Korrekte Software: Grundlagen und Methoden
Vorlesung 1 vom 19.04.22
Einführung

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2022

Organisatorisches

- Veranstalter:

Serge Autexier
serge.autexier@dfki.de
Cartesium 1.49[1], Tel. 59834

Christoph Lüth
christoph.lueth@dfki.de
MZH 4186, Tel. 59830

- Termine:
  - Dienstag, 10 – 12, MZH 1450
  - Donnerstag, 8 – 10**8:30 – 10:00**, MZH 1450
- Webseite: `https://www.informatik.uni-bremen.de/~cxl/lehre/ksgm.ss22`

Veranstaltungskonzept

- Aus den letzten Jahren: **integrierte Veranstaltung** statt **langer Vorlesung**.
- Kürzere **Vortragseinheiten**, dazwischen **Arbeitsfragen** (Kurzübungen)
- Wöchentliche **Übungsaufgaben** zur Vertiefung
- Technisch:
  - Fragen/Kurzübungen in **HedgeDoc**: `http://hackmd.informatik.uni-bremen.de/`
  - Übungsblätter als **Markdown**, Abgabe über `gitlab`.

Prüfungsform

- 10 Übungsblätter (geplant)
- **Bewertung**:
  - A (sehr gut, 1.3) — nichts zu meckern, keine/kaum Fehler
  - B (gut, 2.3) — kleine Fehler, sonst gut
  - C (befriedigend, 3.3) — größere Fehler oder Mängel
  - Nicht bearbeitet — oder mehr Fehler als Bearbeitung
- **Prüfungsleistung**:
  - **Mündliche Prüfung**: Einzelprüfung ca. 20– 30 Minuten
  - **Übungsbetrieb** (bis zu 15% Bonuspunkte, keine Voraussetzung)

Übungsbetrieb

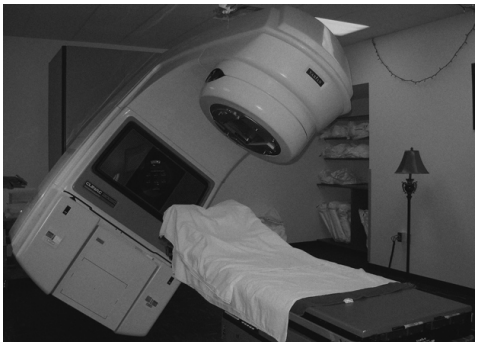
- Abgabe und Korrektur des Übungsbetriebs erfolgt über **gitlab**.
- Dazu legt **pro Gruppe** ein Repository an.
- Ladet uns (`clueth`, `autexier`) als Developer ein.
- Für jedes Übungsblatt:
  1. Das Übungsblatt ladet ihr von der Webseite herunter und bearbeitet es **elektronisch**.
  2. Die Lösung wird als Markdown abgelegt (bitte Namen `uebung-XX.md` nicht verändern; Zusatzmaterial als `uebung-XX-...` wenn nötig), und ladet es **vor** dem Abgabezeitpunkt hoch (`push`).
  3. Nach dem Abgabezeitpunkt laden wir die Änderungen herunter (`pull`), korrigieren direkt im Markdown, fügen die Bewertung hinzu, und laden die Korrektur wieder hoch (`push`)

Arbeitsblatt 1.1: Jetzt seid ihr dran!

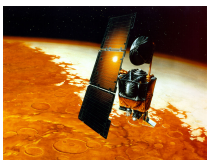
- Gruppiert euch in Gruppen zu drei Teilnehmenden!
- Zu jeder Gruppe gibt es ein Arbeitsblatt:
  `https://hackmd.informatik.uni-bremen.de/Ds7wVjXAQoiszJJPNJffOA#`
- Auf diesem Arbeitsblatt bearbeitet ihr die Arbeitsfragen im Laufe des Kurses.
- Bitte nur in "eurem" Arbeitsblatt arbeiten
- Die Arbeitsblätter sind nicht notenrelevant.

I. Warum Korrekte Software?

Software-Disaster I: Therac-25



Software-Disasters II: Space


Mariner 1 (27.08.1962), Mars Climate Orbiter (1999), Ariane 5 (04.06.1996)

Software-Disaster III: AT&T (15.01.1990)

```
while (! empty(ring_rcv_buffer)
       && ! empty(side_buffer empty)) {
 initialize pointer to first message buffer;
 get copy of buffer;
 switch (message) {
   case (incoming_message):
     if (sender is out_of_service) {
       if (empty(ring_wrt_buffer)) {
         send "in service" to status map;
       } else {
         break;
       }
       process incoming message, set up pointers;
       break;
       }
   }
 do optional parameter work;
 }
```


Software-Disaster IV: Ungeplantes Übergewicht

- „A software mistake caused a Tui flight to take off heavier than expected as female passengers using the title “Miss” were classified as children [...]“
- 38 erwachsene Passagiere als Kinder (35kg) statt als Erwachsene (69kg) klassifiziert.

$$38 \cdot (69\,kg - 35\,kg) = 1292\,kg$$

- Software „was programmed in an unnamed foreign country where the title “Miss” is used for a child and “Ms” for an adult female.“

Quelle: *Guardian, 09.04.2021.*

`https://www.theguardian.com/world/2021/apr/09/tui-plane-serious-incident-every-miss-on-board-child-weight-birmingham-majorca`

Arbeitsblatt 1.2: Jetzt seid ihr dran!

- Sucht im Netz nach weiteren Software-Disastern:
  1. Was ist passiert?
  2. Wie ist es passiert?
  3. Was war der Softwarefehler?
- Quellen: Suchmaschine nach Wahl (“software disasters”), The Risks Digest, `https://catless.ncl.ac.uk/Risks/`

II. Inhalt der Vorlesung

Themen

Korrekte Software im Lehrbuch:
- Spielzeugsprache
- Wenig Konstrukte
- Kleine Beispiele

Korrekte Software im Einsatz:
- Richtige Programmiersprache
- Mehr als nur ganze Zahlen
- Skalierbarkeit — wie können große Programme verifiziert werden?

Inhalt

- Grundlagen:
  - Beweis der **Korrektheit** von Programmen: der **Floyd-Hoare-Kalkül**
  - **Bedeutung** von Programmen: **Semantik**
- Betrachtete Programmiersprache: “C0” (erweiterte Untermenge von C)
- Erweiterung der Programmkonstrukte und des Hoare-Kalküls:
  1. Referenzen (Zeiger)
  2. Funktion und Prozeduren (Modularität)
  3. Reiche **Datenstrukturen** (Felder, `struct`)

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

III. Warum Semantik?

Idee

- Was wird hier berechnet? $p = n!$
- Warum? Wie können wir das **beweisen**?
- Wir berechnen symbolisch, welche Werte Variablen über den Programmverlauf annehmen.

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


Semantik von Programmiersprachen

Drei wesentliche Möglichkeiten:

- **Operationale Semantik**: Ausführung auf einer **abstrakten** Maschine
- **Denotationale Semantik**: Abbildung in ein **mathematisches Objekt**
- **Axiomatische Semantik**: Beschreibung anhand der **Eigenschaften**

Arbeitsblatt 1.3: Maschinen und Funktionen

Was genau kann man sich unter "abstrakten Maschine" vorstellen?

Betrachtet als Beispiele:

- Eine Taschenlampe
- Eine Waschmaschine
- Einen Taschenrechner

Was ist hier die Abstraktion?

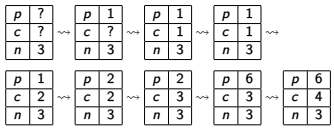
Unsere Sprache C0

- C0 ist eine **Untermenge** der Sprache C
- C0-Programme sind **ausführbare** C-Programme
- Grundausbaustufe:
  - Zuweisungen, Fallunterscheidungen, Schleifen
  - Datentypen: ganze Zahlen mit Arithmetik
  - Relationen: Vergleich ($=, \leq$)
  - Boolsche Operatoren: Konjunktion, Disjunktion, Negation
- 1. Ausbaustufe: Felder und Strukturen
- 2. Ausbaustufe: Funktionen und Prozeduren (nur Ausblick)
- 3. Ausbaustufe: Referenzen (nur Ausblick)
- Fehlt: **union**, **goto**, ...

Operationale Semantik

- Kernkonzept: Zustandstandsübergänge einer abstrakten Maschine
- Abstrakte Maschine hat **impliziten Zustand**
- Zustand ordnet **Adressen** veränderliche **Werte** zu
- Konkretes Beispiel: $n \mapsto 3$, p und c undefiniert

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



Arbeitsblatt 1.4: Operationale Semantik

Gegeben folgendes C0-Programm:

```
1 x= 0;
2 while (n > 0) {
3   x= x+ n*n;
4   n= n-1;
5   }
```

Entwickeln Sie die ersten zehn Schritte der operationalen Semantik wie im Beispiel oben für den initialen Zustand

n	4
x	?

$\rightsquigarrow \ldots$

Denotationale Semantik

- Kernkonzept: Abbildung von Programmen auf mathematisches Gegenstück (**Denotat**)
- **Partielle** Funktionen zwischen Zuständen $[\![c]\!] : \sigma \rightharpoonup \sigma$
- Beispiel:

```
p = 1;
c = 1; // p1
while (c <= n) {
  p = p * c;
  c = c + 1; // p2
  }
// p3
```

$$[\![p_1]\!](\sigma) = \sigma[p \mapsto 1][c \mapsto 1]$$
$$[\![p_2]\!](\sigma) = \sigma[p \mapsto \sigma(p) * \sigma(c)][c \mapsto \sigma(c) + 1]$$
$$[\![p_3]\!](\sigma)[\![p_3]\!] = ??? \; fix(\Gamma([\![c \leq n]\!])([\![p_2]\!]))([\![p_1]\!](\sigma)) \; fix(\Gamma([\![c \leq n]\!])([\![p_2]\!])) \circ [\![$$

$$\Gamma([\![c \leq n]\!])([\![p_2]\!])(\varphi)(\sigma) = \begin{cases} \sigma & \text{if } [\![c \leq n]\!](\sigma) = 0 \\ (\varphi \circ [\![p_2]\!])(\sigma) & \text{if } [\![c \leq n]\!](\sigma) = 1 \end{cases}$$

$$\Gamma(\beta)(\rho)(\varphi)(\sigma) = \begin{cases} \sigma & \text{if } \beta(\sigma) = 0 \\ (\varphi \circ \rho)(\sigma) & \text{if } \beta(\sigma) = 1 \end{cases}$$

Axiomatische Semantik

- Kernkonzept: Charakterisierung von Programmen durch **Zusicherungen**
- Zusicherungen sind zustandsabhängige Prädikate
- Beispiel (mit $n = 3$)

```
// (1)
p = 1; // (2)
c = 1; // (3)
while(c <= n){
  // (4)
  p = p * c;
  c = c + 1;
  // (5)
  }
// (6)
```

(1)
(2)
(3)
(4) $(p = 1 \wedge c = 1 \vee p = 1 \wedge c = 2 \vee p = 2 \wedge c = 3)\ p = (c-1)! \wedge c \leq n \wedge n = 3$
(5)
(6)

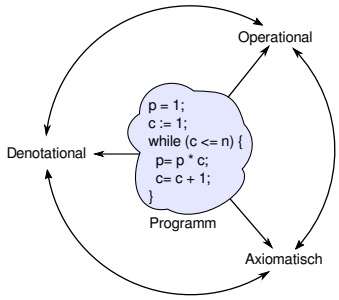
Arbeitsblatt 1.5: Zusicherungen

Betrachten Sie folgende Variation des Programms von oben:

```
// (1)
p = 1; // (2)
c = 1; // (3)
while(c <= n){
  // (4)
  c = c + 1;
  p = p * c;
  }
// (5)
```

- Welche der Zusicherungen (1) – (5) von oben gelten noch?
- Welche nicht? $(p = 1 \wedge c = 2 \vee p = 2 \wedge c = 3 \vee p = 6 \wedge c = 4)\ p = (c-1)! \wedge n = 3 \wedge n = 3$
- Was gilt stattdessen?
  $p = 6 \wedge c = 4 \wedge n = 3$

Drei Semantiken — Eine Sicht



Zusammenfassung

- Wir wollen die **Bedeutung** (Semantik) von Programmen beschreiben, um ihre Korrektheit beweisen zu können.
- Dazu gibt es verschiedene Ansätze, die wir betrachten werden.
- Nächste Woche geht es mit dem ersten los: **operationale** Semantik

Korrekte Software: Grundlagen und Methoden

Vorlesung 2 vom 26.04.22

Operationale Semantik

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2022

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- 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

C0: Ausdrücke und Anweisungen

$$
\begin{array}{rll}
\textbf{Aexp} & a ::= & \mathbf{Z} \mid \mathbf{Idt} \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2 \mid a_1 / a_2 \\
\textbf{Bexp} & b ::= & \mathbf{1} \mid \mathbf{0} \mid a_1 == a_2 \mid a_1 < a_2 \mid !\, b \mid b_1 \,\&\&\, b_2 \mid b_1 \,||\, b_2 \\
\textbf{Exp} & e := & a \mid b \\
\textbf{Stmt} & c ::= & \mathbf{Idt} = \mathbf{Exp} \\
 & \mid & \textbf{if } (b)\ c_1\ \textbf{else}\ c_2 \\
 & \mid & \textbf{while } (b)\ c \\
 & \mid & c_1; c_2 \\
 & \mid & \{\}
\end{array}
$$

NB: Nicht die **konkrete** Syntax.

Was braucht die Semantik?

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

- Ein Programm besteht aus **Anweisungen** und **Ausdrücken**.
- Ausdrücke werden **zustandsabhängig** ausgewertet.
- Anweisungen **überführen** Zustände.

Woraus besteht die Semantik?

1. Mathematische Modellierung des **Zustands**
2. Auswertung von (arithmetischen und boolschen) Ausdrücken
3. Auswertung von Anweisungen: Zustandsübergänge

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.

Systemzustände

- Ausdrücke werten zu **Werten** $\mathbf{V}$ (hier ganze Zahlen) aus.
- Adressen $\mathbf{Loc}$ sind hier Programmvariablen (Namen): $\mathbf{Loc} = \mathbf{Idt}$
- 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).

Partielle, endliche Abbildungen I

Zustände sind **partielle, endliche Abbildungen** (finite partial maps)

$$f : X \rightharpoonup A$$

Notation:

- $f(x)$ für den Wert von x in f (*lookup*)
- $f(x) = \bot$ wenn x nicht in f (*undefined*)
- $f[x \mapsto n]$ für den Update an der Stelle x mit dem Wert n:

$$f[x \mapsto n](y) \stackrel{def}{=} \begin{cases} n & \text{if } x = y \\ f(y) & \text{otherwise} \end{cases}$$

Partielle, endliche Abbildungen II

Zustände sind **partielle, endliche Abbildungen** (finite partial maps)

$$f : X \rightharpoonup A$$

Notation:

- $\langle x \mapsto n, y \mapsto m \rangle$ u.ä. für konkrete Abbildungen.
- $\langle\rangle$ ist die leere (überall undefinierte Abbildung):

$$\text{für alle } x \in X \text{ gilt: } \langle\rangle(x) = \bot$$

- Die Domäne eines Zustands sind alle Stellen, an denen er definiert ist:

$$Dom(f) \stackrel{def}{=} \{x \in X \mid f(x) \neq \bot\}$$

- Updates sind "linksassoziativ":

$$f[x \mapsto n][y \mapsto m] = (f[x \mapsto n])[y \mapsto m]$$

Arbeitsblatt 2.1: Zustände!

- Wie sieht ein Zustand aus, der a den Wert 6 und c den Wert 2 zuweist.
- Welches sind Zustände, und welche nicht:
  - (A) $\langle x \mapsto 1, a \mapsto 3 \rangle$
  - (B) $\langle x \mapsto y, b \mapsto 6 \rangle$
  - (C) $\langle x \mapsto 2, b \mapsto 6, x \mapsto 5 \rangle$
  - (D) $\langle x \mapsto 3, b \mapsto 6, y \mapsto 5 \rangle$
- Update von Zuständen:
  - (A) $\langle x \mapsto 1, a \mapsto 3 \rangle[y \mapsto 1] = ??$
  - (B) $\langle x \mapsto 1, a \mapsto 3 \rangle[x \mapsto 3] = ??$
  - (C) $\langle x \mapsto 1, a \mapsto 3 \rangle[x \mapsto 3][y \mapsto 1][x \mapsto 4] = ??$

Operationale Semantik: Arithmetische Ausdrücke

Ein arithmetischer Ausdruck a wertet unter Zustand σ zu einer ganzen Zahl n (Wert) aus.

$$\textbf{Aexp}\ a ::= \mathbf{Z} \mid \mathbf{Idt} \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2 \mid a_1\ /\ a_2 \qquad \langle a, \sigma \rangle \to_{Aexp} n$$

Regeln:

$$\frac{n \in \mathbf{Z}}{\langle n, \sigma \rangle \to_{Aexp} [\![n]\!]} \qquad \frac{x \in \mathbf{Idt}, x \in Dom(\sigma), \sigma(x) = v}{\langle x, \sigma \rangle \to_{Aexp} v}$$

Operationale Semantik: Arithmetische Ausdrücke

$$\textbf{Aexp}\ a ::= \mathbf{Z} \mid \mathbf{Idt} \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2 \mid a_1\ /\ a_2 \qquad \langle a, \sigma \rangle \to_{Aexp} n$$

$$\frac{\langle a_1, \sigma \rangle \to_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \to_{Aexp} n_2 \qquad n_i \in \mathbb{Z}, n \text{ Summe } n_1 \text{ und } n_2}{\langle a_1 + a_2, \sigma \rangle \to_{Aexp} n}$$

$$\frac{\langle a_1, \sigma \rangle \to_{Aexp} n_1 \qquad \langle a_2, \sigma \rangle \to_{Aexp} n_2 \qquad n_i \in \mathbb{Z}, n \text{ Differenz } n_1 \text{ und } n_2}{\langle a_1 - a_2, \sigma \rangle \to_{Aexp} n}$$

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

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

Ableitungen

- Regeln werden von **unten** nach **oben** gelesen
- Regeln werden **komponiert** — es entsteht ein **Ableitungsbaum**

Beispiel: Auswertung von x+3 mit $\sigma \stackrel{def}{=} \langle x \mapsto 6, y \mapsto 5 \rangle$.

$$\frac{\dfrac{x \in dom(\sigma), \sigma(x) =? 6}{\langle x, \sigma \rangle \to_{Aexp} ?} \qquad \dfrac{x \in dom(\sigma), \sigma(x) = 6}{\langle x, \sigma \rangle \to_{Aexp} 6} \qquad \dfrac{}{\langle 3, \sigma \rangle \to_{Aexp} [\![3]\!]}}{\langle x, \sigma \rangle \to_{Aexp} ?} \qquad \frac{}{\langle 3, \sigma \rangle \to_{Aexp} 3}$$

$$\frac{\dfrac{\langle x, \sigma \rangle \to_{Aexp} ? \qquad \langle 3, \sigma \rangle \to_{Aexp} ?}{\langle x + 3, \sigma \rangle \to_{Aexp} ? + ?} \qquad \dfrac{\langle x, \sigma \rangle \to_{Aexp} 6 \qquad \langle 3, \sigma \rangle \to_{Aexp} 3}{\langle x + 3, \sigma \rangle \to_{Aexp} 6 + 39}}{}$$

Längere Beispiel-Ableitungen

Sei $\sigma \stackrel{def}{=} \langle x \mapsto 6, y \mapsto 5 \rangle$.

$$\frac{\dfrac{\dfrac{x \in dom(\sigma), \sigma(x) = 6}{\langle x, \sigma \rangle \to_{Aexp} 6} \qquad \dfrac{y \in dom(\sigma), \sigma(y) = 5}{\langle y, \sigma \rangle \to_{Aexp} 5}}{\langle x + y, \sigma \rangle \to_{Aexp} 11} \qquad \dfrac{\dfrac{x \in dom(\sigma), \sigma(x) = 6}{\langle x, \sigma \rangle \to_{Aexp} 6} \qquad \dfrac{y \in dom(\sigma), \sigma(y) = 5}{\langle y, \sigma \rangle \to_{Aexp} 5}}{\langle x - y, \sigma \rangle \to_{Aexp} 1}}{\langle (x + y) * (x - y), \sigma \rangle \to_{Aexp} 11}$$

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

Arbeitsblatt 2.2: Auswertung

Konstruiert wie oben die Ableitung für den Ausdruck (3*a)/b mit $\sigma \stackrel{def}{=} \langle a \mapsto 8, b \mapsto 7 \rangle$.

Hinweis: wahrscheinlich einfacher auf Papier...

Eigenschaften der Semantik

- **Frage:** Gegeben einen Ausdruck a, leitet **jeder** Zustand σ zu einem Wert n ab?
- **Antwort:** Nein.
- Betrachte folgende Beispiele für $a \stackrel{def}{=}$ y+3/x

$$\langle a, \langle y \mapsto 5 \rangle \rangle \to_{Aexp} ??? \quad (1)$$
$$\langle a, \langle y \mapsto 5, x \mapsto 0 \rangle \rangle \to_{Aexp} ??? \quad (2)$$

- In diesen Beispielen läßt sich kein **vollständiger** Ableitungsbaum konstruieren.
- Die Auswertung ist **undefiniert** — die Semantik ist **partiell**.

Operationale Semantik: Boolesche Ausdrücke

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

$$\langle b, \sigma\rangle \to_{Bexp} true \mid false$$

Regeln:

$$\frac{}{\langle \mathbf{1}, \sigma\rangle \to_{Bexp} true} \qquad \frac{}{\langle \mathbf{0}, \sigma\rangle \to_{Bexp} false}$$

$$\frac{\langle a_1, \sigma\rangle \to_{Aexp} n_1 \qquad \langle a_2, \sigma\rangle \to_{Aexp} n_2 \qquad n_1 \text{ und } n_2 \text{ gleich}}{\langle a_1 == a_2, \sigma\rangle \to_{Bexp} true}$$

$$\frac{\langle a_1, \sigma\rangle \to_{Aexp} n_1 \qquad \langle a_2, \sigma\rangle \to_{Aexp} n_2 \qquad n_1 \text{ und } n_2 \text{ ungleich}}{\langle a_1 == a_2, \sigma\rangle \to_{Bexp} false}$$

Operationale Semantik: Boolesche Ausdrücke

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

$$\langle b, \sigma\rangle \to_{Bexp} true \mid false$$

Regeln:

$$\frac{\langle b, \sigma\rangle \to_{Bexp} true}{\langle !b, \sigma\rangle \to_{Bexp} false} \qquad \frac{\langle b, \sigma\rangle \to_{Bexp} false}{\langle !b, \sigma\rangle \to_{Bexp} true}$$

$$\frac{\langle b_1, \sigma\rangle \to_{Bexp} false}{\langle b_1 \,\&\&\, b_2, \sigma\rangle \to_{Bexp} false} \qquad \frac{\langle b_1, \sigma\rangle \to_{Bexp} true \qquad \langle b_2, \sigma\rangle \to_{Bexp} t}{\langle b_1 \,\&\&\, b_2, \sigma\rangle \to_{Bexp} t}$$

$$\frac{\langle b_1, \sigma\rangle \to_{Bexp} true}{\langle b_1 \mid\mid b_2, \sigma\rangle \to_{Bexp} true} \qquad \frac{\langle b_1, \sigma\rangle \to_{Bexp} false \qquad \langle b_2, \sigma\rangle \to_{Bexp} t}{\langle b_1 \mid\mid b_2, \sigma\rangle \to_{Bexp} t}$$

Arbeitsblatt 2.3: Boolsche Ausdrücke

Konstruiert die Auswertung des Ausdrucks `x == 7 && y == 3` unter folgenden Zuständen:

1. $\sigma_1 \stackrel{def}{=} \langle x \mapsto 7, y \mapsto 3\rangle$
2. $\sigma_2 \stackrel{def}{=} \langle x \mapsto 6, y \mapsto 3\rangle$
3. $\sigma_3 \stackrel{def}{=} \langle x \mapsto 6, y \mapsto 2\rangle$
4. $\sigma_4 \stackrel{def}{=} \langle y \mapsto 6\rangle$
5. $\sigma_5 \stackrel{def}{=} \langle y \mapsto 7\rangle$
6. $\sigma_6 \stackrel{def}{=} \langle x \mapsto 2\rangle$

Striktheit

- Eine partielle Funktion f ist **strikt** wenn $f(x)$ undefiniert ist, sobald x undefiniert ist.
- In unserer Semantik sind alle Operatoren (arithmetisch und boolesch) strikt, **bis auf** && und || im ersten Argument.
  - Operational nennt man das auch abgekürzte Auswertung (*short-circuit evaluation*)
  - Das erlaubt Idiome wie **if** `(x != 0 && 3/x > 1) { ... }`
- Wie erkennt man Striktheit an den **Regeln**?
  Alle Variablen der Konklusion kommen in den Bedingungen vor.

Operationale Semantik: Anweisungen

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

Beispiel:

$$\langle c, \sigma\rangle \to_{Stmt} \sigma'$$

$$\langle x = 5, \sigma\rangle \to_{Stmt} \sigma'\sigma[x \mapsto 5]$$

wobei $\sigma'(x) = 5$ und $\sigma'(y) = \sigma(y)$ für alle $y \neq x$
bzw. $\sigma' \stackrel{def}{=} \sigma[x \mapsto 5]$

Operationale Semantik: Anweisungen

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

Regeln:

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

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

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

Operationale Semantik: Anweisungen

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

Regeln:

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

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

Beispiel

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

$\sigma \stackrel{def}{=} \langle y \mapsto 2\rangle$

$$\dfrac{\dfrac{}{\langle 1,\sigma\rangle \to_{Aexp} 1}}{\langle x=1,\sigma\rangle \to_{Stmt} \sigma[x\mapsto 1] := \sigma_1} \quad \dfrac{\dfrac{\dfrac{\langle y,\sigma_1\rangle \to_{Aexp} 2}{\langle y!=0,\sigma_1\rangle \to_{Bexp} true} \quad \dfrac{(A)}{\langle y=y-1; x=2*x,\sigma_1\rangle \to_{Stmt} ?} \quad \dfrac{(B)}{\langle w,?\rangle \to_{Stmt} ?}}{\langle \textbf{while}\ (y!=0)\ \{y=y-1; x=2*x\},\sigma_1\rangle \to_{Stmt} ?}}{\langle x=1; \underbrace{\textbf{while}\ (y!=0)\ \{y=y-1; x=2*x\}}_{w},\sigma\rangle \to_{Stmt} ?}$$

(A)

$$\dfrac{\dfrac{\langle y-1,\sigma_1\rangle \to_{Aexp} 1}{\langle y=y-1,\sigma_1\rangle \to_{Stmt} \sigma_1[y\mapsto 1] := \sigma_2} \quad \dfrac{\langle 2*x,\sigma_2\rangle \to_{Aexp} 2}{\langle x=2*x,\sigma_2\rangle \to_{Stmt} \sigma_2[x\mapsto 2] := \sigma_3}}{\langle y=y-1; x=2*x,\sigma_1\rangle \to_{Stmt} \sigma_3}$$

$$\dfrac{\dfrac{}{\langle 1,\sigma\rangle \to_{Aexp} 1}}{\langle x=1,\sigma\rangle \to_{Stmt} \sigma_1} \quad \dfrac{\dfrac{\dfrac{\langle y,\sigma_1\rangle \to_{Aexp} 2}{\langle y!=0,\sigma_1\rangle \to_{Bexp} true} \quad \dfrac{(A)}{\langle y=y-1; x=2*x,\sigma_1\rangle \to_{Stmt} \sigma_3} \quad \dfrac{(B)}{\langle w,\sigma_3\rangle \to_{Stmt} ?}}{\langle \textbf{while}\ (y!=0)\ \{y=y-1; x=2*x\},\sigma_1\rangle \to_{Stmt} ?}}{\langle x=1; \underbrace{\textbf{while}\ (y!=0)\ \{y=y-1; x=2*x\}}_{w},\sigma\rangle \to_{Stmt} ?}$$

(B)

$$\dfrac{\dfrac{\dfrac{\langle y,\sigma_3\rangle \to_{Aexp} 1}{\langle y!=0,\sigma_3\rangle \to_{Bexp} true} \quad \dfrac{\dfrac{\langle y-1,\sigma_3\rangle \to_{Aexp} 0}{\langle y=y-1,\sigma_3\rangle \to_{Stmt} \sigma_3[y\mapsto 0] := \sigma_4} \quad \dfrac{\langle 2*x,\sigma_4\rangle \to_{Aexp} 4}{\langle x=2*x,\sigma_4\rangle \to_{Stmt} \sigma_4[x\mapsto 4] := \sigma_5}}{\langle y=y-1; x=2*x,\sigma_3\rangle \to_{Stmt} \sigma_5} \quad \dfrac{}{\langle w,\sigma_5\rangle \to_{Stmt} \sigma_5}}{\langle w,\sigma_3\rangle \to_{Stmt} \sigma_5}$$

$$\left.\dfrac{\dfrac{\langle y,\sigma_5\rangle \to_{Aexp} 0}{\langle y!=0,\sigma_3\rangle \to_{Bexp} false}}{\langle w,\sigma_5\rangle \to_{Stmt} \sigma_5}\right\}(C)$$

$$\underbrace{\textbf{while}\ (y!=0)\ \{y=y-1; x=2*x\}}_{w}$$

$$\dfrac{\dfrac{\dots \quad \dfrac{\dfrac{\langle y,\sigma_1\rangle \to_{Aexp} 2}{\langle y!=0,\sigma_1\rangle \to_{Bexp} true} \quad \dfrac{(A)}{\langle y=y-1; x=2*x,\sigma_1\rangle \to_{Stmt} \sigma_3} \quad \dfrac{(B)}{\langle w,\sigma_3\rangle \to_{Stmt} \sigma_5}}{\langle \textbf{while}\ (y!=0)\ \{y=y-1; x=2*x\},\sigma_1\rangle \to_{Stmt} \sigma_5}}{\langle x=1; \underbrace{\textbf{while}\ (y!=0)\ \{y=y-1; x=2*x\}}_{w},\sigma\rangle \to_{Stmt} \sigma_5}$$

$$\begin{aligned}\sigma_5 &= \sigma_4[x\mapsto 4] = \sigma_3[y\mapsto 0][x\mapsto 4] = \sigma_2[x\mapsto 2][y\mapsto 0][x\mapsto 4]\\ &= \sigma_1[y\mapsto 1][x\mapsto 2][y\mapsto 0][x\mapsto 4] = \langle y\mapsto 2\rangle[y\mapsto 1][x\mapsto 2][y\mapsto 0][x\mapsto 4]\\ &= \langle y\mapsto 0, x\mapsto 4\rangle\end{aligned}$$

und es gilt $\sigma_5(x) = 4 = 2^2 = 2^{\sigma_1(y)}$

Lineare, abgekürzte Schreibweise

```
// ⟨y ↦ 2⟩
x = 1;
// ⟨y ↦ 2, x ↦ 1⟩
while (y != 0) {
 y = y - 1;
 x = 2 * x;
}
```


Lineare, abgekürzte Schreibweise

```
// ⟨y ↦ 2⟩
x = 1;                          // Ableitung für ⟨x = 1, ⟨y ↦ 2⟩⟩ →Stmt ⟨y ↦ 2, x ↦ 1⟩
// ⟨y ↦ 2, x ↦ 1⟩
while(y!=0)  // ⟨y! = 0, ⟨y ↦ 2, x ↦ 1⟩⟩ →Bexp true
|           y = y - 1;          // Ableitung für ⟨y = y − 1, ⟨y ↦ 2, x ↦ 1⟩⟩ →Stmt ⟨y ↦ 1, x ↦ 1⟩
|           // ⟨y ↦ 1, x ↦ 1⟩
|           x = 2 * x;          // Ableitung für ⟨x = 2 ∗ x, ⟨y ↦ 1, x ↦ 1⟩⟩ →Stmt ...
|           // ⟨y ↦ 1, x ↦ 2⟩
while (y != 0) {
 y = y - 1;
 x = 2 * x;
}
```


Lineare, abgekürzte Schreibweise

```
// ⟨y ↦ 2⟩
x = 1;
// ⟨y ↦ 2, x ↦ 1⟩
while(y!=0)  // ⟨y! = 0, ⟨y ↦ 2, x ↦ 1⟩⟩ →Bexp true
|           y = y - 1;          // Ableitung für y = y − 1
|           // ⟨y ↦ 1, x ↦ 1⟩
|           x = 2 * x;          // Ableitung für x = 2 ∗ x
|           // ⟨y ↦ 1, x ↦ 2⟩
while(y!=0)  // ⟨y! = 0, ⟨y ↦ 1, x ↦ 2⟩⟩ →Bexp true
|           y = y - 1;
|           // ⟨y ↦ 0, x ↦ 2⟩
|           x = 2 * x;
|           // ⟨y ↦ 0, x ↦ 4⟩
while(y!=0)  // ⟨y! = 0, ⟨y ↦ 0, x ↦ 4⟩⟩ →Bexp false
// ⟨y ↦ 0, x ↦ 4⟩
```

Was haben wir gezeigt?

```
// ⟨y ↦ 2⟩                    σ1
x = 1;
// ⟨y ↦ 2, x ↦ 1⟩
while (y != 0) {
 y = y - 1;
 x = 2 * x;
}
// ⟨y ↦ 0, x ↦ 4⟩             σE
```

- Für **einen festen Anfangszustand** $\sigma_1 = \langle y \mapsto 2 \rangle$ gilt am Ende $\sigma_E(x) = 4 = 2^2 = 2^{\sigma_1(y)}$.
- Gilt das für alle?
- Für welche nicht?
- Wie kann man das für alle Anfangs-Zustände, für die es gilt, zeigen?

Was passiert hier?

```
// ⟨y ↦ −1⟩
x = 1;
while (y != 0) {
 y = y - 1;
 x = 2 * x;
}
```

- Ableitung terminiert nicht (Ableitungsbaum der Auswertung der while-Schleife wächst unendlich)
- In linearer Schreibweise geht es immer wieder unten weiter.

Arbeitsblatt 2.4: Programme!

- Werten Sie das nebenstehende Programm aus für den Anfangszustand $\langle x \mapsto 5, y \mapsto 2 \rangle$
- Geben Sie die Auswertung in abgekürzter Schreibweise an.
- Welche Beziehung gilt am Ende des Programms zwischen den Werten von x und y im Endzustand und im Anfangszustand?

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


Äquivalenz arithmetischer Ausdrücke

Gegeben zwei Aexp a_1 and a_2

- Sind sie gleich?

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

`(x*x) + 2*x*y + (y*y)` und `(x+y) * (x+y)`

- Wann sind sie gleich?

$$\forall \sigma, n. \langle a_1, \sigma \rangle \to_{Aexp} n \Leftrightarrow \langle a_2, \sigma \rangle \to_{Aexp} n$$

`x*x` und `8*x+9`
`x*x` und `x*x+1`

Äquivalenz Boolscher Ausdrücke

Gegeben zwei Bexp-Ausdrücke b_1 and b_2

- Sind sie gleich?

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

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

Beweisen

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

Definition

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

Ein einfaches Beispiel:

Lemma

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

Beweis

- Gegeben beliebiger Programmzustand σ.
- **Zu zeigen**: sowohl w also auch **if** $(b)\ \{c; w\}$ **else** $\{\}$ werten zum gleichen Programmzustand aus (wenn sie auswerten).
- Der Beweis geht per Fallunterscheidung über die Auswertung von Teilausdrücken bzw. Teilprogrammen.

Beweis

❶ $\langle b, \sigma \rangle \to_{Bexp} \mathit{false}$:

$$\langle \textbf{while } (b)\ c, \sigma \rangle \to_{Stmt} \sigma$$
$$\langle \textbf{if } (b)\ \{c; w\} \textbf{ else } \{\}, \sigma \rangle \to_{Stmt} \langle \{\}, \sigma \rangle \to_{Stmt} \sigma$$

❷ $\langle b, \sigma \rangle \to_{Bexp} \mathit{true}$: Sei $\langle c, \sigma \rangle \to_{Stmt} \sigma'$, dann:

$$\langle \overbrace{\textbf{while } (b)\ c}^{w}, \sigma \rangle \to_{Stmt} \langle c, \sigma \rangle \to_{Stmt} \sigma'$$
$$\langle w, \sigma' \rangle \to_{Stmt} \sigma''$$
$$\langle \textbf{if } (b)\ \{c; w\} \textbf{ else } \{\}, \sigma \rangle \to_{Stmt} \langle \{c; w\}, \sigma \rangle \to_{Stmt} \langle c, \sigma \rangle \to_{Stmt} \sigma'$$
$$\langle w, \sigma' \rangle \to_{Stmt} \sigma''$$

❸ $\langle b, \sigma \rangle$ wertet gar nicht aus — dann werten weder w noch **if** $(b)\ \{c; w\}$ **else** $\{\}$ aus.

Zusammenfassung

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

Korrekte Software: Grundlagen und Methoden
Vorlesung 3 vom 05.05.22
Denotationale Semantik

Serge Autexier, Christoph Lüth

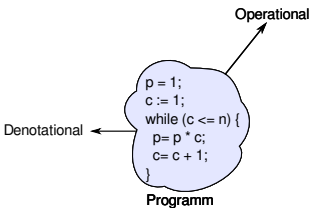
Universität Bremen

Sommersemester 2022

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Überblick



- Denotationale Semantik für C0
- Fixpunkte

Denotationale Semantik — Motivation

- **Operationale Semantik:**

  Eine Menge von Regeln, die einen Zustand und ein Programm in einen neuen Zustand überführen:

$$\langle c, \sigma \rangle \to_{Stmt} \sigma'$$

- **Denotationale Semantik:**

  Eine Menge von Regeln, die ein Programm in eine partielle Funktion (Denotat) von Zustand nach Zustand überführen

$$[\![c]\!]_C : \Sigma \rightharpoonup \Sigma$$

Denotationale Semantik — Kompositionalität

- Semantik von zusammengesetzten Ausdrücken durch Kombination der Semantiken der Teilausdrücke
  - Bsp: Semantik einer Sequenz von Anweisungen durch Verknüpfung der Semantik der einzelnen Anweisungen
- Operationale Semantik ist **nicht** kompositional:

```
x= 3;
y= x+ 7; // (*)
z= x+ y;
```

  - Semantik von Zeile (*) ergibt sich aus der Ableitung davor
  - Kann nicht unabhängig abgeleitet werden
- Denotationale Semantik ist kompositional.
  - Wesentlicher Baustein: **partielle Funktionen**

Partielle Funktionen und ihre Graphen

- Der **Graph** einer partiellen Funktion $f : X \rightharpoonup Y$ ist eine Relation

$$grph(f) \subseteq X \times Y \stackrel{def}{=} \{(x, f(x)) \mid x \in dom(f)\}$$

- Wir können eine partielle Funktion durch ihren Graph definieren:

Definition (Partielle Funktion)

Eine **partielle Funktion** $f : X \rightharpoonup Y$ ist eine Relation $f \subseteq X \times Y$ so dass wenn $(x, y_1) \in f$ und $(x, y_2) \in f$ dann $y_1 = y_2$ (**Rechtseindeutigkeit**)

- Wir benutzen beide Notationen, aber für die denotationale Semantik die Graph-Notation.
- **Systemzustände** sind partielle Abbildungen $\Sigma \stackrel{def}{=} \mathbf{Loc} \rightharpoonup \mathbf{V}$ ($\longrightarrow$ letzte VL)

Beispiel

Als Beispiel betrachten wir die partielle Funktion $div3 : \{0 \ldots 10\} \to \mathbb{N}$

$$div3(x) = y \quad \text{g.d.w.} \quad 3 \cdot y = x$$

- Zuordnung:

$$\begin{array}{rcl} 0 & \mapsto & 0 \\ 1 & & \\ 2 & & \\ 3 & \mapsto & 1 \\ 4 & & \\ 5 & & \\ 6 & \mapsto & 2 \\ 7 & & \\ 8 & & \\ 9 & \mapsto & 3 \\ 10 & & \end{array}$$

- Notation als Relation (**Graph**):

$$div3 \stackrel{def}{=} \{(0,0), (3,1), (6,2), (9,3)\}$$

- Wir schreiben

$$\begin{array}{ll} div3(3) = 1 & \text{für } (3,1) \in div3 \\ div3(5) = \bot & \text{für es gibt kein } y \text{ mit } (5,y) \in div3 \\ div3(5) = \bot & \text{für } \forall y.(5,y) \notin div3 \end{array}$$

- Achtung, Partialität!

Achtung, Partialität!

- Beim Rechnen mit partiellen Funktionen muss die **Definiertheit** beachtet werden.
- Insbesondere darf nicht mit undefinierten Ausdrücken gerechnet werden.
- Bspw. gilt oben **nicht** im allgemeinen:

$$3 \cdot div3(x) = x \quad \times$$

oder

$$div3(1) = \bot = div3(2) \Longrightarrow div3(1) = div3(2) \quad \times$$

- Warum? Dann gälte

$$\begin{array}{c} div3(1) = div3(2) \\ 3 \cdot div3(1) = 3 \cdot div3(2) \\ 1 = 2 \quad \lightning \end{array}$$

- Vgl. `https://de.wikipedia.org/wiki/Trugschluss_(Mathematik)#Division_durch_0`

Arbeitsblatt 3.1: Relationen als Funktionen

Definiert wie im Beispiel eben die Funktion $sqrt : \{0, \ldots, 100\} \to \mathbb{N}$ mit

$$sqrt(x) = y \quad \text{g.d.w.} \quad y^2 = x$$

Was ist der Wert folgender Ausdrücke:

$$t_1 = 5 - sqrt(32) \quad t_2 = sqrt(49) + sqrt(0) \quad t_3 = \sqrt{3} \cdot sqrt(3) \quad t_4 = \frac{sqrt(64)}{0}$$

Denotierende Funktionen (Denotate)

- Arithmetische Ausdrücke: $a \in$ **Aexp** denotieren eine partielle Funktion $\Sigma \rightharpoonup \mathbb{Z}$
- Boolsche Ausdrücke: $b \in$ **Bexp** denotieren eine partielle Funktion $\Sigma \rightharpoonup \mathbb{B}$
- Anweisungen: $c \in$ **Stmt** denotieren eine partielle Funktion $\Sigma \rightharpoonup \Sigma$

Denotat von Aexp

$$[\![a]\!]_{\mathcal{A}} : \textbf{Aexp} \to (\Sigma \rightharpoonup \mathbb{Z})$$

$$\begin{aligned}
[\![n]\!]_{\mathcal{A}} &= \{(\sigma, [\![n]\!]) \mid \sigma \in \Sigma\} \\
[\![x]\!]_{\mathcal{A}} &= \{(\sigma, \sigma(x)) \mid \sigma \in \Sigma, x \in Dom(\sigma)\} \\
[\![a_0 + a_1]\!]_{\mathcal{A}} &= \{(\sigma, n_0 + n_1) \mid (\sigma, n_0) \in [\![a_0]\!]_{\mathcal{A}} \wedge (\sigma, n_1) \in [\![a_1]\!]_{\mathcal{A}}\} \\
[\![a_0 - a_1]\!]_{\mathcal{A}} &= \{(\sigma, n_0 - n_1) \mid (\sigma, n_0) \in [\![a_0]\!]_{\mathcal{A}} \wedge (\sigma, n_1) \in [\![a_1]\!]_{\mathcal{A}}\} \\
[\![a_0 * a_1]\!]_{\mathcal{A}} &= \{(\sigma, n_0 * n_1) \mid (\sigma, n_0) \in [\![a_0]\!]_{\mathcal{A}} \wedge (\sigma, n_1) \in [\![a_1]\!]_{\mathcal{A}}\} \\
[\![a_0 / a_1]\!]_{\mathcal{A}} &= \{(\sigma, n_0 \div n_1) \mid (\sigma, n_0) \in [\![a_0]\!]_{\mathcal{A}} \wedge (\sigma, n_1) \in [\![a_1]\!]_{\mathcal{A}} \wedge n_1 \neq 0\}
\end{aligned}$$

Rechtseindeutigkeit

Lemma (Partielle Funktion)

*$[\![-]\!]_{\mathcal{A}}$ ist rechtseindeutig und damit eine **partielle Funktion**.*

Beweis.

z.z.: wenn $(\sigma, v_1) \in [\![a]\!]_{\mathcal{A}}, (\sigma, v_2) \in [\![a]\!]_{\mathcal{A}}$ dann $v_1 = v_2$.
Strukturelle Induktion über **Aexp**:

- Induktionsbasis sind $n \in \mathbf{Z}$ und $x \in$ **Idt**.
  Sei $a \equiv x$, dann $v_1 = \sigma(x) = v_2$.
- Induktionsschritt sind die anderen Klauseln.
  Sei $a \equiv a_1 + a_2$.
  Induktionsannahme ist: wenn $(\sigma, n_i) \in [\![a_i]\!]_{\mathcal{A}}, (\sigma, m_i) \in [\![a_i]\!]_{\mathcal{A}}$ dann $n_i = m_i$.
  Sei $v_1 = (\sigma, n_1 + n_2)$ mit $(\sigma, n_1) \in [\![a_1]\!]_{\mathcal{A}}, (\sigma, n_2) \in [\![a_2]\!]_{\mathcal{A}}$, und $v_2 = m_1 + m_2$ mit $(\sigma, m_1) \in [\![a_1]\!]_{\mathcal{A}}, (\sigma, m_2) \in [\![a_2]\!]_{\mathcal{A}}$.
  Aus der Annahme folgt $n_1 = m_1$ und $n_2 = m_2$, deshalb $v_1 = v_2$.

□

Kompositionalität und Striktheit

- Die Rechtseindeutigkeit erlaubt die Notation als partielle Funktion:

$$\begin{aligned}
[\![3 * (x + y)]\!]_{\mathcal{A}}(\sigma) &= [\![3]\!]_{\mathcal{A}}(\sigma) \cdot ([\![x]\!]_{\mathcal{A}}(\sigma) + [\![y]\!]_{\mathcal{A}}(\sigma)) \\
&= 3 \cdot ([\![x]\!]_{\mathcal{A}}(\sigma) + [\![y]\!]_{\mathcal{A}}(\sigma)) \\
&= 3 \cdot (\sigma(x) + \sigma(y))
\end{aligned}$$

- Diese Notation versteckt die **Partialität**:

$$[\![1 + x/0]\!]_{\mathcal{A}}(\sigma) = 1 + \sigma(x)/0 = 1 + \bot = \bot$$

- Wenn ein Teilausdruck undefiniert ist, wird der gesamte Ausdruck undefiniert: $[\![-]\!]_{\mathcal{A}}$ ist **strikt** für alle arithmetischen Operatoren.

Arbeitsblatt 3.2: Semantik I

Hier üben wir noch einmal den Zusammenhang zwischen den beiden Notationen. Gegeben sei der Zustand $s = \langle x \mapsto 3, y \mapsto 4 \rangle$ und der Ausdruck $a = 7 * x + y$.
Berechnen Sie die Semantik zum einen als Relation (füllen Sie die Fragezeichen aus):

```
(s, ?) : [[7]]
(s, ?) : [[x]]
(s, ?) : [[7*x]]
(s, ?) : [[y]]
(s, ?) : [[7*x+ y]]
```

Berechnen Sie zum anderen die Semantik in der Funktionsnotation:

```
[[7*x+y]](s) = [[7*x]](s)+[[y]](s) = ... = ?
```

Ist das Ergebnis am Ende gleich?

Lösung

Denotat von Bexp

$$[\![a]\!]_{\mathcal{B}} : \textbf{Bexp} \to (\Sigma \rightharpoonup \mathbb{B})$$

$$\begin{aligned}
[\![\mathbf{1}]\!]_{\mathcal{B}} &= \{(\sigma, true) \mid \sigma \in \Sigma\} \\
[\![\mathbf{0}]\!]_{\mathcal{B}} &= \{(\sigma, false) \mid \sigma \in \Sigma\} \\
[\![a_0 == a_1]\!]_{\mathcal{B}} &= \{(\sigma, true) \mid \sigma \in \Sigma, (\sigma, n_0) \in [\![a_0]\!]_{\mathcal{A}}, (\sigma, n_1) \in [\![a_1]\!]_{\mathcal{A}}, n_0 = n_1\} \\
&\quad \cup \{(\sigma, false) \mid \sigma \in \Sigma, (\sigma, n_0) \in [\![a_0]\!]_{\mathcal{A}}, (\sigma, n_1) \in [\![a_1]\!]_{\mathcal{A}}, n_0 \neq n_1\} \\
[\![a_0 < a_1]\!]_{\mathcal{B}} &= \{(\sigma, true) \mid \sigma \in \Sigma, (\sigma, n_0) \in [\![a_0]\!]_{\mathcal{A}}, (\sigma, n_1) \in [\![a_1]\!]_{\mathcal{A}}, n_0 < n_1\} \\
&\quad \cup \{(\sigma, false) \mid \sigma \in \Sigma, (\sigma, n_0) \in [\![a_0]\!]_{\mathcal{A}}, (\sigma, n_1) \in [\![a_1]\!]_{\mathcal{A}}, n_0 \geq n_1\}
\end{aligned}$$

Denotat von Bexp

$$[\![a]\!]_{\mathcal{B}} : \mathbf{Bexp} \to (\Sigma \rightharpoonup \mathbb{B})$$

$$\begin{aligned}
[\![!b]\!]_{\mathcal{B}} &= \{(\sigma, true) \mid \sigma \in \Sigma, (\sigma, false) \in [\![b]\!]_{\mathcal{B}}\} \\
&\quad \cup \{(\sigma, false) \mid \sigma \in \Sigma, (\sigma, true) \in [\![b]\!]_{\mathcal{B}}\} \\
[\![b_1 \;\&\&\; b2]\!]_{\mathcal{B}} &= \{(\sigma, false) \mid \sigma \in \Sigma, (\sigma, false) \in [\![b_1]\!]_{\mathcal{B}}\} \\
&\quad \cup \{(\sigma, t_2) \mid \sigma \in \Sigma, (\sigma, true) \in [\![b_1]\!]_{\mathcal{B}}, (\sigma, t_2) \in [\![b_2]\!]_{\mathcal{B}}\} \\
[\![b_1 \;||\; b_2]\!]_{\mathcal{B}} &= \{(\sigma, true) \mid \sigma \in \Sigma, (\sigma, true) \in [\![b_1]\!]_{\mathcal{B}}\} \\
&\quad \cup \{(\sigma, t_2) \mid \sigma \in \Sigma, (\sigma, false) \in [\![b_1]\!]_{\mathcal{B}}, (\sigma, t_2) \in [\![b_2]\!]_{\mathcal{B}}\}
\end{aligned}$$

Kompositionalität und Striktheit

Lemma (Partielle Funktion)

$[\![-]\!]_{\mathcal{B}}$ *ist rechtseindeutig und damit eine* ***partielle Funktion****.*

- Beweis analog zu $[\![-]\!]_{\mathcal{A}}$.
- Ist $[\![-]\!]_{\mathcal{B}}$ strikt? Natürlich nicht:
- Sei $[\![b_1]\!]_{\mathcal{B}}(\sigma) = false$, dann $[\![b_1 \;\&\&\; b_2]\!]_{\mathcal{B}}(\sigma) = [\![b_1]\!]_{\mathcal{B}}(\sigma) = false$
- Wir können deshalb nicht so einfach schreiben $[\![b_1 \;\&\&\; b_2]\!]_{\mathcal{B}}(\sigma) = [\![b_1]\!]_{\mathcal{B}}(\sigma) \wedge [\![b_2]\!]_{\mathcal{B}}(\sigma)$
- Die normale zweiwertige Logik behandelt Definiertheit gar nicht. Bei uns müssen die logischen Operatoren links-strikt sein:

$$\begin{array}{lll}
\bot \wedge a = \bot & false \wedge a = false & true \wedge a = a \\
\bot \vee a = \bot & true \vee a = true & false \vee a = a
\end{array}$$

Arbeitsblatt 3.3: Semantik II

Wir üben noch einmal die Nichtstrikheit. Gegeben $s = \langle x \mapsto 7 \rangle$ und
$b \equiv (7 == x) \;||\; (x/0 == 1)$
Berechnenen Sie die Semantik in den Notationen von oben:

```
(s, ?) : [[ (7 == x) || (x/0 == 1) ]]
...

[[ (7 == x) || (x/0 == 1) ]](s) = ... ?
```

Hilfreiche Notation: $a \wedge b =$ `a /\ b`, $a \vee b =$ `a \/ b`

Lösung

Denotationale Semantik von Anweisungen

- Zuweisung: punktweise Änderung des Zustands σ zu $\sigma[x \mapsto n]$
- Sequenz: Komposition von Relationen

Definition (Komposition von Relationen)

Für zwei Relationen $R \subseteq X \times Y, S \subseteq Y \times Z$ ist ihre **Komposition**

$$R \circ S \stackrel{def}{=} \{(x, z) \mid \exists y \in Y.\, (x, y) \in R \wedge (y, z) \in S\}$$

Wenn R, S zwei partielle Funktionen sind, ist $R \circ S$ ihre Funktionskomposition.

- Leere Sequenz: Leere Funktion? Nein, Identität. Für Menge X,

$$\mathbf{Id}_X \stackrel{def}{=} X \times X = \{(x, x) \mid x \in X\}$$

ist die **Identitätsfunktion** ($\mathbf{Id}_X(x) = x$).

Arbeitsblatt 3.4: Komposition von Relationen

Zur Übung: betrachten Sie folgende Relationen:

$$\begin{aligned}
R &= \{(1,7), (2,3), (3,9), (4,3)\} \\
S &= \{(1,0), (2,0), (3,1), (3,5), (4,7), (5,9), (7,3), (8,15)\}
\end{aligned}$$

Berechnen Sie $R \circ S = \{(1, ?), \ldots\}$

Denotat von Stmt

$$[\![.]\!]_{\mathcal{C}} : \mathbf{Stmt} \to (\Sigma \rightharpoonup \Sigma)$$

$$\begin{aligned}
[\![x = a]\!]_{\mathcal{C}} &= \{(\sigma, \sigma[x \mapsto n]) \mid \sigma \in \Sigma \wedge (\sigma, n) \in [\![a]\!]_{\mathcal{A}}\} \\
[\![c_1; c_2]\!]_{\mathcal{C}} &= [\![c_1]\!]_{\mathcal{C}} \circ [\![c_2]\!]_{\mathcal{C}} \\
[\![\{\,\}]\!]_{\mathcal{C}} &= \mathbf{Id}_{\Sigma} \\
[\![\textbf{if } (b) \; c_0 \; \textbf{else} \; c_1]\!]_{\mathcal{C}} &= \{(\sigma, \sigma') \mid (\sigma, true) \in [\![b]\!]_{\mathcal{B}} \wedge (\sigma, \sigma') \in [\![c_0]\!]_{\mathcal{C}}\} \\
&\quad \cup \{(\sigma, \sigma') \mid (\sigma, false) \in [\![b]\!]_{\mathcal{B}} \wedge (\sigma, \sigma') \in [\![c_1]\!]_{\mathcal{C}}\}
\end{aligned}$$

Aber was ist

$$[\![\textbf{while } (b) \; c]\!]_{\mathcal{C}} = ??$$

Denotationale Semantik von while

- Sei $w \equiv \textbf{while } (b) \; c$ (und $\sigma \in \Sigma$). Operational gilt:

$$w \sim \textbf{if } (b) \; \{c; w\} \; \textbf{else} \; \{\,\}$$

- Dann sollte auch gelten

$$\begin{aligned}
[\![w]\!]_{\mathcal{C}} &\stackrel{?}{=} [\![\textbf{if } (b) \; \{c; w\} \; \textbf{else} \; \{\,\}]\!]_{\mathcal{C}} \\
&= \{(\sigma, \sigma') \mid (\sigma, true) \in [\![b]\!]_{\mathcal{B}} \wedge (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}} \circ [\![w]\!]_{\mathcal{C}}\} \\
&\quad \cup \{(\sigma, \sigma') \mid (\sigma, false) \in [\![b]\!]_{\mathcal{B}} \wedge (\sigma, \sigma') \in [\![\{\,\}]\!]_{\mathcal{C}}\}
\end{aligned}$$

- Das ist eine **rekursive** Definition von $[\![w]\!]_{\mathcal{C}}$:

$$x = F(x)$$

- Das ist ein **Fixpunkt**:

$$x = fix(F)$$

- Was ist das?

Fixpunkte

Definition (Fixpunkt)

Für $f : X \rightharpoonup X$ ist ein **Fixpunkt** ein $x \in X$ so dass $f(x) = x$.

- Hat jede Funktion $f : X \rightharpoonup X$ einen Fixpunkt? Nein
- Kann eine Funktion mehrere Fixpunkte haben? Ja — aber nur einen kleinsten.
- Beispiele
  - Fixpunkte von $f(x) = \sqrt{x}$ sind 0 und 1; ebenfalls für $f(x) = x^2$.
  - Für die Sortierfunktion sind alle sortierten Listen Fixpunkte
  - Die Funktion $f(x) = x + 1$ hat keinen Fixpunkt in $\mathbb{Z}$
  - Die Funktion $f(X) = \mathbb{P}(X)$ hat überhaupt keinen Fixpunkt
- $fix(f)$ ist also der **kleinste Fixpunkt** von f.

Konstruktion des kleinsten Fixpunktes (Kurzversion)

- Gegeben Funktion Γ auf Denotaten $\Gamma : (\Sigma \rightharpoonup \Sigma) \rightharpoonup (\Sigma \rightharpoonup \Sigma)$
- Wir konstruieren eine Sequenz $\Gamma^i : \Sigma \rightharpoonup \Sigma$ (mit $i \in \mathbb{N}$) von Funktionen:

$$\Gamma^0(s) \stackrel{def}{=} \emptyset$$
$$\Gamma^{i+1}(s) \stackrel{def}{=} \Gamma(\Gamma^i)(s)$$

- Dann ist

$$fix(\Gamma) \stackrel{def}{=} \bigcup_{i \in \mathbb{N}} \Gamma^i$$

- Verkürzte Version — der Fixpunkt muss so nicht existieren (er tut es aber für alle Programme)

Denotationale Semantik für die Iteration

- Sei $w \equiv$ **while** (b) c
- Konstruktion: "Auffalten" der Schleife (f ist ein Denotat):

$$\Gamma(f) = \{(\sigma, \sigma') \mid (\sigma, true) \in [\![b]\!]_{\mathcal{B}} \wedge (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}} \circ f\} \cup \{(\sigma, \sigma) \mid (\sigma, false) \in [\![b]\!]_{\mathcal{B}}\}$$

- b und c sind Parameter von Γ
- Dann ist

$$[\![w]\!]_{\mathcal{C}} = fix(\Gamma)$$

Denotation für Stmt

$$[\![.]\!]_{\mathcal{C}} : \{Stmt \rightharpoonup (\Sigma \rightharpoonup \Sigma)$$

$$\begin{aligned}
[\![x = a]\!]_{\mathcal{C}} &= \{(\sigma, \sigma[x \mapsto n]) \mid \sigma \in \Sigma \wedge (\sigma, n) \in [\![a]\!]_{\mathcal{A}}\} \\
[\![c_1; c_2]\!]_{\mathcal{C}} &= [\![c_1]\!]_{\mathcal{C}} \circ [\![c_2]\!]_{\mathcal{C}} \\
[\![\{\,\}]\!]_{\mathcal{C}} &= \mathbf{Id}_{\Sigma} \\
[\![\textbf{if } (b) \ c_0 \ \textbf{else} \ c_1]\!]_{\mathcal{C}} &= \{(\sigma, \sigma') \mid (\sigma, true) \in [\![b]\!]_{\mathcal{B}} \wedge (\sigma, \sigma') \in [\![c_0]\!]_{\mathcal{C}}\} \\
&\quad \cup \{(\sigma, \sigma') \mid (\sigma, false) \in [\![b]\!]_{\mathcal{B}} \wedge (\sigma, \sigma') \in [\![c_1]\!]_{\mathcal{C}}\} \\
[\![\textbf{while } (b) \ c]\!]_{\mathcal{C}} &= fix(\Gamma)
\end{aligned}$$

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

Der Fixpunkt bei der Arbeit (I)

```
while (x < 0) {
  x= x+1;
  }
```

$$\Gamma(f)(\sigma) \stackrel{def}{=} \begin{cases} \sigma & \sigma(x) \geq 0 \\ f(\sigma[x \mapsto \sigma(x) + 1]) & \sigma(x) < 0 \end{cases}$$

Wir betrachten den Zustand $s = \langle x \mapsto ? \rangle$ (nur eine Variable):

s	$\Gamma^0(s)$	$\Gamma^1(s)$	$\Gamma^2(s)$	$\Gamma^3(s)$
-2	$\bot$	$\Gamma^0(s[x \mapsto -1]) = \bot$	$\Gamma^1(s[x \mapsto -1]) = \bot$	$\Gamma^2(s[x \mapsto -1]) = 0$
-1	$\bot$	$\Gamma^0(s[x \mapsto 0]) = \bot$	$\Gamma^1(s[x \mapsto 0]) = 0$	$\Gamma^2(s[x \mapsto 0]) = 0$
0	$\bot$	0	0	0
1	$\bot$	1	1	1

Der Fixpunkt bei der Arbeit (II)

```
x= 0;
while (n > 0) {
  x= x+n;
  n= n-1;
  }
```

$$\Gamma(f)(\sigma) = \begin{cases} \sigma & \sigma(n) \leq 0 \\ f(\sigma[x \mapsto \sigma(x) + \sigma(n)][n \mapsto \sigma(n) - 1]) & \sigma(n) > 0 \end{cases}$$

Wir betrachten Zustände $s = \langle x \mapsto ?, n \mapsto ? \rangle$ (zwei Variablen).
Der Wert von x im Initialzustand ist dabei unerheblich:

s	$\Gamma^0(s)$		$\Gamma^1(s)$		$\Gamma^2(s)$		$\Gamma^3(s)$		$\Gamma^4(s)$		$\Gamma^5(s)$	
n	x	n	x	n	x	n	x	n	x	n	x	n
-1	$\bot$	$\bot$	0	-1	0	-1	0	-1	0	-1	0	-1
0	$\bot$	$\bot$	0	0	0	0	0	0	0	0	0	0
1	$\bot$	$\bot$	$\bot$	$\bot$	1	0	1	0	1	0	1	0
2	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	3	0	3	0	3	0
3	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	6	0	6	0
4	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	10	0

Der Fixpunkt bei der Arbeit (III)

Kleine Änderung im Beispielprogramm:

```
x= 0;
while (n != 0) {
  x= x+n;
  n= n-1;
  }
```

$$\Gamma(f)(\sigma) = \begin{cases} \sigma & \sigma(n) = 0 \\ f(\sigma[x \mapsto \sigma(x) + \sigma(n)][n \mapsto \sigma(n) - 1]) & \text{sonst} \end{cases}$$

Jetzt ergibt sich:

s	$\Gamma^0(s)$		$\Gamma^1(s)$		$\Gamma^2(s)$		$\Gamma^3(s)$		$\Gamma^4(s)$	
n	x	n	x	n	x	n	x	n	x	n
-2	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
-1	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
0	$\bot$	$\bot$	0	0	0	0	0	0	0	0
1	$\bot$	$\bot$	$\bot$	$\bot$	1	0	1	0	1	0
2	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	3	0	3	0
3	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	6	0

Der Fixpunkt bei der Arbeit (IV)

```
while (1) {
  x= x+1;
  }
```

$$\Gamma(f)(\sigma) \stackrel{def}{=} f(\sigma[x \mapsto \sigma(x) + 1])$$

Jetzt ergibt sich:

s	$\Gamma^0(s)$	$\Gamma^1(s)$	$\Gamma^2(s)$	$\Gamma^3(s)$
-2	$\bot$	$\bot$	$\bot$	$\bot$
-1	$\bot$	$\bot$	$\bot$	$\bot$
0	$\bot$	$\bot$	$\bot$	$\bot$
1	$\bot$	$\bot$	$\bot$	$\bot$
2	$\bot$	$\bot$	$\bot$	$\bot$
3	$\bot$	$\bot$	$\bot$	$\bot$

Arbeitsblatt 3.5: Semantik III

Wir betrachten das Beispielprogramm:

```
x= 1;
while (n > 0) {
  x= x*n;
  n= n-1;
  }
```

Berechnen Sie wie oben den Fixpunkt:

s	G^0		G^1		G^2		G^3		G^4	
n	x	n	x	n	x	n	x	n	x	n
0										
1										
2										
3										

Arbeitsblatt 3.5: Semantik III

Wir betrachten das Beispielprogramm:

```
x= 1;
while (n > 0) {
  x= x*n;
  n= n-1;
  }
```


Der Fixpunkt bei der Arbeit (V)

```
x= 0;
i= 0;
while (i<=n) {
  x= x+i;
  i= i+1;
  }
```

$$\Gamma(f)(\sigma) \stackrel{def}{=} \begin{cases} \sigma & \sigma(i) > \sigma(n) \\ f(\sigma[x \mapsto \sigma(x) + \sigma(i)][i \mapsto \sigma(i) + 1]) & \text{sonst} \end{cases}$$

Wir betrachten nur die **while**-Schleife mit $s = \langle n \mapsto ?, i \mapsto ?, x \mapsto ? \rangle$.

s		$\Gamma^0(s)$			$\Gamma^1(s)$			$\Gamma^2(s)$			$\Gamma^3(s)$			$\Gamma^4(s)$		
n	i	n	i	x	n	i	x	n	i	x	n	i	x	n	i	x
0	0	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	0	1	x	0	1	x	0	1	x
0	1	$\bot$	$\bot$	$\bot$	0	1	x	0	1	x	0	1	x	0	1	x
1	0	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	1	2	$x+1$	1	2	$x+1$
1	1	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	1	2	$x+1$	1	2	$x+1$	1	2	$x+1$
1	2	$\bot$	$\bot$	$\bot$	1	2	x	1	2	x	1	2	x	1	2	x
2	0	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	2	3	$x+3$
2	1	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	2	3	$x+3$	2	3	$x+3$
2	2	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	2	3	$x+2$	2	3	$x+2$	2	3	$x+2$
2	3	$\bot$	$\bot$	$\bot$	2	3	x	2	3	x	2	3	x	2	3	x

Weitere Eigenschaften der denotationalen Semantik

Lemma (Partielle Funktion)

$[\![-]\!]_C$ *ist rechtseindeutig und damit eine* ***partielle Funktion****.*

- Beweis über strukturelle Induktion über $c \in$ **Stmt** und über **Fixpunktinduktion**:
  - Zu zeigen: wenn s rechtseindeutig, dann ist $\Gamma(s)$ rechtseindeutig
  - Dann ist $fix(\Gamma)$ rechtseindeutig.
- Eigenschaften der Iteration:
  - Sei $w \equiv$ **while** (b) c
  - Dann

$$[\![w]\!]_C = [\![\textbf{if } (b) \{c; w\} \textbf{ else } \{\}]\!]_C \quad (1)$$

$$(\sigma, \sigma') \in [\![w]\!]_C \Longrightarrow (\sigma', \mathit{false}) \in [\![b]\!]_B \quad (2)$$

Beweis (1)

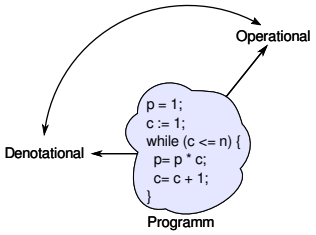
$$\begin{aligned}
[\![w]\!]_C &= fix(\Gamma) \\
&= \Gamma(fix(\Gamma)) \\
&= \Gamma([\![w]\!]_C) \\
&= \{(\sigma,\sigma') \mid (\sigma, \mathit{true}) \in [\![b]\!]_B \wedge (\sigma,\sigma') \in [\![c]\!]_C \circ [\![w]\!]_C\} \\
&\quad \cup \{(\sigma,\sigma) \mid (\sigma, \mathit{false}) \in [\![b]\!]_B\} \\
&= \{(\sigma,\sigma') \mid (\sigma, \mathit{true}) \in [\![b]\!]_B \wedge (\sigma,\sigma') \in [\![c;\ w]\!]_C\} \\
&\quad \cup \{(\sigma,\sigma) \mid (\sigma, \mathit{false}) \in [\![b]\!]_B \wedge (\sigma,\sigma) \in [\![\{\}]\!]_C\} \\
&= [\![\textbf{if } (b) \{c; w\} \textbf{ else } \{\}]\!]_C
\end{aligned}$$

Note

$$fix(\Gamma) = \Gamma(fix(\Gamma))\Gamma(s) = \begin{array}{l} \{(\sigma,\sigma') \mid (\sigma, \mathit{true}) \in [\![b]\!]_B \wedge (\sigma,\sigma') \in [\![c]\!]_C \circ s\} \\ \cup \{(\sigma,\sigma) \mid (\sigma, \mathit{false}) \in [\![b]\!]_B\} \end{array} \quad [\![\textbf{if } (b)\ c_0 \textbf{ else } c_1]\!]_C = \begin{array}{l} \{(\sigma,\sigma') \mid (\sigma, \mathit{true}) \in [\![b]\!]_B \wedge (\sigma,\sigma') \in [\![c_0]\!]_C\} \\ \cup \{(\sigma,\sigma') \mid (\sigma, \mathit{false}) \in [\![b]\!]_B \wedge (\sigma,\sigma') \in [\![c_1]\!]_C\} \end{array}$$

Zusammenfassung

- Die denotationale Semantik bildet Programme (Ausdrücke) auf **partielle Funktionen** $\Sigma \rightharpoonup \Sigma$ ab.
- Zentral ist der Begriff des **kleinsten Fixpunktes**, der die Semantik der while-Schleife bildet.
- Undefiniertheit wird **implizit** behandelt (durch die Partialität von $\Sigma \rightharpoonup \Sigma$).
  - Nicht-Termination und Undefiniertheit sind semantisch äquivalent.
- Genaues Verhältnis zur **operationalen Semantik**? Nächste Vorlesung



Korrekte Software: Grundlagen und Methoden
Vorlesung 4 vom 10.05.22
Äquivalenz der Operationalen und Denotationalen Semantik

Serge Autexier, Christoph Lüth

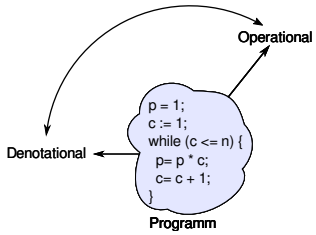
Universität Bremen

Sommersemester 2022

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Operationale und Denotationale Semantik



Äquivalenz der Operationalen und Denotationalen Semantik

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

$$\langle c, \sigma\rangle \to_{Stmt} \sigma' \iff (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}} \quad (1)$$

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

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

- Wie zeigen wir das?

Operationale vs. denotationale Semantik

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

Operationale vs. denotationale Semantik

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

Äquivalenz operationale und denotationale Semantik

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

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

- Beweis Prinzip?

Exkurs: Beweisprinzipien

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

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

- Beispiel: Addition ist definiert durch

$$x + 0 = x$$
$$x + S(y) = S(x + y)$$

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

Arbeitsblatt 4.1: Natürliche Induktion

- Zeigt durch natürliche Induktion:

$$0 + x = x \qquad S(x + y) = S(x) + y$$

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

Wohlfundiertheit

Wohlfundiertheit

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

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

Beispiele:

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

Eigenschaften wohlfundierter Relationen

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

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

Wohlfundierte Induktion

Noethersche Induktion (Wohlfundierte Induktion)

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

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

Beispiele:

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

Strukturelle Ordnung

Strukturelle Ordnung

Die strukturelle Ordnung auf arithmetischen Ausdrücken ist definiert als:

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

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

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

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

Arbeitsblatt 4.2: Strukturelle Induktion

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

Äquivalenz operationale und denotationale Semantik

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

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

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

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

Induktionsanfänge

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

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

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

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

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

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

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

Induktionsschritte

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

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

Dann;

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

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

Induktionsschritte

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

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

1. Fall: $n \neq 0$

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

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

Induktionsschritte

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

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

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

q.e.d.

Operationale vs. denotationale Semantik

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

Operationale vs. denotationale Semantik

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

Operationale vs. denotationale Semantik

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

Äquivalenz operationale und denotationale Semantik

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

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

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

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

Induktionsanfänge

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

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

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

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

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

Induktionsschritte

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

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

1. Fall $v = false$

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

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

Induktionsschritte

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

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

1. Fall $v = true$

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

q.e.d

Arbeitsblatt 4.3: Beweis Induktionsanfang

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

Beweist obige Aussage unter Verwendung des für arithmetische Ausdrücke geltenden Lemmas

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

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

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

- Annahmen: für $n, m \in \mathbb{B}$:

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

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

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

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

- Annahmen: für $m, n \in \mathbb{B}$:

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

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

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

Operationale vs. denotationale Semantik

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

Operationale vs. denotationale Semantik

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

Operationale vs. denotationale Semantik

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

mit

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

Äquivalenz operationale und denotationale Semantik

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

$$\langle c, \sigma\rangle \to_{Stmt} \sigma' \iff (\sigma, \sigma') \in [\![c]\!]_C$$

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

Operationale Semantik: C0 Programme

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

Regeln:

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

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

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

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

Operationale Semantik: C0 Programme

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

Regeln: **Programmstruktur**

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

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

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

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

Strukturelle Induktion über c **nicht** möglich.

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

Ableitungstiefe für Programme

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

$$\frac{\vdots \qquad \cdots \qquad \vdots}{Prämisse_1 \qquad\qquad Prämisse_n}$$
$$Conclusion$$

Operationale Semantik: C0 Programme

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

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

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

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

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

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

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

Äquivalenz operationale und denotationale Semantik

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

$$\langle c, \sigma\rangle \to_{Stmt} \sigma' \iff (\sigma, \sigma') \in [\![c]\!]_C$$

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

Beweis: $\forall c \in$ **Stmt**. $\forall \sigma, \sigma'. \langle c, \sigma\rangle \to_{Stmt} \sigma' \Longrightarrow (\sigma, \sigma') \in [\![c]\!]_C$

Induktionsanfang — Ableitungstiefe 1

- Fall $c \equiv x = a$:

$$[\![x = a]\!]_C = \{(\sigma, \sigma[x \mapsto m]) | (\sigma, m) \in [\![a]\!]_A\}$$

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

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

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

Beweis: $\forall c \in$ **Stmt**. $\forall \sigma, \sigma'. \langle c, \sigma\rangle \to_{Stmt} \sigma' \Longrightarrow (\sigma, \sigma') \in [\![c]\!]_C$

Induktionsschritt:

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

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

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

$$\begin{array}{ccccc} \langle \textbf{if}(b) \ c_1 \ \textbf{else} \ c_2, \sigma\rangle & \xRightarrow{\text{(Def. } \langle .,. \rangle \to_{Stmt} .\text{)}} & \langle b, \sigma\rangle \to_{Bexp} true & \xRightarrow{\text{Lemma für } b} & (\sigma, true) \in [\![b]\!]_B \\ & & \& & & \& \\ & & \langle c_1, \sigma\rangle \to_{Stmt} \sigma' & \xRightarrow{\text{IH für } c_1} & (\sigma, \sigma') \in [\![c_1]\!]_C \\ & & & & \text{Def. } [\![.]\!]_C \Downarrow \\ & & & & (\sigma, \sigma') \in [\![\textbf{if}(b) \ c_1 \ \textbf{else} \ c_2]\!]_C \end{array}$$

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

$$\begin{array}{ccccc} \langle \textbf{if}(b) \ c_1 \ \textbf{else} \ c_2, \sigma\rangle & \xRightarrow{\text{(Def. } \langle .,. \rangle \to_{Stmt} .\text{)}} & \langle b, \sigma\rangle \to_{Bexp} false & \xRightarrow{\text{Lemma für } b} & (\sigma, false) \in [\![b]\!]_B \\ & & \& & & \& \\ & & \langle c_2, \sigma\rangle \to_{Stmt} \sigma' & \xRightarrow{\text{IH für } c_2} & (\sigma, \sigma') \in [\![c_2]\!]_C \\ & & & & \Downarrow \end{array}$$

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

Induktionsschritt:

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

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

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

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

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

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

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

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

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

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

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

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

Äquivalenz operationale und denotationale Semantik

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

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

- $\Longrightarrow$ Beweis per Induktion über **die (Tiefe der) Ableitung** in der operationalen Semantik (Warum?)
- $\Longleftarrow$ Beweis Prinzip?per struktureller Induktion über c (Verwendung der Äquivalenz für arithmetische und boolsche Ausdrücke). Für die While-Schleife Rückgriff auf Definition des Fixpunkts und Induktion über die Teilmengen $\Gamma^i(\emptyset)$ des Fixpunkts. (Warum?)

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

Induktionsanfang:

- Fall $c \equiv x = a$:

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

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

$$\overset{\text{Lemma } \textbf{Aexp}}{\Longrightarrow}$$

$$\overset{\text{Def. } \langle ..,..\rangle \to_{Stmt} .}{\Longrightarrow} \langle x = a,\sigma\rangle \to_{Stmt} \sigma[x \mapsto t]$$

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

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

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

$$\overset{\text{Def. } \langle ..,..\rangle \to_{Stmt} .}{\Longrightarrow} \langle \{\,\},\sigma\rangle \to_{Stmt} \sigma$$

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

Induktionsschritt:

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

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

Induktionsannahme gilt für c_1 und c_2

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

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

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

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

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

Induktionsschritt:

- Fall $\textbf{while}\ (b)\ c$

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

Induktionsannahme gilt für c

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

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

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

Es gilt die Induktionsannahme für c:

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

Beweis per Induktion über i:

- Induktionsanfang $i = 0$:

$$(\sigma,\sigma') \in \Gamma^0(\emptyset) \Longrightarrow (\sigma,\sigma') \in \emptyset \Longrightarrow false$$

Implikation trivialerweise erfüllt da $false \Longrightarrow P$ immer wahr

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

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

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

- Fallunterscheidung über Zugehörigkeit zur Teilmenge

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

Es gilt die Induktionsannahme für c:

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

Beweis per Induktion über i:

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

$$(\sigma,\sigma'') \in \Gamma(\Gamma^i(\emptyset)) \Longrightarrow \underbrace{(\sigma,true) \in [\![b]\!]_{\mathcal{B}}}_{\text{Lemma } \textbf{Bexp}} \wedge \underbrace{(\sigma,\sigma'') \in [\![c]\!]_{\mathcal{C}}}_{\text{IA (*)}} \wedge \underbrace{(\sigma'',\sigma') \wedge \Gamma^i(\emptyset)}_{\text{IA (UB) für } i}$$

$$\Longrightarrow \langle b,\sigma\rangle \to_{Bexp} true \wedge \langle c,\sigma\rangle \to_{Stmt} \sigma' \wedge \langle \textbf{while}\ (b)\ c,\sigma'\rangle \to_{Stmt} \sigma''$$

$$\Longrightarrow \langle \textbf{while}\ (b)\ c,\sigma\rangle \to_{Stmt} \sigma''$$

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

$$(\sigma,\sigma') \in \Gamma(\Gamma^i(\emptyset)) \Longrightarrow (\sigma,false) \in [\![b]\!]_{\mathcal{B}} \wedge \sigma' = \sigma$$

$$\Longrightarrow \langle b,\sigma\rangle \to_{Bexp} false \wedge \sigma' = \sigma \qquad \text{Lemma für } \textbf{Bexp}$$

$$\Longrightarrow \langle \textbf{while}\ (b)\ c,\sigma\rangle \to_{Stmt} \sigma' \qquad \square$$

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

Induktionsschritt:

- Fall $\textbf{while}\ (b)\ c$

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

Induktionsannahme gilt für c

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

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

Zusammenfassung: Äquivalenz der Semantiken

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

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

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

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

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

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Korrekte Software: Grundlagen und Methoden
Vorlesung 5 vom 17.05.22
Die Floyd-Hoare-Logik I

Serge Autexier, Christoph Lüth

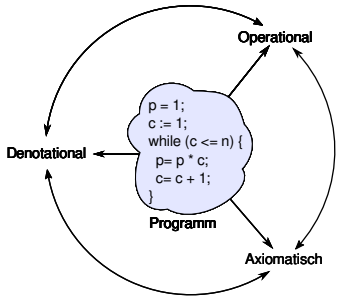
Universität Bremen

Sommersemester 2022

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Drei Semantiken — Eine Sicht



Floyd-Hoare-Logik: Idee

- Was wird hier berechnet? $p = n!$
- Warum? Wie können wir das **beweisen**?
- Wir berechnen symbolisch, welche Werte Variablen über den Programmverlauf annehmen.

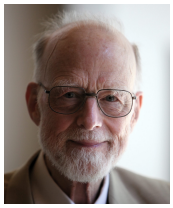
```
p= 1;
c= 1;
while (c <= n) {
  p = p * c;
  c = c + 1;
}
```

- Operationale/denotionale Semantik nicht für **Korrektheitsbeweise** geeignet: Ausdrücke werden zu groß, skaliert nicht — **Abstraktion** nötig.
- Grundprinzip:
  1. Zustandsabhängige **Zusicherungen** für bestimmte Punkte im Programmablauf.
  2. Berechnung der Gültigkeit dieser Zusicherungen durch **zustandsfreie Regeln**.

Bob Floyd und Tony Hoare

Bildquelle: Stanford University

Robert Floyd
1936 – 2001



Bildquelle: Wikipedia

Sir Anthony Charles Richard Hoare
* 1934

Grundbausteine der Floyd-Hoare-Logik

```
// (A)
p= 1;
c= 1;
// (B)
while (c <= n) {
  // (C)
  p= p * c;
  c= c + 1;
  // (D)
}
// (E)
```

- **Zusicherungen** über den Zustand
- Beispiele:
  - (B): Hier gilt $p = c = 1$
  - (D): Hier ist c ist um eines größer als der Wert von c an Punkt (C)
- Gesamtaussage: Wenn bei (A) der Wert von $n \geq 0$ ist, dann ist bei (E) $p = n!$
- Beobachtung:
  - n ist eine „Eingabevariable“, der Wert am Anfang des Programmes (A) ist relevant;
  - p ist eine „Ausgabevariable“, der Wert am Ende des Programmes (E) ist relevant;
  - c ist eine „Arbeitsvariable“, der Wert am Anfang und Ende ist irrelevant

Arbeitsblatt 5.1: Was berechnet dieses Programm?

```
// (A)
x= 1;
c= 1;
// (B)
while (c <= y) {
  // (C)
  x= 2*x;
  c= c+1;
  // (D)
}
// (E)
```

Betrachtet nebenstehendes Programm.
Analog zu dem Beispiel auf der vorherigen Folie:

1. Was berechnet das Programm?
2. Welches sind „Eingabevariablen“, welches „Ausgabevariablen“, welches sind „Arbeitsvariablen“?
3. Welche Zusicherungen und Zusammenhänge gelten zwischen den Variablen an den Punkten (A) bis (E)?

Auf dem Weg zur Floyd-Hoare-Logik

- Kern der Floyd-Hore-Logik sind **zustandsabhängige Aussagen**
- Aber: wie können wir Aussagen **jenseits** des Zustandes treffen?
- Einfaches Beispiel:

```
x = x+ 1;
```

  - Der Wert von x wird um 1 erhöht
  - Der Wert von x ist hinterher größer als vorher
- Wir benötigen **zustandsfreie** Aussagen, um von Zuständen unabhängig **vergleichen** zu können.
- Die Logik **abstrahiert** den Effekt von Programmen.

Grundbausteine der Floyd-Hoare-Logik

- **Logische Variablen** (zustandsfrei) und **Programmvariablen** (zustandsabhängig)
- **Zusicherungen** mit logischen und Programmvariablen
- **Floyd-Hoare-Tripel** $\{P\}\, c\, \{Q\}$
  - Vorbedingung P (Zusicherung)
  - Programm c
  - Nachbedingung Q (Zusicherung)
- Floyd-Hoare-Logik abstrahiert von Programmen zu logischen Formeln.

Zusicherungen (Assertions)

- Erweiterung von **Aexp** and **Bexp** durch
  - **Logische** Variablen **Var** $v := N, M, L, U, V, X, Y, Z$
  - Definierte Funktionen und Prädikate über **Aexp** $n!, x^y, \ldots$
  - Implikation und Quantoren $b_1 \longrightarrow b_2, \forall v.\, b, \exists v.\, b$
- Formal:

$$\begin{aligned}
\textbf{Aexpv}\ a ::= {} & \mathbf{Z} \mid \mathbf{Idt} \mid \mathbf{Var} \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 \times a_2 \mid a_1/a_2 \\
& \mid f(e_1, \ldots, e_n) \\
\textbf{Assn}\ b ::= {} & \mathbf{1} \mid \mathbf{0} \mid a_1 == a_2 \mid a_1 < a_2 \\
& \mid !\, b \mid b_1 \,\&\&\, b2 \mid b_1 \,||\, b_2 \\
& \mid b_1 --> b_2 \mid p(e_1, \ldots, e_n) \mid \backslash\mathbf{forall}\ v.\, b \mid \backslash\mathbf{exists}\ v.\, b \\
\textbf{Assn}\ b ::= {} & \mathit{true} \mid \mathit{false} \mid a_1 = a_2 \mid a_1 \leq a_2 \\
& \mid \neg b \mid b_1 \wedge b2 \mid b_1 \vee b_2 \\
& \mid b_1 \longrightarrow b_2 \mid p(e_1, \ldots, e_n) \mid \forall v.\, b \mid \exists v.\, b
\end{aligned}$$

Denotationale Semantik von Zusicherungen

- Erste Näherung: Funktion

$$[\![a]\!]_{\mathcal{A}} : \mathbf{Aexpv} \to (\Sigma \rightharpoonup \mathbb{Z})$$
$$[\![b]\!]_{\mathcal{B}} : \mathbf{Assn} \to (\Sigma \rightharpoonup \mathbb{B})$$

  - **Konservative** Erweiterung von $[\![a]\!]_{\mathcal{A}} : \mathbf{Aexp} \to (\Sigma \rightharpoonup \mathbb{Z})$
- Aber: was ist mit den logischen Variablen?
- Zusätzlicher Parameter **Belegung** der logischen Variablen $I : \mathbf{Var} \to \mathbb{Z}$

$$[\![a]\!]_{\mathcal{A}} : \mathbf{Aexpv} \to (\mathbf{Var} \to \mathbb{Z}) \to (\Sigma \rightharpoonup \mathbb{Z})$$
$$[\![b]\!]_{\mathcal{B}} : \mathbf{Assn} \to (\mathbf{Var} \to \mathbb{Z}) \to (\Sigma \rightharpoonup \mathcal{B})$$

- Bemerkung: $I : \mathbf{Var} \to \mathbb{Z}$ ist immer eine **totale Funktion** im Gegensatz zu einem Zustand.

Denotat von Aexp

$$[\![a]\!]_{\mathcal{A}} : \mathbf{Aexp} \to (\Sigma \rightharpoonup \mathbb{Z})$$

$$\begin{aligned}
[\![n]\!]_{\mathcal{A}} &= \{(\sigma, [\![n]\!]) \mid \sigma \in \Sigma\} \\
[\![x]\!]_{\mathcal{A}} &= \{(\sigma, \sigma(x)) \mid \sigma \in \Sigma, x \in \mathit{Dom}(\sigma)\} \\
[\![a_0 + a_1]\!]_{\mathcal{A}} &= \{(\sigma, n_0 + n_1) \mid (\sigma, n_0) \in [\![a_0]\!]_{\mathcal{A}} \wedge (\sigma, n_1) \in [\![a_1]\!]_{\mathcal{A}}\} \\
[\![a_0 - a_1]\!]_{\mathcal{A}} &= \{(\sigma, n_0 - n_1) \mid (\sigma, n_0) \in [\![a_0]\!]_{\mathcal{A}} \wedge (\sigma, n_1) \in [\![a_1]\!]_{\mathcal{A}}\} \\
[\![a_0 * a_1]\!]_{\mathcal{A}} &= \{(\sigma, n_0 \times n_1) \mid (\sigma, n_0) \in [\![a_0]\!]_{\mathcal{A}} \wedge (\sigma, n_1) \in [\![a_1]\!]_{\mathcal{A}}\} \\
[\![a_0/a_1]\!]_{\mathcal{A}} &= \{(\sigma, n_0 \div n_1) \mid (\sigma, n_0) \in [\![a_0]\!]_{\mathcal{A}} \wedge (\sigma, n_1) \in [\![a_1]\!]_{\mathcal{A}} \wedge n_1 \neq 0\}
\end{aligned}$$

Denotat von Aexpv

$$[\![a]\!]_{\mathcal{A}} : \mathbf{Aexpv} \to (\mathbf{Var} \to \mathbb{Z}) \to\!\!\to (\Sigma \rightharpoonup \mathbb{Z})$$

Sei $I : \mathbf{Var} \to \mathbb{Z}$ eine beliebige Belegung

$$\begin{aligned}
[\![n]\!]'_{\mathcal{A}} &= \{(\sigma, [\![n]\!]) \mid \sigma \in \Sigma\} \\
[\![x]\!]'_{\mathcal{A}} &= \{(\sigma, \sigma(x)) \mid \sigma \in \Sigma, x \in \mathit{Dom}(\sigma)\} \\
[\![a_0 + a_1]\!]'_{\mathcal{A}} &= \{(\sigma, n_0 + n_1) \mid (\sigma, n_0) \in [\![a_0]\!]'_{\mathcal{A}} \wedge (\sigma, n_1) \in [\![a_1]\!]'_{\mathcal{A}}\} \\
[\![a_0 - a_1]\!]'_{\mathcal{A}} &= \{(\sigma, n_0 - n_1) \mid (\sigma, n_0) \in [\![a_0]\!]'_{\mathcal{A}} \wedge (\sigma, n_1) \in [\![a_1]\!]'_{\mathcal{A}}\} \\
[\![a_0 * a_1]\!]'_{\mathcal{A}} &= \{(\sigma, n_0 \times n_1) \mid (\sigma, n_0) \in [\![a_0]\!]'_{\mathcal{A}} \wedge (\sigma, n_1) \in [\![a_1]\!]'_{\mathcal{A}}\} \\
[\![a_0/a_1]\!]'_{\mathcal{A}} I &= \{(\sigma, n_0 \div n_1) \mid (\sigma, n_0) \in [\![a_0]\!]'_{\mathcal{A}} \wedge (\sigma, n_1) \in [\![a_1]\!]'_{\mathcal{A}} \wedge n_1 \neq 0\} \\
[\![X]\!]'_{\mathcal{A}} &= \{(\sigma, I(X)) \mid \sigma \in \Sigma, X \in V\}
\end{aligned}$$

Erfüllung von Zusicherungen

- Wann gilt eine Zusicherung $b \in \mathbf{Assn}$ in einem Zustand σ?
  - Auswertung (denotationale Semantik) ergibt *true*
  - Belegung ist zusätzlicher Parameter

Erfülltheit von Zusicherungen

$b \in \mathbf{Assn}$ ist in Zustand σ mit Belegung I erfüllt ($\sigma \models^I b$), gdw

$$[\![b]\!]'_{\mathcal{B}}(\sigma) = \mathit{true}$$

Arbeitsblatt 5.2: Zusicherungen

Betrachte folgende Zusicherung:

$$a \quad \equiv \quad \underbrace{2 \cdot x = X}_{p} \longrightarrow \underbrace{x < X}_{q}$$

Gegeben folgende Belegungen $I_1, \ldots, I_3$ und Zustände $s_1, \ldots, s_3$:

$$s_1 = \langle x \mapsto 0 \rangle, s_2 = \langle x \mapsto 1 \rangle, s_3 = \langle x \mapsto 5 \rangle$$
$$I_1 = \langle X \mapsto 0 \rangle, I_2 = \langle X \mapsto 2 \rangle, I_3 = \langle X \mapsto 10 \rangle$$

Unter welchen Belegungen und Zuständen ist a wahr?

	I_1			I_2			I_3		
	p	q	a	p	q	q	p	q	a
s_1									
s_2									
s_3									

Wie kann man a so ändern, dass a für **alle** Belegungen und Zustände wahr ist?

Floyd-Hoare-Tripel

Partielle Korrektheit ($\models \{P\}\, c\, \{Q\}$)

$\{P\}\, c\, \{Q\}$ ist **partiell korrekt**, wenn für all Belegungen I und alle Zustände σ, die P erfüllen, gilt: **wenn** die Ausführung von c mit σ in einem Zustand τ terminiert, **dann** erfüllt τ mit Belegung I Q.

$$\models \{P\}\, c\, \{Q\} \iff \forall I.\, \forall \sigma.\, \sigma \models^I P \wedge \exists \tau.\, (\sigma, \tau) \in [\![c]\!]_{\mathcal{C}} \Longrightarrow \tau \models^I Q$$

- Gleiche Belegung der logischen Variablen in P und Q erlaubt **Vergleich** zwischen Zuständen

Totale Korrektheit ($\models [P]\, c\, [Q]$)

$[P]\, c\, [Q]$ ist **total korrekt**, wenn für all Belegungen I und alle Zustande σ, die P erfüllen, die Ausführung von c mit σ in einem Zustand τ terminiert, und τ mit der Belegung I erfüllt Q.

$$\models [P]\, c\, [Q] \iff \forall I.\, \forall \sigma.\, \sigma \models^I P \Longrightarrow \exists \tau.\, (\sigma, \tau) \in [\![c]\!]_{\mathcal{C}} \wedge \tau \models^I Q$$

Beispiele

- Folgendes **gilt**:

$$\models \{true\}\ \textbf{while}(1)\{\ \}\ \{true\}$$

- Folgendes gilt **nicht**:

$$\models [true]\ \textbf{while}(1)\{\ \}\ [true]$$

- Folgende **gelten**:

$$\models \{false\}\ \textbf{while}\ (\mathbf{1})\ \{\ \}\ \{true\}$$
$$\models [false]\ \textbf{while}\ (\mathbf{1})\ \{\ \}\ [true]$$

Wegen *ex falso quodlibet*: $false \Longrightarrow \phi$

Arbeitsblatt 5.3: Gültigkeit

Welche dieser Hoare-Tripel ist semantisch gültig?

```
// {x = X ∧ x ≥ 3}
x= x−3;
if (x < 0) x= 0;
x= x+3;
// {x = X}
```

```
// {b = B}
b= b−a;
x= a+b;
// {x = a + B}
```

```
// {x = X ∧ y = Y}
x= x+y;
y= x−y;
x= x−y;
// {x = Y ∧ y = X}
```


Gültigkeit und Herleitbarkeit

- **Semantische Gültigkeit:** $\models \{P\}\, c\, \{Q\}$
  - Definiert durch denotationale Semantik:

$$\models \{P\}\, c\, \{Q\} \iff \forall I.\, \forall \sigma.\, \sigma \models^I P \land \exists \tau.\, (\sigma, \tau) \in [\![c]\!]_c \Longrightarrow \tau \models^I Q$$

  - Problem: müssten Semantik von c ausrechnen
- **Syntaktische Herleitbarkeit:** $\vdash \{P\}\, c\, \{Q\}$
  - Durch **Regeln** definiert
  - Kann **hergeleitet** werden
  - Muss **korrekt** bezüglich semantischer Gültigkeit gezeigt werden
- Generelles Vorgehen in der Logik

Regeln des Floyd-Hoare-Kalküls

- Der Floyd-Hoare-Kalkül erlaubt es, Zusicherungen der Form $\vdash \{P\}\, c\, \{Q\}$ syntaktisch **herzuleiten**.
- Der **Kalkül** der Logik besteht aus sechs Regeln der Form

$$\frac{\vdash \{P_1\}\, c_1\, \{Q_1\} \ldots \vdash \{P_n\}\, c_n\, \{Q_n\}}{\vdash \{P\}\, c\, \{Q\}}$$

- Für jedes Konstrukt der Programmiersprache gibt es eine Regel.

Regeln des Floyd-Hoare-Kalküls: Zuweisung

$$\overline{\vdash \{P[e/x]\}\, x = e\, \{P\}}$$

- Eine Zuweisung x=e ändert den Zustand so dass an der Stelle x jetzt der Wert von e steht. Damit **nachher** das Prädikat P gilt, muss also **vorher** das Prädikat gelten, wenn wir x durch e ersetzen.
- Es ist völlig normal (aber dennoch falsch) zu denken, die Substitution gehöre eigentlich in die Nachbedingung.
- Beispiele:

```
// {?(x < 10)[5/x] ⟺ 5 < 10}
x = 5
// {x < 10}
```

```
//{x + 1 < 10 ⟺ x < 9}
x = x+ 1
//{x < 10}
```


Regeln des Floyd-Hoare-Kalküls: Sequenzierung

$$\frac{\vdash \{A\}\, c_1\, \{B\} \qquad \vdash \{B\}\, c_2\, \{C\}}{\vdash \{A\}\, c_1; c_2\, \{C\}}$$

- Hier wird eine Zwischenzusicherung B benötigt.

$$\overline{\vdash \{A\}\, \{\}\, \{A\}}$$

- Trivial.

Ein allererstes Beispiel

```
z= x;
x= y;
y= z;
```

- Was berechnet dieses Programm?
- Die Werte von x und y werden vertauscht.
- Wie spezifizieren wir das?
- $\vdash \{x = X \land y = Y\}\, p\, \{y = X \land x = Y\}$

Herleitung:

$$\dfrac{\dfrac{\dfrac{\vdash \{x = X \land y = Y\}\ z = x;\ \{?z = X \land y = Y\} \qquad \vdash \{?z = X \land y = Y\}\ x = y;\ \{z = X \land x = Y\}}{\vdash \{x = X \land y = Y\}\ z = x; x = y;\ \{?z = X \land x = Y\}} \qquad \overline{\vdash \{?z = X \land x = Y\}\ y = z;\ \{y = X \land x = Y\}}}{\vdash \{x = X \land y = Y\}\ z = x; x = y; y = z;\ \{y = X \land x = Y\}}$$

Vereinfachte Notation für Sequenzen

```
// {y = Y ∧ x = X}
z= x;
// {y = Y ∧ z = X}
x= y;
// {x = Y ∧ z = X}
y= z;
// {x = Y ∧ y = X}
```

- Die **gleiche** Information wie der Herleitungsbaum
- aber **kompakt** dargestellt
- Beweis erfolgt **rückwärts** (von der letzten Zuweisung ausgehend)

Arbeitsblatt 5.4: Ein erster Beweis

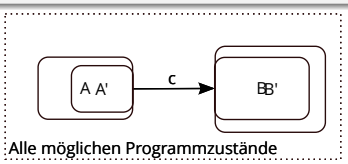
Betrachte den Rumpf des Fakultätsprogramms:

```
// (B)
p= p* c;
// (A)
c= c+ 1;
// {p = (c − 1)!}
```

- Welche Zusicherungen gelten
  1. an der Stelle (A)?
  2. an der Stelle (B)?

Regeln des Floyd-Hoare-Kalküls: Weakening

$$\frac{A' \Longrightarrow A \qquad \vdash \{A\}\, c\, \{B\} \qquad B \Longrightarrow B'}{\vdash \{A'\}\, c\, \{B'\}}$$



- $\models \{A\}\, c\, \{B\}$: Ausführung von c startet in Zustand, in dem A gilt, und endet (ggf) in Zustand, in dem B gilt.
- Zustandsprädikate beschreiben Mengen von Zuständen:

$$\{\sigma \in \Sigma | \sigma \models^I P\} \subseteq \{\sigma \in \Sigma | \sigma \models^I Q\} \text{ gdw. } P \Longrightarrow Q$$

- Wir können A zu A' einschränken ($A' \subseteq A$ oder $A' \Longrightarrow A$), oder B zu B' vergrößern ($B \subseteq B'$ oder $B \Longrightarrow B'$), und erhalten $\models \{A'\}\, c\, \{B'\}$.

Arbeitsblatt 5.5: Ein zweiter Beweis

Wir betrachten noch einmal das Vertauschen, diesmal ohne Hilfsvariable:

```
// {x = X ∧ y = Y}
// (A)
x= x+y;
// (B)
y= x−y;
// (C)
x= x−y;
// {y = X ∧ x = Y}
```

- Welche Zusicherungen gelten an den Stellen (A), (B), (C) und wie werden sie so vereinfacht, dass die Vorbedingung entsteht?
  1. (C)?
  2. (B)?
  3. (A)?

Regeln des Floyd-Hoare-Kalküls: Fallunterscheidung

$$\frac{\vdash \{A \wedge b\}\, c_0\, \{B\} \qquad \vdash \{A \wedge \neg b\}\, c_1\, \{B\}}{\vdash \{A\}\ \textbf{if}\ (b)\ c_0\ \textbf{else}\ c_1\, \{B\}}$$

- In der Vorbedingung des **if**-Zweiges gilt die Bedingung b, und im **else**-Zweig gilt die Negation $\neg b$.
- Beide Zweige müssen mit derselben Nachbedingung enden.

Arbeitsblatt 5.6: Dreimal ist Bremer Recht

Betrachte folgendes Programm:

```
// (F)
if (x < y) {
  // (E)
  // ...
  z = x;
  // (C)
} else {
  // (D)
  // ...
  z= y;
  // (B)
}
// (A)
```

- Was berechnet dieses Programm?
- Wie spezifizieren wir das?
- Welche Zusicherungen müssen an den Stellen (A) – (F) gelten?
- Wo müssen wir welche logische Umformungen nutzen?

Regeln des Floyd-Hoare-Kalküls: Iteration

$$\frac{\vdash \{A \wedge b\}\, c\, \{A\}}{\vdash \{A\}\ \textbf{while}(b)\ c\, \{A \wedge \neg b\}}$$

- Iteration korrespondiert zu **Induktion**.
- Bei wohlfundierter Induktion zeigen wir, dass die **gleiche** Eigenschaft für alle x gilt, $P(x)$, wenn sie für alle kleineren y gilt — d.h. wenn y größer wird muss die Eigenschaft weiterhin gelten.
- Analog dazu benötigen wir hier eine **Invariante** A, die sowohl **vor** als auch **nach** dem Schleifenrumpf gilt.
- In der Vorbedingung des Schleifenrumpfes können wir die Schleifenbedingung b annehmen.
- Die **Vorbedingung** der **Schleife** ist die Invariante A, und die **Nachbedingung** der **Schleife** ist A und die Negation der Schleifenbedingung b.

Wie wir Floyd-Hoare-Beweise aufschreiben

```
// {P}
// {P2[e/x]}
x= e;
// {P3}
while (x< n) {
  // {P3 ∧ x < n}
  // {P3[a/z]}
  z= a;
  // {P3}
}
// {P3 ∧ ¬(x < n)}
// {Q}
```

- Beispiel zeigt: $\vdash \{P\}\, c\, \{Q\}$
- Programm wird mit gültigen Zusicherungen annotiert.
- Vor einer Zeile steht die Vorbedingung, danach die Nachbedingung.
  - Muss genau auf Anweisung passen.
- Implizite Anwendung der Sequenzenregel.
- Weakening wird notiert durch mehrere Zusicherungen, und muss **bewiesen** werden.
  - Im Beispiel: $P \Longrightarrow P_2[e/x]$, $P_2 \Longrightarrow P_3$, $P_3 \wedge x < n \Longrightarrow P_4$, $P_3 \wedge \neg(x < n) \Longrightarrow Q$.

Überblick: die Regeln des Floyd-Hoare-Kalküls

$$\frac{}{\vdash \{P[e/x]\}\, x = e\, \{P\}}$$

$$\frac{\vdash \{A \wedge b\}\, c_0\, \{B\} \qquad \vdash \{A \wedge \neg b\}\, c_1\, \{B\}}{\vdash \{A\}\ \textbf{if}\ (b)\ c_0\ \textbf{else}\ c_1\, \{B\}}$$

$$\frac{\vdash \{A \wedge b\}\, c\, \{A\}}{\vdash \{A\}\ \textbf{while}(b)\ c\, \{A \wedge \neg b\}}$$

$$\frac{}{\vdash \{A\}\, \{\}\, \{A\}} \qquad \frac{\vdash \{A\}\, c_1\, \{B\} \qquad \vdash \{B\}\, c_2\, \{C\}}{\vdash \{A\}\, c_1; c_2\, \{C\}}$$

$$\frac{A' \Longrightarrow A \qquad \vdash \{A\}\, c\, \{B\} \qquad B \Longrightarrow B'}{\vdash \{A'\}\, c\, \{B'\}}$$

Zusammenfassung Floyd-Hoare-Logik

- Die Logik abstrahiert über konkrete Systemzustände durch **Zusicherungen**
- Zusicherungen sind boolsche Ausdrücke, angereichert durch logische Variablen.
- **Hoare-Tripel** $\{P\}\, c\, \{Q\}$ abstrahieren die Semantik von c
  - Semantische **Gültigkeit** von Hoare-Tripeln: $\models \{P\}\, c\, \{Q\}$.
  - Syntaktische **Herleitbarkeit** von Hoare-Tripeln: $\vdash \{P\}\, c\, \{Q\}$
- **Zuweisungen** werden durch **Substitution** modelliert, d.h. die Menge der gültigen Aussagen ändert sich.
- Für Iterationen wird eine **Invariante** benötigt (die **nicht** hergeleitet werden kann).

Korrekte Software: Grundlagen und Methoden

Vorlesung 6 vom 24.05.22

Floyd-Hoare-Logik II: Invarianten

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2022

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Die Floyd-Hoare-Logik bis hierher

- **Hoare-Tripel** $\{P\}\,c\,\{Q\}$ spezifizieren was c berechnet (**Korrektheit**)
  - Semantische **Gültigkeit** von Hoare-Tripeln: $\models \{P\}\,c\,\{Q\}$.
  - Syntaktische **Herleitbarkeit** von Hoare-Tripeln: $\vdash \{P\}\,c\,\{Q\}$
- **Zuweisungen** werden durch **Substitution** modelliert, d.h. die Menge der gültigen Aussagen ändert sich.
- Für Iterationen wird eine **Invariante** benötigt (die **nicht** hergeleitet werden kann).

Überblick: die Regeln des Floyd-Hoare-Kalküls

$$\frac{}{\vdash \{P[e/x]\}\,x = e\,\{P\}}$$

$$\frac{\vdash \{A \wedge b\}\,c_0\,\{B\} \qquad \vdash \{A \wedge \neg b\}\,c_1\,\{B\}}{\vdash \{A\}\ \textbf{if}\ (b)\ c_0\ \textbf{else}\ c_1\,\{B\}}$$

$$\frac{\vdash \{A \wedge b\}\,c\,\{A\}}{\vdash \{A\}\ \textbf{while}(b)\ c\,\{A \wedge \neg b\}}$$

$$\frac{}{\vdash \{A\}\,\{\}\,\{A\}} \qquad \frac{\vdash \{A\}\,c_1\,\{B\} \qquad \vdash \{B\}\,c_2\,\{C\}}{\vdash \{A\}\,c_1; c_2\,\{C\}}$$

$$\frac{A' \Longrightarrow A \qquad \vdash \{A\}\,c\,\{B\} \qquad B \Longrightarrow B'}{\vdash \{A'\}\,c\,\{B'\}}$$

Invarianten finden: die Fakultät

```
1  p= 1;
2  c= 1;
3  // {I}
4  while (c <= n) {
5    // {I ∧ c ≤ n}
6    p = p * c;
7    c = c + 1;
8    // {I}
9  }
10 // {I ∧ ¬(c ≤ n)}
11 // {p = n!}
```

Invariante:

$$p = (c-1)! \wedge c - 1 \leq n \wedge c > 0$$

- Kern der Invariante: Fakultät bis $c-1$ berechnet.
- Invariante impliziert Nachbedingung $p = n! = (c-1)!$
  - $\neg(c \leq n) \Leftrightarrow c - 1 \geq n$ — was fehlt?
- Nebenbedingung für Weakening innerhalb der Schleife.
  - $c! = c * (c-1)!$ gilt nur für $c > 0$.

Invarianten finden

1. Initiale Invariante: momentaner Zustand der Berechnung
2. Invariante und negierte Schleifenbedingung muss Nachbedingung implizieren; ggf. Invariante verstärken.
3. Beweise innerhalb der Schleife benötigen ggf. weiter Nebenbedingungen; Invariante verstärken.

Zählende Schleifen

- Fakultät ist Beispiel für zählende Schleife (**for**).
- Für Nachbedingung $\psi[n]$ ist Invariante:

$$\psi[i-1/n] \wedge i - 1 \leq n$$

- Ggf. weitere Nebenbedingungen erforderlich
- Variante: $i = 0, \ldots, n-1$

```
for (i= 1; i<= n; i++) {
  ...
}
```

ist syntaktischer Zucker für

```
i= 1;
while (i<= b ) {
  ...
  i= i+1;
}
```


Arbeitsblatt 6.1: Summe I

```
1 // {0 ≤ n}
2 x= 0;
3 c= 1;
4 while (c <= n) {
5   x= x+c;
6   c= c+1;
7 }
8 // {x = sum(0, n)}
```

1. Was ist die initiale Invariante?
2. Was fehlt, um aus der initialen Invariante die Nachbedingung zu schließen?
3. Was fehlt, damit der Schleifenrumpf die Invariante erhält?

Annotiert das Programm mit den Korrektheitszusicherungen!

Hierbei ist $sum(a, b)$ die Summe der Zahlen von a bis b, mit folgenden Eigenschaften:

$$a > b \Longrightarrow sum(a, b) = 0$$
$$a \leq b \Longrightarrow sum(a, b) = a + sum(a+1, b)$$
$$a \leq b \Longrightarrow sum(a, b) = sum(a, b-1) + b$$

Variante der zählenden Schleife

```
// {0 ≤ y}
// {0 = sum(0,0) ∧ 0 ≤ y ∧ 0 ≤ 0}
x= 0;
// {x = sum(0,0) ∧ 0 ≤ y ∧ 0 ≤ 0}
c= 0;
// {x = sum(0,c) ∧ c ≤ y ∧ 0 ≤ c}
while (c < y) {
 // {x = sum(0,c) ∧ c ≤ y ∧ 0 ≤ c ∧ c < y}
 // {x + (c+1) = sum(0,c) + (c+1) ∧ c < y ∧ 0 ≤ c}
 // {x + c + 1 = sum(0,c+1) ∧ c+1 ≤ y ∧ 0 ≤ c+1}
 c= c+1;
 // {x + c = sum(0,c) ∧ c ≤ y ∧ 0 ≤ c}
 x= x+c;
 // {x = sum(0,c) ∧ c ≤ y ∧ 0 ≤ c}
}
// {x = sum(0,c) ∧ c ≤ y ∧ 0 ≤ c ∧ ¬(c < y)}
// {x = sum(0,c) ∧ c ≤ y ∧ c ≥ y}
// {x = sum(0,y)}
```

- Was ist hier die Invariante?

$$x = sum(0,c) \land c \leq y \land 0 \leq c$$

- Kein C-Idiom
  - Startwert 0 wird ausgelassen

Arbeitsblatt 6.2: Summe II

```
// {n = N ∧ 0 ≤ n}
x= 0;
while (n != 0) {
 x= x+n;
 n= n−1;
}
// {x = sum(0,N)}
```

- Was ist der erste Teil der Invariante?
- Der Rest ist wie vorher?
- Annotiert das Programm mit dem Korrektheitszusicherungen.

Fakultät Revisited

Dieses Programm berechnet die Fakultat von n:

```
// {n = N ∧ 0 ≤ n}
// {n! = N! ∧ n = N ∧ 0 ≤ n}
// {n! · 1 = N! ∧ n ≤ N ∧ 0 ≤ n}
p= 1;
// {n! · p = N! ∧ n ≤ N ∧ 0 ≤ n}
while (0 < n) {
 // {n! · p = N! ∧ n ≤ N ∧ 0 ≤ n ∧ 0 < n}
 // {n! · p = N! ∧ n ≤ N ∧ 0 < n}
 // {(n−1)! · n · p = N! ∧ n ≤ N ∧ 0 < n}
 p= n*p;
 // {(n−1)! · p = N! ∧ n ≤ N ∧ 0 < n}
 // {(n−1)! · p = N! ∧ n − 1 ≤ N ∧ 0 ≤ n − 1}
 n= n−1;
 // {n! · p = N! ∧ n ≤ N ∧ 0 ≤ n}
}
// {n! · p = N! ∧ n ≤ N ∧ 0 ≤ n ∧ ¬(0 < n)}
// {n! · p = N! ∧ 0 ≤ n ∧ n ≥ 0}
// {p = N!}
```

$n! \cdot p = N!$
$\land\ 0 \leq n$
$\land\ n \leq n$

Arbeitsblatt 6.3: Nicht-zählende Schleife

```
1 // {0 ≤ a}
2 r= a;
3 q= 0;
4 while (b <= r) {
5    r= r−b;
6    q= q+1;
7    }
8 // {a = b · q + r ∧ 0 ≤ r ∧ r < b}
```

Was ist hier die Invariante?

- Hinweis: es ist ganz einfach.

Beispiel 5: Jetzt wird's kompliziert...

```
1  // {0 ≤ a}
2  t= 1;
3  s= 1;
4  i= 0;
5  while (s <= a) {
6     t= t+ 2;
7     s= s+ t;
8     i= i+ 1;
9     }
10 // ?{i² ≤ a ∧ a < (i+1)²}
```

- Was berechnet das? Ganzzahlige Wurzel von a.
- Invariante:

$$s - t \leq a\ \land\ t = 2 \cdot i + 1\ \land\ s = i^2 + t$$

- Nachbedingung 1:
  - $s - t \leq a, s = i^2 + t \Longrightarrow i^2 \leq a$.
- Nachbedingung 2:
  - $s = i^2 + t, t = 2 \cdot i + 1 \Longrightarrow s = (i+1)^2$
  - $a < s, s = (i+1)^2 \Longrightarrow a < (i+1)^2$

Beispiel 5: Jetzt wird's kompliziert...

```
// {0 ≤ a}
// {1 − 1 ≤ a ∧ 1 = 2·0 + 1 ∧ 1 = 0² + 1}
t= 1;
// {1 − t ≤ a ∧ t = 2·0 + 1 ∧ 1 = 0² + t}
s= 1;
// {s − t ≤ a ∧ t = 2·0 + 1 ∧ s = 0² + t}
i= 0;
// {s − t ≤ a ∧ t = 2·i + 1 ∧ s = i² + t}
while (s <= a) {
  // {s − t ≤ a ∧ t = 2·i + 1 ∧ s = i² + t ∧ s ≤ a}
  // {t = 2·i + 1 ∧ s = i² + t ∧ s ≤ a}
  // {s ≤ a ∧ t + 2 = 2·i + 3 ∧ s = i² + 2·i + 1}
  // {s + (t+2) − (t+2) ≤ a ∧ t + 2 = 2·(i+1) + 1 ∧ s + (t+2) = (i+1)² + (t+2)}
  t= t+ 2;
  // {s + t − t ≤ a ∧ t = 2·(i+1) + 1 ∧ s + t = (i+1)² + t}
  s= s+ t;
  // {s − t ≤ a ∧ t = 2·(i+1) + 1 ∧ s = (i+1)² + t}
  i= i+ 1;
  // {s − t ≤ a ∧ t = 2·i + 1 ∧ s = i² + t}
  }
// {s − t ≤ a ∧ t = 2·i + 1 ∧ s = i² + t ∧ ¬(s ≤ a)}
// {?i² ≤ a ∧ a < (i+1)²}
```


Zum Abschluss etwas Magie

Fast Inverse Square Root
(Quake III, John Cormack)

```
float Q_rsqrt( float number )
{
 long i;
 float x2, y;
 const float threehalfs = 1.5F;

 x2 = number* 0.5F;
 y  = number;
 i  = * (long *) &y;
 i  = 0x5f3759df − ( i >> 1 );
 y  = * (float *) &i;
 y  = y * (threehalfs − (x2 * y * y));
// y = y * (threehalfs - (x2 * y * y));
 return y;
}
```

- Berechnet effizient Approximation von $\frac{1}{\sqrt{y}}$
- Verkürztes **Newton-Verfahren**
- „Evil floating-point bit-level hacking“
- $0x5f3759df = 1.597.463.007 \approx \sqrt{2^{127}}$
- Nicht zu verifizieren (nicht standard-konform)

Zusammenfassung

- Der schwierigste Teil bei Korrektheitsbeweisen mit dem Floyd-Hoare-Kalkül sind die while-Schleifen.
- Die Regel für die while-Schleife braucht eine **Invariante**, die nicht aus der Anwendung erschlossen werden kann.
- Wir können die Invariante in drei Stufen konstruieren:
  1. Algorithmischer Kern: was wird bis hier berechnet?
  2. Ist die Invariante **stark** genug, um die Nachbedingung zu implizieren?
  3. Wird die Invariante durch die Schleife erhalten? Werden noch Nebenbedingungen benötigt?
- Vereinfachender Sonderfall: **zählende** Schleifen (for-Schleifen)

Korrekte Software: Grundlagen und Methoden
Vorlesung 7 vom 02.06.22
Korrektheit des Floyd-Hoare-Kalküls

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2022

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Floyd-Hoare-Tripel: Gültigkeit und Herleitbarkeit

- Definition von letzter Woche: $P, Q \in \mathbf{Assn}, c \in \mathbf{Stmt}$

  $\models \{P\}\, c\, \{Q\}$ "Hoare-Tripel gilt" (semantisch)

  $\vdash \{P\}\, c\, \{Q\}$ "Hoare-Tripel herleitbar" (syntaktisch)

- **Frage**: $\vdash \{P\}\, c\, \{Q\} \overset{?}{\rightsquigarrow} \models \{P\}\, c\, \{Q\}$
- **Korrektheit**: $\vdash \{P\}\, c\, \{Q\} \overset{?}{\Longrightarrow} \models \{P\}\, c\, \{Q\}$
  - Wir können nur gültige Eigenschaften von Programmen herleiten.
- **Vollständigkeit**: $\models \{P\}\, c\, \{Q\} \overset{?}{\Longrightarrow} \vdash \{P\}\, c\, \{Q\}$
  - Wir können alle gültigen Eigenschaften auch herleiten.

Überblick: die Regeln des Floyd-Hoare-Kalküls

$$\frac{}{\vdash \{P[e/x]\}\, x = e\, \{P\}}$$

$$\frac{\vdash \{A \wedge b\}\, c_0\, \{B\} \qquad \vdash \{A \wedge \neg b\}\, c_1\, \{B\}}{\vdash \{A\}\ \textbf{if}\ (b)\ c_0\ \textbf{else}\ c_1\, \{B\}}$$

$$\frac{\vdash \{A \wedge b\}\, c\, \{A\}}{\vdash \{A\}\ \textbf{while}(b)\ c\, \{A \wedge \neg b\}}$$

$$\frac{}{\vdash \{A\}\, \{\}\, \{A\}} \qquad \frac{\vdash \{A\}\, c_1\, \{B\} \qquad \vdash \{B\}\, c_2\, \{C\}}{\vdash \{A\}\, c_1; c_2\, \{C\}}$$

$$\frac{A' \Longrightarrow A \qquad \vdash \{A\}\, c\, \{B\} \qquad B \Longrightarrow B'}{\vdash \{A'\}\, c\, \{B'\}}$$

Korrektheit des Floyd-Hoare-Kalküls

Der Floyd-Hoare-Kalkül ist korrekt.
Wenn $\vdash \{P\}\, c\, \{Q\}$, dann $\models \{P\}\, c\, \{Q\}$.

Beweis:

- Definition von $\models \{P\}\, c\, \{Q\}$:

$$\models \{P\}\, c\, \{Q\} \iff \forall I.\, \forall \sigma.\, \sigma \models^I P \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![c]\!]_C \Longrightarrow \sigma' \models^I Q$$

- Beweis durch **Regelinduktion** über der **Herleitung** von $\vdash \{P\}\, c\, \{Q\}$.
- Bsp: Zuweisung, Sequenz, Weakening, While.
  - While-Schleife erfordert Induktion über Fixpunkt-Konstruktion

Korrektheit der Zuweisung

$$\frac{}{\vdash \{P[e/x]\}\, x = e\, \{P\}}$$

Zu zeigen: $\models \{P[e/x]\}\, x = e\, \{P\}$

$$\begin{aligned} &\iff \forall I.\, \forall \sigma.\, \sigma \models^I P[e/x] \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![x = e]\!]^I_C \Longrightarrow \sigma' \models^I P \\ &\iff \forall I.\, \forall \sigma.\, \sigma \models^I P[e/x] \Longrightarrow \sigma([x \mapsto [\![e]\!]_{\mathcal{A}}(\sigma)]) \models^I P \\ &\quad \text{with } (\sigma, \sigma([x \mapsto [\![e]\!]^I_{\mathcal{A}}(\sigma)])) \in [\![x = e]\!]_C \end{aligned}$$

Wir benötigen folgende **Lemmata** (Beweis durch strukturelle Induktion über B und a):

$$\sigma \models^I B[e/x] \iff \sigma[x \mapsto [\![e]\!]_{\mathcal{A}}(\sigma)] \models^I B \quad (1)$$

$$[\![a[e/x]]\!]^I_{\mathcal{A}}(\sigma) = [\![a]\!]^I_{\mathcal{A}}(\sigma[x \mapsto [\![e]\!]^I_{\mathcal{A}}(\sigma)]) \quad (2)$$

Arbeitsblatt 7.1: Substitution und Zustands-Update

$$\sigma \models^I B[e/x] \iff \sigma[x \mapsto [\![e]\!]_{\mathcal{A}}(\sigma)] \models^I B \quad (3)$$

Beweis per strukureller Induktion über B. Zeigt die folgenden Fälle des Beweises:

1. Induktionsanfang: B ist $a_0 = a_1$
2. Induktionsschritt: B ist der Form $B_1 \&\& B_2$

Anmerkung:

- $\sigma \models^I B \iff [\![B]\!]^I_{\mathcal{B}}(\sigma) = \mathit{true}$
- $[\![a[e/y]]\!]^I_{\mathcal{A}}(\sigma) = [\![a]\!]^I_{\mathcal{A}}(\sigma[y \mapsto [\![e]\!]^I_{\mathcal{A}}(\sigma)])$
- $[\![.]\!]_{\mathcal{A}}$ ist strikt
- Falls für einen Ausdruck a $[\![a]\!]^I_{\mathcal{A}}$ undefiniert ist ($[\![a]\!]^I_{\mathcal{A}} = \bot$), dann ist $\sigma[x \mapsto [\![a]\!]^I_{\mathcal{A}}]$ auch undefiniert.
- $[\![.]\!]_{\mathcal{B}}$ ist nicht strikt.

Korrektheit der Sequenzenregel

$$\frac{\vdash \{A\}\, c_1\, \{B\} \qquad \vdash \{B\}\, c_2\, \{C\}}{\vdash \{A\}\, c_1; c_2\, \{C\}}$$

Induktions-Annahmen:

$$(A1)\ \models \{A\}\, c_1\, \{B\} \iff \forall I.\, \forall \sigma.\, \sigma \models^I A \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![c_1]\!]^I_C \Longrightarrow \sigma' \models^I B$$

$$(A2)\ \models \{B\}\, c_2\, \{C\} \iff \forall I.\, \forall \sigma.\, \sigma \models^I B \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![c_2]\!]^I_C \Longrightarrow \sigma' \models^I C$$

Zu zeigen:

$$\begin{aligned} \models \{A\}\, c_1; c_2\, \{C\} &\iff \forall I.\, \forall \sigma.\, \sigma \models^I A \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![c_1; c_2]\!]^I_C \Longrightarrow \sigma' \models^I C \\ (\sigma, \sigma') \in [\![c_1; c_2]\!]^I_C &\iff (\sigma, \sigma') \in [\![c_1]\!]^I_C \circ [\![c_2]\!]^I_C \\ &\iff \exists \rho.\, (\sigma, \rho) \in [\![c_1]\!]^I_C \wedge (\rho, \sigma') \in [\![c_2]\!]^I_C \end{aligned}$$

Aus $\sigma \models^I A$ und $\exists \rho.\, (\sigma, \rho) \in [\![c_1]\!]^I_C$ folgt mit (A1) $\rho \models^I B$

Aus $\rho \models^I B$ und $\exists \sigma'.\, (\rho, \sigma') \in [\![c_2]\!]^I_C$ folgt mit (A2) $\sigma' \models^I C$ □

Korrektheit der If-Then-Else-Regel

$$\frac{\vdash \{A \wedge b\}\, c_1\, \{B\} \qquad \vdash \{A \wedge \neg b\}\, c_2\, \{B\}}{\vdash \{A\}\ \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2\, \{B\}}$$

Induktions-Annahmen:

$$(A1)\ \models \{A \wedge b\}\, c_1\, \{B\} \iff \forall I.\, \forall \sigma.\, \sigma \models^I (A \wedge b) \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![c_1]\!]^I_C \Longrightarrow \sigma' \models^I B$$
$$\iff \forall I.\, \forall \sigma.\, (\sigma, \mathit{true}) \in [\![A \wedge b]\!]^I_B \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![c_1]\!]^I_C \Longrightarrow \sigma' \models^I B$$

$$(A2)\ \models \{A \wedge \neg b\}\, c_2\, \{B\} \iff \forall I.\, \forall \sigma.\, \sigma \models^I (A \wedge \neg b) \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![c_2]\!]^I_C \Longrightarrow \sigma' \models^I B$$
$$\iff \forall I.\, \forall \sigma.\, (\sigma, \mathit{true}) \in [\![(A \wedge \neg b)]\!]^I_B \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![c_2]\!]^I_C \Longrightarrow \sigma' \models^I B$$

Zu zeigen:

$$\models \{A\}\ \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2\, \{B\}$$
$$\Longleftrightarrow \forall I.\, \forall \sigma.\, \sigma \models^I A \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![\textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2]\!]_C \Longrightarrow \sigma' \models^I B$$

Korrektheit der If-Then-Else-Regel

Zu zeigen:

$$\models \{A\}\ \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2\, \{B\}$$
$$\Longleftrightarrow \forall I.\, \forall \sigma.\, \sigma \models^I A \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![\textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2]\!]_C \Longrightarrow \sigma' \models^I B$$
$$\Longleftrightarrow \forall I.\, \forall \sigma.\, (\sigma, \mathit{true}) \in [\![A]\!]^I_A \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![\textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2]\!]_C \Longrightarrow \sigma' \models^I B$$

Folgt aus Definition

$$[\![\textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2]\!]^I_C = \{(\sigma, \sigma') \mid (\sigma, \mathit{true}) \in [\![b]\!]^I_B \wedge (\sigma, \sigma') \in [\![c_1]\!]^I_C\}$$
$$\cup\, \{(\sigma, \sigma') \mid (\sigma, \mathit{false}) \in [\![b]\!]^I_B \wedge (\sigma, \sigma') \in [\![c_2]\!]^I_C\}$$

mit (A1) und (A2)

$$(A1)\ \models \{A \wedge b\}\, c_1\, \{B\} \iff \forall I.\, \forall \sigma.\, (\sigma, \mathit{true}) \in [\![A \wedge b]\!]^I_B \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![c_1]\!]^I_C \Longrightarrow \sigma' \models^I B$$
$$(A2)\ \models \{A \wedge \neg b\}\, c_2\, \{B\} \iff \forall I.\, \forall \sigma.\, (\sigma, \mathit{true}) \in [\![(A \wedge \neg b)]\!]^I_B \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![c_2]\!]^I_C \Longrightarrow \sigma' \models^I B$$

Vollständigkeit der Floyd-Hoare-Logik

Floyd-Hoare-Logik ist vollständig modulo weakening.
Wenn $\models \{P\}\, c\, \{Q\}$, dann $\vdash \{P\}\, c\, \{Q\}$ bis auf die Bedingungen der Weakening-Regel.

- Beweis durch Konstruktion einer schwächsten Vorbedingung $\mathrm{wp}(c, Q)$.
  - Problemfall: while-Schleife.

Vollständigkeitsbeweis

- Zu Zeigen:

$$\forall c \in \textbf{Stmt}.\, \forall Q \in \textbf{Assn}.\, \exists\, \mathrm{wp}(c, Q).\, \forall I.\, \forall \sigma.\, \sigma \models^I \mathrm{wp}(c, Q) \Rightarrow [\![c]\!]_C \sigma \models^I Q$$

- Beweis per struktureller Induktion über c:
  - $c \equiv \{\}$: Wähle $\mathrm{wp}(\{\}, Q) := Q$
  - $c \equiv X = a$: wähle $\mathrm{wp}(X = a, Q) := Q[a/x]$
  - $c \equiv c_0; c_1$: Wähle $\mathrm{wp}(c_0; c_1, Q) := \mathrm{wp}(c_0, \mathrm{wp}(c_1, Q))$
  - $c \equiv \textbf{if}\ b\ c_0\ \textbf{else}\ c_1$: Wähle $\mathrm{wp}(c, Q) := (b \wedge \mathrm{wp}(c_0, Q)) \vee (\neg b \wedge \mathrm{wp}(c_1, Q))$
  - $c \equiv \textbf{while}\ (b)\ c_0$: ??

Vollständigkeitsbeweis: while

- $c \equiv \textbf{while}\ (b)\ c_0$:
  Wie müssen eine Formel finden ($\mathrm{wp}(\textbf{while}\ (b)\ c_0, Q)$) die alle σ charakterisiert, so dass
  $\sigma \models^I \mathrm{wp}(\textbf{while}\ (b)\ c_0, Q)$
  $\longleftrightarrow \forall k \geq 0 \forall \sigma_0, \ldots, \sigma_k.\quad \sigma = \sigma_0$
  $\forall 0 \leq i < k.(\sigma_i \models^I b \wedge \underbrace{[\![c_0]\!]_C \sigma_i = \sigma_{i+1}}_{c_0\ \underline{\text{terminiert}}\ \text{auf}\ \sigma_i\ \text{in}\ \sigma_{i+1}}$
  $\sigma_k \models^I b \vee Q$
- Es gibt so eine Formel ausdrückbar in **Assn**, die im Wesentlichen darauf aufbaut, dass
  1. jede Sequenz an Werten, die die Programmvariablen $\overline{X}$ in jeder Iteration $(\sigma_0, \ldots)$ beim Test b haben, mittels einer Formel beschrieben werden kann (β-Prädikat)
  2. $\mathrm{wp}(c_0, \overline{X} = \overline{\sigma_{i+1}(X)})$ die Formel beschreibt, was vor c_0 gelten muss, damit hinterher die Programmvariablen $\overline{X}$ die Werte $\overline{\sigma_{i+1}(X)}$ haben
  3. $\neg \mathrm{wp}(c_0, \mathit{false})$ beschreibt was vor c_0 nicht gelten darf, damit c_0 nicht terminiert.

Vollständigkeit der Floyd-Hoare-Logik

Floyd-Hoare-Logik ist vollständig modulo weakening.
Wenn $\models \{P\}\, c\, \{Q\}$, dann $\vdash \{P\}\, c\, \{Q\}$ bis auf die Bedingungen der Weakening-Regel.

- Beweis durch Konstruktion einer schwächsten Vorbedingung $\mathrm{wp}(c, Q)$.
  - Problemfall: while-Schleife.
- Vollständigkeit (relativ):

$$\models \{P\}\, c\, \{Q\} \Leftrightarrow P \Rightarrow \mathrm{wp}(c, Q)$$

- Wenn wir eine gültige Zusicherung nicht herleiten können, liegt das nur daran, dass wir eine Beweisverpflichtung nicht beweisen können.
- Logik erster Stufe ist unvollständig, also **können** wir gar nicht besser werden.

Zusammenfassung

- Die Floyd-Hoare-Logik ist **korrekt**, wir können nur gültige Zusicherungen herleiten.
- Beweis durch Struktur über der Ableitung: wir beweisen jede Regel als korrekt.
- Die Floyd-Hoare-Logik ist **vollständig** bis auf das Weakening.

Korrekte Software: Grundlagen und Methoden
Vorlesung 8 vom 07.06.2022
Strukturierte Datentypen: Strukturen und Felder

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2022

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Motivation

- Immer nur ganze Zahlen ist doch etwas langweilig.
- Weitere Basisdatentypen von C (Felder, Zeichenketten, Strukturen)
- Noch rein funktional, keine Referenzen
- Nicht behandelt, aber nur syntaktischer Zucker: **enum**
- Prinzipiell: keine **union**

Arrays

- Beispiele:

```
int six[6] = {1,2,3,4,5,6};
int a[3][2];
int b[][] = { {1, 0},
              {3, 7},
              {5, 8} }; /* Ergibt Array [3][2] */
```

  - b [2][1] liefert 8, b [1][0] liefert 3
- Index startet mit 0, *row-major order*
- In C0: Felder als echte Objekte (in C: Felder ≅ Zeiger)
- Allgemeine Form:

```
typ name[groesse1][groesse2]...[groesseN] =
    { ... }
```

  - Alle Felder haben **feste Größe**.

Zeichenketten

- Zeichenketten sind in C (und C0) Felder von **char**, die mit einer Null abgeschlossen werden.
- Beispiel:

```
char hallo[6] = {'h', 'a', 'l', 'l', 'o', '\0' }
```

- Nützlicher syntaktischer Zucker:

```
char hallo[] = "hallo";
```

- Auswertung: hallo [4] liefert o

Strukturen

- Strukturen haben einen *structure tag* (optional) und Felder:

```
struct Vorlesung {
  char dozenten[2][30];
  char titel[30];
  int cp;
} ksgm;

struct Vorlesung pi3;
```

- Zugriff auf Felder über Selektoren:

```
int i = 0;
char name1[] = "Serge Autexier";
while (i < strlen(name1)) {
  ksgm.dozenten[0][i] = name1[i];
  i = i + 1;
}
```

- Rekursive Strukturen nur über Zeiger erlaubt (kommt noch)

C0: Erweiterte Ausdrücke

- **Lexp** beschreibt L-Werte (l-values), abstrakte Speicheradressen
- Neuer Basisdatentyp **C** für Zeichen
- Erweiterte Grammatik:

Lexp $l ::= \mathbf{Idt} \mid l[a] \mid l.\mathbf{Idt}$

Aexp $a ::= \mathbf{Z} \mid \mathbf{C} \mid \mathbf{Lexp} \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2 \mid a_1/a_2$

Bexp $b ::= \mathbf{1} \mid \mathbf{0} \mid a_1 == a_2 \mid a_1 < a_2 \mid !\, b \mid b_1 \,\&\&\, b_2 \mid b_1 \,||\, b_2$

Exp $e := \mathbf{Aexp} \mid \mathbf{Bexp}$

Werte und Zustände

- Zustände bilden **strukturierte** Adressen auf Werte (wie vorher) ab.

Systemzustände

- **Locations:** $\mathbf{Loc} ::= \mathbf{Idt} \mid \mathbf{Loc}[\mathbb{Z}] \mid \mathbf{Loc}.\mathbf{Idt}$
- Werte: $\mathbf{V} = \mathbb{Z} \uplus \mathbf{C}$
- Zustände: $\Sigma \stackrel{def}{=} \mathbf{Loc} \rightharpoonup \mathbf{V}$

- Wir betrachten nur Zugriffe vom Typ **Z** oder **C** (**elementare Typen**)
- Nützliche Abstraktion des tatsächlichen C-Speichermodells

Beispiel

Programm

```
struct A {
 int c[2];
 struct B {
  char name[20];
 } b;
};

struct A x[] = {
 {{1,2},
  {{'n','a','m','e','1','\0'}}
 },
 {{3,4},
  {{'n','a','m','e','2','\0'}}
 }
};
```

Zustand

$x[0].c[0] \mapsto 1$	$x[1].c[0] \mapsto 3$
$x[0].c[1] \mapsto 2$	$x[1].c[1] \mapsto 4$
$x[0].b.name[0] \mapsto 'n'$	$x[1].b.name[0] \mapsto 'n'$
$x[0].b.name[1] \mapsto 'a'$	$x[1].b.name[1] \mapsto 'a'$
$x[0].b.name[2] \mapsto 'm'$	$x[1].b.name[2] \mapsto 'm'$
$x[0].b.name[3] \mapsto 'e'$	$x[1].b.name[3] \mapsto 'e'$
$x[0].b.name[4] \mapsto '1'$	$x[1].b.name[4] \mapsto '2'$
$x[0].b.name[5] \mapsto '\backslash 0'$	$x[1].b.name[5] \mapsto '\backslash 0'$

Operationale Semantik: L-Werte

- **Lexp** m wertet zu **Loc** l aus: $\langle m, \sigma\rangle \to_{Lexp} l$

$$\frac{x \in \textbf{Idt}}{\langle x, \sigma\rangle \to_{Lexp} x}$$

$$\frac{\langle m, \sigma\rangle \to_{Lexp} l \qquad \langle a, \sigma\rangle \to_{Aexp} i}{\langle m[a], \sigma\rangle \to_{Lexp} l[i]} \qquad \frac{\langle m, \sigma\rangle \to_{Lexp} l}{\langle m.i, \sigma\rangle \to_{Lexp} l.i}$$

Operationale Semantik: Ausdrücke

- Ein L-Wert als Ausdruck wird ausgewertet, indem er ausgelesen wird:

$$\frac{\langle m, \sigma\rangle \to_{Lexp} l \qquad l \in Dom(\sigma)}{\langle m, \sigma\rangle \to_{Aexp} \sigma(l)}$$

- Auswertung für **C**:

$$\frac{}{\langle c :: \mathbf{C}, \sigma\rangle \to_{Aexp} \mathrm{Ord(c)}}$$

wobei Ord : **C** $\to$ **Z** eine bijektive Funktion ist, die jedem Character eine Ordinalzahl zuweist (zum Beispiel ASCII Wert).

Operationale Semantik: Zuweisungen

- Zuweisungen sind nur definiert für elementare Typen:

$$\frac{\langle m :: \tau_1, \sigma\rangle \to_{Lexp} l \qquad \langle e :: \tau_2, \sigma\rangle \to v \qquad \tau_1 = \tau_2 \text{ elementarer Typ}}{\langle m = e, \sigma\rangle \to_{Stmt} \sigma[l \mapsto v]}$$

- Die restlichen Regeln bleiben

Denotationale Semantik

- Denotation für **Lexp**:

$$[\![-]\!]_{\mathcal{L}} : \textbf{Lexp} \to (\Sigma \rightharpoonup \textbf{Loc})$$

$$[\![x]\!]_{\mathcal{L}} = \{(\sigma, x) \mid \sigma \in \Sigma\}$$
$$[\![m[a]]\!]_{\mathcal{L}} = \{(\sigma, l[i]) \mid (\sigma, l) \in [\![m]\!]_{\mathcal{L}}, (\sigma, i) \in [\![a]\!]_{\mathcal{A}}\}$$
$$[\![m.i]\!]_{\mathcal{L}} = \{(\sigma, l.i) \mid (\sigma, l) \in [\![m]\!]_{\mathcal{L}}\}$$

- Denotation für **Characters** $c \in \mathbf{C}$:

$$[\![c]\!]_{\mathcal{A}} = \{(\sigma, \mathrm{Ord}(c)) | \sigma \in \Sigma\}$$

- Denotation für **Zuweisungen**:

$$[\![m = e]\!]_{\mathcal{C}} = \{(\sigma, \sigma[l \mapsto v]) \mid (\sigma, l) \in [\![m]\!]_{\mathcal{L}}, (\sigma, v) \in [\![e]\!]_{\mathcal{A}}\}$$

Floyd-Hoare-Kalkül

- Die Regeln des Floyd-Hoare-Kalküls berechnen geltende Zusicherungen
- Nötige Änderung: Substitution in Zusicherungen wird zur Ersetzung von **Lexp**-Ausdrücken

$$\frac{}{\vdash \{P[e/x]\}\, x = e\, \{P\}}$$

  - Jetzt werden **Lexp** ersetzt, keine **Idt**

$$\frac{}{\vdash \{P[e/l]\}\, l = e\, \{P\}}$$

  Anmerkung: l und e enthalten **keine** logischen Variablen.
- Gleichheit und Ungleichheit von **Lexp** nicht immer entscheidbar
- Problem: Feldzugriffe

Von der Substitution zur Ersetzung

$$\textbf{Assn}\ b ::= \mathit{true} \mid \mathit{false} \mid a_1 = a_2 \mid a_1 \leq a_2 \mid p(e_1, \ldots, e_n) \mid \neg b \mid b_1 \wedge b_2 \mid b_1 \vee b_2 \mid b_1 \longrightarrow b_2 \mid \forall v.\, b \mid \exists v.\, b \qquad \textbf{(Literale)}$$

$$\mathit{true}[e/l] := \mathit{true}$$
$$\mathit{false}[e/l] := \mathit{false}$$
$$(a_1 = a_2)[e/l] := (a_1[e/l] = a_2[e/l])$$
$$(b_1 \wedge b_2)[e/l] := (b_1[t/x] \wedge b_2[e/l])$$
$$(\forall v.\, b)[e/l] := \forall v.\, (b[e/l])$$

$$n[e/l] := n \qquad (n \in \mathbf{Z} \uplus \mathbf{C})$$

$$l'[e/l] := l'[e/l] \begin{cases} e & \text{falls } l = l' \\ l' & \text{sonst} \end{cases} \qquad (l' \in \textbf{Lexp})$$

$$(a_1 + a_2)[e/l] := a_1[e/l] + a_2[e/l]$$
$$\ldots$$

Beispiel Problemsituationen:
$(c[i].x[0])[5/c[1].x[0]] = ?$
$(c[1].x[0])[8/c[1].x[j]] = ?$
$(c[i].x[0])[8/c[1].x[j]] = ?$

Beispiel

```
int a[3];
// {true}
// {3 = 3}
a[2] = 3;
// {a[2] = 3}
// {4 · a[2] = 12}
a[1] = 4;
// {a[1] · a[2] = 12}
// {5 · a[1] · a[2] = 60}
a[0] = 5;
// {a[0] · a[1] · a[2] = 60}
```

$$\frac{}{\vdash \{P[e/l]\}\, l = e\, \{P\}}$$

Beispiel: Problem

```
int a[3];
int i;
// {0 ≤ i < 2}
// ↯
// {i ≠ 1}
a[0] = 3;
// {i ≠ 1}
// {i ≠ 1 ∧ 7 = 7)}
a[1] = 7;
// {i ≠ 1 ∧ a[1] = 7}
a[2] = 9;
// {i ≠ 1 ∧ a[1] = 7}
// {(i = 1 ∧ −1 = 7) ∨ (i ≠ 1 ∧ a[1] = 7)}{a[1] = 7}
a[i] = −1;
// {a[1] = 7}
```

$$\overline{\vdash \{P[e/l]\}\ l = e\ \{P\}}$$

Arbeitsblatt 8.1: Jetzt seid ihr dran

Annotiert die beiden folgenden Programme:

```
int a[2];
int b[2];
// {0 ≤ n ∧ 0 ≤ m ∧ n ≤ m}
a[0] = m;
//
b[0] = a[0] − n;
//
b[1] = a[0] + n
//
a[1] = b[0] ∗ b[1];
// {a[1] = m² − n²}
```

```
int a[3];
int i;
// {0 ≤ n}
i = 2;
//
a[i] = 3;
//
a[0] = n;
//
a[2] = a[2] ∗ a[0];
// {a[2] = 3 ∗ n}
```


Erstes Beispiel: Ein Feld initialisieren

```
1  // {0 ≤ n}
2  // {∀j.0 ≤ j < 0 ⟶ a[j] = j ∧ 0 ≤ n}
3  i= 0;
4  // {∀j.0 ≤ j < i ⟶ a[j] = j ∧ i ≤ n}
5  while (i< n) {
6    // {∀j.0 ≤ j < i ⟶ a[j] = j ∧ i ≤ n ∧ i < n}
7    // {∀j.0 ≤ j < i ⟶ a[j] = j ∧ i + 1 ≤ n}
8    // {∀j.0 ≤ j < i ⟶ ((i = j ∧ i = j) ∨ (j ≠ i ∧ a[j] = j))
9    //     ∧((i = i ∧ i = i) ∨ (i ≠ i ∧ a[i] = i)) ∧ i + 1 ≤ n}
10   // {∀j.0 ≤ j < i + 1 ⟶ ((i = j ∧ i = j) ∨ (j ≠ i ∧ a[j] = j))
11   //     ∧ i + 1 ≤ n}
12   a[i]= i;
13   // {(∀j.0 ≤ j < i + 1 ⟶ a[j] = j) ∧ i + 1 ≤ n}
14   i= i+1;
15   // {(∀j.0 ≤ j < i ⟶ a[j] = j) ∧ i ≤ n}
16   }
17 // {(∀j.0 ≤ j < i ⟶ a[j] = j) ∧ i ≤ n ∧ i ≥ n}
18 // {∀j.0 ≤ j < n ⟶ a[j] = j}
```

- Wichtiges Theorem:

$$(\forall j.\, 0 \le j < n \longrightarrow P[j]) \wedge P[n] \Longrightarrow \forall j.\, 0 \le j < n+1 \longrightarrow P[j]$$

Beispiel: Suche nach dem maximalen Element

```
1  // {0 < n}
2  // {(∀j.0 ≤ j < 0 ⟶ a[j] ≤ a[0]) ∧ 0 ≤ 0 ∧ 0 ≤ 0 < n}
3  i= 0;
4  // {(∀j.0 ≤ j < i ⟶ a[j] ≤ a[0]) ∧ 0 ≤ i ∧ 0 ≤ 0 < n}
5  r= 0;
6  // {(∀j.0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ i ∧ 0 ≤ r < n}
7  while (i< n) {
8    // {(∀j.0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ i < n ∧ 0 ≤ r < n}
9    // {(∀j.0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ i + 1 ≤ n ∧ 0 ≤ r < n}
10   if (a[r] < a[i]) {
11     // {(∀j.0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ i + 1 ≤ n ∧ 0 ≤ r < n ∧ a[r] < a[i]}
12     // {(∀j.0 ≤ j < i ⟶ a[j] ≤ a[i]) ∧ a[i] ≤ a[i] ∧ 0 ≤ i + 1 ≤ n ∧ 0 ≤ i < n}
13     // {(∀j.0 ≤ j < i + 1 ⟶ a[j] ≤ a[i]) ∧ 0 ≤ i + 1 ≤ n ∧ 0 ≤ i < n}
14     r= i;
15     // {(∀j.0 ≤ j < i + 1 ⟶ a[j] ≤ a[r]) ∧ 0 ≤ i + 1 ≤ n ∧ 0 ≤ r < n}
16     }
17   else {
18     // {(∀j.0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ i + 1 ≤ n ∧ 0 ≤ r < n ∧ ¬(a[r] < a[i])}
19     // {(∀j.0 ≤ j < i + 1 ⟶ a[j] ≤ a[r]) ∧ 0 ≤ i + 1 ≤ n ∧ 0 ≤ r < n}
20     }
21   // {(∀j.0 ≤ j < i + 1 ⟶ a[j] ≤ a[r]) ∧ 0 ≤ i + 1 ≤ n ∧ 0 ≤ r < n}
22   i= i+1;
23   // {(∀j.0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ i ≤ n ∧ 0 ≤ r < n}
24 }
25 // {(∀j.0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ i ≤ n ∧ 0 ≤ r < n ∧ n ≤ i}
26 // {(∀j.0 ≤ j < n ⟶ a[j] ≤ a[r]) ∧ 0 ≤ r < n}
```


Vorgehensweise

```
1  // {I}
2  while (b) {
3    // {I ∧ b}
4    c
5    // {I}
6  }
7  // {I ∧ ¬b}
8  // {Φ}
```

1. Finde/rate/formuliere Invariante I
2. Beweise $(I \wedge \neg b) \longrightarrow \Phi$
3. Zeige mittels Floyd-Hoare-Regeln, dass Invariante durch Schleifenrumpf `c` erhalten bleibt
4. Setze Beweis mit Floyd-Hoare Regeln vor der Schleife fort

Längeres Beispiel: Suche nach einem Null-Element

```
1  i= 0;
2  r= −1;
3  while (i< n) {
4    if (a[i] == 0) {
5      r= i;
6    }
7    else {
8    }
9    i= i+1;
10 }
11 // {r ≠ −1 ⟶ 0 ≤ r < n ∧ a[r] = 0}
```

Merkt euch folgende korrekten logischen Umformungen:

- $(F \wedge H) \vee (G \wedge H)$ ist äquivalent zu $(F \vee G) \wedge H$
- $\neg F \vee G$ ist äquivalent zu $F \longrightarrow G$

Längeres Beispiel: Suche nach einem Null-Element

```
1  // {0 ≤ n}
2  // {(−1 ≠ −1 ⟶ 0 ≤ −1 < 0 ∧ a[−1] = 0) ∧ 0 ≤ 0 ≤ n}
3  i= 0;
4  // {(−1 ≠ −1 ⟶ 0 ≤ −1 < i ∧ a[−1] = 0) ∧ 0 ≤ i ≤ n}
5  r= −1;
6  // {(r ≠ −1 ⟶ 0 ≤ r < i ∧ a[r] = 0) ∧ 0 ≤ i ≤ n}
7  while (i< n) {
8    // {(r ≠ −1 ⟶ 0 ≤ r < i ∧ a[r] = 0) ∧ 0 ≤ i ≤ n ∧ i < n}
9    // {(r ≠ −1 ⟶ 0 ≤ r < i ∧ a[r] = 0) ∧ 0 ≤ i + 1 ≤ n}
10   if (a[i] == 0) {
11     // {(r ≠ −1 ⟶ 0 ≤ r < i ∧ a[r] = 0) ∧ 0 ≤ i + 1 ≤ n ∧ a[i] = 0}
12   // {0 ≤ i < i + 1 ∧ a[i] = 0 ∧ 0 ≤ i + 1 ≤ n ∧ a[i] = 0}   (B(i)∧C; ¬A(i); C; B(i); C)
13   // {(i = −1 ∧ 0 ≤ i + 1 ≤ n ∧ a[i] = 0) ∨ (0 ≤ i < i + 1 ∧ a[i] = 0 ∧ 0 ≤ i + 1 ≤ n ∧ a[i] = 0)}
14   // {(i = −1 ∨ (0 ≤ i < i + 1 ∧ a[i] = 0)) ∧ 0 ≤ i + 1 ≤ n ∧ a[i] = 0}
15   // {(i ≠ −1 ⟶ 0 ≤ i < i + 1 ∧ a[i] = 0) ∧ 0 ≤ i + 1 ≤ n ∧ a[i] = 0}   (A(i); B(i); C)
16     r= i;
17     // {(r ≠ −1 ⟶ 0 ≤ r < i + 1 ∧ a[r] = 0) ∧ 0 ≤ i + 1 ≤ n}
18     }
19   else {
20     // {(r ≠ −1 ⟶ 0 ≤ r < i + 1 ∧ a[r] = 0) ∧ 0 ≤ i + 1 ≤ n ∧ a[i] ≠ 0}
21     // {(r ≠ −1 ⟶ 0 ≤ r < i + 1 ∧ a[r] = 0) ∧ 0 ≤ i + 1 ≤ n}
22   }
23   // {(r ≠ −1 ⟶ 0 ≤ r < i + 1 ∧ a[r] = 0) ∧ 0 ≤ i + 1 ≤ n}
24   i= i+1;
25   // {(r ≠ −1 ⟶ 0 ≤ r < i ∧ a[r] = 0) ∧ 0 ≤ i ≤ n}
26 }
27 // {(r ≠ −1 ⟶ 0 ≤ r < i ∧ a[r] = 0) ∧ 0 ≤ i ≤ n ∧ ¬(i < n)}
28 // {(r ≠ −1 ⟶ 0 ≤ r < i ∧ a[r] = 0) ∧ i = n}
29 // {r ≠ −1 ⟶ 0 ≤ r < n ∧ a[r] = 0}
```


Benutzte Logische Umformungen

- Zeilen 11-12:
  - $[D \wedge C] \Rightarrow [C]$ und
  - Erweiterung von C auf $B(i) \wedge C$, weil $C \vdash B(i)$ gilt.
- $[\varphi] \Rightarrow [\psi \vee \varphi]$ in der Form

$$[(B(i) \wedge C)] \Rightarrow [(\neg A(i) \wedge C) \vee (B(i) \wedge C))]$$

- DeMorgan:

$$[(\neg A(i) \wedge C) \vee (B(i) \wedge C))] \Rightarrow [(\neg A(i) \vee B(i)) \wedge C]$$

- Klassische Implikation:

$$[\neg U \vee V] \Leftrightarrow [U \Rightarrow V]$$

Längeres Beispiel: Suche nach einem Null-Element

```
10  /** { 0 ≤ n } */
11  /** { 0 ≤ 0 ≤ n } */
12  i= 0;
13  /** { 0 ≤ i ≤ n } */
14  /** { (−1 ≠ −1 ⟶ 0 ≤ −1< i ∧ a[−1] == 0) ∧ 0 ≤ i ≤ n } */
15  r= −1;
16  /** { (r ≠ −1 ⟶ 0 ≤ r< i ∧ a[r] == 0) ∧ 0 ≤ i ≤ n } */
17  while (i< n) {
18    /** { (r ≠ −1 ⟶ 0 ≤ r< i ∧ a[r] == 0) ∧ 0 ≤ i ≤ n ∧ i < n } */
19    /** { (r ≠ −1 ⟶ 0 ≤ r < i ∧ a[r] == 0) ∧ 0 ≤ i+1 ≤ n } */
20    if (a[i] == 0) {
21      /** { (r ≠ −1 ⟶ 0 ≤ r < i ∧ a[r] == 0) ∧ 0 ≤ i+1 ≤ n ∧ a[i] == 0 } */
22      /** { 0 ≤ i+1 ≤ n ∧ a[i] == 0 } */
23      /** { (i ≠ −1 ⟶ 0 ≤ i< i+1 ∧ a[i] == 0) ∧ 0≤ i+1≤ n } */
24      r= i;
25      /** { (r ≠ −1 ⟶ 0 ≤ r< i+1 ∧ a[r] == 0) ∧ 0≤ i+1≤ n } */
26      }
27    else {
28       /** { (r ≠ −1 ⟶ 0 ≤ r< i ∧ a[r] == 0) ∧ 0 ≤ i+1 ≤ n ∧ a[i] ≠ 0 } */
29      /** { (r ≠ −1 ⟶ 0 ≤ r< i+1 ∧ a[r] == 0) ∧ 0 ≤ i+1 ≤ n } */
30      }
31    /** { (r ≠ −1 ⟶ 0 ≤ r< i+1 ∧ a[r] == 0) ∧ 0 ≤ i+1 ≤ n } */
32    i= i+1;
33    /** { (r ≠ −1 ⟶ 0 ≤ r< i ∧ a[r] == 0) ∧ 0 ≤ i ≤ n } */
34    }
35  /** { (r ≠ −1 ⟶ 0 ≤ r< i ∧ a[r] == 0) ∧ 0 ≤ i ≤ n ∧ ¬(i < n) } */
36  /** { (r ≠ −1 ⟶ 0 ≤ r< i ∧ a[r] == 0) ∧ 0 ≤ i ≤ n ∧ i ≥ n } */
37  /** { (r ≠ −1 ⟶ 0 ≤ r< i ∧ a[r] == 0) ∧ i == n } */
38  /** { r ≠ −1 ⟶ 0 ≤ r< n ∧ a[r] == 0 } */
```


Allgemeine Regel bei Ersetzungen?

Wie sieht nun die allgemeine Regel aus für

$$\overline{\vdash \{P[e/l]\}\ l = e\,\{P\}}$$

```
int a[3];
int i;
a[0] = 3;
a[1] = 7;
a[2] = 9;
a[a[2]−a[1]] = −1;
// {a[2] = −1}
```

```
int a[3];
int i;
i = 8;
a[0] = 3;
a[1] = i;
a[2] = 9;
a[a[2]−a[1]] = −1;
// {a[1] = −1}
```


Allgemeine Regel bei Ersetzungen (Nur Arrays)

Wie sieht nun die allgemeine Regel aus für

$$\overline{\vdash \{P[e/l]\}\ l = e\,\{P\}}$$

1. Wenn l Programmvariable ist, wie gewohnt substituieren
2. Wenn $l = a[s]$:
   1. Vorkommen der Form $a[t]$ in **Literalen** $L(a[t])$ und s und t beide in $\mathbb{Z}$ oder **ldt**,
      - dann ersetze $L(a[t])$ durch $L(e)$, falls $s = t$
   2. Vorkommen der Form $a[t]$ in **Literalen** $L(a[t])$ und s oder t sind nicht aus $\mathbb{Z}$,
      - dann ersetze $L(a[t])$ durch $(t = s \wedge L(e)) \vee (t \neq s \wedge L(a[t]))$

   2.2 könnt ihr immer machen, 2.1 ist eine Optimierung

- Das ist jetzt immer noch nicht die ganz allgemeine Form, aber für unsere Belange reicht das.

Zusammenfassung

- Strukturierte Datentypen (Felder und Structs) erfordern strukturierte Adressen
- Abstraktion über „echtem“ Speichermodell
- Änderungen in der Semantik und im Floyd-Hoare-Kalkül überschaubar
- ... aber mit erheblichen Konsequenzen:
  - Substitution wird zur Ersetzung
  - Anwendung der Zuweisungsregel führt i.A. zu großen Formeln

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Korrekte Software: Grundlagen und Methoden
Vorlesung 9 vom 14.06.22
Verifikationsbedingungen

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2022

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Idee

- Hier ist ein einfaches Programm:

```
// {y = Y ∧ x = X}
z = y;
// {z = Y ∧ x = X}
y = x;
// {z = Y ∧ y = X}
x = z;
// {x = Y ∧ y = X}
```

- Wir sehen:
  1. Die Verifikation erfolgt **rückwärts** (von hinten nach vorne).
  2. Die Vorbedingung kann **berechnet** werden.
- Geht das immer?
- Was bringt uns das?

Rückwärtsanwendung der Regeln

- Zuweisungsregel kann **rückwärts** angewandt werden, weil die Nachbedingung eine offene Variable ist — P passt auf jede beliebige Nachbedingung

$$\frac{}{\vdash \{P[e/l]\}\ l = e\ \{P\}}$$

- Was ist mit den anderen Regeln?

$$\frac{}{\vdash \{A\}\ \{\}\ \{A\}} \qquad \frac{\vdash \{A \wedge b\}\ c_0\ \{B\} \qquad \vdash \{A \wedge \neg b\}\ c_1\ \{B\}}{\vdash \{A\}\ \textbf{if}\ (b)\ c_0\ \textbf{else}\ c_1\ \{B\}}$$

$$\frac{\vdash \{A\}\ c_1\ \{B\} \qquad \vdash \{B\}\ c_2\ \{C\}}{\vdash \{A\}\ c_1; c_2\ \{C\}} \qquad \frac{\vdash \{A \wedge b\}\ c\ \{A\}}{\vdash \{A\}\ \textbf{while}\ (b)\ c\ \{A \wedge \neg b\}}$$

$$\frac{A' \Longrightarrow A \qquad \vdash \{A\}\ c\ \{B\} \qquad B \Longrightarrow B'}{\vdash \{A'\}\ c\ \{B'\}}$$

Arbeitsblatt 9.1: Eine Kleine Fallunterscheidung

Berechnet die Vorbedingungen an den Stellen (A), (B), (?) für folgendes Programm:

```
// (?)
if (y == 7) {
  // (A)
  x= 3;
  //
  }
else {
  // (B)
  y= 0;
  x= 10;
  //
  }
// x+ y == 10
```


Rückwärtsanwendung: if

```
// ?
if (b) {
  // {P1}
  ...
  // {Q}
  }
else {
  // {P2}
  ...
  // {Q}
  }
// {Q}
```

$$\frac{\vdash \{A \wedge b\}\ c_0\ \{B\} \qquad \vdash \{A \wedge \neg b\}\ c_1\ \{B\}}{\vdash \{A\}\ \textbf{if}\ (b)\ c_0\ \textbf{else}\ c_1\ \{B\}}$$

Regel in der Form nicht geeignet. Besser:

$$A \stackrel{def}{=} (P_1 \wedge b) \vee (P_2 \wedge \neg b)$$
$$A \wedge b \Longrightarrow P_1 \quad (1)$$
$$A \wedge \neg b \Longrightarrow P_2 \quad (2)$$

Kombiniert mit Weakening ergibt neue Regel:

$$\frac{\dfrac{A \wedge b \Longrightarrow P_1 \quad \vdash \{P_1\}\ c_0\ \{C\}}{\vdash \{A \wedge b\}\ c_0\ \{B\}} \qquad \dfrac{A \wedge \neg b \Longrightarrow P_2 \quad \vdash \{P_2\}\ c_1\ \{C\}}{\vdash \{A \wedge \neg b\}\ c_1\ \{B\}}}{\vdash \{(P_1 \wedge b) \vee (P_2 \wedge \neg b)\}\ \textbf{if}\ (b)\ c_0\ \textbf{else}\ c_1\ \{B\}} \qquad \vdash \{(P_1 \wedge$$

Arbeitsblatt 9.2: Etwas Logik

Beweist Lemma (1) und (2) von der vorherigen Folie:

$$A = (P_1 \wedge b) \vee (P_2 \wedge \neg b)$$
$$A \wedge b \Longrightarrow P_1 \quad (1)$$
$$A \wedge \neg b \Longrightarrow P_2 \quad (2)$$

Hinweis:

- Nutzt logische Umformungen: Distributivität, Idempotenz, ...

Neue Regeln

- Wir können aus dem Hoare-Kalkül **neue Regeln** ableiten, in dem wir
  1. Existierende Regeln **instantiieren**, oder
  2. existierende Regeln **verknüpfen**.
- Wir benötigen das hier, um die Regeln des Hoare-Kalkül in eine Form zu bringen, welche die Rückwärtsrechnung ermöglicht.

Das Hinzufügen abgeleiteter Regeln ist eine **konservative Erweiterung** — es lassen sich damit nicht mehr oder weniger Hoare-Tripel $\vdash \{P\}\ c\ \{Q\}$ herleiten.

Regeln für die Rückwärtsrechnung

1. **Nachbedingung** der **Konklusion** ist von der Form $\{Q\}$ (**offene** Meta-Variable)
2. Alle **Vorbedingungen** der **Prämissen** ist von der Form $\{P_i\}$ (**unterschiedliche** P_i)
3. Alle Variablen in den Vorbedingungen der Konklusion, den Weakenings und Nachbedingungen der Prämisse sind **determiniert**[1].

Welche Regeln passen noch nicht? **while**-Regel passt noch nicht ...

[1] **Entweder** in der Nachbedingung oder dem Programmausdruck der Konklusion, **oder** den Vorbedingungen der Prämisse enthalten.

Regeln für die Rückwärtsrechnung: while

- **while**-Regel (3) wird mit Weakening zu (4):

$$\frac{\vdash \{I \wedge b\}\, c\, \{I\}}{\vdash \{I\}\ \textbf{while}\ (b)\ c\, \{I \wedge \neg b\}} \quad (3)$$

$$\frac{I \wedge b \Longrightarrow R \qquad \vdash \{R\}\, c\, \{I\} \qquad I \wedge \neg b \Longrightarrow Q}{\vdash \{I\}\ \textbf{while}\ (b)\ c\, \{Q\}} \quad (4)$$

- Implikationen $I \wedge b \Longrightarrow R$, $I \wedge \neg b \Longrightarrow Q$ werden zu **Beweisverpflichtungen**
- Bedingung I (**Invariante**) muss **vorgegeben** werden.
  - Durch **Annotation**: **while** (b) /** **inv** I */ c

Übersicht: Regeln für den Hoare-Kalkül Rückwärts

$$\frac{}{\vdash \{P[e/I]\}\, I = e\, \{P\}} \qquad \frac{}{\vdash \{A\}\, \{\}\, \{A\}} \qquad \frac{\vdash \{A\}\, c_1\, \{B\} \qquad \vdash \{B\}\, c_2\, \{C\}}{\vdash \{A\}\, c_1; c_2\, \{C\}}$$

$$\frac{\vdash \{A_0\}\, c_0\, \{B\} \quad \vdash \{A_1\}\, c_1\, \{B\}}{\vdash \{(A_0 \wedge b) \vee (A_1 \wedge \neg b)\}\ \textbf{if}\ (b)\ c_0\ \textbf{else}\ c_1\, \{B\}}$$

$$\frac{I \wedge b \Longrightarrow B \quad \vdash \{B\}\, c\, \{I\} \quad I \wedge \neg b \Longrightarrow C}{\vdash \{I\}\ \textbf{while}\ (b)\ /{*}{*}\ \textbf{inv}\ I\ {*}/\ c\, \{C\}}$$

Der Hoare-Kalkül Rückwärts

- Mit diesen Regeln können wir für ein gegebenes Programm c und eine Nachbedingung Q eine Vorbedingung P_{pre} **berechnen**.
- Was bringt uns das?
  - Um ein **Hoare-Tripel** $\vdash \{P\}\, c\, \{Q\}$ zu **beweisen**, berechnen wir wie oben die **Vorbedingung** P_{pre}.
  - Jetzt müssen wir nur noch $P \Longrightarrow P_{\text{pre}}$ und alle Weakenings aus der Berechnung von P_{pre} zeigen.
  - Damit **reduzieren** wir die **Korrektheit** auf eine Menge von (zustandsfreien) **Beweisverpflichtungen**.

Berechnung von Vorbedingungen

- Die Rückwärtsrechnung von einer gegebenen Nachbedingung entspricht der Berechnung einer Vorbedingung.
- Gegeben C0-Programm c, Prädikat Q, dann ist
  - $\text{wp}(c, Q)$ die **schwächste Vorbedingung** P so dass $\models \{P\}\, c\, \{Q\}$;
  - Prädikat P **schwächer** als P' wenn $P' \Longrightarrow P$
- Semantische Charakterisierung:

Schwächste Vorbedingung

Gegeben Zusicherung $Q \in$ **Assn** und Programm $c \in$ **Stmt**, dann

$$\models \{P\}\, c\, \{Q\} \Longleftrightarrow P \Longrightarrow \text{wp}(c, Q)$$

- Wie können wir $\text{wp}(c, Q)$ berechnen?

Annotierte Programme

- Wir helfen dem Rechner weiter und **annotieren** die Schleifeninvariante I am Programm.
- Damit berechnen wir:
  - die **approximative** schwächste Vorbedingung $\text{awp}(c, Q)$
  - zusammen mit einer Menge von **Verifikationsbedingungen** $\text{wvc}(c, Q)$
- Die Verifikationsbedingungen treten dort auf, wo die Weakening-Regel angewandt wird.
- Es gilt:

$$\bigwedge \text{wvc}(c, Q) \Longrightarrow \models \{\text{awp}(c, Q)\}\, c\, \{Q\}$$

Überblick: Approximative schwächste Vorbedingung

$$\begin{aligned}
\text{awp}(\{\},P) &\stackrel{\text{def}}{=} P \\
\text{awp}(I = e,P) &\stackrel{\text{def}}{=} P[e/I] \qquad (\textbf{Genauer}: \text{Folie 24 letzte VL}) \\
\text{awp}(c_1; c_2,P) &\stackrel{\text{def}}{=} \text{awp}(c_1, \text{awp}(c_2,P)) \\
\text{awp}(\textbf{if}\ (b)\ c_0\ \textbf{else}\ c_1,P) &\stackrel{\text{def}}{=} (b \wedge \text{awp}(c_0,P)) \vee (\neg b \wedge \text{awp}(c_1,P)) \\
\text{awp}(\textbf{while}\ (b)\ /{*}{*}\ \textbf{inv}\ i\ {*}/\ c,P) &\stackrel{\text{def}}{=} i \\
\\
\text{wvc}(\{\},P) &\stackrel{\text{def}}{=} \emptyset \\
\text{wvc}(I = e,P) &\stackrel{\text{def}}{=} \emptyset \\
\text{wvc}(c_1; c_2,P) &\stackrel{\text{def}}{=} \text{wvc}(c_1, \text{awp}(c_2,P)) \cup \text{wvc}(c_2,P) \\
\text{wvc}(\textbf{if}\ (b)\ c_0\ \textbf{else}\ c_1,P) &\stackrel{\text{def}}{=} \text{wvc}(c_0,P) \cup \text{wvc}(c_1,P) \\
\text{wvc}(\textbf{while}\ (b)\ /{*}{*}\ \textbf{inv}\ i\ {*}/\ c,P) &\stackrel{\text{def}}{=} \text{wvc}(c,i) \cup \{i \wedge b \longrightarrow \text{awp}(c,i)\} \cup \{i \wedge \neg b \longrightarrow P\} \\
\text{wvc}(\{P\}\, c\, \{Q\}) &\stackrel{\text{def}}{=} \{P \longrightarrow \text{awp}(c,Q)\} \cup \text{wvc}(c,Q)
\end{aligned}$$

Berechnung der Verifikationsbedingungen

Programmkorrektheit

- Gegeben: Annotiertes Programm c mit Vorbedingung P und Nachbedingung Q.
- Gesucht: $\text{wvc}(\{P\}\, c\, \{Q\})$

1. Rekursiv von der Nachbedigung ausgehend berechnen wir für jede Zeile des Programmes die gültige approximative Vorbedingung $\text{awp}(c, -)$.
2. Dabei notieren wir alle auftretenden Verifikationsbedingungen $\text{wvc}(c, -)$
3. Dabei werden **keine** Vereinfachungen vorgenommen.

Beispiel: das Fakultätsprogramm

- Sei F das annotierte Fakultätsprogramm:

```
1  // {0 ≤ n}
2  p= 1;
3  c= 1;
4  while (c <= n) //** inv {p = (c − 1)! ∧ c − 1 ≤ n} */
5  { p = p * c;
6    c = c + 1;
7    }
8  // {p = n!}
```

- Berechnung der Verifikationsbedingungen zur Nachbedingung wvc$(F, p = n!)$

Notation für Verifikationsbedingungen

AWP wird am Programm annotiert:

```
1  // {0 ≤ n}
2  // {1 = (1 − 1)! ∧ 1 − 1 ≤ n}
3  p= 1;
4  // {p = (1 − 1)! ∧ 1 − 1 ≤ n}
5  c= 1;
6  // {p = (c − 1)! ∧ c − 1 ≤ n}
7  while (c <= n)
8    /** inv p= (c−1)! ∧ c−1 ≤ n */ {
9    // {p · c = ((c + 1) − 1)! ∧ (c + 1) − 1 ≤ n}
10   p = p * c;
11   // {p = ((c + 1) − 1)! ∧ (c + 1) − 1 ≤ n}
12   c = c + 1;
13   // {p = (c − 1)! ∧ c − 1 ≤ n}
14   }
15 // {p = n!}
```

WVC wird daneben notiert:

1	$p = (c-1)! \wedge c - 1 \leq n \wedge \neg(c \leq n) \longrightarrow p = n!$
2	$p = (c-1)! \wedge c - 1 \leq n \wedge c \leq n \longrightarrow p \cdot c = ((c+1)-1)! \wedge (c+1) - 1 \leq n$
3	$0 \leq n \longrightarrow 1 = (1-1)! \wedge (1-1) \leq n$

Vereinfachung von Verifikationsbedingungen

Wir nehmen folgende **strukturelle Vereinfachungen** vor:

1. Konjunktionen in der Konklusion werden zu einzelnen Verifikationsbedingungen
   - Bsp: $A_1 \wedge A_2 \wedge A_3 \longrightarrow P \wedge Q \rightsquigarrow A_1 \wedge A_2 \wedge A_3 \longrightarrow P, A_1 \wedge A_2 \wedge A_3 \longrightarrow Q$
2. Auswertung konstanter arithmetischer Ausdrücke, einfache arithmetische Gesetze
   - Bsp. $(x+1) - 1 \rightsquigarrow x$, $1 - 1 \rightsquigarrow 0$
3. Normalisierung der Relationen (zu $<, \leq, =, \neq$) und Vereinfachung
   - Bsp: $\neg(x \leq y) \rightsquigarrow x > y \rightsquigarrow y < x$, $x \leq x \rightsquigarrow$ *true*, $4 \leq 5 \rightsquigarrow$ *true*
4. Alle Bedingungen mit einer Prämisse *false* oder einer Konklusion *true* sind trivial erfüllt.

Vereinfachung am Beispiel

- 1: $p = (c-1)! \wedge c - 1 \leq n \wedge \neg(c \leq n) \longrightarrow p = n!$
  $\rightsquigarrow p = (c-1)! \wedge c - 1 \leq n \wedge n < c \longrightarrow p = n!$
- 2: $p = (c-1)! \wedge c - 1 \leq n \wedge c \leq n \longrightarrow p \cdot c = ((c+1)-1)! \wedge (c+1) - 1 \leq n$
  $\rightsquigarrow$ $p = (c-1)! \wedge c - 1 \leq n \wedge c \leq n \longrightarrow p \cdot c = c!$
  $p = (c-1)! \wedge c - 1 \leq n \wedge c \leq n \longrightarrow c \leq n \rightsquigarrow$ *true*
- 3: $0 \leq n \longrightarrow 1 = (1-1)! \wedge (1-1) \leq n$
  $\rightsquigarrow$ $0 \leq n \longrightarrow 1 = 0!$
  $0 \leq n \longrightarrow 0 \leq n \rightsquigarrow$ *true*

Es bleibt zu zeigen:

- 1: $p = (c-1)! \wedge c - 1 \leq n \wedge n < c \longrightarrow p = n!$
  Aus $n < c$ folgt $n \geq c - 1$, also $c - 1 = n$, und mit $p = (c-1)!$ folgt die Behauptung.
- 2: $p = (c-1)! \wedge c - 1 \leq n \wedge c \leq n \longrightarrow p \cdot c = c!$
  Aus $p = (c-1)!$ folgt $p \cdot c = c \cdot (c-1)!$, und mit $c \cdot (c-1)! = c!$ folgt die Behauptung.
- 3: $1 = 0!$ folgt direkt aus der Definition der Fakultät.

Arbeitsblatt 9.3: Da summt was...

```
1  // {0 ≤ n ∧ n = N}
2  p= 0;
3  while (n>0) //** inv p= sum(n+1,N); */
4  { p = p + n;
5    n = n − 1;
6    }
7  // {p = sum(1, N)}
```

1. Berechnet zuerst die **unvereinfachten** VCs (dafür sind die AWPs nötig)
2. Danach vereinfacht die VCs **schematisch** wie oben beschrieben.
3. Welche VCs sind beweisbar?

Dabei gilt: $sum(i,j) = \begin{cases} 0 & i > j \\ i + sum(i+1, j) & i \leq j \end{cases}$

Weiteres Beispiel: Maximales Element

```
1  // {0 < n}
2  i= 0;
3  r= 0;
4  while (i< n) //** inv {(∀j. 0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ r < n ∧ 0 ≤ i ≤ n} */
5  { if (a[r] < a[i]) {
6      r= i;
7    }
8    else {
9    }
10   i= i+1;
11   }
12 // {(∀j. 0 ≤ j < n ⟶ a[j] ≤ a[r]) ∧ 0 ≤ r < n}
```


Maximales Element (Schleifenrumpf)

```
1  while (i< n)
2    /** inv {(∀j. 0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ r < n ∧ 0 ≤ i ≤ n} */
3  {
4    // {a[r] < a[i] ∧ φ(i+1, i) ∨ (¬(a[r] < a[i]) ∧ φ(i+1, r))}
5    if (a[r] < a[i]) {
6      // {φ(i+1, i)}
7      r= i;
8      // {φ(i+1, r)}
9      }
10   else {
11     // {φ(i+1, r)}
12   }
13   // {φ(i+1, r)}
14   i= i+1;
15   // {φ(i, r)}
16   }
17 // {(∀j. 0 ≤ j ⟷ a[j] ≤ a[r]) ∧ 0 ≤ r < n}
```

VC:

1	$\varphi(i,r) \wedge \neg(i < n) \longrightarrow$ $(\forall j.\, 0 \leq j < n \longrightarrow a[j] \leq a[r])$ $\wedge$ $0 \leq r < n$
2	$\varphi(i,r) \wedge i < n \longrightarrow$ $a[r] < a[i] \wedge \varphi(i+1, i)$ $\vee$ $\neg(a[r] < a[i]) \wedge \varphi(i+1, r)$

Maximales Element (Initialisierung)

```
1  // {0 < n}
2  // {φ(0, 0)}
3  i= 0;
4  // {φ(i, 0)}
5  r= 0;
6  // {φ(i, r)}
7  while (i< n)
8    /** inv {(∀j. 0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ r < n ∧ 0 ≤ i < n} */
```

VC:

1	$\varphi(i,r) \wedge \neg(i < n) \longrightarrow$ $(\forall j.\, 0 \leq j \longleftrightarrow a[j] \leq a[r])$ $\wedge$ $0 \leq r < n$
2	$\varphi(i,r) \wedge i < n \longrightarrow$ $a[r] < a[i] \wedge \varphi(i+1, i)$ $\vee$ $\neg(a[r] < a[i]) \wedge \varphi(i+1, r)$
3	$0 \leq n \longrightarrow \varphi(0,0)$

Maximales Element (Verifikationsbedingungen)

Unvereinfacht:

1 $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i \le n \land \neg(i < n) \longrightarrow$
$(\forall j.0 \le j < n \longrightarrow a[j] \le a[r]) \land 0 \le r < n$

2 $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i \le n \land i < n \longrightarrow$
$((a[r] < a[i] \land (\forall j.0 \le j < i+1 \longrightarrow a[j] \le a[i]) \land 0 \le i < n \land 0 \le i+1 \le n) \lor$
$(\neg(a[r] < a[i]) \land (\forall j.0 \le j < i+1 \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i+1 \le n))$

3 $0 \le n \longrightarrow (\forall j.0 \le j < 0 \longrightarrow a[j] \le a[0]) \land 0 \le 0 < n \land 0 \le 0 \le n$

Vereinfacht:

1.1 $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i \le n \land n \le i \longrightarrow$
$\forall j.0 \le j < n \longrightarrow a[j] \le a[r]$

1.2 $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i \le n \land n \le i \longrightarrow 0 \le r \le n$

2 $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i \le n \land i < n \longrightarrow$
$((a[r] < a[i] \land (\forall j.0 \le j < i+1 \longrightarrow a[j] \le a[i]) \land 0 \le i < n \land 0 \le i+1 \le n) \lor$
$(\neg(a[i] \le a[r]) \land (\forall j.0 \le j < i+1 \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i+1 \le n))$

3.1 $0 \le n \longrightarrow \forall j.0 \le j < 0 \longrightarrow a[j] \le a[0]$

3.2 $0 \le n \longrightarrow 0 \le 0 < 0$

3.2 $0 \le n \longrightarrow 0 \le 0 \le 0$

- Sehr **lange** Verifikationsbedingungen (u.a. wegen Fallunterscheidung)
  - Insbesondere schwer zu **vereinfachen**
- Wie können wir das **beheben**?

Explizite Vorbedingungen

Lange Vorbedingung:

```
// {(P1 ∧ b) ∨ (P2 ∧ ¬b)}
if (b) {
  // {P1}
  ...
  // {Q}
  } else {
  // {P2}
  ...
  // {Q}
  }
```

Kurze Vorbedingung:

```
// {A}
if (b) {
  // {A ∧ b}
  ...
  // {Q}
  } else {
  // {A ∧ ¬b}
  ...
  // {Q}
  }
```

Dazu VCs:

$A \land b \longrightarrow P_1$
$A \land \neg b \longrightarrow P_2$

Spracherweiterung: Explizite Spezifikationen

- Erweiterung der Sprache C0 um Invarianten für Schleifen und **explizite Zusicherung**

Assn $a ::= \ldots$ — Zusicherungen

Stmt $c ::= l = e \mid c_1; c_2 \mid \{\} \mid$ **if** (b) c_1 **else** c_2
$\mid$ **while** (b) /** **inv** a */ c
$\mid$ /** $\{a\}$ */

- Zusicherungen haben **keine Semantik** (Kommentar!), sondern erzwingen eine neue Vorbedingung.
- Dazu vereinfachte Regel für Fallunterscheidung:

$$\text{awp}(\textbf{if } (b)\ c_0\ \textbf{else}\ c_1, P) \stackrel{def}{=} (b \land \text{awp}(c_0, P)) \lor (\neg b \land \text{awp}(c_1, P))$$

Wenn $\text{awp}(c_0, P) = b \land P_0$, $\text{awp}(c_1, P) = \neg b \land P_0$, dann gilt

$$(b \land b \land P_0) \lor (\neg b \land \neg b \land P_0) = (b \land P_0) \lor (\neg b \land P_0) = (b \lor \neg b) \land P_0 = P_0$$

Überblick: Approximative schwächste Vorbedingung

$$\begin{aligned}
\text{awp}(\{\}, P) &\stackrel{def}{=} P \\
\text{awp}(l = e, P) &\stackrel{def}{=} P[e/l] \qquad \text{(Genauer: Folie 24 letzte VL)} \\
\text{awp}(c_1; c_2, P) &\stackrel{def}{=} \text{awp}(c_1, \text{awp}(c_2, P)) \\
\text{awp}(\textbf{if } (b)\ c_0\ \textbf{else}\ c_1, P) &\stackrel{def}{=} Q \quad \text{wenn } \text{awp}(c_0, P) = b \land Q, \text{awp}(c_1, P) = \neg b \land Q \\
\text{awp}(\textbf{if } (b)\ c_0\ \textbf{else}\ c_1, P) &\stackrel{def}{=} (b \land \text{awp}(c_0, P)) \lor (\neg b \land \text{awp}(c_1, P)) \\
\text{awp}(\text{/** } \{q\} \text{ */}, P) &\stackrel{def}{=} q \\
\text{awp}(\textbf{while } (b)\ \text{/** } \textbf{inv } i \text{ */ } c, P) &\stackrel{def}{=} i \\
\text{wvc}(\{\}, P) &\stackrel{def}{=} \emptyset \\
\text{wvc}(l = e, P) &\stackrel{def}{=} \emptyset \\
\text{wvc}(c_1; c_2, P) &\stackrel{def}{=} \text{wvc}(c_1, \text{awp}(c_2, P)) \cup \text{wvc}(c_2, P) \\
\text{wvc}(\textbf{if } (b)\ c_0\ \textbf{else}\ c_1, P) &\stackrel{def}{=} \text{wvc}(c_0, P) \cup \text{wvc}(c_1, P) \\
\text{wvc}(\text{/** } \{q\} \text{ */}, P) &\stackrel{def}{=} \{q \longrightarrow P\} \\
\text{wvc}(\textbf{while } (b)\ \text{/** } \textbf{inv } i \text{ */ } c, P) &\stackrel{def}{=} \text{wvc}(c, i) \cup \{i \land b \longrightarrow \text{awp}(c, i)\} \cup \{i \land \neg b \longrightarrow P\}
\end{aligned}$$

Maximales Element mit Zusicherung

```
1  // {0 < n}
2  // {(∀j. 0 ≤ j < 0 ⟶ a[j] ≤ a[0]) ∧ 0 ≤ 0 < 0 ∧ 0 ≤ n}
3  i= 0;
4  r= 0;
5  // {(∀j. 0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ r < i ∧ i < n}
6  while (i< n) /** inv {(∀j.0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ r < n ∧ 0 ≤ i ≤ n} */
7  {
8    // {∀j. 0 ≤ j < i ⟶ a[j] ≤ a[r] ∧ 0 ≤ r < i ∧ i < n}
9    if (a[r] < a[i]) {
10     // {(∀j. 0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ r < n ∧ 0 ≤ i < n ∧ a[r] < a[i]}
11     // {(∀j. 0 ≤ j < i+1 ⟶ a[j] ≤ a[i]) ∧ 0 ≤ i < n ∧ 0 ≤ i+1 ≤ n}
12     r= i;
13     // {(∀j. 0 ≤ j < i+1 ⟶ a[j] ≤ a[r]) ∧ 0 ≤ r < n ∧ 0 ≤ i+1 ≤ n}
14     }
15   else {
16     // {(∀j. 0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ r < n ∧ 0 ≤ i < n ∧ ¬(a[r] < a[i])}
17     // {(∀j. 0 ≤ j < i+1 ⟶ a[j] ≤ a[r]) ∧ 0 ≤ r < n ∧ 0 ≤ i+1 ≤ n}
18     }
19   // {(∀j. 0 ≤ j < i+1 ⟶ a[j] ≤ a[r]) ∧ 0 ≤ r < n ∧ 0 ≤ i+1 ≤ n}
20   i= i+1;
21   // {(∀j. 0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ r < n ∧ 0 ≤ i ≤ n}
22   }
23 // {(∀j. 0 ≤ j < n ⟶ a[j] ≤ a[r]) ∧ 0 ≤ r < n}
```


Maximales Element mit Zusicherung: Beweisverpflichtungen

Unvereinfacht:

(1) $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i \le n \land \neg(i < n)$
$\longrightarrow (\forall j.0 \le j < n \longrightarrow a[j] \le a[r]) \land 0 \le r < n$

(2) $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i < n \land \neg(a[r] < a[i])$
$\longrightarrow (\forall j.0 \le j < i+1 \longrightarrow a[j] \le a[r]) \land 0 \le r < i+1 \land 0 \le i+1 \le n$

(3) $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i < n \land a[r] < a[i]$
$\longrightarrow (\forall j.0 \le j < i+1 \longrightarrow a[j] \le a[i]) \land 0 \le i < n \land 0 \le i+1 \le n$

(4) $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i \le n \longrightarrow$
$(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i < n$

(5) $0 < n \longrightarrow (\forall j.0 \le j < 0 \longrightarrow a[j] \le a[0]) \land 0 \le 0 < n \land 0 \le 0 \le n$

Maximales Element mit Zusicherung: Beweisverpflichtungen

Vereinfacht (Teil 1):

(1.1) $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i \le n \land n \le i$
$\longrightarrow (\forall j.0 \le j < n \longrightarrow a[j] \le a[r])$

(1.2) $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i \le n \land n \le i$
$\longrightarrow 0 \le r < n$

(2.1) $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i < n \land a[i] \le a[r]$
$\longrightarrow (\forall j.0 \le j < i+1 \longrightarrow a[j] \le a[r])$

(2.2) $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i < n \land a[i] \le a[r]$
$\longrightarrow 0 \le r < n$

(2.3) $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i < n \land a[i] \le a[r]$
$\longrightarrow 0 \le i+1 \le n$

Maximales Element mit Zusicherung: Beweisverpflichtungen

Vereinfacht (Teil 2):

(3.1) $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i < n \land a[r] < a[i]$
$\longrightarrow (\forall j.0 \le j < i+1 \longrightarrow a[j] \le a[i])$

(3.2) $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i < n \land a[r] < a[i]$
$\longrightarrow 0 \le i < n$

(3.3) $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i < n \land a[r] < a[i]$
$\longrightarrow 0 \le i+1 \le n$

(4.1) $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i \le n \longrightarrow$
$(\forall j.0 \le j < i \longrightarrow a[j] \le a[r])$

(4.2) $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i \le n \longrightarrow 0 \le r < n$

(4.3) $(\forall j.0 \le j < i \longrightarrow a[j] \le a[r]) \land 0 \le r < n \land 0 \le i \le n \longrightarrow 0 \le i < n$

(5.1) $0 < n \longrightarrow (\forall j.0 \le j < 0 \longrightarrow a[j] \le a[0])$

(5.2) $0 < n \longrightarrow 0 \le 0 < n$

(5.3) $0 < n \longrightarrow 0 \le 0 \le n$

Beweismethoden

- Um $P_1 \wedge \ldots \wedge P_n \longrightarrow Q$ zu zeigen, nehmen wir $P_1, \ldots, P_n$ an und zeigen Q.
- Dabei nutzen wir **u.a.** folgende Regeln:

Wenn P, dann P (Trivial)
Wenn P und $I = t$, dann $P[t/I]$ (Substitution)
$x \leq x$ (Reflexität)
Wenn $x \leq y$ und $y \leq z$, dann $x \leq z$ (Transitivität)
Wenn $x \leq y$ und $y \leq x$, dann $x = y$ (Antisymmetrie)
Wenn $x < y$, dann $x \leq y + 1$ oder $x + 1 \leq y$ (Inc)
Wenn $\forall x.\, P$, dann $P[t/x]$ (Instantiierung)
Wenn *false*, dann P (Ex falso)
Wenn $a \leq b$ und $x \leq y$, dann $a + x \leq b + y$ und Variation mit $x = 0$ etc.
Umformungen mit $(0, +)$ und $(1, \cdot)$
Domänenspezifische Regeln

Arbeitsblatt 9.4: Beweisverpflichtungen Beweisen

Betrachtet die vereinfachten Verifikationsbedingungen. Wie würdet ihr sie beweisen? Was für Methoden verwendet ihr?

- Welches sind **triviale** Beweise?
- Welches sind **einfache** Beweise?
- Welche erfordern längere Argumentation?

Arbeitsblatt 9.5: Kopien

Dieses Programm kopiert ein Array:

```
i= 0;
while (i< m)
  /** inv ??? */ {
  b[m-1-i]= a[i];
  i= i+1;
  }
```

1. Spezifiziert die Funktionalität.
2. Findet die Invariante.
3. Berechnet die Verifikationsbedingungen (VCs) und schwächste Vorbedingung.
4. Beweist die VCs.

Noch ein Beispiel: kleinstes Null-Element

- Folgendes Programm sucht in `a` nach dem **ersten** Null-Element:

```
void find_zero()
{
i= 0;
r= -1;
while (i< n)
  if (r== -1 && a[i] == 0) {
    r= i;
    }
  else {
    }
  }
}
```

- Wie **spezifizieren** wir das?
- Welche **Beweisverpflichtungen** entstehen?
- Wie **beweisen** wir diese?

Zusammenfassung

- Die Regeln des Floyd-Hoare-Kalküls lassen sich, weitgehend schematisch, rückwärts (vom Ende her) anwenden — nur Schleifen machen Probleme.
- Wir **annotieren** daher die Invarianten an Schleifen, und können dann die schwächste Vorbedingung und Verifikationsbedingungen automatisch berechnen.
  - Dabei sind die **Verifikationsbedingungen** das Interessante.
- Um die Verifikationsbedingungen zu vereinfachen führen wir **explizite Zusicherungen** in C0 ein
- Die Generierung von Verifikationsbedingungen korrespondiert zur relativen Vollständigkeit der Floyd-Hoare-Logik.
- Warum eigentlich immer **rückwärts**? Nächstes Mal

Korrekte Software: Grundlagen und Methoden
Vorlesung 10 vom 21.06.22
Vorwärts mit Floyd und Hoare

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2022

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Idee

- Hier ist ein einfaches Programm:

```
// {X = x ∧ Y = y}
z = y;
//{X = x ∧ Y = z}
y = x;
// {X = y ∧ Y = z}
x = z;
//{X = y ∧ Y = x}
```

- Wir haben gesehen:
  1. Die Verifikation erfolgt **rückwärts** (von hinten nach vorne).
  2. Die Verifikation kann **berechnet** werden.
- Muss das rückwärts sein? Warum nicht vorwärts? Was ist der Vorteil?

Nachteile der Rückwärtsberechnung

```
// {i ≠ 3}
.
.  // 400 Zeilen, die
.  // i nicht verändern
.
a[ i ]= 5;
// {a[3] = 7}
```

Errechnete **Vorbedingung** (AWP)

$(a[3] == 7)[5/a[i]] \;=\; ((i == 3\ ?\ 5 : a[i]) == 7)$

- Kann nicht vereinfacht werden, weil wir nicht wissen, ob $i \neq 3$
- AWP wird **sehr groß**.
- Das Problem wächst mit der Länge der Programme.

I. Der Floyd-Hoare-Kalkül Vorwärts

Regelanwendung rückwärts

- Um Regel **rückwärts** anwenden zu können:
  1. **Nachbedingung** der Konklusion muss offene Variable sein
  2. Alle **Vorbedingungen** der Prämissen müssen disjunkte, offene Variablen sein.
  3. Gegenbeispiele: while-Regel, if-Regel
- Um Regeln **vorwärts** anwenden zu können:
  1. **Vorbedingung** der Konklusion muss offene Variable sein
  2. Alle **Nachbedingungen** der Prämissen müssen disjunkte, offene Variablen sein.
  3. Gegenbeispiele: ...

Vorwärtsanwendung der Regeln

- Zuweisungsregel kann **nicht vorwärts** angewandt werden, weil die Vorbedingung keine offene Variable ist:

$$\frac{}{\vdash \{P[e/x]\}\, x = e\, \{P\}}$$

- Andere Regeln passen bis auf if-Regel (keine **disjunkten** Variablen)

$$\frac{}{\vdash \{A\}\,\{\}\,\{A\}} \qquad \frac{\vdash \{A \wedge b\}\, c_0\, \{B\} \qquad \vdash \{A \wedge \neg b\}\, c_1\, \{B\}}{\vdash \{A\}\ \textbf{if}\ (b)\ c_0\ \textbf{else}\ c_1\, \{B\}}$$

$$\frac{\vdash \{A\}\, c_1\, \{B\} \qquad \vdash \{B\}\, c_2\, \{C\}}{\vdash \{A\}\, c_1; c_2\, \{C\}} \qquad \frac{\vdash \{A \wedge b\}\, c\, \{A\}}{\vdash \{A\}\ \textbf{while}\ (b)\ c\, \{A \wedge \neg b\}}$$

$$\frac{A' \longrightarrow A \qquad \vdash \{A\}\, c\, \{B\} \qquad B \longrightarrow B'}{\vdash \{A'\}\, c\, \{B'\}}$$

Arbeitsblatt 10.1: If-Regel Vorwärts

- Wie kann die If-Regel vorwärts aussehen?

Zuweisungsregel Vorwärts

- Alternative Zuweisungsregel (nach Floyd):

$$\frac{V \notin FV(P)}{\vdash \{P\}\, x = e\, \{\exists V.\, P[V/x] \wedge x = (e[V/x])\}}$$

  - $FV(P)$ sind die **freien** logischen Variablen in P.
- Jetzt ist die Vorbedingung offen — Regel kann vorwärts angewandt werden
- Ist keine abgeleitete Regel — muss als korrekt **bewiesen** werden

Arbeitsblatt 10.2: Das Leben mit dem Quantor

- Was bedeutet $\exists V.P$?
  - Die Formel ist wahr, wenn es **irgendeinen** Wert t für V gibt, so dass $P[t/V]$ wahr ist.
- Was bedeutet $\forall V.P$?
  - Die Formel ist wahr, wenn für **alle** Werte t für V $P[t/V]$ wahr ist.
- Sind folgende Formeln wahr (für $x, y \in \mathbb{Z}$)? (Finde Gegenbeispiele oder Zeugen)

$\exists x.\, x < 7$	$\exists x.\, x < 3 \wedge x > 7$	$\exists x.\, x < 7 \vee x < 3$
$\exists y \exists x.\, x + 3 = y$	$\forall x \exists y.\, x \cdot y = 3$	$\exists x \forall y.\, x \cdot y = y$

Vorwärtsverkettung

$$\frac{V \notin FV(P)}{\vdash \{P\}\, x = e\, \{\exists V.\, P[V/x] \wedge x = e[V/x]\}}$$

```
// {0 ≤ x}
x= 2*y;
// {∃V1.0 ≤ V1 ∧ x = 2·y}
x= x+1;
// {∃V2.(∃V1.0 ≤ V1 ∧ x = 2·y)[V2/x] ∧ x = (x+1)[V2/x]}
```

- **Vereinfachung** der letzten Nachbedingung:

$$\begin{aligned}
&\exists V_2.(\exists V_1.0 \le V_1 \wedge x = 2\cdot y)[V_2/x] \wedge x = (x+1)[V_2/x] \\
\iff &\exists V_2.(\exists V_1.0 \le V_1 \wedge V_2 = 2\cdot y) \wedge x = V_2 + 1 \\
\iff &\exists V_2.\exists V_1.0 \le V_1 \wedge x = V_2 + 1 \wedge V_2 = 2\cdot y \\
&\text{Und jetzt...?}
\end{aligned}$$

Regeln der Vorwärtsverkettung

Eigenschaften des Existenzquantors:

$$\begin{aligned}
P(V) \wedge V = t &\longrightarrow P[t/V] \wedge V = t && V \notin FV(t) && (1)\\
\exists V.\, P(V) \wedge V = t &\longrightarrow P[t/V] && V \notin FV(t) && (2)\\
(\exists V.\, P) \wedge Q &\Longleftrightarrow \exists V.\, P \wedge Q && V \notin FV(Q) && (3)\\
\exists V.\, P &\longrightarrow P && V \notin FV(P) && (4)
\end{aligned}$$

Damit gelten folgende Regeln bei der Vorwärtsverkettung:

1. Wenn x nicht in Vorbedingung auftritt, dann $P[V/x] \equiv P$.
2. Wenn x nicht in rechter Seite e auftritt, dann $e[V/x] \equiv e$.
3. Wenn beides der Fall ist, kann der Existenzquantor wegfallen (4)

Vorwärtsverkettung

$$\frac{V \notin FV(P)}{\vdash \{P\}\, x = e\, \{\exists V.\, P[V/x] \wedge x = e[V/x]\}}$$

```
// {0 ≤ x}
x= 2*y;
// {∃V1.0 ≤ V1 ∧ x = 2·y}
x= x+1;
// {∃V2.(∃V1.0 ≤ V1 ∧ x = 2·y)[V2/x] ∧ x = (x+1)[V2/x]}
```

- **Vereinfachung** der letzten Nachbedingung:

$$\begin{aligned}
&\exists V_2.(\exists V_1.0 \le V_1 \wedge x = 2\cdot y)[V_2/x] \wedge x = (x+1)[V_2/x] \\
\iff &\exists V_2.(\exists V_1.0 \le V_1 \wedge V_2 = 2\cdot y) \wedge x = V_2 + 1 \\
\iff &\exists V_2.\exists V_1.0 \le V_1 \wedge x = V_2 + 1 \wedge V_2 = 2\cdot y \\
\iff &\exists V_1.0 \le V_1 \wedge x = 2\cdot y + 1
\end{aligned}$$

Vorwärtsverkettung bei der Arbeit

Vereinfachung erst am Ende:

```
// {i·i ≤ a ∧ t = 2·i+1 ∧ s = i·i+t ∧ s ≤ a}
t= t+2;
// {∃T.(i·i ≤ a ∧ t = 2·i+1 ∧ s = i·i+t ∧ s ≤ a)[T/t] ∧ t = (t+2)[T/t]}
// {∃T.i·i ≤ a ∧ T = 2·i+1 ∧ s = i·i+T ∧ s ≤ a ∧ t = T+2}
s= s+t;
// {∃S.(∃T.i·i ≤ a ∧ T = 2·i+1 ∧ s = i·i+T ∧ s ≤ a ∧ t = T+2)[S/s] ∧ s = (s+t)[S/s]}
// {∃S.∃T.i·i ≤ a ∧ T = 2·i+1 ∧ S = i·i+T ∧ S ≤ a ∧ t = T+2 ∧ s = S+t}
i= i+1;
// {∃I.(∃S.∃T.i·i ≤ a ∧ T = 2·i+1 ∧ S = i·i+T ∧ S ≤ a ∧ t = T+2 ∧ s = S+t)[I/i] ∧ i = (i+1)[I/i]}
// {∃I.∃S.∃T.I·I ≤ a ∧ T = 2·I+1 ∧ S = I·I+T ∧ S ≤ a ∧ t = T+2 ∧ s = S+t ∧ i = I+1}
// {∃I.∃S.∃T.I·I ≤ a ∧ S = I·I+T ∧ S ≤ a ∧ t = T+2 ∧ s = S+t ∧ i = I+1 ∧ T = 2·I+1}
// {∃I.∃S.I·I ≤ a ∧ S = I·I+2·I+1 ∧ S ≤ a ∧ t = 2·I+1+2 ∧ s = S+t ∧ i = I+1}
// {∃I.∃S.I·I ≤ a ∧ S ≤ a ∧ t = 2·I+1+2 ∧ s = S+t ∧ i = I+1 ∧ S = (I+1)·(I+1)}
// {∃I.I·I ≤ a ∧ (I+1)·(I+1) ≤ a ∧ t = 2·I+1+2 ∧ s = (I+1)·(I+1)+t ∧ i = I+1}
// {∃I.I·I ≤ a ∧ (I+1)·(I+1) ≤ a ∧ t = 2·I+3 ∧ s = (I+1)·(I+1)+t ∧ I = i−1}
// {(i−1)·(i−1) ≤ a ∧ ((i−1)+1)·((i−1)+1) ≤ a ∧ t = 2·(i−1)+3 ∧ s = ((i−1)+1)·((i−1)+1)+t}
// {i·i ≤ a ∧ t = 2·i+1 ∧ s = i·i+t}
```


Vorwärtsverkettung bei der Arbeit II

Mit Vereinfachung on-the-fly:

```
// {i·i ≤ a ∧ t = 2·i+1 ∧ s = i·i+t ∧ s ≤ a}
t= t+2;
// {∃T.(i·i ≤ a ∧ t = 2·i+1 ∧ s = i·i+t ∧ s ≤ a)[T/t] ∧ t = (t+2)[T/t]}
// {∃T.i·i ≤ a ∧ s = i·i+T ∧ s ≤ a ∧ t = T+2 ∧ T = 2·i+1}
// {i·i ≤ a ∧ s = i·i+2·i+1 ∧ s ≤ a ∧ t = (2·i+1)+2}
// {i·i ≤ a ∧ s = (i+1)·(i+1) ∧ s ≤ a ∧ t = 2·i+3}
s= s+t;
// {∃S.(i·i ≤ a ∧ s = (i+1)·(i+1) ∧ s ≤ a ∧ t = 2·i+3)[S/s] ∧ s = (s+t)[S/s]}
// {∃S.i·i ≤ a ∧ S = (i+1)·(i+1) ∧ S ≤ a ∧ t = 2·i+3 ∧ s = S+t}
// {i·i ≤ a ∧ (i+1)·(i+1) ≤ a ∧ t = 2·i+3 ∧ s = (i+1)·(i+1)+t}
i= i+1;
// {∃I.(i·i ≤ a ∧ (i+1)·(i+1) ≤ a ∧ t = 2·i+3 ∧ s = (i+1)·(i+1)+t)[I/i] ∧ i = (i+1)[I/i]}
// {∃I.I·I ≤ a ∧ (I+1)·(I+1) ≤ a ∧ t = 2·I+3 ∧ s = (I+1)·(I+1)+t ∧ i = I+1}
// {∃I.I·I ≤ a ∧ (I+1)·(I+1) ≤ a ∧ t = 2·I+3 ∧ s = (I+1)·(I+1)+t ∧ I = i−1}
// {(i−1)·(i−1) ≤ a ∧ ((i−1)+1)·((i−1)+1) ≤ a ∧ t = 2·(i−1)+3 ∧ s = ((i−1)+1)·((i−1)+1)+t}
// {i·i ≤ a ∧ t = 2·i+1 ∧ s = i·i+t}
```


Arbeitsblatt 10.3: Vorwärtsverkettung

Gegeben folgendes Programm. Berechnet die Vorwärtsverkettung der Vorbedingung mit Vereinfachung:

```
// {x = X ∧ y = Y}
x= x+y;
// {???}
y= x−y;
// {???}
x= x−y;
// {???}
```

Was bewirkt das Programm?

Beweis der Zuweisungsregel Vorwärts

Erinnert Euch an das **Substitutionslemma**:

$$\sigma \models^I B[e/x] \iff \sigma[x \mapsto [\![e]\!]_{\mathcal{A}}(\sigma)] \models^I B$$

Zu zeigen:

$$\begin{aligned}
&\models \{P\}\, x = e\, \{\exists V.\, P[V/x] \wedge x = (e[V/x])\} \\
\iff &\forall I.\, \forall \sigma.\, \sigma \models^I P \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![x = e]\!]_{\mathcal{C}} \longrightarrow \sigma' \models^I \exists V.\, P[V/x] \wedge x = (e[V/x]) \\
\iff &\forall I.\, \forall \sigma.\, \sigma \models^I P \longrightarrow \sigma[x \mapsto [\![e]\!]_{\mathcal{A}}(\sigma)] \models^I \exists V.\, P[V/x] \wedge x = (e[V/x]) \\
\iff &\forall I.\, \forall \sigma.\, \sigma \models^I P \longrightarrow \sigma \models^I (\exists V.\, P[V/x] \wedge x = (e[V/x]))[e/x] \\
\iff &\forall I.\, \forall \sigma.\, \sigma \models^I P \longrightarrow \sigma \models^I (\exists V.\, P[V/x] \wedge e = (e[V/x])) \\
\impliedby &\forall I.\, \forall \sigma.\, \sigma \models^I P \longrightarrow \sigma \models^I (P[x/x] \wedge e = (e[x/x])) \\
\iff &\forall I.\, \forall \sigma.\, \sigma \models^I P \longrightarrow \sigma \models^I P \quad \square
\end{aligned}$$

Vorwärtsverkettung

- Vorwärtsregelaxiom äquivalent zum Rückwärtsregelaxiom.
- Vorteil: Vorbedingung bleibt kleiner
- Nachteil: in der Anwendung **umständlicher**
- Die entstehende Nachbedingung beschreibt die **symbolische Auswertung**
- Vereinfachung benötigt Rechnung mit Existenzquantor

Zwischenfazit: Der Floyd-Hoare-Kalkül ist symmetrisch

Es gibt zwei Zuweisungsregeln, eine für die **Rückwärtsanwendung** von Regeln, eine für die **Vorwärtsanwendung**.

II. Vorwärtsberechnung von Verifikationsbedingungen

Stärkste Nachbedingung

- Vorwärtsberechnung von Verifikationsbedingungen: Nachbedingung
- Gegeben C0-Programm c, Prädikat P, dann ist
  - $\mathrm{sp}(P, c)$ die **stärkste Nachbedingung** Q so dass $\models \{P\}\, c\, \{Q\}$
  - Prädikat Q **stärker** als Q' wenn $Q \longrightarrow Q'$.
- Semantische Charakterisierung:

Stärkste Nachbedingung

Gegeben Zusicherung $P \in$ **Assn** und Programm $c \in$ **Stmt**, dann

$$\models \{P\}\, c\, \{Q\} \iff \mathrm{sp}(P, c) \longrightarrow Q$$

- Wie können wir $\mathrm{sp}(P, c)$ berechnen?

Berechnung von Nachbedingungen

- Wir berechnen die **approximative** stärkste Nachbedingung.
- Viele Klauseln sind ähnlich der schwächsten Vorbedingung.
- Ausnahmen:
  - While-Schleife: andere Verifikationsbedingungen
  - If-Anweisung: Weakening eingebaut
  - **Zuweisung**: Vorwärtsregel
- Nach jeder Zuweisung Nachbedingung **vereinfachen**

Überblick: Approximative stärkste Nachbedingung

$$\begin{aligned}
\mathrm{asp}(P, \{\,\}) &\stackrel{\mathrm{def}}{=} P \\
\mathrm{asp}(P, x = e) &\stackrel{\mathrm{def}}{=} \exists V.\, P[V/x] \wedge x = (e[V/x]) \\
\mathrm{asp}(P, c_1; c_2) &\stackrel{\mathrm{def}}{=} \mathrm{asp}(\mathrm{asp}(P, c_1), c_2) \\
\mathrm{asp}(P, \textbf{if}\ (b)\ c_0\ \textbf{else}\ c_1) &\stackrel{\mathrm{def}}{=} \mathrm{asp}(b \wedge P, c_0) \vee \mathrm{asp}(\neg b \wedge P, c_1) \\
\mathrm{asp}(P, /{*}{*}\ \{q\}\ {*}/) &\stackrel{\mathrm{def}}{=} q \\
\mathrm{asp}(P, \textbf{while}\ (b)\ /{*}{*}\ \textbf{inv}\ i\ {*}/\ c) &\stackrel{\mathrm{def}}{=} i \wedge \neg b \\
\\
\mathrm{svc}(P, \{\,\}) &\stackrel{\mathrm{def}}{=} \emptyset \\
\mathrm{svc}(P, x = e) &\stackrel{\mathrm{def}}{=} \emptyset \\
\mathrm{svc}(P, c_1; c_2) &\stackrel{\mathrm{def}}{=} \mathrm{svc}(P, c_1) \cup \mathrm{svc}(\mathrm{asp}(P, c_1), c_2) \\
\mathrm{svc}(P, \textbf{if}\ (b)\ c_0\ \textbf{else}\ c_1) &\stackrel{\mathrm{def}}{=} \mathrm{svc}(P \wedge b, c_0) \cup \mathrm{svc}(P \wedge \neg b, c_1) \\
\mathrm{svc}(P, /{*}{*}\ \{q\}\ {*}/) &\stackrel{\mathrm{def}}{=} \{P \longrightarrow q\} \\
\mathrm{svc}(P, \textbf{while}\ (b)\ /{*}{*}\ \textbf{inv}\ i\ {*}/\ c) &\stackrel{\mathrm{def}}{=} \mathrm{svc}(i \wedge b, c) \cup \{P \longrightarrow i\} \cup \{\mathrm{asp}(i \wedge b, c) \longrightarrow i\} \\
\\
\mathit{svc}(\{P\}\, c\, \{Q\}) &\stackrel{\mathrm{def}}{=} \{\mathrm{asp}(P, c) \longrightarrow Q\} \cup \mathrm{svc}(P, c)
\end{aligned}$$

Beispiel: Fakultät

```
1 // {0 ≤ n}
2 p= 1;
3 c= 1;
4 while (c <= n) //** inv {p = (c − 1)! ∧ c − 1 ≤ n}; */
5   p = p * c;
6   c = c + 1;
7   }
8 // {p = n!}
```


Beispiel: Fakultät, stärkste Nachbedingung

Notation: asp_x = Stärkste Nachbedingung **nach** Zeile x.

```
1 // {0 ≤ n}
2 p= 1;
  // {∃V. 0 ≤ n[V/p] ∧ p = (1[V/p])}
  // {0 ≤ n ∧ p = 1}
3 c= 1;
  // {∃V. (0 ≤ n ∧ p = 1)[V/c] ∧ c = (1[V/c])}
  // {0 ≤ n ∧ p = 1 ∧ c = 1}
4 while (c <= n) //** inv {p = (c − 1)! ∧ c − 1 ≤ n}; */ {
5  p = p * c;
   //
6  c = c + 1;
   //
7  }
  // {¬(c ≤ n) ∧ p = (c − 1)! ∧ c − 1 ≤ n}
8 // {p = n!}
```

$VC_1 = \{asp_3 \longrightarrow p = (c-1)! \wedge c - 1 \leq n\}$

Beispiel: Fakultät, stärkste Nachbedingung (Schleifenrumpf)

```
1  // {0 ≤ n}
2  p= 1;
   // {0 ≤ n ∧ p = 1}
3  c= 1;
   // {0 ≤ n ∧ p = 1 ∧ c = 1}
4  while (c <= n) /** inv p = (c−1)! ∧ c−1 ≤ n; */ \{
5   p = p * c;
    // {∃V1. (p = (c − 1)! ∧ (c − 1) ≤ n ∧ c ≤ n)[V1/p] ∧ p = (p · c)[V1/p]}
    // {∃V1. (V1 = (c − 1)! ∧ (c − 1) ≤ n ∧ c ≤ n) ∧ p = (V1 · c)}
    // {c − 1 ≤ n ∧ c ≤ n ∧ p = (c − 1)! · c}
6   c = c + 1;
    // {∃V2. (c − 1 ≤ n ∧ c ≤ n ∧ p = (c − 1)! · c)[V2/c] ∧ c = (c + 1)[V2/c]}
    // {∃V2. (V2 − 1 ≤ n ∧ V2 ≤ n ∧ p = (V2 − 1)! · V2) ∧ c = (V2 + 1)}
    // {c − 2 ≤ n ∧ c − 1 ≤ n ∧ p = (c − 2)! · (c − 1)}
7   }
   // {¬(c ≤ n) ∧ p = (c − 1)! ∧ c − 1 ≤ n}
8  // {p = n!}
```


Beispiel: Fakultät, Verifikationsbedingungen

Notation: svc_x = in Zeile x generierte Verifikationsbedingung

```
1  // {0 ≤ n}
2  p= 1;
   // svc2 = ∅
   c= 1;
   // svc3 = ∅
4  while (c <= n) //** inv {p = (c − 1)! ∧ c − 1 ≤ n}; */ {
5   p = p * c;
    // svc5 = ∅
6   c = c + 1;
    // svc6 = ∅
7   }
   // svc4 = {asp3 ⟶ (p = (c − 1)! ∧ c − 1 ≤ n),
   //                asp6 ⟶ (p = (c − 1)! ∧ c − 1 ≤ n)}
   // svc4 = {(0 ≤ n ∧ p = 1 ∧ c = 1) ⟶ (p = (c − 1)! ∧ c − 1 ≤ n),
   //                (c − 2 ≤ n ∧ c − 1 ≤ n ∧ p = (c − 2)! · (c − 1))
   //                      ⟶ (p = (c − 1)! ∧ c − 1 ≤ n)}
8  // {p = n!}
```


Schließlich zu zeigen

$$
\begin{aligned}
svc_8 &= \{\{asp_8 \longrightarrow p = n!\} \cup svc_4 \\
&= \{(p = (c-1)! \wedge c - 1 \leq n \;\&\&\; \neg(c <= n)) \longrightarrow p = n!\}, \\
&\quad (0 \leq n \wedge p = 1 \wedge c = 1) \longrightarrow (p = (c-1)! \wedge c - 1 \leq n), \\
&\quad (c - 2 \leq n \wedge c - 1 \leq n \wedge p = (c-2)! \cdot (c-1)) \\
&\qquad \longrightarrow (p = (c-1)! \wedge c - 1 \leq n)\} \\
&\rightsquigarrow \{true\}
\end{aligned}
$$

Arbeitsblatt 10.4: Jetzt seid ihr dran!

Berechnet die stärkste Nachbedingung und Verifikationsbedingungen für die ganzzahlige Division:

```
1  /** {0 ≤ a} */
2  r= a;
3  q= 0;
4  while (b <= r) /** inv { a == b*q+r ∧ 0 ≤ r } */ {
5    r= r−b;
6    q= q+1;
7    }
8  /** { a == b*q+ r ∧ 0 ≤ r ∧ r < b } */
```


Beispiel: Suche nach dem Maximalen Element

```
1  // {0 < n}
2  i= 0;
3  // {∃I0.(0 < n)[I0/i] ∧ i = 0[I0/i]}
4  // {0 < n ∧ i = 0}
5  r= 0;
6  // {0 < n ∧ i = 0 ∧ r = 0}
7  while (i!= n)
8    /** inv (∀j. 0≤ j < i ⟶a[j]≤ a[r])∧ 0≤ i≤ n ∧ 0≤ r< n */ {
9    if (a[r] < a[i]) {
10     r= i;
11   }
12   else {
13     }
14   i= i+1;
15   }
16 // {∀j.0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ i ≤ n ∧ 0 ≤ r < n ∧ ¬(i ≠ n)}
17 // {(∀j.0 ≤ j < n ⟶ a[j] ≤ a[r]) ∧ 0 ≤ r < n}
```


Beispiel: Suche nach dem Maximalen Element (Schleifenrumpf)

```
1  while (i!= n)
2    /** inv (∀j. 0≤ j < i ⟶a[j]≤ a[r])∧ 0≤ i≤ n ∧ 0≤ r< n */ {
3    if (a[r] < a[i]) {
4      // {(∀j.0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ i ≤ n ∧ 0 ≤ r < n ∧ a[r] < a[i]}
5      r= i;
6      // {∃R0.((∀j.0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ i ≤ n ∧ 0 ≤ r < n ∧ a[r] < a[i])[R0/r] ∧ r = i[R0/r]}
7      // {∃R0.(∀j.0 ≤ j < i ⟶ a[j] ≤ a[R0]) ∧ 0 ≤ i ≤ n ∧ 0 ≤ R0 < n ∧ a[R0] < a[i] ∧ r = i}
8    }
9    else {
10     // {(∀j.0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ i ≤ n ∧ 0 ≤ r < n ∧ ¬(a[r] < a[i])}
11     }
12   // {(∃R0.(∀j.0 ≤ j < i ⟶ a[j] ≤ a[R0]) ∧ 0 ≤ i ≤ n ∧ 0 ≤ R0 < n ∧ a[R0] < a[i] ∧ r = i) }
         ∨((∀j.0 ≤ j < i ⟶ a[j] ≤ a[r]) ∧ 0 ≤ i ≤ n ∧ 0 ≤ r < n ∧ a[i] ≤ a[r])
13   i= i+1;
14   // {∃I0.((∃R0.(∀j.0 ≤ j < I0 ⟶ a[j] ≤ a[R0]) ∧ 0 ≤ I0 < n ∧ 0 ≤ R0 < n ∧ a[R0] < a[I0] ∧ r = I0) }
           ∨((∀j.0 ≤ j < I0 ⟶ a[j] ≤ a[r]) ∧ 0 ≤ I0 < n ∧ 0 ≤ r < n ∧ a[I0] ≤ a[r])) ∧ i = I0 + 1
15   }
```


Verifikationsbedingungen

1. $0 < n \wedge i = 0 \wedge r = 0 \longrightarrow (\forall j.0 \leq j < i \longrightarrow a[j] \leq a[r]) \wedge 0 \leq i \leq n \wedge 0 \leq r < n$

2. $(\forall j.0 \leq j < i \longrightarrow a[j] \leq a[r]) \wedge 0 \leq i \leq n \wedge 0 \leq r < n \wedge \neg(i \neq n) \longrightarrow$
   $(\forall j.0 \leq j < n \longrightarrow a[j] \leq a[r]) \wedge 0 \leq r < n$

3. $(\exists I_0.((\exists R_0.(\forall j.0 \leq j < I_0 \longrightarrow a[j] \leq a[R_0]) \wedge 0 \leq I_0 < n \wedge 0 \leq R_0 < n \wedge a[R_0] < a[I_0] \wedge r = I_0)$
   $\vee((\forall j.0 \leq j < I_0 \longrightarrow a[j] \leq a[r]) \wedge 0 \leq I_0 < n \wedge 0 \leq r < n \wedge a[I_0] \leq a[r])) \wedge i = I_0 + 1)$
   $\longrightarrow (\forall j.0 \leq j < i \longrightarrow a[j] \leq a[r]) \wedge 0 \leq i \leq n \wedge 0 \leq r < n$

Weitere Vereinfachungsregeln

Existenzquantoren und Disjunktionen können mit folgenden Regeln vereinfacht werden:

6. Der Gültigkeitsbereich des Existenzquantors kann verkleinert werden:
   - $(\exists x.P \vee Q) \rightsquigarrow (\exists x.P) \vee (\exists x.Q)$
7. Disjunktionen in der Prämisse ergeben eine Fallunterscheidung:
   - $A_1 \vee A_2 \longrightarrow B \rightsquigarrow A_1 \longrightarrow B, A_2 \longrightarrow B$
8. Konjunktion distributiert über Disjunktion:
   - $(A_1 \vee A_2) \wedge B \rightsquigarrow (A_1 \wedge B) \vee (A_2 \wedge B)$
9. . . . und andersherum:
   - $(A_1 \wedge A_2) \vee B \rightsquigarrow (A_1 \vee B) \wedge (A_2 \vee B)$

Vereinfachte Verifikationsbedingungen

1.1 $0 < n \wedge i = 0 \wedge r = 0 \longrightarrow (\forall j.0 \leq j < i \longrightarrow a[j] \leq a[r])$
1.2 $0 < n \wedge i = 0 \wedge r = 0 \longrightarrow 0 \leq r < n$
1.3 $0 < n \wedge i = 0 \wedge r = 0 \longrightarrow 0 \leq i \leq n$

2.1 $(\forall j.0 \leq j < i \longrightarrow a[j] \leq a[r]) \wedge 0 \leq i \leq n \wedge 0 \leq r < n \wedge \neg(i \neq n) \longrightarrow (\forall j.\, 0 \leq j < n \longrightarrow a[j] \leq a[r])$
2.2 $(\forall j.0 \leq j < i \longrightarrow a[j] \leq a[r]) \wedge 0 \leq i \leq n \wedge 0 \leq r < n \wedge \neg(i \neq n) \longrightarrow 0 \leq r < n$

3.1 $(\exists I_0.(\exists R_0.(\forall j.0 \leq j < I_0 \longrightarrow a[j] \leq a[R_0]) \wedge 0 \leq I_0 < n \wedge 0 \leq R_0 < n \wedge a[R_0] < a[I_0] \wedge r = I_0) \wedge i = I_0 + 1)$
$\longrightarrow (\forall j.0 \leq j < i \longrightarrow a[j] \leq a[r])$
3.1 $(\exists R_0.((\forall j.0 \leq j < r \longrightarrow a[j] \leq a[R_0]) \wedge 0 \leq r < n \wedge 0 \leq R_0 < n \wedge a[R_0] < a[r]) \wedge i = r + 1)$
$\longrightarrow (\forall j.0 \leq j < i \longrightarrow a[j] \leq a[r])$
3.2 $(\exists I_0.(\forall j.0 \leq j < I_0 \longrightarrow a[j] \leq a[r]) \wedge 0 \leq I_0 < n \wedge 0 \leq r < n \wedge a[I_0] \leq a[r] \wedge i = I_0 + 1)$
$\longrightarrow (\forall j.0 \leq j < i \longrightarrow a[j] \leq a[r])$
3.3 $(\exists I_0.(\exists R_0.(\forall j.0 \leq j < I_0 \longrightarrow a[j] \leq a[R_0]) \wedge 0 \leq I_0 < n \wedge 0 \leq R_0 < n \wedge a[R_0] < a[I_0] \wedge r = I_0) \wedge i = I_0 + 1)$
$\longrightarrow 0 \leq i \leq n$
3.3 $(\exists R_0.(\forall j.0 \leq j < r \longrightarrow a[j] \leq a[R_0]) \wedge 0 \leq r < n \wedge 0 \leq R_0 < n \wedge a[R_0] < a[r]) \wedge i = r + 1$
$\longrightarrow 0 \leq i \leq n$
3.4 $(\exists I_0.(\forall j.0 \leq j < I_0 \longrightarrow a[j] \leq a[r]) \wedge 0 \leq I_0 < n \wedge 0 \leq r < n \wedge a[I_0] \leq a[r] \wedge i = I_0 + 1)$
$\longrightarrow 0 \leq i \leq n$
3.5 $(\exists I_0.(\exists R_0.(\forall j.0 \leq j < I_0 \longrightarrow a[j] \leq a[R_0]) \wedge 0 \leq I_0 < n \wedge 0 \leq R_0 < n \wedge a[R_0] < a[I_0] \wedge r = I_0) \wedge i = I_0 + 1)$
$\longrightarrow 0 \leq r < n$
3.5 $(\exists R_0.(\forall j.0 \leq j < r \longrightarrow a[j] \leq a[R_0]) \wedge 0 \leq r < n \wedge 0 \leq R_0 < n \wedge a[R_0] < a[r]) \wedge i = r + 1$
$\longrightarrow 0 \leq r < n$
3.6 $(\exists I_0.(\forall j.0 \leq j < I_0 \longrightarrow a[j] \leq a[r]) \wedge 0 \leq I_0 < n \wedge 0 \leq r < n \wedge a[I_0] \leq a[r] \wedge i = I_0 + 1)$
$\longrightarrow 0 \leq r < n$

Vereinfachte Verifikationsbedingungen

1.1 $0 < n \wedge i = 0 \wedge r = 0 \longrightarrow (\forall j.0 \leq j < i \longrightarrow a[j] \leq a[r])$ ✓
1.2 $0 < n \wedge i = 0 \wedge r = 0 \longrightarrow 0 \leq r < n$ ✓
1.3 $0 < n \wedge i = 0 \wedge r = 0 \longrightarrow 0 \leq i \leq n$ ✓

2.1 $(\forall j.0 \leq j < i \longrightarrow a[j] \leq a[r]) \wedge 0 \leq i \leq n \wedge 0 \leq r < n \wedge \neg(i \neq n) \longrightarrow (\forall j.\, 0 \leq j < n \longrightarrow a[j] \leq a[r])$ ✓
2.2 $(\forall j.0 \leq j < i \longrightarrow a[j] \leq a[r]) \wedge 0 \leq i \leq n \wedge 0 \leq r < n \wedge \neg(i \neq n) \longrightarrow 0 \leq r < n$ ✓

3.1 $(\exists R_0.((\forall j.0 \leq j < r \longrightarrow a[j] \leq a[R_0]) \wedge 0 \leq r < n \wedge 0 \leq R_0 < n \wedge a[R_0] < a[r]) \wedge i = r + 1)$
$\longrightarrow (\forall j.0 \leq j < i \longrightarrow a[j] \leq a[r])$ ✓
3.2 $(\exists I_0.(\forall j.0 \leq j < I_0 \longrightarrow a[j] \leq a[r]) \wedge 0 \leq I_0 < n \wedge 0 \leq r < n \wedge a[I_0] \leq a[r] \wedge i = I_0 + 1)$
$\longrightarrow (\forall j.0 \leq j < i \longrightarrow a[j] \leq a[r])$ ✓
3.3 $(\exists R_0.(\forall j.0 \leq j < r \longrightarrow a[j] \leq a[R_0]) \wedge 0 \leq r < n \wedge 0 \leq R_0 < n \wedge a[R_0] < a[r]) \wedge i = r + 1$
$\longrightarrow 0 \leq i \leq n$ ✓
3.4 $(\exists I_0.(\forall j.0 \leq j < I_0 \longrightarrow a[j] \leq a[r]) \wedge 0 \leq I_0 < n \wedge 0 \leq r < n \wedge a[I_0] \leq a[r] \wedge i = I_0 + 1)$
$\longrightarrow 0 \leq i \leq n$ ✓
3.5 $(\exists R_0.(\forall j.0 \leq j < r \longrightarrow a[j] \leq a[R_0]) \wedge 0 \leq r < n \wedge 0 \leq R_0 < n \wedge a[R_0] < a[r]) \wedge i = r + 1$
$\longrightarrow 0 \leq r < n$ ✓
3.6 $(\exists I_0.(\forall j.0 \leq j < I_0 \longrightarrow a[j] \leq a[r]) \wedge 0 \leq I_0 < n \wedge 0 \leq r < n \wedge a[I_0] \leq a[r] \wedge i = I_0 + 1)$
$\longrightarrow 0 \leq r < n$ ✓

Zusammenfassung

- Die Regeln des Floyd-Hoare-Kalküls sind **symmetrisch**: die Zuweisungsregel gibt es“rückwärts” und “vorwärts”.
- Dual zu Beweis und Verifikationsbedingung rückwärts gibt es Regel und Verifkationsbedingungen vorwärts.
- Bis auf die Invarianten an Schleifen können wir Korrektheit automatisch prüfen.
- Kern der Vorwärtsberechnung ist die Zuweisungsregel nach Floyd.
- Vorwärtsberechnung erzeugt kleinere Terme, ist aber umständlicher zu handhaben.
- Rückwärtsberechnung ist einfacher zu handhaben, erzeugt aber (tendenziell sehr) große Terme.

Korrekte Software: Grundlagen und Methoden
Vorlesung 11 vom 28.06.22
Funktionen und Prozeduren I

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2022

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Funktionen & Prozeduren

- **Funktionen** sind das zentrale Modularisierungskonzept von C
  - Kleinste Einheit
  - NB. Prozeduren sind nur Funktionen vom Typ **void**
- In objektorientierten Sprachen: Methoden
  - Funktionen mit (implizitem) erstem Parameter **this**
- Wie behandeln wir Funktionen?

Beispiel: Rekursion

Fakultät

```
// {N == n ∧ 0 ≤ n}
p= 1;
while (0< n)
  /** inv p == (N–n)! ∧ 0≤ n; */ {
  p= p* n;
  n= n–1;
  }
// {p == N!}
```

Verkapselt als Funktion

```
int factorial(int n)
/** pre  0≤ n;
    post \result == n!; */
{
 int p;
 p= 1;
 while (0< n)
   /** inv p == (n@pre–n)! ∧
0≤ n; */ {
   p= p* n;
   n= n–1;
   }
 return n;
}
```

- **Spezifikation** mit Vor-/Nachbedingung
- Keine logischen Variablen nötig, **\result**für Ergebnis
- Lokale Variablen, von außen nicht sichtbar (scoping)

Modellierung und Spezifikation von Funktionen

Wir brauchen:

1. Von Anweisungen zu Funktionen: Deklarationen und Parameter
2. Semantik von Funktionsdefinitionen
3. Spezifikation von Funktionsdefinitionen
4. Beweisregeln für Funktionsdefinitionen
5. Semantik des Funktionsaufrufs
6. Beweisregeln für Funktionsaufrufe

Von Anweisungen zu Funktionen

- Erweiterung unserer Kernsprache um Funktionsdefinition und Deklarationen:

$$
\begin{aligned}
\textbf{FunDef} &::= \textbf{FunHeader FunSpec}^{+}\ \textbf{Blk}\\
\textbf{FunHeader} &::= \textbf{Type Idt}(\textbf{Decl}^{*})\\
\textbf{Decl} &::= \textbf{Type Idt}\\
\textbf{Blk} &::= \{\textbf{Decl}^{*}\ \textbf{Stmt}\}\\
\textbf{Type} &::= \textbf{void} \mid \textbf{char} \mid \textbf{int} \mid \textbf{Struct} \mid \textbf{Array}\\
\textbf{Struct} &::= \textbf{struct}\ \ \textbf{Idt}^{?}\ \{\textbf{Decl}^{+}\}\\
\textbf{Array} &::= \textbf{Type Idt}[\textbf{Aexp}]
\end{aligned}
$$

- Abstrakte Syntax
- Größe von Feldern: **konstanter** Ausdruck
- **FunSpec** wird später erläutert

Rückgaben

Neue Anweisungen: Return-Anweisung

$$
\begin{aligned}
\textbf{Stmt} \qquad & s ::= l = e \mid c_1; c_2 \mid \{\,\} \mid \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2\\
& \mid \textbf{while}\ (b)\ /{**}\ \textbf{inv}\ P\ {*}/\ c \mid /{**}\ \{P\}\ {*}/\\
& \mid \textbf{return}\ a^{?}
\end{aligned}
$$

Rückgabewerte

- Problem: **return** bricht sequentiellen Kontrollfluss:

```
if (x == 0) return –1;
y = y / x;      // Wird nicht immer erreicht
```

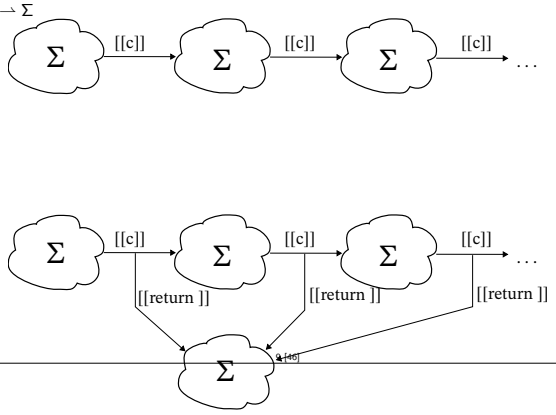
- Lösung 1: verbieten!
  - MISRA-C (Guidelines for the use of the C language in critical systems):

> Rule 14.7 (required)
> A function shall have a single point of exit at the end of the function.

  - Nicht immer möglich, unübersichtlicher Code ...
- Lösung 2: Erweiterung der Semantik

Denotationale Semantik der return-Anweisung

- Alt: $\Sigma \rightharpoonup \Sigma$



- **Neu**: $\Sigma \rightharpoonup (\Sigma + \Sigma \times \mathbf{V})$

Erweiterte Semantik

- Denotat einer Anweisung: $\Sigma \rightharpoonup (\Sigma \cup \Sigma \times \mathbf{V})$ $\Sigma \rightharpoonup (\Sigma \cup \Sigma \times \mathbf{V}_U)$
- Abbildung von Ausgangszustand Σ auf:
  - Sequentieller **Folgezustand** oder **Rückgabewert** und **Rückgabezustand**;
  - Σ und $\Sigma \times \mathbf{V}$ sind **disjunkt**.
- Was ist mit **void**?
  - **Erweiterte Werte**: $\mathbf{V}_U \stackrel{def}{=} \mathbf{V} + \{*\}$

Komposition mit Rückgabewerten

- Komposition zweier Anweisungen $f, g : \Sigma \rightharpoonup (\Sigma \cup \Sigma \times \mathbf{V}_U)$.
- Im Allgemeinen: Wenn $f, g : A \rightharpoonup A + B$ dann $g \circ_S f : A \rightharpoonup A + B$:

$$g \circ_S f(\sigma) \stackrel{def}{=} \begin{cases} g(a') & f(a) = a' \\ (a', b) & f(a) = (a', b) \end{cases}$$

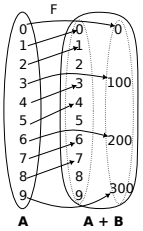
- Als Mengen: $f, g \subseteq (A \times (A + B)) \cong A \times A + A \times B$

$$g \circ_S f = \{(a, x) \mid \exists a' \in A.\, (a, a') \in f \wedge (a', x) \in g\} \cup \{(a, b) \mid (a, b) \in f, b \in B\}$$

- **Frage:** Ist das gleiche wie Komposition von partiellen Funktionen?

Arbeitsblatt 11.1: Komposition mit Rückgabewerten

Sei $\mathbf{A} = \{0, \ldots, 9\}$
$\mathbf{B} = \{0, 100, 200, 300\}$
Betrachte $F : \mathbf{A} \rightharpoonup \mathbf{A} + \mathbf{B}$



1. Wie ist die Funktion F links in Mengenschreibweise definiert?
2. Wie sind folgende Funktionen (als Mengen) definiert:
   $F_2 \stackrel{def}{=} F \circ_S F$?
   $F_3 \stackrel{def}{=} F \circ_S F \circ_S F$?
3. Was ist die **Bedeutung** von F_3?

Semantik von Anweisungen

$$[\![.]\!]_{\mathcal{C}} : \mathbf{Stmt} \to \Sigma \rightharpoonup (\Sigma \cup \Sigma \times \mathbf{V}_U)$$

$$[\![x = e]\!]_{\mathcal{C}} = \{(\sigma, \sigma[l \mapsto a]) \mid (\sigma, l) \in [\![x]\!]_{\mathcal{L}}, (\sigma, a) \in [\![e]\!]_{\mathcal{A}}\}$$
$$[\![c_1; c_2]\!]_{\mathcal{C}} = [\![c_2]\!]_{\mathcal{C}} \circ_S [\![c_1]\!]_{\mathcal{C}} \quad \text{Komposition wie oben}$$
$$[\![\{\,\}]\!]_{\mathcal{C}} = \mathbf{Id}_\Sigma \qquad \mathbf{Id}_\Sigma := \{(\sigma, \sigma) \mid \sigma \in \Sigma\}$$
$$[\![\textbf{if } (b) \ c_0 \ \textbf{else} \ c_1]\!]_{\mathcal{C}} = \{(\sigma, \rho') \mid (\sigma, \mathit{true}) \in [\![b]\!]_{\mathcal{B}} \wedge (\sigma, \rho') \in [\![c_0]\!]_{\mathcal{C}}\} \cup \{(\sigma, \rho') \mid (\sigma, \mathit{false}) \in [\![b]\!]_{\mathcal{B}} \wedge (\sigma, \rho') \in [\![c_1]\!]_{\mathcal{C}}\}$$
mit $\rho' \in \Sigma \cup \Sigma \times \mathbf{V}_U$
$$[\![\textbf{return } e]\!]_{\mathcal{C}} = \{(\sigma, (\sigma, a)) \mid (\sigma, a) \in [\![e]\!]_{\mathcal{A}}\}$$
$$[\![\textbf{return}]\!]_{\mathcal{C}} = \{(\sigma, (\sigma, *))\}$$

$$[\![\textbf{while } (b) \ c]\!]_{\mathcal{C}} = \mathit{fix}(\Gamma)$$
$$\Gamma(\psi) \stackrel{def}{=} \{(\sigma, \rho') \mid (\sigma, \mathit{true}) \in [\![b]\!]_{\mathcal{B}} \wedge (\sigma, \rho') \in \psi \circ_S [\![c]\!]_{\mathcal{C}}\} \cup \{(\sigma, \sigma) \mid (\sigma, \mathit{false}) \in [\![b]\!]_{\mathcal{B}}\}$$

Arbeitsblatt 11.2: Semantik mit Rückgabe

Berechnet die Denotate der folgenden Programme:

1. $$[\![x = 3; x = 4]\!]_{\mathcal{C}} = \textbf{?}$$
2. $$[\![x = 3; \textbf{return } x; x = 4]\!]_{\mathcal{C}} = \textbf{?}$$

Erweiterung des Floyd-Hoare-Kalküls

- Neue Semantik: $\mathbf{Stmt} \to \Sigma \rightharpoonup (\Sigma \cup \Sigma \times \mathbf{V}_U)$
- Wie passt das zu unseren Floyd-Hoare-Tripeln $\models \{P\}\, c\, \{Q\}$?
- Problem: Tripel behandel **einen** Nachzustand, jetzt haben wir **zwei** ...
- Lösung: **Erweiterung** des Tripels um eine explizite Nachbedingung für den **Rückgabezustand**

$$\models \{P\}\, c\, \{Q \mid Q_R\}$$

Erweiterung des Floyd-Hoare-Kalküls

$$[\![.]\!]_{\mathcal{C}} : \mathbf{Stmt} \to \Sigma \rightharpoonup (\Sigma \cup \Sigma \times \mathbf{V}_U)$$

Hoare-Tripel: zusätzliche Spezifikation für **Rückgabewert**.

Partielle Korrektheit ($\models \{P\}\, c\, \{Q \mid Q_R\}$)

c ist **partiell korrekt**, wenn für alle Zustände σ, die P erfüllen:

- die Ausführung von c mit σ in σ' regulär terminiert, so dass σ' die Spezifikation Q erfüllt,
- oder die Ausführung von c in σ' mit dem Rückgabewert v terminiert, so dass (σ', v) die Rückgabespezifikation Q_R erfüllt.

$$\models \{P\}\, c\, \{Q \mid Q_R\} \iff \forall \sigma.\, (\sigma, \mathit{true}) \in [\![P]\!]_{\mathcal{B}}\, \Gamma \wedge (\exists \sigma'.\, (\sigma, \sigma') \in [\![c]\!]_{\mathcal{C}} \implies (\sigma', \mathit{true}) \in [\![Q]\!]_{\mathcal{B}}) \vee (\exists \sigma', v.\, (\sigma, (\sigma', v)) \in [\![c]\!]_{\mathcal{C}} \implies (\sigma', \mathit{true}) \in [\![Q_R]\!]_{\mathcal{B}})$$

Erweiterung des Floyd-Hoare-Kalküls: return

$$\frac{}{\vdash \{Q\}\ \textbf{return}\ \{P \mid Q\}} \qquad \frac{}{\vdash \{Q[e/\backslash\textbf{result}]\}\ \textbf{return}\ e\ \{P \mid Q\}}$$

- Bei **return** wird die Rückgabespezifikation Q zur Vorbedingung, die reguläre Nachfolgespezifikation wird ignoriert, da die Ausführung von **return** kein Nachfolgezustand hat.
- **return** ohne Argument darf nur bei einer Nachbedingung Q auftreten, die kein **\result** enthält.
- Bei **return** mit Argument ersetzt der Rückgabewert den **\result** in der Rückgabespezifikation.

Zusammenfassung: Erweiterter Floyd-Hoare-Kalkül

$$\frac{}{\vdash \{P\}\,\{\}\,\{P \mid Q_R\}} \qquad \frac{\vdash \{P\}\,c_1\,\{R \mid Q_R\} \quad \vdash \{R\}\,c_2\,\{Q \mid Q_R\}}{\vdash \{P\}\,c_1; c_2\,\{Q \mid Q_R\}}$$

$$\frac{}{\vdash \{Q[e/x]\}\ l = e\,\{Q \mid Q_R\}} \qquad \frac{\vdash \{P \wedge b\}\,c\,\{P \mid Q_R\}}{\vdash \{P\}\ \textbf{while}\ (b)\ c\,\{P \wedge \neg b \mid Q_R\}}$$

$$\frac{\vdash \{P \wedge b\}\,c_1\,\{Q \mid Q_R\} \quad \vdash \{P \wedge \neg b\}\,c_2\,\{Q \mid Q_R\}}{\vdash \{P\}\ \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2\,\{Q \mid Q_R\}}$$

$$\frac{P \longrightarrow P' \quad \vdash \{P'\}\,c\,\{Q' \mid R'\} \quad Q' \longrightarrow Q \quad R' \longrightarrow R}{\vdash \{P\}\,c\,\{Q \mid R\}} \qquad \frac{}{\vdash \{Q\}\ \textbf{return}\ \{P \mid Q\}}$$

$$\frac{}{\vdash \{Q[e/\backslash\textbf{result}]\}\ \textbf{return}\ e\,\{P \mid Q\}}$$

Arbeitsblatt 11.3: Kurzbeispiel

Verifiziert folgendes Kurzbeispiel:

```
{  // {x = X}
   // ???
   x= x+1;
   // ???
   return x;
   // {false | \result == X + 1}
}
```


Lösungsblatt 11.3: Kurzbeispiel

```
{  // {x = X}
   // {x + 1 = X + 1}
   x= x+1;
   // {x = X + 1}
   return x;
   // {false | \result = X + 1}
}
```

Beweisverpflichtung:

$$x = X \Longrightarrow x + 1 = X + 1 \quad \checkmark$$

Approximative schwächste Vorbedingung

- Erweiterung zu $\text{awp}(c, Q, Q_R)$ und $\text{wvc}(c, Q, Q_R)$ analog zu der Erweiterung der Floyd-Hoare-Regeln.
  - Es wird immer eine **Rückgabespezifikation** Q_R benötigt.
- Es gilt:

$$\bigwedge \text{wvc}(c, Q, Q_R) \Longrightarrow \vdash \{\text{awp}(c, Q, Q_R)\}\ c\ \{Q \mid Q_R\}$$

Approximative schwächste Vorbedingung (Revisited)

$$\begin{aligned}
\text{awp}(\{\}, Q, Q_R) &\stackrel{def}{=} Q \\
\text{awp}(l = e, Q, Q_R) &\stackrel{def}{=} Q[e/l] \\
\text{awp}(c_1; c_2, Q, Q_R) &\stackrel{def}{=} \text{awp}(c_1, \text{awp}(c_2, Q, Q_R), Q_R) \\
\text{awp}(\textbf{if}\ (b)\ c_0\ \textbf{else}\ c_1, Q, Q_R) &\stackrel{def}{=} (b \wedge \text{awp}(c_0, Q, Q_R)) \vee (\neg b \wedge \text{awp}(c_1, Q, Q_R)) \\
\text{awp}(/{*}{*}\ \{q\}\ {*}/, Q, Q_R) &\stackrel{def}{=} q \\
\text{awp}(\textbf{while}\ (b)\ /{*}{*}\ \textbf{inv}\ i\ {*}/\ c, Q_R) &\stackrel{def}{=} i \\
\text{awp}(\textbf{return}\ e, Q, Q_R) &\stackrel{def}{=} Q_R[e/\backslash\textbf{result}] \\
\text{awp}(\textbf{return}, Q, Q_R) &\stackrel{def}{=} Q_R
\end{aligned}$$

Approximative Verifikationsbedingungen (Revisited)

$$\begin{aligned}
\text{wvc}(\{\}, Q, Q_R) &\stackrel{def}{=} \emptyset \\
\text{wvc}(l = e, Q, Q_R) &\stackrel{def}{=} \emptyset \\
\text{wvc}(c_1; c_2, Q, Q_R) &\stackrel{def}{=} \text{wvc}(c_1, \text{awp}(c_2, Q, Q_R), Q_R) \cup \text{wvc}(c_2, Q, Q_R) \\
\text{wvc}(\textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2, Q, Q_R) &\stackrel{def}{=} \text{wvc}(c_1, Q, Q_R) \cup \text{wvc}(c_2, Q, Q_R) \\
\text{wvc}(/{*}{*}\ \{q\}\ {*}/, Q, Q_R) &\stackrel{def}{=} \{q \Longrightarrow Q\} \\
\text{wvc}(\textbf{while}\ (b)\ /{*}{*}\ \textbf{inv}\ i\ {*}/\ c, Q, Q_R) &\stackrel{def}{=} \text{wvc}(c, i, Q_R) \cup \{i \wedge b \Longrightarrow \text{awp}(c, i, Q_R)\} \\
&\qquad \cup \{i \wedge \neg b \Longrightarrow Q\} \\
\text{wvc}(\textbf{return}\ e, Q, Q_R) &\stackrel{def}{=} \emptyset
\end{aligned}$$

Beispiel: Fakultät

```
1  {  // {0 ≤ n}
2     // {1 = (1 − 1)! ∧ 0 < 1}
3     p= 1;
4     // {p = (1 − 1)! ∧ 0 < 1}
5     c= 1;
6     // {p = (c − 1)! ∧ 0 < c}
7     while (1) /** inv p = (c− 1)! ∧ 0< c; */ {
8        p= p*c;
9        if (c == n) {
10          return p;
11       }
12       c= c+1;
13    }
14    // {false | \result == n!}
15 }
```

Beispiel: Fakultät (Beweisverpflichtungen I)

Unvereinfacht:

$$(1)\quad 0 \le n \longrightarrow 1 = (1-1)! \wedge 0 < 1$$
$$(3)\quad p = (c-1)! \wedge 0 < c \wedge \neg true \longrightarrow false$$

Vereinfacht:

$$(1.1)\quad 0 \le n \longrightarrow 1 = 0! \quad \checkmark$$
$$(1.2)\quad 0 \le n \longrightarrow 0 < 1 \quad \checkmark$$
$$(3)\quad false \longrightarrow false \quad \checkmark$$

Beispiel: Fakultät (Schleifenrumpf)

```
1
2   while (1) /** inv p = (c- 1)! ∧ 0< c; */ {
3     // {(c = n ∧ p · c = n!) ∨ (c ≠ n ∧ p · c = ((c + 1) − 1)! ∧ 0 < c + 1)}
4     p= p*c;
5     // {(c = n ∧ p = n!) ∨ (c ≠ n ∧ p = ((c + 1) − 1)! ∧ 0 < c + 1)}
6     if (c == n) {
7       // {p = n!}
8       return p;
9       // {p = ((c + 1) − 1)! ∧ 0 < c + 1 | \result == n!}
10      }
11    else {
12      // {p = ((c + 1) − 1)! ∧ 0 < c + 1}
13      }
14    // {p = ((c + 1) − 1)! ∧ 0 < c + 1}
15    c= c+1;
16    // {p = (c − 1)! ∧ 0 < c}
17    }
```


Beispiel: Fakultät (Beweisverpflichtung II)

Unvereinfacht:

$$(2)\quad p = (c-1)! \wedge 0 < c \wedge true \longrightarrow (c = n \wedge p \cdot c = n!) \vee (c \neq n \wedge p \cdot c = ((c+1)-1)! \wedge 0 < c+1)$$

Neue **Vereinfachungsregel**:

10. Disjunktionen folgender Form in der Konklusion können vereinfacht werden:
    - $P \longrightarrow (A \wedge B) \vee (C \wedge \neg B) \rightsquigarrow P \wedge B \longrightarrow A, P \wedge \neg B \longrightarrow C$

Damit Vereinfachung:

$$(2.1)\quad p = (c-1)! \wedge 0 < c \wedge c = n \longrightarrow p \cdot c = n! \quad \checkmark\ ((c-1)! \cdot c = c!)$$
$$(2.2)\quad p = (c-1)! \wedge 0 < c \wedge c \neq n \longrightarrow p \cdot c = c! \quad \checkmark\ ((c-1)! \cdot c = c!)$$
$$(2.3)\quad p = (c-1)! \wedge 0 < c \wedge c \neq n \longrightarrow 0 < c+1 \quad \checkmark\ (c < c+1)$$

Was fällt uns auf?

- Die Invariante ist $p = (c-1)! \wedge 0 < c$
- Da fehlt $c - 1 \le n$ — wie können wir $c - 1 = n$ am Ende beweisen?
- Mit der Schleifenbedingung 1 gilt **jede** Nachbedingung.
- Bei der Rückgabe ist $c == n$ — vereinfacht den Beweis.
- Essenziell: Schleife wird **nicht** verlassen.
- Nachbedigung *false* forciert dass Programm nur mit **return** verlassen wird.

Semantik von Funktionsdefinitionen

$$[\![.]\!]_{fd} : \mathbf{FunDef} \to \mathbf{V}^n \rightharpoonup \Sigma \rightharpoonup \Sigma \times \mathbf{V}_U$$

Das Denotat einer Funktion ist eine Anweisung, die über den tatsächlichen Werten für die Funktionsargumente parametriert ist.

$$[\![f(t_1\ p_1, t_2\ p_2, \ldots, t_n\ p_n)\ ds\ c]\!]_{fd}\ \Gamma\ v_1, \ldots, v_n = [\![\underbrace{(t_1\ p_1\ v_1, t_2\ p_2\ v_2, \ldots, t_n\ p_n\ v_n, ds)}_{\text{Deklarationen}}\ c]\!]_{blk}$$

- Die Funktionsargumente sind lokale Deklarationen, die mit den Aufrufwerten initialisiert werden.
  - Insbesondere können sie lokal in der Funktion verändert werden.
  - ... aber was ist die Semantik von Deklarationen?

Deklarationen und ihre Semantik

- Blöcke bestehen aus Deklaration und einem Rumpf — benötigen Semantik für Deklarationen
- Deklarationen erzeugen **lokale Variablen**
- Dadurch **Trennung** von Variablenname und Lokation (im Speicher)
- Vorher: $\mathbf{Idt} \longrightarrow \mathbf{V}$ jetzt: $\mathbf{Idt} \longrightarrow \mathbf{Loc} \longrightarrow \mathbf{V}$
- Nötig bspw. für Rekursion
- Was sind Lokationen?
  1. In C: Lokation ≅ Adressen $\longrightarrow$ Speichermodelle
  2. Hier: abstraktes Speichermodell

Abstraktes Speichermodell

- Der Systemzustand ist $\Sigma = \mathbf{Loc} \rightharpoonup \mathbf{V}$
- **Loc** ist eine Menge so dass
  - **Loc** ist unbegrenzt;
  - Es gibt Operationen:

$\nu : \Sigma \to \mathbf{Loc}$	$\nu(\sigma) \notin dom(\sigma)$	Neue Lokation
$rem : \Sigma \times \mathbf{Loc} \to \Sigma$	$l \notin dom(rem(\sigma, l))$	Deallokation

  - Ferner ist **Loc** abgeschlossen über:

$$l \in \mathbf{Loc}, i \in \mathbf{Idt} \Longrightarrow l.i \in \mathbf{Loc}$$
$$l \in \mathbf{Loc}, n \in \mathbb{Z} \Longrightarrow l[n]\mathbf{Loc}$$

Die Umgebung Γ

- **Umgebung**: **statischer** Teil des Speichers
- Wird zur **Laufzeit** nicht benötigt
- Bildet **Variablenbezeichner** auf Lokationen ab.
- Modelliert als **partielle Funktion**:

$$\mathbf{Env} = \mathbf{Idt} \rightharpoonup \mathbf{Loc}$$

  - Wird später noch erweitert.
- Umgebung ist **zusätzlicher Parameter** für alle Definitionen

Semantik von Deklarationen

- Zuerst: lokale Variablen.

$$\text{local} : (\mathbf{Loc} \to \Sigma \rightharpoonup \Sigma \times \mathbf{V}_U) \to \Sigma \rightharpoonup \Sigma \times \mathbf{V}_U$$
$$\text{local}(b) = \{(\sigma, (\mathit{rem}(\nu(\sigma), \sigma'), v)) \mid (\sigma, (\sigma', v)) \in b(\nu(\sigma))\}$$

- Neue Variable alloziieren, Block ausführen, Variable wieder deallokieren.
  - Ist nicht ganz korrekt: wir müssen neue Variable initialisieren (ggf. mit unbestimmten Wert), ansonsten wird sie nicht Teil von $\mathit{dom}(\sigma)$, dem Definitionsbereich von σ.
  - Gilt insbesondere für die Funktionsparameter, die mit dem aktuellen Wert des Funktion initialisiert werden.

Semantik von Blöcken

- Blöcke bestehen aus Deklarationen und einer Anweisung c:

$$[\![-]\!]_{blk} : \mathbf{Blk} \to \mathbf{Env} \to \Sigma \rightharpoonup \Sigma \times \mathbf{V}_U$$
$$[\![((\mathit{typ}\ \mathit{idt}) : \mathit{ds})\ c]\!]_{blk}\Gamma = \text{local}(\lambda l.\, [\![\mathit{ds}\ c]\!]_{blk}(\Gamma[\mathit{idt} \mapsto l]))$$
$$[\![[]\ c]\!]_{blk}\Gamma = \{(\sigma, (\sigma', v)) \mid (\sigma, (\sigma', v)) \in [\![c]\!]_C\Gamma\}$$

- Rekursive Definition (über der Liste der Deklationen)
- Semantik der Deklationen zusammen mit dem Rumpf.
- Von $[\![c]\!]_C$ sind nur **Rückgabezustände** interessant.
  - Kein „fall-through“
  - Was passiert ohne **return** am Ende?

Arbeitsblatt 11.4: Semantik mit Return

Gegeben folgende Funktion f:

```
int f(int y)
{
 int x;
 x= 7;
 if (y == 0) return x;
 x= x+4;
}
```

Was ist die denotationale Semantik von f?

$$[\![f]\!]_{fd} = ?\lambda v.\, \{(\sigma, \ldots) \mid \ldots\}$$

Spezifikation von Funktionen

- Wir **spezifizieren** Funktionen durch **Vor-** und **Nachbedingungen**
  - Ähnlich den Hoare-Tripeln, aber vereinfachte Syntax
  - **Behavioural specification**, angelehnt an JML, OCL, ACSL (Frama-C)
- Syntaktisch:

FunSpec ::= /** **pre** **Assn** **post** **Assn** */

Vorbedingung **pre** sp; $\quad \overbrace{\Sigma}^{\text{Vorzustand}} \to \mathbb{B}$

Nachbedingung **post** sp; $\quad \underbrace{\Sigma}_{\text{Vorzustand}} \times \underbrace{(\Sigma \times \mathbf{V}_U)}_{\text{Nachzustand und Return-Wert}} \to \mathbb{B}$

e**@pre** Wert von e im **Vorzustand**

\result **Rückgabewert** der Funktion

Beispiel: Fakultät

```
int fac(int n)
/** pre 0 ≤ n;
    post \result == n!};
 */
{
 int p;
 int c;

 p= 1;
 c= 1;
 while (c<= n) /** inv p == (c− 1)! ∧ 0≤ c ∧ c−1≤ n; */ {
    p= p∗c;
    c= c+1;
    }
 return p;
}
```


Arbeitsblatt 11.5: Suche

Spezifiziert die Suche nach dem maximalen Element:

```
int findmax(int a[], int a_len)
/** pre ???
    post ??? */
{
  int r; int j;

  j= 0;
  r= 0;
  while (j< a_len)
    /** inv (∀j. 0≤ j < i ⟶ a[j]≤ a[r])∧ 0≤ i≤ n ∧ 0≤ r< n; */
    {
    if (a[j]> x) { r= j; }
    j= j+1;
    }
  return r;
}
```


Gültigkeit von Spezifikationen

- Ziel ist eine **Semantik von Spezifikationen** $[\![.]\!]_{\mathcal{B}sp}$ zu definieren, um damit **semantische Gültigkeit** zu definieren:

$$\models \mathit{fd}\ \mathbf{pre}\ p\ \mathbf{post}\ q \iff (\forall v_1, \ldots, v_n.\, [\![P]\!]_{\mathcal{B}}\Gamma(\sigma) \implies [\![Q]\!]_{\mathcal{B}sp}\Gamma(\sigma, [\![\mathit{fd}]\!]_{fd}\Gamma(v_1 \ldots v_n)(\sigma)))$$

- Nicht ganz präzise wegen Partialität
- Spezifikationen beziehen sich nicht auf lokale Variablen (nur Parameter).
  - Nicht präzise, Parameter v_i müssen in Γ an die Namen gebunden werden.
- Nachbedingung wird in **Vor-** und **Nachzustand** ausgewertet.
- Kein Hoare-Tripel, aber wir können es zu einem machen:

$$\models \mathit{fd}\ \mathbf{pre}\ p\ \mathbf{post}\ q \iff$$
$$\forall v_1, \ldots, v_n, \sigma_0.\ \models \{\lambda\sigma.\, [\![P]\!]_{\mathcal{B}}\Gamma(\sigma) \wedge \sigma_0 = \sigma\}\ [\![\mathit{fd}]\!]_{blk}\Gamma(v_1, \ldots, v_n)\ \{\mathit{false} \mid \lambda\sigma.[\![Q]\!]_{\mathcal{B}sp}\Gamma(\sigma_0, \sigma)\}$$

Beispiel: Rekursion

```
int factorial(int n)
/** pre  0≤ n;
    post \result == n!; */
{
  int x;

  if (n == 0) {
    return 1;
    }
  else {
    x = factorial(n−1);
    return n ∗ x;
    }
}
```

Semantik von Spezifikationen

- Vorbedingung: Auswertung als $[\![sp]\!]_{\mathcal{B}}\,\Gamma$ über dem Vorzustand
- Nachbedingung: Erweiterung von $[\![.]\!]_{\mathcal{B}}$ und $[\![.]\!]_{\mathcal{A}}$
  - Ausdrücke können in Vor- **oder** Nachzustand ausgewertet werden.
  - \result darf nicht in Funktionen vom Typ **void** auftreten.

Semantik von Spezifikationen

$$[\![.]\!]_{\mathcal{B}sp} : \mathbf{Env} \to \mathbf{Assn} \rightharpoonup (\Sigma \times (\Sigma \times \mathbf{V}_U)) \to \mathbb{B}$$
$$[\![.]\!]_{\mathcal{A}sp} : \mathbf{Env} \to \mathbf{Aexpv} \rightharpoonup (\Sigma \times (\Sigma \times \mathbf{V}_U)) \to \mathbf{V}$$
$$[\![!b]\!]_{\mathcal{B}sp}\,\Gamma = \{((\sigma,(\sigma',v)),true) \mid ((\sigma,(\sigma',v)),false) \in [\![b]\!]_{\mathcal{B}sp}\Gamma\} \cup \{((\sigma,(\sigma',v)),false) \mid ((\sigma,(\sigma',v)),true) \in [\![b]\!]_{\mathcal{B}sp}\Gamma\}$$
$$[\![x]\!]_{\mathcal{A}sp}\,\Gamma = \{((\sigma,(\sigma',v)),\sigma'(x))\}$$
$$\ldots$$
$$[\![e\texttt{@pre}]\!]_{\mathcal{B}sp}\,\Gamma = \{((\sigma,(\sigma',v)),b) \mid (\sigma,b) \in [\![e]\!]_{\mathcal{B}}\,\Gamma\}$$
$$[\![e\texttt{@pre}]\!]_{\mathcal{A}sp}\,\Gamma = \{((\sigma,(\sigma',v)),a) \mid (\sigma,a) \in [\![e]\!]_{\mathcal{A}}\,\Gamma\}$$
$$[\![\backslash\texttt{result}]\!]_{\mathcal{A}sp}\,\Gamma = \{((\sigma,(\sigma',v)),v)\}$$

$$[\![\textbf{pre } p \textbf{ post } q]\!]_{\mathcal{B}sp}\,\Gamma = \{(\sigma,(\sigma',v)) \mid (\sigma,true) \in [\![p]\!]_{\mathcal{B}}\,\Gamma \wedge ((\sigma,(\sigma',v)),true) \in [\![q]\!]_{\mathcal{B}sp}\,\Gamma\}$$

Zusammenfassung

- Funktionsspezifikationen bestehen aus Vorbedingung (**pre**) und Nachbedingung (**post**).
- In der Nachbedingung kann ein Ausdruck mit e**@pre** im **Vorzustand** ausgewertet werden (ersetzt logische Variablen).
  - Funktionsparameter sind Parameter der Spezifikation, keine lokalen Variablen.
- Wir haben die **semantische Gültigkeit** von Funktionsspezfikationen definiert, und auf Hoare-Tripel zurückgeführt.
- Damit können wir die Regeln des Hoare-Kalküls zur Verifikation benutzen.

Verifikation

- Unterscheidung des Parameterwerts x von der lokalen Variablen x durch Notation x **@pre**
  - Im Vorzustand gilt x **@pre** $= x$.
  - Verhindert, dass der Parameter x bei der Zuweisung substituiert wird.
- Verifikationsregel:

$$\frac{P \wedge x_i = x_i\,\texttt{@pre} \Longrightarrow P' \quad \vdash \{P'\}\,c\,\{false \mid Q[x_i\,\texttt{@pre}/x_i]\}}{\vdash f(x_1,\ldots,x_n)/\!*\!*\ \text{pre } P \text{ post } Q\ *\!/\ \{ds\ c\}}$$

- Berechnung von awp und wvc:

$$\text{awp}(\Gamma, f(x_1,\ldots,x_n)/\!*\!*\ \text{pre } P \text{ post } Q\ *\!/\ \{ds\ c\}) \stackrel{def}{=} \text{awp}(\Gamma', c, false, Q[x_i\,\texttt{@pre}/x_i])$$
$$\text{wvc}(\Gamma, f(x_1,\ldots,x_n)/\!*\!*\ \text{pre } P \text{ post } Q\ *\!/\ \{ds\ c\}) \stackrel{def}{=} \{P \wedge x_i = x_i\,\texttt{@pre} \Longrightarrow P'\} \cup \text{wvc}(\Gamma', c, false, Q[x_i\,\texttt{@pre}/x_i])$$
$$\Gamma' \stackrel{def}{=} \Gamma[f \mapsto \forall x_1,\ldots,x_n.\,(P,Q)]$$
$$P' \stackrel{def}{=} \text{awp}(\Gamma', c, false, Q[x_i\,\texttt{@pre}/x_i])$$

Beispiel

Gegeben folgende kurze Funktion vom Arbeitsblatt 11.1:

```
int inc(int x)
/** pre true;
    post x< \result ; */
{ // {x@pre < x+1}
  x= x+1;
  // {x@pre < x}
  return x;
  // {false | x@pre < \result}
}
```

- Verifikationsbedingung:

$$(1)\ true \wedge x\,\texttt{@pre} = x \Longrightarrow x\,\texttt{@pre} < x+1 (1)\ x < x+1 \quad \checkmark$$

Zusammenfassung

- Funktionen können wir mit den Regeln des erweiterten Hoare-Kalküls verifizieren.
- Dabei ersetzen wir Funktionsparameter x in der Nachbedingung mit x **@pre**.
- Die dahinter liegenden weitgehenden Änderungen in der Semantik bleiben weitgehend unsichtbar.
- Probleme:
  - Felder als Parameter werden anders als in C behandelt (hier: wie in Java, in C: wie Referenzen).
  - Wie behandeln wir eigentlich **Funktionsaufrufe**?

Korrekte Software: Grundlagen und Methoden
Vorlesung 12 vom 05.07.22
Funktionen und Prozeduren II

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2022

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Modellierung und Spezifikation von Funktionen

Wir brauchen:

1. Von Anweisungen zu Funktionen: Deklarationen und Parameter ✓
2. Semantik von Funktionsdefinitionen ✓
3. Spezifikation von Funktionsdefinitionen ✓
4. Beweisregeln für Funktionsdefinitionen ✓
5. Semantik des Funktionsaufrufs
6. Beweisregeln für Funktionsaufrufe

Funktionsaufrufe und Rückgaben

Neue Ausdrücke und Anweisungen:

- Funktionsaufrufe
- Prozeduraufrufe (mit Zuweisung eines Rückgabewertes)

$$\begin{array}{rl}
\textbf{Aexp} & a ::= \mathbf{Z} \mid \mathbf{C} \mid \mathbf{Lexp} \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2 \mid a_1 / a_2 \\
\textbf{Bexp} & b ::= \mathbf{1} \mid \mathbf{0} \mid a_1 == a_2 \mid a_1 < a_2 \mid !\, b \mid b_1 \,\&\&\, b_2 \mid b_1 \,||\, b_2 \\
\textbf{Exp} & e := \mathbf{Aexp} \mid \mathbf{Bexp} \\
\textbf{Stmt} & c ::= l = e \mid c_1; c_2 \mid \{\,\} \mid \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2 \\
& \quad \mid \textbf{while}\ (b)\ /{*}{*}\ \textbf{inv}\ a\ {*}/\ c \mid /{*}{*}\ \{a\}\ {*}/ \\
& \quad \mid \textbf{Idt}(a^*) \\
& \quad \mid l = \textbf{Idt}(a^*) \\
& \quad \mid \textbf{return}\ a^?
\end{array}$$

Zur Erinnerung: Semantik von Funktionsdefinitionen

$$[\![.]\!]_{fd} : \mathbf{FunDef} \to \mathbf{Env} \to \mathbf{V}^n \rightharpoonup \Sigma \rightharpoonup \Sigma \times \mathbf{V}_U$$

- Das Denotat einer Funktion ist eine Anweisung, die über den tatsächlichen Werten für die Funktionsargumente parametriert ist.
  $[\![f(t_1\ p_1, t_2\ p_2, \ldots, t_n\ p_n)\ ds\ c]\!]_{fd}\ \Gamma\ v_1, \ldots, v_n = [\![(t_1\ p_1\ v_1, t_2\ p_2\ v_2, \ldots, t_n\ p_n\ v_n, ds)\ c]\!]_{blk}\ \Gamma$
- **Aufruf** der Funktion $f(e_1, \ldots, e_n)$ mit Argumenten $e_1, \ldots, e_n$:
  - **Auswertung** der Argumente $v_i = [\![e_i]\!]_{\mathcal{A}}$
  - Einsetzen in die **Semantik** $[\![f]\!]_{fd}(v_1, \ldots, v_n)$

Seiteneffekte bei Funktionsaufrufe

- Seiteneffekte:
  - Funktionen mit Seiteneffekten in zusammengesetzten Ausdrücken sind problematisch
  - In Java ist die Auswertungsreihenfolge fest (links nach rechts)
  - In C unspezifiziert (!)
- Deshalb keine Funktionen in zusammengesetzten Ausdrücken.
- Funktionsaufrufe nur in zwei Formen:
  - Als reine Prozeduren ($\textbf{Idt}(a^*)$ vom Typ **void**
  - Als direkte Zuweisung ($l = \textbf{Idt}(a^*)$) des Rückgabewertes
- Call by name, call by value, call by reference. . . ?

Arbeitsblatt 12.1: Funktionsaufrufe

Wie werden Parameter in folgenden Programmiersprachen übergeben?

- **C:**
- **Java**:
- **Haskell**:
- **Python**:
- **Other:** (specify)

Funktionsaufrufe

- Um eine Funktion f aufzurufen, müssen wir (statisch!) die Semantik der **Definition** von f dem Bezeichner f zuordnen.
- Aufruf einer nicht-definierten Funktion f oder mit falscher Anzahl n von Parametern ist nicht definiert
  - Muss durch **statische Analyse** verhindert werden
- Deshalb muss die **Umgebung** erweitert werden:

$$\mathbf{Env} = \mathbf{Idt} \rightharpoonup \mathbf{LocEnv} \qquad = \mathbf{Idt} \rightharpoonup (\mathbf{Loc} + (\mathbf{V}^N \rightharpoonup \Sigma \rightharpoonup (\Sigma \times \mathbf{V}_u)))$$

- Wir haben hier einen **Namensraum** für Funktionen und Variablen.

Semantik von Funktionsaufrufen

- Gegegeben Funktionsbezeichner f, Semantik ist

$$\Gamma(f) = \{(\underbrace{(v_1, \ldots, v_n)}_{\text{Parameterwerte}}, (\underbrace{\sigma}_{\text{Anfangszustand}}, \underbrace{(\sigma', a)}_{\text{Endzustand, Rückgabewert}}))\}$$

- Damit:

$$[\![f(t_1, \ldots, t_n)]\!]_C \Gamma = \{(\sigma, \sigma') \mid ((v_1, \ldots, v_n), \sigma, (\sigma', a)) \in \Gamma(f) \wedge (\sigma, v_i) \in [\![t_i]\!]_A \Gamma\}$$
$$[\![x = f(t_1, \ldots, t_n)]\!]_C \Gamma = \{(\sigma, \sigma'[x \mapsto a]) \mid ((v_1, \ldots, v_n), \sigma, (\sigma', a)) \in \Gamma(f) \wedge (\sigma, v_i) \in [\![t_i]\!]_A \Gamma\}$$

- Aufruf einer Prozedur $[\![f(t_1, \ldots, t_n)]\!]_C$ ignoriert Rückgabewert
  - Somit: Kombination mit Zuweisung
- Wir modellieren nur call-by-value.
  - C kennt nur call by value, allerdings sind Referenzen auch Werte (kommt noch)
  - Modellierung erlaubt Felder als Werte, im **Gegensatz** zu C.

Umgebung für den Kalkül

- Für Funktionsaufrufe gibt es eine **Umgebung**:

$$\mathbf{Env} = \mathbf{Idt} \rightharpoonup (\mathbf{Loc} + (\mathbf{V}^N \rightharpoonup \Sigma \rightharpoonup (\Sigma \times \mathbf{V}_u)))$$

- Deshalb muss für den Kalkül eine **Umgebung** Γ Funktionsbezeichnern ihre **Spezifikation** (Vor- und Nachbedingung, sowie Parameter) zuordnen:

$$\mathbf{Env}_{\text{fun}} = \mathbf{Idt} \rightharpoonup (\mathbf{Idt}^N \times \mathbf{Assn} \times \mathbf{Assn})$$

- $\Gamma(f) = \forall x_1, \ldots, x_n. (P, Q)$, für $f(x_1, \ldots, x_n)$/** pre P post Q */
- Korrektheit gilt immer nur im **Kontext** einer Umgebung, dadurch kann jede Funktion separat verifiziert werden (**Modularität**).
  - Umgebung wird zusätzliches Argument der Regeln.
  - Notation: $\Gamma \vdash \{P\}\, c\, \{Q \mid Q_R\}$.

Erweiterung des Floyd-Hoare-Kalküls: Aufruf

$$\frac{\Gamma(f) = \forall x_1, \ldots, x_n. (P, Q)}{\Gamma \vdash \{P[t_i/x_i] \wedge y_i \texttt{@pre} = y_i\}\; l = f(t_1, \ldots, t_n)\; \{Q[t_i/x_i][l/\backslash\texttt{result}] \mid Q_R\}}$$

- Γ muss f mit der Vor-/Nachbedingung P, Q enthalten
- In P und Q werden Parameter x_i durch Argumente t_i ersetzt.
- `\result` in Q wird durch l ersetzt
- Für alle Variablen y in Q, die mit y `@pre` referenziert werden, wird eine Gleichung $y = y$ `@pre` in die Vorbedingung eingefügt.
  - z.Zt. nur für global Variablen sinnvoll

Beispiel: die Fakultätsfunktion, rekursiv

```
1  int fac(int x)
2  /** pre  0 ≤ x;
3      post \result = x!; */
4  {
5   int r = 0;
6
7   // {(x = 0 ∧ 1 = x @pre!) ∨ (x ≠ 0 ∧ 0 ≤ x − 1)}
8   if (x == 0) {
9     // {1 = x @pre!}
10    return 1;
11    // {0 ≤ x − 1 | \result = x @pre!}
12    } else {
13    // {0 ≤ x − 1}
14    }
15  // {0 ≤ x − 1}
16  r = fac(x− 1);
17  // {r = (x − 1)!}
18  // {r · x = x @pre!}
19  return r* x;
20  // {false | \result = x @pre!}
21 }
```

Verifikationsbedingungen:

(1) $0 \le x \wedge x = x$ `@pre` $\longrightarrow (x = 0 \wedge 1 = x$ `@pre`$!) \vee (x \neq 0 \wedge 0 \le x - 1)$

(1.1) $0 \le x \wedge x = x$ `@pre` $\wedge x = 0 \longrightarrow 1 = x$ `@pre`$!$ ✓

(1.2) $0 \le x \wedge x = x$ `@pre` $\wedge x \neq 0 \longrightarrow 0 \le x - 1$ ✓

(2) $r = (x-1)! \longrightarrow r \cdot x = x$ `@pre`$!$

Problem: Beweis von (2) benötigt Voraussetzung $x = x$ `@pre`$!$

Beobachtungen

- Bei der Verifikation von f muss die Spezifikation von f Teil des Kontextes sein.
- Wir brauchen **gar keine** Invariante — ist durch die Nachbedingung gegeben
- Rekursion benötigt keine Extrabehandlung
  - Termination von rekursiven Funktionen wird extra gezeigt
- Der Aufruf einer Funktion **ersetzt** die momentane Nachbedingung — das ist ein Problem!

Frame Rule

- Konstanzregel (Rule of Constancy):

$$\frac{\Gamma \vdash \{P\}\, c\, \{Q \mid Q_R\}}{\Gamma \vdash \{P \wedge R\}\, c\, \{Q \wedge R \mid Q_R\}}$$

- Nebenbedingung:
  - c verändert keine Variablen in R, **oder**
  - für **keine** der Programm-Variablen x, die in R vorkommen, gibt es eine Zuweisung $x = \ldots$ in c
- Das ist eine **neue Regel**, die **bewiesen** werden muss.
- Schwierig zu handhaben bei Rückwärts/Vorwärtsrechung: R muss **annotiert** werden.

Funktionsaufrufe und Rückgaben

Neue Ausdrücke und Anweisungen:

- Funktionsaufrufe mit Zuweisung eines Rückgabewertes

$$\begin{aligned}
\textbf{Stmt}\ c ::= {} & l = e \mid c_1; c_2 \mid \{\,\} \mid \textbf{if}\ (b)\ c_1\ \textbf{else}\ c_2 \\
\mid {} & \textbf{while}\ (b)\ /{*}{*}\ \textbf{inv}\ a\ {*}/\ c \mid /{*}{*}\ \{a\}\ {*}/ \\
\mid {} & \textbf{Idt}(a^*) \\
\mid {} & /{*}{*}\ \textbf{const}\ R\ {*}/\ l = \textbf{Idt}(a^*) \\
\mid {} & \textbf{return}\ a^?
\end{aligned}$$

Approximative schwächste Vorbedingung & Verifikationsbedingung

Sei $\Gamma(f) = \forall x_1, \ldots, x_n. (P, Q)$

$$\text{awp}(\Gamma, /{*}{*}\ \textbf{const}\ R\ {*}/ l = f(t_1, \ldots, t_n), U, U_R) \stackrel{def}{=} R \wedge P[t_i/x_i] \quad \text{wenn } l \notin FV(R)$$

$$\text{wvc}(\Gamma, /{*}{*}\ \textbf{const}\ R\ {*}/ l = f(t_1, \ldots, t_n), U, U_R) \stackrel{def}{=} \{R \wedge Q[t_i/x_i][l/\backslash\texttt{result}] \longrightarrow U\} \quad \text{wenn } l \notin FV(R)$$

Beispiel: die Fakultätsfunktion

```
1  int fac(int x)
2  /** pre   0 ≤ x;
3      post  \result = x!; */
4  {
5   int r = 0;
6
7   // {(x = 0 ∧ 1 = x@pre!) ∨ (x ≠ 0 ∧ 0 ≤ x − 1 ∧ x = x@pre)}
8   if (x == 0) {
9     // {1 = x@pre!}
10    return 1;
11    // {0 ≤ x − 1 ∧ x = x@pre | \result = x@pre!}
12    } else {
13    // {0 ≤ x − 1 ∧ x = x@pre}
14    }
15  // {0 ≤ x − 1 ∧ x = x@pre}
16  /** const x= x@pre */ r = fac(x− 1);
17  // {r · x = x@pre!}
18  return r* x;
19  // {false | \result = x@pre!}
20 }
```

Verifikationsbedingungen:

(1) $0 \le x \wedge x = x\,@pre \longrightarrow (x = 0 \wedge 1 = x\,@pre!) \vee (x \neq 0 \wedge 0 \le x - 1 \wedge x = x\,@pre)$

(1.1) $0 \le x \wedge x = x\,@pre \wedge x = 0 \longrightarrow 1 = x!$ ✓

(1.2) $0 \le x \wedge x = x\,@pre \wedge x \neq 0 \longrightarrow 0 \le x - 1$ ✓

(1.3) $0 \le x \wedge x = x\,@pre \wedge x \neq 0 \longrightarrow x = x\,@pre$ ✓

(2) $x = x\,@pre \wedge r = (x-1)! \longrightarrow r \cdot x = x\,@pre!$ ✓

Arbeitsblatt 12.2: Fakultät endrekursiv

Hier nochmal die Fakultät (endrekursiv und buggy):

```
int factorial(int n)
/** pre ???;
    post ???; */
{
  int f;

  f= fact(0, n);
  return f;

}

int fact(int acc, int n)
/** pre ???;
    post ???; */
{
  int r;

  if (n == 0) return 1;
  r= fact(acc* n, n−1);
  return r;
}
```

1. Annotiert das Programm mit Vor/Nachbedingungen.
2. Findet und berichtigt die Fehler.
3. Berechnet die Verifikationsbedingungen.
4. Beweist die Verifikationsbedingungen.

Arbeitsblatt 12.3: Binäre Produke

Das Binärprodukt, rekursiv:

```
int binprod(int m, int n)
/** pre ?;
    post ?;
 */
{
  int r;

  if (n == 0) return 0;
  r= binprod(2* m, n/2);
  return r+ m*(n%2);
}
```

1. Annotiert das Programm mit Vor/Nachbedingungen
2. Berechnet die Verifikationsbedingungen
3. Beweist die Verfiktionsbedingungen

Arbeitsblatt 12.3: Binäre Produke

Das Binärprodukt, rekursiv:

```
int binprod(int m, int n)
/** pre 0 ≤ n;
    post \result = m* n;
 */
{
  int r;

  if (n == 0) return 0;
  r= binprod(2* m, n/2);
  return r+ m*(n%2);
}
```

1. Annotiert das Programm mit Vor/Nachbedingungen
2. Berechnet die Verifikationsbedingungen
3. Beweist die Verfikationsbedingungen

Zusammenfassung

- Funktionen sind **zentrales Modularisierungskonzept**
- Behandlung von Funktionen erfordert **vielfältige Erweiterungen**
- Erweiterung der **Semantik:**
  - Erweiterung der Semantik um **Rückgabezustand** $\Sigma \rightharpoonup (\Sigma \cup \Sigma \times \mathbf{V}_U)$
  - Die Semantik einer Funktion ist **parametrisiert** $\mathbf{V}^n \rightharpoonup \Sigma \rightharpoonup \Sigma \times \mathbf{V}_U$
- Erweiterung der **Spezifikationen:**
  - Spezifikation von Funktionen: **Vor-/Nachzustand** statt logischer Variablen
- Erweiterung des **Hoare-Kalküls**:
  - **Gesonderte Nachbedingung** für Rückgabewert/Endzustand
  - Aufruf einer Funktion **ersetzt** Vor/Nachbedingung, daher **Framing**
- **Einschränkungen**: nur call-by-value
- Fazit: **ohne Referenzen** sind Funktionen wenig brauchbar

Korrekte Software: Grundlagen und Methoden
Vorlesung 13 vom 12.07.22
Referenzen und Speichermodelle

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2022

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Motivation

- Warum Referenzen?
  - Nötig für *call by reference*
  - Funktionen können sonst nur **globale** Seiteneffekte haben
  - Effizienz
- Kurze Begriffsklärung:
  - Referenzen: getypt, eingeschränkte Arithmetik
  - Zeiger: ungetypt, Zeigerarithmetik

Refenzen in C

- Pointer in C ("pointer type"):
  - Schwach getypt (**void** $*$ kompatibel mit allen Zeigertypen, Typumwandlung)
  - Eingeschränkte Zeigerarithmetik (Addition, Subtraktion)
  - Felder werden durch Zeigerarithmetik implementiert
- Pointer sind *first-class-values*
- C-Standard läßt das Speichermodell relativ offen
  - Repräsentation von Objekten

Referenzen in anderen Sprachen

- Java:
  - (Fast) alles ist eine Referenz
  - Schwach getypt (Subtyping und Typumwandlung)
- Haskell, SML, OCaml:
  - Stark getypt (typsicher)
- Scriptsprachen (Python, Ruby):
  - Ähnlich Java

Ausdrücke

- Neue Operatoren: Addressoperator (&) und Derefenzierung ($*$)

$$
\begin{array}{rl}
\textbf{Lexp} & l ::= \textbf{Idt} \mid l[a] \mid l.\textbf{Idt} \mid *a \\
\textbf{Aexp} & a ::= \textbf{Z} \mid \textbf{C} \mid \textbf{Lexp} \mid \&l \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2 \mid a_1/a_2 \\
\textbf{Bexp} & b ::= \ldots \\
\textbf{Exp} & e := \textbf{Aexp} \mid \textbf{Bexp} \\
\textbf{Stmt} & c ::= \ldots \\
\textbf{Type} & t ::= \textbf{void} \mid \textbf{char} \mid \textbf{int} \mid *t \mid \textbf{struct}\ \textbf{Idt}^?\ \{\textbf{Decl}^+\} \mid t\ \textbf{Idt}[a]
\end{array}
$$

Das Problem mit Zeigern

- **Aliasing:** Verschiedene Bezeichner (**Lexp**) für die gleiche Lokation $l \in$ **Loc**

```
int a;
int *x;

x= &a;
a= 0;
// {a = 0}
*x= 7;
// {a = 7} (*)
```

- Wert von a ändert sich **ohne dass a erwähnt** wird.
- An der Stelle (*) zwei Bezeichner für die gleiche Lokation: a und $*$x
- Großes Problem für Semantik und Hoare-Kalkül.
- Modellierung der Zuweisung durch Substitution nicht mehr möglich

Erweiterung des Zustandmodells

- Bisheriger Zustand $\Sigma \stackrel{def}{=} \textbf{Loc} \rightharpoonup \textbf{V}$ mit
  - **Locations** (siehe Vorlesung 8)
  - Werte: $\textbf{V} = \mathbb{Z}$
- Ansatz reicht nicht mehr: Werte müssen auch Locations sein:

$$\textbf{V} \stackrel{def}{=} \mathbb{Z} + \textbf{Loc}$$

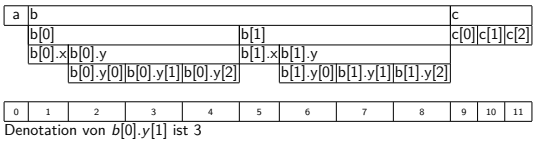
  und somit sind Zustände $\Sigma \stackrel{def}{=} \textbf{Loc} \rightharpoonup (\mathbb{Z} + \textbf{Loc})$
- Was ist die Semantik von **Loc**? $\longrightarrow$ Speichermodelle

Speichermodelle I: Compiler

Beispieldeklarationen:

```
int a;
struct {
  int x;
  int y[3]} b[2];
int c[3];
```

Übersetzung in konkretes **Speicherlayout**:



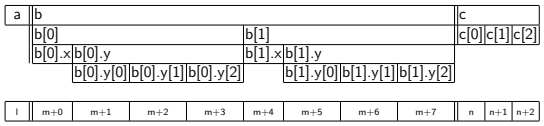
Denotation von $b[0].y[1]$ ist 3

Speichermodelle II: C-Standard

Beispieldeklarationen:

```
int a;
struct {
  int x;
  int y[3]} b[2];
int c[3];
```

Übersetzung in abstraktes **Speicherlayout**:



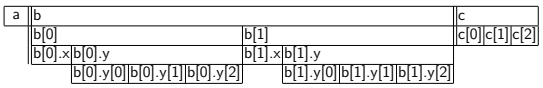
Denotation von $b[0].y[1]$ ist $m+3$, mit m **unbestimmte** Adresse

Speichermodelle III: Symbolisch

Beispieldeklarationen:

```
int a;
struct {
  int x;
  int y[3]} b[2];
int c[3];
```

Übersetzung in **symbolische Adressen**:



Denotation von $b[0].y[1]$ ist $m[0].y[1]$, mit m unbestimmte Adresse

Speichermodelle im Überblick

- Speichermodell I:
  - Ausführbar, aber **spezifisch** für Compiler und **Architektur**
  - Uneingeschränkte **Zeigerarithmetik**: **Loc** $= \mathbb{N}$
- Speichermodell II:
  - Spezifiziert durch den **Standard**
  - **Eingeschränkte** Form der **Zeigerarithmetik** $p + n$ mit p Zeiger, $n \in \mathbb{N}$
- Speichermodell III:
  - **Mischung** von Syntax und Semantik: $a.x$ kann L-Ausdruck, aber auch Location bezeichnen.

Arbeitsblatt 13.1: Jetzt mit Zeigern!

Hier eine weitere Folge von Deklarationen:

```
int *a[1];
struct {
  int p[2];
  struct {
    int x;
    int y; } q[2];
  } b;
```

- Skizziert hier das Speichermodell — konkret, abstrakt, symbolisch.
- Welches sind die jeweiligen Adressen (**Loc**)?
- Was sind die Denotationen für `a[1]`, `b.p[1]`, `b.q[0]`, `b.q[1].y`?
- Welche davon sind definiert/undefiniert?

Arbeitsblatt 13.2: Jetzt mit noch mehr Zeigern!

Hier eine weitere Folge von Deklarationen:

```
int *a[1];
struct {
  int p[2];
  struct {
    int x;
    int y; } *q[2];
  } b;
```

- Skizziert hier das Speichermodell — konkret, abstrakt, symbolisch.
- Welches sind die jeweiligen Adressen (**Loc**)?
- Was sind die Denotationen für `a[1]`, `b.p[1]`, `b.q[0]`, `(*b.q[1]).y`?
- Welche davon sind definiert/undefiniert?

Erweiterung der Semantik

- Problem: **Loc** haben unterschiedliche Semantik auf der linken oder rechten Seite einer Zuweisung.
  - `x = x+1` — Links: Addresse der Variablen, rechts: Wert an dieser Adresse
  - Einführung von Derefenzierung und Adressoperator verschärft dieses Problem
- Lösung in C: "Except when it is (...) the operand of the unary & operator, the left operand of the . operator or an assigment operator, an lvalue that does not have array type is converted to the value stored in the designated object (and is no longer an lvalue)" *C99 Standard*, §6.3.2.1 (2)
- Nicht spezifisch für C

Erweiterung der Semantik: Lexp

$$[\![-]\!]_{\mathcal{L}} : \mathbf{Env} \to \mathbf{Lexp} \to \Sigma \rightharpoonup \mathbf{Loc}$$

$$\begin{aligned}
[\![x]\!]^{\Gamma}_{\mathcal{L}} &= \{(\sigma, \Gamma(x)) \mid \sigma \in \Sigma\} \\
[\![m[a]]\!]^{\Gamma}_{\mathcal{L}} &= \{(\sigma, l[i]) \mid (\sigma, l) \in [\![m]\!]^{\Gamma}_{\mathcal{L}}, (\sigma, i) \in [\![a]\!]^{\Gamma}_{\mathcal{A}}\} \\
[\![m.f]\!]^{\Gamma}_{\mathcal{L}} &= \{(\sigma, l.f) \mid (\sigma, l) \in [\![m]\!]^{\Gamma}_{\mathcal{L}}\} \\
[\![*e]\!]^{\Gamma}_{\mathcal{L}} &= [\![e]\!]^{\Gamma}_{\mathcal{A}}
\end{aligned}$$

Erweiterung der Semantik: Aexp(1)

$$[\![-]\!]_{\mathcal{A}} : \mathbf{Env} \to \mathbf{Aexp} \to \Sigma \rightharpoonup \mathbf{V}$$

$$\begin{aligned}
[\![n]\!]^{\Gamma}_{\mathcal{A}} &= \{(\sigma, n) \mid \sigma \in \Sigma\} \quad \text{für } n \in \mathbb{N} \\
[\![e]\!]^{\Gamma}_{\mathcal{A}} &= \{(\sigma, v \mid (\sigma, l) \in [\![e]\!]^{\Gamma}_{\mathcal{L}}, (l, v) \in \sigma\} && e \in \mathbf{Lexp} \text{ und } e \text{ kein Array-Typ} \\
[\![e]\!]^{\Gamma}_{\mathcal{A}} &= \{(\sigma, l) \mid (\sigma, l) \in [\![e]\!]^{\Gamma}_{\mathcal{L}}\} && e \in \mathbf{Lexp} \text{ und } e \text{ ist Array-Typ} \\
[\![\&e]\!]^{\Gamma}_{\mathcal{A}} &= \{(\sigma, l) \mid (\sigma, l) \in [\![e]\!]^{\Gamma}_{\mathcal{L}}\} \quad [\![e]\!]^{\Gamma}_{\mathcal{L}}
\end{aligned}$$

- Es ist wichtig, die semantischen Funktionen $[\![e]\!]_{\mathcal{A}}$ und $[\![e]\!]_{\mathcal{L}}$ zu unterscheiden!

Erweiterung der Semantik: Aexp(2)

$$[\![-]\!]_{\mathcal{A}} : \mathbf{Env} \to \mathbf{Aexp} \to \Sigma \rightharpoonup \mathbf{V}$$

$$\begin{aligned}
[\![a_0 + a_1]\!]^{\Gamma}_{\mathcal{A}} &= \{(\sigma, n_0 + n_1) \mid (\sigma, n_0) \in [\![a_0]\!]^{\Gamma}_{\mathcal{A}} \wedge (\sigma, n_1) \in [\![a_1]\!]^{\Gamma}_{\mathcal{A}}\} \\
[\![a_0 - a_1]\!]^{\Gamma}_{\mathcal{A}} &= \{(\sigma, n_0 - n_1) \mid (\sigma, n_0) \in [\![a_0]\!]^{\Gamma}_{\mathcal{A}} \wedge (\sigma, n_1) \in [\![a_1]\!]^{\Gamma}_{\mathcal{A}}\} \\
[\![a_0 * a_1]\!]^{\Gamma}_{\mathcal{A}} &= \{(\sigma, n_0 \cdot n_1) \mid (\sigma, n_0) \in [\![a_0]\!]^{\Gamma}_{\mathcal{A}} \wedge (\sigma, n_1) \in [\![a_1]\!]^{\Gamma}_{\mathcal{A}}\} \\
[\![a_0 / a_1]\!]^{\Gamma}_{\mathcal{A}} &= \{(\sigma, n_0 \div n_1) \mid (\sigma, n_0) \in [\![a_0]\!]^{\Gamma}_{\mathcal{A}} \wedge (\sigma, n_1) \in [\![a_1]\!]^{\Gamma}_{\mathcal{A}} \wedge n_1 \neq 0\}
\end{aligned}$$

Beispiel

```
int a, *x;

*x= 5*a;
```

Gegeben folgende Werte, was ist die Semantik?

$$\Gamma \stackrel{def}{=} \langle a \mapsto l_1, x \mapsto l_2 \rangle$$
$$\sigma_1 \stackrel{def}{=} \langle l_1 \mapsto 10, l_2 \mapsto l_1 \rangle$$

$$\begin{aligned}
[\![*x = 5 * a]\!]^{\Gamma}_{\mathcal{C}}(\sigma_1) &= \sigma_1[[\![*x]\!]^{\Gamma}_{\mathcal{L}}(\sigma_1) \mapsto \sigma_1([\![5 * a]\!]^{\Gamma}_{\mathcal{A}}(\sigma_1))] \\
&= \sigma_1[[\![x]\!]^{\Gamma}_{\mathcal{A}}(\sigma_1) \mapsto \sigma_1([\![5]\!]^{\Gamma}_{\mathcal{A}}(\sigma_1) \cdot [\![a]\!]^{\Gamma}_{\mathcal{A}}(\sigma_1))] \\
&= \sigma_1[\sigma_1(\underbrace{[\![x]\!]^{\Gamma}_{\mathcal{L}}(\sigma_1)}_{\Gamma(x)}) \mapsto 5 \cdot \sigma_1(\underbrace{[\![a]\!]^{\Gamma}_{\mathcal{L}}}_{\Gamma(a)})] \\
&= \sigma_1[\sigma_1(l_2) \mapsto 5 \cdot \sigma_1(l_1)] \\
&= \sigma_1[l_1 \mapsto 5 \cdot 10] = \langle l_1 \mapsto 50, l_2 \mapsto l_1 \rangle
\end{aligned}$$

Arbeitsblatt 13.3: Pop-Quiz

Gegeben folgende Funktionen:

```
int f(int *x)
{
  int a;
  a= *x;
  *x= a+1;
  return a;
}
```

```
int a[3] = {0, 0, 0};
void g()
{
  int x= 1;
  a[x]= f(&x);
}
```

Was ist der Wert des Feldes `a` am Ende von `g`?

1. a == {0, 0, 1}
2. a == {0, 0, 2}
3. a == {0, 1, 0}
4. a == {0, 2, 0}

Korrektur der Semantik

- Das Pop-Quiz demonstriert den **Nichtdeterminismus** der C-Semantik.
  - Es ist **unbestimmt**, ob die linke oder rechte Seite der Zuweisung zuerst ausgewertet wird.
- Unsere Teilsprache soll den **deterministischen** Teil von C umfassen.
- Deshalb beim Funktionsaufruf mit Zuweisung links nur **zustandsfreie** Ausdrücke l:

$$\forall \sigma, \sigma'. [\![l]\!]^{\Gamma}_{\mathcal{L}}(\sigma) = [\![l]\!]^{\Gamma}_{\mathcal{L}}(\sigma')$$

- Gilt insbesondere für Bezeichner $l \in \mathbf{Idt}$, deshalb:

  Stmt $c ::= \ldots \mid \mathbf{Idt} = \mathbf{Idt}(a^*) \mid \ldots$

- Bei anderen Zuweisungen $l = e$ sind beide Seiten **zustandsabhängig**, aber frei von **Seiteneffekten**.

Arbeitsblatt 13.4: Kurze Semantik

Gegeben folgende Deklarationen:

```
struct p { int x;          int a;          struct p *q;
           int y; } p;
```

mit folgender Umgebung und Zustand

$$\Gamma \stackrel{def}{=} \langle p \mapsto l_1, a \mapsto l_2, q \mapsto l_3 \rangle, l_1 \neq l_2, \sigma_1 \stackrel{def}{=} \langle l_1.x \mapsto 3, l_1.y \mapsto 5, l_2 \mapsto 7, l_3 \mapsto l_1 \rangle$$

Berechnet die denotationale Semantik (erst für beliebige Zustände, dann für σ_1) von

$$[\![a = a + (*q).x]\!]^{\Gamma}_{\mathcal{C}} = ?$$
$$[\![a = a + (*q).x]\!]^{\Gamma}_{\mathcal{C}}(\sigma_1) = ?$$

Und jetzt?

- Zustand erweitert, so dass wir Zeiger modellieren können.
- Semantik entsprechend erweitert.
- Was machen wir mit dem Hoare-Kalkül, speziell der **Zuweisung**?
- Vorherige Modellierung — Zuweisung durch Substitution modelliert — nicht mehr ausreichend.
- Daher: **explizite Zustandsprädikate**

Explizite Zustandsprädikate

- Zusicherungenen (**Assn**) sind zustandsabhängige Prädikate
  - Mit anderen Worten, Prädikate über Programmvariablen.
- Axiomatische Beschreibung des Zustandes erforderte neue Modellierung auf der Ebene der Prädikate
- Explizite Zustandsprädikate modellieren das Lesen und die Änderung des Zustandes **explizit** mit Operationen read und upd.

Explizite Zustandsprädikate

- Enthalten keine $*$ oder &, und unterscheiden **strikt** zwischen **Lexp** und **Aexp**.
- Erweiterung von **Aexpv** um read, neue Sorte **State** mit Operation upd:

  $\mathbf{Assn}_s$ $b ::= \mathbf{1} \mid \mathbf{0} \mid a_1 == a_2 \mid a_1 < a_2 \mid !\, b \mid b_1 \,\&\&\, b2 \mid \ldots$

  $\mathbf{Lexp}_s$ $l ::= \ldots \mid \cancel{*a}$

  $\mathbf{Aexp}_s$ $a ::= \mathrm{read}(S, l) \mid \mathbf{Z} \mid \mathbf{C} \mid \cancel{\dagger} \mid \cancel{\&l} \mid \ldots \mid e\,\mathbf{@pre} \mid \ldots$

  State $S ::= s \mid r \mid \mathrm{upd}(S, l, e)$
- Zustandsvariablen *StateVar*: aktueller Zustand s, Vorzustand r
- Im Gegensatz zur Semantik rechnen wir mit **symbolischen Namen**

Gleichungen für explizite Zustandsprädikate

- Für die Operationen read, updgelten folgende Gleichungen:

$$\forall l, v, \sigma.\ \mathrm{read}(\mathrm{upd}(\sigma, l, v), l) = v$$
$$\forall l, m, v, \sigma.\ l \neq m \Longrightarrow \mathrm{read}(\mathrm{upd}(\sigma, l, v), m) = \mathrm{read}(\sigma, m)$$
$$\forall l, v, w, \sigma.\ \mathrm{upd}(\mathrm{upd}(\sigma, l, v), l, w) = \mathrm{upd}(\sigma, l, w)$$
$$\forall l, m, v, w, \sigma.\ l \neq m \Longrightarrow \mathrm{upd}(\mathrm{upd}(\sigma, l, v), m, w) = \mathrm{upd}(\mathrm{upd}(\sigma, m, w), l, v)$$

- Diese Gleichungen sind **vollständig.**

Semantik expliziter Zustandsprädikate

- Semantik der expliziten Zustandsprädikate:

$$[\![.]\!]_{\mathcal{B}sp} : \mathbf{Env} \to \mathbf{Assn}_s \rightharpoonup (\Sigma \times (\Sigma \times \mathbf{V}_U)) \to \mathbb{B}$$
$$[\![.]\!]_{\mathcal{A}sp} : \mathbf{Env} \to \mathbf{Aexp}_s \rightharpoonup (\Sigma \rightharpoonup \mathbf{V})$$
$$[\![.]\!]_{\mathcal{L}sp} : \mathbf{Env} \to \mathbf{Lexp}_s \rightharpoonup (\Sigma \rightharpoonup \mathbf{Loc})$$

Hoare-Triple

- Floyd-Hoare-Tripel: $\Gamma \models \{P\}\, c\, \{Q \mid R\}$ mit $P, Q, R \in$ **Assn Prädikate**
- Floyd-Hoare-Kalkül: $\Gamma \vdash \{P\}\, c\, \{Q \mid R\}$ mit $P, Q, R \in \mathbf{Assn}_s$ **explizite Zustandsprädikate**
- Wir brauchen also eine Übersetzung **Assn** nach $\mathbf{Assn}_s$ welche die Semantik erhält:

$$(-)^\dagger : \mathbf{Lexp} \to \mathbf{Lexp}_s \qquad (-)^\# : \mathbf{Aexpv} \to \mathbf{Aexp}_s \qquad (-)^* : \mathbf{Assn} \to \mathbf{Assn}_s$$
$$\forall l \in \mathbf{Lexp}.\ [\![l]\!]^\Gamma_{\mathcal{L}} = [\![l^\dagger]\!]^\Gamma_{\mathcal{L}sp} \qquad \forall a \in \mathbf{Aexpv}.\ [\![a]\!]^\Gamma_{\mathcal{A}} = [\![a^\#]\!]^\Gamma_{\mathcal{A}sp} \qquad \forall a \in \mathbf{Assn}.\ [\![a]\!]^\Gamma_{\mathcal{B}} = [\![a^*]\!]^\Gamma_{\mathcal{B}sp}$$

Konversion in explizite Zustandsprädikaten

Alte Zuweisungsregel

$$\frac{}{\Gamma \vdash \{Q[e/x]\}\, x = e\, \{Q \mid R\}}$$

Umwandlung von Q, x, e in Zustandsprädikate:

- Eine **Lexp** l auf der rechten Seite e wird durch $\mathrm{read}(\sigma, l)$ ersetzt.
- & dient lediglich dazu, diese Konversion zu **verhindern**.
- $*$ **erzwingt** diese Konversion, auch auf der linken Seite x.
- Beispiel: $*a = *\&b;$

Formal: Konversion in Zustandsprädikate

$(-)^\dagger : \mathbf{Lexp} \to \mathbf{Lexp}_s$

$i^\dagger = i \quad (i \in \mathbf{Idt})$

$l.id^\dagger = l^\dagger.id$

$l[e]^\dagger = l^\dagger[e^\#]$

$*l^\dagger = l^\#$

$(-)^\# : \mathbf{Aexp} \to \mathbf{Aexp}_s$

$e^\# = \mathrm{read}(s, e^\dagger) \quad (e \in \mathbf{Lexp})$

$n^\# = n$

$v^\# = v \quad (v$ logische Variable$)$

$(\&e)^\# = e^\dagger$

$(e_1 + e_2)^\# = {e_1}^\# + {e_2}^\#$

$\backslash\mathbf{result}^\# = \backslash\mathbf{result}$

$e\,\mathbf{@pre}^\# = e^\#[s/r]$

$(-)^* : \mathbf{Assn} \to \mathbf{Assn}_s$

$(\forall x.\ b)^* = \forall x.\ b^*$

$(b_1 \wedge b_2)^* = {b_1}^* \wedge {b_2}^*$

$(a_1 == a_2)^* = {a_1}^\# = {a_2}^\#$

$\vdots$

Angepasste Regeln des Hoare-Kalküls

$$\frac{}{\Gamma \vdash \{Q[\mathrm{upd}(s, x^\dagger, e^\#)/s]\}\, x = e\, \{Q \mid R\}}$$

- Beispiel 1: $(*x == 3)^*$ $= \mathrm{read}(s, (*x)^\dagger) = 3$
  $= \mathrm{read}(s, x^\#) = 3$
  $= \mathrm{read}(s, \mathrm{read}(s, x)) = 3$
- Beispiel 2: $\Gamma \vdash \{P\}\, x = \&\, a\, \{*x = 3 \mid R\}$
  $P = (\mathrm{read}(s, \mathrm{read}(s, x)) = 3)[\mathrm{upd}(s, x^\dagger, (\&\, a)^\#)/s]$
  $= (\mathrm{read}(s, \mathrm{read}(s, x)) = 3)[\mathrm{upd}(s, x, a^\dagger)/s]$
  $= \mathrm{read}(\mathrm{upd}(s, x, a), \mathrm{read}(\mathrm{upd}(s, \underline{x}, a), \underline{x})) = 3)$
  $= \mathrm{read}(\mathrm{upd}(s, \underline{x}, a), \underline{a}) = 3)$
  $= \mathrm{read}(s, a) = 3$
  $= (a == 3)^*$

Weitere geänderte Regeln

$$\frac{}{\Gamma \vdash \{Q[e^\#/\backslash\mathbf{result}]\}\ \mathbf{return}\ e\, \{P \mid Q\}}$$

$$\frac{\Gamma(f) = \forall x_1, \ldots, x_n.\ (P, Q)}{\Gamma \vdash \{P[{t_i}^\#/x_i] \wedge y_i\,\mathbf{@pre} = y_i\}\, l = f(t_1, \ldots, t_n)\, \{Q[{t_i}^\#/x_i][l^\#/\backslash\mathbf{result}] \mid Q_R\}}$$

$$\frac{\Gamma \vdash \{P^*\}\, c\, \{false \mid Q^*\}}{\Gamma \vdash f(x_1, \ldots, x_n)/{**}\ \mathrm{pre}\ P\ \mathrm{post}\ Q\ */\ \{ds\ c\}}$$

Rückwärtsrechnung mit Zeigern I

$$\mathrm{awp}(\Gamma, f(x_1,\ldots,x_n)/{*}{*}\ \mathrm{pre}\ P\ \mathrm{post}\ Q\ {*}/\ \{ds\ c\}) \stackrel{def}{=} \mathrm{awp}(\Gamma, c, \mathit{false}, Q^*[x_i\ \texttt{@pre}/x_i])$$
$$\mathrm{wvc}(\Gamma, f(x_1,\ldots,x_n)/{*}{*}\ \mathrm{pre}\ P\ \mathrm{post}\ Q\ {*}/\ \{ds\ c\}) \stackrel{def}{=} \{P^* \wedge x_i = x_i\ \texttt{@pre} \Longrightarrow P'\} \cup \mathrm{wvc}(\Gamma, c, \mathit{false}, Q^*[x_i\ \texttt{@pre}/x_i])$$
$$P' \stackrel{def}{=} \mathrm{awp}(\Gamma, c, \mathit{false}, Q^*[x_i\ \texttt{@pre}/x_i])$$

Sei $\Gamma(f) = \forall x_1,\ldots,x_n.\,(P, Q)$

$$\mathrm{awp}(\Gamma, /{*}{*}\ \texttt{const}\ R\ {*}/ I = f(t_1,\ldots,t_n), U, U_R) \stackrel{def}{=} R^* \wedge P^*[t_i{}^*/x_i], I \notin FV(R)$$
$$\mathrm{wvc}(\Gamma, /{*}{*}\ \texttt{const}\ R\ {*}/ I = f(t_1,\ldots,t_n), U, U_R) \stackrel{def}{=} \{R^* \wedge Q[t_i{}^*/x_i][I/\backslash\texttt{result}] \longrightarrow U\},\ I \notin FV(R)$$

Approximative schwächste Vorbedingung mit Zeigern II

$$\mathrm{awp}(\Gamma, \{\,\}, Q, Q_R) \stackrel{def}{=} Q$$
$$\mathrm{awp}(\Gamma, l = e, Q, Q_R) \stackrel{def}{=} Q[\mathrm{upd}(s, l^\dagger, e^\#)/s]$$
$$\mathrm{awp}(\Gamma, c_1; c_2, Q, Q_R) \stackrel{def}{=} \mathrm{awp}(\Gamma, c_1, \mathrm{awp}(c_2, Q, Q_R), Q_R)$$
$$\mathrm{awp}(\Gamma, \texttt{if}\ (b)\ c_0\ \texttt{else}\ c_1, Q, Q_R) \stackrel{def}{=} (b^* \wedge \mathrm{awp}(\Gamma, c_0, Q, Q_R)) \vee (\neg b^* \wedge \mathrm{awp}(c_1, Q, Q_R))$$
$$\mathrm{awp}(\Gamma, /{*}{*}\ \{q\}\ {*}/, Q, Q_R) \stackrel{def}{=} q^*$$
$$\mathrm{awp}(\Gamma, \texttt{while}\ (b)\ /{*}{*}\ \texttt{inv}\ i\ {*}/\ c, Q, Q_R) \stackrel{def}{=} i^*$$
$$\mathrm{awp}(\Gamma, \texttt{return}\ e, Q, Q_R) \stackrel{def}{=} Q_R[e^\#/\backslash\texttt{result}]$$
$$\mathrm{awp}(\texttt{return}, Q, Q_R) \stackrel{def}{=} Q_R$$

Approximative schwächste Vorbedingung mit Zeigern III

$$\mathrm{wvc}(\Gamma, \{\,\}, Q, Q_R) \stackrel{def}{=} \emptyset$$
$$\mathrm{wvc}(\Gamma, l = e, Q, Q_R) \stackrel{def}{=} \emptyset$$
$$\mathrm{wvc}(\Gamma, c_1; c_2, Q, Q_R) \stackrel{def}{=} \mathrm{wvc}(\Gamma, c_1, \mathrm{awp}(\Gamma, c_2, Q, Q_R), Q_R) \cup \mathrm{wvc}(\Gamma, c_2, Q, Q_R)$$
$$\mathrm{wvc}(\Gamma, \texttt{if}\ (b)\ c_1\ \texttt{else}\ c_2, Q, Q_R) \stackrel{def}{=} \mathrm{wvc}(\Gamma, c_1, Q, Q_R) \cup \mathrm{wvc}(\Gamma, c_2, Q, Q_R)$$
$$\mathrm{wvc}(\Gamma, /{*}{*}\ \{q\}\ {*}/, Q, Q_R) \stackrel{def}{=} \{q^* \Longrightarrow Q\}$$
$$\mathrm{wvc}(\Gamma, \texttt{while}\ (b)\ /{*}{*}\ \texttt{inv}\ i\ {*}/\ c, Q, Q_R) \stackrel{def}{=} \mathrm{wvc}(\Gamma, c, i^*, Q_R) \cup \{i^* \wedge b^* \Longrightarrow \mathrm{awp}(\Gamma, c, i^*, Q_R)\} \cup \{i^* \wedge \neg b^* \Longrightarrow Q\}$$
$$\mathrm{wvc}(\Gamma, \texttt{return}\ e, Q, Q_R) \stackrel{def}{=} \emptyset$$

Arbeitsblatt 13.5: Ein kurzes Beispiel

Betrachtet folgendes Beispiel:

```
void foo(){
 int x, y, z;
 x= 1;
 z= x;
 y= x;
 z= 5;
 // {0 < y}
}
```

1. Konvertiert das Prädikat $0 < y$ in ein explizites Zustandsprädikat.
2. Berechnet (rückwärts) die jeweils gültigen Zwischenzustände.
3. Vereinfacht nach jedem Schritt die Zwischenzustände.

Aliasing

- Das Beispiel mit Aliasing vom Anfang:

```
void foo(){
 int a, *x;

 /** { 5< 10 }
 /** { 5< read(upd(upd(upd(s, x, a), a, 0),                a     , 10), a) } */
 /** { 5< read(upd(upd(upd(s, x, a), a, 0), read(upd(s, x, a), x), 10), a) } */
 x= & a;
 /** { 5< read(upd(upd(s, a, 0), read(    s,        x), 10), a) } */
 /** { 5< read(upd(upd(s, a, 0), read(upd(s, a, 0), x), 10), a) } */
 a= 0;
 /** { 5< read(upd(s, read(s, x), 10), a) } */
 *x= 10;
 /** { 5< read(s, a) } */
}
```

- Aliasing wird korrekt behandelt.

Arbeitsblatt 13.6: Ein problematisches Beispiel

```
void foo(int *p)
/** post  \result  == 7; */
{
 int x;

 x= 7;
 *p= 99;
 return x;
}
```


Spezfikation des Speicherlayout

- Generelles Problem — was ist mit

```
void foo(int *p, int *q)
{ ... }
```

- Deutet auf ein Problem hin
- Entspricht einem "dangling pointer" (d.h. Pointer mit unspezifiziertem Wert)
- Können weder beweisen, dass $*p = *q$ noch $*p \neq *q$
- Muss (in den Vorbedingungen) spezifziert werden.
- Integration in die Logik: separation logic

Weitere Beispiele: Felder

```
int findmax(int a[], int a_len)
/** pre  0  \array (a, a_len) ∧ 0 < a_len;
     post ∀i. 0≤ i< a_len⟶a[i] ≤  \result ;
*/
{
 int x; int j;

 x= a[0]; j= 0;
 while (j< a_len)
   /** inv  (∀i. 0≤ i< j⟶a[i]≤ x ∧ 0≤ j< a_len */ {
   if (a[j]< a_len) {
    x= a[j];
    }
   j= j+1;
   }
 return x;
}
```

Felder und Zeiger revisited

- In C sind Zeiger und Felder schwach spezifiziert
- Insbesondere:
  - a[j]= *(a+j) für a Array-Typ
  - Derefenzierung von $*x$ nur definiert, wenn x "gültig" ist (d.h. auf ein Objekt zeigt) *C99 Standard*, §6.5.3.2(4)
- Bisher in den Hoare-Regeln ignoriert — **partielle** Korrektheit.
- Ist das sinnvoll? Nein, bekannte Fehlerquelle

Spezifikation von Zeigern und Feldern

Das Prädikat \valid(x)

$\backslash\mathbf{valid}(x) \iff \mathrm{read}(\sigma, x^\dagger)$ ist definiert

- Insbesondere: $\backslash\mathbf{valid}(*x) \iff \mathrm{read}(\sigma, \mathrm{read}(\sigma, x))$ ist definiert.
- Felder als Parameter werden zu Zeigern konvertiert, deshalb müssen wir spezifizieren können, dass ein Zeiger ein Feld ist.
- $\backslash\mathbf{array}(a, n)$ bedeutet: a ist ein Feld der Länge n, d.h.

$$\backslash\mathbf{array}(a, n) \iff (\forall i.\, 0 \le i < n \implies \backslash\mathbf{valid}(a[i]))$$

- Gültigkeit kann abgeleitet werden:

$$\frac{\text{x= \&e}}{\backslash\text{valid(*x)}} \qquad \frac{\backslash\text{array(a, n)} \quad 0 \le i \quad i < n}{\backslash\text{valid(a[i])}}$$

Was noch fehlt...

- **Vorwärtsrechung** mit expliziten Zustandsprädikaten.
  - Statt Existenzquantoren über Variablenwerte **unbestimmte Zwischenzustände** $\rho_1, \rho_2, \ldots$:

$$\frac{\rho_i \notin FV(P)}{\Gamma \vdash \{P\}\, x = e\, \{P[\rho_i/\sigma] \wedge \sigma = \mathrm{upd}(\rho_i, x^\dagger[\rho_i/\sigma], e^\#[\rho_i/\sigma]) \mid R\}}$$

  - Zwischenzustände sind **existenzquantifiziert**, d.h. das Prädikat gilt für **irgendeinen** Zustand ρ_i (aber für alle σ).
- Schwächste **Vorbedingung** und stärkste **Nachbedingung**:
  - Ergibt sich aus den Hoare-Regeln.
  - Erfordert durchgängige und agressive **Vereinfachung**.

Zusammenfassung

- Um Referenzen (Pointer) in C behandeln zu können, benötigen wir ein erweitertes **Zustandsmodell**
- Referenzen werden zu Werten wie Zahlen oder Zeichen.
  - Arrays und Strukturen sind **keine** first-class values.
  - Großes Problem: **aliasing**
- Erweiterung der Semantik und der Hoare-Tripel nötig:
  - Vor/Nachbedingungen werden zu **expliziten Zustandsprädikaten**.
  - Zuweisung wird zu **Zustandsupdate**.
  - Problem:
    - Zustände werden **sehr groß**
    - Rückwärtsrechnung erzeugt schnell sehr große „unbestimmte" Zustände, die nicht vereinfacht werden können
    - Hier ist Vorwärtsrechnung vorteilhaft

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Korrekte Software: Grundlagen und Methoden
Vorlesung 14 vom 21.07.21
Rückblick & Ausblick

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2022

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
- Funktionen und Prozeduren I
- Funktionen und Prozeduren II
- Referenzen und Speichermodelle
- Ausblick und Rückblick

Was gibt's heute?

- Rückblick
- Ausblick
- Feedback
- Prüfungsvorbereitung

I. Rückblick

Prüfungsrelevanz

- Was waren die **zentralen** theoretischen Konzepte?
- Wie sind sie formal definiert, was bedeuten sie?
- Wie hängen sie zusammen?

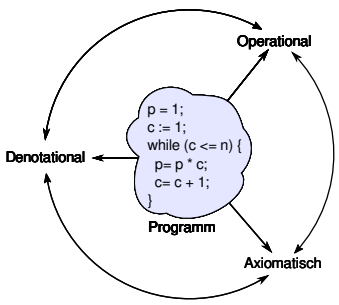
Semantik

- Operational — Auswertungsrelation $\langle c, \sigma\rangle \to \sigma'$
- Denotational — Partielle Funktion $[\![c]\!] : \Sigma \rightharpoonup \Sigma$
- Axiomatisch — Floyd-Hoare-Logik
- Welche Semantik wofür?
- Beweis: Äquivalenz von operationaler und denotationaler Semantik

Floyd-Hoare-Logik

- Floyd-Hoare-Logik: partiell und total
- $\vdash \{P\}\, c\, \{Q\}$ vs. $\models \{P\}\, c\, \{Q\}$: Vollständigkeit, Korrektheit
- Die sechs Basisregeln
- Zuweisungsregel: vorwärts (Floyd) vs. rückwärts (Hoare)
- VCG: Schwächste Vorbedingung und stärkste Nachbedingung
- Beweis: Korrektheit und Vollständigkeit der Floyd-Hoare-Logik

Zusammenhang der Semantiken



Erweiterungen der Programmiersprache

- Für jede Erweiterung:
  - Wie modellieren wir sie semantisch?
  - Wie ändern sich die Regeln der Logik?

1. Erweiterung der Programmiersprache

- Strukturen und Felder
  - Lokationen: strukturierte Werte **Lexp**
  - Erweiterte Substitution in Zuweisungsregel
  - Sonstige Regeln bleiben

2. Erweiterung der Programmiersprache

- Prozeduren und Funktionen
  - Modellierung von **return**: Erweiterung zu $\Sigma \rightharpoonup \Sigma + \Sigma \times \mathbf{V}_U$
  - Spezifikation von Funktionen durch Vor-/Nachbedingungen
  - Spezifikation der Funktionen muss im Kontext stehen
  - Unterscheidung zwischen zwei Nachbedingungen
  - Regeln für den Funktionsaufruf

3. Erweiterung der Programmiersprache

- Referenzen
  - Konversion zwischen **Lexp**und **Aexp**
  - Lokationen nicht mehr symbolisch (Variablennamen), sondern abstrakt $\Sigma = \mathbf{Loc} \rightharpoonup \mathbf{V}, \mathbf{V} = \mathbb{Z} + \mathbf{Loc}$
  - Zustand als **abstrakter Datentyp** mit Operationen read und upd
  - Zuweisung nicht mehr mit Substitution, sondern explizit durch upd
  - Spezifikationen sind **explizite Zustandsprädikate**, Konversion $(-)^\dagger, (-)^\#$

II. Ausblick

Was geht noch?

- Die Sprache C
- Andere Programmiersprachen
- Logik und Spezifikation
- Success Stories

Die Sprache C: Was haben wir ausgelassen?

Semantik:

- Nichtdeterministische Semantik: Seiteneffekte, Sequence Points
  $\longrightarrow$ Umständlich zu modellieren, Effekt zweitrangig
- Implementationsabhängiges, unspezifiziertes und undefiniertes Verhalten
  $\longrightarrow$ Genauere Unterscheidung in der Semantik

Kontrollstrukturen:

- **switch** $\longrightarrow$ Ist im allgemeinen Fall ein **goto**
- **goto**, setjmp/longjmp
  $\longrightarrow$ Allgemeinfall: tiefe Änderung der Semantik (*continuations*)

Die Sprache C: Was haben wir ausgelassen?

Typen:

- Funktionszeiger $\longrightarrow$ Für "saubere" Benutzung gut zu modellieren
- Weitere Typen: **short**/**long int**, **double**/**float**, wchar_t, und Typkonversionen $\longrightarrow$ Fleißarbeit
- Fließkommazahlen $\longrightarrow$ Spezifikation nicht einfach
- **union** $\longrightarrow$ Kompliziert das Speichermodell
- **volatile** $\longrightarrow$ Bricht read/update-Gleichungen
- **typedef** $\longrightarrow$ Ärgernis für Lexer/Parser, sonst harmlos

Die Sprache C: Was haben wir ausgelassen?

Für **realistische C-Programme**:

- Compiler-Erweiterungen (`gcc`, `clang`)
- Büchereien (Standardbücherei, Posix, ...)
- Nebenläufigkeit

Andere Sprachen: Wie modelliert man Java?

- Die **Kernsprache** ist ähnlich zu C0.
- Java hat erschwerend:
  - dynamische Bindung,
  - Klassen mit gekapselten Zustand und Invarianten,
  - Nebenläufigkeit, und
  - Reflektion.
- Java hat dafür aber
  - ein einfacheres Speichermodell, und
  - eine wohldefinierte Ausführungsumgebung (die JVM).

Andere Sprachen: Wie modelliert man C++?

- Sehr **vorsichtig** (konservativ)
- Viele Features, fehlende formale Semantik, ...
- Mehrfachvererbung theoretisch anspruchsvoll
- Es gibt **keine** Formalismen/Werkzeuge, die C++ voll unterstützen
- Ansätze: Übersetzung nach C/LLVM, Behandlung dort

Andere Sprachen: Wie modelliert man PHP?

Gar nicht.

Logik und Spezifikation

- Wir **generieren** Verifikationsbedingungen, wie kann man sie **beweisen**?
- **Automatische Beweiser:**
  - **SAT-Checker** lösen Erfüllbarkeitsproblem der Aussagenlogik (MiniSAT, Chaff)
  - **SMT-Beweiser** beweisen Aussagen der Prädikatenlogik mit linearer Arithmetik, Funktionen und Induktion (Z3, Yices, CVC)
- **Interaktive Beweiser:**
  - Beweisführung durch Benutzer, **Überprüfung** durch Beweiser
  - Sehr **mächtige** Logiken, aber nicht vollautomatisch (Isabelle, Coq, Lean)

Beispiel: Z3

- SMT-Beweiser versuchen Gegenbeweis zu konstruieren
- Daher: um ϕ zu beweisen, versuchen wir $\neg\Phi$ zu widerlegen

Beweis einer VC:
$x \geq 0 \wedge y > 0 \Longrightarrow x = 0 * y + x$

Input Z3:

```
(declare-const x Int)
(declare-const y Int)
(assert
   (not (=> (and (>= x 0) (> y 0))
            (= x (+ (* 0 y) x))))
)
(check-sat)
```

Antwort:

```
unsat
```

Unerfüllbare VC:
$x \geq 0 \wedge y > 0 \Longrightarrow x \geq y$

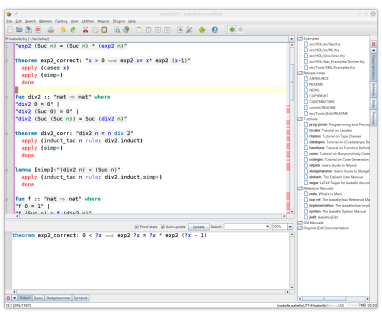
Input Z3:

```
(declare-const x Int)
(declare-const y Int)
(assert
   (not (=> (and (>= x 0) (> y 0))
            (>= x y)))
)
(check-sat)
```

Antwort:

```
sat
```


Beispiel: Isabelle



Korrekte Software in der Industrie

- Meist in speziellen Anwendungsgebieten: Luft-/Raumfahrt, Automotive, sicherheitskritische Systeme, Betriebssysteme
- Ansätze:
  1. Vollautomatisch: **statische Analyse** (Abstrakte Interpretation) für spezielle Aspekte: Freiheit von Ausnahmen und Unter/Überläufen, Programmsicherheit, Laufzeitverhalten (WCET) (nicht immer korrekt, meist vollständig)
     - Werkzeuge: `absint`
  2. Halbautomatisch: **Korrektheitsannotationen**, Überprüfung automatisch
     - Werkzeuge: Spark (ADA), Frama-C (C), JML (ESC/Java, Krakatao; Java), Boogie und Why (generisches VCG), VCC (C)
  3. Interaktiv: Einbettung der Sprache in interaktiven Theorembeweiser (Isabelle, Coq)
     - Beispiele: L4.verified, CompCert, SAMS

III. Prüfungsvorbereitung

Prüfungsvorbereitung

- Termine: 05./07.09.2022 (Anmeldung über stud.ip)
- Mündliche Modulprüfung, 20– 30 Minuten
- Schwerpunkte:
  - **Verständnis** des Stoffes, weniger Folien auswendig lernen
  - Zentrale theoretische Konzepte kennen und benennen
  - Stoff der Vorlesung und Übungsblätter, weniger eure Lösungen
- Bewertung
  - Sicherheit/Beherrschung des Stoffes
  - *covered ground*

IV. Feedback

Deine Meinung zählt

- Bitte die **Evaluation** auf stud.ip beantworten!
- Was war gut, was nicht?
- Arbeitsaufwand?
- Mehr **Theorie** oder mehr **Praxis**?
- Programmieraufgaben?
- Leichtgewichtiger Übungsbetrieb — mehr oder weniger?

Tschüß!