§ 3: BEWEISPRINZIPIEN

3.1 Bedeutung in der Informatik

Informatiker beweisen ständig, sie nennen es oftmals nur nicht so.

- Tut ein Protokoll was es soll?
- Arbeitet ein Algorithmus in allen Spezialfällen richtig?
- Bricht es in endlicher Zeit ab?

Einige der Tautologien aus Satz 2.8 ermöglichen entsprechende Beweisprinzipien.

3.2. Direkter Beweis

- Man möchte $A \Rightarrow B$ zeigen.
- verwende Tautologie

$$(A \Rightarrow C_1) \wedge (C_1 \Rightarrow C_2) \wedge \ldots (C_k \Rightarrow C_{k+1}) \wedge (C_{k+1} \Rightarrow B)$$

- Man zerlegt also $A \Rightarrow B$ in eine Kette von einfachen Implikationen.

3.3. Beispiel: Satz: Ist eine nat. Zahl durch 6 teilbar, so ist sie auch durch 3 teilbar.

Beweis: Sei $n \in \mathbb{N}$ durch 6 teilbar:

$\exists k \in \mathbb{N}: \quad n = 6k$

$\Rightarrow \quad n = 3 \cdot 2k = 3p \quad$ mit $p = 2k \in \mathbb{N}$.

$\Rightarrow \quad n$ durch 3 teilbar.

$\square$

3.4 Beweis durch Kontraposition

- beruht auf der Tautologie $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$
- Statt $A \Rightarrow B$ zeigt man also $\neg B \Rightarrow \neg A$.

3.7. Äquivalenzbeweise

- beruhen auf der Tautologie $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$
- Um $A \Leftrightarrow B$ zu zeigen, beweist man also $A \Rightarrow B$ und $B \Rightarrow A$.
- Will man die Äquivalenz vieler Aussagen zeigen, bietet sich ein Ringschluss an:

$$A \Leftrightarrow B \Leftrightarrow C \Leftrightarrow D$$

zeigt man durch

$$A \Rightarrow B, \quad B \Rightarrow C, \quad C \Rightarrow D, \quad D \Rightarrow A.$$

3.5. Widerspruchsbeweise

- um Aussage B zu beweisen, zeigt man z. B. dass die Verneinung $\neg B$ zu einem Widerspruch führt:

$$\neg B \Rightarrow B$$

- also muss $\neg(\neg B)$ und damit B wahr sein.
- beruht auf Tautologie $(\neg B \Rightarrow B) \Rightarrow B$

3.6. Beispiel

Satz: Es gibt keine größte Primzahl (Aussage B)

Beweis: Ann.: Es gibt eine größte Primzahl ($\neg B$)

Seien $p_1, p_2, \dots, p_n$ alle Primzahlen (*)

Sei $q = p_1 p_2 \cdots p_n + 1$.

Beh.: q ist eine Primzahl (Aussage A)

Angen.: q ist keine Primzahl ($\neg A$)

$\Rightarrow$ q hat Primteiler $p_i \in \{p_1, \dots, p_n\}$:

$\exists\, \alpha, \beta \in \mathbb{Z}$:

$$p_i \cdot \alpha = q = \underbrace{p_1 \cdots p_n}_{p_i \cdot \beta} + 1 = p_i \beta + 1$$

$\Rightarrow$ $p_i (\alpha - \beta) = 1$, wobei $\alpha - \beta$ ganze Zahl ist.

$\Rightarrow$ $p_i = 1$

↯ zu p_i Primteiler. (also gilt *) □

Da q eine Primzahl ist und $q > p_i \ \forall i \in \{1, \dots, n\}$, ist dies ein Widerspruch.

□

3.7. → Blatt 16

3.8. Beweis durch vollständige Induktion

Grundidee:

- Für jede natürliche Zahl $n \in \mathbb{N}$ sei eine Aussage $A(n)$ gegeben.
- Es gilt:
  1. Induktionsanfang: $A(1)$ ist wahr
  2. Induktionsschluss: $\big(A(n) \Rightarrow A(n+1)\big)$ ist wahr.
- Dann gilt die Aussage für alle $n \in \mathbb{N}$.

3.9. Beispiel

Def.: $\sum_{k=m}^{n} a_k = a_m + a_{m+1} + \ldots + a_n$ Summenzeichen

$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot \ldots \cdot a_n$ Produktzeichen.

Satz: $\sum_{k=1}^{n} k = 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$ für alle $n \in \mathbb{N}$.

Beweis mit vollst. Induktion über n:

1. Induktionsanfang:

Für $n = 1$ ist $\sum_{k=1}^{1} k = 1 = \frac{1 \cdot 2}{2}$ ✓

2. Induktionsschluss:

Ann: $A(n)$ für ein bestimmtes $n \in \mathbb{N}$ wahr (Ind.-Voraussetzung):

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \qquad (*)$$

Dann gilt

$$\sum_{k=1}^{n+1} k = n+1 + \sum_{k=1}^{n} k \overset{(*)}{=} n+1 + \frac{n(n+1)}{2}$$

$$= \frac{2(n+1) + n(n+1)}{2} = \frac{(n+2)(n+1)}{2}$$

d.h. $A(n+1)$ ist wahr. $\square$

3.10. Anmerkungen

a) Induktionsbeweise sind sehr häufig bei Summen- und Produktformeln.

b) Der Induktionsanfang muss nicht bei 1 beginnen. Beginnt er mit $A(k)$, so gilt die Aussage $A(n)$ für alle $n \in \mathbb{N}$ mit $n \geq k$.