Vorkurs
Formale Methoden der Informatik

Bettina Esser und Michael Kaibel

2. September bis 13. September 2024, Universität Bonn

Informatik V

Beweistechniken

Grundsätzlicher Aufbau eines Beweises

Ein mathematischer Satz besteht immer aus zwei Teilen:

1. Einer Behauptung und
2. einem Beweis, der die Gültigkeit der Behauptung zeigt.

Die Behauptung besteht meistens aus

1. den Voraussetzungen und
2. der tatsächlichen Aussage.

Beispiel

Seien $\underbrace{a,\ b \in \mathbb{R}}_{\text{Voraussetzungen}}$, dann gilt: $\underbrace{(a+b)^2 = a^2 + 2ab + b^2}_{\text{Aussage}}$.

Äquivalenzumformungen

Um Gleichungen der Form $T_1 = T_2$ zu lösen, wobei T_1 und T_2 gültige Terme sind, benutzen wir sogenannte *Äquivalenzumformungen*. Dabei handelt es sich um Umformungen, die den Wahrheitsgehalt der gesamten Gleichung erhalten.

In $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$ sind dies beispielsweise

- Addition und Subtraktion
- Multiplikation und Division mit beliebigen Konstanten $\neq 0$
- Jede andere umkehrbare Funktion

Beachten Sie, dass Quadrieren nur einem Zahlenbereich ohne negative Zahlen eine Äquivalenzumformung ist (also in $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Q}_+$ oder $\mathbb{R}_+$)!

Das ist schon eine Art Beweis. Die Auflösung der Gleichung rückwarts beweist, dass die gefundene Lösung korrekt ist.

Direkte Beweise

Ein direkter Beweis nimmt die Voraussetzung V als gegeben an, und versucht die Behauptung B direkt herzuleiten. Das geht auf zwei Arten:

- Wir deduzieren logisch: $V \Rightarrow \ldots \Rightarrow B$.
- Wir formen unter Verwendung der Voraussetzungen um: $B \iff \ldots \iff \texttt{wahr}$.

Beispiel: Binomische Formeln

Seien a, $b \in \mathbb{R}$. Dann gilt:

$$(a+b)^2 = a^2 + 2ab + b^2, \qquad \text{(erste binomische Formel)}$$

$$(a-b)^2 = a^2 - 2ab + b^2, \qquad \text{(zweite binomische Formel)}$$

$$(a+b)(a-b) = a^2 - b^2. \qquad \text{(dritte binomische Formel)}$$

Beweis: Erste binomische Formel

Wir beweisen jetzt die erste binomische Formel mittels Äquivalenzumformung der Terme. D.h., eine der beiden Seiten der Gleichung verändert sich nicht, während auf der anderen Seite Äquivalenzumformungen gemacht werden.

$$(a+b)^2 = (a+b)(a+b)$$

Beweis: Erste binomische Formel

Wir beweisen jetzt die erste binomische Formel mittels Äquivalenzumformung der Terme. D.h., eine der beiden Seiten der Gleichung verändert sich nicht, während auf der anderen Seite Äquivalenzumformungen gemacht werden.

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b) \\ &= a(a+b)+b(a+b)\end{aligned}$$

Beweis: Erste binomische Formel

Wir beweisen jetzt die erste binomische Formel mittels Äquivalenzumformung der Terme. D.h., eine der beiden Seiten der Gleichung verändert sich nicht, während auf der anderen Seite Äquivalenzumformungen gemacht werden.

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b)+b(a+b)\\ &= aa+ab+ba+bb\end{aligned}$$

Beweis: Erste binomische Formel

Wir beweisen jetzt die erste binomische Formel mittels Äquivalenzumformung der Terme. D.h., eine der beiden Seiten der Gleichung verändert sich nicht, während auf der anderen Seite Äquivalenzumformungen gemacht werden.

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b)+b(a+b)\\ &= aa+ab+ba+bb\\ &= a^2+ab+ab+b^2\end{aligned}$$

Beweis: Erste binomische Formel

Wir beweisen jetzt die erste binomische Formel mittels Äquivalenzumformung der Terme. D.h., eine der beiden Seiten der Gleichung verändert sich nicht, während auf der anderen Seite Äquivalenzumformungen gemacht werden.

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b)+b(a+b)\\ &= aa+ab+ba+bb\\ &= a^2+ab+ab+b^2\\ &= a^2+2ab+b^2\end{aligned}$$

□

Partialsumme der geometrischen Reihe

Als weiteres Beispiel beweisen wir jetzt die Partialsumme der geometrischen Reihe.

Sei $a \in \mathbb{R}$ mit $a \neq 1$ und $n \in \mathbb{N}_0$. Dann gilt:

$$\sum_{i=0}^{n} a^i = \frac{1 - a^{n+1}}{1 - a}.$$

Partialsumme der geometrischen Reihe

Als weiteres Beispiel beweisen wir jetzt die Partialsumme der geometrischen Reihe.

Sei $a \in \mathbb{R}$ mit $a \neq 1$ und $n \in \mathbb{N}_0$. Dann gilt:

$$\sum_{i=0}^{n} a^i = \frac{1 - a^{n+1}}{1 - a}.$$

Beweis:

$$\Leftrightarrow \qquad a^0 + a^1 + \ldots + a^n = \frac{1 - a^{n+1}}{1 - a}$$

Partialsumme der geometrischen Reihe

Als weiteres Beispiel beweisen wir jetzt die Partialsumme der geometrischen Reihe.

Sei $a \in \mathbb{R}$ mit $a \neq 1$ und $n \in \mathbb{N}_0$. Dann gilt:

$$\sum_{i=0}^{n} a^i = \frac{1 - a^{n+1}}{1 - a}.$$

Beweis:

$$\Leftrightarrow \quad a^0 + a^1 + \ldots + a^n = \frac{1 - a^{n+1}}{1 - a}$$

$$\Leftrightarrow \quad (1 + a + \ldots + a^n)(1 - a) = 1 - a^{n+1}$$

Partialsumme der geometrischen Reihe

Als weiteres Beispiel beweisen wir jetzt die Partialsumme der geometrischen Reihe.

Sei $a \in \mathbb{R}$ mit $a \neq 1$ und $n \in \mathbb{N}_0$. Dann gilt:

$$\sum_{i=0}^{n} a^i = \frac{1 - a^{n+1}}{1 - a}.$$

Beweis:

$$\begin{aligned}
&\Leftrightarrow && a^0 + a^1 + \ldots + a^n = \frac{1 - a^{n+1}}{1 - a} \\
&\Leftrightarrow && (1 + a + \ldots + a^n)(1 - a) = 1 - a^{n+1} \\
&\Leftrightarrow && (1 + a + \ldots + a^n) - a(1 + a + \ldots + a^n) = 1 - a^{n+1}
\end{aligned}$$

Partialsumme der geometrischen Reihe

Als weiteres Beispiel beweisen wir jetzt die Partialsumme der geometrischen Reihe.

Sei $a \in \mathbb{R}$ mit $a \neq 1$ und $n \in \mathbb{N}_0$. Dann gilt:

$$\sum_{i=0}^{n} a^i = \frac{1 - a^{n+1}}{1 - a}.$$

Beweis:

$$\begin{aligned}
&\Leftrightarrow && a^0 + a^1 + \ldots + a^n = \frac{1 - a^{n+1}}{1 - a} \\
&\Leftrightarrow && (1 + a + \ldots + a^n)(1 - a) = 1 - a^{n+1} \\
&\Leftrightarrow && (1 + a + \ldots + a^n) - a(1 + a + \ldots + a^n) = 1 - a^{n+1} \\
&\Leftrightarrow && 1 + a + \ldots + a^n - a - a^2 - \ldots - a^n - a^{n+1} = 1 - a^{n+1}
\end{aligned}$$

Partialsumme der geometrischen Reihe

Als weiteres Beispiel beweisen wir jetzt die Partialsumme der geometrischen Reihe.

Sei $a \in \mathbb{R}$ mit $a \neq 1$ und $n \in \mathbb{N}_0$. Dann gilt:

$$\sum_{i=0}^{n} a^i = \frac{1 - a^{n+1}}{1 - a}.$$

Beweis:

$$\begin{aligned}
&\Leftrightarrow && a^0 + a^1 + \ldots + a^n = \frac{1 - a^{n+1}}{1 - a} \\
&\Leftrightarrow && (1 + a + \ldots + a^n)(1 - a) = 1 - a^{n+1} \\
&\Leftrightarrow && (1 + a + \ldots + a^n) - a(1 + a + \ldots + a^n) = 1 - a^{n+1} \\
&\Leftrightarrow && 1 + a + \ldots + a^n - a - a^2 - \ldots - a^n - a^{n+1} = 1 - a^{n+1}
\end{aligned}$$

Alle Summanden außer 1 und a^{n+1} kürzen sich raus.

$$\Leftrightarrow \qquad 1 - a^{n+1} = 1 - a^{n+1} \qquad \square$$

Fallunterscheidung, erster Fall

Behauptung: Das Produkt zweier natürlicher Zahlen a, b ist genau dann ungerade, wenn sowohl a als auch b ungerade sind.

Beweis: Wir zeigen, dass nur das Produkt zweier ungeraden Zahlen ungerade ist, sonst gerade. Wir machen Fallunterscheidung.

Erster Fall: a, $b \in \mathbb{N}$ sind beide gerade. Dann gibt es k, $\ell \in \mathbb{N}$ mit den Eigenschaften

$$a = 2k, \quad b = 2\ell.$$

Das Produkt $a \cdot b$ ist dann

$$a \cdot b = 2k \cdot 2\ell = 2(2k\ell).$$

Somit ist das Produkt gerade.

Fallunterscheidung, zweiter Fall

Zweiter Fall: Seien a, $b \in \mathbb{N}$ beide ungerade. Dann existieren k, $\ell \in \mathbb{N}$ und es gilt

$$a = 2k - 1, \quad b = 2\ell - 1.$$

Das Produkt $a \cdot b$ ist dann

$$a \cdot b = (2k - 1) \cdot (2\ell - 1) = 4k\ell - 2k - 2\ell + 1 = 2(2k\ell - k - \ell) + 1.$$

Da $2k\ell - k - \ell \in \mathbb{N}$, ist $2(2k\ell - k - \ell)$ gerade. Damit ist das Produkt ungerade.

Fallunterscheidung, dritter Fall

Dritter Fall: Genau eine der beiden Zahlen a, b ist gerade, die andere ist ungerade. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass $a \in \mathbb{N}$ ungerade ist und $b \in \mathbb{N}$ gerade. Sonst könnten wir a und b austauschen, da die Multiplikation in $\mathbb{N}$ kommutativ ist.

Dann gibt es k, $\ell \in \mathbb{N}$ und wir können a und b schreiben als

$$a = 2k - 1, \quad b = 2\ell.$$

Das Produkt $a \cdot b$ ist dann

$$a \cdot b = (2k - 1) \cdot (2\ell) = 4k\ell - 2\ell = 2(2k\ell - \ell).$$

Das Produkt ist also gerade.

Weitere Fälle existieren nicht. □

Noch eine Fallunterscheidung

Für welche $x \in \mathbb{R}$ gilt:

$$x \cdot x = x + x \ ?$$

Wir rechnen es einfach aus:

$$x^2 = 2x.$$

Damit wir im nächsten Schritt durch x dividieren können, müssen wir $x \neq 0$ fordern.

$$x = 2$$

Der Fall $x = 0$ löst die Gleichung aber auch, wovon wir uns durch Einsetzen überzeugen können. Also sind die Lösungen 0 und 2. □

Indirekter Beweis

Um einen indirekten Beweis zu führen, nehmen wir die Voraussetzung sowie die negation der Behauptung an und leiten daraus einen Widerspruch her. Darum nennt man einen solchen Beweis auch Widerspruchsbeweis.

Beachten Sie, dass es bei einem Widerspruchsbeweis ausreicht, Implikationen zu benutzen. Aussagenlogisch wollen zeigen, dass A gilt. Dafür nehmen wir an, dass $\neg A$ gilt und führen das zu einem Widerspruch: $\neg A \Rightarrow \mathtt{f}$. Aus der Logik wissen wir, dass wir den Implikationspfeil umkehren können, wenn wir beide Seiten negieren. Damit erhalten wir $\neg \mathtt{f} \Rightarrow \neg\neg A$, also $\mathtt{w} \Rightarrow A$. Voilà!

$\sqrt{2} \notin \mathbb{Q}$, Vorbereitung

Wir zeigen die Irrationalität von $\sqrt{2}$, d.h., $\sqrt{2} \notin \mathbb{Q}$. Wir zeigen, dass es keine Zahlen a, $b \in \mathbb{Z}$, $b \neq 0$ gibt, für die $a/b = \sqrt{2}$ gilt. Wir führen einen Widerspruchsbeweis: wir nehmen an, dass solche Zahlen existieren und zeigen, dass dies zu einem Widerspruch führt.

O.B.d.A. können wir annehmen, dass a und b teilerfremd sind, d.h., dass es kein $c \in \mathbb{Z}$ gibt, welches sowohl a als auch b teilt. Falls ein solches c existierte, könnten wir a und b damit kürzen und diesen Prozess fortsetzen, bis sie teilerfremd sind, ohne dass sich der Wert des Bruches ändert.

Außerdem können wir aufgrund der Positivität von $\sqrt{2}$ annehmen, dass sowohl a als auch b nicht-negativ sind, sonst könnten wir durch -1 kürzen. Aus dem gleichen Grunde ist auch klar, dass $a \neq 0$.

Damit können wir eine verfeinerte Behauptung treffen: es existieren keine a, $b \in \mathbb{N}$, die teilerfremd sind und für die $a/b = \sqrt{2}$ gilt.

$\sqrt{2} \notin \mathbb{Q}$, erster Schritt

Wir nehmen an, dass ein solches a/b existiert:

$$\frac{a}{b} = \sqrt{2}$$

Wir dürfen quadrieren, da a, $b \in \mathbb{N}$ sind:

$$\frac{a^2}{b^2} = 2$$
$$a^2 = 2b^2.$$

Somit ist a^2 eine gerade Zahl.

Das Produkt zweier natürlicher Zahlen ist ungerade gdw. beide Zahlen ungerade sind. Die Umkehrung gilt ebenso: das Produkt zweier natürlicher Zahlen ist gerade gdw. *mindestens eine der beiden* Zahlen gerade ist. Hier heißen beide Zahlen a und da ihr Produkt $a \cdot a = a^2$ gerade ist, muss auch a gerade sein.

D.h., es gibt ein $k \in \mathbb{N}$ mit $a = 2k$ und wir können schreiben

$$\begin{aligned} a^2 &= 2b^2 \\ (2k)^2 &= 2b^2 \\ 4k^2 &= 2b^2 \\ 2k^2 &= b^2. \end{aligned}$$

Also muss auch b eine gerade Zahl sein. Damit wäre 2 ein gemeinsamer Teiler von a und b. Dies steht aber im Widerspruch zu unserer Annahme. $\lightning$

Damit haben wir gezeigt, dass die Annahme $\sqrt{2} \in \mathbb{Q}$ zu einem Widerspruch führt. Somit muss die gegenteilige Aussage wahr sein und es folgt, dass $\sqrt{2} \notin \mathbb{Q}$. $\square$

Ringschluss

Wenn man mehrere Aussagen A_1, A_2, ..., A_n gegeben hat und zeigen will, dass sie alle äquivalent sind, so reicht es zu zeigen, dass:

$$A_1 \Rightarrow A_2$$
$$A_2 \Rightarrow A_3$$
$$A_{n-1} \Rightarrow A_n$$
$$\vdots$$
$$A_n \Rightarrow A_1.$$

Dies kann uns viel Arbeit sparen, da wir allein für die Äquivalenz von drei Aussagen A, B, C sechs Implikationen zeigen müssten:

$$A \Rightarrow B \qquad A \Rightarrow C \qquad B \Rightarrow C$$
$$B \Rightarrow A \qquad C \Rightarrow A \qquad C \Rightarrow B.$$

Ringschluss Beispiel: Behauptung

Seien A, B Mengen. Dann sind folgende Aussagen äquivalent:

- $A \subseteq B$
- $A \cap B = A$
- $A \cup B = B$

Ringschluss Beispiel: Beweis

Beweis: Wir zeigen, dass folgende Implikationen gelten:

- $A \subseteq B \Rightarrow A \cap B = A$:
  Da $A \subseteq B$ gilt, ist jedes Element aus A auch in B enthalten. Der Schnitt von A und B enthält alle Elemente, die in beiden Mengen liegen. Das ist offensichtlich die ganze Menge A.

Ringschluss Beispiel: Beweis

Beweis: Wir zeigen, dass folgende Implikationen gelten:

- $A \subseteq B \Rightarrow A \cap B = A$:
  Da $A \subseteq B$ gilt, ist jedes Element aus A auch in B enthalten. Der Schnitt von A und B enthält alle Elemente, die in beiden Mengen liegen. Das ist offensichtlich die ganze Menge A.
- $A \cap B = A \Rightarrow A \cup B = B$:
  Nach Voraussetzung besteht A nur aus Elementen, die auch in B enthalten sind. Daher fügt die Vereinigung mit A der Menge B keine weiteren Elemente hinzu.

Ringschluss Beispiel: Beweis

Beweis: Wir zeigen, dass folgende Implikationen gelten:

- $A \subseteq B \Rightarrow A \cap B = A$:
  Da $A \subseteq B$ gilt, ist jedes Element aus A auch in B enthalten. Der Schnitt von A und B enthält alle Elemente, die in beiden Mengen liegen. Das ist offensichtlich die ganze Menge A.
- $A \cap B = A \Rightarrow A \cup B = B$:
  Nach Voraussetzung besteht A nur aus Elementen, die auch in B enthalten sind. Daher fügt die Vereinigung mit A der Menge B keine weiteren Elemente hinzu.
- $A \cup B = B \Rightarrow A \subseteq B$:
  Da B gleich der Vereinigung von A und B ist, sind alle Elemente aus A auch in B enthalten. Das ist die Definition von $A \subseteq B$.

Damit haben wir den Ringschluss vollendet und die Äquivalenz aller drei Aussagen gezeigt.

Einige Fehler

Wie überall in der Mathematik warten auch bei den einfachsten Beweisen Fehler darauf, gemacht zu werden.[1] Hier ein kleines Best-Of als Warnung für die kommenden Jahre:

- Die zu zeigende Aussache annehmen oder im Beweis benutzen.
- Einen direkten Beweis als Widerspruchsbeweis verpacken[2]
- „Tunnelblick". Bloß, weil eine Schlussfolgerung schnell zum Ziel führt, ist sie noch lange nicht richtig. Ein Beweis ist keine Deduktion korrekter Informationen, sondern eine korrekte Deduktion von Informationen!
- Abuse of Notation! Bloß, weil eine Notation korrekt aussieht, macht sie nicht unbedingt Sinn.
- Aus Versehen durch 0 teilen. Manchmal sieht eine 0 gar nicht aus wie eine 0, oder ist in bestimmten Variablenwerten versteckt.
- Die letzte Folgerung in einem Ringschluss vergessen.
- Einen Satz verwenden, ohne die Voraussetzungen korrekt geprüft zu haben.

[1] Im besten Fall nur ein Mal.

[2] Das ist zwar nicht formal falsch, aber gilt als unsauberer Stil.

Letzte Hinweise zu Beweisen

Beweise sind zugleich Kunst und Handwerk. Es wird zwar nach Kreativität gefragt, aber man muss das Beweisen trotzdem üben! Versucht, einige der Aussagen aus den vergangenen Vorlesungen selbstständig zu beweisen.

Ein schönes Buch zum Thema: „Book of Proof" von Richard Hammack. Es ist nicht nur unglaublich gut geschrieben und simpel, es ist sogar kostenlos. Ich empfehle es seit Jahren jedem Ersti, der nicht schnell genug wegläuft:
https://www.people.vcu.edu/ rhammack/BookOfProof/index.html