



Title: Mayr: 2012 ds (30.10.2012)

Date: Tue Oct 30 13:45:17 CET 2012

Duration: 85:22 min

Pages: 32

Diskrete Strukturen

Ernst W. Mayr

Fakultät für Informatik
TU München

<http://www14.in.tum.de/lehre/2012WS/ds/>

Wintersemester 2012



4.6 Beweistechniken

Die meisten mathematischen Behauptungen sind von der Form

$$A \Rightarrow B \text{ bzw. } (A_1 \wedge \dots \wedge A_k) \Rightarrow B.$$

Um $A \Rightarrow B$ zu beweisen, können wir zeigen:



Bemerkungen:

- 1 Die Bedeutung von \equiv (und damit \neq) ist klar. \equiv wird oft, vor allem in Beweisen, auch als \Leftrightarrow geschrieben (im Englischen: iff, if and only if).
- 2 Für zwei boolesche Aussagen A und B ist $A \Rightarrow B$ falsch genau dann wenn $A = t$ und $B = f$.
- 3 $A \Rightarrow B$ ist damit äquivalent zu $\neg A \vee B$.
- 4 $A \Rightarrow B$ ist damit auch äquivalent zu $\neg B \Rightarrow \neg A$.

Wichtige Beobachtung:

Gilt also (oder beweisen wir korrekt) $A \Rightarrow f$ (also: „aus der Bedingung/Annahme A folgt ein Widerspruch“), so ist A falsch!



4.6 Beweistechniken

Die meisten mathematischen Behauptungen sind von der Form

$$A \Rightarrow B \text{ bzw. } (A_1 \wedge \dots \wedge A_k) \Rightarrow B.$$

Um $A \Rightarrow B$ zu beweisen, können wir zeigen:

- 1. Unter der Annahme A können wir B zeigen (direkter Beweis).
- 2. Unter der Annahme $\neg B$ können wir $\neg A$ zeigen (indirekter Beweis).
- 3. Unter den Annahmen $\neg B$ und A können wir einen Widerspruch zeigen (Widerspruchsbeweis).



Beispiel 23 (Direkter Beweis)

Satz 24

Sei $n \in \mathbb{N}_0$ ungerade, dann ist auch n^2 ungerade.

Beweis:

$n \in \mathbb{N}_0$ ungerade

$$\Rightarrow (\exists m \in \mathbb{N}_0) [n = 2m + 1] \Rightarrow n^2 = (2m + 1)^2 = \underbrace{4m^2 + 4m}_{\text{gerade}} + 1 \Rightarrow n^2 \text{ ungerade.} \quad \square$$



Beispiel 25 (Indirekter Beweis)

Satz 26

Sei $n \in \mathbb{N}_0$. Falls n^2 gerade ist, dann ist auch n gerade.

Beweis:

Zunächst überzeugen wir uns (siehe Hausaufgabe), dass

$$(\forall n \in \mathbb{N}_0) [„n \text{ gerade}“ \equiv „n \text{ nicht ungerade}“].$$

Nachdem wir dieses Lemma bewiesen haben, ist die Aussage des Satzes gleichbedeutend mit

„Falls $n \in \mathbb{N}_0$ ungerade, dann ist auch n^2 ungerade.“

Diese Aussage wurde in Satz 24 bewiesen. □



Beispiel 27 (Beweis durch Widerspruch)

Wir nehmen an, dass die zu zeigende Aussage falsch ist und führen diese Annahme zu einem Widerspruch.

Satz 28

$\sqrt{3}$ ist irrational, d. h. $\sqrt{3} \notin \mathbb{Q}$.

Beweis:

Widerspruchsannahme: $\sqrt{3} \in \mathbb{Q}$.

$$\Rightarrow \sqrt{3} = \frac{p}{q}, p, q \in \mathbb{N}, \text{ggT}(p, q) = 1 \quad (*)$$

$$\Rightarrow 3q^2 = p^2 \Rightarrow 3|p \Rightarrow (\exists k \in \mathbb{N}_0) [p = 3k]$$

$$\Rightarrow 3q^2 = 9k^2 \Rightarrow q^2 = 3k^2 \Rightarrow 3|q \Rightarrow 3|\text{ggT}(p, q)$$

Das ist ein Widerspruch zu (*). □



Beispiel 27 (Beweis durch Widerspruch)

Wir nehmen an, dass die zu zeigende Aussage falsch ist und führen diese Annahme zu einem Widerspruch.

Satz 28

$\sqrt{3}$ ist irrational, d. h. $\sqrt{3} \notin \mathbb{Q}$.

Beweis:

Widerspruchsannahme: $\sqrt{3} \in \mathbb{Q}$.

$$\Rightarrow \sqrt{3} = \frac{p}{q}, p, q \in \mathbb{N}, \text{ggT}(p, q) = 1 \quad (*)$$

$$\Rightarrow 3q^2 = p^2 \Rightarrow 3|p \Rightarrow (\exists k \in \mathbb{N}_0) [p = 3k]$$

$$\Rightarrow 3q^2 = 9k^2 \Rightarrow q^2 = 3k^2 \Rightarrow 3|q \Rightarrow 3|\text{ggT}(p, q)$$

Das ist ein Widerspruch zu (*). □

Vollständige Induktion

Wir wollen zeigen, dass eine Aussage $P(n)$ für alle $n \in \mathbb{N}_0$ gilt.

Wir zeigen zunächst den Induktionsanfang, also $P(0)$, und folgern dann aus der Induktionsvoraussetzung, also der Annahme $P(n)$ bzw. den Annahmen $P(0), P(1), \dots, P(n)$, die Behauptung $P(n+1)$.

Vollständige Induktion

Wir wollen zeigen, dass eine Aussage $P(n)$ für alle $n \in \mathbb{N}_0$ gilt.

Wir zeigen zunächst den Induktionsanfang, also $P(0)$, und folgern dann aus der Induktionsvoraussetzung, also der Annahme $P(n)$ bzw. den Annahmen $P(0), P(1), \dots, P(n)$, die Behauptung $P(n+1)$.

Beispiel 29

Satz 30

$$\sum_{i=0}^n i = \frac{n \cdot (n+1)}{2}$$

Beweis:

Induktionsanfang: $n = 0$ trivial $0 = 0$

Induktionsannahme: $P(n)$, also Satz richtig für n

Induktionsschluss:

$$\begin{aligned} \sum_{i=0}^{n+1} i &= \sum_{i=0}^n i + n + 1 \stackrel{(IV)}{=} \frac{n \cdot (n+1)}{2} + n + 1 = \\ &= \frac{2 \cdot (n+1) + n \cdot (n+1)}{2} = \frac{(n+1)(n+2)}{2} \end{aligned}$$

Dies ist $P(n+1)$, die Behauptung für $n+1$. □

Beweis:

Induktionsanfang: $n = 0$ trivial $0 = 0$

Induktionsannahme: $P(n)$, also Satz richtig für n

Induktionsschluss:

$$\begin{aligned} \sum_{i=0}^{n+1} i &= \sum_{i=0}^n i + n + 1 \stackrel{(IV)}{=} \frac{n \cdot (n+1)}{2} + n + 1 = \\ &= \frac{2 \cdot (n+1) + n \cdot (n+1)}{2} = \frac{(n+1)(n+2)}{2} \end{aligned}$$

Dies ist $P(n+1)$, die Behauptung für $n+1$. □

Das Schubfachprinzip (*pigeon hole principle*)

Satz 31

Sei $f : X \rightarrow Y$, sei $\infty > |X| > |Y| \geq 1$, dann

$$(\exists y \in Y)[|f^{-1}(y)| \geq 2]$$

Beweis:

Sei $|X| = n$, $|Y| = m$, und sei $n > m$. Widerspruchsannahme: Kein $y \in Y$ hat mehr als ein Urbild in X . Die Bilder der ersten m Elemente aus X müssen dann notwendigerweise verschieden sein. Damit hat jedes $y \in Y$ ein Urbild in X . Da f total ist, muss das Bild des $(m+1)$ -ten Elements aus X dann als Bild ein Element aus Y haben, das bereits Bild eines anderen $x \in X$ ist. Dies ist ein Widerspruch zur Annahme. □

Das Schubfachprinzip (*pigeon hole principle*)

Satz 31

Sei $f : X \rightarrow Y$, sei $\infty > |X| > |Y| \geq 1$, dann

$$(\exists y \in Y)[|f^{-1}(y)| \geq 2]$$

Beweis:

Sei $|X| = n$, $|Y| = m$, und sei $n > m$. Widerspruchsannahme: Kein $y \in Y$ hat mehr als ein Urbild in X . Die Bilder der ersten m Elemente aus X müssen dann notwendigerweise verschieden sein. Damit hat jedes $y \in Y$ ein Urbild in X . Da f total ist, muss das Bild des $(m+1)$ -ten Elements aus X dann als Bild ein Element aus Y haben, das bereits Bild eines anderen $x \in X$ ist. Dies ist ein Widerspruch zur Annahme. \square

Beispiele:

- Seien 13 oder mehr Personen in einem Raum. Dann haben mindestens 2 der Personen im gleichen Monat Geburtstag.

- Behauptung: In jeder Menge P von Personen ($|P| \geq 2$) gibt es immer mindestens 2 Personen, die gleich viele (andere) Personen in der Menge kennen („kennen“ symmetrische Relation).

Beweis:

\square

- Behauptung: In jeder Menge P von Personen ($|P| \geq 2$) gibt es immer mindestens 2 Personen, die gleich viele (andere) Personen in der Menge kennen („kennen“ symmetrische Relation).

Beweis:

- 1 Überlegung: Sei $n = |P|$. Wir betrachten die Abbildung $P \ni p \mapsto \#$ Personen, die p kennt $\in \{0, \dots, n-1\}$
- 2 Weitere Überlegung:

\square

- Behauptung: In jeder Menge P von Personen ($|P| \geq 2$) gibt es immer mindestens 2 Personen, die gleich viele (andere) Personen in der Menge kennen („kennen“ symmetrische Relation).

Beweis:

1. Überlegung: Sei $n = |P|$. Wir betrachten die Abbildung $P \ni p \mapsto \#$ Personen, die p kennt $\in \{0, \dots, n-1\}$
2. Weitere Überlegung:
 1. Fall: 0 kommt als Bild nicht vor (jeder kennt mindestens eine andere Person).
 \Rightarrow Urbildmenge $= n$ und Bildmenge $\leq n-1$. Das Schubfachprinzip liefert die Behauptung.
 2. Fall: 0 kommt als Bild vor.
 \Rightarrow Es gibt also (wegen der Symmetrie) mindestens eine Person, die kein anderer kennt. Also ist der Wertebereich der Funktion $\subseteq \{0, 1, \dots, n-2\}$. Das Schubfachprinzip liefert nunmehr ebenfalls den Beweis.

□

Das verallgemeinerte Schubfachprinzip

Satz 32

Sei $f : X \rightarrow Y, \infty > |X| \geq |Y| \geq 1$. Dann existiert ein $y \in Y$, so dass

$$|f^{-1}(y)| \geq \left\lceil \frac{|X|}{|Y|} \right\rceil.$$

Beweis:

Es gilt $|X| = \left| \bigcup_{y \in Y} f^{-1}(y) \right| = \sum_{y \in Y} |f^{-1}(y)|$. Das zweite „ $=$ “ gilt, da die $f^{-1}(y)$ alle paarweise disjunkt sind!

Widerspruchsannahme:

$$(\forall y \in Y) \left[|f^{-1}(y)| \leq \left\lfloor \frac{|X|}{|Y|} \right\rfloor - 1 \right]$$

Da

$$\left\lfloor \frac{|X|}{|Y|} \right\rfloor - 1 \leq \frac{|X| + |Y| - 1}{|Y|} - 1 = \frac{|X| - 1}{|Y|},$$

folgt mit der Widerspruchsannahme

$$|X| = \sum_{y \in Y} |f^{-1}(y)| \leq |Y| \cdot \frac{|X| - 1}{|Y|} = |X| - 1.$$

Dies stellt einen Widerspruch dar.

□

2012-ds.pdf - Adobe Acrobat Pro

File Edit View Window Help Citavi Picker

Create

82 (297 of 355) 201%

Tools Comment Share

Beweis:

Es gilt $|X| = \left| \bigcup_{y \in Y} f^{-1}(y) \right| = \sum_{y \in Y} |f^{-1}(y)|$. Das zweite „ $=$ “ gilt, da die $f^{-1}(y)$ alle paarweise disjunkt sind!

Widerspruchsannahme:

$$(\forall y \in Y) \left[|f^{-1}(y)| \leq \left\lfloor \frac{|X|}{|Y|} \right\rfloor - 1 \right]$$

Da

$$\left\lfloor \frac{|X|}{|Y|} \right\rfloor - 1 \leq \frac{|X| + |Y| - 1}{|Y|} - 1 = \frac{|X| - 1}{|Y|},$$

folgt mit der Widerspruchsannahme

$$|X| = \sum_{y \in Y} |f^{-1}(y)| \leq |Y| \cdot \frac{|X| - 1}{|Y|} = |X| - 1.$$

Dies stellt einen Widerspruch dar.

□

TUM Diskrete Strukturen
©Ernst W. Mayr

82/101

LEA

Ein Beispiel aus der Ramsey-Theorie:

Satz 33

In jeder Menge von 6 Personen gibt es 3 Personen, die sich gegenseitig kennen, oder 3 Personen, von denen keiner die beiden anderen kennt.

Beweis:

Es gilt $|X| = \left| \bigcup_{y \in Y} f^{-1}(y) \right| = \sum_{y \in Y}$
paarweise disjunkt sind!

Widerspruchsannahme:

$$(\forall y \in Y$$

Da

$$\left\lceil \frac{|X|}{|Y|} \right\rceil - 1 \leq$$

folgt mit der Widerspruchsannahme

$$|X| = \sum |f^{-1}(y)|$$

Beweis:

$P = \{p_1, p_2, \dots, p_6\}$. Betrachte die Abbildung

$$\begin{aligned} \{2, \dots, 6\} &\rightarrow \{0, 1\} \\ \{2, \dots, 6\} \ni i &\mapsto \begin{cases} 1 & \text{„}p_1 \text{ kennt } p_i\text{“} \\ 0 & \text{„}p_1 \text{ kennt } p_i \text{ nicht“} \end{cases} \end{aligned}$$

Aus dem verallgemeinerten Schubfachprinzip folgt: Es gibt mindestens 3 Leute $\in \{p_2, \dots, p_6\}$, die p_1 kennen, oder es gibt mindestens 3 Leute, die p_1 nicht kennen.

Wir betrachten die erste Alternative, die zweite ist analog. O. B. d. A. kennt p_1 p_2 , p_3 und p_4 .

1. Fall:

$(\exists p_i, p_j \in \{p_2, p_3, p_4\}) [i \neq j \text{ und } p_i \text{ kennt } p_j]$, z. B. $i = 2, j = 4$. Dann erfüllen $\{p_1, p_i, p_j\}$ den ersten Teil der Behauptung.

2. Fall: (Komplement des 1. Falls!)

$(\forall p_i, p_j \in \{p_2, p_3, p_4\}) [i \neq j \Rightarrow p_i \text{ kennt } p_j \text{ nicht}]$. Dann erfüllen $\{p_2, p_3, p_4\}$ den zweiten Teil der Behauptung. \square

Beispiel 34 (Indirekter Beweis, Wohlordnungseigenschaft)

Satz 35

Sei S eine endliche Menge $\neq \emptyset$, und sei $f : S \rightarrow S$ eine Abbildung von S in S . Dann gilt:

$$(\exists r \in \mathbb{N}) [f^r(S) = f(f^r(S))].$$

Dabei ist $f^0 : S \rightarrow S$ als die Identität auf S und, für alle $n \in \mathbb{N}_0$, f^{n+1} als $f \circ f^n$ definiert.

Beweis:

Falls f bijektiv ist, dann erfüllt $r = 1$ die Behauptung. Wir nehmen daher an, dass f nicht bijektiv, also nicht surjektiv ist, so dass $f(S) \subsetneq S$. Man beachte, dass für alle $m \in \mathbb{N}_0$ gilt, dass $f^{m+1}(S) \subseteq f^m(S)$!

Weitere Annahme: Für alle $m \in \mathbb{N}_0$ gilt $f^{m+1}(S) \subsetneq f^m(S)$.

In diesem Fall hätte die Menge $\{|f^m(S)|; m \in \mathbb{N}_0\} \subseteq \mathbb{N}_0$ kein *kleinstes Element*, da stets $|f^{m+1}(S)| < |f^m(S)|$.

Widerspruch zur Wohlordnungseigenschaft!

Sei also $m \in \mathbb{N}$ minimal mit der Eigenschaft

$$f^{m+1}(S) = f^m(S).$$

Dann erfüllt $r = m$ die Behauptung. □

Alternativer, direkter Beweis

Beweis:

Man beachte, dass für alle $m \in \mathbb{N}_0$ gilt: $f^{m+1}(S) \subseteq f^m(S)$!

Die Menge $\{|f^m(S)|; m \in \mathbb{N}\} \subseteq \mathbb{N}_0$ ist nicht leer und besitzt deshalb aufgrund der Wohlordnungseigenschaft ein minimales Element $|f^r(S)|$.

Damit gilt $|f^r(S)| \leq |f^{r+1}(S)|$.

Wegen $f^{r+1}(S) \subseteq f^r(S)$ folgt

$$|f^r(S)| = |f^{r+1}(S)|,$$

also auch $f^r(S) = f^{r+1}(S)$. □

Beispiel 36

Satz

Sei $n \in \mathbb{N}$, $n \geq 3$ und n ungerade. Dann lässt sich n als Differenz zweier Quadratzahlen darstellen.

Beweis:

Falls $n = x^2 - y^2$ mit $x, y \in \mathbb{N}$, $x > y$, dann gilt $n = (x - y)(x + y)$.

Sei nun $s := x + y$ und $t := x - y$. Dann ist

$$s > t > 0$$

$$n = s \cdot t$$

$$x = (s + t)/2$$

$$y = (s - t)/2$$

Also müssen s und t beide gerade oder beide ungerade sein.

Alternativer, direkter Beweis

Beweis:

Man beachte, dass für alle $m \in \mathbb{N}_0$ gilt: $f^{m+1}(S) \subseteq f^m(S)$!

Die Menge $\{|f^m(S)|; m \in \mathbb{N}\} \subseteq \mathbb{N}_0$ ist nicht leer und besitzt deshalb aufgrund der Wohlordnungseigenschaft ein minimales Element $|f^r(S)|$.

Damit gilt $|f^r(S)| \leq |f^{r+1}(S)|$.

Wegen $f^{r+1}(S) \subseteq f^r(S)$ folgt

$$|f^r(S)| = |f^{r+1}(S)|,$$

also auch $f^r(S) = f^{r+1}(S)$. □

