Diskrete Strukturen
SS 2005
Prof. Dr. Eberhard Triesch

Marvin Goblet

13.04.05 - 22.07.05
final 1.5

Inhaltsverzeichnis

0.1 Vorwort

0.1.1 Entstehung des Dokumentes

Dies ist eine Mitschrift der Vorlesung "Diskrete Strukturen" von Prof. Dr. Eberhard Triesch aus dem Sommersemester 2005. Sie dient in erster Linie mir zur persönlichen Lernhilfe. Das Publizieren geschied auf freiwilliger Basis.
Dies ist mein erstes LaTeX Projekt. Fehler im Inhalt können nicht ausgeschlossen werden, daher gebe ich keine Garantie auf Korrektheit.
Falls Fehler erkannt werden oder Anmerkungen zum Layout bestehen, bitte ich um eine konstruktive eMail an : Marvin.Goblet@rwth-aachen.de
Auf Anfrage bin ich auch bereit den source file auszugeben.

0.1.2 Wichtige Informationen

- Für Schäden o.ä. die durch dieses Dokument hervorgerufen werden, übernimmt der Autor keine Haftung.
- Für die Korrektheit des Inhaltes übernimmt der Autor keine Haftung.
- Bei Entdeckung von Fehlern bitte Benachrichtigung an meine eMail-Adresse :

  Marvin.Goblet@rwth-aachen.de
- Dieses Dokument darf **für private Zwecke frei kopiert** werden, nicht aber für kommerzielle Zwecke.

Einen großen Dank an alle Korrekturleser

0.2 Konventionen

13.04.05

$\binom{A}{k} := \{X \subseteq A |\ |X| = k\}$

$2^A = \mathcal{P}(A) := \{X | X \subseteq A\}$
$|2^A| = 2^{|A|}$

Relation und Funktion

A, B Menge $A \times B := \{(a, b) | a \in A, b \in B\}$
Relation: $R \subseteq A \times B$
Funktion: $f : A \to B$
f heist *injektiv* , falls gilt:

$$a, a' \in A\ , a \neq a' \Rightarrow f(a) \neq f(a')$$

surjektiv: für alle $b \in B$ ex ein $a \in A$ mit $b = f(a)$
bijektiv: *injektiv* und *surjektiv*

Beweistechniken

- indirekte Beweise
- Beweise durch vollständige Induktion

Kapitel 1

Abzählprobleme

Typisches Problem:
Geg. sei eine (eventuell unendliche) Familie von Mengen $(S_i | i \in I)$ jedes S_i sei endlich. Bestimme die Funktion.

$$f : I \to \mathbb{N}_0$$
$$f(i) := |f_i|$$

Was heißt "bestimmen" ?
Am liebsten "geschlossene Formen"
z.B. $|A| = n = |2^A| = 2^n$
Manchmal : Summation $\underbrace{1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}}_{H_n \text{ n - te harmonische Zahl}}$

$\sum_{i=1}^{n} \frac{1}{i} \backsim \underbrace{\ln\ n}_{\text{nat. Logarithmus}}$
asymptotisch gleich d.h.
$\frac{1}{\ln\ n} \cdot \sum_{i=1}^{n} \frac{1}{i} \to\ 1\ (n \to \infty)$

Sehr wichtig : Rekursion

1.1 Elementare Zählprinzipien

Gleichheitsregel : $|S| = |T|$ g.d.w. eine Bijektion zwischen S und T ex.

Summenregel : $S = \dot{\bigcup_{i=1}}^{t}$ disjunkte Vereinigung d.h.
$S_i \cap S_j = \emptyset \quad |1 \leq i < j \leq t|$
$\Rightarrow |S| = \sum_{i=1}^{t} |S_i|$

Produktregel : $S = S_1 \times S_2 \times \ldots \times S_t = \{(x_1, x_2, \ldots, x_t)\ | x_i \in S_i, 1 \leq i \leq t\}$
$\Rightarrow |S| = \prod_{i=1}^{t} |S_i|$

Beispiel:

$\binom{n}{k} = |\binom{S}{k}| = |\{X \subseteq S \mid |X| = k\}|$

$|S| = n$ $\qquad$ $0 \leq k \leq n$

$\binom{n}{k}$ heißt Binomialkoeffizient

Es sei $x \in S$ (fest gewählt)

$M := \{X \in \binom{S}{k} \mid x \in X\}$

$N := \{X \in \binom{S}{k} \mid x \notin X\}$

$\binom{S}{k} = M \dot{\bigcup} N$ $\qquad$ $\binom{n}{0} = 1$

$\binom{S}{0} = \{\emptyset\}$

$\binom{n}{k} = |M| + |N|$

$f : M \to \binom{S\backslash\{x\}}{k-1}$ $\qquad$ Bijektion

$f(x) = X\backslash\{x\}$

d.h. $|M| = \binom{n-1}{n-1}$

$N = \binom{S\backslash\{x\}}{k}$ $\qquad$ $|N| = \binom{n-1}{k}$

$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

Beispiel: $R^N := \{f : N \to R \mid f \text{ Funktion}\}$

$|N| = n, \quad |R| = r$

$N = \{x_1, \ldots x_n\}$

$f \in R^N$ Ordnen wir der n - Tupel $(f(x_1), f(x_2), \ldots, f(x_n))$ zu.

Bijektion zwischen $R^{\mathbb{N}}$ und $\underbrace{R \times R \times \ldots \times R}_{n-mal}$

$|R^N| = r \cdot r \cdot \ \ldots \ \cdot r = r^n = |R|^{|N|}$

Folgerung : $|2^N| = 2^{|N|}$

$|2^N| = |\{0,1\}^N|$

$X \subseteq N \to 1_X$

$1_X := \begin{cases} 1, & x \in X \\ 0, & \text{sonst} \end{cases}$

15.04.05

$f : A \to B \quad , \quad g : B \to C$

$g \circ f : A \to C \quad , \quad (g \circ f)(a) = g(f(a))$

„g nach f“

Ist f bijektiv, so ex. ein $g : B \to A$ mit $g \circ f = id_A$ und $f \circ g = id_B$

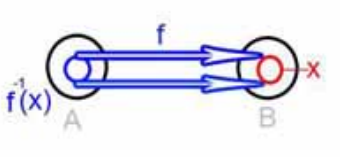
$id_A(a) = a$ für alle $a \in A$

Schreibweise : $g = f^{-1}$

Beachte: f^{-1} wird auch für die folgende Abbildung von 2^B nach 2^A verwendet.

$(f : A \to B)$

$f^{-1}(X) := \{a \in A| \quad f(a) \in X\}$ $(X \subseteq B)$



Eine bijektive Abbildung von A in sich heißt Permutation.

$S_A := \{f : A \to A \mid f$ Permutation$\}$

Bemerkung:

(i) S_A heißt symmetrische Gruppe auf A

(ii) Permutationen werden oft durch eine Reihenfolge der Elemente von A dargestellt

d.h. $A = \{a_1, \ldots, a_n\}$

f wird beschrieben durch $f(a_1), \ldots, f(a_n)$

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ f(a_1) & f(a_2) & & f(a_n) \end{pmatrix}$$

(iii) Für $A = \{1, \ldots, n\}$ schreiben wir einfach

S_n (statt $S_{\{1,\ldots,n\}}$)

Produktregel : $S = S_1 \times S_2 \times \ldots \times S_r$

$\Rightarrow |S| = \prod_{i=1}^{t} |S_i| = |S_i| \cdot |S_2| \cdot \ \ldots \ \cdot |S_t|$

Bemerkung: Wie viele Permutationen enthält S_n ?

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}$$

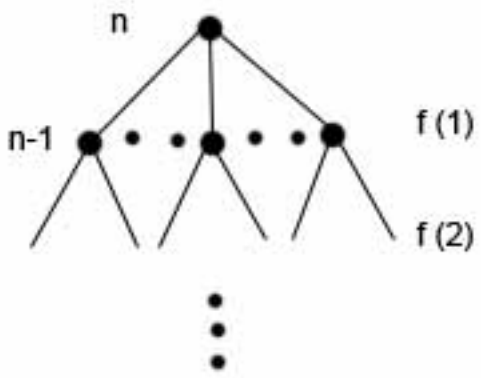
n Wahlmöglichkeiten für $f(1)$

Wenn $f(1)$ gewählt ist:

$n-1$ weitere Wahlmöglichkeiten für $f(2)$

$\vdots$

$n-k+1$ Wahlmöglichkeiten für $f(k)$



$n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 = n!$

Es gibt also $n!$ Permutationen in S_n

Beispiel: $|K| = k, \qquad |N| = n \qquad k \leq n$

Frage : Wie viele injektive Abbildungen von K nach N gibt es ?

$O.B.d.A. \quad K = \{1, \ldots, k\}$

$$\begin{pmatrix} 1 & 2 & \ldots & k \\ f(1) & f(2) & \ldots & f(k) \end{pmatrix} \; f(1), \ldots, f(k) \text{ jeweils Element von } N.$$

Wie oben : Anzahl der Abbildungen

$n \cdot (n-1) \cdot \ \ldots \ \cdot (n-(k-1)) = n \cdot (n-1) \cdot \ \ldots \ \cdot (n-k+1) =: n^{\underline{k}}$

$n^{\overline{k}} := n \cdot (n+1) \cdot (n+2) \cdot \ \ldots \ \cdot (n+k-1)$

1.2 Regel vom zweifachen Abzählen

Es sei $M = (m_{ij})_{1 \leq i \leq n \ , \ 1 \leq j \leq k}$ eine Matrix. Dann ist die Summe aller Matrixelemente die Summe der Spaltensummen.

$$\sum_{i=1}^{n} \underbrace{(\sum_{j=1}^{k} m_{ij})}_{\text{i-te Zeilensumme}} = \sum_{j=1}^{k} \underbrace{(\sum_{i=1}^{n} m_{ij})}_{\text{j-te Spaltensumme}}$$

Beispiel: Es sei $t : \mathbb{N} \to \mathbb{N}$,

$t(j)$ ist Anzahl der Teiler von j.

$t(1) = 1, \quad t(p) = 2 \qquad$ für alle Primzahlen p

$$t(2^n) = n+1, \quad j = \begin{matrix} \alpha_1 & \alpha_2 & \ldots & \alpha_r \\ p_1 & p_2 & \ldots & p_r \end{matrix}$$

$p_1, \ldots, p_r$ verschiedene Primzahlen.

$t(j) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ \ldots \ \cdot (\alpha_r + 1)$

Es sei $t(n) := \frac{1}{n} \sum_{j=1}^{n} t(j)$

$M = (m_{ij})_{1 \le i,j \le n}$

$$m_{i,j} := \begin{cases} 1, & \text{falls } i \mid j; \\ 0, & \text{sonst} \end{cases} \qquad (i \text{ „}teilt\text{“} j)$$

$$\Rightarrow t(i) = \sum_{i=i|j} 1 = \sum_{i=1}^{n} m_{ij},$$

$t(j)$ j-te Spaltensumme von M

$$\sum_{j=1}^{n} t(j) = \sum_{j=1}^{n} (\sum_{i=1}^{n} m_{ij}) = \sum_{i=1}^{n} (\sum_{j=1}^{n} m_{ij}) = \sum_{i=1}^{n} (|\{j| \ \ i \mid j\}|) = \sum_{i=1}^{n} \lfloor \tfrac{n}{i} \rfloor$$

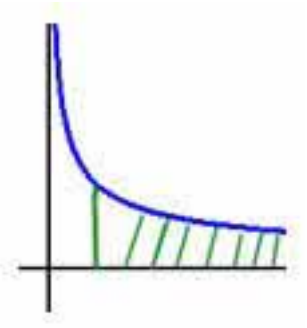
$$\Rightarrow \bar{t}(n) = \frac{1}{n} \sum_{i=1}^{n} \lfloor \tfrac{n}{i} \rfloor \le \frac{1}{n} \sum_{i=1}^{n} \tfrac{n}{i} = \sum_{i=1}^{n} \tfrac{1}{n} = H_n$$

$$\bar{t}(n) \ge \frac{1}{n} \sum_{i=1}^{n} (\tfrac{n}{i} - 1) = H_n - 1$$

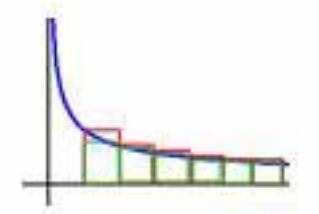
$$H_n - 1 \le \bar{t}(n) \le H_n$$

$$\bar{t}(n) \sim \ln \ n$$

$$\ln \ x = \int_1^x \tfrac{1}{t} \, dt$$



ist $\ln \ x$



$$1 + \tfrac{1}{2} + \tfrac{1}{3} + \ldots + \tfrac{1}{n-1} = H_{n-1} \ge \ln \ n$$

$$\ln \ n \ge \tfrac{1}{2} + \tfrac{1}{3} + \ldots + \tfrac{1}{n} = H_n - 1$$

$$H_n - 1 < \ln \ n < H_{n-1}$$

Beispiel: Wir betrachten $n \times n$- Matrizen

$M = (m_{ij})_{1 \le i,j \le n}$

mit folgenden Eigenschaften:

(i) $m_{ij} \in \mathbb{N}$

(ii) Falls $m_{ij} = n$, so ex. genau ein Paar $(k, l) \ne (i, j)$ mit $m_{ij} = m_{kl} = m$

Wegen (ii) muss n^2 und also auch n gerade sein.

Sei n gerade

Frage: Ex. immer eine „Transversale ohne doppelte Elemente “ (zulässige Transversale) d.h. eine Permutation $\pi \in S_n$ mit :

$|\{m_{i,\pi(i)}|\ 1 \le i \le n\}| = n$?

	$\pi(1)$ ↓	↙ $m_{1,\pi(1)}$
1	O	
2	O	
3		
⋮		
n		O

z.b. $n = 2$ $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ Nein!

$n \ge 4$ Ja!

Beweis: M sei gegeben.

Ein Paar $\{(i,j),(k,l)\}$ mit $i \ne k, j \ne l$ und $m_{ij} = m_{kl}$ heißt singuläres Paar

π zulässig g.d.w. π kein singuläres Paar enthält.

$T := \ Menge\ aller\ singulären\ Paare$

$0 \le |T| \le \frac{n^2}{2}$

$N = (n_{\pi,t})_{\pi \in S_n,\ t \in T}$

$$n_{\pi,t} := \begin{cases} 1, & \text{falls } \pi \text{ das sing. Paar } t \text{ enthällt} \\ 0, & \text{sonst} \end{cases}$$

$$\underbrace{\sum_{\pi} (\sum_{t} n_{\pi,t})}_{n!\text{ Summanden}} = \sum_{t} \underbrace{(\sum_{\pi} n_{\pi,t})}_{(n-2)!} = |T| \cdot (n-2)!$$

Es ex. mind. ein „Summand“π_0 mit

$\sum_t n_{\pi_0,t} \le \lfloor \frac{1}{n!} \cdot |T| \cdot (n-2) \rfloor = \lfloor \frac{|T|}{n \cdot (n-1)} \rfloor$

Aber $|T| \le \frac{n^2}{2}$

$\Rightarrow \frac{|T|}{n \cdot (n-1)} \le \frac{n^2}{2n \cdot (n-1)} = \frac{n}{2(n-1)} \overset{n \ge 4}{\underset{\downarrow}{<}} 1$

$\Rightarrow \sum_t n_{\pi_0,t} = 0$, also π_0 zulässig

20.04.05

1.3 Schubfachprinzip

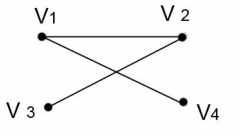
Verteilt man n Elemente aus r Fächer, so ex. im Falle $n > r$ stets ein Fach, das mehr als ein Element enthält.

Verallgemeinerung:
Es gibt stets ein Fach, das mindestens $\lceil \frac{n}{r} \rceil$ Elemente enthält.

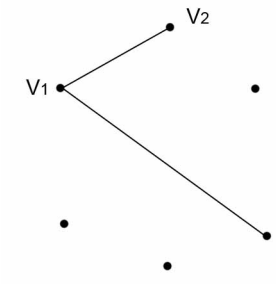
Beispiel:
Unter n^2+1 verschiedenen reellen Zahlen gibt es $n+1$, die eine monotone Folge bilden (steigend oder fallend).

Beweis:
$a_1, a_2, a_3, \ldots, a_{n^2-1}, a_{n^2}, a_{n^2+1}$ seien die Zahlen.
Jedem a_i ordnen wir die Länge t_i der längsten Folge $a_i = a_{j_1} < a_{j_2} < \ldots < a_{j_{t_i}}$ zu, die mit a_i beginnt $(j_1 < j_2 < \ldots < j_{t_i})$.
Falls für ein i $t_i \geq n+1$ ist, so sind wir fertig. Falls nicht, so ist jedes t_i in $\{1, \ldots, n\}$.
Schubfachprinzip:
Es gibt ein $t \in \{1, \ldots, n\}$ mit $t_i = t$ für mindestens $\lceil \frac{n^2+1}{n} \rceil = \lceil n + \frac{1}{n} \rceil = n+1$ Indizes i , etwa für $i_1 < 1_2 < \ldots < i_{n+1}$.
Nun zeigen wir : $a_{i_1} > a_{i_2} > \ldots > a_{i_{n+1}}$
Angenommen , $a_{i_1} < a_{i_2}$. Dann könnte man eine t-elementige monoton steigende Folge, die bei a_{1_2} beginnt, zu einer $(t+1)$-elementigen verlängern, die bei a_{i_1} beginnt, also $t_{i_1} \geq t+1$ im Widerspruch zu $t_{i_1} = t$
Völlig analog : $a_{i_l} > a_{i_{l+1}}$ für alle $1 \leq l \leq n$

Beispiel:
Angenommen, 6 Leute treffen sich. Dann gibt es unter ihnen 3, sodas jeder jeden kennt oder 3, sodas keiner einen der anderen kennt.
Bemerkung:
Veranschaulichung durch Graphen.
Graph G: $G = (V, E)$, V endliche Menge $E \subseteq \binom{V}{2}$. Die Elemente von V heißen Punkte, die Elemente von E Kanten.

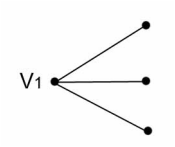


$E = \{\{V_1, V_2\}, \{V_2, V_3\}, \{V_1, V_4\}\}$
$E = \binom{V}{2}$: vollständiger Graph.



Punkte: Personen

Betrachte irgendeinen Punkt, etwa V_1 von den restlichen Punkten. Es gibt drei Leute, die V_1 kennt oder drei Leute, die er nicht kennt.
Angenommen, V_1 kennt drei Leute:

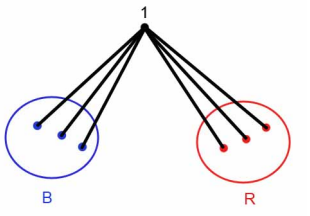


Falls unter diesen dreien zwei einander kennen, so bilden diese, zusammen mit V_1, eine Dreiergruppe, in der jeder jeden kennt.
Anderenfalls kennen die Bekannten von V_1 einander nicht.

Verallgemeinerung:
Satz von Ramsey
Es sein $k, l \in \mathbb{N}$, $k, l \geq 2$
Dann ex. eine $(\min)$ Zahl $R(k,l)$ mit folgenden Eigenschaften:
Färbt man die Kanten eines vollständigen Graphen mit n Punkten, $n \geq R(k,l)$, rot oder blau, so gibt es entweder k Punkte, zwischen denen alle Kanten blau sind oder l Punkte zwischen denen alle Kanten rot sind.
(Im Beispiel gezeigt: $R(3,3) \leq 6$)
Es gilt: $R(k,2) = k$, $R(2,l) = l$
Wir zeigen:

$$R(k,l) \leq R(k-1,l) + R(k,l-1)$$

Dann folgt die Existenz von $R(k,l)$ durch vollst. Induktion nach $k+l$.
Es sei nun $V = \{1, \ldots, n\}$ mit $n = R(k-1,l) + R(k,l-1)$
Die Kanten des vollständigen Graphen auf V seien irgendwie blau und rot gefärbt. Wir zerlegen V folgedenermaßen:



$V = \{1\} \dot{\bigcup} B \dot{\bigcup} R$;
$B = \{j \in V : \{1,j\}$ ist blau$\}$
$R = \{j \in V : \{1,j\}$ ist rot$\}$

Wegen $1 + |B| + |R| = R(k-1,l) + R(k,l-1)$ ist $|B| \geq R(k-1,l)$ oder $|R| \geq R(k,l-1)$.

Falls $|B| \geq R(k-1,l)$, so ex. in B entweder $k-1$ Punkte, die nur über blaue Kanten verbunden sind oder l Punkte, die nur über rote Kanten verbunden sind. Im ersten Fall ergänzen wir die $k-1$ Punkte durch den Punkt 1, im zweiten Fall sind wir fertig.
Falls $|R| \geq R(k,l-1)$ ist, schließen wir analog.

1.4 Die fundamentalen Zählkoeffizienten

z.b. $\binom{n}{k} = |\binom{\{1,\ldots,n\}}{k}|$

„Binomialkoeffizient“

Tauchen im binomischen Lehrsatz auf:

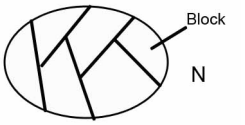
$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^k$$

bzw

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^k \cdot y^{n-k}$$

$x^n \cdot y^{n-k}$ entsteht, wenn aus k Klammern x gewählt wird und aus $n-k$ Klammern y.
Diese Klammern können auf $\binom{n}{k}$ weisen aus den k Klammern ausgewählt werden.

$S_{n,k}$: Anzahl der Mengenpartitionen von $\{1,\ldots,n\}$ in k nicht leere Blöcke



Die $S_{n,k}$ heißen Stirling-Zahlen 2.Art .

$P_{n,k}$ **:** Anzahl der Zahlpartitionen in k Summanden.

$n = n_1 + n_2 + \ldots + n_k \qquad O.B.d.A.\ n_1 \geq n_2 \geq \ldots \geq n_k$

($P_{n,k}$ zählt „ungeordnete“ Partitionen ab, die Reihenfolge der Summanden spielt keine Rolle, analog $S_{n,k}$)

$p(n) = \sum_{k=1}^{n} P_{n,k}$ Darstellung durch

Ferrers-Graphen:

$$\begin{array}{cccc} x & x & x & x \\ x & x & x & x \\ x & x & x & \\ x & x & & \end{array}$$

k-Permutationen von $N = \{1, \ldots, n\}$:

$| \{(a_1, a_2, \ldots, a_n) \ , a_1 \in N, \ldots, a_k \in N \quad \text{alle } a_i \ \text{ verschieden}\} |$

$= n \cdot (n-1) \cdot \ \ldots \ \cdot (n-k+1) = n^{\underline{k}}$

Anderer Weg: Wähle zuerst k Elemente aus N aus. Dann ordnen wir diese auf alle möglichen Weisen zu k-Tupeln (k-Permutationen) an.

Auswahl von $\{a_1, \ldots, a_k\}$: $\binom{n}{k}$ Möglichkeiten

Anordnung auf $k!$ Weisen:

$\binom{n}{k} \cdot k! = n^{\underline{k}}$

$\Rightarrow \binom{n}{k} = \frac{n^{\underline{k}}}{k!} = \frac{n \cdot (n-1) \cdot \ \ldots \ \cdot (n-k+1)}{k!}$

Bemerkung: Die Anzahl der geordneten k-Mengenpartitionen von $\mathbb{N}$ ist $S_{n,n} \cdot k!$

Was ist die Anzahl der geordneten k-Zahlpartitionen ? $\quad Nicht(!) P_{n,n} \cdot k!$

$n = n_1 + \ldots + n_k$ könnte mehrere gleiche Summanden enthalten.

Es gilt aber : Die Anzahl der geordneten k-Partitionen von n ist $\binom{n-1}{k-1}$.

Zum Beweis Konstruieren wir eine Bijektion nach $\binom{\{1,\ldots,n-1\}}{k-1}$

$$f : (n_1, \ldots, n_k) \longmapsto \underbrace{\{n_1, n_1 + n_2, \ldots, n_1 + n_1 + \ldots + n_{k-1}\}}_{\text{lauter verschiedene Zahlen}}$$

Die inverse Funktion $g = f^{-1}$ ist gegeben durch:

$$g(\{a_1 < a_2 < \ldots < a_{k-1}\}) = (a_1, a_2 - a_1, \ldots, a_{k-1} - a_{k-2}, n - a_{k-1})$$

12.04.05

$S_{n,k}$ **:** Stirling-Zahlen 2.Art

Anzahl der Partitionen einer n-Menge in k nicht leere Klassen

$P_{n,k}$ **:** Anzahl d-Zahlpartitionen von n in k-Summanden

$n = n_1 + n_2 + \ldots + n_k \qquad n, n_i \in \mathbb{N} = \{1, 2, 3, \ldots\}$

Geordnete Zahlpartitionen : $\binom{n-1}{k-1}$

$n_1, n_1 + n_2, \ldots, n_1 + \ldots + n_{k-1}$

$\{a_1 < a_2 < \ldots < a_{k-1}\}$

$$a_1 = n_1, \underbrace{a_2 - a_1}_{n_2}, \underbrace{a_3 - a_2}_{n_3}, \ldots, \underbrace{a_{k-1} - a_{k-2}}_{n_{k-1}}, \underbrace{n - a_{k-1}}_{n_k}$$

1.5 Multimengen

Intuitiv: Eine Menge, in der jedes Element mit einer gewissen Vielfachheit gezählt wird.

$\{a, b, b\} = \{a, b\}$ bei Mengen

$\{a, b, b\} \neq \{a, b\}$ bei Multimengen

Formal: Multimenge ist ein Paar (A, f) wobei $f : A \to \mathbb{N}$

$f(a)$: Vielfachheit von $a \in A$

Anzahl der Elemente der Multimenge:

$\sum_{a \in A} f(a)$

Frage: Wie viele k- elementigen Multimengen gibt es in einer n-elementigen Menge

$N = \{1, 2, \ldots, n\}$?

Angenommen, $\{a_1, a_2, \ldots, a_k\}$ ist eine k-Multimenge in N.

$O.B.d.A.$ $1 \leq a_1 \leq a_2 \leq \ldots \leq a_k \leq n$

Behauptung: Gesuchte Anzahl ist $\binom{n+k-1}{k} = \frac{n^{\overline{k}}}{k!} = \frac{n \cdot (n+1) \cdot \ \ldots \ \cdot (n+k-1)}{k!}$

Beweis:

Bijektion auf $\binom{\{1,\ldots,n+k-1\}}{k}$

$f : \{a_1 \leq a_2 \leq \ldots \leq a_k\} \longmapsto \{a_1, a_2 + 1, a_3 + 2; \ldots, a_n + k - 1\}$

$g = f^{-1}$: $g(\{b_1 < b_2 < \ldots < b_k\}) = \{b_1 \underset{\leq}{,} b_2 - 1 \underset{\leq}{,} b_3 - 2 \underset{\leq}{,} \ldots \underset{\leq}{,} b_k - (k-1)\}$

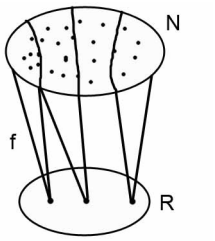
Beispiele : R, N seien Mengen, $|R| = r, \ |N| = n$

(i) $|R^N| = r^n$

(ii) $Injekt.\ (N, R)$ sei die Anzahl der injektiven Abbildungen von N nach R

$|Injekt.\ (N, R)| = r \cdot (r-1) \cdot \ \ldots \ \cdot (r-n+1) = r^{\underline{n}}$

(iii) $Surjekt.\ (N, R)$ sei die Anzahl der surjektiven Abbildungen. Entsprechend den geordneten r-Partitionen von N:



Zerlegung von N in $|R|$ nicht leere Klassen

$|Surj\ (N, R)| = r!\ S_{n,r}$

Jede Abbildung von N nach R ist surjektiv auf eine eindeutige bestimmte Teilmenge $A \subseteq R$

$A = \{f(x) : \ x \in N\}$

Summenregel:

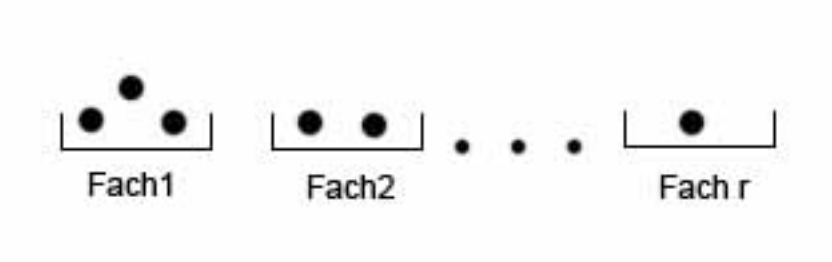
$$r^n = \sum_{\substack{A \subseteq R \\ |A|=k}} \underbrace{|Surj(N,A)|}_{k!S_{n,k}}$$

Beispiel: N sei eine Menge von Bällen

R: Menge von Fächern

Wie viele Möglichkeiten gibt es, die Bälle auf die Fächer zu verteilen?

Nehme an, die Bälle sind unterscheidbar, die Fächer unterscheidbar.



Lösung durch Multimengen : $\frac{r^{\overline{n}}}{n!}$

zusätzliche Forderung: geordnete r-Partitionen von $\binom{n-1}{r-1}$

1.6 Permutationen

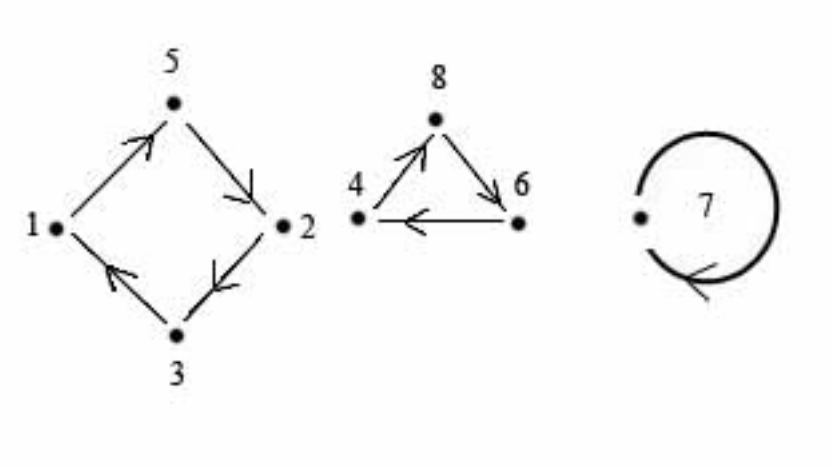
Permutationen $\pi \in S_n = S_{\{1,\ldots,n\}}$ können auf verschiedene Weisen dargestellt werden.

z.B.

$\begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}$. Wenn die Reihenfolge $1, 2, \ldots, n$ festliegt, genügt es π durch das Wort $\pi(1), \pi(2), \ldots, \pi(n)$ zu beschreiben.

Aus der Algebra: Zyklendarstellung von π

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 1 & 8 & 2 & 4 & 7 & 6 \end{pmatrix}$$



$\pi = (1\ 5\ 2\ 3)\ (4\ 8\ 6)\ (7)$

Anzahl der Elemente im Zyklus heißt seine Länge

- Zyklen der Länge 1 heißen Fixpunkte.
- Auf die Reihenfolge der disjunkten Zyklen kommt es nicht an.
- Innerhalb eines Zyklus darf man die Elemente „zyklisch“ vertauschen:
  $(1\ 5\ 2\ 3) = (5\ 2\ 3\ 1) = (2\ 3\ 1\ 5) = (3\ 1\ 5\ 2)$
  $s_{n,k} :=\mid \{\pi \in S_n :\ \pi \text{ hat genau } k \text{ Zyklen}\} \mid$
  Die $s_{n,k}$ heißen Stirling-Zahlen 1.Art
- $s_{n,1} = (n-1)!$
- $s_{n,n-1} = \binom{n}{2}$
- $\sum_{k=1}^{n} s_{n,k} = n! \qquad (n \geq 1)$

Es bezeichne $b_i(\pi)$ die Anzahl der Zyklen der Länge i von π $(i = 1, \ldots, n)$
$b(\pi) := \sum_{i=1}^{n} i \cdot b_i(\pi)$

Der Zykeltyp der Permutation π ist der formale Ausdruck $t(\pi) = 1^{b_1(\pi)}\ 2^{b_2(\pi)}\ \ldots\ n^{b_n(\pi)}$
z.B.: $\pi = (1\ 5\ 2\ 3)\ (4\ 8\ 6)\ (7)$
$t(\pi) = 1^1\ 2^0\ 3^1\ 4^1\ 5^0\ 6^0\ 7^0\ 8^0\ = 1^1\ 3^1\ 4^1$

Es gibt genau soviele Typen von Partitionen wie es Partitionen von n gibt.
$(b_1(\pi), \ldots, b_n(\pi)) \longmapsto \underbrace{1+\ldots+1}_{b_1(\pi)} + \underbrace{2+\ldots+2}_{b_2(\pi)} + \ldots + \underbrace{i+\ldots+i}_{b_i(\pi)} + \ldots$
Die Permutationen vom gegebenen Typ bilden in S_n eine sogenannte Konjugiertenklasse.
$\{\rho \circ \pi \circ \rho^{-1} \mid \rho \in S_n\} = \{\sigma \in S_n \mid t(\pi) = t(\sigma)\}$
$\pi = \ldots(\ldots ij \ldots)\ldots$
$\rho \circ \pi \circ \rho^{-1} = \rho \ldots (\ldots ij \ldots) \ldots \rho^{-1}$
$k = \rho(i) \qquad \rho^{-1}(k) = i$
$l = \rho(j) \qquad \rho^{-1}(l) = j$
$\rho \circ \pi \circ \rho^{-1}(k) = l$
$\ldots(\ldots k\ l \ldots)\ldots$
$\ldots(\ldots \rho(i)\ \rho(j) \ldots)\ldots$

29.04.05
$\rho \circ \pi \circ \rho^{-1}$
$b_i(\pi)$: Anzahl der i-Zyklen von π
$t(\pi) = 1^{b_1(\pi)}\ 2^{b_2(\pi)}\ \ldots\ n^{b_n(\pi)}$
Wie viele Permutationen mit gegebenen Zykeltyp gibt es?
Schreiben wir die Klammern für die verschiedenen Zyklen hin:
$\underbrace{(\bullet)\ldots(\bullet)}_{b_1} \quad \underbrace{(\bullet\bullet)\ldots(\bullet\bullet)}_{b_2} \ldots \underbrace{(\bullet\bullet\bullet\ldots\bullet)\ldots(\bullet\bullet\bullet\ldots\bullet)}_{b_i}$

$$\frac{n!}{b_1!\cdot\ \ldots\ \cdot b_n!\cdot 1^{b_1}\cdot\ \ldots\ \cdot n^{b_n}}$$

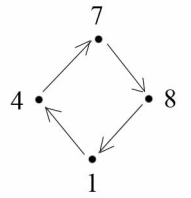
Füllen die Klammern auf $n!$ Weisen mit den Symbolen $1,\ldots,n$ aus, sodas Permutationen von Typ $1^{b_1}\ 2^{b_2}\ldots n^{b_n}$ entstehen.

Wie oft entsteht dabei die gleiche Permutation?

Reihenfolge disjunkter Zyklen ist uninteressant:

$b_1!\ b_2!\ldots b_n!$ verschiedene Reihenfolgen.

$(4\ 7\ 8\ 1) = (7\ 8\ 1\ 4)$



Ein Zyklus der Länge i kann auf i verschiedene Weisen aufgeschrieben werden.

$(4\ 3)\quad (1\ 8)\quad (6\ 5)$

$(3\ 4)\quad (8\ 1)\quad (5\ 6)$

2

$b_2\quad :\quad 2^{b_2}$

$b_i\quad :\quad i^{b_1}$

$1^{b_1}\cdot 2^{b_2}\cdot\ \ldots\ \cdot n^{b_n}$ Weisen, die Zyklen zu schreiben.

Insgesammt : $b_1!\cdot b_2!\cdot\ \ldots\ \cdot b_n!\cdot 1^{b_1}\cdot 2^{b_2}\cdot\ \ldots\ \cdot n^{b_n}$

$\Rightarrow n! = (gesuchte\ Anzahl)\cdot b_1!\cdot b_2!\cdot\ \ldots\ \cdot b_n!\cdot 1^{b_1}\cdot 2^{b_2}\cdot\ \ldots\ \cdot n^{b_n}$

Anzahl der Permutationen vom Typ $1^{b_1}\ldots n^{b_n}$:

$$\frac{n!}{b_1!\cdot b_2!\cdot\ \ldots\ \cdot b_n!\cdot 1^{b_1}\cdot 2^{b_2}\cdot\ \ldots\ \cdot n^{b_n}}$$

$a_1\ a_2\ \ldots\ a_n$ sei eine Permutation von $\{1,2,\ldots,n\}$

Ist $i<j$ und $a_i > a_j$, so heißt das Paar (a_i,a_j) eine Inversion der Permutation.

Beispiel: 4 1 2 3 : Inversionen: (4,1),(4,2),(4,3) ist $inv(\pi)$ die Anzahl der Inversionen von $\pi(1)\ \pi(2)\ldots\pi(n)$, so heißt $(-1)^{inv(\pi)}$ das Signum der Permutation $(sgn(\pi))$

$X=(x_{ij})$ sei eine $(n\times n)$-Matrix. Dann ist

$$det(X) = \sum_{\pi\in S_n} sgn(\pi)\cdot x_{1\ \pi(1)}\cdot x_{2\ \pi(2)}\cdot\ \ldots\ \cdot x_{n\ \pi(n)}$$

Inversionstafel von $a_1\ldots a_n\ :\ b_1\ldots b_n$

b_j = Anzahl der Elemente links von j, die größer als j sind (=Anzahl der Inversionen von $a_1\ldots a_n$ mit 2. Komposition j).

Beispiel: 5 9 1 8 2 6 4 7 3 $\quad = a_1\ldots a_9$

2	3	6	4	0	2	2	1	0
=	=	=	=	=	=	=	=	=
b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9

klar $0 \leq b_1 \leq n-1$, $0 \leq b_2 \leq n-2, \ldots,$ $0 \leq b_i \leq n-i$

$0 \leq b_{n-1} \leq 1$, $b_n = 0$

Bemerkung: Die Permutation ist durch die Inversionstafel eindeutig bestimmt.

Wir zeigen, dass man $a_1 \ldots a_n$ erhält, indem man sukzessive die relative Position der Elemente

$n, n-1, \ldots, 2, 1$

(in dieser Reihenfolge) bestimmt.

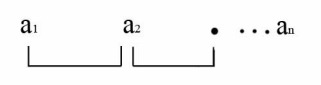
5 9 1 8 2 6 4 7 3

Beispiel: Sortieren mit Bubblesort

Geg. Ein Feld $a[1 \ldots n]$ von n (verschiedenen) Zahlen

Ges. Verfahren zur Sortierung des Feldes, d.h. nach Anwendung soll $a[1] < a[2] < \ldots < a[n]$

Wir versuchen, die Anzahl der Vergleiche zu minimieren.



1. Durchlauf von Bubblesort

   $1 \leq i \leq n-1$ Falls $a[i] > a[i+1]$: Vertauschen wir $a[i]$ und $a[i+1]$

   Nach dem 1. Durchlauf ist $a[n]$ das Größte der Elemente.

2. Durchlauf : Analog : $1 \leq i \leq n-2$

Nach höchstens $n-1$ Durchläufen sind wir fertig. Wir können das Verfahren auch abbrechen, falls bei einem Durchlauf keine Elemente vertauscht werden.

Es sei $a_1, \ldots, a_n$ eine Permutation und $b_1, \ldots, b_n$ ihre Inversionstafel

Ist $a'_1 \ldots a'_n$ mit Inversionstafel $b'_1 \ldots b'_n$ aus $a_1 \ldots a_n$ durch einen Durchlauf von Bubblesort entstanden.

so ist

$$b'_i = \begin{cases} b_i - 1, & \text{falls } b_i > 0 \\ 0, & \text{falls } b_i = 0 \end{cases} \qquad 1 \leq i \leq n$$

Beweis:

Ist links von a_i ein größeres Element, so wird $(\max_{j<i} a_j)$ an a_i vorbeigezogen, d.h. $b'_{a_i} = b_{a_i} - 1$. Ist dies nicht der Fall, so ist $b_{a_i} = b'_{a_i} = 0$

Frage: Wie viele Permutationen gibt es, die höchstens k Durchläufe benötigen?

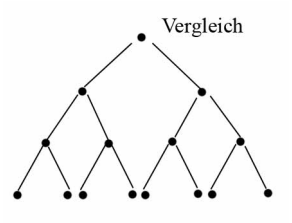
Antwort: $(Anzahl\ der\ Inversionstafeln\ ohne\ Komponente\ \geq k) = k^{n-k} \cdot k!, \quad 1 \leq k \leq n-1$

Genau k Durchläufe :$(k^{n-k} \cdot k! - (k-1)^{n-k+1} \cdot (k-1)!) = A_k$

Durchschnittliche Anzahl von Durchläufen:

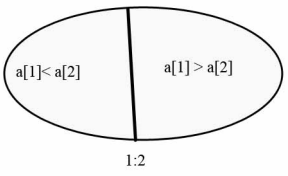
$$\frac{1}{n!} \cdot \sum_k A_k \cdot k = \ldots = (n+1) - \underbrace{\sum_{k=0}^{n} \frac{k^{n-k} \cdot k!}{n!}}_{\sim\sqrt{\frac{\pi \cdot n}{2}}}$$

Bessere Verfahren?



Die Permutationen müssen gewisse Blättern des Baumes entsprechen. Ich brauche also mindestens so viele Blätter wie es Permutationen gibt.

Die Anzahl der benötigten Vergleiche im worst case ist mindestens $\lceil \log_2 n! \rceil$



Stirling-Formel:

$$n! = \sqrt{2 \cdot \pi \cdot n} \cdot (\tfrac{n}{e})^n \cdot e^{\frac{\alpha}{12n}} \ , \quad 0 < \alpha < 1$$

$$\ln\ (n!) = \tfrac{1}{2} \cdot \ln\ (2\pi n) + n \cdot \ln\ n - n + \underbrace{\frac{\alpha}{12 \cdot n}}_{\longrightarrow 0}$$

Größenordnung $c \cdot n \cdot \ln\ n$

Weitere Verfahren!

Binäre Suche:

Vergleichen 2 Elemente x_1, x_2

Dann fügen wir x_3 an die richtige Stelle ein.

$x_1' < x_2' < x_3'$

Anschließend : x_4 in diese Kette einbauen:

$$x_1' < x_2' < x_3' < x_4'$$

$$\vdots$$

$$x_1' < x_2' < \ldots < x_i'$$

$x_i + 1$ wird eingefügt x_{i+1} könnte an $i+1$ verschiedene Positionen stehen.

Indem wir stets mit den mittleren Elementen der relevanten Teilfolge vergleichen, finden wir die Position von x_{i+1} mit $\lceil \log_2(i+1) \rceil$ Tests.

Insgesamt : $\lceil \log_2 2 \rceil + \lceil \log_2 3 \rceil + \ldots + \lceil \log_2 n \rceil$ Vergleiche

$\sum_{i=2}^{n} \lceil \log_2 i \rceil = B(n)$

$B(n) = n \cdot \lceil \log_2 n \rceil - 2^{\lceil \log_2 n \rceil} + 1$

04.05.05

Binäre Suche

Wir nehmen ein Element weg, sortieren rekursiv die übrigen $n-1$ und fügen dann das richtige Element an der richtigen Stelle ein.

$x_1 < x_2 < \ldots < x_{n-1}$

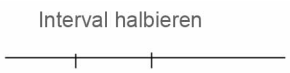
$\uparrow \quad \uparrow \quad \uparrow \quad \uparrow \quad \uparrow$

n-mögliche Positionen für das letzte Element.

Einordnung mit $\lceil \log_2 n \rceil$ Tests

$n = 2^k$ $\qquad x_1 < x_2 < \ldots < x_{2^{k-1}-1} < x_{2^{k-1}} < \ldots < x_{2^k-1}$

$\overset{?}{x} \overset{\uparrow}{\underset{>}{<}} x_{2^{k-1}}$



$2^{k-1} < n \leq 2^k$,d.h. $k = \lceil \log_2 \ n \rceil$

Führen wirklich neue Elemente $x_{n+1} < \ldots < x_{2^k}$ ein, falls nötig und argumentieren wie oben.

Insgesamt ist die Anzahl der Vergleiche

$\lceil \log_2 \ n \rceil + \lceil \log_2 (n-1) \rceil + \ldots + \lceil \log_2 2 \rceil = \sum_{i=2}^{n} \lceil \log_2 \ i \rceil = B(n)$

Es gilt: $B(n) = \lceil \log_2 \ n \rceil \cdot n - 2^{\lceil \log_2 \ n \rceil} + 1$

Betrachte dazu die Summe $\sum_{i=2}^{n} \lceil \log_2 \ i \rceil$, zunächst für den Fall $n = 2^k$:

$$1 + \quad 2 + \quad 3 + \quad 3 + \quad 3 + \quad 3 + \quad 4 + \quad \ldots + \quad 4 + \quad \ldots + \quad \underbrace{k + k + \ldots + k}_{2^{n-1} \text{ mal}}$$

$\lceil \log \ 2 \rceil \quad \lceil \log \ 3 \rceil \quad \lceil \log \ 4 \rceil$

$= 1 + 2 \cdot 2 + 3 \cdot 4 + 4 \cdot 8 + \ldots + k \cdot 2^{k-1} = \sum_{i=1}^{k} i \cdot 2^{i-1} = (k-1) \cdot 2^k + 1$

$1 + x + x^2 + \ldots + x^k \ = \frac{x^{k+1}-1}{x-1}$ $(*)$ geometrische Reihe

$(x-1) \cdot (1 + x + x^2 + \ldots + x^k) =$

$= x + x^2 + x^3 + \ldots + x^k + x^{k+1} - (1 + x + x^2 + x^3 + \ldots + x^k) = x^{k+1} - 1$

Wir differenzieren $(*)$:

$\sum_{i=1}^{k} i \cdot x^{i-1} = \frac{(x-1)\cdot(k+1)\cdot x^k - (x^{k+1}-1)}{(x-1)^2} = \frac{k \cdot xk+1-(k+1)\cdot x^k+1}{(x-1)^2}$

$x = 2$ Nenner : 1

Zähler : $k \cdot 2^{k+1} - (k+1) \cdot 2^k + 1$

$= (2 \cdot k - (k+1)) \cdot 2^k + 1 = (k-1) \cdot 2^k + 1$

$B(2^n) = (k-1) \cdot 2^k + 1 = k \cdot 2^k - 2^k + 1$

$k := \lceil \log_2\ n \rceil$, $O.B.d.A.\ 2^{k-1} < n < 2^k$

$B(n) = (k-1) \cdot 2^k + 1 - \underbrace{(2^k - n) \cdot k}_{\text{zuviel gezählte Summanden}}$

$= k \cdot 2^k - 2^k + 1 - 2^k \cdot k + n \cdot k = n \cdot k + 1 - 2^k = n \cdot \lceil \log_2\ n \rceil + 1 - 2^{\lceil \log_2\ n \rceil}$

Beispiel: Mergesort-Verfahren

„Divide and conquer“-Verfahren:

Das Feld $a[1 \ldots n]$ wird in zwei möglichst gleich große Teile zerlegt und diese werden rekursiv mit Mergesort sortiert. Dann werden die Reihenketten mit $(n-1)$ Vergleichen gemischt.

$a_1 < a_2 < \ldots < a_{\lfloor \frac{n}{2} \rfloor}$

$b_1 < b_2 < \ldots < b_{\lceil \frac{n}{2} \rceil}$

$M(n)$: Anzahl der Vergleiche von Mergesort:

$M(n) = M(\lfloor \frac{n}{2} \rfloor) + M(\lceil \frac{n}{2} \rceil) + (n-1)$

$M(1) = 0$, $M(2) = 1$, $M(3) = 3$, ?

Betrachte $D(n) = M(n) - M(n-1)$

$n = 2k : M(n) - M(n-1) = 2M(k) + 2k - 1$

$-(M(k) + M(k-1) + 2k - 2) = M(k) - M(k-1) + 1 = D(k) + 1$

$n = 2k+1 : M(n) - M(n-1) = M(k+1) + M(k) + 2k$

$-(2M(k) + 2k - 1) = M(k+1) - M(k) + 1$

Insgesamt: $D(n) = D(\lceil \frac{n}{2} \rceil) + 1$,

$D(2) = 1$

$D(3) = 2$

Es gilt: $D(n) = \lceil \log_2\ n \rceil$

$n = 2^k$: $D(n) = D(\frac{n}{2}) + 1 = D(\frac{n}{4}) + 2 = \ldots = D(\frac{n}{2^{k-1}}) + k - 1 = k$

$n = 2^k + a$, $a < 2^k$

$D(n) = D(\lceil \frac{n}{2} \rceil) + 1 = D(2^{k-1} + \frac{a}{2}) + 1$

erlaubt Induktion

$M(n) = \sum_{i=2}^{n} M(i) - M(i-1) = \sum_{i=2}^{n} D(i) = \sum_{i=2}^{n} \lceil \log\ i \rceil = B(n)$

$\uparrow$ $M(1)=0$

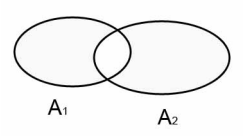
Problem: Bestimme die Anzahl der fixpunktfreien Permutation in S_n

Bezeichnung: D_n (Derangement-Zahlen)

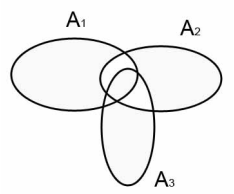
zur Lösung

1.7 Prinzip von Inklusion und Exklusion

$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$



$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$



Frage: Was ist $|A_1 \cup A_2 \cup \ldots \cup A_n|$?

Behauptung: $|A_1 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j|$

$+ \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| \pm \ldots + (-1)^{n-1} \cdot |A_1 \cap \ldots \cap A_n|$

$= \sum_{\emptyset \neq I \subseteq \{1,\ldots,n\}} (-1)^{|I|-1} |\bigcap_{i \in I} A_i|$

Beweis: Angenommen, ein Element a ist in genau k der Mengen A_i Enthalten. Wie oft wird es rechts gezählt?

$k - \binom{k}{2} + \binom{k}{3} \pm = 1 - (1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} \pm \ldots + (-1)^k \cdot \binom{k}{k} = 1 - \underbrace{(1-1)^k}_{0} = 1$

$(1+x)^k \cdot \sum_{j=0}^{k} \binom{k}{j} \cdot x^j$

$x = -1$

$\sum_{j=0}^{k} \binom{k}{j} \cdot (-1)^j = (1-1)^k$

$\mathcal{P}_n := n! - D_n$

$A_i := \{\pi \in S_n \mid \pi(i) = i\}$

$P_n = |A_1 \cup A_2 \cup \ldots \cup A_n|$

$|\bigcap_{j \in J} A_j| = (n - |J|)!$

$P_N = |A_1 \cup \ldots \cup A_n| = \sum_{i=1}^{n} (-1)^{j-1} \cdot \binom{n}{j} \cdot (n-j)!$

$= \sum_{j=1}^{n} (-1)^{j-1} \cdot \frac{n!}{j!(n-j)!} \cdot (n-j)! = n! \sum_{j=1}^{n} (-1)^{j-1} \frac{1}{j}$

$= n!(1 - \frac{1}{2!} + \frac{1}{3!} - \frac{1}{4!} \pm \ldots + (-1)^{n-1} \frac{1}{n!})$

$D_n = n!(1 - 1 + \frac{1}{2!} - \frac{1}{3!} \pm \ldots + \frac{(-1)}{n!})$

$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots$

$\frac{1}{e} = e^{-1} = 1 - 1 + \frac{1}{2!} - \frac{1}{3!} \pm \ldots + \frac{(-1)^n}{n!} + \ldots$

$D_n \approx \frac{n!}{e}$

Inversion

Wir betrachten Stirlingzahlen erster $(s_{n,k})$ und zweiter Art $(S_{n,k})$

Wir wissen: $x^n = \sum_{k=0}^{n} S_{n,k} \cdot x^{\underline{k}} = \sum_{k=0}^{n} S_{n,k} \cdot x \cdot (x-1) - (x-k+1)$

Wenn x eine Variable ist, so ist dies eine Ploynomidentität.

$S_{n,k} = 0$ für $k > n$, $S_{o,o} = 1$

$S_{0,k} = 0$ für $k > 0$

06.05.05

$$x^n = |\{f : N \to X \mid N = \{1, \ldots, n\},\ X = \{1, \ldots, x\}\}|$$
$$= \sum_{Y \subseteq X} \underbrace{|\{f : N \to X \mid f(N) = Y\}|}_{S_{n,|Y|} \cdot |Y|!}$$
$$= \sum_{k=0}^{n} S_{n,k} k! \cdot \binom{x}{k} = \sum_{k=0}^{n} S_{n,k} \cdot x^{\underline{k}}$$

Polynom: $a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_1 \cdot x + a_0 = p(x)$

$Grad\ (p) = n \quad (a_n \neq 0)$

$P(x)$ hat höchstens n Nullstellen.

⌈ $q(x)$ Polynom vom Grad m. Dann ex stets Polynome $h(x)$ und $r(x)$ mit:

⌊ $p(x) = q(x) \cdot h(x) + r(x)$ mit $Grad\ r(x) < m$

Ist etwa $p(\alpha) = 0 \quad \alpha \in \mathbb{C}$, so schreiben wir:

$p(x) = (x - \alpha) \cdot h(x) + r(x), \quad r(x)\ konstant.$

$\Rightarrow 0 = p(\alpha) = 0 + r(\alpha)$, also $r(x) \equiv 0$

$\Rightarrow p(x) = (x - \alpha) \cdot h(x) \Rightarrow Grad\ h(x) = n - 1$

Jede weitere Nullstelle von $p(x)$ ist auch eine von $h(x)$ $\underbrace{\Rightarrow}_{Induktion}$ $p(x)$ hat insgesamt höchstens n Nullstellen.

Bemerkung: Sind $p(x), q(x)$ Polynome vom $Grad$ höchstens n und gilt:

$p(\alpha_i) = q(\alpha_i)$ für $n+1$ verschiedene Zahlen $\alpha_0, \alpha_1, \ldots, \alpha_n$ so ist $p(x) = q(x)$ für alle x.

Denn: $h(x) := p(x) - q(x)$ hat $Grad \leq n$ und hat $n+1$ Nullstellen, also ist $p(x) - q(x)$ das Nullpolynom.

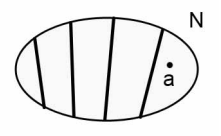
Es gilt die folgende Rekursion:

$$S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k} \qquad (n, k > 0)$$

Beweis: (Summenregel)

Es sei $N = \{1, \ldots, n\}$, $a \in N$
klassifizieren die k-Partitionen von N auf folgende Weise:

1. $\{a\}$ ist ein Block der Partition

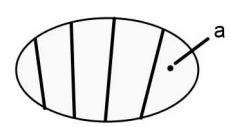


2. a ist in einen Block mit mindestens 2 Elementen enthalten

Ordnen den Partitionen von N Partitionen von $N\backslash\{a\}$ zu, indem wir a entfernen.
Im Fall 1: Eine $(k-1)$-Partition von $N\backslash\{a\}$ entsteht
Fall 2: Eine k-Partition von $N\backslash\{a\}$ entsteht.

Fall 1: Zuordnung ist eine Bijektion
Anzahl: $S_{n-1,k-1}$

Fall 2:



Die Zuordnung ist „k zu 1“, d.h. jede k-Partition von $N\backslash\{a\}$ entsprechen genau k Urbilder, also:
$Anzahl\ der\ entspr.\ Part. = S_{n-1,n} \cdot k$
$\boxed{S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}}$

Beispiel:

$$
\begin{array}{ccccccc}
1 & & & & & & \\
0 & 1 & & & & & \\
0 & 1 & 1 & & & & \\
0 & 1 & 3 & 1 & & & \\
\vdots & & & & \ddots & & \\
0 & & & & & 1 & \\
\vdots & & & & & &
\end{array}
$$

$S_{7,k}:\ 0\ 1\ 6\ 3\ 301\ 350\ 140\ 21\ 1$
$S_{n,2}:\ 2^{n-1}-1,\ S_{n,n-1} = \binom{n}{2}$

Entsprechend suchen wir eine Rekursion für die Stirling-Zahlen 1.Art
$s_{n,k} = |\{\pi \in S_n \mid \pi \text{ hat genau } k \text{ Zyklen}\}|$

$s_{0,0} = 1 \qquad s_{0,k} = 0 \quad (k > 0),\ s_{n,0} = 0\ (n > 0)$

Rekursion

$s_{n,k} = s_{n-1,k-1} + (n-1)s_{n-1,k} \qquad (n, k > 0)$

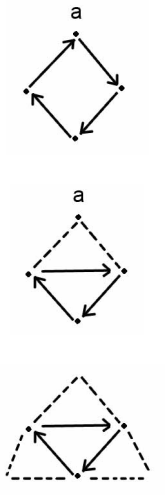
Beweis: Es seien N und a wie oben klassifizierte Permutationen mit genau k-Zyklen:

1. a ist Fixpunkt $\qquad (\#_1)$
2. a ist kein Fixpunkt $\quad (\#_2)$

zu 1. $\#_1 = s_{n-1,k-1}$

zu 2.

Zerstören von a liefert Permutation von $N\backslash\{a\}$ mit k-Zyklen.



Das Bild von a kann jedes Element von $N\backslash\{a\}$ sein,d.h. die Abbildung ist $'(n-1)\ zu\ 1'$

$\Rightarrow \#_1 + \#_2 = s_{n-1,k-1} + (n-1) \cdot s_{n-1,k}$

Beispiel: $s_{n,1} = (n-1)!,\ s_{n,n-1} = \binom{n}{2},\ s_{n,n} = 1$

$\frac{s_{n,2}}{(n-1)!} = \frac{(n-2)!}{(n-1)!} + \frac{s_{n-1,2} \cdot (n-1)}{(n-1)!} = \frac{s_{n-1,2}}{(n-2)!} + \frac{1}{n-1}$

Durch Induktion :

$s_{n,2}(n-1)! \cdot (\frac{1}{n-1} + \frac{1}{n-2} + \ldots + 1) = (n-1)! \cdot H_{n-1}$

Zeige nun: Für $x \in \mathbb{N}$ ist

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

Beweis: Induktion nach n

$n = 0$ ✓ $\qquad 1 = 1$

$n = 1 : \qquad x = x$ ✓

$x^0 := 1,\ x^{\underline{0}} \stackrel{?}{=} 1,\ \sum_{\emptyset} = 0,\ \prod_{\emptyset} = 1$

Ind.Schritt:

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

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

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

$$= \sum_{k=0}^{n} (-1)^{n-k} \cdot x^k \cdot \underbrace{\{s_{n-1,k-1} + (n-1) \cdot s_{n-1,k}\}}_{s_{n,k}}$$

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

1.8 Basisfolgen

Definition: Eine Basisfolge $(p_0(x), p_1(x), \ldots))$ ist eine Folge von Polynomen mit $Grad\ (p_n) = n$ für alle n (Insbesondere: $p_0(x)$ ist eine Konstante $\neq 0$)

z.b. $p_n(x) = x^n, x^{\underline{n}}, x^{\overline{n}}, (x-1)^n$

Die Polynome $p_0(x), p_1(x), \ldots, p_n(x)$ bilden eine Basis im Vektorraum $Poly(n)$ aller Polynome vom Grad $\leq n$.

Sind $(p_0(x), p_1(x), \ldots)$ und $q_0(x), q_1(x), \ldots)$ Basisfolgen, so ex. Zahlen $(a_{n,k})$ und $(b_{n,k})$ mit:

$$q_n(x) = \sum_{k=0}^{n} a_{n,k} \cdot p_k(x)$$

$$\begin{pmatrix} a_{11} & 0 & & \ldots & 0 \\ a_{12} & a_{22} & 0 & \ldots & 0 \\ | & | & \diagdown & & \end{pmatrix}$$

bzw.: $p_n(x) = \sum_{k=0}^{n} b_{n,k} \cdot q_k(x)$

Wir nennen $(a_{n,k})$ und $(b_{n,k})$ die Zusammenhangskoeffizienten der Basisfolgen. Sie bilden untere Dreiecksmatrizen (unendlich) $(a_{n,k} = b_{n,k} = 0 \quad für\ k > n)$

$$\overset{(a_{n,k})}{\begin{pmatrix} \diagdown & & 0 \\ - & \diagdown & \\ - & - & \diagdown \end{pmatrix}} \quad \overset{(b_{n,k})}{\begin{pmatrix} \diagdown & & 0 \\ - & \diagdown & \\ - & - & \diagdown \end{pmatrix}}$$

Diese Matrizen sind invers zueinander.

Betrachte:

$A = (a_{n,k})_{0 \leq n,k \leq m}$

$B = (b_{n,k})_{0 \leq n,k \leq m}$

A beschreibt die identische Abbildung auf $Poly(m)$ bzgl. $(q_0, q_1, \ldots, q_m)$ und $(p_0, p_1, \ldots, p_m)$ (bei Zeilenkonvention) und B ebenfalls die Identität bzgl. $(p_0, p_1, \ldots, p_m)$ und $(q_0, q_1, \ldots, q_m)$

Wir wissen:
Die Stirlingzahlen $(S_{n,k})$ und $(s_{n,k})$ zweiter bzw. erster Art sind die Zusammenhangskoeffizienten der Basisfolgen $(1, x, ^2, \ldots, x^n, \ldots)$ und $(1, x^{\underline{1}}, x^{\underline{2}}, \ldots, x^{\underline{n}}, \ldots)$

Satz: Es sind (p_n) und (q_n) zwei Basisfolgen mit Zush.koeff. $(a_{n,k})$ bzw. $(b_{n,k})$. Dann gilt für 2 Folgen $(u_0, u_1, \ldots)$, $(v_0, v_1, \ldots)$ von Zahlen:

$v_n = \sum_{k=0}^{n} a_{n,k} \cdot u_k$ für alle n

$\Leftrightarrow u_n = \sum_{k=0}^{n} b_{n,k} \cdot v_k$ für alle n

(sog. „Inversionsformel“)

Beweis: A und B sind zueinander invers, also $v = A \cdot u \Leftrightarrow B \cdot v = u$

Beispiel: Binomial - Inversion:

$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot a^k \cdot b^{n-k}$

$a = x - 1\ ,\ b = 1$

$x^n = \sum_{k=0}^{n} \binom{n}{k} \cdot (x-1)^k$ $\quad {\scriptstyle (1,x,x^2,\ldots)} \atop {\scriptstyle (1,x-1,(x-1)^2,\ldots)}$

$\Rightarrow v_n = \sum_{k=0}^{n} a_{n,k} \cdot u_k \qquad \forall n.$

$\Leftrightarrow u_n = \sum_{k=0}^{n} (-1)^{n-k} \cdot \binom{n}{k} \cdot v_k \qquad \forall n.$

denn: $(x-1)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot (-1)^{n-k} \cdot x^k$

statt u_n : $(-1)^k\ u_n$:

$v_n = \sum_{k=0}^{n} \binom{n}{k} \cdot (-1)^k \cdot u_k \Leftrightarrow u_n = \sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} \cdot v_k$

13.05.05

$(p_0, p_1, p_2, \ldots, p_n, \ldots)$ $\qquad Grad\ (p_n) = Grad\ (q_n)$

$(q_0, q_1, q_2, \ldots, q_n, \ldots)$

Zusammenhangskoeff.

$q_n(x) = \sum_{k=0}^{n} a_{nk} \cdot p_k(x)$ $\qquad a_{nk} = b_{nk} = 0 \quad falls\ k > n$

$p_n(x) = \sum_{k=0}^{n} b_{nk} \cdot q_k(x)$

$$\begin{pmatrix} a_{00} & & 0 \\ a_{10} & a_{11} & \\ a_{20} & a_{21} & a_{22} \\ \vdots & \vdots & \ddots \end{pmatrix} \cdot \begin{pmatrix} b_{00} & & 0 \\ b_{10} & b_{11} & \\ b_{20} & b_{21} & b_{22} \\ \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ & & 1 \\ 0 & & \ddots \end{pmatrix}$$

$$q_n(x) = \sum_{k=0}^{n} a_{nk} \cdot \sum_{j=0}^{k} b_{kj} \cdot q_j(x) = \sum_{j=0}^{n} q_j(x) \cdot \underbrace{\sum_{k=0}^{n} a_{n,k} \cdot b_{kj}}_{c_{nj}}$$

$$\Rightarrow c_{nj} = \left\{ \begin{array}{ll} 1, & \text{j = n} \\ 0, & \text{j < n} \end{array} \right\} = [n \overset{Inversion}{\underset{\downarrow}{=}} j]$$

A Aussage: $[A] := \left\{ \begin{array}{ll} 1, & \text{falls } A \text{ wahr} \\ 0, & \text{falls } A \text{ falsch} \end{array} \right.$

(a_{nk}) und (b_{nk}) sind inverse Matrizen

Für Zahlenfolgen $(u_0, u_1, \ldots, u_n, \ldots) = u$

$(v_0, v_1, \ldots, v_n, \ldots) = v$

Für alle n : $v_n = \sum_{k=0}^{n} a_{nk} \cdot u_k$

$\Leftrightarrow v = A \cdot u \qquad (A = (a_{nk}))$

$\Leftrightarrow A \cdot v = u \qquad (B = A^{-1})$

$\Leftrightarrow u_n = \sum_{k=0}^{n} b_{nk} \cdot v_k$

„Inversionsformel“

Beispiel:

(i) Stirling-Inversion:

$v_n = \sum_{k=0}^{n} S_{n,k} \cdot u_k \qquad \forall n$

$\Leftrightarrow u_n = \sum_{k=0}^{n} (-1)^{n-k} \cdot s_{n,k} \cdot v_k$

(insbesondere: $\sum_{k=0}^{n} S_{n,k} \cdot (-1)^{k-j} \cdot s_{k,j} = [n = j]$)

(ii) Binomial - Inversion

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

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

Also: $v_n = \sum_{k=0}^{n} \binom{n}{k} \cdot u_k \qquad \forall n$

$\Leftrightarrow u_k = \sum_{k=0}^{n} (-1)^{n-k} \cdot \binom{n}{k} \cdot v_k \qquad \forall n$

Ersetzen wir u_n durch $(-1)^n \cdot u_n$, so ergibt sich:

$v_n = \sum_{k=0}^{n} \binom{n}{k} \cdot (-1)^k \cdot u_k \qquad \forall n$

$\Leftrightarrow u_n \cdot (-1)^n = \sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} \cdot v_k \qquad \forall n$

$\Leftrightarrow u_n = \sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} \cdot v_k \qquad \forall n$

Anwendung: Derangement-Zahlen

$D_n = \ Anzahl\ der\ fixpunktfeien\ Permutationen\ in\ S_n$

$d(n,k) = \ Anzahl\ der\ Permutationen\ in\ S_n\ mit\ genau\ k\ Fixpunkten$

$d(n,0) = D_n$.

$$\underline{\binom{n}{k} \cdot D_{n-k} = d(n,k)}$$

$$\Rightarrow n! = |S_n| = \sum_{k=0}^{n} d(n,k) = \sum_{k=0}^{n} \binom{n}{k} \cdot D_{n,k}$$

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} = \binom{n}{n-k} \cdot \sum_{k=0}^{n} \binom{n}{k} \cdot D_k$$

Binomialinversion mit $u_k = D_n$, $v_k = n!$ liefert:

$$\underline{D_n} = \sum_{k=0}^{n} (-1)^{n-k} \cdot \binom{n}{k} \cdot k! = n! \cdot \sum_{k=0}^{n} (-1)^{n-k} \cdot \frac{1}{(n-k)!} = \underline{n! \cdot \sum_{k=0}^{n} (-1)^k \cdot \frac{1}{k}}$$

1.9 Lösung von Rekursionen

1.Erzeugende Funktionen

Gelöst:

Mergesort-Rekursion

$M(n) = M(\lfloor \frac{n}{2} \rfloor) + M(\lceil \frac{n}{2} \rceil) + (n-1)$

Binäre Suche

$B(n) = B(n-1) + \lceil \log\ n \rceil$

Ziel: Bestimmung einer Folge

$a_0, a_1, a_2, \ldots, a_n, \ldots$

Wobei eine oder mehrere Anfangsbedingungen gegeben sind, sowie eine Vorschrift, wie man a_n aus $a_0, a_1, a_2, \ldots, a_{n-1}$ berechnet.

Bei der Methode der erzeugenden Funktionen fasst man die Folge (a_n) als Folge der Koeffizienten einer Potenzreihe auf, d.h.

$$A(z) := \sum_{n=0}^{\infty} a_n \cdot z^n$$

und versucht, die Rekursion als Eigenschaft von $A(z)$ zu deuten.

Dabei genügt es, rein formal „nachdem üblichen Rechenregeln“ mit den Reihen zu rechnen und Konvergenzfragen außer acht zu lassen.

$$A(z) = \sum_{z \geq 0} a_n \cdot z^n \ , \ B(z) = \sum_{z \geq 0} b_n \cdot z^n$$

$$\Rightarrow A(z) + B(z) = \sum_{n \geq 0} (a_n + b_n) \cdot z^n$$

$A(z) \cdot B(z)$

	a_0	$+$	$a_1 \cdot z$	$+$	$a_2 \cdot z^2$	$+$	$\ldots$	$+$	$a_n \cdot z^n$	$\ldots$
b_0	$a_0 \cdot b_0$		$a_1 \cdot b_0 \cdot z$		$a_2 \cdot b_0 \cdot z^2$				$a_n \cdot b_0 \cdot z^n$	
$+$										
$b_1 \cdot z$	$a_0 \cdot b_1 \cdot z$		$a_1 \cdot b_1 \cdot z^2$		$a_2 \cdot b_1 \cdot z^3$				$a_n \cdot b_1 \cdot z^{n+1}$	
$+$										
$b_2 \cdot z^2$	$a_0 \cdot b_2 \cdot z^2$		$a_1 \cdot b_2 \cdot z^3$		$a_2 \cdot b_2 \cdot z^4$				$a_n \cdot b_2 \cdot z^{n+2}$	
$+$										
$\vdots$	$\vdots$									
$+$										
$b_n \cdot z^n$	$a_0 \cdot b_n \cdot z^n$		$a_1 \cdot b_n \cdot z^{n+1}$							

$$A(z) \cdot B(z) = \sum_{n=0}^{\infty} (\sum_{k=0}^{n} a_k \cdot b_{n-k}) \cdot z^n$$

„Faltung“ von $A(z)$ und $B(z)$

Bemerkung: $A(z)$ besitzt ein multiplikatives Inverses g.d.w. $a_0 \neq 0$

Notwendig: $klar.$

Hinreichend: Ist $a_0 \neq 0$, so kann $B(z) = \frac{1}{A(z)}$ wie folgt bestimmt werden:

$a_0 \cdot b_0 \stackrel{!}{=} 1$, also $b_0 = \frac{1}{a_0}$

$a_0 \cdot b_1 + a_1 \cdot b_0 \stackrel{!}{=} 0$, also $b_1 = \frac{1}{a_0} \cdot (-a_1 \cdot b_0)$

sind $b_0, b_1, \ldots, b_{n-1}$ bestimmt, so dass

$b_0 \cdot a_0 = 1$, $\sum_{i=0}^{k} a_i \cdot b_{k-i} = 0$ für $1 \leq k \leq n-1$

so sei $b_n := -\frac{1}{a_0} \cdot (\sum_{i=1}^{n} a_i \cdot b_{n-i})$

$(a_0 \cdot b_n + \sum_{i=1}^{n} a_i \cdot b_{n-i} = 0)$

Beispiel:

(i) Geometrische Reihe

$(1-z) \cdot (1 + z + z^2 + \ldots + z^n + \ldots) = 1$

$\sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$

(ii) Weitere Potenzreihen

$\sum_{n=0}^{\infty} \binom{\alpha}{n} \cdot z^n = (1+z)^\alpha \quad (\alpha \in \mathbb{R},\ \binom{\alpha}{n} := \frac{\alpha \cdot (\alpha-1) \cdot \ \ldots \ \cdot (\alpha-n+1)}{n!})$

$\sum_{n=0}^{\infty} \frac{z^n}{n!} = e^z$

$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} \cdot z^n = \ln\ (1+z)$

Anwendungsbeispiele:

Beispiel: Catalan-Zahlen (C_n)

Gegeben: $n+1$ Variablen $x_0, x_1, \ldots, x_n$

Auf wie viele Weisen kann das Produkt $x_0 \cdot x_1 \cdot x_2 \cdot \ \ldots \ \cdot x_n$ Korrekt geklammert werden?

nicht assoziativ
nicht kommutativ

Anzahl sei C_n

$C_0 := 1$, $C_1 = 1$

$n = 2 : (x_0 \cdot x_1) \cdot x_2 = x_0 \cdot (x_1 \cdot x_2) \qquad C_2 = 2$

$n = 3 : (x_0 \cdot x_1) \cdot (x_2 \cdot x_3),\ ((x_0 \cdot x_1) \cdot x_2)x_3,\ x_0 \cdot (x_1 \cdot (x_2 \cdot x_3)),$
$(x_0 \cdot (x_1 \cdot x_2)) \cdot x_3,\ x_0 \cdot ((x_1 \cdot x_2) \cdot x_3) \qquad C_3 = 5$

Rekursion für C_n:

Es gibt genau eine Multiplikation außerhalb aller Klammern (die letzte) falls $n > 0$. Angenommen, dieser letzte Multiplikationsstern steht zwischen x_k und x_{k+1}

$$\underbrace{(x_0 \dots x_k)}_{C_n} \cdot \underbrace{(x_{k+1} \dots x_n)}_{C_{n-k-1}}$$

Dann gibt es C_k Möglichkeiten, $x_0, \dots, x_k$ zu klammern und C_{n-k-1} Möglichkeiten, $x_{k+1}, \dots, x_n$ zu klammern; also:

$C_n = C_0 \cdot C_{n-1} + C_1 \cdot C_{n-2} + \dots + C_{n-1} \cdot C_0 \qquad (n > 0)$

$C_k = \sum_{k=0}^{n-1} C_k \cdot C_{n-1-k} + [n = 0]$

$C(z) = \sum_{n=0}^{\infty} C_n \cdot z^n = \sum_{n=0}^{\infty} (\sum_{k=0}^{k-1} C_k \cdot C_{n-1-k}) \cdot z^n + 1$

$= \sum_{k=0}^{\infty} C_k \cdot z^k \sum_{n=0}^{\infty} C_{n-1-k} \cdot z^{n-k} + 1$

$= C(z) \cdot z \cdot C(z) + 1$, also:

$1 - C(z) + z \cdot C(z)^2 = 0$

$C(z)^2 - \frac{1}{z} \cdot C(z) + \frac{1}{z} = 0$

$C(z) = \frac{1}{2 \cdot z} \pm \sqrt{\frac{1}{4 \cdot z^2} - \frac{1}{z}}$

$= \frac{1}{2 \cdot z} \pm \frac{1}{s \cdot z} \cdot \sqrt{1 - 4 \cdot z} = \frac{1 \pm \sqrt{1 - 4 \cdot z}}{2 \cdot z}$

Potenzreihe für $\sqrt{1 - 4 \cdot z} = 1 + (-4 \cdot z)^{\frac{1}{2}}$

$(1 + z)^{\alpha} = \sum_n \binom{\alpha}{n} \cdot z^n$ mit $\alpha = \frac{1}{2}$, $(-4 \cdot z)$ statt z :

$\sqrt{1 - 4 \cdot z} = \sum_{n \geq 0} \binom{\frac{1}{2}}{n} \cdot (-4 \cdot z)^n \cdot z$

$= 1 + \sum_{n \geq 1} \frac{\frac{1}{2} \cdot (\frac{1}{2} - 1) \cdot \dots \cdot (\frac{1}{2} - n + 1)}{n!} \cdot (-4)^n \cdot z^n$

$= 1 + \sum_{n \geq 1} \frac{1}{2 \cdot n} \cdot \binom{-\frac{1}{2}}{n-1} \cdot (-4)^n \cdot z^n$

Wegen $C_0 = 1$ ist

$C(z) = \frac{1 - \sqrt{1 - 4 \cdot z}}{2 \cdot z} = \sum_{n=1}^{\infty} \frac{1}{n} \cdot \binom{-\frac{1}{2}}{n-1} \cdot (-4)^{n-1} \cdot z^{n-1}$

$= \sum_{n=0}^{\infty} \binom{-\frac{1}{2}}{n} \cdot (-4)^n \cdot \frac{z^n}{n+1} = \sum_{n=0}^{\infty} \binom{2 \cdot n}{n} \cdot \frac{z^n}{n+1}$

$\binom{2 \cdot n}{n} = \frac{(2 \cdot n)!}{n! \cdot n!} = \frac{1}{n!} \cdot 2^n \cdot (2 \cdot n - 1) \cdot (2 \cdot n - 3) \cdot \ \dots \ \cdot 3 \cdot 1$

$= \frac{1}{n!} \cdot (4 \cdot n - 2) \cdot (4 \cdot n - 6) \cdot \dots \cdot 6 \cdot 2$

$\binom{-\frac{1}{2}}{n} \cdot (-4)^n = \frac{(-\frac{1}{2}) \cdot (-\frac{1}{2} - 1) \cdot \ \dots \ \cdot (-\frac{1}{2} - n + 1)}{n!} \cdot (-4)^n$

25.05.05

1.10 Erzeugende Funktionen

$A(z) = \sum_{n=0}^{\infty} a_n \cdot z^n$

$\frac{1}{1-z} = 1 + z + z^2 + \ldots + z^n + \ldots$ geometrische Reihe

$(1+z)^\alpha = \sum_{n=0}^{\infty} \binom{\alpha}{n} \cdot z^n$

$\binom{\alpha}{n} = \frac{\alpha \cdot (\alpha-1) \cdot \ldots \cdot (\alpha-n+1)}{n!}$ Binomialreihe

$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$ $\ln\ (1+z) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} \cdot z^n$

Beispiel: Catalan-Zahlen

$C(z) = \frac{1-\sqrt{1-4\cdot z}}{2\cdot z} = \sum_{n=0}^{\infty} \binom{2\cdot n}{n} \cdot \frac{z^n}{n+1}$,

$C_n = \frac{1}{n+1} \cdot \binom{2\cdot n}{n}$

Beispiel: Fibonacci-Zahlen

$F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2} \quad (n \geq 2)$

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$

Gesucht: „Formel“ für F_n

Ansatz: $F(z) := \sum_{n=0}^{\infty} F_n \cdot z^n$ $\quad (F_n := 0\ (n < 0))$

Schritt 1: Drücke die Rekursion in einer Gleichung aus

(inkl. Anfangsbedingung).

$F_n = F_{n-1} + F_{n-2} \ + [n = 1]$

Schritt 2: Was bedeutet die Rekursion für $F(z)$?

$F(z) = \sum_{n=0}^{\infty} F_n \cdot z^n = \sum_{n=0}^{\infty} F_{n-1} \cdot z^n + \sum_{n=0}^{\infty} F_{n-2} \cdot z^n + \sum_{n=0}^{\infty} [n=1] \cdot z^n$

$= z \cdot \underbrace{\sum_{n=0}^{\infty} F_{n-1} \cdot z^{n-1}}_{F(z)} + z^2 \cdot \underbrace{\sum_{n=0}^{\infty} F_{n-2} \cdot z^{n-2}}_{F(z)} + z$

$= z \cdot F(z) \cdot z^2 \cdot F(z) + z$

$F(z) \cdot (1 - z - z^2) = z$, also

$F(z) = \frac{z}{1-z-z^2}$

Schritt 3: Benutze den gefundenen Ausdruck für $F(z)$, um eine (explizite) Reihenentwicklung zu bekommen.

Hier: Partialbruchzerlegung:

Ansatz: $1 - z - z^2 = (1 - \alpha \cdot z) \cdot (1 - \beta \cdot z) = p(z)$

$z^2 \cdot p(\frac{1}{z}) = z^2 - z - 1 = (z - \alpha) \cdot (z - \beta)$

$\alpha, \beta = \frac{1}{2} \pm \sqrt{\frac{1}{4} + 1} = \frac{1}{2} \pm \sqrt{\frac{5}{4}} = \frac{1 \pm \sqrt{5}}{2}$,

etwa $\alpha = \frac{2+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$

$\frac{1}{(a-\alpha\cdot z)\cdot(1-\beta\cdot z)} = \frac{a}{1-\alpha\cdot z} + \frac{b}{1-\beta\cdot z}$

Bestimme a und b : $\quad |\cdot(1-\alpha\cdot z)$ $dann\ z=\frac{1}{\alpha}$

$a = \frac{1}{1-\frac{\beta}{\alpha}} = \frac{\alpha}{\alpha-\beta} = \frac{\alpha}{\sqrt{5}}$

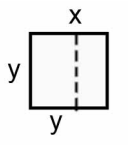
$b = \frac{1}{1-\frac{\alpha}{\beta}} = \frac{\beta}{\beta-\alpha} = -\frac{\beta}{\sqrt{5}}$

Insgesamt:

$$F(z) = z \cdot (\tfrac{a}{1-\alpha\cdot z} + \tfrac{b}{1-\beta\cdot z}) = z \cdot (a \cdot \sum_{n=0}^{\infty} \alpha^n \cdot z^n + b \cdot \sum_{n=0}^{\infty} \beta^n \cdot z^n)$$

$$= \sum_{n=1}^{\infty} (a \cdot \alpha^{n-1} + b \cdot \beta^{n-1}) \cdot z^n = \tfrac{1}{\sqrt{5}} \cdot \sum_{n=1}^{\infty} (\alpha^n - \beta^n) \cdot z^n \ ,$$

also $F_n = \frac{1}{\sqrt{5}} \cdot (\underbrace{(\frac{1+\sqrt{5}}{2})^n}_{\substack{\approx 1{,}618\ldots \\ \Phi\text{:goldener Schnitt}}} - (\frac{1-\sqrt{5}}{2})^n)$



Anwendung: Analyse des Euklidischen Algorithmus zur Ermittlung des ggT.

$u, v \in \mathbb{N}$, $u > v$

$u = q_1 \cdot v + r_1$, $0 < r_1 < v$

$v = q_2 \cdot r_1 + r_2$, $0 < r_2 < r_1$

$\vdots \qquad\qquad \vdots$

$F_4 \leq r_{n-3} = q_{n-1} \cdot \overbrace{r_{n-2}}^{F_3} + \overbrace{r_{n-1}}^{\geq 1 = F_2}$, $\qquad 0 < t_{n-1} < r_{n-2}$

$2 \leq r_{n-2} = q_n \cdot r_{n-1} + 0 \qquad r_{n-1} \geq 1 \ , \ q_n \geq 2$

Wie viele Divisionen sind nötig?

Wie müssen u (und v) gewählt werden:

wenn u möglichst klein sein soll bei exakt n Divisionen ?

$r_{n-2} \geq 2 - F_3$

$\underbrace{r_{n-k}}_{\geq F_{k+1}} = \underbrace{q_{n-k+2}}_{\geq 1} \cdot \underbrace{r_{n-k+1}}_{\geq F_k} + \underbrace{r_{n-k+2}}_{\geq F_{k-1}}$

$\Rightarrow r_{n-k} \geq F_{k+1}$

$r_1 \geq F_n$, $v \geq F_{n+1}$, $u \geq F_{n+2}$

$\Rightarrow$ Das minimale u, für das der euklidische Algorithmus n Divisionen benötigt, ist

F_{n+2}

$\Rightarrow$ Obere Schranke für die Anzahl der Divisionen falls $0 \leq u, v < N$:

$$\underline{\lceil \log_\Phi(\sqrt{5} \cdot N) \rceil - 2}$$

$F_{n+2} \geq N$, $F_{n+1} < N \qquad \frac{1}{\sqrt{5}} \cdot (\underbrace{\alpha^n}_{=\varphi} - \beta^n)$

$\Rightarrow \frac{\Phi^{n+1}}{\sqrt{5}} < N$, $\Phi^{n+1} < \sqrt{5} \cdot N$

$n + 1 < \log_\Phi(\sqrt{5} \cdot N)$

$n + 2 < \lceil \log_\Phi(\sqrt{5} \cdot N) \rceil$, $n < \lceil \log_\Phi(\sqrt{5} \cdot N) \rceil - 2$

Beweis: $\log_\Phi(\sqrt{5} \cdot N) \approx 2{,}078 \cdot \ln N + 1{,}672$

$\approx 4{,}785 \cdot \log_{10} N + 1{,}672$

ungefähr 5 - mal die Anzahl der Dezimalziffern.

1.11 Lineare Rekursionen mit konstanten Koeffizienten

$f(n+d) + q_1 \cdot f(n+d-1) + \ldots + q_d \cdot f(n) = 0$ für alle $u \geq 0$

Gesucht: $f(n)$

$f(n+2) - f(n+1) - f(n) = 0$, $d = 2$, $q_1 = -1$, $q_2 = -1$

Satz: Es sei $q_1, q_2, \ldots, q_d$ eine endliche Zahlenfolge $d \geq 1$, $q_d \neq 0$,

$1 + q_1 \cdot z + q_2 \cdot z^2 + \ldots + q_d \cdot z^d =: q(z)$

$= (1 - \alpha_1 \cdot z)^{d_1} \cdot (1 - \alpha_2 \cdot z)^{d_2} \cdot \ldots \cdot (1 - \alpha_k \cdot z)^{d_k}$,

d.h. $\alpha_1, \alpha_2, \ldots, \alpha_k$ sind die verschiedenen Nullstellen von

$q_R(z) = z^d + q_1 \cdot z^{d-1} + \ldots + q_{d-1} \cdot z + q_d = z^d \cdot q(\frac{1}{z})$

mit Vielfachheiten d_i , $i = 1, \ldots, k$,

$d_1 + d_2 + \ldots + d_k = d$

Für $f(n)$ $(n = 0, 1, 2, \ldots)$ $(f : \mathbb{N}_0 \to \mathbb{C})$ sind die folgenden Bedingungen äquivalent:

(A1) (Rekursion): Für alle $n \geq 0$

$f(n+d) + q_1 \cdot f(n+d-1) + \ldots + q_d \cdot f(n) = 0$

(A2) $F(z) = \sum_{n=0}^{\infty} f(n) \cdot z^n = \frac{p(z)}{q(z)}$, $p(z) \in Poly(d-1)$

(A3) $\sum_{n \geq 0} f(n) \cdot z^n = \sum_{i=1}^{k} \frac{g_i(z)}{(1-\alpha_i \cdot z)^{d_i}}$ wobei $g_i \in Poly(d_i - 1)$

(A4) $f(n) = \sum_{i=1}^{k} p_i(n) \cdot \alpha_i^n$, $p_i \in Poly(d_i - 1)$ $1 \leq i \leq k$

Beweis:

$V_i := \{f : \mathbb{N} \to \mathbb{C} \mid f \text{ erfüllt } (a_i)\}$ $i = 1, 2, 3, 4$

Jedes V_1 ist ein Vektorraum über $\mathbb{C}$ der Dimension d.

Trick : Aus $V_1 \subseteq V_j$ folgt bereits $V_1 = V_j$

(a) $V_2 \subseteq V_1$: Koeffizientenvergleich für z^{d+n} in:

$q(z) \cdot \sum_{n=0}^{\infty} f(n) \cdot z^n = p(z) \quad (n \geq 0)$

$f(n+d) + q_1 \cdot f(n+d-1) + \ldots + q_d \cdot f(n) = 0$

$V_1 = V_2$

Koeffizient von z^{d+n} liefert Bedingung A1

27.05.05

(b) $V_3 \subseteq V_2$: $\sum_{i=1}^{k} \frac{g_i(z)}{(1-\alpha_i \cdot z)^{d_i}} = \frac{g(z)}{\prod_{i=1}^{k} (1-\alpha_i \cdot z)^{d_i}}$

Grad von $g(z) < d_1 + d_2 + \ldots + d_k = d$

(c) $V_3 \subseteq V_4$

$\frac{1}{(1-\alpha_1 \cdot z)^{d_i}} = \sum_{n=0}^{\infty} \binom{-d_i}{n} \cdot (-\alpha_i \cdot z)^n$

$= \sum_{n=0}^{\infty} \frac{(-d_i) \cdot (-d_1 - 1) \cdot \ \ldots \ \cdot (-d_i - n + 1)}{n!} \cdot (-1)^n \cdot \alpha_i^n \cdot z^n$

$$= \sum_{n=0}^{\infty} \binom{d_i+n-1}{n} \cdot \alpha_i^n \cdot z^n = \sum_{n=0}^{\infty} \binom{d_i+n-1}{d_i-1} \cdot \alpha_i^n \cdot z^n$$

$$g_i(z) = g_0^{(i)} + g_1^{(i)} \cdot z + \ldots + g_{d_i-1}^{(i)} \cdot z^{d_i-1}$$

$$\frac{g_i(z)}{(1-\alpha_i \cdot z)^{d_i}} = \sum_{n=0}^{\infty} \left(\sum_{j=0}^{d_i-1} g_j^{(i)} \cdot \binom{d_i+n-j-1}{d_i-1} \cdot \alpha_i^{n-j} \right) \cdot z^n$$

$$= \sum_{n=0}^{\infty} \underbrace{\left(\sum_{j=0}^{d_i-1} g_j^{(i)} \cdot \alpha_i^{-j} \cdot \binom{n+d_i-j-1}{d_i-1} \right) \cdot \alpha_n^i}_{p_i(n) \cdot \alpha_i^n} \cdot z^n$$

Beispiel: $a_0 = a_1$

$$a_n = a_{n-1} + 2 \cdot a_{n-2} + (-1)^n \quad (n \neq 2)$$

n	0	1	2	3	4	5	6	7
$(-1)^n$	1	-1	1	-1	1	-1	1	-1
a_n	1	1	4	5	14	23	52	97

Die Rekursion ($a_n := 0$ für $n < 0$)

$$n = 1: \; a_1 = a_0 + 2 \cdot a_{-1} + (-1)^1 + [n = 1]$$

$$n = 0: \; 1 = a_0 = (-1)^0 \; \checkmark$$

$$n < 0: \; 0 = (-1)^n \cdot [n \geq 0]$$

$$a_n = a_{n-1} + 2 \cdot a_{n-2} + (-1)^n \cdot [n \geq 0] + [n = 1]$$

$$A(z) = \sum_{n \in \mathbb{Z}} a_n \cdot z^n$$

$$A(z) = \sum_n a_{n-1} \cdot z^n + 2 \cdot \sum_n a_{n-2} \cdot z^n + \sum_{n \geq 0} (-1)^n \cdot z^n + z$$

also $A(z) = z \cdot A(z) + 2 \cdot z^2 \cdot A(z) + \frac{1}{1+z} + z$

$$A(z) \cdot (1 - z - 2 \cdot z^2) = \frac{1+z+z^2}{1+z}$$

$$A(z) = \frac{1+z+z^2}{(1-z-2 \cdot z^2) \cdot (1+z)} = \frac{1+z+z^2}{(1-2 \cdot z) \cdot (1+z)^2}$$

Nach unserem Satz gilt (Eigenschaft A4)

$$a_n = a_1 \cdot 2^n + (a_2 \cdot n + b) \cdot (-1)^n$$

es folgt: $a_1 = \frac{7}{9}$, $a_2 = \frac{1}{3}$, $b = \frac{2}{9}$

$$a_n = \frac{7}{9} \cdot 2^n + (\frac{1}{3} \cdot n + \frac{2}{9}) \cdot (-1)^n$$

1.12 Erzeugende Funktionen von Exponentialtyp

$(a_n)_{n \geq 0}$

$\sum_{n \geq 0} a_n \cdot z^n$

$\sum_{n \geq 0} \frac{a_n}{n!} \cdot z^n$

$$\hat{A}(z) := \sum_{n=0}^{\infty} \frac{a_n}{n!} \cdot z^n$$

exponential erzeugende Funktion der Folge $(a_n)_{n=0}^{\infty}$

Multiplizieren wir $\hat{A}(z)$ mit $\hat{B}(z) = \sum_{n=0}^{\infty} b_n \cdot \frac{z^n}{n!}$:

$$\hat{C}(z) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \frac{a_k}{k!} \cdot \frac{b_{n-k}}{(n-k)!} \right) \cdot z^n = \sum_{n=0}^{\infty} \underbrace{\left(\sum_{k=0}^{n} \binom{n}{k} \cdot a_k \cdot b_{n-k} \right)}_{c_n} \cdot \frac{z^n}{n!}$$

(c_n) heißt Binomialfaltung von (a_n) und (b_n)

Beispiel: $e^{a \cdot z} = \sum_{n=0}^{\infty} \frac{a^n}{n!} \cdot z^n$, $e^{b \cdot z} = \sum_{n=0}^{\infty} \frac{b^n}{n!} \cdot z^n$

$$e^{a \cdot z} \cdot e^{b \cdot z} = \qquad e^{a \cdot z + b \cdot z} = \qquad e^{(a+b) \cdot z}$$

$$\| \qquad\qquad\qquad\qquad \|$$

$$\sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \binom{n}{k} \cdot a^k \cdot b^{n-k} \right) \frac{z^n}{n!} \qquad\qquad \sum_{n=0}^{\infty} (a+b)^n \cdot \frac{z^n}{n!}$$

$$\boxed{(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot a^k \cdot b^{n-k}}$$

Beispiel: $\sum_{n=0}^{\infty} \frac{a^{\underline{k}}}{n!} \cdot z^n = \sum_{n=0}^{\infty} \binom{a}{n} \cdot z^n = (1+z)^a$

Wir benutzen : $(1+z)^{a+b} = (1+z)^a \cdot (1+z)^b$

$$(a+b)^{\underline{n}} = \sum_{k=0}^{n} \binom{n}{k} \cdot a^{\underline{k}} \cdot b^{\underline{n-k}}$$

Beispiel: Derangement-Zahlen : D_n

$$n! = \sum_{k=0}^{n} \binom{n}{k} \cdot D_{n-k} = \sum_{k=0}^{n} \binom{n}{k} \cdot D_k \cdot 1$$

Binomialfaltung von (D_n) und (1) ist $(n!)$

$$\underbrace{\sum_{n=0}^{\infty} n! \cdot \frac{z^n}{n!}}_{\frac{1}{1-z}} = \hat{D}(z) \cdot e^z$$

$$\hat{D}(z) = \frac{e^{-z}}{1-z} = \left(\sum_{n \geq 0} (-1)^n \cdot \frac{z^n}{n!} \right) \cdot \left(\sum_n z^n \right) = \sum_n \left(\sum_{k=0}^{n} \frac{(-1)^k}{k!} \right) \cdot z^n$$

$$\frac{D_n}{n!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!} \text{ , } D_n = n! \cdot \left(\sum_{k=0}^{n} \frac{(-1)^k}{k!} \right)$$

Beispiel: (Bernoulli - Zahlen)

$$1 + 2 + 3 + \ldots + n$$

$$\underline{n + n - 1 + n - 2 + \ldots + 1}$$

$$n \cdot (n+1) \qquad n \cdot \frac{(n+1)}{2}$$

$$1^2 + 2^2 + \ldots + n^2 = \frac{n \cdot (n+1) \cdot (2 \cdot n + 1)}{6}$$

$$1^3 + 2^3 + \ldots + n^3 = \left(\frac{n \cdot (n+1)}{2} \right)^2$$

$$1^k + 2^k + \ldots + n^k = ?$$

$$S_m(n) = 0^m + 1^m + \ldots + (n-1)^m = \sum_{0 \leq k < n} k^m$$

$$S(z) := S_0(n) + S_1(n) \cdot z + S_2(n) \cdot z^2 + \ldots + =$$

$$= \sum_{m=0}^{\infty} S_m(n) \cdot z^m = \sum_{m=0}^{\infty} \sum_{0 \leq k < n} k^m \cdot z^m = \sum_{0 \leq k < n} \sum_{m=0}^{\infty} (k \cdot z)^m = \sum_{0 \leq k < n} \frac{1}{1 - k \cdot z}$$

Aber wie entwickelt man geschickt nach z-Potenzen ?

Anderer Ansatz:

$$\hat{S}(z) \text{ , } \hat{S}(z,n) := \sum_{m=0}^{\infty} S_m(n) \cdot \frac{z^m}{m!} =$$

$$= \sum_{m=0}^{\infty} \sum_{0 \leq k < n} k^m \cdot \frac{z^m}{m!} = \sum_{0 \leq k < n} \sum_{m \geq 0} \frac{(k \cdot z)^m}{m!}$$

$$= \sum_{0 \leq k < n} e^{k \cdot z} = \frac{e^{n \cdot z} - 1}{e^z - 1}$$

Beispiel: (Bernoulli - Zahlen)

$\sum_{j=0}^{m} \binom{m+1}{j} \cdot B_j = [m = 0] \quad \forall m \geq 0$

$\binom{1}{0} \cdot B_0 = 1$

$n = m + 1$

$\sum_{j=0}^{n} \binom{n}{j} \cdot B_j = B_n + [n = 1] \quad n \geq 0$

exponential erzeugende Funktion : $\hat{B}(z)$

$\hat{B}(z) \cdot e^z = \hat{B}(z) + z$

$\hat{B}(z) = \frac{z}{e^z - 1}$

$\Rightarrow \hat{S}(z) = \hat{S}(z, n) = \sum_{m \geq 0} \underbrace{S_m(n)}_{(0^m + 1^m + \ldots + (n-1)^m)} \cdot z^m$

$\hat{S}(z) = \frac{\hat{B}(z)}{z} \cdot (e^{n \cdot z} - 1) = \hat{B}(z) \cdot \frac{e^{n \cdot z} - 1}{z}$

$\hat{S}(z) = (B_0 \cdot \frac{z^0}{0!} + B_1 \cdot \frac{z^1}{1!} + \ldots) \cdot (n \cdot \frac{z^0}{1!} + n^2 \cdot \frac{z^1}{2!} + n^3 \cdot \frac{z^2}{3!} + \ldots)$

$S_m(n) = m! \cdot (B_0 \cdot \frac{n^{m+1}}{(m+1)! \cdot 0!} + B_1 \cdot \frac{n^m}{m! \cdot 1!} + \ldots + B_n \cdot \frac{n}{1! \cdot m!})$

03.06.05

$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$, $\sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}$

1.13 Bemerkung zu anderen Typen von Rekursionen

1. Lineare Rekursionen , Konstante Koeffizienten.

aber: inhomogen :

$f(n + d) + g_1 \cdot f(n + d - 1) + \ldots + q_d \cdot f(n9 = g(n) \quad (*) \qquad q_i \; konstant$

Allgemeine Lösung von $(*) =$

(partikuläre Lösung) + (allgemeine Lösung der homogenen Rekursion)

Möglichkeit : partikuläre Lösung erraten oder aus einem Ansatz mit unbestimmten Koeffizienten ermitteln, z.b.

Form von $g(n)$	Ansatz
α^n	$k \cdot \alpha^n$
Polynom	Polynom des gleichen Grades

falls α keine Nullstelle von $gR(z)$

Beispiel: $f_{n+2} - f_{n+1} - f_n = n^2$

Ansatz: $f_n = a \cdot n^2 + b \cdot n + c$

$$\begin{array}{l} a \cdot (n+2)^2 + b \cdot (n+2) + c \\ -a \cdot (n+1)^2 - b \cdot (n+1) - c \\ -a \cdot n^2 - b \cdot n - c \\ \hline -a \cdot n^2 + (2 \cdot a - b) \cdot n + 3 \cdot a + b - c = n^2 \end{array}$$

$a = -1$, $b = 2 \cdot a = -2$, $c = 3 \cdot (-1) - 2 = -5$

$f_n = -n^2 - 2 \cdot n - 5$

Allgemeine Lösung :

$A \cdot \Phi^n + B \cdot \hat{\Phi}^n - n^2 - 2 \cdot n - 5$

A, B unbestimmte Zahlen, die aus den Anfangsbedingungen bestimmt werden müssen.

Variable Koeffizienten

Keine allgemeine Lösung.

$a(n) \cdot f(n) = b(n) \cdot f(n-1) + c(n) \qquad (n \geq 1)$

$a(n)$, $b(n)$, $c(n)$ bekannte Koeffizienten

$f(n)$ gesuchte Folge

Trick: Summationsfaktors

Multipliziere beide Seiten mit

$F(n) = \frac{\prod_{i=1}^{n-1} a(i)}{\prod_{j=1}^{n} b(j)}$ alle $b(n) \neq 0$

Dies Verändert die Rekursion

$(y(n) := b(n+1) \cdot F(n+1) \cdot f(n))$

$\Rightarrow \boxed{y(n) = y(n-1) + F(n) \cdot c(n)}$

$y(n-1) = b(n) \cdot F(n) \cdot f(n-1) = F(n) \cdot (a(n) \cdot f(n) - c(n))$

$= y(n) - F(n) \cdot c(n)$

also $y(n) = y(0) + \sum_{i=1}^{n} F(i) \cdot c(i)$

$b(n+1) \cdot F(n+1) \cdot f(n) = b(1) \cdot F(1) \cdot f(0) + \sum_{i=1}^{n} F(i) \cdot c(i)$

$f(n) = \frac{f(0) + \sum_{i=1}^{n} F(i) \cdot c(i)}{b(n+1) \cdot F(n+1)}$

Beispiel: Quicksort , Q_n

$i : Q_{i-1} + Q_{n-i}$

$Q_n = n + 1 + \frac{1}{n} \cdot \sum_{i=1}^{n} (Q_{i-1} + Q_{n-i}) = n + 1 + \frac{1}{n} \cdot 2 \cdot \sum_{i=0}^{n-1} Q_i \qquad (n > 0)$

$n \cdot Q_n = n^2 + n + 2 \cdot \sum_{i=0}^{n-1} Q_i \qquad (n > 0)$

$(n-1) \cdot Q_{n-1} = (n-1)^2 + (n-1) + 2 \cdot \sum_{i=0}^{n-2} Q_i \qquad (n > 1)$

Subtrahieren:

$n \cdot Q_n - (n-1) \cdot Q_{n-1} = 2 \cdot n + 2 \cdot Q_{n-1} \qquad (n > 1)$

Also Rekursion:

$Q_0 = 0$, $n \cdot Q_n = (n+1) \cdot Q_{n-1} + 2 \cdot n$

$\Rightarrow Q_n = \frac{Q_0 + \sum_{i=1}^{n} F(i) \cdot 2 \cdot i}{(n+2) \cdot F(n+1)}$

mit

$F(n) = \frac{\prod_{i=1}^{n} a(i)}{\prod_{j=1}^{n} b(j)} = \frac{1 \cdot 2 \cdot \ \ldots \ \cdot (n-1)}{2 \cdot 3 \cdot \ \ldots \ \cdot ((n-1) \cdot n \cdot (n+1))} = \frac{1}{n \cdot (n+1)}$

$Q_n = \frac{1}{(n+2) \cdot \frac{1}{(n+1) \cdot (n+2)}} \cdot 2 \cdot \sum_{i=1}^{n} \frac{1}{i \cdot (i+1) \cdot i} = (n+1) \cdot \sum_{i=1}^{n} \frac{1}{i+1}$

$$= 2 \cdot (n+1) \cdot (\underbrace{H_{n+1}}_{\substack{\text{Harmonische Zahl} \\ \approx \ln(n+1)}} - 1)$$

Kapitel 2

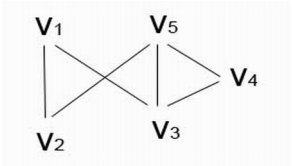
Graphen und Netzwerke

Ein Graph ist ein Paar $(V, E) = G$, (vertices , edges)

V, E endlich, $E \subseteq \begin{pmatrix} V \\ 2 \end{pmatrix}$, z.B.

$V = \{v_1, v_2, \ldots, v_5\}$

$E = \{\{v_1, v_2\}, \{v_1, v_3\}, \{v_3, v_4\}, \{v_3, v_5\}, \{v_2, v_5\}, \{v_4, v_5\}\}$



Elemente von V: Punkte, Ecken, Knoten

Elemente von E: Kanten

Bezeichnung:

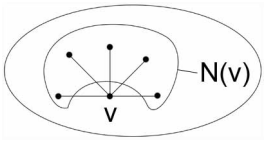
$v_1\ v_2$ statt $\{v_1, v_2\}$

Sprechweise: v_1 und v_2 sind adjazent oder benachbart, verbunden

v_1 inzidiert mit der Kante $v_1\ v_2$

$N(v) := \{w \in V \mid v \text{ und } w \text{ sind in } G \text{ benachbart}\}$

heißt die Menge der Nachbarn von G



Grad von v:

$d(v) := |N(v)|$

$d_G(v) \quad N_G(v)$

Satz: In jedem Graph ist die Anzahl der Punkte ungeraden Grades gerade

(„Handschlag Lemma“)

Beweis: Wir stellen einen gegebenen Graphen G dar durch seine Inzidenzmatrix:

$$\begin{array}{c} \cdots\ e\ \cdots \\ \vdots \\ v \quad \cdots \quad [v \in e] \quad \cdots \\ \vdots \end{array} \quad |V| \times |E| - \text{Matrix } B(G)$$

Doppelte Anzahlung:

Summe der Zeile $v = d(v)$

Summe der Zeilensummen $= \sum_{v \in V} d(v)$

Alle Spaltensummen sind 2

$\Rightarrow \sum_{v \in V} d(v)$ ist eine gerade Zahl.

$\Rightarrow$ die Anzahl der ungeraden Summanden ist gerade.

Bemerkung: Jeder Graph hat zwei Punkte gleichen Grades.

$n = |V|$.

Mögliche Grade $= 0, 1, 2, \ldots, n-1$, aber es kann nicht gleichzeitig ein Punkt von $Grad\ 0$ und einer von $Grad\ n-1$ auftreten

Beispiel: Peter hat bemerkt, dass jeder seiner 25 Mitschüler eine unterschiedliche Zahl von Freunden hat (in seiner Klasse).

Wie viele Freunde hat Peter selbst ? (es gibt nur 2 Lösungen).

2.1 Definition

Kantenfolge:

$v_0, e_1, v_1, e_2, v_2, \ldots, v_{k-1}, e_k, v_k$

$v_0, \ldots, v_k \in V$, $e_1, \ldots, e_k \in E$

$e_i = v_{i-1}\ v_i$, $1 \leq i \leq k$

Kantenzug:

Keine Kante mehrfach

Kantenfolge mit $e_i \neq e_j$ für $i \neq j$

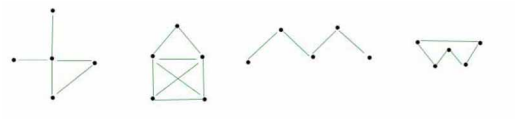
Weg:

kein Punkt mehrfach

Kantenzug mit $v_i \neq v_j$ für $i \neq j$ „geschlossen“ bedeutet : $v_0 = v_k$

Kreis:

geschlossener Kantenzug mit $v_i \neq v_j$, für $0 \leq i < j \leq k-1$

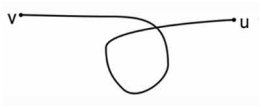


Hamiltonweg bzw Hamiltonkreis

Alle Punkte von G werden durchlaufen.

10.06.05

Graph G heißt zusammenhängend, falls zu je zwei Punkten $v, u \in V$ eine Kantenfolge von v nach u existiert.



Ist G nicht zusammenhängend, so zerfällt G in sogenannte Zusammenhangskomponenten, d.h. maximal zusammenhängende Teilgraphen von G.

(formal: Def. Äquivalenzrelation auf V:

$u \sim v \leftrightarrow$ es ex. $(u - v)$- Weg in G

$u \sim v \sim w$

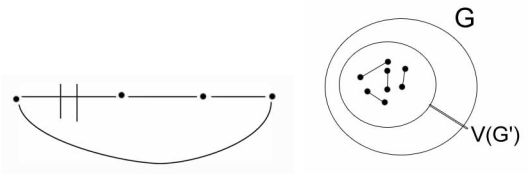
Äquivalenzklassen: Zusammenhangskomponenten).

G Graph. G' Teilgraph von G , falls

$V(G') \subseteq V(G)$, $E(G') \subseteq E(G)$

G' heißt induzierter Teilgraph, falls

$V(G') \subseteq V(G)$ und $E(G') = E \cap \binom{V(G')}{2}$



2.2 Königsberger Brückenproblem

Frage: Kann man einen Spaziergang machen, sodas man über jede Brücke genau einmal geht und zum Anfangspunkt zurückkehrt ?

Leonhard Euler hat diese Frage in viel größerer Allgemeinheit gelöst.

Ein geschlossener Eulerscher Kantenzug heißt Euler-Tour

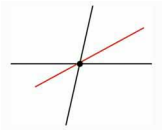
G heißt Eulersch, falls G eine Euler-Tour besitzt.

Satz: (L. Euler, 1736)

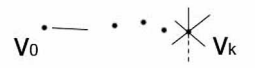
Ein zusammenhängender Graph ist Eulersch genau dann, wenn alle seine Grade gerade sind.
Beweis:

(a) G sei Eulersch, $v \in V$ beliebig.

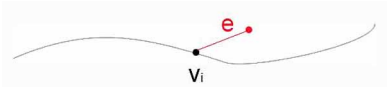
Wird v bei Durchlaufung der Euler-Tour k-mal besucht, so ist $d(v) = 2 \cdot k$



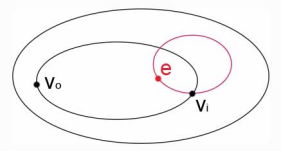
(b) Nun seien alle Grade von G gerade, $v_0, e_1, v_1, e_2, \ldots, v_{k-1}, e_k, v_k$ sei ein Kantenzug maximaler Länge (k) in G. Dann muss $v_0 = v_k$ sein, denn andernfalls wäre eine ungerade Anzahl der Kanten $e_1, \ldots, e_k$ mit v_k inzident und der Kantenzug könnte verlängert werden.



Angenommen, es gibt noch eine Kante $e \in E$, die nicht zu $e_1, \ldots, e_k$ gehört. Da G zusammenhängend ist, können wir davon ausgehen, dass e mit einem der Punkte $v_0, \ldots, v_{k-1}$ inzidiert, etwa mit v_i.



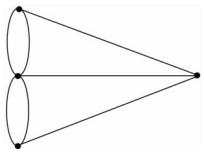
Nun setzen wir v_i, e zu einem Kantenzug maximaler Länge in $G' = G - \{e_1, \ldots, e_k\} = (V(G), E \backslash \{e_1, \ldots, e_k\})$ fort, etwa $v_i, e, u_1, f_1, u_2, \ldots, u_{l-1}, f_{l-1}, u_l$. Weil in G' ebenfalls alle Grade gerade sind, muss $u_l = v_i$ sein.



Der Kantenzug $v_0, e_1, \ldots, e_i, v_i, e, u_1, f_1, u_2, \ldots, f_{l-1}, v_i, e_{i+1}, v_{i+1}, \ldots, e_k, v_0$ hat dann Länge $k + l > k$

Widerspruch zur Maximalität von k.

In Königsberg:



Definition: Ein zusammenhängender Graph ohne Kreis heißt ein Baum, ein Graph ohne Kreise heißt ein Wald.

Satz: Ein Baum mit n Knoten hat immer $n-1$ Kanten.

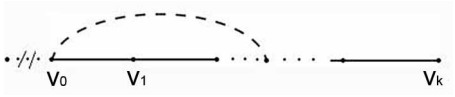
Beweis: Induktion nach n.

$n=1$:

$n=2$:

$n-1 \to n$: Es sei $T=(V,E)$ ein Baum mit $|V|=n$.

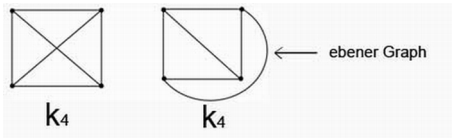
In T sei $v_0, v_1, \ldots, v_k$ ein Weg maximaler Länge. Dann sind v_0 und v_k Punkte von $Grad\ 1$ in T.



Wir streichen v_0 und die Kante $v_0\ v_1$ aus T. Dann entsteht ein Kreisfreier, zush. Graph (also ein Baum) mit $n-1$ Punkten und (Ind. Annahme) $n-2$ Kanten. $\Rightarrow T$ hat $n-1$ Kanten.

2.3 Planare Graphen

Kann der Graph G so in der Ebene gezeichnet werden, dass die Linien, die die Kanten des Graphen darstellen, nur Ecken (der Graphen) als gemeinsame Punkte haben, so heißt G planar.
Eine solche Zeichnung nennen wir einen ebenen Graphen (plane) oder Landkarte (map)



Schneidet man die Ebene entlang der Kanten eines Graphen auf, so zerfällt sie in endlich viele Stücke (die Länder von G), von denen genau eines unbeschränkt ist.

Satz: (Eulerscher Polyedersatz)
Ein ebener Graph mit n Punkten, m Kanten und f Ländern, der zush. ist, erfüllt die Beziehung.

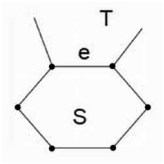
$$\boxed{n-m+f=2}$$

Beweis: Induktion nach f

$f=1$: G ist ein Baum

$n-m+f=n-(n-1)+1=2$ ✓

$f>1$: G enthält einen Kreis, sodas jede Kante des Kreises 2 Länder von G begrenzt. Entfernen wir eine Kante e dieses Kreises,



so werden beide Länder, die e begrenzt, zu einem Land verschmolzen.

$G' = G - e$ erfüllt also die Gleichungen $n' = n$, $m' = m - 1$, $f' = f - 1$

$\Rightarrow$ (Ind. Annahme) $2 = n' - m' + f'$

$$= n - (m-1) + (f-1)$$

$$= n - m + f$$

Folgerung:

(1) Wie viele Kanten kann ein planarer Graph haben ?

$3 \cdot n - 6$

f_i sei die Anzahl der Flächen mit i Ecken (Kanten) , $i = 3, 4, 5, \ldots$

$f = f_3 + f_4 + f_5 + \ldots$

$2 \cdot m = 3 \cdot f_3 + 4 \cdot f_4 + \ldots = \sum_{i \geq 3} i \cdot f_i \geq 3 \cdot f_3 + 3 \cdot f_4 + \ldots = 3 \cdot f$

(G habe keine „ Brücke “, d.h. keine Kanten e, sodas $G - e$ nicht zush. ist)

$2 \cdot m \geq 3 \cdot f$, $f \leq \frac{2}{3} \cdot m$

$n - m + f = 2$, $m = n + f - 2 \leq n + \frac{2}{3} \cdot m - 2$

$\frac{1}{3} \cdot m \leq n - 2$, $m \leq 3 \cdot n - 6$

Ist k_5, der vollständige Graph auf 5 Punkte, planar ?

$n = 5$, $m = 10$, $15 - 6 = 9$

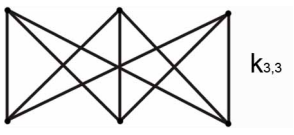
(2) Ein ebener Graph ohne Dreiecke erfüllt $m \leq 2 \cdot n - 4$

$f = f_4 + f_5 + \ldots$

$2 \cdot m = 4 \cdot f_4 + 5 \cdot f_5 + \ldots \geq 4 \cdot f$

$m = n + f - 2 \leq n + \frac{m}{2} = 2$

$\frac{m}{2} \leq n - 2$, $m \leq 2 \cdot n - 4$

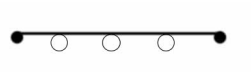


$m = 9$, $n = 6$, $2 \cdot n - 4 = 8$

17.06.05

Satz von Kuratowski

G ist planar g.d.w. G keine Unterteilung von $k_{3,3}$ oder k_5 enthält.



Beispiel: (Confed. Cup)

BMW 1983:

Oberfläche eines Fußballs besteht aus schwarzen 5-Ecken und weißen 6-Ecken.

An die Seiten jedes 5-Ecks grenzen nur 6-Ecke, während an die Seiten jedes 6-Ecks abwechselnd 5-Ecke und 6-Ecke grenzen.

Was ist die Anzahl der 5-Ecke und 6-Ecke?

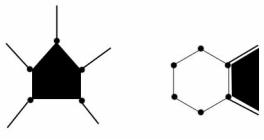
$n - m + f = 2$ $\quad$ f_5: Anzahl der 5-Ecke

$f = f_5 + f_6$ $\quad$ f_6: Anzahl der 6-Ecke

$2 \cdot m = 5 \cdot f_5 + 6 \cdot f_6$

$5 \cdot f_5 = 3 \cdot f_6$

$5 \cdot f_5 = n$



Einsetzen und nach f_5 auflösen:

$f_6 = \frac{5}{3} \cdot f_5$

$m = \frac{5}{2} \cdot f_5 + 3 \cdot f_6 = \frac{5}{2} \cdot f_5 + 5 \cdot f_5 = \frac{15}{2} \cdot f_5$

$2 = 5 \cdot f_5 - \frac{15}{2} \cdot f_5 + f_5 + \frac{5}{3} = f_5 \cdot \frac{30-45+6+10}{6} = f_5 \cdot \frac{1}{6}$

$\Rightarrow f_5 = 12 \quad f_6 = \frac{5}{3} \cdot 12 = 20$

2.4 Matchings

$G = (V, E)$ Graph

$M \subseteq E$ heißt Matching in G, falls gilt:

$e, e' \in M$, $e \neq e' \Rightarrow e \cap e' = \emptyset$

$\nu(G)$

$\nu(G) := max\{|M| \mid M$ Matching in $G\}$

$W \subseteq V$ heißt Knotenüberdeckung von G (Vertex Cover) g.d.w.

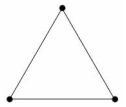
$e \cap W \neq \emptyset$ für alle $e \in E$

$\tau(G) := min\{|W| \mid W$ Knotenüberdeckung von $G\}$

Es gilt stets:

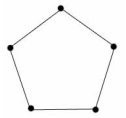
$\nu(G) \leq \tau(G)$

Wann gilt Gleicheit ?



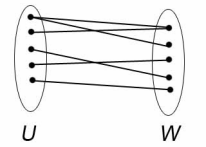
$\nu = 1$, $\tau = 2$

Analog bei ungeraden Kreisen



$n = 2 \cdot k + 1$, $\nu = k$, $\tau = k + 1$

Definition: $G = (V, E)$ heißt bipartit, falls G keine ungeraden Kreise enthält.
Äquivalent: Es gibt eine Partition $V = U \dot{\cup} W$ von V in zwei nicht leere Teilmengen, sodas jedes $e \in E$ genau einen Endpunkt in U und einen in W hat.

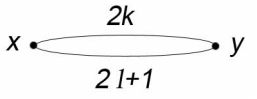


Ist G zusammenhängend und bipartit, so findet man eine Zerlegung $V = U \dot{\cup} W$ mit den gewünschten Eigenschaften wie folgt:

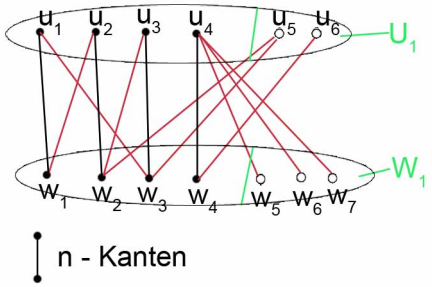
$x \in V$ sei bel., fest. x gehört zu U.

Punkte aus $N(x)$ müssen zu W gehören.

$y \in V$ gehört zu $\begin{cases} U, & \text{falls es einen Weg gerader Länge } x \text{ nach } y \text{ gibt} \\ W, & \text{falls es einen Weg ungerader Länge } x \text{ nach } y \text{ gibt} \end{cases}$



Satz von König:
Ist G bipartit, so gilt : $\nu(G) = \tau(G)$
Beweis: *Später*
Satz: Es sei $G = (V, E)$ bipartit, $V = U \dot{\cup} W$ die zugehörige Partition, M ein Matching in G.
Es seien U_1 bzw. W_1 die Punkte in U bzw. W, die nicht Endpunkte von Matching-Kanten sind.

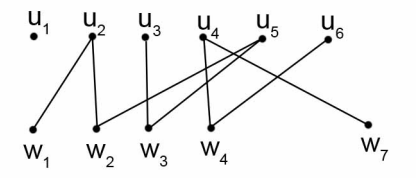


Ferner sei $F \subset G$ ein maximaler Wald (maximal als Teilgraph) mit folgenden Eigenschaften:

(∗) Jeder Punkt w von F in W hat $Grad\ 2$ und inzidiert (in F) mit einer M-Kante.

(∗∗) Jede Komponente von F enthält einen Punkt von U_1.

Dann gilt: M ist Maximum-Matching ($|M| = \nu(G)$) g.d.w. kein Punkt aus W_1 zu einem Punkt von F adjazent ist.



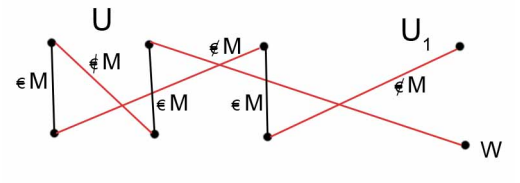
Beweis:

(a) „ $\Rightarrow$ “ Es sei M ein Maximum Matching, $w \in W_1$. Angenommen, es wäre eine Kante $w\ u$ in E mit $u \in V(F)$.

Wir betrachten die F-Komponenten von u. Nach $(**)$ gibt es einen Weg, der aus F-Kanten besteht, und u mit U_1 verbindet.

Dessen Kanten gehören abwechselnd zu M und nicht zu M. Wir nehmen die Kanten des Wegs, die nicht zu M gehören zum Matching hinzu und entfernen die Kanten aus M, die zum Weg gehören.

Das neue Matching M' hat genau so viele Kanten wie M und kann durch $u\ w$ erweitert werden. ↯



(Beweis Satz von König)

(b) Wir nehmen an: Kein Punkt aus W_1 ist mit F adjazent.

Es sei $X := U \backslash V(F)$, $Y := V(F) \cap W$

Wir zeigen: $|X \cup Y| = |M|$ und jede Kante von G ist mit $X \cup Y$ inzident

(dann ist $|X \cup Y| = \tau(G) = \nu(G) = |M|$)

zunächst $X \cup Y \subseteq \bigcup M$

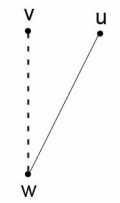
Ferner: Es gehören nicht beide Endpunkte einer M-Kante zu $X \cup Y$

(klar nach Eigenschaft $(*)$)

Es sei nun $u\ w \in E$ mit $u \in U$, $w \in W$.

Angenommen $\{u, w\} \cap (X \cup Y) = \emptyset \Rightarrow u \in V(F)$, $w \notin V(F)$.

Nach Voraussetzung kann w nicht zu W_1 gehören, d.h. es gibt eine Kante $v\ w \in M$ mit $v \in U$. Dann könnte man F erweitern, indem man die Kanten $u\ w$ und $w\ v$ zu F hinzufügt. Widerspruch zur Maximalität von F.



22.06.05

2.5 Die Ungarische Methode

Schritt 0: Der bipartite Graph $G = (U \dot{\cup} W, E)$ ist gegeben, außerdem ein Matching M von G.

Schritt 1: (Markierung)

(1,0) Jeder Punkt in U_1 bekommt die Marke „0“.

(1,1) Wenn es keine noch nicht durchgesehene Marken gibt, so gehen wir zu Schritt 3.

(1,2) Die Marke von v, $v \in U$, wird wie folgt durchgesehen: Für jede Kante $v\ w \in M$ erhält w die Marke „v“, es sei denn w ist bereits markiert.
zurück zu (1,1)

(1,3) Die Marke von v,$v \in W$, wird wie folgt durchgesehen: Ist $v \in W_1$ so gehen wir zu Schritt 2.
Ist $v \in W \backslash W_1$,so suchen wir die Kante $u\ v \in M$ und geben u die Marke „v“.

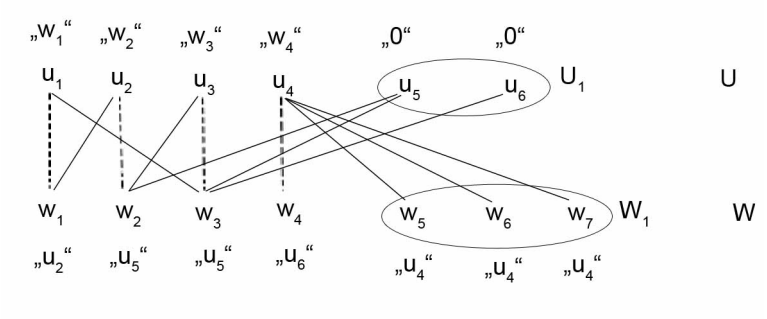
Schritt 2: (Vergrößerung)

Wir finden bzgl. der Kanten von M alternierenden Weg P von $v,\ v \in W_1$, nach U_1 durch „zurückverfolgen“. Ist die Marke von v „u“, so ist $v\ u \in E$ und u ist der zweite Punkt des Weges. Der nächste Punkt ist die Marke von u. Der letzte Punkt hat die Marke „0“.
Mit $E(P) :=$ (Menge der Kanten von P) bilden wir:
$M' := (M \cup E(P)) \backslash (M \cap E(P))$ und $M := M'$.
Alle Marken werden gelöscht.
zurück zu (1,0)

Schritt 3: Stop: M ist ein Maximum Matching.

Was ist dann F ?

$V(F)$: Alle markierten Punkte $u, w \in V(F) :\ u\ w \in E(F)$
$\Leftrightarrow$ Marke von $u =$ „w“ oder
Marke von $w =$ „u“



Folgerung:

Satz von Hall:

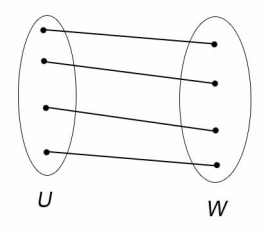
Es sei $G = (U \dot\cup W, E)$ bipartit.

Für $X \subseteq U$ sei $N(X) := \{w \in W \mid$ es ex. ein x $w \in E$, $x \in X\}$

Dann gilt:

$\nu(G) = |U| \Leftrightarrow$ Für alle $X \subseteq U$:

$|N(X)| \geq |X|$ (Hall-Bedingung)

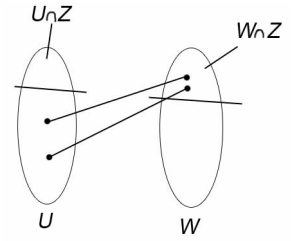


Notwendigkeit der Hall-Bedingung: Klar!

Hinreichend: Es gelte die Hall-Bedingung.

Angenommen: $\nu(G) < |U|$

Nach Satz von König ex. eine Knotenüberdekung Z mit $|Z| = |\nu(G)| < |U|$.



$N(U \backslash Z) \subseteq (W \cap Z)$

$X := U \backslash Z$

$|X| - |N(X)| \geq |X| - |W \cap Z| = |U \backslash (U \cap Z)| - |W \cap Z|$

$= |U| - |U \cap Z| - |W \cap Z| = |U| - |Z| > 0$

$|X| > |N(X)|$

Widerspruch zur Hall-Bedingung.

2.6 Gewichtete Matchings

Gegeben: $G = (U \dot\cup W, E)$ bipartit

$c : E \to R$ Kostenfunktion.

$M \subseteq E$: $c(M) := \sum_{e \in M} c(e)$ Kosten von M.

Problem: Finde ein Matching M in G mit $|M = \nu(G)|$ und $c(M)$ minimal !

Vereinfachungen:

(1) G sei vollständig bipartit.

Ist z.B. $u\ w \in E,\ u \in U,\ w \in W$, so nehmen wir $u\ w$ hinzu und setzen $c(u\ w) = N,\ N$ „sehr groß“, etwa $N > \sum_{e \in E} |c(e)|$.

(2) $|U| = |W|$

c kann dann als quadratische Matrix angegeben werden, etwa

$U = \{u_1, \ldots, u_n\}$, $W = \{w_1, \ldots, w_n\}$

$c_{ij} = c(u_i\ w_j)$

Ein Maximum Matching kann nun durch eine Transversale für C bzw. durch eine Permutation $\pi \in S_n$ beschrieben werden.

Jedes Matching M mit $|M| = n$ kann durch $\pi \in S_n$ beschrieben werden.

vermöge:

$u_i\ w_j \in M \Leftrightarrow j = \pi(i)$

Statt $c(M)$ können wir auch $c(\pi)$ schreiben.

$$C = \begin{array}{c} \\ U_1 \\ \\ \vdots \\ \\ U_5 \end{array} \begin{array}{c} \begin{array}{ccccc} W_1 & & & & W_5 \end{array} \\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 6 & 8 & 1 \\ 3 & 6 & 0 & 3 & 6 \\ 4 & 8 & 3 & 7 & 2 \\ 5 & 1 & 6 & 2 & 7 \end{pmatrix} \end{array} \qquad \begin{array}{c} \begin{array}{ccccc} -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & +\frac{1}{2} \end{array} \\ \begin{pmatrix} \boxed{0} & 1 & 2 & 2 & 4 \\ 1 & 3 & 5 & 6 & \boxed{0} \\ 3 & 6 & \boxed{0} & 2 & 6 \\ 2 & 6 & 1 & 4 & 0 \\ 4 & \boxed{0} & 5 & 0 & 6 \end{pmatrix} \end{array} \begin{array}{l} +\frac{1}{2} \\ -\frac{1}{2} \\ +\frac{1}{2} \\ -\frac{1}{2} \\ +\frac{1}{2} \end{array}$$

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 3 & 5 & 7 & 0 \\ 3 & 6 & 0 & 3 & 6 \\ 2 & 6 & 1 & 5 & 0 \\ 4 & 0 & 5 & 1 & 6 \end{pmatrix} Z\ R \qquad \begin{pmatrix} \boxed{0} & 1 & 2 & 2 & 5 \\ 0 & 2 & 4 & 5 & \boxed{0} \\ 3 & 6 & \boxed{0} & 2 & 7 \\ 1 & 5 & 0 & 3 & 0 \\ 4 & \boxed{0} & 5 & 0 & 7 \end{pmatrix}$$

$$\begin{pmatrix} \boxed{0} & 1 & 2 & 2 & 4 \\ 1 & 3 & 5 & 6 & \boxed{0} \\ 3 & 6 & \boxed{0} & 2 & 6 \\ 2 & 6 & 1 & 4 & 0 \\ 4 & \boxed{0} & 5 & 0 & 6 \end{pmatrix} S\ R \qquad \begin{pmatrix} \boxed{0} & \boxed{0} & 2 & 1 & 5 \\ \boxed{0} & 1 & 4 & 4 & \boxed{0} \\ 3 & 5 & \boxed{0} & 1 & 7 \\ 1 & 4 & 0 & 2 & \boxed{0} \\ 5 & \boxed{0} & 4 & \boxed{0} & 8 \end{pmatrix}$$

Lemma: Es sei C eine Kostenmatrix, $x, y \in \mathbb{R}^n$.

$C' = (c'_{ij})$ entsteht wie folgt:

$c'_{ij} = c_{ij} + x_i + y_j$

Dann gilt: π^* ist optimal für c g.d.w. π optimal für c'

Beweis: $c(\pi^*) = \sum_{i=1}^{n} c'_{i,\pi^*(i)}$

$$c'(\pi^*) = \sum_{i=1}^{n} c'_{i,\pi^*(i)} = \sum_{i=1}^{n} (c_{i,\pi^*(i)} + x_i + y_{\pi^*(i)})$$

$$= \underbrace{\sum_{i=1}^{n} c'_{i,\pi^*(i)}}_{c(\pi^*)} + \left(\sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i \right)$$

Die Kosten jedes Matchings ändert sich nur um eine Konstante $\left(\sum_{i=1}^{n} (x_i + y_i) \right)$

24.06.05

Bemerkung: Unser Problem wird oft „Zuordnungsproblem “ genannt.

(engl. Assignment Problem)

Konstruieren wir die Folge $C = C^{(0)}, C^{(1)}, C^{(2)}, \ldots, C^t$ von Kostenmatrizen, sodas $C^{(i+1)}$ aus $C^{(i)}$ durch Modifikation der Zeilen und Spalten wie im Lemma entsteht.

(1) $C^{(1)}$ entsteht aus C, indem zuerst von jeder Zeile i $\underbrace{\min_j c_{ij}}_{-x_i}$ subtrahiert wird und dann von jeder Spalte $\underbrace{\min_i (c_{ij} - \min_l c_{il})}_{-y_j}$ subtrahiert wird.

(Zeilen- und Spaltenreduktion)

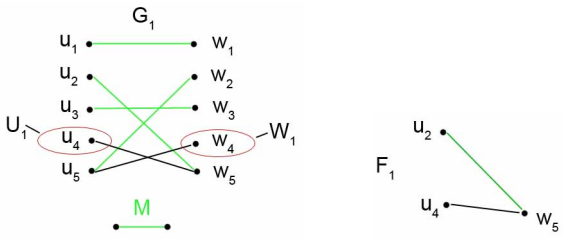
Dann ist $c^{(1)}_{ij} \geq 0$ für alle i, j und jede Zeile und jede Spalte enthält mindestens eine 0.

(2) $G_1 := (U \cup W, E_1)$ mit $u_i\ w_j \in E_1 \Leftrightarrow c^{(1)}_{ij} = 0$

Konstruiere mit der ungarischen Methode ein Max. Matching M und ein Min. Vertex Cover $X \cup Y$ für G_1.

Falls $|M| = n$, so ist $c^{(1)}(M) = 0$ und M ist optimal (für $C^{(1)}$ und damit auch für C).

Ist $|M| < n$, so betrachten wir $X \cup Y$



$$Y = W \cap V(F)\ ,\ X = U \backslash V(F)$$

$$Y = \{w_5\}\ ,\ X = \{u_1, u_3, u_5\}$$

$m := \min\{c^{(1)}_{ij} \mid u_i \notin X,\ w_j \notin Y\} > 0$

Addiere $\frac{m}{2}$ zu allen Zeilen i mit $u_i \in X$ und zu allen Spalten j mit $w_j \in Y$. Subtrahiere $\frac{m}{2}$

von den übrigen Zeilen und Spalten.
(Äquivalent: Addiere m zu dem $c_{ij}^{(1)}$ mit $u_i \in X$ und $w_j \in Y$. Subtrahiere m von den $c_{ij}^{(1)}$mit $u_i \notin X$ und $w_j \notin Y$).
Die neue Matrix sei $C^{(2)}$.

(3) Nun bilden wir $G_2 = (U \cup W, E_2)$ analog:
$u_i\ w_j \in E_2 \Leftrightarrow c_{ij}^{(2)} = 0$
Eigenschaften von G_2:

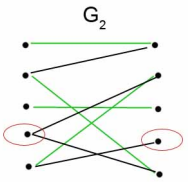
(i) $M \subseteq E_2$ (vgl. Konstruktion des Vertex Covers $X \cup Y$) $\nu(G_2) \geq \nu(G_1)$

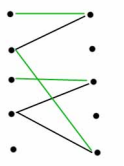
(ii) $E(F_1) \subseteq E_2$, wobei F_1 der Wald ist, den die Ungarische Methode in G_1 konstruiert hat. (Nur solche Kanten gehören zu $E_1 \backslash E_2$, deren Endpunkte in X und Y liegen. Aber $X = U \backslash V(F_1)$.)

(iii) Es gibt eine Kante $u_j\ w_k \in E_2$ mit $u_j \notin X$, $w_k \notin Y$, also $u_j \in V(F_1)$, $w_k \in W \backslash V(F_1)$

Nun erweitern wir F_1 zu einem max. Wald F_2 in G_2 mit Eigenschaft $(*)$ und $(**)$. Falls $\nu(G_2) = \nu(G_1)$, so ist M ein max. Matching für G_2 und $W \cap V(F_2)$ enthält w_k (nach (iii)), also $|W \cap V(F_2)| > |W \cap V(F_1)|$

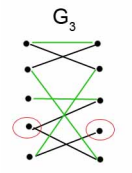
(4) Analog erzeugen wir $C^{(3)}, C^{(4)}, \ldots$
Der Algorithmus terminiert, sobald der Graph G_k ein perfektes Matching besitzt. $(\nu(G_k) = n)$.
Aber $\nu(G_{i+n}) > \nu(G_i)$, denn $|W \cap V(F_j)|$ kann höchstens $(n-1)$-mal in Folge größer werden.
$\Rightarrow$ Anzahl der Iterationen ist höchstens $(n-1) \cdot n + 1 \leq n^2$





$Y = \{w_1, w_3, w_5\}$

$X = \{u_5\}$



$C^{(i)} \rightarrow C^{(i+1)}$

$\sum_{k,l} c_{kl}^{(i)} > \sum_{k,l} c_{kl}^{(i+1)}$

Falls G nicht bipartit ist:
Berechnung von $\nu(G)$ ist in polynomialer Zeit möglich (Edmonds' Matching Algorithmus). Berechnung von $\tau(G)$ ist NP-schwer.

Wir zeigen den

1-Faktor-Satz von Tutte

Es sei $G = (V, E)$ ein Graph.

G besitzt ein perfektes Matching g.d.w.

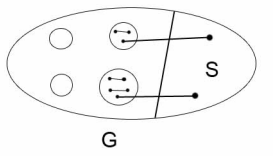
$q(G - S) \leq |S|$ für alle $S \subseteq V \quad (*)$

($q(G - S) =$ Anzahl der ungeraden Komponenten von G)

Die Tuttsche Bedingung ist sicher notwendig: Angenommen, G besitzt ein perfektes Matching, $S \subseteq V(G)$ von jeder ungeraden Komponente aus.

$G - S$ muss dann eine Matching-Kante nach S führen.

$\Rightarrow |S| \geq q(G - S)$



Beweis: (L. Lovász)

Angenommen, es ex. ein G, das die Tutte-Bedingung erfüllt, aber kein perfektes Matching besitzt

$\underset{S=\emptyset}{\Rightarrow} |V(G)| = 2 \cdot s, \ s \in \mathbb{N}$

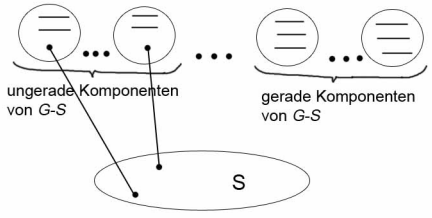
Wir fügen zu G Kanten hinzu bis $\nu(G + e) = s$ für alle $e \in \binom{V}{2} \backslash E(G), \ \nu(G) < s$

G ist weiter ein Gegenbeispiel.

Wir betrachten

$S := \{x \in V(G) \mid d_G(x) = |V(G)| - 1\}$

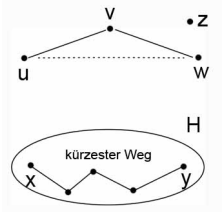
Behauptung: Alle Komponenten von $G - S$ sind vollständige Graphen.



01.07.05

Es sei H eine Komponente von $G - S$

Wir zeigen: $u, v, w \in V(H)$ mit $u\ v \in E, \ v\ w \in E$, so ist auch $u\ w \in E$



Angenommen, $u\ w \notin E$.

Da $G + u\ w$ ein perfektes Matching M_1 besitzt, G aber nicht, muss $u\ w \in M_1$ sein. Zu v ex (nach

Def. von S) ein Punkt z mit $z \notin S,\ v\ z \notin E$.

M_2 sei ein perfektes Matching von $G + v\ z$;

$M_1' := M_1 \backslash \{u\ w\},\ M_2' := M_2 \backslash \{v\ z\}$ $\quad$ $M_1',\ M_2' \subseteq E$

Wir betrachten

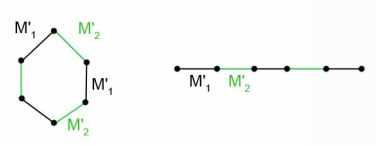
$M_1' \oplus M_2' := (M_1' \backslash M_2') \cup (M_2' \backslash M_1')$

$G' = (V, M_1' \oplus M_2')$

Wie sehen die Komponenten von G' aus?

- isolierte Punkte
- Wege - gerade Kantenanzahl

  $\rangle$ alternierend bzgl. M_1' und M_2'
- Kreise - gerade

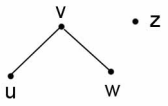


Unmöglich, da die M_1' - Kanten dieser Komponente und die übrigen M_2' - Kanten ein perfektes Matching bilden würden.

Wir betrachten die Komponenten in G' der Punkte u, w, v, z :

P_u, P_w, P_v, P_z.

Diese Komponenten sind alternierende Wege.

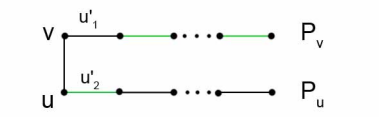


(Da M_1' nur u und w nicht überdeckt lässt und M_2' nur v und z nicht überdeckt lässt, ist $d_{G'}(u) = d_{G'}(w) = d_{G'}(v) = d_{G'}(z) = 1$,

u ist also ein Endpunkt des Weges P_u, u.s.w.)

Es könnte $P_v = P_u$ oder $P_v = P_w$ sein, aber nicht beides.

$o.B.d.A.$ $P_v \neq P_u$



Wir erhalten einen vergrößerten Weg!

$M := (M_1' \cap E(P_u)) \cup (M_2' \cap E(P_v)) \cup \{u\ v\}$

$$\cup\{e \in M_1' \mid e \cap (V(P_u) \cup V(P_v)) = \emptyset\}$$

ist dann ein perfektes Matching in G.

Widerspruch! ↯

Nun wählen wir in jeder geraden Komponente von $G - S$ ein perfektes Matching und in jeder ungeraden ein Matching, das nur einen Punkt der Komponenten nicht überdeckt. Die unüberdeckten Punkte von $G - S$ werden mit verschiedenen Punkten in S verbunden (möglich, da $q(G - S) \leq |S|$) Eventuell bleibt eine gerade Anzahl von Punkten aus S dabei unüberdeckt. Nach Definition von S induzieren diese aber auch einen vollständigen Graphen und wir können unsere Kantenmenge zu einem perfekten Matching ergänzen.

Widerspruch! ↯

Anwendung:

Satz von Petersun

G sei 3-regulär, zusammenhängend, brückenlos.

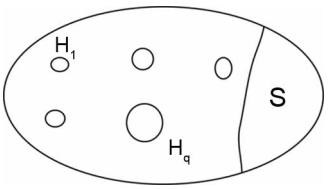
Dann besitzt G ein perfektes Matching.

(Brückenlos bedeutet: $G - e$ ist zush. für alle $e \in E$.)

Beweis:

Wir verifizieren die Tutte-Bedingung.

Sei $S \subseteq V(G),\ H_1, \ldots, H_q$ seien die ungeraden Komponenten von $G - S$.



Wegen Zusammenhang und Brückenlosigkeit von G müssen mindestens 2 Kanten von jedem H_i nach S führen. Aber

$$3 \cdot |V(H_i)| = \sum_{x \in V(H_i)} d_G(x) = \sum_{x \in V(H_i)} d_{H_i}(x) + m_i,$$

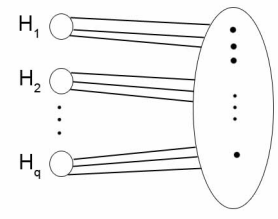
wobei m_i die Anzahl der Kanten zwischen H_i und S ist, $1 \leq i \leq q$

Wäre $m_i = 2$, so wäre

$$\sum_{x \in V(H_i)} d_{H_i}(x) + m_i = 2 \cdot (|E(H_i)| + 1),$$

also gerade, während $3 \cdot |V(H_i)|$ ungerade wäre

$\Rightarrow m_i \geq 3$ für alle i

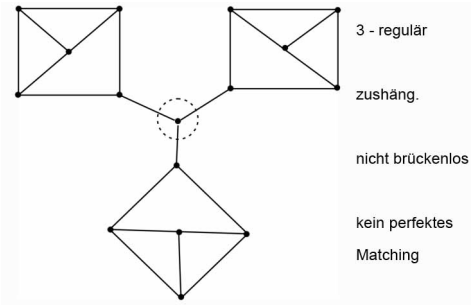


$$\Rightarrow 3 \cdot q \leq \sum_{x \in S} d_G(x) = |S| \cdot 3$$

$\Rightarrow q \leq |S|$

$\Rightarrow$ Behauptung

Beispiel:



Kapitel 3

Algebraische Strukturen

3.1 Monoide

Definition: Ein Paar $(M, *)$ mit

$* : \ M \times M \to M$

heist Monoid, falls die Verknüpfung $*$ assoziativ ist.

$(a, b, c \in M : \ a * (b * c) = (a * b) * c)$

$*(a * (b, c)) = *(*(a, b), c)$

Außerdem soll M ein Element e enthalten mit

$m * e = e * m = m$ für alle $m \in M$

(neutrales Element)

Bemerkung: e ist eindeutig bestimmt

e, e' neutrales Element : $e = e * e' = e'$

Beispiel:

(i) $(\mathbb{N}, \cdot), (\mathbb{N}_0, +)$

(ii) X Menge, $M = X^X = \{f : X \to X\}$

$(M, \circ)$ ist ein Monoid, falls $id_X \in M$

(iii) A sei eine Menge („Alphabet“)

$A^* := \{a_1, \ldots, a_n \mid n \in \mathbb{N}_0 \ , \ a_i \in A, \ 1 \leq i \leq n\}$

sei die Menge der endlichen Wörter über A

$(a_1, \ldots, a_n = b_1, \ldots, b_m \Leftrightarrow n = m$ und $a_i = b_i, \ 1 \leq i \leq n = m)$

Das Wort e ohne Buchstabe heißt leeres Wort.

Verknüpfung $*$: (Konkatenation)

$a_1 \ a_2 \ldots a_n * b_1 \ b_2 \ldots b_m := a_1 \ldots a_n \ b_1 \ldots b_m$

In (i) gilt das Kommutativgesetz,

in (ii) und (iii) i.a. nicht.

Def: Es sei $\sim$ eine Äquivalenzrelation (ÄR) auf M, $(M, *)$ Monoid.

$\sim$ heißt verträglich mit $*$, falls für alle $x, y, u, v \in M$ gilt:

$x \sim y$ und $u \sim v \Rightarrow x * u \sim y * v \quad (*)$

Bemerkung: $\sim$ ist genau dann $*$ - verträglich, falls für alle $x, y, u \in M$ gilt:

$x \sim y \Rightarrow x * u \sim y * u$ und

$u * y \sim u * y \quad (**)$

(Wegen der Reflexivität von $\sim$ folgt $(**)$ aus $(*)$)

Falls $x \sim y$ und $u \sim v$:

$(**) \Rightarrow x * u \sim y * u$ und $y * u \sim y * v$

$\sim$ transitiv: $x * u \sim y * v$, also $(*)$

Satz: Ist $\sim$ verträglich bzgl. $*$, so ist die Menge der Äquivalenzklassen $M/_\sim$ zusammen mit der Verknüpfung

$$[x]_\sim * [y]_\sim \quad := [x * y]_\sim$$

Äquivalenzklassen

ein Monoid von x bzw. y

(Produkt der Äquivalenzklassen ist die Äquivalenzklasse des Produktes)

Beweis: Wohldefiniertheit der Verknüpfung folgt aus der Verträglichkeit:

$[x] = [x'] \quad [y] = [y'] \quad \Rightarrow \quad [x * y] = [x' * y']$

$x \sim x' \qquad y \sim y' \qquad \Rightarrow \qquad x * y \sim x' * y'$

„Faktormonoid von M nach $\sim$“

$(M/_\sim, *)$

06.07.05

Beispiel: $(\mathbb{Z}, +)$ ist ein Monoid

$n \in N,\ n \geq 2$

$x \sim_n y \Leftrightarrow n$ teilt $(x - y)$

$\mathbb{Z}$ zerfällt in n Äquivalenzklassen $[0], [1], \ldots, [n-1]$, die den Resten bei Teilung durch n entstehen.

Verträglichkeit?

$x \sim_n x'$ und $y \sim_n y' \overset{?}{\Rightarrow} x + y \sim_n x' + y'$

n teilt $x - x'$ und $y - y'$, also auch

$x - x' + y'_y = (x + y) - (x' + y')$

Def.: Direkte Produkte, direkte Summe

(i) $(M_1, *_1), \ldots, (M_n, *_n)$ seien Monoide

$\prod_{i=1}^{n} M_i = \bigoplus_{i=1}^{n} M_i = (M, *)$ mit

$M = M_1 \times M_2 \times \ldots \times M_n$

$(m_1, \ldots, m_n) * (m'_1, \ldots, m'_n) = (m_1 * m'_1, \ldots, m_n * m'_n)$

(ii) Angenommen, eine unendliche Familie $(M_i, *)_{i \in I}$ von Monoiden sei gegeben.

$M := \{f : I \to \bigcup_{i \in I} M_i \mid f(i) \in M_i\}$

$M' := \{f \in M \mid \{i \in I \mid f(i) \neq e_i\}$ist endlich$\}$

Für $f, g \in M$: $(f * g)(i) := f(i) *_i g(i)$

$\prod_{i \in I} M_i := (M, *)$ heißt direktes Produkt der M_i

$\bigoplus_{i \in I} M_i := (M', *)$ heißt direkte Summe der M_i

3.2 Gruppen

$(G, \cdot)$ ist eine Gruppe g.d.w.

$(G, \cdot)$ ein Monoid ist mit

Für alle $x \in G$ ex. ein $y \in G$ mit

$x \cdot y = y \cdot x = e$ (neutrales Element)

y heißt das Inverse von x $(y = x^{-1})$

Bemerkung: Ist G eine Gruppe, so ex. zu je zwei Elementen $a, b \in G$ Elemente $x, y \in G$ mit:

$a \cdot x = b$ und $y \cdot a = b$

Dabei sind x, y eindeutig bestimmt.

Beweis: $x = a^{-1} \cdot b$ und $y = b \cdot a^{-1}$ lösen die Gleichung.

Umgekehrt ist klar, dass aus $a \cdot x = b$ durch Linksmultiplikation mit a^{-1} folgt:

$x = a^{-1} \cdot b$, analog

$y \cdot a = b \Rightarrow y = b \cdot a^{-1}$

Bemerkung:

(i) In Gruppen kann man „kürzen“

$a \cdot c = b \cdot c \Rightarrow a = b$

$c \cdot a = c \cdot b \Rightarrow a = b$

Das folgt durch Rechts-bzw. Linksmultiplikation mit c^{-1}

(ii) Gelten in einem endlichen Monoid die Kürzungsregeln, so ist es eine Gruppe

Bemerkung: Für $a \in G$ setzen wir:

$L_a : G \to G : x \mapsto a \cdot x$

$R_a : G \to G : x \mapsto x \cdot a$

Dann sind L_a und R_a beide injektiv (Kürzungsregeln), also bijektiv.

$\Rightarrow$ zu $a \in G$ ex. ein Element a^{-1} mit $L_a(a^{-1}) = e \quad a \cdot a^{-1} = e$

Dann ist:

$a \cdot (a^{-1} \cdot a) = (a \cdot a^{-1}) \cdot a = e \cdot a = a \cdot e$

Wir kürzen das a : $a^{-1} \cdot a = e$

3.3 Beispiele von Gruppen

(i) $(\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{C}, +)$

sind abelsche Gruppen

(ii) $(\mathbb{Q}\backslash\{0\},\cdot),(\mathbb{R}\backslash\{0\},\cdot),(\mathbb{C},\cdot),(\{+1,-1\},\cdot)$

abelsche Gruppen

(iii) $(\mathbb{Z}/_{\sim_n},+)=(\mathbb{Z}_n,+)$

ist ebenfalls eine abelsche Gruppe

(iv) $S_n=\{\pi:\{1,\ldots,n\}\to\{1,\ldots,n\}\mid \pi \text{ bijektiv}\}$

Verknüpfung : Komposition "$\circ$"

$$\pi:\begin{pmatrix}1 & \ldots & n\\ \pi(1) & \ldots & \pi(n)\end{pmatrix}$$

$$\pi^{-1}:\begin{pmatrix}\pi(1) & \ldots & \pi(n)\\ 1 & \ldots & n\end{pmatrix}$$

(v) $\{A\in\mathbb{R}^{n\times n}\mid \det(A)\neq 0\}=^{\text{„general Linear“}} GL(n,\mathbb{R})$

bilden eine Gruppe mit der Matrixmultiplikation.

(vi) $O(n,\mathbb{R})\subseteq GL(n,\mathbb{R})\quad \det(A\cdot A^T)=\det A\cdot\det A^T=(\det A)^2=1$

$O(n,\mathbb{R}):=\{A\in\mathbb{R}^{n\times n}\mid A\cdot A^T=E_n\}$

orthogonale Gruppe

$SO(n,\mathbb{R})=\{A\in O(n,\mathbb{R})\mid \det A=1\}$

„spezial orthogonal group“

(vii) Isometrien der Ebene

$\{f:\mathbb{R}^2\to\mathbb{R}^2\mid ||f(x)-f(y)||=||x-y|| \text{ für alle } x,y\in\mathbb{R}^2\}$

Man kann zeigen: Alle diese Abbildungen sind affin-Linear, d.h.

$f(t\cdot x+(1-t)\cot y)=t\cdot f(x)+(1-t)\cdot f(y)$ für alle $x,y\in\mathbb{R}^2$,$t\in\mathbb{R}$

Äquivalent: $g(x):=f(x)-f(0)$ ist linear

Also sind Isometrien bijektiv und bilden eine Gruppe.

Die Isometrien bestehen aus

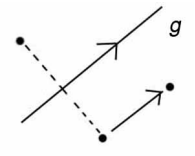
(a) Translationen $T_a\ a\in\mathbb{R}^2$

$T_a(x)=a+x$

(b) Drehungen um beliebige Mittelpunkte und Winkel

(c) Geradenspiegelungen

(d) Schubspiegelungen



Spiegelung an g, dann Translation entlang g.

Dies sind alle Isometrien der Ebene.

(viii) Freie Gruppe über A : $F(A)$

Wir betrachten das freie Monoid über $A \dot{\cup} A^{-1}$: M_A

$A^{-1} = \{a^{-1} \mid a \in A\} \cap A = \emptyset$

$\rho : M_A \to M_A$ sei die folgende Reduktionsabbildung

Ein Wort $w \in M_A$ heiße reduziert, wenn es kein Teilwort der Form $a \cdot a^{-1}$ oder $a^{-1} \cdot a$ $(a \in A)$ enthält.

Wir definieren $\rho(w) := w$, falls w reduziert.

Ist $|w| = n$ und $w = u \cdot a \cdot a^{-1} \cdot v$ oder $w = u \cdot a^{-1} \cdot a \cdot v$, wobei $a \cdot a^{-1}$ und $a^{-1} \cdot a$ von links ausgesehen das erste Paar von Symbolen ist, so dass ein Symbol neben seinem Inversen steht.

Dann sei $\rho(w) := \rho(u \cdot v)$

$u \sim w \Leftrightarrow \rho(u) = \rho(w)$ ist ÄR auf M_A.

Die Äquivalenzklassen von $M_A/_\sim$ sind die Elemente der freien Gruppe.

Wir müssen zeigen: $\sim$ ist verträglich mit der Konkatination, d.h.

$u \sim v$, $w \sim z \Rightarrow u \cdot w \sim v \cdot z$

$\rho(u) = \rho(v)$, $\rho(w) = \rho(z) \Rightarrow \rho(u \cdot w) = \rho(v \cdot z)$

Äquivalent zur Verträglichkeitsbedingung:

$u \sim v$, $w \Rightarrow u \cdot w \sim v \cdot w$ und $w \cdot u \sim w \cdot v$

Dies folgt aus folgendem

Lemma:

(i) $\rho(w) = w$,falls w reduziert

(ii) $\rho(\rho(w)) = \rho(w)$ für alle $w \in M_A$

(iii) $\rho(u \cdot a \cdot a^{-1} \cdot v) = \rho(u \cdot a^{-1} \cdot a \cdot v) = \rho(u \cdot v)$ für alle $u, v \in M_A, a \in A$

(iv) $\rho(\rho(u) \cdot v) = \rho(u \cdot v) = \rho(u \cdot \rho(v))$ $u, v \in M_A$

(i),(ii) sind klar, (iii) folgt durch Induktion nach $|u \cdot v|$, ebenfalls (iv)
zu (iv) Induktionsanfang ist trivial.

$\rho(\rho(u) \cdot v) = \rho(u \cdot v$ ist trivial, falls u reduziert ist $(u = \rho(u))$

Andernfalls: $u = u_1 \cdot a \cdot a^{-1} \cdot u_2$ oder $u_1 \cdot a^{-1} \cdot a \cdot u_2$ mit u_1 reduziert

$O.B.d.A. \quad u = u_1 \cdot a \cdot a^{-1} \cdot u_2$

$\rho(u \cdot v) \underset{\text{Def von } \rho \text{ bzw (iii)}}{=} \rho(u_1 \cdot u_2 \cdot v) \underset{\text{Ind.Annahme}}{=} \rho(\rho(u_1 \cdot u_2) \cdot v)$

Aber $\rho(u_1 \cdot u_2) = \rho(u)$ (wiederum nach (iii))

Analog: $\rho(u \cdot v) = \rho(u \cdot \rho(v))$

Verträglichkeit: $u, v, w \in M_A$

$u \sim v$,d.h. $\rho(u) = \rho(v)$

$\overset{(iv)}{\Rightarrow} \rho(u \cdot w) = \rho(\rho(u) \cdot w)$

$= \rho(\rho(v) \cdot w) = \rho(v \cdot w)$, genauso

$\rho(w \cdot u) = \rho(w \cdot v)$

Das Faktormonoid ist eine Gruppe, denn:

$[w_1 \dots w_n]_\sim^{-1} = [w_n^{-1} \dots w_1^{-1}]_\sim$

wobei $(a^{-1})^{-1} := a$

$[w_1 \dots w_n \; w_n^{-1} \dots w_1^{-1}]_\sim = [e]_\sim$

13.07.05

Die Äquivalenzrelation $\sim$ ist auch verträglich bzgl. der Multiplikation in $\mathbb{Z}$

$x = q \cdot n + r \quad y = \overline{q} \cdot n + s$

$x' = q' \cdot n + r \quad y' = \widehat{q} \cdot n + s$

$x \sim x' \qquad y \sim y'$

$x \cdot y \sim x' \cdot y'$

$(q \cdot n + r) \cdot (\overline{q} \cdot n + s) - (q' \cdot n + r) \cdot (\widehat{q} \cdot n + s)$

$= q \cdot n \cdot \overline{q} \cdot n + q \cdot n \cdot s + \overline{q} \cdot n \cdot r + r \cdot s$

$-(q' \cdot \widehat{q} \cdot n^2 + q' \cdot n \cdot s + \widehat{q} \cdot n \cdot r + r \cdot s)$

$= n \cdot [q \cdot \overline{q} \cdot n + q \cdot s + \overline{q} \cdot r - \widehat{q} \cdot q' \cdot n - q' \cdot s - \widehat{q} \cdot r]$

Beispiel: Neunerprobe

Dezimalzahl $a_n \; a_{n-1} \; \dots a_0$

$= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0$

Welches ist der Rest beim Teilen durch 9 ?

$10 = 9 + 1 \qquad$ „$10 \equiv 1 \mod 9$“

Allgemein: $x \equiv r \mod n \qquad n|(x - r)$

$100 = 10 \cdot 10 \equiv 1 \cdot 1 \equiv 1 \mod 9$

$10^n = \underbrace{10 \cdot 10 \cdot \dots \cdot 10}_{n\text{-mal}} \equiv 1 \mod 9$

$\Rightarrow a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0 \equiv a_n + a_{n-1} + \dots + a_1 + a_0,$

d.h. Rest von $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0 =$ Rest der Quersumme.

Analog bei Teilbarkeit durch 11:

$10 \equiv -1 \mod 11$

$100 \equiv (-1) \cdot (-1) \equiv 1 \mod 11$

$10^3 \equiv -1 \mod 11$

$$10^n \equiv \left\{ \begin{array}{ll} -1, & ,n \text{ ungerade} \\ 1, & ,n \text{ gerade} \end{array} \right\} \equiv (-1)^n \mod 11$$

Rest von $a_n\ a_{n-1} \ldots a_1\ a_0 \mod 11$ = Rest von $a_0 - a_1 + a_2 - a_3 \pm \ldots + (-1)^n \cdot a_n$

Faktorgruppe $\mathbb{Z} = \mathbb{Z}/_\sim$

$(\mathbb{Z}_n \backslash \{0\}, \cdot)$ ist i.a. kein Monoid

$n = p \cdot q \quad , p, q > 1 \qquad : \ p \cdot q \equiv 0 \mod n$

Wir erhalten eine Gruppe wie folgt:

$\{m \in \mathbb{Z} \mid o \leq m < n, \ ggT(m,n) = 1\} =: \mathbb{Z}_n^*$

Behauptung: Die Restklasse dieser Zahlen bilden eine Gruppe m, n.

Was bedeutet es, dass $ggT(m,n) = 1$ ist ?

$m = p_1^{\alpha_1} \ldots p_r^{\alpha_r} \qquad p_1 < p_2 < \ldots < p_r$ Primzahlen

$n = p_1^{\beta_1} \ldots p_r^{\beta_r} \qquad 0 \leq \alpha_i, \beta_i \quad 1 \leq i \leq r$

$ggT(m,n) = p_1^{\min(\alpha_1, \beta_1)} \ldots p_r^{\min(\alpha_r, \beta_r)}$

$ggT(m,n) = 1$ g.d.w. m und n haben disjunkte Primfaktorzerlegung.

jeder Teiler von m und n teilt auch r.

$ggT(m,n) = ggT(n,r)$

$m = q \cdot n + r,\ 0 \leq r < n$

$n = q_1 \cdot r + r_1,\ 0 \leq r_1 < r$

$\vdots$

$r_{k-1} = q_k \cdot n_k + r_{k+1}$

$r_k = q_{k+1} \cdot k+1$

$r_{k+1} = ggT(m,n)$

Man kann den $ggT(m,n)$ stets als ganzzahlige Linearkombination von m und n schreiben, d.h.

Falls $d = ggT(m,n)$, so ex. $x, y \in \mathbb{Z}$ mit

$d = x \cdot m + y \cdot n$

(i) $1 \in \mathbb{Z}_n^*$

(ii) $p, q \in \mathbb{Z}_n^* \Rightarrow p \cdot q$ ebenfalls teilerfremd zu n (Betrachte Primfaktorzerlegung!)

(iii) Es sei $p \in \mathbb{Z}_n^*$. Dann ex. $x, y \in \mathbb{Z}$ mit:

$1 = x \cdot p + y \cdot n,$

d.h. $x \cdot p \equiv 1 \mod n,$

d.h. die Restklasse von x ist invers zu p.

Bezeichnung: $|\mathbb{Z}_n^*| =: \varphi(n)$ „Eulersche φ-Funktion“

3.4 Untergruppen

$(G; \cdot)$ Gruppe

$\emptyset \neq U \subseteq G$ heißt Untergruppe von G, falls U mit der Verknüpfung von G eine Gruppe ist.

Bezeichnung: $U \leq G$

Bemerkung:

(i) Ist $a \in G$ mit $a^2 = a$, so ist $a = e$.

Das neutrale Element von U ist also das neutrale Element von G.

(ii) Wegen (i) und der Eindeutigkeit der Inversenbildung müssen die Inversen von $u \in U$ in U und in G übereinstimmen.

Satz: $\emptyset \neq U \subseteq G$ ist Untergruppe g.d.w. eine der folgenden äquivalenten Bedingungen erfüllt ist:

(i) $e \in U \ ; \ a, b \in U \Rightarrow a \cdot b \in U \ ; \ a \in U$

(ii) $a, b \in U \Rightarrow a \cdot b^{-1} \in U$

(iii) $a, b \in U \Rightarrow a^{-1} \cdot b \in U$

Beweis:

(i) ist (fast) die Definition und impliziert (ii) und (iii)

(ii) $\Rightarrow (i) \ : \ U \neq \emptyset$, etwa $a \in U$

$\Rightarrow a \cdot a^{-1} = e \in U$

$\Rightarrow$ zu $a \in U$ ist auch $e \cdot a^{-1} = a^{-1} \in U$

zu $a, b \in U \Rightarrow b^{-} \in U$

$\Rightarrow a \cdot (b^{-1})^{-1} = a \cdot b \in U$

Analog: (iii) $\Rightarrow$ (i)

Definition: $A, B \subseteq G$

$A \cdot B := \{a \cdot b \mid a \in A, b \in B\}$

heißt Komplexprodukt von A und B

$\{a\} \cdot B = a \cdot B$

Definition: $U \leq G \ , \ a \in G$

$a \cdot U$ heißt Linksnebenklasse von a bzgl. U

$U \cdot a$ heißt Rechtsnebenklasse von a bzgl. U

Satz: $U \leq G$

(i) Zwei Linksnebenklassen $a \cdot U \ , \ b \cdot U$ sind entweder gleich oder disjunkt.

(ii) Die Linksnebenklassen bilden eine Partition der Gruppen G. Die entsprechende ÄR ist:

$a \sim b :\Leftrightarrow a^{-1} \cdot b \in U$

Beweis:

(i) Es sei $a \cdot U \cap b \cdot U \neq \emptyset$

etwa $a \cdot u_1 = b \cdot u_2$ für $u_1, u_2 \in U$

$\Rightarrow$ Für alle $u \in U$ ist:

$a \cdot u = b \cdot \underbrace{(u_2 \cdot u_1^{-1} \cdot u)}_{\in U}$, also $a \cdot U \subseteq b \cdot U$

$b \cdot u = a \cdot u_1 \cdot u_2^{-1} \cdot u \in a \cdot U$, also $b \cdot U \subseteq a \cdot U$

$a \cdot U = b \cdot U$

(ii) Für alle $g \in G$ ist $g \in g \cdot U$, also folgt die Partitionseigenschaft mit (i).

Es ist $a \cdot U = b \cdot U \Leftrightarrow U = a^{-1} \cdot b \cdot U$

also $a \sim b \Leftrightarrow U = a^{-1} \cdot b \cdot U$

$a^{-1} \cdot b \in U \Rightarrow a^{-1} \cdot b \cdot U = U$

Ist umgekehrt $U = a^{-1} \cdot b \cdot U$, so gilt $a^{-1} \cdot b = a^{-1} \cdot b \cdot e \in U$

Es gilt ein analoges Ergebnis für Rechtsnebenklassen (ÄR: $a \sim b \Leftrightarrow a \cdot b^{-1} \in U$)

Die Anzahl der Linksnebenklassen und Rechtsnebenklassen ist gleich

$G = \dot{\bigcup}_{i \in I} a_i \cdot U$ disjunkte Zerlegung in Linksnebenklassen.

$\Rightarrow G = \dot{\bigcup}_{i \in I} U \cdot a_i^{-1}$ ist die disjunkte Zerlegung in Rechtsnebenklassen.

$(\underbrace{a_i^{-1} \cdot a_j \in U}_{a_i \cdot U = a_j \cdot U} \Leftrightarrow \underbrace{a_i^{-1} \cdot (a_j^{-1} \in U)}_{U \cdot a_i^{-1} = U \cdot a_j^{-1}}$

Definition: Die Anzahl der verschiedenen Linksnebenklassen heißt Index von U in G ($[G : U]$)

Satz von Lagrange: Ist G endlich, $U \leq G$, so gilt:

$|G| = |U| \cdot [G : U]$

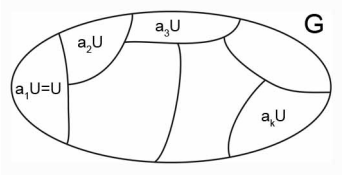
insbesondere ist $|U|$ ein Teiler von $|G|$

Beweis: Jede Linksnebenklasse $a \cdot U$ enthält genau soviele Elemente wie U, denn: Die Linksmultiplikation mit a ist eine bijektive Abbildung.

$\Rightarrow$ Behauptung.

$a^m = a^s \quad s < m$

$a^{m-s} = e$



Ist G endlich, so erzeugt jedes $a \in G$ eine Gruppe $< a >:= \{e, a, a^2, \ldots, a^{k-1}\}$,

wobei $k = \min\{l \mid a^l = e\}$

k heißt die Ordnung von a

$< a >$ heißt auch zyklische Untergruppe von G.

Wir können in $< a >$ mit den Exponenten rechnen wie in $\mathbb{Z}_k$.

Es gilt: $k \mid |G|$

Beispiel: Betrachte $(\mathbb{Z}_n^*, \cdot)$, die zu n teilerfremden Zahlen.

Es sei m zu n teilerfremd, k sei die Ordnung von m in $\mathbb{Z}_n^*$, also $m^k \equiv 1 \mod n$, also

$$m^{\varphi(n)} \equiv 1 \mod n$$

Satz von Euler:

Falls $ggT(m.n) = 1$, so ist $m^{\varphi(n)} \equiv 1 \mod n$

Falls n Primzahl, $n = p$, $\varphi(p) = p - 1$

$1 \leq m < p$: $\quad m^{p-1} \equiv 1 \mod p$ (kleiner Fermatscher Satz)

Frage: Wann bildet die ÄR $\sim$ der Linksnebenklassen bzgl. U eine $\bullet$ - verträgliche ÄR?

$[a] = [a']$, $[b] = [b']$

Es soll gelten : $[a \cdot b] = [a' \cdot b']$

$a \cdot U = a' \cdot U$, $b \cdot U = b' \cdot U \quad \overset{!}{\Rightarrow} a \cdot b \cdot U = a' \cdot b' \cdot U$

Nicht jede Untergruppe erfüllt diese Bedingung $\rightarrow$ „Normalteiler“

N Normalteiler $\Leftrightarrow a \cdot N = N \cdot a$ für alle $a \in G$.

20.07.05

Zusammenfassung

$\mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{0\}$ bildet mit “ $\cdot$ “ eine Gruppe mit $p - 1$ Elementen.

$U := \{1, a, a^2, \ldots, a^k\}$

k minimal mit $a^{k+1} \equiv 1 \mod p$

$(k + 1) = |U| \mid |\mathbb{Z}_p^*| = p - 1$

$a^{p-1} \equiv 1 \mod p \quad (k + 1) \cdot s = (p - 1)$

$a^{p-1} = (a^{k+1})^s \equiv 1^s \equiv 1 \mod p$

$\mathbb{Z}_p^*$: Alle Reste $\mod n$, die zu n teilerfremd sind $\varphi(n) := |\mathbb{Z}_n^*|$

$a^{\varphi} \equiv 1 \mod n$

$\sim$ Sei eine ÄR auf einer Gruppe G.

$\sim$ heißt verträglich, falls gilt:

Für alle $a, a', b, b' \in G$:

$a \sim a'$ und $b \sim b' \Rightarrow a \cdot b \sim a' \cdot b'$

Dann können wir die Äquivalenzklassen multiplizieren:

$[a]_\sim \cdot [b]_\sim := [a \cdot b]_\sim$

Nicht für alle Untergruppen ist die Linksnebenklassenzerlegung verträglich, nur für sogenannte „Normalteiler“.

Definition: $U \subseteq G$ heißt Normalteiler von G, falls für alle $a \in G$ gilt:

$a \cdot U = U \cdot a$

Bezeichnung: $U \underset{\text{Normalteiler}}{\trianglelefteq} G$

$äquiv$: $a \cdot U \cdot a^{-1} = U$ für alle $a \in G$

$äquiv$: $a \cdot U \cdot a^{-1} \subseteq U$ für alle $a \in G$

$a^{-1} \cdot a \cdot U \cdot a^{-1} \cdot a \subseteq a^{-1} \cdot U \cdot a$

$U \subseteq a^{-1} \cdot U \cdot a$ für alle $a \in G$

Es sei $U \trianglelefteq G$,

zu Zeigen:

(i) $a' \in a \cdot U,\ b' \in b \cdot U \Rightarrow a' \cdot b' \in a \cdot b \cdot U$

$a' = a \cdot u_1 \qquad u_1 \in U$

$b' = b \cdot u_2 \qquad u_2 \in U$

$a' \cdot b' = (a \cdot u_1) \cdot (b \cdot u_2) = a \cdot (u_1 \cdot b) \cdot u_2$

[Wegen $U \cdot b = b \cdot U$ ex ein $u_3 \in U$ mit $u_1 \cdot b = b \cdot u_3$]

$= a \cdot b \cdot (u_3 \cdot u_2) \in a \cdot b \cdot U$

(ii) $\sim$ sei eine verträgliche ÄR. Dann ist $[e]_\sim$ ein Normalteiler in G

$a, b \in [e]_\sim\ ,\ a \sim e\ ,\ b \sim e$

$a \cdot b \sim e \cdot e = e$

$a \sim e\ ,\ a^{-1} \cdot a \sim a^{-1} \cdot e\ ,\ e \sim a^{-1}$

$b \sim e\ ,\ a \in G$

$\Rightarrow a \cdot b \cdot a^{-1} \sim a \cdot e \cdot a^{-1} \sim a \cdot a^{-1} = e$

$\Rightarrow$ Behauptung

$a \cdot N \cdot b \cdot N = a \cdot b \cdot N$

Die Gruppe der Äquivalenzklassen heißt Faktorgruppe von G nach N : $G/_N$

Beispiel:

(i) Alle Untergruppen abelscher Gruppen sind Normalteiler.

(ii) Alle Untergruppen von Index 2 sind Normalteiler.

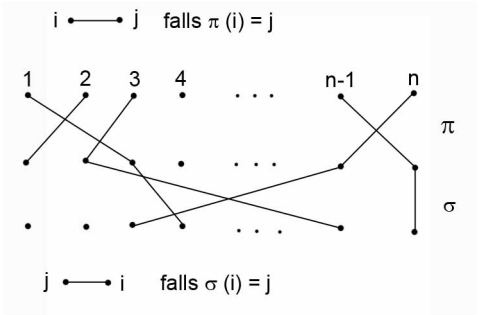
Die symmetrische Gruppe S_n enthält einen Normalteiler von Index 2, die sogenannte alternierende Gruppe von Grad n.

$a_n := \{\sigma \in S_n \mid\ sgn(\sigma) = 1\}$

$sgn(\sigma) := (-1)^{\text{Anzahl der Inversionen von } \sigma}$

Es gilt : $\sigma\ ,\ \pi \in S_n \Rightarrow sgn(\sigma \cdot \pi) = sgn(\sigma) \cdot sgn(\pi)$

Dies impliziert sofort, dass A_n eine Untergruppe ist.



Inversionen von π :

Kreuzungspunkte

σ :

Anzahl der Inversionen von $\sigma \circ \pi$:

Summe aller Kreuzungspunkte - gerade Zahl

$\Rightarrow sgn(\sigma \circ \pi) = (-1)^{\text{Summe aller Kreuzungspunkte}}$

$= (-1)^{\text{Anzahl der Inversionen von } \pi + \text{ Anzahl der Inversionen von } \sigma}$

$= sgn\ \pi \cdot sgn\ \sigma$

(iii) $G = \{f :\ \mathbb{R}^n \to \mathbb{R}^n \mid$ Es ex. eine Matrix A und $b \in \mathbb{R}^n$ mit $f(x) = A \cdot x + b\}$

invertierbare affin-lineare Abbildungen

$f_{A,b}(x) = A \cdot x + b$

$(f_{A,b} \circ f_{B,c})(x) = f_{A,b}(B \cdot x + c) = A \cdot (B \cdot x + c) + b$

$= A \cdot B \cdot x + A \cdot c + b = f_{A \cdot B, A \cdot c + b}$

Neutrales Element : $f_{E,0}$

$f_{B,c}^{-1} = f_{B^{-1}, -B^{-1} \cdot c}$

$A \cdot c + b = 0 \quad b = -A \cdot c = -B^{-1} \cdot c$

$U := \{f_{E,b} \mid b \in \mathbb{R}^n\}$ Translationen

U ist ein Normalteiler.

$f_{A,b} \circ f_{E,a} \circ f_{A^{-1}, -A^{-1} \cdot b}(x)$

$= f_{A,b}(f_{E,a}(A^{-1} \cdot x - A^{-1} \cdot b))$

$= f_{A,b}(A^{-1} \cdot x - A^{-1} \cdot b + a)$

$= x - b + A \cdot a + b = x + A \cdot a = f_{E, A \cdot a}(x)$

3.5 Homomorphismen

G, H Gruppen, $f :\ G \to H$ heißt Homomorphismus falls:

Für alle $a, b \in G$: $f(a \underset{\text{in } G}{\cdot} b) = f(a) \underset{\text{in } H}{\cdot} f(b)$

3.6 Eigenschaften von Homomorphismen

- $f(e_G) = e_h$: $f(e_G) \cdot f(e_G) = f(e_G \cdot e_G) = f(e_G) \Rightarrow f(e_G) = e_H$
- $f(a^{-1}) = f(a)^{-1}$: $f(a^{-1}) \cdot f(a) = f(a^{-1} \cdot a) = f(e_G) = e_H$

  $\Rightarrow f(a^{-1}) = f(a)^{-1}$
- $f(G) \leq H$: Beweis ist klar.

Definition: $Kern\ f := \{a \in G \mid f(a) = e_H\}$

Behauptung: $N := Kern\ f \trianglelefteq G$

Untergruppeneigenschaft: $f(e_G = e_H\ ,\ e_G \in N)$

$a, b \in N \quad f(a \cdot b) = f(a) \cdot f(b) = e_H \cdot e_H = e_H \Rightarrow a \cdot b \in N$

$a \in N \Rightarrow f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H$

$a \in N\ ,\ b \in G$ zu Zeigen: $b \cdot a \cdot b^{-1} \in N$

$f(b \cdot a \cdot b{-}1) = f(b) \cdot f(a) \cdot f(b)^{-1} = f(b) \cdot e_H \cdot f(b)^{-1} = f(b) \cdot f(b^{-1}) = e_H$

Beispiel: $A_n \trianglelefteq S_n$, A_n ist $Kern\ sgn.$

$sgn:\ S_n \to H\ ,\ H(\{\pm 1\}, \cdot)$

Definition: Isomorphismen sind bijektive Homomorphismen

Es gilt:

Satz: (Homomorphiesatz)

Es sei $f:\ G \to H$ ein Homomorphismus. Dann ist:

$f(G) \underset{\text{isomorph}}{\backsimeq} G/_{Kern\ f}$

$\pi:\ G/_{Kern\ f} \to f(G):\ a \cdot Kern\ f \mapsto f(a)$

ist der gewünschte Isomorphismus:

$N := Kern\ f$

$a \cdot N = a' \cdot N \Leftrightarrow a^{-1} \cdot a' \in N \Leftrightarrow f(a^{-1} \cdot a') = e_H$

$\Leftrightarrow f(a)^{-1} \cdot f(a') = e_H \Leftrightarrow f(a') = f(a)$

$\Rightarrow \pi$ wohldefiniert und bijektiv.

$\pi(a \cdot N \cdot b \cdot N) = \pi(a \cdot b \cdot N) = f(a \cdot b) = f(a) \cdot f(b)$

$= \pi(a \cdot N) \cdot \pi(b \cdot N)$

π Homomorphismus, also Isomorphismus.

22.07.05

Zusammenfassung

$N \trianglelefteq G$

$a \cdot N = N \cdot a \qquad (a \in G)$

$a \cdot N \cdot a^{-1} = N \qquad (a \in G)$

$a \cdot N \cdot a^{-1} \subseteq N$

$a \sim a'\ ,\ b \sim b' \Rightarrow a \cdot b \sim a' \cdot b'$

$[a]_\sim \cdot [b]_\sim = [a \cdot b]_\sim$

$a \cdot N \cdot b \cdot N = a \cdot b \cdot N$

$\sim$ verträglich $\Rightarrow [e]_\sim \trianglelefteq G$

$a \sim b \Leftrightarrow b^{-1} \cdot a \sim e \Leftrightarrow b^{-1} \cdot a \in [e]_\sim$

$:\ G \to H, \qquad f(g) \leq H$

$Kern\ f := \{g \in G \mid f(g) = e_H\} \trianglelefteq G$

$f(G) \backsimeq G/_{Kern\ f}$

Definition: $S \subseteq G$

$< S >= \bigcap \{U \mid U \leq G\ ,\ S \subseteq U\} \leq G$

„Erzeugnis von S in G“

Bemerkung: Falls $< S >= G$, so ist G stets homomorphes Bild der von S erzeugten freien Gruppe.

3.7 Direkte Produkte

$G_1, \ldots, G_n$ seien Gruppen

$G_1 \times \ldots G_n := \{(a_1, \ldots, a_n) \mid a_i \in G_i \ , \ 1 \leq i \leq n\}$

$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) := (a_1 \cdot b_1, \ldots, a_n \cdot b_n)$

direktes Produkt von $G_1, \ldots, G_n$

(„äußeres“ direktes Produkt)

$G_i' := \{(a_1, \ldots, a_n) \in G_1 \times \ldots \times G_n \mid a_i \in G_i \ , \ a_j = e \text{ für } j \neq i\}$

$(e_1, \ldots, e_{i-1}, a_i, e_{i+1}, \ldots, e_n)$

G_i' ist isomorph zu G_i

Definition: G ist inneres direktes Produkt seiner Untergruppen $G_1, \ldots, G_n$, falls zu jedem $a \in G$ eindeutig Elemente $a_1 \in G_1, \ldots, a_n \in G_n$ ex. mit:

$a = a_1 \cdot a_2 \cdot \ldots \cdot a_n$.

Bemerkung: G ist inneres direktes Produkt von $G_1, \ldots, G_n$

(Untergruppen von G) g.d.w.

$G_1, \ldots, G_n$ sind Normalteiler in G,

$G = G_1 \cdot G_2 \cdot \ldots \cdot G_n$,

$G_i \cap (G_1 \cdot \ldots \cdot G_{i-1} \cdot G_{i+1} \cdot \ldots \cdot G_n) = \{e\} \ , \ 1 \leq i \leq n$

Bemerkung: $U \leq G \ , \ N \trianglelefteq G \Rightarrow U \cdot N \leq G$

$e \in U \cdot N, \ (u_1 \cdot n_1) \cdot (u_2 \cdot n_2) = u_1 \cdot (n_1 \cdot u_2) \cdot n_2$

$= (u_1 \cdot u_2) \cdot (n_1 \cdot n_2) \in U \cdot N$

$(u_1 \cdot n_1)^{-1} = n_1^{-1} \cdot u_1^{-1} = u_1^{-1} \cdot n_2 \in U \cdot N$

Beispiel: Zyklische Gruppen

$G =< a >$ $\quad$ G unendlich $\Rightarrow G \simeq \mathbb{Z}$

G endlich: $a^n = e, \ a^k \neq e \ (1 \leq k < n)$

$G = \{e, a, a^2, \ldots, a^{n-1}\} \Rightarrow G \simeq \mathbb{Z}$

Sind die $\mathbb{Z}_n$ direkte Produkte?

Das ist möglich, denn es gilt:

$\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{n \cdot m}$ g.d.w. n und m teilerfremd (chinesischer Restsatz)

Verallgemeinerung: $\mathbb{Z}_{m_1 \cdot m_2 \cdot \ldots \cdot m_k} \backsimeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_k}$

falls alle $ggT(m_i, m_j) = 1 \ (i \neq j)$

$G = \{e, g, g^2, \ldots, g^{n-1}\} \simeq \mathbb{Z}_n$

$H = \{e, h, h^2, \ldots, h^{m-1}\} \simeq \mathbb{Z}_m$

$(g, h) \in G \times H$.

Was ist die Ordnung von (g, h)?

$(g,h)^k = (g^k, h^k) = (e_G, e_H) \Leftrightarrow n|k \ , \ m|k$

Falls n, m teilerfremd, ist dies äquivalent mit $n \cdot m|k$

$\Rightarrow$ Ordnung von (g,h) ist $n \cdot m$

$\underset{|G\times H|=n\cdot m}{\Rightarrow} G \times H \simeq \mathbb{Z}_{n\cdot m}.$

Ist umgekehrt $d = ggT(m,n) > 1$,

so betrachten wir ein beliebiges Element $(g^r, h^s) \in G \times H$

$(g^r, h^s)^{\frac{m\cdot n}{d}} = (g^{\frac{r\cdot m\cdot n}{d}}, h^{\frac{s\cdot m\cdot n}{d}}) = ((g^n)^{r\cdot\frac{m}{d}}, (h^m)^{s\cdot\frac{n}{d}}) = (e_G, e_H)$

Bemerkung: Die Isomorphie bedeutet:

Es ex. genau ein $t \in \{0, 1, \ldots, m\cdot n - 1\}$ mit $t \equiv r(m)$ und $t \equiv s(n)$, falls m, n teilerfremd sind und r, s beliebig.

Es ex. nämlich $x, y \in \mathbb{Z}$ mit:

$1 = x \cdot m + y \cdot n \Rightarrow y \cdot n \equiv 1 \mod m$

$x \cdot m \equiv 1 \mod n$

$t = r \cdot n \cdot y + s \cdot m \cdot x$

$t \equiv r \mod m, \quad t \equiv s \mod n$

Falls $ggT(m_i, m_j) = 1 \ , \ i \neq j \ , \ 1 \leq i, j \leq k$

Suchen wir ein x mit $x \equiv r_i \mod m_i \ , \ 1 \leq i \leq k$

$M := m_1 \cdot m_2 \cdot \ldots \cdot m_k$

$M_i := M/_{m_i} = \prod_{j\neq i} m_j$

Dann sind m_i und M_i teilerfremd

$\Rightarrow$ es ex. $z_i \ , \ M_i'$ mit:

$1 = z_i \cdot m_i + M_i' \cdot M_i \qquad z_i, M_i \in \mathbb{Z}$

d.h. $M_i' \cdot M_i \equiv 1 \mod m_i$

Dann setzen wir

$x := \sum_{i=1}^{k} r_i \cdot M_i' \cdot M_i$

Dieses x tut's !

Es gilt der folgende

Basissatz:

Es sei G eine endlich erzeugte abelsche Gruppe. Dann ist G direktes Produkt von zyklischen Gruppen.

Beweis: Schreibe die Gruppe additiv (mit neutralem Element 0)

$n = n(G) := \min\{|S| \mid S \subseteq G \ , \ < S >= G\}$

Vollständige Induktion nach $n(G)$

$n = 1$**:** G ist zyklisch

$n > 1$ Die Behauptung gelte für abelsche Gruppen mit weniger als n Erzeugenden.

Fall 1: Es ex. ein Erzeugendensystem $(\min.)$ $\{g_1, \ldots, g_n\}$ von G mit:

$\gamma_1 \cdot g_1 + \gamma_2 \cdot g_2 + \ldots + \gamma_n \cdot g_n = 0$ mit $\gamma_i \in \mathbb{Z} \ , \ 1 \leq i \leq n,$

so ist stets

$\gamma_1 = \gamma_2 = \ldots = \gamma_n = 0$

Dann ist $G =< g_1 > \times < g_2 > \times \ldots \times < g_n > \simeq \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$

$\nu_1 \cdot g_1 + \nu_2 \cdot g_2 + \ldots + \nu_n \cdot g_n = g = \mu_1 \cdot g_1 + \ldots + \mu_n \cdot g_n$

$\Rightarrow (\nu_1 - \mu_1) \cdot g_1 + (\nu_2 - \mu_2) \cdot g_2 + \ldots + (\nu_n - \mu_n) \cdot g_n = 0$

also $\nu_1 = \mu_1, \ldots, \nu_n = \mu_n$.

Fall 2: Für jedes $\min$ Erzeugendensystem $\{g_1, \ldots, g_n\}$ ex. eine Beziehung $\sum_{i=1}^{n} \gamma_i \cdot g_i = 0$, so dass nicht alle γ_i Null sind.

Unter allen diesen Beziehungen für alle $\min$ Erzeugendensysteme gibt es einen kleinsten positiven Koeffizienten α_1

zugehöriges Erzeugendensystem sei $\{a_1, \ldots, a_n\}$,

O.B.d.A. gelte $\alpha_1 \cdot a_1 + \alpha_2 \cdot a_2 + \ldots + \alpha_n \cdot a_n = 0$

Behauptung:

$\alpha_1 | \alpha_i \quad (i \geq 2)$

$(i \geq 2)$ fest: $\alpha_i = \beta_i \cdot \alpha_1 + \rho_i \ , \ \beta_i \in \mathbb{Z} \ , \ 0 \leq \rho_i < \alpha_1$

$\Rightarrow \alpha \cdot (a_1 + \beta_i \cdot a_i) + \alpha_2 \cdot a_2 + \ldots + \alpha_{i-1} \cdot a_{i-1} + \rho_i \cdot a_i + \alpha_{i+1} \cdot a_{i+1} + \ldots + a_n = 0$

$\{a_1 + \beta_i \cdot a_1, a_2, \ldots, a_n\}$ ist $\min$. Erzeugendensystem von G und ρ_i muss nach Wahl von α_1 Null sein.

$\alpha_i = \beta_i \cdot \alpha_1$ für jedes $i \geq 2$

$a := a_1 + \beta_2 \cdot a_2 + \beta_3 \cdot a_3 + \ldots + \beta_n \cdot a_n$ erfüllt $\alpha_1 \cdot a = 0$

(a erzeugt zyklische Gruppe mit α_1 Elementen)

Ferner: $\{a, a_2, \ldots, a_n\}$ ist $\min$. Erzeugendensystem von G.

$G =< a > + < \{a_2, \ldots, a_n\} >$. Diese Summe ist direkt:

Es sei $g = \overline{a} + \overline{b}$ mit $\overline{a} \in < a > \ , \ \overline{b} \in < \{a_2, \ldots, a_n\} >$

Äquivalent zur Eindeutigkeit ist der Spezialfall $g = 0$

$\big(\overline{a} + \overline{b} = 0 \Rightarrow (\text{ Eindeutigkeit von } \overline{a}, \overline{b})\ \overline{a} = \overline{b} = 0\big)$

$\overline{a} + \overline{b} = \overline{a} + \overline{b} \Rightarrow (\overline{a} - a') + (\overline{b} - b') = 0$

$\Rightarrow \overline{a} = a' \ , \ \overline{b} = b'$

$\overline{a} + \overline{b} = 0$,

$\overline{a} = k \cdot a \ , \ \overline{b} = k_2 \cdot a_2 + k_3 \cdot a_3 + \ldots + k_n \cdot a_n$

$\overline{a} + \overline{b} = k \cdot a + \sum_{i=2}^{n} k_i \cdot a_i = 0$

Schreibe: $k = q \cdot \alpha_1 + r \quad , 0 \leq r \leq \alpha_1$

$\Rightarrow r \cdot a + \sum_{i=2}^{n} k_i \cdot a_i = 0$

$\Rightarrow r = 0 \ , \ \overline{a} = 0$

$\Rightarrow \overline{b} = 0$

$< a >, \ < \{a_2, \ldots, a_n\} >$

Nach Induktionsannahme ist $< \{a_2, \ldots, a_n\} >$ direktes Produkt von zyklischen Gruppen, also auch G.

Index