Endliche Körper Tabellen

$\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$, $\omega = [X]$

$l(i)$	i	ω^i
$*$	0	1
2	1	ω
1	2	$\omega+1$

$\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3+X+1)$, $\beta = [X]$

$l(i)$	i	β^i
$*$	0	1
3	1	β
6	2	β^2
1	3	$\beta+1$
5	4	$\beta^2+\beta$
4	5	$\beta^2+\beta+1$
2	6	β^2+1

$\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+1)$, $\iota = [X]$

$l(i)$	i	$(\iota+1)^i$
4	0	1
7	1	$\iota+1$
3	2	$-\iota$
5	3	$-\iota+1$
$*$	4	-1
2	5	$-\iota-1$
1	6	ι
6	7	$\iota-1$

$\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4+X+1)$, $\gamma = [X]$

$l(i)$	i	γ^i
$*$	0	1
4	1	γ
8	2	γ^2
14	3	γ^3
1	4	$\gamma+1$
10	5	$\gamma^2+\gamma$
13	6	$\gamma^3+\gamma^2$
9	7	$\gamma^3+\gamma+1$
2	8	γ^2+1
7	9	$\gamma^3+\gamma$
5	10	$\gamma^2+\gamma+1$
12	11	$\gamma^3+\gamma^2+\gamma$
11	12	$\gamma^3+\gamma^2+\gamma+1$
6	13	$\gamma^3+\gamma^2+1$
3	14	γ^3+1

Zählen

	geordnet	ungeordnet
zur.	$\lvert S(n,k)\rvert = n^k$	$\lvert M(n,k)\rvert = \binom{n+k-1}{k}$
o. zur.	$\lvert S_0(n,k)\rvert = \frac{n!}{(n-k)!}$	$\lvert M_0(n,k)\rvert = \binom{n}{k}$

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

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

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

$\sum_{k=0}^{n} \binom{n}{k} = 2^n = |\operatorname{Pot}(\underline{n})|$

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

$\binom{w+m}{k} = \sum_{l=0}^{k} \binom{w}{l}\binom{m}{k-l}$

Gruppentheorie

G, H endliche Gruppen, $\varphi : G \to H$ Homomorphismus dann gilt
$\operatorname{Kern}(\varphi) \leq G$, $\operatorname{Bild}(\varphi) \leq H$ und $|\operatorname{Kern}(\varphi)| \cdot |\operatorname{Bild}(\varphi)| = |G|$.

G operiert auf M mit $\cdot$ falls $g \cdot m \in M$, $(g \cdot h) \cdot m = g \cdot (h \cdot m)$ und $1 \cdot m = m$.
Bahn: $G \cdot m = \{g \cdot m | g \in G\}$
$\operatorname{Stab}_G(m) = \{g \in G | gm = m\} \leq G$
$\operatorname{Fix}_M(g) = \{m \in M | gm = m\}$
$|G| = |G \cdot m| \cdot |\operatorname{Stab}_G(m)|$
$\operatorname{Stab}_G(g \cdot m) = g \cdot \operatorname{Stab}_G(m) g^{-1}$
$U \leq G \Rightarrow |U| \mid |G|$
$|\operatorname{Fix}_M(g)| = |\operatorname{Fix}_M({}^h g)|$

G operiert auf G durch Linksmultiplikation und Konjugation.
G operiere auf M, Anzahl der Bahnen sei n, $G = \uplus_{j=1}^{k} {}^G g_j$.
$n = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}_M(g)| = \frac{1}{|G|} \sum_{j=1}^{k} |\operatorname{Fix}_M(g_j)| \cdot |{}^G g_j| = \sum_{j=1}^{k} \frac{|\operatorname{Fix}_M(g_j)|}{|\operatorname{Stab}_G(g_j)|}$

Färbungen: M Menge, $W \leq S_M$ Symmetriegruppe, A Farben, $\mathfrak{F} = \{f : M \to A\}$ Färbungen. Bestimme Zykeltypen der Konjugationsklassen und Anzahl der Elemente (meist durch W bestimmen). Anzahl der Färbungen:
$p(|A|) = \frac{1}{|W|} \sum_{\text{Konjugationsklassen K}} |K| \cdot |A|^{\text{Länge des Zykeltyps von } K}$
Achtung: Einerzykel mitzählen!

Siebformel

Sei M Menge, $N = \{1, ..., n\}$, $A_i \subseteq M$, $A_\emptyset := M$, $A_I := \bigcap_{i \in I} A_i$.
$|M \setminus \bigcup_{i \in \mathbb{N}} A_i| = \sum_{I \subseteq N} (-1)^{|I|} |A_I|$ oder
$|\bigcup_{i \in \mathbb{N}} A_i| = -\sum_{\emptyset \neq I \subsetneq N} (-1)^{|I|} |A_I|$

$|\{f : \underline{n} \to \underline{k} | f \text{ ist surjektiv }\}| = \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n$

$\operatorname{fpf}(n) = |\{\pi \in S_n | \forall i \in \underline{n} : \pi(i) \neq i\}| = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}$

$N = \{1, \ldots, n\}$, $f, g : \operatorname{Pot}(N) \to \mathbb{R}$ Funktionen. Äquivalent sind:
$\forall I \subseteq N : g(I) = \sum_{J \supseteq I} f(J)$ und
$\forall I \subseteq N : f(I) = \sum_{J \supseteq I} (-1)^{|J \setminus I|} g(J)$
Äquivalente Formulierung:
$\forall I \subseteq N : g(I) = \sum_{J \subseteq I} f(J)$ und
$\forall I \subseteq N : f(I) = \sum_{J \subseteq I} (-1)^{|I \setminus J|} g(J)$

$N = \{1, \ldots, n\}$, $f, g : N \to \mathbb{R}$. Äquivalent sind:
$\forall i \in N : g(i) = \sum_{j=0}^{i} \binom{i}{j} f(j)$ und
$\forall i \in N : f(i) = \sum_{j=0}^{i} (-1)^{i-j} \binom{i}{j} g(j)$

Möbiusinversion

Eine partiell geordnete Menge $(M, \trianglelefteq)$ ist eine Menge M mit einer reflexiven ($x \trianglelefteq x$), antisymmetrischen ($x \trianglelefteq y, y \trianglelefteq x \Rightarrow x = y$) und transitiven ($x \trianglelefteq y, y \trianglelefteq z \Rightarrow x \trianglelefteq z$) Relation $\trianglelefteq$. Aus der Relation kann eine Totalordnung konstruiert werden.

Inzidenzalgebra von $(M, \trianglelefteq)$: $I(M) := \{A \in \mathbb{R}^{n \times n} | A_{ij} \neq 0 \Rightarrow m_i \trianglelefteq m_j\}$
$\iota_\trianglelefteq$ ist die charakteristische Funktion von $\trianglelefteq$: $\iota_\trianglelefteq(x, y) = 1$ für $x \trianglelefteq y$, 0 sonst
$\mu_\trianglelefteq = (\iota_\trianglelefteq)^{-1}$ (inverse Matrix).

$$\mu_{\text{teilt}}(a,b) = \begin{cases} 0 & a \nmid b \text{ oder } p^2 | b/a \text{ mit } p \text{ Primzahl} \\ (-1)^s & d = \prod_{i=1}^{s} p_i \text{ mit pw. versch. Primz.} \\ 1 & b = a \end{cases}$$

Klassische Möbiusfunktion der Zahlentheorie: $\mu : \mathbb{N}_{\geq 1} \to \{0, 1, -1\}$ mit

$$\mu(d) := \mu_{\text{teilt}}(1,d) = \begin{cases} (-1)^s & d = \prod_{i=1}^{s} p_i \text{ mit pw. versch. Primz.} \\ 0 & \text{sonst} \end{cases}$$

$(\mu(1) = 1)$
Klassische Möbiusinversion: $f, g : \mathbb{N}_{\geq 1} \to \mathbb{R}$. Äquivalent sind:
$\forall n \in \mathbb{N}_{\geq 1} : f(n) = \sum_{d|n} g(d)$ und
$\forall n \in \mathbb{N}_{\geq 1} : g(n) = \sum_{d|n} f(d) \cdot \mu(\frac{n}{d})$

Graphentheorie

$\mu(G) = |E| - |V| + \kappa = m - n + \kappa$
$G = (V, E, f)$ Wald $\Leftrightarrow \mu(G) = 0$
Eine endliche Folge $K = \{v_0 e_1 v_1 e_2 v_2 \ldots e_n v_n)$ mit $v_i \in V$, $e_j \in E$ heißt *Kantenzug*, falls $f(e_i) = \{v_{i-1}, v_i\}$ für alle $i \in \{1, \ldots, n\}$.

- K heißt *offen* $:\Leftrightarrow v_0 \neq v_n$
- K heißt *geschlossen* $:\Leftrightarrow v_0 = v_n$
- K heißt *Weg* $:\Leftrightarrow v_i \neq v_j \ \forall i \neq j$
- K heißt *Kreis* $:\Leftrightarrow v_i \neq v_j \ \forall i \neq j$, $1 \leq i, j \leq n$ und $v_0 = v_n$

$A \in \mathbb{N}^{V \times V}$ mit $A_{v,w} = |f^{-1}(\{\{v, w\}\})|$ (Anzahl Kanten zwischen v und w) Adjazenzmatrix von G.

Euklidische Ringe

$(R/(f))^* = \{[a]_f | a \in R, \operatorname{ggT}(a, f) = 1\}$ $(|\mathbb{Z}/(n)|^* = \varphi(n))$
$\operatorname{ord}(a^i) = \frac{\operatorname{ord}(a)}{\operatorname{ggT}(\operatorname{ord}(a), i)}$

$I_1 \trianglelefteq R, I_2 \trianglelefteq R$ teilerfremd $:\Leftrightarrow R = I_1 + I_2 = \{a + b | a \in I_1, b \in I_2\}$
$(a_1), (a_2)$ teilerfremd $\Leftrightarrow \operatorname{ggT}(a_1, a_2) = 1$
$I_1, ..., I_k$ paarweise teilerfremd, dann:
$R/(I_1 \cap ... \cap I_k) \cong R/I_1 \times ... \times R/I_k$ und
$(R/(I_1 \cap ... \cap I_k))^* \cong (R/I_1)^* \times ... \times (R/I_k)^*$

p Primzahl, $n \in \mathbb{N}$:
$(\mathbb{Z}/(p^n))^* \cong C_{p^{n-1}(p-1)}$ für $p > 2$
$(\mathbb{Z}/(2^n))^* \cong C_2 \times C_{2^{n-1}}$ für $p = 2$, $n \geq 3$
$(\mathbb{Z}/(2^2))^* \cong C_2$, $(\mathbb{Z}/(2))^* \cong C_1$

Invertieren in $(R/(f))^*$: $[a]^{-1} = [x]$ falls $xa + yf = 1$ also Euklid mit f und a ausführen und nach 1 auflösen.

Kongruenzsystem lösen: $\operatorname{ggT}(a, b \cdot c \cdot \ldots) = 1$, dann nach 1 auflösen und nur den Teil mit $b \cdot c \cdot \ldots$ nehmen, dieser ist $\mod a = 1$ und $\mod x = 0$ für $x \in \{b, c, \ldots\}$.

RSA

p, q Prim. Öffentlich: $m = p \cdot q$ und v mit $\operatorname{ggT}(v, (p-1)(q-1)) = 1$. Privat: e mit $e \cdot v = 1 \mod (p-1)(q-1)$.
$f_E(n) = n^v \mod m$ für $n \in \{0, \ldots, (m-1)\}$
$f_E^{-1}(n) = n^e \mod m$

Endliche Körper

$a^{p^f} = a$ für $a \in \mathbb{F}_{p^f}$
$Frob_p : \mathbb{F}_{p^f} \to \mathbb{F}_{p^f} : a \mapsto a^p$ ist $\mathbb{F}_{p^f}$-Automorphismus

Zech-Logarithmus: α primitiv $(< \alpha >= K^*)$
$\alpha^i + \alpha^j = \alpha^i(1 + \alpha^{j-i}) = \alpha^i \alpha^{l(j-i)} = \alpha^{i+l(j-i)}$
$\mathbb{F}_{p^d}$ Teilkörper von $\mathbb{F}_{p^f} \Leftrightarrow d | f$

$g(X) \in \mathbb{F}_p[X]$ irreduzibel normiert von Grad $f \Rightarrow g(X) | X^{p^f} - X$
$f(X)$ zerfällt in pw. versch. norm. irred. Polynome $\Leftrightarrow \operatorname{ggT}(f(X), f'(X)) = 1$
P_n ist die Menge der norm. irred. Polynome von Grad n
$|P_n| = \frac{1}{n} \sum_{d|n} p^d \mu(\frac{n}{d})$

Codes

C Code der Länge N: $C \subseteq A^N$, $|A| < \infty$
Informationsrate: $r(C) := \frac{1}{N} \log_{|A|}(|C|) = \frac{\log(|C|)}{\log(|A^N|)}$
Hamming-Abstand: $d(x,y) := |\{i \in \underline{N} | x_i \neq y_i\}|$
Gewicht: $w(x) = d(x,0)$, $x \in C$
Minimalabstand: $d(C) := \min\{d(x,y) | x \neq y\}$
Dreiecksungleichung: $d(x,y) + d(y,z) \geq d(x,z) \forall x,y,z \in C$
MDD: f mit $d(f(a),a) = \min\{d(c,a) | c \in C\} \forall a \in A^N$
e Fehler bei der Übertragung:
$e < \frac{d}{2} \Rightarrow f(a) = c$
$e < d \Rightarrow a = c \vee a \notin C$ (fehlerhafte Übertragung wird erkannt)

Lineare Codes

Erzeugermatrix zu C: Zeilen erzeugen C
$E \in A^{k \times N}$, N Länge, k Dimension von C
$r(C) = \frac{k}{N}$
$d(C) = \min\{d(c,0) | c \in C\}$
$C^\perp = \{x \in A^N | (x,c) = 0 \ \forall \ c \in C\}$
$\dim(C^\perp) = N - k$
$E = (I_k | P_{N-k}) \Rightarrow E_\perp = (-P_{N-k}^{tr} | I_{N-k})$
Prüfmatrix: $H = E_\perp^{tr}$, denn $c \in C \Leftrightarrow c \cdot E_\perp^{tr} = 0$
$d(C) = 1 + \text{Rang}(H)$

Syndrom

Syndrom von x: $x \cdot H$
$H^{-1}(s) = \{x \in A^N | x \cdot H = s\} = \{a + c | c \in C\}$ für $a \cdot H = s$

$f : A^N \to C : a \mapsto a - a_s$ ist ein MDD mit s Syndrom von a und a_s minimaler Vertreter, also $w(a_s) = \min\{w(x) | x \in H^{-1}(s)\}$.

Hamming Codes

q Primzahlpotenz, $r \in \mathbb{N}$
$A = \mathbb{F}_q$, $N = \frac{q^r - 1}{q-1}$, $k = N - r$, der Code wird auch mit $H_N(q)$ bezeichnet.
Prüfmatrix: Zeilen sind die Erzeuger der 1-dimensionalen Teilräume von $A^r = \mathbb{F}_q^r$
$d(H_N(q)) = 3$, perfekter Code mit $e = 1$

Perfekte Codes

C perfekt $\Leftrightarrow$ falls eine eine Zahl e existiert, so dass für alle $a \in A^N$ genau ein $c \in C$ existiert mit $d(a,c) \leq e$.
Perfekte Codes: Hammingcode $\Rightarrow e = 1$.
Wiederholungscode $\{(0,...,0),(1,...,1)\}$ über $\mathbb{F}_2$ mit N ungerade $\Rightarrow e = \frac{N-1}{2}$
Golay Code G_{23}, $N = 23$, $k = 12$, $d(G_{23}) = 7 \Rightarrow e = 3$
Ist C ein perfekter binärer Code, so gilt:
$e = 1 \Rightarrow$ Hamming-Code
$e > 1 \Rightarrow$ Wiederholungscode oder Golay Code G_{23}

Erweiterter Code

$\tilde{C} = \{(c_1,...,c_{N+1}) | (c_1,...,c_N) \in C, c_{N+1} = -\sum_{i=1}^N c_i\}$

$$\tilde{H} = \begin{pmatrix} & & & 1 \\ & H & & \vdots \\ & & & 1 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Für lineare binäre Codes gilt: $d(\tilde{C})$ gerade, also für $d(C)$ ungerade ist $d(\tilde{C}) = d(C) + 1$.

Zyklische Codes

$p \not| N$, $X^N - 1 = f_1(X) \cdot ... \cdot f_t(X)$ pw. versch. norm. irred. Polynome.
2^t Ideale aus Produkten von f_i in $\mathbb{F}_p[X]/(X^N - 1)$
Erzeugerpolynom $g(X)$ ist ein Produkt aus f_is für einen zyklischen Code der Länge N: $g_{N-k}X^k + g_{N-k-1}X^{k-1} + ... + g_0$. Dann ist die Erzeugermatrix

$$\begin{pmatrix} g_{N-k} & g_{N-k-1} & \cdots & g_0 & 0 & \cdots & 0 \\ 0 & g_{N-k} & \cdots & g_1 & g_0 & \cdots & 0 \\ \vdots & & \ddots & & & & \vdots \\ 0 & \cdots & & & & & g_0 \end{pmatrix} \in \mathbb{F}_q^{k \times N}$$

Prüfpolynom $h(X) : g(X) \cdot h(X) = X^N - 1$

$$H = \begin{pmatrix} h_0 & 0 & 0 & \cdots & 0 \\ h_1 & h_0 & 0 & \cdots & 0 \\ h_2 & h_1 & h_0 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & \cdots & 0 & \cdots & h_k \end{pmatrix} \in \mathbb{F}_q^{N \times N-k}$$

Codieren: $u \in A^k$. Betrachte u als Koeffizienten für ein Polynom. Führe Polynomdivision von $(u \cdot X^k)/g$ durch mit Rest r, dann ist $(u|r) \in C \subseteq A^{1 \times N}$ das Codewort zu u.
α ist eine primitive N-te Einheitswurzel falls α eine Nullstelle von $X^N - 1$ ist und $N = \min\{n \in \mathbb{N} | n \geq 1, \alpha^n = 1\}$
Designierter Minimalabstand: Wenn $g | X^N - 1$, α primitive N-te Einheitswurzel und r aufeinanderfolgende Potenzen $\alpha^b, \alpha^{b+1}, ..., \alpha^{b+r-1}$ Nullstellen von $X^N - 1$ existieren $\Rightarrow d(C_g) \geq r + 1$
Decodieren: $t = \lfloor \frac{d-1}{2} \rfloor$, $r(X)$ Polynom zum empfangenen Wort, α primitive Einheitswurzel mit erster Nullstelle der Folge α.
Bestimme $\omega(Z) = \omega_t Z^t + \cdots + \omega_1 Z$ und $\sigma(Z) = \sigma_t Z^t + \ldots \sigma_1 Z + 1$, sodass $\omega(Z) \equiv_{Z^{2t+1}} \sigma(Z)(r(\alpha)Z + \cdots + r(\alpha^{2t})Z^{2t})$ mit Hilfe von Koeffizientenvergleich für Z bis Z^{2t}. Fehler an Stelle $i \Leftrightarrow \sigma(\alpha^{-i}) = 0$. Korrektur: Addiere zum Koeffizienten von i: $\frac{\omega(\alpha^{-i})\alpha^i}{\sigma'(\alpha^{-i})}$.

Schranken

$K_q(N,d) = \max\{k |$ es gibt einen $[N,k,d]$-Code über $\mathbb{F}_q\}$
Singleton: $K_q(N,d) \leq N - d + 1$
$|B_r(a)| = |\{x \in \mathbb{F}_q^N | d(x,a) \leq r\}| = \sum_{i=0}^r \binom{n}{i}(q-1)^i =: V_q(N,r)$
$|S_r(a)| = |\{x \in \mathbb{F}_q^N | d(x,a) = r\}| = \binom{n}{r}(q-1)^r$
Hamming: $K_q(N,d) \leq N - \log_q(V_q(N, \lfloor \frac{d-1}{2} \rfloor))$
Gilbert-Varshamov: $K_q(N,d) \geq N - \log_q(V_q(N, d-1))$

Reed-Muller Codes

C_i sei ein $[N,k_i,d_i]$-Code mit Erzeugermatrix E_i.
$C = (C_1|C_2) = \{(u, u+v) | u \in C_1, v \in C_2\}$
ist ein $[2N, k_1 + k_2, \min\{2d_1, d_2\}]$-Code mit Erzeugermatrix
$E = \begin{pmatrix} E_1 & E_1 \\ 0 & E_2 \end{pmatrix}$.
$C^\perp$ ist äquivalent zu $(C_2^\perp | C_1^\perp)$.

Binärer Reed-Muller Code $R(r,m)$:
$N = 2^m$, $d(R(r,m)) = 2^{m-r}$ für $r \geq 0$, $k = \dim(R(r,m)) = \sum_{j=0}^r \binom{m}{j}$
$R(r,m)^\perp$ ist äquivalent zu $R(m-r-1,m)$
Rekursive Definition:
$R(-1,m) = \{0\}$
$R(m,m) = \mathbb{F}_{2^N}$
$R(r,m) = (R(r,m-1) | R(r-1,m-1)) \ \forall 0 \leq r < m$