Metodología de la Programación. El sistema de Floyd–Hoare

Curso 98–99

Ejercicio 1.–Justificar que la regla del WHILE no es "adecuada"para especificaciones de corrección **total** (es decir, dar ejemplo de una especificación de corrección total que semánticamente debe ser falsa y que, en cambio, la presunta regla probaría que es un teorema del sistema de Floyd–Hoare).

Ejercicio 2.–Supongamos que ampliamos nuestro lenguaje de programación con una nueva instrucción, **skip**, que *no produce efecto alguno*. Entonces consideramos un nuevo axioma en nuestro sistema: "$\{P\}$ **skip** $\{P\}$", y admitimos que la e.c.p.a. $\{P\}$ **skip** $\{Q\}$ genera la condición de verificación $P \to Q$. Probar que si son demostrables las condiciones de verificación generadas por la e.c.p.a. $\{P\}\ C\ ;\ \{R\}$ **skip** $\{Q\}$ (en donde C es un programa anotado propiamente que no contiene la instrucción **skip**), entonces se verifica que $\vdash \{P\}\ C\ ;$ **skip** $\{Q\}$.

Ejercicio 3.–Decidir razonadamente si las siguientes e.c.p. son válidas o no (todas las variables que aparecen son enteras). En caso afirmativo, demostrarlas.

1. $\{X = 1\}\ X \leftarrow X^2\ \{X = 1\}$
2. $\{X \neq 0\}$ **mientras** $X \neq 0$ **hacer** $X \leftarrow X + 1$ $\{X = 0\}$
3. $\{X = 1\}\ X \leftarrow XY\ \{X \neq 1 \vee Y = 1\}$
4. $\{X \geq 0 \wedge X = Y\}$ **mientras** $X \neq 0$ **hacer** $X \leftarrow X - 1$ $\{Y = 0\}$
5. $[X > Y]$ **mientras** $X > 0$ **hacer** $X \leftarrow X + 1$ $[X > Y]$
6. $\{X > Y\}$ **mientras** $X > 0$ **hacer** $X \leftarrow X + 1$ $\{X > Y\}$
7. $\{F \wedge X = 0\}\ X \leftarrow X + 2\ \{X = 1\}$
8. $\{X > 0 \wedge X = A \wedge Y = 0\}$

   mientras $X > Y$ **hacer** $X \leftarrow X - Y\ ;\ Y \leftarrow Y + 1$

   $\{X > 0 \wedge X = A - \frac{Y(Y+1)}{2}\}$
9. $\{X$ impar$\}$ **mientras** $X \neq 0$ **hacer** $X \leftarrow X^2$ $\{X$ impar$\}$
10. $\{Y = 1 \wedge N \geq 1\}$ **para** $X \leftarrow 1$ **hasta** N **hacer** $Y \leftarrow Y + 1$ $\{Y = N + 1\}$
11. $\{X > Y \wedge X < Y\}\ X \leftarrow X - Y\ \{X > 0\}$
12. $\{T\}$ **si** $X > 0$ **entonces** $X \leftarrow X - 1$ $\{T\}$
13. $[T]$ **mientras** $X = 0$ **hacer** $X \leftarrow 0$ $[X = 0]$
14. $\{F\}$ **mientras** F **hacer** $X \leftarrow 0$ $\{X = 0\}$
15. $\{X = 0\}$ **mientras** $X = 0$ **hacer** $Y \leftarrow Y + 1$ $\{X = 0\}$
16. $[T]$ **mientras** T **hacer** $X \leftarrow X + 1$ $[T]$
17. $\{X = a\}$ **si** $X > 0$ **entonces** $X \leftarrow X^2$ $\{a = 1 \to X = a\}$
18. $\{X = a\}$

    $Y \leftarrow 0\ ;$

    para $Z \leftarrow 1$ **hasta** X **hacer** $Y \leftarrow Y + 2$

    $\{Y = 2a\}$

Ejercicio 4.–Diseñar un programa tal que dados tres números enteros X, Y, Z, devuelva en Z el máximo de los tres números. Escribe una especificación de corrección parcial que exprese tal propiedad y demostrar la corrección del programa.

Ejercicio 5.–Diseñar un programa tal que dados tres números enteros X, Y, Z, devuelva en X la suma de los tres, en Y el producto y en Z la media aritmética. Escribe una especificación de corrección parcial que exprese tal propiedad y demostrar la corrección del programa.

Ejercicio 6.–Diseñar un programa tal que dados dos números enteros X, Y, devuelva en X la suma de los dos y en Y la diferencia. Escribe una especificación de corrección parcial que exprese tal propiedad y demostrar la corrección del programa.

Ejercicio 7.–Diseñar un programa tal que dados tres números enteros X, Y, Z, devuelva en Z el máximo de X e Y, y en Y el máximo de Z y X. Escribe una especificación de corrección parcial que exprese tal propiedad y demostrar la corrección del programa.

Ejercicio 8.–Probar:

$\vdash \{X = R + YQ\}\ Ppio.\ R \leftarrow R - Y; Q \leftarrow Q + 1.\ Fin\ \{X = R + YQ\}$

Ejercicio 9.–Probar:

$\vdash \{X = a + Y \wedge Y < Z\}$

$X \leftarrow X + 1\ ;\ Y \leftarrow Y + 1\ ;$

mientras $Y \neq Z$ **hacer**

$X \leftarrow X + 1\ ;\ Y \leftarrow Y + 1$

$\{X = a + Z\}$

Ejercicio 10.–Probar:

$\vdash \{Z = ab - XY\}$

mientras X sea par **hacer**

$Y \leftarrow 2Y; X \leftarrow \lfloor \frac{X}{2} \rfloor$

$\{Z = ab - XY \wedge X \text{ impar}\}$

Ejercicio 11.–Probar:

$\vdash \{X = a \wedge Y = b\}$

$Z \leftarrow 0\ ;$

mientras $X \neq 0$ **hacer**

mientras X sea par **hacer**

$Y \leftarrow 2Y\ ;\ X \leftarrow \lfloor \frac{X}{2} \rfloor$

$Z \leftarrow Z + Y\ ;\ X \leftarrow X - 1$

$\{Z = ab\}$

Ejercicio 12.–Probar:

$\vdash \{Z = (a - X) \cdot b\}$

$Ppio.\ Var\ R\ ;$

$R \leftarrow 0\ ;$

mientras $R \neq b$ **hacer**

$Z \leftarrow Z + 1\ ;\ R \leftarrow R + 1$

$X \leftarrow X - 1$

$Fin.$

$\{Z = (a - X) \cdot b\}$

Ejercicio 13.–Probar:

$\vdash \{X = a \wedge Y = b\}$

$Z \leftarrow 0$;

mientras $X \neq 0$ **hacer**

$Ppio.\ Var\ R$;

$R \leftarrow 0$;

mientras $R \neq Y$ **hacer** ;

$Z \leftarrow Z + 1$; $R \leftarrow R + 1$

$X \leftarrow X - 1$

$Fin.$

$\{Z = ab\}$

Ejercicio 14.–Probar:

$\vdash \{M \geq 1\}$

$X \leftarrow 0$;

para $N \leftarrow 1$ **hasta** M **hacer**

$X \leftarrow X + N$

$\{X = (M(M + 1))/2\}$

Ejercicio 15.–Se define la instrucción **repetir** como sigue:

Sintaxis: "**repetir** C **hasta que** S" (en donde C es un conjunto de instrucciones y S es una fórmula de primer orden)

Semántica: Se ejecuta C. A continuación se evalúa S, si es verdadera, entonces finaliza la ejecución de la instrucción, si es falsa se vuelve a ejecutar C reiterando el proceso.

Es decir, la instrucción "**repetir** C **hasta que** S"equivale a "C; **mientras** $\neg S$ **hacer** C".

Justificar que la regla de inferencia asociada a la instrucción **repetir**:

$$\frac{\vdash \{P\}C\{Q\} \ ; \ \vdash Q \wedge (\neg S) \rightarrow P}{\vdash \{P\} \ \textbf{repetir} \ C \ \textbf{hasta que} \ S \ \ \{Q \wedge S\}}$$

es consecuencia de las reglas de pre-condición fuerte, de composición y del bucle **while**.

Ejercicio 16.–Probar:

$\vdash \{Z = C + R \wedge R < Y\}$

repetir $Z \leftarrow Z + 1$; $R \leftarrow R + 1$ **hasta que** $R = Y$

$\{Z = C + Y\}$

Ejercicio 17.–Probar:

$\vdash \{X = a \wedge Y = b\}$

$Z \leftarrow 0$;

$\quad$ **repetir** $R \leftarrow 0$;

$\qquad$ **repetir** $Z \leftarrow Z + 1$; $R \leftarrow R + 1$ **hasta que** $R = Y$;

$\qquad X \leftarrow X - 1$

$\quad$ **hasta que** $X = 0$

$\{Z = ab\}$

Ejercicio 18.–En el sistema de verificación de Floyd–Hoare, hallar las condiciones de verificación generadas por la e.c.p.a.

$$\{P\} \textbf{ repetir } C \textbf{ hasta que } S \ \{Q\}$$

Ejercicio 19.–Utilizando condiciones de verificación probar que:

$\vdash \{Z = C + R \wedge R < Y\}$

$\quad$ **repetir** $Z \leftarrow Z + 1$; $R \leftarrow R + 1$ **hasta que** $R = Y$

$\{Z = C + Y\}$

y que

$\vdash \{X = a \wedge Y = b\}$

$\quad Z \leftarrow 0$;

$\quad$ **repetir** $R \leftarrow 0$;

$\qquad$ **repetir** $Z \leftarrow Z + 1$; $R \leftarrow R + 1$ **hasta que** $R = Y$;

$\qquad X \leftarrow X - 1$

$\quad$ **hasta que** $X = 0$

$\{Z = ab\}$

Ejercicio 20.–Dada la especificación de corrección parcial

$\vdash \{X = n\}$

$\quad Y \leftarrow 1$;

$\quad$ **mientras** $X \neq 0$ **hacer**

$\qquad Y \leftarrow Y \cdot X$; $X \leftarrow X - 1$

$\{X = 0 \wedge Y = n!\}$

se pide:

1. Anotarla adecuadamente.
2. Hallar las c.v. generadas por la e.c.p.a. obtenida en 1.
3. Probar que la e.c.p. de partida es un teorema del sistema de Floyd–Hoare.

Ejercicio 21.–Dada la especificación de corrección parcial

$\vdash \{T\}$

$\quad R \leftarrow X$; $Q \leftarrow 0$;

$\quad$ **mientras** $Y \leq R$ **hacer**

$\qquad R \leftarrow R - Y$; $Q \leftarrow Q + 1$

$\{X = R + YQ \wedge R < Y\}$

se pide:

1. Anotarla adecuadamente.
2. Hallar las c.v. generadas por la e.c.p.a. obtenida en 1.
3. Probar que la e.c.p. de partida es un teorema del sistema de Floyd–Hoare.

Ejercicio 22.–Utilizando condiciones de verificación probar que las siguientes e.c.p. son demostrables en el sistema de Floyd–Hoare.

$\vdash \{Z = ab - XY\}$

  mientras X sea par **hacer**

    $Y \leftarrow 2Y; X \leftarrow \lfloor \frac{X}{2} \rfloor$

 $\{Z = ab - XY \wedge X \text{ impar}\}$

y que

$\vdash \{X = a \wedge Y = b\}$

  $Z \leftarrow 0$;

  mientras $X \neq 0$ **hacer**

    mientras X sea par **hacer**

      $Z \leftarrow 2Y$; $X \leftarrow \lfloor \frac{X}{2} \rfloor$

    $Y \leftarrow Z + Y$; $X \leftarrow X - 1$

 $\{Z = ab\}$

Ejercicio 23.–Utilizando condiciones de verificación probar que la siguiente e.c.p. es demostrable en el sistema de Floyd–Hoare.

$\vdash \{X > 0 \wedge Y > 0\}$

  $Z \leftarrow 0$;

  para $j \leftarrow 1$ **hasta** X **hacer**

    para $k \leftarrow 1$ **hasta** Y **hacer**

      $Z \leftarrow Z + 1$

 $\{Z = XY\}$

Ejercicio 24.–Sean P una fómula de primer orden y C un programa tales que ninguna variable que aparece en P es asignada en C. Utilizando condiciones de verificación, probar por inducción sobre la complejidad del programa C que $\vdash \{P\}C\{P\}$.

Ejercicio 25.–Justificar razonadamente la veracidad o falsedad de las siguientes e.c.p.

(a) $\{F \wedge N > 0\}$

  $X \leftarrow 0$;

  para $k \leftarrow 0$ **hasta** N **hacer**

    $X \leftarrow X + k$

 $\{X = N^2 + N\}$

(b) $\{X > 0\}$

  mientras $X > 0$ **hacer**

    si X es par **entonces** $X \leftarrow \lfloor \frac{X}{2} \rfloor$

 $\{X = 0\}$