Korrekte Software: Grundlagen und Methoden
Vorlesung 5 vom 04.05.17: Äquivalenz der Operationalen und Denotationalen Semantik

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2017

Fahrplan

- Einführung
- Die Floyd-Hoare-Logik
- Operationale Semantik
- Denotationale Semantik
- Äquivalenz der Operationalen und Denotationalen Semantik
- Korrektheit des Hoare-Kalküls
- Vorwärts und Rückwärts mit Floyd und Hoare
- Funktionen und Prozeduren
- Referenzen und Speichermodelle
- Verifikationsbedingungen Revisited
- Vorwärtsrechnung Revisited
- Programmsicherheit und Frame Conditions
- Ausblick und Rückblick

Operationale vs. denotationale Semantik

	Operational $\langle a, \sigma \rangle \rightarrow_{Aexp} n$	Denotational $\mathcal{A}[\![a]\!]$
$m \in \mathbf{N}$	$\langle m, \sigma \rangle \rightarrow_{Aexp} m$	$\{(\sigma, m) \mid \sigma \in \Sigma\}$
$x \in \mathbf{Loc}$	$\dfrac{x \in Dom(\sigma)}{\langle x, \sigma \rangle \rightarrow_{Aexp} \sigma(x)}$	$\{(\sigma, \sigma(x)) \mid \sigma \in \Sigma, x \in Dom(\sigma)\}$
$a_1 \circ a_2$	$\dfrac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n \quad \langle a_2, \sigma \rangle \rightarrow_{Aexp} m \quad n, m \neq \bot}{\langle a_1 \circ a_2, \sigma \rangle \rightarrow_{Aexp} n \circ^I m}$	$\{(\sigma, n \circ^I m) \mid \sigma \in \Sigma, (\sigma, n) \in \mathcal{A}[\![a_1]\!], (\sigma, m) \in \mathcal{A}[\![a_2]\!]\}$
	$\dfrac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n \quad \langle a_2, \sigma \rangle \rightarrow_{Aexp} m \quad n = \bot \text{ oder } m = \bot}{\langle a_1 \circ a_2, \sigma \rangle \rightarrow_{Aexp} \bot}$	
	$\circ \in \{+, *, -\}$	

Operationale vs. denotationale Semantik

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

Äquivalenz operationale und denotationale Semantik

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

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

- Beweis per struktureller Induktion über a.

Operationale vs. denotationale Semantik

	Operational $\langle b, \sigma \rangle \rightarrow_{Bexp} 0 \vert 1$	Denotational $\mathcal{B}[\![b]\!]$
1	$\langle 1, \sigma \rangle \rightarrow_{Bexp} 1$	$\{(\sigma, 1) \mid \sigma \in \Sigma\}$
0	$\langle 0, \sigma \rangle \rightarrow_{Bexp} 0$	$\{(\sigma, 0) \mid \sigma \in \Sigma\}$

Operationale vs. denotationale Semantik

	Operat. $\langle b, \sigma \rangle \rightarrow_{Bexp} 0 \vert 1$	Denotational $\mathcal{B}[\![b]\!]$
$a_0 == a_1$	$\dfrac{\langle a_0, \sigma \rangle \rightarrow_{Aexp} n \quad \langle a_1, \sigma \rangle \rightarrow_{Aexp} m \quad n, m \neq \bot \quad n = m}{\langle a_0 == a_1, \sigma \rangle \rightarrow_{Bexp} 1}$	$\{(\sigma, 1) \mid \sigma \in \Sigma, (\sigma, n_0) \in \mathcal{A}[\![a_0]\!], (\sigma, n_1) \in \mathcal{A}[\![a_1]\!], n_0 = n_1\}$
	$\dfrac{\langle a_0, \sigma \rangle \rightarrow_{Aexp} n \quad \langle a_1, \sigma \rangle \rightarrow_{Aexp} m \quad n, m \neq \bot \quad n \neq m}{\langle a_0 == a_1, \sigma \rangle \rightarrow_{Bexp} 0}$	$\cup$ $\{(\sigma, 0) \mid \sigma \in \Sigma, (\sigma, n_0) \in \mathcal{A}[\![a_0]\!], (\sigma, n_1) \in \mathcal{A}[\![a_1]\!], n_0 \neq n_1\}$
	$\dfrac{\langle a_0, \sigma \rangle \rightarrow_{Aexp} n \quad \langle a_1, \sigma \rangle \rightarrow_{Aexp} m \quad n = \bot \text{ oder } m = \bot}{\langle a_0 == a_1, \sigma \rangle \rightarrow_{Bexp} \bot}$	
$a1 <= a2$	analog	

Operationale vs. denotationale Semantik

	Operational $\langle a, \sigma \rangle \rightarrow_{Bexp} b$	Denotational $\mathcal{B}[\![b]\!]$
$b_1 \&\& b_0$	$\dfrac{\langle b_1, \sigma \rangle \rightarrow_{Bexp} 0}{\langle b_1 \&\& b_2, \sigma \rangle \rightarrow 0}$	$\{(\sigma, 0) \mid (\sigma, 0) \in \mathcal{B}[\![b_1]\!]\}$
	$\dfrac{\langle b_1, \sigma \rangle \rightarrow_{Bexp} 1 \quad \langle b_2, \sigma \rangle \rightarrow_{Bexp} b}{\langle b_1 \&\& b_2, \sigma \rangle \rightarrow b}$	$\{(\sigma, b) \mid (\sigma, 1) \in \mathcal{B}[\![b_1]\!], (\sigma, b) \in \mathcal{B}[\![b_2]\!]\}$
	$\dfrac{\langle b_1, \sigma \rangle \rightarrow_{Bexp} \bot}{\langle b_1 \&\& b_2, \sigma \rangle \rightarrow \bot}$	
$b_1 \vert\vert b_2$	analog	
$!n$	...	

Äquivalenz operationale und denotationale Semantik

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

$$\langle b, \sigma\rangle \to_{Bexp} t \Leftrightarrow (\sigma, t) \in \mathcal{B}[\![b]\!]$$
$$\langle b, \sigma\rangle \to_{Bexp} \bot \Leftrightarrow \sigma \notin Dom(\mathcal{B}[\![b]\!])$$

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

Operationale vs. denotationale Semantik

	Operational $\langle c, \sigma\rangle \to_{Stmt} \sigma' \vert \bot$	Denotational $\mathcal{C}[\![c]\!]$
$\{c_1 \ldots c_n\}$	$\frac{}{\langle \{\}, \sigma\rangle \to_{Stmt} \sigma}$ $\frac{\langle c_1, \sigma\rangle \to_{Stmt} \sigma'' \neq \bot \quad \langle \{c_2 \ldots c_n\}, \sigma'\rangle \to_{Stmt} \sigma''}{\langle \{c_1 \ldots c_n\}, \sigma\rangle \to_{Stmt} \sigma''}$ $\frac{\langle c_1, \sigma\rangle \to_{Stmt} \bot}{\langle \{c_1 \ldots c_n\}, \sigma\rangle \to_{Stmt} \bot}$	$\mathcal{B}[\![c_n]\!] \circ \ldots \mathcal{B}[\![c_1]\!] \circ Id$
$x = a$	$\frac{\langle a, \sigma\rangle \to_{Aexp} n}{\langle x = a, \sigma\rangle \to_{Stmt} \sigma[n/x]}$ $\frac{\langle a, \sigma\rangle \to_{Aexp} \bot}{\langle x = a, \sigma\rangle \to_{Stmt} \bot}$	$\{(\sigma, \sigma[n/X]) \vert (\sigma, n) \in \mathcal{A}[\![a]\!]\}$

Operationale vs. denotationale Semantik

	Operational $\langle c, \sigma\rangle \to_{Stmt} \sigma' \vert \bot$	Denotational $\mathcal{C}[\![c]\!]$
if (b) c_0	$\frac{\langle b, \sigma\rangle \to_{Bexp} 1 \quad \langle c_0, \sigma\rangle \to_{Stmt} \sigma'}{\langle c, \sigma\rangle \to_{Stmt} \sigma'}$ $\frac{\langle b, \sigma\rangle \to_{Bexp} \bot}{\langle c, \sigma\rangle \to_{Stmt} \bot}$	$\{(\sigma, \sigma') \vert (\sigma, 1) \in \mathcal{B}[\![b]\!], (\sigma, \sigma') \in \mathcal{C}[\![c_0]\!]\}$
else c_1	$\frac{\langle b, \sigma\rangle \to_{Bexp} 0 \quad \langle c_1, \sigma\rangle \to_{Stmt} \sigma'}{\langle c, \sigma\rangle \to_{Stmt} \sigma'}$	$\{(\sigma, \sigma') \vert (\sigma, 0) \in \mathcal{B}[\![b]\!], (\sigma, \sigma') \in \mathcal{C}[\![c_1]\!]\}$

Operationale vs. denotationale Semantik

	Operational $\langle c, \sigma\rangle \to_{Stmt} \sigma' \vert \bot$	Denotational $\mathcal{C}[\![c]\!]$
$\underbrace{while\ (b)\ c}_{w}$	$\frac{\langle b, \sigma\rangle \to_{Bexp} 0}{\langle w, \sigma\rangle \to_{Stmt} \sigma}$ $\frac{\langle b, \sigma\rangle \to_{Bexp} \bot}{\langle w, \sigma\rangle \to_{Stmt} \bot}$ $\frac{\langle b, \sigma\rangle \to_{Bexp} 1 \quad \langle c, \sigma\rangle \to_{Stmt} \sigma' \neq \bot \quad \langle w, \sigma'\rangle \to_{Stmt} \sigma''}{\langle w, \sigma\rangle \to_{Stmt} \sigma''}$ $\frac{\langle b, \sigma\rangle \to_{Bexp} 1 \quad \langle c, \sigma\rangle \to_{Stmt} \bot}{\langle w, \sigma\rangle \to_{Stmt} \bot}$	$fix(\Gamma)$

mit

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

Äquivalenz operationale und denotationale Semantik

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

$$\langle c, \sigma\rangle \to_{Stmt} \sigma' \Leftrightarrow (\sigma, \sigma') \in \mathcal{C}[\![c]\!]$$
$$\langle c, \sigma\rangle \to_{Stmt} \bot \Rightarrow \sigma \notin Dom(\mathcal{C}[\![c]\!])$$

- $\Rightarrow$ Beweis per Induktion über die Ableitung in der operationalen Semantik
- $\Leftarrow$ 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.
  - Gegenbeispiel für $\Leftarrow$ in der zweiten Aussage: wähle $c \equiv while(1)\{\}$: $\mathcal{C}[\![c]\!] = \emptyset$ aber $\langle c, \sigma\rangle \to_{Stmt} \bot$ gilt nicht (sondern?).