Tecnología de la Programación

Semántica Axiomática

David Cabrero Souto

Facultad de Informática
Universidade da Coruña

Curso 2007/2008

Semántica Axiomática

- Busca demostrar la corrección de un programa respecto a una especificación.
- Especificación = precondición y postcondición (Diseño por contrato)
- C.A.R. Hoare
  - Quicksort, Lógica de Hoare, Communicating Sequential Processes
- Lógica de Hoare
  - Paper “An axiomatic basis for computer programming”, 1969.
  - Reglas lógicas para razonar sobre la corrección de programas

Triple de Hoare

- $\{P\}\ S\ \{Q\}$
- El triple es válido si

  siempre que la ejecución del programa S comienza en un estado σ que satisface P, entonces termina en un estado σ' que satisface Q

- P Precondición, Q Postcondición
- Si el triple $\{P\}\ S\ \{Q\}$ es válido, entonces el programa S es correcto respecto a la especificación

Ejemplos

- Triples válidos

```
{ i = 0 }
    i := i + 1;
{ i = 1 }

{ i+j = 0 }
    i := i + 1;
    j := j -1 ;
{ i+j = 0}

{ true }
    i := 1;
{ i = 1}
```

- Triples no válidos

```
{ i = 1}
    i := i + 1;
{ i = 0}

{ i+j <> 0 }
    i := i +1;
    j := j -1;
{ i+j = 0 }

{ true }
    i := 1;
{ i = 0 }
```

Corrección parcial vs. total

- Corrección parcial
  Si termina, el programa es correcto respecto a la especificación
- Corrección total
  El programa termina y es correcto respecto a la especificación
- Ejemplo: $\{A\}\ c\ \{B\}$

  $c \equiv$ `while true do skip done`

  Es inmediato demostrar la corrección parcial, pero no es posible demostrar la corrección total
- La Lógica de Hoare (original) sólo prueba la corrección parcial

Reglas de Hoare para corrección parcial
Axiomas

- Skip

$$\frac{}{\{A\} \quad \texttt{skip;} \quad \{A\}}$$

- Asignación

$$\frac{}{\{A[a/X]\} \quad \texttt{X := a;} \quad \{A\}}$$

Ejemplo

- $\{P\}$ `i := 2*i;` $\{i < 10\}$
- Calcular la precondición
  1. Aplicamos el axioma de la asignación

     $$\{i < 10[2 * i/i]\} \texttt{ i := 2*i; } \{i < 10\}$$

  2. Simplificamos

     $$\{2 * i < 10\} \texttt{ i := 2*i; } \{i < 10\}$$

  3. Simplificamos

     $$\{i < 5\} \texttt{ i := 2*i; } \{i < 10\}$$

Reglas de Hoare para corrección parcial
Regla de secuencia

- Secuencia

$$\frac{\{A\}\ c_0;\ \{C\} \qquad \{C\}\ c_1\ \{B\}}{\{A\}\quad c_0; c_1\quad \{B\}}$$

Ejemplo (I)

- Swap de X e Y:

$\{X = n \wedge Y = m\}$
Z := X;
X := Y;
Y := Z;
$\{X = m \wedge Y = n\}$

- ¿ Es correcto ?

1. Axioma asignación

$\{X = n \wedge Y = m\}$
$Z := X;$
$\{Z = n \wedge Y = m\}$

2. Axioma asignación

$\{Z = n \wedge Y = m\}$
$X := Y;$
$\{Z = n \wedge X = m\}$

3. Regla de secuencia (1 y 2)

$\{X = n \wedge Y = m\}$
$Z := X;$
$X := Y;$
$\{Z = n \wedge X = m\}$

Ejemplo (II)

4. Axioma asignación

$$\{Z = n \wedge X = m\}$$
$$Y := Z;$$
$$\{Y = n \wedge X = m\}$$

5. Regla de secuencia (3 y 4)

$$\{X = n \wedge Y = m\}$$
$$Z := X;$$
$$X := Y;$$
$$Y := Z;$$
$$\{Y = n \wedge X = m\}$$

6. q.e.d.

Reglas de Hoare para corrección parcial
Regla del condicional

- Condicional

$$\frac{\{A \wedge b\}\ c_0;\ \{B\} \qquad \{A \wedge \neg b\}\ c_1\ \{B\}}{\{A\}\ \texttt{if}\ b\ \texttt{then}\ c_0\ \texttt{else}\ c_1\ \texttt{fi}\ \{B\}}$$

- La instrucción es no determinista ($b \vee \neg b$)
- Se verifican ambas alternativas

Ejemplo: if (I)

- Valor absoluto de X:

$\{true\}$
```
   if (X <= 0) then
      Y := -X;
   else
      Y := X;
   fi
```
$\{Y = |X|\}$

- ¿ Es correcto ?

$$\frac{\{true \wedge X \leq 0\}\ \texttt{Y := -X;}\ \{Y = |X|\} \quad \{true \wedge \neg X \leq 0\}\ \texttt{Y := X;}\ \{Y = |X|\}}{\{true\}\ \texttt{if (X <= 0) then ...fi}\ \{Y = |X|\}}$$

Notación alternativa

- Intercalar condiciones en el código.

$\{true\}$
if (X <= 0) then
$\{true \wedge X \leq 0\}$ `Y := -X;` $\{Y = |X|\}$
else
$\{true \wedge \neg X \leq 0\}$ `Y := X;` $\{Y = |X|\}$
fi
$\{Y = |X|\}$

Ejemplo: if (II)

- Primera premisa: $\{true \wedge X \leq 0\}\ \mathtt{Y := -X;}\ \{Y = |X|\}$
  1. Regla de asignación para $\{P\}\ \mathtt{Y := -X;}\ \{Y = |X|\}$:

     $\{-X = |X|\}\ \mathtt{Y := -X;}\ \{Y = |X|\}$

- Segunda premisa: $\{true \wedge \neg X \leq 0\}\ \mathtt{Y := -X;}\ \{Y = |X|\}$
  1. Regla de asignación para $\{P\}\ \mathtt{Y := -X;}\ \{Y = |X|\}$:

     $\{X = |X|\}\ \mathtt{Y := -X;}\ \{Y = |X|\}$

- Necesitamos una nueva regla para continuar.

Reglas de Hoare para corrección parcial
Regla de la implicación

- Implicación

$$\frac{\models (A \Rightarrow A') \qquad \{A'\}\ c\ \{B'\} \qquad \models (B' \Rightarrow B)}{\{A\}\quad c\quad \{B\}}$$

Ejemplo: if (III)

- Primera premisa
  2. Por la definición de valor absoluto:
     $$\{true \wedge X \leq 0\} \Rightarrow \{-X = |X|\}$$
  3. Regla de la implicación (1 y 2)
     $$\{true \wedge X \leq 0\}\ \texttt{Y := -X;}\ \{Y = |X|\}$$
- Segunda premisa
  2. Por la definición de valor absoluto:
     $$\{true \wedge \neg X \leq 0\} \Rightarrow \{X = |X|\}$$
  3. Regla de la implicación (1 y 2)
     $$\{true \wedge \neg X \leq 0\}\ \texttt{Y := X;}\ \{Y = |X|\}$$
- q.e.d.

Reglas de Hoare para corrección parcial
Regla del while

- While

$$\frac{\{A \wedge b\}\ c\ \{A\}}{\{A\}\ \texttt{while b do c done}\ \{A \wedge \neg b\}}$$

- A es la invariante del bucle

Ejemplo: while (I)

- Cálculo del factorial de n

$\{X = n \wedge n \geq 0 \wedge Y = 1\}$

while X>0 do

*Y := Y * X;*

X := X - 1;

done

$\{Y = n!\}$

- Invariante

$I \equiv Y * X! = n! \wedge X \geq 0$

- ¿ Es correcto ?

$$\frac{\{I \wedge X > 0\}\ c\ \{I\}}{\{I\}\ \texttt{while X>0 do c done}\ \{I \wedge \neg X > 0\}}$$

$c \equiv$ *Y := Y * X; X := X - 1;*

Ejemplo: while (II)

- La invariante es: $I \equiv Y * X! = n! \ \wedge \ X \geq 0$
- Comprobamos la premisa: $\{I \wedge X > 0\}\ c\ \{I\}$

1. Axioma de asignación

$$\{Y * (X-1)! = n! \wedge (X-1) \geq 0\}$$
$$X := X - 1;$$
$$\{I\} \equiv \{Y * X! = n! \ \wedge \ X \geq 0\}$$

2. Axioma de asignación

$$\{Y * X * (X-1)! = n! \wedge (X-1) \geq 0\}$$
$$Y := Y - X;$$
$$\{Y * (X-1)! = n! \wedge (X-1) \geq 0\}$$

3. Regla de la secuencia (1 y 2)

$$\{Y * X * (X-1)! = n! \wedge (X-1) \geq 0\}$$
$$Y := Y * X;$$
$$X := X - 1;$$
$$\{I\} \equiv \{Y * X! = n! \ \wedge \ X \geq 0\}$$

Ejemplo: while (III)

4. Por la definición de factorial

$$\{Y * X * (X-1)! = n! \wedge (X-1) \geq 0\} \equiv$$
$$\{Y * X! = n! \wedge (X-1) \geq 0\}$$

5. Y

$$\{Y * X! = n! \wedge (X-1) \geq 0\} \equiv \{Y * X! = n! \wedge X > 0\}$$
$$\{Y * X! = n! \wedge X > 0\} \Rightarrow \{I \wedge X > 0\}$$

6. Regla de la implicación (3 y 5)

$$\{I \wedge X > 0\}$$
*Y := Y * X;*
X := X - 1;
$$\{I\}$$

7. Regla del while (6)

$$\{I\}$$
while X>0 do c done
$$\{I \wedge \neg X > 0\} \quad \equiv \quad \{I \wedge X \leq 0\}$$

Ejemplo: while (IV)

8. Desarrollamos $\{I \wedge X \leq 0\}$

$$\begin{array}{ll} \{I \wedge X \leq 0\} & \equiv \\ \{Y * X! = n! \wedge X \geq 0 \wedge X \leq 0\} & \Rightarrow \\ \{Y * X! = n! \wedge X = 0\} & \Rightarrow \\ \{Y = n!\} & \end{array}$$

9. Trabajando sobre la precondición

$$Y = 1 \quad \Rightarrow \quad Y * X! = n!$$

y por tanto

$$\{X = n \wedge n \geq 0 \wedge Y = 1\} \quad \Rightarrow \quad \{Y * X! = n! \wedge n \geq 0\}$$

10. Regla de la implicación (7, 8 y 9)

$$\begin{array}{l} \{X = n \wedge n \geq 0 \wedge Y = 1\} \\ \quad \textit{while X>0 do c done} \\ \{Y = n! \end{array}$$