

Korrekte Software: Grundlagen und Methoden
Vorlesung 6 vom 14.05.17: Korrektheit der Floyd-Hoare-Logik

Serge Autexier, Christoph Lüth
Universität Bremen
Sommersemester 2017



Fahrplan

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

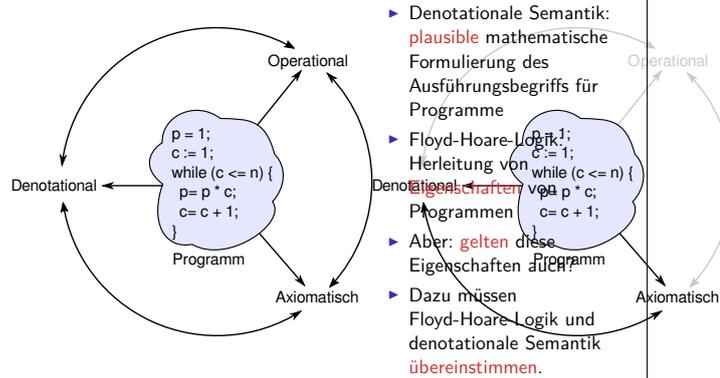


Motivation

- ▶ In den letzten Wochen: **Semantik**
- ▶ Warum?
 - ▶ Bedeutung von Programmen **mathematisch** präzise fassen,
 - ▶ um insbesondere die über die Korrektheit von **Programmen** zu reden.
- ▶ Fragen:
 1. Was **bedeutet** es, wenn ein Programm **korrekt** ist?
 2. Wie können wir das **beweisen**?



Was gibt es heute?



Denotationale Semantik

- ▶ Denotat eines Ausdrucks (Programms) ist partielle Funktion:

$$\mathcal{A}[-] : \mathbf{Aexp} \rightarrow \Sigma \rightarrow \mathbf{N}$$

$$\mathcal{B}[-] : \mathbf{Bexp} \rightarrow \Sigma \rightarrow \mathbf{T}$$

$$\mathcal{C}[-] : \mathbf{Stmt} \rightarrow \Sigma \rightarrow \Sigma$$

- ▶ $f : A \rightarrow B$, dann (\perp steht für "undefiniert"):

$$\text{def}(f(x)) \iff f(x) \neq \perp$$



Floyd-Hoare-Tripel: Gültigkeit und Herleitbarkeit

$P, Q \in \mathbf{Bexp}, c \in \mathbf{Stmt}$

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

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

Remember:

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

c ist **partiell korrekt**, wenn für alle Zustände σ , die P erfüllen: **wenn** die Ausführung von c mit σ in σ' terminiert, **dann** erfüllt $\sigma' Q$

Bezug zur Semantik?



Hoare-Tripel und denotationale Semantik

- ▶ Mit der denotationalen Semantik können wir die Gültigkeit von Hoare-Tripeln **formal** definieren.

- ▶ Notation: für $P \in \mathbf{Bexp}, \sigma \models P \iff \mathcal{B}[P](\sigma) = 1$

Gültigkeit von Hoare-Tripeln

$$\models \{P\} c \{Q\} \iff \forall \sigma \in \Sigma. \sigma \models P \wedge \text{def}(\mathcal{C}[c](\sigma)) \implies \mathcal{C}[c]\sigma \models Q$$

- ▶ Aber: $\models \{P\} c \{Q\} \stackrel{?}{\iff} \vdash \{P\} c \{Q\}$



Überblick: die Regeln des Floyd-Hoare-Kalküls

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

$$\frac{}{\vdash \{A\} \{ \{A\} \}}$$

$$\frac{\vdash \{A\} c \{B\} \quad \vdash \{B\} \{c_s\} \{C\}}{\vdash \{A\} \{c_s\} \{C\}}$$

$$\frac{\vdash \{A \wedge b\} c_0 \{B\} \quad \vdash \{A \wedge \neg b\} c_1 \{B\}}{\vdash \{A\} \text{if } (b) \text{ c}_0 \text{ else } c_1 \{B\}}$$

$$\frac{\vdash \{A \wedge b\} c \{A\} \quad A' \implies A \quad \vdash \{A\} c \{B\} \quad B \implies B'}{\vdash \{A\} \text{while}(b) c \{A \wedge \neg b\} \quad \vdash \{A'\} c \{B'\}}$$



Korrektheit und Vollständigkeit

► **Korrektheit:** $\vdash \{P\} c \{Q\} \stackrel{?}{\implies} \models \{P\} c \{Q\}$

► Wir können nur gültige Eigenschaften von Programmen herleiten.

► **Vollständigkeit:** $\models \{P\} c \{Q\} \stackrel{?}{\implies} \vdash \{P\} c \{Q\}$

► Wir können alle gültigen Eigenschaften auch herleiten.



Korrektheit der Floyd-Hoare-Logik

Floyd-Hoare-Logik ist korrekt.

Wenn $\vdash \{P\} c \{Q\}$, dann $\models \{P\} c \{Q\}$.

Beweis:

► Durch **strukturelle Induktion** über der **Herleitung** von $\vdash \{P\} c \{Q\}$

► Bsp: Sequenz, Zuweisung, Weakening, While.



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 der schwächsten Vorbedingung $wp(c, Q)$.

► 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 **Gültigkeit** von Hoare-Tripeln ist ein **semantisches** Konzept, und über die denotationale Semantik definiert.

► Das Verhältnis von denotationaler Semantik zur Floyd-Hoare-Logik ist also die Frage nach Korrektheit und Vollständigkeit.

► Floyd-Hoare-Logik ist **korrekt**, wir können nur gültige Zusicherungen herleiten.

► Floyd-Hoare-Logik ist **vollständig** bis auf das Weakening.

