

## Prinzip

Schrittweiser Nachweis von Eigenschaften eines Programmes mit Vor- und Nachbedingungen

## Technik

Hoare-Kalkül = Transformationsregeln zwischen Vor- und Nachbedingung

## Typische Regeln

$$\frac{\{p\} S_1 \{r\}, \quad \{r\} S_2 \{q\}}{\{p\} S_1; S_2 \{q\}}$$

$$\{p[v/e]\} v := e \{p\}$$

$$\{p \wedge B\} S \{p\}$$

mit Schleifeninvariante  $p$

$$\{p\} \text{ while } B \text{ do } S \text{ end } \{p \wedge \neg B\}$$

$\{n > 0\}$  $i := 0; s := 0$  $\{n > 0, i = 0, s = 0\}$  $\{i \leq n, s = \sum_{j=0}^i j\}$ while  $i < n$  do $\{i < n, i \leq n, s = \sum_{j=0}^i j\}$  $\{i < n, s = \sum_{j=0}^i j\}$  $i := i + 1;$  $\{i \leq n, s = \sum_{j=0}^{i-1} j\}$  $s := s + i;$  $\{i \leq n, s = i + \sum_{j=0}^{i-1} j\}$  $\{i \leq n, s = \sum_{j=0}^i j\}$ 

end;

 $\{\neg i < n, i \leq n, s = \sum_{j=0}^i j\}$  $\{s = \sum_{j=0}^n j\}$ Schleifeninvariante  $p$ Bedingung  $B \equiv i < n$ Terminierungsfunktion  $n - i$

## Halteproblem

Es gibt kein Programm, das die Terminierung von Programmen berechnen kann!

Schleifen lassen sich automatisch nur begrenzt aufrollen

- Schleifeninvarianten sind schwer zu finden (entspricht Induktionsinvarianten)
- Nach- bzw. Vorbedingungen von Schleifen lassen sich nicht automatisch berechnen
- Terminierungsfunktionen sind schwer zu finden
- Pointer und Heap-Speicher problematisch, z.B. Aliasing

Ähnliches gilt für Rekursion statt Schleifen.