Zusammenfassung zu Codierungstheorie

Sara Adams

5. Juli 2005

Diese Zusammenfassung basiert auf der Vorlesung
Codierungstheorie
gehalten im Sommersemester 2005
von Prof. Dr. Hans-Dietrich Gronau
an der Universität Rostock

Inhaltsverzeichnis

1 Grundlagen **2**
1.1 Motivation . . . 2
1.2 Grundbegriffe und erste Definitionen . . . 2

2 Quellencodierung **3**
2.1 Präfix-Codes . . . 3
2.2 Statistische Codes . . . 3
2.3 Entropie und Codierungsaufwand . . . 4

3 Fehler-erkennende Codes **5**
3.1 Fehlertypen . . . 5
3.2 Prüfzeichen-Codierung . . . 5

4 Fehler-korrigierende Codes **6**
4.1 Einführung . . . 6
4.2 Schranken . . . 6
4.3 Hadamard-Matrizen . . . 7
4.4 Lineare Codes . . . 8
4.5 Zyklische Codes . . . 9

5 Perfekte binäre Codes **12**

1 Grundlagen

1.1 Motivation

Bei der Übertragen von Nachrichten benötigen wir eine Darstellungsform für die enthaltenen Informationen, eine sogenannte *Codierung*. Des weiteren können auf dem Übermittlungsweg Störungen zu Verfälschungen führen. Es ist daher erstrebenswert einen Code zu entwickeln, der Fehler erkennen und korrigieren kann.

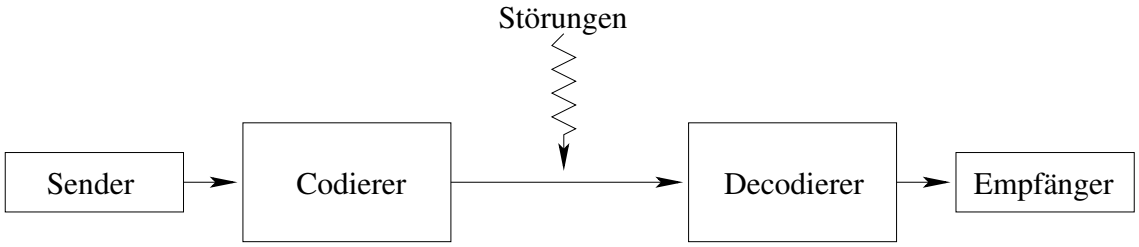

Abbildung 1: Einfaches Schema von Nachrichtenübertragungen

1.2 Grundbegriffe und erste Definitionen

1. Bezeichnung: $[n] := \{i \in \mathbb{N} : \ i \leq n\}$
2. Ein *Alphabet* $\mathcal{A}$ ist eine endliche Menge von Zeichen.
3. Ein *Wort* ω über einem Alphabet $\mathcal{A}$ ist eine endliche Folge $\omega = (a_1, \ldots, a_n) \in \mathcal{A}^n$ von Zeichen aus $\mathcal{A}$. Die Länge $|\omega| = n$ beschreibt die Anzahl der Zeichen in ω.
4. Die*Menge aller Wörter* über dem Alphabet $\mathcal{A}$ wird mit $\mathcal{A}^* := \{\omega \in \mathcal{A}^n : \ n \in \mathbb{N}_0\}$ bezeichnet.
5. Ein *Code* C ist eine Menge von Codewörtern $C \subseteq \mathcal{A}^*$.
6. Ein *Blockcode* ist ein Code $C \subseteq \mathcal{A}^n$, das heißt alle Wörter haben die Länge n.
7. Ein *DMC (discrete memoryless channel)* ist ein Tripel (X, Y, P), wobie X und Y endliche Mengen sind und P eine Matrix der Übertragunswahrscheinlichkeiten:
$$P = (p_{x,y})_{x \in X, y \in Y}), \ p_{x,y} = P(y|x) \geq 0, \ \sum_{x \in X} P(y|x) = \sum_{y \in Y} P(y|x) = 1$$
8. Ein *BSC (binary symmetric channel)* ist ein DMC (X, Y, P) mit
$$X = Y = \{0, 1\} \text{ und } P = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}, \quad p \in [1, 0.5]$$
9. Ein *qSC (q-ary symmetric channel)* ist ein DMC (X, Y, P) mit
$$X = Y = \mathbb{F}_q \text{ und } P = (p_{i,j})_{i,j \in [q]}, \ p_{i,j} = \begin{cases} 1-p & i = j \\ \frac{p}{q-1} & i \neq j \end{cases}, \quad p \in [0, 0.5]$$

10. Sei C ein Blockcode, der auf einem DMC benutzt wird. Wenn die Nachricht y empfangen wurde, so wählt man beim Decodieren eine der folgenden Wörter:

    - ein Wort x, für das $P(x|y)$ am größten ist (*MED (minimum error probability decoding)*
    - ein Wort x, für das $P(y|x)$ am größten ist (*MLD (maximum likelihood decoding)*

    Bemerkung: Wird jedes Wort mit der gleichen Wahrscheinlichkeit übertragen, so liefern beide Decodierungen das gleiche Wort.

11. Sei C ein Blockcode, bei dem k die Länge des zu sendenden Wortes und n die Länge des codierten Wortes ist. Dann ist die *Informationsrate* R des (n, k)-Blockcodes definiert durch $R := \frac{k}{n}$.

2 Quellencodierung

2.1 Präfix-Codes

Definition Ein *Präfix-Code* ist eine Menge von Codewörtern, bei denen kein Codewort Anfang eines anderen Codeworts ist.
Bemerkung Präfix-Codes sind eindeutig decodierbar.

Satz (Kraftsche Ungleichung)
Seien $m_i \in \mathbb{N}, i \in [n]$ gegeben. Genau dann existiert ein binärer Wurzelbaum mit n Blättern, deren Abstände von der Wurzel m_i sind, wenn

$$\sum_{i=1}^{n} \frac{1}{2^{m_i}} \geq 1.$$

Gleichheit tritt genau für reguläre binäre Wurzelbäume ein.
Bemerkung Ein Wurzelbaum ist ein Baum, bei dem ein Knoten als Wurzel festgelegt ist. Ein regulärer binärer Wurzelbaum ist ein binärer Wurzelbaum, bei dem alle inneren Knoten genau zwei Kinder haben.

Satz Jeder binäre Präfix-Code C mit $|C| = n$ und Wörtern der Länge $m_i, i \in [n]$ erfüllt $\sum_{i=1}^{n} \sum \frac{1}{2^{m_i}} = 1$. Ebenso lässt sich aus jeder Menge $\{m_i \in \mathbb{N} : \ i \in [n]\}$ mit $\sum_{i=1}^{n} \frac{1}{2^{m_i}} = 1$ ein Präfix-Code C mit $|C| = n$ und Wörtern der Länge $m_i, i \in [n]$ konstruieren.

2.2 Statistische Codes

Definition Sei ein DMC (X, Y, P) mit $|X| = n$ und eine Wahrscheinlichkeitsverteilung $p = (p_1, \ldots, p_n)$ auf den Zeichen von X gegeben. Dann heißt $\overline{l} := \sum_{i=1}^{n} l_i p_i$ die *durschnittliche Codewortlänge*.

Bei der statistischen Codierung möchte man die durchschnittliche Länge der Codewörter minimieren. Gegeben eine Wahrscheinlichkeitsverteilung codiert man also häufig zu erwartende Symbole mit möglichst wenigen Zeichen.

Bei der *Huffmann-Codierung* wird die durchschnittliche Codewortlänge unter einer gewissen Wahrscheinlichkeitsverteilung minimiert.

Konstruktion eines binären Huffmann-Codierung:
Es werden jeweils die beiden Elemente mit der kleinsten Wahrscheinlichkeit zusammengefasst, wobei daraus ein neues Element entsteht, das die Summe der beiden Ausgangselemente besitzt. Dieser Vorgang wird solange fortgesetzt, bis nur noch zwei Elemente vorliegen. Das erste der beiden erhält die Codierung 0, das zweite die Codierung 1. Dieser Vorgang wird sukzessive fortgesetzt, bis alle Zeichen eine eindeutige Codierung zugewiesen bekommen haben.

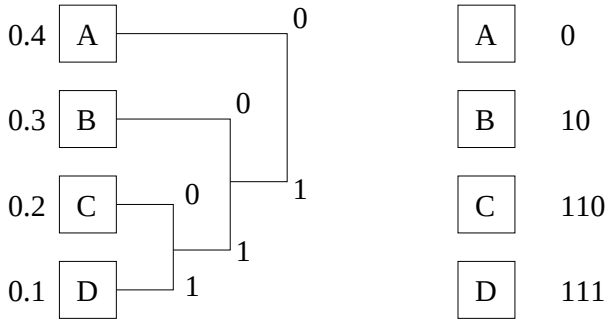

Abbildung 2: Beispiel einer binären Huffmann-Codierung mit $\overline{l} = 1.9$

2.3 Entropie und Codierungsaufwand

Definition Sei ein DMC (X, Y, P) mit $|X| = n$ und eine Wahrscheinlichkeitsverteilung $p = (p_1, \ldots, p_n)$ auf den Zeichen von X gegeben. Dann heißt

$$H(X) := \sum_{i=1}^{n} p_i \log_2 \frac{1}{p_i}$$

die *Entropie* von X.

Satz Sei X eine Datenquelle mit Wahrscheinlichkeitsverteilung p auf den Zeichen von X. Dann gilt: $H(X) \leq \overline{l}_{opt}(X) < H(X) + 1$

Lemma

$$H(Q_1 \times Q_2) = H(Q_1) + H(Q_2), \quad H(Q^k) = k \cdot H(Q)$$

Satz (Fundamentalsatz der Quellencodierung)
Bei jeder diskreten Quelle Q ohne Gedächtnis ist der mittlere Codierungsaufwand durch $H(Q)$ (mittels eines Präfixcodes für Wörter der Länge k) beschränkt. Bei genügend großer Codewortlänge k lässt sich diese Schranke beliebig annähern.

Definition Es sei $H(X|Y) := \sum_{i,j} P(x_i|y_i) \log_2 \frac{1}{p(x_i|y_i)}$ die *bedingte Entropie* und $T(X) := H(X) - H(X|Y)$ die *Transinformation*. Dann heißt $c := \max_X T(X)$ die *Kapazität*.

Satz (channel coding theorem von Shannon)
Gegeben sei ein DMC (X, Y, P) mit Kapazität c. Für jede Rate $R < c$ und für jedes $\varepsilon > 0$ gibt es eine $n \in \mathbb{N}$ und einen Code $C = \{c_i : \ i \in [M]\}$ aus Worten der Länge n mit folgender Eigenschaft:

- $M \geq 2^{\lceil Rn \rceil}$
- $p_e(i) < \epsilon \ i \in [n]$, wobei $p_E(i)$ die Wahrscheinlichkeit bezeichnet, dass das gesendete Wort c_i falsch decodiert wird.

3 Fehler-erkennende Codes

3.1 Fehlertypen

Verhoeff hat 1969 eine Zusammenstellung von möglichen Fehlern und deren Häufigkeit des Auftretens untersucht. Dabei ergaben sich die in Tabelle 1 angegebenen Daten.

Typ	Beispiel			%
Einzelfehler	a	$\rightarrow$	b	79.0
Nachbar-Transpositionen	ab	$\rightarrow$	ba	10.2
Sprung-Transpositionen	acb	$\rightarrow$	bca	0.8
Zwillingsfehler	aa	$\rightarrow$	bb	0.6
phonetische Fehler	13	$\rightarrow$	31	0.5
Sprungzwillinge	aca	$\rightarrow$	bcb	0.3
Übrige Fehler				8.6

Tabelle 1: Fehlertypen und deren Häufigkeit nach Verhoeff

3.2 Prüfzeichen-Codierung

Bei der Prüfzeichen-Codierung soll durch eine Prüfziffer eine Fehlererkennung ermöglicht werden. Dabei ist es erstrebenswert insbesondere Einzelfehlern und Nachbar-Transpositionen zu erkennen (siehe Tabelle 1).

Definition Sei $\mathcal{A}$ ein Alphabet und $G = (\mathcal{A}, \circ)$ eine Gruppe über $\mathcal{A}$. Eine *Prüfzeichen-Codierung* über G besteht aus n Permutationen $\pi_i,\ i \in [n]$ sowie einem Element $c \in \mathcal{A}$. Dabei wird ein Wort $a_1 a_2 \dots a_{n-1}$ um ein Prüfzeichen a_n erweitert, so dass die Prüfgleichung

$$\pi_1(a_1) \circ \pi_2(a_2) \circ \dots \circ \pi_n(a_n) = c$$

erfüllt ist.

Lemma
Für gegebene $a_i,\ i \in [n-1]$ ist a_n durch die Prüfgleichung eindeutig bestimmt.
Prüfzeichen-Codierungen erkennen alle Einzelfehler.
Falls G abelsch ist, so werden Nachbar-Transpositionen genau dann erkannt, wenn

$$x\pi_{i+1}\pi_i^{-1}(y) \neq y\pi_{i+1}\pi_i^{-1}(x)\ \forall x \neq y \in G, i \in [n-1].$$

Satz Sei G eine abelsche Gruppe. Genau dann existiert eine Prüfzeichen-Codierung über G, die jede Nachbar-Transposition erkennt, wenn es ein Permuation δ gibt, für die $x \mapsto x\delta(x)$ wieder eine Permuation ist (d.h. G besitzt einen Orthomorphismus).

Satz Sei G eine endliche, abelsche Gruppe der Ordnung m. Genau dann besitzt G einen Orthomorphismus, wenn m ungerade ist oder G mindestens zwei verschiedene Involutionen $(g \in G :\ g^2 = 1 \neq g)$ enthält.

4 Fehler-korrigierende Codes

4.1 Einführung

Definition Es sei $\mathcal{A}$ eine endliche Menge. Der *Hamming-Abstand* auf $\mathcal{A}^n$ ist definiert durch

$$d(\underline{a}, \underline{b}) := |\{i : \ a_i \neq b_j, i \in [n]\}|.$$

Bemerkung Der Hamming-Abstand d ist eine Metrik.

Definition Es sei $\mathcal{A}$ eine endliche Menge mit $q = |\mathcal{A}|$. Dann ist ein $(n, M, d; q)$-Code C auf $\mathcal{A}$ eine M-elementige Menge $C \subseteq \mathcal{A}^n$, für die gilt:

$$d(x, y) \geq d \forall x, y \in C, x \neq y, \quad \exists \, x_0, y_0 \in C : \ d(x_0, y_0) = d$$

Dabei heißt d der *Minimalabstand* von C.

Definition Ein $(n, M, d; q)$-Code mit $d = 2e + 1$ heißt *e-Fehler-korrigierend.*

Definition $A(n, d; q) := \max\{M \in \mathbb{N} : \ \exists (n, M, d; q)\text{-Code}\}$

Lemma Sei $d \geq 2$. Dann gilt: $A(n, d; q) \leq A(n - 1, d - 1; q)$.

Lemma $q \cdot A(n - 1, d; q) \geq A(n, d; q)$

Satz Seien $C_i, i = 1, 2$ ein $(n, M_i, d_i; q)$-Code gebegeben. Dann ist der Code $C = \{(u|u + v) : u \in C_1, v \in C_2\}$ ein $(2n, M_1 \cdot M_2, d; q)$-Code mit $d = \min\{2d_1, d_2\}$.

Lemma $A(n, 2e - 1; 2) = A(n + 1, 2e; 2)$

4.2 Schranken

Satz (Singelton-Schranke)

$$A(n, d; q) \leq q^{n-d+1}$$

Definition Codes mit $M = A(n, d; q) = q^{n-d+1}$ heißen *MDS-Codes (maximum distance seperation).*

Satz (Plotkin-Schranke)
Sei $\theta = \frac{q-1}{q}$ und $d > \theta n$. Dann gilt:

$$A(n, d; q) \leq \frac{d}{d - \theta n}$$

Insbesondere ist $A(n, d; 2) \leq \frac{2d}{2d-n}$ für $n < 2d$.

Definition Codes mit Gleichheit in der Plotkin-Schranke heißen *äquidistante Codes.*

Folgerung

$$A(n, d; 2) \leq 2 \cdot \left\lfloor \frac{d}{2d - n} \right\rfloor \text{ für } n < 2d$$

Satz (Hamming-Schranke bzw. Kugelpackungs-Schranke)

$$A(n, 2e + 1; q) \leq \frac{q^n}{\sum_{i=0}^{e} \binom{n}{i} (q - 1)^i}$$

Definition Codes mit Gleichheit in der Hamming-Schranke heißen *perfekte Codes.*

Satz (Gilbert-Varshamov)

$$A(n, d; q) \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i} (q - 1)^i}$$

4.3 Hadamard-Matrizen

Definition Eine *Hadamard-Matrix* der Ordnung n ist eine $n \times n$-Matrix mit Einträgen ± 1, die die Gleichung $H \cdot H^T = n \cdot I$ erfüllt.

Bemerkung Je zwei Zeilen einer Hadamardmatrix sind orthogonal. Insbesondere gibt es keine Hadamard-Matrizen mit ungerader Ordnung $n > 2$.

Lemma Ist H eine Hadamard-Matrix der Ordnung n, so ist $n \in \{1, 2\} \cup 4\mathbb{N}$.

Lemma Es seinen H, H' Hadamard-Matrizen der Ordnung n, n'. Dann ist die $(nn' \times nn')$-Matrix $H \otimes H'$ eine Hadamard-Matrix.

Folgerung $\forall k \in \mathbb{N} \exists$ Hadamardmatrix der Ordung 2^k.

Folgerung $\exists$ Hadamardmatrix der Ordnung $n \Rightarrow \exists$ Hadamard-Matrix der Ordnung $2^k \cdot n \; \forall k \in \mathbb{N}$

Satz Die folgenden Aussagen sind äquivalent:

1. Es gibt eine Hadamard-Matrix der Ordnung $4d$.
2. $A(4d, 2d; 2) = 8d$
3. $A(4d - 1, 2d; 2) = 4d$

Lemma Die folgenen Aussagen sind äquivalent:

1. Es gibt eine Hadamardmatrix der Ordnung $4d$.
2. $A(4d - 1, 2d - 1; 2) = 8d$
3. $A(4d - 2, 2d - 1; 2) = 4d$

Ferner implizieren diese Aussagen:

1. $A(4d - 2, 2d; 2) = 2d$
2. $A(4d - 3, 2d - 1; 2) = 2d$

Definition Die Funktion $\chi : \mathbb{F}_q \to \{0, \pm 1\}$ mit

$$\chi(x) := \begin{cases} 0 & x = 0 \\ 1 & \exists y \in \mathbb{F}_q : \; y^2 = x \\ -1 & \text{sonst} \end{cases}$$

heißt der *quadratische Charakter* in $\mathbb{F}_q$.

Satz (Paley)
Es sei $q \equiv 3 \mod 4$ eine Primzahlpotenz. Wir definieren eine $(q \times q)$-Matrix Q durch $q_{i,j} = \chi(j - i)$. H entstehe aus Q durch Ersetzen der Einträge 0 durch -1 und durch Anfügen einer Zeile und einer Spalte aus 1-Einträgen. Dann ist H eine Hadamard-Matrix der Ordnung $q+1$.

Satz Es sei $q \equiv 1 \mod 4$ eine Primzahlpotenz. Dann gibt es eine Hadamard-Matrix der Ordnung $2(q + 1)$.

4.4 Lineare Codes

Definition Ein $(n, M, d; q)$-Code heißt *linear*, wenn er einen Unterraum des $\mathbb{F}_q^n$ ist. Mit $M = q^k$ wird code durch $[n, k, d; q]$ bezeichnet.

Definition Sei $x \in \mathbb{F}_q^n$. Das Gewicht $w(x) := |\{i : \ x_i \neq 0\}|$ ist die Anzahl der von 0 verschiedenen Koordinaten.

Definition Das Minimalgewicht von C ist definiert durch $\min\{w(c) : \ 0 \neq c \in C\}$

Lemma

1. $\forall x, y \in \mathbb{F}_q^n : \ d(x, y) = w(x - y)$
2. Bei einem linearen Code sind Minimalabstand und Minimalgewicht identisch.

Definition Sei C ein $[n, k, d; q]$-Code. Dann heißt der zu C orthogonale Unterraum $C^\perp$ *der zu C duale Code* mit der Dimension $n - k$.

Definition Sei C ein $[n, k, d; q]$-Code. Wenn $a_1, \ldots, a_r$ ein erzeugendes System von C bilden, so heißt die Matrix mit den Zeilen $a_1, \ldots, a_r$ eine *Generatormatrix* von C.
Eine Generatormatrix H von $C^\perp$ heißt *Kontrollmatrix* von C.

Lemma Sei H eine Kontrollmatrix des $[n, k, d; q]$-Codes C. Dann gilt für jeden Vektor $c \in \mathbb{F}_q^n$:

$$c \in C \Leftrightarrow \ H \cdot c^T = 0$$

Lemma Die $(k \times n)$-Matrix G sei eine Generatormatrix des $[n, k, d; q]$-Codes C. Dabei sei G *systematisch*, das heißt $G = (I_k|A)$ mit einer Matrix A vom Format $(k \times n - k)$. Dann ist $H = (-A^T|I_{n-k})$ eine Kontrollmatrix für C.

Satz Sei H die Kontrollmatrix eines $[n, k, d; q]$-Codes C. Dann gilt:

1. $dim(C) = k = n\text{rg}(H)$
2. $d = \min\{i : \ \exists i \text{ linear abhängige Spalten in } H\}$

Definition Die *Sylvester-Matrizen* H_q können wie folgt beschrieben werden:

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad H_{q+1} = \begin{pmatrix} H_q & H_q \\ H_q & -H_q \end{pmatrix}$$

Satz Die durch die Sylvester-Matrizen erzeugten optimal äquidistanten Codes sind linear.

Definition Der kleinste Wert n, für den es einen $[n, k, d; q]$-Code gibt, wird mit $N(k, d; q)$ bezeichnet.

Satz (Singleton)

$$C \text{ ist } [n, k, d; q]\text{-Code} \Rightarrow \ k \leq n - d + 1$$

Satz (Bilbert-Varshanov)

$$\sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k} \Rightarrow \ \exists\, [n, k, d; q]\text{-Code}$$

Lemma

$$N(k,d;q) \geq d + N(k-1, \left\lceil \frac{d}{q} \right\rceil; q)$$

Satz (Griesmer-Schranke)

$$N(k,d;q) \geq d + \sum_{i=1}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$$

Lemma Seien $C_i, i = 1,2$ ein $[n_i, k_i, d_i; q]$-Code. Dann gibt es einen $[n,k,d;q]$-Code mit $n = 2\max\{n_1, n_2\}$, $k = k_1 + k_2$, $d = \min\{2d_1, d_2\}$.

Definition Man nennt einen perfekten, linearen, 1-fehlerkorrigierenden binären Code mit Minimalabstand 3 auch $[n,k]$-*Hamming-Code*, wobei n die Länge der Codewörter angibt und k die Dimension des Codes.

Bemerkung Der Code, der durch die Kontrollmatrix

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

definiert wird, ist ein $[7,4]$-Hamming-Code.

4.5 Zyklische Codes

Definition Ein $[n,k,d;q]$-Code heißt *zyklisch*, wenn aus $(c_0, \ldots, c_n)$ stets $(c_n, c_0, \ldots, c_{n-1})$ folgt.

Satz Die zyklischen Codes der Länge n über $\mathbb{F}_q$ sind genau die Indeale in $R = \mathbb{F}_q[x]/(x^n - 1)$.

Satz Sei C ein Ideal in R. Dann gilt:

1. C ist ein Hauptideal und wird durch das eindeutig bestimmte, monische Polynom g kleinsten Grades in C erzeugt.
2. $g | (x^n - 1)$ in $\mathbb{F}_q[x]$
3. Sei $r := \deg(g) \neq 0$. Dann hat jedes $c \in C$ eine eindeutige Darstellung $c = f \cdot g$ mit $\deg(f) \leq n - r - 1$.
4. $\dim(C) = n - r$

Satz Sei $g = \sum_{i=0}^{r} g_i x^i$ Generatorpolynom von C. Dann gilt:

$$G = \begin{pmatrix} g_0 & g_1 & \ldots & g_r & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & g_{r-1} & g_r & \ldots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \ldots & g_0 & g_1 & \ldots & g_r & 0 \\ 0 & \ldots & 0 & g_0 & \ldots & g_{r-1} & g_r \end{pmatrix} = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{n-r-1}g(x) \end{pmatrix}$$

ist Generatormatrix von C. Außerdem entsprechen die zyklischen Codes der Länge n bijektiv den Teilern von $x^n - 1$ über $\mathbb{F}_q$.

Folgerung Sei g das Generatorpolynom von C und $h = \frac{x^n-1}{g}$. Dann gilt:

$$c \in C \Leftrightarrow \ h \cdot c = 0 \text{ in } R$$

Lemma Wenn $x^n - 1$ über $\mathbb{F}_q$ in genau s irreduzible Faktoren zerfällt, so ist 2^s genau die Anzahl der zyklischen Codes der Länge n über $\mathbb{F}_q$. s ist dabei grösergleich der Anzahl der Teiler von n.

Satz Sei C ein zyklischer Code mit Generatorpolynom g und Kontrollpolynom $h = \frac{x^n-1}{g}$ über $\mathbb{F}_q$. Dann ist auch $C^\perp$ zyklisch und hat das Generatorpolynom $g^\perp = \frac{x^k h(x^{-1})}{h(0)}$. $C^\perp$ ist äquivalent zu (h).

Folgerung

$$\sum_{i=0}^{k} h_i x^k | (x^n - 1) \Rightarrow \ \sum_{i=0}^{k} h_{k-i} x^i | (x^n - 1)$$

Satz Sei $ggT(n, q) = 1$ und $\mathbb{F}_{q^m}$ der Zerfällungskörper von $x^n - 1$ über $\mathbb{F}_q$. Dann ist die Menge N der n-ten Einheitswurzeln in $\mathbb{F}_{q^m}$ invariant unter der Permutation $\pi(a) = \alpha^q$.
Wenn $B_1, \ldots, B_s$ Die Bahnen von π auf N sind, so ist $g_i = \prod_{a_i \in B_i}(x - \alpha_i)$ irreduzibel. Folglich ist $x^n - 1 = \prod_{i=1}^{s} g_i$ die Primfaktorzerlegung von $x^n - 1$ über $\mathbb{F}_{\text{ıı}}$.

Definition Sei C ein zyklischer Code der Länge n über $\mathbb{F}_q$ mit Generatorpolynom $g = \prod_{i=1}^{r}(x - \alpha_i)$. Die α_i heißen *Nullstellen* von C, während die restlichen n-ten Einheitswurzeln *Nichtnullstellen* von C heißen.
Bemerkung Die Nichtnullstellen von C sind die Nullstellen des Kontrollpolynom von C.

Lemma Sei C ein zyklischer Code der Länge n über $\mathbb{F}_q$ mit Nullstellen $\alpha_i, i \in [r]$. Dann gilt:

$$C = C(a_1, \ldots, a_r) := \{c \in R : \ c(\alpha_i) = 0 \ \forall i \in [r]\}$$

Satz Sei $\frac{q^k-1}{q-1}$ und $ggT(k, q-1) = 1$. Ist α eine primitive n-te Einheitswurzel in $\mathbb{F}_q^k$, so ist der zyklische Code $C = C(\alpha)$ äquivalent zum $[n, n-k]$-Hamming-Code. Inbesondere sind die Hamming-Codes zyklisch.

Definition Sei α eine primitive n-te Einheitswurzel über $\mathbb{F}_q$ und $A = \{\alpha^{i_j} : j \in [m]\}$ eine Menge von Potenzen von α. Dann ist

$$M(A) := \begin{pmatrix} 1 & \alpha^{1i_1} & \ldots & \alpha^{(n-1)i_1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{1i_m} & \ldots & \alpha^{(n-1)i_m} \end{pmatrix}$$

Ist $A = \{\alpha^{(j-1)+i} : \ j \in [m]\}$, so heißt A *lückenlose Menge* der Länge m von n-ten Einheitswurzeln.

Lemma Sei α eine primitive n-te Einheitswurzel über $\mathbb{F}_q$ und A eine lückenlose Menge der Länge m. Dann sind je m Spalten von $M(A)$ linear unabhängig.

Satz (BCH-Schranke)
Sei C ein zyklischer Code der Länge n über $\mathbb{F}_q$ mit Generatorpolynom G. Ferner sei α eine primitive n-te Einheitswurzel über $\mathbb{F}_q$. Falls es $b \geq 0$ und $\delta \geq 2$ gibt mit

$$g(a^{b+i}) = 0 \quad \forall i \in \{j \in \mathbb{N}_0 : \ j \leq \delta - 2\},$$

so hat C Minimalgewicht $d \geq \delta$.

Definition Sei $ggT(n,q) = 1$ und α eine primitive n-te Einheitswurzel über $\mathbb{F}_q$. Dann heißt der Code $C = C(\alpha^b, \ldots, \alpha^{b+\delta-2})$ *BCH-Code*.
Im Fall $b = 1$ heißt C *BCH-Code im engeren Sinne*.
Sei $\mathbb{F}_{q^m}$ der Zerfällungskörper von $x^n - 1$ über $\mathbb{F}_q$. Im Fall $n = q^m - 1$ heißt C *primitiver BCH-Code*.

Satz Sei $\mathbb{F}_{q^m}$ der Zerfällungskörper von $x^n - 1$ über $\mathbb{F}_q$. Für jeden BCH-Code der Länge n über $\mathbb{F}_q$ zum Abstand δ gilt:

$$d \geq \delta, \quad k \geq n - m(\delta - 1)$$

Für $q = 2$ gibt es einen BCH-Code zum Abstand $\delta = 2t + 1$ mit $k \geq n - mt$.

Satz Seien α, α' zwei primitive n-te Einheitswurzeln über $\mathbb{F}_q$ und $K \subset \{i \in \mathbb{N}_0 : i \leq n-1\}$ sei unter $\pi(i) = qi \mod n$ abgeschlossen. Dann sind die folgenden zyklischen Codes äquivalent:

$$(g) = \Big(\prod_{i \in K}(x - \alpha^i)\Big) \text{ und } (g') = \Big(\prod_{i \in K}(x - \alpha'^i)\Big)$$

Lemma Sei α eine primitive n-te Einheitswurzel über $\mathbb{F}_q$ und $A = \{\alpha^{i_j} : \ j \in [k]\}$ mit $i_j < i_{j+1},\ i_k = i_1 + t - 1$. Sei J eine beliebige t-Teilmenge der Spaltenindizes von $M(A)$, so hat die zugehörige Untermatrix $M(A)_J$ den Rang k.

Satz Sei $K := \mathbb{F}_{q^k}$ der Zerfällungskörper von $x^n - 1$ über $\mathbb{F}_q$. Ferner seien A und B Mengen von n-ten Einheitswurzeln in K und C der Code der Länge n über K, der zur Kontrollmatrix $M(AB)$ gehört und $c \in C$ beliebig. Es sei $I = \mathrm{supp}(C) := \{i : \ c_i \neq 0\}$. Dann gilt:

$$\mathrm{rg}\Big(M(A)_I\Big) + \mathrm{rg}\Big(M(B)_I\Big) \leq |I|$$

Folgerung Sei C ein zyklischer Code der Länge n über $\mathbb{F}_q$. Ferner seien A und B zwei Mengen von n-ten Einheitswurzeln über $\mathbb{F}_q$. Wenn die Nullstellenmenge von C die Menge AB umfasst, so gilt:

$$\mathrm{rg}\Big(M(A)_I\Big) + \mathrm{rg}\Big(M(B)_I\Big) \leq |I|$$

für jede Menge $I \subset \{j \in \mathbb{N}_0 : \ j \leq n - 1\}$, die Träger eines Codeworts von C ist.

Definition Sei C ein Code der Länge n über $\mathbb{F}_q$. Dann ist der *erweiterte Code* C' von C definiert als

$$C' := \Big\{(c_0, \ldots, c_n) : \ (c_0, \ldots, c_{n-1}) \in C,\ \sum_{i=0}^{n} c_i = 0\Big\}$$

Satz Sei C ein primitiver BCH-Code der Länge $n = q^m - 1$ über $\mathbb{F}_q$ und α eine primitive n-te Einheitswurzel. Dann läßt der erweiterte Code C' die affine Gruppe $G = AGL(1, q^m)$ als Automorphismengruppe zu.

Lemma Sei C ein binärer Code der Länge n, in dem alle Gewichte gerade sind. Ferner sei die Gewichtsverteilung des in der i-ten Koordinate punktierten Codes unabhängig von der Auswahl von i. Wenn A_j (bzw. a_j) die Zahl der Wörter mit Gewicht j in C (bzw. C') bezeichnet, so gilt:

$$a_{2j-1} = \frac{2jA_{2j}}{n}, \quad a_{2j} = \frac{(n-2j)A_{2j}}{n}$$

Insbesondere ist das Minimalgewicht des punktierten Codes ungerade.

Satz Sei C ein binärer, primitiver BCH-Code. Dann hat C ungerades Minimalgewicht.

Satz Der binäre, primitive BCH-Code der Länge $2^m - 1$ mit $m \geq 4$ zum Abstand 5 hat Minimalgewicht $d = 5$ und Dimension $k = 2^m - 1 - 2m$.

Satz Sei C ein BCH-Code im engeren Sinne der Länge $n = ab$. Dann gilt: $\delta = a \Rightarrow\ d = \delta$

5 Perfekte binäre Codes

Definition A_k sei eine $(2^k \times 2^k)$-Matrix mit folgender Struktur: Die Zeilen und Spalten werden binär durch die Zahlen 0 bis $2^k - 1$ beschrieben. Dann gilt:

$$A_k = (a^k_{i,j}),\ a^k_{i,j} := \begin{cases} 1 & \text{falls Zeilen und Spaltennummer den Hammingabstand 1 haben} \\ 0 & \text{sonst} \end{cases}$$

Lemma Die Eigenwerte von A_k sind $-k + 2j, j \in \{i \in \mathbb{N}_0 :\ i \leq k\}$ mit Vielfachheit $\binom{k}{j}$.

Definition Die $(e + 1 \times e + 1)$-Triagonalmatrix $Q_e = Q_e(a, b)$ wird definiert durch:

$$(Q_e)_{i,j} := \begin{cases} a & j = i \\ b - i & j = i + 1 \\ i & j = i - 1 \\ 0 & \text{sonst} \end{cases}$$

Ferner sei

$$P_e = P_e(a, b) = \begin{pmatrix} & & & 1 \\ & Q_{e-1}(a,b) & & \vdots \\ & & & 1 \\ 0 & \dots & 0 & e & 1 \end{pmatrix}$$

Definition Seien $n, q \in \mathbb{N}$ fest und $q \geq 2$. Dann ist für $k \in \mathbb{N}_0$ das k-te *Krawtschuk-Polynom* definiert durch

$$K_k(x; n, q) = K_k(x) := \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j} (q-1)^{k-j}$$

Lemma

$$\sum_{i=0}^{n} K_l(i) K_i(k) = \delta_{lk} \cdot q^n$$

Lemma Sei $q = 2$. Dann gilt:

$$(k+1) \cdot K_{k+1}(x) = (n - 2x) \cdot K_k(x) - (n - k + 1) \cdot K_{k-1}(x)$$

Lemma Sei $q = 2$. Dann hat $K_k(x)$ paarweise verschiendene Nullstellen.

Lemma Sei $q = 2$ und $v_1 < \dots < v_k$ die Nullstellen von $K_k(x)$, $u_1 < \dots < u_{k-1}$ die Nullstellen von $K_{k-1}(x)$. Dann gilt:

$$0 < v_1 < u_1 < v_2 < \dots < u_{k-1} < v_k < n$$

Lemma Sei $q = 2$ und $K_k(x) = \sum_{i=0}^{k} c_i x^k$. Dann gilt:

1. $c_k = \frac{(-2)^k}{k!} \neq 0$
2. $c_{k-1} = \frac{(-1)^{k-1}2^{k-1}}{(k-1)!} \cdot n$
3. $c_{k-2} = \frac{(-1)^{k-2}2^{k-2}}{(k-2)!} \cdot \frac{3n^2-3n+2k-4}{6}$
4. $c_0 = \binom{n}{k}$

Lemma Sei $\Psi_e(x) := K_e(x-1; n-1, 2)$. Dann gilt: $|P_e(2x-n, n)| = (-1)^e e! \Psi_e(x)$

Lemma Sei A eine $(m \times m)$-Matrix der Form $A = (A_{ij})_{i,j\in[k]}$, wobei A_{ij} eine $(m_i \times m_j)$-Matrix ist und $\sum_{i=1}^{k} m_i = m$. Die Matrizen A_ij haben eine konstante Zeilensumme b_{ij}. Bezeichnen wir mit $B = (b_{ij})_{i,j\in[k]}$, so sind die Eigenwerte von B auch Eigenwerte von A.

Satz (Lloyd)
Falls ein perfekter, binärer, e-korrigierender Code der Länge n existiert, so hat $\Psi(x)$ e verschiedene Nullstellen in der Menge $[n]$.

Satz Es sei C ein perfekter, binärer e-Fehler-korrigierender Code mit $e > 1$ und $n \geq 2e + 1$. Dann ist C der Wiederholungscode ($n = 2e + 1$) oder der binäre Golay-Code, der ein $[23, 12, 7; 2]$-Code ist.