Korrekte Software: Grundlagen und Methoden
Vorlesung 3 vom 20.04.17: Operationale Semantik

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2017

Fahrplan

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

Zutaten

```
// GGT(A,B)
if (a == 0) r = b;
else {
  while (b != 0) {
   if (a <= b)
      b = b - a;
   else a = a - b;
  }
  r = a;
}
```

- Programme berechnen Werte
- Basierend auf
  - Werte sind Variablen zugewiesen
  - Evaluation von Ausdrücken
- Folgt dem Programmablauf

Unsere Programmiersprache

Wir betrachten einen Ausschnitt der Programmiersprache C (C0).

Ausbaustufe 1 kennt folgende Konstrukte:

- Typen: **int**;
- Ausdrücke: Variablen, Literale (für ganze Zahlen), arithmetische Operatoren (für ganze Zahlen), Relationen (==, !=, <=, ...), boolsche Operatoren (&&, ||);
- Anweisungen:
  - Fallunterscheidung (**if** ... **else** ...), Iteration (**while**), Zuweisung, Blöcke;
  - Sequenzierung und leere Anweisung sind implizit

Semantik von C0

- Die (operationale) Semantik einer imperativen Sprache wie C0 ist ein Zustandsübergang: das System hat einen impliziten Zustand, der durch Zuweisung von Werten an Adressen geändert werden kann.
- Konkretes Beispiel: $n = 3$

$$\begin{array}{|c|c|}\hline p & ? \\ \hline c & ? \\ \hline n & 3 \\ \hline\end{array} \rightsquigarrow \begin{array}{|c|c|}\hline p & 1 \\ \hline c & ? \\ \hline n & 3 \\ \hline\end{array} \rightsquigarrow \begin{array}{|c|c|}\hline p & 1 \\ \hline c & 1 \\ \hline n & 3 \\ \hline\end{array} \rightsquigarrow \begin{array}{|c|c|}\hline p & 1 \\ \hline c & 1 \\ \hline n & 3 \\ \hline\end{array} \rightsquigarrow \ldots \begin{array}{|c|c|}\hline p & 6 \\ \hline c & 4 \\ \hline n & 3 \\ \hline\end{array}$$

```
p = 1;
c = 1;
while (c <= n){
  p = p * c;
  c = c + 1; }
```

Systemzustände

- Ausdrücke werten zu Werten $\mathbf{V}$ (hier ganze Zahlen) aus.
- Adressen **Loc** sind hier Programmvariablen (Namen)
- Ein Systemzustand bildet Adressen auf Werte ab: $\Sigma = \mathbf{Loc} \rightharpoonup \mathbf{V}$
- Ein Programm bildet einen Anfangszustand möglicherweise auf einen Endzustand ab (wenn es terminiert).
- Zusicherungen sind Prädikate über dem Systemzustand.

C0: Ausdrücke und Anweisungen

$$
\begin{array}{rl}
\text{Aexp} & a ::= \mathbf{N} \mid \mathbf{Loc} \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2 \mid a_1 / a_2 \\
\text{Bexp} & b ::= \mathbf{0} \mid \mathbf{1} \mid a_1 == a_2 \mid a_1 != a_2 \\
 & \quad \mid a_1 <= a_2 \mid !b \mid b_1 \mathbin{\&\&} b2 \mid b_1 \mathbin{||} b_2 \\
\text{Exp} & e := \mathbf{Aexp} \mid \mathbf{Bexp} \\
\text{Stmt} & c \ ::= \quad \mathbf{Loc} = \mathbf{Exp}; \\
 & \quad \mid \quad \mathbf{if}\ (\ b\ )\ c_1\ \ \mathbf{else}\ \ c_2 \\
 & \quad \mid \quad \mathbf{while}\ (\ b\ )\ c \\
 & \quad \mid \quad \{c^*\}
\end{array}
$$

Eine Handvoll Beispiele

```
// {y = Y ∧ y ≥ 0}
x = 1;
while (y != 0) {
 y = y-1;
 x = 2*x;
}
// {x = 2^Y}
```

```
// {a ≥ 0 ∧ b ≥ 0}
r = b;
q = 0;
while (b <= r) {
   r = r-y;
   q = q+1;
   }
// {a = b * q + r ∧ r < b}
```

```
p = 1;
c = 1;
while (c<=n) {
   c = c+1;
   p = p*c;
}
// {p = n!}
```

```
// {0 ≤ a}
t = 1;
s = 1;
i = 0;
while (s <= a) {
   t = t + 2;
   s = s + t;
   i = i + 1;
   }
// {i^2 ≤ a ∧ a < (i + 1)^2}
```

Operationale Semantik: Arithmetische Ausdrücke

Ein arithmetischer Ausdruck a wertet unter gegebenen Zustand σ zu einer ganzen Zahl n (Wert) aus oder zu einem Fehler $\perp$.

- **Aexp** $a ::= \mathbf{N} \mid \mathbf{Loc} \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2 \mid a_1 \ / \ a_2$
- Zustände bilden Adressen/Programmvariablen auf **Werte** ab (σ)

$$\langle a, \sigma \rangle \rightarrow_{Aexp} n | \perp$$

Operationale Semantik: Arithmetische Ausdrücke

Ein arithmetischer Ausdruck a wertet unter gegebenen Zustand σ zu einer ganzen Zahl n (Wert) aus oder zu einem Fehler $\perp$.

- **Aexp** $a ::=$ **N** $|$ **Loc** $| \; a_1 + a_2 \; | \; a_1 - a_2 \; | \; a_1 * a_2 \; | \; a_1 \; / \; a_2$
- Zustände bilden Adressen/Programmvariablen auf **Werte** ab (σ)

$$\langle a, \sigma \rangle \rightarrow_{Aexp} n | \perp$$

Regeln:

$$\frac{}{\langle n, \sigma \rangle \rightarrow_{Aexp} n}$$

Operationale Semantik: Arithmetische Ausdrücke

Ein arithmetischer Ausdruck a wertet unter gegebenen Zustand σ zu einer ganzen Zahl n (Wert) aus oder zu einem Fehler $\perp$.

- **Aexp** $a ::= \mathbf{N} \mid \mathbf{Loc} \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2 \mid a_1 \ / \ a_2$
- Zustände bilden Adressen/Programmvariablen auf **Werte** ab (σ)

$$\langle a, \sigma \rangle \rightarrow_{Aexp} n | \perp$$

Regeln:

$$\frac{}{\langle n, \sigma \rangle \rightarrow_{Aexp} n}$$

$$\frac{X \in \mathbf{Loc}, X \in Dom(\sigma), \sigma(X) = v}{\langle X, \sigma \rangle \rightarrow_{Aexp} v} \qquad \frac{X \in \mathbf{Loc}, X \notin Dom(\sigma)}{\langle X, \sigma \rangle \rightarrow_{Aexp} \perp}$$

Operationale Semantik: Arithmetische Ausdrücke

- **Aexp** $a ::= \mathbf{N} \mid \mathbf{Loc} \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2 \mid a_1 \,/\, a_2$

$$\langle a, \sigma \rangle \rightarrow_{Aexp} n | \bot$$

$$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \rightarrow_{Aexp} n_2 \qquad n_i \in \mathbf{N}, n \text{ Summe } n_1 \text{ und } n_2}{\langle a_1 + a_2, \sigma \rangle \rightarrow_{Aexp} n}$$

$$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \rightarrow_{Aexp} n_2 \qquad \text{falls } n_1 = \bot \text{ oder } n_2 = \bot}{\langle a_1 + a_2, \sigma \rangle \rightarrow_{Aexp} \bot}$$

Operationale Semantik: Arithmetische Ausdrücke

- **Aexp** $a ::= \mathbf{N} \mid \mathbf{Loc} \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2 \mid a_1 \;/\; a_2$

$$\langle a, \sigma \rangle \rightarrow_{Aexp} n | \bot$$

$$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \rightarrow_{Aexp} n_2 \qquad n_i \in \mathbf{N}, n \text{ Summe } n_1 \text{ und } n_2}{\langle a_1 + a_2, \sigma \rangle \rightarrow_{Aexp} n}$$

$$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \rightarrow_{Aexp} n_2 \qquad \text{falls } n_1 = \bot \text{ oder } n_2 = \bot}{\langle a_1 + a_2, \sigma \rangle \rightarrow_{Aexp} \bot}$$

$$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \rightarrow_{Aexp} n_2 \qquad n_i \in \mathbf{N}, n \text{ Diff. } n_1 \text{ und } n_2}{\langle a_1 - a_2, \sigma \rangle \rightarrow_{Aexp} n}$$

$$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \rightarrow_{Aexp} n_2 \qquad \text{falls } n_1 = \bot \text{ oder } n_2 = \bot}{\langle a_1 - a_2, \sigma \rangle \rightarrow_{Aexp} \bot}$$

Operationale Semantik: Arithmetische Ausdrücke

- **Aexp** $a ::= \mathbf{N} \mid \mathbf{Loc} \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2 \mid a_1 \ / \ a_2$

$$\langle a, \sigma \rangle \rightarrow_{Aexp} n | \perp$$

$$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \rightarrow_{Aexp} n_2 \qquad n_i \in \mathbf{N}, n \text{ Produkt } n_1 \text{ und } n_2}{\langle a_1 * a_2, \sigma \rangle \rightarrow_{Aexp} n}$$

$$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \rightarrow_{Aexp} n_2 \qquad \text{falls } n_1 = \perp \text{ oder } n_2 = \perp}{\langle a_1 * a_2, \sigma \rangle \rightarrow_{Aexp} \perp}$$

Operationale Semantik: Arithmetische Ausdrücke

- **Aexp** $a ::= \mathbf{N} \mid \mathbf{Loc} \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2 \mid a_1 \ / \ a_2$

$$\langle a, \sigma \rangle \to_{Aexp} n | \bot$$

$$\frac{\langle a_1, \sigma \rangle \to_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \to_{Aexp} n_2 \qquad n_i \in \mathbf{N}, n \text{ Produkt } n_1 \text{ und } n_2}{\langle a_1 * a_2, \sigma \rangle \to_{Aexp} n}$$

$$\frac{\langle a_1, \sigma \rangle \to_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \to_{Aexp} n_2 \qquad \text{falls } n_1 = \bot \text{ oder } n_2 = \bot}{\langle a_1 * a_2, \sigma \rangle \to_{Aexp} \bot}$$

$$\frac{\langle a_1, \sigma \rangle \to_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \to_{Aexp} n_2 \qquad n_i \in \mathbf{N}, n_2 \neq 0, n \text{ Quotient } n_1, n_2}{\langle a_1 / a_2, \sigma \rangle \to_{Aexp} n}$$

$$\frac{\langle a_1, \sigma \rangle \to_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \to_{Aexp} n_2 \qquad \text{falls } n_1 = \bot, n_2 = \bot \text{ oder } n_2 = 0}{\langle a_1 / a_2, \sigma \rangle \to_{Aexp} \bot}$$

Beispiel-Ableitungen

Sei $\sigma(X) = 6, \sigma(Y) = 5$.

$$\frac{}{\langle (X + Y) * (X - Y), \sigma \rangle \to_{Aexp}}$$

Beispiel-Ableitungen

Sei $\sigma(X) = 6, \sigma(Y) = 5$.

$$\dfrac{\dfrac{}{\langle X + Y, \sigma \rangle \rightarrow_{Aexp}} \qquad \dfrac{}{\langle X - Y, \sigma \rangle \rightarrow_{Aexp}}}{\langle (X + Y) * (X - Y), \sigma \rangle \rightarrow_{Aexp}}$$

Beispiel-Ableitungen

Sei $\sigma(X) = 6, \sigma(Y) = 5$.

$$\dfrac{\dfrac{\langle X, \sigma\rangle \to_{Aexp} 6}{\langle X + Y, \sigma\rangle \to_{Aexp}} \qquad \dfrac{}{\langle X - Y, \sigma\rangle \to_{Aexp}}}{\langle (X + Y) * (X - Y), \sigma\rangle \to_{Aexp}}$$

Beispiel-Ableitungen

Sei $\sigma(X) = 6, \sigma(Y) = 5$.

$$\dfrac{\dfrac{\langle X, \sigma\rangle \to_{Aexp} 6 \qquad \langle Y, \sigma\rangle \to_{Aexp} 5}{\langle X + Y, \sigma\rangle \to_{Aexp}} \qquad \dfrac{}{\langle X - Y, \sigma\rangle \to_{Aexp}}}{\langle (X + Y) * (X - Y), \sigma\rangle \to_{Aexp}}$$

Beispiel-Ableitungen

Sei $\sigma(X) = 6, \sigma(Y) = 5$.

$$\cfrac{\cfrac{\langle X, \sigma\rangle \to_{Aexp} 6 \qquad \langle Y, \sigma\rangle \to_{Aexp} 5}{\langle X + Y, \sigma\rangle \to_{Aexp} 11} \qquad \cfrac{}{\langle X - Y, \sigma\rangle \to_{Aexp}}}{\langle (X + Y) * (X - Y), \sigma\rangle \to_{Aexp}}$$

Beispiel-Ableitungen

Sei $\sigma(X) = 6, \sigma(Y) = 5$.

$$\dfrac{\dfrac{\langle X, \sigma\rangle \to_{Aexp} 6 \qquad \langle Y, \sigma\rangle \to_{Aexp} 5}{\langle X + Y, \sigma\rangle \to_{Aexp} 11} \qquad \dfrac{\langle X, \sigma\rangle \to_{Aexp} 6 \qquad \langle Y, \sigma\rangle \to_{Aexp} 5}{\langle X - Y, \sigma\rangle \to_{Aexp}}}{\langle (X + Y) * (X - Y), \sigma\rangle \to_{Aexp}}$$

Beispiel-Ableitungen

Sei $\sigma(X) = 6, \sigma(Y) = 5$.

$$\dfrac{\dfrac{\langle X, \sigma\rangle \rightarrow_{Aexp} 6 \qquad \langle Y, \sigma\rangle \rightarrow_{Aexp} 5}{\langle X + Y, \sigma\rangle \rightarrow_{Aexp} 11} \qquad \dfrac{\langle X, \sigma\rangle \rightarrow_{Aexp} 6 \qquad \langle Y, \sigma\rangle \rightarrow_{Aexp} 5}{\langle X - Y, \sigma\rangle \rightarrow_{Aexp} 1}}{\langle (X + Y) * (X - Y), \sigma\rangle \rightarrow_{Aexp}}$$

Beispiel-Ableitungen

Sei $\sigma(X) = 6, \sigma(Y) = 5$.

$$\dfrac{\dfrac{\langle X, \sigma \rangle \rightarrow_{Aexp} 6 \qquad \langle Y, \sigma \rangle \rightarrow_{Aexp} 5}{\langle X + Y, \sigma \rangle \rightarrow_{Aexp} 11} \qquad \dfrac{\langle X, \sigma \rangle \rightarrow_{Aexp} 6 \qquad \langle Y, \sigma \rangle \rightarrow_{Aexp} 5}{\langle X - Y, \sigma \rangle \rightarrow_{Aexp} 1}}{\langle (X + Y) * (X - Y), \sigma \rangle \rightarrow_{Aexp} 11}$$

Beispiel-Ableitungen

Sei $\sigma(X) = 6, \sigma(Y) = 5$.

$$\dfrac{\dfrac{\langle X, \sigma\rangle \rightarrow_{Aexp} 6 \qquad \langle Y, \sigma\rangle \rightarrow_{Aexp} 5}{\langle X + Y, \sigma\rangle \rightarrow_{Aexp} 11} \qquad \dfrac{\langle X, \sigma\rangle \rightarrow_{Aexp} 6 \qquad \langle Y, \sigma\rangle \rightarrow_{Aexp} 5}{\langle X - Y, \sigma\rangle \rightarrow_{Aexp} 1}}{\langle (X + Y) * (X - Y), \sigma\rangle \rightarrow_{Aexp} 11}$$

$$\dfrac{}{\langle (X * X) - (Y * Y), \sigma\rangle \rightarrow_{Aexp}}$$

Beispiel-Ableitungen

Sei $\sigma(X) = 6, \sigma(Y) = 5$.

$$\cfrac{\cfrac{\langle X, \sigma\rangle \rightarrow_{Aexp} 6 \qquad \langle Y, \sigma\rangle \rightarrow_{Aexp} 5}{\langle X + Y, \sigma\rangle \rightarrow_{Aexp} 11} \qquad \cfrac{\langle X, \sigma\rangle \rightarrow_{Aexp} 6 \qquad \langle Y, \sigma\rangle \rightarrow_{Aexp} 5}{\langle X - Y, \sigma\rangle \rightarrow_{Aexp} 1}}{\langle (X + Y) * (X - Y), \sigma\rangle \rightarrow_{Aexp} 11}$$

$$\cfrac{\cfrac{\langle X, \sigma\rangle \rightarrow_{Aexp} 6 \qquad \langle X, \sigma\rangle \rightarrow_{Aexp} 6}{\langle X * X, \sigma\rangle \rightarrow_{Aexp} 36}}{\langle (X * X) - (Y * Y), \sigma\rangle \rightarrow_{Aexp}}$$

Beispiel-Ableitungen

Sei $\sigma(X) = 6, \sigma(Y) = 5.$

$$\dfrac{\dfrac{\langle X, \sigma\rangle \rightarrow_{Aexp} 6 \qquad \langle Y, \sigma\rangle \rightarrow_{Aexp} 5}{\langle X + Y, \sigma\rangle \rightarrow_{Aexp} 11} \qquad \dfrac{\langle X, \sigma\rangle \rightarrow_{Aexp} 6 \qquad \langle Y, \sigma\rangle \rightarrow_{Aexp} 5}{\langle X - Y, \sigma\rangle \rightarrow_{Aexp} 1}}{\langle (X + Y) * (X - Y), \sigma\rangle \rightarrow_{Aexp} 11}$$

$$\dfrac{\dfrac{\langle X, \sigma\rangle \rightarrow_{Aexp} 6 \qquad \langle X, \sigma\rangle \rightarrow_{Aexp} 6}{\langle X * X, \sigma\rangle \rightarrow_{Aexp} 36} \qquad \dfrac{\langle Y, \sigma\rangle \rightarrow_{Aexp} 5 \qquad \langle Y, \sigma\rangle \rightarrow_{Aexp} 5}{\langle Y * Y, \sigma\rangle \rightarrow_{Aexp} 25}}{\langle (X * X) - (Y * Y), \sigma\rangle \rightarrow_{Aexp}}$$

Beispiel-Ableitungen

Sei $\sigma(X) = 6, \sigma(Y) = 5$.

$$\frac{\dfrac{\langle X, \sigma\rangle \to_{Aexp} 6 \qquad \langle Y, \sigma\rangle \to_{Aexp} 5}{\langle X + Y, \sigma\rangle \to_{Aexp} 11} \qquad \dfrac{\langle X, \sigma\rangle \to_{Aexp} 6 \qquad \langle Y, \sigma\rangle \to_{Aexp} 5}{\langle X - Y, \sigma\rangle \to_{Aexp} 1}}{\langle (X + Y) * (X - Y), \sigma\rangle \to_{Aexp} 11}$$

$$\frac{\dfrac{\langle X, \sigma\rangle \to_{Aexp} 6 \qquad \langle X, \sigma\rangle \to_{Aexp} 6}{\langle X * X, \sigma\rangle \to_{Aexp} 36} \qquad \dfrac{\langle Y, \sigma\rangle \to_{Aexp} 5 \qquad \langle Y, \sigma\rangle \to_{Aexp} 5}{\langle Y * Y, \sigma\rangle \to_{Aexp} 25}}{\langle (X * X) - (Y * Y), \sigma\rangle \to_{Aexp} 11}$$

Operationale Semantik: Boolesche Ausdrücke

- **Bexp** $b ::= 0 \mid 1 \mid a_1 == a_2 \mid a_1 \;<=\; a_2 \mid !b \mid b_1 \;\&\&\; b2 \mid b_1 \;||\; b_2$

Regeln:

$$\langle b, \sigma \rangle \rightarrow_{Bexp} 1|0|\bot$$

$$\frac{}{\langle \mathbf{1}, \sigma \rangle \rightarrow_{Bexp} \mathbf{1}} \qquad \frac{}{\langle \mathbf{0}, \sigma \rangle \rightarrow_{Bexp} \mathbf{0}}$$

$$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \rightarrow_{Aexp} n_2 \qquad n_i \neq \bot, n_1 \text{ und } n_2 \text{ gleich}}{\langle a_1 == a_2, \sigma \rangle \rightarrow_{Bexp} 1}$$

$$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \rightarrow_{Aexp} n_2 \qquad n_i \neq \bot, n_1 \text{ und } n_2 \text{ ungleich}}{\langle a_1 == a_2, \sigma \rangle \rightarrow_{Bexp} 0}$$

$$\frac{\langle a_1, \sigma \rangle \rightarrow_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \rightarrow_{Aexp} n_2 \qquad n_1 = \bot \text{ or } n_2 = \bot}{\langle a_1 == a_2, \sigma \rangle \rightarrow_{Bexp} \bot}$$

Operationale Semantik: Boolesche Ausdrücke

- **Bexp** $b ::= 0 \mid 1 \mid a_1 == a_2 \mid a_1 \;<=\; a_2 \mid !b \mid b_1 \,\&\&\, b2 \mid b_1 \;\;||\;\; b_2$

Regeln:

$$\langle b, \sigma \rangle \rightarrow_{Bexp} 1|0|\bot$$

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} 1}{\langle !b, \sigma \rangle \rightarrow_{Bexp} 0} \qquad \frac{\langle b, \sigma \rangle \rightarrow_{Bexp} 0}{\langle !b, \sigma \rangle \rightarrow_{Bexp} 1} \qquad \frac{\langle b, \sigma \rangle \rightarrow_{Bexp} \bot}{\langle !b, \sigma \rangle \rightarrow_{Bexp} \bot}$$

$$\frac{\langle b_1, \sigma \rangle \rightarrow_{Bexp} t_1 \qquad \langle b_2, \sigma \rangle \rightarrow_{Bexp} t_2}{\langle b_1 \,\&\&\, b_2, \sigma \rangle \rightarrow_{Bexp} t}$$

$$\begin{array}{ll} \text{wobei} & t = 1 \text{ wenn } t_1 = t_2 = 1; \\ & t = 0 \text{ wenn } t_1 = 0 \text{ oder } (t_1 = 1 \text{ und } t_2 = 0); \\ & t = \bot \text{ sonst} \end{array}$$

Operationale Semantik: Boolesche Ausdrücke

- **Bexp** $b ::= 0 \mid 1 \mid a_1 == a_2 \mid a_1 \;\; <= \;\; a_2 \mid !b \mid b_1 \,\&\&\, b2 \mid b_1 \;\; || \;\; b_2$

Regeln:

$$\langle b, \sigma \rangle \rightarrow_{Bexp} 1|0|\bot$$

$$\frac{\langle b_1, \sigma \rangle \rightarrow_{Bexp} t_1 \qquad \langle b_2, \sigma \rangle \rightarrow_{Bexp} t_2}{\langle b_1 \;||\; b_2, \sigma \rangle \rightarrow_{Bexp} t}$$

$$\text{wobei} \quad \begin{array}{l} t = 0 \text{ wenn } t_1 = t_2 = 0; \\ t = 1 \text{ wenn } t_1 = 1 \text{ oder } (t_1 = 0 \text{ und } t_2 = 1); \\ t = \bot \text{ sonst} \end{array}$$

Operationale Semantik: Anweisungen

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

Beispiel:

$$\langle c, \sigma \rangle \rightarrow_{Stmt} \sigma' | \bot$$

$$\langle X = 5, \sigma \rangle \rightarrow_{Stmt} \sigma'$$

wobei $\sigma'(X) = 5$ und $\sigma'(Y) = \sigma(Y)$ für alle $Y \neq X$

Operationale Semantik: Anweisungen

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

Regeln:

Definiere :

$$\sigma[m/X](Y) := \begin{cases} m & \text{if } X = Y \\ \sigma(Y) & \text{sonst} \end{cases}$$

$$\langle X = 5, \sigma \rangle \rightarrow_{Stmt} \sigma[5/X]$$

Es gilt:

$$\begin{aligned} \forall \sigma, n, m, \forall X, Y \,.\, X \neq Y \Rightarrow \sigma[n/X][m/Y] &= \sigma[m/Y][n/X] \\ \forall \sigma, n, m, \forall X \,.\, \sigma[n/X][m/X] &= \sigma[m/X] \end{aligned}$$

Operationale Semantik: Anweisungen

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

Regeln:

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

$$\frac{\langle a, \sigma\rangle \rightarrow_{Aexp} n \in \mathbf{N}}{\langle X = a, \sigma\rangle \rightarrow_{Stmt} \sigma[n/X]} \qquad \frac{\langle a, \sigma\rangle \rightarrow_{Aexp} \perp}{\langle X = a, \sigma\rangle \rightarrow_{Stmt} \perp}$$

$$\frac{\langle c, \sigma\rangle \rightarrow_{Stmt} \sigma' \neq \perp \qquad \langle \{c_s\}, \sigma'\rangle \rightarrow_{Stmt} \sigma'' \neq \perp}{\langle \{c\ \ c_s\}, \sigma\rangle \rightarrow_{Stmt} \sigma''}$$

$$\frac{\langle c, \sigma\rangle \rightarrow_{Stmt} \perp}{\langle \{c\ \ c_s\}, \sigma\rangle \rightarrow_{Stmt} \perp}$$

$$\frac{\langle c, \sigma\rangle \rightarrow_{Stmt} \sigma' \neq \perp \qquad \langle \{c_s\}, \sigma'\rangle \rightarrow_{Stmt} \perp}{\langle \{c\ \ c_s\}, \sigma\rangle \rightarrow_{Stmt} \perp}$$

Operationale Semantik: Anweisungen

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

Regeln:

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

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} 1 \qquad \langle c_1, \sigma \rangle \rightarrow_{Stmt} \sigma'}{\langle \textbf{if}\ (\ b\ )\ c_1\ \textbf{else}\ c_2, \sigma \rangle \rightarrow_{Stmt} \sigma'}$$

$$\frac{\langle b, \sigma \rangle \rightarrow_{Bexp} 0 \qquad \langle c_2, \sigma \rangle \rightarrow_{Stmt} \sigma'}{\langle \textbf{if}\ (\ b\ )\ c_1\ \textbf{else}\ c_2, \sigma \rangle \rightarrow_{Stmt} \sigma'}$$

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

Operationale Semantik: Anweisungen

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

Regeln:

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

$$\frac{\langle b, \sigma\rangle \rightarrow_{Bexp} 0}{\langle \textbf{while}\ (\ b\ )\ c, \sigma\rangle \rightarrow_{Stmt} \sigma}$$

$$\frac{\langle b, \sigma\rangle \rightarrow_{Bexp} 1 \qquad \langle c, \sigma\rangle \rightarrow_{Stmt} \sigma' \qquad \langle \textbf{while}\ (\ b\ )\ c, \sigma'\rangle \rightarrow_{Stmt} \sigma''}{\langle \textbf{while}\ (\ b\ )\ c, \sigma\rangle \rightarrow_{Stmt} \sigma''}$$

$$\frac{\langle b, \sigma\rangle \rightarrow_{Bexp} 1 \qquad \langle c, \sigma\rangle \rightarrow_{Stmt} \perp}{\langle \textbf{while}\ (\ b\ )\ c, \sigma\rangle \rightarrow_{Stmt} \perp} \qquad \frac{\langle b, \sigma\rangle \rightarrow_{Bexp} \perp}{\langle \textbf{while}\ (\ b\ )\ c, \sigma\rangle \rightarrow_{Stmt} \perp}$$

Beispiel

```
x = 1;
while (y != 0) {
 y = y - 1;
 x = 2 * x;
}
// x = 2^y
```

$\sigma(y) = 3$

Äquivalenz arithmetischer Ausdrücke

Gegeben zwei Aexp a_1 and a_2

- Sind sie gleich?

$$a_1 \sim_{Aexp} a_2 \text{ gdw } \forall \sigma, n. \langle a_1, \sigma \rangle \rightarrow_{Aexp} n \Leftrightarrow \langle a_2, \sigma \rangle \rightarrow_{Aexp} n$$

(X*X) + 2*X*Y + (Y*Y) und (X+Y) * (X+Y)

- Wann sind sie gleich?

$$\exists \sigma, n. \langle a_1, \sigma \rangle \rightarrow_{Aexp} n \Leftrightarrow \langle a_2, \sigma \rangle \rightarrow_{Aexp} n$$

X*X und 9*X+22
X*X und X*X+1

Äquivalenz Boolscher Ausdrücke

Gegeben zwei Bexp-Ausdrücke b_1 and b_2

- Sind sie gleich?

$$b_1 \sim_{Bexp} b_2 \text{ iff } \forall \sigma, b. \langle b_1, \sigma \rangle \rightarrow_{Bexp} b \Leftrightarrow \langle b_2, \sigma \rangle \rightarrow_{Bexp} b$$

```
A || (A && B)     und    A
```

Beweisen

Zwei Programme c_0, c_1 sind äquivalent gdw. sie die gleichen Zustandsveränderungen bewirken. Formal definieren wir

Definition

$$c_0 \sim c_1 \text{ iff } \forall \sigma, \sigma'.\ \langle c_0, \sigma \rangle \rightarrow_{Stmt} \sigma' \Leftrightarrow \langle c_1, \sigma \rangle \rightarrow_{Stmt} \sigma'$$

Ein einfaches Beispiel:

Lemma

Sei $w \equiv \textbf{while}\ (\ b\ )\ \ c$ *mit* $b \in \textbf{Bexp}$, $c \in \textbf{Stmt}$.
Dann gilt: $w \sim \textbf{if}\ (\ b\ )\ \{c; w\}\ \ \textbf{else}\ \{\}$

Beweis an der Tafel

Zusammenfassung

- Operationale Semantik als ein Mittel für Beschreibung der Semantik
- Auswertungsregeln arbeiten entlang der syntaktischen Struktur
- Werten Ausdrücke zu Werten aus und Programme zu Zuständen (zu gegebenen Zustand)
- Fragen zu Programmen: Gleichheit