1 Kombinatorik

1.1 Sterlingzahlen 1.Art

Die Stirling-Zahl erster Art $s_{n,k}$ ist die Anzahl der Permutationen einer n-elementigen Menge, die genau k Zykeln haben.

$$s_{n,k} = \left[{n \atop k} \right] = s_{n-1,k-1} + (n-1)\, s_{n-1,k}, \qquad s_{0,0} = 1 = s_{n,n}, \quad s_{n,0} = 0 = s_{0,k}$$

$$x^{\underline{n}} = \sum_{k=0}^{n} (-1)^{n-k}\, s_{n,k}\, x^k$$

1.2 Sterlingzahlen 2.Art

Die Stirling-Zahl zweiter Art $S_{n,k}$ ist die Anzahl der k-elementigen Partitionen einer n-elementigen Menge, also die Anzahl der Möglichkeiten, eine n-elementige Menge in k nichtleere disjunkte Teilmengen aufzuteilen.

$$S_{n,k} = S_{n-1,k-1} + k\, S_{n-1,k}, \qquad S_{0,0} = 1 = S_{n,n}, \quad S_{n,0} = 0 = S_{0,k}$$

$$x^n = \sum_{k=0}^{n} S_{n,k}\, x^{\underline{k}}$$

1.3 Erzeugende Funktionen

Satz (Fundamentalsatz der Algebra)**.** *Sei ein* **Polynom**

$$P(z) = \sum_{k=0}^{n} b_k z^k = a_0 + a_1 z^1 + a_2 z^2 + \ldots + z^n, \qquad b_k \in \mathbb{C}, \quad a_k = \frac{b_k}{b_n}, \quad n \geq 1$$

$\Longrightarrow \exists z_1, \ldots, z_n \in \mathbb{C}$:

(1) $p(z) = (z - z_1)(z - z_2) \ldots (z - z_n)$

(2) $z_1, \ldots z_n$ sind alle NS von $p(z)$

Die Anzahl der Nullstellen (wenn man die Vielfachheit beachtet) ist insgesamt gleich dem Grad des Polynoms.

Der **Konvergenzradius** einer Potenzreihe $f(z) = \sum_{n\geq 0} a_n \cdot z^n \qquad z, a_n \in \mathbb{C}$ ist definiert als:

$$R = \frac{1}{\lim_{n\to\infty} \sqrt[n]{|a_n|}} \in [0, \infty]$$

Cauchyprodukt

$$\sum_{n\geq 0} a_n z^n \cdot \sum_{n\geq 0} b_n z^n = \sum_{n\geq 0} \left(\sum_{k\geq 0}^{n} a_n b_{n-k} \right) z^n$$

Cauchy'sche Abschätzung

Für $f(z) = \sum_{n\geq 0} a_n (z - z_0)^n, \qquad |z - z_0| < R$ gilt:

$$|a_n| \leq \frac{|z - z_0|}{|z - z_0|^n}.$$

Asymptotische Abschätzung der Koeffizienten — Abspalten der dominanten Polstelle

$$f(z) = \sum_{n\geq 0} a_n z^n = \frac{g(z)}{1 - \alpha z}, \qquad g(z) \text{ komplex diffbar}, \quad |z| < |\frac{1}{\alpha}| < R$$

$$\Longrightarrow a_n = g\left(\frac{1}{\alpha}\right) \alpha^n + \mathcal{O}\left(\frac{1}{(R-\varepsilon)^n}\right), \qquad \varepsilon > 0$$

Definition

$$\begin{aligned}
&\text{Folge } a_0, a_1, a_2, \ldots \\
&\iff a_0 + a_1 z + a_2 z^2 + \ldots = \sum_{n\geq 0} a_n (z - z_0)^n \qquad \text{formale Potenzreihe} \\
&\iff \sum_{n\geq 0} a_n (z - z_0)^n = A(z) \qquad \text{Erzeugende Funktion}
\end{aligned}$$

Sei die Folge $(a_n)_{n\geq 0}$ in $\mathbb{R}$ oder $\mathbb{C}$, dann heißt

$$A(z) = \sum_{n\geq 0} a_n z^n \text{ (gewichtete) EF und}$$

$$\hat{A}(z) = \sum_{n\geq 0} \frac{a_n}{n!} z^n \text{ EEF der Folge}(a_n).$$

Anwendung — Zusammenhang mit kombinatorischen Strukturen

EF/EEF können zum Lösen von kombinatorischen Problemen verwendet werden:

- ungeordnete/unmarkierte Strukturen (Kombinationen) $\Longrightarrow$ EF
  z.B. Kugelziehen oder Würfeln, wenn es auf die Reihenfolge *nicht* ankommt.
- geordnete/markierte Strukturen (Variationen) $\Longrightarrow$ EEF
  Reihenfolge wichtig.

Außerdem kann man mit EF explizite Lösungen für Rekursionen und Differenzengleichungen finden.

Rechnen mit EF

Gelte $(a_n) \Leftrightarrow A(z) = \sum_{n\geq 0} a_n z^n$ und $(b_n) \Leftrightarrow B(z)$, dann gilt:

- $(\alpha a_n + \beta b_n) \Leftrightarrow \alpha A(z) + \beta B(z)$
- $(\sum_{k=0}^{n} a_k b_{n-k}) \Leftrightarrow A(z) \cdot B(z)$ (Cauchyprodukt)
  inkl. $b_n = 1 : \left(\sum_{k\geq 0}^{n} a_k\right) \Leftrightarrow \frac{A(z)}{1-z}$
- $(a_n \gamma^n) \Leftrightarrow A(\gamma z)$
- $(a_{n-1}) \Leftrightarrow z \cdot A(z)$
- $(n \cdot a_n) \Leftrightarrow z \cdot A'(z)$

2 Zahlentheorie

Satz (Fundamentalsatz der Zahlentheorie)**.** *Jede natürliche Zahl $a \geq 2$ läßt sich als Produkt von Primzahlen darstellen:*

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_r \qquad \text{mit } p_1, p_2, \ldots, p_r \in \mathbb{P},$$

wobei die Darstellung bis auf die Reihenfolge eindeutig ist.

2.1 Kongruenzen

Zwei Zahlen $a, b \in \mathbb{Z}$ heißen **kongruent modulo** m, falls m ein Teiler von $b - a$ ist:

$$a \equiv b \bmod m \equiv b(m)$$

Unter einer **Restklasse** $\bar{r}$ modulo m versteht man die Menge

$$\begin{aligned}\bar{r} &= r + m \cdot \mathbb{Z} = \{\ldots, r-2m, r-m, r, r+m, r+2m, \ldots\} \\ &= \{a \in \mathbb{Z} \mid a \equiv r \bmod m\}.\end{aligned}$$

Der Name "Restklasse" kommt daher, daß in einer Restklasse genau jene ganzen Zahlen zusammengefaßt werden, die bei der Division durch m denselben Rest r haben. Die Menge alle Restklassen modulo m wird mit $\mathbb{Z}_m$ bezeichnet. $\mathbb{Z}_m$ bildet mit $+$ und $\cdot$ einen sogenannten **Restklassenring** $(\mathbb{Z}_m, +, \cdot)$.

Für Restklassen $\bar{a}, \bar{b} \in \mathbb{Z}_m$ definiert man Summe und Produkt durch

$$\bar{a} + \bar{b} = \overline{a+b} \qquad \text{und} \qquad \bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

Eine multiplikativ **inverse Restklasse** $\bar{b}$ zu $\bar{a}$ muß $\bar{a} \cdot \bar{b} = \bar{1}$ erfüllen. Eine Restklasse $\bar{a} \in \mathbb{Z}_m$ besitzt genau dann eine multiplikativ inverse Restklasse, wenn $\mathrm{ggT}(a, m) = 1$ ist. Oder anders ausgedrückt: Die Menge aller invertierbaren (i.e. primen) Restklassen $\mathbb{Z}^* = \{\bar{a} \in \mathbb{Z}_m \mid \exists \bar{x} \in \mathbb{Z}_m : \bar{a} \cdot \bar{x} = \bar{1}\}$. Das Inverse kann mit Hilfe des Euklidischen Algorithmus gefunden werden.
$(\mathbb{Z}_m, +, \cdot)$ ist ein Körper $\Leftrightarrow m \in \mathbb{P}$ (Komm. Ring & alle Elemente außer 0 sind multiplikativ invers).
$(\mathbb{Z}_m^*, \cdot)$ ist eine Gruppe (assoziativ, neutrales Element, inverse Elemente).

Eulersche φ-Funktion Die Eulersche φ-Funktion $\varphi(m)$ gibt die Anzahl der invertierbaren Restklassen modulo m an (d.h. wieviele positive ganze Zahlen $a \leq m$ zu m teilerfremd sind):

$$\varphi(m) = |\mathbb{Z}_m^\star| = \{a \in \mathbb{Z} \mid 1 \leq a \leq m, \mathrm{ggT}(a, m) = 1\}.$$

Satz (Kleiner Satz von Fermat)**.** *Für teilerfremde ganze Zahlen a, m gilt*

$$a^{\varphi(m)} \equiv 1 \bmod m.$$

Ist $m = p$ eine Primzahl, so vereinfacht sich dies zu $p \nmid a \Longrightarrow a^{p-1} \equiv 1 \bmod p \quad$ bzw. $\quad p \mid (a^{p-1} - 1)$. Dies kann umgekehrt auch zur schnellen Überprüfbarkeit, ob eine Zahl *wahrscheinlich* prim ist, genutzt werden: Bei großen Zahlen ist praktisch nicht daran zu zweifeln, daß p eine Primzahl ist, falls die Gleichung für ein a mit $1 < a < p$ gilt. Details siehe z.B. WP:Fermatscher_Primzahltest.

2.2 RSA

Das RSA-Verfahren beruht auf dem folgenden Satz:

Satz. *Seien p, q zwei verschiedene ungerade Primzahlen, $m = pq$ und $v = \mathrm{kgV}(p-1, q-1)$. Dann gilt $\forall a, m \in \mathbb{Z}$*

$$a^{mv+1} \equiv a(m).$$

Sind also $e, d \in \mathbb{Z}$ zwei Zahlen mit $ed \equiv 1 \bmod v$, so gilt für alle $a \in \mathbb{Z}$

$$(a^e)^d \equiv a(m).$$

Möchte eine Person **A** verschlüsselte Nachrichten empfangen können, so multipliziert **A** zwei Primzahlen p, q miteinander und veröffentlicht das Produkt $n = pq$ und zwei Zahlen e und d (decrypt/encrypt), die zu $v = \mathrm{kgV}(p-1, q-1)$ teilerfremd ist.

Ist nun eine weitere Person **B** daran interessiert, Person **A** eine Nachricht zu senden, die nur **A** lesen kann, so unterteilt er die Nachricht in Bläcke $a_1, a_2, \ldots$, so daß jeder Block durch eine nichtnegative Zahl $< n$ repräsentiert werden kann. Anschließend verschlüsselt er $a_1, a_2, \ldots$ durch

$$b_j = a_j^e(m) \qquad (j \geq 1)$$

und läßt A die Zahlen $b_1, b_2, \ldots$ ohne weitere Geheimhaltung zukommen. **A** kann nun die ursprüngliche Nachricht $a_1, a_2, \ldots$ durch

$$a_j = b_j^d(m) \qquad (j \geq 1)$$

zurückgewinnen, also entschlüsseln.

Öffentlicher Schlüssel (m, e)

Verschlüsselung: $E: \quad a \to a^e \bmod m \qquad a \in \{0, 1, \ldots, m-1\}$

Entschlüsselung: $D: \quad b \to b^d \bmod m \qquad D(E(a)) = a$

$m = p \cdot q, \qquad e \cdot d \equiv 1(v), \qquad v = \text{kgV}(p-1, q-1)$

Auf dem ersten Blick erscheint das RSA-Verfahren nicht sehr sicher zu sein. Da m und e bekannt sind, sollte man doch $d = e^{-1} \bmod v$ berechnen können. Der Grund, warum dies nicht funktioniert, ist die Tatsache, daß $v = \text{kgV}(p-1, q-1)$ nur mit Hilfe der Primfaktorenzerlegung von $m = pq$ errechnet werden kann, und diese wird nicht bekanntgegeben.

2.3 Heiratssatz

Seien D, H endliche, disjunkte Mengen und sei $\forall d \in D : \exists\, \Gamma(d) \subseteq H$, dann

$$\begin{array}{l} \exists f : D \to H \text{ injektiv} \\ \text{mit } f(d) \in \Gamma(d), \quad (\forall d \in D) \end{array} \iff \forall\, U \subseteq D : |\Gamma(U)| \geq |U|$$

$\iff \exists$ maximales Matching im bipartiten Graph $(V = \{D, H\}, E = \{(d, h) | d \in D, h \in \Gamma(d)\})$

D sei eine Menge von Damen und H eine Menge von Herren. Für eine Dame $d \in D$ sei $\Gamma(d)$

Abbildung 1: Heiratssatz

die Menge von Herren, die d bekannt sind. Eine *zulässige Heirat* ist nun eine injektive Funktion $f : D \to H$, die respektiert, daß jede Dame $d \in D$ einen ihr vorher schon bekannten Herren heiratet, d.h. $f(d) \in \Gamma(d)$. Der Heiratssatz besagt nun, daß genau dann eine zulässige Heirat möglich ist, wenn jede Gruppe U von Damen insgesamt wenigstens so viele Herren kennen, wie ihre Anzahl groß ist.

Satz (Satz von Dilworth)**.** *Sei $(P, \leq)$ eine Halbordnung, dann gilt:*

Die maximale Größe einer Antikette ist gleich der minimalen Anzahl an disjunkten Ketten, die eine Zerlegung von P bilden.

Eine Kette ist dabei eine Teilmenge von P, in der alle Elemente paarweise vergleichbar sind: Für $a, b \in P$ gilt entweder $a \leq b$ oder $b \leq a$. Dagegen ist eine Antikette eine Teilmenge von P in der für jeweils 2 Elemente stets gilt, daß sie nicht in Relation stehen: Für $a, b \in P$ gilt $a \not\leq b$ und $b \not\leq a$.

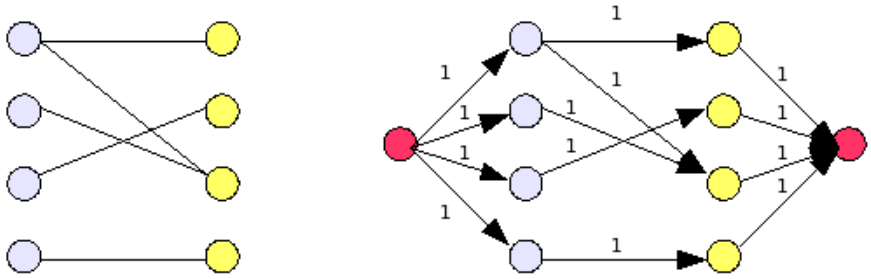

Abbildung 2: Maximum matching — Flow problem.

2.4 Möbius

$(H, \leq)$ lokalendlich, dann ist die Möbiusfunktion:

$$\mu : H \times H \to \mathbb{R} \iff \sum_{z \in [x,y]_H} \mu(z,y) = \begin{cases} 1 & \text{für } x = y \\ 0 & \text{für } x \leq m, x \neq y \end{cases}$$

Möbische Umkehrformel: $(H, \leq)$ nicht notwendigerweise lokalendlich(?), $\forall x \in H : \{z \in H | z \leq x\}$ endlich, dann

$$S_f(x) = \sum_{z \leq y} f(z) \Rightarrow f(x) = \sum_{z \leq y} S_{f(z)} \mu(z,x).$$

3 Graphentheorie

3.1 Planare Graphen

K_n ist ein vollständiger Graph mit n Knoten.
$K_{n,m}$ ist ein paarer Graph, bestehend aus zwei disjunkten Mengen mit je n und m Knoten, wobei jeder Knoten der einen Menge mit allen Knoten der anderen verbunden ist.

Die Anzahl ...
der Knoten $= \alpha_0(G) = |V(G)|$,
der Kanten $= \alpha_1(G) = |E(G)|$,
der Flächen $= \alpha_2(G)$.

Satz (Eulersche Polyederformel)**.** *Für einen zusammenhängenden planaren Graphen G gilt*

$$\alpha_0(G) - \alpha_1(G) + \alpha_2(G) = 2.$$

Satz (Kuratowski)**.** *Ein Graph G ist genau dann nicht planar, wenn er einen Teilgraphen enthält, der aus C_5 oder $K_{3,3}$ durch eventuelle Unterteilung (von Kanten) entsteht.*

Stereographische Projektion

Die stereographische Projektion bildet eine Kugeloberfläche auf eine Ebene ab.

- Es werden ein Projektionspunkt N auf der Kugel (z.B. Nordpol) und eine Projektionsebene A (z.B. die Ebene mit $z = 0$, deren Schnitt mit der Kugel den Äquator bildet) gewählt.
- Ausgehend von N kann man durch jeden Punkt P auf der Kugel eine Gerade legen, die A an Stelle P' schneidet. Auf diesen Schnittpunkt P' wird P abgebildet.

\+ Winkel–, Kreistreue
− Entfernungen und Flächen nicht verhältnismäßig.

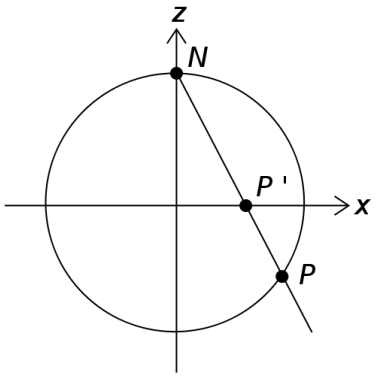

Abbildung 3: Stereographische Projektion

3.2 Färbungen — Ramsey

Sei $G = (V, E)$ ein schlichter, ungerichteter Graph. Eine **Färbung** ist eine Abbildung

$$c : V \to C, \quad (C = \text{Menge von Farben}).$$

Eine Färbung $c : V \to C$ heißt **zulässig**, wenn für alle Kanten $e = (x, y) \in E$

$$c(x) \neq c(y)$$

gilt, d.h. benachbarte Knoten verschieden gefärbt sind. Die **chromatische Zahl** $\chi(G)$ eines Graphen G ist die minimale Anzahl von Farben, für die es eine zulässige Knotenfärbung gibt.

$$\begin{aligned} \chi(G) = 2 &\iff G \text{ paarer } (= \text{bipartiter}) \text{ Graph} \wedge E(G) \neq \emptyset \\ &\iff \text{Alle Kreise haben gerade Länge} \wedge E(G) \neq \emptyset \end{aligned}$$

Ramseytheorie

Die Ramseytheorie behandelt die Frage, wie viele Elemente aus einer mit einer gewissen Struktur versehenen Menge ausgewählt werden müssen, damit diese Struktur in der Teilmenge wieder gefunden werden kann und eine bestimmte Eigenschaft erfüllt ist.

Die **Ramseyzahl** $R(r, s)$ = minimale n, so daß in jeder 2-Färbung des K_n entweder
ein einfärbiger K_r der einen Farbe oder
ein einfärbiger K_s der anderen Farbe auftritt.

- $R(r, s) < \infty$ Satz von Ramsey
- $R(r, s) \leq R(r, s-1) + R(r-1, s)$
- $(\Rightarrow)\ R(r, s) \leq \binom{r+s-2}{r-1} \leq 2^{r+s-2}$ $\left(\text{da } \binom{n}{k} \leq 2^n\right)$

Verallgemeinerung auf mehr als 2 Farben: Die $R(s_1, s_2, \ldots s_k)$ = minimale n, so daß in jeder k-Färbung des K_n entweder
ein einfärbiger K_{s_1} der Farbe 1 oder
ein einfärbiger K_{s_2} der Farbe 2 oder
$\vdots$
ein einfärbiger K_{s_k} der Farbe k auftritt.

3.3 Flußprobleme

Vorraussetzungen für gültigen Fluß

$$\varphi : E \to \mathbb{R} \ :\Longleftrightarrow 0 \leq \varphi(e) \leq w(e), \qquad (e \in E) \qquad \textit{Fluss auf jeder Kante} \ \leq \ \textit{Kapazität}$$
$$\wedge \sum_{y \in \Gamma^+(x)} \varphi(x,y) = \sum_{y \in \Gamma^-(z)} \varphi(z,y) \qquad (\forall x \in V \setminus s,t) \qquad \textit{Zufluss} = \textit{Abfluss}$$

Satz (Ford Fulkerson — max-flow min-cut)**.**

$$\max v(\phi) = \min \varsigma(S)$$
$$v(\phi) = \sum_{y \in \Gamma_s^+} \varphi(s,y) = \sum_{z \in \Gamma_t^-} \varphi(z,t) \qquad S = (V_1, V_2), \qquad s \in V_1, t \in V_2$$

Ford Fulkerson Algorithmus

$i \leftarrow 0$;
$f_i \leftarrow$ null flow;

while $\exists$ augmenting path P from s to t in G_{f_i} do
    $x \leftarrow$ minimum residual capacity along P;
    augment flow of value x along P;
    $f_{i+1} \leftarrow f_i + x$;
    $i \leftarrow i + 1$;
return f_i;

Quellen

- Eigene Aufzeichnungen der Vorlesung "Diskrete Mathematik für Informatiker" von Prof. Drmota WS 2008.
- Skriptum fuer Hoehere Mathematik f. Inf, Kirner und Drmota, 2006.
- Skriptum fuer Diskrete Methoden. Drmota(?), 2002(?).
- "Mathematik für Informatiker", Drmota et al., 2007.
- Vortragsfolien zur VO "Algorithmen auf Graphen" WS 2007.
- {en,de}.wikipedia.org
- Vorlesungswiki der FSInf.

Zuletzt generiert am 17. Februar 2010.