

Korrekte Software: Grundlagen und Methoden
Vorlesung 4 vom 24.04.18: Äquivalenz der Operationalen und
Denotationalen Semantik

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2018

Fahrplan

- ▶ Einführung
- ▶ Operationale Semantik
- ▶ Denotationale Semantik
- ▶ Äquivalenz der Operationalen und Denotationalen Semantik
- ▶ Die Floyd-Hoare-Logik
- ▶ Invarianten und die Korrektheit des Floyd-Hoare-Kalküls
- ▶ Strukturierte Datentypen
- ▶ Modellierung und Spezifikation
- ▶ Verifikationsbedingungen
- ▶ Vorwärts mit Floyd und Hoare
- ▶ Funktionen und Prozeduren
- ▶ Referenzen
- ▶ Ausblick und Rückblick

Operationale vs. denotationale Semantik

Operational $\langle a, \sigma \rangle \rightarrow_{Aexp} n$

Denotational $\mathcal{A}[[a]]$

$$m \in \mathbf{Z} \quad \langle m, \sigma \rangle \rightarrow_{Aexp} m$$

$$\{(\sigma, m) \mid \sigma \in \Sigma\}$$

$$x \in \mathbf{Loc} \quad \frac{x \in Dom(\sigma)}{\langle x, \sigma \rangle \rightarrow_{Aexp} \sigma(x)}$$

$$\{(\sigma, \sigma(x)) \mid \sigma \in \Sigma, x \in Dom(\sigma)\}$$

$$a_1 \circ a_2 \quad \frac{\begin{array}{l} \langle a_1, \sigma \rangle \rightarrow_{Aexp} n \\ \langle a_2, \sigma \rangle \rightarrow_{Aexp} m \\ n, m \neq \perp \end{array}}{\langle a_1 \circ a_2, \sigma \rangle \rightarrow_{Aexp} n \circ^I m}$$

$$\{(\sigma, n \circ^I m) \mid \sigma \in \Sigma, (\sigma, n) \in \mathcal{A}[[a_1]], (\sigma, m) \in \mathcal{A}[[a_2]]\}$$

$$\frac{\begin{array}{l} \langle a_1, \sigma \rangle \rightarrow_{Aexp} n \\ \langle a_2, \sigma \rangle \rightarrow_{Aexp} m \\ n = \perp \text{ oder } m = \perp \end{array}}{\langle a_1 \circ a_2, \sigma \rangle \rightarrow_{Aexp} \perp}$$

$\circ \in \{+, *, -\}$

Operationale vs. denotationale Semantik

Operational $\langle a, \sigma \rangle \rightarrow_{Aexp} n$

$$a_1/a_2 \quad \frac{\begin{array}{l} \langle a_1, \sigma \rangle \rightarrow_{Aexp} n \\ \langle a_2, \sigma \rangle \rightarrow_{Aexp} m \\ m \neq 0 \quad m, n \neq \perp \end{array}}{\langle a_1 \circ a_2, \sigma \rangle \rightarrow_{Aexp} n \circ^I m}$$

$$\frac{\begin{array}{l} \langle a_1, \sigma \rangle \rightarrow_{Aexp} n \\ \langle a_2, \sigma \rangle \rightarrow_{Aexp} m \\ n = \perp, m = \perp \text{ oder } m = 0 \end{array}}{\langle a_1/a_2, \sigma \rangle \rightarrow_{Aexp} \perp}$$

Denotational $\mathcal{A}[[a]]$

$$\{(\sigma, n/m) \mid \sigma \in \Sigma, (\sigma, n) \in \mathcal{A}[[a_1]], (\sigma, m) \in \mathcal{A}[[a_2]], m \neq 0\}$$

Äquivalenz operationale und denotationale Semantik

- Für alle $a \in \mathbf{Aexp}$, für alle $n \in \mathbf{Z}$, für alle Zustände σ :

$$\langle a, \sigma \rangle \rightarrow_{Aexp} n \Leftrightarrow (\sigma, n) \in \mathcal{A}[[a]]$$

$$\langle a, \sigma \rangle \rightarrow_{Aexp} \perp \Leftrightarrow \sigma \notin Dom(\mathcal{A}[[a]])$$

- Beweis Prinzip?

Äquivalenz operationale und denotationale Semantik

- Für alle $a \in \mathbf{Aexp}$, für alle $n \in \mathbf{Z}$, für alle Zustände σ :

$$\langle a, \sigma \rangle \rightarrow_{Aexp} n \Leftrightarrow (\sigma, n) \in \mathcal{A}[[a]]$$

$$\langle a, \sigma \rangle \rightarrow_{Aexp} \perp \Leftrightarrow \sigma \notin Dom(\mathcal{A}[[a]])$$

- Beweis per struktureller Induktion über a . (Warum?)

Operationale vs. denotationale Semantik

Operational $\langle b, \sigma \rangle \rightarrow_{Bexp} 0|1$

$$1 \quad \langle 1, \sigma \rangle \rightarrow_{Bexp} 1$$

$$0 \quad \langle 0, \sigma \rangle \rightarrow_{Bexp} 0$$

Denotational $\mathcal{B}[[b]]$

$$\{(\sigma, 1) \mid \sigma \in \Sigma\}$$

$$\{(\sigma, 0) \mid \sigma \in \Sigma\}$$

Operationale vs. denotationale Semantik

Operat. $\langle b, \sigma \rangle \rightarrow_{Bexp} 0 \mid 1$

$$\begin{array}{c}
 \langle a_0, \sigma \rangle \rightarrow_{Aexp} n \\
 \langle a_1, \sigma \rangle \rightarrow_{Aexp} m \\
 \hline
 n, m \neq \perp \quad n = m \\
 \hline
 \langle a_0 == a_1, \sigma \rangle \rightarrow_{Bexp} 1 \\
 \\
 \langle a_0, \sigma \rangle \rightarrow_{Aexp} n \\
 \langle a_1, \sigma \rangle \rightarrow_{Aexp} m \\
 \hline
 n, m \neq \perp \quad n \neq m \\
 \hline
 \langle a_0 == a_1, \sigma \rangle \rightarrow_{Bexp} 0 \\
 \\
 \langle a_0, \sigma \rangle \rightarrow_{Aexp} n \\
 \langle a_1, \sigma \rangle \rightarrow_{Aexp} m \\
 n = \perp \text{ oder } m = \perp \\
 \hline
 \langle a_0 == a_1, \sigma \rangle \rightarrow_{Bexp} \perp
 \end{array}$$

$a_1 \leq a_2$

Denotational $\mathcal{B}[[b]]$

$$\begin{aligned}
 &\{(\sigma, 1) \mid \sigma \in \Sigma, \\
 &\quad (\sigma, n_0) \in \mathcal{A}[[a_0]], \\
 &\quad (\sigma, n_1) \in \mathcal{A}[[a_1]], \\
 &\quad n_0 = n_1 \}
 \end{aligned}$$

$\cup$

$$\begin{aligned}
 &\{(\sigma, 0) \mid \sigma \in \Sigma, \\
 &\quad (\sigma, n_0) \in \mathcal{A}[[a_0]], \\
 &\quad (\sigma, n_1) \in \mathcal{A}[[a_1]], \\
 &\quad n_0 \neq n_1 \}
 \end{aligned}$$

analog

Operationale vs. denotationale Semantik

Operational $\langle a, \sigma \rangle \rightarrow_{Bexp} b$

$$\begin{array}{l} b_1 \&\& b_0 \\ \frac{\langle b_1, \sigma \rangle \rightarrow_{Bexp} 0}{\langle b_1 \&\& b_2, \sigma \rangle \rightarrow 0} \\ \frac{\langle b_1, \sigma \rangle \rightarrow_{Bexp} 1}{\langle b_1 \&\& b_2, \sigma \rangle \rightarrow b} \\ \frac{\langle b_2, \sigma \rangle \rightarrow_{Bexp} b}{\langle b_1 \&\& b_2, \sigma \rangle \rightarrow b} \\ \frac{\langle b_1, \sigma \rangle \rightarrow_{Bexp} \perp}{\langle b_1 \&\& b_2, \sigma \rangle \rightarrow \perp} \end{array}$$

$b_1 || b_2$

$!n$

...

Denotational $\mathcal{B}[[b]]$

$$\{(\sigma, 0) \mid (\sigma, 0) \in \mathcal{B}[[b_1]]\}$$

$$\{(\sigma, b) \mid (\sigma, 1) \in \mathcal{B}[[b_1]], (\sigma, b) \in \mathcal{B}[[b_2]]\}$$

analog

Äquivalenz operationale und denotationale Semantik

- Für alle $b \in \mathbf{Bexp}$, für alle $t \in \mathbf{B}$, for alle Zustände σ :

$$\langle b, \sigma \rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma, t) \in \mathcal{B}[[b]]$$

$$\langle b, \sigma \rangle \rightarrow_{Bexp} \perp \Leftrightarrow \sigma \notin Dom(\mathcal{B}[[b]])$$

- Beweis Prinzip?

Äquivalenz operationale und denotationale Semantik

- Für alle $b \in \mathbf{Bexp}$, für alle $t \in \mathbf{B}$, for alle Zustände σ :

$$\langle b, \sigma \rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma, t) \in \mathcal{B}[[b]]$$

$$\langle b, \sigma \rangle \rightarrow_{Bexp} \perp \Leftrightarrow \sigma \notin Dom(\mathcal{B}[[b]])$$

- Beweis per struktureller Induktion über b (unter Verwendung der Äquivalenz für AExp). (Warum?)

Operationale vs. denotationale Semantik

Operational

$$\{\} \quad \frac{\langle c, \sigma \rangle \rightarrow_{Stmt} \sigma' \mid \perp}{\langle \{\}, \sigma \rangle \rightarrow_{Stmt} \sigma}$$

$$c_1; c_2 \quad \frac{\frac{\langle c_1, \sigma \rangle \rightarrow_{Stmt} \sigma' \neq \perp \quad \langle c_2, \sigma' \rangle \rightarrow_{Stmt} \sigma''}{\langle c_1; c_2, \sigma \rangle \rightarrow_{Stmt} \sigma''} \quad \frac{\langle c_1, \sigma \rangle \rightarrow_{Stmt} \perp}{\langle c_1; c_2, \sigma \rangle \rightarrow_{Stmt} \perp}$$

$$x = a \quad \frac{\frac{\langle a, \sigma \rangle \rightarrow_{Aexp} n}{\langle x = a, \sigma \rangle \rightarrow_{Stmt} \sigma[n/x]} \quad \frac{\langle a, \sigma \rangle \rightarrow_{Aexp} \perp}{\langle x = a, \sigma \rangle \rightarrow_{Stmt} \perp}$$

Denotational $\mathcal{C}[[c]]$

$$\mathcal{C}[[\{\}]] = Id$$

$$\mathcal{C}[[c_2]] \circ \mathcal{C}[[c_1]]$$

$$\{(\sigma, \sigma[n/x]) \mid (\sigma, n) \in \mathcal{A}[[a]]\}$$

Operationale vs. denotationale Semantik

Operational

$$\langle c, \sigma \rangle \rightarrow_{Stmt} \sigma' \mid \perp$$

if (b) c_0

$$\frac{\begin{array}{l} \langle b, \sigma \rangle \rightarrow_{Bexp} 1 \\ \langle c_0, \sigma \rangle \rightarrow_{Stmt} \sigma' \end{array}}{\langle c, \sigma \rangle \rightarrow_{Stmt} \sigma'}$$

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} \perp}{\langle c, \sigma \rangle \rightarrow_{Stmt} \perp}$$

$$\langle c, \sigma \rangle \rightarrow_{Stmt} \perp$$

$$\langle b, \sigma \rangle \rightarrow_{Bexp} 0$$

$$\frac{\langle c_1, \sigma \rangle \rightarrow_{Stmt} \sigma'}{\langle c, \sigma \rangle \rightarrow_{Stmt} \sigma'}$$

else c_1

$$\langle c, \sigma \rangle \rightarrow_{Stmt} \sigma'$$

Denotational $\mathcal{C}[[c]]$

$$\{(\sigma, \sigma') \mid (\sigma, 1) \in \mathcal{B}[[b]], (\sigma, \sigma') \in \mathcal{C}[[c_0]]\}$$

$$\{(\sigma, \sigma') \mid (\sigma, 0) \in \mathcal{B}[[b]], (\sigma, \sigma') \in \mathcal{C}[[c_1]]\}$$

Operationale vs. denotationale Semantik

Operational

$$\langle c, \sigma \rangle \rightarrow_{Stmnt} \sigma' \mid \perp$$

Denotational $\mathcal{C}[[c]]$

$$\underbrace{\text{while } (b) \text{ c}}_w \quad \frac{\langle b, \sigma \rangle \rightarrow_{Bexp} 0 \quad \langle b, \sigma \rangle \rightarrow_{Bexp} \perp}{\langle w, \sigma \rangle \rightarrow_{Stmnt} \sigma \quad \langle w, \sigma \rangle \rightarrow_{Stmnt} \perp} \quad fix(\Gamma)$$

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} 1 \quad \langle c, \sigma \rangle \rightarrow_{Stmnt} \sigma' \neq \perp \quad \langle w, \sigma' \rangle \rightarrow_{Stmnt} \sigma''}{\langle w, \sigma \rangle \rightarrow_{Stmnt} \sigma''}$$

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} 1 \quad \langle c, \sigma \rangle \rightarrow_{Stmnt} \perp}{\langle w, \sigma \rangle \rightarrow_{Stmnt} \perp}$$

mit

$$\begin{aligned} \Gamma(\varphi) = & \{(\sigma, \sigma') \mid (\sigma, 1) \in \mathcal{B}[[b]], (\sigma, \sigma') \in \varphi \circ \mathcal{C}[[c]]\} \\ & \cup \{(\sigma, \sigma) \mid (\sigma, 0) \in \mathcal{B}[[b]]\} \end{aligned}$$

Äquivalenz operationale und denotationale Semantik

- Für alle $c \in \mathbf{Stmt}$, für alle Zustände σ, σ' :

$$\langle c, \sigma \rangle \rightarrow_{\mathbf{Stmt}} \sigma' \Leftrightarrow (\sigma, \sigma') \in \mathcal{C}[\![c]\!]$$

$$\langle c, \sigma \rangle \rightarrow_{\mathbf{Stmt}} \perp \Rightarrow \sigma \notin \text{Dom}(\mathcal{C}[\![c]\!])$$

- $\Rightarrow$ Beweis Prinzip?

- $\Leftarrow$ Beweis Prinzip?

Äquivalenz operationale und denotationale Semantik

- Für alle $c \in \mathbf{Stmt}$, für alle Zustände σ, σ' :

$$\langle c, \sigma \rangle \rightarrow_{\mathbf{Stmt}} \sigma' \Leftrightarrow (\sigma, \sigma') \in \mathcal{C}[\![c]\!]$$

$$\langle c, \sigma \rangle \rightarrow_{\mathbf{Stmt}} \perp \Rightarrow \sigma \notin \text{Dom}(\mathcal{C}[\![c]\!])$$

- $\Rightarrow$ Beweis per Induktion über die Ableitung in der operationalen Semantik (Warum?)
- $\Leftarrow$ Beweis Prinzip?

Äquivalenz operationale und denotationale Semantik

- Für alle $c \in \mathbf{Stmt}$, für alle Zustände σ, σ' :

$$\langle c, \sigma \rangle \rightarrow_{\mathbf{Stmt}} \sigma' \Leftrightarrow (\sigma, \sigma') \in \mathcal{C}[\![c]\!]$$

$$\langle c, \sigma \rangle \rightarrow_{\mathbf{Stmt}} \perp \Rightarrow \sigma \notin \text{Dom}(\mathcal{C}[\![c]\!])$$

- $\Rightarrow$ Beweis per Induktion über die Ableitung in der operationalen Semantik (Warum?)
- $\Leftarrow$ Beweis per struktureller Induktion über c (Verwendung der Äquivalenz für arithmetische und boolsche Ausdrücke). Für die While-Schleife Rückgriff auf Definition des Fixpunkts und Induktion über die Teilmengen $\Gamma^i(\emptyset)$ des Fixpunkts. (Warum?)

Äquivalenz operationale und denotationale Semantik

- Für alle $c \in \mathbf{Stmt}$, für alle Zustände σ, σ' :

$$\langle c, \sigma \rangle \rightarrow_{\mathbf{Stmt}} \sigma' \Leftrightarrow (\sigma, \sigma') \in \mathcal{C}[\![c]\!]$$

$$\langle c, \sigma \rangle \rightarrow_{\mathbf{Stmt}} \perp \Rightarrow \sigma \notin \text{Dom}(\mathcal{C}[\![c]\!])$$

- $\Rightarrow$ Beweis per Induktion über die Ableitung in der operationalen Semantik (Warum?)
- $\Leftarrow$ Beweis per struktureller Induktion über c (Verwendung der Äquivalenz für arithmetische und boolsche Ausdrücke). Für die While-Schleife Rückgriff auf Definition des Fixpunkts und Induktion über die Teilmengen $\Gamma^i(\emptyset)$ des Fixpunkts. (Warum?)
- Gegenbeispiel für $\Leftarrow$ in der zweiten Aussage: wähle $c \equiv \text{while}(1)\{\}$: $\mathcal{C}[\![c]\!] = \emptyset$ aber $\langle c, \sigma \rangle \rightarrow_{\mathbf{Stmt}} \perp$ gilt nicht (sondern?).

Fahrplan

- ▶ Einführung
- ▶ Operationale Semantik
- ▶ Denotationale Semantik
- ▶ Äquivalenz der Operationalen und Denotationalen Semantik
- ▶ Die Floyd-Hoare-Logik
- ▶ Invarianten und die Korrektheit des Floyd-Hoare-Kalküls
- ▶ Strukturierte Datentypen
- ▶ Modellierung und Spezifikation
- ▶ Verifikationsbedingungen
- ▶ Vorwärts mit Floyd und Hoare
- ▶ Funktionen und Prozeduren
- ▶ Referenzen
- ▶ Ausblick und Rückblick