



Diskrete Mathematik

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

cbr.uibk.ac.at

Definition

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

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

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

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^*

Zusammenfassung der letzten LVA

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 $i = 0, \dots, k-1$ und

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

Satz

\leq_{lex} ist totale Ordnung auf Σ^*

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

Induktives Schließen

Vollständige Induktion

- 1 Sei m eine fest gewählte natürliche Zahl, z.B. $m = 0$ oder $m = 1$
- 2 Eine Aussage $A(n)$ soll für alle natürlichen Zahlen $n \geq m$ gezeigt werden
- 3 In diesem Fall gehen wir wie folgt vor:
 - **Induktionsbasis:** Wir zeigen, dass A für den Basiswert m gilt.
 - **Induktionsschritt:** Wir zeigen, dass für alle $n \geq m$ aus $A(n)$ auch $A(n+1)$ folgt.
- 4 Dann gilt $A(n)$ für alle $n \geq m$

Formal

$$(A(m) \wedge \forall n \geq m. (A(n) \rightarrow A(n+1))) \rightarrow (\forall n \geq m. A(n))$$

4

Erweiterte vollständige Induktion

Vollständige Induktion (II)

- 1 Es gibt mehrere Basiswerte

$$A(m), A(m+1), \dots, A(l),$$

- 2 wir setzen im Beweis des Induktionsschritts $n \geq l$ voraus
- 3 $(A(m) \wedge \dots \wedge A(l) \wedge \forall n \geq l (A(m) \wedge \dots \wedge A(l) \wedge A(n) \rightarrow A(n+1))) \rightarrow (\forall n \geq m A(n))$
- 4 Um $A(n+1)$ zu beweisen, können als Hypothesen alle Aussagen

$$A(m), A(m+1), \dots, A(l), A(n)$$

verwendet werden.

Die Erweiterung folgt aus der Urform und ist somit gleichmächtig

5

Wohlfundierte Ordnung

Definition (wohlfundierte Ordnung)

- Sei \leq eine partielle Ordnung auf einer Menge M
- Eine Folge (x_0, x_1, x_2, \dots) von Elementen in M heißt eine **unendliche absteigende Kette**, falls
$$x_0 > x_1 > x_2 > \dots$$
- Man nennt \leq **wohlfundiert**, wenn es in M keine unendliche absteigende Kette gibt

Beispiel

- Die natürliche Ordnung auf \mathbb{N} ist wohlfundiert
- Die natürliche Ordnung auf \mathbb{Z} ist nicht wohlfundiert
- Für Alphabete mit mindestens zwei Buchstaben ist die lexikographische Ordnung nicht wohlfundiert

6

Grundlagen der wohlfundierten Induktion

Beispiel

Sei $f: M \rightarrow \mathbb{N}$ eine beliebige Abbildung. Dann wird durch

$$x < y \quad :\Leftrightarrow \quad f(x) <_{\mathbb{N}} f(y)$$

eine wohlfundierte Ordnung auf M definiert

Satz

Sei \leq eine partielle Ordnung auf einer Menge M . Dann ist \leq wohlfundiert genau dann, wenn jede nichtleere Teilmenge von M ein minimales Element besitzt.

7

Beweis.

Sei \leq wohlfundiert und sei N eine nichtleere Teilmenge von M . Dann gibt es ein Element x_0 in N . Wenn x_0 minimal in N ist, ist man fertig. Andernfalls gibt es ein Element $x_1 \in N$ mit $x_1 < x_0$. Wenn x_1 nicht minimal ist, dann gibt es ein $x_2 \in N$ mit $x_2 < x_1$, usw. Wegen

$$x_0 > x_1 > x_2 > \dots$$

erreicht man nach endlich vielen Schritten ein minimales Element x_n . Um die umgekehrte Richtung zu beweisen, nehmen wir an, \leq sei nicht wohlfundiert. Dann gibt es eine unendliche absteigende Kette

$$x_0 > x_1 > x_2 > \dots,$$

und die nichtleere Teilmenge $N = \{x_0, x_1, x_2, \dots\}$ hat kein minimales Element. ■

8

Satz

Sei \leq eine wohlfundierte Ordnung auf einer Menge M , und sei W eine Teilmenge von M mit folgenden zwei Eigenschaften:

- W enthält alle minimalen Elemente von M .
- Wenn für ein nicht-minimales Element x in M alle Vorgänger in W liegen, dann liegt auch x in W .

Dann ist $W = M$.

Beweis.

Wir führen einen Widerspruchsbeweis und nehmen an, dass $W \subsetneq M$ ist. Dann ist die Menge

$$N := \{x \in M \mid x \notin W\} = M \setminus W$$

nichtleer und hat nach vorigen Satz ein minimales Element y . Nach der ersten Eigenschaft von W ist y kein minimales Element von M . Da alle Vorgänger von y in W liegen, folgt nach der zweiten Eigenschaft von W der Widerspruch $y \in W$. ■

9

Wohlfundierte Induktion

- 1 Sei \leq eine wohlfundierte Ordnung auf einer Menge M
- 2 Eine Aussage $A(x)$ soll für alle Elemente x in M gezeigt werden
- 3 Wir gehen wie folgt vor:
 - **Induktionsbasis:** Wir zeigen, dass $A(m)$ wahr ist für alle minimalen Elemente m von M .
 - **Induktionsschritt:** Sei x ein nicht-minimales Element von M , und sei $A(y)$ wahr für alle Vorgänger y von x . Wir zeigen, dass auch $A(x)$ wahr ist
- 4 Dann ist $A(x)$ für alle $x \in M$ wahr

Beispiel

Sei P die formale Sprache der Palindrome über dem Alphabet $\{a, b\}$. Wir zeigen „Wenn $x \in P$ und $\ell(x)$ gerade, dann hat x eine gerade Anzahl von a .“

10

Satz

Sei \mathbb{N} mit der natürlichen Ordnung versehen. Dann ist die lexicographische Ordnung auf der Menge \mathbb{N}^k wohlfundiert.

Beweis.

an der Tafel ■

Beispiel

Die folgende Definition (der **Ackermannfunktion**) ist wohldefiniert:

$$f(n, m) := \begin{cases} m + 1 & \text{falls } n = 0 \\ f(n - 1, 1) & \text{falls } n > 0 \text{ und } m = 0 \\ f(n - 1, f(n, m - 1)) & \text{sonst} \end{cases}$$

NB: Die Ackermannfunktion wächst sehr flott

11

Definition (induktiv)

Eine Menge M kann induktiv definiert werden durch:

- **Induktionsbasis:** Man gibt ein oder mehr Elemente von M an.
- **Induktionsschritt:** Man spezifiziert, wie man neue Elemente von M aus den vorliegenden Elementen von M bekommt.

Die Menge M besteht dann aus genau jenen Elementen, die man durch Induktionsbasis und ein- oder mehrmalige Anwendung des Induktionsschritts erhält.

Beispiel

Die **Formeln** der Aussagenlogik sind induktiv definiert:

- 1 Eine atomare Formel p ist eine **Formel**
- 2 ein Wahrheitswertsymbol (True, False) ist eine **Formel**
- 3 Wenn A und B **Formeln** sind, dann sind $\neg A$, $(A \wedge B)$, $(A \vee B)$ und $(A \rightarrow B)$ auch **Formeln**

12

Asymptotisches Wachstum

Definition (Groß-O)

Sei $g: \{\ell, \ell + 1, \ell + 2, \dots\} \rightarrow [0, \infty)$ mit $\ell \in \mathbb{N}$.

Die Menge $O(g)$ umfasst alle Funktionen

$$f: \{k, k + 1, k + 2, \dots\} \rightarrow [0, \infty) \quad \text{mit } k \in \mathbb{N},$$

für die eine positive reelle Zahl c und eine natürliche Zahl m mit $m \geq k$ und $m \geq \ell$ existieren, sodass für alle natürlichen Zahlen n mit $n \geq m$

$$f(n) \leq c \cdot g(n)$$

gilt. In Kurzform ist $f \in O(g)$, wenn für hinreichend große Argumente der Funktionswert von f durch ein konstantes Vielfaches des Funktionswerts von g **nach oben beschränkt** ist.

14

Satz (Strukturelle Induktion)

- 1 Die Aussage $A(x)$ soll für alle Strukturen $x \in M$, die induktiv definiert sind, gezeigt werden
- 2 Wir gehen wie folgt vor:
 - **Induktionsbasis:** Wir zeigen, dass $A(x)$ für die Basisstruktur(en) x gilt
 - **Induktionsschritt:** Wir wählen eine Struktur y , die rekursiv aus den Strukturen y_1, y_2, \dots, y_k gebildet wird. IH besagt, dass die Aussagen $A(y_1), A(y_2), \dots, A(y_k)$ wahr sind. Mit Hilfe der IH zeigen wir $A(y)$

Beweis.

Wir zeigen die Korrektheit der strukturellen Induktion:

- 1 Es genügt eine Abbildung $f: M \rightarrow \mathbb{N}$ zu finden, sodass eine wohlfundierte Ordnung $<$ mittels $x < y :\Leftrightarrow f(x) <_{\mathbb{N}} f(y)$ definierbar ist
- 2 Wir wählen die Ableitungsschritte der Definition von $x \in M$

13

Groß-Omega und Groß-Theta

Definition (Groß-Omega und Groß-Theta)

- Die Menge $\Omega(g)$ umfasst alle Funktionen

$$f: \{k, k + 1, k + 2, \dots\} \rightarrow [0, \infty) \quad \text{mit } k \in \mathbb{N},$$

für die eine positive reelle Zahl c und eine natürliche Zahl m mit $m \geq k$ und $m \geq \ell$ existieren, sodass für alle natürlichen Zahlen n mit $n \geq m$

$$f(n) \geq c \cdot g(n)$$

gilt. In Kurzform ist $f \in \Omega(g)$, wenn für hinreichend große Argumente der Funktionswert von f durch ein konstantes Vielfaches des Funktionswerts von g **nach unten beschränkt** ist.

- Schließlich ist

$$\Theta(g) := O(g) \cap \Omega(g).$$

15

Beispiel

Seien $f: \mathbb{N} \rightarrow \mathbb{N}$ mit $n \mapsto 3n^2 + 5n + 100$ und $g: \mathbb{N} \rightarrow \mathbb{N}$ mit $n \mapsto n^2$. Dann ist $f \in \Theta(g)$.

Beweis.

- Wir zeigen $f \in O(g)$.
In der Definition wählen wir $c = 4$ und $m = 13$. Aus Aufgabe 3.2 folgt $f(n) \leq 4 \cdot g(n)$ für alle $n \geq 13$.
- Wir zeigen $f \in \Omega(g)$.
In der Definition wählen wir $c = 1$ und $m = 0$. Mittels vollständiger Induktion zeigen wir $f(n) \geq g(n)$ für alle $n \geq 0$.
- Somit gilt $f \in \Theta(g)$.

16

Definition

Sei $f: \mathbb{N} \rightarrow [0, \infty)$ eine Abbildung. Dann ist

$$\lim_{n \rightarrow \infty} f(n) = L$$

wenn es für alle positiven reellen ε ein $m \in \mathbb{N}$ gibt, sodass $|f(n) - L| < \varepsilon$ für alle $n \geq m$. Man nennt L den **Grenzwert** bzw. **Limes** von f .

Beispiel

Seien $f: \mathbb{N} \rightarrow [0, \infty)$ mit $n \mapsto n^2$ und $g: \mathbb{N} \rightarrow [0, \infty)$ mit $n \mapsto \frac{1}{n}$. Dann ist $\lim_{n \rightarrow \infty} f(n) = \infty$ und $\lim_{n \rightarrow \infty} g(n) = 0$. Die Abbildung $h: \mathbb{N} \rightarrow [0, \infty)$ mit

$$h(n) = \begin{cases} 1 & \text{wenn } n \text{ gerade} \\ 0 & \text{wenn } n \text{ ungerade} \end{cases}$$

besitzt keinen Grenzwert.

18

Infimum, Supremum und Grenzwerte

Definition

Sei \leq eine partielle Ordnung auf M und $S \subseteq M$.

- Dann ist $y \in M$ ein **Infimum von S** , wenn für alle $x \in S$ $y \leq x$ gilt und für alle $z \in M$ mit dieser Eigenschaft gilt, dass $z \leq y$ (**größte untere Schranke**).
- Dann ist $y \in M$ ein **Supremum von S** , wenn für alle $x \in S$ $x \leq y$ gilt und für alle $z \in M$ mit dieser Eigenschaft gilt, dass $y \leq z$ (**kleinste obere Schranke**).

Bemerkung

Infimum oder Supremum müssen nicht immer existieren

17

Definition (Limes inferior und superior)

- Sei $f: \mathbb{N} \rightarrow [0, \infty)$. Dann ist

$$\liminf_{n \rightarrow \infty} f(n) := \lim_{n \rightarrow \infty} (\inf\{f(m) \mid m \geq n\})$$

und

$$\limsup_{n \rightarrow \infty} f(n) := \lim_{n \rightarrow \infty} (\sup\{f(m) \mid m \geq n\}).$$

Hier bezeichnet \inf (\sup) das Infimum (Supremum).

- Als Elemente der erweiterten reellen Zahlen $\mathbb{R} \cup [-\infty, +\infty]$ existieren Limes inferior und Limes superior für jede Folge reeller Zahlen $f(n)_{n \geq \ell}$

Satz

Sei $f: \mathbb{N} \rightarrow [0, \infty)$. Wenn $\lim_{n \rightarrow \infty} f(n)$ definiert ist, dann gilt $\lim_{n \rightarrow \infty} f(n) = \limsup_{n \rightarrow \infty} f(n) = \liminf_{n \rightarrow \infty} f(n)$.

19

Satz

Seien $f: \{k, k+1, \dots\} \rightarrow [0, \infty)$ und $g: \{\ell, \ell+1, \dots\} \rightarrow (0, \infty)$. Dann gilt

$$f \in O(g) \Leftrightarrow \limsup_{n \rightarrow \infty} \frac{f(n)}{g(n)} < \infty$$

und

$$f \in \Omega(g) \Leftrightarrow \liminf_{n \rightarrow \infty} \frac{f(n)}{g(n)} > 0.$$

Beweis.

Wir zeigen die erste Äquivalenz, die zweite ist analog. Wenn $f(n) \leq c \cdot g(n)$ für hinreichend große n gilt, dann ist $\limsup_{n \rightarrow \infty} \frac{f(n)}{g(n)} \leq c$.

Wenn umgekehrt $s := \limsup_{n \rightarrow \infty} \frac{f(n)}{g(n)} < \infty$ ist, dann gilt $\frac{f(n)}{g(n)} \leq s + 1$ für hinreichend große n . ■

20

Definition (Klein-o)

Seien $f: \{k, k+1, \dots\} \rightarrow [0, \infty)$ und $g: \{\ell, \ell+1, \dots\} \rightarrow (0, \infty)$. Dann ist $f \in o(g)$, wenn

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0,$$

d.h. asymptotisch ist f vernachlässigbar gegenüber g .

Beispiel

Es gilt $n \in o(n^2)$, da

$$\lim_{n \rightarrow \infty} \frac{n}{n^2} = \lim_{n \rightarrow \infty} \frac{1}{n} = 0,$$

aber $n \notin o(2n)$, da

$$\lim_{n \rightarrow \infty} \frac{n}{2n} = \lim_{n \rightarrow \infty} \frac{1}{2} = \frac{1}{2}.$$

21