

Diskrete Mathematik

Vorlesung FU Berlin, Wintersemester 2004/05 von David Ploog ploog@math.fu-berlin.de
<http://www.mathematik.hu-berlin.de/~ploog/WS2004/diskret.html>

Struktur

1 Zähltheorie

- 1.1 Kombinatorik (Kombinationen, Permutationen, Zyklen, Inklusion-Exklusion)
- 1.2 Differenzenrechnung (diskrete Stammfunktionen, Summationen)
- 1.3 Erzeugende Funktionen (formale Potenzreihen, Rekursionen, Partitionen)

2 Graphentheorie

- 2.1 Grundlagen (Ramsey-Zahlen, Wege und Zusammenhang, Bäume, 5-Farbensatz)
- 2.2 Flüsse und Netzwerke
- 2.3 Pólya-Theorie (Automorphismengruppen von Graphen, Abzählung von Graphen)

3 Kodierung und Verschlüsselung

- 3.1 Endliche Körper (multiplikative Funktionen, irreduzible Polynome)
- 3.2 Quellencodes (Komprimierung) (Entropie, Shannon-Satz, Huffman-Algorithmus)
- 3.3 Kanalkodes (Shannon-Satz; Kodes: Reed-Solomon, Hamming, Golay; Hadamard-Matrizen)
- 3.4 Kryptographie (diskretes Radizieren, diskreter Logarithmus)

4 Endliche Geometrie und diskrete Strukturen

- 4.1 Endliche algebraische Geometrie (affine ebene Kurven, Singularitäten, rationale Punkte, projektive ebene Kurven, elliptische Kurven: Gruppengesetz und Hasse-Weil)
- 4.2 Strukturen (kombinatorische Geometrien, Steiner-Systeme, Designs)

Literatur und Quellen

- A** M. Aigner: Diskrete Mathematik, Vieweg 1993
- Br** R. Brualdi: Introductory Combinatorics, Prentice Hall 1992
- GKP** R. Graham, D. Knuth, O. Patashnik: Concrete Mathematics, Addison-Wesley 1994
- vL** J. van Lint: Introduction to Coding Theory, GTM 86 Springer 1982
- vLW** J. van Lint, R. Wilson: A Course in Combinatorics, Cambridge University Press 1992

Kombinatorik: **A**§1; **Br**§3,§8.

Stirling-Zahlen, Mengenbild: **GKP**§6.1.

Differenzenrechnung: **A**§2.2; **GKP**§2.6.

Erzeugende Funktionen: **GKP**§7; **A**§3; **Br**§7.5.

Allgemeine Graphen-Theorie: **A**§5; **Br**§11; **vLW**§1.

Ramsey-Theorie: **vLW**§3.

5-Farbensatz: **Br**§13; **vLW**§33.

Netzwerke: **vLW**§7; **Br**§12; **A**§7.

Pólya-Theorie: **Br**§14; **vLW**§35.

Endliche Körper: **vL** pp.7–9 (Existenz und Eindeutigkeit, Einheitengruppe zyklisch).

Quellencodes: **A**§12.2.

Kanalkodes: Shannon-Satz in **vL**§2; Beispiele in **vL**§3, §4;

Hadamard-Matrizen, Reed-Muller-Kodes in **vLW**§18.

Kryptographie: **A**§12.5.

Elementare algebraische Geometrie

Kombinatorische Geometrien: **vLW**§23.

Steiner-Systeme und Designs: **vLW**§19; **Br**§10.

Mengenbild in der Kombinatorik

Wir zählen die Abbildungen $f : K \rightarrow N$ endlicher Mengen mit $k = \#K$, $n = \#N$. Unterscheiden die drei Fälle, ob f beliebig, injektiv oder surjektiv ist. Und betrachten die vier Möglichkeiten, ob die Elemente von K oder N unterscheidbar sind (nu=nicht unterscheidbar; u=unterscheidbar).

K	N	$f : K \rightarrow N$ ist	f beliebig	f injektiv	f surjektiv
u	u	Mengenabbildung	n^k	$n^{\underline{k}}$	$k!S_{k,n}$
nu	u	Auswahl von k aus n Elementen	$\binom{n+k-1}{k} = \frac{n^{\overline{k}}}{k!}$	$\binom{n}{k} = \frac{n^{\underline{k}}}{k!}$	$\binom{k}{k-n} = \binom{k}{n}$
u	nu	Mengenpartition von K in n Blöcke	$S_{k,1} + \dots + S_{k,n}$	$1, n \leq k$ $0, n > k$	$S_{k,n}$
nu	nu	Zahlenpartition von k in n Summanden	$p_{k,1} + \dots + p_{k,n}$	$1, n \leq k$ $0, n > k$	$p_{k,n}$

Dabei sind

$n^{\underline{k}} = n(n-1) \cdots (n-k+1)$ die fallende Faktorielle;

$n^{\overline{k}} = n(n+1) \cdots (n+k-1)$ die steigende Faktorielle;

$s_{k,n}$ die Anzahl der Permutationen in S_n mit k Zyklen (Stirling-Zahl 1. Art);

$S_{k,n}$ die Anzahl aller Mengenpartitionen von K in n nichtleere Teilmengen (Stirling-Zahl 2. Art);

$p_{k,n}$ die Anzahl der Zahlpartitionen von k in n positive Summanden.

(Oft werden die Stirling-Zahlen 1. Art als $(-1)^{k-n} s_{k,n}$ definiert.)

Es gelten die Rekursionen

$s_{k,n} = s_{k-1,n-1} + (k-1)s_{k-1,n}$ (Unterscheidung, ob n Fixpunkt der Permutation ist)

$S_{k,n} = S_{k-1,n-1} + nS_{k-1,n}$ (Unterscheidung, ob $\{n\} \subset N$ ein 1-Block der Partition ist)

$p_{k,n} = p_{k-1,n-1} + p_{n-k,n}$ (Unterscheidung, ob ein Summand der Partition 1 ist).

Für die Stirling-Zahlen gibt es eine alternative Beschreibung mit erzeugenden Funktionen

$$\sum_{k \geq n} (-1)^{k-n} s_{k,n} \frac{x^k}{k!} = \frac{1}{n!} (\log(1+x))^n, \quad \sum_{k \geq n} S_{k,n} \frac{x^k}{k!} = \frac{1}{n!} (e^x - 1)^n$$

sowie eine Darstellung als Basiswechselkoeffizienten

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

Mit Inversion bezüglich (x^n, x^{n-1}) oder Inklusion-Exklusion folgt

$$S_{n,k} = \frac{1}{k!} \sum_{i=0}^k (-1)^{k-i} \binom{k}{i} i^n.$$

Mit den diskreten Ableitungen $\Delta f(k) := f(k+1) - f(k)$ und $\nabla f(k) := f(k) - f(k-1)$ für Funktionen $f : \mathbb{Z} \rightarrow \mathbb{C}$ gilt $\Delta x^{\underline{n}} = n x^{\underline{n-1}}$ für alle $n \in \mathbb{Z}$ (mit $x^{\underline{n}} := 1/(x+1)^{-n}$ für $n < 0$). Analog $\nabla x^{\overline{n}} = n x^{\overline{n-1}}$.

Aufgaben zur Diskreten Mathematik

Abgabe von Serie 1: Bis Donnerstag, 28.10.2004 um 14 Uhr in das Tutorenfach.

Aufgabe 1. Die Fibonacci-Folge (F_n) ist definiert durch $F_1 := 1$, $F_2 := 1$ und $F_{n+2} := F_n + F_{n+1}$ für $n \neq 0$. Beweisen Sie, dass die Summen der Diagonalen im Pascal-Dreieck immer Fibonacci-Zahlen sind. (Im Diagramm ist die fünfte Diagonale fett gedruckt.)

1				
1	1			
1	2	1		
1	3	3	1	
1	4	6	4	1

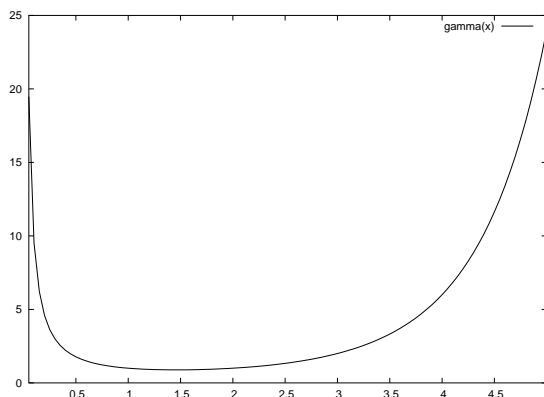
Aufgabe 2. Sei $\mathbb{Q}[x]_n := \{p \in \mathbb{Q}[x] : \deg(p) \leq n\}$ der Vektorraum der Polynome mit rationalen Koeffizienten vom Grad höchstens n . Die Polynome $x^{\underline{k}} := x(x-1)\cdots(x-k+1)$, $x^{\overline{k}} := x(x+1)\cdots(x+k-1)$ und x^k haben den Grad k und geben daher die folgenden Basen von $\mathbb{Q}[x]_n$: $B_M := \{1, x, x^2, \dots, x^n\}$ (Monome), $B_F := \{1, x, x^{\underline{2}}, \dots, x^{\underline{n}}\}$ (fallende Faktorielle), $B_S := \{1, x, x^{\overline{2}}, \dots, x^{\overline{n}}\}$ (steigende Faktorielle). Berechnen Sie im Fall $n = 4$ die Matrizen für die Basiswechsel $B_M \rightarrow B_F$ und $B_M \rightarrow B_S$, d.h. stellen Sie die Monome als rationale Linearkombinationen der fallenden bzw. steigenden Faktoriellen dar.

Lösung: Hier werden von Hand die Stirling-Zahlen berechnet.

Aufgabe 3. Ein Pokerkartenspiel enthält 52 Karten mit 13 Werten (2,3,...,10,B,D,K,A) in jeweils vier Farben ($\diamond, \heartsuit, \spadesuit, \clubsuit$). Wertvoll sind einerseits Vierling, Drilling, Pärchen, Doppelpärchen, Full House (ein Drilling und ein Zwilling) und andererseits kleine bzw. große Straße (vier bzw. fünf aufeinanderfolgende Werte beliebiger Farbe), Flush (alle fünf Karten von derselben Farbe) und Straight Flush (eine einfarbige große Straße). (Die erstgenannten Kombinationen schließen sich gegenseitig aus, so dass etwa ein Drilling nicht als Pärchen zählt.) Ermitteln Sie die Wahrscheinlichkeiten, diese Kombinationen in fünf zufällig gezogenen Karten zu erhalten. Wie ändert sich die Rangfolge der Kombinationen, wenn ein Blatt mit 32 Karten benutzt wird (das nur die Werte 7,8,9,10,B,D,K,A enthält)?

Warnung: Bei den offiziellen Pokerregeln gibt es keine Straßen aus vier Karten; dafür ist dort A,2,3,4,5 zulässig und heißt kleine Straße.

Aufgabe 4. Beweisen Sie, dass die Gamma-Funktion $\Gamma(x) := \int_0^\infty e^{-t} t^{x-1} dt$ stetig ist und $\Gamma(1) = 1$ sowie $\Gamma(x+1) = x \cdot \Gamma(x)$ für $x > 0$ erfüllt.



Aufgaben zur Diskreten Mathematik

Abgabe von Serie 2: Bis Donnerstag, 4.11.2004 um 14 Uhr in das Tutorenfach.

Aufgabe 5. Gegeben seien die folgenden Permutationen in S_5 :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix}.$$

Geben Sie $\sigma \circ \tau$ und $\tau \circ \sigma$ in Abbildungs- und in Zykelschreibweise an.

Welche Zykelklassen gibt es in S_5 und wie viele Elemente hat jede dieser Klassen?

Aufgabe 6. Zeigen Sie, dass für die Funktion $H : \mathbb{N} \rightarrow \mathbb{R}$, $n \mapsto H_n := 1 + \frac{1}{2} + \dots + \frac{1}{n}$ der Grenzwert

$$\gamma := \lim_{n \rightarrow \infty} (H_n - \ln(n))$$

existiert mit $\frac{1}{2} < \gamma < 1$. Bestimmen Sie weiterhin eine diskrete Stammfunktion von H .

Aufgabe 7. Berechnen Sie mit Hilfe der Differenzenrechnung die folgenden Summen in geschlossener Form:

$$\sum_{k=1}^n k^3, \quad \sum_{k=1}^n k^4, \quad \sum_{k=1}^n H_k, \quad \sum_{k=1}^n kH_k.$$

Aufgabe 8. Zwei Spieler A und B haben jeder ein gemischtes Pokerkartenspiel. Sie decken jeweils gleichzeitig eine Karte auf. A gewinnt, wenn dabei einmal zwei identische Karten erscheinen; anderenfalls gewinnt B . Wie hoch sind die Gewinnwahrscheinlichkeiten für A bzw. B ? Was ändert sich, wenn man Kartenspiele mit jeweils n (paarweise verschiedenen) Karten benutzt?

Lösung: Gesucht ist die Anzahl D_n aller Permutationen in S_n ohne Fixpunkte ('Derangements'). Von Hand oder mit Inklusion-Exklusion oder mit Binomialinversion erhält man $D_n = \sum_{i=0}^n (-1)^i n! / i!$. Für $n \rightarrow \infty$ strebt die Wahrscheinlichkeit $D_n/n!$ gegen $1/e \approx 0,368$ zu Ungunsten von B .

Aufgaben zur Diskreten Mathematik

Abgabe von Serie 3: Bis Donnerstag, 11.11.2004 um 14 Uhr in das Tutorenfach.

Aufgabe 9. Beweisen Sie für $a, b \in \mathbb{R}$ und $n, m \in \mathbb{N}$ die Formeln

$$\begin{aligned}(a+b)^n &= \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}, \\ \binom{a+b}{n} &= \sum_{k=0}^n \binom{a}{k} \binom{b}{n-k}, \\ \binom{n}{m} &= \binom{n-1}{m-1} + \binom{n-1}{m}, \\ (a+b)^n &= \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}.\end{aligned}$$

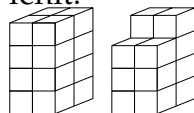
Benutzen Sie erzeugende Funktionen für die ersten drei Relationen, und dabei speziell $e^{ax} \cdot e^{bx} = e^{(a+b)x}$ sowie $(1+x)^{a+b} = (1+x)^a(1+x)^b$.

Aufgabe 10. Berechnen Sie die Anzahl der Möglichkeiten, ein Gitter vom Format 3×20 mit 3×1 -Kacheln zu pflastern. Geben Sie weiterhin die erzeugende Funktion an!



Lösung: Unterscheiden, ob die letzte Kachel senkrecht steht oder am Ende drei Kacheln liegen, gibt die Rekursion $a_n = a_{n-1} + a_{n-3}$ mit Anfangswerten $a_0 = a_1 = a_2 = 1$ und $a_3 = 2$. Die erzeugende Funktion ist $a(z) = \sum_{i \geq 1} a_i z^i = 1 + z \cdot a(z) + z^3 \cdot a(z)$, somit $a(z) = 1/(1 - z - z^3)$. Eine Nennernullstelle ist $(\sqrt[3]{108 + 12\sqrt{93}})/6 - 2/(\sqrt[3]{108 + 12\sqrt{93}})$. Man sollte $a(20)$ natürlich mit der Rekursion berechnen.

Aufgabe 11. Bestimmen Sie, wie viele Möglichkeiten es gibt, einen Turm aus $2 \times 2 \times n$ Einheitsquadraten mit $2n$ Bausteinen des Formats $1 \times 1 \times 2$ zu bauen. Betrachten Sie dafür parallel die gleiche Aufgabe mit einem solchen Turm, in dessen oberster Schicht ein $2 \times 1 \times 1$ -Stein fehlt.



Lösung: Doppelrekursion mit $a_n = 2a_{n-1} + 4b_{n-1} + a_{n-2} + \delta_{n,0}$ (für den $2 \times 2 \times n$ -Turm) und $b_n = a_{n-1} + b_{n-1}$ (wenn ein Stein fehlt). Damit für die erzeugenden Funktionen $A = 2zA + 4zB + z^2A + 1$ und $B = zA + zB$; insgesamt $A(z) = \frac{1-z}{(1+z)(1-4z+z^2)}$.
Graham/Knuth/Patashnik: Exercise 7.23.

Aufgabe 12. Ein Gefängnis habe N besetzte, verschlossene Einzelzellen. Beim ersten nächtlichen Rundgang öffnet der betrunkene Gefängniswärter jede Tür, beim zweiten Rundgang schließt er jede zweite Zelle und allgemein ändert er beim k -ten Rundgang den Status jeder k -ten Tür. Wie viele Gefangene können das Gebäude am Morgen verlassen, wenn $N = 200$ und $k = 7$? Welche glücklichen Insassen können entkommen, wenn ein noch ausdauernderer Wärter N Rundgänge macht?

Lösung: Mit Inklusion-Exklusion über gemeinsame Vielfache. Aufgabe ist zu aufwändig; besser mit $k = 5$.
Bei der zweiten Frage bleiben genau die $14 = \lfloor \sqrt{200} \rfloor$ Quadratzahlen übrig.

Aufgaben zur Diskreten Mathematik

Abgabe von Serie 4: Bis Donnerstag, 18.11.2004 um 14 Uhr in das Tutorenfach.

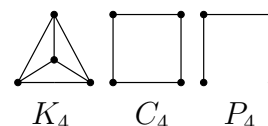
Aufgabe 13. Jede politische Karte gibt einen Graphen, wenn man als Ecken die Gebiete nimmt und zwei Ecken durch eine Kante verbindet, falls die beiden Gebiete benachbart sind. Geben Sie einen konkreten Graphen dieser Art an; zum Beispiel Deutschland (mit Bundesländern, $n = 16$), Berlin (mit neuen Bezirken und Brandenburg, $n = 13$), Südamerika (mit Staaten, $n = 13$) oder die Staaten der EU (ohne Schweden, Finnland, Großbritannien und Irland, $n = 21$). Ermitteln Sie für Ihr Beispiel Gradsequenz, Farbzahl, Cliquenzahl, Tailleweite und Durchmesser. Hat der Graph offene oder geschlossene Euler- bzw. Hamiltonwege?

Aufgabe 14. Für einen zusammenhängenden endlichen Graphen G zeige man:

G ist Baum $\iff G$ enthält keine Zykel C_n ,

G ist bipartit $\iff G$ enthält keine Zykel C_n ungerade Länge.

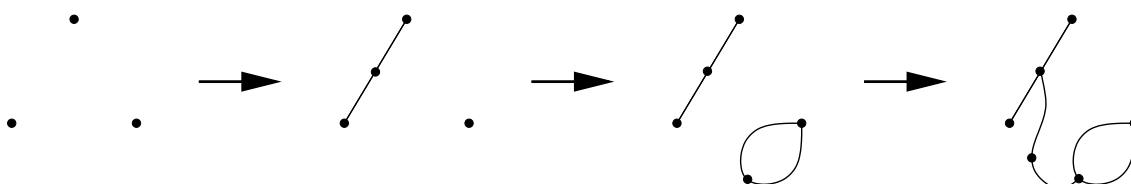
Aufgabe 15. Für zwei endliche Graphen G_1 und G_2 sei die Ramsey-Zahl $R(G_1, G_2)$ die kleinste Zahl n , so dass jede Färbung der Kanten des vollständigen Graphen K_n mit den Farben rot und blau stets einen roten Untergraphen G_1 oder einen blauen Untergraphen G_2 enthält.



Bestimmen Sie $R(P_3, P_4)$, $R(C_4, C_4)$ und $R(K_3, K_4)$.

Lösung: $R(P_3, P_4) = 4$ und $R(C_4, C_4) = 6$ von Hand. $R(K_3, K_4) \leq 10$ mit der Ramsey-Rekursion; dort sind beide Summanden gerade und daher kann Gleichheit nicht eintreten $\implies R(K_3, K_4) \leq 9$, ein explizites Beispiel zeigt $R(K_3, K_4) = 9$.

Aufgabe 16. Das 1967 von J.H. Conway erfundene Spiel Sprouts (Sprößlinge) erzeugt Multigraphen, beginnend mit n Punkten ohne Kanten. Zwei Spieler ziehen abwechselnd; ein Zug besteht darin, eine Kante einzuzichnen, so dass der Multigraph in der Zeichenebene planar bleibt mit Maximalgrad ≤ 3 . Die neue Kante erhält anschließend eine zusätzliche Ecke. Es verliert, wer keinen Zug mehr ausführen kann. Zeigen Sie, dass die Anzahl der Züge zwischen $2n$ und $3n - 1$ liegt. Sind diese Grenzen scharf für $n \leq 3$? Gewinnt bei optimalem Spiel der Anziehende oder der Nachziehende in den Fällen $n = 1$ und $n = 2$?



Die ersten drei Züge eines Spiels mit $n = 3$.

Lösung: Grenzen werden angenommen. Für $n \leq 2$ gewinnt immer der Nachziehende.

Aufgaben zur Diskreten Mathematik

Abgabe von Serie 5: Bis Donnerstag, 25.11.2004 um 14 Uhr in das Tutorenfach.

Aufgabe 17. Für einen planaren Multigraphen G sei G^* der duale Multigraph. Ein Multigraph heißt d -regulär, wenn alle Eckengrade gleich d sind.

- G^* ist immer zusammenhängend.
- Zeige, dass G und $(G^*)^*$ isomorph sind für zusammenhängendes G .
- Finde alle Paare (d_1, d_2) positiver ganzer Zahlen, für die es einen d_1 -regulären Multigraphen G gibt mit d_2 -regulärem G^* .

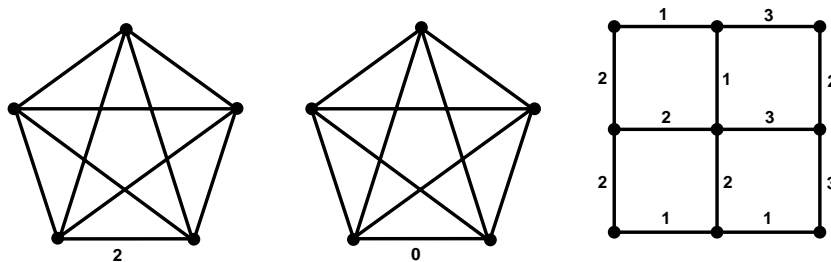
Lösung: (a) trivial; (b) braucht die korrekte Definition von G^* : einander entsprechende Kanten $e \in E(G)$ und $e^* \in E(G^*)$ müssen sich schneiden, damit gibt jede Region in G^* eine Ecke in $(G^*)^*$; (c) mit Euler-Formel, es sind die fünf regelmäßigen Polyeder möglich sowie Zykel C_n und Multigraphen mit 2 Ecken und n Mehrfachkanten zwischen diesen (also $(d_1, d_2) = (3, 3), (3, 4), (3, 5), (4, 3), (5, 3), (2, n), (n, 2)$).

Wilson/Van Lint: Problem 32E.

Aufgabe 18. Zu fixiertem $d \geq 3$ sei G ein endlicher Graph mit Maximalgrad $\leq d$, der weiterhin keinen vollständigen Graphen K_{d+1} enthalte. Man zeige, dass die Farbzahl von G durch d beschränkt ist: $\chi(G) \leq d$.

Lösung: Wilson/van Lint: Theorem 3.1.

Aufgabe 19. Wie viele aufspannende Bäume mit minimalem Gewicht enthalten die folgenden drei Graphen? Alle nicht besonders gekennzeichneten Kanten haben dabei ein Gewicht von 1.

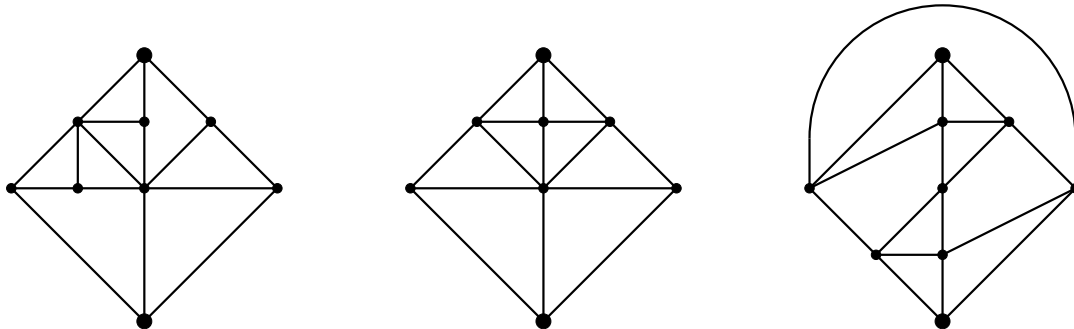


Lösung: $\#E(K_5) = \binom{5}{2} = 10$, K_5 hat $5^3 = 125$ aufspannende Bäume und jeder dieser Bäume hat vier Kanten. Wenn wir alle diese Bäume durchgehen, zählen wir 500 Kanten, also jede Kante 50-fach. Im rechten K_5 muss die 0-er Kante benutzt werden, also gibt es 50 aufspannende Bäume; dementsprechend darf im linken K_5 die 2-er Kante nicht benutzt werden und es gibt $125 - 50 = 75$ Bäume.

Der rechte Graph hat 15 minimale Bäume.

Aufgabe 20. Das von Shannon um 1960 erfundene Wechselspiel (switching game) beruht auf einem Multigraphen mit zwei markierten Ecken. Die beiden Spieler heißen P und N ; sie bezeichnen in ihrem Zug eine leere Kante mit '+' bzw. '-'. P gewinnt, wenn er einen Weg von '+'-bezeichneten Kanten zwischen den markierten Ecken erzeugen kann; anderenfalls siegt N .

Ein markierter Graph heißt *positiv*, wenn P den Sieg erzwingen kann, unabhängig davon, wer beginnt, analog für *negativ*; ansonsten heißt der Graph *unentschieden*. Was sind die Zustände der folgenden drei Graphen?



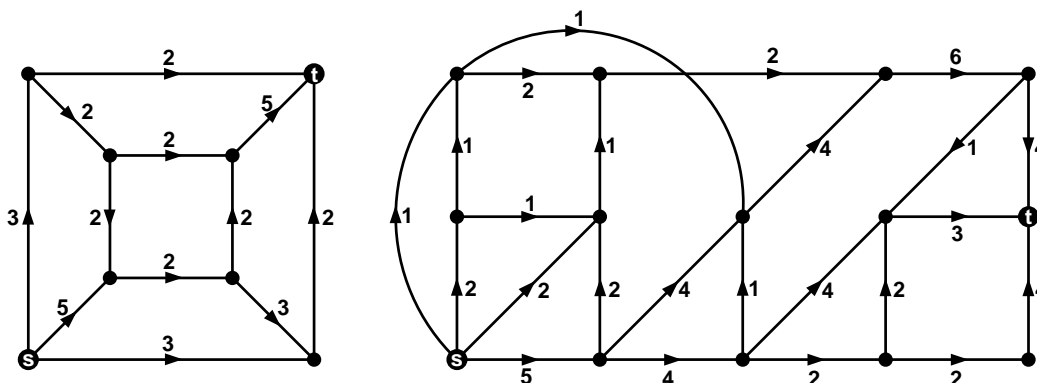
Können Sie mit Hilfe von aufspannenden Bäumen ein hinreichendes und notwendiges Kriterium dafür angeben, dass ein Graph positiv ist?

Lösung: Ein Graph G ist positiv genau dann, wenn es eine Eckenteilmenge $U \subset V(G)$ gibt, die beide markierten Ecken enthält und so dass für U zwei kantendisjunkte aufspannende Bäume existieren.
 Alle drei Graphen sind positiv.

Aufgaben zur Diskreten Mathematik

Abgabe von Serie 6: Bis Donnerstag, 2.12.2004 um 14 Uhr in das Tutorenfach.

Aufgabe 21. Bestimmen Sie die maximalen Flüsse in folgenden Netzwerken:



Lösung: Das linke Netzwerk hat einen minimalen Schnitt mit Kapazität 7 aus drei eckendisjunkten Kanten. Brualdi: Exercise 12.22.

Das rechte Netzwerk ist (ungefähr) ein Ausschnitt aus dem Berliner Straßenbahnnetz: 's'=Hackescher Markt, 't'=Prerower Platz, Kapazität=Anzahl der Linien. Es gibt mehrere minimale Schnitte mit Kapazität 8.

Aufgabe 22. Eine *Orientierung* eines Graphen G ist die Wahl einer Richtung für jede Kante in G , so dass also ein gerichteter Graph entsteht.

- Wenn alle Eckengrade in G gerade sind, so gibt eine Orientierung mit $\text{indeg}(x) = \text{outdeg}(x)$ für alle $x \in V(G)$.
- Für eine beliebige Orientierung des vollständigen Graphen K_n gibt es einen offenen, gerichteten Hamilton-Weg.

Lösung: (a) ist trivial mit Euler-Weg.

(b) indirekt oder mit vollständiger Induktion. Brualdi: Theorem 12.1.5.

Aufgabe 23. Geben Sie einen Graphen H und einen Baum T an mit minimaler Eckenzahl > 1 , die keine nichttrivialen Automorphismen haben, d.h. $\text{Aut}(H) = \{\text{id}_H\}$ und $\text{Aut}(T) = \{\text{id}_T\}$. Finden Sie weiterhin Graphen G_n mit $\text{Aut}(G_n) = \mathbb{Z}/n\mathbb{Z}$.

Lösung: $\#V(H) = 6$, $\#V(T) = 7$. Für G_n die Spiegelsymmetrie der Polygongraphen C_n brechen.

Aufgabe 24. Pflanzen Sie zehn Bäume so, dass zehn Geraden aus jeweils drei Bäumen entstehen.

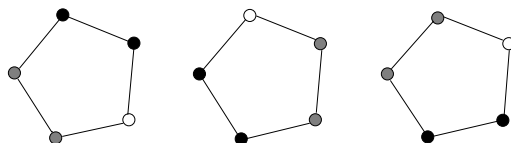
Dabei können Sie folgende Konstruktion benutzen: Für einen zusammenhängenden, nicht bipartiten Graphen G mit $V(G) = \{1, 2, \dots, v\}$ sei $2G$ der Graph mit Ecken $V(2G) := \{\pm 1, \dots, \pm v\}$ und Kanten $E(2G) := \{\{i, j\} : \{|i|, |j|\} \in E(G), ij < 0\}$. $2G$ heißt *bipartite Verdopplung* von G . Nehmen Sie die bipartite Verdopplung des Petersen-Graphen, um das Schnittverhalten der zehn Geraden zu finden.

Lösung:

Aufgaben zur Diskreten Mathematik

Abgabe von Serie 7: Bis Donnerstag, 9.12.2004 um 14 Uhr in das Tutorenfach.

Aufgabe 25. Es sei $f(n, k)$ die Anzahl der Möglichkeiten, n Kugeln in k Farben im Kreis anzuordnen, wobei Anordnungen nicht unterschieden werden sollen, wenn sie durch Drehungen oder Spiegelungen auseinander hervorgehen. Geben Sie eine Formel für $f(n, k)$ an, wenn n prim ist. Berechnen Sie damit $f(5, 3)$ und $f(3, 5)$. Was ist $f(4, 4)$?



Drei äquivalente Färbungen für $n = 5$ und $k = 3$.

Lösung: $f(n, k) = \frac{1}{2n}(k^n + (n-1)k + nk^{\frac{n+1}{2}})$ für n prim mit Burnside: D_n enthält außer der Identität $n-1$ Rotationen (n -Zykel) und n Spiegelungen (lauter 2-Zykel und ein Fixpunkt). Die Identität lässt alle k^n Färbungen invariant; die Rotationen lassen nur die k einfarbigen Färbungen invariant (da n prim) und die Spiegelungen lassen $k^{(n+1)/2}$ Färbungen invariant (für $n > 2$). $f(4, 4) = 2$.

Aufgabe 26. Ermitteln Sie die Anzahl der Isomorphietypen von Graphen mit 5 Ecken mittels Pólya-Theorie.

Lösung: $Z_{S_5}(z_1, \dots, z_5) = \frac{1}{120}(z_1^5 + 10z_1^3z_2 + 20z_1^2z_3 + 15z_1z_2^2 + 30z_1z_4 + 20z_2z_3 + 24z_5)$
 $Z_{S_5^{(2)}}(z_1, \dots, z_5) = \frac{1}{120}(z_1^{10} + 10z_1^4z_2^3 + 15z_1^2z_2^4 + 20z_1z_3^3 + 20z_1z_3z_6 + 30z_2z_4^2 + 24z_5^2)$

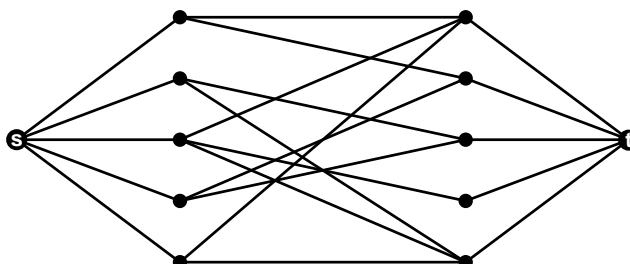
und die gesuchte Anzahl ist $Z_{S_5^{(2)}}(2, \dots, 2) = 34$.

Aigner: Skript zur Kombinatorik, 6.5, Seite 93

Aufgabe 27. Bestimmen Sie die Indexpolynome von $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$, D_8 und D_9 ; also zyklischen und Diedergruppen auf dem regelmäßigen 8-Eck bzw. 9-Eck.

Aufgabe 28. Beweisen Sie den Heiratssatz von Hall (1935): Der bipartite Graph G mit Eckenzerlegung $V(G) = V_1 \amalg V_2$ und $\#V_1 = \#V_2 =: n$ erfülle die Heiratsbedingung: Für jede Teilmenge $A \subset V_1$ gelte $\#\Gamma(A) \geq \#(A)$, wobei $\Gamma(A) \subset V(G)$ die Menge aller Nachbarn von A -Ecken ist. Dann gibt es eine vollständige Paarung, d.h. eine Kantenmenge $\{e_1, \dots, e_n\} \subset E(G)$, die den ganzen Graphen G aufspannt.

Sie können den Satz mit Hilfe des Theorems über Flüsse in Netzwerken beweisen, indem Sie den folgenden Graphen zu einem geeigneten Netzwerk erweitern.



V_1 V_2

Lösung: Alle Kanten werden von links nach rechts gerichtet. Kapazitäten auf Kanten von s bzw. nach t sind 1; Kapazitäten auf G -Kanten sind $n + 1$. Damit enthalten minimale Schnitte nur Kanten von s oder nach t . Ein maximaler Fluss f mit Flussstärke $|f| = n$ entspricht genau einer vollständigen Paarung (man beachte, dass maximale Flüsse hier ganzzahlig sind). Gäbe es einen minimalen Schnitt C mit Kapazität $c(C) < n$, dann würde er d_1 Kanten von s und d_2 Kanten nach t enthalten mit $d_1 + d_2 = c(C)$. Sei A die Menge der Endpunkte der $n - d_1$ Kanten von s nach V_1 , die nicht in C sind. Nach Voraussetzung $\Gamma(A) \subset V_2$ mit $\#\Gamma(A) \geq n - d_1$; zusammen mit den d_2 Kanten aus C von V_2 bleiben aber $n - d_1 - d_2 > 0$ Wege von s nach t übrig—Widerspruch!
Direkter Beweis in Wilson/van Lint: Theorem 5.1.

Aufgaben zur Diskreten Mathematik

Abgabe von Serie 8: Bis Donnerstag, 16.12.2004 um 14 Uhr in das Tutorenfach.

Aufgabe 29. Bestimmen Sie die Zykelpolynome der zyklischen Gruppen $\mathbb{Z}/n\mathbb{Z}$ und der Diedergruppen D_n als Untergruppen in S_n .

Lösung: $\mathbb{Z}/n\mathbb{Z}$ hat $\varphi(d)$ Elemente der Ordnung d für alle Teiler $d|n$, die (als Elemente in S_n) aus n/d Zykeln der Länge d bestehen. D_n enthält weiterhin n Spiegelungen vom Typ $[2, 2, \dots, 2, 1]$ für ungerades n sowie jeweils $n/2$ Spiegelungen der Typen $[2, 2, \dots, 2]$ und $[2, 2, \dots, 2, 1, 1]$ für gerades n . Damit

$$\begin{aligned} Z_{\mathbb{Z}/n\mathbb{Z}}(x_1, \dots, x_n) &= \frac{1}{n} \sum_{d|n} \varphi(d) x_d^{n/d} \\ Z_{D_n}(x_1, \dots, x_n) &= \frac{1}{2n} (n x_1 x_2^{(n-1)/2} + \sum_{d|n} \varphi(d) x_d^{n/d}) && \text{für } n \text{ ungerade} \\ Z_{D_n}(x_1, \dots, x_n) &= \frac{1}{2n} \left(\frac{n}{2} x_1^2 x_2^{n/2-1} + \frac{n}{2} 2 x_2^{n/2} + \sum_{d|n} \varphi(d) x_d^{n/d} \right) && \text{für } n \text{ gerade} \end{aligned}$$

Wilson/van Lint: Examples 35.1, 35.2

Aufgabe 30. Geben Sie die Gruppentafeln für \mathbb{F}_8 (mit Addition) und für $\mathbb{F}_9^* := \mathbb{F}_9 \setminus \{0\}$ (mit Multiplikation) an! Können Sie dabei die Gruppenelemente so anordnen, dass die Einsen in Ihrer Tafel das Problem lösen, acht paarweise ungedeckte Damen auf ein Schachbrett zu stellen?

Aufgabe 31. Es bezeichne $U_d(\mathbb{F}_p)$ die Anzahl der irreduziblen Polynome über dem Körper \mathbb{F}_p vom Grad d . Berechnen Sie $U_{12}(\mathbb{F}_2)$, $U_8(\mathbb{F}_3)$ und $U_6(\mathbb{F}_5)$.

Lösung: $U_n(\mathbb{F}_p) = \frac{1}{n} \sum_{d|n} \mu(n/d) p^d$; damit ist

$$\begin{aligned} U_{12}(\mathbb{F}_2) &= (2^{12} - 2^6 - 2^4 + 2^2)/12 = 4020/12 = 335, \\ U_8(\mathbb{F}_3) &= (3^8 - 3^4)/8 = 6480/8 = 810, \\ U_6(\mathbb{F}_5) &= (5^6 - 5^3 - 5^2 + 5^1)/5 = 15480/5 = 3096. \end{aligned}$$

Aufgabe 32. Sei k ein endlicher Körper. Zeigen Sie, dass dann $\#k = p^n$ für eine Primzahl p und eine natürliche Zahl n gilt.

Lösung: k enthält einen kleinsten Körper $k_0 \subset k$; er ist isomorph zu \mathbb{F}_p für eine Primzahl p . Weiterhin ist k ein k_0 -Vektorraum und somit $\#k = p^n$, wenn $n = \dim_{k_0}(k)$.

Aufgaben zur Diskreten Mathematik

Abgabe von Serie 9: Bis Donnerstag, 6.1.2005 um 14 Uhr in das Tutorenfach.

Aufgabe 33. Berechnen Sie Erzeuger der multiplikativen Gruppen \mathbb{F}_8^* , \mathbb{F}_9^* sowie \mathbb{F}_{17}^* !

Lösung: $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$, dann $\langle x \rangle = \mathbb{F}_8^*$,
 $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + 1)$, dann $\langle x + 1 \rangle = \mathbb{F}_9^*$,
 $\langle 3 \rangle = \mathbb{F}_{17}^*$.

Aufgabe 34. Bestimmen Sie die letzten beiden Dezimalstellen der Zahl $3^{(3^{(3^3)})}$.

Lösung: Zu berechnen ist $3^{(3^{(3^3)})} \in \mathbb{Z}/100\mathbb{Z}$. Wegen $\varphi(100) = 40$ und $\varphi(40) = 16$ gilt
 $3^{27} \equiv 3^{11} \equiv 27 \pmod{40}$ und $3^{(3^{(3^3)})} \equiv 3^{27} \equiv (3^9)^3 \equiv 83^3 \equiv 87 \pmod{100}$.

Aufgabe 35. Wir betrachten das Alphabet und die folgenden Quellenkodes:

- (A) die triviale Kodierung mit 5 Bits,
- (H) den Huffman-Kode,
- (M) den Morse-Kode.

Berechnen Sie die Entropie der Wahrscheinlichkeitsverteilung sowie die durchschnittlichen Wortlängen für die drei Codes. Berücksichtigen Sie dabei, dass im Morse-Kode ein drittes Symbol zur Worttrennung nötig ist. Geben Sie außerdem den Huffman-Baum im Fall des Huffman-Kodes an.

	A	B	C	D	E	F	G	H	I	J	K	L	M
%	6,51	1,89	3,06	5,08	17,4	1,66	3,01	4,76	7,55	0,27	1,21	3,44	2,53
M	10	0111	0101	011	1	1101	001	1111	11	1000	010	1011	00

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
%	9,78	2,51	0,79	0,02	7,00	7,27	6,15	4,35	0,67	1,89	0,03	0,04	1,13
M	01	000	1001	0010	101	111	0	110	1110	100	0110	0100	0011

Lösung: Entropie ist $H(0,0651, \dots, 0,0113) = 4,063$.

Der ASCII-Code hat Durchschnittslänge $L(A) = 5$.

Der Morse-Kode hat $L(M) = 3,443 \cdot \log_2 3 = 5,457$ mit zusätzlichem Trennzeichen. Der Faktor $\log_2 3$ muss benutzt werden, um den ternären Morse-Kode mit den anderen, binären Codes vergleichen zu können.

Der Huffman-Kode hat $L(H) = 4,1$.

Aufgabe 36. Zeigen Sie, dass die Entropie maximal wird bei der gleichmäßigen Wahrscheinlichkeitsverteilung, d.h. beweisen Sie für $p_1, \dots, p_n \in \mathbb{R}_+$ mit $p_1 + \dots + p_n = 1$

$$H(p_1, \dots, p_n) \leq H(1/n, \dots, 1/n).$$

Lösung: $\sum_{i=1}^n p_i \log_2 \frac{1/n}{p_i} \leq \sum_{i=1}^n p_i (\frac{1/n}{p_i} - 1) = \sum_{i=1}^n \frac{1}{n} - p_i = 0$ wegen $\log_2(t) \leq t - 1$ und somit $H(p_1, \dots, p_n) = -\sum_{i=1}^n p_i \log_2 p_i \leq -\sum_{i=1}^n p_i \log_2 n = H(1/n, \dots, 1/n)$

Aufgaben zur Diskreten Mathematik

Abgabe von Serie 10: Bis Donnerstag, 13.1.2005 um 14 Uhr in das Tutorenfach.

Aufgabe 37. Man berechne die Invarianten (n, M, d) für die folgenden beiden binären Codes, deren Kodewörter zeilenweise angegeben sind:

$$\begin{array}{l}
 \text{(a)} \quad \begin{array}{ccc} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{array}
 \end{array}
 \qquad
 \begin{array}{l}
 \text{(b)} \quad \begin{array}{cccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}
 \end{array}$$

Lösung: (a) hat $(3,4,2)$ und (b) hat $(8,4,4)$.

Aufgabe 38. Für natürliche Zahlen q, n und d sei Q ein Alphabet aus q Buchstaben und $M_q(n, d) := \max\{M : \text{es gibt einen } (n, M, d)\text{-Kode } C \subset Q^n\}$. Man zeige $M_3(3, 2) = 9$. Was ist $M_q(3, 2)$ für $q \geq 4$?

Lösung: $M_q(3, 2) = q^2$

Aufgabe 39. Wir betrachten den binären Code mit vier Wörtern der Länge 6

$$\begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{array}$$

Bestimmen Sie die Wahrscheinlichkeiten P_i , die Wörter $i = 1, \dots, 4$ bei der Übertragung auf einem symmetrischem Kanal fehlerhaft zu dekodieren, wenn die Fehler der einzelnen Bits unabhängig mit $p = 0,01$ auftreten. Es wird die Dekodierungsmethode des kürzesten Abstands benutzt. Berechnen Sie außerdem die durchschnittliche Fehlerwahrscheinlichkeit P_C des Codes.

Lösung: Besser einen unsymmetrischeren Code nehmen.

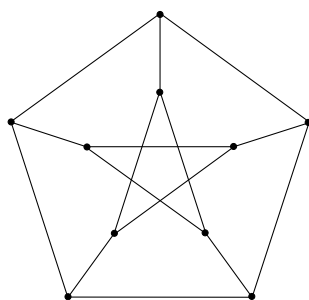
Aufgabe 40. Man zeige $\log(n!) = n \log n - n + O(\log n)$.

Lösung: Stirling-Formel

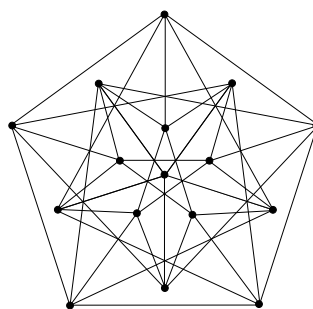
Aufgaben zur Diskreten Mathematik

Abgabe von Serie 11: Bis Donnerstag, 20.1.2005 um 14 Uhr in das Tutorenfach.

Aufgabe 41. Zu dem endlichen Graphen G mit n Ecken erhalten wir folgendermaßen eine $n \times n$ -Matrix $A(G)$: Zuerst werden die Ecken durchnummeriert; für $1 \leq i, j \leq n$ ist $A(G)_{ij} = 1$, wenn die Ecken i und j durch eine Kante verbunden sind und $A(G)_{ij} = 0$ sonst. $A(G)$ heißt *Adjazenzmatrix* von G . Diese Matrix fassen wir als binären Kode $C(G) \subset \mathbb{F}_2^n$ auf. Man gebe die Minimalabstände $d(C(G))$ für die folgenden Graphen an: vollständige Graphen, vollständige bipartite Graphen, Petersen-Graph und Clebsch-Graph.



Petersen-Graph



Clebsch-Graph

Lösung: Für Ecken $u, v \in E(G)$ ist $d(u, v) = \#\Gamma(u) + \#\Gamma(v) - \#\Gamma(u) \cap \Gamma(v)$; dabei ist $\Gamma(u) \subset E(G)$ die Menge der Nachbarecken.

$d(C(K_n)) = 1$, $d(C(K_{r,s})) = 0$, $d(C(P)) = 4$, $d(C(C)) = 6$

Aufgabe 42. Man zeige, dass ein binärer linearer perfekter Kode mit $d(C) = 7$ nur $n(C) = 7$ oder $n(C) = 23$ haben kann.

Lösung: $C \subset \mathbb{F}_2^n$ perfekt 3-fehlerkorrigierend $\Rightarrow \#C \sum_{i=0}^3 \binom{n}{i} = 2^n$; C linear $\Rightarrow \#C = 2^k$. Die Summe wird zu $(n+1)(n^2 - n + 6) = 3 \cdot 2^{l+1}$ mit $l = n - k$. Es gilt $n+1 \mid 24$ (indem man zuerst $16 \mid n+1$ annimmt und widerlegt). Von den Kandidaten $n = 7, 11, 23$ erfüllt $n = 11$ die erste Gleichung nicht.

Beide Codes existieren: $n = 7$ ist der Wiederholungskode, $n = 23$ der Golay-Kode. van Lint (GTM 86): Ex. 3.7.1

Aufgabe 43. Wir betrachten den durch die folgende Generatormatrix gegebenen binären Kode C

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Dekodieren Sie die folgenden drei empfangenen Wörter:

- (a) (1 1 0 1 0 1 1)
- (b) (0 1 1 0 1 1 1)
- (c) (0 1 1 1 0 0 0)

Lösung: van Lint (GTM 86): Ex. 3.7.7

Aufgabe 44. Berechnen Sie die Vandermonde-Determinante

$$\det \begin{pmatrix} 1 & x_1 & \cdots & x_1^{d-1} \\ 1 & x_2 & \cdots & x_2^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_d & \cdots & x_d^{d-1} \end{pmatrix} = \prod_{i < j} (x_j - x_i).$$

Lösung: Die Determinante ist ein homogenes Polynom $V(x_1, \dots, x_d) \in \mathbb{Q}[x_1, \dots, x_d]$ vom Grad $1 + 2 + \cdots + d = \binom{d+1}{2}$. Außerdem gilt $V(x_1, \dots, x_d) = 0$, sobald $x_i = x_j$ mit $i \neq j$. Das heißt aber, dass $(x_j - x_i)$ ein Teiler von $V(x_1, \dots, x_d)$ ist für alle $i < j$. Somit gilt $\prod_{i < j} (x_j - x_i) | V(x_1, \dots, x_d)$. Wegen $\deg(V(x_1, \dots, x_d)) = \deg(\prod_{i < j} (x_j - x_i))$ unterscheiden sie sich nur um einen Faktor, der genau 1 ist, wie man nach Inspektion der Koeffizienten vor $1 \cdot x_2 \cdot x_3^2 \cdots x_d^{d-1}$ sieht.

Es gibt natürlich eine Lösung mit Zeilen- und Spaltenumformungen.

Aufgaben zur Diskreten Mathematik

Abgabe von Serie 12: Bis Donnerstag, 27.1.2005 um 14 Uhr in das Tutorenfach.

Aufgabe 45. Es sei H_8 eine Hadamard-Matrix mit acht Zeilen. Man erhält einen Kode C , indem die Zeilen von H_8 zusammen mit den Zeilen von $-H_8$ genommen werden und am Ende $-1 \mapsto 1, 1 \mapsto 0$ ersetzt wird. Man zeige, dass C der erweiterte binäre Hamming-Kode vom Typ $[8, 4, 4]$ ist.

Aufgabe 46. Es sei $\mathbb{F}_4 := \mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1) = \{0, 1, \alpha, \bar{\alpha} := \alpha + 1\}$ der endliche Körper mit vier Elementen. Betrachtet wird die folgende Teilmenge von \mathbb{F}_4^6 :

$$C := \{(a, b, c, f(1), f(\alpha), f(\bar{\alpha})) : a, b, c \in \mathbb{F}_4, f(t) := at^2 + bt + c \in \mathbb{F}_4[t]\}.$$

(a) Man zeige, dass C ein $[6, 3, 4]$ -Kode über \mathbb{F}_4 ohne Wörter vom Gewicht 5 ist.

Weiter sei G die Menge aller 4×6 -Matrizen

$$A = \begin{pmatrix} a_{11} & \cdots & a_{16} \\ \vdots & & \vdots \\ a_{41} & \cdots & a_{46} \end{pmatrix} =: \begin{pmatrix} \mathbf{a}_0 \\ \mathbf{a}_1 \\ \mathbf{a}_\alpha \\ \mathbf{a}_{\bar{\alpha}} \end{pmatrix}$$

mit Einträgen aus \mathbb{F}_2 , so dass das Gewicht jeder der sechs Spalten gleich dem Gewicht der ersten Zeile ist und dass für die drei unteren Zeilen $\mathbf{a}_1 + \alpha \mathbf{a}_\alpha + \bar{\alpha} \mathbf{a}_{\bar{\alpha}} \in C$ gilt.

(b) Man zeige, dass $G \subset \mathbb{F}_2^{24}$ ein linearer \mathbb{F}_2 -Kode ist, dass seine Dimension 12 ist und dass der Minimalabstand 8 ist.

Lösung: van Lint/Wilson: Problem 20I

Aufgabe 47. Es sei G ein endlicher Graph mit $n = \#V(G)$ Ecken und $m = \#E(G)$ Kanten. Zu G konstruieren wir die *Inzidenzmatrix* $I(G)$, deren Zeilen durch $V(G)$ und deren Spalten durch $E(G)$ nummeriert werden. Der Eintrag von $I(G)$ an der Stelle (e, v) ist 1, wenn die Kante e die Ecke v berührt; ansonsten ist der Eintrag 0. Wir fassen $I(G)$ als $m \times n$ -Matrix mit Einträgen in \mathbb{F}_2 auf und bezeichnen mit $C(G) \subset \mathbb{F}_2^m$ den von den $I(G)$ -Zeilen erzeugten linearen Kode. Man zeige:

- Wenn G zusammenhängend ist, so gilt $\dim_{\mathbb{F}_2}(C(G)) = n - 1$.
Was ist die Dimension für beliebiges G ?
- $C(C_n) = \{x \in \mathbb{F}_2^n : w(x) \text{ gerade}\}$, wobei C_n der Zykelgraph mit n Ecken ist.
- $C(T) = \mathbb{F}_2^{n-1}$ für einen Baum T mit n Ecken.
- $C(K_6)^\perp$ ist ein $[15, 10, 3]$ -Kode, wobei K_6 der vollständige Graph mit 6 Ecken ist.
- $C(P)^\perp$ ist ein $[15, 6, 5]$ -Kode, wobei P der Petersen-Graph ist.

Aufgabe 48. Ist 7777 quadratischer Rest in $\mathbb{Z}/9781\mathbb{Z}$?

Aufgaben zur Diskreten Mathematik

Abgabe von Serie 13: Bis Donnerstag, 3.2.2005 um 14 Uhr in das Tutorenfach.

Aufgabe 49. Es seien p_1 und p_2 zwei verschiedene Primzahlen und k das kleinste gemeinsame Vielfache von $p_1 - 1$ und $p_2 - 1$. Weiter sei $e \in \mathbb{Z}$ mit $(e, p_1 - 1) = (e, p_2 - 1) = 1$. Man zeige, dass es ein $d \in \mathbb{Z}$ gibt mit $de \equiv 1 \pmod{p_1 - 1}$ und $de \equiv 1 \pmod{p_2 - 1}$. Damit gilt $m^{de} \equiv m \pmod{p_1 p_2}$ für alle $m \in \mathbb{Z}$.

Aufgabe 50. Wir betrachten den 4-dimensionalen affinen Raum $\mathbb{A}_{\mathbb{F}_3}^4$ über \mathbb{F}_3 . Weiter sei $P \in \mathbb{A}_{\mathbb{F}_3}^4$ ein beliebiger fixierter Punkt.

- (a) Wie viele Geraden gibt es in $\mathbb{A}_{\mathbb{F}_3}^4$?
- (b) Wie viele dieser Geraden gehen durch P ?
- (c) Wie viele Elemente hat eine maximale Teilmenge $S \subset \mathbb{A}_{\mathbb{F}_3}^4 \setminus \{P\}$, so dass $S \cup \{P\}$ keine Geraden durch P enthält?
- (d) Wie viele Elemente hat eine Geraden-lose, maximale Teilmenge von $\mathbb{A}_{\mathbb{F}_3}^4$?

Lösung: (a) Eine affine Gerade in $\mathbb{A}_{\mathbb{F}_3}^4$ besteht aus 3 Punkten und ist durch 2 davon eindeutig bestimmt. Also gibt es $3^4(3^4 - 1)/6 = 1080$ affine Geraden.

(b) Ein linearer Unterraum in \mathbb{F}_3^4 ist durch einen Vektor $\neq 0$ eindeutig bestimmt. Also gibt es $(3^4 - 1)/2 = 40$ affine Geraden durch P .

(c) Natürlich ebenfalls 40 Punkte.

(d) (Claus Härtling) Eine maximale Menge hat 20 Elemente, zum Beispiel

1000, 1110, 1120, 1101, 1102, 1211, 1211, 1212, 1221, 1222,

2010, 2020, 2001, 2002, 2211, 2212, 2221, 2222, 2100, 0100.

Die Maximalität der 20 ist von Pellegrino (1970); Claus Härtling gibt Referenzen:

T. Hirschfeld: General Galois Geometries. Oxford (1991), §27.1

Hill: Caps and codes. Discrete Mathematics 22 (1978), 111–137.

Aufgabe 51. Es sei k ein Körper mit $\text{char}(k) \neq 2$. Wir betrachten die affine ebene Kurve $C = V(f) \subset \mathbb{A}_k^2$ mit der Gleichung

$$f(x, y) = (x^2 + 1)^2 + (x^2 - 1)y^2 + y^4.$$

Bestimmen Sie die Singularitäten von C über $k = \mathbb{C}$. Welche Ordnung haben sie? Für welche q sind sie \mathbb{F}_q -rational?

Lösung: (x, y) singular $\iff y = 0, x^2 = -1$. Damit hat C über \mathbb{C} die beiden Singularitäten $(i, 0)$ und $(-i, 0)$. In \mathbb{F}_q ist -1 ein Quadrat $\iff q \equiv 1(4)$. Koordinatentransformation der Gleichung $x \mapsto x + i, y \mapsto y$ gibt eine Gleichung mit quadratischem Term $-4x^2 - 2y^2$, d.h. f hat in $(-i, 0)$ eine Singularität 1. Ordnung; die beiden Tangenten haben Richtungen $\pm\sqrt{-2}$.

Aufgabe 52. Für die affine ebene Kurve $C = V(f)$ mit

$$f(x, y) = x^3y + y^3 + x$$

bestimme man die Anzahl aller \mathbb{F}_8 -rationalen Punkte.

Aufgaben zur Diskreten Mathematik

Abgabe von Serie 14: Bis Donnerstag, 10.2.2005 um 14 Uhr in das Tutorenfach.

Aufgabe 53. Auf der über \mathbb{Q} definierten elliptischen Kurve mit affiner Gleichung $y^2 = x^3 - 36x$ liegen die Punkte $P = (-3, 9)$ und $Q = (-2, 8)$. Man berechne $P + Q$ und $2P$.

Lösung: Koblitz, Algebraic Aspects of Cryptography, Ex. 6.1.7

Aufgabe 54. Es sei k ein Körper mit Charakteristik > 3 und $a, b \in k$ fixiert. Wir betrachten die durch die homogene Gleichung

$$F(X, Y, Z) := Y^2Z - X^3 - aXZ^2 - bZ^3$$

gegebene ebene projektive Kurve $C \subset \mathbb{P}_k^2$. Man zeige, dass es im Unendlichen (d.h. $Z = 0$) keine singulären Punkte gibt. Weiter beweise man, dass C genau dann glatt ist, wenn $4a^3 + 27b^2 \neq 0$ gilt.

Lösung: Die Tangente für den unendlich fernen Punkt $P = (0 : 1 : 0)$ kann man zum Beispiel in der affinen Ebene $X \neq 0$ bestimmen. Dort hat P die Koordinaten $(1, 0)$ und die Kurve ist gegeben durch $f(y, z) = y^2z - 1 - az^2 - bz^3$. Diese Gleichung hat gar keine singulären Punkte.

Aufgabe 55. Die Zeta-Funktion der über \mathbb{F}_q definierten elliptischen Kurve E ist nach dem Satz von Hasse-Weil gegeben durch

$$Z(E/\mathbb{F}_q, T) := \exp \sum_{r \geq 1} \frac{N_r}{r} T^r = \frac{1 - (q + 1 - N_1)T + qT^2}{(1 - T)(1 - qT)},$$

wobei $N_r = \#E(\mathbb{F}_{q^r})$ die Anzahl der \mathbb{F}_{q^r} -rationalen Punkte von E ist. Das Polynom $T^2 - (q + 1 - N_1)T + q$ habe die beiden komplexen Nullstellen $\alpha, \bar{\alpha} \in \mathbb{C}$. Man zeige $N_r = q^r + 1 - \alpha^r - \bar{\alpha}^r$.

Lösung: Koblitz, Algebraic Aspects of Cryptography, Cor. 6.1.1

Aufgabe 56. Wir betrachten die elliptische Kurve E mit der projektiven Gleichung $Y^2Z = X^3 - XZ^2$ über dem Körper \mathbb{F}_5 . Man bestimme N_1 und gebe mittels Hasse-Weil eine Formel für N_r an, $r = 2, 3, 4$.

Lösung: Koblitz, Algebraic Aspects of Cryptography, Ex. 6.1.10

Aufgaben zur Diskreten Mathematik

Abgabe von Serie 15: Bis Dienstag, 15.2.2005 um 14 Uhr in das Tutorenfach. Die Serie ist freiwillig, Punkte werden aber für die Zulassung zur Klausur mitgezählt.

Ein Graph G ergibt eine kombinatorische Geometrie $L(G) := (E(G), \mathcal{F}(G))$ mit den Kanten als Punkten und folgenden Ebenen: jede Partition $V(G) = V_1 \sqcup \dots \sqcup V_k$ der Eckenmenge definiert die Ebene $\{e = (x, y) \in E(G) : x, y \in V_i \text{ für ein } i\}$, sofern alle induzierten Graphen $G|_{V_i}$ zusammenhängend sind.

Aufgabe 57. Unter der Annahme, dass G zusammenhängend ist, zeige man: Basen der kombinatorischen Geometrie $L(G)$ entsprechen genau den Kantenmengen von aufspannenden Bäumen für G .

Lösung: (Aus vL/W:) Für eine Teilmenge $S \subset E(G)$ besteht $\bar{S} \subset L(G)$ genau aus den Kanten $e = (x, y) \in E(G)$, so dass in von S induzierten Graph $G(S)$ die Ecken x und y in der gleichen Zusammenhangskomponente liegen.

van Lint/Wilson: Problem 23A

Aufgabe 58. Gibt es einen Graphen G , dessen zugehörige kombinatorische Geometrie die Fano-Ebene ist, d.h. $L(G) = PG_2(2)$? Existiert ein Graph G' , so dass $L(G') = AG_2(2)$ die affine Ebene über \mathbb{F}_2 ist?

Lösung: $L(C_4) = AG_2(2)$, dabei ist C_4 wie immer der Zykelgraph mit 4 Ecken und 4 Kanten. Die Fano-Ebene $PG_2(2)$ hat 7 Punkte; der Graph G müsste also 7 Kanten besitzen. Außerdem hat $PG_2(2)$ den Rang 3, nach der vorigen Aufgabe hätten aufspannende Bäume für G daher 3 Kanten. Es gibt solche Graphen, aber keiner gibt $PG_2(2)$.

Einfacheres Argument? $PG_2(2)$ muss $AG_2(2)$ enthalten, sogar dreimal.

Aufgabe 59. Es sei $C \subset \mathbb{F}_2^n$ ein binärer perfekter Code, der e Fehler korrigiert und den Nullvektor $0 \in C$ enthält. Es sei $\mathcal{P} := \{1, 2, \dots, n\}$ und wir identifizieren ein Wort $v \in \mathbb{F}_2^n$ mit der Teilmenge $v \subset \mathcal{P}$ der 1-Stellen von v . Man beweise, dass $(\mathcal{P}, \mathcal{B})$ mit $\mathcal{B} := \{c \subset \mathcal{P} : c \in C, d(0, c) = 2e + 1\}$ ein Steiner-System $S(e + 1, 2e + 1, n)$ bildet.

Lösung: van Lint/Wilson: Problem 20F

Aufgabe 60. Das Komplement eines Steiner-Systems $(\mathcal{P}, \mathcal{B})$ hat als Punktmenge ebenfalls \mathcal{P} , aber alle Blöcke $B \in \mathcal{B}$ werden durch ihre Komplemente $\mathcal{P} \setminus B$ ersetzt. Man zeige, dass das Komplement eines Steiner-Systems $S(t, k, v)$ wieder ein t -Design ist. Welche Kenngrößen hat es?

Lösung: Das Komplement zu $(\mathcal{P}, \mathcal{B})$ ist ein $S_\lambda(t, v - k, v)$ mit $\lambda = \binom{v-t}{k} / \binom{v-t}{k-t}$.

van Lint/Wilson: Problem 19C; das ist Theorem 19.4.

Aufgabe 61. Es sei K_6 der vollständige Graph mit 6 Ecken, dessen Kanten als Punkte einer Inzidenzstruktur betrachtet werden sollen. Blöcke seien dabei Teilmengen $B \subset E(K_6)$ aus drei Kanten, die entweder ein Dreieck oder drei disjunkte Kanten bilden. Man zeige, dass damit $(E(K_6), \mathcal{P})$ ein Steiner-System $S(2, 3, 15)$ wird. Weiter beweise man, dass es isomorph zur Struktur $(\mathbb{P}_{\mathbb{F}_2}^3, V(X + Y + Z))$ ist.

Lösung: van Lint/Wilson: Problem 19A(i)

Aufgabe 62. Es sei $H \in M(8 \times 8, \{\pm 1\})$ eine Hadamard-Matrix, deren erste Zeile und Spalte vollständig aus Einsen bestehe. Die 7×7 -Matrix M entstehe aus H durch Streichen von erster Zeile und Spalte. Wir bilden eine Inzidenzstruktur mit Punkten $\mathcal{P} := \{1, 2, \dots, 7\}$ (die wir uns als die sieben Zeilen von M vorstellen). Jede Spalte $c = (c_1, \dots, c_7)^t$ von M gibt nun einen Block $B := \{i \in \mathcal{P} : c_i = +1\}$. Man zeige, dass $(\mathcal{P}, \mathcal{B})$ ein Steiner-System $S(2, 3, 7)$ bildet.

Lösung: van Lint/Wilson: Example 19.3 mit Verallgemeinerung für beliebige Hadamard-Matrizen mit $4k$ Zeilen.

Klausur zur Diskreten Mathematik

Jede Aufgabe ist vier Punkte wert. Bei den Auswahlaufgaben 1, 6, 8, 9 wird eine falsche Lösung mit einem Minuspunkt bewertet; bei Aufgabe 7 mit einem halben Minuspunkt.

Aufgabe 1. Wie viele Möglichkeiten gibt es, zehn Schüler in drei Hallenfußballteams mit je drei Spielern und einen Schiedsrichter einzuteilen?

2800	5600	8400	16800

Lösung: Anzahl ist $10 \cdot \binom{9}{3} \cdot \binom{6}{3} / 3! = 2800$ (erst 10 Möglichkeiten für den Schiedsrichter, dann erste und zweite Mannschaft; Reihenfolge der Mannschaften egal).

Aufgabe 2. Gegeben seien die folgenden Permutationen in S_6 :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 2 & 4 & 1 & 5 \end{pmatrix}.$$

Stellen Sie $\sigma \circ \tau$ und $\tau \circ \sigma$ in Zykelschreibweise dar. Liegen $\sigma \circ \tau$ und $\tau \circ \sigma$ in der gleichen Zykelklasse? Wie viele Zykelklassen gibt es in S_6 ?

Lösung: $\sigma = (2465)$, $\tau = (1365)$ mit gleichem Zykeltyp. Anzahl der Zykelklassen in S_6 ist Anzahl der Partitionen von 6; davon gibt es 11, nämlich 1^6 , $1^4 2$, $1^3 3$, $1^2 2^2$, $1^2 4$, 15 , 123 , 6 , 2^3 , 24 , 3^2 .

Aufgabe 3. Man finde eine geschlossene Formel für die Summe

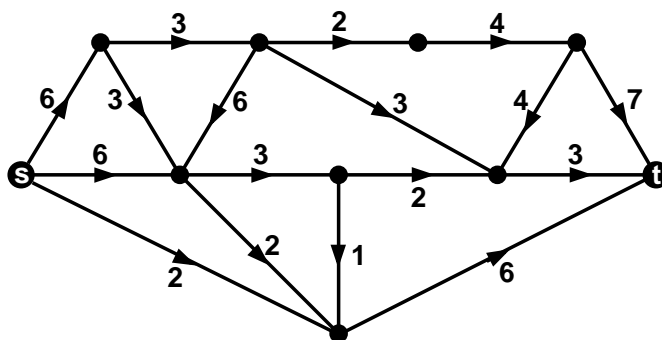
$$\sum_{k=1}^n k(k-1)^2(k-2).$$

Lösung: Eine Lösung mit fallenden Faktoriellen: $k(k-1)^2(k-2) = k^4 + 2k^3$ und damit $\sum_{k=1}^n k(k-1)^2(k-2) = \frac{1}{5}(n+1)^5 + \frac{2}{4}(n+1)^3 = \frac{1}{10}(2n^5 - 5n^4 + 5n^2 - 2n)$. Alternativ mit Produktregel für Summationen.

Aufgabe 4. Geben Sie eine geschlossene Formel für die Rekursion $a_{n+2} = 2a_{n+1} + a_n$ mit den Anfangswerten $a_0 = 0$ und $a_1 = 1$ an.

Lösung: $a(z) := \sum_{n \geq 0} a_n z^n \Rightarrow a(z)(1 - 2z - z^2) = z$ und $a(z) = \frac{z}{1-2z-z^2} = \frac{z}{(1-\alpha z)(1-\beta z)} = \frac{A}{1-\alpha z} + \frac{B}{1-\beta z}$ mit $\alpha = 1 + \sqrt{2}$, $\beta = 1 - \sqrt{2}$ und $A = 1/(\alpha - \beta) = \sqrt{2}/4 = -B$. Insgesamt mit geometrischer Reihe $a_n = \frac{\sqrt{2}}{4}((1 + \sqrt{2})^n + (1 - \sqrt{2})^n)$.

Aufgabe 5. Geben Sie einen maximalen Fluss im nachstehenden Netzwerk an. Ist er eindeutig?

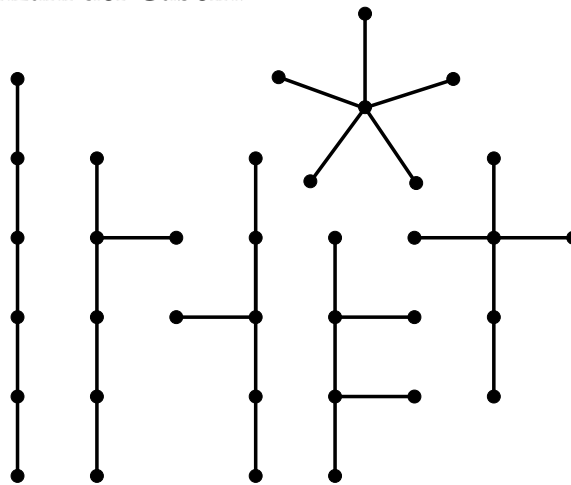


Lösung: Maximale Flussstärke ist 10; maximaler Fluss ist leider nicht eindeutig.

Aufgabe 6. Die Anzahl der Bäume mit 6 Ecken (bis auf Isomorphie) ist

4	5	6	7

Lösung: 6. Man kann zum Beispiel Fallunterscheidung nach dem längsten Weg machen oder auch nach der Anzahl der Gabeln.



Aufgabe 7. Geben Sie in der folgenden Tabelle für die acht Werte von n an, ob ein endlicher Körper \mathbb{F}_n mit n Elementen existiert:

n	100	101	121	128	144	169	225	243
\mathbb{F}_n existiert								
\mathbb{F}_n existiert nicht								

Lösung: Körper mit 101, 121 = 11², 128 = 2⁷, 169 = 13², 243 = 3⁵ Elementen existieren.

Aufgabe 8. Es gibt einen perfekten linearen ternären $[11, k, 5]$ -Kode $C \subset \mathbb{F}_3^{11}$ mit Minimalabstand $d = 5$. Dann ist die Dimension $k = \dim_{\mathbb{F}_3}(C)$ gleich

4	5	6	7

Lösung: $q = 3; n = 11; d = 5 \Rightarrow e = 2$. Mit $\#B_e = \sum_{i=0}^e \binom{n}{i} (q-1)^i = 1 + 11 \cdot 2 + 11 \cdot 20 = 243 = 3^5$ ist $\#C = q^n / \#B_e = 3^{11} / 3^5 = 3^6$, da C perfekt. Also $k = 6$.

Aufgabe 9. Wir betrachten einen binären Informationskanal, bei dem jedes Bit mit Wahrscheinlichkeit $p = 0,01 = 1\%$ gestört wird. Bemerkung: näherungsweise gilt $1 + p \log_2(p) + (1-p) \log_2(1-p) \approx 0,919$. Welche der folgenden Aussagen ist eine korrekte Folgerung des Satzes von Shannon über Kanalkodes?

- Sobald die Kodewortlänge groß genug ist, korrigieren alle Codes etwa 91% der Fehler.
- Es gibt einen Code mit Informationsrate 99% und beliebig kleiner Dekodierungsfehler-Wahrscheinlichkeit.
- Es gibt einen Code mit Informationsrate 90% und beliebig kleiner Dekodierungsfehler-Wahrscheinlichkeit.
- Es gibt einen linearen Code mit Informationsrate 90% und beliebig kleiner Dekodierungsfehler-Wahrscheinlichkeit.

Lösung: Die dritte Antwort ist richtig.

Aufgabe 10. Gegeben sei das Alphabet $Q = \{1, 2, \dots, 7\}$, in dem die einzelnen Buchstaben mit folgenden Häufigkeiten p_i auftreten:

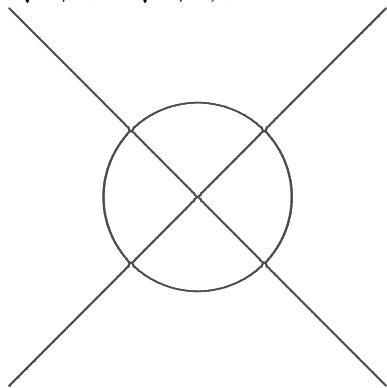
i	1	2	3	4	5	6	7
p_i	$\frac{2}{20}$	$\frac{1}{20}$	$\frac{3}{20}$	$\frac{6}{20}$	$\frac{2}{20}$	$\frac{5}{20}$	$\frac{1}{20}$

Geben Sie ein Verfahren an, Texte mit diesem Alphabet optimal binär zu kodieren. Was ist die durchschnittliche Wortlänge?

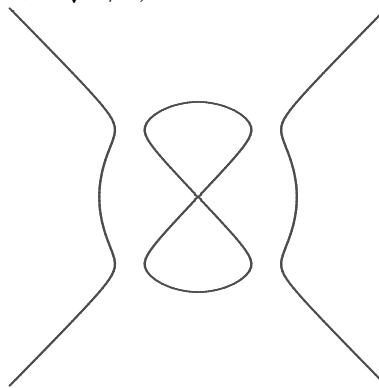
Lösung: Huffman-Algorithmus, Baum war gefordert. Durchschnittliche Wortlänge ist $51/20$.

Aufgabe 11. Berechnen Sie die singulären Punkte der affinen Kurve $C = V(f) \subset \mathbb{A}_{\mathbb{C}}^2$ mit der Gleichung $f(x, y) = y^4 - x^4 - y^2 + ax^2 = 0$ in Abhängigkeit von dem Parameter $a \neq 0$.

Lösung: Partielle Ableitungen sind $\partial f / \partial x = 2x(a - 2x^2)$ und $\partial f / \partial y = 2y(2y^2 - 1)$. Aus $x = 0$ folgt wegen $f(0, y) = y^4 - y^2 = 0$ entweder $y = 0$ oder $y = \pm 1$. Dabei ist aber $\partial f / \partial y(0, \pm 1) = \pm 2 \neq 0$. Analog erfüllt für $y = 0$ nur $x = 0$ alle drei Gleichungen. Sind $x, y \neq 0$, so geben die partiellen Ableitungen $x^2 = a/2$ und $y^2 = 1/2$. Wegen $f(\pm\sqrt{a/2}, \pm\sqrt{1/2}) = \frac{1}{4} - \frac{a^2}{4} - \frac{1}{2} + \frac{a^2}{2} = \frac{a^2}{2} - \frac{1}{2}$ liegen die Punkte $(\pm\sqrt{a/2}, \pm\sqrt{1/2})$ auf der Kurve genau dann, wenn $a = \pm 1$. Insgesamt ist also der Ursprung $(0, 0)$ immer singulär. Falls $a = \pm 1$, so gibt es vier weitere singuläre Punkte
 $a = 1 \Rightarrow (\pm\sqrt{1/2}, \pm\sqrt{1/2}), \quad a = -1 \Rightarrow (\pm i\sqrt{1/2}, \pm\sqrt{1/2})$.



$a = 1$



$a = 11/10$