Diskrete Strukturen und Logik

WiSe 2006/07 in Trier

Henning Fernau
Universität Trier
fernau@informatik.uni-trier.de

Diskrete Strukturen und Logik Gesamtübersicht

- Organisatorisches
- Einführung
- Logik & Mengenlehre
- Beweisverfahren
- Kombinatorik: Die Kunst des Zählens
- algebraische Strukturen

Beweisverfahren — Eine Übersicht

Direkter Beweis
Beweis durch Umkehrschluss
Widerspruchsbeweis (Indirekter Beweis)
Fallunterscheidungen
Schubfachprinzip
Induktion

Was wollen wir beweisen ?

Die zu beweisende Aussage ist oft von der Form $\mathrm{p} \Rightarrow \mathrm{q}$.

Hinweis: Manchmal ist p nicht ausdrücklich angegeben.

Ohne jedwede Annahmen kann man aber nichts beweisen (wollen).

p ist dann (implizit) z.B. durch *Grundannahmen* (*Axiome*) gegeben.

Es “hilft” auch manchmal die Tautologie $\mathrm{q} \equiv (\mathrm{t} \Rightarrow \mathrm{q})$.

Manchmal sind auch *Äquivalenzaussagen* zu zeigen: $\mathrm{p} \iff \mathrm{q}$:
Hierzu verwendet man meist die Tautologie $(\mathrm{p} \iff \mathrm{q}) \equiv ((\mathrm{p} \to \mathrm{q}) \wedge (\mathrm{q} \to \mathrm{p}))$.

Einfachste Beweise für $p \Rightarrow q$. (interessant für “Induktionsanfänge”)

Inhaltsleerer Beweis: Wir zeigen: p ist stets falsch.
Betrachte Aussageformen $p(n) := (n > 1)$ und $q(n) := (n^3 > n)$.
$p(0) \to q(0)$ durch inhaltsleeren Beweis.

Trivialer Beweis: Wir zeigen: q ist wahr, unabhängig von p.
Betrachte $p := (0 < a \leq b)$ und $q(n) := (a^n \leq b^n)$.
$\rightsquigarrow q(0) = (a^0 \leq b^0) = (1 \leq 1)$ ✓

Direkter Beweis

Die zu beweisende Aussage ist von der Form $\mathrm{p} \Rightarrow \mathrm{q}$.

Erinnerung: Eine Implikation ist nur dann falsch, wenn p wahr ist und q falsch.

$\rightsquigarrow$ zu untersuchender Fall (Annahme): p ist wahr.

Aus dieser Annahme muss jetzt gefolgert werden, dass q wahr ist.

Dann ist nämlich die Implikation wahr.

Der Beweis selbst hat oft die Form von Schlussketten, auf die dann der *modus ponens* angewendet wird.

Es seien a, b ganze Zahlen. a heißt durch b *teilbar* gdw. b *teilt* a, i.Z. $b \mid a$, gdw. es gibt eine ganze Zahl k mit $a = b \cdot k$.

Direkter Beweis — Ein einfaches Beispiel

Es sei a eine ganze Zahl. $(6 \mid a) \Rightarrow (3 \mid a)$.

Schlusskette:

$$\begin{aligned}(6 \mid a) \quad &\Rightarrow (\exists k(a = 6k)) \quad \Rightarrow (\exists k(a = (3 \cdot 2) \cdot k)) \Rightarrow (\exists k(a = 3 \cdot (2 \cdot k))) \\ &\Rightarrow (\exists k'(a = 3k')) \quad \Rightarrow (3 \mid a).\end{aligned}$$

Warum sind die einzelnen Schritte richtig ?
Wie schreibt man einen Beweis in Prosa auf ?

Direkter Beweis —

Ein weiteres Beispiel aus der *Zahlentheorie* (Restklassenarithmetik)

Lemma: Gilt $t \mid n$ und $t \mid m$, so auch $t \mid (n + m)$.

Beweis: 1. $(t \mid n) \Rightarrow (\exists k_n (n = t \cdot k_n))$.
2. $(t \mid m) \Rightarrow (\exists k_m (m = t \cdot k_m))$.
Aus 1. und 2. folgt:

$$n + m = t \cdot k_n + t \cdot k_m = t(k_n + k_m)$$

$\rightsquigarrow \exists k((n + m) = t \cdot k)$ (wähle $k = k_m + k_m$)

$\rightsquigarrow t \mid (n + m)$.

Analog: Lemma: Gilt $t \mid n$ und $t \mid m$, so auch $t \mid (n - m)$.

Zum Umgang mit Quantoren

Viele mathematische Aussagen haben die Gestalt von *Allaussagen*:

$$\forall x(p(x) \Rightarrow q(x)) \qquad (*)$$

Man beweist sie, indem man die Aussage $p(a) \Rightarrow q(a)$ für jedes a aus dem zugrundeliegenden Universum beweist.

Das liefert folgende Beweisstruktur:

1. Wähle a beliebig aus dem Universum.
2. Beweise die Implikation $p(a) \Rightarrow q(a)$.
3. Da a beliebig gewählt werden kann, folgt $(*)$.

Daher liefert der vorige Beweis die Aussage: $\forall x \in \mathbb{Z}((6 \mid x) \Rightarrow (3 \mid x))$.

direkter Beweis mit Allquantor

Lemma: (Einsteiler) $\forall t \in \mathbb{N}(t \mid 1 \implies t = 1)$.

Beweis: Wähle $t \in \mathbb{N}$ beliebig.

$t \mid 1 \rightsquigarrow \exists k(1 = tk) \rightsquigarrow \exists k(1/t = k)$

$\rightsquigarrow$ (Universum!) $t = 1$

Zum Umgang mit Quantoren

Manche mathematische Aussagen haben die Gestalt von *Existenzaussagen*:

$$[p \implies](\exists x(q(x)))$$

Solche Aussagen lassen sich oft *konstruktiv* beweisen.

Eine natürliche Zahl n heißt *zusammengesetzt* gdw. $\exists t \in \mathbb{N}((1 < t < n) \wedge (t|n))$.

Satz: Zu jeder natürlichen Zahl n gibt es n aufeinander folgende zusammengesetzte Zahlen.

Etwas formaler: $\forall n(\exists k(\forall i \in \{1, \ldots, n\}(\text{zusammengesetzt}(k + i))))$.

Beweis: Wähle $k = (n + 1)! + 1$. $\rightsquigarrow \forall i \in \{1, \ldots, n\}((i + 1) \mid (k + i))$.
(Denn $(i + 1) \mid (k - 1)$ und $(i + 1) \mid (i + 1)$, s. vorvoriges Lemma.)

Zum Umgang mit Quantoren

Manche mathematische Aussagen haben die Gestalt von *Existenzaussagen*:

$$\exists x(p(x) \Rightarrow q(x)) \qquad (*)$$

Man beweist sie, indem man die Aussage $p(a) \Rightarrow q(a)$ für *irgendein geeignet gewähltes* a aus dem zugrundeliegenden Universum beweist.

Das liefert folgende Beweisstruktur:

1. Wähle a geeignet aus dem Universum.
2. Beweise die Implikation $p(a) \Rightarrow q(a)$.
3. Da a speziell gewählt wurde, folgt $(*)$.

Beweis durch Umkehrschluss (Kontraposition)

Erinnerung: Tautologie $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$

Lemma: Ist eine Quadratzahl ungerade, so auch ihre Wurzel.

Was bedeutet dieser Satz ? Ausführliche Schreibweise:

Es sei a *eine natürliche Zahl.*
Wenn a^2 *eine ungerade Zahl ist, dann ist* a *ungerade.*

Wir haben also die Aussage(forme)n:
$p(a) := (a^2$ ist ungerade$)$ und $q(a) := (a$ ist ungerade$)$.
Unser Satz lautet also: $\forall a \in \mathbb{N}(p(a) \Rightarrow q(a))$.

Kontraposition $\rightsquigarrow \forall a \in \mathbb{N}(\neg q(a) \Rightarrow \neg p(a))$.

Beweis durch Umkehrschluss (Kontraposition) (Forts. des Bsp.)

Zu zeigen ist also: *Es sei* a *eine natürliche Zahl.*
Wenn a *keine ungerade Zahl ist, dann ist* a^2 *nicht ungerade.*
Dies ist offensichtlich eine komplizierte Formulierung für:
Ist a gerade, so auch a^2.
Eine Zahl a heißt *gerade* gdw. $2 \mid a$.

Beweis: a gerade $\Rightarrow (\exists k(a = 2k)) \Rightarrow (\exists k(a \cdot a = (2k) \cdot a)) \Rightarrow (\exists k(a^2 = 2 \cdot (ka))) \Rightarrow a^2$ gerade.

Hinweis: Verallgemeinerung: Ist t kein Teiler von a^2, so auch nicht von a.

Satz: Eine Quadratzahl ist genau dann gerade, wenn ihre Wurzel gerade ist.

Beweis durch Widerspruch (indirekter Beweis, reductio ad absurdum)

Erinnerung: Tautologie $(p \Rightarrow q) \equiv ((p \wedge \neg q) \Rightarrow f)$; klassisches Falsum: $r \wedge \neg r$

Satz: $\sqrt{2}$ ist irrational.

Beweis: Mit $p = t$ und $q =$ "$\sqrt{2}$ ist irrational" müssen wir die Annahme, $x = \sqrt{2}$ wäre rational, zum Widerspruch führen.

x rational $\rightsquigarrow$ es gibt *teilerfremde* $a, b \in \mathbb{Z} : x = a/b$.

$\rightsquigarrow 2 = x^2 = a^2/b^2 \rightsquigarrow 2b^2 = a^2$

$\rightsquigarrow a^2$ ist gerade $\rightsquigarrow a$ ist gerade (s. obiger Satz)

$\rightsquigarrow a = 2c$ für eine ganze Zahl $c \rightsquigarrow 2b^2 = 4c^2$

$\rightsquigarrow b^2 = 2c^2 \rightsquigarrow b^2$ ist gerade $\rightsquigarrow b$ ist gerade

Also: 2 ist Teiler von a und von b, im Widerspruch zur Wahl von a und b.

Beweis durch Widerspruch (indirekter Beweis, reductio ad absurdum)

Lemma: Für jede natürliche Zahl t und jede natürliche Zahl n gilt: Wenn $t \geq 2$ und wenn t ein Teiler von n ist, dann ist t kein Teiler von $n+1$.

Beweis: Unsere Aussage lautet formal (mit Universum $\mathbb{N}$):

$$\forall n \forall t((t \geq 2) \wedge (t \mid n)) \implies \neg(t \mid n+1).$$

Dies ist logisch äquivalent zu:

$$\forall n \forall t(t \geq 2) \implies ((t \mid n)) \implies \neg(t \mid n+1)).$$

Wähle t, n beliebig mit $t \geq 2$. Führe einen Widerspruchsbeweis für die verbleibende Implikation.

$\rightsquigarrow$ Nimm an: $(t \mid n) \wedge (t \mid n+1)$.

$\rightsquigarrow$ $t \mid (n+1) - n \rightsquigarrow$ (Lemma Restklassenarithmetik) $t \mid 1$

$\rightsquigarrow$ (Universum ! und Lemma Einsteiler) $t = 1$ Widerspruch !

Beweis durch Widerspruch (indirekter Beweis, reductio ad absurdum)

Allgemeine Hinweise

Erinnerung: Tautologie $(p \Rightarrow q) \equiv ((p \wedge \neg q) \Rightarrow f)$; klassisches Falsum: $r \wedge \neg r$

Ist p nicht (explizit) vorhanden, setzen wir $p = t$; um q zu beweisen, zeigen wir daher $\neg q \Rightarrow f$.

Wir können einen Beweis durch Kontraposition als Widerspruchsbeweis lesen: Haben wir $\neg q \Rightarrow \neg p$ gezeigt, so gilt auch:

$$(p \wedge \neg q) \Rightarrow (p \wedge \neg p)$$

In obiger Beweisfigur haben wir also $r = p$.
Umgekehrt ist ein Widerspruchsbeweis der Form $\neg q \Rightarrow f$ auch ein Umkehrschluss der Implikation $(t \Rightarrow q) \equiv q$.

Der Satz von Euklid

Satz: Es gibt unendlich viele Primzahlen.

Wie können wir diese Aussage formal aufschreiben ?

$\mathbb{N}$: Menge der natürlichen Zahlen
$\mathbb{P} \subseteq \mathbb{N} \setminus \{0, 1\}$: Menge der *Primzahlen*
$p \in \mathbb{P} \iff \forall q \in \mathbb{N}(q|p \implies (q = 1 \vee q = p))$.

Der Satz von Euklid lässt sich also wie folgt notieren (mit Universum $\mathbb{N}$):

Der Satz von Euklid — ein *nicht-konstruktiv*er Existenzbeweis für $\forall n \exists p((n < p) \wedge p \in \mathbb{P})$.

Die Negation lautet daher: $\exists n \forall p((n \geq p) \vee p \notin \mathbb{P})$.
Diese Aussage ist äquivalent zu:

$$\exists n \forall p(p \in \mathbb{P} \implies (p \leq n)).$$

Beweis: M.a.W.: Es gäbe dann eine größte Primzahl p_k, d.h.: $\mathbb{P} = \{p_1, \ldots, p_k\}$.
Setze $b := p_1 \cdot \cdots \cdot p_k + 1$.
Da $b > p_k$, gilt $b \notin \mathbb{P}$. $\rightsquigarrow \exists 1 < t < b(t \mid b)$.
Wir können annehmen, dass $t \in \mathbb{P}$ (Warum ? s.u.).
Nach vorigem Lemma ist t kein Teiler von $b - 1 = p_1 \cdot \cdots \cdot p_k$.
$\rightsquigarrow t \notin \mathbb{P}$. Widerspruch !

Das Königsberger Brückenproblem

Satz: In einer Stadt (gegeben durch Gebiete und Brücken) gibt es einen Spaziergang, auf dem jede der Brücken genau einmal gequert wird, gdw. die Eulerbedingung gilt und es zwischen je zwei Gebieten einen Weg gibt (Zusammenhang).

Das Königsberger Brückenproblem

Die entsprechenden Dateien finden Sie original hier.