

# Zusammenfassung Codierungstheorie

© Tim Baumann, <http://timbaumann.info/uni-spicker>

Datenquelle  $\xrightarrow{\text{senden}}$  Kanal  $\xrightarrow{\text{empfangen}}$  Senke

Die Daten liegen bereits digitalisiert vor. Mit dem Problem wie Daten wie bspw. natürliche Sprache möglichst effizient codiert werden, befasst sich die Informationstheorie. In dieser Vorlesung soll es darum gehen, Daten mit einer Kanalcodierung so zu übersetzen, dass Fehler, die bei einer Übertragung über einen fehlerhaften Kanal, korrigiert oder zumindest bemerkt werden.

Datenquelle  $\xrightarrow[E]{\text{codieren}}$  Code  $\xrightarrow{\text{senden}}$  Kanal  $\xrightarrow{\text{empfangen}}$   $\square$   
 $\xrightarrow[D]{\text{decodieren}}$  Code  $\xrightarrow{E^{-1}}$  Senke

**Def.** Ein **Alphabet** ist eine Menge  $Q$  mit  $q > 1$  Elementen, typischerweise  $\{0, 1, \dots, q-1\} \cong \mathbb{Z}_q$ .

*Bem.*  $\mathbb{Z}_q$  trägt die Struktur eines Ringes. Falls  $q$  eine Primzahlpotenz ist, so gibt es einen Körper  $\mathbb{F}_q$  mit  $q$  Elementen.

**Def.** Sei  $n \geq 1$ . Eine nichtleere Menge  $C \subseteq Q^n$  mit  $q = |Q|$  heißt **Blockcode** der Länge  $n$  über  $Q$  oder  **$q$ -närer Code** der Länge  $n$ . Jedes  $c = (c_1, \dots, c_n) \in C$  heißt ein **Codewort**. Falls  $M = |C|$ , so nennt man  $C$  einen  **$(n, M)$ -Code** über  $Q$ .

**Def.** Die **Informationsrate** von  $C$  ist dann  $R(C) := \log_n(M)/n$ . Falls  $|M| = q^k$ , dann ist  $R(C) = k/n$ .

*Bem.* Ist  $Q \cong \mathbb{F}_q$ , dann ist  $Q^n$  ein  $\mathbb{F}_q$ -VR. Falls  $C$  ein Unterraum von  $Q^n$  ist, so ist  $R(C) = \dim_{\mathbb{F}_q}(C)/n$ .

**Def.** Der **Hamming-Abstand** von  $u, v \in Q^n$  ist

$$d(u, v) := |\{i = 1, \dots, n \mid u_i \neq v_i\}|.$$

**Lem.** Der Hamming-Abstand ist eine Metrik auf  $Q^n$ .

**Notation.** Es sei  $C \subseteq Q^n$  ein Code und  $y \in Q^n$ . Wenn  $y$  empfangen wurde, so geht man davon aus, dass das gesendete Wort dasjenige des Codes mit den wenigsten Unterschieden zu  $y$  ist, also ein Wort, welches den **Hamming-Abstand**  $d(y, C) := \min_{c \in C} d(y, c)$  von  $y$  zu  $C$  realisiert. Es existiert i. A. kein eindeutiges solches Element, sondern eine Menge

$$N_c(y) := \{\bar{c} \mid d(y, C) = d(y, \bar{c})\}.$$

**Def.** • Man nennt einen Kanal einen  **$q$ -nären symmetrischen Kanal**, falls ein  $p \in \mathbb{R}$  mit  $0 < p < (q-1)/q$  existiert, sodass

$$\mathbb{P}(\beta \text{ empfangen} \mid \alpha \text{ gesendet}) = p/q-1$$

für alle  $\beta \neq \alpha \in Q$ , also  $\mathbb{P}(\alpha \text{ empfangen} \mid \alpha \text{ gesendet}) = 1 - p$ .

• Man nennt einen Kanal **gedächtnislos**, falls

$$\mathbb{P}(y \text{ empfangen} \mid c \text{ gesendet}) = \prod_{i=1}^n \mathbb{P}(y_i \text{ empfangen} \mid c_i \text{ gesendet})$$

für alle Wörter  $x, y \in Q^n$  gilt.

**Def (Maximum-Likelihood-Prinzip).** Gegeben sei ein Code  $C \subseteq Q^n$  und  $y \in Q^n$ . Gesucht ist  $\hat{c} = \arg \max_{c \in C} \mathbb{P}(y \mid c)$ .

**Satz.** Es seien ein  $q$ -närer symm. gedächtnisloser Kanal und ein Code  $C \subseteq Q^n$  gegeben. Sei  $y \in Q^n$  und  $\hat{c} \in C$ . Dann sind äquivalent:

- $\mathbb{P}(y \mid \hat{c}) = \max_{c \in C} \mathbb{P}(y \mid c)$
- $\hat{c} \in N_c(y)$

**Def.**  $D : Q^n \rightarrow C$  heißt **vollständige Decodierabbildung**, falls

$$\forall y \in Q^n : D(y) \in N_C(y).$$

**Def.** Die **Kanalkapazität** eines  $q$ -nären symmetrischen Kanal ist

$$\kappa(q, p) := \log_2(q) + p \cdot \log_2(p/q-1) + (1-p) \cdot \log_2(1-p).$$

Sie ist ein Maß für die maximale Information, die über den Kanal übertragen werden kann. Die **Entropiefunktion** ist

$$H(q, p) := 1 - \kappa(q, p).$$

**Def.** Sei  $C$  ein Code und  $D$  sei eine zugehörige (vollständige) Decodierabbildung. Die **Restfehlerwahrscheinlichkeit** zu  $(C, D)$ :

$$\mathbb{P}_{\text{err}}(C) := \max_{y \in Q^n, c \in C} \mathbb{P}(D(y) \neq c \mid c \text{ gesendet}, y \text{ empfangen})$$

**Satz (Shannon).** Sei  $0 < R < \kappa(q, p)$ . Dann gibt es eine Folge  $(C_n)_{n \in \mathbb{N}}$  von Codes und zugehörigen Decodierabbildungen  $D_n$  mit:

- $C_n$  ist ein  $(n, M_n)$ -Code mit Informationsrate  $R \leq R(C_n) < \kappa(q, p)$
- $\lim_{n \rightarrow \infty} (\mathbb{P}_{\text{err}}(C_n)) = 0$

## Fehlerkorrektur und zwei Schranken

**Def.** Der **Minimalabstand** eines  $(n, M)$ -Codes  $C$  über  $Q$  ist

$$d := d(C) := \min_{c, c' \in C, c \neq c'} d(c, c').$$

Man sagt dann,  $C$  ist ein  $q$ -närer  $(n, M, d)$ -Code.

**Notation.** Für  $u \in Q^n$ ,  $l \in \mathbb{N}$  sei  $B_l(u) := \{x \in Q^n \mid d(x, u) \leq l\}$ .

**Def.** • Ein Code  $C$  heißt  **$l$ -fehlerkorrigierend**, falls  $B_l(c) \cap B_l(c') = \emptyset$  für alle  $c, c' \in C$  mit  $c \neq c'$ .  
•  $C$  heißt  **$m$ -fehlererkennend**, wenn  $B_m(c) \cap C = \{c\}$  f. a.  $c \in C$ .  
•  $C$  heißt **genau  $l$ -fehlerkorrigierend/-erkennend**, falls  $C$   $m$ -fehlerkorrr.-erkennend für  $m := l$  aber nicht  $m := l+1$  ist.

**Satz.** Jeder  $(n, M, d)$ -Code  $C$  ist genau

- $(d-1)$ -fehlererkennend und
- $(t := \lfloor d-1/2 \rfloor)$ -fehlerkorrigierend.

**Bsp.**  $C = \{000, 111\}$  ist ein binärer  $(3, 2, 3)$ -Code.

**Problem.** Gegeben:  $q$ , Länge  $n$ , Minimalabstand  $d$ . Gesucht:

$$A_q(n, d) := \max\{M \mid \exists (n, M, d)\text{-Code}\}$$

**Def.** Ein  $(n, M, d)$ -Code heißt **optimal**, falls  $M = A_q(n, d)$ .

**Lem.** Seien  $q, n \in \mathbb{N}$ ,  $q \geq 2$ ,  $n \geq 1$ .

- $A_q(n, 1) = q^n$ , realisiert durch  $C = Q^n$ .
- $A_q(n, n) = q$ , realisiert durch  $C = \{(a, \dots, a) \mid a \in Q\} \subseteq Q^n$
- $d \leq d' \implies A_q(n, d) \geq A_q(n, d')$
- Sei  $n \geq 2$  und  $d \geq 2$ . Dann gilt  $A_q(n, d) \leq A_q(n-1, d-1)$ .

**Kor (Singletonschränke).**  $A_q(n, d) \leq q^{n-d+1}$

**Def.** Ein Code, der die Singletonsschränke mit Gleichheit erfüllt, heißt ein **MDS-Code** (MDS = maximum distance separable).

*Bem.* Sei  $C \subseteq Q^n$  ein  $(n, M, d)$ -Code,  $T = \{1 \leq t_1 < \dots < t_{|T|} \leq n\}$  und  $\pi_T : C \rightarrow Q^{|T|}$ ,  $c \mapsto (c_{t_1}, \dots, c_{t_{|T|}})$ . Ist  $C$  ein MDS-Code, so ist  $\pi_T$  bijektiv für alle  $T$  mit  $|T| = n - d + 1$ .

**Satz.**  $A_q(n, 2) = q^{n-1}$ , realisiert durch einen Code mit Prüffziffer

**Def.** Sei  $(G, +, 0)$  eine kommutative Gruppe. Das **Hamming-Gewicht** von  $x \in G^n$  ist

$$\text{wt}(x) := |\text{supp}(x)|, \quad \text{wobei} \quad \text{supp}(x) := \{i \mid x_i \neq 0\}.$$

**Lem.** Sei  $G$  wie oben,  $x, y \in G^n$ . Dann  $\text{wt}(x-y) = d(x, y)$ .

**Satz.**  $A_q(n, 2) = q^{n-1}$  für alle  $q \geq 2$  und alle  $n \geq 2$ .

*Beweis.* Wir konstruieren einen  $(n, q^{n-1}, 2)$ -Code. Sei  $R$  ein kommutativer Ring mit  $q$  Elementen,  $\lambda_1, \dots, \lambda_{n-1} \in R$  Einheiten und  $\lambda_n := -1$ . Wir betrachten die Kontrollgleichung

$$\kappa : R^n \rightarrow R, \quad z \mapsto \lambda_1 z_1 + \dots + \lambda_n z_n.$$

Dann ist  $C := \ker(\kappa)$  ein 1-fehlererkennender Code.  $\square$

**Lem.** Falls  $\lambda_2 - \lambda_1, \dots, \lambda_n - \lambda_{n-1}$  ebenfalls Einheiten sind, so sind Nachbarvertauschungen als Fehler erkennbar.

**Bspe.** • Für  $q = 2, R = \mathbb{Z}_2, \lambda_1 = \dots = \lambda_{n-1} = 1$  heißt  $C := \ker(\kappa)$  **Parity-Check-Erweiterung**.

- Beim ISBN-Code ist  $R = \mathbb{Z}_{11}, \lambda_1 = 1, \dots, \lambda_9 = 9$ , also  $\kappa(z) = \sum_{i=1}^{10} i z_i$ .

*Bem.* Es gilt  $A_q(4, 3) = q^2 \iff$  es gibt ein Paar orthogonaler lateinischer Quadrate der Größe  $q \iff q \neq 2$  oder  $q \neq 6$ .

**Lem.** Für  $x, y \in \mathbb{Z}_2^n$  gilt  $d(x, y) = \text{wt}(x) + \text{wt}(y) - 2 \cdot \text{wt}(x \cdot y)$ .

**Satz.** Für alle  $n \geq 1$  und  $d$  ungerade gilt  $A_2(n, d) = A_2(n+1, d+1)$ , realisiert durch die Parity-Check-Erweiterung.

**Def.** Zwei  $(n, M)$ -Codes  $C, C'$  über  $Q$  heißen **äquivalent**, falls gilt: Es gibt eine Permutation  $\gamma$  auf  $\{1, \dots, n\}$  und Permutationen  $\sigma_1, \dots, \sigma_n$  auf  $Q$ , sodass

$$\alpha : Q^n \rightarrow Q^n, \quad (x_1, \dots, x_n) \mapsto (\sigma_1(x_{\gamma(1)}), \dots, \sigma_n(x_{\gamma(n)}))$$

den Code  $C$  auf  $C'$  abbildet.

**Bsp.**  $A_2(5, 3) = 4$  realisiert durch  $\{00000, 11100, 00111, 11011\}$

**Lem.** Sei  $Q$  ein Alphabet,  $u \in Q^n$ . Dann gilt

$$|B_l(u)| = \sum_{j=0}^l \binom{n}{j} (|Q| - 1)^j.$$

**Satz (Kugelpackungsschranke (KPS)).** Sei  $q \geq 2$ ,  $n \geq 2$ ,  $1 \leq d \leq n$ ,  $t := \lfloor \frac{d-1}{2} \rfloor$ . Dann ist

$$A_q(n, d) \leq q^n / \sum_{j=0}^t \binom{n}{j} (q-1)^j.$$

**Def.** Ein  $q$ -ärer  $(n, M, d)$ -Code  $C$  heißt **perfekt**, falls  $M$  gleich der Kugelpackungsschranke ist.

*Bem.* Die KPS kann zur **Johnsen-Schranke** verbessert werden. Zusammen mit dem letzten Beispiel liefert diese  $A_2(6, 3) = 8$ .

**Bsp.** Für  $q=2$ ,  $n=7$ ,  $d=3$  liefert die KGS genau  $A_2(7, 3) \leq 16$ .

## Lineare Codes

*Bem.* Zu jeder Primzahlpotenz  $q = p^m \geq 2$  gibt es bis auf Isomorphie genau einen Körper  $\mathbb{F}_q = \mathbb{F}_p$  mit  $q$  Elementen. Die Charakteristik dieses Körpers ist  $p$ . Ist  $q$  keine Primzahlpotenz, so gibt es auch keinen Körper mit  $q$  Elementen.

*Konstr.* Sei  $q = p^m$ ,  $p$  prim. Dann gibt es ein irreduzibles Polynom  $g(x)$  in  $\mathbb{Z}_p$  mit  $\deg(g) = m$ . Dann ist  $\mathbb{F}_q := \mathbb{Z}_p[x]/(g(x))$ .

**Def.** Ein  **$\mathbb{F}_q$ -linearer Code** der Länge  $n$  ist ein  $\mathbb{F}_q$ -Teilraum  $\mathbb{F}_q^n$ .

**Notation.** Sei  $C$  ein  $\mathbb{F}_q$ -linearer Code. Sei  $k := \dim(C)$ . Dann ist  $|C| = q^k$ , also  $C$  ein  $(n, q^k)$ -Code. Man sagt,  $C$  ist ein  $[n, k]$ -Code. Ist  $d$  der Minimalabstand von  $C$ , so:  $C$  ist ein  $[n, k, d]$ -Code.

**Def.** Sei  $C$  ein  $\mathbb{F}_q$ -linearer Code mit  $\dim(C) \geq 1$ . Das **Minimalgewicht** von  $C$  ist  $\min\{\text{wt}(c) \mid c \in C, c \neq 0\}$ .

**Lem.** Sei  $C$  ein  $\mathbb{F}_q$ -linearer Code mit  $\dim(C) \geq 1$ . Dann:

Minimalgewicht von  $C$  = Minimalabstand von  $C$ .

**Bsp.** Folgender Code ist ein bin.  $(6, 8, 3)$ -Code bzw.  $[6, 3, 3]$ -Code:

$$\left\{ \begin{array}{l} 000000, 100101, 010110, 001111, \\ 110011, 101010, 011001, 111100 \end{array} \right\} = \text{span}\{100101, 010110, 001111\}$$

**Problem.** Gegeben sei  $\mathbb{F}_q$ , die Länge  $n$  und der Minimalabstand  $d$ . Gesucht ist  $A_q^{\text{lin}}(n, d)$ , die bestmögliche Anzahl Wörter eines Codes mit diesen Parametern.

*Bem.* Klar ist  $A_q^{\text{lin}}(n, d) \leq A_q(n, d)$ .

**Lem.** •  $A_q^{\text{lin}}(n, 1) = q^n = A_q(n, 1)$

•  $A_q^{\text{lin}}(n, n) = q = A_q(n, n)$

•  $d \leq d' \implies A_q^{\text{lin}}(n, d) \geq A_q^{\text{lin}}(n, d')$

• Für  $n \geq 2$ ,  $d \geq 2$  ist  $A_q^{\text{lin}}(n, d) \leq A_q^{\text{lin}}(n-1, d-1)$ .

*Bem.* Da die Parity-Check-Erweiterung durch eine lineare Abbildung geschieht, gilt:

**Satz.**  $A_1^{\text{lin}}(n, 2) = q^{n-1} = A_q(n, 2)$

**Satz.** Falls  $d$  ungerade, so ist  $A_2^{\text{lin}}(n, d) = A_2^{\text{lin}}(n+1, d+1)$

**Def.** Sei  $C$  ein  $[n, k]$ -Code über  $\mathbb{F}_q$ , d. h. es gibt eine injektive Codierabbildung  $E: \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n$  mit  $\text{im}(E) = C$ . Dann heißt für jede Basis  $g^1, \dots, g^k \in C$  von  $C$  die Matrix

$$G := \begin{pmatrix} g^1 \\ \vdots \\ g^k \end{pmatrix} \in \mathbb{F}_q^{k \times n} \quad \text{eine } \mathbf{Generatormatrix} \text{ von } C.$$

*Bem.* Dann ist  $E(u) = uG = \sum_{j=1}^k u_j g^j \in C$

**Def.** Zwei  $[n, k]$ -Codes  $C, C' \subseteq \mathbb{F}_q^n$  heißen **linear äquivalent**, falls es  $\gamma \in S_n$  und  $\lambda_1, \dots, \lambda_n \in \mathbb{F}_q^\times$  gibt, sodass die monomiale Transf.

$$\alpha: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n, (x_1, \dots, x_n) \mapsto (\lambda_1 x_{\gamma(1)}, \dots, \lambda_n x_{\gamma(n)})$$

den Code  $C$  in  $C'$  überführt.

**Def.** Ein  $[n, k]$ -Code heißt **systematisch**, falls die ersten  $k$  Spalten seiner Generatormatrix die Standardbasisvektoren sind.

**Notation.** Sei  $C \subset \mathbb{F}_q^n$  ein UVR. Für  $x, y \in \mathbb{F}_q^n$  schreiben wir

$$x \equiv y \pmod{C} : \iff x - y \in C.$$

Die zu  $x \in V$  gehörende Kongruenzklasse modulo  $C$  ist  $x + C$ .

**Def.** Ein Repräsentantensystem  $\mathcal{R}$  dieser Klassen heißt **gewichtsminimal**, falls  $\text{wt}(r) = \min_{c \in C} \text{wt}(r + c)$  für alle  $r \in \mathcal{R}$ .

**Satz.** Sei  $C$  ein  $[n, k]$ -Code über  $\mathbb{F}_q$ ,  $\mathcal{R}$  ein gewichtsmin. Repräsentantensystem mod  $C$ . Zu  $y \in \mathbb{F}_q^n$  sei  $\mathcal{R}(y) \in \mathcal{R}$  mit  $\mathcal{R}(y) + C = y + C$ . Dann ist  $D: \mathbb{F}_q^n \rightarrow C$ ,  $y \mapsto y - \mathcal{R}(y)$  eine Decodierabbildung.

*Bem.* Sei  $\mathbb{F}$  ein Körper,  $n \in \mathbb{N}^*$ . Das Standard-Skalarprodukt

$$\langle -, - \rangle: \mathbb{F}^n \times \mathbb{F}^n \rightarrow \mathbb{F}, (x, y) \mapsto \sum_{i=1}^n x_i y_i$$

ist eine nicht-ausgeartete, symmetrische Bilinearform.

**Achtung.** Es ist  $\dim(U^\perp) = n - k$ , im Allgemeinen gilt aber  $U \cap U^\perp \neq 0$ , z. B. ist  $11011 \in \mathbb{F}_2^5$  senkrecht zu sich selbst.

**Def.** Sei  $C$  ein  $[n, k]$ -Code über  $\mathbb{F}_q$ . Dann heißt  $C^\perp$  der zu  $C$  gehörende **duale Code**.

**Def.** Die Generatormatrix  $H$  von  $C^\perp$  heißt **Kontrollmatrix** zu  $C$ .

**Lem.**  $x \in C \iff Hx^T = 0$

**Algorithmus.** Sei  $C$  ein  $[n, k]$ -Code,  $H \in \mathbb{F}_q^{n-k \times n}$  die Kontrollmatrix. Dann ist

$$\psi_H: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^{n-k}, x \mapsto Hx^T$$

eine surjektive lineare Abbildung mit  $\ker(\psi_H) = C$ .

- Sei  $c \in C$  gesendet,  $y \in \mathbb{F}_q^n$  empfangen, etwa  $y = c + e$ . Wir als Empfänger kennen jedoch  $c$  und  $e$  nicht, nur  $y$ . Trotzdem können wir das **Syndrom**  $s := \phi_H(y) = Hc^T + He^T = He^T \in \mathbb{F}_q^{n-k}$  berechnen.
- Wahrscheinlich ist  $e$  ein gewichtsminimaler Repräsentant von  $y$ . Sei also  $\mathcal{R}$  ein minimales Repräsentantensystem. Dann ist  $\psi := \psi_H|_{\mathcal{R}}: \mathcal{R} \rightarrow \mathbb{F}_q^{n-k}$  bijektiv. Dann definiert  $D(y) := y - \psi^{-1}(s)$  eine Decodierabbildung.

**Satz.** Sei  $C$  ein linearer  $[n, k, d]$ -Code über  $\mathbb{F}_q$ ,  $H$  eine Kontrollmatrix zu  $C$ . Dann gilt:

$$d = 1 + \max\{a \in \mathbb{N}^* \mid \text{je } a \text{ Spalten von } H \text{ sind linear unabhängige}\} \\ = \min\{m \in \mathbb{N}^* \mid \text{es gibt } m \text{ linear abhängige Spalten in } H\}$$

**Def.** Sei  $C$  ein linearer Code der Länge  $n$  über  $\mathbb{F}_q$ . Die **Gewichtsverteilung von  $C$**  ist  $A = A_C \in \mathbb{N}^{\{0,1,\dots,n\}}$  mit

$$A(i) := \{w \in C \mid \text{wt}(w) = i\}, \quad 0 \leq i \leq n.$$

*Bem.* Es gilt  $A_0 = 1$  und  $A_1 = A_2 = \dots = A_{d-1} = 0$ , falls  $d$  das Minimalgewicht von  $C$  ist.

**Def.**  $A_C(Z) := \sum_{i=0}^k A_i Z^i \in \mathbb{C}[Z]$  heißt **Gewichtszählpolynom**,

$$A_C^{\text{hom}}(X, Y) := \sum_{i=0}^n A_i X^{n-i} \cdot Y^i \in \mathbb{C}[X, Y]$$

heißt **homogenes Gewichtszählpolynom**.

*Bem.* •  $A_C(Z) = A_C^{\text{hom}}(1, Z)$  •  $A_C^{\text{hom}}(X, Y) = X^n \cdot A_C(\frac{Y}{X})$

- Aus  $A_C(X, Y)$  erhält man durch die sogenannte Mac-Williams-Transformation  $A_{C^\perp}(X, Y)$

## Hamming-Codes

**Lem.** Sei  $C$  ein perfekter  $(n, M, d)$ -Code. Dann ist  $d$  ungerade.

*Bem.* Wir betrachten nun perfekte Codes  $C$  mit  $t = 1$ , also  $d = 3$ . Es gilt dann  $|C| = q^n / (1 + n(q-1))$ , es ist also  $1 + n(q-1)$  ein Teiler von  $q^n$ . Beispielsweise ist für  $q \geq 2$  und  $n = q + 1$  die Zahl  $1 + n(q-1) = q^2$  ein Teiler von  $q^n$ . Diese Teilbarkeit ist eine notwendige, aber nicht hinreichende Bedingung für die Existenz eines perfekten  $(n, M, 3)$ -Codes über  $Q$  mit  $q = |Q|$ .

**Lem.** Seien  $p, u, v \in \mathbb{N}$ ,  $p \geq 2$ . Dann gilt  $u|v \iff p^u - 1 | p^v - 1$ .

**Prop.** Sei  $C$  perfekt mit  $t = 1$  über  $Q$ , wobei  $|Q| = q$  eine Primzahlpotenz ist. Dann ist  $|C|$  eine  $q$ -Potenz.

*Bem.* Sei nun  $q \geq 2$  eine Primzahlpotenz,  $C$  ein  $q$ -ärer perfekter  $(n, M, 3)$ -Code. Dann ist

$$q^k = |C| = M = q^{n/1+n(q-1)} \iff n = (q^{n-k}-1)/q-1$$

Wie viele Lösungspaare  $(n, k)$  gibt es bei festem  $q$ ? Wir setzen  $m := n - k$ . Dann ist  $k(m) := n - m$  und  $n(m) := \frac{q^m-1}{q-1}$ . Die Lösungspaare hängen damit nur noch vom Parameter  $m$  ab.

**Satz.** Zu jedem  $m \geq 2$  und zu jeder Primzahlpotenz  $q \geq 2$  gibt es einen linearen perfekten  $[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1} - m, 3]$ -Code über  $\mathbb{F}_q$ .

**Kor.** Ist  $q \geq 2$  eine Primzahlpotenz, so gilt

$$A_q^{\text{lin}}(\frac{q^m-1}{q-1}, 3) = A_q(\frac{q^m-1}{q-1}, 3) = q^{q^0+\dots+q^{m-1}-m} \quad \forall m \geq 2, m \in \mathbb{N}$$

*Konstr.* Ein bin. **Hamming-Code**  $\text{Ham}_2(m)$  (ein  $[n, n-m, 3]$ -Code mit  $n := 2^m - 1$ ) ist geg. durch die Kontrollmatrix  $H \in \mathbb{F}_2^{m \times n}$ , welche jeden Vektor aus  $\mathbb{F}_2^n \setminus \{0\}$  in genau einer Spalte stehen hat.

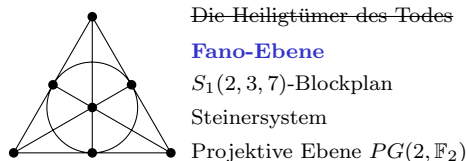
**Algorithmus** (Decodierung von binären Hamming-Codes). Angenommen, die Spalten der Kontrollmatrix  $H$  codieren die Zahlen  $1, \dots, 2^m - 1$  im Binärsystem und sind geordnet. Sei  $y \in \mathbb{F}_2^n$  empfangen worden. Falls  $Hy = 0$ , so wurde wsl.  $y$  gesendet. Falls das Syndrom  $Hy$  ungleich null ist, so ist vermutlich das  $j$ -te Bit gekippt, wobei  $j$  die Zahl ist, deren Binärcodierung  $Hy$  ist.

**Prop.** Sei  $m \geq 2$ ,  $n = 2^m - 1$  und  $A \in \mathbb{N}^{0,1,\dots,n}$  die Gewichtsverteilung des  $[n, n-m, 3]$ -Hamming-Codes. Dann gilt  $A_{n-j} = A_j$  für alle  $j = 0, 1, \dots, 2^{m-1} - 1$ .

**Satz.** Die Gewichtsverteilung des binären  $[7, 4]$ -Hamming-Codes ist

$$A = (1, 0, 0, 7, 7, 0, 0, 1).$$

*Bem.* Sei  $C = \text{Ham}_2(3)$ ,  $C_3 := \{c \in C \mid \text{wt}(c) = 3\}$ . Für  $c \in C_3$  seien  $P(c) := \{i = 1, \dots, 7 \mid c_i = 1\}$  die Positionen der in  $c$  gesetzten Bits. Falls  $i \in P(c)$ , so sagen wir, dass  $i$  auf der Geraden  $c$  liege. Dies definiert die folgende geometrische Struktur:



Wir bemerken, dass jede Gerade drei Punkte enthält, jeder Punkt auf drei Geraden liegt, durch je zwei verschiedene Punkte genau eine Gerade verläuft und jedes Paar von Geraden sich in genau einem Punkt schneidet. Die Vierecke in der Fano-Ebene sind die Komplemente von Geraden. Sie entsprechen den Codeworten mit Hamming-Gewicht 4.

**Satz.** Die Parity-Check-Erweiterung des  $[7, 4]$ -Hamming-Codes ist ein binärer  $[8, 4, 4]$ -Code. Dieser ist selbst-dual und optimal. Sein homogenes Gewichtszählpolynom ist  $X^8 + 14X^4Y^4 + Y^8$ .

*Konstr.* Wir definieren auf  $A := \mathbb{F}_q^n \setminus \{0\}$  eine Äq'-relation durch

$$u \sim v : \iff \exists \lambda \in \mathbb{F}_q : u = \lambda v.$$

Wir setzen  $\mathbb{P} := PG(m-1, \mathbb{F}_q) := A/\sim$ . Es gilt  $|\mathbb{P}| = q^m - 1/q - 1 = n$ . Sei  $v_1, \dots, v_n$  ein Representantensystem der Äquivalenzklassen. Dann definiert die Kontrollmatrix  $H_q(m) := (v_1 \cdots v_n)^T \in \mathbb{F}_q^{m \times n}$  den  **$q$ -ären Hamming-Code**  $\text{Ham}_q(n)$ .

*Bem.* Wir wählen das Representantensystem wie folgt:

$$\left\{ \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ * \end{pmatrix} \right\} \cup \dots \cup \left\{ \begin{pmatrix} 1 \\ * \\ \vdots \\ * \end{pmatrix} \right\},$$

also so, dass der erste Eintrag jedes Vektors eine 1 ist.

**Algorithmus** (Decodieren des  $q$ -ären Hamming-Codes). Sei  $y$  empfangen mit höchstens einem Fehler. Berechne das Syndrom  $s = H_q(m)y^T$ . Falls  $s = 0$ , so ist  $D(y) := y$ . Angenommen,  $s_i \neq 0$ . Sei  $i$  minimal mit  $s_i \neq 0$ . Dann ist  $s/s_i$  eine Spalte von  $H_q(m)$ , etwa die  $l$ -te Spalte. Decodiere  $D(y) := y - s_i \cdot e_l$ .

**Def.** Sei  $q \geq 2$  eine Primzahlpotenz und  $m \geq 2$ . Der Code  $\text{Sim}_q(m) := \text{Ham}_q(m)^\perp$  heißt **Simplex-Code**.

*Bem.*  $\text{Sim}_q(m)$  ist ein  $[n, m]$ -Code.

**Satz.**  $\text{Sim}_q(m)$  ist **gewichtskonstant**, d. h. jedes vom Nullwort verschiedene Codewort hat Gewicht  $q^{m-1}$ .

*Bem.* Also ist  $A_{\text{Sim}_q(m)}(z) = 1 + (q^m - 1) \cdot z^{q^{m-1}}$ .

**Satz.**  $A_{\text{Ham}_2(m)}(z) = \frac{1}{n+1}(1+z)^n + \frac{n}{n+1}(1+z)^{\frac{n-1}{2}} \cdot (1-z)^{\frac{n+1}{2}}$ , wobei  $n = 2^m - 1$ . Es gilt die Rekursionsgleichung

$$\binom{n}{l-1} = (n-l+2) \cdot A_{l-2} + A_{l-1} + l \cdot A_l.$$

## Golay-Codes und ihre Erweiterungen

**Prop.** Ist  $n \geq 3$  ungerade, so ist der binäre  $n$ -Wiederholungscode ein perfekter Code.

*Bem.* Es sei  $d \geq 5$ ,  $q$  eine Primzahlpotenz. Für  $n \leq 1000$ ,  $\log_q(M) \leq 1000$  und  $q \leq 1000$  könnte es nur Codes mit folgenden Parametern geben:

- $q = 2$ ,  $n = 23$ ,  $d = 7$ ,  $M = 2^{12} = 4096$
- $q = 2$ ,  $n = 90$ ,  $d = 5$ ,  $M = 2^{78}$
- $q = 3$ ,  $n = 11$ ,  $d = 5$ ,  $M = 3^6 = 729$

**Satz.** Es gibt keinen binären  $(90, 2^{78}, 5)$ -Code.

*Bem.* Sei  $q$  eine Primzahlpotenz,  $C$  ein perfekter  $q$ -ärer  $(n, M, 2t+1)$ -Code. Dann hat das **Lloyd-Polynom**

$$L_t(X) := \sum_{j=0}^t (-1)^j \cdot (q-1)^{t-j} \cdot \binom{X-1}{j} \binom{n-1-X}{t-j}$$

mindestens  $t$  verschiedene Nullstellen in  $\{1, \dots, n\}$ .

**Bsp.** Für  $n = 90$ ,  $q = 2$ ,  $t = 2$  ist  $L_2(X) = 2(X^2 - 90 + 2003)$ . Dessen Diskriminante ist 88, also keine Quadratzahl. Somit besitzt  $L_2(X)$  keine natürlichen Nullstellen.

**Prop.** Sei  $C$  ein binärer selbst-dualer Code (insb. linear). Dann gilt:

- Jedes Codewort hat ein gerades Gewicht.
- $\forall c \in C : 4 \mid \text{wt}(c) \iff C$  hat eine Basis  $B$  mit  $\forall b \in B : 4 \mid \text{wt}(b)$

**Prop.** Für jeden ternären selbstdualen Code  $C$  gilt  $\forall c \in C : 3 \mid \text{wt}(c)$ .

*Konstr.* Beginne mit dem  $[7, 4, 3]$ -Hamming-Code  $C_1$  mit Generatormatrix

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Sei  $\overline{C}_1$  die Parity-Check-Erweiterung von  $C_1$  mit Generatormatrix

$$\overline{G}_1 = \left( G_1 \mid \begin{array}{c} 1 \\ 1 \\ 1 \\ 1 \end{array} \right)$$

Dann ist  $\overline{C}_1$  eine selbstdualer  $[8, 4, 4]$ -Code über  $\mathbb{F}_2$ .

Sei  $G_2$  die Matrix  $G_1$  mit Spalten in umgekehrter Reihenfolge,

$$G_2 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

der Code  $C_2$  von  $G_2$  erzeugt,  $\overline{C}_2$  die Parity-Check-Erw. von  $C_2$ . Dann ist  $\overline{C}_2$  selbstdual.

**Satz.** Sei  $\Gamma \subset \mathbb{F}_2^{24}$  definiert durch

$$\Gamma := \{(a+f, b+f, a+b+f) \mid a, b \in \overline{C}_1, f \in \overline{C}_2\}$$

Dann ist  $\Gamma$  ein selbst-dualer binärer  $[24, 12, 8]$ -Code.

**Def.**  $\Gamma$  wird **erweiterter binärer Golay-Code  $\mathcal{G}(24)$**  genannt.

**Satz.** Es gibt einen perfekten binären  $[23, 12, 7]$ -Code, den **Golay-Code  $\mathcal{G}(23)$** . Diesen erhält man aus  $\mathcal{G}(24)$  durch Streichen einer Koordinate.

*Bem.* Umgekehrt ist  $\mathcal{G}(24)$  eine Parity-Check-Erw. von  $\mathcal{G}(23)$ .

**Satz.** •  $A_{\mathcal{G}(24)}(z) = 1(z^0 + z^{24}) + 759(z^8 + z^{16}) + 2576z^{12}$   
•  $A_{\mathcal{G}(23)}(z) = 1(z^0 + z^{23}) + 253(z^7 + z^{16}) + 506(z^8 + z^{15}) + 1288(z^{11} + z^{12})$

*Bem.*  $\mathcal{G}(24)$  hat eine Generatormatrizen der Form  $G_1 = [E|M]$  und  $G_2 = [M|E]$ , wobei  $M$  symmetrisch ist. Beide Matrizen sind gleichzeitig auch Kontrollmatrizen. Die Matrix  $M$  hat dabei besondere Eigenschaften, die zum Decodieren ausnutzen kann.

**Satz.**  $\mathcal{G}(12) := \Omega \subset \mathbb{F}_3^{12}$  sei der Code mit Generatormatrix  $G = [E_6 | M] \in \mathbb{F}_3^{6 \times 12}$ , wobei

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 2 & 1 & 2 \\ 1 & 0 & 1 & 2 & 2 & 2 \\ 2 & 1 & 0 & 1 & 2 & 2 \\ 2 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 2 \end{pmatrix}$$

Dann ist  $\Omega$  ein selbstdualer  $[12, 6, 6]$ -Code über  $\mathbb{F}_3$ .

**Satz.** Es gibt einen  $[11, 6, 5]$ -Code über  $\mathbb{F}_3$ . Dieser ist perfekt und heißt **ternärer Golay-Code  $\mathcal{G}(11)$** .

*Konstr.* Streichen der letzten Koordinate von  $\mathcal{G}(12)$ .

## Verbindungen mit der Designtheorie

**Def.** Eine **Inzidenzstruktur** (IS) ist ein Tupel  $\mathcal{D} = (V, \mathcal{B}, I)$  mit

- einer (nichtleeren) Menge von **Punkten** (oder *Knoten*)  $V$ ,
- einer (nichtleeren) Menge von **Blöcken** (oder *Geraden*)  $\mathcal{B}$  und
- einer **Inzidenzrelation**  $I \subseteq V \times \mathcal{B}$ .

**Notation.**  $pIB \text{ :} \Longleftrightarrow (p, B) \in I$

*Bem.* Wir können die Inzidenzrelation durch eine Matrix  $M \in \mathbb{C}^{|V| \times |\mathcal{B}|}$  darstellen, welche Einträge in  $\{0, 1\}$  besitzt.

**Def.**  $\sigma(p) := \{B \in \mathcal{B} | pIB\}$ ,  $\sigma(B) := \{p \in V | pIB\}$  heißen **Bahnen**

**Def.**  $\mathcal{D}$  heißt **einfach**, falls  $\sigma$  injektiv ist.

**Notation.** Falls  $\mathcal{D}$  einfach ist, kann man  $\mathcal{B}$  als Teilmenge von  $\mathcal{P}(V)$  auffassen. Man schreibt daher  $p \in B \text{ :} \Longleftrightarrow pIB$ .

**Notation.**  $v := |V|$ ,  $b := |\mathcal{B}|$

**Def.** Eine endl. IS  $\mathcal{D} = (V, \mathcal{B}, I)$  heißt **linearer Raum**, falls

- $|\sigma(B)| \geq 2$  für alle  $B \in \mathcal{B}$
- $|\sigma(x) \cap \sigma(y)| = 1$  für alle  $x \neq y \in V$ .

**Satz.**  $\mathcal{D} = (V, \mathcal{B}, \in)$  sei ein lin. Raum mit  $b \leq 2$ . Dann gilt  $b \geq v$ .

**Bsp.** Die Inzidenzstruktur

$$V = \{x_1, \dots, x_{v-1}, x_v\}, \quad \mathcal{B} = \{L_1, \dots, L_{v-1}, B\} \\ \sigma(L_i) = \{x_i, x_v\}, \quad \sigma(B) = \{x_1, \dots, x_{v-1}\}$$

ist ein linearer Raum mit  $b = v$ . Dieser besitzt einen Block, der alle Pkte bis auf einen enthält und dual einen Punkt, der in allen Blöcken bis auf einen liegt. Solche Inzidenzstrukturen heißen **entartet**.

**Lem.** Für je zwei Punkte  $x, y$  eines nicht-entarteten Raumes gibt es eine Gerade, die weder  $x$  noch  $y$  enthält.

**Def.** Ein nicht-entarteter linearer Raum mit  $v = b$  heißt eine (endliche) **projektive Ebene**.

**Satz.** Sei  $\pi = (V, G, \in)$  eine projektive Ebene. Dann gilt:

- Je zwei verschiedene Geraden schneiden sich in genau einem Pkt.
- Es gibt ein  $n \in \mathbb{N}$  mit  $n \geq 2$ , sodass:
  - Jede Gerade enthält  $n + 1$  Punkte.
  - Jeder Punkt liegt auf genau  $n + 1$  Geraden.
  - $b = v = n^2 + n + 1$

**Def.**  $n$  heißt **Ordnung** von  $\pi$ .

**Bsp.** Die Fano-Ebene ist die projektive Ebene der Ordnung 2.

**Fakten.** • Es gibt keine proj. Ebene der Ordnung 10.

- Jede *heute bekannte* proj. Ebene hat Primzahlpotenzordnung.
- Zu jeder Primzahlpotenz  $q \geq 2$  ex. eine proj. Ebene der Ord.  $q$ .
- Es ist nicht bekannt, ob eine proj. Ebene mit  $n = 12$  existiert.

**Satz (Bruck, Ryser).** Sei  $n \geq 2$ . Angenommen,  $n \equiv 1 \bmod 4$  oder  $n \equiv 2 \bmod 4$ . Sei  $n = p_1^{a_1} \cdot \dots \cdot p_l^{a_l}$  eine Primfaktorzerlegung von  $n$ . Gibt es ein  $i$  mit  $p_i \equiv 3 \bmod 4$  und  $a_i$  ungerade, so existiert keine projektive Ebene der Ordnung  $n$ .

**Kor.** Ist  $n \equiv 6 \bmod 8$ , so gibt es keine proj. Ebene der Ordnung  $n$ .

**Satz.** Sei  $q \geq 2$  eine Primzahlpotenz. Dann gibt es eine projektive Ebene der Ordnung  $q$ .

*Konstr.*      Punkte  $p$     := die ein-dim. Teilräume von  $\mathbb{F}_q^3$ ,  
Geraden  $\mathcal{B}$      := die zwei-dim. Teilräume von  $\mathbb{F}_q^3$ ,  
 $p \in B$         :=  $\Longleftrightarrow p \subseteq B$ .

**Def.** Sei  $\mathcal{D} = (V, \mathcal{B}, I)$  eine endl. Inzidenzstruktur. Es gebe  $r, k \in \mathbb{N}$  mit  $r \geq 2$  und  $k \geq 2$  mit  $|\sigma(x)| = r$  für alle  $x \in V$  und  $|\sigma(B)| = k$  für alle  $B \in \mathcal{B}$ . Dann heißt  $\mathcal{D}$  eine **taktische Konfiguration**.

*Bem.* Doppeltes Zählen der Inzidenzen  $I$  ergibt:  $v \cdot r = |I| = b \cdot k$ .

**Def.** Sei  $\mathcal{D} = (V, \mathcal{B}, I)$  eine endliche IS. Es gebe  $k, t, \lambda \in \mathbb{N}$  mit:

- $v = |V| \geq k \geq t$ ,                      •  $|\sigma(B)| = k$  für alle  $B \in \mathcal{B}$ ,
- Zu jeder  $t$ -elementigen Teilmenge  $T \subseteq V$  gibt es genau  $\lambda$  Blöcke aus  $\mathcal{B}$  mit  $T \subseteq \sigma(B)$ .

Dann heißt  $\mathcal{D}$  ein  **$t$ -( $v, k, \lambda$ )-Blockplan**,  **$S_\lambda(t, k, v)$ -Steinersystem** oder  **$t$ -Design**.

**Bsp.** Eine proj. Ebene der Ordnung  $n$  ist ein  $S_1(2, n + 1, n^2 + n + 1)$ .

**Bsp.** Sei  $V$  eine Menge,  $v \geq 2$ ,  $t \leq k$ . Sei  $\mathcal{B} := \{B \subseteq V | |B| = k\}$ . Dann ist  $(V, \mathcal{B}, \in)$  ein  $t$ -Design mit  $\lambda = \binom{v-t}{k-t}$ .

**Prop.** Sei  $\mathcal{D} = (V, \mathcal{B}, I)$  ein  $S_\lambda(t, k, v)$ . Ist  $s \in \mathbb{N}$  mit  $s \leq t$ , dann ist  $\mathcal{D}$  auch ein  $s$ -Design und zwar mit  $\lambda_s = \frac{\lambda \cdot v - st - s}{\binom{k-s}{t-s}}$ .

**Kor.** Ist  $t \geq 1$ , so ist  $\mathcal{D}$  eine taktische Konf. mit Replikationszahl

$$r = \lambda_1 = \frac{\lambda \binom{v-1}{t-1}}{\binom{k-1}{t-1}}$$

Die Anzahl der Blöcke in einem Blockplan ist

$$b = \lambda_0 = \frac{\lambda \binom{v}{t}}{\binom{k}{t}}.$$

**Satz.** Sei  $C$  ein bin. perfekter  $(n, M, d)$ -Code wobei  $d = 2t + 1$ . Setze  $V := \{1, \dots, n\}$ ,  $\mathcal{B} := \{\text{supp}(c) | c \in C \text{ mit } \text{wt}(c) = d\}$ .

Dann ist  $(V, \mathcal{B}, \in)$  ein  $S_1(\tau, d, n)$  wobei  $\tau := t + 1$ .

**Bspe.** • Ein  $[2^m - 1, 2^m - 1 - m, 3]$ -Hamming-Code über  $\mathbb{F}_2$  liefert ein  $S_1(2, 3, 2^m - 1)$ .

- $\mathcal{G}(23)$  ist ein perfekter, binärer  $[23, 12, 7]$ -Code  $\implies \exists S_1(4, 7, 23)$ .
- Angenommen, es gibt einen bin.  $(90, 2^{78}, 5)$ -Code (also perfekt). Dann  $\exists$  ein  $S_1(3, 5, 90)$ , etwa  $\mathcal{D}$ . Dann ist  $\mathcal{D}$  ein  $S_{\lambda_2}(2, 5, 90)$  mit

$$\lambda_2 = \frac{\lambda \binom{v-2}{t-2}}{\binom{k-2}{t-2}} = \frac{1 \binom{88}{1}}{\binom{3}{1}} = \frac{88}{3} \notin \mathbb{N}.$$

*Bem.* Sei  $C$  ein binärer perfekter  $(n, M, d)$ -Code,  $\overline{C}$  dessen Parity-Check-Erweiterung (ein  $(n + 1, M, d + 1)$ -Code). Dann gibt es ein  $S(t + 2, d + 1, n + 1)$ . Konstruktion:

$$\mathcal{B} = \{\text{supp}(\overline{c}) | \overline{c} \in \overline{C}, \text{wt}(\overline{c}) = d + 1\}, \quad V = \{1, \dots, n + 1\}$$

Insbesondere  $\mathcal{G}(23) \rightsquigarrow \mathcal{G}(24) \implies \exists S_1(5, 8, 24)$

**Satz.** Es gibt ein  $S_1(5, 6, 12)$

*Konstr.* Sei  $\mathcal{G}(12)$  der ternäre  $[12, 6, 6]$ -Code.

$$V = \{1, \dots, 12\}, \quad \mathcal{B} = \{\text{supp}(c) | c \in \mathcal{G}(12), \text{wt}(c) = 6\}$$

**Satz.** Es gibt ein  $S_1(4, 5, 11)$

**Def.** Sei  $n \geq 2$ . Ein  $S_1(2, n, n^2)$  heißt **affine Ebene** der Ord.  $n$ .

**Satz.**  $\exists S_1(2, n, n^2) \iff \exists S_1(2, n + 1, n^2 + n + 1)$

*Konstr.* • Sei zunächst  $(V, \mathcal{G}, \in)$  eine projektive Ebene der Ord.  $n$ . Wähle eine Gerade  $L \in \mathcal{G}$ . Dann ist

$$\alpha := (V', \mathcal{G}', \in) := (V \setminus L, \mathcal{G} \setminus \{L\}, \in)$$

eine affine Ebene der Ordnung  $n$ .

- Sei umgekehrt  $(W, \mathcal{H}, \in)$  eine aff. Ebene der Ord.  $n$ . Dann def.  $L$  ist parallel zu  $K \text{ :} \Longleftrightarrow L \parallel K \text{ :} \Longleftrightarrow (L = K) \vee (L \cap K = \emptyset)$  eine Äq'relation auf  $\mathcal{H}$ . Dann ist  $(V, \mathcal{G}, \in)$  mit  $V := W \amalg (\mathcal{H} / \parallel)$ ,  $\mathcal{G} := \{K \amalg \{[K]\} | K \in \mathcal{H}\} \amalg \{\mathcal{H} / \parallel\}$  eine projektive Ebene der Ordnung  $n$ .

**Def.**  $\mathcal{D}$  sei ein  $S_\lambda(t, k, v)$ , wobei  $t \geq 2$ . Sei  $x \in V$ . Dann heißt  $\mathcal{D}' := (V', \mathcal{B}', \in)$ , wobei  $V' := V \setminus \{x\}$ ,  $\mathcal{B}' := \{B \setminus \{x\} | B \in \mathcal{B}, x \in B\}$  das nach  $x$  **abgeleitete Design**. Es ist  $\mathcal{D}'$  ein  $S_\lambda(t - 1, k - 1, v - 1)$ .

*Bem.* Wie in Analysis gilt: Ableiten ist leicht, „Integrieren“ schwer.

**Bsp.**  $S_1(5, 6, 12)'''' = S_1(4, 5, 11)''' = S_1(3, 4, 10)'' = S_1(2, 3, 9)' = S_1(1, 2, 8)$



**Lem (Fisher).** Für jeden  $2-(v, k, \lambda)$ -Blockplan mit  $v > k$  gilt  $b \geq v$ . Falls  $v = b > k$ , so ist die Inzidenzmatrix invertierbar.

**Def.** Ein  $2-(v, k, \lambda)$ -Blockplan mit  $v = b > k$  heißt **symmetrisch** mit **Ordnung**  $n := k - \lambda$ .

**Achtung.** „symmetrisch“ bezieht sich nicht auf die Inzidenzmatrix!

**Bsp.** Endliche projektive Ebenen sind symmetrisch (mit  $\lambda = 1$ ).

**Satz (Ryser).** Sei  $\mathcal{D} = (V, \mathcal{B}, I)$  ein symm.  $2-(v, k, \lambda)$ -Blockplan. Dann gilt  $r = k$  und je zwei verschiedene Blöcke haben genau  $\lambda$  gemeinsame Punkte.

*Bem.* Somit ist der duale Blockplan zu  $\mathcal{D}$ , der durch Vertauschen der Rollen von Blöcken und Punkten entsteht, ebenfalls ein  $2-(v = b, k = r, \lambda)$ -Blockplan. Darauf bezieht sich das „symmetrisch“.

**Satz.** Sei  $\mathcal{D}$  ein symm.  $2-(v, k, \lambda)$ -Blockplan der Ordnung  $n$ .

- Ist  $n$  gerade, so ist  $n$  eine Quadratzahl.
- Ist  $v$  ungerade, so gibt es ein ganzzahliges Tripel  $z = (z_1, z_2, z_3) \neq (0, 0, 0)$  mit

$$z_1^2 = n \cdot z_2^2 + (-1)^{(v-1)/2} \lambda \cdot z_3^2.$$

*Bem.* Der Satz von Bruck und Ryser ist eine Korollar hiervon.

*Bem.* Sei  $\mathcal{D} = (V, \mathcal{B}, I)$  ein symm.  $2-(v, k, \lambda)$ -Blockplan. Das zu  $\mathcal{D}$  **komplementäre Design** ist  $\mathcal{D}^c := (V, \mathcal{B}, I^c)$ ,  $pI^c B : \iff \neg(pIB)$ . Dann ist  $\mathcal{D}^c$  ein  $2-(v, v - k, \lambda^c)$ -Blockplan mit  $\lambda^c = v - 2n - \lambda$ .

**Satz.** Sei  $\mathcal{D}$  ein symmetrischer  $2-(v, k, \lambda)$ -Blockplan der Ordnung  $n$  mit  $1 < k < v - 1$ . Dann gilt  $4n - 1 \leq v \leq n^2 + n + 1$ . Das Polynom  $X^2 + (2n - v)X + (n - 1)n = 0$  besitzt die Nullstellen  $\lambda$  und  $\lambda^c$ .

*Bem.* Projektive Ebenen besitzen also die maximale Anzahl an Punkten unter allen symmetrischen Blockplänen der Ordnung  $n$ . Blockpläne, deren Punktzahl die untere Schranke erfüllt, besitzen auch eine eigene Bezeichnung:

**Def.**  $2-(4n-1, 2n-1, n-1)$ -Designs heißen **Hadamard-Designs**.

# Reed-Muller-Codes

**Satz (Plotkin-Schranke).** Sei  $q \geq 2$ ,  $d > \frac{q-1}{q} \cdot n$ . Dann gilt

$$A_q(n, d) \leq \frac{d}{d - \frac{q-1}{q} \cdot n}.$$

**Lem.** Sei  $n \geq 2$ ,  $1 \leq d < n$ . Dann:  $A_2(n, d) \leq 2 \cdot A_2(n - 1, d)$

**Satz.** Für  $l \geq 1$  gilt  $A_2(4l, 2l) \leq 8l$ .

**Satz.** Für  $m \geq 1$  gilt  $A_2^{\text{lin}}(2^m, 2^{m-1}) = A_2(2^m, 2^{m-1}) = 2^{m+1}$ , d. h. es existiert ein  $[2^m, m + 1, 2^{m-1}]$ -Code.

*Konstr.* Man definiert rekursiv Generatormatrizen durch

$$G_{m+1} = \left( \begin{array}{ccc|ccc} 0 & \cdots & 0 & 1 & \cdots & 1 \\ \hline & G_m & & & G_m & \end{array} \right), \quad G_1 := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

**Def.** Sei  $m \geq 1$ . Eine **Boolesche Funktion** in  $m$  Variablen ist eine Abbildung von  $\mathbb{F}_2^m$  nach  $\mathbb{F}_2$ .

**Notation.**  $\mathcal{B}_m := \mathbb{F}_2^{\mathbb{F}_2^m} =$  Algebra der Booleschen Fktn in  $m$  Var.

**Def.**  $\Gamma : \mathbb{F}_2[x_1, \dots, x_m] \rightarrow \mathcal{B}_m$ ,  $f(x) \mapsto (\bar{f} : v \mapsto f(v_1, \dots, v_m))$

**Satz.**  $\Gamma$  ist ein surjektiver Algebra-Homomorphismus mit

$$\ker \Gamma = \langle x_1^2 + x_1, \dots, x_m^2 + x_m \rangle \subset \mathbb{F}_2[x_1, \dots, x_m] = \mathbb{F}_2[\vec{x}].$$

**Kor.**  $\mathcal{B}_m \cong \mathbb{F}_2[\vec{x}] / \langle x_1^2 + x_1, \dots, x_m^2 + x_m \rangle$   
 $\cong \mathbb{F}_2[\vec{x}]_{\text{red}} := \text{span}\{\text{Monome } x^\alpha \text{ mit } \alpha \leq (1, \dots, 1)\}$

**Notation.**  $x_I := \prod_{i \in I} x_i$  für  $I \subset \{1, \dots, m\}$

**Def.** Der (binäre) **Reed-Muller-Code** zu  $(r, m)$  ist

$$\mathcal{R}(r, m) := \Gamma(X(r, m)) \quad \text{mit } X(r, m) := \text{span}\{x_I \mid I \subset \{1, \dots, m\}, |I| \leq r\}$$

**Bspe.** •  $\mathcal{R}(0, m) = \{0 \cdots 0, 1 \cdots 1\} = (2^m)$ -Wiederholungscode

•  $\mathcal{R}(-1, m) := \{0 \cdots 0\}$  •  $\mathcal{R}(m, m) := \mathcal{B}_m$

$$\begin{array}{ccccccc} \text{Bem.} & \bullet & \mathcal{R}(-1, m) & \subseteq & \mathcal{R}(0, m) & \subseteq & \mathcal{R}(1, m) & \subseteq & \cdots \\ & & \perp & & \perp & & \perp & & \\ & & \mathcal{R}(m, m) & \supseteq & \mathcal{R}(m-1, m) & \supseteq & \mathcal{R}(m-2, m) & \supseteq & \cdots \end{array}$$

$$\bullet \dim \mathcal{R}(r, m) = \sum_{j=0}^r \binom{m}{j}$$

**Satz.**  $\mathcal{R}(1, m)$  hat Minimalgewicht  $2^{m-1}$ . Gewichtsverteilung:  $A_0 = 1$ ,  $A_{2^m} = 1$ ,  $A_{2^m-1} = 2^{m+1} - 2$ ,  $A_i = 0$  für alle anderen  $i$ .

*Bem.*  $\mathcal{R}(1, m) = \Gamma(\text{span}\{1\}) \oplus \widehat{\text{Sim}}_2(m)$

**Satz.**  $\mathcal{R}(r, m)^\perp = \mathcal{R}(m - r - r, m)$  für alle  $r$

**Kor.** Ist  $m$  ungerade, so ist  $\mathcal{R}(\frac{m-1}{2}, m)$  selbstdual.

**Bsp.**  $\mathcal{R}(1, 3) = \widehat{\text{Ham}}_2(3)$  ist ein selbst-dualer  $[2^3, 3 + 1, 2^2]$ -Code.

**Lem.**  $\widehat{\text{Ham}}_2(m) = \mathcal{R}(m - 2, m)$

**Satz.** Sei  $0 \leq r \leq m \geq 1$ . Der binäre Reed-Muller-Code  $\mathcal{R}(r, m)$  hat das Minimalgewicht  $2^{m-r}$

**Kor.**  $\mathcal{R}(r, m)$  ist ein  $[2^m, \sum_{i=0}^r \binom{m}{i}, 2^{m-r}]$ -Code

## Hadamard-Matrizen und Hadamard-Designs

**Satz.** Für  $A \in \mathbb{R}^{n \times n}$  mit  $|A_{ij}| \leq 1$  gilt  $|\det(A)| \leq \sqrt{n^n}$ .  
Gleichheit liegt genau dann vor, wenn  $|A_{ij}| = 1$  für alle  $i, j$  und wenn  $AA^T = nE_n$ .

**Def.** Eine Matrix  $H \in \mathbb{R}^{n \times n}$  mit  $H_{ij} \in \{\pm 1\}$  heißt **Hadamard-Matrix** der Ordnung  $n$ , falls  $HH^T = nE_n$ .

**Bsp.**  $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$  ist eine Hadamard-Matrix.

**Satz.** Ist  $H \in \mathbb{R}^{n \times n}$  eine Hadamard-Matrix, so gilt  $n \in \{1, 2\} \cup 4\mathbb{N}$ .

**Satz.** Sei  $l \geq 1$  und  $H$  eine Hadamard-Matrix der Ordnung  $4l$ .

- Es gibt einen symmetrischen  $S_{l-1}(2, 2l-1, 4l-1)$ -Blockplan.
- Es gibt einen binären  $(4l, 8l, 2l)$ -Code.  
Dieser ist optimal, also  $A_2(4l, 2l) = 8l$ .

**Konstr.** • Wir können davon ausgehen, dass die erste Zeile und Spalte von  $H$  nur Einsen enthalten (durch Multiplizieren mit  $-1$ ).  
Durch Streichen der ersten Zeile und Spalte erhalten wir aus  $H$  eine Matrix  $M \in \mathbb{R}^{4l-1, 4l-1}$ . In  $M$  ersetzen wir  $-1$  durch  $0$  und bekommen so die Inzidenzmatrix des gesuchten Blockplans.  
(Diese Konstruktion lässt sich umkehren.)

• Der Code besteht aus den Zeilen von  $H$  und  $-H$  (wobei wir  $\{0, 1\} \leftrightarrow \{-1, 1\}$  anwenden).

**Lem (Produktkonstruktion).** Das Kronecker-Produkt  $H \otimes L$  von Hadamard-Matrizen  $H$  und  $L$  der Ordnung  $n$  bzw.  $m$  ist selbst eine Hadamard-Matrix der Ordnung  $n \cdot m$ .

**Satz (Paley).** Sei  $p > 2$  prim,  $q = p^k$ . Sei  $\epsilon \in \mathbb{N}$  sodass  $4|2^\epsilon \cdot (q+1)$ .  
Dann existiert eine Hadamard-Matrix der Ord.  $n = 2^\epsilon \cdot (q+1)$ .

**Konstr.** Der **quadratische Charakter** von  $\mathbb{F}_q$  ist die Abbildung

$$\psi : \mathbb{F}_q \rightarrow \mathbb{C}, \quad x \mapsto \begin{cases} 0 & \text{falls } x = 0, \\ 1 & \text{falls } \exists y \in \mathbb{F}_q \setminus \{0\} : x = y^2, \\ -1 & \text{sonst.} \end{cases}$$

- Falls  $q \equiv 3 \pmod{4}$ : Dann definiert

$$M_{xy} := \begin{cases} \psi(x-y) & \text{falls } x \neq y \\ -1 & \text{falls } x = y \end{cases}$$

eine Matrix  $M \in \{\pm 1\}^{\mathbb{F}_q \times \mathbb{F}_q}$ . Durch Hinzufügen einer 1-Spalte und 1-Zeile erhalten wir eine Hadamard-Matrix  $H \in \mathbb{R}^{q+1 \times q+1}$ .  
Durch die Produkt-konstruktion mit  $H_2$  erhält man die gesuchten Matrizen.

- Falls  $q \equiv 1 \pmod{4}$ : Dann ist  $2(q+1)$  durch 4 teilbar. Setze  $\mathbb{F}'_q := \mathbb{F}_q \cup \{\infty\}$ . Wir definieren  $M \in \{-1, 0, 1\}^{\mathbb{F}'_q \times \mathbb{F}'_q}$  durch

$$M_{xy} := \begin{cases} 1 & \text{falls } \infty \in \{x, y\} \neq \{\infty\}, \\ 0 & \text{falls } x = y = \infty, \\ \psi(x-y) & \text{sonst.} \end{cases}$$

Weiter sei  $A = H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ ,  $B = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$ .

Schließlich bestehe  $H = (H_{xy})_{x, y \in \mathbb{F}'_q}$  aus den  $(2 \times 2)$ -Blöcken

$$H_{xy} := \begin{cases} B & \text{falls } M_{xy} = 0, \\ A & \text{falls } M_{xy} = 1, \\ -A & \text{falls } M_{xy} = -1. \end{cases}$$

Dann ist  $H$  eine Hadamard-Matrix der Größe  $2(q+1)$ . Durch Produktbildung mit  $H_2$  erhält man Hadamard-Matrizen der gesuchten Ordnung.

**Prop.** Sei  $H \in \{1, -1\}^{\mathbb{F}_2^m \times \mathbb{F}_2^m}$  definiert durch  $H_{uv} := (-1)^{\langle u, v \rangle}$  für alle  $u, v \in \mathbb{F}_2^m$ . Dann ist  $H$  eine Hadamard-Matrix der Ordnung  $2^m$ .

**Def.** Sei  $F \in \mathbb{R}^{\mathbb{F}_2^m} = \text{Abbildungen } \mathbb{F}_2^m \rightarrow \mathbb{R}$ . Die **Hadamard-Transformierte** von  $F$  ist

$$\hat{F} : \mathbb{F}_2^m \rightarrow \mathbb{R}, \quad u \mapsto \sum_{v \in \mathbb{F}_2^m} (-1)^{\langle u, v \rangle} F(v).$$

Die **inverse Hadamard-Transformation** ist gegeben durch

$$G \in \mathbb{R}^{\mathbb{F}_2^m} \mapsto G^* \in \mathbb{R}^{\mathbb{F}_2^m} \quad \text{mit} \quad G^*(u) = \frac{1}{2^m} \cdot \sum_{v \in \mathbb{F}_2^m} (-1)^{\langle u, v \rangle} G(v).$$

**Notation.** Für  $\beta \in \mathcal{B}_m$ , also eine boolsche Funktion in  $m$  Variablen, sei  $B_\beta$  definiert durch  $B_\beta(u) := (-1)^{\beta(u)}$ .

$$\begin{aligned} \mathcal{R}(1, m) &\hat{=} \text{span}\{1, x_1, \dots, x_m\} \\ &= \text{span}\{1\} \oplus \underbrace{\text{span}\{x_1, \dots, x_m\}}_{O(1, m) :=} = O(1, m) \sqcup [1 + O(1, m)] \end{aligned}$$

Sei  $\phi \in \mathcal{R}(1, m)$  gesendet,  $\beta \in \mathcal{B}_m$  empfangen. Gesucht:  $\gamma \in \mathcal{R}(1, m)$  mit  $d(\gamma, \beta)$  minimal.

**Satz.** Sei  $\beta \in \mathcal{B}_m$ ,  $\gamma \in O(1, m)$ ; schreibe  $\gamma = \lambda_1 x_1 + \dots + \lambda_m x_m$ .

- $d(\beta, \gamma) = \frac{1}{2}(2^m - \hat{B}_\beta(\lambda))$       •  $d(\beta, 1 + \gamma) = \frac{1}{2}(2^m + \hat{B}_\beta(\lambda))$

Zur Decodierung von  $\mathcal{R}(1, m)$ : Dies ist ein  $[2^m, 1 + m, 2^{m-1}]$ -Code, also  $t = \frac{2^{m-1}-1}{2} < 2^{m-2}$ . Angenommen,  $\phi \in \mathcal{R}(1, m)$  ist gesendet, es sind höchstens  $t$  Fehler aufgetreten,  $\beta$  empfangen. Dann gilt  $d(\phi, \beta) \leq t$  und

- Falls  $\phi \in O(1, m)$ :  $\phi = \sum_{i=1}^m \alpha_i x_i$ ,  $\hat{B}_\beta(\alpha) = 2^m - 2 \cdot d(\beta, \phi) > 0$ .
- Falls  $\phi \in 1 + O(1, m)$ :  $\phi = 1 + \sum_{i=1}^m \alpha_i x_i$ .

Beachte:  $\min\{d(\beta, \gamma), d(\beta, 1 + \gamma)\} = \frac{1}{2} \cdot (2^m - |\hat{B}_\beta(\lambda)|)$  für  $\gamma \in O(1, m)$ . Gesucht ist ein  $\gamma$  mit  $\frac{1}{2}(2^m - |\hat{B}_\beta(\lambda)|)$  minimal  $\iff |\hat{B}_\beta(\lambda)|$  maximal.

(Beachte:  $\hat{B}_\beta = H \cdot B_\beta$  mit  $H = H_2 \otimes \dots \otimes H_2$  ( $m$ -mal) mit schneller Hadamard-Transformation berechenbar.)

$\hat{B}_\beta$  liegt vor, das heißt  $\hat{B}_\beta(\lambda)$  ist bekannt für alle  $\lambda \in \mathbb{F}_2^m$ .

Suche nun ein  $\lambda \in \mathbb{F}_2^m$  mit  $|\hat{B}_\beta(\lambda)|$  ist minimal.

- Annahme,  $\hat{B}_\beta(\lambda) > 0$ . Decodiere  $\beta$  zu  $\sum_{i=1}^m \lambda_i x_i \in o(1, m)$ .

- Annahme,  $\hat{B}_\beta(\lambda) < 0$ . Decodiere  $\beta$  zu  $1 + \sum_{i=1}^m \lambda_i x_i \in 1 + o(1, m)$ .

# Die Gewichtsverteilung von dualen Codes

**Def.** Betrachte einen Code  $C \subseteq \mathbb{F}_q^n$ . Für  $j = 0, \dots, n$  sei

$$\Delta_C(j) := \frac{1}{|C|} |\{(x, y) \in C \times C \mid d(x, y) = j\}|.$$

$\Delta_C \in \mathbb{Q}^{\{0, \dots, n\}}$  heißt **Distanzverteilung** von  $C$ .

**Prop.** Ist speziell  $C$  ein  $\mathbb{F}_q$ -linearer Code, dann gilt:  $\Delta_C = A_C =$  Gewichtsverteilung von  $C$ .

**Def.** Ein **additiver Charakter** von  $\mathbb{F}_q$  ist eine Gruppen-Homomorphismus von  $(\mathbb{F}_q, +, 0)$  nach  $(\mathbb{C}^*, \cdot, 1)$ .

**Notation.**  $\hat{\mathbb{F}}_q :=$  Menge aller additiven Charaktere

*Bem.*  $\hat{\mathbb{F}}_q$  ist eine Gruppe mit

$$[\chi \cdot \psi](x) := \chi(x) \cdot \psi(x), \quad \chi_0(x) := 1.$$

Es gilt  $(\hat{\mathbb{F}}_q, \cdot, \chi_0) \cong (\mathbb{F}_q, +, 0)$ .

Für  $q = p$  prim ist

$$\gamma : (\mathbb{F}_p = \mathbb{Z}_p, +, 0) \rightarrow (\mathbb{C}^*, \cdot, 1), \quad z \mapsto \exp\left(\frac{2\pi z i}{p}\right)$$

ein additiver Charakter.

Für  $q = p^k$ ,  $k \geq 2$  verwenden wir die Spurabbildung

$$\text{trace} : \mathbb{F}_q \rightarrow \mathbb{F}_p, \quad x \mapsto \sum_{j=0}^{k-1} x^{p^j}. \quad (\text{Dies ist eine nicht-triviale$$

Linearform.)) Dann ist

$$\chi : \mathbb{F}_q \rightarrow \mathbb{C}^*, \quad x \mapsto \gamma \circ \text{trace}(x)$$

eine nicht-triviale Charakter, der sogenannte **Hauptcharakter**.

*Bem.* Zu jedem  $y \in \mathbb{F}_q$  ist  $\chi_y : \mathbb{F}_q \rightarrow \mathbb{C}^*, \quad x \mapsto \exp\left(\frac{2\pi \text{trace}(xy)i}{p}\right)$

ein weiterer Charakter und es gilt

$$\hat{\mathbb{F}}_q = \{\chi_y \mid y \in \mathbb{F}_q\}.$$

Sei  $V$  ein  $\mathbb{C}$ -Vektorraum. Wir betrachten Abbildung von  $\mathbb{F}_q^n$  nach  $V$ .

Sei  $\chi \in \hat{\mathbb{F}}_q$ ,  $\chi \neq \chi_0$  Zu  $f : \mathbb{F}_q^n \rightarrow V$  definieren wir eine **transformierte Abbildung** durch

$$\hat{f} : \mathbb{F}_q^n \rightarrow V, \quad u \mapsto \sum_{v \in \mathbb{F}_q^n} \chi(\langle u, v \rangle) \cdot f(v).$$

**Satz.** Sei  $U$  ein  $\mathbb{F}_q$ -Teilraum von  $\mathbb{F}_q^n$  und  $f : \mathbb{F}_q^n \rightarrow V$  eine Abbildung. Dann gilt

$$\sum_{u \in U} \hat{f}(u) = |U| \cdot \sum_{w \in U^\perp} f(w).$$

**Satz.** Sei  $C \subseteq \mathbb{F}_q^m$  ein linearer Code. Betrachte den dualen Code  $C^\perp$  zu  $C$ . Dann:

$$A_{C^\perp}^{\text{hom}}(X, Y) = \frac{1}{|C|} \cdot A_C^{\text{hom}}(X + (q-1)Y, X - Y), \quad A_{C^\perp}(Z) = \frac{1}{|C|} \cdot (1 + (q-1)Z)^n \cdot A_C\left(\frac{1}{1+(q-1)Z}\right).$$

*Beweisidee.* Verwende den letzten Satz mit  $V = \mathbb{C}[X, Y]$  und

$$f(v) := X^{n-\text{wt}(v)} Y^{\text{wt}(v)}.$$

**Bsp.** Sei  $m \geq 1$ . Für den Simplex-Code gilt

$$A_{\text{Sim}_q(m)}^{\text{hom}}(X, Y) = X^n + (q^m - 1)X^{n-q^{m-1}}Y^{q^{m-1}}.$$

Somit gilt für den Hamming-Code  $\text{Ham}_q(m) = \text{Sim}_q(m)^\perp$ :

$$A_{\text{Ham}_q(m)}^{\text{hom}}(X, Y) = \frac{1}{q^m} \left( [X + (q-1)Y]^n + (q^m - 1) \cdot [X + (q-1)Y]^{n-q^{m-1}} \right).$$

**Bsp.** Wir betrachten den  $[24, 8, 12]$ -Code  $C = \mathcal{G}(24) = C^\perp$ . Es gilt

$$A_C^{\text{hom}}(X, Y) = X^{24} + A_8 X^{16} Y^8 + A_{12} X^{12} Y^{12} + A_8 X^8 Y^{16} + Y^{24}.$$

TODO: weiter?

**Def.** Eine Matrix  $A \in \mathbb{Z}_q^{q \times q}$  heißt **lateinisches Quadrat** der Ordnung  $q$ , falls in jeder Zeile und Spalte jede Zahl aus  $\mathbb{Z}_q$  genau einmal vorkommt.

**Def.** Zwei lateinische Quadrate  $A, B \in \mathbb{Z}_q^{q \times q}$  heißen **orthogonal** ( $A \perp B$ ), falls folgende Abbildung bijektiv ist:

$$\{1, \dots, q\}^2 \rightarrow \mathbb{Z}_q^2, \quad (i, j) \mapsto (A_{ij}, B_{ij})$$

**Satz.** Es gibt genau dann ein Paar orthogonaler Quadrate der Ordnung  $q$ , wenn  $q \notin \{2, 6\}$ .

**Satz.** Sei  $n = 4$ ,  $d = 3$ . Dann gilt

- $A_2(4, 3) = 2 < 4 = 2^{4-3+1}$
- $A_6(4, 3) = 34 < 36 = 6^{4-3+1}$
- $A_q(4, 3) = q^2 = q^{4-3+1}$  für  $q \geq 3$ ,  $q \neq 6$

*Beweisidee.* Man zeigt: Existenz eines MDS-Codes  $\iff$  es gibt ein Paar orthogonaler lateinischer Quadrate der Ordnung  $q$ .

**Satz.** Es gibt keinen (perfekten) 6-ären  $(7, 6^5, 3)$ -Code.

**Def.** Seien  $\psi_1, \dots, \psi_l$  lateinische Quadrate der Ordnung  $q$  über  $\mathbb{Z}_q$ . Diese heißen **paarweise orthogonal**, falls  $\psi_i \perp \psi_j$  für alle  $i \neq j$ . Man sagt,  $\psi_1, \dots, \psi_l$  ist eine Liste von MOLS (mutually orthogonal latin squares) der Ordnung  $q$ .

*Bem.* Sei  $N(q) :=$  die maximale Anzahl von MOLS der Ordnung  $q$ .

- Es gilt  $N(q) \leq q - 1$ .
- Eine Produkt-Konstruktion liefert:  $N(q) \geq \min\{N(r), N(s)\}$ , falls  $q = rs$  mit  $\text{ggT}(r, s) = 1$ .  $q = \prod_{i=1}^m p_i^{a_i}$  Primfaktorzerlegung. Dann:
$$N(q) \geq \min\{N(p_i^{a_i}) \mid i = 1, \dots, m\}.$$
- Sei  $q \geq 2$  eine Primzahlpotenz. Dann ist  $N(q) = q - 1$ .
- $N(q) = q - 1 \iff \exists$  projektive Ebene der Ordnung  $q$

**Notation.**  $[n] := \{1, \dots, n\}$

Für  $I \subseteq [n]$  sei  $U_I := \text{span}\{e_i \mid i \in I\} \subseteq \mathbb{F}_q^n$

**Def.** Sei  $C$  ein  $[n, k]$ -Code. Dann sei  $\delta_C(I) := \delta(I) := \dim(C \cap U_I)$ .

**Prop.** •  $\delta(I) \geq 0$  falls  $|I| < d$

- $\exists I \subseteq [n] : |I| = d \wedge \delta(I) = 1$
- $\forall I \subseteq [n] : |I| = d \wedge \delta(I) = 1 \implies \delta(I) = 1$

**Def.** • Für  $i \in [n]$  sei  $A_C(i) := A_i := |\{w \in C \mid \text{wt}(w) = i\}|$

• Für  $I \subseteq [n]$  sei  $a_C(I) := a(I) := |\{w \in C \mid \text{supp}(w) = I\}|$

$$\text{Bem. } A_i = \sum_{I \subseteq [n], |I|=i} a(I)$$

**Satz.** Sei  $C$  ein  $[n, k]$ -Code über  $\mathbb{F}_q$ . Dann ist

$$a(I) = \sum_{K \subseteq I} (-1)^{|I|-|K|} \cdot q^{\delta(K)}.$$

*Bem.* Es gibt auch eine invertierte Formel:

$$|C \cap U_I| = q^{\delta(I)} = \sum_{K \subseteq I} a(K).$$

**Satz.** Sei  $C$  ein  $[n, k, d]$ -MDS-Code über  $\mathbb{F}_q$ . Dann gilt

- $\delta(I) = \max(0, |I| - (d - 1))$  für alle  $I \subseteq [n]$
- $A_j = \binom{n}{j} \sum_{l=d}^j \binom{j}{l} \cdot (-1)^{j-l} \cdot (q^{l-d+1} - 1)$  für  $j \geq d$

Sei  $C$  ein  $[n, k, d]$ -Code über  $\mathbb{F}_q$ . Dann ist  $C^\perp$  ein  $[n, k^\perp, d^\perp]$ -Code mit  $k^\perp = n - k$ . Frage: Was ist  $d^\perp$ ? Falls  $C$  ein MDS-Code ist, so ist  $k = n - d + 1$ , also  $k^\perp = n - k = d - 1$

**Satz.** Ist  $C$  ein linearer MDS-Code, so ist auch  $C^\perp$  ein linearer MDS-Code.

**Lem.**  $(\mathbb{Z}_{q-1}, +, 0) \cong (\mathbb{F}_q^\times, \cdot, 1)$ . Der Isomorphismus ist gegeben durch  $1 \mapsto \beta$ , wobei  $\beta \in \mathbb{F}_q^\times$  mit  $\text{ord } \beta = q - 1$ . Solche  $\beta$  heißen **primitive Elemente**.

*Bem.* Die Anzahl primitiver Elemente in  $\mathbb{F}_q^\times$  ist  $\phi(q - 1)$ , wobei  $\phi$  die Eulersche  $\phi$ -Funktion ist.

**Def.** Betrachte  $\mathbb{F}_q$ . Wähle ein  $n$  mit  $n < q$ . Sei  $\beta$  ein primitives Element von  $\mathbb{F}_q$ . Sei  $l \in \mathbb{N}$  mit  $1 \leq l \leq n$ . Setze  $P_l := \{f(x) \in \mathbb{F}_q[x] \mid \deg(f) < l\}$ . Betrachte

$$\epsilon = \epsilon_\beta : P_l \rightarrow \mathbb{F}_q^n, \quad f(x) \mapsto (f(\beta), f(\beta^2), \dots, f(\beta^n)).$$

Dann heißt  $C := \text{im } \epsilon$  ein **Reed-Solomon-Code**.

**Satz.** Jeder Reed-Solomon-Code ist ein linearer MDS-Code.

**Bsp.** Sei  $q = 8$ ,  $n = 7$ . Wir wollen einen 2-Fehler-korrigierenden MDS-Code  $C$  über  $\mathbb{F}_8$  konstruieren. Somit  $t = 2$ , also  $d = 2t + 1 = 5$ . Dann:  $k = n - d + 1 = 7 - 5 + 1 = 3$ . Dann ist

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta & \beta^3 & \beta^5 \end{pmatrix}$$

eine Generatormatrix von  $C$ .

**Bsp.** Sei  $q = 11$ ,  $\mathbb{F}_{11} \cong \mathbb{Z}_{11}$ . Gesucht ist ein  $[10, 6, 5]$ -MDS-Code  $C$  über  $\mathbb{F}_{11}$ . Wir wissen, dass  $C^\perp$  dann ein  $[10, 4, 7]$ -Code ist. Diesen können wir als Reed-Solomon-Code konstruieren.

TODO: Rest des Beispiels, insbesondere Decodierung

## Zyklische Codes

**Def.** Ein linearer Code  $C \subseteq \mathbb{F}_q^n$  heißt **zyklischer Code**, falls

$$(c_0, c_1, \dots, c_{n-1}) \in C \implies (c_{n-1}, c_0, \dots, c_{n-2}) \in C.$$

*Bem.* Als Koordinaten verwenden wir  $\{0, \dots, n-1\} \cong \mathbb{Z}_n$ . Der **Shift-Operator** ist  $S: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ ,  $e^i \mapsto e^{i+1 \pmod n}$ . Ein zyklischer Code ist ein  $S$ -invarianter Teilraum von  $\mathbb{F}_q^n$ .

**Notation.** Wir identifizieren Wörter  $v \in \mathbb{F}_q^n$  mit Polynomen  $v(x) \in \mathbb{F}_q[x]_{<n} := \{f \in \mathbb{F}_q[x] \mid \deg(f) < n\}$  vermöge

$$\mathbb{F}_q^n \rightarrow \mathbb{F}_q[x]_{<n}, \quad v \mapsto v(x) := v_0 + v_1x + \dots + v_{n-1}x^{n-1}.$$

**Fakt.**  $\mathbb{F}_q[x]$  ist ein euklidischer Hauptidealbereich.

*Bem.* Für  $c \in \mathbb{F}_q^n$  gilt für  $c(x)$  und  $\bar{c}(x) := (Sc)(x) \in \mathbb{F}_q[x]$ :

$$x \cdot c(x) = \bar{c}(x) \pmod{x^n - 1}.$$

Somit gilt:  $C \subseteq \mathbb{F}_q[x]_{<n}$  ist genau dann ein zyklischer Code, wenn  $x \cdot c(x) \bmod (x^n - 1) \in C$  für alle  $c(x) \in C$ .

**Notation.**  $\mathcal{R} := \mathcal{R}_{q,n} := \mathbb{F}_q[x]/(x^n - 1)$

**Satz.** Es gibt kanonische bijektive Korrespondenzen

$$\begin{aligned} & \{ \text{zyklische Codes der Länge } n \text{ über } \mathbb{F}_q \} \\ & \cong \{ \text{Ideale } J \subseteq \mathcal{R}_{q,n} \} \\ & \cong \{ \text{Ideale } I \subseteq \mathbb{F}_q[x] \text{ mit } (x^n - 1) \in I \} \\ & \cong \{ \text{monische Polynome } g(x) \in \mathbb{F}_q[x] \text{ mit } g(x) \mid (x^n - 1) \} \end{aligned}$$

Das zu einem Code  $C \subseteq \mathbb{F}_q[x]_{<n}$  zugehörige monische Polynom ist das (eindeutige!) monische Polynom  $g(x) \in C$  mit minimalem Grad. Es gilt  $C = \{f(x)g(x) \mid f(x) \in \mathbb{F}_q[x] \text{ mit } \deg(f) < n - \deg(g)\}$  und  $\dim(C) = n - \deg(g)$ .

**Def.**  $g(x)$  heißt das **Generatorpolynom** zu  $C$ .  
 $h(x) := (x^n - 1)/g(x)$  heißt **Kontrollpolynom** zu  $C$ .

**Lem.**  $c(x) \in C \iff h(x)c(x) \equiv 0 \pmod{x^n - 1}$

**Notation.**  $k := n - \deg(g)$

*Bem.* Die Generatormatrix von  $C$  ist

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-k} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & g_0 & g_1 & \dots & g_{n-k} \end{pmatrix} \in \mathbb{F}_q^{k \times n}.$$

**Prop.** Sei  $h(x) = h_0 + h_1x + \dots + h_kx^k$ . Dann ist die Kontrollmatrix von  $C$

$$H = \begin{pmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_0 \end{pmatrix} \in \mathbb{F}_q^{n-k \times n}.$$

**Def.** Sei  $f(x) = f_dx^d + \dots + f_0 \in \mathbb{F}_q[x]$  mit  $f_0 \neq 0$  (also  $f(0) \neq 0$ ). Das zu  $f(x)$  **reziproke Polynom** ist

$$f^{\text{rez}}(x) = f\left(\frac{1}{x}\right) \cdot x^d = f_0x^d + f_1x^{d-1} + \dots + f_{n-1}x + f_n.$$

**Satz.** Sei  $C$  ein zyklischer Code der Länge  $n$  über  $\mathbb{F}_q$  mit Generatorpolynom  $g(x)$  und Kontrollpolynom  $h(x)$ . Dann ist  $C^\perp$  ebenfalls zyklisch mit Generatorpolynom  $h^*(x)$  und Kontrollpolynom  $g^*(x)$ , wobei

$$h^*(x) := \frac{1}{h_0} \cdot h^{\text{rez}}(x), \quad g^*(x) := \frac{1}{g_0} \cdot g^{\text{rez}}(x).$$

**Bsp.** Sei  $q = 2$ ,  $n = 7$ . Wir wählen

$$x^7 - 1 = \underbrace{(x-1) \cdot (x^3 + x^2 + 1)}_{h(x) := x^4 + x^2 + x + 1} \cdot \underbrace{(x^3 + x + 1)}_{g(x) :=}$$

Die Generator- und Kontrollmatrix zu  $C_g$  sind

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

$C_g$  ist ein  $[7, 4, 3]$ -Code und äquivalent zu  $\text{Ham}_2(3)$ .

**Bsp.** Sei  $q = 3$ ,  $n = 11$ . Wir wählen

$$x^{11} - 1 = \underbrace{(x-1) \cdot (x^5 + x^4 - x^3 + x^2 - 1)}_{h(x) := x^6 + x^4 - x^3 - x^2 - x + 1} \cdot \underbrace{(x^5 - x^3 + x^2 - x - 1)}_{g(x) :=}$$

Betrachte die Parity-Check-Erw.  $\hat{C}_g$  von  $C_g$ . Die Generatormatrix ist

$$\hat{G} = \begin{pmatrix} -1 & -1 & 1 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & -1 & -1 & 1 & -1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & 1 & -1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & -1 & 1 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1 & 1 & -1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 & -1 & 1 & -1 & 0 & 1 \end{pmatrix}$$

$\hat{C}_g$  ist selbstdual, da  $\hat{G} \cdot \hat{G} = 0$ . Das Minimalgew. von  $\hat{C}_g$  ist somit durch drei teilbar. Je drei Spalten von  $\hat{G}$  sind lin. unabhängig. Daher ist das Minimalgewicht  $\geq 6$ . Wegen der Kugelpackungsschranke gilt Gleichheit. Somit ist  $\hat{C}_g$  ein  $[12, 6, 6]$ -Code und  $C_g$  ein  $[11, 6, 5]$ -Code über  $\mathbb{F}_3$ . Letzterer ist perfekt. Also  $C_g = \mathcal{G}(11)$  und  $\hat{C}_g = \mathcal{G}(12)$ .

**Bsp.** Sei  $q = 2$ ,  $n = 23$ . Die Zerlegung von  $x^{23} - 1 \in \mathbb{F}_2[x]$  in irreduzible Faktoren ist

$$x^{23} - 1 = (x-1) \cdot (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1) \cdot \underbrace{(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)}_{g(x) :=}$$

Es stellt sich heraus, dass  $C_g = \mathcal{G}(23)$ .

## CRC-Codes (*cyclic redundancy check*)

**Verfahren** (CRC-Codierung). Sei  $g(x) \in \mathbb{F}_q[x]_{<n}$  das Generatorpolynom des zyklischen  $[n, k]$ -Codes  $C_g \subset \mathbb{F}_q^n$  mit  $\deg(g) = n - k$ . Der Nachrichtenraum sei  $\mathbb{F}_q^k \cong \mathbb{F}_q[x]_{<k}$ .

• Codierungsabbildung:  $E: \mathbb{F}_q[x]_{<k} \rightarrow C_g$ ,  $m(x) \mapsto c(x)$  mit

$$c(x) := m(x) \cdot x^{n-k} - [m(x) \cdot x^{n-k} \pmod{g(x)}].$$

• Decodierung und Fehlererkennung:  
Angenommen,  $y(x) = y_0 + y_1x + \dots + y_{n-1}x^{n-1} \in \mathbb{F}_q[x]_{<n}$  wurde empfangen. Gilt  $g(x) \mid y(x)$ , also  $y(x) \in C$ , so wurde wahrscheinlich auch  $y(x)$  gesendet. Die zugehörige Nachricht ist

$$m(x) = y_{n-k} + y_{n-k+1}x + \dots + y_{n-1}x^{n-1}.$$

**Def.** Sei  $2 \leq b \leq n$ . Eine Teilmenge  $I \subseteq \mathbb{Z}_n$  heißt ein **zyklisches Intervall der Länge  $b$** , d. h.  $I = \{l + j \bmod n \mid 0 \leq j \leq b-1\}$  für ein  $l \in \mathbb{Z}_n$ . Ein  $v \in \mathbb{F}_q^n$  ist ein **Fehlerbündel der Länge  $b$** , falls  $b$  minimal ist mit: Es existiert ein zyklisches Intervall  $I$  der Länge  $b$  mit  $v_l \neq 0$ ,  $v_{l+b-1 \pmod n} \neq 0$  und  $\text{supp}(v) \subseteq I$ .

**Bsp.**  $v = (0, 2, 0, 0, 0, 0, 1, 1, 0)$  ist ein Fehlerbündel der Länge  $b = 5$ .

**Prop.** Sei  $g(x)$  wie oben und  $n \geq 3$ . Dann erkennt  $C_g$  *Einzelfehler* und Fehlerbündel der Länge  $b$ , falls  $b \leq n - k < n$ , d. h. ist  $v$  ein solches Fehlerbündel, so gilt  $v \notin C_g$ .

*Bem.* Diese Eigenschaft ist nützlich bei Transportmedien, bei denen sich Fehler lokal häufen z. B. bei CDs durch Kratzer.

**Bspe.** Folgende CRC-Codes mit  $q = 2$  sind standardisiert:

Name	$g(x)$	$\min\{\ell \mid g(x) \mid (x^\ell - 1)\}$
CRC-12	$x^{12} + x^4 + x^3 + x^2 + x + 1$	$n = 511 = 2^9 - 1$
CRC-16	$x^{16} + x^{15} + x^2 + 1$	$n = 32767 = 2^{15} - 1$
CRC-16'	$x^{16} + x^{12} + x^5 + 1$	$n = 32767 = 2^{15} - 1$



## Nullstellen von zyklischen Codes

**Ziel.** Ein zyklischer Code  $C \subseteq \mathbb{F}_q^n$  ist gegeben durch sein Generatorpolynom  $g(x) \in \mathbb{F}_q[x]$  mit  $g(x)|(x^n - 1)$ . Dieses  $g(x)$  können wir als Produkt einer Auswahl von irred. Faktoren von  $x^n - 1$  schreiben. Wir können also die zyklischen Codes  $C \subseteq \mathbb{F}_q^n$  studieren, indem wir die irreduziblen Faktoren von  $x^n - 1$  herausfinden.

*Bem.* Sei  $n = p^s \cdot \ell$ , wobei  $\ell$  nicht durch  $p$  teilbar ist.

$$x^n - 1 = (x^\ell - 1)^{p^s}.$$

Die irreduziblen Faktoren von  $(x^n - 1)$  sind also die gleichen wie von  $(x^\ell - 1)$ , jeweils mit  $p^s$ -facher Vielfachheit.

**Voraussetzung.** Wir können daher im Folgenden annehmen, dass  $n$  nicht durch  $q$  teilbar ist.

*Bem.* Wegen  $\text{ggT}(x^n - 1, nx^{n-1}) = 1$  treten die irreduziblen Faktoren von  $(x^n - 1)$  in einfacher Vielfachheit auf.

**Def.** Die **Ordnung von  $q$  modulo  $n$**  ist

$$m := \text{ord}_q(n) := \min \{ \ell \geq 1 \mid q^\ell \equiv 1 \pmod{n} \}.$$

*Bem.* Betrachte die Erweiterung  $\mathbb{F}_{q^m} \supseteq \mathbb{F}_q$ . Die Einheitengruppe  $(\mathbb{F}_{q^m}^\times, \cdot, 1)$  ist zyklisch, also isomorph zu  $(\mathbb{Z}/q^m - 1, +, 0)$ .

Für  $d|n$  gibt es wegen  $d|(q^m - 1)$  genau eine Untergruppe  $Z_d \subset \mathbb{F}_{q^m}^\times$  mit  $d$  Elementen, nämlich

$$Z_d = \{ \alpha \in \mathbb{F}_{q^m}^\times \mid \alpha^d = 1 \} = \{ \alpha \in \mathbb{F}_{q^m}^\times \mid \text{ord}(\alpha) \mid d \}.$$

**Def.** Die Elemente  $\alpha \in Z_d$  heißen  **$d$ -te Einheitswurzeln**.

*Bem.* Da jedes  $\alpha \in Z_n$  eine Wurzel von  $(x^n - 1)$  ist, gilt

$$x^n - 1 = \prod_{\alpha \in Z_n} (x - \alpha)$$

Es ist  $\mathbb{F}_{q^m}$  sogar der kleinste Erweiterungskörper von  $\mathbb{F}_q$ , in dem  $(x^n - 1)$  in Linearfaktoren zerfällt. Man nennt ihn deshalb *Zerfällungskörper* von  $(x^n - 1)$  über  $\mathbb{F}_q$ . Wir müssen jetzt also noch die Teilmengen  $J \subset Z_n$  mit  $\prod_{\alpha \in J} (x - \alpha) \in \mathbb{F}_q[x]$  bestimmen.

**Def.** Eine **primitive  $d$ -te Einheitswurzel** ist ein Erzeuger von  $Z_d$ , also ein Element von  $\Gamma_d := \{ \alpha \in \mathbb{F}_{q^m}^\times \mid \text{ord}(\alpha) = d \}$ .

*Bem.* Sei  $\zeta$  eine primitive  $n$ -te Einheitswurzel. Für jeden Teiler  $d$  von  $n$  ist dann  $\zeta^{n/d}$  eine primitive  $d$ -te Einheitswurzel. Es gilt

$$Z_n = \bigsqcup_{d|n} \Gamma_d \quad \text{und} \quad |\Gamma_d| = \phi(n) := |\{ 1 \leq \ell \leq n \mid \text{ggT}(n, \ell) = 1 \}|.$$

**Def.** Gelte  $d|n$ . Das  **$d$ -te Kreisteilungspolynom** ist

$$\Phi_d(x) := \prod_{\alpha \in \Gamma_d} (x - \alpha).$$

**Lem.** Es gilt sogar  $\Phi_d(x) \in \mathbb{F}_q[x]$ .

**Kor.**  $x^n - 1 = \prod_{d|n} \Phi_d(x)$

*Bem.* Es bleibt zu untersuchen, wie  $\Phi_d(x)$  über  $\mathbb{F}_q$  zerfällt.

**Def.** Sei  $\xi$  eine primitive  $d$ -te Einheitswurzel.

Die zu  $\xi^i$  gehörende **Kreisteilungsklasse** ist

$$\Gamma_{d,i} := \Gamma_{d,i}^{(\xi)} := \{ \xi^{iq^\ell} \mid \ell \geq 1 \} \subseteq \Gamma_d.$$

*Bem.* Für versch. Wahlen  $\xi$  und  $\xi'$ , bzw.  $i$  und  $i'$  sind  $\Gamma_{d,i}^{(\xi)}$  und  $\Gamma_{d,i'}^{(\xi')}$  entweder gleich oder disjunkt. Die Kreisteilungsklassen sind daher wohldefiniert. Es gilt  $|\Gamma_{d,i}| = \text{ord}_d(q)$ . Es zerfällt  $\Gamma_d$  in  $\phi(d)/\text{ord}_d(q)$  Kreisteilungsklassen. Sei nun  $\xi$  fest gewählt.

**Lem.**  $\mu_i^{(d)}(x) := \prod_{\alpha \in \Gamma_{d,i}} (x - \alpha)$  ist ein irreduzibles Polynom in  $\mathbb{F}_q[x]$

**Kor.** Sei  $K_d$  ein Repräsentantensystem von Kreisteilungsklassen, also  $\Gamma_d = \bigsqcup_{i \in K_d} \Gamma_{d,i}$ . Dann ist  $\Phi_d(x) = \prod_{i \in K_d} \mu_i^{(d)}(x)$ .

**Fazit.** Sei  $n = \ell p^s$  mit  $\text{ggT}(p, \ell) = 1$ . Die Zerlegung von  $x^n - 1$  in irreduzible Faktoren über  $\mathbb{F}_q$  ist dann

$$x^n - 1 = \prod_{d|\ell} \prod_{i \in K_d} \left( \mu_i^{(d)}(x) \right)^{p^s}.$$

**Bsp.** Sei  $q = 2$  und  $n = 2^m - 1$  mit  $m \geq 2$ . Dann ist  $\text{ord}_n(2) = m$ . Sei  $\zeta \in \mathbb{F}_{2^m}$  eine primitive  $n$ -te Einheitswurzel und  $g(x)$  das Minimalpolynom von  $\zeta$ . Betrachte den zyklischen Code  $C_g$ . Man kann zeigen, dass das Minimalgewicht  $\geq 3$  ist. Wegen der Kugelpackungsschranke gilt Gleichheit. Der Code  $C_g$  besitzt die gleichen Parameter wie der Hamming-Code  $\text{Ham}_2(m)$ .

**TODO:** Sind diese Codes äquivalent?

## BCH-Codes

Sei  $\mathcal{N} \subseteq Z_n \leftrightarrow N \subseteq Z_n$  ( $N = \{ i \mid \zeta^i \in \mathcal{N} \}$ )

Zu  $N \subseteq Z_n$  sei  $g_N(x) := \text{kgV} \{ \mu_i(x) \mid i \in SN \}$ . Es sei  $C := C(g_N) = C(N) = C(\mathcal{N})$  der von  $g_N$  erzeugte zyklische Code.

Für  $c(x) \in \mathbb{F}_q[x] \leq n - 1$  gilt dann:  $c(x) \in Ca \iff c(\zeta^i) = 0$  für alle  $i \in N$ .

**Def.**  $b \in \{ 0, \dots, n - 1 \}$  und  $\delta \in \mathbb{N}$  mit  $2 \leq \delta \leq n$ .

$L := \{ i \bmod n \mid b \leq i \leq b + \delta - 2 \}$  ein zyklisches Intervall. Dann heißt  $C(L)$  ein BCH-Code mit designedem Abstand  $\delta$ . Speziell:  $b = 1$  (im engeren Sinne),  $n = q^m - 1$  (primitiver BCH-Code)

**Satz.**  $L$ , etc. wie in (12.1).  $C = C(g_L) = C(L)$  Dann:

- $d :=$  Minimalgewicht von  $C \geq \delta$
- $k := \dim(C) \geq n - m \cdot (\delta - 1)$

**TODO:** Beispiele

**TODO:** Beispiel 12.5

**Def.** Sei  $\mathcal{N} \subseteq \mathbb{F}_{q^m}^*$  nichtleer. Ein Mengensystem  $U(\mathcal{N}) \subset \mathcal{P}(\mathcal{N})$  heißt **unabhängig**, falls gilt:

- $\emptyset \in U(\mathcal{N})$
- $A \in U(\mathcal{N}), A \subseteq \mathcal{N}, \beta \in \mathcal{N} \setminus \mathcal{N} \implies A \cup \{ \beta \} \in U(\mathcal{N})$
- $A \in U(\mathcal{N}), \gamma \in \mathbb{F}_{q^m}^* \implies \gamma A \in U(\mathcal{N})$

**Prop.** Sei  $f(x) \in \mathbb{F}_q[x]$ ,  $f \neq 0$ ,  $\mathcal{N}$  sei die Nullstellenmenge von  $f$  innerhalb  $\mathbb{F}_{q^m}^*$  und  $U(\mathcal{N})$  sei ein unabhängiges Mengensystem. Dann gilt  $\text{wt}(f) \geq \max \{ |A| \mid A \in U(\mathcal{N}) \}$ .

**TODO:** Beispiel

**Satz.** Sei  $q = 2$ ,  $\delta = 2\epsilon + 1$ ,  $L = \{ i \bmod n \mid 1 \leq i \leq \delta - 1 \}$  und  $C = C(L)$  der zugehörige BCH-Code. Dann gilt  $\dim(C) \geq n - m \cdot \epsilon$ .