Semántica Axiomática

David de Frutos Escrig

versión original elaborada por

Yolanda Ortega Mallén

Dpto. de Sistemas Informáticos y Computación

Universidad Complutense de Madrid

Sumario

- Aserciones de corrección parcial.
- Semántica axiomática (con corrección parcial).
- Corrección de la semántica axiomática.
- Completitud de la semántica axiomática.

Bibliografía

- Hanne Riis Nielson & Flemming Nielson,
  Semantics with Applications. An Appetizer, Springer, 2007.
  Capítulo 9.

Aserciones de corrección parcial

$S \in \mathbf{Stm}$; predicados P y Q (sobre variables del lenguaje y variables *estáticas* adicionales):

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

Si la precondición P se satisface en el estado inicial,
y la ejecución de S partiendo del mismo termina, entonces
la postcondición Q se satisface en el estado final alcanzado.

No se impone la terminación de S; es más, cuando no se cumple,
¡se tiene por definición cualquier postcondición!

Ejemplo

$$\{\mathtt{x} = \mathtt{n}\}$$
$$\mathtt{y} := 1; \mathtt{while}\ \neg \mathtt{x} = 1\ \mathtt{do}\ (\mathtt{y} := \mathtt{x} \times \mathtt{y}; \mathtt{x} := \mathtt{x} - 1)$$
$$\{\mathtt{y} = \mathtt{n}! \ \wedge\ \mathtt{n} > 0\}$$

`n` es una variable estática que no puede aparecer en las instrucciones

Las variables estáticas sirven para relacionar en la postcondición los valores iniciales de las variables utilizadas en S, con sus valores finales.

Lenguaje de aserciones

Intensional Introducimos explícitamente un lenguaje preciso de aserciones para formular los predicados.
Lenguaje de aserciones suficientemente potente para poder expresar todas las condiciones que se necesitan en la práctica.

Extensional Admitimos como predicados cualesquiera funciones en $\mathbf{State} \longrightarrow \mathbf{T}$, denotandolas como mejor nos convenga.

Aproximación extensional - Notación habitual

Cada expresión booleana b define el predicado $\mathcal{B}[\![b]\!]$.
Nos permitiremos incluir variables estáticas en ellas, que técnicamente funcionan como constantes genéricas. Dados P, P_1, P_2 predicados:

$$
\begin{array}{lll}
P_1 \wedge P_2 & \text{viene dado por} & (P_1 \wedge P_2)\ s = (P_1\ s) \text{ y } (P_2\ s) \\
P_1 \vee P_2 & \text{viene dado por} & (P_1 \vee P_2)\ s = (P_1\ s) \text{ o } (P_2\ s) \\
\neg P & \text{viene dado por} & (\neg P)\ s = \neg (P\ s) \\
P[x \mapsto \mathcal{A}[\![a]\!]] & \text{viene dado por} & (P[x \mapsto \mathcal{A}[\![a]\!]])\ s = P\ (s[x \mapsto \mathcal{A}[\![a]\!]s])
\end{array}
$$

$P_1 \Rightarrow P_2$ es abreviatura para $\forall s \in State\ P_1\ s \Longrightarrow P_2\ s$

Sistema de inferencia

Semántica axiomática para **While** (reglas de Hoare)

$$[\text{ass}_p] \quad \{P[x \mapsto \mathcal{A}[\![a]\!]]\}\ x := a\ \{P\}$$

$$[\text{skip}_p] \quad \{P\}\ \texttt{skip}\ \{P\}$$

$$[\text{comp}_p] \quad \frac{\{P\}\ S_1\ \{Q\},\ \{Q\}\ S_2\ \{R\}}{\{P\}\ S_1\ ;\ S_2\ \{R\}}$$

$$[\text{if}_p] \quad \frac{\{\mathcal{B}[\![b]\!] \wedge P\}\ S_1\ \{Q\},\ \{\neg\mathcal{B}[\![b]\!] \wedge P\}\ S_2\ \{Q\}}{\{P\}\ \texttt{if}\ b\ \texttt{then}\ S_1\ \texttt{else}\ S_2\ \{Q\}}$$

$$[\text{while}_p] \quad \frac{\{\mathcal{B}[\![b]\!] \wedge P\}\ S\ \{P\}}{\{P\}\ \texttt{while}\ b\ \texttt{do}\ S\ \{\neg\mathcal{B}[\![b]\!] \wedge P\}}$$

$$[\text{cons}_p] \quad \frac{\{P'\}\ S\ \{Q'\}}{\{P\}\ S\ \{Q\}}\ \text{si}\ P \Rightarrow P' \wedge\ Q' \Rightarrow Q$$

Invariante se satisface antes y después de cada ejecución del cuerpo del bucle.
Árbol de inferencia demostración de la propiedad expresada en la raíz:

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

Ejercicio 9.10

Expresar una propiedad de corrección parcial para el programa

$$\texttt{z} := 0\,;\,\texttt{while y} \leq \texttt{x do } (\texttt{z} := \texttt{z} + 1\,;\,\texttt{x} := \texttt{x} - \texttt{y})$$

que exprese que el mismo calcula la división entera y el resto de $\texttt{x}$ entre $\texttt{y}$.

Construir el árbol de inferencia que demuestre tal propiedad.

Ejercicio: 9.11

Proponer una regla de inferencia para $\texttt{repeat}\ S\ \texttt{until}\ b$.

Ejercicio 9.15

Demostrar que $\vdash_p \{P\}\ S\ \{\texttt{true}\}$, para cualquier sentencia S
y cualquier predicado P.

Equivalencia demostrable

Equivalencia bajo la semántica axiomática

S_1 y S_2 son demostrablemente equivalentes (equivalentes bajo la semántica axiomática) cuando

$$\vdash_p \{P\}\ S_1\ \{Q\} \iff \vdash_p \{P\}\ S_2\ \{Q\}$$

Ejercicio 9.13

- Demostrar que S ; `skip` y S son demostrablemente equivalentes.
- Demostrar que S_1 ; $(S_2$; $S_3)$ y $(S_1$; $S_2)$; S_3 son demostrablemente equivalentes.

Ejercicio 9.14

Demostrar que `repeat` S `until` b es demostrablemente equivalente a S ; `while` $\neg b$ `do` S .

Corrección y completitud

Corrección y completitud de un sistema de inferencia

Bajo una determinada semántica de referencia, un sistema de inferencia de la corrección parcial es:

correcto si las aserciones de corrección parcial que son demostrables con el sistema se satisfacen bajo la semántica.

completo si toda aserción de corrección parcial que se satisface bajo la semántica se puede demostrar utilizando el sistema.

Aserciones de corrección parcial válidas bajo la semántica operacional

$$\models_p \{P\}\ S\ \{Q\} \stackrel{\text{def}}{=} \forall s \in \mathit{State}\ [(P\ s = \mathbf{tt} \wedge \exists s'\ \langle S, s\rangle \to s') \implies Q\ s' = \mathbf{tt}\,]$$

Teorema 9.16

Para toda aserción de corrección parcial $\{P\}\ S\ \{Q\}$:

$$\models_p \{P\}\ S\ \{Q\} \iff \vdash_p \{P\}\ S\ \{Q\}$$

Corrección

Demostracción de la corrección del sistema de inferencia - Lema 9.17

$$\vdash_p \{P\}\ S\ \{Q\} \implies \models_p \{P\}\ S\ \{Q\}$$

Por inducción respecto de las reglas de inferencia del mismo.

Ejercicio 9.18

Extender la demostración del Lema 9.17 incluyendo la regla correspondiente a `repeat` S `until` b.

Ejercicio 9.19

Considerar la definición alternativa de validez siguiente:

$$\models' \{P\}\ S\ \{Q\} \stackrel{\text{def}}{=} \forall s \in \mathit{State}\,[\,P\ s = \mathbf{tt} \implies \exists s'\,(\langle S, s\rangle \to s' \wedge Q\ s' = \mathbf{tt})\,]$$

Demostrar que $\vdash_p \{P\}\ S\ \{Q\} \not\Longleftrightarrow \models' \{P\}\ S\ \{Q\}$.

Completitud

Precondición posible más débil

$$\text{wlp}(S, Q) \iff (\langle S, s\rangle \to s' \implies Q\ s')$$

lo mínimo exigible al estado inicial, para que si S termina, lo haga cumpliendose Q.

Lema 35: Equivalentemente, la podemos describir mediante:

- $\models_p \{\text{wlp}(S, Q)\}\ S\ \{Q\}$
- $\models_p \{P\}\ S\ \{Q\} \implies (P \Rightarrow \text{wlp}(S, Q))$

Postcondición más fuerte - Ejercicio 9.22

Describe lo que cumplen los estados alcanzables desde P:

$$\text{sp}(P, S)\ s' \iff \exists s \in \textbf{State}(\langle S, s\rangle \to s' \wedge P\ s)$$

Demostrar que para toda sentencia S y todo predicado P :

- $\models_p \{P\}\ S\ \{\text{sp}(P, S)\}$
- $\models_p \{P\}\ S\ \{Q\} \implies (\text{sp}(P, S) \Rightarrow Q)$

Completitud

Demostracción de la completitud del sistema de inferencia - Lema 9.23

$$\vdash_p \{\mathrm{wlp}(S, Q)\}\ S\ \{Q\}$$

$$\models_p \{P\}\ S\ \{Q\} \Longrightarrow \vdash_p \{P\}\ S\ \{Q\}$$

Ejercicio 9.24

Extender la demostración anterior para incluir la instrucción `repeat` S `until` b.

Ejercicio 9.25

Demostrar la completitud del sistema de inferencia utilizando las postcondiciones más fuertes.

Ejercicios 9.26 + 9.27

Definir una noción de validez basada en la semántica denotacional.

Demostrar la corrección y completitud del sistema de inferencia respecto de ella.

Lenguaje para la descripción de pre/post-condiciones

Por ejemplo, tomemos como $\mathcal{L}$: el lenguaje que define las expresiones booleanas de **While**. Tendremos entonces:

- corrección: caso particular de lo probado con la aproximación extensional.
- completitud: no va a ser posible representar todos los predicados $\mathrm{wlp}(S, Q)$ como fórmulas de $\mathcal{L}$.

Sea S un programa universal, que tendrá problema de parada indecidible.
Si existiera una fórmula b_S de $\mathcal{L}$ que cumpliese:

$$\mathcal{B}[\![b_S]\!]\ s \iff \neg(\mathrm{wlp}(S, \texttt{false})\ s)$$

entonces, $\neg b_S$ sería también una fórmula de $\mathcal{L}$, que cumpliría:

$$\mathcal{B}[\![b_S]\!]\ s \iff \text{el cómputo de } S \text{ a partir de } s \text{ cicla}$$

$$\mathcal{B}[\![\neg b_S]\!]\ s = \mathbf{tt} \iff \text{el cómputo de } S \text{ a partir de } s \text{ termina}$$

Contradicción!!!

Extender $\mathcal{L}$ con cuantificadores: expresividad y completitud relativa (Cook)