Beweistechniken

Sommersemester 2018
Ronja Düffel

15. März 2018

Wozu Beweise in der Informatik?

- … um Aussagen wie
  1. “Das Programm erfüllt die gewünschte Aufgabe.”
  2. “Das Programm führt zu keiner Endlosschleife.”
  3. “Für diese Art Probleme gibt es keine effiziente Lösung”

  auf ihren Wahrheitsgehalt zu prüfen, wenn unsere Intuition versagt.
- Richtigkeit eigener Gedanken beurteilen

Warum ist Beweisen so schwierig?

- unsere natürliche Sprache ist oft mehrdeutig
- wir sind in unserem Alltag von logischen Fehlschlüssen umgeben
- Logik hilft beim Argumentieren und Aufschreiben von Beweisen
- beim *Finden* von Beweisen helfen:
  - **Erfahrung**
  - Problemlösungsstrategien
  - Kenntnis typischer Beweismuster

Beweis

Definition (Beweis)

Ein Beweis ist eine **logisch vollständige Begründung** *einer Aussage.*

Solange eine Aussage nicht bewiesen ist, kann es sein, dass sie falsch ist. Egal durch wie viele Beispiele sie gestützt wird.

FERMAT-Zahlen

$$F_n = 2^{2^n} + 1$$

Vermutung (1637): Alle F_n sind Primzahlen

Widerlegt (1732) von EULER: $F_5 = 4294967297$ ist durch 641 teilbar

Übersicht

- **direkter Beweis**
- Beweis durch Kontraposition
- Beweis durch Widerspruch

Vorgehensweise beim direkten Beweis

Wir leiten *sukessive* und *in logisch nachvollziehbaren Schritten* die Behauptung her.

Dabei benutzen wir:

- Definitionen
- bereits bekannte Ergebnisse
- weitere Voraussetzungen (falls notwendig)

$$A$$

$$\downarrow$$

logische Schlussfolgerungen

$$\downarrow$$

$$B$$

Beispiel

Die Summe zweier gerader Zahlen ist wiederum eine gerade Zahl.

Was brauchen wir?

Beispiel

Die Summe zweier gerader Zahlen ist wiederum eine gerade Zahl.

Definition (gerade Zahl)

Eine Zahl ist genau dann gerade, wenn sie durch 2 teilbar ist.

Definition (Teilbarkeit)

Eine Zahl a ist genau dann durch eine Zahl $b \neq 0$ teilbar, wenn es eine ganze Zahl $k \in \mathbb{Z}$ gibt, sodass $a = b \cdot k$.

Beispiel für einen direkten Beweis I

Beispiel

Die Summe zweier gerader Zahlen ist wiederung eine gerade Zahl.

- Seien a und b gerade Zahlen.

$\Rightarrow$ $a = 2 \cdot k,\ b = 2 \cdot l,\ k, l \in \mathbb{Z}$ (Def. gerade Zahlen)

$\Rightarrow$ $a + b = 2 \cdot k + 2 \cdot l = 2 \cdot (k + l)$ (Einsetzen, Ausklammern)

$\Rightarrow$ $a + b = 2 \cdot m, m = l + k, m \in \mathbb{Z}$ (Abgeschlossenheit $(\mathbb{Z}, +)$)

$\Rightarrow$ $a + b$ ist durch 2 teilbar

$\Rightarrow$ $a + b$ ist gerade.

$\square$

Beweis Satz 2

Satz

Seien A und B Mengen.
$A = B$ gilt genau dann, wenn $A \subseteq B$ und $B \subseteq A$ gelten.

Definition (Gleichheit, Teilmenge)

- *Mengen A und B sind genau dann* **gleich** *(kurz: $A = B$), wenn sie* **dieselben** *Elemente enthalten.*
- *A ist genau dann eine* **Teilmenge** *von B (kurz: $A \subseteq B$), wenn jedes Element von A auch ein Element von B ist.*

Beweis (Satz 2 von gestern)

Satz

Seien A und B Mengen.
$A = B$ gilt **genau dann, wenn** *$A \subseteq B$ und $B \subseteq A$ gelten.*

Biimplikation: $\varphi \leftrightarrow \psi$

Wir müssen **zwei** “Richtungen” zeigen.

1. Wenn $A = B$ gilt, dann gilt $A \subseteq B$ und $B \subseteq A$.
2. Wenn $A \subseteq B$ und $B \subseteq A$ gilt, dann gilt auch $A = B$.

$\Longrightarrow$

z.Z: Wenn $A = B$ gilt, dann gilt $A \subseteq B$ und $B \subseteq A$.

Es gelte $A = B$.

$\Longrightarrow$ A und B enthalten dieselben Elemente

$\Longrightarrow$ jedes $x \in A$ ist auch $\in B$ und
jedes $x \in B$ ist auch $\in A$

$\Longrightarrow$ es gilt $A \subseteq B$ und $B \subseteq A$

$\Longleftarrow$

z.Z: Wenn $A \subseteq B$ und $B \subseteq A$ gilt, dann gilt auch $A = B$.

Es gelte $A \subseteq B$ und $B \subseteq A$

$\Longrightarrow$ jedes $x \in A$ ist auch $\in B$ und
jedes $x \in B$ ist auch $\in A$

$\Longrightarrow$ A und B enthalten dieselben Elemente

$\Longrightarrow$ es gilt $A = B$

$\square$

Beispiel für einen direkten Beweis III

Beispiel

Alle Primzahlen bis auf die 2 sind ungerade.

Sei $x \in \mathbb{N}, x \neq 2$ eine Primzahl

$\Longrightarrow$ x ist nur durch sich selbst und 1 teilbar

$\Longrightarrow$ x ist **nicht** durch $2 \cdot k, k \in \mathbb{Z}$ darstellbar

$\Longrightarrow$ x ist nicht gerade

$\Longrightarrow$ x ist ungerade

$\square$

Übersicht

- direkter Beweis
- **Beweis durch Kontraposition**
- Beweis durch Widerspruch

Beweis durch Kontraposition

Beispiel

Wenn a^2 gerade ist, dann ist a gerade.

Problem: Es bietet sich kein direkter Beweis an.

Lösung: *Beweis durch Kontraposition*

Zurück zur Wahrheitstafel...

A	B	$A \to B$	$\neg A$	$\neg B$	$\neg B \to \neg A$
0	0	1	1	1	1
0	1	1	1	0	1
1	0	0	0	1	0
1	1	1	0	0	1

Fazit

$A \to B \equiv \neg B \to \neg A$

Beispiel (Planet Zutan)

Wenn der Bewohner rot ist, hat er grüne Haare.
$\equiv$*Wenn der Bewohner keine grünen Haare hat, ist er auch nicht rot.*

Beispiel für einen Beweis durch Kontraposition I

Beispiel

Wenn a^2 gerade ist, dann ist a gerade.

Aussage	Negation
a^2 ist eine gerade Zahl.	a^2 ist eine ungerade Zahl.
a ist eine gerade Zahl.	a ist eine ungerade Zahl.

Wir zeigen also:

Satz

Wenn a ungerade ist, ist auch a^2 ungerade.

Beispiel für einen Beweis durch Kontraposition

Satz

Wenn a ungerade ist, ist auch a^2 ungerade.

Beweis:

Sei a eine beliebige **ungerade** Zahl.

$\Longrightarrow$ $a = 2 \cdot k + 1$ für eine ganze Zahl k

$\Longrightarrow$ $a^2 = (2k+1)^2$ für eine ganze Zahl k (Quadrieren)

$\Longrightarrow$ $a^2 = 2 \cdot 2 \cdot k^2 + 2(2k \cdot 1) + 1^2 = 2 \cdot (2k^2 + 2k) + 1^2$ (Binomische Formel, Ausklammern)

$\Longrightarrow$ $a^2 = 2 \cdot l + 1$ mit $l = 2 \cdot k^2 + 2k$ für eine ganze Zahl k

$\Longrightarrow$ $a^2 = 2 \cdot l + 1$ für eine ganze Zahl l, da $2k^2 + 2k$ eine ganze Zahl ist, wenn k eine ganze Zahl ist (Abgeschlossenheit $(\mathbb{Z}, +)$)

$\Longrightarrow$ a^2 ist nicht durch 2 teilbar, d.h. a^2 ist ungerade.

$\square$

Beweis durch Kontraposition

Ziel: Beweis der Aussage

Satz (1)

Wenn a^2 gerade ist, dann ist a gerade.

Direkter Beweis schwierig, daher Beweis der **aussagenlogisch äquivalenten** Aussage:

Satz (2)

Wenn a ungerade ist, dann ist a^2 ebenfalls ungerade.

Damit haben wir Aussage 1 indirekt bewiesen.

Übersicht

- direkter Beweis
- Beweis durch Kontraposition
- **Beweis durch Widerspruch**

Beispiel für einen Beweis durch Widerspruch I

Beispiel

$\sqrt{2}$ *ist irrational.*

Problem: Wo sind Voraussetzung A und Folgerung B?
atomare Aussage
Weder ein direkter noch ein Beweis durch Kontraposition bieten sich an.

Lösung: Angenommen, $\sqrt{2}$ ist rational.
Wir wollen zeigen, dass das zu einem Widerspruch führt.

Beispiel Widerspruchsbeweis

Angenommen, $\sqrt{2}$ ist rational, also $\sqrt{2} \in \mathbb{Q}$.

$\Rightarrow$ $\sqrt{2} = \frac{p}{q}$,mit $p, q \in \mathbb{Z}$ und $\mathrm{ggT}(p, q) = 1$ (Definition $\mathbb{Q}$)

Nun ist $2 = \frac{p^2}{q^2}$ (Quadrieren) und $2 \cdot q^2 = p^2$ (Umformen)

$\Rightarrow$ p^2 ist durch 2 teilbar, da $q^2 \in \mathbb{Z}$ (Def. Teilbarkeit, Abgeschlossenheit $(\mathbb{Z}, \cdot)$).

$\Rightarrow$ a ist durch 2 teilbar (bereits bewiesen)

und darstellbar als $p = 2 \cdot k, k \in \mathbb{Z}$ (Definition der Teilbarkeit)

$2 \cdot q^2 = (2 \cdot k)^2 \Leftrightarrow q^2 = 2 \cdot k^2$ ebenfalls durch 2 teilbar (Einsetzen und Def. Teilbarkeit),

und q ist ebenfalls durch 2 teilbar (bereits bewiesen).

Also teilt 2 sowohl p, wie auch q, was ein Widerspruch zu der Annahme ist, dass $\mathrm{ggT}(p, q) = 1$.

Damit ist $\sqrt{2}$ irrational.

$\square$

Beweistechniken

- direkter Beweis
  $A \rightarrow A_1 \rightarrow \cdots \rightarrow B$
- Beweis durch Kontraposition
  $\neg B \rightarrow A_1 \rightarrow \cdots \rightarrow \neg A$
- Beweis durch Widerspruch
  $\neg A \rightarrow A_1 \rightarrow \cdots \rightarrow$ Widerspruch (Falsche Aussage)

Worauf man beim Beweisen achten sollte

- Angabe der Beweistechnik am Anfang hilft dem Leser die Idee zu verstehen.
- keine Gedankensprünge im Beweis, nur leicht nachvollziehbare Schlussfolgerungen
- Kennzeichnung am Ende eines Beweises (z.B. durch $\square$)
- Bei längeren Beweisen ist zum Schluss ein kurzer Satz, was gezeigt wurde, hilfreich.