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 (Gerichteter Multigraph)

Ein gerichteter Multigraph G ist gegeben durch

- eine Eckenmenge oder Knotenmenge E
- eine Kantenmenge K
- Abbildungen $q\colon K \to E$, $z\colon K \to E$,
- k heißt Kante von $q(k)$ nach $z(k)$

Definition (Ungerichteter Multigraph)

Ein ungerichteter Multigraph ist gegeben durch

- eine Eckenmenge (oder Knotenmenge) E
- eine Kantenmenge K
- eine Abbildung $r\colon K \to \{\{c, d\} \mid c, d \in E\}$ mit $k \mapsto r(k)$
- k ist Kante zwischen diesen Ecken

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

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

Definition

- Eine Menge M heißt endlich, wenn es eine natürliche Zahl m und eine bijektive Abbildung $\alpha\colon \{0, 1, \ldots, m-1\} \to M$ gibt
- In diesem Fall ist m eindeutig bestimmt und man nennt $\#(M) := m$ die Anzahl der Elemente von M
- Die Abbildung α ist im Allgemeinen nicht eindeutig und heißt eine Aufzählung von M
- Eine bijektive Abbildung $\nu\colon M \to \{0, 1, \ldots, m-1\}$ wird eine Nummerierung von M genannt
- Die Umkehrabbildung einer Aufzählung von M ist eine Nummerierung
- Die Umkehrabbildung einer Nummerierung von M ist eine Aufzählung
- Wenn M nicht endlich ist, dann heißt M unendlich und man schreibt $\#(M) = \infty$ (oder manchmal $\#(M) = \omega$)

Satz

1. *Gleichheitsregel Sind M und N endliche Mengen und ist $f : M \to N$ eine bijektive Abbildung, so gilt $\#(M) = \#(N)$*

Satz

1. *Gleichheitsregel Sind M und N endliche Mengen und ist $f : M \to N$ eine bijektive Abbildung, so gilt $\#(M) = \#(N)$*
2. *Summenregel Sind $A_1, A_2, \ldots, A_k$ paarweise disjunkte endliche Mengen, so gilt für die Vereinigung*

$$\#(A_1 \cup A_2 \cup \ldots \cup A_k) = \sum_{i=1}^{k} \#(A_i) \,.$$

Satz

1. *Gleichheitsregel Sind M und N endliche Mengen und ist $f : M \to N$ eine bijektive Abbildung, so gilt $\#(M) = \#(N)$*
2. *Summenregel Sind $A_1, A_2, \ldots, A_k$ paarweise disjunkte endliche Mengen, so gilt für die Vereinigung*

$$\#(A_1 \cup A_2 \cup \ldots \cup A_k) = \sum_{i=1}^{k} \#(A_i)\,.$$

3. *Differenzregel Für endliche Mengen A und B gilt*

$$\#(A \setminus B) = \#(A) - \#(A \cap B)\,.$$

Beweis.

(1) M ist endlich, also gibt es laut Definition eine natürliche Zahl m und eine bijektive Abbildung $\alpha\colon \{0, 1, \ldots, m-1\} \to M$

Beweis.

(1) M ist endlich, also gibt es laut Definition eine natürliche Zahl m und eine bijektive Abbildung $\alpha\colon \{0, 1, \ldots, m-1\} \to M$

Betrachte die zusammengesetzte Abbildung

$$f \circ \alpha\colon \{0, 1, \ldots, m-1\} \to N\ ,\ i \mapsto f(\alpha(i))\ ,$$

Beweis.

(1) M ist endlich, also gibt es laut Definition eine natürliche Zahl m und eine bijektive Abbildung $\alpha\colon \{0, 1, \ldots, m-1\} \to M$

Betrachte die zusammengesetzte Abbildung

$$f \circ \alpha\colon \{0, 1, \ldots, m-1\} \to N\ ,\ i \mapsto f(\alpha(i))\,,$$

$f \circ \alpha$ ist bijektiv, also $\#(N) = m$

Beweis.

(1) M ist endlich, also gibt es laut Definition eine natürliche Zahl m und eine bijektive Abbildung $\alpha\colon \{0, 1, \dots, m-1\} \to M$

Betrachte die zusammengesetzte Abbildung

$$f \circ \alpha\colon \{0, 1, \dots, m-1\} \to N\ ,\ i \mapsto f(\alpha(i))\,,$$

$f \circ \alpha$ ist bijektiv, also $\#(N) = m$

(3) Aus der folgenden Beobachtung zur disjunkten Vereinigung

$$A = (A \setminus B) \cup (A \cap B)$$

folgt nach der Summenregel:

$$\#(A \setminus B) = \#(A) - \#(A \cap B)$$

Beweis.

(2) Seien die folgenden Abbildungen bijektiv

$$\alpha_1\colon \{0,1,\ldots,m_1-1\} \to M_1, \ldots, \alpha_k\colon \{0,1,\ldots,m_k-1\} \to M_k$$

Dann ist auch die zusammengesetzte Abbildung
$\alpha\colon \{0,1,\ldots,m_1+\ldots+m_k-1\} \to M_1 \cup \ldots \cup M_k$ bijektiv:

$$i \mapsto \begin{cases} \alpha_1(i) & i \in \{0,1,\cdots,m_1-1\} \\ \alpha_2(i-m_1) & i \in \{m_1,\cdots,m_1+m_2-1\} \\ \vdots & \vdots \\ \alpha_k(i-m_1-\ldots-m_{k-1}) & i \in \{m_1+\ldots+m_{k-1},\cdots,m_1+\ldots+m_k-1\} \end{cases}$$

Beweis.

(2) Seien die folgenden Abbildungen bijektiv

$$\alpha_1\colon \{0,1,\ldots,m_1-1\} \to M_1, \ldots, \alpha_k\colon \{0,1,\ldots,m_k-1\} \to M_k$$

Dann ist auch die zusammengesetzte Abbildung
$\alpha\colon \{0,1,\ldots,m_1+\ldots+m_k-1\} \to M_1 \cup \ldots \cup M_k$ bijektiv:

$$i \mapsto \begin{cases} \alpha_1(i) & i \in \{0,1,\cdots,m_1-1\} \\ \alpha_2(i-m_1) & i \in \{m_1,\cdots,m_1+m_2-1\} \\ \vdots & \vdots \\ \alpha_k(i-m_1-\ldots-m_{k-1}) & i \in \{m_1+\ldots+m_{k-1},\cdots,m_1+\ldots+m_k-1\} \end{cases}$$

∎

Satz

4 *Siebformel Für endliche Mengen $A_1, A_2, \ldots, A_k$ gilt*

$$\#(A_1 \cup \ldots \cup A_k) = \sum_{\substack{I \subseteq \{1,2,\ldots,k\} \\ I \neq \varnothing}} (-1)^{\#(I)-1} \, \#\Big(\bigcap_{i \in I} A_i\Big)$$

Insbesondere ist für endliche Mengen A und B

$$\#(A \cup B) = \#(A) + \#(B) - \#(A \cap B)$$

Satz

4 *Siebformel* *Für endliche Mengen* $A_1, A_2, \dots, A_k$ *gilt*

$$\#(A_1 \cup \ldots \cup A_k) = \sum_{\substack{I \subseteq \{1,2,\ldots,k\} \\ I \neq \emptyset}} (-1)^{\#(I)-1} \#\Big(\bigcap_{i \in I} A_i\Big)$$

Insbesondere ist für endliche Mengen A und B

$$\#(A \cup B) = \#(A) + \#(B) - \#(A \cap B)$$

5 *Produktregel* *Sind* $M_1, M_2, \dots, M_k$ *endliche Mengen, so gilt für das kartesische Produkt*

$$\#(M_1 \times M_2 \times \ldots \times M_k) = \prod_{i=1}^{k} \#(M_i)\,.$$

Insbesondere ist für eine endliche Menge M

$$\#(M^k) = \#(M)^k$$

Beweis.

(4) Mit Induktion über k, aus der disjunkten Vereinigung $A_1 \cup A_2 = A_1 \cup (A_2 \setminus A_1)$ folgt

$$\#(A_1 \cup A_2) = \#(A_1) + \#(A_2 \setminus A_1) = \#(A_1) + \#(A_2) - \#(A_1 \cap A_2)$$

Beweis.

(4) Mit Induktion über k, aus der disjunkten Vereinigung $A_1 \cup A_2 = A_1 \cup (A_2 \setminus A_1)$ folgt

$$\#(A_1 \cup A_2) = \#(A_1) + \#(A_2 \setminus A_1) = \#(A_1) + \#(A_2) - \#(A_1 \cap A_2)$$

Für $k > 2$ gilt nach Induktionsannahme

$$\#\Big(\bigcup_{i=1}^{k} A_i\Big) = \#\Big(\Big(\bigcup_{i=1}^{k-1} A_i\Big) \cup A_k\Big) = \#\Big(\bigcup_{i=1}^{k-1} A_i\Big) + \#(A_k) - \#\Big(\bigcup_{i=1}^{k-1} (A_i \cap A_k)\Big) =$$

$$= \sum_{\substack{I \subseteq \{1,\ldots,k-1\} \\ I \neq \varnothing}} (-1)^{\#(I)-1} \, \#\Big(\bigcap_{i \in I} A_i\Big) + \#(A_k) -$$

$$- \sum_{\substack{I \subseteq \{1,\ldots,k-1\} \\ I \neq \varnothing}} (-1)^{\#(I)-1} \, \#\Big(\bigcap_{i \in I} A_i \cap A_k\Big) = \sum_{\substack{J \subseteq \{1,\ldots,k\} \\ J \neq \varnothing}} (-1)^{\#(J)-1} \, \#\Big(\bigcap_{i \in J} A_i\Big)$$

Beweis.

(4) Mit Induktion über k, aus der disjunkten Vereinigung $A_1 \cup A_2 = A_1 \cup (A_2 \setminus A_1)$ folgt

$$\#(A_1 \cup A_2) = \#(A_1) + \#(A_2 \setminus A_1) = \#(A_1) + \#(A_2) - \#(A_1 \cap A_2)$$

Für $k > 2$ gilt nach Induktionsannahme

$$\#(\bigcup_{i=1}^{k} A_i) = \#((\bigcup_{i=1}^{k-1} A_i) \cup A_k) = \#(\bigcup_{i=1}^{k-1} A_i) + \#(A_k) - \#(\bigcup_{i=1}^{k-1} (A_i \cap A_k)) =$$

$$= \sum_{\substack{I \subseteq \{1,\dots,k-1\} \\ I \neq \varnothing}} (-1)^{\#(I)-1} \#(\bigcap_{i \in I} A_i) + \#(A_k) -$$

$$- \sum_{\substack{I \subseteq \{1,\dots,k-1\} \\ I \neq \varnothing}} (-1)^{\#(I)-1} \#(\bigcap_{i \in I} A_i \cap A_k) = \sum_{\substack{J \subseteq \{1,\dots,k\} \\ J \neq \varnothing}} (-1)^{\#(J)-1} \#(\bigcap_{i \in J} A_i)$$

Die letzte Gleichung gilt für die drei Fälle (i) $J = I$, (ii) $J = \{k\}$, (iii) $J = I \cup \{k\}$

Beweis.

(5) Laut Voraussetzung sind die folgenden Funktionen α_i bijektiv

$$\alpha_1\colon \{0, 1, \ldots, m_1 - 1\} \to M_1, \ldots, \alpha_k\colon \{0, 1, \ldots, m_k - 1\} \to M_k$$

Beweis.

(5) Laut Voraussetzung sind die folgenden Funktionen α_i bijektiv

$$\alpha_1 \colon \{0, 1, \ldots, m_1 - 1\} \to M_1, \ldots, \alpha_k \colon \{0, 1, \ldots, m_k - 1\} \to M_k$$

Also ist $\alpha \colon \{0, 1, \ldots, m_1 \cdots m_k - 1\} \to M_1 \times \ldots \times M_k$ mit

$$n \mapsto (\alpha_1(n/m_2 \cdots m_k), \ldots, \alpha_{k-1}((n/m_k) \bmod m_{k-1}), \alpha_k(n \bmod m_k))$$

bijektiv.

Beweis.

(5) Laut Voraussetzung sind die folgenden Funktionen α_i bijektiv

$$\alpha_1\colon \{0, 1, \ldots, m_1 - 1\} \to M_1, \ldots, \alpha_k\colon \{0, 1, \ldots, m_k - 1\} \to M_k$$

Also ist $\alpha\colon \{0, 1, \ldots, m_1 \cdots m_k - 1\} \to M_1 \times \ldots \times M_k$ mit

$$n \mapsto (\alpha_1(n/m_2 \cdots m_k), \ldots, \alpha_{k-1}((n/m_k) \bmod m_{k-1}), \alpha_k(n \bmod m_k))$$

bijektiv. Aus den Einzelnummern

$$\begin{aligned} i_k &= n \bmod m_k \\ i_{k-1} &= (n/m_k) \bmod m_{k-1} \\ &\vdots \\ i_2 &= (n/(m_3 \cdots m_k)) \bmod m_2 \\ i_1 &= n/(m_2 \cdots m_k) \end{aligned}$$

erhält man die Gesamtnummer

$$n := i_1 \cdot m_2 \cdots m_k + i_2 \cdot m_3 \cdots m_k + \ldots + i_{k-1} \cdot m_k + i_k$$

Beweis.

(5) Laut Voraussetzung sind die folgenden Funktionen α_i bijektiv

$$\alpha_1 \colon \{0, 1, \ldots, m_1 - 1\} \to M_1, \ldots, \alpha_k \colon \{0, 1, \ldots, m_k - 1\} \to M_k$$

Also ist $\alpha \colon \{0, 1, \ldots, m_1 \cdots m_k - 1\} \to M_1 \times \ldots \times M_k$ mit

$$n \mapsto (\alpha_1(n/m_2 \cdots m_k), \ldots, \alpha_{k-1}((n/m_k) \bmod m_{k-1}), \alpha_k(n \bmod m_k))$$

bijektiv. Aus den Einzelnummern

$$\begin{aligned} i_k &= n \bmod m_k \\ i_{k-1} &= (n/m_k) \bmod m_{k-1} \\ &\vdots \\ i_2 &= (n/(m_3 \cdots m_k)) \bmod m_2 \\ i_1 &= n/(m_2 \cdots m_k) \end{aligned}$$

erhält man die Gesamtnummer

$$n := i_1 \cdot m_2 \cdots m_k + i_2 \cdot m_3 \cdots m_k + \ldots + i_{k-1} \cdot m_k + i_k$$

∎

Beispiel

In C-Programmen werden die Elemente mehrdimensionaler Felder hintereinander im Speicher abgelegt, wobei die Reihenfolge so geregelt ist, dass „hintere Indizes schneller laufen als vordere“. Zum Beispiel liegen für

```
int M[2][3] = {{3,5,-2},{1,0,2}};
```

die Feldelemente wie folgt im Speicher:

M[0][0] 3	M[0][1] 5	M[0][2] -2	M[1][0] 1	M[1][1] 0	M[1][2] 2

M

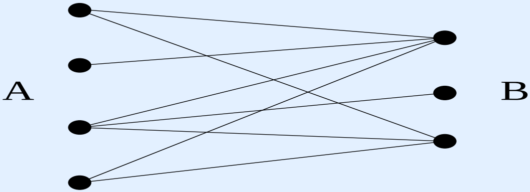
Beispiel (cont'd)

```
double f(double *z, int m1, int m2, int m3)
{
  ...
}
...
int main( void)
{
   double x, y, A[2][3][4], B[3][4][2];
   ...
   x = f(&A[0][0][0],2,3,4);
   y = f(&B[0][0][0],3,4,2);
   ...
}
```

In der Funktion `f` kann das Feldelement „`z[i][j][k]`“ als `*(z+i*m2*m3+j*m3+k)` angesprochen werden; die Indizes `i`, `j`, `k` des Feldelements an der Adresse `z+l` können wie folgt berechnet werden `k = l%m3`, `j = (l/m3)%m2` und `i = l/(m2*m3)`

Satz

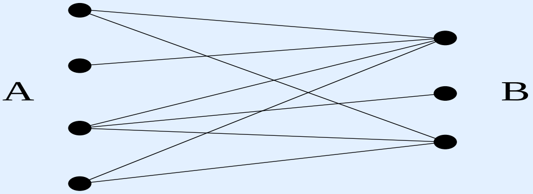
6 *Regel des zweifachen Abzählens* *Ein ungerichteter Graph heißt* *bipartit*, *wenn es eine Partition der Eckenmenge in zwei Blöcke A und B gibt, sodass jede Kante eine Endecke in A und eine Endecke in B hat.*



Für einen endlichen bipartiten Graphen gilt $\sum_{e_1 \in A} \mathrm{Grad}(e_1) = \sum_{e_2 \in B} \mathrm{Grad}(e_2)$

Satz

6 *Regel des zweifachen Abzählens* *Ein ungerichteter Graph heißt* *bipartit*, *wenn es eine Partition der Eckenmenge in zwei Blöcke A und B gibt, sodass jede Kante eine Endecke in A und eine Endecke in B hat.*



Für einen endlichen bipartiten Graphen gilt $\sum_{e_1 \in A} \mathrm{Grad}(e_1) = \sum_{e_2 \in B} \mathrm{Grad}(e_2)$

Beweis.

(6) Beide Summen geben die Zahl der Kanten an ∎

Satz (Schubfachprinzip)

Seien $f : M \to N$ eine Abbildung und M, N endliche Mengen. Wenn $\#(M) > \#(N)$ ist, dann gibt es mindestens ein Element $y \in N$ mit mehr als einem Urbild.

Satz (Schubfachprinzip)

Seien $f : M \to N$ eine Abbildung und M, N endliche Mengen. Wenn $\#(M) > \#(N)$ ist, dann gibt es mindestens ein Element $y \in N$ mit mehr als einem Urbild.

Beweis.

Angenommen jedes Element von N hat höchstens ein Urbild; dann ist f injektiv und somit die eingeschränkte Abbildung $M \to f(M)$ bijektiv. Also $\#(M) = \#(f(M))$ und aus $f(M) \subseteq N$ folgt $\#(M) \leqslant \#(N)$ ∎

Satz (Schubfachprinzip)

Seien $f : M \to N$ eine Abbildung und M, N endliche Mengen. Wenn $\#(M) > \#(N)$ ist, dann gibt es mindestens ein Element $y \in N$ mit mehr als einem Urbild.

Beweis.

Angenommen jedes Element von N hat höchstens ein Urbild; dann ist f injektiv und somit die eingeschränkte Abbildung $M \to f(M)$ bijektiv. Also $\#(M) = \#(f(M))$ und aus $f(M) \subseteq N$ folgt $\#(M) \leqslant \#(N)$ ■

Satz

Seien K und M endliche Mengen mit k bzw. m Elementen. Dann gibt es genau m^k verschiedene Abbildungen von K nach M.

Satz (Schubfachprinzip)

Seien $f\colon M \to N$ eine Abbildung und M, N endliche Mengen. Wenn $\#(M) > \#(N)$ ist, dann gibt es mindestens ein Element $y \in N$ mit mehr als einem Urbild.

Beweis.

Angenommen jedes Element von N hat höchstens ein Urbild; dann ist f injektiv und somit die eingeschränkte Abbildung $M \to f(M)$ bijektiv. Also $\#(M) = \#(f(M))$ und aus $f(M) \subseteq N$ folgt $\#(M) \leqslant \#(N)$ ∎

Satz

Seien K und M endliche Mengen mit k bzw. m Elementen. Dann gibt es genau m^k verschiedene Abbildungen von K nach M.

Beweis.

Schreibt man $K = \{x_1, \dots, x_k\}$, dann ist $f\colon K \to M$ durch das Tupel $(f(x_i))_{i=1}^k$ in M^k eindeutig bestimmt ∎

Satz

Seien K und M endliche Mengen mit k bzw. m Elementen. Dann gibt es genau

$$(m)_k := \begin{cases} m(m-1)(m-2)\cdots(m-k+1) & \text{falls } k \geqslant 1 \\ 1 & \text{falls } k = 0 \end{cases}$$

verschiedene injektive Abbildungen von K nach M. Man nennt die Zahl $(m)_k$ die fallende Faktorielle von m und k.

Satz

Seien K und M endliche Mengen mit k bzw. m Elementen. Dann gibt es genau

$$(m)_k \;:= \begin{cases} m(m-1)(m-2)\cdots(m-k+1) & \text{falls } k \geqslant 1 \\ 1 & \text{falls } k = 0 \end{cases}$$

verschiedene injektive Abbildungen von K nach M. Man nennt die Zahl $(m)_k$ die fallende Faktorielle von m und k.

Beispiel

Offensichtlich gibt es keine (totale) injektive Abbildung von $\{0, 1, 2, 3\}$ nach $\{0, 1\}$, was mit dem Satz übereinstimmt, da $(2)_4 = 2 \cdot 1 \cdot 0 \cdot -1 = 0$.

Beweis.

Wir zeigen die Formel durch Induktion über k. Am Induktionsanfang ist $k = 0$, somit K leer und die einzige injektive Abbildung die leere Abbildung. Für den Induktionsschluss schreiben wir

$$K = \{x_0, x_1, \ldots, x_k\}$$

und überlegen uns, wie viele injektive Abbildungen $f\colon K \to M$ es geben kann.

Beweis.

Wir zeigen die Formel durch Induktion über k. Am Induktionsanfang ist $k = 0$, somit K leer und die einzige injektive Abbildung die leere Abbildung. Für den Induktionsschluss schreiben wir

$$K = \{x_0, x_1, \ldots, x_k\}$$

und überlegen uns, wie viele injektive Abbildungen $f\colon K \to M$ es geben kann. Für x_0 gibt es m Möglichkeiten, ein Bild $f(x_0) \in M$ zu wählen. Dieses Element

$$y_0 := f(x_0)$$

darf dann aber nicht mehr als Bild eines anderen Elements in K gewählt werden, sodass für die Wahl der Bilder von $x_1, \ldots, x_k$ nur die Elemente in $M \setminus \{y_0\}$ in Frage kommen.

Beweis.

Wir zeigen die Formel durch Induktion über k. Am Induktionsanfang ist $k = 0$, somit K leer und die einzige injektive Abbildung die leere Abbildung. Für den Induktionsschluss schreiben wir

$$K = \{x_0, x_1, \ldots, x_k\}$$

und überlegen uns, wie viele injektive Abbildungen $f\colon K \to M$ es geben kann. Für x_0 gibt es m Möglichkeiten, ein Bild $f(x_0) \in M$ zu wählen. Dieses Element

$$y_0 := f(x_0)$$

darf dann aber nicht mehr als Bild eines anderen Elements in K gewählt werden, sodass für die Wahl der Bilder von $x_1, \ldots, x_k$ nur die Elemente in $M \setminus \{y_0\}$ in Frage kommen. Nach Induktionsannahme gibt es dafür $(m-1)_k$ Möglichkeiten. Die Gesamtzahl der Möglichkeiten ist somit

$$m \cdot (m-1)_k = (m)_{k+1}$$

Beweis.

Wir zeigen die Formel durch Induktion über k. Am Induktionsanfang ist $k = 0$, somit K leer und die einzige injektive Abbildung die leere Abbildung. Für den Induktionsschluss schreiben wir

$$K = \{x_0, x_1, \ldots, x_k\}$$

und überlegen uns, wie viele injektive Abbildungen $f\colon K \to M$ es geben kann. Für x_0 gibt es m Möglichkeiten, ein Bild $f(x_0) \in M$ zu wählen. Dieses Element

$$y_0 := f(x_0)$$

darf dann aber nicht mehr als Bild eines anderen Elements in K gewählt werden, sodass für die Wahl der Bilder von $x_1, \ldots, x_k$ nur die Elemente in $M \setminus \{y_0\}$ in Frage kommen. Nach Induktionsannahme gibt es dafür $(m-1)_k$ Möglichkeiten. Die Gesamtzahl der Möglichkeiten ist somit

$$m \cdot (m-1)_k = (m)_{k+1}$$

■

Satz

Seien K und M endliche Mengen mit jeweils m Elementen. Dann gibt es genau

$$m! := \begin{cases} m(m-1)(m-2)\cdots 3\cdot 2\cdot 1 & m \geqslant 1 \\ 1 & m = 0 \end{cases}$$

verschiedene bijektive Abbildungen von K nach M. Man nennt die Zahl $m!$ die Faktorielle oder Fakultät von m.

Satz

Seien K und M endliche Mengen mit jeweils m Elementen. Dann gibt es genau

$$m! \; := \begin{cases} m(m-1)(m-2)\cdots 3\cdot 2\cdot 1 & m \geqslant 1 \\ 1 & m = 0 \end{cases}$$

verschiedene bijektive Abbildungen von K nach M. Man nennt die Zahl $m!$ die Faktorielle oder Fakultät von m.

Beweis.

Wegen $\#(K) = \#(M) = m$ ist jede injektive Abbildung von K nach M bijektiv. Damit folgen die Behauptungen aus dem Satz mit $(m)_m = m!$.

Satz

Seien K und M endliche Mengen mit jeweils m Elementen. Dann gibt es genau

$$m! := \begin{cases} m(m-1)(m-2)\cdots 3\cdot 2\cdot 1 & m \geqslant 1 \\ 1 & m = 0 \end{cases}$$

verschiedene bijektive Abbildungen von K nach M. Man nennt die Zahl $m!$ die Faktorielle oder Fakultät von m.

Beweis.

Wegen $\#(K) = \#(M) = m$ ist jede injektive Abbildung von K nach M bijektiv. Damit folgen die Behauptungen aus dem Satz mit $(m)_m = m!$. ∎

Satz

Sei M eine endliche Menge mit m Elementen. Dann gilt

$$\#(\mathcal{P}(M)) = 2^m \,.$$

Satz

Sei M eine endliche Menge mit m Elementen. Dann gilt

$$\#(\mathcal{P}(M)) = 2^m \,.$$

Beweis.

Wir fixieren eine Aufzählung $\alpha\colon \{0, 1, \ldots, m-1\} \to M$. Dann ist die folgende Abbildung bijektiv, insbesondere können Teilmengen als Bitmuster programmiert werden.

$$F\colon \mathcal{P}(M) \to \{0,1\}^m \,,\; T \mapsto (t_0, \ldots, t_{m-1}) \,,\; t_i := \begin{cases} 1 & \text{falls } \alpha(i) \in T \\ 0 & \text{sonst.} \end{cases}$$

Satz

Sei M eine endliche Menge mit m Elementen. Dann gilt

$$\#(\mathcal{P}(M)) = 2^m \, .$$

Beweis.

Wir fixieren eine Aufzählung $\alpha \colon \{0, 1, \ldots, m-1\} \to M$. Dann ist die folgende Abbildung bijektiv, insbesondere können Teilmengen als Bitmuster programmiert werden.

$$F \colon \mathcal{P}(M) \to \{0,1\}^m \, , \; T \mapsto (t_0, \ldots, t_{m-1}) \, , \; t_i := \begin{cases} 1 & \text{falls } \alpha(i) \in T \\ 0 & \text{sonst.} \end{cases}$$

$\blacksquare$

Satz

Sei M eine endliche Menge mit m Elementen und sei k eine natürliche Zahl. Dann gilt

$$\#(\mathcal{P}_k(M)) = \binom{m}{k}.$$

Dabei ist der Binomialkoeffizient „m über k“ definiert als

$$\binom{m}{k} := \frac{m \cdot (m-1) \cdots (m-k+1)}{k \cdot (k-1) \cdots 1} = \begin{cases} \dfrac{m!}{k!(m-k)!} & \text{falls } k \leqslant m \\ 0 & \text{sonst} \end{cases}$$

Beweis.

Eine Aufzählung $\alpha\colon \{0, 1, \ldots, k-1\} \to T$ einer k-elementigen Teilmenge T von M erhält man durch Wählen

- eines beliebigen Elements $\alpha(0) \in M$,
- eines beliebigen Elements $\alpha(1) \in M \setminus \{\alpha(0)\}$,
- eines beliebigen Elements $\alpha(2) \in M \setminus \{\alpha(0), \alpha(1)\}$, usw.

Da es bei der Teilmenge T nicht auf die Reihenfolge der gewählten Elemente ankommt, ergibt sich die gesuchte Anzahl als

$$m \cdot (m-1) \cdots (m-k+1)/k!\,.$$

Beweis.

Eine Aufzählung $\alpha\colon \{0, 1, \ldots, k-1\} \to T$ einer k-elementigen Teilmenge T von M erhält man durch Wählen

- eines beliebigen Elements $\alpha(0) \in M$,
- eines beliebigen Elements $\alpha(1) \in M \setminus \{\alpha(0)\}$,
- eines beliebigen Elements $\alpha(2) \in M \setminus \{\alpha(0), \alpha(1)\}$, usw.

Da es bei der Teilmenge T nicht auf die Reihenfolge der gewählten Elemente ankommt, ergibt sich die gesuchte Anzahl als

$$m \cdot (m-1) \cdots (m-k+1)/k!\,.$$

∎

Definition

Eine Menge M heißt abzählbar unendlich, wenn eine bijektive Abbildung

$$\alpha\colon\ \mathbb{N} \to M\ ,\ i \mapsto x_i\ ,$$

existiert. Man schreibt dann

$$M = \{x_0, x_1, x_2, \ldots\}\ ,$$

nennt α eine Aufzählung von M und α^{-1} eine Nummerierung von M.

Definition

Eine Menge M heißt abzählbar unendlich, wenn eine bijektive Abbildung

$$\alpha\colon \mathbb{N} \to M \,, \; i \mapsto x_i \,,$$

existiert. Man schreibt dann

$$M = \{x_0, x_1, x_2, \ldots\} \,,$$

nennt α eine Aufzählung von M und α^{-1} eine Nummerierung von M.

Beispiel

- Die Menge $\mathbb{N}$ der natürlichen Zahlen ist abzählbar unendlich
- Auch die Menge $\mathbb{Z}$ der ganzen Zahlen ist abzählbar unendlich

Satz

Die Menge $\mathbb{N} \times \mathbb{N}$ *ist abzählbar unendlich.*

Satz

Die Menge $\mathbb{N} \times \mathbb{N}$ ist abzählbar unendlich.

Beweis.

Anstatt einer Aufzählung $\alpha\colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ geben wir eine Nummerierung $\nu\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ an. Wir schreiben die Paare (m, n) zweidimensional

$$\begin{array}{ccccc} (0,0) & (1,0) & (2,0) & (3,0) & \dots \\ (0,1) & (1,1) & (2,1) & (3,1) & \dots \\ (0,2) & (1,2) & (2,2) & (3,2) & \dots \\ (0,3) & (1,3) & (2,3) & (3,3) & \dots \\ \vdots & & & & \end{array}$$

auf und nummerieren diagonal, dabei bekommt das Paar (m, n) die Nummer $\left(\sum_{i=0}^{m+n-1}(i+1)\right) + m$. Somit ist die Abbildung $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(m, n) \mapsto \frac{(m+n)(m+n+1)}{2} + m$ bijektiv

Satz

Die Menge $\mathbb{N} \times \mathbb{N}$ ist abzählbar unendlich.

Beweis.

Anstatt einer Aufzählung $\alpha\colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ geben wir eine Nummerierung $\nu\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ an. Wir schreiben die Paare (m, n) zweidimensional

$$\begin{array}{ccccc} (0,0) & (1,0) & (2,0) & (3,0) & \dots \\ (0,1) & (1,1) & (2,1) & (3,1) & \dots \\ (0,2) & (1,2) & (2,2) & (3,2) & \dots \\ (0,3) & (1,3) & (2,3) & (3,3) & \dots \\ \vdots & & & & \end{array}$$

auf und nummerieren diagonal, dabei bekommt das Paar (m, n) die Nummer $\left(\sum_{i=0}^{m+n-1}(i+1)\right) + m$. Somit ist die Abbildung $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(m, n) \mapsto \frac{(m+n)(m+n+1)}{2} + m$ bijektiv ∎

Definition

Für $x, y \in \mathbb{N}^k$ sei

$$x <_{\text{gradlex}} y\,,$$

falls entweder

$$\sum_{i=1}^{k} x_i <_{\mathbb{N}} \sum_{i=1}^{k} y_i$$

oder

$$\sum_{i=1}^{k} x_i = \sum_{i=1}^{k} y_i \quad \text{und} \quad x <_{\text{lex}} y$$

ist. Wir nennen $\leq_{\text{gradlex}}$ die graduiert-lexikographische Ordnung auf Zahlentupeln.
Zudem ist $\leq_{\text{gradlex}}$ eine totale Ordnung auf $\mathbb{N}^k$.

Satz

Die Menge $\mathbb{N}^k$ ist abzählbar unendlich. ■

Definition

Eine Menge heißt abzählbar, wenn sie endlich oder abzählbar unendlich ist.

Definition

Eine Menge heißt abzählbar, wenn sie endlich oder abzählbar unendlich ist.

Satz

1. *Jede Teilmenge einer abzählbaren Menge ist abzählbar.*
2. *Das Bild einer abzählbaren Menge ist abzählbar.*
3. *Die Vereinigung einer Folge von abzählbaren Mengen ist abzählbar*
4. *Das kartesische Produkt endlich vieler abzählbarer Mengen ist abzählbar*

∎

Definition

Eine Menge heißt abzählbar, wenn sie endlich oder abzählbar unendlich ist.

Satz

1. *Jede Teilmenge einer abzählbaren Menge ist abzählbar.*
2. *Das Bild einer abzählbaren Menge ist abzählbar.*
3. *Die Vereinigung einer Folge von abzählbaren Mengen ist abzählbar*
4. *Das kartesische Produkt endlich vieler abzählbarer Mengen ist abzählbar*

■

Beispiel

Sei Σ ein endliches Alphabet. Dann ist das Wortmonoid Σ^* abzählbar

$$\Sigma^* := \bigcup_{n \geqslant 0} \Sigma^n = \Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \cup \cdots$$

Satz (Satz von Cantor-Schröder-Bernstein)

Seien $f\colon M \to N$ und $g\colon N \to M$ injektive Abbildungen. Dann existiert eine bijektive Abbildung $h\colon M \to N$

Beweis (nach Dongvu Tonien).

An der Tafel ∎

Satz (Satz von Cantor-Schröder-Bernstein)

Seien $f\colon M \to N$ und $g\colon N \to M$ injektive Abbildungen. Dann existiert eine bijektive Abbildung $h\colon M \to N$

Beweis (nach Dongvu Tonien).

An der Tafel ■

Beispiel

Sei $A = B = \{0, 1, 2, \ldots, \omega\}$ und $f\colon A \to B$, $g\colon B \to A$ wie folgt:

$$f(n) := \begin{cases} n+1 & n < \omega \\ \omega & \text{sonst} \end{cases} \qquad g(n) := \begin{cases} n+1 & n < \omega \\ \omega & \text{sonst} \end{cases}$$

f und g sind injektiv; wir gewinnen eine Bijektion $h\colon A \to B$ wie folgt:

$$h(n) := \begin{cases} 2m+1 & \text{n=2m} \\ 2m & \text{n=2m+1} \\ \omega & \text{sonst} \end{cases}$$

Satz

Sei Σ ein Alphabet mit mindestens zwei Buchstaben a und b, und sei $s_0, s_1, s_2, \ldots$ *eine Folge von Folgen in Σ:*

$$\begin{aligned} s_0 &= s_{00}s_{01}s_{02}\ldots \\ s_1 &= s_{10}s_{11}s_{12}\ldots \\ s_2 &= s_{20}s_{21}s_{22}\ldots \\ &\vdots \end{aligned}$$

Dann ist die Folge

$$d_n := \begin{cases} b & \text{falls } s_{nn} = a \\ a & \text{falls } s_{nn} \neq a \end{cases}$$

eine neue Folge

Satz

Sei Σ ein Alphabet mit mindestens zwei Buchstaben a und b, und sei $s_0, s_1, s_2, \ldots$ eine Folge von Folgen in Σ:

$$\begin{aligned} s_0 &= s_{00}s_{01}s_{02}\ldots \\ s_1 &= s_{10}s_{11}s_{12}\ldots \\ s_2 &= s_{20}s_{21}s_{22}\ldots \\ &\vdots \end{aligned}$$

Dann ist die Folge

$$d_n := \begin{cases} b & \textit{falls } s_{nn} = a \\ a & \textit{falls } s_{nn} \neq a \end{cases}$$

eine neue Folge

Beweis.

Wenn d keine neue Folge ist, dann gibt es einen Index n mit $d = s_n$, woraus $d_n = s_{nn}$ im Widerspruch zur Konstruktion von d folgt. ∎

Definition

Wenn es eine bijektive Abbildung $f\colon M \to N$ gibt, dann heißen die Mengen M und N gleichmächtig. Offensichtlich ist Gleichmächtigkeit eine Äquivalenzrelation, und man nennt die Äquivalenzklasse

$$|M| := \{N \mid N \text{ gleichmächtig wie } M\}$$

die Mächtigkeit oder Kardinalität der Menge M. Für eine endliche Menge M ist die Menge

$$\{0, 1, 2, \ldots, \#(M) - 1\}$$

ein Repräsentant von $|M|$. Daher werden die Kardinalitäten endlicher Mengen oft mit den natürlichen Zahlen identifiziert.

Satz

Für Mengen M und N sei

$$|M| \leq |N|\,,$$

wenn es eine injektive Abbildung $f\colon M \to N$ gibt. Dann ist $\leq$ eine partielle Ordnung auf den Kardinalitäten.

Satz

Für Mengen M und N sei

$$|M| \leq |N| \,,$$

wenn es eine injektive Abbildung $f\colon M \to N$ gibt. Dann ist $\leq$ eine partielle Ordnung auf den Kardinalitäten.

Beweisskizze

Nur die Antisymmetrie ist schwierig und diese folgt aus dem Satz von Schröder-Bernstein ∎

Satz

Für Mengen M und N sei

$$|M| \leq |N| \,,$$

wenn es eine injektive Abbildung $f\colon M \to N$ gibt. Dann ist $\leq$ eine partielle Ordnung auf den Kardinalitäten.

Beweisskizze

Nur die Antisymmetrie ist schwierig und diese folgt aus dem Satz von Schröder-Bernstein ∎

Satz

Für endliche Mengen M und N gilt

$$|M| \leq |N| \;\text{ genau dann, wenn }\; \#(M) \leqslant \#(N)$$

Die kleinste Kardinalität einer unendlichen Menge ist $|\mathbb{N}|$, und es gilt $|\mathbb{N}| < |\mathbb{B}^{\mathbb{N}}|$ ∎