Korrekte Software: Grundlagen und Methoden

Vorlesung 4 vom 4/6.05.21

Äquivalenz der Operationalen und Denotationalen Semantik

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2021

Fahrplan

- Einführung
- Operationale Semantik
- Denotationale Semantik
- Äquivalenz der Operationalen und Denotationalen Semantik
- Der Floyd-Hoare-Kalkül I
- Der Floyd-Hoare-Kalkül II: Invarianten
- 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∈ **Z**	$\langle m, \sigma\rangle \rightarrow_{Aexp} m$	$\{(\sigma, m) \mid \sigma \in \Sigma\}$
x∈ **Loc**	$\dfrac{x \in Dom(\sigma)}{\langle x, \sigma\rangle \rightarrow_{Aexp} \sigma(x)}$ $\dfrac{x \notin Dom(\sigma)}{\langle x, \sigma\rangle \rightarrow_{Aexp} \bot}$	$\{(\sigma, \sigma(x)) \mid \sigma \in \Sigma, x \in Dom(\sigma)\}$
$a_1 \circ a_2$	$\dfrac{\langle a_1, \sigma\rangle \rightarrow_{Aexp} n \quad \langle a_2, \sigma\rangle \rightarrow_{Aexp} m \quad n, m \neq \bot}{\langle a_1 \circ a_2, \sigma\rangle \rightarrow_{Aexp} n \circ^I m}$ $\dfrac{\langle a_1, \sigma\rangle \rightarrow_{Aexp} n \quad \langle a_2, \sigma\rangle \rightarrow_{Aexp} m \quad n = \bot \text{ oder } m = \bot}{\langle a_1 \circ a_2, \sigma\rangle \rightarrow_{Aexp} \bot}$ $\circ \in \{+, *, -\}$	$\{(\sigma, n \circ^I m) \mid \sigma \in \Sigma, (\sigma, n) \in [\![a_1]\!]_{\mathcal{A}}, (\sigma, m) \in [\![a_2]\!]_{\mathcal{A}}\}$

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

$$\forall x \in S. x \not\succ x \qquad (irreflexiv)$$
$$\forall x, y \in S. x \succ y \Rightarrow y \not\succ x \qquad (asymmetrisch)$$
$$\forall x, y, z \in S. (x \succ y \wedge y \succ z) \Rightarrow x \succ z \qquad (transitiv)$$

- 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 Bspw: x Teilausdruck von $(2 * x + 1)$ Ebenso $2 * x$ und 1

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

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

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

  ist.

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?per struktureller Induktion über a. (Warum?)

Beweis $\forall a \in \mathbf{Aexp}.\forall n \in \mathbb{Z}.\forall \sigma.\ \langle a, \sigma\rangle \rightarrow_{Aexp} n \Leftrightarrow (\sigma, n) \in \llbracket a \rrbracket_{\mathcal{A}}$
$\wedge\ \langle a, \sigma\rangle \rightarrow_{Aexp} \bot \Leftrightarrow \sigma \notin \mathbf{Dom}(\llbracket a \rrbracket_{\mathcal{A}})$

Induktionsanfänge

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

$$\left.\begin{array}{l}\langle m, \sigma\rangle \rightarrow_{Aexp} \llbracket m \rrbracket \\ \llbracket m \rrbracket_{\mathcal{A}} = \{(\sigma', \llbracket m \rrbracket) \mid \sigma' \in \Sigma\} \Rightarrow (\sigma, \llbracket m \rrbracket) \in \llbracket m \rrbracket_{\mathcal{A}}\end{array}\right] \Leftrightarrow$$

- $a \equiv X \in \mathbf{Loc}$:
  1. $X \in Dom(\sigma)$:

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

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

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

Beweis $\forall a \in \mathbf{Aexp}.\forall n \in \mathbb{Z}.\forall \sigma.\ \langle a, \sigma\rangle \rightarrow_{Aexp} n \Leftrightarrow (\sigma, n) \in \llbracket a \rrbracket_{\mathcal{A}}$
$\wedge\ \langle a, \sigma\rangle \rightarrow_{Aexp} \bot \Leftrightarrow \sigma \notin \mathbf{Dom}(\llbracket a \rrbracket_{\mathcal{A}})$

Induktionsschritte

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

$$\llbracket a_1 + a_2 \rrbracket_{\mathcal{A}} = \{(\sigma', u + v) | (\sigma', u) \in \llbracket a_1 \rrbracket_{\mathcal{A}} \text{ und } (\sigma', v) \in \llbracket a_2 \rrbracket_{\mathcal{A}}\}$$

Induktionsannahme gilt für a_1 und a_2.

$$\begin{array}{cccc}\langle a_1 + a_2, \sigma\rangle \rightarrow_{Aexp} m + n & \overset{(\text{Def. } \langle .,. \rangle \rightarrow_{Aexp})}{\Longleftrightarrow} & \langle a_1, \sigma\rangle \rightarrow_{Aexp} m \overset{\text{IA für } a_1}{\Longleftrightarrow} (\sigma, m) \in \llbracket a_1 \rrbracket_{\mathcal{A}} \\ & & \& \qquad\qquad \& \\ & & \langle a_2, \sigma\rangle \rightarrow_{Aexp} n \overset{\text{IA für } a_2}{\Longleftrightarrow} (\sigma, n) \in \llbracket a_2 \rrbracket_{\mathcal{A}} \\ & & \Updownarrow (\mathit{Def}.\llbracket . \rrbracket_{\mathcal{A}}) \\ & & (\sigma, m + n) \in \llbracket a_1 + a_2 \rrbracket_{\mathcal{A}}\end{array}$$

Beweis $\forall a \in \mathbf{Aexp}.\forall n \in \mathbb{Z}.\forall \sigma.\ \langle a, \sigma\rangle \rightarrow_{Aexp} n \Leftrightarrow (\sigma, n) \in \llbracket a \rrbracket_{\mathcal{A}}$
$\wedge\ \langle a, \sigma\rangle \rightarrow_{Aexp} \bot \Leftrightarrow \sigma \notin \mathbf{Dom}(\llbracket a \rrbracket_{\mathcal{A}})$

Induktionsschritte

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

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

  - Fall $n = \bot$.
    Aus Induktionsannahme folgt, dass $\langle a_1, \sigma\rangle \rightarrow_{Aexp} \bot \Leftrightarrow \sigma \notin Dom(\llbracket a_1 \rrbracket_{\mathcal{A}})$.
    Weiterhin gilt

$$\llbracket a_1 + a_2 \rrbracket_{\mathcal{A}} = \{(\sigma', u + v) | (\sigma', u) \in \llbracket a_1 \rrbracket_{\mathcal{A}} \text{ und } (\sigma', v) \in \llbracket a_2 \rrbracket_{\mathcal{A}}\}$$

    Somit gilt $\sigma \notin Dom(\llbracket a_1 + a_2 \rrbracket_{\mathcal{A}})$.
  - Fall $n \neq \bot, m = \bot$: analog.

Beweis $\forall a \in \mathbf{Aexp}.\forall n \in \mathbb{Z}.\forall \sigma.\ \langle a, \sigma\rangle \rightarrow_{Aexp} n \Leftrightarrow (\sigma, n) \in \llbracket a \rrbracket_{\mathcal{A}}$
$\wedge\ \langle a, \sigma\rangle \rightarrow_{Aexp} \bot \Leftrightarrow \sigma \notin \mathbf{Dom}(\llbracket a \rrbracket_{\mathcal{A}})$

Induktionsschritte

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

$$\llbracket a_1 / a_2 \rrbracket_{\mathcal{A}} = \{(\sigma', u/v) | (\sigma', u) \in \llbracket a_1 \rrbracket_{\mathcal{A}}, (\sigma', v) \in \llbracket a_2 \rrbracket_{\mathcal{A}} \text{ und } v \neq 0\}$$

Induktionsannahme gilt für a_1 und a_2.

$$\begin{array}{cccc}\langle a_1 / a_2, \sigma\rangle \rightarrow_{Aexp} m/n & \overset{(\text{Def. } \langle .,. \rangle \rightarrow_{Aexp})}{\Longleftrightarrow} & \langle a_1, \sigma\rangle \rightarrow_{Aexp} m \overset{\text{IA für } a_1}{\Longleftrightarrow} (\sigma, m) \in \llbracket a_1 \rrbracket_{\mathcal{A}} \\ & & \& \qquad\qquad \& \\ & & \langle a_2, \sigma\rangle \rightarrow_{Aexp} n \overset{\text{IA für } a_2}{\Longleftrightarrow} (\sigma, n) \in \llbracket a_2 \rrbracket_{\mathcal{A}} \\ & & \Updownarrow (\mathit{Def}.\llbracket . \rrbracket_{\mathcal{A}}) \\ & & (\sigma, m/n) \in \llbracket a_1 / a_2 \rrbracket_{\mathcal{A}}\end{array}$$

Beweis $\forall a \in \mathbf{Aexp}.\forall n \in \mathbb{Z}.\forall \sigma.\ \langle a, \sigma\rangle \rightarrow_{Aexp} n \Leftrightarrow (\sigma, n) \in \llbracket a \rrbracket_{\mathcal{A}}$
$\wedge\ \langle a, \sigma\rangle \rightarrow_{Aexp} \bot \Leftrightarrow \sigma \notin \mathbf{Dom}(\llbracket a \rrbracket_{\mathcal{A}})$

Induktionsschritte

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

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

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

$$\llbracket a_1 / a_2 \rrbracket_{\mathcal{A}} = \{(\sigma', u/v) | (\sigma', u) \in \llbracket a_1 \rrbracket_{\mathcal{A}}, (\sigma', v) \in \llbracket a_2 \rrbracket_{\mathcal{A}} \text{ und } v \neq 0\}$$

    Somit gilt $\sigma \notin Dom(\llbracket a_1 / a_2 \rrbracket_{\mathcal{A}})$.
  - Fall $n = \bot, m = \bot$: analog wie bei $+$

q.e.d.

Operationale vs. denotationale Semantik

	Operational $\langle b, \sigma\rangle \rightarrow_{Bexp}$ *false* | *true* | $\bot$	Denotational $\llbracket b \rrbracket_{\mathcal{B}}$
1	$\langle \mathbf{1}, \sigma\rangle \rightarrow_{Bexp} \mathit{true}$	$\{(\sigma, \mathit{true}) \vert \sigma \in \Sigma\}$
0	$\langle \mathbf{0}, \sigma\rangle \rightarrow_{Bexp} \mathit{false}$	$\{(\sigma, \mathit{false}) \vert \sigma \in \Sigma\}$

Operationale vs. denotationale Semantik

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

Operationale vs. denotationale Semantik

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

Äquivalenz operationale und denotationale Semantik

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

$$\langle b, \sigma \rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma, t) \in \llbracket b \rrbracket_{\mathcal{B}}$$
$$\langle b, \sigma \rangle \rightarrow_{Bexp} \bot \Leftrightarrow \sigma \notin Dom(\llbracket b \rrbracket_{\mathcal{B}})$$

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

Beweis $\forall b \in \textbf{Bexp}. \forall t \in \mathbb{B}. \forall \sigma.\quad \langle b, \sigma \rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma, t) \in \llbracket b \rrbracket_{\mathcal{B}}$
$\wedge \quad \langle b, \sigma \rangle \rightarrow_{Bexp} \bot \Leftrightarrow \sigma \notin \textbf{\textit{Dom}}(\llbracket b \rrbracket_{\mathcal{B}})$

Induktionsanfänge

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

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

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

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

Beweis $\forall b \in \textbf{Bexp}. \forall t \in \mathbb{B}. \forall \sigma.\quad \langle b, \sigma \rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma, t) \in \llbracket b \rrbracket_{\mathcal{B}}$
$\wedge \quad \langle b, \sigma \rangle \rightarrow_{Bexp} \bot \Leftrightarrow \sigma \notin \textbf{\textit{Dom}}(\llbracket b \rrbracket_{\mathcal{B}})$

Induktionsschritte

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

$$\begin{aligned} \llbracket b_1 \&\& b_2 \rrbracket_{\mathcal{B}} =& \{(\sigma', \mathit{false}) | (\sigma', \mathit{false}) \in \llbracket b_1 \rrbracket_{\mathcal{B}}\} \\ & \cup \{(\sigma', t_2) | (\sigma', \mathit{true}) \in \llbracket b_1 \rrbracket_{\mathcal{B}} \text{ und } (\sigma', t_2) \in \llbracket b_2 \rrbracket_{\mathcal{B}}\} \end{aligned}$$

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

$$\begin{array}{lcl} \langle b_1 \&\& b_2, \sigma \rangle \rightarrow_{Bexp} \bot \overset{(\text{Def. } \langle .,. \rangle \rightarrow_{Bexp})}{\Longleftrightarrow} & \langle b_1, \sigma \rangle \rightarrow_{Bexp} \bot \overset{\text{IA für } b_1}{\Longleftrightarrow} & \sigma \notin Dom(\llbracket b_1 \rrbracket_{\mathcal{B}}) \\ & & \Big\Downarrow \text{Def. } \llbracket . \rrbracket_{\mathcal{B}} \\ & & \sigma \notin \llbracket b_1 \&\& b_2 \rrbracket_{\mathcal{B}} \end{array}$$

Beweis $\forall b \in \textbf{Bexp}. \forall t \in \mathbb{B}. \forall \sigma.\quad \langle b, \sigma \rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma, t) \in \llbracket b \rrbracket_{\mathcal{B}}$
$\wedge \quad \langle b, \sigma \rangle \rightarrow_{Bexp} \bot \Leftrightarrow \sigma \notin \textbf{\textit{Dom}}(\llbracket b \rrbracket_{\mathcal{B}})$

Induktionsschritte

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

$$\begin{aligned} \llbracket b_1 \&\& b_2 \rrbracket_{\mathcal{B}} =& \{(\sigma', \mathit{false}) | (\sigma', \mathit{false}) \in \llbracket b_1 \rrbracket_{\mathcal{B}}\} \\ & \cup \{(\sigma', t_2) | (\sigma', \mathit{true}) \in \llbracket b_1 \rrbracket_{\mathcal{B}} \text{ und } (\sigma', t_2) \in \llbracket b_2 \rrbracket_{\mathcal{B}}\} \end{aligned}$$

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

$$\begin{array}{lcl} \langle b_1 \&\& b_2, \sigma \rangle \rightarrow_{Bexp} \mathit{false} \overset{(\text{Def. } \langle .,. \rangle \rightarrow_{Bexp})}{\Longleftrightarrow} & \langle b_1, \sigma \rangle \rightarrow_{Bexp} \mathit{false} \overset{\text{IA für } b_1}{\Longleftrightarrow} & (\sigma, \mathit{false}) \in \llbracket b_1 \rrbracket_{\mathcal{B}} \\ & & \Big\Downarrow \text{Def. } \llbracket . \rrbracket_{\mathcal{B}} \\ & & (\sigma, \mathit{false}) \in \llbracket b_1 \&\& b_2 \rrbracket_{\mathcal{B}} \end{array}$$

Beweis $\forall b \in \textbf{Bexp}. \forall t \in \mathbb{B}. \forall \sigma.\quad \langle b, \sigma \rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma, t) \in \llbracket b \rrbracket_{\mathcal{B}}$
$\wedge \quad \langle b, \sigma \rangle \rightarrow_{Bexp} \bot \Leftrightarrow \sigma \notin \textbf{\textit{Dom}}(\llbracket b \rrbracket_{\mathcal{B}})$

Induktionsschritte

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

$$\begin{aligned} \llbracket b_1 \&\& b_2 \rrbracket_{\mathcal{B}} =& \{(\sigma', \mathit{false}) | (\sigma', \mathit{false}) \in \llbracket b_1 \rrbracket_{\mathcal{B}}\} \\ & \cup \{(\sigma', t_2) | (\sigma', \mathit{true}) \in \llbracket b_1 \rrbracket_{\mathcal{B}} \text{ und } (\sigma', t_2) \in \llbracket b_2 \rrbracket_{\mathcal{B}}\} \end{aligned}$$

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

$$\begin{array}{lcl} \langle b_1 \&\& b_2, \sigma \rangle \rightarrow_{Bexp} \mathit{false} \overset{(\text{Def. } \langle .,. \rangle \rightarrow_{Bexp})}{\Longleftrightarrow} & \langle b_1, \sigma \rangle \rightarrow_{Bexp} \mathit{true} \overset{\text{IA für } b_1}{\Longleftrightarrow} & (\sigma, \mathit{true}) \in \llbracket b_1 \rrbracket_{\mathcal{B}} \\ & \& & \& \\ & \langle b_2, \sigma \rangle \rightarrow_{Bexp} \mathit{false} \overset{\text{IA für } b_2}{\Longleftrightarrow} & (\sigma, \mathit{false}) \in \llbracket b_2 \rrbracket_{\mathcal{B}} \\ & & \Big\Downarrow \text{Def. } \llbracket . \rrbracket_{\mathcal{B}} \\ & & (\sigma, \mathit{false}) \in \llbracket b_1 \&\& b_2 \rrbracket_{\mathcal{B}} \end{array}$$

Beweis $\forall b \in \textbf{Bexp}. \forall t \in \mathbb{B}. \forall \sigma.\quad \langle b, \sigma \rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma, t) \in \llbracket b \rrbracket_{\mathcal{B}}$
$\wedge \quad \langle b, \sigma \rangle \rightarrow_{Bexp} \bot \Leftrightarrow \sigma \notin \textbf{\textit{Dom}}(\llbracket b \rrbracket_{\mathcal{B}})$

Induktionsschritte

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

$$\begin{aligned} \llbracket b_1 \&\& b_2 \rrbracket_{\mathcal{B}} =& \{(\sigma', \mathit{false}) | (\sigma', \mathit{false}) \in \llbracket b_1 \rrbracket_{\mathcal{B}}\} \\ & \cup \{(\sigma', t_2) | (\sigma', \mathit{true}) \in \llbracket b_1 \rrbracket_{\mathcal{B}} \text{ und } (\sigma', t_2) \in \llbracket b_2 \rrbracket_{\mathcal{B}}\} \end{aligned}$$

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

$$\begin{array}{lcl} \langle b_1 \&\& b_2, \sigma \rangle \rightarrow_{Bexp} \mathit{true} \overset{(\text{Def. } \langle .,. \rangle \rightarrow_{Bexp})}{\Longleftrightarrow} & \langle b_1, \sigma \rangle \rightarrow_{Bexp} \mathit{true} \overset{\text{IA für } b_1}{\Longleftrightarrow} & (\sigma, \mathit{true}) \in \llbracket b_1 \rrbracket_{\mathcal{B}} \\ & \& & \& \\ & \langle b_2, \sigma \rangle \rightarrow_{Bexp} \mathit{true} \overset{\text{IA für } b_2}{\Longleftrightarrow} & (\sigma, \mathit{true}) \in \llbracket b_2 \rrbracket_{\mathcal{B}} \\ & & \Big\Updownarrow \text{Def. } \llbracket . \rrbracket_{\mathcal{B}} \\ & & (\sigma, \mathit{true}) \in \llbracket b_1 \&\& b_2 \rrbracket_{\mathcal{B}} \end{array}$$

Beweis $\forall b \in \textbf{Bexp}. \forall t \in \mathbb{B}. \forall \sigma.\quad \langle b, \sigma \rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma, t) \in \llbracket b \rrbracket_{\mathcal{B}}$
$\wedge \quad \langle b, \sigma \rangle \rightarrow_{Bexp} \bot \Leftrightarrow \sigma \notin \textbf{\textit{Dom}}(\llbracket b \rrbracket_{\mathcal{B}})$

Induktionsschritte

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

$$\begin{aligned} \llbracket b_1 \&\& b_2 \rrbracket_{\mathcal{B}} =& \{(\sigma', \mathit{false}) | (\sigma', \mathit{false}) \in \llbracket b_1 \rrbracket_{\mathcal{B}}\} \\ & \cup \{(\sigma', t_2) | (\sigma', \mathit{true}) \in \llbracket b_1 \rrbracket_{\mathcal{B}} \text{ und } (\sigma', t_2) \in \llbracket b_2 \rrbracket_{\mathcal{B}}\} \end{aligned}$$

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

$$\begin{array}{lcl} \langle b_1 \&\& b_2, \sigma \rangle \rightarrow_{Bexp} \bot \overset{(\text{Def. } \langle .,. \rangle \rightarrow_{Bexp})}{\Longleftrightarrow} & \langle b_1, \sigma \rangle \rightarrow_{Bexp} \mathit{true} \overset{\text{IA für } b_1}{\Longleftrightarrow} & (\sigma, \mathit{true}) \in \llbracket b_1 \rrbracket_{\mathcal{B}} \\ & \& & \& \\ & \langle b_2, \sigma \rangle \rightarrow_{Bexp} \bot \overset{\text{IA für } b_2}{\Longleftrightarrow} & \sigma \notin Dom(\llbracket b_2 \rrbracket_{\mathcal{B}}) \\ & & \Big\Downarrow \text{Def. } \llbracket . \rrbracket_{\mathcal{B}} \\ & & \sigma \notin Dom(\llbracket b_1 \&\& b_2 \rrbracket_{\mathcal{B}}) \end{array}$$

Beweis $\forall b \in \textbf{Bexp}. \forall t \in \mathbb{B}. \forall \sigma.\quad \langle b, \sigma \rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma, t) \in \llbracket b \rrbracket_{\mathcal{B}}$
$\wedge \quad \langle b, \sigma \rangle \rightarrow_{Bexp} \bot \Leftrightarrow \sigma \notin \textbf{\textit{Dom}}(\llbracket b \rrbracket_{\mathcal{B}})$

- $(\sigma, \mathit{true}) \in \llbracket b_1 \&\& b_2 \rrbracket_{\mathcal{B}} \overset{\text{Def. } \llbracket . \rrbracket_{\mathcal{B}}}{\Longleftrightarrow} (\sigma, \mathit{true}) \in \llbracket b_1 \rrbracket_{\mathcal{B}}$ und $(\sigma, \mathit{true}) \in \llbracket b_2 \rrbracket_{\mathcal{B}}$
  - Siehe Folie 22
- $(\sigma, \mathit{false}) \in \llbracket b_1 \&\& b_2 \rrbracket_{\mathcal{B}} \overset{\text{Def. } \llbracket . \rrbracket_{\mathcal{B}}}{\Longleftrightarrow} (\sigma, \mathit{false}) \in \llbracket b_1 \rrbracket_{\mathcal{B}}$ oder
  $(\sigma, \mathit{true}) \in \llbracket b_1 \rrbracket_{\mathcal{B}}$ und $(\sigma, \mathit{false}) \in \llbracket b_2 \rrbracket_{\mathcal{B}}$
  - Siehe Folie 20 und 21
- $\sigma \notin Dom(\llbracket b_1 \&\& b_2 \rrbracket_{\mathcal{B}}) \overset{\text{Def. } \llbracket . \rrbracket_{\mathcal{B}}}{\Longleftrightarrow} \sigma \notin Dom(\llbracket b_1 \rrbracket_{\mathcal{B}})$ oder $\sigma \notin Dom(\llbracket b_2 \rrbracket_{\mathcal{B}})$
  - Siehe Folie 19 und 23

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

Arbeitsblatt 4.2: Beweis Induktionsanfang

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

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

$$\begin{array}{rl}\forall a \in \textbf{Aexp}. \forall n \in \mathbb{Z}. \forall \sigma. & \langle a, \sigma\rangle \to_{Aexp} n \Leftrightarrow (\sigma, n) \in [\![a]\!]_{\mathcal{A}} \\ \wedge & \langle a, \sigma\rangle \to_{Bexp} \bot \Leftrightarrow \sigma \notin Dom([\![a]\!]_{\mathcal{A}})\end{array}$$

Beweis

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

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

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

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

Beweis

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

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

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

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

Beweis

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

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

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

$$\begin{array}{ccccc}\langle a_1 == a_2, \sigma\rangle \to_{Bexp} \bot & \overset{(\text{Def. } \langle .,. \rangle \to_{Bexp})}{\Longleftrightarrow} & \langle a_1, \sigma\rangle \to_{Aexp} \bot & \overset{\text{Lemma für } a_1}{\Longleftrightarrow} & \sigma \notin Dom([\![a_1]\!]_{\mathcal{A}}) \\ & & \vee & & \vee \\ & & \langle a_2, \sigma\rangle \to_{Aexp} \bot & \overset{\text{Lemma für } a_2}{\Longleftrightarrow} & \sigma \notin Dom([\![a_2]\!]_{\mathcal{A}}) \\ & & & & \Updownarrow \text{Def. } [\![.]\!]_{\mathcal{B}} \\ & & & & \sigma \notin Dom([\![a_1 == a_2]\!]_{\mathcal{B}})\end{array}$$

Operationale vs. denotationale Semantik

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

Operationale vs. denotationale Semantik

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

Operationale vs. denotationale Semantik

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

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

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

mit

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

Äquivalenz operationale und denotationale Semantik

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

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

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

Operationale Semantik: C0 Programme

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

Regeln:

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

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

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

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

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

Operationale Semantik: C0 Programme

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

Regeln:

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

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

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

Operationale Semantik: C0 Programme

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

Regeln:

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

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

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

Ableitungstiefe für Programme

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

$$\frac{\begin{matrix}\vdots \\ \textit{Prämisse}_1\end{matrix} \quad \cdots \quad \begin{matrix}\vdots \\ \textit{Prämisse}_n\end{matrix}}{\textit{Conclusion}}$$

Operationale Semantik: C0 Programme

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

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

Äquivalenz operationale und denotationale Semantik

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

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

- $\Rightarrow$ 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. $\langle c, \sigma\rangle \rightarrow_{Stmt} \sigma' \Rightarrow (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}}$
2. $\langle c, \sigma\rangle \rightarrow_{Stmt} \bot \Rightarrow \sigma \notin \textbf{\textit{Dom}}([\![c]\!]_{\mathcal{C}})$

Induktionsanfang – Ableitungstiefe 1

- Fall $c \equiv x = a$:

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

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

$$\langle x = a, \sigma\rangle \rightarrow_{Stmt} \sigma[x \mapsto m]$$
$$\Big\Updownarrow \text{(Def. } \langle .,.\rangle \rightarrow_{Stmt} .)$$
$$\langle a, \sigma\rangle \rightarrow_{Aexp} m \in \mathbb{Z} \overset{\text{Lemma für } a}{\Longleftrightarrow} (\sigma, m) \in [\![a]\!]_{\mathcal{A}}$$
$$\text{Def. } [\![.]\!]_{\mathcal{C}} \Big\Downarrow$$
$$(\sigma, \sigma[x \mapsto m]) \in [\![x = a]\!]_{\mathcal{C}}$$

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

$$\langle x = a, \sigma\rangle \rightarrow_{Stmt} \bot$$
$$\Big\Updownarrow \text{(Def. } \langle .,.\rangle \rightarrow_{Stmt} .)$$
$$\langle a, \sigma\rangle \rightarrow_{Aexp} \bot \overset{\text{Lemma für } a}{\Longleftrightarrow} \sigma \notin Dom([\![a]\!]_{\mathcal{A}})$$
$$\text{Def. } [\![.]\!]_{\mathcal{C}} \Big\Downarrow$$
$$\sigma \notin Dom([\![x = a]\!]_{\mathcal{C}})$$

Beweis $\forall c \in \textbf{Stmt}. \forall \sigma, \sigma'.$ 1. $\langle c, \sigma\rangle \rightarrow_{Stmt} \sigma' \Rightarrow (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}}$
2. $\langle c, \sigma\rangle \rightarrow_{Stmt} \bot \Rightarrow \sigma \notin \textbf{\textit{Dom}}([\![c]\!]_{\mathcal{C}})$

Induktionsschritt:

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

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

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

$$\langle \textbf{if}(b)\ c_1\ \textbf{else}\ c_2, \sigma\rangle \rightarrow_{Stmt} \sigma' \overset{\text{(Def. } \langle .,.\rangle \rightarrow_{Stmt} .)}{\Longleftrightarrow} \langle b, \sigma\rangle \rightarrow_{Bexp} true \overset{\text{Lemma für } b}{\Longleftrightarrow} (\sigma, true) \in [\![b]\!]_{\mathcal{B}}$$
$$\& \qquad \qquad \&$$
$$\langle c_1, \sigma\rangle \rightarrow_{Stmt} \sigma' \overset{\text{IH für } c_1}{\Longleftrightarrow} (\sigma, \sigma') \in [\![c_1]\!]_{\mathcal{C}}$$
$$\text{Def. } [\![.]\!]_{\mathcal{C}} \Big\Downarrow$$
$$(\sigma, \sigma') \in [\![\textbf{if}(b)\ c_1\ \textbf{else}\ c_2]\!]_{\mathcal{C}}$$

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

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

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

Induktionsschritt:

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

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

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

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

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

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

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

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

Äquivalenz operationale und denotationale Semantik

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

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

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

Induktionsanfang:

- Fall $c \equiv x = a$:

$$[\![x = a]\!]_{\mathcal{C}} = \{(\sigma'', \sigma''[x \mapsto t]) | (\sigma'', t) \in [\![a]\!]_{\mathcal{A}}\}$$

$$\begin{aligned}
& (\sigma, \sigma') \in \{(\sigma'', \sigma''[x \mapsto t]) | (\sigma'', t) \in [\![a]\!]_{\mathcal{A}}\} \\
\xRightarrow{\text{Def. } [\![.]\!]_{\mathcal{C}} .} \quad & \underbrace{(\sigma, t) \in [\![a]\!]_{\mathcal{A}}} \wedge \sigma' = \sigma[x \mapsto t] \\
\xRightarrow{\text{Lemma } \textbf{AExp}} \quad & \langle a, \sigma\rangle \to_{Aexp} t \wedge \sigma' = \sigma[x \mapsto t] \\
\xRightarrow{\text{Def. } \langle .,.\rangle \to_{Stmt} .} \quad & \langle x = a, \sigma\rangle \to_{Stmt} \sigma[x \mapsto t] \wedge \sigma' = \sigma[x \mapsto t] \\
\Longrightarrow \quad & \langle x = a, \sigma\rangle \to_{Stmt} \sigma'
\end{aligned}$$

- Fall $c \equiv \{\}$

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

$$\begin{aligned}
& (\sigma, \sigma') \in \{(\sigma'', \sigma'') | \sigma'' \in \Sigma\} \\
\xRightarrow{\text{Def. } [\![.]\!]_{\mathcal{C}} .} \quad & \sigma = \sigma' \\
\xRightarrow{\text{Def. } \langle .,.\rangle \to_{Stmt} .} \quad & \langle \{\}, \sigma\rangle \to_{Stmt} \sigma \wedge \sigma = \sigma' \\
\Longrightarrow \quad & \langle \{\}, \sigma\rangle \to_{Stmt} \sigma'
\end{aligned}$$

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

Induktionsschritt:

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

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

Induktionsannahme gilt für c_1 und c_2

- Fall: $(\sigma, \sigma') \in \{(\sigma'', \sigma''') | (\sigma'', \textit{true}) \in [\![b]\!]_{\mathcal{B}}, (\sigma'', \sigma''') \in [\![c_1]\!]_{\mathcal{C}}\}$

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

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

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

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

Induktionsschritt:

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

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

Induktionshypothese gilt für c

$$\begin{aligned}
& (\sigma, \sigma') \in [\![\textbf{while}\ (b)\ c]\!]_{\mathcal{C}} \\
\xRightarrow{\text{Def. } [\![.]\!]_{\mathcal{C}} .} \quad & (\sigma, \sigma') \in \textit{fix}(\Gamma)
\end{aligned}$$

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

Induktionsschritt:

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

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

Induktionshypothese gilt für c

$$(\sigma, \sigma') \in [\![\textbf{while}\ (b)\ c]\!]_{\mathcal{C}} \xRightarrow{\text{Def. } [\![.]\!]_{\mathcal{C}} .} (\sigma, \sigma') \in \textit{fix}(\Gamma) \xRightarrow{\text{Def. } \textit{fix}(\Gamma)} (\sigma, \sigma') \in \bigcup_{i \in \mathbb{N}} \Gamma^i(\emptyset)$$

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

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

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

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

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

Beweis per Induktion über i:
Induktionsanfang

- $i = 0$:

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

Implikation trivialerweise erfüllt da $\textit{false} \Rightarrow F$ immer wahr

Induktionsschritt $i \to i + 1$:
Induktionsannahme (UB) gilt für i

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

Fallunterscheidung über Zugehörigkeit zu welcher Teilmenge

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

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

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

Beweis per Induktion über i:
Induktionsschritt $i \to i + 1$:
Induktionsannahme (UB) gilt für i

- **Fall** $(\sigma, \sigma') \in \{(\sigma'', \sigma''') \mid (\sigma'', \textbf{\textit{true}}) \in [\![b]\!]_{\mathcal{B}}, (\sigma'', \sigma'''') \in [\![c]\!]_{\mathcal{C}}, (\sigma'''', \sigma''') \in \Gamma^i(\emptyset)\}$

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

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

$$(\sigma, \sigma') \in \Gamma(\Gamma^i(\emptyset))$$

Def. Γ

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:

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

Induktionshypothese gilt für c

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

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

Äquivalenz operationale und denotationale Semantik

- Für alle $c \in \textbf{Stmt}$, 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 $c \equiv while(1)\{\}$: $[\![c]\!]_{\mathcal{C}} = \emptyset$ aber $\langle c, \sigma \rangle \rightarrow_{Stmt} \bot$ gilt nicht (sondern?).

Fahrplan