Korrekte Software: Grundlagen und Methoden

Vorlesung 4 vom 12/14.05.20

Äquivalenz der Operationalen und Denotationalen Semantik

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2020

Fahrplan

- Einführung
- Operationale Semantik
- Denotationale Semantik
- Äquivalenz der Operationalen und Denotationalen Semantik
- Der Floyd-Hoare-Kalkül
- Invarianten und die Korrektheit des Floyd-Hoare-Kalküls
- Strukturierte Datentypen
- Verifikationsbedingungen
- Vorwärts mit Floyd und Hoare
- Modellierung
- Spezifikation von Funktionen
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Operationale vs. denotationale Semantik

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

Operationale vs. denotationale Semantik

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

Äquivalenz operationale und denotationale Semantik

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

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

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

- Beweis Prinzip?

Induktionsprinzip

Noether'sche Induktion

Sei $\succ$ eine **wohlfundierte Ordnung** über S und P eine Aussage über Elemente von S. Dann gilt

$$\frac{\forall v \in S.(\forall u \in S. v \succ u \wedge P(u)) \Rightarrow P(v)}{\forall x \in S. P(x)}$$

- Eine binäre Relation $\succ \subseteq S \times S$ ist eine Ordnung wenn gilt

$$\forall x \in S. x \not\succ x \qquad (\textit{irreflexiv})$$
$$\forall x, y \in S. x \succ y \Rightarrow y \not\succ x \qquad (\textit{assymetrisch})$$
$$\forall x, y, z \in S.(x \succ y \wedge y \succ z) \Rightarrow x \succ z \qquad (\textit{transitiv})$$

- Eine Ordnung $\prec$ ist wohlfundiert, wenn es keine unendlich **absteigenden** Ketten gibt

$$a_1 \succ a_2 \succ a_3 \succ \ldots$$

	S	$\succ$
Mathematische Induktion	$\mathbb{N}$	$n \rightarrow n+1$
Strukturelle Induktion **Aexp**	**Aexp**	$a \succ a'$ genau dann, wenn a' ist Teilausdruck von a

Arbeitsblatt 4.1: Übung zu struktureller Ordnung

Die strukturelle Ordnung auf arithmetischen Ausdrücken ist definiert als:

$$\forall a, a' \in \textbf{AExp}. a \succ a' \Leftrightarrow a' \text{ ist Teilausdruck von } a$$

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

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

- Argumentiert/beweist, dass die Relation "Teilausdruck-von"
  1. irreflexiv
  2. assymmetrisch und
  3. transitiv

  ist.

Besprechung

Argumentiert/beweist, die Relation "Teilausdruck-von" ist

1. irreflexiv Für Variablen und Zahlen gilt es nicht.

$$\begin{aligned} &(a_1 \circ a_2) \text{ Teilausdruck-von}(a_1 \circ a_2) \\ \Leftrightarrow &(a_1 \circ a_2) = a_1 \vee (a_1 \circ a_2) \text{ Teilausdruck-von } a_1 \qquad \text{Widerspruch} \end{aligned}$$

2. assymmetrisch

$$\begin{aligned} &(a_1 \circ a_2) \text{ Teilausdruck-von}(a'_1 \circ a'_2) \\ \wedge &(a'_1 \circ a'_2) \text{ Teilausdruck-von}(a_1 \circ a_2) \\ \Leftrightarrow &[(a_1 \circ a_2) \text{ Teilausdruck-von } a'_1 \\ &\vee (a_1 \circ a_2) \text{ Teilausdruck-von } a'_2] \\ &\wedge [(a'_1 \circ a'_2) \text{ Teilausdruck-von } a_1 \\ &\vee (a'_1 \circ a'_2) \text{ Teilausdruck-von } a_2] \end{aligned}$$

Besprechung

Argumentiert/beweist, die Relation "Teilausdruck-von" ist

3. transitiv

$$a \text{ Teilausdruck-von}(a_1 \circ a_2) \wedge (a_1 \circ a_2) \text{ Teilausdruck-von}(a_1' \circ a_2')$$

$\Leftrightarrow$

1. Fall: $a = a_1 \vee a$ Teilausdruck-von $a_1 \Rightarrow a$ Teilausdruck-von$(a_1' \circ a_2')$
2. Fall: $a = a_2 \vee a$ Teilausdruck-von $a_2 \Rightarrow a$ Teilausdruck-von$(a_1' \circ a_2')$

Äquivalenz operationale und denotationale Semantik

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

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

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

Beweis $\forall a \in \textbf{Aexp}. \forall n \in \mathbb{Z}. \forall \sigma. \quad \langle a, \sigma \rangle \rightarrow_{Aexp} n \Leftrightarrow (\sigma, n) \in [\![a]\!]_{\mathcal{A}}$
$\wedge \quad \langle a, \sigma \rangle \rightarrow_{Aexp} \perp \Leftrightarrow \sigma \notin \textbf{Dom}([\![a]\!]_{\mathcal{A}})$

Induktionsanfänge

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

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

- $a \equiv X \in$ **Loc**:
  1. $X \in Dom(\sigma)$:

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

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

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

Beweis $\forall a \in \textbf{Aexp}. \forall n \in \mathbb{Z}. \forall \sigma. \quad \langle a, \sigma \rangle \rightarrow_{Aexp} n \Leftrightarrow (\sigma, n) \in [\![a]\!]_{\mathcal{A}}$
$\wedge \quad \langle a, \sigma \rangle \rightarrow_{Aexp} \perp \Leftrightarrow \sigma \notin \textbf{Dom}([\![a]\!]_{\mathcal{A}})$

Induktionsschritte

- $a \equiv a_1 + a_2$:
  1. Fall: $m \neq \perp$ und $n \neq \perp$

     Es gilt

$$[\![a_1 + a_2]\!]_{\mathcal{A}} = \{(\sigma', u + v) | (\sigma', u) \in [\![a_1]\!]_{\mathcal{A}} \text{ und } (\sigma', v) \in [\![a_2]\!]_{\mathcal{A}}\}$$

Induktionsannahme gilt für a_1 und a_2.

$$\begin{array}{ccc}
\langle a_1 + a_2, \sigma \rangle \rightarrow_{Aexp} m + n & & \\
\Updownarrow \scriptstyle(\text{Def. } \langle .,. \rangle \rightarrow_{Aexp}) & & \\
\langle a_1, \sigma \rangle \rightarrow_{Aexp} m & \xLeftrightarrow{\text{IA fuer } a_1} & (\sigma, m) \in [\![a_1]\!]_{\mathcal{A}} \\
\& & & \& \\
\langle a_2, \sigma \rangle \rightarrow_{Aexp} n & \xLeftrightarrow{\text{IA fuer } a_2} & (\sigma, n) \in [\![a_2]\!]_{\mathcal{A}} \\
 & & \Updownarrow \scriptstyle(Def\, [\![.]\!]_{\mathcal{A}}) \\
 & & (\sigma, m + n) \in [\![a_1 + a_2]\!]_{\mathcal{A}}
\end{array}$$

Beweis $\forall a \in \textbf{Aexp}. \forall n \in \mathbb{Z}. \forall \sigma. \quad \langle a, \sigma \rangle \rightarrow_{Aexp} n \Leftrightarrow (\sigma, n) \in [\![a]\!]_{\mathcal{A}}$
$\wedge \quad \langle a, \sigma \rangle \rightarrow_{Aexp} \perp \Leftrightarrow \sigma \notin \textbf{Dom}([\![a]\!]_{\mathcal{A}})$

Induktionsschritte

- $a \equiv a_1 + a_2$: Induktionsannahme gilt für a_1 und a_2.
  2. Fall: $m = \perp$ oder $n = \perp$

$$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n \qquad \langle a_2, \sigma \rangle \rightarrow_{Aexp} m \qquad m = \perp \text{ oder } n = \perp}{\langle a_1 + a_2, \sigma \rangle \rightarrow_{Aexp} \perp}$$

  - Fall $n = \perp$.
    Aus Induktionsannahme folgt, dass $\langle a_1, \sigma \rangle \rightarrow_{Aexp} \perp \Leftrightarrow \sigma \notin Dom([\![a_1]\!]_{\mathcal{A}})$.
    Weiterhin gilt

$$[\![a_1 + a_2]\!]_{\mathcal{A}} = \{(\sigma', u + v) | (\sigma', u) \in [\![a_1]\!]_{\mathcal{A}} \text{ und } (\sigma', v) \in [\![a_2]\!]_{\mathcal{A}}\}$$

    Somit gilt $\sigma \notin Dom([\![a_1 + a_2]\!]_{\mathcal{A}})$.
  - Fall $n \neq \perp, m = \perp$: analog.

Beweis $\forall a \in \textbf{Aexp}. \forall n \in \mathbb{Z}. \forall \sigma. \quad \langle a, \sigma \rangle \rightarrow_{Aexp} n \Leftrightarrow (\sigma, n) \in [\![a]\!]_{\mathcal{A}}$
$\wedge \quad \langle a, \sigma \rangle \rightarrow_{Aexp} \perp \Leftrightarrow \sigma \notin \textbf{Dom}([\![a]\!]_{\mathcal{A}})$

Induktionsschritte

- $a \equiv a_1 / a_2$:
  1. Fall: $m \neq \perp$ und $n \neq \perp$, $n \neq 0$

     Es gilt

$$[\![a_1 / a_2]\!]_{\mathcal{A}} = \{(\sigma', u / v) | (\sigma', u) \in [\![a_1]\!]_{\mathcal{A}}, (\sigma', v) \in [\![a_2]\!]_{\mathcal{A}} \text{ und } v \neq 0\}$$

Induktionsannahme gilt für a_1 und a_2.

$$\begin{array}{ccc}
\langle a_1 / a_2, \sigma \rangle \rightarrow_{Aexp} m / n & & \\
\Updownarrow \scriptstyle(\text{Def. } \langle .,. \rangle \rightarrow_{Aexp}) & & \\
\langle a_1, \sigma \rangle \rightarrow_{Aexp} m & \xLeftrightarrow{\text{IA fuer } a_1} & (\sigma, m) \in [\![a_1]\!]_{\mathcal{A}} \\
\& & & \& \\
\langle a_2, \sigma \rangle \rightarrow_{Aexp} n & \xLeftrightarrow{\text{IA fuer } a_2} & (\sigma, n) \in [\![a_2]\!]_{\mathcal{A}} \\
 & & \Updownarrow \scriptstyle(Def\, [\![.]\!]_{\mathcal{A}}) \\
 & & (\sigma, m + n) \in [\![a_1 / a_2]\!]_{\mathcal{A}}
\end{array}$$

Beweis $\forall a \in \textbf{Aexp}. \forall n \in \mathbb{Z}. \forall \sigma. \quad \langle a, \sigma \rangle \rightarrow_{Aexp} n \Leftrightarrow (\sigma, n) \in [\![a]\!]_{\mathcal{A}}$
$\wedge \quad \langle a, \sigma \rangle \rightarrow_{Aexp} \perp \Leftrightarrow \sigma \notin \textbf{Dom}([\![a]\!]_{\mathcal{A}})$

Induktionsschritte

- $a \equiv a_1 / a_2$: Induktionsannahme gilt für a_1 und a_2.
  2. Fall:

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

  - Fall $n = 0$.
    Aus Induktionsannahme folgt, dass $\langle a_2, \sigma \rangle \rightarrow_{Aexp} 0 \Leftrightarrow (\sigma, 0) \in [\![a_2]\!]_{\mathcal{A}}$.
    Weiterhin gilt

$$[\![a_1 / a_2]\!]_{\mathcal{A}} = \{(\sigma', u / v) | (\sigma', u) \in [\![a_1]\!]_{\mathcal{A}}, (\sigma', v) \in [\![a_2]\!]_{\mathcal{A}} \text{ und } v \neq 0\}$$

    Somit gilt $\sigma \notin Dom([\![a_1 / a_2]\!]_{\mathcal{A}})$.
  - Fall $n = \perp, m = \perp$: analog wie bei $+$

q.e.d.

Operationale vs. denotationale Semantik

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

Operationale vs. denotationale Semantik

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

Operationale vs. denotationale Semantik

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

Äquivalenz operationale und denotationale Semantik

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

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

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

Beweis $\forall a \in \mathbf{Bexp}.\forall n \in \mathbb{Z}.\forall \sigma.\quad \langle b,\sigma\rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma,t) \in [\![b]\!]_{\mathcal{B}} \wedge \langle b,\sigma\rangle \rightarrow_{Bexp} \bot \Leftrightarrow \sigma \notin \mathbf{Dom}([\![b]\!]_{\mathcal{B}})$

Induktionsanfänge

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

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

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

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

Beweis $\forall a \in \mathbf{Bexp}.\forall n \in \mathbb{Z}.\forall \sigma.\quad \langle b,\sigma\rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma,t) \in [\![b]\!]_{\mathcal{B}} \wedge \langle b,\sigma\rangle \rightarrow_{Bexp} \bot \Leftrightarrow \sigma \notin \mathbf{Dom}([\![b]\!]_{\mathcal{B}})$

Induktionsschritte

- $b \equiv b_1 \&\& b_2$:
  Es gilt

$$[\![b_1 \&\& b_2]\!]_{\mathcal{B}} = \{(\sigma', false) \mid (\sigma', false) \in [\![b_1]\!]_{\mathcal{B}}\} \cup \{(\sigma', t_2) \mid (\sigma', true) \in [\![b_1]\!]_{\mathcal{B}} \text{ und } (\sigma', t_2) \in [\![b_2]\!]_{\mathcal{B}}\}$$

  Induktionsannahme gilt für b_1 und b_2.
  - Fall $\langle b_1,\sigma\rangle \rightarrow_{Bexp} \bot$

$$\begin{array}{ccc}\langle b_1 \&\& b_2,\sigma\rangle \rightarrow_{Bexp} \bot & & \\ \Updownarrow \text{(Def. } \langle\cdot,\cdot\rangle \rightarrow_{Bexp}) & & \\ \langle b_1,\sigma\rangle \rightarrow_{Bexp} \bot & \xLeftrightarrow{\text{IA fuer } b_1} & \sigma \notin Dom([\![b_1]\!]_{\mathcal{B}}) \\ & & \Downarrow \text{Def. } [\![.]\!]_{\mathcal{B}} \\ & & \sigma \notin [\![b_1 \&\& b_2]\!]_{\mathcal{B}}\end{array}$$

Beweis $\forall a \in \mathbf{Bexp}.\forall n \in \mathbb{Z}.\forall \sigma.\quad \langle b,\sigma\rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma,t) \in [\![b]\!]_{\mathcal{B}} \wedge \langle b,\sigma\rangle \rightarrow_{Bexp} \bot \Leftrightarrow \sigma \notin \mathbf{Dom}([\![b]\!]_{\mathcal{B}})$

Induktionsschritte

- $b \equiv b_1 \&\& b_2$:
  Es gilt

$$[\![b_1 \&\& b_2]\!]_{\mathcal{B}} = \{(\sigma', false) \mid (\sigma', false) \in [\![b_1]\!]_{\mathcal{B}}\} \cup \{(\sigma', t_2) \mid (\sigma', true) \in [\![b_1]\!]_{\mathcal{B}} \text{ und } (\sigma', t_2) \in [\![b_2]\!]_{\mathcal{B}}\}$$

  Induktionsannahme gilt für b_1 und b_2.
  - Fall $\langle b_1,\sigma\rangle \rightarrow_{Bexp} false$

$$\begin{array}{ccc}\langle b_1 \&\& b_2,\sigma\rangle \rightarrow_{Bexp} false & & \\ \Updownarrow \text{(Def. } \langle\cdot,\cdot\rangle \rightarrow_{Bexp}) & & \\ \langle b_1,\sigma\rangle \rightarrow_{Bexp} false & \xLeftrightarrow{\text{IA fuer } b_1} & (\sigma, false) \in [\![b_1]\!]_{\mathcal{B}} \\ & & \Downarrow \text{Def. } [\![.]\!]_{\mathcal{B}} \\ & & (\sigma, false) \in [\![b_1 \&\& b_2]\!]_{\mathcal{B}}\end{array}$$

Beweis $\forall a \in \mathbf{Bexp}.\forall n \in \mathbb{Z}.\forall \sigma.\quad \langle b,\sigma\rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma,t) \in [\![b]\!]_{\mathcal{B}} \wedge \langle b,\sigma\rangle \rightarrow_{Bexp} \bot \Leftrightarrow \sigma \notin \mathbf{Dom}([\![b]\!]_{\mathcal{B}})$

Induktionsschritte

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

$$[\![b_1 \&\& b_2]\!]_{\mathcal{B}} = \{(\sigma', false) \mid (\sigma', false) \in [\![b_1]\!]_{\mathcal{B}}\} \cup \{(\sigma', t_2) \mid (\sigma', true) \in [\![b_1]\!]_{\mathcal{B}} \text{ und } (\sigma', t_2) \in [\![b_2]\!]_{\mathcal{B}}\}$$

  Induktionsannahme gilt für b_1 und b_2.
  - Fall $\langle b_1,\sigma\rangle \rightarrow_{Bexp} true, \langle b_2,\sigma\rangle \rightarrow_{Bexp} false$

$$\begin{array}{ccc}\langle b_1 \&\& b_2,\sigma\rangle \rightarrow_{Bexp} false & & \\ \Updownarrow \text{(Def. } \langle\cdot,\cdot\rangle \rightarrow_{Bexp}) & & \\ \langle b_1,\sigma\rangle \rightarrow_{Bexp} true & \xLeftrightarrow{\text{IA fuer } b_1} & (\sigma, true) \in [\![b_1]\!]_{\mathcal{B}} \\ \& & & \& \\ \langle b_2,\sigma\rangle \rightarrow_{Bexp} false & \xLeftrightarrow{\text{IA fuer } b_2} & (\sigma, false) \in [\![b_2]\!]_{\mathcal{B}} \\ & & \Downarrow \text{Def. } [\![.]\!]_{\mathcal{B}} \\ & & (\sigma, false) \in [\![b_1 \&\& b_2]\!]_{\mathcal{B}}\end{array}$$

Beweis $\forall a \in \mathbf{Bexp}.\forall n \in \mathbb{Z}.\forall \sigma.\quad \langle b,\sigma\rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma,t) \in [\![b]\!]_{\mathcal{B}} \wedge \langle b,\sigma\rangle \rightarrow_{Bexp} \bot \Leftrightarrow \sigma \notin \mathbf{Dom}([\![b]\!]_{\mathcal{B}})$

Induktionsschritte

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

$$[\![b_1 \&\& b_2]\!]_{\mathcal{B}} = \{(\sigma', false) \mid (\sigma', false) \in [\![b_1]\!]_{\mathcal{B}}\} \cup \{(\sigma', t_2) \mid (\sigma', true) \in [\![b_1]\!]_{\mathcal{B}} \text{ und } (\sigma', t_2) \in [\![b_2]\!]_{\mathcal{B}}\}$$

  Induktionsannahme gilt für b_1 und b_2.
  - Fall $\langle b_1,\sigma\rangle \rightarrow_{Bexp} true, \langle b_2,\sigma\rangle \rightarrow_{Bexp} true$

$$\begin{array}{ccc}\langle b_1 \&\& b_2,\sigma\rangle \rightarrow_{Bexp} true & & \\ \Updownarrow \text{(Def. } \langle\cdot,\cdot\rangle \rightarrow_{Bexp}) & & \\ \langle b_1,\sigma\rangle \rightarrow_{Bexp} true & \xLeftrightarrow{\text{IA fuer } b_1} & (\sigma, true) \in [\![b_1]\!]_{\mathcal{B}} \\ \& & & \& \\ \langle b_2,\sigma\rangle \rightarrow_{Bexp} true & \xLeftrightarrow{\text{IA fuer } b_2} & (\sigma, true) \in [\![b_2]\!]_{\mathcal{B}} \\ & & \Updownarrow \text{Def. } [\![.]\!]_{\mathcal{B}} \\ & & (\sigma, true) \in [\![b_1 \&\& b_2]\!]_{\mathcal{B}}\end{array}$$

Beweis $\forall a \in \mathbf{Bexp}.\forall n \in \mathbb{Z}.\forall \sigma.\quad \langle b,\sigma\rangle \to_{Bexp} t \Leftrightarrow (\sigma,t) \in [\![b]\!]_\mathcal{B}$
$\qquad\wedge\quad \langle b,\sigma\rangle \to_{Bexp} \bot \Leftrightarrow \sigma \notin \mathit{Dom}([\![b]\!]_\mathcal{B})$

Induktionsschritte

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

$$[\![b_1\&\&b_2]\!]_\mathcal{B} = \{(\sigma',\mathit{false}) | (\sigma',\mathit{false}) \in [\![b_1]\!]_\mathcal{B}\} \cup \{(\sigma',t_2) | (\sigma',\mathit{true}) \in [\![b_1]\!]_\mathcal{B} \text{ und } (\sigma',t_2) \in [\![b_2]\!]_\mathcal{B}\}$$

Induktionsannahme gilt für b_1 und b_2.

- Fall $\langle b_1,\sigma\rangle \to_{Bexp} \mathit{true}, \langle b_2,\sigma\rangle \to_{Bexp} \bot$

$\langle b_1\&\&b_2,\sigma\rangle \to_{Bexp} \bot$

$\Updownarrow$ (Def. $\langle .,.\rangle \to_{Bexp}$)

$\langle b_1,\sigma\rangle \to_{Bexp} \mathit{true} \overset{\text{IA fuer } b_1}{\Longleftrightarrow} (\sigma,\mathit{true}) \in [\![b_1]\!]_\mathcal{B}$

& &

$\langle b_2,\sigma\rangle \to_{Bexp} \bot \overset{\text{IA fuer } b_2}{\Longleftrightarrow} \sigma \notin \mathit{Dom}([\![b_2]\!]_\mathcal{B})$

$\Downarrow$ Def. $[\![.]\!]_\mathcal{B}$

$\sigma \notin \mathit{Dom}([\![b_1\&\&b_2]\!]_\mathcal{B})$

Beweis $\forall a \in \mathbf{Bexp}.\forall n \in \mathbb{Z}.\forall \sigma.\quad \langle b,\sigma\rangle \to_{Bexp} t \Leftrightarrow (\sigma,t) \in [\![b]\!]_\mathcal{B}$
$\qquad\wedge\quad \langle b,\sigma\rangle \to_{Bexp} \bot \Leftrightarrow \sigma \notin \mathit{Dom}([\![b]\!]_\mathcal{B})$

- $(\sigma,\mathit{true}) \in [\![b_1\&\&b_2]\!]_\mathcal{B} \overset{\text{Def. } [\![.]\!]_\mathcal{B}}{\Longleftrightarrow} (\sigma,\mathit{true}) \in [\![b_1]\!]_\mathcal{B}$ und $(\sigma,\mathit{true}) \in [\![b_2]\!]_\mathcal{B}$
  - Siehe Folie 24
- $(\sigma,\mathit{false}) \in [\![b_1\&\&b_2]\!]_\mathcal{B} \overset{\text{Def. } [\![.]\!]_\mathcal{B}}{\Longleftrightarrow} (\sigma,\mathit{false}) \in [\![b_1]\!]_\mathcal{B}$ oder $(\sigma,\mathit{true}) \in [\![b_1]\!]_\mathcal{B}$ und $(\sigma,\mathit{false}) \in [\![b_2]\!]_\mathcal{B}$
  - Siehe Folie 22 und 23
- $\sigma \notin \mathit{Dom}([\![b_1\&\&b_2]\!]_\mathcal{B}) \overset{\text{Def. } [\![.]\!]_\mathcal{B}}{\Longleftrightarrow} \sigma \notin \mathit{Dom}([\![b_1]\!]_\mathcal{B})$ oder $\sigma \notin \mathit{Dom}([\![b_2]\!]_\mathcal{B})$
  - Siehe Folie 21 und 25

Somit gilt dann auch $\Leftrightarrow$ *q.e.d.*

Arbeitsblatt 4.2: Beweis Induktionsanfang

1. $\langle a_1 == a_2,\sigma\rangle \to_{Bexp} \mathbf{\mathit{false}} \Leftrightarrow (\sigma,\mathbf{\mathit{false}}) \in [\![a_1 == a_2]\!]_\mathcal{B}$
2. $\langle a_1 == a_2,\sigma\rangle \to_{Bexp} \mathbf{\mathit{true}} \Leftrightarrow (\sigma,\mathbf{\mathit{true}}) \in [\![a_1 == a_2]\!]_\mathcal{B}$
3. $\langle a_1 == a_2,\sigma\rangle \to_{Bexp} \bot \Leftrightarrow \sigma \notin \mathbf{\mathit{Dom}}([\![a_1 == a_2]\!]_\mathcal{B})$

Beweist obige drei Aussagen unter Verwendung des für arithmetische Ausdrücke geltenden Lemmas

$$\forall a \in \mathbf{Aexp}.\forall n \in \mathbb{Z}.\forall \sigma.\quad \langle a,\sigma\rangle \to_{Aexp} n \Leftrightarrow (\sigma,n) \in [\![a]\!]_\mathcal{A} \quad\wedge\quad \langle b,\sigma\rangle \to_{Bexp} \bot \Leftrightarrow \sigma \notin \mathit{Dom}([\![a]\!]_\mathcal{A})$$

Beweis
1. $\langle a_1 == a_2,\sigma\rangle \to_{Bexp} \mathbf{\mathit{false}} \Leftrightarrow (\sigma,\mathbf{\mathit{false}}) \in [\![a_1 == a_2]\!]_\mathcal{B}$
2. $\langle a_1 == a_2,\sigma\rangle \to_{Bexp} \mathbf{\mathit{true}} \Leftrightarrow (\sigma,\mathbf{\mathit{true}}) \in [\![a_1 == a_2]\!]_\mathcal{B}$
3. $\langle a_1 == a_2,\sigma\rangle \to_{Bexp} \bot \Leftrightarrow \sigma \notin \mathbf{\mathit{Dom}}([\![a_1 == a_2]\!]_\mathcal{B})$

$$[\![a_1 == a_2]\!]_\mathcal{B} = \{(\sigma',\mathit{true}) | (\sigma',m) \in [\![a_1]\!]_\mathcal{A}, (\sigma',n) \in [\![a_2]\!]_\mathcal{A}, m = n\} \cup \{(\sigma',\mathit{false}) | (\sigma',m) \in [\![a_1]\!]_\mathcal{A}, (\sigma',n) \in [\![a_2]\!]_\mathcal{A}, m \neq n\}$$

- Fall $\langle a_1,\sigma\rangle \to_{Bexp} m, \langle b_2,\sigma\rangle \to_{Bexp} n, m = n$

$\langle a_1 == a_2,\sigma\rangle \to_{Bexp} \mathit{true}$

$\Updownarrow$ (Def. $\langle .,.\rangle \to_{Bexp}$)

$\langle a_1,\sigma\rangle \to_{Bexp} m \overset{\text{IA fuer } a_1}{\Longleftrightarrow} (\sigma,m) \in [\![a_2]\!]_\mathcal{A}$

& &

$\langle a_2,\sigma\rangle \to_{Bexp} m \overset{\text{IA fuer } a_2}{\Longleftrightarrow} (\sigma,m) \in [\![a_1]\!]_\mathcal{A}$

$\Updownarrow$ Def. $[\![.]\!]_\mathcal{B}$

$(\sigma,\mathit{true}) [\![a_1 == a_2]\!]_\mathcal{B}$

Beweis
1. $\langle a_1 == a_2,\sigma\rangle \to_{Bexp} \mathbf{\mathit{false}} \Leftrightarrow (\sigma,\mathbf{\mathit{false}}) \in [\![a_1 == a_2]\!]_\mathcal{B}$
2. $\langle a_1 == a_2,\sigma\rangle \to_{Bexp} \mathbf{\mathit{true}} \Leftrightarrow (\sigma,\mathbf{\mathit{true}}) \in [\![a_1 == a_2]\!]_\mathcal{B}$
3. $\langle a_1 == a_2,\sigma\rangle \to_{Bexp} \bot \Leftrightarrow \sigma \notin \mathbf{\mathit{Dom}}([\![a_1 == a_2]\!]_\mathcal{B})$

$$[\![a_1 == a_2]\!]_\mathcal{B} = \{(\sigma',\mathit{true}) | (\sigma',m) \in [\![a_1]\!]_\mathcal{A}, (\sigma',n) \in [\![a_2]\!]_\mathcal{A}, m = n\} \cup \{(\sigma',\mathit{false}) | (\sigma',m) \in [\![a_1]\!]_\mathcal{A}, (\sigma',n) \in [\![a_2]\!]_\mathcal{A}, m \neq n\}$$

- Fall $\langle a_1,\sigma\rangle \to_{Bexp} m, \langle b_2,\sigma\rangle \to_{Bexp} n, m \neq n$

$\langle a_1 == a_2,\sigma\rangle \to_{Bexp} \mathit{false}$

$\Updownarrow$ (Def. $\langle .,.\rangle \to_{Bexp}$)

$\langle a_1,\sigma\rangle \to_{Aexp} m \overset{\text{Lemma fuer } a_1}{\Longleftrightarrow} (\sigma,m) \in [\![a_1]\!]_\mathcal{A}$

& &

$\langle a_2,\sigma\rangle \to_{Aexp} n \overset{\text{Lemma fuer } a_2}{\Longleftrightarrow} (\sigma,n) \in [\![a_2]\!]_\mathcal{A}$

$\Updownarrow$ Def. $[\![.]\!]_\mathcal{B}$

$(\sigma,\mathit{false}) [\![a_1 == a_2]\!]_\mathcal{B}$

Beweis
1. $\langle a_1 == a_2,\sigma\rangle \to_{Bexp} \mathbf{\mathit{false}} \Leftrightarrow (\sigma,\mathbf{\mathit{false}}) \in [\![a_1 == a_2]\!]_\mathcal{B}$
2. $\langle a_1 == a_2,\sigma\rangle \to_{Bexp} \mathbf{\mathit{true}} \Leftrightarrow (\sigma,\mathbf{\mathit{true}}) \in [\![a_1 == a_2]\!]_\mathcal{B}$
3. $\langle a_1 == a_2,\sigma\rangle \to_{Bexp} \bot \Leftrightarrow \sigma \notin \mathbf{\mathit{Dom}}([\![a_1 == a_2]\!]_\mathcal{B})$

$$[\![a_1 == a_2]\!]_\mathcal{B} = \{(\sigma',\mathit{true}) | (\sigma',m) \in [\![a_1]\!]_\mathcal{A}, (\sigma',n) \in [\![a_1]\!]_\mathcal{A}, m = n\} \cup \{(\sigma',\mathit{false}) | (\sigma',m) \in [\![a_1]\!]_\mathcal{A}, (\sigma',n) \in [\![a_2]\!]_\mathcal{A}, m \neq n\}$$

- Fall $\langle a_1,\sigma\rangle \to_{Bexp} \bot$:

$\langle a_1 == a_2,\sigma\rangle \to_{Bexp} \bot$

$\Updownarrow$ (Def. $\langle .,.\rangle \to_{Bexp}$)

$\langle a_1,\sigma\rangle \to_{Aexp} \bot \overset{\text{Lemma fuer } a}{\Longleftrightarrow} \sigma \notin \mathit{Dom}([\![a_1]\!]_\mathcal{A})$

& $\Downarrow$ Def. $[\![.]\!]_\mathcal{B}$

$\sigma \notin \mathit{Dom}([\![a_1 == a_2]\!]_\mathcal{B})$

- Fall $\langle a_2,\sigma\rangle \to_{Bexp} \bot$:

$\langle a_1 == a_2,\sigma\rangle \to_{Bexp} \bot$

$\Updownarrow$ (Def. $\langle .,.\rangle \to_{Bexp}$)

$\langle a_2,\sigma\rangle \to_{Aexp} \bot \overset{\text{Lemma fuer } a}{\Longleftrightarrow} \sigma \notin \mathit{Dom}([\![a_2]\!]_\mathcal{A})$

& $\Downarrow$ Def. $[\![.]\!]_\mathcal{B}$

$\sigma \notin \mathit{Dom}([\![a_1 == a_2]\!]_\mathcal{B})$

- $\sigma \notin \mathit{Dom}([\![a_1 == a_2]\!]_\mathcal{B}) \overset{\text{Def. } [\![.]\!]_\mathcal{B}}{\Longleftrightarrow} \sigma \notin \mathit{Dom}([\![a_1]\!]_\mathcal{A})$ oder $\sigma \notin \mathit{Dom}([\![a_2]\!]_\mathcal{A})$
  - Siehe die beiden Fälle auf den beiden vorangegangenen Folien.

Operationale vs. denotationale Semantik

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

Operationale vs. denotationale Semantik

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

Operationale vs. denotationale Semantik

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

$$\frac{\langle b, \sigma\rangle \rightarrow_{Bexp} \mathit{true} \quad \langle c, \sigma\rangle \rightarrow_{Stmt} \sigma' \neq \bot \quad \langle w, \sigma'\rangle \rightarrow_{Stmt} \sigma''}{\langle w, \sigma\rangle \rightarrow_{Stmt} \sigma''}$$

$$\frac{\langle b, \sigma\rangle \rightarrow_{Bexp} \mathit{true} \quad \langle c, \sigma\rangle \rightarrow_{Stmt} \bot}{\langle w, \sigma\rangle \rightarrow_{Stmt} \bot}$$

mit

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

Äquivalenz operationale und denotationale Semantik

- Für alle $c \in$ **Stmt**, für alle Zustände σ, σ':

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

- $\Rightarrow$ Beweis Prinzip?
- $\Leftarrow$ Beweis Prinzip?

Operationale Semantik: C0 Programme

- **Stmt** c ::= **Idt** = **Exp** | **if** (b) c_1 **else** c_2 | **while** (b) c | $c_1; c_2$ | { }

Regeln:

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

$$\frac{\langle a, \sigma\rangle \rightarrow_{Aexp} n \in \mathbb{Z}}{\langle x = a, \sigma\rangle \rightarrow_{Stmt} \sigma[n/x]} \qquad \frac{\langle a, \sigma\rangle \rightarrow_{Aexp} \bot}{\langle x = a, \sigma\rangle \rightarrow_{Stmt} \bot}$$

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

$$\frac{\langle c_1, \sigma\rangle \rightarrow_{Stmt} \bot}{\langle c_1; c_2, \sigma\rangle \rightarrow_{Stmt} \bot}$$

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

Operationale Semantik: C0 Programme

- **Stmt** c ::= **Idt** = **Exp** | **if** (b) c_1 **else** c_2 | **while** (b) c | $c_1; c_2$ | { }

Regeln:

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

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

$$\frac{\langle b, \sigma\rangle \rightarrow_{Bexp} \bot}{\langle \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2, \sigma\rangle \rightarrow_{Stmt} \bot}$$

Operationale Semantik: C0 Programme

- **Stmt** c ::= **Idt** = **Exp** | **if** (b) c_1 **else** c_2 | **while** (b) c | $c_1; c_2$ | { }

Regeln:

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

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

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

Ableitungstiefe für Programme

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

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

Operationale Semantik: C0 Programme

- **Stmt** c ::= **Idt** = **Exp** | **if** (b) c_1 **else** c_2 | **while** (b) c | $c_1; c_2$ | { }

Regeln:	**Programmstruktur**	**Ableitungstiefe**
$\dfrac{\langle c_1, \sigma\rangle \rightarrow_{Stmt} \sigma' \neq \bot \quad \langle c_2, \sigma'\rangle \rightarrow_{Stmt} \sigma'' \neq \bot}{\langle c_1; c_2, \sigma\rangle \rightarrow_{Stmt} \sigma''}$	↘	↘
$\dfrac{\langle b, \sigma\rangle \rightarrow_{Bexp} \mathit{true} \quad \langle c_1, \sigma\rangle \rightarrow_{Stmt} \sigma'}{\langle \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2, \sigma\rangle \rightarrow_{Stmt} \sigma'}$	↘	↘
$\dfrac{\langle b, \sigma\rangle \rightarrow_{Bexp} \mathit{false} \quad \langle c_2, \sigma\rangle \rightarrow_{Stmt} \sigma'}{\langle \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2, \sigma\rangle \rightarrow_{Stmt} \sigma'}$	↘	↘
$\dfrac{\langle b, \sigma\rangle \rightarrow_{Bexp} \mathit{true} \quad \langle c, \sigma\rangle \rightarrow_{Stmt} \sigma' \quad \langle \textbf{while}\ (b)\ c, \sigma'\rangle \rightarrow_{Stmt} \sigma''}{\langle \textbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma''}$	→	↘
$\dfrac{\langle b, \sigma\rangle \rightarrow_{Bexp} \mathit{true} \quad \langle c, \sigma\rangle \rightarrow_{Stmt} \bot}{\langle \textbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \bot}$	↘	↘

Äquivalenz operationale und denotationale Semantik

- Für alle $c \in$ **Stmt**, für alle Zustände σ, σ':

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

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

Beweis $\forall c \in \textbf{Stmt}.\forall \sigma, \sigma'.$ 1. $\langle c, \sigma\rangle \to_{Stmt} \sigma' \Rightarrow (\sigma, \sigma') \in \llbracket c \rrbracket_{\mathcal{C}}$
2. $\langle c, \sigma\rangle \to_{Stmt} \bot \Rightarrow \sigma \notin \textit{Dom}(\llbracket c \rrbracket_{\mathcal{C}})$

Induktionsanfang – Ableitungstiefe 1

- Fall $c \equiv x = a$:

$$\llbracket x = a \rrbracket_{\mathcal{C}} = \{(\sigma, \sigma[m/x]) | (\sigma, m) \in \llbracket a \rrbracket_{\mathcal{A}}\}$$

- Fall $\langle a, \sigma\rangle \to_{Aexp} m \in \mathbb{Z}$

$$\langle x = a, \sigma\rangle \to_{Stmt} \sigma[m/x]$$
$$\Updownarrow (\text{Def. } \langle .,.\rangle \to_{Stmt} .)$$
$$\langle a, \sigma\rangle \to_{Aexp} m \in \mathbb{Z} \overset{\text{Lemma fuer } a}{\Longleftrightarrow} (\sigma, m) \in \llbracket a \rrbracket_{\mathcal{A}}$$
$$\Downarrow \text{Def. } \llbracket . \rrbracket_{\mathcal{C}}$$
$$(\sigma, \sigma[m/x]) \in \llbracket x = a \rrbracket_{\mathcal{C}}$$

- Fall $\langle a, \sigma\rangle \to_{Aexp} \bot$:

$$\langle x = a, \sigma\rangle \to_{Stmt} \bot$$
$$\Updownarrow (\text{Def. } \langle .,.\rangle \to_{Stmt} .)$$
$$\langle a, \sigma\rangle \to_{Aexp} \bot \overset{\text{Lemma fuer } a}{\Longleftrightarrow} \sigma \notin \textit{Dom}(\llbracket a \rrbracket_{\mathcal{A}})$$
$$\Downarrow \text{Def. } \llbracket . \rrbracket_{\mathcal{C}}$$
$$\sigma \notin \textit{Dom}(\llbracket x = a \rrbracket_{\mathcal{C}})$$

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

Beweis $\forall c \in \textbf{Stmt}.\forall \sigma, \sigma'.$ 1. $\langle c, \sigma\rangle \to_{Stmt} \sigma' \Rightarrow (\sigma, \sigma') \in \llbracket c \rrbracket_{\mathcal{C}}$
2. $\langle c, \sigma\rangle \to_{Stmt} \bot \Rightarrow \sigma \notin \textit{Dom}(\llbracket c \rrbracket_{\mathcal{C}})$

Induktionsschritt:

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

$$\llbracket \textbf{if}(b)\ c_1\ \textbf{else}\ c_2 \rrbracket_{\mathcal{C}} = \{(\sigma, \sigma') | (\sigma, \sigma') \in \llbracket c_1 \rrbracket_{\mathcal{C}}, (\sigma, \textit{true}) \in \llbracket b \rrbracket_{\mathcal{B}}\} \cup \{(\sigma, \sigma') | (\sigma, \sigma') \in \llbracket c_2 \rrbracket_{\mathcal{C}}, (\sigma, \textit{false}) \in \llbracket b \rrbracket_{\mathcal{B}}\}$$

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

$$\langle \textbf{if}(b)\ c_1\ \textbf{else}\ c_2, \sigma\rangle \to_{Stmt} \sigma'$$
$$\Updownarrow (\text{Def. } \langle .,.\rangle \to_{Stmt} .)$$
$$\langle b, \sigma\rangle \to_{Bexp} \textit{true} \overset{\text{Lemma fuer } b}{\Longleftrightarrow} (\sigma, \textit{true}) \in \llbracket b \rrbracket_{\mathcal{B}}$$
$$\& \qquad \&$$
$$\langle c_1, \sigma\rangle \to_{Stmt} \sigma' \overset{\text{IH fuer } c_1}{\Longleftrightarrow} (\sigma, \sigma') \in \llbracket c_1 \rrbracket_{\mathcal{C}}$$
$$\Downarrow \text{Def. } \llbracket . \rrbracket_{\mathcal{C}}$$
$$(\sigma, \sigma') \in \llbracket \textbf{if}(b)\ c_1\ \textbf{else}\ c_2 \rrbracket_{\mathcal{C}}$$

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

$$\langle \textbf{if}(b)\ c_1\ \textbf{else}\ c_2, \sigma\rangle \to_{Stmt} \sigma'$$
$$\Updownarrow (\text{Def. } \langle .,.\rangle \to_{Stmt} .)$$
$$\langle b, \sigma\rangle \to_{Bexp} \textit{false} \overset{\text{Lemma fuer } b}{\Longleftrightarrow} (\sigma, \textit{false}) \in \llbracket b \rrbracket_{\mathcal{B}}$$
$$\& \qquad \&$$
$$\langle c_2, \sigma\rangle \to_{Stmt} \sigma' \overset{\text{IH fuer } c_2}{\Longleftrightarrow} (\sigma, \sigma') \in \llbracket c_2 \rrbracket_{\mathcal{C}}$$
$$\Downarrow \text{Def. } \llbracket . \rrbracket_{\mathcal{C}}$$
$$(\sigma, \sigma') \in \llbracket \textbf{if}(b)\ c_1\ \textbf{else}\ c_2 \rrbracket_{\mathcal{C}}$$

- Fall $\langle \sigma, b\rangle \to_{Bexp} \textit{true}, \langle c_1, \sigma\rangle \to_{Stmt} \bot$:

$$\langle \textbf{if}(b)\ c_1\ \textbf{else}\ c_2, \sigma\rangle \to_{Stmt} \bot$$
$$\Updownarrow (\text{Def. } \langle .,.\rangle \to_{Stmt} .)$$
$$\langle b, \sigma\rangle \to_{Bexp} \textit{true} \overset{\text{Lemma fuer } b}{\Longleftrightarrow} (\sigma, \textit{true}) \in \llbracket b \rrbracket_{\mathcal{B}}$$
$$\& \qquad \&$$
$$\langle c_1, \sigma\rangle \to_{Stmt} \bot \overset{\text{IH fuer } c_1}{\Longleftrightarrow} \sigma \notin \textit{Dom}(\llbracket c_1 \rrbracket_{\mathcal{C}})$$
$$\Downarrow \text{Def. } \llbracket . \rrbracket_{\mathcal{C}}$$
$$\sigma \notin \textit{Dom}(\llbracket \textbf{if}(b)\ c_1\ \textbf{else}\ c_2 \rrbracket_{\mathcal{C}})$$

- Fall $\langle \sigma, b\rangle \to_{Bexp} \bot$:

$$\langle \textbf{if}(b)\ c_1\ \textbf{else}\ c_2, \sigma\rangle \to_{Stmt} \bot$$
$$\Updownarrow (\text{Def. } \langle .,.\rangle \to_{Stmt} .)$$
$$\langle b, \sigma\rangle \to_{Bexp} \bot \overset{\text{Lemma fuer } b}{\Longleftrightarrow} \sigma \notin \textit{Dom}(\llbracket b \rrbracket_{\mathcal{B}})$$
$$\Downarrow \text{Def. } \llbracket . \rrbracket_{\mathcal{C}}$$
$$\sigma \notin \textit{Dom}(\llbracket \textbf{if}(b)\ c_1\ \textbf{else}\ c_2 \rrbracket_{\mathcal{C}})$$

Beweis $\forall c \in \textbf{Stmt}.\forall \sigma, \sigma'.$ 1. $\langle c, \sigma\rangle \to_{Stmt} \sigma' \Rightarrow (\sigma, \sigma') \in \llbracket c \rrbracket_{\mathcal{C}}$
2. $\langle c, \sigma\rangle \to_{Stmt} \bot \Rightarrow \sigma \notin \textit{Dom}(\llbracket c \rrbracket_{\mathcal{C}})$

Induktionsschritt:

- Fall $c \equiv \textbf{while}(b)\ c$: $\quad \llbracket \textbf{while}(b)\ c \rrbracket_{\mathcal{C}} = \textit{fix}(\Gamma)$
  - Fall $\langle b, \sigma\rangle \to_{Bexp} \textit{true}$, $\langle c, \sigma\rangle \to_{Stmt} \sigma'$, $\langle \textbf{while}(b)\ c, \sigma'\rangle \to_{Stmt} \sigma''$

$$\langle \textbf{while}(b)\ c, \sigma\rangle \to_{Stmt} \sigma''$$
$$\Updownarrow (\text{Def. } \langle .,.\rangle \to_{Stmt} .)$$
$$\langle b, \sigma\rangle \to_{Bexp} \textit{true} \overset{\text{Lemma fuer } b}{\Longleftrightarrow} (\sigma, \textit{true}) \in \llbracket b \rrbracket_{\mathcal{B}}$$
$$\& \qquad \&$$
$$\langle c, \sigma\rangle \to_{Stmt} \sigma' \overset{\text{IH fuer } \langle c,\sigma\rangle \to_{Stmt} \sigma'}{\Longleftrightarrow} (\sigma, \sigma') \in \llbracket c \rrbracket_{\mathcal{C}}$$
$$\& \qquad \&$$
$$\langle \textbf{while}(b)\ c, \sigma'\rangle \to_{Stmt} \sigma'' \overset{\text{IH fuer } \langle \textbf{while}(b)\ c,\sigma'\rangle \to_{Stmt} \sigma''}{\Longleftrightarrow} (\sigma', \sigma'') \in \llbracket \textbf{while}(b)\ c \rrbracket_{\mathcal{C}}$$
$$\Downarrow \text{Def. } \llbracket . \rrbracket_{\mathcal{C}}$$
$$(\sigma, \sigma'') \in \llbracket \textbf{while}(b)\ c \rrbracket_{\mathcal{C}}$$

Äquivalenz operationale und denotationale Semantik

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

$$\langle c, \sigma\rangle \to_{Stmt} \sigma' \Leftrightarrow (\sigma, \sigma') \in \llbracket c \rrbracket_{\mathcal{C}}$$
$$\langle c, \sigma\rangle \to_{Stmt} \bot \Rightarrow \sigma \notin \textit{Dom}(\llbracket c \rrbracket_{\mathcal{C}})$$

- $\Rightarrow$ Beweis per Induktion über **die (Tiefe der) 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 $\Gamma^i(\emptyset)$ des Fixpunkts. (Warum?)

Beweis $\forall c \in \textbf{Stmt}.\forall \sigma, \sigma'.(\sigma, \sigma') \in \llbracket c \rrbracket_{\mathcal{C}} \Rightarrow \langle c, \sigma\rangle \to_{Stmt} \sigma'$

Induktionsanfang:

- Fall $c \equiv x = a$:

$$\llbracket x = a \rrbracket_{\mathcal{C}} = \{(\sigma'', \sigma''[t/x]) | (\sigma'', t) \in \llbracket a \rrbracket_{\mathcal{A}}\}$$

$$\begin{aligned}
& (\sigma, \sigma') \in \{(\sigma'', \sigma''[t/x]) | (\sigma'', t) \in \llbracket a \rrbracket_{\mathcal{A}}\} \\
\overset{\text{Def. } \llbracket . \rrbracket_{\mathcal{C}} ..}{\Longrightarrow}\ & (\sigma, t) = \llbracket a \rrbracket_{\mathcal{A}} \wedge \sigma' = \sigma[t/x] \\
\overset{\text{Lemma } \textbf{AExp}}{\Longrightarrow}\ & \langle a, \sigma\rangle \to_{Aexp} t \wedge \sigma' = \sigma[t/x] \\
\overset{\text{Def. } \langle .,.\rangle \to_{Stmt} .}{\Longrightarrow}\ & \langle x = a, \sigma\rangle \to_{Stmt} \sigma[t/x] \wedge \sigma' = \sigma[t/x] \\
\Longrightarrow\ & \langle x = a, \sigma\rangle \to_{Stmt} \sigma'
\end{aligned}$$

- Fall $c \equiv \{\}$

$$\llbracket \{\} \rrbracket_{\mathcal{C}} = \{(\sigma, \sigma) | \sigma \in \Sigma\}$$

$$\begin{aligned}
& (\sigma, \sigma') \in \{(\sigma'', \sigma'') | \sigma'' \in \Sigma\} \\
\overset{\text{Def. } \llbracket . \rrbracket_{\mathcal{C}} ..}{\Longrightarrow}\ & \sigma = \sigma' \\
\overset{\text{Def. } \langle .,.\rangle \to_{Stmt} .}{\Longrightarrow}\ & \langle \{\}, \sigma\rangle \to_{Stmt} \sigma \wedge \sigma = \sigma' \\
\Longrightarrow\ & \langle \{\}, \sigma\rangle \to_{Stmt} \sigma'
\end{aligned}$$

Beweis $\forall c \in \textbf{Stmt}.\forall \sigma, \sigma'.(\sigma, \sigma') \in \llbracket c \rrbracket_{\mathcal{C}} \Rightarrow \langle c, \sigma\rangle \to_{Stmt} \sigma'$

Induktionsschritt:

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

$$\llbracket \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2 \rrbracket_{\mathcal{C}} = \{(\sigma'', \sigma''') | (\sigma'', \textit{true}) \in \llbracket b \rrbracket_{\mathcal{B}}, (\sigma'', \sigma''') \in \llbracket c_1 \rrbracket_{\mathcal{C}}\} \cup \{(\sigma'', \sigma''') | (\sigma'', \textit{false}) \in \llbracket b \rrbracket_{\mathcal{B}}, (\sigma'', \sigma''') \in \llbracket c_2 \rrbracket_{\mathcal{C}}\}$$

Induktionsannahme gilt für c_1 und c_2

- Fall: $(\sigma, \sigma') \in \{(\sigma'', \sigma''') | (\sigma'', \textit{true}) \in \llbracket b \rrbracket_{\mathcal{B}}, (\sigma'', \sigma''') \in \llbracket c_1 \rrbracket_{\mathcal{C}}\}$

$$\begin{aligned}
& (\sigma, \sigma') \in \{(\sigma'', \sigma''') | (\sigma'', \textit{true}) \in \llbracket b \rrbracket_{\mathcal{B}}, (\sigma'', \sigma''') \in \llbracket c_1 \rrbracket_{\mathcal{C}}\} \\
\overset{\text{Def. } \llbracket . \rrbracket_{\mathcal{C}} ..}{\Longrightarrow}\ & (\sigma, \textit{true}) \in \llbracket b \rrbracket_{\mathcal{B}} \wedge (\sigma, \sigma') \in \llbracket c_1 \rrbracket_{\mathcal{C}} \\
\overset{\text{Lemma } \textbf{BExp}}{\Longrightarrow}\ & \langle b, \sigma\rangle \to_{Bexp} \textit{true} \wedge (\sigma, \sigma') \in \llbracket c_1 \rrbracket_{\mathcal{C}} \\
\overset{\text{IA für } c_1}{\Longrightarrow}\ & \langle b, \sigma\rangle \to_{Bexp} \textit{true} \wedge \langle c_1, \sigma\rangle \to_{Stmt} \sigma' \\
\overset{\text{Def. } \langle .,.\rangle \to_{Stmt} .}{\Longrightarrow}\ & \langle \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2, \sigma\rangle \to_{Stmt} \sigma'
\end{aligned}$$

- Fall: $(\sigma, \sigma') \in \{(\sigma'', \sigma''') | (\sigma'', \textit{false}) \in \llbracket b \rrbracket_{\mathcal{B}}, (\sigma'', \sigma''') \in \llbracket c_2 \rrbracket_{\mathcal{C}}\}$

$$\begin{aligned}
& (\sigma, \sigma') \in \{(\sigma'', \sigma''') | (\sigma'', \textit{true}) \in \llbracket b \rrbracket_{\mathcal{B}}, (\sigma'', \sigma''') \in \llbracket c_2 \rrbracket_{\mathcal{C}}\} \\
\overset{\text{Def. } \llbracket . \rrbracket_{\mathcal{C}} ..}{\Longrightarrow}\ & (\sigma, \textit{false}) \in \llbracket b \rrbracket_{\mathcal{B}} \wedge (\sigma, \sigma') \in \llbracket c_2 \rrbracket_{\mathcal{C}} \\
\overset{\text{Lemma } \textbf{BExp}}{\Longrightarrow}\ & \langle b, \sigma\rangle \to_{Bexp} \textit{false} \wedge (\sigma, \sigma') \in \llbracket c_2 \rrbracket_{\mathcal{C}} \\
\overset{\text{IA für } c_1}{\Longrightarrow}\ & \langle b, \sigma\rangle \to_{Bexp} \textit{false} \wedge \langle c_2, \sigma\rangle \to_{Stmt} \sigma' \\
\overset{\text{Def. } \langle .,.\rangle \to_{Stmt} .}{\Longrightarrow}\ & \langle \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2, \sigma\rangle \to_{Stmt} \sigma'
\end{aligned}$$

Beweis $\forall c \in \textbf{Stmt}.\forall \sigma, \sigma'.(\sigma, \sigma') \in \llbracket c \rrbracket_{\mathcal{C}} \Rightarrow \langle c, \sigma\rangle \to_{Stmt} \sigma'$

Induktionsschritt:

- Fall **while** (b) $c2$:

$$\llbracket \textbf{while}\ (b)\ c \rrbracket_{\mathcal{C}} = \textit{fix}(\Gamma)$$
$$\text{mit } \Gamma(s) = \{(\sigma, \sigma') \mid (\sigma, \textit{true}) \in \llbracket b \rrbracket_{\mathcal{B}} \wedge (\sigma, \sigma') \in \llbracket c \rrbracket_{\mathcal{C}} \circ s\} \cup \{(\sigma, \sigma) \mid (\sigma, \textit{false}) \in \llbracket b \rrbracket_{\mathcal{B}}\}$$

Induktionshypothese gilt für c

$$\begin{aligned}
& (\sigma, \sigma') \in \llbracket \textbf{while}\ (b)\ c \rrbracket_{\mathcal{C}} \\
\overset{\text{Def. } \llbracket . \rrbracket_{\mathcal{C}} ..}{\Longrightarrow}\ & (\sigma, \sigma') \in \textit{fix}(\Gamma)
\end{aligned}$$

Beweis $\forall c \in \textbf{Stmt}.\forall \sigma, \sigma'.(\sigma, \sigma') \in \llbracket c \rrbracket_{\mathcal{C}} \Rightarrow \langle c, \sigma\rangle \to_{Stmt} \sigma'$

Induktionsschritt:

- Fall **while** (b) c:

$$\llbracket \textbf{while}\ (b)\ c \rrbracket_{\mathcal{C}} = \textit{fix}(\Gamma)$$
$$\text{mit } \Gamma(s) = \{(\sigma, \sigma') \mid (\sigma, \textit{true}) \in \llbracket b \rrbracket_{\mathcal{B}} \wedge (\sigma, \sigma') \in \llbracket c \rrbracket_{\mathcal{C}} \circ s\} \cup \{(\sigma, \sigma) \mid (\sigma, \textit{false}) \in \llbracket b \rrbracket_{\mathcal{B}}\}$$

Induktionshypothese gilt für c

$$(\sigma, \sigma') \in \llbracket \textbf{while}\ (b)\ c \rrbracket_{\mathcal{C}} \overset{\text{Def. } \llbracket . \rrbracket_{\mathcal{C}} ..}{\Longrightarrow} (\sigma, \sigma') \in \textit{fix}(\Gamma) \overset{\text{Def. } \textit{fix}(\Gamma)}{\Longrightarrow} (\sigma, \sigma') \in \bigcup_{i \in \mathbb{N}} \Gamma^i(\emptyset)$$

Unterbeweis: $\forall i \in \mathbb{N}.(\sigma, \sigma') \in \Gamma^i(\emptyset) \Rightarrow \langle \textbf{while}\ (b)\ c, \sigma\rangle \to_{Stmt} \sigma'$ (UB)
Woraus dann folgt, dass

$$(\sigma, \sigma') \in \bigcup_{i \in \mathbb{N}} \Gamma^i(\emptyset) \Rightarrow \langle \textbf{while}\ (b)\ c, \sigma\rangle \to_{Stmt} \sigma' \qquad (1)$$

$\forall i \in \mathbb{N}.(\sigma,\sigma') \in \Gamma^i(\emptyset) \Rightarrow \langle \textbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma'$ (UB)

Es gilt nach wie vor die Induktionshypothese für dieses c, dass

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

Beweis per Induktion über i:
Induktionsanfang

- $i = 0$:

$$\begin{aligned}(\sigma,\sigma') \in \Gamma^0(\emptyset) \Rightarrow &\quad (\sigma,\sigma') \in \emptyset \\ \Rightarrow &\quad \mathit{false}\end{aligned}$$

Implikation trivialerweise erfüllt da *false* $\Rightarrow F$ immer wahr

Induktionsschritt

- $i \rightarrow i+1$:
  Induktionsannahme (UB) gilt für i

$$\begin{aligned}& (\sigma,\sigma') \in \Gamma^{i+1}(\emptyset) \\ \Longrightarrow\ & (\sigma,\sigma') \in \Gamma(\Gamma^i(\emptyset)) \\ \overset{\text{Def. }\Gamma}{\Longrightarrow}\ & (\sigma,\sigma') \in \{(\sigma'',\sigma''') \mid (\sigma'',\mathit{true}) \in [\![b]\!]_{\mathcal{B}}, (\sigma'',\sigma'''') \in [\![c]\!]_{\mathcal{C}}, \\ & \qquad (\sigma'''',\sigma''') \in \Gamma^i(\emptyset)\} \\ & \qquad \cup \{(\sigma'',\sigma'') \mid (\sigma'',\mathit{false}) \in [\![b]\!]_{\mathcal{B}}\}\end{aligned}$$

Fallunterscheidung über Zugehörigkeit zu welcher Teilmenge

$\forall i \in \mathbb{N}.(\sigma,\sigma') \in \Gamma^i(\emptyset) \Rightarrow \langle \textbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma'$ (UB)

Es gilt nach wie vor die Induktionshypothese für dieses c, dass

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

Beweis per Induktion über i:
Induktionsschritt

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

$$\begin{aligned}& (\sigma,\sigma') \in \Gamma(\Gamma^i(\emptyset)) \\ \overset{\text{Def. }\Gamma}{\Rightarrow}\ & (\sigma,\sigma') \in \{(\sigma'',\sigma''') \mid (\sigma'',\mathit{true}) \in [\![b]\!]_{\mathcal{B}}, (\sigma'',\sigma'''') \in [\![c]\!]_{\mathcal{C}}, \\ & \qquad (\sigma'''',\sigma''') \in \Gamma^i(\emptyset)\} \\ & \qquad \cup \{(\sigma'',\sigma'') \mid (\sigma'',\mathit{false}) \in [\![b]\!]_{\mathcal{B}}\} \\ \overset{\text{Fall}}{\Longrightarrow}\ & \underbrace{(\sigma,\mathit{true}) \in [\![b]\!]_{\mathcal{B}}}_{\text{Lemma } \textbf{BExp}} \wedge \underbrace{(\sigma,\sigma'') \in [\![c]\!]_{\mathcal{C}}}_{\text{IH (IB)}} \wedge \underbrace{(\sigma'',\sigma') \wedge \Gamma^i(\emptyset)}_{\text{IH (UB) für } i} \\ \Longrightarrow\ & \langle b,\sigma\rangle \rightarrow_{Bexp} \mathit{true} \wedge \langle c,\sigma\rangle \rightarrow_{Stmt} \sigma'' \wedge \langle \textbf{while}\ (b)\ c, \sigma''\rangle \rightarrow_{Stmt} \sigma' \\ \overset{\langle .,. \rangle \rightarrow_{Stmt} .}{\Longrightarrow}\ & \langle \textbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma'\end{aligned}$$

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

$$\begin{aligned}& (\sigma,\sigma') \in \Gamma(\Gamma^i(\emptyset)) \\ \overset{\text{Def. }\Gamma}{\Rightarrow}\ & (\sigma,\sigma') \in \{(\sigma'',\sigma''') \mid (\sigma'',\mathit{true}) \in [\![b]\!]_{\mathcal{B}}, (\sigma'',\sigma'''') \in [\![c]\!]_{\mathcal{C}}, \\ & \qquad (\sigma'''',\sigma''') \in \Gamma^i(\emptyset)\} \\ & \qquad \cup \{(\sigma'',\sigma'') \mid (\sigma'',\mathit{false}) \in [\![b]\!]_{\mathcal{B}}\} \\ \overset{\text{Fall}}{\Longrightarrow}\ & (\sigma,\mathit{false}) \in [\![b]\!]_{\mathcal{B}} \wedge \sigma = \sigma' \\ \overset{\text{Lemma für } \textbf{BExp}}{\Longrightarrow}\ & \langle b,\sigma\rangle \rightarrow_{Bexp} \mathit{false} \wedge \sigma = \sigma' \\ \overset{\langle .,. \rangle \rightarrow_{Stmt} .}{\Longrightarrow}\ & \langle \textbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma \wedge \sigma = \sigma' \\ \Longrightarrow\ & \langle \textbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma'\end{aligned}$$

q.e.d.

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

Induktionsschritt:

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

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

Induktionshypothese gilt für c

$$\begin{aligned}(\sigma,\sigma') \in [\![\textbf{while}\ (b)\ c]\!]_{\mathcal{C}} &\overset{\text{Def. } [\![.]\!]_{\mathcal{C}}..}{\Longrightarrow} (\sigma,\sigma') \in \mathit{fix}(\Gamma) \\ &\overset{\text{Def. } \mathit{fix}(\Gamma)}{\Longrightarrow} (\sigma,\sigma') \in \bigcup_{i \in \mathbb{N}} \Gamma^i(\emptyset)\end{aligned}$$

Unterbeweis: $\forall i \in \mathbb{N}.(\sigma,\sigma') \in \Gamma^i(\emptyset) \Rightarrow \langle \textbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma'$ (UB)
Woraus dann folgt, dass

$$(\sigma,\sigma') \in \bigcup_{i \in \mathbb{N}} \Gamma^i(\emptyset) \Rightarrow \langle \textbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma' \qquad (1)$$

Äquivalenz operationale und denotationale Semantik

- Für alle $c \in$ **Stmt**, für alle Zustände σ, σ':

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

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

  - Gegenbeispiel für $\Leftarrow$ in der zweiten Aussage: wähle $c \equiv \mathit{while}(1)\{\}$: $[\![c]\!]_{\mathcal{C}} = \emptyset$ aber $\langle c,\sigma\rangle \rightarrow_{Stmt} \bot$ gilt nicht (sondern?).

Fahrplan

- Einführung
- Operationale Semantik
- Denotationale Semantik
- Äquivalenz der Operationalen und Denotationalen Semantik
- Der Floyd-Hoare-Kalkül
- Invarianten und die Korrektheit des Floyd-Hoare-Kalküls
- Strukturierte Datentypen
- Verifikationsbedingungen
- Vorwärts mit Floyd und Hoare
- Modellierung
- Spezifikation von Funktionen
- Referenzen und Speichermodelle
- Ausblick und Rückblick