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

# Operationale vs. denotationale Semantik

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

**Denotational** $[\![a]\!]_{\mathcal{A}}$

$a_1 / a_2$

$$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n \qquad \langle a_2, \sigma \rangle \rightarrow_{Aexp} m \\ m \neq 0 \qquad m, n \neq \bot}{\langle a_1 \circ a_2, \sigma \rangle \rightarrow_{Aexp} n \circ^I m}$$

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

$$\{(\sigma, n/m) | \sigma \in \Sigma, (\sigma, n) \in [\![a_1]\!]_{\mathcal{A}}, (\sigma, m) \in [\![a_2]\!]_{\mathcal{A}}, m \neq 0\}$$

# Äquivalenz operationale und denotationale Semantik

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

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

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

- 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

$$\begin{aligned} \forall x \in S.\, x \not\succ x & \qquad (\textit{irreflexiv}) \\ \forall x, y \in S.\, x \succ y \Rightarrow y \not\succ x & \qquad (\textit{asymmetrisch}) \\ \forall x, y, z \in S.\, (x \succ y \wedge y \succ z) \Rightarrow x \succ z & \qquad (\textit{transitiv}) \end{aligned}$$

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

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

# Induktionsprinzip

**Noether'sche Induktion**

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

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

| | $S$ | $\succ$ |
|---|---|---|
| Mathematische Induktion | $\mathbb{N}$ | $n \to n+1$ |
| Strukturelle Induktion **Aexp** | **Aexp** | $a \succ a'$ genau dann, wenn<br>$a'$ ist Teilausdruck von $a$<br>Bspw: $x$ Teilausdruck von $(2 * x + 1)$<br>Ebenso $2 * x$ und $1$ |

# Arbeitsblatt 4.1: Übung zu struktureller Ordnung

Die strukturelle Ordnung auf arithmetischen Ausdrücken ist definiert als:

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

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

$$a \,\text{Teilausdruck-von}(a_1 \circ a_2) \Leftrightarrow \begin{pmatrix} a = a_1 \vee a \,\text{Teilausdruck-von}\, a_1 \vee \\ a = a_2 \vee a \,\text{Teilausdruck-von}\, a_2 \end{pmatrix}$$

- 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 $\sigma$:

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

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

- Beweis Prinzip?

# Äquivalenz operationale und denotationale Semantik

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

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

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

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

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

## Induktionsanfänge

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

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

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

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

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

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

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

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

## 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 $a_2$.

$$\langle a_1 + a_2, \sigma\rangle \rightarrow_{Aexp} m + n \overset{(\text{Def. } \langle .,. \rangle \rightarrow_{Aexp}.)}{\Longleftrightarrow} \langle a_1, \sigma\rangle \rightarrow_{Aexp} m \overset{\text{IA für } a_1}{\Longleftrightarrow} (\sigma, m) \in [\![a_1]\!]_{\mathcal{A}}$$

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

$$\langle a_2, \sigma\rangle \rightarrow_{Aexp} n \overset{\text{IA für } a_2}{\Longleftrightarrow} (\sigma, n) \in [\![a_2]\!]_{\mathcal{A}}$$

$$\Big\Updownarrow (Def.[\![.]\!]_{\mathcal{A}})$$

$$(\sigma, m + n) \in [\![a_1 + a_2]\!]_{\mathcal{A}}$$

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

## 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 $\langle a_1, \sigma\rangle \rightarrow_{Aexp} \bot \Leftrightarrow \sigma \notin Dom([\![a_1]\!]_{\mathcal{A}})$.
    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 $n \neq \bot$, $m = \bot$: analog.

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

## Induktionsschritte

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

$$\langle a_1/a_2, \sigma\rangle \rightarrow_{Aexp} m/n \overset{(\text{Def. } \langle .,.\rangle \rightarrow_{Aexp})}{\Longleftrightarrow} \langle a_1, \sigma\rangle \rightarrow_{Aexp} m \overset{\text{IA für } a_1}{\Longleftrightarrow} (\sigma, m) \in [\![a_1]\!]_{\mathcal{A}}$$

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

$$\langle a_2, \sigma\rangle \rightarrow_{Aexp} n \overset{\text{IA für } a_2}{\Longleftrightarrow} (\sigma, n) \in [\![a_2]\!]_{\mathcal{A}}$$

$$\Updownarrow (Def.[\![.]\!]_{\mathcal{A}})$$

$$(\sigma, m/n) \in [\![a_1/a_2]\!]_{\mathcal{A}}$$

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

## Induktionsschritte

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

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

# Operationale vs. denotationale Semantik

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

# Operationale vs. denotationale Semantik

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

# Äquivalenz operationale und denotationale Semantik

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

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

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

- Beweis Prinzip?

# Äquivalenz operationale und denotationale Semantik

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

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

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

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

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

## Induktionsanfänge

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

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

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

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

**Beweis** $\forall b \in \textbf{Bexp}. \forall t \in \mathbb{B}. \forall \sigma. \quad \langle b, \sigma \rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma, t) \in [\![b]\!]_{\mathcal{B}}$
$\wedge \quad \langle b, \sigma \rangle \rightarrow_{Bexp} \perp \Leftrightarrow \sigma \notin \textbf{\textit{Dom}}([\![b]\!]_{\mathcal{B}})$

## Induktionsschritte

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

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

  Induktionsannahme gilt für $b_1$ und $b_2$.

  - Fall $\langle b_1, \sigma \rangle \rightarrow_{Bexp} \perp$

$$\langle b_1 \&\& b_2, \sigma \rangle \rightarrow_{Bexp} \perp \xLeftrightarrow{(\text{Def. } \langle .,. \rangle \rightarrow_{Bexp} .)} \langle b_1, \sigma \rangle \rightarrow_{Bexp} \perp \xLeftrightarrow{\text{IA für } b_1} \sigma \notin \mathit{Dom}([\![b_1]\!]_{\mathcal{B}})$$

$$\sigma \notin \mathit{Dom}([\![b_1]\!]_{\mathcal{B}}) \overset{\text{Def. } [\![.]\!]_{\mathcal{B}}}{\Longrightarrow} \sigma \notin [\![b_1 \&\& b_2]\!]_{\mathcal{B}}$$

**Beweis** $\forall b \in \textbf{Bexp}. \forall t \in \mathbb{B}. \forall \sigma. \quad \langle b, \sigma \rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma, t) \in [\![b]\!]_{\mathcal{B}}$
$\quad \wedge \quad \langle b, \sigma \rangle \rightarrow_{Bexp} \perp \Leftrightarrow \sigma \notin \textbf{\textit{Dom}}([\![b]\!]_{\mathcal{B}})$

## Induktionsschritte

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

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

  Induktionsannahme gilt für $b_1$ und $b_2$.

  - Fall $\langle b_1, \sigma \rangle \rightarrow_{Bexp} \mathit{false}$

$$\langle b_1 \&\& b_2, \sigma \rangle \rightarrow_{Bexp} \mathit{false} \overset{(\text{Def. } \langle .,. \rangle \rightarrow_{Bexp}.)}{\Longleftrightarrow} \langle b_1, \sigma \rangle \rightarrow_{Bexp} \mathit{false} \overset{\text{IA für } b_1}{\Longleftrightarrow} (\sigma, \mathit{false}) \in [\![b_1]\!]_{\mathcal{B}}$$

$$\overset{\text{Def. } [\![.]\!]_{\mathcal{B}}}{\Longrightarrow} (\sigma, \mathit{false}) \in [\![b_1 \&\& b_2]\!]_{\mathcal{B}}$$

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

## Induktionsschritte

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

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

Induktionsannahme gilt für $b_1$ und $b_2$.

- Fall $\langle b_1, \sigma \rangle \rightarrow_{Bexp} \mathit{true}, \langle b_2, \sigma \rangle \rightarrow_{Bexp} \mathit{false}$

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

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

$$\langle b_2, \sigma \rangle \rightarrow_{Bexp} \mathit{false} \xLeftrightarrow{\text{IA für } b_2} (\sigma, \mathit{false}) \in [\![b_2]\!]_{\mathcal{B}}$$

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

$$(\sigma, \mathit{false}) \in [\![b_1 \&\& b_2]\!]_{\mathcal{B}}$$

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

## Induktionsschritte

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

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

Induktionsannahme gilt für $b_1$ und $b_2$.

- Fall $\langle b_1, \sigma \rangle \rightarrow_{Bexp} true, \langle b_2, \sigma \rangle \rightarrow_{Bexp} true$

$$
\langle b_1 \&\& b_2, \sigma \rangle \rightarrow_{Bexp} true \overset{(\text{Def. } \langle .,. \rangle \rightarrow_{Bexp})}{\Longleftrightarrow} \langle b_1, \sigma \rangle \rightarrow_{Bexp} true \overset{\text{IA für } b_1}{\Longleftrightarrow} (\sigma, true) \in [\![b_1]\!]_{\mathcal{B}}
$$

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

$$
\langle b_2, \sigma \rangle \rightarrow_{Bexp} true \overset{\text{IA für } b_2}{\Longleftrightarrow} (\sigma, true) \in [\![b_2]\!]_{\mathcal{B}}
$$

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

$$
(\sigma, true) \in [\![b_1 \&\& b_2]\!]_{\mathcal{B}}
$$

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

## Induktionsschritte

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

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

Induktionsannahme gilt für $b_1$ und $b_2$.

- Fall $\langle b_1, \sigma \rangle \rightarrow_{Bexp} \mathit{true}, \langle b_2, \sigma \rangle \rightarrow_{Bexp} \perp$

$$\begin{array}{ccccc}
\langle b_1 \&\& b_2, \sigma \rangle \rightarrow_{Bexp} \perp & \overset{(\text{Def. } \langle .,. \rangle \rightarrow_{Bexp})}{\Longleftrightarrow} & \langle b_1, \sigma \rangle \rightarrow_{Bexp} \mathit{true} & \overset{\text{IA für } b_1}{\Longleftrightarrow} & (\sigma, \mathit{true}) \in [\![b_1]\!]_{\mathcal{B}} \\
 & & \& & & \& \\
 & & \langle b_2, \sigma \rangle \rightarrow_{Bexp} \perp & \overset{\text{IA für } b_2}{\Longleftrightarrow} & \sigma \notin Dom([\![b_2]\!]_{\mathcal{B}}) \\
 & & & & \Big\Downarrow {\scriptstyle \text{Def. } [\![.]\!]_{\mathcal{B}}} \\
 & & & & \sigma \notin Dom([\![b_1 \&\& b_2]\!]_{\mathcal{B}})
\end{array}$$

**Beweis** $\forall b \in \mathbf{Bexp}.\, \forall t \in \mathbb{B}.\, \forall \sigma. \quad \langle b, \sigma\rangle \rightarrow_{Bexp} t \Leftrightarrow (\sigma, t) \in [\![b]\!]_{\mathcal{B}}$
$\qquad\qquad\qquad\qquad\qquad \wedge \quad \langle b, \sigma\rangle \rightarrow_{Bexp} \perp \Leftrightarrow \sigma \notin \boldsymbol{Dom}([\![b]\!]_{\mathcal{B}})$

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

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

# Arbeitsblatt 4.2: Beweis Induktionsanfang

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

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

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

**Beweis**

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

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

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

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

**Beweis**

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

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

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

$$
\langle a_1 == a_2, \sigma\rangle \rightarrow_{Bexp} false \overset{(\text{Def. } \langle .,. \rangle \rightarrow_{Bexp}.)}{\Longleftrightarrow} \langle a_1, \sigma\rangle \rightarrow_{Aexp} m \overset{\text{Lemma für } a_1}{\Longleftrightarrow} (\sigma, m) \in [\![a_1]\!]_{\mathcal{A}}
$$

$$
\&
$$

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

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

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

**Beweis**

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

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

- Fall $\langle a_1 == a_2, \sigma\rangle \rightarrow_{Bexp} \perp$:

$$\begin{tikzcd}
\langle a_1 == a_2, \sigma\rangle \rightarrow_{Bexp} \perp \arrow[r, Leftrightarrow, "(\text{Def. } \langle .,. \rangle \rightarrow_{Bexp})"] & \langle a_1, \sigma\rangle \rightarrow_{Aexp} \perp \arrow[r, Leftrightarrow, "\text{Lemma für } a_1"] \arrow[d, phantom, "\vee"] & \sigma \notin Dom([\![a_1]\!]_{\mathcal{A}}) \arrow[d, phantom, "\vee"] \\
& \langle a_2, \sigma\rangle \rightarrow_{Aexp} \perp \arrow[r, Leftrightarrow, "\text{Lemma für } a_2"] & \sigma \notin Dom([\![a_2]\!]_{\mathcal{A}}) \arrow[d, Leftrightarrow, "\text{Def. } [\![.]\!]_{\mathcal{B}}"'] \\
& & \sigma \notin Dom([\![a_1 == a_2]\!]_{\mathcal{B}})
\end{tikzcd}$$

# Operationale vs. denotationale Semantik

| | **Operational** $\langle c, \sigma \rangle \rightarrow_{Stmt} \sigma' \mid \perp$ | **Denotational** $[\![c]\!]_{\mathcal{C}}$ |
|---|---|---|
| $\{\,\}$ | $\dfrac{}{\langle \{\}, \sigma \rangle \rightarrow_{Stmt} \sigma}$ | $[\![\{\,\}]\!]_{\mathcal{C}} = Id$ |
| $c_1; c_2$ | $\dfrac{\langle c_1, \sigma \rangle \rightarrow_{Stmt} \sigma' \neq \perp \quad \langle c_2, \sigma' \rangle \rightarrow_{Stmt} \sigma''}{\langle c_1; c_2, \sigma \rangle \rightarrow_{Stmt} \sigma''}$ <br> $\dfrac{\langle c_1, \sigma \rangle \rightarrow_{Stmt} \perp}{\langle c_1; c_2, \sigma \rangle \rightarrow_{Stmt} \perp}$ | $[\![c_1]\!]_{\mathcal{C}} \circ [\![c_2]\!]_{\mathcal{C}}$ |
| $x = a$ | $\dfrac{\langle a, \sigma \rangle \rightarrow_{Aexp} n}{\langle x = a, \sigma \rangle \rightarrow_{Stmt} \sigma[x \mapsto n]}$ <br> $\dfrac{\langle a, \sigma \rangle \rightarrow_{Aexp} \perp}{\langle x = a, \sigma \rangle \rightarrow_{Stmt} \perp}$ | $\{(\sigma, \sigma[x \mapsto n]) \mid (\sigma, n) \in [\![a]\!]_{\mathcal{A}}\}$ |

# Operationale vs. denotationale Semantik

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

# Operationale vs. denotationale Semantik

**Operational** $\langle c, \sigma \rangle \to_{Stmt} \sigma' \mid \perp$ **Denotational** $[\![c]\!]_{\mathcal{C}}$

$\underbrace{\textbf{while } (b)\ c}_{w}$

$$\frac{\langle b, \sigma \rangle \to_{Bexp} \mathit{false}}{\langle w, \sigma \rangle \to_{Stmt} \sigma} \qquad \frac{\langle b, \sigma \rangle \to_{Bexp} \perp}{\langle w, \sigma \rangle \to_{Stmt} \perp}$$

$$\mathit{fix}(\Gamma)$$

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

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

mit

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

# Äquivalenz operationale und denotationale Semantik

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

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

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

- $\Rightarrow$ Beweis Prinzip?

- $\Leftarrow$ Beweis Prinzip?

# Operationale Semantik: C0 Programme

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

**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** | **if** $(b)$ $c_1$ **else** $c_2$ | **while** $(b)$ $c$ | $c_1; c_2$ | $\{\,\}$

**Regeln:**

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

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

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

# Operationale Semantik: C0 Programme

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

**Regeln:**

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

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

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

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

# Ableitungstiefe für Programme

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

$$\frac{\begin{array}{c}\vdots\\ \mathit{Prämisse}_1\end{array} \quad \cdots \quad \begin{array}{c}\vdots\\ \mathit{Prämisse}_n\end{array}}{\mathit{Conclusion}}$$

# Operationale Semantik: C0 Programme

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

**Regeln:** **Programmstruktur**

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

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

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

$$\frac{\langle b, \sigma\rangle \to_{Bexp} \mathit{true} \qquad \langle c, \sigma\rangle \to_{Stmt} \sigma' \qquad \langle \mathbf{while}\ (b)\ c, \sigma'\rangle \to_{Stmt} \sigma''}{\langle \mathbf{while}\ (b)\ c, \sigma\rangle \to_{Stmt} \sigma''} \quad \to$$

$$\frac{\langle b, \sigma\rangle \to_{Bexp} \mathit{true} \qquad \langle c, \sigma\rangle \to_{Stmt} \bot}{\langle \mathbf{while}\ (b)\ c, \sigma\rangle \to_{Stmt} \bot} \quad \searrow$$

# Operationale Semantik: C0 Programme

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

## Regeln:

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

# Äquivalenz operationale und denotationale Semantik

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

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

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

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

# Äquivalenz operationale und denotationale Semantik

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

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

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

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

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

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

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

**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 $c \equiv \{\}$: ...

**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. $\langle c, \sigma\rangle \rightarrow_{Stmt} \perp \Rightarrow \sigma \notin \textbf{\textit{Dom}}([\![c]\!]_{\mathcal{C}})$

Induktionsschritt:

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

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

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

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

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

$$\langle c_1, \sigma\rangle \rightarrow_{Stmt} \sigma' \overset{\text{IH für } c_1}{\Longleftrightarrow} (\sigma, \sigma') \in [\![c_1]\!]_{\mathcal{C}}$$

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

$$(\sigma, \sigma') \in [\![\textbf{if}(b)\ c_1\ \textbf{else}\ c_2]\!]_{\mathcal{C}}$$

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

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

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

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

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

$$
\langle c_2, \sigma\rangle \rightarrow_{Stmt} \sigma' \overset{\text{IH für } c_2}{\Longleftrightarrow} (\sigma, \sigma') \in [\![c_2]\!]_{\mathcal{C}}
$$

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

$$
(\sigma, \sigma') \in [\![\textbf{if}(b)\ c_1\ \textbf{else}\ c_2]\!]_{\mathcal{C}}
$$

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

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

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

$$
\langle \textbf{if}(b)\ c_1\ \textbf{else}\ c_2, \sigma\rangle \rightarrow_{Stmt} \bot \overset{(\text{Def. } \langle .,.\rangle \rightarrow_{Stmt}.)}{\Longleftrightarrow} \langle b, \sigma\rangle \rightarrow_{Bexp} \mathit{true} \overset{\text{Lemma für } b}{\Longleftrightarrow} (\sigma, \mathit{true}) \in [\![b]\!]_{\mathcal{B}}
$$

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

$$
\langle c_1, \sigma\rangle \rightarrow_{Stmt} \bot \overset{\text{IH für } c_1}{\Longleftrightarrow} \sigma \notin \mathit{Dom}([\![c_1]\!]_{\mathcal{C}})
$$

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

$$
\sigma \notin \mathit{Dom}([\![\textbf{if}(b)\ c_1\ \textbf{else}\ c_2]\!]_{\mathcal{C}})
$$

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

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

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

$$
\langle \textbf{if}(b)\ c_1\ \textbf{else}\ c_2, \sigma\rangle \rightarrow_{Stmt} \bot \overset{\text{(Def. } \langle .,.\rangle \rightarrow_{Stmt}.)}{\Longleftrightarrow} \langle b, \sigma\rangle \rightarrow_{Bexp} \bot \overset{\text{Lemma für } b}{\Longleftrightarrow} \sigma \notin \mathit{Dom}([\![b]\!]_{\mathcal{B}})
$$

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

$$
\sigma \notin \mathit{Dom}([\![\textbf{if}(b)\ c_1\ \textbf{else}\ c_2]\!]_{\mathcal{C}})
$$

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

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

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

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

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

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

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

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

# Äquivalenz operationale und denotationale Semantik

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

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

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

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

- $\Leftarrow$ Beweis Prinzip?

# Äquivalenz operationale und denotationale Semantik

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

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

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

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

- $\Leftarrow$ Beweis per struktureller Induktion über $c$ (Verwendung der Äquivalenz für arithmetische und boolsche Ausdrücke). Für die While-Schleife Rückgriff auf Definition des Fixpunkts und Induktion über die Teilmengen $\Gamma^i(\emptyset)$ des Fixpunkts. (Warum?)

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

Induktionsanfang:

- Fall $c \equiv x = a$:

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

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

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

Induktionsanfang:

- Fall $c \equiv \{\}$

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

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

## 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 **if** $(b)$ $c_1$ **else** $c_2$:

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

Induktionsannahme gilt für $c_1$ und $c_2$

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

$$\begin{array}{rl} & (\sigma, \sigma') \in \{(\sigma'', \sigma''') | (\sigma'', \mathit{true}) \in [\![b]\!]_{\mathcal{B}}, (\sigma'', \sigma''') \in [\![c_1]\!]_{\mathcal{C}}\} \\ \stackrel{\text{Def. } [\![.]\!]_{\mathcal{C}}\,..}{\Longrightarrow} & (\sigma, \mathit{true}) \in [\![b]\!]_{\mathcal{B}} \wedge (\sigma, \sigma') \in [\![c_1]\!]_{\mathcal{C}} \\ \stackrel{\text{Lemma } \textbf{BExp}}{\Longrightarrow} & \langle b, \sigma \rangle \rightarrow_{Bexp} \mathit{true} \wedge (\sigma, \sigma') \in [\![c_1]\!]_{\mathcal{C}} \\ \stackrel{\text{IA für } c_1}{\Longrightarrow} & \langle b, \sigma \rangle \rightarrow_{Bexp} \mathit{true} \wedge \langle c_1, \sigma \rangle \rightarrow_{Stmt} \sigma' \\ \stackrel{\text{Def. } \langle .,. \rangle \rightarrow_{Stmt}\,.}{\Longrightarrow} & \langle \textbf{if } (b)\ c_1 \textbf{ else } c_2, \sigma \rangle \rightarrow_{Stmt} \sigma' \end{array}$$

**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 **if** $(b)$ $c_1$ **else** $c_2$:

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

Induktionsannahme gilt für $c_1$ und $c_2$

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

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

## **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** $(b)$ $c$:

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

Induktionshypothese gilt für $c$

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

## **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** $(b)$ $c$:

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

Induktionshypothese gilt für $c$

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

## **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** $(b)$ $c$:

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

Induktionshypothese gilt für $c$

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

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

## 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** $(b)$ $c$:

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

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

## 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** $(b)$ $c$:

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

Induktionshypothese gilt für $c$

$$
\begin{aligned}
(\sigma, \sigma') \in [\![\textbf{while}\ (b)\ c]\!]_{\mathcal{C}} &\overset{\text{Def. } [\![.]\!]_{\mathcal{C}}..}{\Longrightarrow} (\sigma, \sigma') \in \mathit{fix}(\Gamma) \\
&\overset{\text{Def. } \mathit{fix}(\Gamma)}{\Longrightarrow} (\sigma, \sigma') \in \bigcup_{i \in \mathbb{N}} \Gamma^i(\emptyset) \\
&\overset{(1)}{\Longrightarrow} \langle \textbf{while}\ (b)\ c, \sigma \rangle \rightarrow_{Stmt} \sigma'
\end{aligned}
$$

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)

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

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

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

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 $\mathit{false} \Rightarrow F$ immer wahr

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**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 $c$

$$
\begin{aligned}
(\sigma, \sigma') \in [\![\textbf{while}\ (b)\ c]\!]_{\mathcal{C}} &\overset{\text{Def. } [\![.]\!]_{\mathcal{C}}..}{\Longrightarrow} && (\sigma, \sigma') \in \mathit{fix}(\Gamma) \\
&\overset{\text{Def. } \mathit{fix}(\Gamma)}{\Longrightarrow} && (\sigma, \sigma') \in \bigcup_{i \in \mathbb{N}} \Gamma^i(\emptyset) \\
&\overset{(1)}{\Longrightarrow} && \langle \textbf{while}\ (b)\ c, \sigma\rangle \rightarrow_{Stmt} \sigma'
\end{aligned}
$$

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 $c \in \mathbf{Stmt}$, für alle Zustände $\sigma, \sigma'$:

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

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

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

# 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