universität innsbruck

Diskrete Mathematik

Ralph Bottesch David Obwaller
Burak Ekici Vincent van Oostrom
Johannes Koch Oleksandra Panasiuk
Georg Moser

cbr.uibk.ac.at

Zusammenfassung der letzten LVA

Definition (Beweisformen)

Beweisformen sind etwa (i) deduktive Beweise (ii) Beweise von Mengeninklusionen (iii) Kontraposition (iv) indirekte Beweise (v) induktive Beweise (vi) Gegenbeispiele

Beispiel

Die Kontraposition der Aussage

„es regnet ⇒ die Straße ist nass“

ist

„die Straße ist trocken ⇒ es regnet nicht“

Beispiel (Kontraposition in der Realität)

We arrive at the following paradox in a globalised world: when nationalists pursue more formal sovereignty they achieve less real sovereignty of the people. They want to take back control and they end up with less control. That's what the UK will end up with. And that's also what the Catalan nationalists will achieve if they pursue their nationalistic dreams.
Yet this paradox also has a corollary: when countries in Europe renounce formal sovereignty this leads to more real sovereignty for the peoples of Europe.[1]

Beispiel

Für alle natürlichen Zahlen $n \geqslant 2$ gilt: $n^2 \geqslant 2n$

[1] Paul De Grauwe, https://blogs.lse.ac.uk/brexit/2017/10/06/the-catalan-crisis-and-brexit-stem-from-the-same-kind-of-nationalism/

Inhalte der Lehrveranstaltung

Beweismethoden

deduktive Beweise, Beweise von Mengeninklusionen, Kontraposition, Widerspruchsbeweise, vollständige Induktion, wohlfundierte Induktion, strukturelle Induktion, Gegenbeispiele

Relationen, Ordnungen und Funktionen

Äquivalenzrelationen, partielle Ordnungen, Wörter, asymptotisches Wachstum

Graphentheorie

gerichtete Graphen, ungerichtete Graphen

Zähl- und Zahlentheorie

Aufzählen und Nummerieren von Objekten Lösen von Rekursionsformeln, Mastertheorem, Rechnen mit ganzen Zahlen, euklidischer Algorithmus, Primzahlen, Restklassen

Relationen und Ordnungen

Definition

$R \subseteq M \times M$ heißt Relation auf M; R heißt

- reflexiv, wenn für alle $x \in M$, $(x,x) \in R$
- irreflexiv, wenn für kein $x \in M$, $(x,x) \in R$
- symmetrisch, wenn für alle $x,y \in M$
  $(x,y) \in R \Rightarrow (y,x) \in R$
- antisymmetrisch, wenn für alle $x,y \in M$
  $(x,y) \in R$ und $(y,x) \in R \Rightarrow x = y$
- transitiv, wenn für alle $x,y,z \in M$
  $(x,y) \in R$ und $(y,z) \in R \Rightarrow (x,z) \in R$

Beispiel

- $R_1 := \{(0,0),(1,1),(2,2)\}$ auf $\{0,1,2\}$
- $R_2 := \varnothing$ auf $\{0\}$
- $R_3 := \{(0,0),(2,1)\}$ auf $\{0,1,2\}$
- $R_4 := \{(0,0),(1,2),(2,1)\}$ auf $\{0,1,2\}$
- $R_5 := \varnothing$ auf $\varnothing$

	reflexiv	irreflexiv	symmetrisch	antisymmetrisch	transitiv
R_1	✓	×	✓	✓	✓
R_2	×	✓	✓	✓	✓
R_3	×	×	×	✓	✓
R_4	×	×	✓	×	×
R_5	✓	✓	✓	✓	✓

Äquivalenzrelationen

Definition

Eine Äquivalenzrelation $\sim$ ist eine reflexive, symmetrische, transitive Relation

Definition

- x und y heißen äquivalent, wenn $(x,y) \in \sim$ bzw. $x \sim y$
- Äquivalenzklasse von x $\quad [x] := \{y \in M \mid x \sim y\}$
- Elemente einer Äquivalenzklasse K heißen Repräsentanten von K
- Repräsentantensystem von $\sim$ enthält aus jeder Äquivalenzklasse genau ein Element

Bemerkung

Äquivalenzklasse umfasst alle Objekte mit gleichem Merkmal

Beispiel

R_1 und R_5 sind Äquivalenzrelationen

Beispiel

Tripel aus $\mathbb{B}^3$ seien äquivalent, wenn sie durch Umordnen der Komponenten ineinander übergeführt werden können.

$$\begin{aligned}\sim = \{&(000,000),(001,001),(001,010),(001,100),(010,001),\\ &(010,010),(010,100),(100,001),(100,010),(100,100),\\ &(011,011),(011,101),(011,110),(101,011),(101,101),\\ &(101,110),(110,011),(110,101),(110,110),(111,111)\}\end{aligned}$$

bzw. 000, $001 \sim 010 \sim 100$, $011 \sim 101 \sim 110$, 111
Äquivalenzklassen: $\{000\},\{001,010,100\},\{011,101,110\},\{111\}$
Repräsentantensysteme: $\{000,001,011,111\}$, $\{000,010,011,111\}$, ...

Satz

$x \sim z \Leftrightarrow [x] = [z]$ *für Äquivalenzrelation* $\sim$

Beweis.

- $\Rightarrow$ (wir zeigen $[x] \subseteq [z]$; andere Inklusion analog)
  $x \sim z$ und $y \in [x] \Rightarrow z \sim x$ (Symmetrie) $\Rightarrow x \sim y$ (Def. ÄK) $\Rightarrow z \sim y$ (Transitivität)
  $\Rightarrow y \in [z]$ (Def. ÄK)
- $\Leftarrow [x] = [z] \Rightarrow \{y \mid x \sim y\} = \{y \mid z \sim y\} \Rightarrow x \sim z$

■

Lemma

Sei $f : M \to N$ Abbildung. Dann wird durch

$$x \sim z \ :\Leftrightarrow f(x) = f(z)$$

eine Äquivalenzrelation definiert. Die Äquivalenzklassen sind die Urbildmengen $f^{-1}(y) = \{x \in M \mid f(x) = y\}$ mit $y \in f(M)$.

Definition

$\{B_1, \ldots, B_n\}$ ist Partition von M, wenn $B_1 \uplus \ldots \uplus B_n = M$
B_i heißen Blöcke

Beispiel

$\{\{000\}, \{001, 010, 100\}, \{011, 101, 110\}, \{111\}\}$ ist Partition von $\mathbb{B}^3$

Satz

(1) *Sei P Partition von M. Dann ist $\sim$ Äquivalenzrelation auf M, mit*

$$x \sim y :\Leftrightarrow x \text{ und } y \text{ liegen im gleichen Block von } P$$

(2) *Sei $\sim$ eine Äquivalenzrelation auf M. Dann ist die Menge P aller Äquivalenzklassen bezüglich $\sim$ eine Partition von M*

(3) *Die Abbildungen $P \mapsto \sim$ aus (1) und $\sim \mapsto P$ aus (2) sind zueinander invers*

Partielle Ordnungen

Definition

(partielle) Ordnung $\leq$ ist reflexive, antisymmetrische, transitive Relation

Definition

$x \leq y$ wenn $(x, y) \in \leq$ $\quad$ $x < y$ wenn $x \leq y$ und $x \neq y$
x ist Vorgänger von y wenn $x < y$ (y ist Nachfolger von x)

Definition

Ordnung $\leq$ heißt total (linear), wenn für alle x, y

$$x = y \text{ oder } x < y \text{ oder } y < x$$

Satz

Wenn R partielle bzw. totale Ordnung auf M ist und $N \subseteq M$, dann ist $R \cap (N \times N)$ partielle bzw. totale Ordnung auf N

Beispiel

Die natürliche Ordnung $\leq$ auf $\mathbb{Z}$, definiert durch

$$x \leq y \text{ genau dann, wenn } y - x \in \mathbb{N}$$

ist eine totale Ordnung

Beispiel

$m \in \mathbb{N}$ teilt $n \in \mathbb{N}$, wenn es $p \in \mathbb{N}$ gibt, sodass

$$n = m \cdot p$$

Teilbarkeitsordnung auf $\mathbb{N}$ ist partielle, aber keine totale Ordnung auf $\mathbb{N}$

Beispiel

$\leq$ partielle Ordnung auf M
Für Tupel $x = (x_1, x_2, \ldots, x_k)$ und $y = (y_1, y_2, \ldots, y_k)$ in M^k sei

$$x \leq_{\text{komp}} y \quad \text{genau dann, wenn} \quad x_i \leq y_i \quad \text{für alle } i = 1, \ldots, k$$

Die komponentenweise Erweiterung von $\leq$, $\leq_{\text{komp}}$ ist eine partielle Ordnung

Definition

$\mathcal{P}(M) := \{T \mid T \subseteq M\}$ Potenzmenge von M
$\mathcal{P}_k(M) := \{T \mid T \subseteq M \text{ und } \#(T) = k\}$ k-elementige Teilmengen

Beispiel

$\mathcal{P}(\{a,b\}) = \{\varnothing, \{a\}, \{b\}, \{a,b\}\}$ $\mathcal{P}_1(\{a,b\}) = \{\{a\}, \{b\}\}$

Satz

Teilmengenrelation (Inklusion) $S \subseteq T$ *ist partielle Ordnung auf* $\mathcal{P}(M)$

Definition (Verfeinerung und Vergröberung von Partitionen)

Seien P, Q Partitionen von M

$$P \leq Q :\Leftrightarrow \text{jeder Block von } P \text{ ist Teilmenge eines Blocks von } Q$$

Wenn $P < Q$, dann heißt P feiner als Q (Q gröber als P)

Beispiel

Partition $\{\{a\}, \{b\}, \{c\}\}$ ist feiner als jede der Partitionen

$$\{\{a\}, \{b,c\}\} \quad \{\{b\}, \{a,c\}\} \quad \{\{c\}, \{a,b\}\} \quad \{\{a,b,c\}\}$$

Satz

(1) *$\leq$ partielle Ordnung $\Rightarrow$ Vorgängerrelation $<$ irreflexiv und transitiv*

(2) *Wenn R irreflexive und transitive Relation, dann definiert*

$$x \leq y \;:\Leftrightarrow\; x\,R\,y \text{ oder } x = y$$

partielle Ordnung

(3) *Abbildungen $\leq \mapsto <$ aus (1) und $R \mapsto \leq$ aus (2) sind invers*

Bemerkung

partielle Ordnung kann über irreflexive und transitive Relation definiert werden

Beispiel

$< = \{(0,1), (1,2), (0,2)\}$ definiert partielle Ordnung
$\leq = \{(0,0), (0,1), (1,1), (1,2), (0,2), (2,2)\}$

Beweis.

(1) Nach Definition gilt $x < y$ genau dann, wenn $x \leq y$ und $x \neq y$. Somit ist $<$ irreflexiv. Um die Transitivität von $<$ zu zeigen, seien $x < y$ und $y < z$. Aus der Transitivität von $\leq$ folgt $x \leq z$. Wegen der Antisymmetrie von $\leq$ kann x nicht gleich z sein. Daher ist $x < z$.
(2) Nach Definition ist $\leq$ reflexiv. Nun zeigen wir Transitivität. Gelte $x, y, z \in M$ mit $x \leq y$ und $y \leq z$. Wenn $x = y$ und $y = z$ ist, dann folgt $x = z$. In den anderen Fällen gilt $x\,R\,z$, wobei wir im Fall dass $x\,R\,y$ und $y\,R\,z$ die Transitivität von R verwenden. Um die Antisymmetrie von $\leq$ einzusehen, genügt es zu sehen, dass $x \leq y$ und $y \leq x$ nur gelten kann, wenn $x = y$ (und $y = x$) ; die anderen Fälle stehen im Widerspruch zur Irreflexivität von R
(3) Wenn man von einer partiellen Ordnung $\leq$ ausgeht, dann bekommt man durch $x < y \vee x = y$ die partielle Ordnung $x \leq y$ zurück. Wenn man von einer irreflexiven und transitiven Relation R ausgeht, dann bekommt man durch $x \leq y \wedge x \neq y$ die Relation R zurück. ■

Definition

Sei $\leq$ partielle Ordnung auf M. Dann heißt $x \in M$

- kleinstes Element von M, falls für alle $y \in M$ mit $x \leq y$
- größtes Element von M, falls für alle $y \in M$ mit $y \leq x$
- minimales Element von M, falls für alle $y \in M$ mit $y \neq x$ ist $y \not< x$
- maximales Element von M, falls für alle $y \in M$ mit $y \neq x$ ist $x \not< y$

Beispiel

$\leq$ gegeben durch Vorgängerrelation

$$< = \{(1,2), (1,4), (1,5), (2,4), (2,5), (3,4), (3,5), (4,5)\}$$

- minimale Elemente: 1, 3
- maximale Elemente: 5
- kleinstes Element:
- größtes Element: 5

Lemma

$\leq$ *totale Ordnung*

- *x kleinstes Element* $\Leftrightarrow$ *x minimales Element*
- *x größtes Element* $\Leftrightarrow$ *x maximales Element*

Satz

$\leq$ *partielle Ordnung*

(1) *x kleinstes Element* $\Rightarrow$ *x eindeutig, x einziges minimales Element*

(2) *x größtes Element* $\Rightarrow$ *x eindeutig, x einziges maximales Element*

Beweis.

(1) eindeutig: x, w kleinste Elemente $\Rightarrow w \leq x \leq w \Rightarrow w = x$
einziges min. Element: x kleinstes Element und $y \leq x \Rightarrow y \leq x \leq y \Rightarrow y = x$
(2) analog ■

Satz

(3) *M endlich* $\Rightarrow$ *es gibt zu jedem* $x \in M$ *minimales Element w mit* $w \leq x$ *und maximales Element z mit* $x \leq z$

(4) *Wenn M endlich und nur ein minimales Element x besitzt, ist x kleinstes Element*

(5) *Wenn M endlich und nur ein maximales Element x besitzt, ist x größtes Element*

Beweis.

(3) Wir zeigen nur die Existenz eines minimalen Elements: Wenn x minimal, ist man fertig. Sonst gibt es $x_1 \in M$ mit $x_1 < x$. Wenn x_1 nicht minimal, gibt es $x_2 \in M$ mit $x_2 < x_1$, usw. Da

$$x > x_1 > x_2 > \dots$$

verschiedene Elemente von M sind, erreicht man nach endlich vielen Schritten ein minimales Element x_n mit $x_n < x$.
(4) und (5) folgen aus (3) ■

Das Wortmonoid

Definition (Alphabet)

Menge Σ heißt Alphabet $a \in \Sigma$ heißt Zeichen

Beispiel

- $\mathbb{B} = \{0, 1\}$ ist das binäre Alphabet
- $\{a, b, \dots, z\}$ ist das Alphabet der (lateinischen) Kleinbuchstaben
- $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ ist das Alphabet der (arabischen) Ziffern

Definition (Wort)

$(w_0, \dots, w_{n-1}) \in \Sigma^n$ heißt Wort (String) der Länge n über Σ
Σ^* ist die Menge aller Wörter über Σ

Definition (Verkettung, Konkatenation)

Für Wörter $v = (v_0, \dots, v_{m-1}) \in \Sigma^*$ und $w = (w_0, \dots, w_{n-1}) \in \Sigma^*$ ist die Verkettung (Konkatenation)

$$vw := (v_0, \dots, v_{m-1}, w_0, \dots, w_{n-1}) \in \Sigma^*$$

Lemma

Für Wörter $u, v, w \in \Sigma^*$ *gilt* $(uv)w = u(vw)$ *Assoziativgesetz und das leere Wort* $\epsilon = ()$ *ist das neutrale Element:* $w\epsilon = \epsilon w = w$

Bemerkung

Wie in ETI lassen wir Klammern und Beistriche in Wörtern weg; Wörter der Länge 1 werden wie Zeichen geschrieben

Satz

Das Wortmonoid mit $\langle \Sigma^*; \cdot, \epsilon \rangle$ *ist ein Monoid, wobei* $\cdot$ *Konkatenation und* ϵ *das Leerwort bezeichnet.*

Lemma

Für die Längenfunktion $\ell\colon \Sigma^* \to \mathbb{N},\ (w_0,\ldots,w_{n-1}) \mapsto n$ *gilt*

$$\ell(vw) = \ell(v) + \ell(w) \quad \textit{und} \quad \ell(\epsilon) = 0$$

Beispiel

Wort 01101 über $\{0,1\}$ hat Länge 5.
Für $x = 01101$, $y = 110$ und $z = 10101$ sind

$$\begin{aligned} xy &= 01101110 \\ yx &= 11001101 \\ (xy)z &= (01101110)10101 = 0110111010101 \\ x(yz) &= 01101(11010101) = 0110111010101 \end{aligned}$$

Definition (lexikographische Ordnung)

$\leq$ totale Ordnung auf Σ
Für Wörter $v, w \in \Sigma^*$ sei

$$v <_{\text{lex}} w$$

falls ein $k \in \mathbb{N}$ mit $k \leq \ell(v)$ und $k \leq \ell(w)$ existiert, sodass

(1) $v_i = w_i$ für $i = 0,\ldots,k-1$ und

(2) $(\ell(v) = k \text{ und } \ell(w) > k)$ oder $(\ell(v) > k \text{ und } \ell(w) > k \text{ und } v_k < w_k)$

Beispiel

Sei $\Sigma = \{a,b\}$ und $a < b$. Dann ist

$$\epsilon <_{\text{lex}} a \qquad \epsilon <_{\text{lex}} b \qquad a <_{\text{lex}} b \qquad aa <_{\text{lex}} ab \qquad aaaa <_{\text{lex}} ab$$

Satz

$\leq_{lex}$ *ist totale Ordnung auf* Σ^*

Beweis ($\leq_{\text{lex}}$ partielle Ordnung).

Um zu zeigen, dass $\leq_{\text{lex}}$ eine partielle Ordnung ist, zeigen wir Irreflexivität und Transitivität von $<_{\text{lex}}$. Offensichtlich ist $<_{\text{lex}}$ irreflexiv. Um die Transitivität zu zeigen, seien $u, v, w \in \Sigma^*$ mit

$$u <_{\text{lex}} v \qquad \text{und} \qquad v <_{\text{lex}} w$$

Dann gibt es ein $k \in \mathbb{N}$ mit $k \leq \ell(u)$ und $k \leq \ell(v)$ und

(1) $u_i = v_i$ für $i = 0,\ldots,k-1$ und

(2) $(\ell(u) = k \text{ und } \ell(v) > k)$ oder $(\ell(u) > k \text{ und } \ell(v) > k \text{ und } u_k < v_k)$

sowie ein $l \in \mathbb{N}$ mit $l \leq \ell(v)$ und $l \leq \ell(w)$ und

(1) $v_i = w_i$ für $i = 0,\ldots,l-1$ und

(2) $(\ell(v) = l \text{ und } \ell(w) > l)$ oder $(\ell(v) > l \text{ und } \ell(w) > l \text{ und } v_l < w_l)$

Dann gilt für $m := \min(k,l)$ auch $m \leq \ell(u)$ und $m \leq \ell(w)$ und

(a) $u_i = w_i$ für $i = 0,\ldots,m-1$ und

(b) $(\ell(u) = m \text{ und } \ell(w) > m)$ oder $(\ell(u) > m \text{ und } \ell(w) > m \text{ und } u_m < w_m)$

sodass $u <_{\text{lex}} w$ folgt

Beweis ($\leq_{\text{lex}}$ total)

Um zu zeigen, dass $\leq_{\text{lex}}$ total ist, seien $v, w \in \Sigma^*$ mit $v \neq w$
Dann existiert ein $k \in \mathbb{N}$ mit $k \leq \ell(v)$ und $k \leq \ell(w)$, sodass

(a) $v_i = w_i$ für $i = 0,\ldots,k-1$ und

(b) $(\ell(v) = k \text{ und } \ell(w) > k)$ oder $(\ell(v) > k \text{ und } \ell(w) = k)$ oder
$(\ell(v) > k \text{ und } \ell(w) > k \text{ und } v_k \neq w_k)$

Da $\leq$ total auf Σ ist, gilt somit entweder $v <_{\text{lex}} w$ oder $w <_{\text{lex}} v$

Definition

$\leq$ totale Ordnung auf Σ
Für Wörter $v, w \in \Sigma^*$ sei

$$v <_{\text{gradlex}} w$$

falls $\ell(v) < \ell(w)$ oder $(\ell(v) = \ell(w)$ und $v <_{\text{lex}} w)$

Beispiel

Sei $\Sigma = \{a, b\}$ und $a < b$. Dann ist

$$\epsilon <_{\text{gradlex}} a \quad \epsilon <_{\text{gradlex}} b \quad a <_{\text{gradlex}} b \quad aa <_{\text{gradlex}} ab \quad aaaa >_{\text{gradlex}} ab$$

Satz

$\leq_{gradlex}$ *ist eine totale Ordnung auf* Σ^*

Beweis

Man prüft Irreflexivität, Transitivität und Totalität von $<_{\text{gradlex}}$ nach

Definition

$L \subseteq \Sigma^*$ heißt formale Sprache über Σ

Beispiel

Die formale Sprache der Palindrome über $\Sigma = \{a, b\}$ ist

$$\{w_0 w_1 \dots w_{n-1} \mid w_0 w_1 \dots w_{n-1} = w_{n-1} w_{n-2} \dots w_0\} =$$
$$\{\epsilon, a, b, aa, bb, aaa, aba, bab, bbb, aaaa, abba, baab, bbbb, \dots\}$$