

Vorkurs Theoretische Informatik

Grundlagen der Beweise

Arbeitskreis Theo-Vorkurs

Dienstag, 11. Oktober 2022

Fachgruppe Informatik Universität Stuttgart

1. Quantoren

2. Beweisen

Beweisbeispiel: Transitivität der Teilmenge

Beweistechnik: Direkter Beweis

Beweistechnik: Kontraposition

Beweistechnik: Widerspruch

3. Mengenbeweise

Aufgaben

4. Wiederholung

Quantoren

Oft wollen wir Aussagen nicht nur für ein Element, sondern für viele Elemente treffen.

Beispiel

A_1 : Für die Zahl 5 gilt: Sie hat einen Nachfolger

Allgemeiner:

A_2 : Für jede natürliche Zahl n gilt: n hat einen Nachfolger

Beispiel

A_3 : Für die Zahl 5 gilt: Sie ist eine Primzahl

Allgemeiner:

A_4 : Es gibt eine natürliche Zahl n , so dass gilt: n ist eine Primzahl

Mithilfe von **Quantoren** vereinfachen wir uns die Schreibweise dieser Aussagen.

Quantor \forall : Die Aussage gilt für alle Elemente.

Beispiel

$A_1: \forall k \in \mathbb{N} : 2k \text{ ist gerade}$

Quantor \exists : Die Aussage gilt für mindestens ein Element.

Beispiel

$A_2: \exists k \in \mathbb{N} : k \text{ ist Primzahl}$

In einer Aussage können mehrere Quantoren vorkommen.
Wir lesen dann von links nach rechts.

Beispiel

$$A_1: \forall x, y \in \mathbb{N} : \exists z \in \mathbb{N} : x + y = z$$

Bedeutung: Für zwei beliebige Zahlen x und y aus \mathbb{N} gibt es eine weitere natürliche Zahl z , so dass $x + y = z$ gilt.

Achtung!

Die Reihenfolge von zwei Quantoren zu vertauschen, kann die Bedeutung einer Aussage deutlich verändern.

Beispiel

$x, y \in \text{Studenten}$

$A_1: \forall x \exists y : x \text{ schlägt } y$

$A_2: \exists x \forall y : x \text{ schlägt } y$

Was ist der Unterschied zwischen beiden Aussagen?

Aufgabe

Wir formulieren folgende Aussage mithilfe von Quantoren und den Symbolen der Aussagenlogik (Junktoren).

Beispiel

- A_1 : Eine ganze Zahl ist eine natürliche Zahl, wenn sie positiv oder null ist.

Hinführung

- A_1 : Für alle ganzen Zahlen x gilt: Wenn x positiv oder null ist, ist x eine natürliche Zahl.

Lösung

- $A_1: \forall x \in \mathbb{Z} : x \geq 0 \implies x \in \mathbb{N}$

Aufgaben

Formuliere folgende Aussagen mithilfe von Quantoren und den Symbolen der Aussagenlogik (Junktoren).

Normal

- A_1 : Die Differenz zweier ganzer Zahlen ist wieder eine ganze Zahl.

Schwer

- A_2 : Jede natürliche Zahl lässt sich als Summe von vier Quadratzahlen darstellen.

Da haben selbst wir keinen Bock drauf

- A_3 : Eine natürliche Zahl, die von einer von ihr verschiedenen natürlichen Zahl größer als 1 geteilt wird, ist nicht prim.

Äquivalente Schreibweisen von Mengenoperationen

Oft benötigen wir eine Aussagenlogische Äquivalente Bedingung von Mengenoperationen. *Dafür nehmen wir mal die Obermenge Σ^**

Operationen

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

Beweisen

Was ist ein Beweis?

- lückenlose Folge von logischen Schlüssen, welche zur zu beweisenden Behauptung führen
- nicht nur einleuchtend, sondern zweifelsfrei korrekt

Warum Beweisen?

- Aussage basierend auf Fakten und nicht subjektiv belegen
- Bestätigung von Aussagen für weitere Nutzung

Zu zeigen: Teilmengen sind transitiv.

1. z.z. $A \subseteq B \wedge B \subseteq C \implies A \subseteq C$

2. $\iff ((\forall x: x \in A \implies x \in B) \wedge (\forall x: x \in B \implies x \in C))$
 $\implies (\forall x: x \in A \implies x \in C)$

3. Ang., $A \subseteq B \wedge B \subseteq C$.

4. Sei x beliebig

5. $\implies x \in B \implies x \in C$

□

Aufgaben

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

Sei x aus \mathbb{R}

$$x^2 + x + 1 = 0 \quad (\text{es muss } x \neq 0)$$

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

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

$$x^3 + x^2 + x + 1 = 0 + 1 \quad (+1)$$

$$x^3 = 1 \quad (\sqrt[3]{\quad})$$

$$x = 1$$

Wir setzen unser Ergebnis oben ein und erhalten

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

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 $n = 2k$.

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. $\overset{\text{quadrieren}}{\rightsquigarrow} n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
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.

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 $\exists p, q \in \mathbb{Z} : \sqrt{2} = \frac{p}{q} \wedge p, q$ sind teilerfremd
3. $\rightsquigarrow (\sqrt{2})^2 = (\frac{p}{q})^2 \iff 2 = \frac{p^2}{q^2} \iff 2q^2 = p^2$
4. $\rightsquigarrow p^2$ ist gerade $\rightsquigarrow p$ ist gerade
5. Also ist p^2 durch 4 teilbar $\rightsquigarrow 2q^2$ ist durch 4 teilbar
6. $\rightsquigarrow q^2$ ist gerade $\rightsquigarrow q$ ist gerade
7. $\rightsquigarrow p, q$ nicht teilerfremd \rightsquigarrow 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

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

- **Fall 2:** n ist ungerade

$$n^2 = n \cdot n \stackrel{n \text{ ungerade}}{=} (2k+1) \cdot (2k+1) = (2k)^2 + 2(2k) + 1 = 4(k^2 + k) + 1,$$

mit $k \in \mathbb{Z}$

$$\implies \frac{4(k^2+k)+1}{4} = k^2 + k \text{ Rest: } 1$$

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.

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

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

„ \implies “:

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

„ \impliedby “:

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

□

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

$$L_1 = \{w^n \mid n \in \mathbb{N}, w \in \{aaaa\}\}$$

$$L_2 = \{w \mid |w| \equiv 0 \pmod{4}, w \in \{a\}^*\}$$

Zu zeigen: $L_1 = L_2$

$$\text{d.h. } (\forall x : x \in L_1 \implies x \in L_2) \wedge (\forall x : x \in L_2 \implies x \in L_1)$$

Weiterer Mengenbeweis

$$\forall x : x \in L_1 \implies x \in L_2$$

Sei x beliebig.

Angenommen, $x \in L_1$.

Es gilt: $w \in \{aaaa\}$. Damit gilt $|w| = 4$. Es folgt $|x| = |w^n| = |w| \cdot n = 4 \cdot n$ mit $n \in \mathbb{N}$. Daraus folgt $|x| \equiv 0 \pmod{4}$. Weiterhin gilt $(aaaa)^n \in \{a\}^*$.

$$\leadsto x \in L_2$$

$$\forall x : x \in L_2 \implies x \in L_1$$

Sei x beliebig.

Angenommen, $x \in L_2$.

Es gilt: $|x| \equiv 0 \pmod{4}$.

Damit gilt $|x| = 4 \cdot n = |w| \cdot n = |w^n|$ mit $w \in \{aaaa\}$ und $n \in \mathbb{N}$.

Weiterhin gilt $w \in \{a\}^*$.

$$\leadsto x \in L_1$$

Da gezeigt wurde:

$$\forall x : x \in L_1 \implies x \in L_2$$

und

$$\forall x : x \in L_2 \implies x \in L_1$$

gilt $L_1 = L_2$.

Aufgaben

Versuche dich an folgenden Mengenbeweisen.

Etwas Schwerer

$$L_1 = \{a^n b^m \mid n < m \text{ mit } n, m \in \mathbb{N}\}$$

$$L_2 = \{w \mid |w|_a < |w|_b, w \in \{a, b\}^*\}$$

Zu zeigen: $L_1 \subsetneq L_2$

Schwer

$$L_1 = \{a^n b^n \mid n \in \mathbb{N}\}$$

$$L_2 = \{w \in \{a, b\}^* \mid |w|_a = |w|_b\}$$

$$L_3 = \{a^k b^l \mid k, l \in \mathbb{N}\}$$

Zu zeigen: $L_1 = L_2 \cap L_3$

Wiederholung

Grundlagen Beweise

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

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	$x = y$	<i>genau</i> wird verwendet bei Äquivalenz
x ist eindeutig der, die, das	$\exists!x$	bestimmte Artikel weisen auf Eindeutigkeit hin
gdw.	genau dann, wenn	Äquivalenz zwischen Aussagen

Abk.	Bedeutung	Was?!
A ist notwendig für B	$B \implies A$	A muss wahr sein, wenn B wahr ist
A ist hinreichend für B	$A \implies B$	B muss wahr sein, wenn A wahr ist
notwendig und hinreichend	$A \iff B$	genau dann, wenn

Abk.	Bedeutung	Was?!
∅	ohne Einschränkung	die Allgemeinheit der Aussage wird nicht durch getroffene Aussagen eingeschränkt
o.B.d.A.	ohne Beschränkung der Allgemeinheit	wie ∅
trivial	offensichtlich	Beweisschritte, welche keine weiter 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.

- 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`