

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

Serge Autexier, Christoph L  th

Universit  t Bremen

Sommersemester 2018

11.50.49 2018-06-05

1 [14]



Fahrplan

- Einf  hrung
- Operationale Semantik
- Denotationale Semantik
- **  quivalenz der Operationalen und Denotationalen Semantik**
- Die Floyd-Hoare-Logik
- Invarianten und die Korrektheit des Floyd-Hoare-Kalk  ls
- Strukturierte Datentypen
- Modellierung und Spezifikation
- Verifikationsbedingungen
- Vorw  rts mit Floyd und Hoare
- Funktionen und Prozeduren
- Referenzen
- Ausblick und R  ckblick

Korrekte Software

2 [14]



Operationale vs. denotationale Semantik

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

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

$m \in \mathbf{Z}$	$\langle m, \sigma \rangle \rightarrow_{Aexp} m$	$\{(\sigma, m) \mid \sigma \in \Sigma\}$
$x \in \mathbf{Loc}$	$\frac{x \in \text{Dom}(\sigma)}{\langle x, \sigma \rangle \rightarrow_{Aexp} \sigma(x)}$	$\{(\sigma, \sigma(x)) \mid \sigma \in \Sigma, x \in \text{Dom}(\sigma)\}$
$a_1 \circ a_2$	$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n \quad \langle a_2, \sigma \rangle \rightarrow_{Aexp} m \quad n, m \neq \perp}{\langle a_1 \circ a_2, \sigma \rangle \rightarrow_{Aexp} n \circ^I m}$	$\{(\sigma, n \circ^I m) \mid \sigma \in \Sigma, (\sigma, n) \in \mathcal{A}[[a_1]], (\sigma, m) \in \mathcal{A}[[a_2]]\}$
	$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n \quad \langle a_2, \sigma \rangle \rightarrow_{Aexp} m \quad n = \perp \text{ oder } m = \perp}{\langle a_1 \circ a_2, \sigma \rangle \rightarrow_{Aexp} \perp}$	$\circ \in \{+, *, -\}$

Korrekte Software

3 [14]



Operationale vs. denotationale Semantik

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

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

a_1 / a_2	$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n \quad \langle a_2, \sigma \rangle \rightarrow_{Aexp} m \quad m \neq 0 \quad m, n \neq \perp}{\langle a_1 \circ a_2, \sigma \rangle \rightarrow_{Aexp} n \circ^I m}$	$\{(\sigma, n/m) \mid \sigma \in \Sigma, (\sigma, n) \in \mathcal{A}[[a_1]], (\sigma, m) \in \mathcal{A}[[a_2]], m \neq 0\}$
	$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n \quad \langle a_2, \sigma \rangle \rightarrow_{Aexp} m \quad n = \perp, m = \perp \text{ oder } m = 0}{\langle a_1 / a_2, \sigma \rangle \rightarrow_{Aexp} \perp}$	

Korrekte Software

4 [14]



  quivalenz operationale und denotationale Semantik

- F  r alle $a \in \mathbf{Aexp}$, f  r alle $n \in \mathbf{Z}$, f  r alle Zust  nde σ :

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

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

- Beweis Prinzip? per struktureller Induktion   ber a . (Warum?)

Korrekte Software

5 [14]



Operationale vs. denotationale Semantik

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

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

1	$\langle 1, \sigma \rangle \rightarrow_{Bexp} 1$	$\{(\sigma, 1) \mid \sigma \in \Sigma\}$
0	$\langle 0, \sigma \rangle \rightarrow_{Bexp} 0$	$\{(\sigma, 0) \mid \sigma \in \Sigma\}$

Korrekte Software

6 [14]



Operationale vs. denotationale Semantik

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

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

$a_0 == a_1$	$\frac{\langle a_0, \sigma \rangle \rightarrow_{Aexp} n \quad \langle a_1, \sigma \rangle \rightarrow_{Aexp} m \quad n, m \neq \perp \quad n = m}{\langle a_0 == a_1, \sigma \rangle \rightarrow_{Bexp} 1}$	$\{(\sigma, 1) \mid \sigma \in \Sigma, (\sigma, n_0) \in \mathcal{A}[[a_0]], (\sigma, n_1) \in \mathcal{A}[[a_1]], n_0 = n_1\}$
	$\frac{\langle a_0, \sigma \rangle \rightarrow_{Aexp} n \quad \langle a_1, \sigma \rangle \rightarrow_{Aexp} m \quad n, m \neq \perp \quad n \neq m}{\langle a_0 == a_1, \sigma \rangle \rightarrow_{Bexp} 0}$	$\cup$
	$\frac{\langle a_0, \sigma \rangle \rightarrow_{Aexp} n \quad \langle a_1, \sigma \rangle \rightarrow_{Aexp} m \quad n = \perp \text{ oder } m = \perp}{\langle a_0 == a_1, \sigma \rangle \rightarrow_{Bexp} \perp}$	$\{(\sigma, 0) \mid \sigma \in \Sigma, (\sigma, n_0) \in \mathcal{A}[[a_0]], (\sigma, n_1) \in \mathcal{A}[[a_1]], n_0 \neq n_1\}$
$a_1 \leq a_2$	analog	

Korrekte Software

7 [14]



Operationale vs. denotationale Semantik

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

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

$b_1 \&\& b_2$	$\frac{\langle b_1, \sigma \rangle \rightarrow_{Bexp} 0 \quad \langle b_1 \&\& b_2, \sigma \rangle \rightarrow 0 \quad \langle b_1, \sigma \rangle \rightarrow_{Bexp} 1 \quad \langle b_2, \sigma \rangle \rightarrow_{Bexp} b}{\langle b_1 \&\& b_2, \sigma \rangle \rightarrow b}$	$\{(\sigma, 0) \mid (\sigma, 0) \in \mathcal{B}[[b_1]]\}$
	$\frac{\langle b_1, \sigma \rangle \rightarrow_{Bexp} \perp}{\langle b_1 \&\& b_2, \sigma \rangle \rightarrow \perp}$	$\{(\sigma, b) \mid (\sigma, 1) \in \mathcal{B}[[b_1]], (\sigma, b) \in \mathcal{B}[[b_2]]\}$
$b_1 b_2$	analog	
$!n$	...	

Korrekte Software

8 [14]



Äquivalenz operationale und denotationale Semantik

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

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

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

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



Operationale vs. denotationale Semantik

	Operational	Denotational $\mathcal{C}[c]$
$\{\}$	$\frac{\langle c, \sigma \rangle \rightarrow_{Stmnt} \sigma' \mid \perp}{\langle \{\}, \sigma \rangle \rightarrow_{Stmnt} \sigma}$	$\mathcal{C}[\{\}] = Id$
$c_1; c_2$	$\frac{\frac{\langle c_1, \sigma \rangle \rightarrow_{Stmnt} \sigma' \neq \perp \quad \langle c_2, \sigma' \rangle \rightarrow_{Stmnt} \sigma''}{\langle c_1; c_2, \sigma \rangle \rightarrow_{Stmnt} \sigma''} \quad \frac{\langle c_1, \sigma \rangle \rightarrow_{Stmnt} \perp}{\langle c_1; c_2, \sigma \rangle \rightarrow_{Stmnt} \perp}$	$\mathcal{C}[c_2] \circ \mathcal{C}[c_1]$
$x = a$	$\frac{\frac{\langle a, \sigma \rangle \rightarrow_{Aexp} n \quad \langle x = a, \sigma \rangle \rightarrow_{Stmnt} \sigma[n/x]}{\langle a, \sigma \rangle \rightarrow_{Aexp} \perp} \quad \frac{\langle a, \sigma \rangle \rightarrow_{Aexp} \perp}{\langle x = a, \sigma \rangle \rightarrow_{Stmnt} \perp}$	$\{(\sigma, \sigma[n/x]) \mid (\sigma, n) \in \mathcal{A}[a]\}$



Operationale vs. denotationale Semantik

	Operational	Denotational $\mathcal{C}[c]$
if $(b) \ c_0$	$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} 1 \quad \frac{\langle c_0, \sigma \rangle \rightarrow_{Stmnt} \sigma'}{\langle c, \sigma \rangle \rightarrow_{Stmnt} \sigma'} \quad \frac{\langle b, \sigma \rangle \rightarrow_{Bexp} \perp \quad \langle c, \sigma \rangle \rightarrow_{Stmnt} \perp}{\langle c, \sigma \rangle \rightarrow_{Stmnt} \perp}}{\langle c, \sigma \rangle \rightarrow_{Stmnt} \sigma'}$	$\{(\sigma, \sigma') \mid (\sigma, 1) \in \mathcal{B}[b], (\sigma, \sigma') \in \mathcal{C}[c_0]\}$
else c_1	$\frac{\langle c_1, \sigma \rangle \rightarrow_{Stmnt} \sigma' \quad \frac{\langle b, \sigma \rangle \rightarrow_{Bexp} 0 \quad \langle c, \sigma \rangle \rightarrow_{Stmnt} \perp}{\langle c, \sigma \rangle \rightarrow_{Stmnt} \perp}}{\langle c, \sigma \rangle \rightarrow_{Stmnt} \sigma'}$	$\{(\sigma, \sigma') \mid (\sigma, 0) \in \mathcal{B}[b], (\sigma, \sigma') \in \mathcal{C}[c_1]\}$



Operationale vs. denotationale Semantik

	Operational	Denotational $\mathcal{C}[c]$
while $(b) \ c$	$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} 0 \quad \frac{\langle w, \sigma \rangle \rightarrow_{Stmnt} \sigma \quad \langle b, \sigma \rangle \rightarrow_{Bexp} 1 \quad \langle c, \sigma \rangle \rightarrow_{Stmnt} \sigma' \neq \perp \quad \langle w, \sigma' \rangle \rightarrow_{Stmnt} \sigma''}{\langle w, \sigma \rangle \rightarrow_{Stmnt} \sigma''}}{\langle w, \sigma \rangle \rightarrow_{Stmnt} \perp}$	$fix(\Gamma)$
mit	$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} 1 \quad \langle c, \sigma \rangle \rightarrow_{Stmnt} \perp}{\langle w, \sigma \rangle \rightarrow_{Stmnt} \perp}$	
		$\Gamma(\varphi) = \{(\sigma, \sigma') \mid (\sigma, 1) \in \mathcal{B}[b], (\sigma, \sigma') \in \varphi \circ \mathcal{C}[c]\} \cup \{(\sigma, \sigma) \mid (\sigma, 0) \in \mathcal{B}[b]\}$



Äquivalenz operationale und denotationale Semantik

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

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

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

- $\Rightarrow$ Beweis Prinzip? per Induktion über die Ableitung in der operationalen Semantik (Warum?)
- $\Leftarrow$ Beweis Prinzip? 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 $\Gamma'(\emptyset)$ des Fixpunkts. (Warum?)
- Gegenbeispiel für $\Leftarrow$ in der zweiten Aussage: wähle $c \equiv \text{while}(1)\{\}$: $\mathcal{C}[c] = \emptyset$ aber $\langle c, \sigma \rangle \rightarrow_{Stmnt} \perp$ 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

