Freie Universität Berlin

Axiome und Inferenzschemata des Hoare-Kalküls

Anja Wolffgramm

5. Juni 2017

Wie sind die Regeln zu lesen?

Prämisse

$$\text{RegelXY: } \frac{\boxed{\{P\}S_1\{R\}},\ \boxed{\{R\}S_2\{Q\}}}{\boxed{\{P\}S_1; S_2\{Q\}}}$$

Konklusion

Wenn die Prämisse(n) gezeigt wurde(n), dann gilt nach **RegelXY** die Konklusion.

Stärkere und schwächere Aussagen (Statements) unterscheiden

Im Nachfolgenden beschäftigen wir uns mit Logik und wollen stärkere und schwächere Aussagen unterscheiden lernen.

Aussage A	**Aussage B**	**Implikation**
„Zum Bestehen der Klausur benötigt man $\geq 50\%$ der Punkte“	„Zum Bestehen der Klausur benötigt man $\geq 50\%$ der Punkte **und** muss Anja einen Kuchen backen“	B ist stärker, da A eine Teilmenge ist. Es gilt: $B \implies A$
„Zum Bestehen der Klausur benötigt man $\geq 50\%$ der Punkte“	„Zum Bestehen der Klausur benötigt man $\geq 50\%$ der Punkte **oder** muss Anja einen Kuchen backen“	A ist stärker, da B eine Teilmenge ist. Es gilt: $A \implies B$
„Zum Bestehen der Klausur benötigt man $\geq 50\%$ der Punkte“	„Zum Bestehen der Klausur muss man Anja einen Kuchen backen“	A und B sind nicht vergleichbar, da sie disjunkt sind. Keine von beiden ist stärker.
„True“	„$n = 2k + 1$“	B ist stärker, da A keine Einschränkungen hat. Es gilt: $B \implies A$
„False“	„$n = 2k + 1$“	A ist stärker, da es kein Tupel (n, k) geben kann, sodass A erfüllt wäre. Es gilt: $A \implies B$

Regeln

1. **Nullaxiom** (es findet keine Zuweisung zwischen P und Q statt und $P \equiv Q$)

   $$\{P\} \quad \{Q\}$$

   $\{P\} \equiv \{n \geq 1 \land n \in \mathbb{N}\}$
   $\{Q\} \equiv \{n > 0 \land n \in \mathbb{N}\}$ Nullaxiom

2. **Zuweisungsaxiom** (ersetzt alle Vorkommen von x in Q durch expr)

   $$\{Q\langle x \leftarrow \mathit{expr}\rangle\}\ x = \text{expr}\{Q\}$$

   $\{P\} \equiv \{2x + y > 5 \land y = 7\}$
   `x = 2*x+y` Zuweisungsaxiom
   $\{Q\} \equiv \{x > 5 \land y = 7\}$

3. **Sequenzregel**

   - Sequenzregel

     $$\frac{\boxed{\{P\}S_1\{R\}},\ \boxed{\{R\}S_2\{Q\}}}{\boxed{\{P\}S_1; S_2\{Q\}}}$$

     $\{P\} \equiv \{(x+5)^2 > 0\}$
     `x = x+5` Zuweisungsaxiom
     Sequenzregel $\{R\} \equiv \{x^2 \neq 0\} \equiv \{x^2 > 0\}$
     `x = x*x`
     $\{Q\} \equiv \{x \neq 0\}$ Zuweisungsaxiom

   - erweiterte Sequenzregel: Per Induktion lässt sich nachweisen, dass beliebig viele Sequenzen mit der Sequenzregel zusammen gefasst werden können:

     $$\frac{\boxed{\{P\}S_1\{R_1\}},\ \boxed{\{R_1\}S_2\{R_2\}},\ \ldots\ \boxed{\{R_{k-1}\}S_k\{Q\}}}{\boxed{\{P\}S_1; S_2; \ldots; S_k\{Q\}}}$$

4. **Konsequenzregel**

   - Konsequenzregel I (Regel der schwächeren Nachbedingung)

     $$\frac{\boxed{\{P\}S\{R\}},\ \boxed{\overset{\text{stärker}}{R} \implies \overset{\text{schwächer}}{Q}}}{\boxed{\{P\}S\{Q\}}}$$

     $\{P\} \equiv \{\text{True} \land x \geq 0\}$
     `res = math.sqrt(x)` Zuweisungsaxiom
     Konsequenzregel I $\{R\} \equiv \{res = \sqrt{x} \land x \geq 0\}$
     $\{Q\} \equiv \{res = \sqrt{x}\}$

     Und aus R folgt Q, da R stärker ist.

   - Konsequenzregel II (Regel der stärkeren Vorbedingung)

     $$\frac{\boxed{\overset{\text{stärker}}{P} \implies \overset{\text{schwächer}}{R}},\ \boxed{\{R\}S\{Q\}}}{\boxed{\{P\}S\{Q\}}}$$

     $\{P\} \equiv \{x = 42\}$
     $\{R\} \equiv \{(2x) \text{ gerade}\} \equiv \{\text{True}\}$
     Konsequenzregel II `x = x*2` Zuweisungsaxiom
     $\{Q\} \equiv \{x \text{ gerade}\}$

     Und aus P folgt R, da P stärker ist.

5. **Bedingungsregel**

- Bedingungsregel I

$$\frac{\boxed{\{P \wedge B\} S_1 \{Q\}},\ \boxed{\{P \wedge \neg B\} S_2 \{Q\}}}{\boxed{\begin{array}{l}\{P\}\ \text{if } B : S_1 \\ \quad\quad \text{else} : S_2 \{Q\}\end{array}}}$$

Bedingungsregel I

$\{P\}$
`if B:`
$\boxed{\{P \wedge B\}\ \texttt{S1}\ \{Q\}}$
`else:` ?
$\boxed{\{P \wedge \neg B\}\ \texttt{S2}\ \{Q\}}$
$\{Q\}$?

- Bedingungsregel II (ohne else-Fall)

$$\frac{\boxed{\{P \wedge B\} S \{Q\}},\ \boxed{(P \wedge \neg B) \implies Q}}{\boxed{\{P\}\ \text{if } B : S\{Q\}}}$$

Bedingungsregel II

$\{P\} = \{n > 0\}$
`if` $\boxed{\texttt{n\% 2 != 0}}$`:` B
$\{P \wedge B\} \equiv \{n > 0 \wedge n\%2 \neq 0\}$
`n = n+1`
$\{Q\}$ Konsequenzregel II
$\{Q\} = \{n > 0 \wedge n\%2 = 0\}$

Und es gilt: $\boxed{(P \wedge \neg B) \implies Q)}$

- erweiterte Bedingungsregel (if-elif-else)

$$\frac{\boxed{\{P \wedge B_1\} S_1 \{Q\}},\ \boxed{\{P \wedge \neg B_1 \wedge B_2\} S_2 \{Q\}},\ \boxed{\{P \wedge \neg B_1 \wedge \neg B_2\} S_3 \{Q\}}}{\boxed{\begin{array}{llll}\{P\} & \text{if } B_1 : & S_1 & \\ & \text{elif } B_2 : & S_2 & \\ & \text{else} : & S_3 & \{Q\}\end{array}}}$$

6. **while-Regel**

$$\frac{\boxed{\{\text{INV} \wedge B\}\ S\ \{\text{INV}\}}}{\boxed{\{\text{INV}\}\ \text{while } B : S\{\text{INV} \wedge \neg B\}}}$$

while-Regel

$\{\text{INV}\}$
`while B:`
$\{\text{INV} \wedge B\}$
`S` ?
$\{Q\}$
$\{Q \wedge \neg B\}$