Tema 8. Semántica axiomática

Aserciones de corrección parcial

La semántica axiomática se basa en el uso de *aserciciones de corrección parcial* que podemos definir como tuplas con la siguiente estructura

$$\{P\}\, S\, \{Q\}$$

donde P y Q son dos predicados y S una sentencia. El significado de esta tupla es el siguiente: «Si la precondición P se cumple en el *estado inicial* y la sentencia S *acaba* partiendo de ese mismo estado, el *estado final* cumplirá la postcondición Q».

***Observación*:**
Si la sentencia S *no* acaba, no podemos afirmar nada sobre el estado final en relación con la postcondición. Esto es lo que llamamos *corrección parcial* pues no sabemos nada sobre su *terminación*.

Como lenguaje para expresar los predicados podemos seguir dos “filosofías”, la *intensional* o la *extensional*. En este caso, usaremos la extensional en la que los predicados pueden ser considerados como funciones del tipo $\mathbf{State} \to \mathbf{T}$. Por ejemplo, cualquier expresión booleana describe un predicado $\mathcal{B}[\![b]\!]$. Tendremos la siguiente notación:

$$\begin{aligned}
P_1 \wedge P_2 &\equiv P, \text{ donde } P\ s = (P_1\ s)\ \text{y}\ (P_2\ s) \\
P_1 \vee P_2 &\equiv P, \text{ donde } P\ s = (P_1\ s)\ \text{ó}\ (P_2\ s) \\
\neg P_1 &\equiv P, \text{ donde } P\ s = \neg\,(P_1\ s) \\
P_1\,[x \mapsto \mathcal{A}[\![a]\!]] &\equiv P, \text{ donde } P\ s = P_1\,(s\,[x \mapsto \mathcal{A}[\![a]\!]s]) \\
P_1 \Rightarrow P_2 &\equiv P_1\ s \Rightarrow P_2\ s,\ \forall s \in \mathbf{State}
\end{aligned}$$

Considero necesario dar una breve aclaración sobre el significado del predicado asignación. Simplemente, este predicado será *verdadero* si el predicado sobre el que se aplica es verdadero una vez que se realice la sustitución indicada en la asignación.

Sistema de inferencia

Para describir la semántica de **WHILE** de manera axiomática será necesario dar lo que conocemos como *sistema de inferencia* que, al igual que la semántica operacional, consiste en un conjunto de axiomas y reglas a través de las tuplas que hemos descrito antes. Para cada instrucción del lenguaje tenemos una regla y son las siguientes:

$$
\begin{aligned}
[\mathrm{ass_p}] &:= \{P\,[x \mapsto \mathcal{A}[\![a]\!]]\}\; x := a\; \{P\} \\
[\mathrm{skip_p}] &:= \{P\}\; \texttt{skip}\; \{P\} \\
[\mathrm{comp_p}] &:= \frac{\{P\}\; S_1\; \{Q\}\,,\ \{Q\}\; S_2\; \{R\}}{\{P\}\; S_1; S_2\; \{R\}} \\
[\mathrm{if_p}] &:= \frac{\{\mathcal{B}[\![b]\!] \wedge P\}\; S_1\; \{Q\}\,,\ \{\neg\mathcal{B}[\![b]\!] \wedge P\}\; S_2\; \{Q\}}{\{P\}\; \texttt{if}\; b\; \texttt{then}\; S_1\; \texttt{else}\; S_2\; \{Q\}} \\
[\mathrm{while_p}] &:= \frac{\{\mathcal{B}[\![b]\!] \wedge P\}\; S\; \{P\}}{\{P\}\; \texttt{while}\; b\; \texttt{do}\; S\; \{\neg\mathcal{B}[\![b]\!] \wedge P\}} \\
[\mathrm{cons_p}] &:= \frac{\{P'\}\; S\; \{Q'\}}{\{P\}\; S\; \{Q\}},\ \text{donde } P \Rightarrow P' \text{ y } Q' \Rightarrow Q.
\end{aligned}
$$

Daré un par de aclaraciones que considero convenientes:

- La asignación, a primera vista, parece estar al revés. Sin embargo, esto no es así ya que si recordamos la definición de la notación para $P\,[x \mapsto \mathcal{A}[\![a]\!]]$ tenemos que será cierto el predicado si lo es P tras realizar la sustitución. Por lo tanto, lo que nos dice la tupla de la asignación es que P se cumplirá si sigue siendo cierto al realizar la sustitución.

- La última regla nos permite *fortalecer* las precondiciones y *debilitar* las postcondiciones. Es decir, nos permite dar un caso más concreto que se sigue cumpliendo. De esta forma podemos, por ejemplo, encontrar un predicado que se cumpla para las dos postcondiciones de un `if`.

Notación: (Demostrabilidad de una tupla)
Cuando una tupla quede probada (al realizar todo su *árbol de inferencia*) lo denotaremos por:

$$\vdash_p \{P\}\; S\; \{Q\}$$

Equivalencia axiomática

Definición: (Equivalencia semántica)

Diremos que dos sentencias S_1 y S_2 son *equivalentes demostrablemente* si, $\forall P, Q$ precondiciones y postcondiciones tenemos que:

$$\vdash_p \{P\}\, S_1\, \{Q\} \Leftrightarrow \vdash_p \{P\}\, S_2\, \{Q\}$$

Corrección y completitud de la semántica axiomática

Definición: (Aserciones bajo semántica)
Una aserción de corrección parcial es válida bajo una semántica (por ejemplo, operacional de paso largo) si cumple que

$$\vDash_p \{P\}\, S\, \{Q\} \overset{\text{def}}{\Longleftrightarrow} \forall s \in \mathbf{State}\, [(P\ s = \mathbf{tt} \wedge \exists s' : \langle S, s\rangle \to s') \Rightarrow Q\ s' = \mathbf{tt}]$$

Es decir, que la postcondición se cumple para todos los estados en los que la precondición se cumple y la ejecución de S termina exitosamente.

Teorema:
Para toda aserción de corrección parcial $\{P\}\, S\, \{Q\}$ tenemos que

$$\vDash_p \{P\}\, S\, \{Q\} \Leftrightarrow \vdash_p \{P\}\, S\, \{Q\}\,.$$

O en tras palabras, la semántica axiomática es *completa* y *correcta*.