Corrección de la semántica asercional o axiomática

1 Corrección

Veamos primero un par de resultados técnicos.

Si $\mathcal{A}v[\![a]\!]I\sigma = m$, entonces

- $\mathcal{A}v[\![a_0[a/X]]\!]I\sigma = \mathcal{A}v[\![a_0]\!]I(\sigma[m/X])$

  Se prueba por inducción estructural en a_0 y el único caso interesante es cuando $a_0 \equiv X$.

  $$\mathcal{A}v[\![X[a/X]]\!]I\sigma = \mathcal{A}v[\![a]\!]I\sigma = m$$

  y por otro lado:

  $$\mathcal{A}v[\![X]\!]I(\sigma[m/X]) = (\sigma[m/X])(X) = m$$

- $$\sigma \models^I B[a/X] \text{ sí, y solo si } (\sigma[m/X]) \models^I B \tag{1}$$

  De nuevo se procede por inducción estructural en B. Si B no contiene X entonces el resultado es evidente. Veamos un par del resto de casos (los demás son análogos):

  Si $B \equiv a_0 = a_1$ entonces, por la construcción de la sustitución,

  $$(a_0 = a_1)[a/X] = ((a_0[a/X]) = (a_1[a/X]))$$

  y el hecho de que

  $$\sigma \models^I (a_0[a/X]) = (a_1[a/X])$$

  equivale, por definición de la semántica denotacional, a

  $$\mathcal{A}v[\![a_0[a/X]]\!]I\sigma = \mathcal{A}v[\![a_1[a/X]]\!]I\sigma$$

  lo cual, como acabamos de ver en el resultado anterior, es equivalente también a

  $$\mathcal{A}v[\![a_0]\!]I(\sigma[m/X]) = \mathcal{A}v[\![a_1]\!]I(\sigma[m/X])$$

  que es, de nuevo, claramente cierto por la semántica de $a_0 = a_1$.

  Como segundo caso consideremos $B \equiv A_1 \Rightarrow A_2$ y recordemos que $\sigma \models^I A_1 \Rightarrow A_2$ significa, por definición, que

  $$\sigma \not\models^I A_1 \text{ o } \sigma \models^I A_2$$

  .

En primer lugar, ¿Qué significa ahora $\sigma \models^I B[a/X]$? Por construcción será

$$\sigma \not\models^I A_1[a/X] \;\text{ o }\; \sigma \models^I A_2[a/X]$$

y, por hipótesis de inducción estructural, se tiene:

$$\sigma \models^I A_1[a/X] \;\text{ sí, y solo si }\; (\sigma[m/X]) \models^I A_1$$

(o lo que es equivalente $\sigma \not\models^I A_1[a/X]$ sí, y solo si $\sigma[m/X]) \not\models^I A_1$ y

$$\sigma \models^I A_2[a/X] \;\text{ sí, y solo si }\; (\sigma[m/X]) \models^I A_2$$

por lo tanto

$$\sigma \not\models^I A_1[a/X] \;\text{ o }\; \sigma \models^I A_2[a/X]$$

es equivalente a

$$(\sigma[m/X]) \not\models^I A_1 \;\text{ o }\; (\sigma[m/X]) \models^I A_2$$

lo cual, por definición, es lo mismo que

$$(\sigma[m/X]) \models^I A_1 \Rightarrow A_2$$

que es lo que queríamos probar.

2 Resultado principal de corrección

Sea $\{A\}\, c\, \{B\}$ una aserción de corrección parcial. Entonces: Si $\vdash \{A\}\, c\, \{B\}$, entonces $\models \{A\}\, c\, \{B\}$

Demostración:

Bastará probar que cada regla de Hoare es correcta en el sentido que si las premisas son válidas, entonces la conclusión también lo es.

2.1

La regla skip es evidentemente correcta.

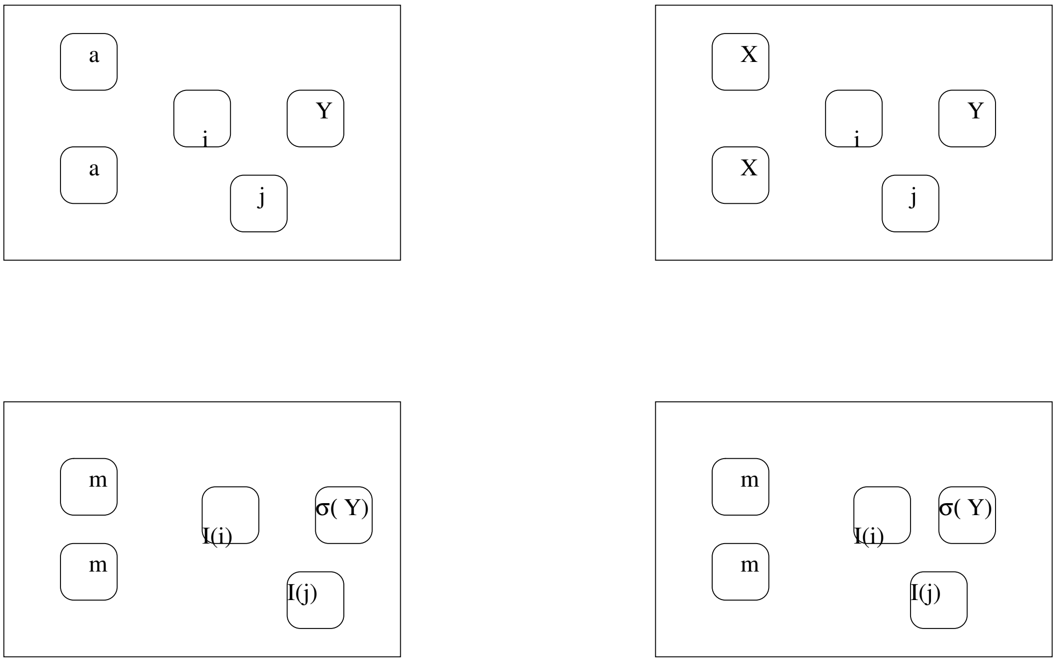

Figure 1: Arriba izquierda $B[a/X]$, derecha B. Abajo izquierda $\sigma \models^I B[a/X]$ y derecha $(\sigma[m/X]) \models^I B$

2.2

Si $c \equiv X := a$ habrá que probar que (dado que no hay premisas) $\models \{B[a/X]\}\, X := a\, \{B\}$ y para ello habrá que probar que dada cualquier interpretación I y cualquier estado σ, se tiene:

$$\sigma \models^I \{B[a/X]\}\, X := a\, \{B\}$$

que, por definición equivale a:

$$(\sigma \models^I B[a/X]) \Rightarrow ((\mathcal{C}[\![X := a]\!]\sigma) \models^I B)$$

pero sabemos que $\mathcal{C}[\![X := a]\!]\sigma = \sigma[m/X]$ (nótese que seguimos suponiendo que $\mathcal{A}v[\![a]\!]I\sigma = m$) de modo que lo que tenemos que probar es:

$$\sigma \models^I B[a/X]) \Rightarrow \sigma[m/X] \models^I B)$$

pero esto es precisamente el resultado anterior 1.

2.3

Para el caso de la concatenación, supongamos que

$$\models \{A\}\, c_0\, \{C\} \tag{2}$$

y que

$$\models \{C\}\, c_1\, \{B\}. \tag{3}$$

De aquí hemos de obtener que $\models \{A\}\, c_0; c_1\, \{B\}$. O sea que si $\sigma \models^I A$, entonces $\mathcal{C}[\![c_0; c_1]\!]\sigma \models^I B$. Pero, por definición, y llamando $\sigma' = \mathcal{C}[\![c_0]\!]\sigma$ y $\sigma'' = \mathcal{C}[\![c_1]\!]\sigma'$ tenemos que $\sigma' \models^I C$ por 2 y que $\sigma'' \models^I B$ por 3 .

2.4

Supongamos, para la regla del condicional, que

$$\models \{A \wedge b\}\, c_0\, \{B\} \tag{4}$$

y

$$\models \{A \wedge \neg b\}\, c_1\, \{B\} \tag{5}$$

Habrá que ver que:

$$\models \{A\}\, \texttt{if}\ b\ \texttt{then}\ c_0\ \texttt{else}\ c_1\, \{B\}$$

Para ello supongamos que para un estado σ y una interpretación I se tiene que $\sigma \models^I A$.

Si $\mathcal{C}[\![b]\!]\sigma = \texttt{true}$ (con lo cual tendremos ya que $\sigma \models^I A \wedge b$) y llamamos σ' a $\mathcal{C}[\![c_0]\!]\sigma$ sabemos, por semántica denotacional que

$$\mathcal{C}[\![\texttt{if}\ b\ \texttt{then}\ c_0\ \texttt{else}\ c_1]\!]\sigma = \sigma'$$

Pero por 4 se tiene $\sigma' \models^I B$.

Análogamente se prueba si $\mathcal{C}[\![b]\!]\sigma = \texttt{false}$ y los dos casos agotan todas las posibilidades.

Introduciremos ahora una notación que resulta cómoda.

$$\sigma^c = \mathcal{C}[\![c]\!]\sigma$$

(Nótese que, implicitamente, estamos suponiendo que la ejecución de c en el estado σ termina y lo hace en el estado σ^c.)

Entonces, debido a la semántica denotacional de la concatenación de programas es fácil ver que:

$$\mathcal{C}[\![c]\!](\sigma^{(c^n)}) = \sigma^{(c^{n+1})}$$

entendiendo que c^n representa la concatenación $\overbrace{c; c; \cdots; c}^{n}$.

2.5

Veamos ahora el caso del bucle while. Recordemos que la semántica de `while` b `do` c es justamente $\bigcup_{n\in\omega}\Gamma^n(\emptyset)$ que es el menor punto fijo de $\Gamma : (\Sigma \rightharpoonup \Sigma) \to (\Sigma \rightharpoonup \Sigma)$ definida por:

$$\Gamma(f)\sigma = \begin{cases} f(\sigma^c) & \text{si } \mathcal{B}[\![b]\!]\sigma = \texttt{true} \\ \sigma & \text{si } \mathcal{B}[\![b]\!]\sigma = \texttt{false} \end{cases}$$

Si llamamos

$$\Omega \equiv \mathcal{C}[\![\texttt{while}\ b\ \texttt{do}\ c]\!] :$$

$$\Omega(\sigma) = \Gamma(\Omega)(\sigma) = \begin{cases} \Omega(\sigma^c) & \text{si } \sigma \models b \\ \sigma & \text{si } \sigma \models \neg b \end{cases}$$

Si Ω está definida en σ y $\sigma \models b$ habrá un **primer** m tal que $\sigma^{(c^m)} \models \neg b$ y $m = n + 1$. Entonces

$$\Omega(\sigma) = \Omega(\sigma^c) = \Omega(\sigma^{(c^2)}) = \cdots = \Omega(\sigma^{(c^n)}) = \Omega(\sigma^{(c^m)}) = \sigma^{(c^m)}$$

Abreviemos también $D = \{\sigma \in \Sigma \mid \mathcal{B}[\![b]\!]\sigma = \texttt{false}\}$ De esta forma es fácil representar los dominios de las sucesivas potencias $\Gamma^n(\emptyset)$ que nos ayudará a comprender su significado:

$\Gamma^0(\emptyset) = \emptyset$	D_0
$\Gamma(\emptyset)(\sigma) = \begin{cases} \emptyset(\sigma^c) & \text{si } \sigma \models b \\ \sigma & \text{si } \sigma \models \neg b \end{cases}$	D_1
$\Gamma^2(\emptyset)(\sigma) = \begin{cases} \Gamma(\emptyset)(\sigma^c) & \text{si } \sigma \models b \\ \sigma & \text{si } \sigma \models \neg b \end{cases}$	$\begin{aligned} D_2 = D_1 \cup \{\sigma \in \Sigma \mid \sigma \models b \\ \&\ \ \sigma^c \models \neg b\} \end{aligned}$
$\Gamma^3(\emptyset)(\sigma) = \begin{cases} \Gamma^2(\emptyset)(\sigma^c) & \text{si } \sigma \models b \\ \sigma & \text{si } \sigma \models \neg b \end{cases}$	$\begin{aligned} D_3 = D_2 \cup \{\sigma \in \Sigma \mid \sigma \models b \\ \&\ \ \sigma^c \models b \\ \&\ \ \sigma^{(c^2)} \models \neg b\} \end{aligned}$
$\vdots$	$\vdots$
$\Gamma^{n+1}(\emptyset)(\sigma) = \begin{cases} \Gamma^n(\emptyset)(\sigma^c) & \text{si } \sigma \models b \\ \sigma & \text{si } \sigma \models \neg b \end{cases}$	$\begin{aligned} D_{n+1} = D_n \cup \{\sigma \in \Sigma \mid \sigma \models b \\ \&\ \ \sigma^c \models b \\ \&\ \ \sigma^{(c^2)} \models b \\ \vdots \\ \&\ \ \sigma^{(c^{n-1})} \models b \\ \&\ \ \sigma^{(c^n)} \models \neg b\} \end{aligned}$

Resumiendo,

$$\Gamma^{n+1}(\emptyset)(\sigma) = \sigma' \tag{6}$$

significa que si se ejecuta `while` b `do` c en el estado σ el programa termina en el estado σ' despues de, a lo sumo n ejecuciones del bucle c y además σ' no satisface el test b.

Después de estas consideraciones abordemos ya la veracidad de la regla de Hoare para el bucle while. Supongamos que

$$\models \{A \wedge b\}\, c\, \{A\}$$

Hemos de probar que

$$\models\ \{A\}\, \texttt{while}\ b\ \texttt{do}\ c\, \{A \wedge \neg b\}$$

Partamos pues de la hipótesis $\sigma \models^I A$ y supongamos que

$$\mathcal{C}[\![\texttt{while}\ b\ \texttt{do}\ c]\!]\sigma = \sigma'$$

Entonces, lo que hay que comprobar es que $\sigma' \models^I A \wedge \neg b$.

Sabemos, por semántica denotacional que

$$\sigma' = \left(\bigcup_{n \in \omega} \Gamma^n(\emptyset) \right) (\sigma) \tag{7}$$

o sea, que existe un **más pequeño** m para el cual:

$$\sigma' = (\Gamma^m(\emptyset))\,(\sigma)$$

Si $\sigma \models^I \neg b$, (o sea $\mathcal{B}[\![b]\!]\sigma = \texttt{false}$), entonces $\sigma' = \sigma$ y $\sigma \models^I A \wedge \neg b$ y habremos terminado.

Si, por el contrario, $\sigma \models^I b$, entonces estamos en la situación descrita en 6 y $m = n + 1$ para algún n, pero ahora además, por la hipótesis $\models \{A \wedge b\}\, c\, \{A\}$ se tiene que, como $\sigma \models^I A \wedge b$ entonces $\sigma^{(c^k)} \models^I A \;\; \forall k \leq n$ y tendremos que el estado resultante $\sigma^{(c^m)} = \mathcal{C}[\![c]\!](\sigma^{(n)})$ debe satisfacer A, es decir $\sigma' = \sigma^{(c^m)} \models^I A$ pero para este último $\sigma' = \sigma^{(c^m)} \models^I \neg b$ por lo tanto $\sigma' \models^I A \wedge \neg b$ como queríamos demostrar.