

PROGRAMMIERUNG

ÜBUNG 12: HOARE-KALKÜL

Eric Kunze

`eric.kunze@tu-dresden.de`

1. Funktionale Programmierung
 - 1.1 Einführung in Haskell: Listen
 - 1.2 Algebraische Datentypen
 - 1.3 Funktionen höherer Ordnung
 - 1.4 Typpolymorphie & Unifikation
 - 1.5 Beweis von Programmeigenschaften
 - 1.6 λ -Kalkül
2. Logikprogrammierung
3. Implementierung einer imperativen Programmiersprache
 - 3.1 Implementierung von C_0
 - 3.2 Implementierung von C_1
4. **Verifikation von Programmeigenschaften**
5. H_0 – ein einfacher Kern von Haskell

HOARE-Kalkül

- ▶ Beweis / Verifikation von Programmeigenschaften

- ▶ Beweis / Verifikation von Programmeigenschaften
- ▶ Verifikationsformeln der Form $\{P\}A\{Q\}$
 - ▶ P und Q sind Zusicherungen (prädikatenlogische Ausdrücke)
 - ▶ P heißt **Vorbedingung**, Q heißt **Nachbedingung**
 - ▶ Beschreibung der Veränderung von Zusicherungen

- ▶ Beweis / Verifikation von Programmeigenschaften
- ▶ Verifikationsformeln der Form $\{P\} \mathbf{A} \{Q\}$
 - ▶ P und Q sind Zusicherungen (prädikatenlogische Ausdrücke)
 - ▶ P heißt **Vorbedingung**, Q heißt **Nachbedingung**
 - ▶ Beschreibung der Veränderung von Zusicherungen
 - ▶ **Bedeutung:** Wenn die Variablenwerte vor Ausführung von \mathbf{A} die Zusicherung P erfüllen und \mathbf{A} terminiert, dann erfüllen die Variablen nach Ausführung von \mathbf{A} die Zusicherung Q

$$\{x > 0\} \quad x = x + 5; \quad \{x > 5\}$$

- ▶ Beweis / Verifikation von Programmeigenschaften
- ▶ Verifikationsformeln der Form $\{P\} \mathbf{A} \{Q\}$
 - ▶ P und Q sind Zusicherungen (prädikatenlogische Ausdrücke)
 - ▶ P heißt **Vorbedingung**, Q heißt **Nachbedingung**
 - ▶ Beschreibung der Veränderung von Zusicherungen
 - ▶ **Bedeutung**: Wenn die Variablenwerte vor Ausführung von \mathbf{A} die Zusicherung P erfüllen und \mathbf{A} terminiert, dann erfüllen die Variablen nach Ausführung von \mathbf{A} die Zusicherung Q
- ▶ Aufstellen eines Beweisbaumes mit zur Verfügung stehenden Regeln

- ▶ Zuweisungsaxiom
- ▶ Sequenzregel
- ▶ CompRegel
- ▶ Iterationsregel
- ▶ (erste und zweite) Alternativregel
- ▶ Konsequenzregeln
 - ▶ stärkere Vorbedingung
 - ▶ schwächere Nachbedingung

SCHLEIFENINVARIANTE

Für die Iterationsregel benötigen wir die Schleifeninvariante SI . In den meisten unserer Fälle ist diese von der Form

$SI = \underline{A \wedge B}$, wobei

- ▶ A den Zusammenhang zwischen Zählvariable und Akkumulationsvariablen beschreibt. Führe dazu einige Iterationen der Schleife durch und leite daraus einen Zusammenhang her.
- ▶ B die abgeschwächte Schleifenbedingung ist. Dabei nehmen wir die letztmögliche Variablenbelegung, für die die Schleifenbedingung π noch wahr ist und führen den Schleifenrumpf noch einmal darauf aus ($\rightarrow \pi'$).

$$\rightsquigarrow B = \pi \cup \underline{\pi'}$$

$$\left. \begin{array}{l} \pi = x > 0 \\ \pi' = x = 0 \end{array} \right\} \text{" } \pi \cup \pi' \text{"} = x \geq 0$$