Zusammenfassung Codierungstheorie

(cc) (BY) Tim Baumann, http://timbaumann.info/uni-spicker

Diese Zusammenfassung basiert auf der Vorlesung von Prof. Dr. Dirk Hachenberger an der Universität Augsburg im WS 15/16.

§1. Grundproblemstellung

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

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

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

§2. Formalisierung der Grundbegriffe

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

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 $c = (c_1, \ldots, c_n) \in C$ heißt ein **Codewort**. Falls $M = |C|$, so nennt man C einen **(n, M)-Code** über Q.

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

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

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

Das Decodierprinzip des nächsten Nachbarn

Notation. Es sei $C \subseteq Q^n$ ein Code. Wenn $y \in Q^n$ 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

$$N_C(y) := \{\overline{c} \mid d(y, C) = d(y, \overline{c})\}.$$

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 $\mathbb{P}(\alpha \text{ empfangen} \mid \alpha \text{ gesendet}) = 1 - p$.
- Ein Kanal heißt **gedächtnislos**, falls für alle $y \in Q^n$ gilt:
$$\mathbb{P}(y \text{ empfangen} \mid c \text{ gesendet}) = \prod_{i=1}^{n} \mathbb{P}(y_i \text{ empfangen} \mid c_i \text{ gesendet})$$

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

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

Shannons Hauptsatz der Kanalcodierung

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 $R \leq R(C_n) < \kappa(q, p)$
- $\lim_{n \to \infty} (\mathbb{P}_{\text{err}}(C_n)) = 0$

§3. 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 $u \in Q^n$, $\ell \in \mathbb{N}$ sei $B_\ell(u) := \{x \in Q^n \mid d(x, u) \leq \ell\}$.

Def.
- Ein Code C heißt **ℓ-fehlerkorrigierend**, falls $B_\ell(c) \cap B_\ell(c') = \emptyset$ 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-fehlerkorr./-erkennend für $m := \ell$ aber nicht $m := \ell + 1$ 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 $M = A_q(n, d)$.

Die Singleton-Schranke

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

Letztere Aussage bekommt man durch *Punktieren*, d. h. Streichen einer Koordinate von Q^n.

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

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

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

Abelsche Gruppen als Alphabete

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

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

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

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, $\lambda_1, \ldots, \lambda_{n-1} \in R$ Einheiten und $\lambda_n := -1$. Wir betrachten die Kontrollgleichung

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

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

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

Bspe.
- Für $q = 2, R = \mathbb{Z}_2, \lambda_1 = \ldots = \lambda_{n-1} = 1$ heißt $C := \ker(\kappa)$ **Parity-Check-Erweiterung**.
- Beim ISBN-Code ist $R = \mathbb{Z}_{11}$, $\lambda_1 = 1, \ldots, \lambda_9 = 9$, also $\kappa(z) = \sum_{i=1}^{10} i z_i$.

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

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 γ auf $\{1, \ldots, n\}$ und Permutationen $\sigma_1, \ldots, \sigma_n$ auf Q, sodass

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

den Code C auf C' abbildet.

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

Die Kugelpackungsschranke

Lem. Sei Q ein Alphabet, $u \in Q^n$. Dann gilt
$$|B_\ell(u)| = \sum_{j=0}^{\ell} \binom{n}{j}(|Q|-1)^j.$$

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-närer (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 $A_2(7,3) \leq 16$.

§4. Grundlagen zu linearen Codes

Bem. Zu jeder Primzahlpotenz $q = p^m \geq 2$ gibt es bis auf Isomorphie genau einen Körper $\mathbb{GF}_q = \mathbb{F}_q$ 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 $g(x) \in \mathbb{Z}_p[x]$ 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 $\min\{\mathrm{wt}(c) \,|\, c \in C, c \neq 0\}$.

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:
$$\left\{\begin{matrix} 000000, 100101, 010110, 001111, \\ 110011, 101010, 011001, 111100 \end{matrix}\right\} = \mathrm{span}\{100101, 010110, 001111\}$$

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

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

Lem. • $A_q^{\mathrm{lin}}(n,1) = q^n = A_q(n,1)$ • $A_q^{\mathrm{lin}}(n,n) = q = A_q(n,n)$
- $d \leq d' \implies A_q^{\mathrm{lin}}(n,d) \geq A_q^{\mathrm{lin}}(n,d')$
- Für $n \geq 2$, $d \geq 2$ ist $A_q^{\mathrm{lin}}(n,d) \leq A_q^{\mathrm{lin}}(n-1,d-1)$.

Da die Parity-Check-Erw. durch eine lin. Abb. geschieht, gilt:

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

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

Die Generatormatrix

Def. Sei C ein $[n,k]$-Code über $\mathbb{F}_q$, d. h. es gibt eine injektive Codierabbildung $E : \mathbb{F}_q^k \to \mathbb{F}_q^n$ mit $\mathrm{im}(E) = C$. Dann heißt für jede Basis $g^1, \ldots, g^k \in C$ von C die Matrix
$$G := \begin{pmatrix} g^1 \\ \vdots \\ g^k \end{pmatrix} \in \mathbb{F}_q^{k \times n} \qquad \text{eine **Generatormatrix** von } C.$$

Bem. Dann ist folgende Abbildung eine Codierabbildung:
$$E : \mathbb{F}_q^k \to C, \quad u \mapsto uG = \textstyle\sum_{j=1}^k u_j g^j \in C.$$

Def. Zwei $[n,k]$-Codes $C, C' \subseteq \mathbb{F}_q^n$ heißen **linear äquivalent**, falls es $\gamma \in S_n$ und $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_q^\times$ gibt, sodass die monomiale Transf.
$$\alpha : \mathbb{F}_q^n \to \mathbb{F}_q^n, \ (x_1, \ldots, x_n) \mapsto (\lambda_1 x_{\gamma(1)}, \ldots, \lambda_n x_{\gamma(n)})$$
den Code C in C' überführt.

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

Gewichtsminimale Repräsentanten

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 $x \in \mathbb{F}_q^n$ gehörende Kongruenzklasse modulo C ist $x + C$.

Def. Ein Repräsentantensystem $\mathcal{R}$ dieser Klassen heißt **gewichtsminimal**, falls $\mathrm{wt}(r) = \min_{c \in C} \mathrm{wt}(r+c)$ 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 $D : \mathbb{F}_q^n \to C$, $y \mapsto y - \mathcal{R}(y)$ eine Decodierabbildung.

Verfahren (**Standard-Array-Decodierung**)**.** Speichere die Werte der Funktion $y \mapsto \mathcal{R}(y)$ in einer Lookup-Tabelle.
Dann müssen wir zum Decodieren von y nur noch in dieser Tabelle den Wert von $\mathcal{R}(y)$ nachschlagen und $c := y - \mathcal{R}(y)$ berechnen.

Dualer Code: Kontrollmatrix, Syndromdecod.

Bem. Sei $\mathbb{F}$ ein Körper, $n \in \mathbb{N}^*$. Das Standard-Skalarprodukt
$$\langle -,- \rangle : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}, \ (x,y) \mapsto \textstyle\sum_{i=1}^n x_i y_i$$
ist eine nicht-ausgeartete, symmetrische Bilinearform.

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

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

Lem. $\forall\, x \in \mathbb{F}_q^n \ : x \in C \iff Hx^T = 0$

Algorithmus (**Syndromdecodierung**)**.**
Sei C ein $[n,k]$-Code, $H \in \mathbb{F}_q^{n-k \times n}$ die Kontrollmatrix. Dann ist
$$\psi_H : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k}, \ x \mapsto Hx^T$$
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** $s := \psi_H(y) = Hc^T + He^T = He^T \in \mathbb{F}_q^{n-k}$ berechnen.
- Wahrscheinlich ist e ein gewichtsminimaler Repräsentant von y. Sei also $\mathcal{R}$ ein minimales Repräsentantensystem.
Dann ist $\psi := \psi_H|_{\mathcal{R}} : \mathcal{R} \to \mathbb{F}_q^{n-k}$ 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:
$$\begin{aligned} d &= 1 + \max\{a \in \mathbb{N} \,|\, \text{je } a \text{ Spalten von } H \text{ sind linear unabhängig}\} \\ &= \min\{m \in \mathbb{N} \,|\, \text{es gibt } m \text{ linear abhängige Spalten in } H\} \end{aligned}$$

Def. Sei C ein linearer Code der Länge n über $\mathbb{F}_q$.
Die **Gewichtsverteilung von C** ist $A = A_C \in \mathbb{N}^{\{0,1,\ldots,n\}}$ mit
$$A(i) := |\{w \in C \,|\, \mathrm{wt}(w) = i\}|, \quad 0 \leq i \leq n.$$

Bem. Es gilt $A_0 = 1$ und $A_1 = A_2 = \ldots = A_{d-1} = 0$ für $d = d(C)$.

Def. $A_C(Z) := \sum_{i=0}^k A_i Z^k \in \mathbb{C}[Z]$ heißt **Gewichtszählpolynom**,
$$A_C^{\mathrm{hom}}(X,Y) := \textstyle\sum_{i=0}^n A_i X^{n-i} \cdot Y^i \in \mathbb{C}[X,Y]$$
heißt **homogenes Gewichtszählpolynom**.

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

§5. 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-närer 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
$$A_q^{\mathrm{lin}}\left(\tfrac{q^m-1}{q-1}, 3\right) = A_q\left(\tfrac{q^m-1}{q-1}, 3\right) = q^{q^0+\ldots+q^{m-1}-m} \quad \forall m \geq 2, m \in \mathbb{N}$$

Der binäre lineare Hamming-Code

Konstr. Ein **bin. Hamming-Code** $\mathrm{Ham}_2(m)$ (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 $\mathbb{F}_2^m \setminus \{0\}$ in genau einer Spalte stehen hat.

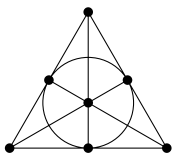
Algorithmus (Decodierung von binären Hamming-Codes)**.** Angenommen, die Spalten der Kontrollmatrix H codieren die Zahlen $1, \ldots, 2^m - 1$ im Binärsystem und sind geordnet. Sei $y \in \mathbb{F}_2^n$ empfangen worden. Falls $Hy = 0$, so wurde wsl. y gesendet. Falls das Syndrom Hy ungleich null ist, 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 $A \in \mathbb{N}^{0,1,\ldots,\mathbb{N}}$ die Gewichtsverteilung des $[n, n-m, 3]$-Hamming-Codes. Dann gilt $A_{n-j} = A_j$ für alle $j = 0, 1, \ldots, 2^{m-1} - 1$.

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

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

Bem. Sei $C = \mathrm{Ham}_2(3)$, $C_3 := \{c \in C \mid \mathrm{wt}(c) = 3\}$. Für $c \in C_3$ seien $P(c) := \{i = 1, \ldots, 7 \mid c_i = 1\}$ 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:



~~Die Heiligtümer des Todes~~

Fano-Ebene

$S_1(2, 3, 7)$-Blockplan

Steinersystem

Projektive Ebene $PG(2, \mathbb{F}_2)$

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 $X^8 + 14X^4Y^4 + Y^8$.

q-näre lineare Hamming-Codes

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

$$u \sim v \quad :\Longleftrightarrow \; \exists\, \lambda \in \mathbb{F}_q^\times \; : \; u = \lambda v.$$

Wir setzen $\mathbb{P} := PG(m-1, \mathbb{F}_q) := A/{\sim}$. Es gilt $|\mathbb{P}| = {}^{q^m-1}/_{q-1} = n$. Sei $v_1, \ldots, v_n$ 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-nären Hamming-Code** $\mathrm{Ham}_q(n)$.

Bem. Wir wählen das Representantensystem wie folgt:

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

also so, dass der erste Eintrag $\neq 0$ jedes Vektors eine 1 ist.

Algorithmus (Decodieren des q-nären 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, $s \neq 0$. 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 $D(y) := y - s_i \cdot e_\ell$.

Die Familie der Simplex-Codes

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

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

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

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

Gewichtsverteilung der binären Hamming-Codes

Wir betrachten den binären Hamming-Code $C = \mathrm{Ham}_2(m) \subset \mathbb{F}_2^n$ mit $n = 2^m - 1$.

Lem. Für $2 \leq \ell \leq n$ gilt die Rekursionsgleichung

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

Satz. Das Gewichtszählpolynom von C ist

$$A_C(z) = \tfrac{1}{n+1}(1+z)^n + \tfrac{n}{n+1}(1+z)^{(n-1)/2} \cdot (1-z)^{(n+1)/2}.$$

§6. Golay-Codes und ihre Erweiterungen

Ziel. Konstruktion des binären Golay-Codes $\mathcal{G}(23)$ und seiner Erweiterung $\mathcal{G}(24)$ und des ternären Golay-Codes $\mathcal{G}(11)$ und seiner Erweiterung $\mathcal{G}(12)$. Diese vier Codes sind optimal, $\mathcal{G}(23)$ und $\mathcal{G}(11)$ sogar perfekt.

Existenz perfekter Codes

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

Bem. Es sei $d \geq 5$ (d. h. wir schließen z. B. die Hamming-Codes aus), q eine Primzahlpotenz. Durch Computer-Suche kann man zeigen: Für $n \leq 1000$, $\log_q(M) \leq 1000$ und $q \leq 1000$ könnte es nur perfekte lineare 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.

Beweisidee. Angenommen, C wäre ein solcher Code. Man zeigt, dass es für jedes $w \in \mathbb{F}_2^{90}$ mit $\mathrm{wt}(w) = 3$ genau ein $\varphi(w) \in C$ mit $\mathrm{supp}(w) \subset \mathrm{supp}(\varphi(w))$ und $\mathrm{wt}(\varphi(w)) = 5$ gibt. Somit ist die Abbildung $\varphi : X \to Y$ mit

$$X := \{w \in \mathbb{F}_2^{90} \mid \mathrm{wt}(w) = 3 \text{ und } w_1 = w_2 = 1\},$$
$$Y := \{c \in C \mid \mathrm{wt}(c) = 6 \text{ und } c_1 = c_2 = 1\}$$

surjektiv. Die Fasern $\varphi^{-1}(c)$ haben je drei Elemente. Wegen $\frac{|X|}{|\varphi^{-1}(c)|} = \frac{88}{3} \notin \mathbb{N}$ folgt der Widerspruch. □

Bem. Tietäväinen sowie Zinov'ev und Leont'ev konnten zeigen, dass jeder q-näre t-fehlerkorrigierende perfekte Code mit Primzahlpotenz $q \geq 2$ und $t \geq 2$ entweder ein binärer $(23, 2^{12}, 7)$-Code oder ein ternärer $(11, 3^6, 5)$-Code ist.

Mit einer Methode aus ihrem Beweis lässt sich ein alternativer Beweis des letzten Satzes führen:

Satz. Sei q eine Primzahlpotenz, C ein perfekter q-närer $(n, M, 2t+1)$-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 $\{1, \ldots, n\}$.

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.

Selbstduale Codes

Def. Ein Code C heißt **selbstdual**, falls $C = C^\perp$.

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

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

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

Der binäre Golay-Code und seine Erweiterung

Konstr. Sei C_1 der $[7, 4, 3]$-Hamming-Code und $\overline{C}_1$ dessen Parity-Check-Erweiterung. Die Generatormatrizen dieser Codes sind

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \quad \text{bzw.} \quad \overline{G}_1 = \left(\begin{array}{c|c} & 1 \\ G_1 & 1 \\ & 1 \\ & 1 \end{array}\right).$$

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 $\overline{C}_2$ ein selbstdualer $[8, 4, 4]$-Code.

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 Γ ein selbst-dualer binärer $[24, 12, 8]$-Code.

Def. Γ 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 man zum Decodieren ausnutzen kann.

Der ternäre Golay-Code und seine Erweiterung

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 Ω 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 $\mathcal{G}(12)$.

§7. 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. $pIB \;:\Longleftrightarrow\; (p, B) \in I$

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

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

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

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

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

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. Sei $\mathcal{D}$ ein lin. Raum. Dann gilt entweder $b = 1$ oder $b \geq v$.

Bsp. Die Inzidenzstruktur

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

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 π.

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 $n = p_1^{a_1} \cdot \ldots \cdot p_l^{a_l}$ 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 Ordung n.

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

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

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 λ Blöcke aus $\mathcal{B}$ mit $T \subseteq \sigma(B)$.

Dann heißt $\mathcal{D}$ ein **t-(v, k, λ)-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 $\mathcal{B} := \{B \subseteq V \mid |B| = k\}$. 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 $\lambda_s = \dfrac{\lambda \cdot \binom{v-s}{t-s}}{\binom{k-s}{t-s}}$.

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

$$V := \{1, \dots, n\}, \quad \mathcal{B} := \{\mathrm{supp}(c) \mid c \in C \text{ mit } \mathrm{wt}(c) = d\}.$$

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 $S_1(2, 3, 2^m - 1)$-Steinersystem.

- $\mathcal{G}(23)$ 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:

$$\mathcal{B} = \{\operatorname{supp}(\overline{c}) \mid \overline{c} \in \overline{C}, \operatorname{wt}(\overline{c}) = d+1\}, \quad V = \{1, \ldots, n+1\}$$

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.

$$V = \{1, \ldots, 12\}, \quad \mathcal{B} = \{\operatorname{supp}(c) \mid c \in \mathcal{G}(12), \operatorname{wt}(c) = 6\}$$

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.

$$L \text{ ist parallel zu } K \quad :\iff \quad L \parallel K \quad :\iff \quad (L = K) \vee (L \cap K = \emptyset)$$

eine Äquivalenzrelation auf $\mathcal{H}$. Dann ist

$$(V, \mathcal{G}, \in) \text{ mit } V := W \amalg (\mathcal{H}/\|), \quad \mathcal{G} := \{K \amalg \{[K]\} \mid K \in \mathcal{H}\} \amalg \{\mathcal{H}/\|\}$$

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

$$\mathcal{D}' := (V', \mathcal{B}', \in), \text{ wobei } V' := V \backslash \{x\}, \quad \mathcal{B}' := \{B \backslash \{x\} \mid B \in \mathcal{B}, x \in B\}$$

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,λ)-Blockplan mit $v > k$ gilt $b \geq v$. Falls $v = b > k$, so ist die Inzidenzmatrix invertierbar.

Def. Ein 2-(v,k,λ)-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,λ)-Blockplan. Dann gilt $r = k$ und je zwei verschiedene Blöcke haben genau λ 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,λ)-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 ein Korollar hiervon.

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

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

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

§8. Reed-Muller-Codes

Die Plotkin-Schranke

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

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

Die Algebra der Booleschen Funktionen

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. $\Gamma : \mathbb{F}_2[x_1, \ldots, x_m] \to \mathcal{B}_m, \quad f(x) \mapsto (\overline{f} : v \mapsto f(v_1, \ldots, v_m))$

Satz. Γ ist ein surjektiver Algebra-Homomorphismus mit

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

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

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

Die binären Reed-Muller-Codes

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

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

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

Bem.
- $$\begin{array}{ccccccc} \mathcal{R}(-1,m) & \subseteq & \mathcal{R}(0,m) & \subseteq & \mathcal{R}(1,m) & \subseteq & \cdots \\ \perp & & \perp & & \perp & & \\ \mathcal{R}(m,m) & \supseteq & \mathcal{R}(m-1,m) & \supseteq & \mathcal{R}(m-2,m) & \supseteq & \cdots \end{array}$$
- $\dim \mathcal{R}(r,m) = \sum_{j=0}^{r} \binom{m}{j}$

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

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

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

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 $|A_{ij}| \le 1$ gilt $|\det(A)| \le \sqrt{n^n}$. 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. $H_2 = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ 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 $l \ge 1$ 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 $M \in \mathbb{R}^{(4l-1)\times(4l-1)}$. 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

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

- Falls $q \equiv 3 \bmod 4$: Dann definiert
$$M_{xy} := \begin{cases} \psi(x - y) & \text{falls } x \ne y \\ -1 & \text{falls } x = y \end{cases}$$
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 $q \equiv 1 \bmod 1$: 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
$$M_{xy} := \begin{cases} 1 & \text{falls } \infty \in \{x, y\} \ne \{\infty\}, \\ 0 & \text{falls } x = y = \infty, \\ \psi(x - y) & \text{sonst.} \end{cases}$$
Weiter sei $A = H_2 = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 1 & -1 \\ -1 & -1 \end{smallmatrix}\right)$.
Schließlich bestehe $H = (H_{xy})_{x,y\in\mathbb{F}'_q}$ aus den (2×2)-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 $F \in \mathbb{R}^{\mathbb{F}_2^m}$ = Abbildungen $\mathbb{F}_2^m \to \mathbb{R}$. Die **Hadamard-Transformierte** von F ist

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

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

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

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

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

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 $\gamma = \lambda_1 x_1 + \ldots + \lambda_m x_m$.
- $d(\beta, \gamma) = \frac{1}{2}(2^m - \hat{B}_\beta(\lambda))$
- $d(\beta, 1 + \gamma) = \frac{1}{2}(2^m + \hat{B}_\beta(\lambda))$

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, β empfangen. Dann gilt $d(\phi, \beta) \le t$ 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 γ 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 $H = H_2 \otimes \ldots \otimes H_2$ (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 β zu $\sum_{i=1}^m \lambda_i x_i \in o(1, m)$.
- Annahme, $\hat{B}_\beta(\lambda) < 0$. Decodiere β zu $1 + \sum_{i=1}^m \lambda_i x_i \in 1 + o(1, m)$.

§9. Die Gewichtsvert. 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 Character** 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 Charactere

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

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

ein additiver Charakter.

Für $q = p^k$, $k \geq 2$ verwenden wir die Spurabbildung $\mathrm{trace} : \mathbb{F}_q \to \mathbb{F}_p,\ x \mapsto \sum_{j=0}^{k-1} x^{p^j}$. (Dies ist eine nicht-triviale Linearform.) Dann ist

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

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

Bem. Zu jedem $y \in \mathbb{F}_q$ ist $\chi_y : \mathbb{F}_q \to \mathbb{C}^*,\ x \mapsto \exp(\dfrac{2\pi\, \mathrm{trace}(xy) i}{p})$ 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 Abbildungen von $\mathbb{F}_q^n$ nach V. Sei $\chi \hat{\mathbb{F}_q}$, $\chi \neq \chi_0$ Zu $f : \mathbb{F}_q^n \to V$ definieren wir eine **transformierte Abbildung** durch

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

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

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

Satz (Mac-Williams-Transformation). Sei $C \subseteq \mathbb{F}_q^m$ ein linearer Code. Betrachte den dualen Code $C^\perp$ zu C. Dann gilt:

$$A_{C^\perp}^{\mathrm{hom}}(X,Y) = \frac{1}{|C|} \cdot A_C^{\mathrm{hom}}(X + (q-1)Y, X - Y),$$

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

Beweisidee. Verwende den letzten Satz mit $V = \mathbb{C}[X,Y]$ und $f(v) := X^{n - \mathrm{wt}(v)} Y^{\mathrm{wt}(v)}$.

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

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

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

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

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

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

TODO: weiter?

§10. MDS-Codes

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:

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

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 $\mathrm{ggT}(r,s) = 1$. $q = \prod_{i=1}^m p_i^{a_i}$ 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 $U_I := \mathrm{span}\{e_i \mid i \in I\} \subseteq \mathbb{F}_q^n$

Def. Sei C ein lin. Code. Dann sei $\delta_C(I) := \delta(I) := \dim(C \cap U_i)$.

Prop.
- $\delta(I) = 0$ 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 $A_C(i) := A_i := |\{w \in C \mid \mathrm{wt}(w) = i\}|$
- Für $I \subseteq [n]$ sei $a_C(I) := a(I) := |\{w \in C \mid \mathrm{supp}(w) = I\}|$

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

Satz. Sei C ein $[n,k,d]$-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 $\mathrm{ord}\,\beta = q - 1$. Solche β heißen **primitive Elemente**.

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

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

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

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

Satz. Der konstruierte Reed-Solomon-Code ist ein linearer $[n, \ell, n - \ell + 1]$-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

§11. Zyklische Codes

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

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

Bem. Als Koordinaten verwenden wir $\{0, \ldots, n-1\} \cong \mathbb{Z}_n$.
Der **Shift-Operator** ist $S : \mathbb{F}_q^n \to \mathbb{F}_q^n,\ e^i \mapsto e^{i+1 \pmod n}$.
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

$$\mathbb{F}_q^n \to \mathbb{F}_q[x]_{<n},\ \ v \mapsto v(x) := v_0 + v_1 x + \ldots + v_{n-1}x^{n-1}.$$

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

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

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

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

Prop. Sei $h(x) = h_0 + h_1 x + \ldots + h_k x^k$. Dann ist die Kontrollmatrix von C

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

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

$$f^{\mathrm{rez}}(x) = f(\tfrac{1}{x}) \cdot x^d = f_0 x^d + f_1 x^{d-1} + \ldots + f_{n-1}x + f_n.$$

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

$$h^*(x) := \tfrac{1}{h_0} \cdot h^{\mathrm{rez}}(x), \qquad g^*(x) := \tfrac{1}{g_0} \cdot g^{\mathrm{rez}}(x).$$

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

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

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

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

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

$\hat{C}_g$ 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 ≥ 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

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

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 $\mathbb{F}_q^k \hat{=} \mathbb{F}_q[x]_{<k}$.

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

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

- Decodierung und Fehlererkennung:
  Angenommen, $y(x) = y_0 + y_1 x + \ldots + y_{n-1}x^{n-1} \in \mathbb{F}_q[x]_{<n}$ wurde empfangen. Gilt $g(x) | y(x)$, also $y(x) \in C$, so wurde wahrscheinlich auch $y(x)$ gesendet. Die zugehörige Nachricht ist

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

Def. Sei $2 \leq b \leq n$. Eine Teilmenge $I \subseteq \mathbb{Z}_n$ heißt ein **zyklisches Intervall der Länge b**, falls ein $\ell \in \mathbb{Z}_n$ existiert mit

$$I = [\ell, \ell + b - 1]_{\bmod n} := \{\ell + j \bmod n \mid 0 \leq j \leq b - 1\}.$$

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 $v_\ell \neq 0$, $v_{\ell+b-1 \pmod n} \neq 0$ und $\mathrm{supp}(v) \subseteq I$.

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 ℓ 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 p teilbar ist.

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

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

$$m := \mathrm{ord}_n(q) := \min\{\ell \geq 1 \,|\, q^\ell \equiv 1 \pmod n\}.$$

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

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

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 Einheitwurzel** ist ein Erzeuger von Z_d, also ein Element von $\Gamma_d := \{\alpha \in \mathbb{F}_{q^m}^\times \mid \mathrm{ord}(\alpha) = d\}$.

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

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

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 ζ eine primitive d-te Einheitswurzel.
Die zu ζ^i gehörende **Kreisteilungsklasse** ist

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

Bem. Für versch. Wahlen ζ und ζ', bzw. i und i' sind $\Gamma_{d,i}^{(\zeta)}$ und $\Gamma_{d,i'}^{(\zeta')}$ entweder gleich oder disjunkt. Die Kreisteilungsklassen sind daher wohldefiniert. Es gilt $|\Gamma_{d,i}| = \mathrm{ord}_d(q)$. Es zerfällt Γ_d in $\phi(d)/\mathrm{ord}_d(q)$ Kreisteilungsklassen. Sei nun ζ 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 $\mathrm{ggT}(p, \ell) = 1$. 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 $\mathrm{ord}_n(2) = m$. Sei $\zeta \in \mathbb{F}_{2^m}$ eine primitive n-te Einheitswurzel und $g(x)$ das Minimalpolynom von ζ. Betrachte den zyklischen Code C_g. Man kann zeigen, dass das Minimalgewicht ≥ 3 ist. Wegen der Kugelpackungsschranke gilt Gleichheit. Der Code C_g besitzt die gleichen Parameter wie der Hamming-Code $\mathrm{Ham}_2(m)$.

TODO: Sind diese Codes äquivalent?

§12. BCH-Codes

Situation. Sei $\mathbb{F}_q$ der endliche Körper mit q Elementen. Gelte $\mathrm{ggT}(q, n) = 1$ und $m := \mathrm{ord}_n(q)$. Dann ist $\mathbb{F}_{q^m}$ der Zerfällungskörper von $x^n - 1$. Sei $\zeta \in \mathbb{F}_{q^m}$ eine primitive n-te Einheitswurzel und $Z_n = \{\zeta^0, \ldots, \zeta^{n-1}\}$ die Menge aller n-ten Einheitswurzeln.

Konstr. Sei $\mathcal{N} \subseteq Z_n$ eine Teilmenge. Wir setzen

$$N(\mathcal{N}) := \{i = 0, \ldots, n-1 \,|\, \zeta^i \in \mathcal{N}\} \subset \mathbb{Z}_n,$$
$$g_N(x) := \mathrm{kgV}\{\mu_i(x) \,|\, i \in N\},$$

wobei $\mu_i(x)$ das Minimalpolynom von ζ^i sei. Zuletzt sei $C(\mathcal{N}) := C(g_N)$ der von g_N erzeugte zyklische Code.

Bem. $C(\mathcal{N})$ ist der kleinste Code, der die Elemente von $\mathcal{N}$ als Nullstellen besitzt. Für ein Wort $c(x) \in \mathbb{F}_q[x]_{< n}$ gilt dann:

$$c(x) \in C(\mathcal{N}) \iff c(\zeta^i) = 0 \quad \text{für alle } i \in N.$$

Def (**B**ose, Ray-**C**haudhuri, **H**ocquenghem)**.**
Sei $b \in \{0, \ldots, n-1\}$ und $\delta \in \mathbb{N}$ mit $2 \leq \delta \leq n$. Setze

$$L := [b, b + \delta - 2] := \{i \bmod n \,|\, b \leq i \leq b + \delta - 2\}.$$

Dann heißt $C(L)$ ein **BCH-Code** mit **designiertem Abstand** δ.
Für $b = 1$ heißt $C(L)$ ein BCH-Code *im engeren Sinne.*
Falls $n = q^m - 1$, so ist ζ ein primitives Element in $\mathbb{F}_{q^m}$ und $C(L)$ heißt ein **primitiver BCH-Code**.

Satz (BCH-Schranke)**.** Für den Minimalabstand d und die Dimension k von $C(L)$ gilt: $\quad d \geq \delta, \quad k \geq n - m \cdot (\delta - 1).$

Satz. Sei $q = 2$, $\delta = 2\epsilon + 1$ und $L = [1, \delta - 1]_{\bmod n}$.
Dann gilt $\dim(C(L)) \geq n - m \cdot \epsilon$.

Bsp. Die Nullstellenmenge des ternären Golay-Code $\mathcal{G}(11)$ ist $\{\zeta, \zeta^3, \zeta^5, \zeta^9\}$. Dies ist ein BCH-Code mit $b = 3$ und $\delta = 4$.
Die Parity-Check-Erweiterung von $\mathcal{G}(11)$ hat damit Minimalgewicht mindestens 4, also 6 wegen Selbstdualität.
Für den Minimalabstand d von $C(L)$ gilt daher $d \geq 5$.
Aus der Kugelpackungsschranke folgt Gleichheit.

Die Methode von Lint und Wilson

Def. Sei $\mathcal{N} \subseteq \mathbb{F}_{q^m}^*$ nichtleer. Das bzgl. $\mathcal{N}$ **unabhängige Mengensystem** $U(\mathcal{N})$ ist rekursiv definiert durch

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

Prop (Lint, Wilson)**.** Sei $f(x) \in \mathbb{F}_q[x]$, $f \neq 0$, und $\mathcal{N}$ die Nullstellenmenge von f innerhalb $\mathbb{F}_{q^m}^*$. Dann gilt

$$\mathrm{wt}(f) \geq \max\{|A| \,|\, A \in U(\mathcal{N})\}.$$

Bem. Die BCH-Schranke ist ein Korollar hiervon.

Bsp. Der binäre Golay-Code $\mathcal{G}(23)$ ist der von

$$g(x) \coloneqq x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$$

erzeugte Code. Die zugehörige Nullstellenmenge ist

$$\{\zeta^i \mid i \in \Gamma_1\} \quad \text{mit} \quad \Gamma_1 \coloneqq \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}.$$

Sei $c(x) \in \mathcal{G}(23)$ und $\mathcal{N}$ dessen Nullstellenmenge. Es sei $c(x)$ kein Vielfaches von $\Phi_{23}(x)$ und damit $\Gamma_1 \subseteq \mathcal{N} \cap Z_n \subseteq \Gamma_1 \cup \{1\}$. Man schließt nun, dass folg. Teilmengen von $\mathbb{F}_{2048}$ in $U(\mathcal{N})$ liegen:

$$\emptyset \xrightarrow{c} \{\zeta^5\} \xrightarrow{b} \{\zeta^4\} \xrightarrow{c} \{\zeta^4, \zeta^5\} \xrightarrow{b} \{\zeta, \zeta^2\} \xrightarrow{c} \{\zeta, \zeta^2, \zeta^5\} \xrightarrow{b} \{\zeta^8, \zeta^9, \zeta^{12}\}$$
$$\xrightarrow{c} \{\zeta^8, \zeta^9, \zeta^{12}, \zeta^{14}\} \xrightarrow{b} \{\zeta^{12}, \zeta^{13}, \zeta^{16}, \zeta^{18}\} \xrightarrow{c} \{\zeta^5, \zeta^{12}, \zeta^{13}, \zeta^{16}, \zeta^{18}\}$$
$$\xrightarrow{b} \{\zeta^{18}, \zeta^2, \zeta^3, \zeta^6, \zeta^8\} \xrightarrow{c} \{\zeta^2, \zeta^3, \zeta^5, \zeta^6, \zeta^8, \zeta^{18}\} \xrightarrow{b} \{1, \zeta^1, \zeta^3, \zeta^4, \zeta^6, \zeta^{16}\}$$

Aus der Prop folgt, dass $c(x)$ Gewicht ≥ 6 hat.

- Falls $c(1) = \mathrm{wt}(c) = 0$, so ist $\{1, \zeta^1, \zeta^3, \zeta^4, \zeta^6, \zeta^{16}\} \in \mathcal{N}$ und somit $\{1, \zeta^1, \zeta^3, \zeta^5, \zeta^4, \zeta^6, \zeta^{16}\} \in U(\mathcal{N})$. Mit der Prop folgt, dass $c(x)$ Gewicht ≥ 7 hat.
- Falls $c(1) = \mathrm{wt}(c) = 1 \bmod 2$, so hat $c(x)$ ungerades Gewicht, also Gewicht ≥ 7.

Somit hat $\mathcal{G}(23)$ das Minimalgewicht ≥ 7.
Aus der Kugelpackungsschranke folgt Gleichheit.

TODO: Beispiel

Konstr (von MDS-Codes). Angenommen, $n | q - 1$. Dann ist $m = \mathrm{ord}_n(q) = 1$ und $x^n - 1$ zerfällt über $\mathbb{F}_q$ in Linearfaktoren.
Sei ζ eine prim. n-te Einheitswurzel, $b \geq 1$ und $2 \leq \delta \leq n$. Dann ist

$$g(x) \coloneqq (x - \zeta^b) \cdot (x - \zeta^{b+1}) \cdot \ldots \cdot (x - \zeta^{b+\delta-2})$$

das kleinste mon. Polynom aus $\mathbb{F}_q[x]$ mit $\mathcal{N} = \{\zeta^b, \ldots, \zeta^{b+\delta-2}\}$ als Nullstellen. Für BCH-Code $C = C(\mathcal{N}) = C_g$ gilt

$$\mathrm{wt}(g) \leq \deg(g) + 1 = \delta \leq d(C) \leq \mathrm{wt}(g),$$

also $d(C) = \delta$. Es handelt sich darum um einen MDS-Code, da

$$\dim(C) = n - \deg(g) = n - (\delta - 1) = n - d + 1.$$

Def. Im Falle $n = q - 1$ spricht man hier auch von einem **Reed-Solomon-Code**.

Einiges zu binären BCH-Codes

Sei $q = 2$ und C ein binärer BCH-Code im engeren Sinne. Gelte $n = 2^m - 1$. Sei $\zeta \in \mathbb{F}_{2^m}$ eine primitive n-te Einheitswurzel.

Satz. C hat ungerades Minimalgewicht.

Zusammen mit der Kugelpackungsschranke folgt:

Prop. Hat C den designierten Abstand $\delta = 2\epsilon + 1$ und gilt $2^{m\epsilon} < \sum_{i=0}^{\epsilon+1} \binom{n}{i}$, so hat C das Minimalgewicht δ.

Satz. Gelte $m \geq 4$. Der designierte Abstand von C sei $\delta = 5$. Dann:
- $d = d(C) = 5$
- $k = \dim(C) = 2^m - 1 - 2m$

Bem. Der Code C mit $\delta = 5$ wird von $g(x) = \mu_1(x)\mu_3(x)$ erzeugt.

Def. Sei C ein q-närer Code der Länge n. Dann heißt

$$\rho(C) \coloneqq \max\{r \geq 0 \mid \forall c, c' \in C : B_r(c) \cap B_r(c') = \emptyset\} \quad \textbf{Packungsradius}$$
$$\sigma(C) \coloneqq \min\{s \geq 0 \mid \mathbb{F}_q^n = \bigcup_{c \in C} B_s(c)\} \geq \rho(C) \quad \textbf{Überdeckungsradius}$$

Bem. $\rho(C) = \sigma(C) \iff C$ ist ein perfekter Code

Def. Codes mit $\rho + 1 = \sigma$ heißen **quasi-perfekt**.

Bsp. Man kann zeigen: Binäre, primitive BCH-Codes im engeren Sinne mit $\delta = 5$ sind quasi-perfekt.

Prop. Sei C ein primitiver BCH-Code im engeren Sinne der Länge $n = q^m - 1$ und designiertem Abstand δ über $\mathbb{F}_q$. Falls $\delta | n$, so ist δ das Minimalgewicht von C.

TODO: Wo ist der folgende Satz im Skript?

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 $\dim(C) \geq n - m \cdot \epsilon$.

Decodierung von BCH-Codes

Satz. Sei $m \geq 4$ und C der binäre, primitive BCH-Code im engeren Sinne mit Minimalabstand $d = 5$, d. h. C hat $\zeta, \zeta^2, \zeta^3, \zeta^4$ als Nullstellen für ein prim. Element $\zeta \in \mathbb{F}_{2^m}$. Angenommen, $c(x)$ wurde gesendet und $u(x) = c(x) + e(x)$ empfangen, wobei für das Fehlerpolynom $\mathrm{wt}(e(x)) \leq 2$ gilt. Setze $s_1 \coloneqq u(\zeta)$ und $s_3 \coloneqq u(\zeta^3)$. Dann gilt:
- Falls $s_1 = 0$, so ist $e(x) = 0$.
- Falls $s_3 = s_1^3 \neq 0$, so ist $e(x) = x^\ell$, wobei $s_1 = \zeta^\ell$.
- Falls $s_1 \neq 0$ und $s_1^3 \neq s_3$, so gilt $e(x) = x^i + x^j$, wobei ζ^{-i} u. ζ^{-j} die Nullstellen von $L(z) = 1 - s_1 z + (\frac{s_3}{s_1} - s_1^2) z^2 \in \mathbb{F}_{2^m}[z]$ sind.

Situation. Sei C ein BHC-Code im engeren Sinne mit designiertem Abstand δ. Wir nehmen an, dass $c(x) \in C$ gesendet und $u(x) = c(x) + e(x) \in \mathbb{F}_q[x]_{<n}$ empfangen wurde. Dabei habe das Fehlerpolynom $e(x)$ das Gewicht $w \coloneqq \mathrm{wt}(e(x)) \leq \tau \coloneqq \lfloor \frac{\delta-1}{2} \rfloor$.
Die Fehlerstellen seien $1 \leq \varphi(1) < \ldots < \varphi(w) \leq n$, also

$$e(x) = \sum_{i=1}^{w} e_{\varphi(i)} x^{\varphi(i)} \quad \text{mit} \quad e_{\varphi(i)} \in \mathbb{F}_q^*.$$

Ziel. Bestimmung 1 der Anzahl w von Fehlern, 2 der Fehlerpositionen $\varphi(i)$ und 3 der nötigen Korrekturen $e_{\varphi(i)}$ gegeben $u(x)$.

Notation.
- $X_i \coloneqq \zeta^{\varphi(i)}$, $Y_i \coloneqq e_{\varphi(i)}$ für $1 \leq i \leq w$,
- $X_j \coloneqq Y_j \coloneqq 0$ für $w < j \leq \tau$,
- $s_k \coloneqq u(\zeta^k)$ für $1 \leq k \leq \delta - 1$ (*Syndrom*)

Bem. Die X_i's codieren 2, die Y_i's 3. Für $1 \leq j \leq \delta - 1$ gilt

$$s_j = u(\zeta^j) = e(\zeta^j) = \sum_{i=1}^{w} e_{\varphi(i)} \zeta^{j\varphi(i)} = \sum_{i=1}^{w} Y_i X_i^j = \sum_{i=1}^{\tau} Y_i X_i^j$$

Satz. Für $\ell \in \mathbb{N}$ mit $w \leq \ell \leq \tau$ sei

$$M_\ell \coloneqq \begin{pmatrix} s_1 & s_2 & \cdots & s_\ell \\ s_2 & s_3 & \cdots & s_{\ell+1} \\ \vdots & \vdots & \ddots & \vdots \\ s_\ell & s_{\ell+1} & \cdots & s_{2\ell-1} \end{pmatrix}.$$

Dann gilt:
- M_w ist invertierbar
- $M_{w+1}, \ldots, M_\tau$ sind nicht invertierbar (falls $w < \tau$)

Kor. $w = \max\{\ell \leq \tau \mid \det(M_\ell) \neq 0\}$ (Lsg von 1)

Def. Das **Lokatorpolynom** ist

$$L(z) \coloneqq (1 - X_1 z) \cdot \ldots \cdot (1 - X_w z) \in \mathbb{F}_{q^m}[z].$$

Bem. Die Nullstellen von $L(z)$ sind $\zeta^{-\varphi(1)}, \ldots, \zeta^{-\varphi(w)}$. Es gilt

$$L(z) = \sum_{i=0}^{w} (-1)^i \cdot p_i \cdot z^i \quad \text{wobei} \quad p_i \coloneqq \sum_{I \subseteq [w],\ |I| = i} X_I, \quad X_I \coloneqq \prod_{j \in I} X_j$$

Satz. Die eindeutige Lösung des linearen Gleichungssystems

$$M_w \cdot x = -\begin{pmatrix} s_{w+1} \\ s_{w+2} \\ \vdots \\ s_{2w-1} \\ s_{2w} \end{pmatrix} \quad \text{ist} \quad P \coloneqq \begin{pmatrix} (-1)^w p_w \\ (-1)^{w-1} p_{w-1} \\ \vdots \\ p_2 \\ -p_1 \end{pmatrix}.$$

Folgerung. Die elementarsymm. Fktn $p_0, \dots, p_w$ in $X_1, \dots, X_w$ kann man aus $s_1, \dots, s_{2w}$ berechnen. Gleiches gilt somit für $L(z)$. Die Exponenten in der Darstellung der Nullstellen von $L(z)$ als ζ-Potenz geben dann die Fehlerstellen an. (Lsg von 2)

Satz. Die eindeutige Lösung des linearen Gleichungssystems

$$\begin{pmatrix} X_1 & X_2 & \cdots & X_w \\ X_1^2 & X_2^2 & \cdots & X_w^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^w & X_2^w & \cdots & X_w^w \end{pmatrix} \cdot z = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_w \end{pmatrix} \qquad \text{ist} \qquad z = \begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_w \end{pmatrix}$$

Folgerung. Da sich, wie schon gesehen, die Werte X_i aus den Syndromen s_k berechnen lassen, liefert dies eine Methode, die Werte Y_i aus den Syndromen zu berechnen. (Lsg von 3)

Ein weiteres Decodierverfahren

Ziel. Entwicklung eines effizienteren Decodierverfahrens für die gleiche Situation wie im letzten Abschnitt.

Def. Das **Fehlerauswertungspolynom** ist

$$F(z) := \sum_{i=1}^{w} Y_i X_i \cdot \prod_{\ell=1, \ell \neq i} (1 - X_\ell \cdot z) \in \mathbb{F}_{q^m}[z].$$

Satz. Sei $L'(z)$ die formale Ableitung des Lokatorpolynoms. Dann:

$$Y_k = -\frac{F(X_k^{-1})}{L'(X_k^{-1})} \qquad \text{für alle } k = 1, \dots, w.$$

Def. Das **Syndrompolynom** ist

$$S(z) := \sum_{j=1}^{\delta-1} s_j z^{j-1} \in \mathbb{F}_{q^m}[z].$$

Prop. $F(z) = S(z) \cdot L(z) \pmod{z^{\delta-1}}$

Bem. In anderen Worten: Es gibt ein Polynom $v(z) \in \mathbb{F}_{q^m}[z]$ mit

$$v(z) \cdot z^{\delta-1} + L(z) \cdot S(z) = F(z).$$

Der erweiterte euklidische Algorithmus berechnet eine *Bézout-Darstellung* des ggT, d. h. Polynome $a(z), b(z) \in \mathbb{F}_{q^m}[z]$ mit

$$a(z) \cdot z^{\delta-1} + b(z) \cdot S(z) = \mathrm{ggT}(z^{\delta-1}, S(z)).$$

Algorithmus. Wir initialisieren dazu

$$\begin{pmatrix} r_{-1}(z) \\ r_0(z) \end{pmatrix} := \begin{pmatrix} z^{\delta-1} \\ S(z) \end{pmatrix} \quad \text{sowie} \quad \begin{pmatrix} a_{-1}(z) & b_{-1}(z) \\ a_0(z) & b_0(z) \end{pmatrix} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Solange $r_k(z) \neq 0$ ist, führen wir eine Division von $r_{k-1}(z)$ durch $r_k(z)$ mit Rest durch und erhalten $q_{k+1}(z), r_{k+1}(z) \in \mathbb{F}_{q^m}[z]$ mit

$$r_{k-1}(z) = q_{k+1}(z) \cdot r_k(z) + r_{k+1}(z) \quad \text{und} \quad \deg(r_{k+1}(z)) < \deg(r_k(z)).$$

Wir setzen

$$a_{k+1}(z) := a_{k-1}(z) - q_{k+1}(z) \cdot a_k(z),$$
$$b_{k+1}(z) := b_{k-1}(z) - q_{k+1}(z) \cdot b_k(z).$$

Man prüft leicht nach, dass bei dieser Update-Regel die Invariante

$$a_k(z) \cdot z^{\delta-1} + b_k(z) \cdot S(z) = r_k(z)$$

erhalten bleibt. Sei m maximal unter $r_m(z) \neq 0$. Dann ist

$$a_m(z) \cdot z^{\delta-1} + b_m(z) \cdot S(z) = r_m(z) = \mathrm{ggT}(z^{\delta-1}, S(z))$$

die gesuchte Bézout-Darstellung des ggT.

Satz. Sei ℓ minimal unter $\deg(r_\ell(z)) < {}^{(\delta-1)}/_2$. Dann gilt:

- $L(z) = b_\ell(0)^{-1} \cdot b_\ell(z)$
- $F(z) = b_\ell(0)^{-1} \cdot r_\ell(z)$

Folgerung. Man kann aus den Syndromen das Lokatorpolynom $L(z)$ mit hilfe des erweiterten euklidischen Algorithmus berechnen. Dieses enthält alle Informationen über 1 und 2. Mit dem letzten Satz aus dem letzen Abschnitt kann man 3 bestimmen.

Satz (**Newton-Identitäten**)**.** Sei $\mathbb{K}$ ein Körper und $x_1, \dots, x_t$ sowie z Variablen. Für $k \in \mathbb{N}$ sei $\sigma_k := x_1^k + \dots + x_t^k$ (insb. $\sigma_0 = t$). Wir betrachten

$$S(z) := \sum_{k=0}^{\infty} \sigma_k z^k \qquad \in \mathbb{K}[x_1, \dots, x_t][\![z]\!] \subseteq \mathbb{K}(x_1, \dots, x_t)[\![z]\!],$$

$$L(z) := \prod_{j=1}^{t} (1 - x_j z) \in \mathbb{K}[x_1, \dots, x_t][z] \subseteq \mathbb{K}(x_1, \dots, x_t)[\![z]\!].$$

Dann ist $L(z) \cdot S(z)$ ein Polynom mit Grad $\leq t-1$. Genauer gilt

$$L(z) \cdot S(z) = \sum_{r=0}^{t-1} (-1)^r \cdot p_r \cdot (t-r) \cdot z^r,$$

wobei $p_0, \dots, p_t$ die elementarsymm. Fktn in $x_1, \dots, x_t$ sind.