PROGRAMMIERUNG

ÜBUNG 12: HOARE-KALKÜL

Eric Kunze
eric.kunze@tu-dresden.de

INHALT

Hoare-Kalkül

HOARE-KALKÜL

- Beweis / Verifikation von Programmeigenschaften

HOARE-KALKÜL

- 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

HOARE-KALKÜL

- 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 **A** die Zusicherung P erfüllen und **A** terminiert, dann erfüllen die Variablen nach Ausführung von **A** die Zusicherung Q

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

HOARE-KALKÜL

- 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
  - **Bedeutung**: Wenn die Variablenwerte vor Ausführung von **A** die Zusicherung P erfüllen und **A** terminiert, dann erfüllen die Variablen nach Ausführung von **A** die Zusicherung Q
- Aufstellen eines Beweisbaumes mit zur Verfügung stehenden Regeln

HOARE-KALKÜL — 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 $SI = A \wedge B$, 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 ($\rightarrow \pi'$).

  $\rightsquigarrow B = \pi \cup \pi'$

$\pi = x > 0$
$\pi' = x = 0$
} "$\pi \cup \pi'$" = $x \geq 0$