

# Vorlesung Diskrete Strukturen Abbildungen

Bernhard Ganter

Institut für Algebra  
TU Dresden  
D-01062 Dresden  
[bernhard.ganter@tu-dresden.de](mailto:bernhard.ganter@tu-dresden.de)

WS 2009/10

# Hashfunktionen

Wenn eine Datenbank Millionen von Dokumenten enthält und immer neue dazu kommen, stellt sich folgendes Problem:

Bei neuen Dokumenten muss geprüft werden, ob sie bereits in der Datenbank vorhanden sind. Jedes neue Dokument mit allen bereits vorhandenen vollständig zu vergleichen wäre aber viel zu zeitaufwändig.

Deshalb berechnet man zu jedem Dokument einen sogenannten *Hashwert*, und zwar so, dass gleiche Dokumente den gleichen Hashwert haben, und vergleicht neue Dokumente nur mit solchen, die den gleichen Hashwert haben. Ein primitiver Hashwert für Textdokumente kann z.B. die Anzahl der Buchstaben sein.

Die wichtigsten Relationen sind die Abbildungen:

Eine **Abbildung**

$(A, B, f)$  von  $A$  nach  $B$

besteht aus

- dem **Definitionsbereich**  $A$ ,
- dem **Zielbereich**  $B$
- und einer Relation  $f \subseteq A \times B$  mit folgender Eigenschaft:

Zu jedem  $a \in A$  existiert genau ein  $b \in B$  mit  $(a, b) \in f$ .

# Mehr zu Abbildungen

Statt  $(a, b) \in f$  schreibt man meistens

$$f(a) = b,$$

manchmal auch

$$a \xrightarrow{f} b,$$

und sagt,  $b$  sei das **Bild** von  $a$  unter  $f$ .

Statt  $(A, B, f)$  schreibt man

$$f : A \rightarrow B.$$

Man nennt  $f$  den **Graphen** der Abbildung  $(A, B, f)$ .

Die Menge

$$f(A) := \{f(a) \mid a \in A\}$$

ist die **Wertemenge** von  $f$ , synonym auch das **Bild** von  $f$ .

Die englischen Bezeichnungen sind:

- Abbildung  $\mapsto$  mapping
- Definitionsbereich  $\mapsto$  domain
- Zielbereich  $\mapsto$  codomain
- Wertemenge  $\mapsto$  range.

Ist aus dem Zusammenhang klar, welche Mengen  $A$  und  $B$  gemeint sind, sagt man auch „die Abbildung  $f$ “.

Andere Worte für „Abbildung“ sind z.B.

- „**Funktion**“,
- „**Zuweisung**“,
- „**Operator**“,
- „**Transformation**“.

- Für jede Menge  $M$  ist die **identische Abbildung**  $\text{id}_M : M \rightarrow M$  definiert durch  $\text{id}_M(m) := m$  für alle  $m \in M$ .
- Ist  $p(X) := a_0 + a_1X + a_2X^2 + \dots + a_nX^n$  ein Polynom mit reellen Koeffizienten, dann ist die zugehörige reelle **Polynomfunktion** die durch

$$r \mapsto p(r) := a_0 + a_1r + a_2r^2 + \dots + a_nr^n$$

festlegte Abbildung von  $\mathbb{R}$  nach  $\mathbb{R}$ .

- Als die **untere Gaussklammer** bezeichnet man die Abbildung  $\lfloor \cdot \rfloor : \mathbb{R} \rightarrow \mathbb{Z}$ , die jeder reellen Zahl  $r$  die größte ganze Zahl  $\lfloor r \rfloor$  zuordnet, die kleiner oder gleich  $r$  ist.

Eine Abbildung  $f : A \rightarrow B$  ist

- **injektiv**, wenn aus  $a_1 \neq a_2$  stets  $f(a_1) \neq f(a_2)$  folgt (für alle  $a_1, a_2 \in A$ ),
- **surjektiv**, wenn zu jedem Element  $b \in B$  ein Element  $a \in A$  existiert mit  $f(a) = b$ , und
- **bijektiv**, wenn sie sowohl injektiv als auch surjektiv ist.

# Hintereinanderausführung

Sind  $f : A \rightarrow B$  und  $g : B \rightarrow C$  Abbildungen, so definiert man die **Hintereinanderausführung** (auch **Komposition** genannt)

$$g \circ f \text{ von } f \text{ und } g$$

durch

$$g \circ f : A \rightarrow C \quad \text{mit} \quad (g \circ f)(a) := g(f(a)) \quad \text{für alle } a \in A.$$

Man liest  $g \circ f$  als „**g nach f**“, und schreibt oft auch einfach  $gf$  dafür.

Zu jeder Abbildung  $f : A \rightarrow B$  erhält man auf natürliche Weise eine Abbildung zwischen den Potenzmengen von  $A$  und  $B$ , die jeder Teilmenge  $T \subseteq A$  folgendes Bild zuordnet:

$$T \mapsto f(T) := \{f(t) \mid t \in T\}.$$

Man nennt dies die auf die Potenzmenge **geliftete** Abbildung  $f$ .

Die Schreibweise  $f(T)$  ist nicht ganz korrekt, aber üblich. Manche Autoren schreiben  $f[T]$  oder ähnlich, um den Unterschied deutlich zu machen.

Ist  $T \subseteq B$  eine Teilmenge des Zielbereichs, so bezeichnet

$$f^{-1}(T) := \{a \in A \mid f(a) \in T\}$$

die **Urbildmenge** von  $T$ , also die Menge derjenigen Elemente des Definitionsbereiches, die von  $f$  in  $T$  abgebildet werden.

Die Schreibweise  $f^{-1}(T)$  kann zu Missverständnissen führen, besonders wenn man in dem Fall, dass die Menge  $T$  einelementig ist, also im Falle  $T = \{b\}$ , die Mengenklammern weglässt und

$$f^{-1}(b) := \{a \in A \mid f(a) = b\}$$

schreibt.

Man könnte fälschlicherweise meinen, die zu einer Abbildung  $f : A \rightarrow B$  inverse Relation müsste automatisch selbst eine Abbildung von  $B$  nach  $A$  sein. Das ist aber nicht der Fall, außer wenn  $f$  injektiv ist.

# $f^{-1}$ als Abbildung

Wenn  $f : A \rightarrow B$  eine Abbildung ist, dann ordnet  $f^{-1}$  jeder Teilmenge von  $B$  eine Teilmenge von  $A$  zu .

$f^{-1}$  kann also als Abbildung von der Potenzmenge von  $B$  in die Potenzmenge von  $A$  gedeutet werden:

$$f^{-1} : \mathfrak{P}(B) \rightarrow \mathfrak{P}(A).$$

Ist  $f : A \rightarrow B$  injektiv, so wird durch

$$f^{-1} : \text{rg } f \rightarrow A$$

mit

$$f^{-1}(b) = a : \iff f(a) = b$$

eine Abbildung vom Bild von  $f$  in den Definitionsbereich erklärt, die **Umkehrabbildung** von  $f$ .

Die Hintereinanderausführung  $f^{-1}f$  ist dann die Identität auf  $A$  und  $ff^{-1}$  ist die Identität auf  $\text{rg } f$ .

Die Eigenschaften injektiv und surjektiv kann man benutzen, um Mengen bezüglich ihrer Elementanzahl zu vergleichen. Dazu beobachten wir folgendes:

- Wenn  $f : A \rightarrow B$  eine Abbildung ist, dann bedeutet dies:  
Zu jedem  $a \in A$  gibt es genau ein  $b \in B$  mit  $(a, b) \in f$ .

Eine Abbildung  $f : A \rightarrow B$ , verstanden als Menge von Paaren, enthält also genau so viele Elemente wie ihr Definitionsbereich  $A$ .

- Ist  $f : A \rightarrow B$  außerdem *injektiv*, dann gilt außerdem  
Zu jedem  $b \in B$  gibt es *höchstens* ein  $a \in A$  mit  $(a, b) \in f$ .

Eine injektive Abbildung enthält also höchstens soviele Paare, wie ihr Zielbereich Elemente hat.

Kombiniert man diese Überlegungen, so erhält man:

- Ist  $f : A \rightarrow B$  eine injektive Abbildung, dann hat die Menge  $B$  mindestens so viele Elemente wie  $A$ .

Entsprechend gilt

- Ist  $f : A \rightarrow B$  surjektiv, dann gilt  
Zu jedem  $b \in B$  gibt es *mindestens* ein  $a \in A$  mit  $(a, b) \in f$ .

Eine surjektive Abbildung enthält also mindestens soviele Paare, wie ihr Zielbereich Elemente hat. Man hat

- Ist  $f : A \rightarrow B$  eine surjektive Abbildung, dann hat die Menge  $B$  höchstens so viele Elemente wie  $A$ .

Zusammen ergibt dies:

- Ist  $f : A \rightarrow B$  eine bijektive Abbildung, dann hat die Menge  $B$  genau so viele Elemente wie  $A$ .

**Definition** Zwei Mengen  $A$  und  $B$  heißen **gleich mächtig**, wenn es eine bijektive Abbildung  $f : A \rightarrow B$  gibt.

Für endliche Mengen gilt: Sie sind gleich mächtig, wenn sie gleich viele Elemente haben.

**Satz (Schröder und Bernstein)** *Es gibt eine bijektive Abbildung  $h : A \rightarrow B$  genau dann, wenn es eine injektive Abbildung  $f : A \rightarrow B$  und eine injektive Abbildung  $g : B \rightarrow A$  gibt.*

**Definition** Eine Menge heißt **abzählbar unendlich**, wenn sie gleich mächtig zur Menge  $\mathbb{N}$  der natürlichen Zahlen ist.

Statt „abzählbar unendlich“ sagt man einfach „abzählbar“, wenn klar ist, dass es sich um eine unendliche Menge handelt.

**Satz** Die Menge  $\mathbb{Q}$  der rationalen Zahlen ist abzählbar.

**Satz**[Cantor] Die Menge  $\mathbb{R}$  der reellen Zahlen ist nicht abzählbar.

Nicht abzählbare unendliche Mengen nennt man **überabzählbar**.

# Die Potenzmenge ist mächtiger

**Satz**[Cantor] Für jede Menge  $M$  gilt:  $M$  ist nicht gleich mächtig zur Potenzmenge  $\mathfrak{P}(M)$  von  $M$ .

Das bedeutet insbesondere, dass es auch bei unendlich großen Mengen unendlich viele verschiedene Mächtigkeiten gibt!

# Alle Abbildungen

Die Menge *aller* Abbildungen von  $A$  nach  $B$  wird mit

$$B^A$$

notiert. Das hat einen guten Grund, denn wenn  $A$  und  $B$  endliche Mengen sind, dann ist die Anzahl der Abbildungen von  $A$  nach  $B$  gleich  $|B|^{|A|}$ , es gilt also

$$|B^A| = |B|^{|A|}.$$

Beispielsweise ist also die Anzahl der Abbildungen von einer fünfelementigen Menge in eine siebenelementige Menge gleich

$$7^5 = 16807.$$

Wir benutzen das Zeichen  $\mathbb{Z}_n$  als Abkürzung für die Menge der ersten  $n$  natürlichen Zahlen:

$$\mathbb{Z}_n := \{0, 1, 2, \dots, n-1\}.$$

Für  $n \geq 1$  ist

$$z \mapsto z \bmod n$$

diejenige Abbildung von  $\mathbb{Z}$  nach  $\mathbb{Z}_n$ , die jeder ganzen Zahl  $z$  ihren **Rest** bei ganzzahliger Division durch  $n$  zuordnet. Es ist also

$$z \bmod n := z - n \cdot \left\lfloor \frac{z}{n} \right\rfloor.$$

Eine Abbildung von  $\mathbb{Z}_n$  in eine Menge  $A$  nennt man ein  **$n$ -Tupel mit Komponenten aus  $A$** . Man notiert solche Tupel  $a : \mathbb{Z}_n \rightarrow A$  in der Form

$$(a_0, a_1, \dots, a_{n-1}),$$

wobei  $a_i := a(i)$  für alle  $i \in \mathbb{Z}_n$  gilt.

Die Menge aller  $n$ -Tupel über  $A$  wird mit  $A^n$  notiert. Es gilt stets

$$|A^n| = |A|^n.$$

Teilmengen  $R \subseteq A^n$ , also Mengen von  $n$ -Tupeln über  $A$ , nennt man  **$n$ -stellige Relationen** oder auch **Prädikate** über  $A$ .

Informatiker lassen bei Tupeln gern die Klammern und die Kommata weg und schreiben

$$a_0 a_1 \dots a_{n-1} \quad \text{statt} \quad (a_0, a_1, \dots, a_{n-1}).$$

Sie sprechen dann auch nicht von Tupeln, sondern von **Wörtern über dem Alphabet**  $A$ . Die Menge aller Wörter über  $A$  wird mit dem Zeichen  $A^*$  symbolisiert. Es ist also

$$A^* := \bigcup_{n \in \mathbb{N}} A^n.$$

Teilmengen von  $A^*$  nennt man in der Informatik **formale Sprachen**.

Abbildungen von  $\mathbb{N}$  in eine Menge  $A$  nennt man (unendliche) **Folgen** von Elementen aus  $A$ .

Notiert werden solche Folgen in der Form

$$(a_n \mid n \in \mathbb{N}) \quad \text{oder} \quad (a_n)_{n \in \mathbb{N}}.$$

Die Komponenten einer solchen Folge werden als **Folglied** bezeichnet.

$\mathbb{Z}_m \times \mathbb{Z}_n$  ist dann die Menge aller Paare natürlicher Zahlen, bei denen die erste kleiner als  $m$  und die zweite kleiner als  $n$  ist, also

$$\mathbb{Z}_m \times \mathbb{Z}_n = \{(i, j) \mid i, j \in \mathbb{N}, i < m, j < n\}.$$

Beispielsweise ist

$$\mathbb{Z}_3 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1)\}.$$

Abbildungen von  $\mathbb{Z}_z \times \mathbb{Z}_s$  nach  $A$  nennt man  $z \times s$ -**Matrizen** mit Komponenten aus  $A$ . Eine solche Matrix  $m : \mathbb{Z}_z \times \mathbb{Z}_s \rightarrow A$  schreibt man gewöhnlich nicht als Abbildung auf, sondern als rechteckiges Schema der Form

$$\begin{pmatrix} m_{0,0} & m_{0,1} & \dots & m_{0,s-1} \\ m_{1,0} & m_{1,1} & \dots & m_{1,s-1} \\ \vdots & \vdots & \ddots & \vdots \\ m_{z-1,0} & m_{z-1,1} & \dots & m_{z-1,s-1} \end{pmatrix},$$

wobei jeweils  $m_{i,j}$  für das Bild des Paares  $(i,j)$  unter der Abbildung  $m$  steht.

# Operationen

Abbildungen von  $A^n$  nach  $A$ , also Abbildungen der Form

$$f : A^n \rightarrow A,$$

nennen wir  **$n$ -stellige Operationen** auf  $A$ .

Addition, Subtraktion und Multiplikation reeller Zahlen sind Beispiele 2-stelliger Operationen auf  $\mathbb{R}$ .

Zwei der 16 zweistelligen Operationen auf  $\{0,1\}$  sind

$\vee$	0	1
0	0	1
1	1	1

und

$\wedge$	0	1
0	0	0
1	0	1

# Charakteristische Funktion

Jeder Teilmenge  $T \subseteq S$  einer beliebigen Menge  $S$  kann man eine Abbildung  $\chi_T : S \rightarrow \{0, 1\}$  zuordnen durch

$$\chi_T(s) := \begin{cases} 0 & \text{falls } s \notin T \\ 1 & \text{falls } s \in T \end{cases}.$$

Man nennt  $\chi_T$  die **charakteristische Funktion** der Teilmenge  $T$ .

Definiert man  $\chi_A \wedge \chi_B$  und  $\chi_A \vee \chi_B$  punktweise, also durch

- $(\chi_A \wedge \chi_B)(s) := \chi_A(s) \wedge \chi_B(s)$  für  $s \in S$
- $(\chi_A \vee \chi_B)(s) := \chi_A(s) \vee \chi_B(s)$  für  $s \in S$ ,

so ergibt sich

$$\chi_A \wedge \chi_B = \chi_{A \cap B} \quad \text{und} \quad \chi_A \vee \chi_B = \chi_{A \cup B}.$$

Dadurch lassen sich die Mengenoperationen in das Rechnen mit Abbildungen übersetzen.

# Verallgemeinerte Mengen

Die Darstellung von Mengen über ihre charakteristischen Funktionen lädt zum Verallgemeinern ein. Man kann nun leicht Variationen des Mengenbegriffs erfinden, z.B.

- **Multimengen**, bei denen Elemente mehrfach vorkommen dürfen, als Abbildungen der Form

$$\mu : S \rightarrow (\mathbb{N}, \min, \max)$$

oder

- **Fuzzymengen**, in denen Elemente nur teilweise vorkommen, als Abbildungen der Form

$$\varphi : S \rightarrow ([0, 1], \min, \max).$$

# Ausgelassen: Einschränkung

Die **Einschränkung** von  $f : A \rightarrow B$  auf eine Teilmenge  $S \subseteq A$ ,

$$f|_S : S \rightarrow B$$

hat als Definitionsbereich die Menge  $S$  und stimmt ansonsten mit  $f$  überein.

Es gilt also

$$f|_S(x) = f(x) \quad \text{für alle } x \in S.$$

Gleichbedeutend dazu ist die Bedingung

$$f|_S = f \cap (S \times B).$$

# Ausgelassen: kanonische Projektionen

Die **kanonischen Projektionen** vom direkten Produkt  $A \times B$  auf die Faktoren sind die Abbildungen

$$\begin{array}{ll} \pi_1 : A \times B \rightarrow A & \text{mit} \quad \pi_1((a, b)) := a, \\ \pi_2 : A \times B \rightarrow B & \text{mit} \quad \pi_2((a, b)) := b. \end{array}$$

Diese Eigenschaft ist in folgendem Sinne charakteristisch für das Mengenprodukt: Wenn  $S$  irgendeine Menge ist und  $\varphi_1 : S \rightarrow A$  sowie  $\varphi_2 : S \rightarrow B$  Abbildungen sind, dann gibt es eine Abbildung  $\varphi : S \rightarrow A \times B$  mit

$$\varphi_1 = \pi_1 \varphi \quad \text{und} \quad \varphi_2 = \pi_2 \varphi.$$

# Ausgelassen: disjunkte Vereinigung

Die **disjunkte Vereinigung** oder, synonym, das **Koprodukt** zweier Mengen  $A$  und  $B$  ist definiert als

$$A \dot{\cup} B := (A \times \{1\}) \cup (B \times \{2\}).$$

Man hat dafür die natürlichen Einbettungen

$$\begin{aligned} \varepsilon_1 : A &\rightarrow A \dot{\cup} B & \text{mit} & \quad \varepsilon_1(a) := (a, 1), \\ \varepsilon_2 : B &\rightarrow A \dot{\cup} B & \text{mit} & \quad \varepsilon_2(b) := (b, 2). \end{aligned}$$

Die charakteristische Eigenschaft des Koproduktes ist die folgende: Wenn  $S$  irgendeine Menge ist und  $\varphi_1 : A \rightarrow S$  sowie  $\varphi_2 : B \rightarrow S$  Abbildungen sind, dann gibt es eine Abbildung  $\varphi : A \dot{\cup} B \rightarrow S$  mit

$$\varphi_1 = \varphi \varepsilon_1 \quad \text{und} \quad \varphi_2 = \varphi \varepsilon_2.$$