Endliche Körper

$F_4 := F_2[X]/(X^2+X+1) = \{s+t\omega \mid s,t \in F_2\} = \{0,1,\omega,\omega^2=\omega+1\}, 2=0, \omega := [X]_{X^2+X+1}, \omega^2+\omega+1=0$

$F_8 := F_2[X]/(X^3+X+1) = \{s+t\beta+u\beta^2 \mid s,t,u \in F_2\}, 2=0, \beta := [X]_{X^3+X+1}, \beta^3+\beta+1=0$

$F_{16} := F_2[X]/(X^4+X+1) = \{s+t\gamma+u\gamma^2+v\gamma^3 \mid s,t,u,v \in F_2\}, 2=0, \gamma := [X]_{X^4+X+1}, \gamma^4+\gamma+1=0$

$F_9 := F_3[X]/(X^2+1) = \{s+t\iota \mid s,t \in F_3\}, 3=0, \iota := [X]_{X^2+1}, \iota^2+1=0$

	F_4 ω^i		F_8 β^i		F_{16} γ^i		F_9 $(\iota+1)^i$	
0	1	-	1	-	1	-	1	4
1	ω	2	β	3	γ	4	$\iota+1$	7
2	$\omega+1$	1	β^2	6	γ^2	8	$-\iota$	3
3	1		$\beta+1$	1	γ^3	14	$-\iota+1$	5
4			$\beta^2+\beta$	5	$\gamma+1$	1	-1	-
5			$\beta^2+\beta+1$	4	$\gamma^2+\gamma$	10	$-\iota-1$	2
6			β^2+1	2	$\gamma^3+\gamma^2$	13	ι	1
7			1		$\gamma^3+\gamma+1$	9	$\iota-1$	6
8					γ^2+1	2	1	
9					$\gamma^3+\gamma$	7		
10					$\gamma^2+\gamma+1$	5		
11					$\gamma^3+\gamma^2+\gamma$	12		
12					$\gamma^3+\gamma^2+\gamma+1$	11		
13					$\gamma^3+\gamma^2+1$	6		
14					γ^3+1	3		
15					1			

Kombinatorik

Ziehen von m aus n Kugeln:

	mit Beachtung der Reihenfolge	ohne Beachtung der Reihenfolge
mit Zurücklegen	n^m	$\binom{n+m-1}{m} = \frac{(n+m-1)!}{(n-1)!\cdot m!}$
ohne Zurücklegen	$\frac{n!}{(n-m)!}$	$\binom{n}{m} = \frac{n!}{(n-m)!\cdot m!}$ *nCr bei Sharp*

Operationen von Gruppen

$G \cdot m := \{g \cdot m \mid g \in G\}$ Bahn von m, $Stab_G(m) := \{g \in G \mid g \cdot m = m\}$ Stabilisator von $m \in M$ in G

$Fix_M(g) := \{m \in M \mid g \cdot m = m\}$ Fixpunktmenge von $g \in G$ in M

$m \in M: \ |G \cdot m| = \frac{|G|}{|Stab_G(m)|}$ (Bahnenlemma)

Sei $M = \coprod_{i=1}^{l} G \cdot m$ disjunkt in Bahnen zerlegt. Dann: $l = \frac{1}{|G|} \sum_{g \in G} |Fix_M(g)|$ (Burnside Fixpunktlemma)

Nützlich dabei: $|Fix_M({}^x g)| = |Fix_M(g)|, \ g, x \in G$

G operiert auf G via Konjugation: $G \times G \to G, (x,g) \to {}^x g = x \cdot g \cdot x^{-1}$

Dann heißen Bahnen Konjugationsklassen: ${}^G x = \{{}^x g \mid x \in G\}$

$U \le G \Rightarrow |U|$ teilt $|G|$

Siebformel / Möbius

$A_I := \bigcap_{i \in I} A_i, A_\emptyset := M$ Dann: $|M - \bigcup_{i=1}^{n} A_i| = \sum_{I \subseteq N} (-1)^{|I|} |A_I|$ (Siebformel)

Anzahl surjektiver Abbildungen $f: \{1,\dots,n\} \to \{1,\dots,k\}$ ist $\sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n$

Anzahl fixpunktfreier Permutationen in S_n ist $n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}$

$\mu(x) = (-1)^s$ falls x ist Produkt von s verschiedenen Primzahlen, 0 sonst

Äquivalent sind $f(n) = \sum_{d|n} g(d)$ und $g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d)$

Graphen

$G = (V, E, f)$, V = Ecken, E = Kanten

$\mu(G) = |E| - |V| + $ #Zsg.komponenten $\quad \mu(G) = 0 \Leftrightarrow G$ Wald

Ein zusammenhängender endlicher Graph hat genau dann eine Eulertour, wenn der Grad jeder Ecke gerade ist.

Codes

C ist ein $[N, k = dim\, C, d = d(C)]$ - Code. Informationsrate $r(C) := \frac{1}{N} \log_{|A|}(|C|) = \frac{\log(|C|)}{\log(|A^N|)}$

Hammingabstand: $d(x,y) := |\{i \in \{1,\dots,N\} \mid x \neq y \in C\}|$ Minimalabstand: $d(C) := min\{d(x,y) \mid x \neq y \in C\}$

Gewicht: $w(c) := d(c,0) c \in C$

Ist $(E_k \ P) \in A^{k \times N}$ Erzeugermatrix von $C \subseteq A^N$, so ist $\begin{pmatrix} -P \\ E_{N-k} \end{pmatrix} \in A^{N \times (N-k)}$ eine Prüfmatrix von C.

$C \subseteq A^N$ heißt perfekt $:\Leftrightarrow \exists e \in \mathbb{N}$ so dass es zu jedem $a \in A^N$ genau ein $c \in C$ gibt mit $d(c,a) \le e$

Für lineare Codes gilt: $|C| = |A|^k, \ r(C) = \frac{k}{N}$

$d(C) = 1 + max\{n \ge 0 \mid$ jedes Tupel aus n Zeilen ist linear unabhängig$\}$

Hamming

$A = F_q, N = \frac{q^r - 1}{q - 1}$ Sei $H \in F_q^{N \times r}$ eine Matrix deren Zeilen genau die N verschiedenen 1-dim Teilräume von F_q^r erzeugen. Der Code C mit Prüfmatrix H heißt Hammingcode der Länge N.

$dim(C) = N - r, d(C) = 3$, Hamming Codes sind perfekte Codes mit $e = 1$

Erw. Code

$\tilde{C} := \{(c_1,\dots,c_N,c_{N+1}) \mid (c_1,\dots,c_N) \in C, c_{n+1} = -\sum_{i=1}^{N} c_i\} \qquad dim(\tilde{C}) = k \qquad d(C)$ ungerade $\Rightarrow d(\tilde{C}) = d(C) + 1$

$\tilde{G} := (G|g), \quad \tilde{H} := \begin{pmatrix} & H & & 1 \\ & & & \vdots \\ & & & 1 \\ 0 & \dots & 0 & 1 \end{pmatrix}$ mit $g_k := -\sum_{i=1}^{N} G_{ki}$

Reed-Muller

$\Re(-1,m) = 0$ (Matrix mit 0 Zeilen)

$\Re(m,m) = F_2^{2^m}$ (Erz.-Matrix E_{2^m})

$\Re(r,m) = (\Re(r,m-1) \mid \Re(r-1,m-1))$

$\Re(r,m)$ hat Länge $N = 2^m$, $d = 2^{m-r}, k = \sum_{j=0}^{r} \binom{m}{j}$

$(C|C') = \begin{pmatrix} C & C \\ 0 & C' \end{pmatrix}$

$d((C|C')) = min\{2 \cdot d(C), d(C')\}$

Bis auf Äquivalenz zueinander dual sind $\Re(r,m)$ und $\Re(m-r-1,m)$.

Zyklische Codes

linearer Code zyklisch, falls $(C_1,\dots,C_N) \in C \Rightarrow (C_N, C_1,\dots,C_{N-1}) \in C$

Aus Koeffizienten des Erzeugerpolynoms $f(x)$ Matrix aufstellen und bis Länge N erreicht ist zeilenweise nach rechts shiften. Prüfpolynom ergibt sich durch $(x^N - 1)/f(x)$. Die Koeffizienten in umgekehrter Reihenfolge spaltenweise in Prüfmatrix einfüllen und nach unten shiften.

$dim(C) = N - grad(f)$

Designierte Minimalabstand: $d = $ #aufeinanderfolgender Nullstellen von $f(x) + 1$

Codieren: Aus zu codierendem Wort Polynom ablesen, das codierte Wort erhält man durch Division mit Rest durch $f(X)$ (Alle Codewörter sind vielfache von $f(X)$).

Unvollständiges Decodieren: Nullstellen einer primitiven Einheitswurzel sollten bei 1 anfangen, dann d ablesen. Korrigierbare Fehler: $t = \lfloor \frac{d-1}{2} \rfloor$. Zu decodierendes Polynom sei $r(x)$.

Per Koeffizientenvergleich von z^0 bis z^{2t} löse:

$\omega(Z) = \omega_t Z^t + \dots + \omega_1 Z \qquad \sigma(Z) = \sigma_t Z^t + \dots + \sigma_1 Z + 1 \qquad \omega(Z) \equiv_{z^{2t+1}} \sigma(Z)(r(\xi^1) z^1 + \dots + r(\xi^{2t}) z^{2t})$

Fehler an Stelle $x^i \Leftrightarrow \sigma(\xi^{-i}) = 0$ Fehlerkorrektur: Addiere zum Koeffizienten von x^i: $\frac{\omega(\xi^{-i}) \cdot \xi^i}{\sigma'(\xi^{-i})}$

Abschneiden der Prüfstellen ergibt das dekodierte Wort.

Schranken

$V_q(N,r) := \sum_{i=0}^{r} \binom{N}{i} (q-1)^i \qquad K_q(N,d) := max\{k \ge 0 \mid$ es gibt einen linearen $[N,k,d]$ - Code$\}$

Singleton-Schranke: $k \le N - d + 1$ **Hamming-Schranke:** $k \le N - \log_q(V_q(N, \lfloor \frac{d-1}{2} \rfloor))$

Gilbert-Varshamov-Schranke: $K_q(N,d) \ge N - \log_q(V_q(N,d-1))$ Bedenke: $k \le K_q(N,d)$

RSA

Eulersche Φ-Funktion: $\Phi(n) := |\{x \in \mathbb{N} \mid 1 \le x \le n, ggT(x,n) = 1\}| \quad n \ge 1$

p, q prim, groß. Public: $m = p \cdot q$, v mit $ggT(v, (p-1)\cdot(q-1)) = 1$

Private: e mit $e \cdot v = 1 \ mod\, (p-1)\cdot(q-1)$

Verschlüsseln von x: $x^v \ mod\, m$ Entschlüsseln von y: $y^e \ mod\, m$

G. Nebe, M. Künzer 21.08.2006

Diskrete Strukturen, SS 06

Scheinklausur

Bearbeitungszeit: 120 Minuten.

Zugelassene Hilfsmittel: Ein beliebig beschriebenes Blatt DIN A4 und ein nichtprogrammierbarer Taschenrechner.

Es sind insgesamt 36 Punkte erreichbar.

Ist ein **Kasten** bei einer Frage, so bitte die Antwort in den Kasten. Die für diese Antwort benötigten Rechnungen gehen diesenfalls in die Bewertung nicht ein. Eine falsche Antwort gibt 0 Punkte (aber keine negativen Punkte).

Bitte zu jeder Bearbeitung einer Frage **ohne Kasten** deutlich die Aufgabennummer angeben.

Wer mehr Papier benötigt, bitte melden.

Aufgabe 1 **(1+2+2+1 Punkte)**

(1) Auf wieviele Arten kann man 4 Kugeln aus 4 Kugeln ziehen, wenn man jeweils wieder zurücklegt und nicht auf die Reihenfolge achtet? $\boxed{}$

(2) Bestimme die Ordnung des Elements $\big((1,3,2)\circ(1,4,3)\circ(1,3)\big)^2$ von $\mathcal{S}_4$. $\boxed{}$

(3) Seien 5 verschiedene Briefe in 5 verschiedene Briefumschläge zu stecken. Wieviele Möglichkeiten gibt es, keinen Brief in den richtigen Umschlag zu stecken? $\boxed{}$ (Hinweis: Permutationen, Fixpunkte.)

(4) Bestimme $\mu(91)$. $\boxed{}$

Aufgabe 2 **(6 Punkte)**

Bestimme das Polynom $f(X)\in\mathbf{F}_2[X]$ von Grad <6, welches folgenden Kongruenzen genügt, und trage es hier ein: $\boxed{}$ (Hinweis: Euklid.)

$$\begin{array}{lll} f(X) & \equiv_X & 1 \\ f(X) & \equiv_{X^2+X+1} & 1 \\ f(X) & \equiv_{X^3+X+1} & X^2 \end{array}$$

Aufgabe 3 **(4+2 Punkte)**

Sei $m\geq 1$. Sei A_m die Menge der Abbildungen von $\{1,\ldots,6\}$ nach $\{1,\ldots,m\}$. Wir interpretieren A_m als die Menge der Perlenfärbungen der 6 Perlen einer Kette mit m möglichen Farben. Auf A_m operiere dementsprechend die Gruppe

$$G \;:=\; \langle a:=(1,2,3,4,5,6),\, b:=(2,6)(3,5)\rangle \;\leq\; \mathcal{S}_6$$

via $(g\cdot f)(x):=f(g^{-1}x)$, wobei $f\in A_m$, $g\in G$ und $x\in\{1,\ldots,6\}$. Zwei Perlenfärbungen f und f' sind bis auf Perlenkettenbewegung als gleich anzusehen, falls sie in derselben G-Bahn von A_m liegen.

(1) Liste alle Elemente von G auf. (Hinweis: Eine Betrachtung von ${}^b a$ kann helfen.)

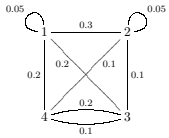
$\boxed{}$

$\boxed{}$

(2) Bestimme die Anzahl der G-Bahnen auf A_3, d.h. die Anzahl der auch nach Perlenkettenbewegung verschiedenen Perlenfärbungen mit 3 Farben. $\boxed{}$

Aufgabe 4 **(2 Punkte)**

Betrachte folgenden bewerteten Graphen $\mathcal{G}$.



Bestimme einen minimalen aufspannenden Teilgraphen. Trage diesen mit Farbe in $\mathcal{G}$ ein.

Aufgabe 5 **(2+2 Punkte)**

Sei C der lineare Code über $\mathbf{F}_2$ mit der Erzeugermatrix $\left(\begin{smallmatrix}1&0&1\\1&1&1\end{smallmatrix}\right)$. Sei C' der lineare Code über $\mathbf{F}_2$ mit der Erzeugermatrix $\left(\begin{smallmatrix}1&0&1\\0&1&1\end{smallmatrix}\right)$.

(1) Bestimme eine Erzeugermatrix von $(C|C')$.

(2) Bestimme den Minimalabstand von $(C|C')$. $\boxed{}$

Aufgabe 6 **(2+1 Punkte)**

Sei $f(X)=X^4+X+\omega\in\mathbf{F}_4[X]$. Sei C der zyklische Code der Länge 15 mit Erzeugerpolynom $f(X)$. Betrachte $\mathbf{F}_4$ als Teilkörper von $\mathbf{F}_{16}$ vermöge $\omega\longmapsto\gamma^5=\gamma^2+\gamma$.

(1) Bestimme alle Nullstellen von $f(X)$ in $\mathbf{F}_{16}$ unter Verwendung der Tatsache, daß γ^9 und γ^{13} als Nullstellen bekannt sind.

(2) Bestimme den designierten Minimalabstand von C, d.h. die vermittels aufeinanderfolgender Potenzen einer primitiven 15-ten Einheitswurzel als Nullstellen von $f(X)$ bestimmbare untere Schranke für $d(C)$.

Aufgabe 7 **(4+2 Punkte)**

Sei C der Hammingcode mit den Parametern $q=8$ und $r=2$ in Standardbezeichnung.

(1) Bestimme eine Prüfmatrix und eine Erzeugermatrix von C.

(2) Vergleiche die Dimension von C mit der Singleton-Schranke im vorliegenden Fall, d.h. für Länge und Minimalabstand wie C.

Aufgabe 8 **(3 Punkte)**

Zeige oder widerlege die folgende Aussage.

Sei G eine endliche Gruppe. Ist p eine Primzahl, ist $k\geq 1$, und ist p^k ein Teiler von $|G|$, so gibt es in G ein Element von Ordnung p^k.

G. Nebe, M. Künzer 21.08.2006

Diskrete Strukturen, SS 06

Lösung zur Scheinklausur

Aufgabe 1

(1) Wir haben $\binom{4+4-1}{4-1}=35$ Möglichkeiten.

(2) Wir erhalten $\big((1,3,2)\circ(1,4,3)\circ(1,3)\big)^2=(1,3,4,2)^2=(1,4)(2,3)$, und dieses Element hat Ordnung 2.

(3) Wir müssen die Anzahl der fixpunktfreien Permutationen in $\mathcal{S}_5$ bestimmen. Diese ergibt sich zu

$$5!\cdot\sum_{i=0}^{5}\frac{(-1)^i}{i!} \;=\; 5!\left(\frac{1}{0!}-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\frac{1}{4!}-\frac{1}{5!}\right) \;=\; 44\,.$$

(4) Da $91=7\cdot 13$ in eine gerade Zahl paarweise verschiedener Primfaktoren zerfällt, ist $\mu(91)=1$.

Aufgabe 2

Wir kürzen $u(X):=X$, $v(X):=X^2+X+1$ und $w(X):=X^3+X+1$ ab. Zwischenergebnisse sind

$$\begin{array}{rcll} 1 & = & u(X)\cdot(X^4+X^3) & + \;\; v(X)w(X)\cdot 1 \\ 1 & = & v(X)\cdot(X^3+X^2+X+1) & + \;\; u(X)w(X)\cdot X \\ 1 & = & w(X)\cdot(X+1) & + \;\; u(X)v(X)\cdot X \end{array}$$

Somit erfüllt

$$\tilde f(X) \;:=\; 1\cdot v(X)w(X)\cdot 1+1\cdot u(X)w(X)\cdot X+X^2\cdot u(X)v(X)\cdot X \;=\; X^6+X^5+X^3+X^2+1$$

die verlangten Kongruenzen. Polynomdivision durch $u(X)v(X)w(X)$ liefert dann die Lösung

$$f(X) \;=\; X^3+X^2+X+1\,,$$

die die Gradbedingung erfüllt.

Aufgabe 3

(1) Es ist ${}^b a=(1,6,5,4,3,2)=a^{-1}=a^5$. Also ist jedes Element von G von der Form a^ib^j mit $0\leq i\leq 5$ und $0\leq j\leq 1$.

Somit wird

$$\begin{array}{rcl} G & = & \{a^0,\, a^1,\, a^2,\, a^3,\, a^4,\, a^5,\, a^0b,\, a^1b,\, a^2b,\, a^3b,\, a^4b,\, a^5b\} \\ & = & \{\mathrm{id},\ (1,2,3,4,5,6),\ (1,3,5)(2,4,6),\ (1,4)(2,5)(3,6),\ (1,5,3)(2,6,4),\ (1,6,5,4,3,2)\,, \\ & & \ (2,6)(3,5),\ (1,2)(3,6)(4,5),\ (1,3)(4,6),\ (1,4)(2,3)(5,6),\ (1,5)(2,4),\ (1,6)(2,5)(3,4)\}\,. \end{array}$$

Man kann auch einen Baum erstellen. Der Aufwand dafür ist etwas größer.

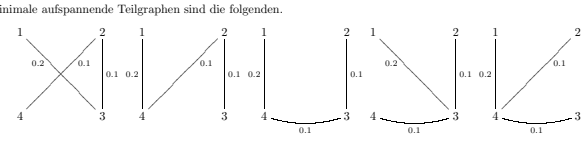
(2) Nach dem Lemma von Burnside ergibt sich die Anzahl der Bahnen von G auf A_m zu

$$\frac{1}{12}\Big(\underbrace{1\cdot m^6}_{\text{zu id}}+\underbrace{2\cdot m^1}_{\text{zu }(1,2,3,4,5,6)\text{ etc.}}+\underbrace{2\cdot m^2}_{\text{zu }(1,3,5)(2,4,6)\text{ etc.}}+\underbrace{4\cdot m^3}_{\text{zu }(1,4)(2,5)(3,6)\text{ etc.}}+\underbrace{3\cdot m^4}_{\text{zu }(2,6)(3,5)\text{ etc.}}\Big)\,.$$

Insbesondere ergibt sich die gefragte Anzahl der Bahnen von G auf A_3 zu 92.

Aufgabe 4

Minimale aufspannende Teilgraphen sind die folgenden.



Verlangt war, einen von diesen anzugeben.

Aufgabe 5

(1) Eine Erzeugermatrix von $(C|C')$ ist gegeben durch

$$\left(\begin{smallmatrix}1&0&1&1&0&1\\1&1&1&1&1&1\\0&0&0&1&0&1\\0&0&0&0&1&1\end{smallmatrix}\right)\,.$$

(2) Der Minimalabstand ist gegeben durch $d\big((C|C')\big)=\min\{2d(C),\,d(C')\}$. Wir erkennen direkt, daß $d(C)=1$ und $d(C')=2$. Also ist $d\big((C|C')\big)=\min\{2,2\}=2$.

Den Minimalabstand aus einer Prüfmatrix für $(C|C')$ abzulesen, ist möglich, aber aufwendiger.

Aufgabe 6

(1) Es sind mit γ^9 und γ^{13} auch $(\gamma^9)^4=\gamma^{36}=\gamma^6$ und $(\gamma^{13})^4=\gamma^{52}=\gamma^7$ Nullstellen von $f(X)$. Wegen $\deg f=4$ ist die Menge der Nullstellen von $f(X)$ in $\mathbf{F}_{16}$ damit zu $\{\gamma^6,\,\gamma^7,\,\gamma^9,\,\gamma^{13}\}$ bekannt.

(2) Es ist γ eine primitive 15-Einheitswurzel (da $\gamma^3\neq 1$ und $\gamma^5=\gamma^2+\gamma\neq 1$), und deren 2 aufeinanderfolgende Potenzen γ^6, γ^7 sind Nullstellen von $f(X)$. Also beträgt der designierte Minimalabstand $2+1=3$.

Aufgabe 7

(1) Die Prüfmatrix ist nur bis auf eine Permutation der Zeilen bestimmt. Wir können geschickterweise folgende nehmen.

$$\left(\begin{smallmatrix}1&0\\0&1\\1&\beta^0\\1&\beta^1\\1&\beta^2\\1&\beta^3\\1&\beta^4\\1&\beta^5\\1&\beta^6\end{smallmatrix}\right)$$

Denn dann liefern die Erzeugnisse der Zeilen gerade alle eindimensionalen Teilräume von $\mathbf{F}_8^{1\times 2}$. Dazugehörend erhalten wir die Prüfmatrix

$$\left(\begin{smallmatrix}1&\beta^0&1&0&0&0&0&0&0\\1&\beta^1&0&1&0&0&0&0&0\\1&\beta^2&0&0&1&0&0&0&0\\1&\beta^3&0&0&0&1&0&0&0\\1&\beta^4&0&0&0&0&1&0&0\\1&\beta^5&0&0&0&0&0&1&0\\1&\beta^6&0&0&0&0&0&0&1\end{smallmatrix}\right)$$

(2) Die Länge von C beträgt $N=9$, der Minimalabstand $d=3$ (wie bei allen Hammingcodes). Die Singleton-Schranke besagt nun, daß die Dimension von C nicht über $N-d+1=7$ liegen sollte. Nun ist die Dimension von C gerade $k=7$, d.h. die Singleton-Schranke wird angenommen.

Aufgabe 8

Die Aussage ist falsch. Z.B. ist 2^3 ein Teiler von $|\mathcal{S}_4|$, ohne daß $\mathcal{S}_4$ ein Element der Ordnung 2^3 enthält. In der Tat müßte es hierzu ein Element in $\mathcal{S}_4$ geben, welches in Zykeldarstellung einen Zykel der Länge 8 aufweist, was wegen $8>4$ nicht möglich ist.