Korrekte Software: Grundlagen und Methoden

Vorlesung 7 vom 25.05.21

Korrektheit des Floyd-Hoare-Kalküls

Serge Autexier, Christoph Lüth

Universität Bremen

Sommersemester 2021

Fahrplan

- Einführung
- Operationale Semantik
- Denotationale Semantik
- Äquivalenz der Operationalen und Denotationalen Semantik
- Der Floyd-Hoare-Kalkül I
- Der Floyd-Hoare-Kalkül II: Invarianten
- Korrektheit des Floyd-Hoare-Kalküls
- Strukturierte Datentypen
- Verifikationsbedingungen
- Vorwärts mit Floyd und Hoare
- Modellierung
- Spezifikation von Funktionen
- Referenzen und Speichermodelle
- Ausblick und Rückblick

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**: $\vdash \{P\}\, c\, \{Q\} \overset{?}{\rightsquigarrow} \models \{P\}\, c\, \{Q\}$

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**: $\vdash \{P\}\, c\, \{Q\} \overset{?}{\leftrightsquigarrow} \models \{P\}\, c\, \{Q\}$
- **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 $\models \{P\}\, c\, \{Q\}$:

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

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

Korrektheit der Zuweisung

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

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

$\iff \quad \forall I.\, \forall \sigma.\, \sigma \models^I P[e/x] \land \exists \sigma'.\, (\sigma, \sigma') \in [\![x = e]\!]_{\mathcal{C}} \Longrightarrow \sigma' \models^I P$

Korrektheit der Zuweisung

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

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

$\iff$ $\quad \forall I.\, \forall \sigma.\, \sigma \models^I P[e/x] \land \exists \sigma'.\, (\sigma, \sigma') \in [\![x = e]\!]_{\mathcal{C}} \Longrightarrow \sigma' \models^I P$

$\iff$ $\quad \forall I.\, \forall \sigma.\, \sigma \models^I P[e/x] \Longrightarrow \sigma([x \mapsto [\![e]\!]_{\mathcal{A}}(\sigma)]) \models^I P$

with $(\sigma, \sigma([x \mapsto [\![e]\!]_{\mathcal{A}}(\sigma)])) \in [\![x = e]\!]_{\mathcal{C}}$

Korrektheit der Zuweisung

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

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

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

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

$$\begin{aligned}
\sigma \models^I B[e/x] \Longleftrightarrow & \sigma[x \mapsto [\![e]\!]_{\mathcal{A}}(\sigma)] \models^I B \\
[\![a[e/x]]\!]^I_{\mathcal{A}\nu}(\sigma) = & [\![a]\!]^I_{\mathcal{A}\nu}(\sigma[x \mapsto [\![e]\!]^I_{\mathcal{A}\nu}(\sigma)])
\end{aligned}$$

Korrektheit der Sequenzenregel

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

Annahmen:

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

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

Zu zeigen:

$$\models \{A\}\, c_1; c_2\, \{C\}$$

Korrektheit der Sequenzenregel

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

Annahmen:

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

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

Zu zeigen:

$$\models \{A\}\, c_1; c_2\, \{C\} \Longleftrightarrow \forall I.\, \forall \sigma.\, \sigma \models^I A \land \exists \sigma'.\, (\sigma, \sigma') \in [\![c_1; c_2]\!]_{\mathcal{C}} \Longrightarrow \sigma' \models^I C$$

Korrektheit der Sequenzenregel

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

Annahmen:

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

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

Zu zeigen:

$$\models \{A\}\, c_1; c_2\, \{C\} \Longleftrightarrow \forall I.\, \forall \sigma.\, \sigma \models^I A \land \exists \sigma'.\, (\sigma, \sigma') \in [\![c_1; c_2]\!]_{\mathcal{C}} \Longrightarrow \sigma' \models^I C$$

$$(\sigma, \sigma') \in [\![c_1; c_2]\!]_{\mathcal{C}} \iff (\sigma, \sigma') \in [\![c_1]\!]_{\mathcal{C}} \circ [\![c_2]\!]_{\mathcal{C}}$$

$$\iff \exists \rho.\, (\sigma, \rho) \in [\![c_1]\!]_{\mathcal{C}} \land (\rho, \sigma') \in [\![c_2]\!]_{\mathcal{C}}$$

Korrektheit der Sequenzenregel

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

Annahmen:

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

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

Zu zeigen:

$$\models \{A\}\, c_1; c_2\, \{C\} \Longleftrightarrow \forall I.\, \forall \sigma.\, \sigma \models^I A \land \exists \sigma'.\, (\sigma, \sigma') \in [\![c_1; c_2]\!]_{\mathcal{C}} \Longrightarrow \sigma' \models^I C$$

$$(\sigma, \sigma') \in [\![c_1; c_2]\!]_{\mathcal{C}} \iff (\sigma, \sigma') \in [\![c_1]\!]_{\mathcal{C}} \circ [\![c_2]\!]_{\mathcal{C}}$$

$$\iff \exists \rho.\, (\sigma, \rho) \in [\![c_1]\!]_{\mathcal{C}} \land (\rho, \sigma') \in [\![c_2]\!]_{\mathcal{C}}$$

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

Korrektheit der Sequenzenregel

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

Annahmen:

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

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

Zu zeigen:

$$\models \{A\}\, c_1; c_2\, \{C\} \Longleftrightarrow \forall I.\, \forall \sigma.\, \sigma \models^I A \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![c_1; c_2]\!]_{\mathcal{C}} \Longrightarrow \sigma' \models^I C$$

$$(\sigma, \sigma') \in [\![c_1; c_2]\!]_{\mathcal{C}} \iff (\sigma, \sigma') \in [\![c_1]\!]_{\mathcal{C}} \circ [\![c_2]\!]_{\mathcal{C}}$$

$$\iff \exists \rho.\, (\sigma, \rho) \in [\![c_1]\!]_{\mathcal{C}} \wedge (\rho, \sigma') \in [\![c_2]\!]_{\mathcal{C}}$$

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

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

Korrektheit der Sequenzenregel

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

Annahmen:

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

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

Zu zeigen:

$$\models \{A\}\, c_1; c_2\, \{C\} \Longleftrightarrow \forall I.\, \forall \sigma.\, \sigma \models^I A \wedge \exists \sigma'.\, (\sigma, \sigma') \in [\![c_1; c_2]\!]_{\mathcal{C}} \Longrightarrow \sigma' \models^I C$$

$$(\sigma, \sigma') \in [\![c_1; c_2]\!]_{\mathcal{C}} \iff (\sigma, \sigma') \in [\![c_1]\!]_{\mathcal{C}} \circ [\![c_2]\!]_{\mathcal{C}}$$

$$\iff \exists \rho.\, (\sigma, \rho) \in [\![c_1]\!]_{\mathcal{C}} \wedge (\rho, \sigma') \in [\![c_2]\!]_{\mathcal{C}}$$

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

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

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:

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

- 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 $\mathrm{wp}(c_0; c_1, Q) := \mathrm{wp}(c_0, \mathrm{wp}(c_1, Q))$
  - $c \equiv$ **if** b c_0 **else** c_1: Wähle $\mathrm{wp}(c, Q) := (b \wedge \mathrm{wp}(c_0, Q)) \vee (\neg b \wedge \mathrm{wp}(c_1, Q))$
  - $c \equiv$ **while** (b) c_0: ??

Vollständigkeitsbeweis: while

- $c \equiv$ **while** $(b)\ c_0$:
  Wie müssen eine Formel finden (wp(**while** $(b)\ c_0, Q$)) die alle σ charakterisiert, so dass
  $\sigma \models^I \text{wp}(\textbf{while}\ (b)\ c_0, Q)$
  $\longleftrightarrow \forall k \geq 0 \forall \sigma_0, \ldots, \sigma_k.$ $\quad \sigma = \sigma_0$
  $\forall 0 \leq i < k.(\sigma_i \models^I b \wedge \underbrace{[\![c_0]\!]_C \sigma_i = \sigma_{i+1}}_{c_0 \text{ terminiert auf } \sigma_i \text{ in } \sigma_{i+1}}$
  $\sigma_k \models^I b \vee Q$
- 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 b und c_0 annehmen, mittels einer Formel beschrieben werden kann (β-Prädikat)
  2. $\text{wp}(c_0, \overline{X} = \overline{\sigma_{i+1}(X)})$ die Formel beschreibt, was vor c_0 gelten muss, damit hinterher die Programmvariablen $\overline{X}$ die Werte $\overline{\sigma_{i+1}(X)}$ haben
  3. $\neg\, \text{wp}(c_0, \mathit{false})$ 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.