Exemplo

Exercício 15.1. *Mostra que*

$\{x \geq 0\} z := x; y := 0,$ `while` $\neg z = 0$ `do` $(y := y + 1; z := z - 1)\{x = y\}.$

$\diamond$

Integridade e Completude

Para o sistema dedutivo de Hoare, vamos considerar duas propriedades usuais em sistemas lógicos:

- **Integridade:** Cada regra deve preservar validade. O que implica (por indução nas derivações) que os teoremas obtidos correspondem a asserções válidas de correcção parcial.

$$\vdash_p \{\phi\} C \{\psi\} \qquad \Rightarrow \qquad \models_p \{\phi\} C \{\psi\}.$$

- **Completude:** Gostaríamos que o sistema fosse suficientemente forte para inferir todas as asserções de correção parcial válidas.

$$\models_p \{\phi\} C \{\psi\} \qquad \Rightarrow \qquad \vdash_p \{\phi\} C \{\psi\}.$$

Vamos começar por formalizar a noção de execução/avaliação.

Estado de execução

Para a avaliação duma expressão é necessário saber o valor das variáveis.

Um **estado** s é uma função que associa a cada variável um valor.

Representamos o conjunto de estados por

$$\mathbf{State} = \mathbf{Var} \longrightarrow \mathbb{Z}$$

e $s \in \mathbf{State}$ tal que $s : \mathbf{Var} \longrightarrow \mathbb{Z}$.

Seja $s\ x$ ou $s(x)$ o valor da variável x no estado s. Se $v \in \mathbb{Z}$,

$$s[v/x](y) = \begin{cases} s(y) & \text{se } y \neq x \\ v & \text{se } y = x \end{cases}$$

Semântica das expressões

Aexp - Expressões aritméticas

$\mathcal{A} : \mathbf{Aexp} \longrightarrow (\mathbf{State} \longrightarrow Z)$

$$
\begin{aligned}
\mathcal{A}[\![n]\!]s &= n \\
\mathcal{A}[\![x]\!]s &= s(x) \\
\mathcal{A}[\![E_1 + E_2]\!]s &= \mathcal{A}[\![E_1]\!]s + \mathcal{A}[\![E_2]\!]s \\
\mathcal{A}[\![E_1 - E_2]\!]s &= \mathcal{A}[\![E_1]\!]s - \mathcal{A}[\![E_2]\!]s \\
\mathcal{A}[\![E_1 \times E_2]\!]s &= \mathcal{A}[\![E_1]\!]s.\mathcal{A}[\![E_2]\!]s
\end{aligned}
$$

Semântica das expressões

Bexp - Expressões booleanas

$\mathbf{T} = \{\mathbf{V}, \mathrm{F}\}$

$\mathcal{B} : \mathbf{Bexp} \longrightarrow (\mathbf{State} \longrightarrow \mathbf{T})$

$$
\begin{aligned}
\mathcal{B}[\![\texttt{true}]\!]s &= \mathbf{V} \\
\mathcal{B}[\![\texttt{false}]\!]s &= \mathrm{F} \\
\mathcal{B}[\![E_1 = E_2]\!]s &= \begin{cases} \mathbf{V} & \text{se } \mathcal{A}[\![E_1]\!]s = \mathcal{A}[\![E_2]\!]s \\ \mathrm{F} & \text{se } \mathcal{A}[\![E_1]\!]s \neq \mathcal{A}[\![E_2]\!]s \end{cases} \\
\mathcal{B}[\![E_1 \leq E_2]\!]s &= \begin{cases} \mathbf{V} & \text{se } \mathcal{A}[\![E_1]\!]s \leq \mathcal{A}[\![E_2]\!]s \\ \mathrm{F} & \text{se } \mathcal{A}[\![E_1]\!]s > \mathcal{A}[\![E_2]\!]s \end{cases} \\
\mathcal{B}[\![\neg b]\!]s &= \begin{cases} \mathbf{V} & \text{se } \mathcal{B}[\![b]\!]s = \mathrm{F} \\ \mathrm{F} & \text{se } \mathcal{B}[\![b]\!]s = \mathbf{V} \end{cases} \\
\mathcal{B}[\![b_1 \ \wedge \ b_2]\!]s &= \begin{cases} \mathbf{V} & \text{se } \mathcal{B}[\![b_1]\!]s = \mathbf{V} \text{ e } \mathcal{B}[\![b_2]\!]s = \mathbf{V} \\ \mathrm{F} & \text{se } \mathcal{B}[\![b_1]\!]s = \mathrm{F} \text{ ou } \mathcal{B}[\![b_2]\!]s = \mathrm{F} \end{cases}
\end{aligned}
$$

Semântica operacional natural (*big-step*)

Descreve a execução completa de cada comando.

Configurações: $\langle C, s\rangle$ ou s, onde C é um comando e s um estado $\Gamma = (\mathbf{Com} \times \mathbf{State}) \cup \mathbf{State}$

Configurações Finais: $s \in State$

Transições: $\langle C, s\rangle \ \rightarrow \ s'$

Regras:

$$\frac{\langle C_1, s_1\rangle \ \rightarrow \ s'_1 \ ... \ \langle C_n, s_n\rangle \ \rightarrow \ s'_n}{\langle C, s\rangle \ \rightarrow \ s'}$$

Hipóteses: $\langle C_i, s_i\rangle \;\to\; s'_i$

Conclusão: $\langle C, s\rangle \;\to\; s'$

Se $n = 0$ diz-se um **Axioma**.

Semântica operacional natural (*big-step*)

Semântica operacional para comandos do While

$$\texttt{att}_{sn} \qquad \langle x := E, s\rangle \;\to\; s[\mathcal{A}[\![E]\!]s/x]$$

$$\texttt{comp}_{sn} \qquad \frac{\langle C_1, s\rangle \;\to\; s' \;,\; \langle C_2, s'\rangle \;\to\; s''}{\langle C_1; C_2, s\rangle \;\to\; s''}$$

$$\texttt{if}^{v}{}_{sn} \qquad \frac{\langle C_1, s\rangle \;\to\; s'}{\langle \texttt{if } B \texttt{ then } C_1 \texttt{ else } C_2, s\rangle \;\to\; s'} \text{ se } \mathcal{B}[\![B]\!]s = \mathbf{V}$$

$$\texttt{if}^{f}{}_{sn} \qquad \frac{\langle C_2, s\rangle \;\to\; s'}{\langle \texttt{if } B \texttt{ then } C_1 \texttt{ else } C_2, s\rangle \;\to\; s'} \text{ se } \mathcal{B}[\![B]\!]s = \mathrm{F}$$

$$\texttt{while}^{v}{}_{sn} \qquad \frac{\langle C, s\rangle \;\to\; s',\; \langle \texttt{while } B \texttt{ do } C, s'\rangle \;\to\; s''}{\langle \texttt{while } B \texttt{ do } C, s\rangle \;\to\; s''} \text{ se } \mathcal{B}[\![B]\!]s = \mathbf{V}$$

$$\texttt{while}^{f}{}_{sn} \qquad \langle \texttt{while } B \texttt{ do } C, s\rangle \;\to\; s \text{ se } \mathcal{B}[\![B]\!]s = \mathrm{F}$$

Exemplos

Sendo $s_0 = [x = 5, y = 7]$ determinar o estado após a execução de:

$$(z := x; x := y); y := z.$$

Para tal constrói-se uma **Árvore de derivação** com esse comando como raiz:

$$\frac{\dfrac{\langle z{:=}x, s_0\rangle \;\to\; s_1 \quad \langle x{:=}y, s_1\rangle \;\to\; s_2}{\langle z{:=}x; x{:=}y, s_0\rangle \;\to\; s_2} \quad \langle y := z, s_2\rangle \;\to\; s_3}{\langle (z := x; x := y); y := z, s_0\rangle \;\to\; s_3}$$

onde,

$$\begin{aligned} s_1 &= s_0[5/z] \\ s_2 &= s_1[7/x] \\ s_3 &= s_2[5/y] \end{aligned}$$

Integridade da semântica axiomática

Teorema 15.1 (Integridade)**.** *Para todas as asserções de correcção parcial* $\{\phi\}C\{\psi\}$*,*

$$\vdash_p \{\phi\}C\{\psi\} \textit{ implica } \models_p \{\phi\}C\{\psi\}$$

A demonstração é por indução na árvore de inferência de $\vdash_p \{\phi\}C\{\psi\}$:

- Mostrar que a propriedade se verifica para as árvores simples, i.e os **axiomas** do sistema de inferência.
- Mostrar que a propriedade se verifica para as Árvores de inferência compostas: para cada regra, supor que a propriedade se verifica para as premissas (e as condições se verificam) e mostrar que a propriedade também se verifica para a conclusão da regra.

Integridade da semântica axiomática

Caso ass_p**.** Suponhamos que $\vdash_p \{\phi[E/x]\}x := E\{\phi\}$.

Seja

$$\langle x := E, s\rangle \quad \rightarrow \quad s'$$

e $s \models \phi[E/x]$ se e só se $s[\mathcal{A}[\![E]\!]s/x] \models \phi$. (Exercício)

Temos que provar que $s' \models \phi$.

Por $[ass_{sn}]$ temos que $s' = s[\mathcal{A}[\![E]\!]s/x]$, e portanto

$$s' \models \phi \text{ sse } s[\mathcal{A}[\![E]\!]s/x] \models \phi$$

Integridade da semântica axiomática

Caso $comp_p$**.** Por hip. de indução $\models_p \{\phi\}C_1\{\eta\}$ e $\models_p \{\eta\}C_2\{\psi\}$.

Queremos mostrar que $\models_p \{\phi\}C_1; C_2\{\psi\}$. Sejam s e s'' estados, tal que $s \models \phi$ e $\langle C_1; C_2, s\rangle \quad \rightarrow \quad s''$. Pela regra $[comp_{sn}]$ existe s' tal que

$$\langle C_1, s\rangle \quad \rightarrow \quad s' \text{ e } \langle C_2, s'\rangle \quad \rightarrow \quad s''$$

De $\langle C_1, s\rangle \quad \rightarrow \quad s'$, $s \models \phi$ e $\models_p \{\phi\}C_1\{\eta\}$, temos que $s' \models \eta$. De $\langle C_2, s'\rangle \quad \rightarrow \quad s''$, $s' \models \eta$ e $\models_p \{\eta\}C_2\{\psi\}$, temos que $s'' \models \psi$. Que é o que queríamos.

Integridade da semântica axiomática

Caso if_p**.** Por hip. de indução $\models_p \{B \wedge \phi\}C_1\{\psi\}$ e $\models_p \{\neg B \wedge \phi\}C_2\{\psi\}$.

Para provar que

$$\models_p \{\phi\}\ \texttt{if}\ B\ \texttt{then}\ C_1\ \texttt{else}\ C_2\ \{\psi\}$$

sejam s e s' estados tais que $s \models \phi$ e $\langle \texttt{if}\ B\ \texttt{then}\ C_1\ \texttt{else}\ C_2, s\rangle \quad \rightarrow \quad s'$.

Se $\mathcal{B}[\![B]\!]s = \mathbf{V}$ então por $[if_{sn}]$, temos que $\langle C_1, s\rangle \quad \rightarrow \quad s'$. Então dado que $\models_p \{B \wedge \phi\}C_1\{\psi\}$, concluímos que $s' \models \psi$.

Analogamente se conclui, caso $\mathcal{B}[\![B]\!]s = \mathrm{F}$.

Integridade da semântica axiomática

Caso $while_p$**.** Por hip. de indução

$$\models_p \{B \ \wedge \ \phi\}C\{\phi\}. \tag{1}$$

Para provar que

$$\models_p \{\phi\}\,\texttt{while}\,B\,\texttt{do}\,C\,\{\neg B \ \wedge \ \phi\},$$

sejam s e s'' estados tais que $s \models \phi$ e

$$\langle \texttt{while}\,B\,\texttt{do}\,C, s\rangle \ \rightarrow \ s''.$$

Temos que mostrar que $s'' \models \neg B \ \wedge \ \phi$. Usamos indução na árvore de derivação da semântica natural.

Integridade da semântica axiomática

Caso $while_p$**.** Há dois casos a considerar, consoante $[while_{sn}]$.

Se $\mathcal{B}[\![B]\!]s = \text{F}$ então $s'' = s$ e $s'' \models (\neg B \ \wedge \ \phi)$.

Senão, $\mathcal{B}[\![b]\!]s = \mathbf{V}$ e existe s' tal que $\langle C, s\rangle \ \rightarrow \ s'$ e $\langle \texttt{while}\,B\,\texttt{do}\,C, s'\rangle \ \rightarrow \ s''$.

Temos que $s \models (B \ \wedge \ \phi)$ e pela hipótese (1) temos que $s' \models \phi$. Aplicando a hipótese de indução a $\langle \texttt{while}\,B\,\texttt{do}\,C, s'\rangle \ \rightarrow \ s''$, temos que $s'' \models (\neg B \ \wedge \ \phi)$, como queríamos.

Integridade da semântica axiomática

Caso $cons_p$**.** Por hip. de indução

$$\models_p \{\phi'\}C\{\psi'\}, \ \phi \rightarrow \phi', \ \text{e} \ \psi' \rightarrow \psi. \tag{2}$$

Para provar que $\models_p \{\phi\}C\{\psi\}$, sejam s e s' tal que $s \models \phi$ e $\langle C, s\rangle \ \rightarrow \ s'$.

Como $s \models \phi$ e $\phi \rightarrow \phi'$ então $s \models \phi'$ e pela hipótese (2), $s' \models \psi'$. Mas como $\psi' \rightarrow \psi$, temos que $s' \models \psi$, como queríamos.

Completude da semântica axiomática

Teorema 15.2 (Incompletude de Gödel (1931))**.** *Não existe um sistema de demonstração para* ***PA*** *(aritmética), de tal forma que os teoremas coincidam com as asserções válidas de* ***PA****.*

Teorema 15.3 (Completude)**.** *Para todas as asserções de correcção parcial* $\{\phi\}C\{\psi\}$*,*

$$\models_p \{\phi\}C\{\psi\} \ \textit{implica} \ \vdash_p \{\phi\}C\{\psi\}$$

Note-se que $\models \psi$, se e só se $\models \{\texttt{true}\}\texttt{skip}\{\psi\}$. O que significa que a completude de $\vdash_p$ contraria o teorema de incompletude de Gödel.

Completude da semântica axiomática

Proposição 15.1. *Não existe um sistema de demonstração para asserções de correcção parcial, de tal forma que os teoremas coincidam com as asserções de correcção parcial válidas.*

Prova: Note-se que

$$\models \{\texttt{true}\}C\{\texttt{false}\}$$

se e só se o comando C diverge em todos os estados.

Um sistema de demonstração para asserções de correcção parcial, poderia ser usado para confirmar que o comando diverge em todos os estados. O que é impossível (*Halting Problem*).

Completude relativa

Teorema 15.4. *O sistema de prova para correcção parcial é relativamente completo, i.e. para qualquer asserção de correcção parcial* $\{\phi\}C\{\psi\}$*:*

$$\vdash_p \{\phi\}C\{\psi\} \text{ se } \models_p \{\phi\}C\{\psi\}$$

O resultado de correcção parcial relativa foi estabelecido por S. Cook (1978).

O facto de $\vdash_p \{\phi\}C\{\psi\}$ ser uma prova depende do facto de certas asserções em **PA** serem válidas.

Para a demonstração de completude relativa ver Capítulo 7 [Winskel].