Korrekte Software: Grundlagen und Methoden

Vorlesung 4 vom 24.04.24

Äquivalenz der Operationalen und Denotationalen Semantik

Serge Autexier, Christoph Lüth

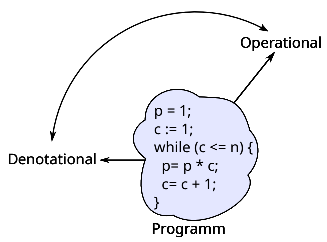
Universität Bremen

Sommersemester 2024

Fahrplan

- Einführung
- Operationale Semantik
- Denotationale Semantik
- Äquivalenz der Operationalen und Denotationalen Semantik
- Der Floyd-Hoare-Kalkül
- Invarianten im Floyd-Hoare-Kalkül
- Korrektheit des Floyd-Hoare-Kalküls
- Strukturierte Datentypen
- Verifikationsbedingungen
- Vorwärts mit Floyd und Hoare
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Operationale und Denotationale Semantik



Äquivalenz der Operationalen und Denotationalen Semantik

- Was müssen wir zeigen?
- Auf oberster Ebene: für alle $c \in \mathbf{Stmt}, \sigma, \sigma' \in \Sigma$:

$$\langle c, \sigma\rangle \rightarrow_{Stmt} \sigma' \Longleftrightarrow (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}} \qquad (1)$$

- Semantik von Anweisungen ist über Semantik von Ausdrücken definiert, deshalb benötigen wir Hilfsaussagen

$$\langle b, \sigma\rangle \rightarrow_{Bexp} t \Longleftrightarrow (\sigma, t) \in [\![b]\!]_{\mathcal{B}} \qquad (2)$$
$$\langle a, \sigma\rangle \rightarrow_{Aexp} n \Longleftrightarrow (\sigma, n) \in [\![a]\!]_{\mathcal{A}} \qquad (3)$$

- Wie zeigen wir das?

Operationale vs. denotationale Semantik

	Operational $\langle a, \sigma\rangle \rightarrow_{Aexp} n$	Denotational $[\![a]\!]_{\mathcal{A}}$
m∈ **Z**	$\langle m, \sigma\rangle \rightarrow_{Aexp} m$	$\{(\sigma, m) \mid \sigma \in \Sigma\}$
x∈ **Loc**	$\dfrac{x \in Dom(\sigma)}{\langle x, \sigma\rangle \rightarrow_{Aexp} \sigma(x)}$	$\{(\sigma, \sigma(x)) \mid \sigma \in \Sigma, x \in Dom(\sigma)\}$

Operationale vs. denotationale Semantik

	Operational $\langle a, \sigma\rangle \rightarrow_{Aexp} n$	Denotational $[\![a]\!]_{\mathcal{A}}$
$a_1 \otimes a_2$	$\dfrac{\langle a_1, \sigma\rangle \rightarrow_{Aexp} n \quad \langle a_2, \sigma\rangle \rightarrow_{Aexp} m}{\langle a_1 \otimes a_2, \sigma\rangle \rightarrow_{Aexp} n \otimes^I m}$ $\otimes \in \{+, *, -\}$	$\{(\sigma, n \otimes^I m) \mid \sigma \in \Sigma, (\sigma, n) \in [\![a_1]\!]_{\mathcal{A}}, (\sigma, m) \in [\![a_2]\!]_{\mathcal{A}}\}$
a_1/a_2	$\dfrac{\langle a_1, \sigma\rangle \rightarrow_{Aexp} n \quad \langle a_2, \sigma\rangle \rightarrow_{Aexp} m \quad m \neq 0}{\langle a_1/a_2, \sigma\rangle \rightarrow_{Aexp} n \div m}$	$\{(\sigma, n \div m) \mid \sigma \in \Sigma, (\sigma, n) \in [\![a_1]\!]_{\mathcal{A}}, (\sigma, m) \in [\![a_2]\!]_{\mathcal{A}}, m \neq 0\}$

Äquivalenz operationale und denotationale Semantik

- Zu zeigen Gleichung (3) von Folie 4:
- Für alle $a \in \mathbf{Aexp}$, für alle $n \in \mathbb{Z}$, für alle Zustände σ:

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

- Beweis Prinzip?

Exkurs: Beweisprinzipien

- Induktion über $\mathbb{N}$ ($\mathrm{nf}(n)$ ist der **Nachfolger** von n):

$$\frac{P(0) \wedge \forall n \in \mathbb{N}.\, P(n) \Longrightarrow P(\mathrm{nf}(n))}{\forall x \in \mathbb{N}.\, P(x)}$$

- Beispiel: Addition ist definiert durch

$$x + 0 = x$$
$$x + \mathrm{nf}(y) = \mathrm{nf}(x + y)$$

- Zeige $x + y = y + x$ durch Induktion über y:
  1. Basis: $x + 0 = 0 + x$
  2. Induktionsschritt: Annahme $x + y = y + x$, dann zeige $x + \mathrm{nf}(y) = \mathrm{nf}(y) + x$.
  - Benötigt Hilfsbeweise $0 + x = x$ und $\mathrm{nf}(x + y) = \mathrm{nf}(x) + y$

Arbeitsblatt 4.1: Natürliche Induktion

- Zeigt durch natürliche Induktion:

$$0 + x = x \qquad \mathsf{nf}(x + y) = \mathsf{nf}(x) + y$$

- Welche Variable benutzt ihr für die Induktion? Was ist der Unterschied?

Wohlfundiertheit

Wohlfundiertheit

Eine binäre Relation $\prec \subseteq S \times S$ ist **wohlfundiert**, wenn es keine unendlich **absteigenden** Ketten gibt

$$\cdots \prec a_3 \prec a_2 \prec a_1$$

Beispiele:

- $(N, \leq)$? Nein: $\cdots \leq 1 \leq 1 \leq 1$
- $(\mathbb{N}, <)$? Ja.
- $(\mathbb{Z}, <)$? Nein: $\cdots < -3 < -2 < -1 < 0$
- $(\mathbb{Q}^+, <)$? Nein: $\ldots < \frac{1}{n} \ldots < \frac{1}{4} < \frac{1}{3} < \frac{1}{2} < 1$

Eigenschaften wohlfundierter Relationen

- Eine wohlfundierte Relation ist **irreflexiv:** $\forall x \in S. x \not\prec x$
  - Ansonsten gäbe es $\cdots \prec x \prec x \prec x$
- **Lemma**: $\prec$ ist wohlfundiert gdw. jede nicht-leere Untermenge $Q \subseteq S$ ein minimales Element $\min Q$ hat:

$$\min Q \in Q \wedge \forall b.\, b \prec \min Q \Longrightarrow b \notin Q$$

Wohlfundierte Induktion

Noethersche Induktion (Wohlfundierte Induktion)

Sei $\prec \subseteq R \times R$ **wohlfundiert** und P eine Aussage über Elemente von R. Dann gilt

$$\frac{\forall v \in R. (\forall u \in R.\, u \prec v \Longrightarrow P(u)) \Longrightarrow P(v)}{\forall x \in R.\, P(x)}$$

Beispiele:

- Mit $S = \mathbb{N}$, $a \prec a + 1$: natürliche Induktion.
- Warum? Fallunterscheidung über v: entweder $v = 0$, dann gibt es kein u so dass $u \prec 0$ und die Voraussetzung ist $P(0)$; oder $v = w + 1$, dann $w \prec w + 1$, und die Voraussetzung ist $P(w) \Longrightarrow P(w + 1)$

Strukturelle Ordnung

Strukturelle Ordnung

Die strukturelle Ordnung auf arithmetischen Ausdrücken ist definiert als:

$$\forall a, a' \in \mathbf{Aexp}., a' \prec a \Longleftrightarrow a' \text{ ist Teilausdruck von } a$$

Dabei ist "Teilausdruck" formalisiert als $\otimes \in \{+, *, -, /\}$:

$$a \text{ Teilausdruck-von } (a_1 \otimes a_2) \Longleftrightarrow \left(\begin{array}{c} a = a_1 \vee a \text{ Teilausdruck-von } a_1 \vee \\ a = a_2 \vee a \text{ Teilausdruck-von } a_2 \end{array} \right)$$

- Beispiel für strukturelle Induktion: Rechtseindeutigkeit von $[\![-]\!]_{\mathcal{A}}$ ($\longrightarrow$ Vorlesung 3)

Arbeitsblatt 4.2: Strukturelle Induktion

- **Beweist**, dass die Relation "Teilausdruck-von" wohlfundiert ist.

Äquivalenz operationale und denotationale Semantik

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

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

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

Beweis: $\forall a \in \mathbf{Aexp}. \forall n \in \mathbb{Z}. \forall \sigma. \langle a, \sigma \rangle \rightarrow_{Aexp} n \Longleftrightarrow (\sigma, n) \in [\![a]\!]_{\mathcal{A}}$

Induktionsanfänge

- $a \equiv m \in \mathbf{Z}$:

$$\left. \begin{array}{l} \langle m, \sigma \rangle \rightarrow_{Aexp} [\![m]\!] \\ [\![m]\!]_{\mathcal{A}} = \{(\sigma', [\![m]\!]) \mid \sigma' \in \Sigma\} \Rightarrow (\sigma, [\![m]\!]) \in [\![m]\!]_{\mathcal{A}} \end{array} \right] \Longleftrightarrow$$

- $a \equiv X \in \mathbf{Loc}$:

1. $X \in Dom(\sigma)$:

$$\left. \begin{array}{l} \langle X, \sigma \rangle \rightarrow_{Aexp} \sigma(X) \\ [\![X]\!]_{\mathcal{A}} = \{(\sigma', \sigma'(X)) | \sigma' \in \Sigma, X \in Dom(\sigma')\} \Rightarrow (\sigma, \sigma(X)) \in [\![X]\!]_{\mathcal{A}} \end{array} \right] \Longleftrightarrow$$

2. $X \notin Dom(\sigma)$:

$$\left. \begin{array}{l} \langle X, \sigma \rangle \rightarrow_{Aexp} \bot \\ [\![X]\!]_{\mathcal{A}} = \{(\sigma', \sigma'(X)) | \sigma' \in \Sigma, X \in Dom(\sigma')\} \Rightarrow \sigma \notin Dom([\![X]\!]_{\mathcal{A}}) \end{array} \right] \Longleftrightarrow$$

Beweis: $\forall a \in \mathbf{Aexp}. \forall n \in \mathbb{Z}. \forall \sigma. \langle a, \sigma \rangle \to_{Aexp} n \Longleftrightarrow (\sigma, n) \in [\![a]\!]_{\mathcal{A}}$

Induktionsschritte

- $a \equiv a_1 + a_2$ — Induktionsannahme: für alle m, n

$$\langle a_1, \sigma \rangle \to_{Aexp} m \Longleftrightarrow (\sigma, m) \in [\![a_1]\!]_{\mathcal{A}}$$
$$\langle a_2, \sigma \rangle \to_{Aexp} n \Longleftrightarrow (\sigma, n) \in [\![a_2]\!]_{\mathcal{A}}$$

Dann;

$$\begin{array}{ccccc}
\langle a_1 + a_2, \sigma \rangle \to_{Aexp} m + n & \overset{(\text{Def. } \langle .,. \rangle \to_{Aexp})}{\Longleftrightarrow} & \langle a_1, \sigma \rangle \to_{Aexp} m & \overset{\text{IA für } a_1}{\Longleftrightarrow} & (\sigma, m) \in [\![a_1]\!]_{\mathcal{A}} \\
 & & \& & & \& \\
 & & \langle a_2, \sigma \rangle \to_{Aexp} n & \overset{\text{IA für } a_2}{\Longleftrightarrow} & (\sigma, n) \in [\![a_2]\!]_{\mathcal{A}} \\
 & & & & \Updownarrow (Def\, [\![.]\!]_{\mathcal{A}}) \\
 & & & & (\sigma, m + n) \in [\![a_1 + a_2]\!]_{\mathcal{A}}
\end{array}$$

Beweis: $\forall a \in \mathbf{Aexp}. \forall n \in \mathbb{Z}. \forall \sigma. \langle a, \sigma \rangle \to_{Aexp} n \Longleftrightarrow (\sigma, n) \in [\![a]\!]_{\mathcal{A}}$

Induktionsschritte

- $a \equiv a_1 / a_2$ — Induktionsannahme:

$$\langle a_1, \sigma \rangle \to_{Aexp} m \Longleftrightarrow (\sigma, m) \in [\![a_1]\!]_{\mathcal{A}}$$
$$\langle a_2, \sigma \rangle \to_{Aexp} n \Longleftrightarrow (\sigma, n) \in [\![a_2]\!]_{\mathcal{A}}$$

1. Fall: $n \neq 0$

$$\begin{array}{ccccc}
\langle a_1 / a_2, \sigma \rangle \to_{Aexp} m/n & \overset{(\text{Def. } \langle .,. \rangle \to_{Aexp})}{\Longleftrightarrow} & \langle a_1, \sigma \rangle \to_{Aexp} m & \overset{\text{IA für } a_1}{\Longleftrightarrow} & (\sigma, m) \in [\![a_1]\!]_{\mathcal{A}} \\
 & & \& & & \& \\
 & & \langle a_2, \sigma \rangle \to_{Aexp} n & \overset{\text{IA für } a_2}{\Longleftrightarrow} & (\sigma, n) \in [\![a_2]\!]_{\mathcal{A}} \\
 & & & & \Updownarrow (Def\, [\![.]\!]_{\mathcal{A}}) \\
 & & & & (\sigma, m/n) \in [\![a_1 / a_2]\!]_{\mathcal{A}}
\end{array}$$

Beweis: $\forall a \in \mathbf{Aexp}. \forall n \in \mathbb{Z}. \forall \sigma. \langle a, \sigma \rangle \to_{Aexp} n \Longleftrightarrow (\sigma, n) \in [\![a]\!]_{\mathcal{A}}$

Induktionsschritte

- $a \equiv a_1 / a_2$ — Induktionsannahme:

$$\langle a_1, \sigma \rangle \to_{Aexp} m \Longleftrightarrow (\sigma, m) \in [\![a_1]\!]_{\mathcal{A}}$$
$$\langle a_2, \sigma \rangle \to_{Aexp} n \Longleftrightarrow (\sigma, n) \in [\![a_2]\!]_{\mathcal{A}}$$

1. Fall: $n = 0$
   Dann gibt es kein v so dass $\langle a_1/a_2, \sigma \rangle \to_{Aexp} v$, aber auch $\sigma \notin \text{dom}\, [\![a_1/a_2]\!]_{\mathcal{A}}$.

q.e.d.

Operationale vs. denotationale Semantik

	Operational $\langle b, \sigma \rangle \to_{Bexp}$ *false* | *true*	**Denotational** $[\![b]\!]_{\mathcal{B}}$
1	$\langle \mathbf{1}, \sigma \rangle \to_{Bexp} true$	$\{(\sigma, true) \mid \sigma \in \Sigma\}$
0	$\langle \mathbf{0}, \sigma \rangle \to_{Bexp} false$	$\{(\sigma, false) \mid \sigma \in \Sigma\}$

Operationale vs. denotationale Semantik

	Operat. $\langle b, \sigma \rangle \to_{Bexp} t$	**Denotational** $[\![b]\!]_{\mathcal{B}}$
$a_0 == a_1$	$\dfrac{\langle a_0, \sigma \rangle \to_{Aexp} n \quad \langle a_1, \sigma \rangle \to_{Aexp} m \quad n = m}{\langle a_0 == a_1, \sigma \rangle \to_{Bexp} true}$ $\dfrac{\langle a_0, \sigma \rangle \to_{Aexp} n \quad \langle a_1, \sigma \rangle \to_{Aexp} m \quad n \neq m}{\langle a_0 == a_1, \sigma \rangle \to_{Bexp} false}$	$\{(\sigma, true) \mid \sigma \in \Sigma, (\sigma, n_0) \in [\![a_0]\!]_{\mathcal{A}}, (\sigma, n_1) \in [\![a_1]\!]_{\mathcal{A}}, n_0 = n_1\}$ $\cup$ $\{(\sigma, false) \mid \sigma \in \Sigma, (\sigma, n_0) \in [\![a_0]\!]_{\mathcal{A}}, (\sigma, n_1) \in [\![a_1]\!]_{\mathcal{A}}, n_0 \neq n_1\}$
$a1 < a2$	analog	

Operationale vs. denotationale Semantik

	Operational $\langle a, \sigma \rangle \to_{Bexp} b$	**Denotational** $[\![b]\!]_{\mathcal{B}}$
$b_1 \,\&\&\, b_2$	$\dfrac{\langle b_1, \sigma \rangle \to_{Bexp} false}{\langle b_1 \,\&\&\, b_2, \sigma \rangle \to false}$	$\{(\sigma, false) \mid (\sigma, false) \in [\![b_1]\!]_{\mathcal{B}}\}$
	$\dfrac{\langle b_1, \sigma \rangle \to_{Bexp} true \quad \langle b_2, \sigma \rangle \to_{Bexp} t}{\langle b_1 \,\&\&\, b_2, \sigma \rangle \to t}$	$\{(\sigma, t) \mid (\sigma, true) \in [\![b_1]\!]_{\mathcal{B}}, (\sigma, t) \in [\![b_2]\!]_{\mathcal{B}}\}$
$b_1 \,\|\|\, b_2$	analog	
$!n$	...	

Äquivalenz operationale und denotationale Semantik

- Zu zeigen Gleichung (2) von Folie 4:
- Für alle $b \in \mathbf{Bexp}$, für alle $t \in \mathbb{B}$, for alle Zustände σ:

$$\langle b, \sigma \rangle \to_{Bexp} t \Longleftrightarrow (\sigma, t) \in [\![b]\!]_{\mathcal{B}}$$

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

Beweis $\langle b, \sigma \rangle \to_{Bexp} t \Longleftrightarrow (\sigma, t) \in [\![b]\!]_{\mathcal{B}}$

Induktionsanfänge

- $b \equiv \mathbf{0}$:

$$\left.\begin{array}{l} \langle \mathbf{0}, \sigma \rangle \to_{Bexp} false \\ [\![\mathbf{0}]\!]_{\mathcal{B}} = \{(\sigma', false) \mid \sigma' \in \Sigma\} \Rightarrow (\sigma, false) \in [\![\mathbf{0}]\!]_{\mathcal{B}} \end{array}\right] \Longleftrightarrow$$

- $b \equiv \mathbf{1}$:

$$\left.\begin{array}{l} \langle \mathbf{1}, \sigma \rangle \to_{Bexp} true \\ [\![\mathbf{1}]\!]_{\mathcal{B}} = \{(\sigma', true) \mid \sigma' \in \Sigma\} \Rightarrow (\sigma, true) \in [\![\mathbf{1}]\!]_{\mathcal{B}} \end{array}\right] \Longleftrightarrow$$

Beweis $\langle b,\sigma\rangle \to_{Bexp} t \iff (\sigma,t)\in [\![b]\!]_{\mathcal{B}}$

Induktionsschritte

- $b \equiv b_1\&\&b_2$ — Induktionsannahme:

$$\langle b_1,\sigma\rangle \to_{Bexp} v \iff (\sigma,v)\in [\![b_1]\!]_{\mathcal{B}}$$
$$\langle b_2,\sigma\rangle \to_{Bexp} w \iff (\sigma,w)\in [\![b_2]\!]_{\mathcal{B}}$$

1. Fall $v = false$

$$\langle b_1\&\&b_2,\sigma\rangle \to_{Bexp} false \xLeftrightarrow{\text{(Def. } \langle .,.\rangle \to_{Bexp})} \langle b_1,\sigma\rangle \to_{Bexp} false \xLeftrightarrow{\text{IA für } b_1} (\sigma,false)\in [\![b_1]\!]_{\mathcal{B}}$$
$$\Updownarrow \text{Def. } [\![.]\!]_{\mathcal{B}}$$
$$(\sigma,false)\in [\![b_1\&\&b_2]\!]_{\mathcal{B}}$$

Beweis $\langle b,\sigma\rangle \to_{Bexp} t \iff (\sigma,t)\in [\![b]\!]_{\mathcal{B}}$

Induktionsschritte

- $b \equiv b_1\&\&b_2$ — Induktionsannahme:

$$\langle b_1,\sigma\rangle \to_{Bexp} v \iff (\sigma,v)\in [\![b_1]\!]_{\mathcal{B}}$$
$$\langle b_2,\sigma\rangle \to_{Bexp} w \iff (\sigma,w)\in [\![b_2]\!]_{\mathcal{B}}$$

1. Fall $v = true$

$$\langle b_1\&\&b_2,\sigma\rangle \to_{Bexp} w \xLeftrightarrow{\text{(Def. } \langle .,.\rangle \to_{Bexp})} \langle b_1,\sigma\rangle \to_{Bexp} true \xLeftrightarrow{\text{IA für } b_1} (\sigma,true)\in [\![b_1]\!]_{\mathcal{B}}$$
$$\& \qquad \qquad \&$$
$$\langle b_2,\sigma\rangle \to_{Bexp} w \xLeftrightarrow{\text{IA für } b_2} (\sigma,w)\in [\![b_2]\!]_{\mathcal{B}}$$
$$\Updownarrow \text{Def. } [\![.]\!]_{\mathcal{B}}$$
$$(\sigma,w)\in [\![b_1\&\&b_2]\!]_{\mathcal{B}}$$

q.e.d.

Arbeitsblatt 4.3: Beweis Induktionsanfang

$\langle a_1 == a_2,\sigma\rangle \to_{Bexp} v \iff (\sigma,v)\in [\![a_1 == a_2]\!]_{\mathcal{B}}$

Beweist obige Aussage unter Verwendung des für arithmetische Ausdrücke geltenden Lemmas

$$\forall a\in \mathbf{Aexp}.\, \forall n\in\mathbb{Z}.\, \forall\sigma.\, \langle a,\sigma\rangle \to_{Aexp} n \iff (\sigma,n)\in [\![a]\!]_{\mathcal{A}}$$

1. Was sind die Annahmen?
2. Welche Fälle unterscheiden wir?

Beweis $\langle a_1 == a_2,\sigma\rangle \to_{Bexp} v \iff (\sigma,v)\in [\![a_1 == a_2]\!]_{\mathcal{B}}$

- Annahmen: für $n, m\in\mathbb{B}$:

$$\langle a_1,\sigma\rangle \to_{Aexp} m \iff (\sigma,m)\in [\![a_1]\!]_{\mathcal{B}}$$
$$\langle a_2,\sigma\rangle \to_{Aexp} n \iff (\sigma,n)\in [\![a_2]\!]_{\mathcal{B}}$$

- 1. Fall: $v = true$ $(m = n)$

$$\langle a_1 == a_2,\sigma\rangle \to_{Bexp} true \xLeftrightarrow{\text{(Def. } \langle .,.\rangle \to_{Bexp})} \langle a_1,\sigma\rangle \to_{Bexp} m \xLeftrightarrow{\text{Annahme für } a_1} (\sigma,m)\in [\![a_1]\!]_{\mathcal{A}}$$
$$\& \qquad \qquad \&$$
$$\langle a_2,\sigma\rangle \to_{Bexp} m \xLeftrightarrow{\text{Annahme für } a_2} (\sigma,m)\in [\![a_2]\!]_{\mathcal{A}}$$
$$\Updownarrow \text{Def. } [\![.]\!]_{\mathcal{B}}$$
$$(\sigma,true)[\![a_1 == a_2]\!]_{\mathcal{B}}$$

Beweis $\langle a_1 == a_2,\sigma\rangle \to_{Bexp} v \iff (\sigma,v)\in [\![a_1 == a_2]\!]_{\mathcal{B}}$

- Annahmen: für $m, n\in\mathbb{B}$:

$$\langle a_1,\sigma\rangle \to_{Aexp} m \iff (\sigma,m)\in [\![a_1]\!]_{\mathcal{B}}$$
$$\langle a_2,\sigma\rangle \to_{Aexp} n \iff (\sigma,n)\in [\![a_2]\!]_{\mathcal{B}}$$

- 2. Fall: $v = false$ $(m \neq n)$

$$\langle a_1 == a_2,\sigma\rangle \to_{Bexp} false \xLeftrightarrow{\text{(Def. } \langle .,.\rangle \to_{Bexp})} \langle a_1,\sigma\rangle \to_{Aexp} m \xLeftrightarrow{\text{Annahme für } a_1} (\sigma,m)\in [\![a_1]\!]_{\mathcal{A}}$$
$$\& \qquad \qquad \&$$
$$\langle a_2,\sigma\rangle \to_{Aexp} n \xLeftrightarrow{\text{Annahme für } a_2} (\sigma,n)\in [\![a_2]\!]_{\mathcal{A}}$$
$$\Updownarrow \text{Def. } [\![.]\!]_{\mathcal{B}}$$
$$(\sigma,false)[\![a_1 == a_2]\!]_{\mathcal{B}}$$

Operationale vs. denotationale Semantik

	Operational $\langle c,\sigma\rangle \to_{Stmt} \sigma'$	Denotational $[\![c]\!]_{\mathcal{C}}$
$\{\,\}$	$\dfrac{}{\langle\{\},\sigma\rangle \to_{Stmt} \sigma}$	$[\![\{\,\}]\!]_{\mathcal{C}} = Id$
$c_1; c_2$	$\dfrac{\langle c_1,\sigma\rangle \to_{Stmt} \sigma' \quad \langle c_2,\sigma'\rangle \to_{Stmt} \sigma''}{\langle c_1;c_2,\sigma\rangle \to_{Stmt} \sigma''}$	$[\![c_1]\!]_{\mathcal{C}} \circ [\![c_2]\!]_{\mathcal{C}}$
$x = a$	$\dfrac{\langle a,\sigma\rangle \to_{Aexp} n}{\langle x = a,\sigma\rangle \to_{Stmt} \sigma[x\mapsto n]}$	$\{(\sigma,\sigma[x\mapsto n]) \mid (\sigma,n)\in[\![a]\!]_{\mathcal{A}}\}$

Operationale vs. denotationale Semantik

	Operational $\langle c,\sigma\rangle \to_{Stmt} \sigma'$	Denotational $[\![c]\!]_{\mathcal{C}}$
if (b) c_0	$\dfrac{\langle b,\sigma\rangle \to_{Bexp} true \quad \langle c_0,\sigma\rangle \to_{Stmt} \sigma'}{\langle c,\sigma\rangle \to_{Stmt} \sigma'}$	$\{(\sigma,\sigma') \mid (\sigma,true)\in[\![b]\!]_{\mathcal{B}}, (\sigma,\sigma')\in [\![c_0]\!]_{\mathcal{C}}\}$
else c_1	$\dfrac{\langle b,\sigma\rangle \to_{Bexp} false \quad \langle c_1,\sigma\rangle \to_{Stmt} \sigma'}{\langle c,\sigma\rangle \to_{Stmt} \sigma'}$	$\{(\sigma,\sigma') \mid (\sigma,false)\in[\![b]\!]_{\mathcal{B}}, (\sigma,\sigma')\in [\![c_1]\!]_{\mathcal{C}}\}$

Operationale vs. denotationale Semantik

	Operational $\langle c,\sigma\rangle \to_{Stmt} \sigma'$	Denotational $[\![c]\!]_{\mathcal{C}}$
$\underbrace{\textbf{while}\ (b)\ c}_{w}$	$\dfrac{\langle b,\sigma\rangle \to_{Bexp} false}{\langle w,\sigma\rangle \to_{Stmt} \sigma}$	$fix(\Gamma)$
	$\dfrac{\langle b,\sigma\rangle \to_{Bexp} true \quad \langle c,\sigma\rangle \to_{Stmt} \sigma' \quad \langle w,\sigma'\rangle \to_{Stmt} \sigma''}{\langle w,\sigma\rangle \to_{Stmt} \sigma''}$	

mit

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

Äquivalenz operationale und denotationale Semantik

- Zu zeigen Gleichung (1) von Folie 4:
- Für alle $c \in \textbf{Stmt}$, für alle Zustände σ, σ':

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

- $\Longrightarrow$ Beweis Prinzip?
- $\Longleftarrow$ Beweis Prinzip?

Operationale Semantik: C0 Programme

- $\textbf{Stmt} c ::= \textbf{Idt} = \textbf{Exp} \mid \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2 \mid \textbf{while}\ (b)\ c \mid c_1; c_2 \mid \{\ \}$

Regeln:

$$\frac{}{\langle \{\ \}, \sigma \rangle \rightarrow_{Stmt} \sigma} \qquad \frac{\langle a, \sigma \rangle \rightarrow_{Aexp} n \in \mathbb{Z}}{\langle x = a, \sigma \rangle \rightarrow_{Stmt} \sigma[x \mapsto n]} \qquad \frac{\langle c_1, \sigma \rangle \rightarrow_{Stmt} \sigma' \quad \langle c_2, \sigma' \rangle \rightarrow_{Stmt} \sigma''}{\langle c_1; c_2, \sigma \rangle \rightarrow_{Stmt} \sigma''}$$

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} true \quad \langle c_1, \sigma \rangle \rightarrow_{Stmt} \sigma'}{\langle \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2, \sigma \rangle \rightarrow_{Stmt} \sigma'} \qquad \frac{\langle b, \sigma \rangle \rightarrow_{Bexp} false \quad \langle c_2, \sigma \rangle \rightarrow_{Stmt} \sigma'}{\langle \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2, \sigma \rangle \rightarrow_{Stmt} \sigma'}$$

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} false}{\langle \textbf{while}\ (b)\ c, \sigma \rangle \rightarrow_{Stmt} \sigma}$$

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} true \quad \langle c, \sigma \rangle \rightarrow_{Stmt} \sigma' \quad \langle \textbf{while}\ (b)\ c, \sigma' \rangle \rightarrow_{Stmt} \sigma''}{\langle \textbf{while}\ (b)\ c, \sigma \rangle \rightarrow_{Stmt} \sigma''}$$

Operationale Semantik: C0 Programme

- $\textbf{Stmt} c ::= \textbf{Idt} = \textbf{Exp} \mid \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2 \mid \textbf{while}\ (b)\ c \mid c_1; c_2 \mid \{\ \}$

Regeln: **Programmstruktur**

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

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} true \quad \langle c_1, \sigma \rangle \rightarrow_{Stmt} \sigma'}{\langle \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2, \sigma \rangle \rightarrow_{Stmt} \sigma'} \qquad \searrow$$

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} false \quad \langle c_2, \sigma \rangle \rightarrow_{Stmt} \sigma'}{\langle \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2, \sigma \rangle \rightarrow_{Stmt} \sigma'} \qquad \searrow$$

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} true \quad \langle c, \sigma \rangle \rightarrow_{Stmt} \sigma' \quad \langle \textbf{while}\ (b)\ c, \sigma' \rangle \rightarrow_{Stmt} \sigma''}{\langle \textbf{while}\ (b)\ c, \sigma \rangle \rightarrow_{Stmt} \sigma''} \qquad \rightarrow$$

Strukturelle Induktion über c **nicht** möglich.

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} false}{\langle \textbf{while}\ (b)\ c, \sigma \rangle \rightarrow_{Stmt} \sigma} \qquad \searrow$$

Ableitungstiefe für Programme

- Die Ableitungstiefe einer Programmauswertung mittels Regeln der operationaler Semantik ist die **Anzahl der Regelanwendungen** mit Conclusion der Form $\langle ., . \rangle \rightarrow_{Stmt} ..$

$$\frac{\vdots \qquad\qquad \vdots}{\textit{Prämisse}_1 \quad \cdots \quad \textit{Prämisse}_n} \qquad \frac{\textit{Prämisse}_1 \quad \cdots \quad \textit{Prämisse}_n}{\textit{Conclusion}}$$

Operationale Semantik: C0 Programme

- $\textbf{Stmt} c ::= \textbf{Idt} = \textbf{Exp} \mid \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2 \mid \textbf{while}\ (b)\ c \mid c_1; c_2 \mid \{\ \}$

Regeln: **Programmstruktur** **Ableitungstiefe**

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

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} true \quad \langle c_1, \sigma \rangle \rightarrow_{Stmt} \sigma'}{\langle \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2, \sigma \rangle \rightarrow_{Stmt} \sigma'} \qquad \searrow \qquad \searrow$$

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} false \quad \langle c_2, \sigma \rangle \rightarrow_{Stmt} \sigma'}{\langle \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2, \sigma \rangle \rightarrow_{Stmt} \sigma'} \qquad \searrow \qquad \searrow$$

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} true \quad \langle c, \sigma \rangle \rightarrow_{Stmt} \sigma' \quad \langle \textbf{while}\ (b)\ c, \sigma' \rangle \rightarrow_{Stmt} \sigma''}{\langle \textbf{while}\ (b)\ c, \sigma \rangle \rightarrow_{Stmt} \sigma''} \qquad \rightarrow \qquad \searrow$$

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} false}{\langle \textbf{while}\ (b)\ c, \sigma \rangle \rightarrow_{Stmt} \sigma} \qquad \searrow \qquad \searrow$$

Äquivalenz operationale und denotationale Semantik

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

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

- $\Longrightarrow$ Beweis Prinzip?per Induktion über **die (Tiefe der) Ableitung** in der operationalen Semantik (Warum?)
- $\Longleftarrow$ Beweis Prinzip?

Beweis: $\forall c \in \textbf{Stmt}. \forall \sigma, \sigma'. \langle c, \sigma \rangle \rightarrow_{Stmt} \sigma' \Longrightarrow (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}}$

Induktionsanfang — Ableitungstiefe 1

- Fall $c \equiv x = a$:

$$[\![x = a]\!]_{\mathcal{C}} = \{(\sigma, \sigma[x \mapsto m]) | (\sigma, m) \in [\![a]\!]_{\mathcal{A}}\}$$

Sei $\langle a, \sigma \rangle \rightarrow_{Aexp} m \in \mathbb{Z}$:

$$\begin{array}{ccc} \langle x = a, \sigma \rangle \rightarrow_{Stmt} \sigma[x \mapsto m] & & \\ \Updownarrow \text{(Def. } \langle .,. \rangle \rightarrow_{Stmt} .) & & \\ \langle a, \sigma \rangle \rightarrow_{Aexp} m \in \mathbb{Z} & \xLeftrightarrow{\text{Lemma für } a} & (\sigma, m) \in [\![a]\!]_{\mathcal{A}} \\ & & \Downarrow \text{Def. } [\![.]\!]_{\mathcal{C}} \\ & & (\sigma, \sigma[x \mapsto m]) \in [\![x = a]\!]_{\mathcal{C}} \end{array}$$

- Fall $c \equiv \{\}$: ...

Beweis: $\forall c \in \textbf{Stmt}. \forall \sigma, \sigma'. \langle c, \sigma \rangle \rightarrow_{Stmt} \sigma' \Longrightarrow (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}}$

Induktionsschritt:

- Fall $c \equiv \textbf{if}(b)\ c_1\ \textbf{else}\ c_2$:

$$\begin{aligned} [\![\textbf{if}(b)\ c_1\ \textbf{else}\ c_2]\!]_{\mathcal{C}} = & \{(\sigma, \sigma') | (\sigma, \sigma') \in [\![c_1]\!]_{\mathcal{C}}, (\sigma, true) \in [\![b]\!]_{\mathcal{B}}\} \\ & \cup \{(\sigma, \sigma') | (\sigma, \sigma') \in [\![c_2]\!]_{\mathcal{C}}, (\sigma, false) \in [\![b]\!]_{\mathcal{B}}\} \end{aligned}$$

- Fall $\langle \sigma, b \rangle \rightarrow_{Bexp} true$ mit $\langle c_1, \sigma \rangle \rightarrow_{Stmt} \sigma'$:

$$\begin{array}{ccc} \langle \textbf{if}(b)\ c_1\ \textbf{else}\ c_2, \sigma \rangle \rightarrow_{Stmt} \sigma' \xLeftrightarrow{\text{(Def. } \langle .,. \rangle \rightarrow_{Stmt} .)} \langle b, \sigma \rangle \rightarrow_{Bexp} true & \xLeftrightarrow{\text{Lemma für } b} & (\sigma, true) \in [\![b]\!]_{\mathcal{B}} \\ \& & & \& \\ \langle c_1, \sigma \rangle \rightarrow_{Stmt} \sigma' & \xRightarrow{\text{IH für } c_1} & (\sigma, \sigma') \in [\![c_1]\!]_{\mathcal{C}} \\ & & \Downarrow \text{Def. } [\![.]\!]_{\mathcal{C}} \\ & & (\sigma, \sigma') \in [\![\textbf{if}(b)\ c_1\ \textbf{else}\ c_2]\!]_{\mathcal{C}} \end{array}$$

- Fall $\langle \sigma, b \rangle \rightarrow_{Bexp} false$ mit $\langle c_2, \sigma \rangle \rightarrow_{Stmt} \sigma'$:

$$\begin{array}{ccc} \langle \textbf{if}(b)\ c_1\ \textbf{else}\ c_2, \sigma \rangle \rightarrow_{Stmt} \sigma' \xLeftrightarrow{\text{(Def. } \langle .,. \rangle \rightarrow_{Stmt} .)} \langle b, \sigma \rangle \rightarrow_{Bexp} false & \xLeftrightarrow{\text{Lemma für } b} & (\sigma, false) \in [\![b]\!]_{\mathcal{B}} \\ \& & & \& \\ \langle c_2, \sigma \rangle \rightarrow_{Stmt} \sigma' & \xRightarrow{\text{IH für } c_2} & (\sigma, \sigma') \in [\![c_2]\!]_{\mathcal{C}} \end{array}$$

Beweis: $\forall c \in \mathbf{Stmt}. \forall \sigma, \sigma'. \langle c, \sigma\rangle \rightarrow_{Stmt} \sigma' \Longrightarrow (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}}$

Induktionsschritt:

- Fall $c \equiv \mathbf{while}(b)\ c$: $\qquad [\![\mathbf{while}(b)\ c]\!]_{\mathcal{C}} = fix(\Gamma)$
  - Fall $\langle b, \sigma\rangle \rightarrow_{Bexp} true$ mit $\langle c, \sigma\rangle \rightarrow_{Stmt} \sigma'$, $\langle \mathbf{while}(b)\ c, \sigma'\rangle \rightarrow_{Stmt} \sigma''$

$$\langle \mathbf{while}(b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma'' \xLeftrightarrow{(\text{Def. } \langle.,.\rangle \rightarrow_{Stmt}.)} \langle b, \sigma\rangle \rightarrow_{Bexp} true \xLeftrightarrow{\text{Lemma für } b} (\sigma, true) \in [\![b]\!]_{\mathcal{B}}$$

$$\&\qquad\qquad\qquad\&$$

$$\langle c, \sigma\rangle \rightarrow_{Stmt} \sigma' \xRightarrow{\text{IH für } \langle c,\sigma\rangle \rightarrow_{Stmt} \sigma'} (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}}$$

$$\&\qquad\qquad\qquad\&$$

$$\langle \mathbf{while}(b)\ c, \sigma'\rangle \rightarrow_{Stmt} \sigma'' \xRightarrow{\text{IH für } \langle \mathbf{while}(b)\ c,\sigma'\rangle \rightarrow_{Stmt} \sigma''} (\sigma', \sigma'') \in [\![\mathbf{while}(b)\ c]\!]_{\mathcal{C}}$$

$$\Big\Downarrow \text{Def. } [\![.]\!]_{\mathcal{C}} \text{ \& Fixpunkt Eigenschaft}$$

$$(\sigma, \sigma'') \in [\![\mathbf{while}(b)\ c]\!]_{\mathcal{C}}$$

  - Fall $\langle b, \sigma\rangle \rightarrow_{Bexp} false$, $\langle \mathbf{while}(b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma$

$$\langle \mathbf{while}(b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma \xLeftrightarrow{(\text{Def. } \langle.,.\rangle \rightarrow_{Stmt})} \langle b, \sigma\rangle \rightarrow_{Bexp} false \xLeftrightarrow{\text{Lemma für } b} (\sigma, false) \in [\![b]\!]_{\mathcal{B}}$$

$$\Big\Downarrow \text{Def. } [\![.]\!]_{\mathcal{C}}$$

$$(\sigma, \sigma) \in [\![\mathbf{while}(b)\ c]\!]_{\mathcal{C}}$$

Äquivalenz operationale und denotationale Semantik

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

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

- $\Longrightarrow$ Beweis per Induktion über **die (Tiefe der) Ableitung** in der operationalen Semantik (Warum?)
- $\Longleftarrow$ 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 $\Gamma^i(\emptyset)$ des Fixpunkts. (Warum?)

Beweis: $\forall c \in \mathbf{Stmt}. \forall \sigma, \sigma'. (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}} \Longrightarrow \langle c, \sigma\rangle \rightarrow_{Stmt} \sigma'$

Induktionsanfang:

- Fall $c \equiv x = a$:

$$[\![x = a]\!]_{\mathcal{C}} = \{(\sigma, \sigma[x \mapsto t]) | (\sigma, t) \in [\![a]\!]_{\mathcal{A}}\}$$

$$(\sigma, \sigma[x \mapsto t]) \in [\![x = a]\!]_{\mathcal{C}} \wedge \underbrace{(\sigma, t) \in [\![a]\!]_{\mathcal{A}}}$$

$$\xRightarrow{\text{Lemma Aexp}} \qquad \langle a, \sigma\rangle \rightarrow_{Aexp} t$$

$$\xRightarrow{\text{Def. } \langle.,.\rangle \rightarrow_{Stmt}.} \langle x = a, \sigma\rangle \rightarrow_{Stmt} \sigma[x \mapsto t]$$

- Fall $c \equiv \{\,\}$

$$[\![\{\,\}]\!]_{\mathcal{C}} = \{(\sigma, \sigma) | \sigma \in \Sigma\}$$

$$(\sigma, \sigma) \in [\![\{\,\}]\!]_{\mathcal{C}}$$

$$\xRightarrow{\text{Def. } \langle.,.\rangle \rightarrow_{Stmt}.} \langle \{\,\}, \sigma\rangle \rightarrow_{Stmt} \sigma$$

Beweis: $\forall c \in \mathbf{Stmt}. \forall \sigma, \sigma'. (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}} \Longrightarrow \langle c, \sigma\rangle \rightarrow_{Stmt} \sigma'$

Induktionsschritt:

- Fall **if** $(b)\ c_1$ **else** c_2:

$$[\![\mathbf{if}\ (b)\ c_1\ \mathbf{else}\ c_2]\!]_{\mathcal{C}} = \{(\sigma, \sigma') | (\sigma, true) \in [\![b]\!]_{\mathcal{B}}, (\sigma, \sigma') \in [\![c_1]\!]_{\mathcal{C}}\} \cup \{(\sigma, \sigma') | (\sigma, false) \in [\![b]\!]_{\mathcal{B}}, (\sigma, \sigma') \in [\![c_2]\!]_{\mathcal{C}}\}$$

  Induktionsannahme gilt für c_1 und c_2
  - Fall: $(\sigma, true) \in [\![b]\!]_{\mathcal{B}}$ mit $(\sigma, \sigma') \in [\![c_1]\!]_{\mathcal{C}}$

$$\begin{aligned} & (\sigma, true) \in [\![b]\!]_{\mathcal{B}} \wedge (\sigma, \sigma') \in [\![c_1]\!]_{\mathcal{C}} \\ \xRightarrow{\text{Lemma Bexp}} & \langle b, \sigma\rangle \rightarrow_{Bexp} true \wedge (\sigma, \sigma') \in [\![c_1]\!]_{\mathcal{C}} \\ \xRightarrow{\text{IA für } c_1} & \langle b, \sigma\rangle \rightarrow_{Bexp} true \wedge \langle c_1, \sigma\rangle \rightarrow_{Stmt} \sigma' \\ \xRightarrow{\text{Def. } \langle.,.\rangle \rightarrow_{Stmt}.} & \langle \mathbf{if}\ (b)\ c_1\ \mathbf{else}\ c_2, \sigma\rangle \rightarrow_{Stmt} \sigma' \end{aligned}$$

  - Fall: $(\sigma, false) \in [\![b]\!]_{\mathcal{B}}$ mit $(\sigma, \sigma') \in [\![c_2]\!]_{\mathcal{C}}$

$$\begin{aligned} & (\sigma, false) \in [\![b]\!]_{\mathcal{B}} \wedge (\sigma, \sigma') \in [\![c_2]\!]_{\mathcal{C}} \\ \xRightarrow{\text{Lemma Bexp}} & \langle b, \sigma\rangle \rightarrow_{Bexp} false \wedge (\sigma, \sigma') \in [\![c_2]\!]_{\mathcal{C}} \\ \xRightarrow{\text{IA für } c_2} & \langle b, \sigma\rangle \rightarrow_{Bexp} false \wedge \langle c_2, \sigma\rangle \rightarrow_{Stmt} \sigma' \\ \xRightarrow{\text{Def. } \langle.,.\rangle \rightarrow_{Stmt}.} & \langle \mathbf{if}\ (b)\ c_1\ \mathbf{else}\ c_2, \sigma\rangle \rightarrow_{Stmt} \sigma' \end{aligned}$$

Beweis: $\forall c \in \mathbf{Stmt}. \forall \sigma, \sigma'. (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}} \Longrightarrow \langle c, \sigma\rangle \rightarrow_{Stmt} \sigma'$

Induktionsschritt:

- Fall **while** $(b)\ c$

$$\begin{aligned} [\![\mathbf{while}\ (b)\ c]\!]_{\mathcal{C}} &= fix(\Gamma) \\ \text{mit } \Gamma(s) &= \{(\sigma, \sigma') \mid (\sigma, true) \in [\![b]\!]_{\mathcal{B}} \wedge (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}} \circ s\} \\ &\cup \{(\sigma, \sigma) \mid (\sigma, false) \in [\![b]\!]_{\mathcal{B}}\} \end{aligned}$$

  Induktionsannahme gilt für c

$$\begin{aligned} (\sigma, \sigma') \in [\![\mathbf{while}\ (b)\ c]\!]_{\mathcal{C}} &\Longrightarrow (\sigma, \sigma') \in fix(\Gamma) && \text{nach Def. } [\![.]\!]_{\mathcal{C}} \\ &\Longrightarrow (\sigma, \sigma') \in \bigcup_{i \in \mathbb{N}} \Gamma^i(\emptyset) && \text{nach Def. } fix(\Gamma) \\ &\Longrightarrow (\sigma, \sigma') \in \Gamma^i(\emptyset) \text{ für ein } i \in \mathbb{N} \\ &\Longrightarrow \langle \mathbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma' && \text{nach (UB)} \end{aligned}$$

  Unterbeweis: $\qquad \forall i \in \mathbb{N}. (\sigma, \sigma') \in \Gamma^i(\emptyset) \Rightarrow \langle \mathbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma' \quad \text{(UB)}$

Unterbeweis: $\forall i \in \mathbb{N}. (\sigma, \sigma') \in \Gamma^i(\emptyset) \Longrightarrow \langle \mathbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma'$

Es gilt die Induktionsannahme für c:

$$\forall \rho, \rho'. (\rho, \rho') \in [\![c]\!]_{\mathcal{C}} \Rightarrow \langle c, \rho\rangle \rightarrow_{Stmt} \rho' \quad (*)$$

Beweis per Induktion über i:

- Induktionsanfang $i = 0$:

$$(\sigma, \sigma') \in \underbrace{\Gamma^0(\emptyset)}_{\emptyset} \Longrightarrow (\sigma, \sigma') \in \emptyset \Longrightarrow false$$

  Implikation trivialerweise erfüllt da $false \Longrightarrow P$ immer wahr
- Induktionsschritt $i \rightarrow i + 1$:
- Induktionsannahme (UB) gilt für i

$$(\sigma, \sigma') \in \Gamma^{i+1}(\emptyset) \Longrightarrow (\sigma, \sigma') \in \Gamma(\Gamma^i(\emptyset))$$

$$\xRightarrow{\text{Def. } \Gamma} (\sigma, \sigma') \in \{(\sigma, \sigma'') \mid (\sigma, true) \in [\![b]\!]_{\mathcal{B}}, (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}}, (\sigma', \sigma'') \in \Gamma^i(\emptyset)\} \cup \{(\sigma, \sigma) \mid (\sigma, false) \in [\![b]\!]_{\mathcal{B}}\}$$

- Fallunterscheidung über Zugehörigkeit zur Teilmenge

Unterbeweis: $\forall i \in \mathbb{N}. (\sigma, \sigma') \in \Gamma^i(\emptyset) \Longrightarrow \langle \mathbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma'$

Es gilt die Induktionsannahme für c:

$$\forall \rho, \rho'. (\rho, \rho') \in [\![c]\!]_{\mathcal{C}} \Rightarrow \langle c, \rho\rangle \rightarrow_{Stmt} \rho' \quad (*)$$

Beweis per Induktion über i:

- Induktionsschritt $i \rightarrow i + 1$:
- Induktionsannahme (UB) gilt für i
- Fall $(\sigma, true) \in [\![b]\!]_{\mathcal{B}}$ mit $(\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}}, (\sigma', \sigma'') \in \Gamma^i(\emptyset)$

$$\begin{aligned} (\sigma, \sigma'') \in \Gamma(\Gamma^i(\emptyset)) &\Longrightarrow \underbrace{(\sigma, true) \in [\![b]\!]_{\mathcal{B}}}_{\text{Lemma Bexp}} \wedge \underbrace{(\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}}}_{\text{IA }(*)} \wedge \underbrace{(\sigma', \sigma'') \in \Gamma^i(\emptyset)}_{\text{IA (UB) für } i} \\ &\Longrightarrow \langle b, \sigma\rangle \rightarrow_{Bexp} true \wedge \langle c, \sigma\rangle \rightarrow_{Stmt} \sigma' \wedge \langle \mathbf{while}\ (b)\ c, \sigma'\rangle \rightarrow_{Stmt} \sigma'' \\ &\Longrightarrow \langle \mathbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma'' \end{aligned}$$

- Fall $(\sigma, false) \in [\![b]\!]_{\mathcal{B}}$

$$\begin{aligned} (\sigma, \sigma') \in \Gamma(\Gamma^i(\emptyset)) &\Longrightarrow (\sigma, false) \in [\![b]\!]_{\mathcal{B}} \wedge \sigma' = \sigma \\ &\Longrightarrow \langle b, \sigma\rangle \rightarrow_{Bexp} false \wedge \sigma' = \sigma && \text{Lemma für } \mathbf{Bexp} \\ &\Longrightarrow \langle \mathbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma (= \sigma') && \square \end{aligned}$$

Beweis: $\forall c \in \mathbf{Stmt}. \forall \sigma, \sigma'. (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}} \Longrightarrow \langle c, \sigma\rangle \rightarrow_{Stmt} \sigma'$

Induktionsschritt:

- Fall **while** $(b)\ c$

$$\begin{aligned} [\![\mathbf{while}\ (b)\ c]\!]_{\mathcal{C}} &= fix(\Gamma) \\ \text{mit } \Gamma(s) &= \{(\sigma, \sigma') \mid (\sigma, true) \in [\![b]\!]_{\mathcal{B}} \wedge (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}} \circ s\} \\ &\cup \{(\sigma, \sigma) \mid (\sigma, false) \in [\![b]\!]_{\mathcal{B}}\} \end{aligned}$$

  Induktionsannahme gilt für c

$$\begin{aligned} (\sigma, \sigma') \in [\![\mathbf{while}\ (b)\ c]\!]_{\mathcal{C}} &\Longrightarrow (\sigma, \sigma') \in fix(\Gamma) && \text{nach Def. } [\![.]\!]_{\mathcal{C}} \\ &\Longrightarrow (\sigma, \sigma') \in \bigcup_{i \in \mathbb{N}} \Gamma^i(\emptyset) && \text{nach Def. } fix(\Gamma) \\ &\Longrightarrow (\sigma, \sigma') \in \Gamma^i(\emptyset) \text{ für ein } i \in \mathbb{N} \\ &\Longrightarrow \langle \mathbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma' && \text{nach (UB)} \end{aligned}$$

  Unterbeweis: $\qquad \forall i \in \mathbb{N}. (\sigma, \sigma') \in \Gamma^i(\emptyset) \Rightarrow \langle \mathbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma' \quad \text{(UB)}$

Zusammenfassung: Äquivalenz der Semantiken

- Wir haben gezeigt: für alle $c \in$ **Stmt**, für alle Zustände σ, σ'

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

- Das ist äquivalent zu (für alle $c \in$ **Stmt**, für alle Zustände σ, σ'):

$$[\![c]\!]_{\mathcal{C}} = \{(\sigma, \sigma') \mid \langle c, \sigma \rangle \rightarrow_{Stmt} \sigma'\}$$

- Insbesondere ist die Undefiniertheit gleich:
wenn es keine Ableitung für c, σ gibt, dann ist auch $\sigma \notin Dom([\![c]\!]_{\mathcal{C}})$.

Fahrplan

- Einführung
- Operationale Semantik
- Denotationale Semantik
- Äquivalenz der Operationalen und Denotationalen Semantik
- Der Floyd-Hoare-Kalkül
- Invarianten im Floyd-Hoare-Kalkül
- Korrektheit des Floyd-Hoare-Kalküls
- Strukturierte Datentypen
- Verifikationsbedingungen
- Vorwärts mit Floyd und Hoare
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick