$ tenemos demostrado que $x^2 \leq n$
$n=A \Rightarrow n=A$

Por tanto, el predicado $n=A\geq 0 \wedge x=0 \Rightarrow x^2 \leq A \wedge n=A$ es cierto.

b) $I \wedge \neg B \Rightarrow Q$

$$x^2 \leq n \wedge n=A \wedge \neg((x+1)^2 \leq n) \Rightarrow x^2 \leq A < (x+1)^2$$

$x^2 \leq n \wedge \neg((x+1)^2 \leq n) \Leftrightarrow x^2 \leq n \wedge (x+1)^2 > n \Leftrightarrow x^2 \leq n < (x+1)^2$, junto con $n=A$, demostramos que se cumple $x^2 \leq A < (x+1)^2$ (equivalente a $x = \lfloor\sqrt{A}\rfloor$).

c) Y las generadas por $\{I \wedge B\}$ S $\{I\}$

$\{ x^2 \leq n \wedge n=A \wedge (x+1)^2 \leq n \}$
$x \leftarrow x+1$
$\{ x^2 \leq n \wedge n=A \}$

Tenemos que aplicar la **regla de inferencia de la asignación**, donde el papel de P y Q lo cumplirían respectivamente la precondición y postcondición, y tendríamos que demostrar $P \Rightarrow Q^x_{x+1}$, que en nuestro caso concreto sería

$$x^2 \leq n \wedge n=A \wedge (x+1)^2 \leq n \Rightarrow (x+1)^2 \leq n \wedge n=A$$

cuya demostración es trivial, ya que los dos términos del consecuente aparecen en el antecedente ($(x+1)^2 \leq n \Rightarrow (x+1)^2 \leq n$ y $n=A \Rightarrow n=A$.

Por lo tanto tendríamos que la especificación es parcialmente correcta, y para demostrar la corrección total faltaría:

d) $I\wedge B \Rightarrow t>0$
e) $\{ I\wedge B\wedge t=T\}S\{t<T\}$

Podemos fijar como función t asociada a cada iteración del bucle $t=n-x^2$

d) $I\wedge B \Rightarrow t>0$

$$x^2 \leq n \wedge n=A \wedge (x+1)^2 \leq n \Rightarrow t = n-x^2 > 0$$

$x<x+1 \Rightarrow x^2 < (x+1)^2$, y junto con $(x+1)^2 \leq n$, entonces $x^2 < n \Rightarrow t = n-x^2 > 0$

e) $\{ I\wedge B\wedge t=T\}S\{t<T\}$

$\{ x^2 \leq n \wedge n=A \wedge (x+1)^2 \leq n \wedge n-x^2 = T\}$
$x \leftarrow x+1$
$\{ n-x^2 < T \}$

Tenemos que aplicar la regla de inferencia de la asignación, donde el papel de P y Q lo cumplirían respectivamente la precondición y postcondición, y tendríamos que demostrar $P \Rightarrow Q^x_{x+1}$, que en nuestro caso concreto sería

$$x^2 \leq n \wedge n=A \wedge (x+1)^2 \leq n \wedge n-x^2 = T \Rightarrow n-(x+1)^2 < T$$

$x<x+1 \Rightarrow x^2 < (x+1)^2 \Rightarrow -x^2 > -(x+1)^2 \Rightarrow n-x^2 > n-(x+1)^2$, y junto con $n-x^2 = T$ tenemos la demostración de $n-(x+1)^2 < T$

Con lo que queda demostrado este apartado y se ha comprobado la corrección total del bucle.