

Vorkurs Theoretische Informatik

Grundlagen der Beweise

reloading 0 % complete...

Arbeitskreis Theo-Vorkurs

Mittwoch, 1. Oktober 2025

Fachgruppe Informatik Universität Stuttgart

1. Beweisen

Beweistechnik: Direkter Beweis

Beweistechnik: Kontraposition

Beweistechnik: Widerspruch

2. Mengenbeweise

Aufgaben

3. Wiederholung

Beweisen

reloading 3.45 % complete...

Aufgaben

Hier wird $3 = 0$ gefolgert. Was ist schief gelaufen?

Sei x aus $\mathbb{R}$

$$x^2 + x + 1 = 0$$

(es muss $x \neq 0$)

$$x(x^2 + x + 1) = x \cdot 0$$

($\cdot x$)

$$x^3 + x^2 + x = 0$$

$$x^3 + x^2 + x + 1 = 0 + 1$$

($+1$)

$$x^3 = 1$$

($\sqrt[3]{}$)

$$x = 1$$

Wir setzen unser Ergebnis oben ein und erhalten

$$1^2 + 1 + 1 = 3 = 0.$$

Beweisen



reloading 10.34 % complete...

Beweistechnik: Direkter Beweis

Zeige $A \implies B$ direkt

Setze A voraus und folgere dann schrittweise B .

Durch jede korrekte Folgerung, vergrößert sich die Menge der Aussagen, die wir weiterverwenden können.

Beispiel

Z.z.: $\forall n \in \mathbb{Z} : n \text{ ist gerade} \implies n^2 \text{ gerade.}$

1. Sei $n \in \mathbb{Z}$ beliebig.
2. Angenommen, n ist gerade.
3. $\implies \exists k \in \mathbb{Z} : n = 2k$
4. $\implies n^2 = (2k)^2 = 4k^2 = 2 \cdot 2k^2$
5. $\implies n^2$ ist gerade



Anmerkung: Zahl $n \in \mathbb{Z}$ heißt gerade, wenn es ein $k \in \mathbb{Z}$ gibt mit $n = 2k$.

Beweisen



reloading 13.79 % complete...

Beweistechnik: Kontraposition

Beweis durch Kontraposition

Zeige $A \implies B$, indem man stattdessen $\neg B \implies \neg A$ zeigt.

Beispiel

Z.z.: $\forall n \in \mathbb{N}: n^2 \text{ gerade} \implies n \text{ gerade}$

bzw. $\forall n \in \mathbb{N}: \neg(n \text{ gerade}) \implies \neg(n^2 \text{ gerade})$

1. Sei $n \in \mathbb{N}$ beliebig.
2. Angenommen, n ist nicht gerade.
3. $\implies n = 2k + 1$, für ein $k \in \mathbb{N}$
4. $\overset{\text{quadrieren}}{\leadsto} n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
5. $\implies n^2 = 2m + 1$, für $m = 2k^2 + 2k$
6. $\implies n^2$ ist ungerade.
7. Da $(\forall n \in \mathbb{N}: n \text{ ungerade} \implies n^2 \text{ ungerade})$ gilt,
folgt $(\forall n \in \mathbb{N}: n^2 \text{ gerade} \implies n \text{ gerade})$, was zu beweisen war. $\square$

Anmerkung: Zahl $n \in \mathbb{Z}$ heißt ungerade, wenn es ein $k \in \mathbb{Z}$ gibt mit $n = 2k + 1$.

Wieso dürfen wir das so machen?

Beweis

$$\text{Z.z.: } (\neg A \implies \neg B) \iff (B \implies A)$$

$$(\neg A \implies \neg B) \iff (\neg(\neg A) \vee \neg B)$$

$$\iff (A \vee \neg B)$$

$$\iff (\neg B \vee A)$$

$$\iff (B \implies A)$$

□

Erinnerung: $A \implies B$ kann man auch $\neg A \vee B$ schreiben.

Beweisen



reloading 20.69 % complete...

Beweistechnik: Widerspruch

Beweis durch Widerspruch

Zeige, dass A gilt, indem man zeigt dass $\neg A$ falsch ist.

Erinnerung: Eine Aussage ist entweder wahr oder falsch.

Wenn $\neg A$ falsch ist, muss A wahr sein.

Beispiel

Z. z. $\sqrt{2}$ ist irrational.

1. Ang. $\sqrt{2}$ ist rational.
2. Dann $\exists p \in \mathbb{Z} \ q \in \mathbb{Z} \setminus \{0\} : \sqrt{2} = \frac{p}{q} \wedge p, q$ sind teilerfremd
3. $\leadsto (\sqrt{2})^2 = (\frac{p}{q})^2 \implies 2 = \frac{p^2}{q^2} \iff 2q^2 = p^2$
4. $\leadsto p^2$ ist gerade $\leadsto p$ ist gerade
5. Also ist p^2 durch 4 teilbar $\leadsto 2q^2$ ist durch 4 teilbar
6. $\leadsto q^2$ ist gerade $\leadsto q$ ist gerade
7. $\leadsto p, q$ nicht teilerfremd $\leadsto$ Widerspruch

□

Hilfe! Der Beweis ist zu komplex! Was nun?

Manchmal lässt sich ein Beweis in kleinere Aussagen zerlegen. Wenn wir alle Teilaussagen beweisen, haben wir die Gesamtaussage gezeigt.

Beispiel

Z.z. für alle $n \in \mathbb{N}$ gilt, dass der Rest von $\frac{n^2}{4}$ entweder 0 oder 1 ist.

- **Fall 1:** n ist gerade

$$\begin{aligned} n^2 &= n \cdot n \stackrel{n \text{ gerade}}{=} (2k) \cdot (2k) = 4k^2, \text{ mit } k \in \mathbb{Z} \\ \implies \frac{4k^2}{4} &= k^2 \text{ Rest: } 0 \end{aligned}$$

- **Fall 2:** n ist ungerade

$$\begin{aligned} n^2 &= n \cdot n \stackrel{n \text{ ungerade}}{=} (2k+1) \cdot (2k+1) = (2k)^2 + 2(2k) + 1 = 4(k^2 + k) + 1, \\ \text{mit } k &\in \mathbb{Z} \\ \implies \frac{4(k^2+k)+1}{4} &= k^2 + k \text{ Rest: } 1 \end{aligned}$$

Da n nur gerade oder ungerade sein kann, ist der Rest von $\frac{n^2}{4}$ entweder 0 oder 1. □

Reicht nicht auch ein Beispiel als Beweis?

Wann ein Beispiel nicht ausreicht:

Zeige allgemeine Aussagen, also Aussagen der Form:

$\forall n \in \mathbb{N}$ gilt ..., $\neg \exists n \in \mathbb{N}$..., $\exists! n \in \mathbb{N}$..., etc.

Warum nicht?

Beispiele zeigen uns nur endlich viele Möglichkeiten.

„für alle gilt...“, „es existiert kein...“, „es existiert genau ein...“, etc.

sind meist zu allgemeine Aussagen um sie mit endlich vielen Beispielen lückenlos zu beweisen.

Reicht nicht auch ein Beispiel als Beweis?

Wann ein Beispiel ausreichen kann:

Zeige nicht allgemeine Aussagen der Form:

$\exists n \in \mathbb{N}, \neg \forall n \in \mathbb{N}$ gilt, ...

Warum?

„es gibt ein Element, sodass...“, „für nicht alle Element gilt...“
wären durch Angabe eines solchen Elements gezeigt.

$\leadsto$ will man zeigen, dass eine Aussage falsch ist, sind die Formen entsprechend negiert.

$$3 + 4 \equiv 1 \pmod{6}$$

Das bedeutet so viel wie:

$$(3 + 4) \% 6 = 1 \% 6$$

Aufgaben

Welche Beweistechnik könnte sich für die folgenden Aussagen eignen? Warum?

Einfach

- Alle $6n + 1$ für ungerade $n \in \mathbb{N}$ und $n > 0$ sind Primzahlen.

Normal

- Für jede ganze Zahl x gilt $x \equiv 1 \pmod{4} \implies x \equiv 1 \pmod{2}$

Etwas schwerer

- Für alle $n \in \mathbb{N}$ mit $n > 0$ gilt n teilt $5n + 22!$.

Mengenbeweise



Reminder: Äquivalente Schreibweisen von Mengenoperationen

Oft benötigen wir eine Aussagenlogische Äquivalente Bedingung von Mengenoperationen. Dafür nehmen wir mal die Obermenge $\mathbb{N}$

Operationen

- **Teilmenge:** $A \subseteq B \rightsquigarrow \forall x \in \mathbb{N} : x \in A \implies x \in B$
- **Vereinigung:** $A \cup B \rightsquigarrow \forall x \in \mathbb{N} : x \in A \cup B \iff x \in A \vee x \in B$
- **Schnitt:** $A \cap B \rightsquigarrow \forall x \in \mathbb{N} : x \in A \cap B \iff x \in A \wedge x \in B$
- **Komplement:** $\bar{A} \rightsquigarrow \forall x \in \mathbb{N} : x \in \bar{A} \iff x \notin A$

Zu zeigen: Schnitt ist kommutativ, d.h. $A \cap B = B \cap A$

„ $\implies$ “ :

$$\begin{aligned}x \in A \cap B &\implies x \in A \wedge x \in B \\&\implies x \in B \wedge x \in A \\&\implies x \in B \cap A\end{aligned}$$

„ $\longleftarrow$ “ :

$$\begin{aligned}x \in B \cap A &\implies x \in B \wedge x \in A \\&\implies x \in A \wedge x \in B \\&\implies x \in A \cap B\end{aligned}$$

□

Anmerkung: $\wedge$ ist kommutativ

Zu zeigen: $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

$$\begin{aligned}x \in A \setminus (B \cup C) &\iff x \in A \wedge \neg(x \in B \cup C) \\&\iff x \in A \wedge \neg(x \in B \vee x \in C) \\&\iff x \in A \wedge \neg(x \in B) \wedge \neg(x \in C) \\&\iff x \in A \wedge \neg(x \in B) \wedge x \in A \wedge \neg(x \in C) \\&\iff (x \in A \wedge \neg(x \in B)) \wedge (x \in A \wedge \neg(x \in C)) \\&\iff (x \in A \setminus B) \wedge (x \in A \setminus C) \\&\iff x \in (A \setminus B) \cap (A \setminus C)\end{aligned}$$

□

Rechenregel: $\neg(A \wedge B) \iff \neg A \vee \neg B,$
 $\neg(A \vee B) \iff \neg A \wedge \neg B$

Aufgaben

Versuche dich an den folgenden Mengenbeweisen.

Normal

- $\overline{\overline{A}} = A$

Etwas schwerer

- $A \cap B = \overline{(\overline{A} \cup \overline{B})}$

Ein weiterer Mengenbeweis...

Aufgabe

$$M_1 = \{6m \mid m \in \mathbb{N}\}$$

$$M_2 = \{2n \mid n \in \mathbb{N}\}$$

Zu zeigen:

$$M_1 \subsetneq M_2$$

$$\text{d.h. } (\forall x : x \in M_1 \implies x \in M_2) \wedge (\exists x : x \in M_2 \wedge x \notin M_1)$$

$$\forall x : x \in M_1 \implies x \in M_2$$

Sei x beliebig.

Angenommen, $x \in M_1$.

Es gilt: $x = 6m = 2 \cdot 3 \cdot m = 2 \cdot (3m)$

Da $m \in \mathbb{N}$, setze $n = 3m$

Daraus folgt: $x = 2n$

$\leadsto x \in M_2$

$$\exists x : x \in M_2 \wedge x \notin M_1$$

Beweis durch Angabe eines Gegenbeispiels: $x = 2$

$x \in M_2$, für $n = 1$, da $x = 2 \cdot 1 \in M_2$,

aber $6m = 2$ mit $m = \frac{2}{6} = \frac{1}{3} \notin \mathbb{N}$

$\leadsto x \notin M_1$

Da gezeigt wurde:

$$\forall x : x \in M_1 \implies x \in M_2$$

und

$$\exists x : x \in M_2 \wedge x \notin M_1$$

gilt $M_1 \subsetneq M_2$.

Aufgabe

Versuche dich an folgendem Mengenbeweis.

Etwas Schwerer

$$M_1 = \{l \in \mathbb{Z} \mid l \text{ ist gerade}\}$$

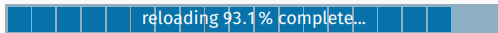
$$M_2 = \{n \in \mathbb{Z} \mid n \text{ ist durch 3 teilbar}\}$$

$$M_3 = \{m \in \mathbb{Z} \mid m \text{ ist durch 6 teilbar}\}$$

Zu zeigen: $M_1 \cap M_2 = M_3$

$$\text{d.h. } (\forall x : x \in M_1 \cap M_2 \Rightarrow x \in M_3) \wedge (\forall x : x \in M_3 \Rightarrow x \in M_1 \cap M_2)$$

Wiederholung



Grundlagen Beweise

- Was ist die Idee der Kontraposition?
- Was ist die Idee des Widerspruchsbeweis?
- Wann reicht ein Beispiel als Beweis?

Mengenbeweise

- Wie werden die Mengenoperationen mit Hilfe Aussagenlogik geschrieben?
- Wie können wir Beziehungen von Mengen zueinander beweisen?
- Welche (Teil-)Aussagen/Schritte müssen wir Beweisen um die Gleichheit/Teilmengenbeziehung zweier Mengen zu beweisen?

Glossar — Mengen

Abk.	Bedeutung	Was?!
$\mathbb{N}$	natürliche Zahlen (mit 0)	In der theoretischen Informatik enthält $\mathbb{N}$ die 0: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ (Auch $\mathbb{N}_0$)
$\mathbb{Z}$	ganze Zahlen	$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
$\mathbb{R}$	reelle Zahlen	$\mathbb{R} = \{\text{z.B. } 2, -3, \sqrt{17}, \pi, \text{ usw.}\}$
$\emptyset$	$\{\}$	leere Menge
$a b$	teilt	a ist Teiler von b , d.h. a teilt b ohne Rest
:	sodass	z.B. $\forall a, b \in \mathbb{Z} : a b$

Glossar — Mengenoperationen

Abk.	Bedeutung	Was?!
$A \subseteq B$	Teilmenge	Alle Elemente aus A sind auch in B enthalten. Dabei können die Mengen auch gleich sein.
$A \subsetneq B$	echte Teilmenge	$A \subseteq B$. Und zusätzlich enthält B Elemente, die nicht in A enthalten sind. $\implies$ Mengen sind nicht gleich!
$A \subset B$	Teilmenge <u>oder</u> echte Teilmenge	Bei manchen Leuten $\subseteq$, bei manchen $\subsetneq$. Mehrdeutig, lieber nicht verwenden!
$A \cap B$	Schnitt	Enthält alle Elemente, die in A <i>und</i> in B enthalten sind
$A \cup B$	Vereinigung	Enthält alle Elemente, die in A , B oder beiden enthalten sind
$A \setminus B$	Komplement, gespr. "A ohne B"	Enthält alle Elemente aus A , die <i>nicht</i> in B enthalten sind
$\overline{B}$	B Komplement	Enthält alle Elemente aus einer geg. Obermenge, die <i>nicht</i> in B enthalten sind

Glossar — Aussagenlogik (Operatoren)

Abk.	Bedeutung	Was?!
$A \wedge B$	<i>A und B</i>	A und B müssen wahr sein, damit die Gesamtaussage wahr ist
$A \vee B$	<i>A oder B</i>	Es müssen mindestens A, B oder beide wahr sein
$\neg A$	<i>nicht A</i>	A muss falsch sein, damit $\neg A$ wahr ist
$B \implies B$	A ist notwendig für B	A muss wahr sein, wenn B wahr ist
$A \implies B$	A ist hinreichend für / impliziert B	B muss wahr sein, wenn A wahr ist
$A \iff B$	notwendig und hinreichend	genau dann, wenn

Glossar — Aussagenlogik (Sprachlich)

Abk.	Bedeutung	Was?!
$A \text{ gdw. } B$	genau dann, wenn	Äquivalenz zwischen Aussagen
$A \text{ ist notwendig für } B$	$B \implies A$	A muss wahr sein, wenn B wahr ist
$A \text{ ist hinreichend für } B$	$A \implies B$	B muss wahr sein, wenn A wahr ist
notwendig und hinreichend	$A \iff B$	genau dann, wenn

Glossar — Quantoren

Abk.	Bedeutung	Was?!
$\forall x \in M : A(x)$	Für alle x aus M gilt $A(x)$	Die Aussage A muss für alle Elemente der Menge M wahr sein
$\exists x \in M : A(x)$	Es existiert ein x in M für das $A(x)$ gilt	Die Aussage $A(x)$ muss für mind. 1 (oder mehr) Elemente wahr sein
$\forall x, y \in M : A(x, y)$	Für alle x und alle y gilt $A(x, y)$	Äquivalent zu $\forall x \forall y : A(x, y)$

Abk.	Bedeutung	Was?!
z.z. Sei	zu zeigen	Was zu beweisen ist bereits bekannte Objekte werden eingeführt und benannt
$\exists$	es gibt ein	
$\exists!$	es gibt genau ein	
x ist genau y	$x = y$	<u>genau</u> wird verwendet bei Äquiva- lenz
x ist eindeutig	$\exists!x$	

Glossar — Beweise

Abk.	Bedeutung	Was?!
œ	ohne Einschränkung	die Allgemeinheit der Aussage wird nicht durch getroffene Aussagen eingeschränkt
o.B.d.A.	ohne Beschränkung der Allgemeinheit	wie œ
trivial	offensichtlich	Beweisschritte, welche keine weitere Begründung brauchen. (nicht verwenden!)
□	Mic Drop	Kommt am Ende eines erfolgreichen Beweises
q.e.d.	quod erat demonstrandum	Was zu beweisen war

Gestalt	mögliches Vorgehen
nicht F	Zeige, dass F nicht gilt.
F und G	Zeige F und G in zwei getrennten Beweisen.
$F \implies G$	Füge F in die Menge der Annahmen hinzu und zeige G.
F oder G	Zeige: nicht $F \implies G$. (Alternativ zeige: nicht $G \implies F$)
$F \iff G$	Zeige: $F \implies G$ und $G \implies F$.
$\forall x \in A : F$	Sei x ein beliebiges Element aus A. Zeige dann F.
$\exists x \in A : F$	Sei x ein konkretes Element aus A. Zeige dann F.

Lizenz

- Unsere Folien sind frei!
- Jeder darf die Folien unter den Bedingungen der **GNU General Public License v3** (oder jeder späteren Version) weiterverwenden.
- Ihr findet den Quelltext unter
<https://www.github.com/FIUS/theo-vorkurs-folien>