Methoden der Diskreten Mathematik in der Informatik

Prof. P. Hauck[1]

Wintersemester 2011/2012

Stand: 4. Januar 2012, 15:24

[1]Mitschrift: Volodymyr Piven

Inhaltsverzeichnis

Vorwort

Beim vorliegenden Text handelt es sich um eine inoffizielle Mitschrift. Als solche kann sie selbstverständlich Fehler enthalten und ist daher für Übungsblätter und Klausuren nicht zitierfähig.
Korrekturen und Verbesserungsvorschläge sind jederzeit willkommen und können an `wpiven@gmail.com` gerichtet werden.
Der Text wurde mit LaTeX2ε in Verbindung mit dem AMS-TeX-Paket für die mathematischen Formeln gesetzt.
Alle Grafiken und Bilder wurden mit Ti*k*Z-Paket erstellt.

Literatur:

- M. Aigner, *Diskrete Mathematik.* Vieweg + Teubner, 2006.
- P. Cameron, *Combinatorics - Topics, Techniques, Algorithms.* Cambridge University Press, 1994.
- R.L. Graham, M. Grötschel and L. Lovász (editors), *Handbook of Combinatorics, Vol.I, II.* Elsevier, The MIT Press, 1995.
- R.L. Graham, D. Knuth and O. Patashnik, *Concrete Mathematics.* Addison-Wesley, 1994.
- R.P. Grimaldi, *Discrete and Combinatorial Mathematics. An applied Introduction.* Addison-Wesley, 2003.
- T. Ihringer, *Diskrete Mathematik.* Heldermann, 2002.
- K. Jacobs und D. Jungnickel, *Einführung in die Kombinatorik.* de Gruyter, 2003.
- W. Koepf, *Computeralgebra: Eine algorithmisch orientierte Einführung.* Springer, 2006.
- G.E. Martin, *Counting: The Art of Enumerative Combinatorics.* Springer, 2010.
- J. Matousek und J. Nesetril, *Diskrete Mathematik.* Springer, 2002.
- K.H. Rosen (editor), *Handbook of Discrete and Combinatorial Mathematics.* CRC Press, 2000.
- P. Tittmann, *Einführung in die Kombinatorik.* Spektrum, 2000.
- J. van Lint and R.M. Wilson, *A Course in Combinatorics.* Cambridge University Press, 2001.

Kapitel 0

Einleitung

Dozent:

- Professor Dr. Peter Hauck
  Tel.: +49-7071-2978962
  Email: hauck@informatik.uni-tuebingen.de

Vorlesungszeiten:

- Dienstag 16-18 Uhr Hörsaal 1 - F119
- Donnerstag 16-18 Uhr Hörsaal 1 - F119

Übungsleitung;

- Professor Dr. Peter Hauck

Kapitel 1

Rekursion

Definition 1.1.

a) Eine Rekursion ist ein unendliches System von Gleichungen der Form:

$$x_n = f_n\left(x_{n-1}, x_{n-2}, \ldots, x_1\right) \forall n \geq n_0$$

Also sind bei Vorgabe $x_1 = a_1, \ldots, x_{n_0-1} = a_{n_0-1}$ die übrigen $x_{n_0}, x_{n_0+1}, \ldots$ eindeutig bestimmt.

Beispiel. $x_n = 5x_{n-1} \cdot x_{n-2} \cdot x_{n-3} \cdot \ldots \cdot x_1 + 6 \ \forall \ n \geq 2$

$$\begin{array}{cc} x_1 = 1 & x_1 = 0 \\ x_2 = 11 & x_2 = 6 \\ x_3 = 61 & x_3 = 6 \\ \vdots & \vdots \end{array}$$

Eine Folge $x_1, x_2, \ldots, x_n$, die sämtliche Gleichungen $(*)$ erfüllt, heißt Lösung der Rekursion.

b) Eine Rekursion k-ter Ordnung liegt vor, falls:

$$x_n = f_n\left(x_{n-1}, \ldots, x_{n-k}\right) \forall n \geq k+1$$

Beispiel. $x_n = 4x_{n-1} \cdot x_{n-2} + x_{n-4}$ Rekursion 4-ter Ordnung

c) Eine Rekursion heißt linear, falls:

$$x_n = g_{n-1}(n)x_{n-1} + g_{n-2}(n)x_{n-2} + \ldots + g_1(n)x_1 + g_0(n) \forall n \geq n_0$$

Ist $g_0(n) = 0 \ \forall \ n \geq n_0$: homogene lineare Rekursion, sonst inhomogene lineare Rekursion.

Beispiel. $x_n = x_{n-1} + 2x_{n-2} + \ldots + (n-1)x_1 + 1 \ \forall \ n \geq 2$
$g_0(n) = 1 \ \forall \ n \geq 2$
$k \geq 1 : g_k(n) = \begin{cases} n-k, & \forall n > k \\ 0, & \forall n < k \end{cases}$

d) Ein Rekursion $x_n = c_1 x_{n-1} + c_2 x_{n-2} + \ldots + c_k x_{n-k} + c_0$ (k fest) heißt linear mit konstanten Koeffizienten, von Ordnung k.

Beispiel 1.2.

a) Fibonacci-Zahlen
Auf wie viele Arten lässt sich natürliche Zahl als geordnete Summe von Einsen und Zweier schreiben?

$$F_1 = 1, F_2 = 2, F_3 = 3 \ (3 = 1 + 2 = 2 + 1 = 1 + 1 + 1)$$

$n \geq 3$: Jede solche Darstellung von n endet mit 1 oder 2

$$\overbrace{+\cdots\cdots+\cdots}^{n-1}+1$$
$$\underbrace{+\cdots\cdots+\cdot\cdot}_{n-2}\ +2$$

$F_n = F_{n-1} + F_{n-2}$ lineare homogene Rekursion mit konstanten Koeffizienten der Ordnung 2. (Fibonacci: Leonardo von Pisa, 1175– $\sim$ 1250, Liber baci)
Wie viele 0-1-Folgen der Länge n gibt es, die kein aufeinander folgendes Paar 00 enthalten?

Anzahl: $a_1 = 2$
$a_2 = 3$
$a_3 =$
Folge der Länge n: Endet auf 1: $\underbrace{\cdots\cdots\cdots}_{a_{n-1}}1$
Endet auf 0: $\underbrace{\cdots\cdots\cdots}_{a_{n-2}}10$

$a_n = a_{n-1} + a_{n-2}$
$a_n = F_{n+1}$

b) Türme von Hanoi

Spielregeln:

- Pro Zug eine Scheibe umlegen
- Nie Größere auf kleinere
- Am Ende Turm auf anderen Staffel

Aufgabe: Minimalanzahl von Zügen?

Zahl: $s_1 = 1$
$s_n = s_{n-1} + 1 + s_{n-1} = 2s_{n-1} + 1$

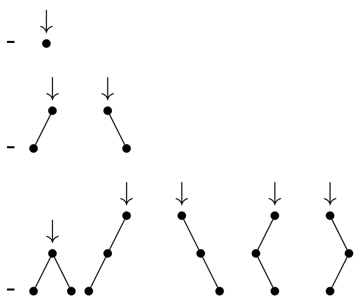
Lineare inhomogene Rekursion mit konst. Koeffizienten von Ordnung 1.

c) Sortieren mit Bubblesort
Liste $(a_1, \ldots, a_n)$ von Zahlen soll im aufsteigender Reihenfolge sortiert werden:
Vergleiche a_1, a_2
Wenn $a_1 \leq a_2 \quad \surd$
Wenn $a_1 > a_2$, so a_1, a_2 vertauschen
Vergleich neues a_2 mit a_3
Am Ende steht größte Element an Stelle n. Wiederhole Algorithmus mit den ersten $n-1$ Stellen. Anzahl der Vergleiche: $V(n) = V(n-1) + n - 1$.
Lineare inhomogene Rekursion mit konst. Koeffizienten von Ordnung 1.

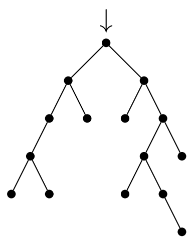
d) <u>Catalan-Zahlen</u>

d1) Produkt von n Faktoren; wie viele sinnvolle Klammerungen? c_n
$n = 3 \quad (x_1 \cdot x_2) \cdot x_3, x_1 \cdot (x_2 \cdot x_3) \quad c_3 = 2$
$n = 4 \quad x_1 \cdot (x_2 \cdot (x_3 \cdot x_4)), x_1 \cdot ((x_2 \cdot x_3) \cdot x_4), ((x_1 \cdot x_2) \cdot x_3) \cdot x_4,$
$(x_1 \cdot (x_2 \cdot x_3)) \cdot x_4, (x_1 \cdot x_2) \cdot (x_3 \cdot x_4) \quad c_4 = 5$
Rekursive Beschreibung: $\left(\underbrace{\ldots\ldots}_{j}\right) \cdot \left(\underbrace{\ldots\ldots}_{n-j}\right)$
$c_n = \sum_{j=1}^{n-1} c_j c_{n-j}$, nicht lineare Rekursion unbeschränkter Ordnung.
$\left[c_n = \frac{(2n-)!}{n!(n-1)!} = \frac{1}{2n-1}\binom{2n-1}{n}\right]$

d2) Geordnete binäre Wurzelbäume
Leere Baum ist geordneter binärer Wurzekbaum oder ausgezeichneter Knoten (Wurzel) + geordneter <u>Paar</u> geordneter binärer Wurzelbäume.
Frage: Anzahl der Wurzebäume mit n Knoten $= b_n$. (Rek. Def.)
- Leerer Baum



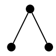
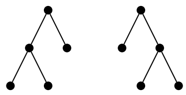
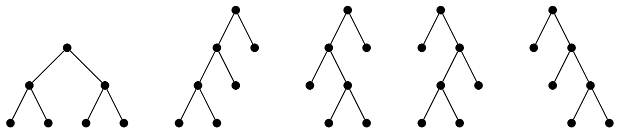
$b_0 = 1, b_1 = 1, b_2 = 2, b_3 = 5, \ldots$
$b_n = \sum_{j=0}^{n-1} b_j b_{n-1-j}, \; n \geq 1$
$b_n = c_{n+1}$



d3) Vollständig geordneter binäre Wurzelbäume
Geordneter binärer Wurzelbaum, jeder Knoten hat zwei Kinder oder

keine. Knoten ohne Kinder: Blätter

a_k = Anzahl der vollständigen binären Wurzelbäume mit k Blättern.

- $a_1 = 1, a_2 = 1$ 
- $a_3 = 2$ 
- $a_4 = 5$ 
- $a_k = \sum\limits_{j=1}^{k-1} a_j a_{k-j} = c_k$

e) Sortieren mit MergeSort

Liste L mit n Elementen, sortieren!

Zerlege L in Listen $L^{'}, L^{''}$ der länge $\frac{n}{2}$

Sortiere $L^{'}, L^{''}$ mit Merge Sort

Sort. $L^{'}$ | | Sort. $L^{''}$ Durch max. $n-1$ Vergleiche Liste insgesamt sortieren.

Max. Anzahl der Vergleiche:

$$V(n) = 2 \cdot V\left(\frac{n}{2}\right) + (n-1) \qquad O(n \log n)$$

Lineare inhomogene Rekursion.

f) e) ist typisches Beispiel für Aufwandsabschätzung bei Divide-and-Conquer-Algorithmen.

- Zerlege eine Menge einer Größe n in a etwa gleich große Teilmengen der Größe $\frac{n}{b}$, löse Problem auf jeder der Teilmengen, führe Teillösungen zusammen. Aufwand: $\boxed{T(n) = a \cdot T\left(\frac{n}{b}\right) + f(n)}$

  $f(n)$ - Aufwand für Zerlegen und Zusammenfassen.
- Zerlege Problem der Größe n in a Teilprobleme der Größe $n-1$. Aufwand: $\boxed{T(n) = a \cdot T(n-1) + g(n)}$ (z.B. Turm von Hanoi)

Lineare Rekursion k-ter Ordnung mit konst. Koeffizienten.

$$x_n = c_1 x_{n-1} + \ldots + c_k x_{n-k} \forall n > k \quad (c_k \neq 0)$$

Zu geg. $(a_1, \ldots, a_k) \in \mathbb{C}^k \left(\mathbb{R}^k\right)$ existiert genau eine Lösung $(x_1, x_2, \ldots) \in \mathbb{C}^{\mathbb{N}}$ mit $x_1 = a_1, \ldots, x_k = a_k$

$$R : \begin{cases} \mathbb{C}^k \longrightarrow \mathbb{C}^{\mathbb{N}} \\ a = (a_1, \ldots, a_k) \longmapsto R(a) \text{ Lösungsfolge zu der Anfanswerten } a_1, \ldots, a_k \end{cases}$$

Satz 1.3.

a) Gegeben homogene lineare Rekursion k-ter Ordnung mit konst. Koeffizienten

$$(R_n) \quad x_n = c_1 x_{n-1} + \ldots + c_k x_{n-k} \quad (n > k) \qquad c_k \neq 0$$

Die Lösungen von (R_n) bilden einen Unterraum L der $\mathbb{C}^{\mathbb{N}}$, $\dim L = k$ und die Abb. $R : \mathbb{C}^k \to \mathbb{C}^{\mathbb{N}}, a \mapsto R(a)$, ist bijektive lineare Abb. von $\mathbb{C}^K$ auf L

b) Gegeben sei inhomogene lineare Rekursion k-ter Ordnung mit konst. Koeffizienten.

$$(R) \quad x_n = c_1 x_{n-1} + \ldots + c_k x_{n-k} + f(n), \quad (n > k) \qquad c_k \neq 0$$

Sei (R_n) die zug. homogene Rekursion (streiche $f(n)$).
Ist $w = (x_1, x_2, x_3, \ldots)$ irgendeine spezielle Lösung von (R), so ist die Menge aller Lösungen von (R) gerade

$$w + L = \{(x_1 + y_1, x_2 + y_2, \ldots) : (y_1, y_2, \ldots) \in L\},$$

wobei L der Lösungsraum von (R_n) ist.

Beweis. Wie bei LGS. □

1.1 Homogene lineare Rekursion

Suche Basis von L. Wie? Wähle Basis $v_1, \ldots, v_k$ von $\mathbb{C}^k$
$\Rightarrow$ $R(v_1), \ldots, R(v_k)$ Basis von L.

z.B. $v_1 = l_1 = (1, 0, \ldots, 0)$
$v_2 = l_2 = (0, 1, \ldots, 0)$
$\vdots$
$v_k = l_k = (0, 0, \ldots, 1)$

$R(l_1) = (1, 0, \ldots, 0, c_k, c_1 c_k, c_1^2 c_k + c_2 c_k, \ldots)$
$x_{k+1} = c_1 x_k + c_2 x_{k-1} + \ldots + c_k x_1$
$x_{k+2} = c_1 x_{k+1} + c_2 x_k + \ldots + c_k x_2$
$x_{k+3} = c_1 x_{k+2} + c_2 x_{k+1} + \ldots + c_k x_3$
$a = (a_1, \ldots, a_k)$ geg. $\hookrightarrow$ Lösung $R(a) \in L$

$$\begin{aligned} R(a) &= s_1 R(l_1) + \ldots + s_k R(l_k) \\ (a_1, \ldots, a_k, a_{k+1}) &= (s_1, 0, \ldots, 0, s_1 c_k, s_1 c_1 c_k, \ldots) \\ &+ \ldots \\ &+ (0, \ldots, 0, s_k, *, \ldots) \\ &= (s_1, s_2, \ldots, *, *, \ldots) \end{aligned}$$

(R_n) $x_n = c_1 x_{n-1} + \ldots + c_k x_{n-k}, c_k \neq 0 \quad \forall n > k$
$a = (a_1, \ldots, a_k) \longrightarrow R(a) = (a_1, \ldots, a_k, a_{k+1}, \ldots)$
$L = \left\{R(a) : a \in \mathbb{C}^k\right\}$

$$\text{Betrachten lineare Abb. } \alpha \begin{cases} \mathbb{C}^k \to \mathbb{C}^k \\ \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} \mapsto \begin{pmatrix} x_2 \\ \vdots \\ x_{k+1} \\ c_1 x_k + c_2 x_{k-1} + \ldots + c_k x_1 \end{pmatrix} \end{cases}$$

$$\alpha^n \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} x_{1+n} \\ \vdots \\ x_{k+n} \end{pmatrix}$$

Bezüglich kanonische Basis $\mathfrak{B}$ von $\mathbb{C}^k$ hat α folgende Matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & 1 & \cdots & 0 \\ \vdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 1 \\ c_k & c_{k-1} & c_{k-2} & \cdots & c_1 \end{pmatrix}$$

$$A \cdot \begin{pmatrix} x_1 \\ \vdots \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} x_2 \\ \vdots \\ x_k \\ c_k x_1 + \ldots c_1 x_k \end{pmatrix} = \begin{pmatrix} x_2 \\ \vdots \\ \vdots \\ x_{k+1} \end{pmatrix}$$

$$\det(t \cdot E_k - A) = t^k - c_1 t^{k-1} - c_2 t^{k-2} - \ldots - c_{k-1} t - c_k$$

Bestimme die Lösungen von $\underbrace{t^k - c_1 t^{k-1} - \ldots - c_k = 0}_{\text{charakteristische Gleichung}}$

Sei d Nullstelle der charakteristischer Gleichung, d.h. ein Eigenwert von A. D.h. es existiert Vektor $v = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} \in \mathbb{C}^k$ mit $Av = d \cdot v$

$$\begin{aligned} v_2 &= dv_1 \\ v_3 &= dv_2 = d^2 v_1 \\ &\vdots \\ v_k &= d^{k-1} v_1 \end{aligned}$$

$\Rightarrow$ v ist durch v_1 eindeutig bestimmt, d.h. der Eigenraum zu d ist 1-dim. Wähle z.B. $v_1 = 1$: $\begin{pmatrix} 1 \\ d \\ d^2 \\ \vdots \\ d^{k-1} \end{pmatrix}$ ist Eigenvektor von A zu Eigenwert von d.

$$A^n \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} x_{1+n} \\ \vdots \\ x_{k+n} \end{pmatrix}$$

Zug. Lösung $R(v)$ zu $v \in \mathbb{C}^k$:

$$\begin{pmatrix} v_{n+1} \\ \vdots \\ v_{n+k} \end{pmatrix} \underset{(*)}{=} A^n \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = A^n \begin{pmatrix} 1 \\ d \\ \vdots \\ d^{k-1} \end{pmatrix} = \begin{pmatrix} d^n \\ d^{n+1} \\ \vdots \\ d^{n+k-1} \end{pmatrix}$$

$R(v) = (v_1, v_2, \ldots, v_k, v_{k+1}, \ldots, v_n, \ldots)$
$R(v) = (1, d, \ldots, d^{k-1}, d^k, d^{k+1}, \ldots)$
<u>Annahme:</u> Charakteristische Gleichung hat k verschiedene Lösingen $d_1, \ldots, d_k$.
$w_i = \left(1, d_i, d_i^2, d_i^3, \ldots\right), i = 1, \ldots, k$ bilden Basis des Lösungsraums.
Seien Anfangswerte $a_1, \ldots, a_k$ vorgegeben.

$$\begin{aligned} R(a) &= (a_1, \ldots, a_k, a_{k+1}, a_{k+2}, \ldots) \\ &= s_1 w_1 + \ldots + s_k w_k \\ &= \left(s_1, s_1 d_1, \ldots, s_1 d_1^{n-1}, \ldots\right) + \ldots + \left(s_k, s_k d_k, \ldots, s_k d_k^{n-1}, \ldots\right) \\ &= \left(s_1 + \ldots + s_k, s_1 d_1 + \ldots + s_k d_k, \ldots, s_1 d_1^{n-1} + \ldots + s_k d_k^{n-1}, \ldots\right) \end{aligned}$$

Löse das LGS für $s_1, \ldots, s_k$: $\Rightarrow$ $s_1, \ldots, s_k$ sind eindeutig bestimmt.

$$\begin{array}{ccccccc} s_1 & + & \ldots & + & s_k & = & a_1 \\ s_1 d_1 & + & \ldots & + & s_k d_k & = & a_2 \\ \vdots & + & & + & \vdots & = & \vdots \\ s_1 d_1^{k-1} & + & \ldots & + & s_k d_k^{k-1} & = & a_k \end{array}$$

Satz 1.4.
Gegeben sei homogene lineare Rekursion der Ordnung k.

$$(R_n) \quad x_n = c_1 x_{n-1} + \ldots + c_k x_{n-k} \quad c_k \neq 0, \ \forall n > k$$

a) Ist $d \in \mathbb{C}$ eine Lösung der char. Gleichung $t^k - c_1 t^{k-1} - \ldots - c_k = 0$, so ist $w = (1, d, d^2, \ldots)$ eine Lösung von (R_n)

b) Besitzt char. Gleichung k verschiedene Nullstellen $d_1, \ldots, d_k$, so bilden die Folgen $w_i = \left(1, d_i, d_i^2, d_i^3, \ldots\right), i = 1, \ldots, k$ Basis des Lösungsraums von R_n)

c) Unter Voraussetzung b) sei $a = (a_1, \ldots, a_k) \in \mathbb{C}^k$ beliebiger Vektor von Anfangswerten und $s_1, \ldots, s_k$ die Lösung des LGS so ist $R(a) = (s_1 + \ldots +$

$$\begin{array}{ccccccc} s_1 & + & \ldots & + & s_k & = & a_1 \\ s_1 d_1 & + & \ldots & + & s_k d_k & = & a_2 \\ \vdots & + & & + & \vdots & = & \vdots \\ s_1 d_1^{k-1} & + & \ldots & + & s_k d_k^{k-1} & = & a_k \end{array}$$

$s_k, s_1 d_1 + \ldots + s_k d_k, s_1 d_1^2 + \ldots + s_k d_k^2, \ldots)$ d.h. $a_n = d_1^{n-1} s_1 + \ldots + d_k^{n-1} s_k$

Beispiel 1.5.
Fibonacci-Folge aus Beispiel 1.2a: $F_n = F_{n-1} + F_{n-2}, n \geq 3, F_1 = 1, F_2 = 2$
Char. Gleichung: $t^2 - t - 1 = 0$
Lösungen: $d_{1,2} = \frac{1 \pm \sqrt{5}}{2}$
$s_1 + s_2 = 1$
$s_1 \left(\frac{1+\sqrt{5}}{2}\right) + s_2 \left(\frac{1-\sqrt{5}}{2}\right) = 2$
$s_1 = \frac{1}{\sqrt{5}} \left(\frac{3+\sqrt{5}}{2}\right), s_2 = \frac{1}{\sqrt{5}} \left(\frac{-3+\sqrt{5}}{2}\right)$
$F_n = \frac{1}{\sqrt{5}} \left(\frac{3+\sqrt{5}}{2}\right) \left(\frac{1+\sqrt{5}}{2}\right)^{n-1} + \frac{1}{\sqrt{5}} \left(\frac{-3+\sqrt{5}}{2}\right) \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}$

$$\boxed{F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}}$$

$x_n = c_1 x_{n-1} + \ldots + c_k x_{n-k}$
$t^k - c_1 t^{k-1} - \ldots c_{k-1} t - c_k = 0$, Nullstellen bestimmen.
d Lösung. $\left(1, d, d^2, \ldots\right)$
Falls k **verschiedene** Lösungen existieren, $d_1, \cdots, d_k$. Jede Lösung ist von der Form:

$$s_1\left(1, d_1, d_1^2, \ldots\right) + \ldots + s_k\left(1, d_k, d_k^2, \ldots\right)$$

Suche Lösung mit Anfangsbedingungen: $a_1, \ldots, a_k \quad \Rightarrow$ LGS
$F_n = F_{n-1} + F_{n-2} \quad F_1 = 1, F_2 = 2$

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}$$

$\boxed{\frac{1+\sqrt{5}}{2}}$ Zahl des Goldenes Schnitts.

Satz 1.6.
$x_n = c_1 x_{n-1} + \ldots + c_k x_{n-k}, d_1, \ldots, d_s$ verschiedene Nullstellen der charakteristischen Gleichung mit Vielfachheiten $m_1, \ldots, m_s$.

$$\left(\text{D.h. } t^k - c_1 t^{k-1} - \ldots - c_k = (t-d_1)^{m_1}(t-d_2)^{m_2} \cdots (t-d_k)^{m_s}\right)$$

Dann bilden $W_{1,1}, \ldots, W_{1,m_1}, W_{2,1}, \ldots, W_{2,m_2}, \ldots, W_{s,1}, \ldots, W_{s,m_s}$ eine Basis des Lösungsraums wobei

$$W_{i,j} = \left(i^{j-1} d_i, 2^{j-1} d_i^2, 3^{j-1} d_i^3, \ldots, n^{j-1} d_i^n, \ldots\right)$$

$i = 1, \ldots, s; j = 1, \ldots, m$ (Beweis z.B. Aigner (sihe Seite III))

Beispiel 1.7.
$x_n = 7x_{n-1} - 15x_{n-2} + 9x_{n-3}, n \geq 4$ Anfangswerte: $a_1 = 2, a_2 = 35, a_3 = 188$

$$\begin{aligned} t^3 - 7t^2 + 15t - 9 &= 0 \\ (t-1)(t^2 - 6t + 9) &= 0 \\ (t-1)(t-3)^2 &= 0 \end{aligned}$$

$$\begin{aligned} w_{1,1} &= (1, 1, 1, \ldots) \\ w_{2,1} &= (3, 3^2, 3^3, \ldots) \\ w_{2,2} &= (3, 2 \cdot 3^2, 3 \cdot 3^3, \ldots, n \cdot 3^n, \ldots) \end{aligned}$$

LGS:

$$\begin{array}{ccccccc} s_1 & + & 3s_2 & + & 3s_3 & = & 2 \\ s_1 & + & 9s_2 & + & 18s_3 & = & 35 \\ s_1 & + & 27s_2 & + & 81s_3 & = & 188 \end{array}$$

$$\begin{aligned} a^n &= s_1 + s_2 \cdot 3^n + s_3 \cdot n \cdot 3^n \\ &= -1 - 2 \cdot 3^n + n \cdot 3^{n+1} \\ &= -1 + (3n-2)3^n \end{aligned}$$

1.2 Inhomogene lineare Rekursionen

$$(R)_{exp} \quad x_n = c_1 x_{n-1} + \ldots + c_k x_{n-k} + a \cdot r^n, \quad a, r \text{ fest}, a, r \neq 0$$

Benötige eine spezielle Lösung von $(R)_{exp}$
Ansatz für spezielle Lösung: $(dr, dr^2, dr^3, \ldots, dr^n, \ldots)$ für geeignetes d. Dann muss gelten:

$$\begin{aligned} d \cdot r^n &= c_1 \cdot d \cdot r^{n-1} + \ldots + c_k \cdot d \cdot r_{n-k} + a \cdot r^n \\ \frac{d-a}{d} r^n &= c_1 \cdot r^{n-1} + \ldots + c_k r^{n-k} && \textit{Div. durch } r^{n-k} \\ \frac{d-a}{d} r^k &= c_1 \cdot r^{k-1} + \ldots + c_{k-1} r + c_k \\ -\frac{a}{d} r^k &= \underbrace{-r^k + c_1 r^{k-1} + \ldots + c_{k-1} r + c_k}_{-b} \end{aligned}$$

Ist $-b \neq 0 \;\Leftrightarrow\; d = \frac{a}{b} r^k$

Satz 1.8.
Gegeben sei $(R)_{exp} : x_n = c_1 x_{n-1} + \ldots + c_k x_{n-k} + a \cdot r^n, n > k (a, r \neq 0)$
$b = r^k - c_1 r^{k-1} - \ldots c_{k-1} r - c_k$. *Ist* $b \neq 0$, *so setze* $d = \frac{a}{b} r^k$. *Dann ist* $(dr, dr^2, dr^3, \ldots)$ *spezielle Lösung von* $(R)_{exp}$.

Beispiel 1.9 (Türme von Hanoi (1.2b)).
$a_n = 2a_{n-1} + 1, n \geq 2, a_1 1. \quad (k = 1, a = 1, r = 1)$
Char. Gleichung $t - 2$. $r = 1$ ist keine Nullstelle von $t - 2$.
$b = 1 - 2 = -1, d = \frac{a}{b} r^k = -1$. Nach Satz 1.8: $(-1, -1, -1, \ldots)$ spezielle Lösung der Rekursion. $x_n = 2x_{n-1} + 1$.
Allgemeine Lösung von $x_n = 2x_{n-1}$:

$$(s, s \cdot 2, s \cdot 2^2, \ldots), s \in \mathbb{C}$$

Allgemeine Lösung der inhomogenen System:

$$(s - 1, 2s - 1, 2^2 s - 1, \ldots, \underbrace{2^{n-1} s - 1}_{a_n}, \ldots), s \in \mathbb{C}$$

$s - 1 = a_1 = 1, s = 2$

Satz 1.10.
$(R)_{exp}$ *gegeben,* r *sei eine* m*-fache Nullstelle von* $f(t) = t^k - c_1 t^{k-1} - \ldots - c - k$, *d.h.* $f(t) = (t - r)^m \cdot g(t), g(r) \neq 0$. *Dann ist* $b := \binom{k+m}{m} r^k - c_1 \binom{k+m-1}{m} r^{k-1} - \ldots - c_{k-1} \binom{m+1}{m} r - c_k \neq 0$. *Setzt man* $d = \frac{a}{b} \cdot r^k$, *so ist*

$$\left(dr, d\binom{m+1}{m} r^2, d\binom{m+2}{m} r^3, \ldots, d\binom{m+n-1}{m} r^n, \ldots \right)$$

eine Lösung von $(R)_{exp}$.
<u>*Beweis:*</u> *Siehe Skript „Kombinatorische Mathematik in der Informatik“*

Beispiel 1.11.

a) $(R)\quad a_n = 2a_{n-1} + 2^n, \quad r = 2, a = 1, k = 1$. Anfangswert $a_1 = 4$.
Char. Gleihung $t - 2 = 0. \quad r = 2, m = 1$
Nach Satz 1.10: $b = \binom{1+1}{1} r - 2 = 2, \quad d = 1$
Spezielle Lösung: $(2, 2 \cdot 2^2, 3 \cdot 2^3, \ldots, n \cdot 2^n, \ldots)$
Allgemeine Lösung des homogenen Systems: $(s \cdot 2, s \cdot 2^2, s \cdot 2^3, \ldots)$
Allgemeine Lösung von (R) : $(2s+2, 2^2 s+s \cdot 2^2, 2^3 s+3 \cdot 2^3, \ldots, s \cdot 2^n + n \cdot 2^n, \ldots)$
Spezielle Lösung: $2s + 2 = 4,\ s = 1,\ \underline{a_n = (n+1) \cdot 2^n}$

b) $(R)\quad a_n = 3a_{n-1} - 3a_{n-2} + a_{n-3} + 1, n \geq 4, a_1 = 4, a_2 = 13, a_3 = 29$
Char. Gleihung $t^3 - 3t^2 + 3t - 1 = (t-1)^3. \quad a = 1, r = 1$
r 3-fache Nullstelle, $m = 3$
$b = \binom{3+3}{3} - 3\binom{3+3-1}{3} + 3\binom{3+3-2}{3} - \binom{3+3-3}{3} = \binom{6}{2} - 3\binom{5}{3} + 3\binom{4}{3} - 1, \quad d = 1$
Spezielle Lösung: $l = \left(1, \binom{4}{3}, \binom{5}{3}, \ldots, \binom{n+2}{3}, \ldots\right) = 20 - 3 \cdot 10 + 3 \cdot 4 - 1 = 1.$
Lösungsraum der zug. hom. Rekursion (nach Satz 1.6):

$$\begin{aligned} w_{11} &= (1, 1, \ldots) \\ w_{12} &= (1, 2, 3, 4, \ldots) \\ w_{13} &= (1, 2^2, 3^2, 4^2, \ldots) \end{aligned}$$

$$\binom{n}{i} = \frac{n!}{(n-i)!i!}$$
$$s_1 = 1,\ s_2 = 0\ s_3 = 2$$

Satz 1.12. *Geg.* (R)*pol:* $x_n = c_1 x_{n-1} + \ldots + c_k x_{n-k} + q(n)$, q *Polynom vom Grad* l. *Die char.. Gleichung* $t^k - c_1 t^{k-1} - \ldots - c_k = 0$ *habe Lösung* 1 *mit Vielfachheit* m $(m = 0$ *möglich*$)$, *d.h.* $t^k - c_1 t^{k-1} - \ldots - c_k = (t-1)^m \cdot g(t),\ g(1) \neq 0$. *Dann gibt es ein Polygon*

$$p(t) = b_m t^m + \ldots + + b_{m+l} t^{m+l}, b_m, \ldots, b_{m+l} \in \mathbb{C},$$

sodass $(p(1), p(2), p(3), \ldots)$ *Lösung von* (R)*pol ist. Die Koeffizienten* $b_m, \ldots, b_{m+l}$ *lassen sich folgender Maßen bestimmen.*
Man setzt $p(n), p(n-1), \ldots, p(n-k)$ *für* $x_n, \ldots, x_{n-k}$ *in* (R)*pol ein, multiplizieret aus, ordnet nach Potenzen von* n *und bestimmt* $b_m, \ldots, b_{m+l}$ *durch Koeffizientenvergleich.*

Beispiel 1.13.
Bubblesort: $V(n) = V(n-1) + (n-1), \quad V(1) = 0$
$\left(\text{Klar } V(n) = \frac{n^2-n}{2}\right)$

$$x_n = x_{n-1} + \underbrace{(n-1)}_{q(n)} \qquad l = 1$$

Kapitel 2

Wachstum und Rekursionsformen

Satz 2.1.
Sei (R) $x_n = ax_{n-1} + g(n)$ für $n \geq 2, a > 1$. Gegeben sei Anfangswert $a_1 = g_1$. Sei $(a_1, a_2, \ldots)$ Lösung von (R) zum Anfangswert a_1.

a) Ist $|g(n)| \in O(a^{n(1-\varepsilon)})$ für $\varepsilon > 0$, so ist $|a_n| \in O(a^n$. Ist überdies $g(n) \geq 0$ für alle n, g macht die Nullfunktion, ς_0 ist $a_n \in \Theta(a^n)$. (Dann ist $a_n \geq 0$ f.a. n)

b) Ist $|g(n)| \in \Theta(n^k (\log n)^l a^n)$ für $k, l \in \mathbb{N}_0$, so ist $|a_n| \in O(n^{k+1} (\log n)^l a^n)$. Ist überdies $g(n) \geq 0$ für alle $n \geq n_1$ (n_1 geeignet), so ist $a_n \in \Theta(n^{k+1} (\log n)^l a^n)$ (und $a_n \geq 0$ ab gewissen n_2.)

c) Existieren $0 < c < 1, n_2 \in \mathbb{N}$, so dass

$$0 < a \cdot g(n-1) \leq c \cdot g(n) \ \forall \ n \geq n_2,$$

so ist $a_n \in \Theta(g(n))$. (Es ist $a_n \geq 0$ für $n \geq n_3, n_3$ geeignet)

Bemerkung. Im Fall c) gilt:

$$\begin{aligned} g(n) &\geq \left(\frac{a}{c}\right)^{n-n_2} g(n_2) = \left(\frac{a}{c}\right)^n \cdot \left(\frac{c}{a}\right)^{n_2} g(n_2) \\ &= a^{n(1+\varepsilon)} \left(\frac{c}{a}\right)^{n_2} g(n_2) \forall n \geq n_2 \\ &\text{wobei } \varepsilon = -\log_a c > 0 \end{aligned}$$

$$g(n) \in \Omega\left(a^{n(1+\varepsilon)}\right)$$

Beweis. Nach 1.14 ist $a_n = \sum\limits_{i=1}^{n} g(i) \prod\limits_{j=i}^{n-1} a = \sum\limits_{i=1}^{n} g(i) a^{n-i}$

a) $|g(n)| \leq C \cdot a^{n(1-\varepsilon)}$ für geeignete Konstante C, für alle n.

$$\begin{aligned}
|a_n| &= \left|\sum_{i=1}^{n} g(i)a^{n-i}\right| \leq \sum_{i=1}^{n} \left|g(i)a^{n-i}\right| = \sum_{i=1}^{n} |g(i)| \cdot a^{n-i} \\
&\leq C \cdot a^n \sum_{i=1}^{n} a^{i(1-\varepsilon)}a^{-i} = C \cdot a^n \sum_{i=1}^{n} (a^{-\varepsilon})^i \\
&\leq C \cdot a^n \frac{1-a^{-(n+1)\varepsilon}}{1-a^{-\varepsilon}} \leq \left(C \cdot \frac{1}{1-a^{-\varepsilon}}\right) a
\end{aligned}$$

$|a_n| \in O(a^n)$. Ist $g(n) \geq 0 \forall n \in \mathbb{N}, g(n_1) > 0$ für ein $n_1 \in \mathbb{N}, a_n = \sum\limits_{i=1}^{n} g(i)a^{n-i} \geq g(n_1)a^{n-n_1} = \frac{g(n_1)}{a^{n_1}}a^n > 0$ für alls $n \geq n_1$
$a_n \in \Theta(a^n)$

b) $|g(n)| \leq C \cdot n^k(\log n)^l a^n \forall n \in \mathbb{N}$

$$\begin{aligned}
|a_n| &\leq \sum_{i=1}^{n} g(i)|a^{n-i} \leq \sum_{i=1}^{n} C \cdot i^k(\log i)^l a^i a^{n-1} \\
&\leq C \cdot a^n \cdot n \cdot n^k \cdot (\log n)^l = n^{k+1}(\log n)^l a^n
\end{aligned}$$

2.Teil: Übungsaufgabe

c) $n \geq n_2 : |a_n| \leq \sum\limits_{i=1}^{n_2-1} |g(i)|a^{n-i} + \sum\limits_{i=n_2}^{n} |g(i)|a^{n-i} \leq D \cdot a^n + \sum\limits_{i=n_2}^{n} \frac{c}{a}^{n-i} = D \cdot a^n + g(n) \sum\limits_{i=n_2}^{n} c^{n-i} = D \cdot a^n + g(n) \sum\limits_{j=0}^{n-n_2} c^j \leq D \cdot a^n + g(n)\frac{1}{1-c}$
$g(n) \geq D_1 a^{n(1+\varepsilon)} \geq D_1 a^n$.
$\frac{D}{D_1}g(n) \geq Da^n \leq \left(\frac{D}{D_1} + \frac{1}{1-c}\right) g(n)$

□

Bemerkung 2.2.

a) Wichtigster Fall in b) $k = l = 0$

$$g(n) \in \Theta(a^n) \Rightarrow a_n \in \Theta(n \cdot a^n)$$

b) Divide-and-Conquer-Alg. mit Komplexität

$$T(n) = aT(n-1) + g(n)$$

Hauptanwendungsgebiet.

Beispiel 2.3.

a) $x_n = ax_{n-1} + p(n), a > 1, p$ Polynom. $|a_n|$ Lösung.

$$|a_n| \in O(a^n), \text{ denn } p(n) \leq a^{\frac{n}{2}} - a^{n\left(1-\frac{1}{2}\right)}$$

b) $x_n = ax_{n-1} + a^n, a_n \in \Theta(n \cdot a^n)$

c) $x_n = ax_{n-1} + n!$
$0 \leq a(n-1)! \leq \frac{1}{2}n!$ für $n \geq 2a \quad \left(C = \frac{1}{2}\right)$
$a_n \in \Theta(n!) = \Theta\left(\sqrt{n}\left(\frac{n}{e}\right)^n\right)$

Satz 2.4.
$a, b, \in \mathbb{R}, a \geq 1, b > 1, k, l \in \mathbb{N}_0$
$\frac{n}{b}$ steht für $\lfloor \frac{n}{b} \rfloor$ oder $\lceil \frac{n}{b} \rceil$. Gegeben sei

$$(R) \quad x(n) = a \cdot x\left(\frac{n}{b}\right) + g(n) \text{ für } n \geq b$$

$g(n)$ sei monoton wachsend, nicht negativ, nicht die Nullfunktionen. Gegeben seien Anfangswerte $a_i =: g(i)$ für $i = 1, \ldots, \lceil b \rceil - 1$. Sei $(a_1, a_2, \ldots)$ die zugehörige Lösug von (R)

a) Ist $g(n) \in O\left(n^{(\log_b a) - \varepsilon}\right)$ für ein $\varepsilon > 0$, so ist $a_n \in \Theta\left(n^{\log_b a}\right)$

b) Ist $g_n \in \Theta\left((\log n)^k \cdot (log \log n)^l \cdot n^{\log_b a}\right)$, so ist
$a_n \in \Theta\left((\log n)^{k+1} \cdot (\log \log n)^l \cdot n^{\log_b a}\right)$

c) Existiert $0 < c < 1$ mit $a \cdot g\left(\lceil \frac{n}{b} \rceil\right) \leq c \cdot g(n)$ für alle $n \geq n_0$ (n_0 geeignet), so ist $a_n \in \Theta(g(n))$.

Bemerkung. Ähnlich wie in 2.1 kann man Zeigen, dass im Fall c) gilt:

$$g(n) \in \Omega\left(n^{\log_b a + \varepsilon}\right), \text{ wobei } \varepsilon = -\log_b c$$

Beweisidee:
Ist $n = b^m, m \in \mathbb{N}_0, b$ ganzzahlig, so setze $x_m = x(m), g(m) = g(n)$. Dann $x_m = a \cdot x_{m-1} + g(m)$. Anw. von 2.1 liefert 2.4 für die spez. n.

Beispiel 2.5.

a) Wichtigster Fall: $a = b > 1$.
Dann:

- $g(n) \in O\left(n^{1-\varepsilon}\right) \Rightarrow a_n \in \Theta(n)$
- $g(n) \in \Theta(n) \Rightarrow a_n \in \Theta(n \log n)$

b) 1.2.e: MergeSort
$V(n) = 2 \cdot V\left(\frac{n}{2}\right) + (n-1)$
Nach a): $V(n) \in \Theta(n \log n)$

c) $X(n) = 2 \cdot x\left(\frac{n}{2}\right) + n \log n, n \geq 2, a_1 \geq 0$ Anf.Wert

$$a_n \in \Theta\left(n(\log n)^2\right)$$

d) $x(n) = 2 \cdot x\left(\frac{n}{2}\right) + n^2, n \geq 2, a_1 \geq 0$

$$a_n \in \Theta\left(n^2\right)$$

$2\left(\frac{n}{2}\right)^2 = \frac{n^2}{2} \Rightarrow c = \frac{1}{2}$ in 2.4.c

e) Multiplikation großer Zahlen:
Übliches Verfahren: $x = x_1 \cdot 2^{\frac{n}{2}} + x_2, y = y_1 \cdot 2^{\frac{n}{2}} + y_2$ (n-stellige Binärzahlen)
$x \cdot y = x_1 \cdot y_1 \cdot 2^n + (x_1 y_2 + x_2 y_1) \cdot 2^{\frac{n}{2}} + x_2 y_2$
Anzahl der Bitop. $T(n) = 4 \cdot T\left(\frac{n}{2}\right) + f(n), f(n) \in \Theta(n)$
Schneller (Karatsuba-Multiplikation):
$u = (x_1 + x_2)(y_1 + y_2), v = x_1 y_1, w = x_2 y_2$
$x \cdot y = v \cdot 2^n + (u - v - w) 2^{\frac{n}{2}} + w$
$T(n) = 3 \cdot T\left(\frac{n}{2}\right) + g(n), g(n) \in \Theta(n)$

Kapitel 3

Erzeugende Funktionen

$(a_0, a_1, \ldots) \longmapsto \sum_{i=0}^{\infty} a_i t^i$ formale Potenzreihe

Definition 3.1.

a) Eine formale Potenzreihe ist ein Ausdruck der Form

$$\phi(t) = a_0 + a_1 t + a_2 t^2 + \cdots = \sum_{i=0}^{\infty} a_i t^i, a_i \in \mathbb{C}$$

Terme mit $a_i = 0$ kann man weglassen. Existiert ein k ,it $a_n = o$ für alle $n > k$, dann ist $\phi(t) = a_0 + a_1 t + \ldots + a_k t^k$ formales Polynom.

b) Zwei formale Potenzreihen $\phi(t) = \sum ait^i, \psi(t) = \sum = b_i t^i$ sind gleich, wenn $a_i = b_i$ für alle $i \in \mathbb{N}_0$

c) $\phi(t), \psi(t)$ wie in b).
$(\phi + \psi)(t)\,(= \phi(t) + \psi(t)) := \sum_{i=0}^{\infty} (a_i + b_i) t^i$
$(\phi \cdot \psi)(t)\,(= \phi(t) \cdot \psi(t)) := \sum_{i=0}^{\infty} c_i t^i$, wobei

$$c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

Beispiel.
$\phi(t) = \sum_{i=0}^{\infty} t^i$
$\psi(t) = \sum_{i=0}^{\infty} i \cdot t^i$
$\phi(t) \cdot \psi(t) = \sum_{i=0}^{\infty} c_i t^i$
$c_i = \sum_{j=0}^{i} 1 \cdot j = \frac{i(i+1)}{2}$
$\phi(t) \cdot \psi(t) = \sum_{i=0}^{\infty} \frac{i(i+1)}{2} t^i$

Bemerkung 3.2. Mit + und $\cdot$ aus 3.1 wird die Menge der formalen Potenzreihen über $\mathbb{C}$ wird kommutativer Ring mit Eins:

$$\mathbb{C}\,[[t]]$$

Unterring: formale Polynome $\mathbb{C}[t]$

Satz 3.3.

a) $\phi(t) \cdot \psi(t) = 0 \leftarrow$ *Potenzreihen mit allen Koeff.* $= 0$
$\Rightarrow\ \phi(t) = 0$ *oder* $\psi(t) = 0$

b) $\phi(t) = \sum_{i=0}^{\infty} a_i t^i$ *invertierbar bezüglich* $\cdot$ *(d.h.* $\exists \psi(t)$ *mit* $\phi(t) \cdot \psi(t) = 1 \leftarrow c_0 = 1, c_{i \neq 0} = 0$*)*

$$\Longleftrightarrow a_0 \neq 0$$

Beweis.

a) Ang. $\phi(t) \cdot \psi(t) = 0$, aber $\phi(t) \neq 0, \psi(t) \neq 0$. Wähle n, m minimal mit $a_n \neq 0, b_m \neq 0$. $\phi(t) \cdot \psi(t)$ Koeff. von $t^{n+m} = a_n b_m \neq 0$. ↯

b) $\phi(t) = \sum_{i=0}^{\infty} a_i t^i$

$$\begin{aligned}
\phi(t) \text{ invertierbar} &\Leftrightarrow \exists \psi(t) = \sum_{i=0}^{\infty} b_i t^i \text{ mit } \phi(t) \cdot \psi t = 1 \\
&\Leftrightarrow 1 = \left(\sum_{i=0}^{\infty} a_i t^i\right) \cdot \left(\sum_{i=0}^{\infty} b_i t^i\right) = \sum_{i=0}^{\infty} c_i t^i \\
&\Leftrightarrow c_0 = 1, c_i = 0 \text{ für alle } i \geq 1 \\
&\Leftrightarrow a_0 b_0 = 1 \\
&\quad\ a_o b_1 + a_1 b_0 \\
&\quad\ a_o b_2 + a_1 b_1 + a_2 b_0 \\
&\Leftrightarrow a_0 \neq 0,\ b_0 = a_0^{-1} = \frac{1}{a_0} \\
&\quad\ b_1 = -\frac{a_1 b_0}{a_0} \\
&\quad\ b_2 = -\frac{a_1 b_1 + a_2 b_0}{a_0} = (-a_1 b_1 - a_2 b_0) \cdot a_0^{-1} \\
&\quad\ b_i = \left(-\sum_{j=1}^{i} a_j b_{i-j}\right) \cdot a_0^{-1}
\end{aligned}$$

□

Beispiel 3.4.

a) $\frac{1}{1-\alpha t} = (1-\alpha t)^{-1} = \sum\limits_{i=0}^{\infty} \alpha^i t^i, \quad \alpha \in \mathbb{C}$

$(1-\alpha t)\cdot\left(\sum\limits_{i=0}^{\infty} \alpha^i t^i\right) = 1 + \underbrace{(1\cdot\alpha - \alpha\cdot 1)}_{0} t + \ldots + \underbrace{(\alpha^i - \alpha^i)}_{0} t^i + \ldots = 1$

Speziell: $\frac{1}{1-t} = \sum\limits_{i=0}^{\infty} t^i$, $\frac{1}{1+t} = \sum\limits_{i=0}^{\infty} (-1)^i t^i$

b) $k \in \mathbb{N}$

$(1\alpha t)^{-k} = \left((1-\alpha t)^{-1}\right)^k = \left((1-\alpha t)^k\right)^{-1}$

$$\left((1-\alpha t)^{-1}\right)^k = \left(\sum_{i=0}^{\infty} \alpha^i t^i\right)^k = \sum_{i=0}^{\infty} \left(\sum_{\substack{\text{alle geordneten n-Tupel} \\ (i_1,\ldots,i_k), i_j \in \{0,\ldots,i\} \\ i_1,\ldots,i_k = i}} \alpha^{i_1+i_2+\ldots+i_k} \right) t^i$$

Definition 3.5.

a) Für $r \in \mathbb{R}, n \in \mathbb{N}$ ist der verallgemeinerter Binominialkoeffizient

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

und $\binom{r}{0} = 1$. (Stimmt für $r \in \mathbb{N}$ mit normalem Binominialkoeffizient überein.)

Beispiel.

$$\binom{\frac{1}{2}}{3} = \frac{\frac{1}{2}\cdot\left(\frac{1}{2}-1\right)\left(\frac{1}{2}-2\right)}{3!} = \frac{\frac{1}{2}\cdot\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)}{6} = \frac{3}{8\cdot 6} = \frac{1}{16}$$

b) $(1+\alpha t)^r := \sum\limits_{i=0}^{\infty} \binom{r}{i} \alpha^i t^i$, für $r \in \mathbb{R}$

Für $r \in \mathbb{N}_0$ $\surd$, für $r \in \mathbb{Z} \setminus \mathbb{N}_0$, d.h. $r = -k, k \in \mathbb{N}$ $\surd$

$$\begin{aligned}\binom{-k}{i} &= \frac{(-k)(-k-1)\ldots(-k-i+1)}{i!} \\ &= \frac{(-1)^i k(k+1)\ldots(k+i-1)}{i!} = (-1)^i\binom{k+i-1}{i}\end{aligned}$$

Satz 3.6.

a) $(1+\alpha t)^r (1+\alpha t)^s = (1+\alpha t)^{r+s}\ \forall \alpha \in \mathbb{C},\ r,s \in \mathbb{R}$

b) $\left((1+\alpha t)^r\right)^{-1} = (1+\alpha t)^{-r}$

Beweis. a) Mühsames Nachrechnen

b) $(1+\alpha t)^r (1+\alpha t)^{-r} \stackrel{a)}{=} (1+\alpha t)^0 = 1$

□

Bemerkung 3.7.
Nach 3.6a): $(1+\alpha t)^{\frac{1}{2}} \cdot (1+\alpha t)^{\frac{1}{2}} = (1+\alpha t)$. $(1+\alpha t)^{\frac{1}{2}} = \sum\limits_{i=0}^{\infty} \binom{\frac{1}{2}}{i} \alpha^i t^i$ ist tatsächlich Quadratwurzel aus $1+\alpha t$. Ebenso: $-\sum\limits_{i=0}^{\infty} \binom{\frac{1}{2}}{i} \alpha^i t^i$. Andere Wurzeln gibt es nicht.
$\phi(t)^2 = \psi(t)^2 \Rightarrow (\phi(t) - \psi(t))(\phi(t) + \psi(t)) = 0$.
$\overset{3.3a)}{\Rightarrow} \phi(t) = \pm\varphi(t)$

Satz 3.8 (Partialbruchzerlegung)**.**
Sei $p(t), q(t) \in \mathbb{C}[t], \mathrm{Grad} p(t) < \mathrm{Grad} q(t)$.
$q(t) = (t-\alpha_1)^{n_1} \cdot \ldots \cdot (t-\alpha_r)^{n_r}, \alpha_i \in \mathbb{C}$ *Nullstelle von* q.

$$\frac{p(t)}{q(t)} = \frac{a_{11}}{t-\alpha_1} + \frac{a_{12}}{(t-\alpha_1)^2} + \ldots + \frac{a_{1n_1}}{(t-\alpha_1)^{n_1}} + \ldots + \frac{a_{r1}}{t-\alpha_r} + \ldots + \frac{a_{rn_r}}{(t-\alpha_r)^{n_r}}$$

für geeignete komplexe Zahlen $a_{11}, \ldots, a_{1n_1}, \ldots, a_{rn_r}$*, diese sind eindeutig bestimmt.*
(Beweis: Hachenberger, Mathematik für Informatiker, 2. Auflage, s.520-526)

Beispiel 3.9.

$$\frac{\overbrace{4+2t}^{p(t)}}{\underbrace{(t-1)(t-2)}_{q(t)}} \overset{3.8}{=} \frac{a_1}{t-1} + \frac{a_2}{t-2}$$
$$= \frac{a_1(t-2) + a_2(t-1)}{(t-1)(t-2)}$$
$$= \frac{(-2a_1 - a_2) + (a_1 + a_2)t}{q(t)}$$

$$\text{Koeffizientenregel:} \quad \begin{aligned} -2a_1 - a_2 &= 4 \\ a_1 + a_2 &= 2 \\ &\Rightarrow a_1 = -6, a_2 = 8 \end{aligned}$$

$\Rightarrow \frac{4+2t}{(t-1)(t-2)} = -\frac{6}{t-1} + \frac{8}{t-2}$

Definition 3.10.
Jeder Folge $(a_0, a_1, \ldots)$ kann man eine formale Potenzreihe zuordnen, $\phi(t) = \sum\limits_{i=0}^{\infty} a_i t^i$. $\phi(t)$ ist die erzeugende Funktion für die Folge $(a_0, a_1, \ldots) \leftrightarrow \phi(t)$.

Beachte: $t^n \cdot \phi(t) \leftrightarrow \left(\underbrace{0, \ldots, 0,}_{n} a_0, a_1, \ldots\right)$

Beispiel 3.11.
$a_n = \frac{3}{2}a_{n-2} - \frac{1}{2}a_{n-1}, n \geq 2, a_0 = 2, a_1 = 4$

$$\begin{aligned}
\phi(t) &= a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \dots \\
\frac{3}{2}t\phi(t) &= 0 + \frac{3}{2}a_0 t + \frac{3}{2}a_1 t^2 + \frac{3}{2}a_2 t^3 + \dots \\
-\frac{1}{2}t^2\phi(t) &= 0 + 0 - \frac{1}{2}a_0 t^2 - \frac{1}{2}a_1 t^3 - \dots \\
\frac{3}{2}t^2\phi(t) - \frac{1}{2}t\phi(t) &= \frac{3}{2}a_0 t + \underbrace{\frac{3}{2}a_1 - \frac{1}{2}a_0}_{=a_2} t^2 + \underbrace{\frac{3}{2}a_2 - \frac{1}{2}a_1}_{=a_3} t^3 + \dots
\end{aligned}$$

Ab t^2 stimmt $\frac{3}{2}t\phi(t) - \frac{1}{2}t^2\phi(t)$ mit $\phi(t)$ überein. Daher $\phi(t) = a + bt + \frac{3}{2}t\phi(t) - \frac{1}{2}t^2\phi(t)$. $2 = a_0 = a, 4 = a_1 = b + \frac{3}{2}a_0 = b + 3 \Rightarrow b = 1$

$$\phi(t) = 2 + t + \frac{3}{2}t\phi(t) - \frac{1}{2}t^2\phi(t)$$

$$\begin{aligned}
\phi(t) \cdot \underbrace{\left(1 - \frac{3}{2}t + \frac{1}{2}t^2\right)}_{\text{invert. in}\mathbb{C}[[t]]} = 2 + t : \phi(t) &= \frac{2+t}{1 - \frac{3}{2}t + \frac{1}{2}t^2} \\
&= \frac{4+2t}{(t-1)(t-2)} \\
&= \frac{-6}{t-1} + \frac{8}{t-2}
\end{aligned}$$

$-\frac{6}{t-1} = (-6) \cdot (-1) \frac{1}{1-t} \overset{3.4a)}{=} 6 \cdot \sum t^i$
$\frac{8}{t-2} = 8 \cdot \left(-\frac{1}{2}\right) \frac{1}{1 - \frac{1}{2}t} \overset{3.4a)}{=} -4 \sum \left(\frac{1}{2}\right)^i t^i$
$\underline{a_n = 6 - 4\left(\frac{1}{2}\right)^n \ \forall n \geq 0}$

Definition 3.12 (Erzeugende Funktionen und homogene lineare Rekursion)**.**
Geg. $a_n = c_1 a_{n-1} + \ldots + c_k a_{n-k} \forall n \geq k, c_k \neq 0, a_0, \ldots, a_{k-1}$ Anfangswerte

1) $\phi(t) \leftrightarrow (a_0, a_1, a_2, \ldots)$
   $c_1 t \cdot \phi(t) \leftrightarrow (0, c_1 a_0, c_1 a_1, \ldots)$
   $\vdots$
   $c_k t^k \phi(t) \leftrightarrow (0, \ldots, 0, c_k a_0, c_k a_1, \ldots)$
   $c_1 t\phi(t) + c_2 t^2 \phi(t) + \cdots + c_k t^k \phi(t) =$
   $c_1 a_0 t + (c_1 a_1 + c_2 a_0) t^2 + \cdots + (c_1 a_{k-2} + \cdots + c_{k-1} a_0) t^{k-1}$
   $+ \underbrace{(c_1 a_{k-1} + c_2 a_{k-2} + \cdots + c_k a_0)}_{=a_k} t^k + a_{k+1} t^{k+1} + \cdots + a_n t^n + \cdots$
   Also: $\phi(t) = s_0 + s_1 t + \ldots + s_{k-1} t^{k-1} + c_1 t\phi(t) + c_2 t^2 \phi(t) + \ldots + c_k t^k \phi(t)$
   $s_0, \ldots, s_{k-1}$ best. durch Koeffvgl. an den Stellen $t^0, \ldots, t^{k-1}$ von $\phi(t)$ und $c_1 t\phi(t) + \ldots + c_k t^k \phi(t)$.

2) $\phi(t)\left(\underbrace{1-c_1t-c_2t^2-\cdots-c_kt^k}_{\text{invertierbar in }\mathbb{C}[[t]]}\right)=s_0+s_1t+\cdots+s_{k-1}t^{k-1}$

$$\begin{aligned}\phi(t)&=\frac{s_0+s_1t+\cdots+s_{k-1}t^{k-1}}{1-c_1t-\cdots-c_kt^k}\\&=\frac{\left(-\frac{1}{c_k}\right)\left(s_0+s_1t+\cdots+s_{k-1}t^{k-1}\right)}{t^k+\underbrace{\frac{c_{k-1}}{c_k}}_{=b_{k-1}}t^{k-1}+\cdots+\underbrace{\frac{c_1}{c_k}}_{=b_1}t+\underbrace{\left(-\frac{1}{c_k}\right)}_{=b_0}}\end{aligned}$$

3) Bestimme in $\mathbb{C}$ Nullstellen von $t^k+b_{k-1}t^{k-1}+\cdots+b_1t+b_0$
$\phi(t)=\frac{\left(-\frac{1}{c_k}\right)\left(s_0+s_1t+\cdots+s_{k-1}t^{k-1}\right)}{(t-\alpha)^{m_1}\cdot\ldots\cdot(t-\alpha)^{m_r}}, \alpha_i\neq\alpha_j$ für $i\neq j, m_i\in\mathbb{N}, \sum m_i=k$

4) Führe Partialbruchzerlegung gemäß 3.8 durch:

$$\phi(t)=\frac{a_{11}}{t-\alpha_1}+\cdots+\frac{a_{1,m_1}}{(t-\alpha_1)^{m_1}}+\cdots+\frac{a_{r1}}{t-\alpha_r}+\cdots+\frac{a_{r,m_r}}{(t-\alpha_r)^{m_r}},\ a_{ij}\in\mathbb{C}$$

5) Für jeden

$$\begin{aligned}\frac{1}{(t-\alpha_i)^j}&=(t-\alpha_i)^{-j}=(-\alpha_i)^{-j}\left(1-\frac{1}{\alpha_i}t\right)^{-j}\\&=(-\alpha_i)^{-j}\sum_{n=0}^{\infty}\binom{n+j-1}{n}\left(\frac{1}{\alpha_i}\right)^n t^n\end{aligned}$$

6) Aus 4) und 5) ergibt sich:

$$\begin{aligned}a_n&=\sum_{i=1}^{r}\sum_{j=1}^{m_i}a_{ij}(-\alpha_i)^{-j}\binom{n+j-1}{n}\left(\frac{1}{\alpha_i}\right)^n\\&=\sum\sum(-1)^j a_{ij}\binom{n+j-1}{n}\left(\frac{1}{\alpha_i}\right)^{n+j}\end{aligned}$$

geschlossene Form.

7) Vergleich mit 1.6:

$$\begin{aligned}\binom{n+j-1}{n}&=\frac{(n+j-1)!}{n!(j-1)!}=\frac{(n+j-1)\cdot\ldots\cdot(n+1)}{(j-1)!}\\&=\text{ Polynom in } n \text{ von Grad } j-1\end{aligned}$$

a_n = Summe von Termen der Form $f_{ij}\cdot n^{j-1}\left(\frac{1}{\alpha}\right)^n$ α_i ist Nullstelle von $1-c_1t-\cdots-c_kt^k \Leftrightarrow$
$\frac{1}{\alpha_i}$ ist Nullstelle von $t^k-c_1t^{k-1}-\cdots-c_k$
Lösung entspricht genau 1.6

Beispiel 3.13 (Catalan-Zahlen).
1.2d): $c_n = \sum\limits_{i=1}^{n-1} c_i c_{n-i},\ n > 1,\ c_1 = 1.$
Setze $c_0 = 0$

$$c_n = \underbrace{\sum_{i=0}^{n} c_i c_{n-i}}_{\text{Koeff. von } \phi(t)^2} \quad , \ n > 1$$

Koeff. von $\phi(t)$ und von $\phi(t)^2$ stimmen an allen Potenzen $t^n, n \geq 2$ überein
$\phi(t) = \sum\limits_{n=0}^{\infty} c_n t^n$
$\phi(t) : 0 \cdot t^0 + 1 \cdot t + c_2 t^2 + \dots$
$\phi(t)^2 : 0 \cdot t^0 + 0 \cdot t + 1 \cdot t^2 + \dots$
$\Rightarrow \ \phi(t) = \phi(t)^2 + t$
$\left(\phi(t) - \frac{1}{2}\right)^2 = \frac{1}{4} - t = \frac{1-4t}{4}$
$\phi(t) = \frac{1}{2} \pm \frac{1}{2} \sum\limits_{n=0}^{\infty} \binom{\frac{1}{2}}{n} (-4)^n t^n$
Koeff. bei t^0 im $\phi(t) = 0$: Minuszeichen bei der Wurzel
$n \geq 1:$

$$\begin{aligned} c_n &= -\frac{1}{2} \binom{\frac{1}{2}}{n} (-4)^n \\ &= \left(-\frac{1}{2}\right) (-1)^n \frac{4^n}{n!} \underbrace{\left(\frac{1}{2}\right) \cdot \left(-\frac{1}{2}\right) \cdot \left(-\frac{3}{2}\right) \cdot \dots \cdot \left(-\frac{2n-3}{2}\right)}_{n \text{Faktoren}} \\ &= \frac{1}{2^{n+1}} \cdot \frac{2^{2n}}{n!} \cdot 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n-3) \end{aligned}$$

$(2n-2)! = 1 \cdot 3 \cdot \dots \cdot (2n-3) \cdot \underbrace{2 \cdot 4 \cdot \dots \cdot (2n-2)}_{2^{n-1} \cdot (n-1)!} \Rightarrow 1 \cdot 3 \cdot (2n-3) = \dfrac{(2n-2)!}{2^{n-1}(n-1)!}$

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

Bemerkung (Methoden der erzeugenden Funktionen für Rekursionen).
$\phi(t)$ Drücke die Rekursion durch möglichst einfache allgemeine Gleichung in $\phi(t)$ aus (im Ring $\mathbb{C}[[t]]$). Versuche nach $\phi(t)$ aufzuhören, so dass $\phi(t)$ durch explizit angebbare Potenzreihen beschrieben wird. Koeffizientenvergleich liefert geschlossene Form der Rekursionsglieder.

Kapitel 4

Grundlagen der abzählenden Kombinatorik

Satz 4.1.
$n, k \in \mathbb{N}$

a) Anzahl der Möglichkeiten aus einer Menge mit n Elementen k Elemente auszuwählen:

	ohne	*mit Wdh.*
ohne	$\binom{n}{k}$	$[n]_k$
mit	$\binom{n+k-1}{k}$	n^k

Berücksichtigen der Reihenfolge
$\binom{n}{k} = \frac{n!}{k!(n-k)!}$
$k > n \Rightarrow \binom{n}{k} = 0$
$[n]_k = n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}$
$k > n \Rightarrow [n]_k = 0$

b) $\sum\limits_{k=0}^{n} \binom{n}{k}$ = *Anzahl aller Teilmengen einer Menge mit n Elementen* $= 2^n$

c) $\binom{n+k-1}{k} = |\{(x_1, \ldots, x_n) : x_i \in \mathbb{N}_0, \sum x_i = k\}|$

Beispiel 4.2.
Wie viele Möglichkeiten gibt es 12 identische Kugeln in 8 verschiedene Kisten zu verteilen (Kisten können beliebig viele Kugeln aufnehmen oder leer bleiben.).

$$\text{mit 4.1c):} \quad \binom{8+12-1}{12} = \binom{19}{12} = \frac{19!}{12!7!} = 50.388$$

Satz 4.3.
Die Anzahl der Möglichkeiten k unterschiedliche/identische Objekte auf n unterschiedliche/identische Kisten zu verteilen, wobei nicht alle Kisten belegt sein müssen und Kisten auch mehrere Objekte enthalten können, beträgt:

$k \backslash n$	*id. Kisten*	*unter. Kisten*
id. Obj.	$P_n(k)$	$\binom{n+k-1}{k}$
unter. Objekte	$\sum_{i=1}^{n} S(k,i)$	n^k

Definition 4.4.

a) A sei eine Menge. Eine Partition von A ist eine Menge $\{A_1, \ldots, A_r\}$, $A_i \subseteq A, A_i \neq \emptyset, A_i \cap A_j = \emptyset \ \forall i \neq j \ A = A_1 \cup \ldots \cup A_r$

b) Die Anzahl aller Partitionen einer Menge mit k Elementen in r (nicht-leere) Teilmengen wird mit $S(k,r)$ bezeichnet.
<u>Stirling-Zahlen 2. Art</u> (James Stirling, 1692-1770)

$$S(k,r) = 0, \text{ falls } r > k \qquad \text{Bsp.: } S(4,2) = 7$$

c) Die Anzahl aller Partitionen einer Menge mit k Elementen: B_k (<u>Bell-Zahlen</u>)

$$B_k = \sum_{r=1}^{k} S(k,r)$$

d) $P_n(k)$ = Anzahl der Zerlegungen von k in Summanden aus $\mathbb{N}_0$, ohne Berüksichtigen der Reihenfolge der Summanden

$$= \left| \left\{ (x_1, \ldots, x_n) : x_i \in \mathbb{N}_0, x_1 \geq x_2 \geq \ldots \geq x_n, \sum_{i=1}^{k} x_i = k \right\} \right|$$

(<u>Partialzahl</u>) Bsp.: $P_8(12) = 70$

Beweis von 4.3.

a) k unterschiedliche Objekte auf k unterschiedliche Kisten

$$\begin{array}{lcccccc} \text{Object:} & 1 & 2 & \ldots & k & \Rightarrow & n^k \\ & \uparrow & \uparrow & & \uparrow & & \\ & & n & \text{Knoten zur Auswahl} & & & \end{array}$$

b) k identische Objekte auf n unterschiedliche Kisten $\binom{n+k-1}{k}$ siehe Bsp. 4.2

c) k unterschiedliche Objekte, n identische Kisten
Anzahl = Anzahl aller Partitionen einer Menge mit k Elementen in höchstens n Teilmengen

d) Anzahl $= |[\{x_1, \ldots, x_n\}; x_1 \geq x_2 \geq \ldots \geq x_n, \sum x_i = k]|$ = Eine Kiste enthält x_1 Objekte, eine x_2 Objekte, ...

$\square$

Satz 4.5.
Wie 4.3, aber keine Kiste darf leer bleiben

$k \backslash n$	*id. Kisten*	*unter. Kisten*
id. Obj.	$P_n(k) - P_{n-1}(k)$	$\binom{k-1}{n-1}$
unter. Objekte	$S(k,n)$	$S(k,n) \cdot n!$

Beweis. Fälle mit identischen Kisten folgen direkt aus 4.3.
unterschiedliche Objekte/unterschiedliche Kisten: Eine Partition fürt zu $n!$ Verteilungsmöglichkeiten.
identische Objekte/unterschiedliche Kisten: Lege ein Objekt in jede Kiste. Verteile $k-n$ Objekten auf n Kisten nach 4.3

$$\text{Anzahl: } \binom{n+k-n-1}{k-n} = \binom{k-1}{k-n} = \binom{k-1}{n-k}$$

□

Definition 4.6 (Einschließungs-Ausschließungsprinzip)**.**
$S_1, \ldots, S_m$ endliche Mengen

$$|S_1 \cup \ldots \cup S_m| = \sum_{k=1}^{m} (-1)^{k+1} \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq m} |S_{i_1} \cap S_{i_2} \cap \ldots \cap S_{i_k}|$$

$(m = 2: \quad |S_1 \cup S_2| = |S_1| + |S_2| - |S_1 \cap S_2|)$

Beweis. Induktion nach m: $m = 2$ $\surd$
$m - 1 \to m:$

$$\begin{aligned}
|S_1 \cup \ldots \cup S_m| &= |S_1 \cup \ldots \cup S_{m-1}| + |S_m| - |(S_1 \cup \ldots \cup S_{m-1}) \cap S_m| \\
&= |S_1 \cup \ldots \cup S_{m-1}| + |S_m| - |(S_1 \cap S_m) \cup \ldots \cup (S_{m-1} \cap S_m)| \\
&= \sum_{k=1}^{m-1} (-1)^{k+1} \sum_{1 \leq \ldots \leq m-1} |S_{i_1} \cap \ldots \cap S_{i_k}| + |S_m| \\
&\quad - \sum_{k=1}^{m-1} (-1)^{k+1} \sum_{1 \leq \ldots \leq m-1} |S_{i_1} \cap \ldots \cap S_{i_k} \cap S_m| \\
&= \sum_{k=1}^{m} (-1)^{k+1} \sum_{1 \leq \ldots \leq m} |S_{i_1} \cap \ldots \cap S_{i_k}|
\end{aligned}$$

□

Satz 4.7. *A, B Mengen, $|A| = k, |B| = n$. Dann gilt:*

Abb. $A \to B$	*alle*	*injektiv*	*surjektiv*	*bijektiv*
Anzahl	n^k	$[n]_k$	$\sum_{j=0}^{n-1} (-1)^j \binom{n}{j} (n-j)^k$	$0, n \neq k$ $n!, n = k$

Beweis.

- alle Abb. $[a_1 \to b_1, \ldots, a_k \to b_k] \leftarrow A$.
  $\Rightarrow$ n^k Möglichkeiten für $b_1, \ldots, b_k$. $\surd$
- injektive Abb. $\surd$
- bijektive Abb. $\surd$
- Anzahl der surjektiven Abb.: $B = \{b_1, \ldots, b_n\}$.

$T_i := \{\alpha : A \to B : b_i \notin \alpha(A)\}, i = 1, \ldots, n. \alpha \in T_i \Leftrightarrow \alpha : A \to B \setminus \{b_i\}$
$S =$ Anzahl der surjektiven Abbildungen $A \to B$
$T =$ Menge aller Abbildungen

$$|S| = |T| - |T_1 \cup \ldots \cup T_n| \quad |T| = n^k$$

Bestimme $|T_1 \cup \ldots \cup T_n|$ nach 4.6
$|T_i| = (n-1)^k$ mit $n = \binom{n}{1}$ Möglichkeiten dür i
$i < j : |T_i \cap T_j| = (n-2)^k$ mit $n = \binom{n}{2}$ Möglichkeiten für i, j
$\vdots$
$|T_1 \cap \ldots \cap T_n| = (n-n)^k = 0$ mit $\binom{n}{n}$ Möglichkeiten

$$\begin{aligned} 4.6 : &|T_1 \cup \ldots \cup T_n| \\ &= \sum_{j=1}^{n} (-1)^{j+1} \sum_{1 \le i_1 < i_2 < \ldots < i_j \le n} |T_1 \cap \ldots \cap T_n| \\ &= \sum_{j=1}^{n} (-1)^{j+1} \binom{n}{j} (n-j)^k \end{aligned}$$

$$\begin{aligned} |S| = |T| - |T_1 \cup \ldots \cup T_n| &= n^k - \sum_{j=1}^{n} (-1)^{j+1} \binom{n}{j} (n-j)^k \\ &= n^k + \sum_{j=1}^{n-1} (-1)^{j+1} \binom{n}{j} (n-j)^k = \sum_{j=0}^{n-1} (-1)^{j+1} \binom{n}{j} (n-j)^k \end{aligned}$$

$\square$

Korollar 4.8.

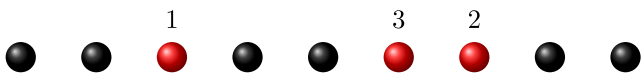
$$S(k, n) = \frac{1}{n!} \sum_{j=0}^{n-1} (-1)^{j+1} \binom{n}{j} (n-j)^k$$

Partition einer Menge mit k Elementen in n paarweise disjunkten Teilmengen.

Beweis. $|A| = k, |B| = n$ Anzahl der surjektiven Abb. von $A \to B =$ Anzahl aller Möglichkeiten, k verschiedene Objekte auf n verschiedene Plätze anzuordnen, wobei jeder Platz besetzt sein muss $\overset{4.5}{=} S(k, n) \cdot n!$ $\square$

Satz 4.9. *Gegeben sein n verschieden Sorten von Gegenständen (Gegenstände der gleichen Sorte sind nicht unterscheidbar). Von den $j-ten$ Sorte seien k_j Exemplare gegeben, $j = 1, \ldots, n, k_j \in \mathbb{N}_0, k_1 + \cdots + k_n = k$.*
Dann gilt es $\frac{k!}{k_1!k_2!\cdot\cdots\cdot k_n!}$ Möglichkeiten, diese k Gegenstände auf k Plätze anzuordnen.

Beweis. Nummeriere alle k Gegenstände durch. Jetzt sind alle unterscheidbar. Jetzt gibt es $k!$ Anordnungen.



Lösche Markierungen an Sorte 1.

Dann nur noch $\frac{k!}{k_1!}$ veschiedene Anordnungen. Fahre so fort. □

Beispiel. Je 3xA, C und je 4xG, T. Wieviele Anordnungen dieser auf 14 Plätze gibt es?

$$\frac{14!}{3!3!4!4!} = 4.204.200$$

Kapitel 5

Probabilistische Methoden für Existenzbeweise und Anzahlabschätzungen

Idee an einfachem „Zählbeispiel“

Definition 5.1 (Boole'sche Funktionen)**.**

a) Boole'sche Funktion in n Variablen ist Abb. $f : \{0,1\}^n \to \{0,1\}$. Z.B. Beschreibung von Bool'schen Funktionen durch Wertetabellen mit 2^n Zeilen. Andere Möglichkeit: Beschreibung durch Aussagenlogische Ausdrücke in n Variablen. z.B. $(\neg x_1 \wedge x_2) \vee x_3$

b) Jede Boole'sche Funktion lässt sich durch aussagenlogische Formel in n Variablen darstellen, z.B. mit Hilfe der DNF:

$$f = \bigvee_{\substack{(a_1,\ldots,a_n)\in\{0,1\}^n \\ f(a_1,\ldots,a_n)=1}} \bigwedge_{\substack{i \\ a_i=0}} \neg x_i \wedge \bigwedge_{\substack{i \\ a_i=1}} x_i$$

c) Aussagenlogische Ausdruck enthält max.

- $2^n - 1$ $\vee$-Symbole
- $2^n \cdot (n-1)$ $\wedge$-Symbole
- $2^n \cdot n$ $\neg$-Symbole
- $2^n \cdot n$ Variablen

max. $3 \cdot 2^n \cdot n$ Symbole $O(2^n \cdot n)$

d) Frage: Gibt es für jede Boole'sche Funktion „kurze“ aussagenlogische Formeln, die die Funktion beschreiben?
Antwort: Nein

Satz 5.2 (Shannon)**.**
Für jede $n \in \mathbb{N}$ gibt es Boole'sche Funktion, in n Variablen, die sich nicht durch eine logische Formel (mit $x_1, \ldots, x_n, \vee, \wedge, \neg, (,)$) mit kürzerer Länge als $\frac{2^n}{\log(n+6)}$ beschreiben lässt.

Beweis.
Anzahl der Boole'schen Funktionen in n Variablen: $2^{(2^n)}$. $m \in \mathbb{N}$. Wieviele aussagenlogische Funktionen der Länge $\leq m$ gibt es?
Maximal $(n+6)^m$ viele.
Wenn $2^{(2^n)} > (n+6)^m$, dann gibt es eine Boole'sche Funktion, die sich nicht durcch aussagenlogische Formel der Länge $\leq m$ darstellen lässt.

$$2^{(2^n)} > (n+6)^m \Leftrightarrow 2^n > m \cdot \log(n+6) \Leftrightarrow m < \frac{2^n}{\log(n+6)}$$

□

Bemerkung 5.3 (Lupanov).
Jede Boole'sche Funktion lässt sich beschreiben durch aussagenlogische Formel der Länge $\leq c \cdot \frac{2^n}{\log(n)}$

Satz 5.4.
Sei $0 < \varepsilon < 1$. Sei $a_\varepsilon(n)$ die Anzahl der Boole'schen Funktionen, die sich durch logische Formel der Länge $\leq \frac{(1-\varepsilon)2^n}{\log_2(n)}$ darstellen lassen. Dann gilt:

$$\lim_{n\to\infty} \frac{a_\varepsilon(n)}{2^{2^n}} = 0$$

Beweis.

(1) Für jeden $\delta > 0$ existiert $n_0 \in \mathbb{N}$, sodass für alle $n \geq n_0$ gilt $\log(n+6) \leq (1+\delta)\log(n)$.

$$\lim_{x\to\infty} \frac{\log(x+6)}{\log(x)} \overset{\text{L'Hopital}}{=} \lim_{x\to\infty} \frac{\frac{1}{\ln 2}\cdot\frac{1}{x+6}}{\frac{1}{\ln 2}\cdot\frac{1}{x}} = \lim_{x\to\infty} \frac{x}{x+6}$$
$$= \lim_{x\to\infty} 1 - \frac{6}{x+6} = 1$$

(2) Setze $g_\varepsilon(n) = \frac{(1-\varepsilon)2^n}{\log_2(n)}$. Anzahl der logischen Formeln der Länge $\leq g_\varepsilon(n)$ ist maximal $(n+6)^{g_\varepsilon(n)}$. $a_\varepsilon(n) \leq (n+6)^{g_\varepsilon(n)}$. Wähle $\delta, 0 < \delta < \frac{\varepsilon}{1-\varepsilon}$ $(*)$. Nach (1). Für genügend Große n: $\log(n+6) \leq (1+\delta)\log(n)$ $(**)$

$$\frac{a_\varepsilon(n)}{2^{2^n}} \leq \frac{(n+6)^{g_\varepsilon(n)}}{2^{2^n}} = \frac{2^{\log(n+6)(1-\varepsilon)\frac{2^n}{\log(n)}}}{2^{2^n}} \overset{(**)}{\leq} \frac{2^{(1+\delta)(1-\varepsilon)2^n}}{2^{2^n}}$$
$$= 2^{\underbrace{((1+\delta)(1-\varepsilon)-1)}_{<0}\cdot 2^n}$$
$$(1+\delta)(1-\varepsilon) = 1+\delta-\varepsilon-\varepsilon\delta = 1+\delta(1-\varepsilon)-\varepsilon$$
$$\overset{(*)}{<} 1+\varepsilon-\varepsilon = 1$$

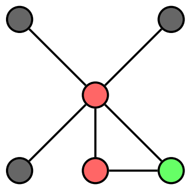
$$\Rightarrow \lim_{n\to\infty} \frac{a_\varepsilon(n)}{2^{2^n}} = 0$$

□

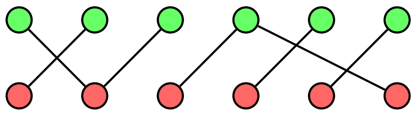
Idee: Gegeben Menge von Objekten (5.2/5.4: Boole'sche Funktionen). Zu zeigen: Es gint mindestens einen was „gut“ ist (in unserem Fall „gut“: keine Beschränkung durch kurze logische Formel). Zähle alle Objekte, bestimmt obere Schranke für die Anzahl der „schlechten“ Objekten. Falls obere Schranke < Anzahl aller Objekten $\Rightarrow$ Existenz von guten.

Definition 5.5.
X endliche Menge, M Menge von Teilmengen von X, $M \subseteq \mathcal{P}(X)$ (Mengensystem). M heißt 2-färbig, wenn sich die Elemente von X derart mit 2 Farben (rot, blau) färben lassen, so dass M keine monochromatische Teilmenge enthält (d.h. jede Menge

Beispiel.
X = Ecken (Knoten) eines einfachen, ungerichteten Graph G. M = Menge der Kanten von G; Kante auffassen als 2-Teilmenge von X.



Graph G ist 2-färbig $\Leftrightarrow$ G ist bipartit.



Definition 5.6.
Sei $k \in \mathbb{N}, k > 1$.

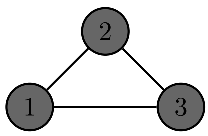
$$m(k) = \min\{|M| : M \subseteq \mathcal{P}_k(X), X \text{ endliche Menge, } M \text{ nicht 2-färbbar}\}$$

Beachte: $m(k)$ existiert.
Wähle X mit $|X| = 2k-1, M = \mathcal{P}_k(X)$. M ist nicht 2-färbbar. Es gibt mindestens k Elemente in X, die gleiche Farbe haben. Also existieren k-elementige Teilmenge von X, die monochrom ist.

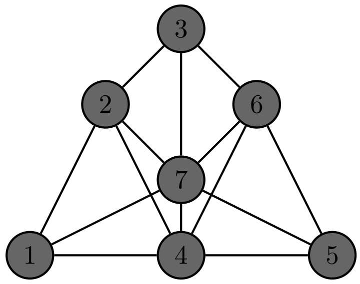
$$|M| = \binom{2k-1}{k}, \; m(k) \leq \binom{2k-1}{k}$$

Bemerkung 5.7.

a) $m(2) = 3 \;\Rightarrow\; M = \{\{1,2\},\{1,3\},\{2,3\}\}$



b) $m(3) = 7$
Zeige: M aus 3-Teilmengen, $|M| \leq 6$. $\Rightarrow$ M ist 2-färbbar.



$\Rightarrow$ nicht 2-färbbar (Projektive Ebene)
Für $k > 3$ ist $n(k)$ unbekannt.

Definition 5.8 (Wahrscheinlichkeitstheoretische Grundlagen I)**.**

a) Endlicher Wahrscheinlichkeitsraum (Ω, P), $\mathrm{P} : \mathcal{P}(\Omega) \to [0, 1]$

   (i) $\mathrm{P}(\emptyset) = 0$

   (ii) $\mathrm{P}(\Omega) = 1$

   (iii) $\mathrm{P}(A \cup B) = \mathrm{P}(A) + \mathrm{P}(B)$, falls $A \cap B = \emptyset, A, B \leq \Omega$

b) (iii) verallgemeinerbar:

$$\mathrm{P}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \mathrm{P}\left(A_i\right), \text{ falls } A_i \cap A_j = \emptyset \text{ für } i \neq j$$

c) Aus (iii) folgt: $B \subseteq A \subseteq \Omega$, so ist $\mathrm{P}(B) \leq \mathrm{P}(A)$

d) Interpretation: Ω = Menge der Ergebnissen eines Zufallsexperiment $\omega \in \Omega$ Ergebnis.
   $\mathrm{P}(A)$ = Wahrscheinlichkeit, dass Ausgang von Zufallsexperimenten in $A \subseteq \Omega$ Ereignisse.

e) Wichtiges Beispiel: Gleichverteilung

$$\mathrm{P}(\omega) = \frac{1}{|\Omega|}, A \subseteq \Omega : \mathrm{P}(A) = \frac{|A|}{|\Omega|}$$

   z.B. d) mit 'fairem' Würfel.

f) 0-1-Zufallsgolge der Länge n.
   $\Omega = \{0, 1\}^n$, alle Elemente sind gleich wahrscheinlich,
   $s \in \{0, 1\}^n : \mathrm{P}(s) = \frac{1}{2^n}$

g) $A_1, \ldots A_n \subseteq \Omega$, so $\mathrm{P}\left(\bigcup\limits_{i=1}^{n} A_i\right) \leq \sum\limits_{i=1}^{n} \mathrm{P}\left(A_i\right)$ (Subadditivität)

   Beweis.
   $B_i = A_i \setminus \bigcup\limits_{j \neq i} A_j$
   $B_i \cap B_j = \emptyset$ für $i \neq j$
   $\bigcup\limits_{i=1}^{n} B_i = \bigcup\limits_{i=1}^{n} A_i$
   $\mathrm{P}\left(\bigcup A_i\right) = \mathrm{P}\left(\bigcup B_i\right) \overset{a)(iii)}{=} \sum \mathrm{P}(B_i) \overset{c)}{\leq} \sum \mathrm{P}(A_i)$ $\square$

Satz 5.9 (Erdös, 1963).
$m(k) \geq 2^{k-1}$, d.h. jedes Mengensystem, das aus weniger als 2^{k-1} Teilmengen der Größe k besteht, ist 2-färbbar.

Beweis.
X endliche Menge. $|X| = n, \mathcal{M} \subseteq \mathcal{P}_k(X), |\mathcal{M}| = m$. Wir färben die Elemente von X mit Wahrscheinlichkeit $\frac{1}{2}$ unabhängig von einander mit blau oder rot. (Ident. $X = \{1, \dots, n\}$. (Ω, P) wie im 5.8.f mit b, r statt 0, 1. d.h. jede Färbung $\hat{=}$ b-r-Folge der Länge n ist gleich wahrscheinlich)
Sei $M \in \mathcal{M}$. Wahrscheinlichkeit, dass alle Elemente von M blau sind: $\frac{1}{2^k}$

$$\begin{pmatrix} M = \{i_n, \dots, i_k\}, A = \{s \in \Omega, s \text{ hat an den Stellen } i_n, \dots, i_k \text{ Eintrag } b\}, \\ |A| = 2^{n-k}.p(A) = \frac{|A|}{|\Omega|} = \frac{2^{n-k}}{2^n} = \frac{1}{2^k} \end{pmatrix}$$

Wahrscheinlichkeit, dass alle Elemente von M rot sind: $\frac{1}{2^k}$
Wahrscheinlichkeit, dass M monochromatisch ist:

$$\stackrel{5.8a(iii)}{=} 2 \cdot \frac{1}{2^k} = \frac{1}{2^{k-1}}$$

Wahrscheinlichkeit, dass mindestens ein $M \in \mathcal{M}$ monochromatisch ist nach 5.8g): $\leq m \cdot \frac{1}{2^{k-1}}$. Falls $m < 2^{k-1}$ folgt, Wahrscheinlichkeit, dass mindestens ein $M \in \mathcal{M}$ monochromatisch ist, ist < 1.
$\Rightarrow$ $\exists$ Fährbung, sodass kein $M \in \mathcal{M}$ monochromatisch ist. □

Bemerkung 5.10.

a) $m(k) \in \Omega\left(2^k\left(\sqrt{k} - \varepsilon\right)\right)$ für jeden $\varepsilon > 0$
$m(k) \in O\left(2^k \cdot k^2\right)$

b) Angenommen wir haben Mengensystem $\mathcal{M} \subseteq \mathcal{P}_k(X), |\mathcal{M} = 2^{k-1} - 1$. Laut 5.9 existiert Färbung der Elemente von $|X|$, so dass keine Menge in $\mathcal{M}$ monochromatisch ist. Wie findet man eine solche Färbung? Färbe X zufällig. Wahrscheinlichkeit, dass mindestens eine Menge monochromatisch ist nach Beweis von 5.9 $\leq \frac{2^k - 1}{2^{k-1}} < 1$.
t mal Wiederholungen. Wahrscheinlichkeit, dass dabei nie 2-Färbung aufgetreten ist: $\leq \left(1 - \frac{1}{2^{k-1}}\right)^t \underset{t \mapsto \infty}{\longrightarrow} 0$
$k = 5$, 15 Teilmengen, 12 Versuche (t = 12)
Wahrscheinlichkeit, 2-Färbung zu finden $\geq 1 - \left(\frac{15}{10}\right)^t > \frac{1}{2}$

<u>Grundidee:</u> Wollen Existenz eines 'guten' Objektes beweisen. Zerlege die schlechten Fälle in Teile A_i, sodass $\mathrm{P}(A_i)$ leicht berechendar sind.

$$\mathrm{P}\left(\bigcup A_i\right) \stackrel{5.8.a)}{\leq} \sum \mathrm{P}(A_i) < 1$$

Satz 5.11 (Ramsey, 1930).
Sei K_n der vollständiger Graph auf n Ecken (mit $\binom{n}{2}$ Kanten). Färbe die Kanten mit 2 Farben b, r. Seien $k, l \in \mathbb{N}, k, l \geq 2$. Ist n genügend groß, so enthält K_n entweder einen vollständigen Teilgraph (Clique) der Größe k, dessen Kanten alle rot sind, oder es existiert Clique der Größe l, deren Kanten alle blau sind.

Bemerkung 5.12.

a) 5.11 andere Formulierung:
Beliebiger Graph mit hinreichend vielen Elementen enhält entweder eine Clique der Größe k oder eine unabhängige Menge von Ecken der Größe l. (Unabhängige Menge von Ecken: keine zwei Ecken sind durch Kante verbunden)

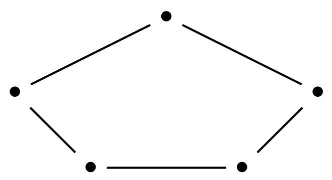
b) 5.11 gilt allgemein für t-Teilmengen (anstelle von 2-Teilmengen $\hat{=}$ Kanten) und beliebig viele Farben.

Definition 5.13 (Ramsey-Zahl)**.**
$\mathrm{R}(k, l)$ ist die kleinste natürliche Zahl n, für die 5.11 (bzgl. n, l) gilt.
Klar: $\mathrm{R}(k, l) = \mathrm{R}(l, k)$

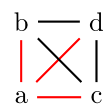
Beispiel 5.14.

a) $\mathrm{R}(2, l) = l$

b) $\mathrm{R}(3, 3) = 6$
$\mathrm{R}(3, 3) > 5$



Graph enthält keine Clique der Größe 3 und keine unabhängige Menge der Größe 3. $\mathrm{R}(3, 3) \leq 6:$ K_6: Alle Kanten färben.
Ecke a wählen. Von a gehen 5 Kanten aus. $\Rightarrow$ Es gibt 3 Kanten gleicher Farbe, rot. Wenn eine der Kanten $(a, b), (b, c), (a, c)$ rot $\Rightarrow$ rotes Dreieck.



Definition 5.15 (Zufallsgraph auf n Ecken)**.**
Wahrscheinlichkeitsraum (Ω, P)
Ω = Menge aller Graphen auf n Ecken, jedes mit gleicher Wahrscheinlichkeit von $\frac{1}{2^{\binom{n}{2}}}$
(Punktpaare erhalten mit Wahrscheinlichkeit $\frac{1}{2}$ Kante oder nicht, unabhängig voneinander)

Satz 5.16.
$\mathrm{R}(k, k) > 2^{\frac{k}{2}-1}$ *für* $k \geq 3$

Beweis. Betrachte Zufallsgraph G auf n Ecken. Für gegebene Menge von k Ecken die Wahrscheinlichkeit, dass die Clique bilden, ist $\frac{1}{2^{\binom{k}{2}}}$. Analog hat eine Menge von k Ecken die Wahrscheinlichkeit, dass sie unabhängig ist, $\frac{1}{2^{\binom{k}{2}}}$. Wahrscheinlichkeit, dass k Ecken Clique bilden oder unabhängig sind ist $\frac{2}{2^{\binom{k}{2}}}$.
5.8.h: Wahrscheinlichkeit, dass G eine Clique oder unabhängige Menge der Größe k enthält, ist $\leq \binom{n}{k}\frac{2}{2^{\binom{k}{2}}}$. Wähle n so, dass $\binom{n}{k}\frac{2}{2^{\binom{k}{2}}} < 1$.
Trivial: $\binom{n}{k} \leq n^k$
Ist $n \leq 2^{\frac{k}{2}} - 1$, so

$$\binom{n}{k}\frac{2}{2^{\binom{k}{2}}} \leq n^k \frac{2}{2^{\frac{k(k-1)}{2}}} \leq \frac{2^{\left(\frac{k}{2}-1\right)k+1}}{2^{\frac{k(k-1)}{2}}} = \frac{2^{\frac{(k-2)k+2}{2}}}{2^{\frac{k(k-1)}{2}}} < 1,$$

denn $(k-2)k + 2 = k^2 - 2k + 2 < k^2 - k = k(k-1)$, da $k > 2$.
Wahrscheinlichkeit, dass ein Graph mit $2^{\frac{k}{2}-1}$ Ecken einen vollständigen Teilgraph oder unabhängige Menge der Größe k enthällt, ist < 1. Also existiert ein Graph mit n Ecken ohne Clique der Größe k und ohne unabhängige Menge der Größe k. □

Bemerkung 5.17.
Mit besseren Abschätzungen kann man die untere Schranke verbessern. Liegen in der Nähe von $2^{\frac{k}{2}} = \left(\sqrt{2}\right)^k$. Es ist keine untere Schranke der Form c^k bekannt mit $c > \sqrt{2}$. Bekannte obere Schranke für $\mathrm{R}(k, k)$: $\sim 4^k$.

Definition 5.18 (Wahrscheinlichkeitstheoretische Grundlagen II)**.**

a) Sei (Ω, P) endliche Wahrscheinlichkeitsraum, so heißt jede Funktion $f : \Omega \to \mathrm{P}$ Zufallsvariable.

b) Ist f Zufallsvariable, so ist der Erwartungswert von f definiert durch:

$$\mathrm{E}[f] := \sum_{w \in \Omega} \mathrm{P}\left(\{w\}\right) \cdot f(w)$$

Speziell: (Ω, P) Gleichverteilt: $\mathrm{E}[f] = \frac{1}{\Omega} \sum\limits_{w \in \Omega} f(w)$ Mittelwert von f.

c) Ist $A \subseteq \Omega$, so ist die Indikatorfunktion (charakteristische Funktion) von A definiert durch

$$\mathrm{I}_A(w) = \begin{cases} 1, & \text{falls } w \in A \\ 0, & \text{falls } w \notin A \end{cases}$$

Zufallsvariable.
$\mathrm{E}[\mathrm{I}_A] = \sum\limits_{w \in \Omega} \mathrm{P}\left(\{w\}\right) = \mathrm{P}(A)$

d) Linearität des Erwartungswerts: f, g Zufallsvariable auf (Ω, P), $\alpha \in \mathbb{R}$, so $\mathrm{E}[f + g] = \mathrm{E}[f] + \mathrm{E}[g]$, $\mathrm{E}[\alpha \cdot f] = \alpha \cdot \mathrm{E}[f]$.

Satz 5.19.
Sei G ein Graph mit gerader Anzahl von Ecken, $2n$. G habe $m > 0$ Kanten. Dann lässt sich die Eckenmenge V von Ecken zerlegen in $V = A \cup B, |A| = |B| = n$, so dass mehr als $\frac{m}{2}$ Kanten zwischen A und B verlaufen.

Beweis. Wir setzen $\Omega = \mathrm{P}_n(V) = \{A \subseteq V : |A| = n\}$. $|\Omega| = \binom{2n}{n}$. $\mathrm{P}(A) = \frac{1}{|\Omega|}$ für jedes $A \in \Omega$. Def. $X : \Omega \to \mathbb{R}$: $X(A) =$ Anzahl der Kanten zwischen A und $V \setminus A$. Wir berechnen $\mathrm{E}[X]$.
Ist e Kante in G, so sei $C_e = \{A \in \Omega : e$ Kante zwischen einer Ecke in A und einer Ecke in $V \setminus A\}$. Dann gilt $X = \sum\limits_{\substack{e \text{ Kante} \\ \text{von } G}} \mathrm{I}_{C_e}$
($A \in \Omega : X(A) =$ #Kanten e zwischen A und $V \setminus A =$ #Kanten e mit $A \in C_e$, $= \sum \mathrm{I}_{C_e}(A)$)

$$\mathrm{E}[X] \overset{5.18}{=} \sum_{\substack{e \text{ Kante} \\ \text{von } G}} \mathrm{E}\left(\mathrm{I}_{C_e}\right) = \sum_{\substack{e \text{ Kante} \\ \text{von } G}} \mathrm{P}(C_e)$$

e Kante zwischen $u, v \in V$. Ingesamt gibt es $\binom{2n}{n}$ Möglichkeiten für $A \in \Omega$. Wie viele Teilmengen A von V gibt es, $|A| = n$, mit $u \in A, v \notin A$.
$A = \{u, \ldots\} : \binom{2n-2}{n-1}$. Es gibt $\binom{2n-2}{n-1}$ A's mit $|A| = n$ und $u \notin A, v \in A$.
Also: $|C_e| = 2 \cdot \binom{2n-2}{n-1}$.

$$\mathrm{P}(C_e) = \frac{2\binom{2n-2}{n-1}}{\binom{2n}{n}} = \frac{2 \cdot (2n-2)!n!n!}{(n-1)!(n-1)!(2n)!} = \frac{\cancel{2 \cdot n} \cdot n}{\cancel{(2n)}(2n-1)} = \frac{n}{2n-1} > \frac{1}{2}$$

$$\mathrm{E}[X] = \sum_{e \text{ Kante}} \mathrm{P}(C_e) > m \cdot \frac{1}{2} = \frac{m}{2}$$

Arithmetische Mittel der $X(A), A \in \Omega$. $\exists A \subseteq \Omega : X(A) > \frac{m}{2}$.
Weiterführende Literatur: Alon, Spencer, Erdös: The Probabilistische Method, Wiley 1992. $\square$

Kapitel 6

Permutationsgruppen

Definition 6.1.

a) Eine Menge G mit Verknüpfung $\cdot$ (Für alle $g, n \in G : g \cdot n \in G$) heißt Gruppe, falls gilt:

   (1) $(g \cdot h) \cdot k = g \cdot (h \cdot k) \forall g, h, k \in G$ (Assoziativitätgesetz)

   (2) Es existiert Element e (neutrales Element) mit $e \cdot g = g \cdot e = g \ \forall \ g \in G$

   (3) Zu jedem Element der Gruppe existiert ein inverses Element g^{-1}, d.h.

$$g \cdot g^{-1} = g^{-1} \cdot g = e$$

b) Eine Gruppe heißt kommutativ (oder abelsch), falls

$$g \cdot h = h \cdot g \ \forall g, h \in G$$

c) Ist G endlich, so nennt man die Anzahl der Elemente von G, $|G|$, die Ordnung von G.

Bemerkung 6.2.

a) Das neutrale Element e ist eindeutig.

b) Zu jedem $g \in G$ gibt es genau ein inverses Element.

c) Statt e schreibt man häufig 1. Schreibt man die Verknüpfung als $+$, dann bezeichnet neutrale Element mit 0 und inverse Element mit $-g$.

d) In Gruppen kann man „teilen“, d.h. jede Gleichung die Form $\underline{a} \cdot x = \underline{b}$ $(a, b \in G)$ hat eindeutige Lösung $x \in G : x = a^{-1} \cdot b$
Analog: $x \cdot a = b$ hat eindeutige Lösung: $x = ba^{-1}$

e) $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$
$(g \cdot h)(h^{-1} \cdot g^{-1}) = g \cdot (h \cdot h^{-1}) \cdot g^{-1} = e$
$\Rightarrow$ $(h^{-1} \cdot g^{-1})$ ist invers zu$(g \cdot h)$

Beispiel 6.3.

a) $(\mathbb{Z}, +)$ Gruppe, $(\mathbb{Z}, \cdot)$ keine Gruppe

b) $(\mathbb{Q} \setminus \{0\}, \cdot)$ Gruppe

c) $X = \emptyset$ Menge. Die Menge aller bijektiven Abbildungen $X \to X$ wird Gruppe bezüglich Hintereinaderausführung $\circ$.
$f : X \to X, g : X \to X$
$f \circ g : X \to X \quad (f \circ g)(x) := f(g(x))$
neutrales Element: id_x, f^{-1} existiert, da f bijektiv ist
Diese Gruppe wird mit $\mathrm{Sym}(X)$ bezeichnet, die symmetrische Gruppe auf X.
Speziell: $X = \{1, \dots, n\}$ S_n statt $\mathrm{Sym}(X)$, symmetrische Gruppe von Grad n

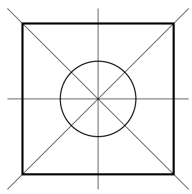
$$\pi \in S_n : \begin{pmatrix} 1 & 2 & \dots & n \\ \bar{n}(1) & \bar{n}(2) & \dots & \bar{n}(n) \end{pmatrix} (\widehat{=} (\bar{n}(1), \bar{n}(2), \dots, \bar{n}(n)))$$

Elemente vvon S_n = Permutation, $|S_n| = n!$

d) V Vektorraum, $\mathrm{GL}(V)$ = Menge der invertierbaren (bijektiven) linearen Abbildungen $V \to V$, Verknüpfung - Hintereinanderausführung, Gruppe

e) $\mathbb{R}^n$ Vektorraum, Skalarprodukt $(a, b) = \sum\limits_{i=1}^{n} a_i b_i$.
$O(\mathbb{R}^n)$ Menge der orthogonalen Abbildungen $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ (d.h. linear und $(\varphi(a), \varphi(b) = (a, b)\ \forall a, b \in \mathbb{R}^n))$ mit Hintereinanderausführung, Gruppe

f) Quadrat



Symmetriegruppe des Quadrats = Menge aller orthogonalen Abbildungen, die das Quadrat in sich überführen. Gruppe bezüglich Hintereinanderausfürung.
4 Drehungen, 4 Spiegeln
Diedergruppe D_8

Definition 6.4.
G Gruppe. $H \subseteq G$ heißt Untergruppe von G, falls H bezüglich Verknüpfung von G selbst Gruppe ist. $(H \leq G)$

Bemerkung 6.5.
$\emptyset \neq H \subseteq G$ ist Untermenge genau dann, wenn

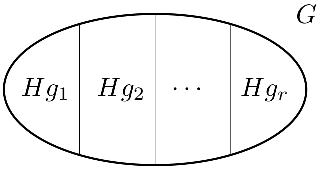
(1) $h_1 \circ h_2 \in H\ \forall h_1, h_2 \in H$

(2) $h^{-1} \in H\ \forall h \in H$

Satz 6.6 (Satz von Lagrange)**.**
Ist G eine endliche Gruppe, $H \leq G$. Dann gilt: $|H|$ ist Teiler von $|G|$.
<u>Beweisidee</u>: $H, g \in G,\ Hg := \{h \cdot g : h \in H\}$
$g_1, g_2 \in G$, so ist $Hg_1 = Hg_2$ oder $Hg_1 \cap Hg_2 = \emptyset$. Angenommen $Hg_1 \cap Hg_2 \neq \emptyset$.
Dann existieren $h_1, h_2 \in H$ mit $h_1 g_1 = h_2 g_2$. Wähle $hg_1 \in Hg_1$.

$$hg_1 = \left(hh_1^{-1}\right)(h_1 g_1) = \underbrace{\left(h \cdot h_1^{-1} \cdot h_2\right)}_{\in H} \cdot g_2 \in Hg_2$$

Analog Umkehrung $hg_2 \in Hg_1$.
$H = He, \quad H = Hh\ \forall h \in H$
Ist $x \in G$, so ist $x \in Hx,\ x = x \cdot e \in H$



$$g \in G, \begin{cases} H \to Hg \\ h \mapsto hg \end{cases} \qquad \textit{bijektiv}$$

$$|G| = \sum_{i=1}^{r} |Hg_i| = \sum_{i=1}^{r} |H| = r \cdot |H|$$

$\square$

Satz 6.7.
G endliche Gruppe, $g \in G$.
$g^0 := 1, g^m = \underbrace{g \cdot \ldots \cdot g}_{m-mal}, m \in \mathbb{N}$.

a) Es existiert ein kleinstes $n \in \mathbb{N}$ mit $g^n = 1$. (n heißt die <u>Ordnung</u> von g)

b) Es ist $\{g^0, g^1, \ldots, g^{n-1}\} \leq G$, die von g erzeugte zyklische Untergruppe von G, $\langle g \rangle$, $|\langle g \rangle| = u$

c) Es ist $n \mid |G|$ und $g^{|G|} = 1$

Beweis. a) Betrachte $\left\{g^i : i \in \mathbb{N}_0\right\}$. G endlich $\Rightarrow \exists i < j$ mit $g^i = g^j$. Multipliziert mit $\left(g^{-1}\right)^i$. $1 = g^{j-i},\ j - i \in \mathbb{N}$. Also existiert kleinstes n mit $g^n = 1$.

b) $g^0, g^1, \ldots, g^{n-1}$ sind paarweise verschieden. Mit Argumenten wie in a). $g^i \cdot g^j = g^{i+j}$. $i + j = k \cdot n + r, 0 \leq r \leq n - 1$. $g^{i+j} = (g^n)^k \cdot g^r = g^r \in \left\{g^0, \ldots, g^{n-1}\right\}$

c) $n \mid |G|$ nach b) und Lagrange. $|G| = k \cdot n, k \in \mathbb{N}$. $g^{|G|} = g^{k \cdot n} = (g^n)^k = 1$.

$\square$

Definition 6.8 (Schreibweise von Permutationen)**.**

a) Permutation $\pi \in S_n : \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$ Kurz $(\pi(1), \pi(2), \ldots \pi(n))$

b) Zyklenschreibweise

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

Zyklus $(a_1, \ldots, a_r)$ beschreibt Permutation:

$$a_1 \to a_2 \to a_3 \to \ldots \to a_r \to a_1$$

Beachte: $(1,2,5) = (2,5,1) = (5,2,1)$. Ordnung von Zyklus = Länge

c) Jede Permutation lässt sich als Produkt von elementefremden Zyklen schreiben. Eindeutig bis auf Reihenfolge der Zyklen und zyklischer Vertauschung der Ziffern innerhalb eines Zyklus. Ordnung von Permutationen = kgV der Zyklenlängen. (Einerzyklen werden oft weggelassen.)

Beispiel 6.9.

$$\begin{aligned} S_7 \quad g &= (12)(34)(56) \\ h &= (1356)(247) \\ g \cdot h &= (12)(34)(56)(1356)(247) \\ &= (1,4,7)(2,3,6)(5) \leftarrow \text{Zyklenzerlegung} h \cdot g \quad = (1356)(247)(12)(34)(56) \\ &= (1,4,5)(2,3,7)(6) \\ g \cdot h &\neq h \cdot g \end{aligned}$$

Definition 6.10.
$g \in S_n$. Der Permutationstyp von g ist das Folgende Polynom in n Variablen $x_1, \ldots, x_n$:

$$t(g) = \prod_{i=1}^{n} x_i^{k(i)}$$

$k(i)$ = Anzahl der Zyklen der Länge i in der Zyklenzerlegung von g. $\sum_{i=1}^{n} k(i) = k$ = Anzahl aller Zyklen in der Zyklenzerlegung.

$$\sum_{i=1}^{n} i \cdot k(i) = n$$

Beispiel. $g = (1234)(56)(7)(8)$
$t(g) = x_1^2 \cdot x_2 \cdot x_4$
$h = (12345678)$
$t(h) = x_8$

Definition 6.11.
Ω = endliche Menge, $\mathrm{Sym}(\Omega)$ = Gruppe aller Permutationen auf Ω. Jede Untergruppe von $\mathrm{Sym}(\Omega)$ heißt Permutationsgruppe auf Ω.

Definition 6.12.
$G \leq \mathrm{Sym}(\Omega)$. Zykluszeiger

indexZyklus!Zykluszeiger Z_G von G ist Polynom in n Variablen $x_1, \ldots, x_n$ mit Koeffizienten in $\mathbb{Q}$ ist definiert durch:

$$Z_G\left(x_1, \ldots, x_n\right) = \frac{1}{|G|} \sum_{g \in G} t(g)$$

Beispiel.

$$\begin{aligned} Z_{S_3}(x_1, x_2, x_3 \quad & g = \mathrm{id}; t(g) = x_1^3 \\ & g = (12), (13), (23); t(g) = x_1 x_2 \\ & g = (1,2,3), (1,3,2); t(g) = x_3 \\ Z_{S_3}(x_1, x_2, x_3 = & \frac{1}{6} \cdot \left(x_1^3 + 3x_1x_2 + 2x_3\right) = \frac{1}{6}x_1^3 + \frac{1}{2}x_1x_2 + \frac{1}{3}x_3 \end{aligned}$$

Definition 6.13.
$G \leq \mathrm{Sym}(\Omega)$. Definiere Relation $\sim_G$ auf Ω:

$$\alpha, \beta \in \Omega : \alpha \sim_G \beta \Leftrightarrow \exists g \in G : g(\alpha) = \beta$$

$\sim_G$ ist Äquivalenzrelation auf Ω.

(1) $\alpha \sim_G \alpha$ für alle $\alpha \in \Omega$, da $\mathrm{id}_\Omega(\alpha) = \alpha, \mathrm{id}_\Omega \in G$ (neutrales Element)

(2) $\alpha \sim_G \beta \Rightarrow \beta \sim_G \alpha : \exists g \in G : g(\alpha) = \beta$. Dann $g^{-1}(\beta) = \alpha, g^{-1} \in G$

(3) $\alpha \sim_G \beta, \beta \sim_G \gamma \Rightarrow \alpha \sim_G \gamma : \exists g, h \in G : g(\alpha) = \beta, h(\beta) = \gamma . h \circ g(\alpha) = \gamma . \alpha \sim_G \gamma$, da $h \circ g \in G$

Die Äquivalenzklassen zu $\sim_G$ heißen die <u>Bahnen</u> von G auf Ω. $\alpha \in \Omega$. $G(\alpha)$ $=$ Bahn von G auf Ω, die α enthält $= \{g(\alpha) : g \in G\}$. $\beta \in G(\alpha) : G(\beta) = G(\alpha), \beta \notin G(\alpha) : G(\alpha) \cap G(\beta) = \emptyset$.

Beispiel 6.14.

a) S_n ist transitiv auf $\{1, \ldots, n\}$.

b) $g = (123)(45) \in S_5$

$$\langle g \rangle = \left\{ \overbrace{id}^{g^0}, \overbrace{(123)(45)}^{g^1}, \overbrace{(132)}^{g^2}, \overbrace{(45)}^{g^3}, \overbrace{(123)}^{g^4}, \overbrace{(132)(45)}^{g^5} \right\}$$

$Z_G(x_1, \ldots, x_5) = \frac{1}{6}\left(x_1^5 + x_1^3 x_2 + 2x_1^2 x_3 + 2x_2 x_3\right)$

Index