§3: BEWEISPRINZIPIEN

3.1. Bedeutung in der Informatik

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

- Macht ein Protokoll, was es soll?
- Arbeitet ein Algorithmus in allen Fällen korrekt?
- 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.
- Hierzu zerlegt man $A \Rightarrow B$ in eine Kette von einfacheren Implikationen
- verwendete Tautologie:

$$(A \Rightarrow B) \iff \big((A \Rightarrow C) \wedge (C \Rightarrow B)\big)$$

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.

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

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

$\Rightarrow n$ ist durch 3 teilbar. $\square$

3.4. Beweis durch Kontraposition (Indirekter Beweis)

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

3.5. Beispiel

Satz: Sei $n \in \mathbb{Z}$ und n^2 gerade.
Dann ist auch n gerade.

Beweis: Ann.: n ungerade

$\Rightarrow \exists\, m \in \mathbb{Z}: \quad n = 2m+1$

$\Rightarrow \quad n^2 = (2m+1)^2 = 4m^2 + 4m + 1$

$= 2\underbrace{(2m^2 + 4m)}_{\in \mathbb{Z}} + 1$

$\Rightarrow n^2$ ungerade. $\square$

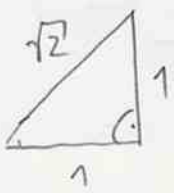
3.6. Widerspruchsbeweis

- wollen Aussage A beweise
- nehmen an, A ist nicht wahr
- folgen Widerspruch
- also ist A wahr
- beruht auf Tautologie $\neg(A \wedge \neg A)$

3,7. Beispiel

Satz: $\sqrt{2}$ ist irrational, d.h. $\sqrt{2}$ kann nicht als Bruch $\sqrt{2} = \frac{n}{m}$ mit $n, m \in \mathbb{N}$ dargestellt werden.

Beweis: Ann.: $\sqrt{2} = \frac{n}{m}$ mit gekürztem Bruch $\frac{n}{m}$ (d.h. n, m teilerfremd)



$\Rightarrow 2m^2 = n^2$ (*)

$\Rightarrow n^2$ gerade

$\overset{3.5}{\Rightarrow} n$ gerade

$\Rightarrow \exists k \in \mathbb{N}: \quad n = 2k$

Einsetzen in (*):

$2m^2 = (2k)^2 = 4k^2$

$\Rightarrow m^2 = 2k^2$

$\Rightarrow m^2$ gerade

$\Rightarrow m$ gerade

Da also n und m gerade sind, war $\frac{n}{m}$ nicht teilerfremd.

Somit ist $\sqrt{2} = \frac{n}{m}$ falsch. □

3.8. Beweis von Äquivalenz

- Um $A \Leftrightarrow B$ zu zeigen, beweist man $A \Rightarrow B$ und $B \Rightarrow A$
- verwendete Tautologie: $(A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow A)$
- Um Äquivalenz von vielen Aussagen zu zeigen, bietet sich ein zyklisches Beweisverfahren an:

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

  zeigt man durch

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

27.10.'06

3.9. Beweis durch vollständige Induktion

Grundidee:

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

3.10. Beispiel

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

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

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

Beweis durch vollst. Induktion über n:

1. Induktionsanfang:

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

2. Induktionsschluss:

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

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

Dann folgt:

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

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

d.h. $A(n+1)$ ist wahr. □

3.11. Anmerkungen

a) Induktionsbeweise sind 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 $n \geq k$.