1 Kombinatorik endlicher Mengen

Definition 1.1 Eine n-Menge ist eine Menge, die genau n, $n \in \mathbb{N}$, Elemente enthält.

Satz 1.1 *Ist* $M = \{a_1, \ldots, a_n\}$ *eine* n*-Menge, so hat ihre Potenzmenge* $P(M) := \{X : X \subseteq \{a_1, \ldots, a_n\}\}$ *genau* 2^n *Elemente.*

Anzahl der Elemente	Menge	Potenzmenge	Anzahl der Teilmengen
$\|M\|$	M	$P(M)$	$\|P(M)\|$
0	$\emptyset$	$\{\emptyset\}$	1
1	$\{a_1\}$	$\{\emptyset, \{a_1\}\}$	2
2	$\{a_1, a_2\}$	$\{\emptyset, \{a_1\}, \{a_2\}, \{a_1, a_2\}\}$	4
	$\vdots$	$\vdots$	
$k-1$	$\{a_1, \ldots, a_{k-1}\}$	$P(\{a_1, \ldots, a_{k-1}\})$	2^{k-1}
k	$\{a_1, \ldots, a_k\}$	$P(\{a_1, \ldots, a_{k-1}\}) \cup \{X \cup \{a_k\} : X \subseteq \{a_1, \ldots, a_{k-1}\}\}$	2^k

1.1 Einfache Kombinatorische Auswahlprinzipien

1.1.1 Auswahl von k Elementen aus einer n-Menge mit Wiederholung und unter Berücksichtigung der Anordnung

Lemma 1.2 *Es gibt* n^k *Wörter der Länge* k *über dem Alphabet* $\{a_1, \ldots, a_n\}$.

1.1.2 Auswahl von k Elementen aus einer n-Menge ohne Wiederholung und unter Berücksichtigung der Anordnung

Lemma 1.3 *Es gibt*

$$V(n,k) := \begin{cases} 1 & \text{, falls } k = 0 \\ 0 & \text{, falls } k > n \text{ und} \\ \prod_{i=0}^{k-1}(n-i) & \text{, anderenfalls} \end{cases}$$

wiederholungsfreie Wörter der Länge k *über dem Alphabet* $\{a_1, \ldots, a_n\}$.

$$
\left.
\begin{array}{rcl}
 & & b_1 \cdots b_{k-1}\ b_k \\
 & \nearrow & \\
b_1 \cdots b_{k-1} & \rightarrow & \vdots \\
 & \searrow & \\
 & & b_1 \cdots b_{k-1}\ b_n \\
\neq & & \\
 & & b'_1 \cdots b'_{k-1}\ b'_k \\
 & \nearrow & \\
b'_1 \cdots b'_{k-1} & \rightarrow & \vdots \\
 & \searrow & \\
 & & b'_1 \cdots b'_{k-1}\ b'_n
\end{array}
\right\} \text{paarweise verschieden}
$$

wobei $\{a_1, \ldots, a_n\} = \{b_1, \ldots, b_n\} = \{b'_1, \ldots, b'_n\}$

1.1.3 Auswahl von k Elementen aus einer n-Menge ohne Wiederholung und ohne Berücksichtigung der Anordnung

$$\binom{n}{k} := \prod_{i=1}^{k} \frac{n+1-i}{i} = \frac{n \cdot (n-1) \cdots (n-k+1)}{1 \cdot 2 \cdots k}$$

Lemma 1.4 *Die Anzahl der verschiedenen k-Teilmengen einer n-Menge ist $\binom{n}{k}$.*

Eigenschaft 1.5 *1. Es gilt $\binom{n}{0} = \binom{n}{n} = 1$ für alle $n \in \mathbb{N}$.*

2. Es gilt $\binom{n}{k} = 0$ für $k > n$.

2. Es gilt $\binom{n}{k} = \binom{n}{n-k}$ für $0 \leq k \leq n$.

Weitere Eigenschaften der Binomialkoeffizienten

Eigenschaft 1.6
$$\begin{aligned} \sum_{k=0}^{n} \binom{n}{k} &= 2^n \\ \binom{n-1}{k-1} + \binom{n-1}{k} &= \binom{n}{k} \end{aligned}$$

Lemma 1.7
$$\sum_{i=0}^{k} (-1)^i \cdot \binom{n}{i} = (-1)^k \cdot \binom{n-1}{k}$$

Folgerung 1.8
$$\sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} = 0$$

Lemma 1.9
$$\sum_{i=0}^{k} \binom{n+i}{i} = \binom{n+k+1}{k}$$

1.1.4 Auswahl von k Elementen aus einer n-Menge mit Wiederholung und ohne Berücksichtigung der Anordnung

Lemma 1.10 *Es gibt $\binom{n+k-1}{n-1}$ Möglichkeiten der Auswahl von k Elementen aus einer n-Menge mit Wiederholung und ohne Berücksichtigung der Anordnung.*

1.1.5 Noch eine Gleichung für Binomialkoeffizienten

Lemma 1.11 (Vandermondesche Konvolution)
$$\begin{aligned} \sum_{i=1}^{k} \binom{n}{i} \cdot \binom{m}{k-i} &= \binom{n+m}{k} \\ \sum_{i=1}^{n} \binom{n}{i}^2 &= \binom{2n}{n} \end{aligned}$$

1.2 Der DIRICHLETsche Schubfachschluss (Taubenschlagprinzip)

Satz 1.12 *Sind* $k, n \geq 1$ *und sind* $k \cdot n + 1$ *Gegenstände auf* n *Schubfächer so zu verteilen, daß jeder Gegenstand in eines der Fächer gelegt wird, so gibt es ein Schubfach, welches wenigstens* $k + 1$ *Gegenstände enthält.*

Der Fall $k = 1$.

Folgerung 1.13 *Ist* $n \geq 1$ *und sind* $n + 1$ *Gegenstände auf* n *Schubfächer so zu verteilen, daß jeder Gegenstand in eines der Fächer gelegt wird, so gibt es ein Schubfach, welches wenigstens zwei Gegenstände enthält.*

Der unendliche Fall

Folgerung 1.14 *Sind unendliche viele Gegenstände auf endlich viele Schubfächer so zu verteilen, daß jeder Gegenstand in eines der Fächer gelegt wird, so gibt es ein Schubfach, welches unendliche viele Gegenstände enthält.*

Eine Anwendung für $k = 1$.

Lemma 1.15 *Es sei* $n \geq 1$. *Unter beliebig aus der Menge* $\{1, \ldots, 2n\}$ *gewählten* $n + 1$ *Zahlen gibt es stets zwei, von denen eine die andere teilt.*

1.3 Inzidenzstrukturen

Definition 1.2 Ein Tripel $(P, \mathbb{B}, I)$ heißt Inzidenzstruktur, falls

1. P und $\mathbb{B}$ zwei disjunkte Mengen und
2. $I \subseteq \{(p, B) : p \in P \text{ und } B \in \mathbb{B}\}$ sind.

Die Menge P wird Menge der *Punkte* und $\mathbb{B}$ wird Menge der *Blöcke* genannt.

Schreibweise: $p\ I\ B$ für $(p, B) \in I$.

Ist $p \in P$ so setzen wir

$$\mathbb{B}(p) := \{B : B \in \mathbb{B} \text{ und } p\ I\ B\}$$

Folgerung 1.16 *Sind für eine Inzidenzstruktur* P *und* $\mathbb{B}$ *endlich, so gilt*

$$\sum_{p \in P} |\mathbb{B}(p)| = |I| = \sum_{B \in \mathbb{B}} |\{p : p\ I\ B\}| .$$

Definition 1.3 Ist $(P, \mathbb{B}, I)$ Inzidenzstruktur, so heißt $(\mathbb{B}, P, \widehat{I})$ mit

$$\widehat{I} := \{(B, p) : (p, B) \in I\}$$

die zu $(P, \mathbb{B}, I)$ *duale* Inzidenzstruktur.

1.4 Das Prinzip der Inklusion und Exklusion

Einführendes Beispiel

$$|B \cup T \cup K| = \underbrace{|B| + |T| + |K|}_{\text{erste Gruppe}} \underbrace{- |B \cap T| - |B \cap K| - |T \cap K|}_{\text{zweite Gruppe}} + \underbrace{|B \cap T \cap K|}_{\text{dritte Gruppe}}$$

Notation für Mengen

linke Mengenklammer ↓ — rechte Mengenklammer ↓

$$A_i \quad = \quad \Big\{ \quad x \quad : \quad \underbrace{x \text{ hat Eigenschaft } i}_{\uparrow} \quad \Big\}$$

↑ Bezeichnung der Menge; ↑ Variable für Elemente; ↑ Separator; ↑ Eigenschaft der Elemente

Das Prinzip der Inklusion und Exklusion

allgemeiner Fall, erste Notation

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$$
$$-|A_1 \cap A_2| - |A_1 \cap A_3| - \cdots - |A_1 \cap A_n| - |A_2 \cap A_3| - \cdots - |A_{n-1} \cap A_n|$$
$$+|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \cdots + |A_{n-2} \cap A_{n-1} \cap A_n|$$
$$\vdots$$
$$+ (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|$$

Beobachtungen: $\sum_{1 \le i < j \le n} |A_i \cap A_j| =$

$$|A_1 \cap A_2| + |A_1 \cap A_3| + \cdots + |A_1 \cap A_n| + |A_2 \cap A_3| + \cdots + |A_{n-1} \cap A_n|$$

$$\sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| =$$

$$|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \cdots + |A_{n-2} \cap A_{n-1} \cap A_n|$$

Das Prinzip der Inklusion und Exklusion

allgemeiner Fall, zweite Notation

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_n| \quad = \quad & \sum_{i=1}^{n} |A_i| - \sum_{1 \le i_1 < i_2 \le n} |A_{i_1} \cap A_{i_2}| \\ & + \sum_{1 \le i_1 < i_2 < i_3 \le n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \\ & \vdots \\ & - \cdots + \ (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n| \end{aligned}$$

Notation:

$$\binom{M}{k} := \{ X : X \subseteq M \text{ und } |X| = k \}$$

Eigenschaft 1.17

$$\left|\binom{M}{k}\right| = \binom{|M|}{k}$$

Satz 1.18 (Prinzip der Inklusion-Exklusion) *Für endliche Mengen* $A_1, \ldots, A_n$ *gilt*

$$\begin{aligned}\left|\bigcup_{i=1}^{n} A_i\right| &= \sum_{k=1}^{n}\left((-1)^{k-1}\sum_{M\in\binom{\{1,\ldots,n\}}{k}}\left|\bigcap_{i\in M} A_i\right|\right)\\ &= \sum_{\emptyset\neq M\subseteq\{1,\ldots,n\}}(-1)^{|M|-1}\left|\bigcap_{i\in M} A_i\right| .\end{aligned}$$

nochmals Inklusion-Exklusion

Lemma 1.19 *Falls* $x_i \cdot x_j = x_j \cdot x_i$ *für alle* $i, j \in \{1, \ldots, n\}$*, so gilt*

$$\prod_{i=1}^{n}(1 - x_i) = \sum_{M\subseteq\{1,\ldots,n\}}(-1)^{|M|}\cdot\prod_{i\in M} x_i .$$

Teilbarkeit

Es seien $k, n \in \mathbb{N}$. Die Zahl k *teilt* n (Schreibweise $k \mid n$), falls es eine Zahl $m \in \mathbb{N}$ gibt, so daß $k \cdot m = n$.

Eigenschaft 1.20 *1. Es gelten* $1 \mid n$*,* $n \mid n$ *und* $n \mid 0$ *für alle* $n \in \mathbb{N}$*.*

2. *Wenn* $k \mid n$ *und* $n \mid m$*, so gilt* $k \mid m$*.*
3. *Sind* $n \neq 0$ *und* $k \mid n$*, so gilt* $k \leq n$*.*
4. *Gelten* $k \mid n$*,* $k \mid m$ *und* $l \mid l'$*, so gelten auch* $k \mid n + m$*,* $k \mid |n - m|$ *und* $l \cdot k \mid l' \cdot n$*.*
5. *Sind* $k, n \in \mathbb{N}$ *,* $k > 0$*, so gibt es eindeutig bestimmte* $q, r \in \mathbb{N}$ *derart, daß* $0 \leq r < k$ *und* $n = q \cdot k + r$*.*

Größter gemeinsamer Teiler

Definition 1.4

$$\gcd(n, m) := \begin{cases} 0, & \text{falls } n = m = 0 \\ \max\{k : k \mid n \text{ und } k \mid m\}, & \text{anderenfalls.}\end{cases}$$

Eigenschaft 1.21 *1.* $\gcd(n, m) = \gcd(n, m + n) = \gcd(n, |m - n|)$

2. $\gcd(k \cdot n, k \cdot m) = k \cdot \gcd(n, m)$
3. *Sind* $n, m \in \mathbb{N}$*, so gibt es ganze Zahlen* $a, b \in \mathbb{Z}$ *derart, daß* $\gcd(n, m) = a \cdot n + b \cdot m$*.*
4. $\gcd(k, n \cdot m) \mid \gcd(k, n) \cdot \gcd(k, m)$

Primzahlen

Definition 1.5 Eine Zahl $p \in \mathbb{N}$ heißt *Primzahl*, falls $p \notin \{0, 1\}$ und aus $p \mid k \cdot n$ stets $p \mid k$ oder $p \mid n$ folgt.

Eigenschaft 1.22 *$p \in \mathbb{N}$ ist genau dann Primzahl, wenn $p \neq 1$, $p \neq 0$ und es keine Zahl $n \in \mathbb{N}$ mit der Eigenschaft $1 < n < p$ und $n \mid p$ gibt.*

Eigenschaft 1.23 *Jede natürliche Zahl $n \neq 0$ läßt sich eindeutig in der Form $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, wobei die p_i Primzahlen, $p_{i+1} > p_i$, und die Exponenten $\alpha_i \in \mathbb{N} \setminus \{0\}$ sind, darstellen.*

Die Eulersche φ-Funktion

Definition 1.6 Für $n \in \mathbb{N} \setminus \{0\}$ setzen wir

$$\varphi(n) := \left|\left\{m : m \in \{1, \ldots, n\} \text{ und } \gcd(n, m) = 1\right\}\right| .$$

Satz 1.24 *Ist $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ mit paarweise verschiedenen Primzahlen p_i und $\alpha_i > 0$, so gilt $\varphi(n) = n \cdot \prod_{i=1}^{k} \left(1 - p_i^{-1}\right)$.*

Das Sieb des Eratosthenes I

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2		×		×		×		×		×		×		×		×	
	3			×			×			×			×			×	
$\sqrt{x}$-Grenze$(x = 19)$																	
			5					×					×				
						7						×					
									11								
											13						
															17		
																	19

Das Sieb des Eratosthenes II

Definition 1.7 $\pi(x) := |\{p : p \text{ ist Primzahl und } p \leq x\}|$

Satz 1.25 *Es sei $P_n := \{p : p \text{ ist Primzahl, und } p \leq \sqrt{n}\}$. Dann gilt*

$$\begin{aligned} \pi(n) - \pi(\sqrt{n}) &= n - 1 + \sum_{\emptyset \neq M \subseteq P_n} (-1)^{|M|} \cdot \left\lfloor \frac{n}{\prod_{p \in M} p} \right\rfloor \\ &= -1 + \sum_{M \subseteq P_n} (-1)^{|M|} \cdot \left\lfloor \frac{n}{\prod_{p \in M} p} \right\rfloor . \end{aligned}$$