

# Codierungstheorie

Vorlesungsskript von Arne Winterhof

Dieses Skript ist die schriftliche Ausarbeitung einer Vorlesung, die ich im Wintersemester 2003/2004 an der Universität Wien und im Sommersemester 2005 an der JKU Linz gehalten habe.

Arne Winterhof

# Inhaltsverzeichnis

1	Problemstellung	1
2	Fehlererkennung, Korrektur und Decodierung	3
3	Schnellkurs über endliche Körper	7
4	Prüfziffersysteme und Orthomorphismen	14
5	Linearcodes	19
6	Schranken in der Codierungstheorie	28
7	Hadamard-Matrix Codes	33
8	Zyklische Codes	35
9	BCH-Codes	42
10	Quadratische Reste Codes	46
11	Goppa Codes	49
12	Überdeckungsradius	54

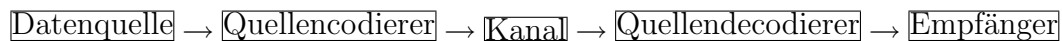
# Kapitel 1

## Problemstellung

Die Codierungstheorie beschäftigt sich mit dem Problem, wie man Informationen über einen gestörten Kanal so übertragen kann, dass auch aus einer verfälschten empfangenen Nachricht die ursprüngliche Information korrekt abgeleitet werden kann (Fehlerkorrektur). Dazu fügt man an die zu übertragende Nachricht Zusatzinformation an (Codierung), so dass, wenn nicht zu viele Fehler auftreten, aus der empfangenen Nachricht die ursprüngliche Nachricht eindeutig rekonstruiert werden kann (Decodierung).

Die Vorlesung gibt eine Einführung in die Codierungstheorie.

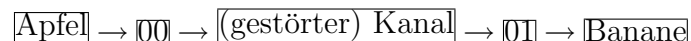
Modell der Nachrichtenübertragung:



Beispiel (fehlerhafte Nachricht):

Datenquelle: {Apfel, Banane, Kirsche, Traube}

Quellencodierung: Apfel  $\rightarrow$  00, Banane  $\rightarrow$  01, Kirsche  $\rightarrow$  10, Traube  $\rightarrow$  11

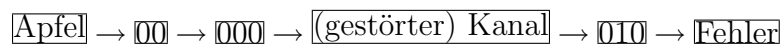


Erweitertes Modell der Datenübertragung:



Beispiel (1-Fehler entdeckend, Paritätskontrollcode):

00  $\rightarrow$  000, 01  $\rightarrow$  011, 10  $\rightarrow$  101, 11  $\rightarrow$  110



Beispiel (1-Fehler korrigierend, Wiederholungscode):

$00 \rightarrow 000000$ ,  $01 \rightarrow 010101$ ,  $10 \rightarrow 101010$ ,  $11 \rightarrow 111111$

$\boxed{\text{Apfel}} \rightarrow \boxed{00} \rightarrow \boxed{000000} \rightarrow \boxed{\text{(gestörter) Kanal}} \rightarrow \boxed{010000} \rightarrow \boxed{00} \rightarrow \boxed{\text{Apfel}}$

Ziele:

1. schnelle Codierung
2. einfache Übertragung der codierten Nachricht
3. schnelle Decodierung
4. Maximale Informationsübertragung
5. Optimale Entdeckung bzw. Korrektur von Fehlern

Aus mathematischer Sicht sind 4. und 5. vorrangige Ziele.

## Aufgabe

Gegeben sei die Nachrichtenmenge

$\{000, 100, 010, 001, 110, 101, 011, 111\}$ .

- a) Entwirf einen 1-Fehler entdeckenden Code für diese Nachrichtenmenge.
- b) Entwirf einen 1-Fehler korrigierenden Code für diese Nachrichtenmenge.

# Kapitel 2

## Fehlererkennung, Korrektur und Decodierung

### Grundbegriffe

#### Definition 1

- Wir bezeichnen eine Menge  $A = \{a_1, a_2, \dots, a_q\}$  mit  $q$  Elementen als Codealphabet. Die Elemente heißen Codesymbole.
- Ein Wort der Länge  $n$  über  $A$  ist eine Zeichenfolge  $\mathbf{w} = w_1 w_2 \dots w_n$  mit  $w_1, w_2, \dots, w_n \in A$ . Manchmal schreiben wir auch  $\mathbf{w} = (w_1, w_2, \dots, w_n)$ .
- Ein Blockcode der Länge  $n$  über  $A$  ist eine nichtleere Menge  $C$  von Wörtern der Länge  $n$  über  $A$ . Für das Alphabet  $\mathbb{F}_2 = \{0, 1\}$  nennt man  $C$  einen Binärcode.
- Ein Element von  $C$  heißt Codewort aus  $C$ .
- Die Anzahl der Codewörter in  $C$  bezeichnen wir mit  $|C|$  und nennen sie Größe von  $C$ .
- Die Informationsrate eines Codes  $C$  wird definiert als  $\frac{\log_q |C|}{n}$ .
- Ein Code der Länge  $n$  und der Größe  $M$  wird  $(n, M)$ -Code genannt.

**Definition 2** Ein Kommunikationskanal besteht aus einem Alphabet

$$A = \{a_1, a_2, \dots, a_q\}$$

und Übergangswahrscheinlichkeiten

$$\mathcal{P}(a_j | a_i) \geq 0, \quad i, j = 1, 2, \dots, q,$$

dass  $a_j$  empfangen wird, falls  $a_i$  gesendet wurde, mit der Bedingung

$$\sum_{j=1}^q \mathcal{P}(a_j | a_i) = 1, \quad i = 1, 2, \dots, q.$$

**Definition 3** Ein Kommunikationskanal heißt gedächtnislos, wenn für je zwei Wörter  $\mathbf{c} = c_1 c_2 \dots c_n$  und  $\mathbf{x} = x_1 x_2 \dots x_n$  der Länge  $n$

$$\mathcal{P}(\mathbf{x} | \mathbf{c}) = \prod_{i=1}^n \mathcal{P}(x_i | c_i).$$

**Definition 4** Ein symmetrischer Kanal ist ein gedächtnisloser Kanal mit

$$\mathcal{P}(a_i | a_i) = 1 - p, \quad i = 1, 2, \dots, q$$

und

$$\mathcal{P}(a_i | a_j) = \frac{p}{q-1}, \quad i \neq j, \quad i, j = 1, 2, \dots, q,$$

mit  $0 \leq p < 1/2$ .

Beispiel:

$A = \{0, 1\}$ ,  $C = \{000, 111\}$ ,  $p = 0,1$   
empfangenes Codewort: 110

$$\mathcal{P}(110 | 000) = \mathcal{P}(1 | 0)^2 \cdot \mathcal{P}(0 | 0) = 0,1^2 \cdot 0,9 = 0,009$$

$$\mathcal{P}(110 | 111) = \mathcal{P}(1 | 1)^2 \cdot \mathcal{P}(0 | 1) = 0,9^2 \cdot 0,1 = 0,081$$

wahrscheinlich 111 gesendet

## Maximum Likelihood Decodierung

Bei der Übermittlung eines Codewortes aus einem Code  $C$  wurde das Wort  $\mathbf{x}$  empfangen. Bei der *Maximum Likelihood Decodierung* schließt man, dass  $\mathbf{c}_{\mathbf{x}}$  das am wahrscheinlichsten gesendete Codewort ist, wenn

$$\mathcal{P}(\mathbf{x} | \mathbf{c}_{\mathbf{x}}) = \max_{\mathbf{c} \in C} \mathcal{P}(\mathbf{x} | \mathbf{c}).$$

## Hamming-Abstand

**Definition 5** Der Hammingabstand  $d(\mathbf{x}, \mathbf{y})$  zweier Wörter  $\mathbf{x} = x_1 x_2 \dots x_n, \mathbf{y} = y_1 y_2 \dots y_n \in A^n$  ist die Anzahl der Stellen  $i = 1, 2, \dots, n$  mit  $x_i \neq y_i$ .

**Hilfssatz 1** Seien  $\mathbf{x}, \mathbf{y}, \mathbf{z} \in A^n$ . Dann gilt:

1.  $0 \leq d(\mathbf{x}, \mathbf{y}) \leq n$ ,
2.  $d(\mathbf{x}, \mathbf{y}) = 0$  genau dann, wenn  $\mathbf{x} = \mathbf{y}$ ,
3.  $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$ ,
4.  $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$ .

Beweis: 1.-3. trivial.

Für 4. reicht es wegen

$$d(\mathbf{x}, \mathbf{y}) = d(x_1, y_1) + d(x_2, y_2) + \dots + d(x_n, y_n),$$

den Fall  $n = 1$  zu überprüfen:

$$x = z: d(x, z) = 0$$

$$x \neq z: \text{entweder } y \neq x \text{ oder } y \neq z$$

□

## Nearest Neighbour Decodierung

Bei der *Nearest Neighbour Decodierung* decodieren wir  $\mathbf{x}$  zu  $\mathbf{c}_x$ , falls

$$d(\mathbf{x}, \mathbf{c}_x) = \min_{\mathbf{c} \in C} d(\mathbf{x}, \mathbf{c}).$$

**Satz 1** Für einen symmetrischen Kanal stimmen Maximum Likelihood und Nearest Neighbour Decodierung überein.

Beweis: Sei  $\mathbf{x} \in A^n$  ein empfangenes Wort. Für ein Codewort  $\mathbf{c} \in C$  gilt:

$$d(\mathbf{x}, \mathbf{c}) = i \iff \mathcal{P}(\mathbf{x} | \mathbf{c}) = p^i(1-p)^{n-i}.$$

Wegen  $p < 1/2$  gilt

$$p^0(1-p)^n > p(1-p)^{n-1} > \dots > p^n(1-p)^0$$

und

$$\min_{\mathbf{c} \in C} d(\mathbf{x}, \mathbf{c}) = i \iff \max_{\mathbf{c} \in C} \mathcal{P}(\mathbf{x} | \mathbf{c}) = p^i(1-p)^{n-i},$$

woraus die Behauptung folgt.

□

Beispiel:  $C = \{000, 111\}$ , empfangenes Wort 010

1. Nearest Neighbour: 000 gesendet
2. symmetrischer Kanal  
 $\mathcal{P}(010 | 000) = (1-p)^2p > (1-p)p^2 = \mathcal{P}(010 | 111)$   
 Maximum Likelihood: 000 gesendet
3. nicht symmetrischer Kanal mit  $\mathcal{P}(0 | 0) = 0,9$ ,  $\mathcal{P}(1 | 1) = 0,6$ :  
 $\mathcal{P}(010 | 000) = 0,9^2 \cdot 0,1 = 0,081 < 0,096 = 0,4^2 \cdot 0,6 = \mathcal{P}(010 | 111)$   
 Maximum Likelihood: 111 gesendet

# Minimalabstand

**Definition 6** Für einen Code  $C$  mit mindestens zwei Codewörtern heißt

$$d(C) := \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}$$

Minimalabstand von  $C$ .

Ein Code der Länge  $n$  und Größe  $M$  mit Minimalabstand  $d$  wird als  $(n, M, d)$ -Code bezeichnet.

Ein Code  $C$  mit Minimalabstand  $d$  heißt  $(d-1)$ -Fehler entdeckend und  $\lfloor (d-1)/2 \rfloor$ -Fehler korrigierend.

## Aufgaben

1. Die Codewörter des *binären* Codes  $\{000, 100, 111\}$  werden über einen symmetrischen Kanal mit  $p = 0.03$  geschickt. Benutze Maximum Likelihood Decodierung, um die folgenden empfangenen Wörter zu decodieren:  
a) 010, b) 011, c) 001.

2. Sei  $C = \{001, 011\}$  ein Binärcode.  
a) Wir nehmen einen gedächtnislosen Kanal mit den folgenden Wahrscheinlichkeiten an:

$$\mathcal{P}(0 | 0) = 0.1 \quad \text{und} \quad \mathcal{P}(1 | 1) = 0.5.$$

Benutze Maximum Likelihood Decodierung, um das empfangene Wort 000 zu decodieren.

- b) Benutze Nearest Neighbour Decodierung, um 000 zu decodieren.

3. Benutze für den Binärcode  $\{01101, 00011, 10110, 11000\}$  Nearest Neighbour Decodierung, um die folgenden empfangenen Wörter zu decodieren:  
a) 00000, b) 01111, c) 10110.

4. Benutze für den *ternären* Code  $\{00122, 12201, 20110, 22000\}$  Nearest Neighbour Decodierung, um die folgenden empfangenen Wörter zu decodieren:  
a) 01122, b) 10021.

5. Bestimme die Anzahl der Binär-codes mit Parametern  $(n, 2, n)$  für  $n \geq 2$ .

# Kapitel 3

## Schnellkurs über endliche Körper

Ein *Körper*  $\mathbb{K}$  ist ein kommutativer Ring mit 1, in dem zu jedem  $a \in \mathbb{K} \setminus \{0\}$  ein multiplikativ Inverses  $a^{-1}$  existiert, d.h.:  $a^{-1}a = 1$ . Ein *endlicher Körper* ist ein Körper mit nur endlich vielen Elementen.

Körper sind *nullteilerfrei*, d.h.:  $ab = 0 \Rightarrow a = 0$  oder  $b = 0$ .

Die Menge  $\mathbb{Z}_m := \{0, 1, \dots, m-1\}$  ist mit den folgenden Operationen ein kommutativer Ring mit 1: Für  $a, b, c \in \mathbb{Z}_m$  sei

$$a + b = c :\Leftrightarrow m \text{ teilt } a + b - c,$$

$$a \cdot b = c :\Leftrightarrow m \text{ teilt } a \cdot b - c.$$

Beispiel:  $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$+$	$0$	$1$	$2$	$3$	$\cdot$	$0$	$1$	$2$	$3$
$0$	$0$	$1$	$2$	$3$	$0$	$0$	$0$	$0$	$0$
$1$	$1$	$2$	$3$	$0$	$1$	$0$	$1$	$2$	$3$
$2$	$2$	$3$	$0$	$1$	$2$	$0$	$2$	$0$	$2$
$3$	$3$	$0$	$1$	$2$	$3$	$0$	$3$	$2$	$1$

Wegen  $2 \cdot 2 = 0$  ist  $\mathbb{Z}_4$  kein Körper.

### Körper mit Primzahlordnung

**Satz 2**  $\mathbb{Z}_m$  ist genau dann ein Körper, wenn  $m$  eine Primzahl ist.

Beweis: Ist  $m = ab \in \mathbb{Z}$  mit  $1 < a, b < m$ , so gilt  $a \cdot b = 0 \in \mathbb{Z}_m$ . Dann ist  $\mathbb{Z}_m$  nicht nullteilerfrei und somit kein Körper.

Ist  $m$  eine Primzahl und  $0 \neq a \in \mathbb{Z}_m$ , so ist  $a$  teilerfremd zu  $p$  und es existiert  $a^{-1} \in \mathbb{Z}_m$  mit  $a^{-1} \cdot a = 1 \in \mathbb{Z}_m$  (Euklidischer Algorithmus), d.h.  $\mathbb{Z}_m$  ist ein

Körper. □

Beispiel: Bestimme  $5^{-1}$  in  $\mathbb{Z}_{13}$ :

$$\begin{aligned}13 &= 5 \cdot 2 + 3 \\5 &= 3 \cdot 1 + 2 \\3 &= 2 \cdot 1 + 1; \\1 &= 3 - 2 \\&= 3 - (5 - 3) = 3 \cdot 2 - 5 \\&= (13 - 5 \cdot 2) \cdot 2 - 5 = 13 \cdot 2 - 5 \cdot 5.\end{aligned}$$

D.h.  $5^{-1} = -5 = 8 \in \mathbb{Z}_{13}$ .

## Körper mit Primzahlpotenzordnung

**Definition 7** Ist  $\mathbb{K}$  ein Körper und existiert eine natürliche Zahl  $n$  mit  $na = 0$  für alle  $a \in \mathbb{K}$ , dann heißt das kleinste natürliche  $n$  mit dieser Eigenschaft die Charakteristik von  $\mathbb{K}$ . Falls solch ein  $n$  nicht existiert, so habe  $\mathbb{K}$  die Charakteristik 0.

**Hilfssatz 2** Die Charakteristik eines endlichen Körpers  $\mathbb{K}$  ist eine Primzahl.

Beweis: Sei  $0 \neq a \in \mathbb{K}$ . Da  $\mathbb{K}$  endlich ist, gilt  $n_1 a = n_2 a$  für zwei ganze Zahlen  $0 < n_1 < n_2$  und somit  $(n_2 - n_1)a = 0$ , weswegen  $\mathbb{K}$  Charakteristik  $n > 1$  hat. Wäre  $n = kl$  zusammengesetzt mit  $1 < k, l < n$ , so würde wegen der Existenz von  $k^{-1}$  aus  $na = kla = 0$  im Widerspruch zur Definition der Charakteristik  $la = k^{-1}0 = 0$  folgen. □

**Hilfssatz 3** Die Anzahl der Elemente eines endlichen Körpers  $\mathbb{K}$  ist eine Primzahlpotenz.

Beweis: Jeder endliche Körper besitzt einen kleinsten Unterkörper (*Primkörper*), der isomorph zu  $\mathbb{Z}_p$  mit einer Primzahl  $p$  ist.  $\mathbb{K}$  ist also ein endlich dimensionaler Vektorraum über  $\mathbb{Z}_p$  der Dimension  $r \geq 1$ , hat also  $p^r$  Elemente. □

Sei  $\mathbb{K}$  ein Körper. Die Menge

$$\mathbb{K}[X] := \{a_0 + a_1 X + \dots + a_n X^n : a_i \in \mathbb{K}, n \geq 0\}$$

ist mit der Addition

$$\begin{aligned}&(a_0 + a_1 X + \dots + a_n X^n) + (b_0 + b_1 X + \dots + b_n X^n) \\&= (a_0 + b_0) + (a_1 + b_1)X + \dots + (a_n + b_n)X^n\end{aligned}$$

und der Multiplikation

$$\begin{aligned} & (a_0 + a_1X + \dots + a_nX^n) \cdot (b_0 + b_1X + \dots + b_nX^n) \\ &= (a_0b_0) + (a_0b_1 + a_1b_0)X + \dots + (a_nb_n)X^{2n} \end{aligned}$$

(wobei ggf. Nullen aufgefüllt werden) ein kommutativer Ring mit 1 und heißt *Polynomring über  $\mathbb{K}$* . Die Elemente  $f(X) = a_0 + a_1X + \dots + a_nX^n$  heißen *Polynome*. Ist  $a_n \neq 0$ , so heißt  $n$  der *Grad von  $f(X)$* . Falls  $a_n = 1$ , so nennt man  $f(X)$  *normiert*. Ein Polynom  $f(X)$  vom Grad  $n \geq 1$  heißt *reduzibel über  $\mathbb{K}$* , wenn es Polynome  $g(X)$  und  $h(X)$  in  $\mathbb{K}[X]$  vom Grad kleiner als  $n$  mit  $f(X) = g(X)h(X)$  gibt. Anderenfalls heißt  $f(X)$  *irreduzibel über  $\mathbb{K}$* .

Für ein Polynom  $f(X) \in \mathbb{K}[X]$  vom Grad  $n$  sei

$$\mathbb{K}[X]/(f(X)) := \{a_0 + a_1X + \dots + a_{n-1}X^{n-1} : a_0, a_1, \dots, a_{n-1} \in \mathbb{K}\}$$

die Menge der Polynome vom Grad kleiner als  $n$  mit den Operationen

$$\begin{aligned} g_1(X) + g_2(X) = g_3(X) & \iff f(X) \text{ teilt } g_1(X) + g_2(X) - g_3(X), \\ g_1(X) \cdot g_2(X) = g_3(X) & \iff f(X) \text{ teilt } g_1(X) \cdot g_2(X) - g_3(X), \end{aligned}$$

$$g_1(X), g_2(X), g_3(X) \in \mathbb{K}[X]/(f(X)).$$

**Hilfssatz 4**  $\mathbb{K}[X]/(f(X))$  ist genau dann ein Körper, wenn  $f(X)$  irreduzibel über  $\mathbb{K}$  ist.

Beweis:  $\mathbb{K}[X]/(f(X))$  ist offensichtlich ein kommutativer Ring mit 1.

Ist  $f(X) = g(X) \cdot h(X)$  reduzibel, so ist  $\mathbb{K}[X]/(f(X))$  nicht nullteilerfrei und daher kein Körper.

Ist  $f(X)$  irreduzibel und  $a(X) \in \mathbb{K}[X]/(f(X))$  nicht das Nullpolynom, so gilt  $\text{ggT}(a(X), f(X)) = 1$  und es existieren  $r(X)$  und  $m(X) \in \mathbb{K}[X]$  mit

$$a(X)r(X) + m(X)f(X) = 1$$

(Polynomdivision und Rückwärtseinsetzen), also  $a(X)^{-1} \in \mathbb{K}[X]/(f(X))$ .  $\square$

Beispiel:  $X^3 + X + 1$  ist irreduzibel über  $\mathbb{Z}_2$  und  $\mathbb{Z}_2[X]/(X^3 + X + 1) = \{a + bX + cX^2 : a, b, c \in \mathbb{Z}_2\}$  ist ein Körper.

Die Additionsregel lautet

$$(a + bX + cX^2) + (d + eX + fX^2) = (a + d) + (b + e)X + (c + f)X^2 \in \mathbb{Z}_2[X]$$

und die Multiplikationsregel lautet:

$$(a + bX + cX^2)(d + eX + fX^2) =$$

$(ad+bf+ce)+(ae+bd+bf+ce+cf)X+(af+be+cd+cf)X^2 \in \mathbb{Z}_2[X]/(X^3+X+1)$ .

Bestimme  $(X^2)^{-1} \in \mathbb{Z}_2[X]/(X^3+X+1)$ :

$$\begin{aligned} X^3 + X + 1 &= X^2 \cdot X + (X + 1) \\ X^2 &= (X + 1)(X + 1) + 1; \\ 1 &= X^2 - (X + 1)^2 \\ &= X^2 - ((X^3 + X + 1) - X^2 \cdot X)(X + 1) \\ &= X^2(X^2 + X + 1) - (X^3 + X + 1)(X + 1). \end{aligned}$$

D.h.  $(X^2)^{-1} = (X^2 + X + 1)$ .

Ist  $f(X)$  irreduzibel über dem Körper  $\mathbb{K}$  und  $\alpha$  eine Nullstelle von  $f(X)$  (in einem Erweiterungskörper von  $\mathbb{K}$ ), so können wir den Körper  $\mathbb{K}[X]/(f(X))$  als  $\mathbb{K}(\alpha) = \{g(\alpha) : g \in \mathbb{K}[X]\}$  darstellen, indem wir  $\alpha$  und  $X$  identifizieren.

Beispiel (Fortsetzung): Ersetzen wir  $X$  durch  $\alpha$ , wobei  $\alpha$  eine Nullstelle von  $X^3 + X + 1$  ist, so erhalten wir die Darstellung desselben Körpers als  $\mathbb{Z}_2(\alpha)$ .

## Existenz und Eindeutigkeit

**Hilfssatz 5** *Ist  $\mathbb{K}$  ein endlicher Körper mit  $q$  Elementen, so gilt  $a^q = a$ ,  $a \in \mathbb{K}$ .*

Beweis: Für  $a = 0$  ist die Aussage trivial und für  $a \neq 0$  gilt  $a^{q-1} = 1$  nach dem kleinen Fermat.  $\square$

**Hilfssatz 6** *Ist  $\mathbb{K}$  ein endlicher Körper mit  $q$  Elementen, so hat das Polynom  $X^q - X \in \mathbb{K}[X]$  die Faktorisierung*

$$X^q - X = \prod_{a \in \mathbb{K}} (X - a).$$

Beweis: Das Polynom  $X^q - X$  hat höchstens  $q$  Nullstellen. Hilfssatz 5 liefert die Nullstellen. Mit Polynomdivision lassen sich die Nullstellen sukzessive abspalten.  $\square$

**Hilfssatz 7** *In einem Körper  $\mathbb{K}$  der Charakteristik  $p$  gilt:*

$$(a + b)^{p^i} = a^{p^i} + b^{p^i}, \quad a, b \in \mathbb{K}, \quad i = 1, 2, \dots$$

Beweis: Für  $i = 1$  gilt nach dem binomischen Lehrsatz:

$$(a + b)^p = \sum_{k=0}^p \binom{p}{k} a^k b^{p-k}.$$

Für  $k = 1, \dots, p-1$  gilt

$$\binom{p}{k} = p \frac{(p-1)!}{k!(p-k)!} = 0 \in \mathbb{K}$$

und daher die Behauptung für  $i = 1$ . Für  $i \geq 2$  folgt die Behauptung induktiv.  $\square$

**Satz 3** *Zu jeder Primzahlpotenz  $q$  gibt es bis auf Isomorphie genau einen endlichen Körper  $\mathbb{F}_q$ .*

Beweis: Existenz: Für  $q = p^r$  sei  $\mathbb{K}$  der Zerfällungskörper von  $X^q - X$  über  $\mathbb{Z}_p$  (d. h.  $X^q - X = (X - a_1) \cdots (X - a_q)$  mit  $a_1, \dots, a_q \in \mathbb{K}$ ). Dann ist  $S := \{a \in \mathbb{K} : a^q = a\}$  ein Unterkörper von  $\mathbb{K}$  wegen

$$(a - b)^q = a^q - b^q = a - b, \quad a, b \in S$$

und

$$(ab^{-1})^q = a^q(b^q)^{-1} = ab^{-1}, \quad a, b \in S \setminus \{0\}.$$

Wegen  $(X^q - X)' = qX^{q-1} - 1 = -1 \neq 0$  hat  $X^q - X$  keine doppelten Nullstellen und es gilt  $|S| = q$ . Außerdem zerfällt  $X^q - X$  über  $S$ , woraus  $S = \mathbb{K}$  folgt.

Eindeutigkeit: Dieses folgt aus der Eindeutigkeit von Zerfällungskörpern.  $\square$

## Multiplikative Struktur

Die *Ordnung* von  $0 \neq a \in \mathbb{F}_q$  ist die kleinste natürliche Zahl  $n$ , für die  $a^n = 1$  gilt.

Jedes  $k$  mit  $a^k = 1$  ist durch die Ordnung von  $a$  teilbar.

**Satz 4** *Die multiplikative Gruppe  $\mathbb{F}_q^*$  eines endlichen Körpers ist zyklisch, d. h. es gibt ein Element der Ordnung  $q - 1$ .*

Beweis: Sei  $q - 1 = p_1^{r_1} \cdots p_m^{r_m}$  die Primfaktorzerlegung von  $q - 1$ . Die Polynome  $X^{(q-1)/p_i} - 1$  haben höchstens  $(q-1)/p_i < q-1$  Nullstellen in  $\mathbb{F}_q$ ,  $i = 1, \dots, m$ . Sei  $a_i \in \mathbb{F}_q^*$  keine Nullstelle von  $X^{(q-1)/p_i} - 1$  und  $b_i := a_i^{(q-1)/p_i^{r_i}}$ ,  $i = 1, \dots, m$ . Wegen  $b_i^{p_i^{r_i}} = 1$  und  $b_i^{p_i^{r_i-1}} = a_i^{(q-1)/p_i} \neq 1$  ist die Ordnung von  $b_i$  gleich  $p_i^{r_i}$ . Das Element  $b = b_1 \cdots b_m$  hat die Ordnung  $q - 1$ , da sonst  $1 = b^{(q-1)/p_i} = b_1^{(q-1)/p_i} \cdots b_m^{(q-1)/p_i} = b_i^{(q-1)/p_i}$  für ein  $i$  gelten würde. Da die Ordnung  $p_i^{r_i}$  von  $b_i$  aber dann  $(q-1)/p_i$  teilen müsste, erhält man einen Widerspruch.  $\square$

**Definition 8** *Ein Element  $a \in \mathbb{F}_q^*$  der Ordnung  $q - 1$  heißt primitives Element von  $\mathbb{F}_q$ .*

# Charaktere

**Definition 9** Eine Abbildung  $\chi : \mathbb{F}_q^* \rightarrow \mathbb{C} \setminus \{0\}$  mit der Eigenschaft

$$\chi(xy) = \chi(x)\chi(y), \quad x, y \in \mathbb{F}_q^*$$

heißt (multiplikativer) Charakter von  $\mathbb{F}_q$ .

Wir definieren  $\chi(0) := 0$ .

Es gilt:  $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1) = 1$ .

Nach dem kleinen Fermat gilt:  $\chi(x)^{q-1} = \chi(x^{q-1}) = \chi(1) = 1$  für alle  $x \in \mathbb{F}_q^*$ .

Die kleinste natürliche Zahl  $n$  mit  $\chi(x)^n = 1$  für alle  $x \in \mathbb{F}_q^*$  heißt *Ordnung von  $\chi$* .

Sei  $g$  ein primitives Element von  $\mathbb{F}_q$ , so sind die Abbildungen  $\chi_j$ ,  $j = 0, 1, \dots, q-2$ , definiert durch

$$\chi_j(g^k) = e^{2\pi i j k / (q-1)}, \quad k = 0, 1, \dots, q-2,$$

Charaktere. (Dies sind in der Tat alle Charaktere von  $\mathbb{F}_q$ , da ein Charakter  $\chi$  durch den Wert  $\chi(g)$  eindeutig festgelegt wird und es wegen  $\chi(g)^{q-1} = 1$  nur  $q-1$  verschiedene Werte  $\chi(g)$  geben kann.)

Beispiel: Der Charakter  $\chi_0(g^k) = 1$  hat die Ordnung 1 und heißt *trivialer Charakter* von  $\mathbb{F}_q^*$ .  $\chi_1$  hat die Ordnung  $q-1$  und heißt *erzeugender Charakter*. Ist  $q$  ungerade, so hat  $\chi_{(q-1)/2}(g^k) = (-1)^k$  die Ordnung 2 und heißt *quadratischer Charakter* von  $\mathbb{F}_q^*$ .

**Hilfssatz 8** Für einen Charakter  $\chi_j$  von  $\mathbb{F}_q$  mit  $1 \leq j \leq q-2$  gilt:

$$\sum_{x \in \mathbb{F}_q^*} \chi_j(x) = 0.$$

Beweis: Sei  $g$  ein primitives Element von  $\mathbb{F}_q$ . Dann gilt:

$$\sum_{x \in \mathbb{F}_q^*} \chi_j(x) = \sum_{k=0}^{q-2} \chi_j(g^k) = \sum_{k=0}^{q-2} \chi_j(g)^k = \frac{\chi_j(g)^{q-1} - 1}{\chi_j(g) - 1} = 0.$$

□

**Hilfssatz 9** Für  $1 \leq j \leq q-2$  gilt

$$\sum_{x \in \mathbb{F}_q} \chi_j(x) \chi_{q-1-j}(x+a) = -1, \quad a \in \mathbb{F}_q^*.$$

Beweis: Offensichtlich gilt

$$\chi_j(x)\chi_{q-1-j}(x+a) = \chi_j(x(x+a)^{-1}), \quad x \neq -a,$$

und  $x(x+a)^{-1}$  durchläuft alle Elemente von  $\mathbb{F}_q$  bis auf 1, wenn  $x$  ganz  $\mathbb{F}_q$  bis auf  $-a$  durchläuft.

$$\sum_{x \in \mathbb{F}_q} \chi_j(x)\chi_{q-1-j}(x+a) = \sum_{y \in \mathbb{F}_q} \chi_j(y) - \chi_j(1) = -1$$

nach dem vorherigen Lemma. □

Für eine genauere Einführung siehe:

R. Lidl und H. Niederreiter, Finite Fields, 1983.

## Aufgaben

1. Konstruiere Additions- und Multiplikationstabelle für  $\mathbb{Z}_5$  und  $\mathbb{Z}_8$ .
2. Finde das Inverse von
  - a) 2, 5 und 8 in  $\mathbb{Z}_{11}$ ,
  - b) 4, 7 und 11 in  $\mathbb{Z}_{17}$ .
3. Zeige, dass die folgenden Polynome irreduzibel sind:
  - a)  $1 + X + X^2 + X^3 + X^4$  und  $1 + X^3 + X^4$  über  $\mathbb{F}_2$ ,
  - b)  $1 + X^2$  und  $2 + 2X + X^2$  über  $\mathbb{F}_3$ .
4. Sei  $\alpha$  eine Nullstelle von  $1 + X^2$  und  $\beta$  eine Nullstelle von  $2 + 2X + X^2$  über  $\mathbb{F}_3$ .
  - a) Konstruiere Additions- und Multiplikationstabellen für  $\mathbb{F}_3(\alpha)$  und  $\mathbb{F}_3(\beta)$ .
  - b) Schreibe  $\alpha$  als Ausdruck von  $\beta$ . (Es gibt zwei Möglichkeiten.)
5.
  - a) Bestimme die Ordnung von 2, 7, 10 und 12 in  $\mathbb{F}_{17}$ .
  - b) Bestimme die Ordnung von  $\alpha$ ,  $\alpha^3$ ,  $\alpha + 1$  und  $\alpha^3 + 1$  in  $\mathbb{F}_{16}$ , wobei  $\alpha$  eine Nullstelle von  $1 + X + X^4$  ist.
6. Bestimme alle primitiven Elemente der Körper  $\mathbb{F}_7$  und  $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$  mit  $\alpha^2 = 2$ .
7. Zeige, dass die Menge der Charaktere  $G$  von  $\mathbb{F}_q$  bzgl. der Multiplikation  $(\chi \cdot \psi)(x) = \chi(x)\psi(x)$ ,  $\chi, \psi \in G$ , eine (zyklische) Gruppe ist.
8. Bestimme alle Charaktere von  $\mathbb{F}_5$ .

# Kapitel 4

## Prüfziffersysteme und Orthomorphismen

**Definition 10** Eine Prüfzeichen-Codierung über  $\mathbb{F}_q$  besteht aus  $n$  Permutationen  $f_1, \dots, f_n$  von  $\mathbb{F}_q$  und einem Element  $c \in \mathbb{F}_q$ . Dabei wird ein Wort  $a_1 \dots a_{n-1} \in \mathbb{F}_q^{n-1}$  so um ein Prüfzeichen  $a_n$  erweitert, dass die Kontrollgleichung

$$f_1(a_1) + \dots + f_n(a_n) = c$$

erfüllt ist.

### Beispiele für Prüfziffersysteme

ISBN (International Standard Book Number):

Sprache–Buch–Verlag–Prüfziffer ( $a_1 - a_2a_3a_4a_5a_6 - a_7a_8a_9 - a_{10}$ )

Beispiel: Das Buch von D. Jungnickel: Codierungstheorie hat die ISBN

3 – 86025 – 432 – 4.

Bei einer korrekten ISBN muss  $a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 + 10a_{10}$  durch 11 teilbar sein.

IBAN (International Bank Account Number):

Land–Prüfziffer–BLZ–Kontonummer

Beispiel: AT – 76 – 29811 – 39726427366

Ersetzt man die Buchstaben für das Land nach dem Schema

$A \mapsto 10, B \mapsto 11, \dots, T \mapsto 29, \dots, Z \mapsto 35$

und verschiebt die Länderkennzahl und die Prüfziffer nach hinten, so muss bei einer korrekten IBAN die entstehende Zahl  $-1$  durch 97 teilbar sein.

VSNR (Versicherungsnummer):

Laufnummer–Prüfziffer–Geburtsdatum

$L_1L_2L_3 - P - T_1T_2M_1M_2J_1J_2$

Bei einer korrekten VSNR muss

$$3L_1 + 7L_2 + 9L_3 + 10P + 5T_1 + 8T_2 + 4M_1 + 2M_2 + J_1 + 6J_2$$

durch 11 teilbar sein.

EAN (European Article Number, Strichcode):

Basisnummer–Prüfziffer

$$X_1X_2X_3X_4X_5X_6X_7X_8X_9X_{10}X_{11}X_{12} - P$$

Bei einer korrekten EAN muss

$$X_1 + X_3 + X_5 + X_7 + X_9 + X_{11} + 3(X_2 + X_4 + X_6 + X_8 + X_{10} + X_{12}) + P$$

durch 10 teilbar sein.

Weitere Beispiele für Prüfziffersysteme findet man auf

<http://www.pruefziffernberechnung.de>.

## Nachbartranspositionen und Orthomorphismen

Statistiken zeigen, dass ca. 80 Prozent aller Eingabefehler Einzelfehler sind ( $a \mapsto b$ ) und ca. 10 Prozent Nachbar-Transpositionen ( $ab \mapsto ba$ ).

Offensichtlich erkennt jede Prüfzeichen-Codierung alle Einzelfehler.

**Hilfssatz 10** *Eine Prüfziffer-Codierung erkennt genau dann alle Nachbar-Transpositionen, wenn*

$$f_{i+1}(f_i^{-1}(y)) + x \neq f_{i+1}(f_i^{-1}(x)) + y, \quad x, y \in \mathbb{F}_q, \quad x \neq y, \quad i = 1, 2, \dots, n-1, \quad (4.1)$$

*gilt.*

Beweis: Wegen der Kontrollgleichung  $\sum_{k=1}^n f_k(a_k) = c$  wird die Transposition  $a_i a_{i+1} \mapsto a_{i+1} a_i$  genau dann erkannt, wenn

$$f_i(a_i) + f_{i+1}(a_{i+1}) \neq f_i(a_{i+1}) + f_{i+1}(a_i)$$

gilt. Mit  $x := f_i(a_i)$  und  $y := f_i(a_{i+1})$  folgt die Behauptung.  $\square$

Mit  $F_i := f_{i+1} \circ f_i^{-1}$  lautet (4.1):

$$F_i(x) - x \neq F_i(y) - y, \quad x, y \in \mathbb{F}_q, \quad x \neq y.$$

Eine Abbildung mit dieser Eigenschaft heißt *Orthomorphismus*.

**Definition 11** *Ein Polynom  $f(X) \in \mathbb{F}_q[X]$  heißt Orthomorphismus von  $\mathbb{F}_q$ , wenn  $f(X)$  und  $f(X) - X$  Permutationspolynome sind.*

**Satz 5** *Es existiert genau dann eine Prüfzeichen-Codierung über  $\mathbb{F}_q$ , die jede Nachbar-Transposition erkennt, wenn es einen Orthomorphismus von  $\mathbb{F}_q$  gibt.*

Beweis: Jedes  $F_i$  ist ein Orthomorphismus, falls alle Nachbar-Transpositionen erkannt werden. Ist umgekehrt  $f$  ein Orthomorphismus, so wählen wir  $f_0(X) := X$  und  $f_i(X) := f(f_{i-1}(X))$ ,  $i = 1, 2, \dots, n$ . Damit ergibt sich für jedes  $i$ :

$$F_i(X) := f_{i+1}(f_i^{-1}(X)) = f(X)$$

und es folgt (4.1). □

## Lineare Orthomorphismen

Ein Polynom der Form  $f(X) = aX$  ist genau dann ein Orthomorphismus, wenn  $a \notin \{0, 1\}$ . Diese Orthomorphismen heißen *lineare Orthomorphismen* und über  $\mathbb{F}_q$  gibt es  $q - 2$  verschiedene lineare Orthomorphismen.

## Quadratische Orthomorphismen

**Hilfssatz 11** *Sei  $q$  eine ungerade Primzahlpotenz. Ein Polynom  $f_{a,b}(X) \in \mathbb{F}_q[X]$  der Form*

$$f_{a,b}(X) = \frac{a-b}{2}X^{(q+1)/2} + \frac{a+b}{2}X, \quad a, b \in \mathbb{F}_q^*, \quad a \neq b, \quad (4.2)$$

erfüllt

$$f_{a,b}(x) = \left\{ \begin{array}{ll} ax, & x = g^{2j}, \\ bx, & x = g^{2j+1}, \end{array} \right\}, \quad j = 0, 1, \dots, (q-3)/2,$$

wobei  $g$  ein primitives Element von  $\mathbb{F}_q$  ist.

Beweis: Es gilt  $(g^{2j})^{(q-1)/2} = 1$  und  $(g^{2j+1})^{(q-1)/2} = g^{(q-1)/2} = -1$ . □

**Hilfssatz 12** *Ein Polynom  $f_{a,b}(X)$  der Form (4.2) ist genau dann ein Permutationspolynom, wenn*

$$\chi_{(q-1)/2}(a) = \chi_{(q-1)/2}(b)$$

*gilt. Ist  $f_{a,b}(X)$  ein Permutationspolynom, so ist  $f_{a,b}(X)$  genau dann ein Orthomorphismus, wenn*

$$\chi_{(q-1)/2}(a-1) = \chi_{(q-1)/2}(b-1)$$

*gilt.*

Beweis: Sei  $x = g^{2j}$  und  $y = g^{2k}$ , dann folgt aus  $f_{a,b}(x) = f_{a,b}(y)$ ,  $ax = ay$  und somit  $x = y$ . Sei  $x = g^{2j+1}$  und  $y = g^{2k+1}$ , dann folgt aus  $f_{a,b}(x) = f_{a,b}(y)$ ,  $bx = by$  und somit  $x = y$ . Sei schließlich  $x = g^{2j}$  und  $y = g^{2k+1}$ , so folgt aus  $f_{a,b}(x) = f_{a,b}(y)$ ,  $ax = by$  und somit

$$\chi_{(q-1)/2}(a) = \chi_{(q-1)/2}(ax) = \chi_{(q-1)/2}(by) = -\chi(b).$$

Wegen  $\chi_{(q-1)/2}(a), \chi_{(q-1)/2}(b) \in \{-1, 1\}$  folgt die erste Behauptung. Die zweite folgt unmittelbar aus der Definition eines Orthomorphismus.  $\square$

Orthomorphismen der Form (4.2) heißen *quadratische Orthomorphismen*.

**Satz 6** Die Anzahl der verschiedenen Permutationspolynome von  $\mathbb{F}_q$  der Form (4.2) ist

$$\frac{(q-1)(q-3)}{2}$$

und die Anzahl der quadratischen Orthomorphismen von  $\mathbb{F}_q$  ist

$$\frac{(q-3)(q-5)}{4}.$$

Beweis: Für ein Permutationspolynom können wir  $a \in \mathbb{F}_q^*$  beliebig wählen und  $b \in \mathbb{F}_q^*, b \neq a$ , so dass

$$\chi_{(q-1)/2}(a) = \chi_{(q-1)/2}(b).$$

Insgesamt gibt es also  $(q-1) \cdot (q-3)/2$  dieser Permutationspolynome.

Ein Polynom der Form (4.2) mit  $a, b \neq 1, a \neq b$ , ist genau dann ein Orthomorphismus, wenn

$$\chi_{(q-1)/2}(a) = \chi_{(q-1)/2}(b) \quad \text{und} \quad \chi_{(q-1)/2}(a-1) = \chi_{(q-1)/2}(b-1).$$

Durchläuft  $(a, b)$  ganz  $(\mathbb{F}_q^*)^2$ , so auch  $(a, ab)$  und  $f_{a,ab}, b \neq 1$ , ist genau dann ein Orthomorphismus, wenn

$$\chi_{(q-1)/2}(a) = \chi_{(q-1)/2}(ab) \quad \text{und} \quad \chi_{(q-1)/2}(a-1) = \chi_{(q-1)/2}(ab-1),$$

d.h.

$$\chi_{(q-1)/2}(b) = 1 \quad \text{und} \quad \chi_{(q-1)/2}(a-1) = \chi_{(q-1)/2}(a-b^{-1}).$$

Zu gegebenem  $b \neq 1$  mit  $\chi_{(q-1)/2}(b) = 1$  erfüllt die folgende Funktion

$$\varphi_b(a) = (\chi_{(q-1)/2}(a-1)\chi_{(q-1)/2}(a-b^{-1}) + 1)/2, \quad a \notin \{1, b^{-1}\},$$

die Bedingung

$$\varphi_b(a) = \begin{cases} 1, & f_{a,ab} \text{ ist Orthomorphismus,} \\ 0, & \text{sonst.} \end{cases}$$

Die Anzahl der Orthomorphismen  $f_{a,ab}$  ist also

$$\begin{aligned}
 & \sum_{\substack{b \in \mathbb{F}_q^* \\ \chi_{(q-1)/2}(b)=1, \ b \neq 1}} \sum_{\substack{a \in \mathbb{F}_q^* \\ a \notin \{1, b^{-1}\}}} \varphi_b(a) \\
 = & \frac{1}{2} \sum_{\substack{b \in \mathbb{F}_q^* \\ \chi_{(q-1)/2}(b)=1, \ b \neq 1}} \sum_{\substack{a \in \mathbb{F}_q^* \\ a \notin \{1, b^{-1}\}}} (\chi_{(q-1)/2}(a-1)\chi_{(q-1)/2}(a-b^{-1}) + 1) \\
 = & \frac{1}{2} \sum_{\substack{b \in \mathbb{F}_q^* \\ \chi_{(q-1)/2}(b)=1, \ b \neq 1}} (-1 - \chi_{(q-1)/2}(b) + q - 3) \\
 = & \frac{(q-3)(q-5)}{4}
 \end{aligned}$$

nach Hilfssatz 9. □

Wählt man  $a$  und  $b$  zufällig, so ist die Wahrscheinlichkeit, dass  $f_{a,b}$  ein Orthomorphismus ist ungefähr  $1/4$ .

## Aufgaben

1. Welche der folgenden ISBN ist gültig?  
a) 3 – 61990 – 540 – 8, b) 0 – 19330 – 201 – 2, c) 9 – 67861 – 971 – 9.
2. Welche Prüfziffer muss man an 762220000460 anfügen, um eine korrekte EAN zu erhalten?
3. Ist 6151 – 110968 eine korrekte VSNR?
4. Gebe  $f_i(X)$ ,  $i = 1, \dots, 10$ , und  $c$  aus Definition 10 für die ISBN an und berechne  $F_i(X) = f_{i+1}(f_i^{-1}(X))$ ,  $i = 1, \dots, 9$ . Ist  $F_i(X)$  ein (linearer) Orthomorphismus?
5. Auf welchen Orthomorphismen basieren IBAN, VSNR und EAN?
6. Bestimme alle linearen und quadratischen Orthomorphismen von  $\mathbb{F}_5$  und  $\mathbb{F}_7$ .

# Kapitel 5

## Linearcodes

**Definition 12** Ein Linearcode  $C$  der Länge  $n$  über  $\mathbb{F}_q$  ist ein Untervektorraum von  $\mathbb{F}_q^n$ .

Sei  $k$  die Dimension des Linearcodes  $C$  über  $\mathbb{F}_q$ , so ist  $C$  ein  $(n, q^k)$ -Code. Bei Linearcodes verwendet man stattdessen die Bezeichnung  $[n, k]$ -Code.

## Dualcodes

**Definition 13** Das innere Produkt zweier Vektoren

$$\mathbf{v} = (v_1, \dots, v_n), \quad \mathbf{w} = (w_1, \dots, w_n) \in \mathbb{F}_q^n$$

ist definiert als

$$\mathbf{v} \cdot \mathbf{w} := v_1 \cdot w_1 + \dots + v_n w_n \in \mathbb{F}_q.$$

Zwei Vektoren  $\mathbf{v}$  und  $\mathbf{w}$  heißen orthogonal, wenn  $\mathbf{v} \cdot \mathbf{w} = 0$ .

Sei  $S = \{\mathbf{v}_1, \dots, \mathbf{v}_l\}$  eine nichtleere Teilmenge von  $\mathbb{F}_q^n$ , so heißt

$$\langle S \rangle := \{\lambda_1 \mathbf{v}_1 + \dots + \lambda_l \mathbf{v}_l : \lambda_i \in \mathbb{F}_q\}$$

lineare Hülle von  $S$  und

$$S^\perp := \{\mathbf{v} \in \mathbb{F}_q^n : \mathbf{v} \cdot \mathbf{s} = 0 \text{ für alle } \mathbf{s} \in S\}$$

duale Menge von  $S$ .

**Hilfssatz 13**  $\langle S \rangle$  und  $S^\perp$  sind Vektorräume und es gilt

$$\dim(\langle S \rangle) + \dim(S^\perp) = n.$$

Beweis: Für die erste Aussage muss man das Untervektorraumkriterium überprüfen:

$$\mathbf{u}, \mathbf{v} \in U, a, b \in \mathbb{F}_q \Rightarrow a\mathbf{u} + b\mathbf{v} \in U.$$

Sei  $k := \dim(\langle S \rangle)$  und  $\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$  eine Basis von  $\langle S \rangle$ . Dann ist  $\mathbf{x} \in S^\perp$  genau dann, wenn

$$\mathbf{v}_1 \cdot \mathbf{x} = \dots = \mathbf{v}_k \cdot \mathbf{x} = 0.$$

Die Lösungen dieses linearen Gleichungssystems bilden einen  $n - k$ -dimensionalen Vektorraum.  $\square$

**Definition 14** Sei  $C$  ein Linearcode, so heißt  $C^\perp$  Dualcode von  $C$ .

**Hilfssatz 14** Es gilt:  $(C^\perp)^\perp = C$ .

Beweis: Sei  $\mathbf{c} \in C$ . Für alle  $\mathbf{x} \in C^\perp$  gilt  $\mathbf{c} \cdot \mathbf{x} = 0$ , d.h.  $\mathbf{c} \in (C^\perp)^\perp$ . Damit haben wir  $C \subseteq (C^\perp)^\perp$ . Nach Hilfssatz 13 gilt  $\dim(C) = \dim((C^\perp)^\perp)$  und somit  $C = (C^\perp)^\perp$ .  $\square$

**Definition 15** Sei  $C$  ein Linearcode.  $C$  heißt selbstorthogonal, wenn  $C \subseteq C^\perp$  und selbstdual, wenn  $C = C^\perp$ .

**Hilfssatz 15** Die Dimension eines selbstorthogonalen Codes der Länge  $n$  ist  $\leq n/2$  und die Dimension eines selbstdualen Codes ist  $n/2$ .

## Hamminggewicht

**Definition 16** Das (Hamming-)Gewicht  $w(\mathbf{x})$  eines Wortes  $\mathbf{x} \in \mathbb{F}_q^n$  ist die Anzahl der von Null verschiedenen Koordinaten von  $\mathbf{x}$ , d.h.  $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$ .

Es gilt:  $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$ .

Für  $\mathbf{x} = (x_1, x_2, \dots, x_n), \mathbf{y} = (y_1, y_2, \dots, y_n) \in \mathbb{F}_q^n$  sei

$$\mathbf{x} * \mathbf{y} = (x_1 y_1, x_2 y_2, \dots, x_n y_n).$$

**Hilfssatz 16** Für  $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$  gilt

$$w(\mathbf{x} + \mathbf{y}) = w(\mathbf{x}) + w(\mathbf{y}) - 2w(\mathbf{x} * \mathbf{y}).$$

Beweis: Wegen  $w(\mathbf{x}) = w(x_1) + w(x_2) + \dots + w(x_n)$  brauchen wir nur den Fall  $n = 1$  zu überprüfen.  $\square$

**Hilfssatz 17** Für eine beliebige Primzahlpotenz  $q$  und  $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$  gilt

$$w(\mathbf{x}) + w(\mathbf{y}) \geq w(\mathbf{x} + \mathbf{y}) \geq w(\mathbf{x}) - w(\mathbf{y}).$$

**Definition 17** Sei  $C$  ein Code. Dann heißt

$$w(C) := \min_{\mathbf{0} \neq \mathbf{c} \in C} w(\mathbf{c})$$

Minimalgewicht von  $C$ .

**Hilfssatz 18** Für Linearcodes gilt  $w(C) = d(C)$ .

Beweis: Nach Definition existieren  $\mathbf{x}, \mathbf{y} \in C$ ,  $\mathbf{x} \neq \mathbf{y}$ , mit  $d(\mathbf{x}, \mathbf{y}) = d(C)$ . Daher gilt

$$d(C) = d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y}) \geq w(C).$$

Umgekehrt existiert  $\mathbf{0} \neq \mathbf{z} \in C$  mit  $w(\mathbf{z}) = w(C)$  und daher

$$w(C) = w(\mathbf{z}) = d(\mathbf{z}, \mathbf{0}) \geq d(C). \quad \square$$

## Aufgaben

- Bestimme zu jeder der folgenden Mengen  $S$  die lineare Hülle  $\langle S \rangle$  und die duale Menge  $S^\perp$ :
  - $S = \{101, 111, 010\}$ ,  $q = 2$ ,
  - $S = \{1020, 0201, 2001\}$ ,  $q = 3$ ,
  - $S = \{00101, 10001, 11011\}$ ,  $q = 2$ .
- Bestimme, welche der folgenden Codes Linearcodes über  $\mathbb{F}_q$  sind:
  - $q = 2$ ,  $C = \{1101, 1110, 1011, 1111\}$ ,
  - $q = 3$ ,  $C = \{0000, 1001, 0110, 2002, 1111, 0220, 1221, 2112, 2222\}$ ,
  - $q = 2$ ,  $C = \{00000, 11110, 01111, 10001\}$ .
- $C$  und  $D$  seien Linearcodes über  $\mathbb{F}_q$  derselben Länge. Zeige, dass

$$C + D := \{\mathbf{c} + \mathbf{d} : \mathbf{c} \in C, \mathbf{d} \in D\}$$

ein Linearcode ist und dass

$$(C + D)^\perp = C^\perp \cap D^\perp.$$

- Überprüfe, welche der folgenden Aussagen wahr ist:
  - Sind  $C$  und  $D$  Linearcodes, so ist auch  $C \cap D$  ein Linearcode.
  - Sind  $C$  und  $D$  Linearcodes, so ist auch  $C \cup D$  ein Linearcode.
  - Sei  $C = \langle \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3 \rangle$  mit  $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3 \in \mathbb{F}_q^n$ , so gilt  $\dim(C) = 3$ .
  - Sei  $C = \langle \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3 \rangle$  mit  $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3 \in \mathbb{F}_q^n$ , so gilt

$$d(C) = \min\{w(\mathbf{c}_1), w(\mathbf{c}_2), w(\mathbf{c}_3)\}.$$

- Sind  $C$  und  $D$  Linearcodes mit  $C \subseteq D$ , so gilt  $D^\perp \subseteq C^\perp$ .

5. Entscheide, welche der folgenden Linearcodes selbstdual sind:
  - a)  $C = \langle 1110100, 1101010, 1011001 \rangle$  über  $\mathbb{F}_2$ ,
  - b)  $C = \langle 1110, 1201 \rangle$  über  $\mathbb{F}_3$ ,
  - c)  $C = \langle 1001\rho\rho, 010\rho1\rho, 0011\rho\rho \rangle$  über  $\mathbb{F}_4 = \mathbb{F}_2(\rho)$  (d.h.  $\rho^2 = \rho + 1$ ).
6. Sei  $n$  ungerade und  $C$  ein selbstorthogonaler binärer  $[n, (n-1)/2]$ -Code. Sei  $\mathbf{1}$  der Vektor der Länge  $n$ , der nur aus Einsen besteht, und setze  $\mathbf{1} + C := \{\mathbf{1} + \mathbf{c} : \mathbf{c} \in C\}$ . Zeige  $C^\perp = C \cup (\mathbf{1} + C)$ .
7. Seien  $\mathbf{c}, \mathbf{d} \in \mathbb{F}_2^n$ . Zeige:
  - a) Haben entweder beide Vektoren  $\mathbf{c}$  und  $\mathbf{d}$  gerades oder beide ungerades Gewicht, so hat  $\mathbf{c} + \mathbf{d}$  gerades Gewicht.
  - b) Hat genau einer der beiden Vektoren  $\mathbf{c}$  oder  $\mathbf{d}$  gerades Gewicht, so hat  $\mathbf{c} + \mathbf{d}$  ungerades Gewicht.
  - c) Bei einem binären Linearcode  $C$  haben entweder alle oder genau die Hälfte aller Codewörter gerades Gewicht.
8. a) Zeige, dass in einem selbstorthogonalen Binärcode jedes Codewort gerades Gewicht hat.  
 b) Zeige, dass in einem selbstorthogonalen Ternärcode (d.h. über  $\mathbb{F}_3$ ) das Gewicht jedes Codewortes durch 3 teilbar ist.  
 c) Konstruiere einen selbstorthogonalen Code über  $\mathbb{F}_5$  mit einem Codewort, dessen Gewicht nicht durch 5 teilbar ist.
9. Seien  $\mathbf{c}$  und  $\mathbf{d}$  Codewörter eines selbstorthogonalen Binär-codes.
  - a) Zeige, dass  $\mathbf{c} * \mathbf{d}$  gerades Gewicht hat.
  - b) Sind die Gewichte von  $\mathbf{c}$  und  $\mathbf{d}$  beide durch 4 teilbar, so auch das Gewicht von  $\mathbf{c} + \mathbf{d}$ .

## Generatormatrix und Kontrollmatrix

**Definition 18** Eine Matrix  $G$  heißt Generatormatrix eines Linear-codes  $C$ , wenn ihre Zeilen eine Basis von  $C$  bilden. Eine Matrix  $H$  heißt Kontrollmatrix von  $C$ , wenn sie eine Generatormatrix von  $C^\perp$  ist. Eine Generatormatrix der Form  $(E_k|X)$  heißt Generatormatrix in Standardform und eine Kontrollmatrix der Form  $(Y|E_{n-k})$  Kontrollmatrix in Standardform, wobei  $E_l$  die  $l \times l$  Einheitsmatrix ist.

**Hilfssatz 19** Sei  $C$  ein  $[n, k]$ -Linearcode über  $\mathbb{F}_q$  mit Generatormatrix  $G$ . Dann gilt

$$\mathbf{v} \in C^\perp \Leftrightarrow \mathbf{v}G^T = \mathbf{0}.$$

Eine  $(n-k) \times n$ -Matrix  $H$  mit linear unabhängigen Zeilen ist genau dann eine Kontrollmatrix von  $C$ , wenn  $HG^T = O$ .

Beweis: Sei  $\mathbf{z}_i$  die  $i$ te Zeile von  $G$ ,  $i = 1, \dots, k$ . (Insbesondere gilt  $\mathbf{z}_i \in C$ .) Jedes Codewort  $\mathbf{c} \in C$  kann eindeutig als

$$\mathbf{c} = \lambda_1 \mathbf{z}_1 + \dots + \lambda_k \mathbf{z}_k, \quad \lambda_1, \dots, \lambda_k \in \mathbb{F}_q,$$

geschrieben werden.

Ist  $\mathbf{v} \in C^\perp$ , so gilt  $\mathbf{v} \cdot \mathbf{c} = 0$  für alle  $\mathbf{c} \in C$ , insbesondere  $\mathbf{v} \cdot \mathbf{z}_i = 0$ ,  $i = 1, \dots, k$ , d.h.  $\mathbf{v}G^T = \mathbf{0}$ .

Umgekehrt gelte  $\mathbf{v} \cdot \mathbf{z}_i = 0$ ,  $i = 1, \dots, k$ , so auch

$$\mathbf{v} \cdot \mathbf{c} = \lambda_1(\mathbf{v} \cdot \mathbf{z}_1) + \dots + \lambda_k(\mathbf{v} \cdot \mathbf{z}_k) = 0$$

für jedes  $\mathbf{c} \in C$ , d.h.  $\mathbf{v} \in C^\perp$ .

Nach Definition sind die Zeilen einer Kontrollmatrix linear unabhängig.

Da die Zeilen von  $H$  Codewörter in  $C^\perp$  sind, folgt  $HG^T = O$  aus dem ersten Teil des Hilfssatzes.

Gelte umgekehrt  $HG^T = O$ , dann sind nach dem ersten Teil alle Zeilen von  $H$  Codewörter von  $C^\perp$  und  $H$  Kontrollmatrix.  $\square$

**Satz 7** *Sei  $C$  ein Linearcode mit Kontrollmatrix  $H$ . Dann hat  $C$  Minimalgewicht  $d$  genau dann, wenn je  $d - 1$  Spalten von  $H$  linear unabhängig sind und  $d$  linear abhängige Spalten von  $H$  existieren.*

Beweis: Sei  $\mathbf{0} \neq \mathbf{v} = (v_1, \dots, v_n) \in C$  ein Codewort mit Gewicht  $w$  und seien  $v_{i_1}, \dots, v_{i_w}$  die von Null verschiedenen Koordinaten von  $\mathbf{v}$ . Sei  $\mathbf{s}_i$  die  $i$ te Spalte von  $H$ . Hilfssatz 19 ist äquivalent zu

$$\mathbf{v} \in C \Leftrightarrow \mathbf{0} = \mathbf{v}H^T = v_{i_1} \mathbf{s}_{i_1} + \dots + v_{i_w} \mathbf{s}_{i_w},$$

so dass  $\mathbf{s}_{i_1}, \dots, \mathbf{s}_{i_w}$  linear abhängig sind.

Je  $d - 1$  Spalten von  $H$  sind genau dann linear unabhängig, wenn  $w(C) \geq d$ , und es existieren genau dann  $d$  linear abhängige Spalten von  $H$ , wenn  $w(C) \leq d$ .  $\square$

Beispiel: Sei  $C$  der binäre Linearcode mit Kontrollmatrix

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

Je zwei Spalten von  $H$  sind linear unabhängig und die Summe der 1., 3. und 4. Spalte ergibt  $\mathbf{0}$ . Also ist  $w(C) = 3$ .

**Hilfssatz 20** *Ist  $G = (E_k | X)$  eine Generatormatrix in Standardform von  $C$ , so ist  $H = (-X^T | E_{n-k})$  Kontrollmatrix in Standardform von  $C$ .*

Beweis: Offensichtlich gilt  $HG^T = O$ . Wegen der letzten  $n - k$  Koordinaten sind die Zeilen von  $H$  linear unabhängig und das Ergebnis folgt aus Hilfssatz 19.  $\square$

Beispiel: Finde eine Generator- und eine Kontrollmatrix für den binären Linearcode  $C = \langle 11101, 10110, 01011, 11010 \rangle$ .

Mit dem Gauß-Algorithmus erhält man drei linear unabhängige Vektoren aus  $C$ , die Zeilen einer Generatormatrix sind, z.B.:

$$G = \left( \begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{array} \right).$$

Dann ist

$$H = \left( \begin{array}{ccc|cc} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{array} \right)$$

eine Kontrollmatrix von  $C$ .

## Äquivalenz

Zwei  $[n, k]$ -Codes  $C_1$  und  $C_2$  über  $\mathbb{F}_q$  heißen *äquivalent*, wenn die Wörter von  $C_2$  aus den Wörtern von  $C_1$  durch eine feste Koordinatenpermutation und Multiplikation fixer Koordinaten mit derselben Konstanten  $a \in \mathbb{F}_q^*$  erhalten werden können.

Beispiel:  $q = 3$ ,  $n = 3$

$C_1 = \{000, 011, 022\}$  und  $C_2 = \{000, 102, 201\}$  sind äquivalent.

Jeder  $[n, k]$ -Code ist zu einem  $[n, k]$ -Code mit einer Generatormatrix in Standardform äquivalent.

## Codierung

Sei  $C$  ein  $[n, k]$ -Code über  $\mathbb{F}_q$  und  $G$  eine Generatormatrix. Eine Nachricht  $\mathbf{u} \in \mathbb{F}_q^k$  der Länge  $k$  wird zu

$$\mathbf{v} = \mathbf{u}G \in \mathbb{F}_q^n$$

codiert. Ist  $G$  in Standardform, so ist  $\mathbf{v} = (\mathbf{u} | \mathbf{u}X)$ , d.h. die ersten  $k$  Symbole von  $\mathbf{v}$  beinhalten die Information (die Nachricht  $\mathbf{u}$ ) und die restlichen  $n - k$  Symbole sind Kontrollsymbole.

Beispiel: Sei  $G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$ . Die Nachricht  $\mathbf{u} = (101)$  wird zu  $\mathbf{v} = \mathbf{u}G = 10011$  codiert.

## Decodierung

**Definition 19** Sei  $C$  ein Linearcode der Länge  $n$  über  $\mathbb{F}_q$  und  $\mathbf{u} \in \mathbb{F}_q^n$ . Die Nebenklasse von  $C$  nach  $\mathbf{u}$  ist die Menge

$$\mathbf{u} + C := \{\mathbf{u} + \mathbf{v} : \mathbf{v} \in C\}.$$

Ein Wort mit kleinstem Gewicht in einer Nebenklasse heißt Nebenklassenführer.

Maximum Likelihood Decodierung:

Sei  $\mathbf{v}$  das gesendete Codewort und  $\mathbf{w}$  das empfangene Wort. Dann gilt für den Fehlervektor

$$\mathbf{e} := \mathbf{w} - \mathbf{v} \in \mathbf{w} + C.$$

Man nimmt an, dass Fehlervektoren mit minimalem Gewicht am wahrscheinlichsten sind und wählt einen Nebenklassenführer  $\mathbf{e}$  von  $\mathbf{w} + C$  und decodiert  $\mathbf{w}$  zu  $\mathbf{v} := \mathbf{w} - \mathbf{e}$ .

Beispiel: Sei  $q = 2$  und  $C = \{0000, 1011, 0101, 1110\}$ . Wir decodieren das Wort  $\mathbf{w} = (1101)$  nach Maximum Likelihood. Wir haben

$$\mathbf{w} + C = \{1101, 0110, 1000, 0011\}$$

und der eindeutige Nebenklassenführer ist  $\mathbf{e} = (1000)$ . Wir decodieren  $\mathbf{w}$  zu

$$\mathbf{v} = \mathbf{w} - \mathbf{e} = 0101.$$

Syndrom-Decodierung:

**Definition 20** Sei  $C$  ein  $[n, k]$ -Code und  $H$  eine Kontrollmatrix. Das Syndrom von  $\mathbf{w} \in \mathbb{F}_q^n$  ist das Wort

$$S(\mathbf{w}) := \mathbf{w}H^T \in \mathbb{F}_q^{n-k}.$$

**Hilfssatz 21** Für  $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$  gilt:

1.  $S(\mathbf{u} + \mathbf{v}) = S(\mathbf{u}) + S(\mathbf{v})$ ;
2.  $S(\mathbf{u}) = \mathbf{0} \Leftrightarrow \mathbf{u} \in C$ ;
3.  $S(\mathbf{u}) = S(\mathbf{v}) \Leftrightarrow \mathbf{u} + C = \mathbf{v} + C$ .

Bestimme eine Syndrom-Tabelle mit zugehörigen Nebenklassenführern. Berechne das Syndrom des empfangenen Wortes und subtrahiere den zugehörigen Nebenklassenführer  $\mathbf{e}$ .

Beispiel: Wir betrachten den binären Linearcode  $C = \{0000, 1011, 0101, 1110\}$  mit der Kontrollmatrix  $H = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}$ . Wir bestimmen eine Syndromtabelle beginnend mit den möglichen Nebenklassenführern, die das kleinste Gewicht haben.

Nebenklassenführer $\mathbf{u}$	Syndrom $S(\mathbf{u})$
0000	00
0001	01
0010	10
(0100)	01
1000	11

Zur Decodierung von  $\mathbf{w} = 1101$  berechnen wir  $S(\mathbf{w}) = 11$  und nehmen an, dass  $\mathbf{e} = 1000$  der Fehlervektor ist. Dann decodieren wir zu  $\mathbf{w} - \mathbf{e} = 0101$ .

## Aufgaben

- Finde je eine Generator- und eine Kontrollmatrix für die folgenden Codes und bestimme die Parameter  $[n, k, d]$ :
  - $q = 2$ ,  $S = \langle 1000, 0110, 0010, 0001, 1001 \rangle$ ,
  - $q = 3$ ,  $S = \langle 110000, 011000, 001100, 000110, 000011 \rangle$ ,
  - $q = 2$ ,  $S = \langle 10101010, 11001100, 11110000, 01100110, 00111100 \rangle$ .
- Konstruiere folgendermaßen einen binären Code  $C$  der Länge 6:  
Zu  $(x_1, x_2, x_3) \in \mathbb{F}_2^3$  konstruiere  $(x_1, x_2, x_3, x_4, x_5, x_6) \in C$  mit

$$x_4 = x_1 + x_2 + x_3$$

$$x_5 = x_1 + x_3$$

$$x_6 = x_2 + x_3.$$

- Zeige, dass  $C$  ein Linearcode ist.
  - Finde eine Generator- und Kontrollmatrix von  $C$ .
- a) Zeige, dass

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

eine Kontrollmatrix für den ternären Code  $C = \langle 1001, 0110 \rangle$  ist.

b) Ist

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

eine Generatormatrix von  $C^\perp$ , wobei  $C$  der Binärcode  $C = \langle 11110, 01111 \rangle$  ist?

4. Bestimme den Minimalabstand des binären Linearcodes mit Kontrollmatrix

$$\text{a) } H = \begin{pmatrix} 0111000 \\ 1110100 \\ 1100010 \\ 1010001 \end{pmatrix}, \quad \text{b) } H = \begin{pmatrix} 1101000 \\ 1010100 \\ 0110010 \\ 1100001 \end{pmatrix}.$$

5. a) Liste die Nebenklassen des binären Linearcodes

$$C = \{00000, 10001, 01010, 11011, 11011, 00100, 10101, 01110, 11111\}$$

auf.

b) Benutze a), um 11100 und 11010 zu decodieren.

c) Zeige, dass  $\begin{pmatrix} 10001 \\ 01010 \end{pmatrix}$  eine Kontrollmatrix von  $C$  ist.

d) Konstruiere eine Syndrom-Tabelle.

e) Decodiere mit d) die Wörter 11100 und 11010.

# Kapitel 6

## Schranken in der Codierungstheorie

**Definition 21** Sei  $C$  ein  $(n, M, d)$ -Code über  $A$  mit  $|A| = q$ . Dann heißt

$$\mathcal{R}(C) := \frac{\log_q |C|}{n}$$

Rate von  $C$  und

$$\delta(C) := \frac{d-1}{n}$$

relativer Minimalabstand von  $C$ .

Die Rate ist ein Maß für die Effizienz und der relative Minimalabstand für Fehlerkorrigierkapazität eines Codes.

Beispiel: 1.  $C = \mathbb{F}_q^n$ :  $\mathcal{R}(C) = 1$ ,  $\delta(C) = 0$  (optimale Rate, schlechtester relativer Minimalabstand).

2.  $C = \langle \underbrace{11 \dots 1}_n \rangle$ :  $\mathcal{R}(C) = 1/n \rightarrow 0$ ,  $\delta(C) = (n-1)/n \rightarrow 1$ ,  $n \rightarrow \infty$  (optimaler relativer Minimalabstand, schlechteste Rate).

**Definition 22** Zu einer Alphabet  $A$  mit  $q$  Elementen und gegebenen  $n$  und  $d$  sei

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

Ein  $(n, M, d)$ -Code mit  $M = A_q(n, d)$  heißt optimal.

**Definition 23** Zu einer Primzahlpotenz  $q$  und gegebenen  $n$  und  $d$  sei

$$B_q(n, d) := \max\{q^k : \exists [n, k, d]\text{-Code über } \mathbb{F}_q\}.$$

## Gilbert-Varshamov-Schranke

Sei  $K_r(\mathbf{x}) := \{\mathbf{u} \in A^n : d(\mathbf{x}, \mathbf{u}) \leq r\}$  die Kugel um  $\mathbf{x}$  mit Radius  $r$ . Dann gilt

$$|K_r(\mathbf{x})| = 1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \dots + \binom{n}{r}(q-1)^r.$$

(Der Summand  $\binom{n}{i}(q-1)^i$  entspricht der Anzahl der Wörter mit Abstand  $i$ .)

**Satz 8** Für  $1 \leq d \leq n$  gilt:

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

Beweis: Bei einem optimalen Code  $C$  gibt es kein  $\mathbf{x} \in A^n$  mit Abstand  $\geq d$  zu jedem Codewort  $\mathbf{c} \in C$ . D.h.

$$\bigcup_{\mathbf{c} \in C} K_{d-1}(\mathbf{c}) = A^n$$

also

$$\sum_{\mathbf{c} \in C} |K_{d-1}(\mathbf{c})| \geq q^n,$$

woraus die Behauptung folgt. □

## Kugelpackungsschranke

**Satz 9** Für  $1 \leq d \leq n$  gilt:

$$A_q(n, d) \leq \frac{q^n}{\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} (q-1)^i}.$$

Beweis: Sei  $C$  ein  $(n, M, d)$ -Code. Dann sind die Kugeln  $K_{\lfloor (d-1)/2 \rfloor}(\mathbf{c})$ ,  $\mathbf{c} \in C$ , paarweise disjunkt und wir haben

$$\bigcup_{\mathbf{c} \in C} K_{\lfloor (d-1)/2 \rfloor}(\mathbf{c}) \subseteq A^n.$$

D.h.

$$\sum_{\mathbf{c} \in C} |K_{\lfloor (d-1)/2 \rfloor}(\mathbf{c})| \leq q^n,$$

woraus die Behauptung folgt. □

**Definition 24** Ein  $(n, M, d)$ -Code über einem Alphabet mit  $q$  Elementen heißt perfekter Code, wenn

$$M = \frac{q^n}{\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} (q-1)^i}.$$

Beispiel: 1.  $C = \mathbb{F}_q^n$ , d.h.  $d = 1$ .

2.  $q = 2$ ,  $n$  ungerade,  $C = \{\mathbf{x}, \mathbf{y}\}$  mit  $d(\mathbf{x}, \mathbf{y}) = n$ .

## Hamming-Codes

Die Anzahl der verschiedenen 1-dimensionalen Untervektorräume von  $\mathbb{F}_q^r$  ist gleich  $(q^r - 1)/(q - 1)$ .

**Definition 25** Sei  $q$  eine Primzahlpotenz,  $r \geq 2$  und  $n := (q^r - 1)/(q - 1)$ . Wir wählen als Spalten der Matrix  $H$  von Null verschiedene Vektoren aus den  $n$  verschiedenen 1-dimensionalen Untervektorräumen von  $\mathbb{F}_q^r$ . Der Code mit Kontrollmatrix  $H$  heißt  $[n, n - r]$ -Hamming-Code.

**Satz 10** Hamming-Codes sind perfekt.

Beweis: Je zwei Spalten von  $H$  liegen in verschiedenen 1-dimensionalen Untervektorräumen, sind also linear unabhängig. Nach Satz 7 gilt also  $d \geq 3$  und der Code hat  $q^{n-r} = q^n/(1 + n(q - 1))$  Elemente und ist somit perfekt.  $\square$

Beispiel: Sei  $q = 2$ ,  $n = 7$ ,  $r = 3$ . Der  $[7, 4]$ -Hamming-Code hat die Kontrollmatrix

$$H = \begin{pmatrix} 1001101 \\ 0101011 \\ 0010111 \end{pmatrix}.$$

(Bei binären Hamming-Codes besteht die Kontrollmatrix aus den verschiedenen  $r$ -dimensionalen Vektoren ungleich  $\mathbf{0}$ .)

## Singleton Schranke und MDS Codes

**Satz 11** Für  $1 \leq d \leq n$  gilt:

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

Für einen linearen  $[n, k, d]$ -Code gilt:

$$k \leq n - d + 1.$$

Beweis: Sei  $C$  ein  $(n, M, d)$ -Code über einem Alphabet mit  $q$  Elementen. Lösche die letzten  $d - 1$  Zeichen von jedem Codewort. Diese Wörter der Länge  $n - d + 1$  sind paarweise verschieden wegen des Minimalabstandes  $d$ . Es gibt höchstens  $q^{n-d+1}$  Wörter der Länge  $n - d + 1$ , so dass  $M \leq q^{n-d+1}$  gelten muss.  $\square$

**Definition 26** Ein  $[n, k, d]$ -Code mit  $k = n - d + 1$  heißt MDS-Code (*maximum distance separable code*).

Singleton:  $\mathcal{R}(C) + \delta(C) \leq 1$ .

- Beispiele: 1.  $C = \mathbb{F}_q^n$   
 2.  $C = \langle 11 \dots 1 \rangle$   
 3.  $C = \langle 11 \dots 1 \rangle^\perp$

## Plotkin Schranke

**Satz 12** Für ein  $q > 1$  setze  $r := (q - 1)/q$  und gelte  $rn < d$ . Dann haben wir

$$A_q(n, d) \leq \left\lfloor \frac{d}{d - rn} \right\rfloor.$$

Beweis: Sei  $C$  ein  $(n, M, d)$ -Code über einem Alphabet  $A$  mit  $q$  Elementen und

$$T := \sum_{\mathbf{c}, \mathbf{c}' \in C} d(\mathbf{c}, \mathbf{c}').$$

Offensichtlich gilt

$$T \geq M(M - 1)d.$$

Sei  $B$  die  $M \times n$  Matrix, deren Zeilen die verschiedenen Codewörter von  $M$  sind und  $n_{i,a}$  die Anzahl der Einträge der  $i$ ten Spalte gleich  $a$  für  $a \in A$  und  $i = 1, \dots, n$ . Mit der Schreibweise  $\mathbf{c} = (c_1, \dots, c_n)$  bzw.  $\mathbf{c}' = (c'_1, \dots, c'_n)$  gilt:

$$\begin{aligned} T &= \sum_{i=1}^n \left( \sum_{\mathbf{c}, \mathbf{c}' \in C} d(c_i, c'_i) \right) = \sum_{i=1}^n \sum_{a \in A} n_{i,a} (M - n_{i,a}) = M^2 n - \sum_{i=1}^n \sum_{a \in A} n_{i,a}^2 \\ &\leq M^2 n - \frac{1}{q} \sum_{i=1}^n \left( \sum_{a \in A} n_{i,a} \right)^2 = M^2 r n \end{aligned}$$

nach der Cauchy-Schwarz-Ungleichung und die Behauptung folgt.  $\square$

## Griesmer Schranke

**Satz 13** Für einen  $[n, k, d]$ -Code gilt:

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil.$$

Beweis: Induktion über  $k$ : Der Fall  $k = 1$  ist trivial.

Sei  $k > 1$  und  $\mathbf{c}$  ein Codewort mit minimalem Gewicht. OBdA. nehmen wir  $\mathbf{c} = (1, 1, \dots, 1, 0, 0, \dots, 0)$  an. Sei  $C'$  der Code, den man aus den Codewörtern von  $C$  erhält, wenn man die ersten  $d$  Koordinaten streicht.  $C'$  hat Länge  $n' := n - d$ . Die obige Streichungsabbildung von  $C$  in  $C'$  ist linear und ihr Kern ist der 1-dimensionale Raum  $\langle \mathbf{c} \rangle$ . (Wäre  $\mathbf{v}$  im Kern aber nicht in  $\langle \mathbf{c} \rangle$ , so wäre  $\mathbf{v} - v_i \mathbf{c} \in C$ , wobei  $v_i \neq 0$  mit geeignetem  $i$ . Dieser Vektor hat aber Gewicht  $< d$ .) Nach dem Bild-Kern-Satz ist also  $k' := \dim C' = k - 1$ .

Weiterhin zeigen wir:  $d' := w(C') \geq \lfloor d/q \rfloor$ .

Sei  $\mathbf{0} \neq \mathbf{x}' \in C'$  und  $\mathbf{x} \in C$  ein zugehöriges Wort vor der Streichung. Dann

gibt es ein  $a \in \mathbb{F}_q$ , so dass  $(x_1, \dots, x_d)$  mindestens  $d/q$  Koordinaten gleich  $a$  hat (Schubfachprinzip). Somit gilt

$$d \leq w(\mathbf{x} - a\mathbf{c}) \leq d - \frac{d}{q} + w(\mathbf{x}')$$

und  $d' \geq \lceil d/q \rceil$  folgt.

Nach Induktionsvoraussetzung gilt:

$$n - d = n' \geq \sum_{i=0}^{k'-1} \left\lceil \frac{d'}{q^i} \right\rceil \geq \sum_{i=0}^{k-2} \left\lceil \frac{d}{q^{i+1}} \right\rceil,$$

woraus die Behauptung folgt. □

Beispiel: 1.  $q = 2$ ,  $n = 13$ ,  $d = 5$ .

Gilbert-Varshamov:  $A_2(13, 5) \geq 8$

Kugelpackung:  $A_2(13, 5) \leq 89$

Singleton:  $A_2(13, 5) \leq 512$

Plotkin: nicht direkt anwendbar.

Griesmer:  $B_2(13, 5) \leq 64$

2.  $q = 2$ ,  $n = 9$ ,  $d = 5$ .

Gilbert-Varshamov:  $A_2(9, 5) \geq 2$

Kugelpackung:  $A_2(9, 5) \leq 11$

Singleton:  $A_2(9, 5) \leq 32$

Plotkin:  $A_2(9, 5) \leq 10$

Griesmer:  $B_2(9, 5) \leq 4$

## Aufgaben

1. Beweise  $A_q(n, d) \leq qA_q(n-1, d)$ .
2. Liste alle Elemente folgender Kugeln in  $\mathbb{F}_2^n$  auf:
  - a)  $K_4(110)$ ,   b)  $K_3(1100)$ ,   c)  $K_2(10101)$ .
3. Vergleiche für  $9 \leq n \leq 16$  die Singleton, Plotkin und Kugelpackungsschranke für  $A_2(n, 9)$ .

# Kapitel 7

## Hadamard-Matrix Codes

**Definition 27** Eine Hadamard-Matrix der Ordnung  $n$  ist eine  $(n \times n)$ -Matrix mit Einträgen  $1$  und  $-1$ , für die  $HH^T = nE_n$  gilt.

Beispiele:  $(1)$ ,  $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ ,  $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$

**Hilfssatz 22** Sei  $H$  eine Hadamard-Matrix der Ordnung  $n > 2$ , so ist  $n$  durch  $4$  teilbar.

Beweis: O.B.d.A. sei die erste Zeile von  $H$  gleich

$$11 \dots 1,$$

die zweite

$$\underbrace{1 \dots 1}_{n/2} \underbrace{-1 \dots -1}_{n/2}$$

und die dritte

$$\underbrace{\underbrace{1 \dots 1}_x \underbrace{-1 \dots -1}_{n/2-x} \underbrace{1 \dots 1}_y \underbrace{-1 \dots -1}_{n/2-y}}_{n/2}$$

Wegen  $HH^T = nE_n$  ergibt sich  $x+y = n/2$  und  $x+n/2-y = n/2$  also  $x = n/4$ .  $\square$

**Satz 14** Gibt es eine Hadamard-Matrix der Ordnung  $4d$ , so gilt:

$$A_2(4d, 2d) = 8d \quad \text{und} \quad A_2(4d-1, 2d) = 4d.$$

Beweis: Sei  $H$  eine Hadamard-Matrix der Ordnung  $4d$ . Die  $4d$  Zeilen von  $H$  sind Vektoren in  $\{-1, 1\}^{4d}$  und je zwei dieser Vektoren haben Hamming-Abstand  $2d$ . Dasselbe gilt für die Vektoren, die man aus den Zeilen von  $H$  durch Multiplikation mit  $-1$  erhält. Jeder der ersten  $4d$  Vektoren hat zu jedem der zweiten  $4d$  Vektoren Abstand  $2d$  oder  $4d$  und es gilt  $A_2(4d, 2d) \geq 8d$ .

Nach Aufgabe 1 in Kapitel 6 folgt  $2A_2(4d - 1, 2d) \geq A_2(4d, 2d) \geq 8d$  und nach der Plotkin-Schranke  $A_2(4d - 1, 2d) \leq 4d$  und somit die Gleichheit.  $\square$

**Satz 15** *Ist  $q+1$  durch 4 teilbar, so existiert eine Hadamard-Matrix der Ordnung  $q+1$ .*

Beweis: Sei  $\chi$  der quadratische Charakter von  $\mathbb{F}_q$ . Wir definieren eine  $q \times q$ -Matrix  $Q = (q_{x,y})_{x,y \in \mathbb{F}_q}$  durch  $q_{x,y} := \chi(y - x)$ .  $H$  entsteht durch Ersetzen der Einträge 0 durch  $-1$  und durch Anfügen einer Zeile und einer Spalte mit sämtlichen Einträgen 1.  $H$  ist dann eine Hadamard-Matrix nach Hilfssatz 9.  $\square$

Ist  $q - 1$  durch 4 teilbar, so kann man zeigen, dass eine Hadamard-Matrix der Ordnung  $2(q + 1)$  existiert. Man vermutet, dass Hadamard-Matrizen für jede durch 4 teilbare Ordnung existieren.

## Aufgaben

1. Konstruiere einen binären  $(4, 8, 2)$ -Code und einen binären  $(3, 4, 2)$ -Code.
2. Gib eine Hadamard-Matrix der Ordnung 12 explizit an.

# Kapitel 8

## Zyklische Codes

**Definition 28** Ein Linearcode  $C$  über  $\mathbb{F}_q$  heißt zyklisch, wenn mit  $(a_0, \dots, a_{n-1}) \in C$  auch  $(a_{n-1}, a_0, \dots, a_{n-2}) \in C$  gilt.

Im folgenden identifizieren wir Vektoren über  $\mathbb{F}_q$  mit Polynomen mittels folgender Abbildung:

$$\pi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q[X]/(X^n - 1), \quad (a_0, a_1, \dots, a_{n-1}) \mapsto a_0 + a_1X + \dots + a_{n-1}X^{n-1}.$$

**Definition 29** Sei  $R$  ein kommutativer Ring. Eine nichtleere Teilmenge  $I$  von  $R$  heißt Ideal, wenn

$$a + b, a - b \in I, \quad a, b \in I,$$

und

$$ra \in I, \quad a \in I, r \in R.$$

Ein Ideal heißt Hauptideal, wenn es ein  $g \in R$  mit  $I = (g) := \{gr : r \in R\}$  gibt. Ein Ring heißt Hauptidealring, wenn jedes Ideal ein Hauptideal ist.

**Hilfssatz 23** Die Ringe  $\mathbb{F}_q[X]$  und  $\mathbb{F}_q[X]/(X^n - 1)$  sind Hauptidealringe.

Beweis: Sei  $I \neq \{0\}$  ein Ideal in  $\mathbb{F}_q[X]$  und  $0 \neq g(X) \in I$  ein Polynom kleinsten Grades in  $I$ . Sei  $f(X) \in I$ , so gilt (Polynomdivision)

$$f(X) = s(X)g(X) + r(X)$$

mit einem Polynom  $r(X)$  mit  $\text{grad}(r) < \text{grad}(g)$ . Da  $s(X)g(X)$  und somit  $r(X) = f(X) - s(X)g(X)$  in  $I$  liegen muss  $r(X) = 0$  gelten, da der Grad von  $g(X)$  minimal ist.

Dieselben Argumente gelten auch für  $\mathbb{F}_q[X]/(X^n - 1)$ . □

**Satz 16**  $C \subseteq \mathbb{F}_q^n$  ist genau dann ein zyklischer Code, wenn  $\pi(C)$  ein Ideal in  $\mathbb{F}_q[X]/(X^n - 1)$  ist.

Beweis: Sei  $\pi(C)$  ein Ideal, dann gilt

$$af(X) + bg(X) \in \pi(C), \quad a, b \in \mathbb{F}_q, f(X), g(X) \in \pi(C)$$

und  $C$  ist ein Linearcode.

Für  $f(X) = a_0 + a_1 + \dots + a_{n-1}X^{n-1} \in \pi(C)$  ist stets auch  $Xf(X) = a_0X + a_1X^2 + \dots + a_{n-2}X^{n-1} + a_{n-1} \in \pi(C)$  und  $C$  ist zyklisch.

Sei umgekehrt  $C$  ein zyklischer Code. Dann gilt  $af(x), f(X) \pm g(X) \in \pi(C)$  für alle Polynome  $f(X), g(X) \in \pi(C), a \in \mathbb{F}_q$ . Für jedes Polynom  $f(X) = a_0 + \dots + a_{n-1}X^{n-1} \in \pi(C)$  liegen auch  $Xf(X), X^2f(X), \dots$  in  $\pi(C)$  und somit alle Linearkombinationen, d.h.  $f(X)h(X) \in \pi(C), h(X) \in \mathbb{F}_q[X]/(X^n - 1)$ .  $\square$

**Hilfssatz 24** Sei  $I \neq \{0\}$  ein Ideal in  $\mathbb{F}_q[X]/(X^n - 1)$  und  $g(X) \neq 0$  ein normiertes Polynom mit kleinstem Grad in  $I$ . Dann gilt  $I = (g(X))$  und  $g(X)$  teilt  $X^n - 1$ .

Beweis: Der erste Teil folgt aus dem Beweis von Hilfssatz 23.

Weiterhin gilt

$$X^n - 1 = s(X)g(X) + r(X)$$

mit  $\text{grad}(r) < \text{grad}(g)$  und wegen  $r(X) \in I$  folgt  $r(X) = 0$ , da mit  $r(X)$  auch das zugehörige normierte Polynom in  $I$  ist.  $\square$

**Satz 17** Es existiert genau ein normiertes Polynom  $g(X)$  kleinsten Grades in jedem Ideal  $I \neq (0)$  von  $\mathbb{F}_q[X]/(X^n - 1)$ , für das  $I = (g(X))$  gilt.

Beweis: Seien  $g_1(X)$  und  $g_2(X)$  zwei normierte Polynome kleinsten Grades in  $I$ . Dann ist  $g_1(X) - g_2(X)$  ein Polynom kleineren Grades in  $I$ , also das Nullpolynom.  $\square$

**Definition 30** Das eindeutige normierte Polynom kleinsten Grades in einem Ideal  $I \neq (0)$  von  $\mathbb{F}_q[X]/(X^n - 1)$  heißt Generatorpolynom von  $I$  bzw. von  $C$ , wenn  $I = \pi(C)$ .

**Satz 18** Jeder normierte Teiler von  $X^n - 1$  ist Generatorpolynom eines zyklischen Codes von  $\mathbb{F}_q^n$ .

Beweis: Sei  $g(X)$  ein normierter Teiler von  $X^n - 1$  und  $I = (g(X))$  und  $C$  der zugehörige zyklische Code. Sei  $h(X)$  Generatorpolynom von  $C$ , so existiert ein Polynom  $b(X)$  mit

$$h(X) = g(X)b(X) + r(X)(X^n - 1) = g(X)b(X) \in \mathbb{F}_q[X]/(X^n - 1).$$

$g(X)$  teilt also  $h(X)$ . Da  $h(X)$  minimalen Grad hat, muss  $g(X) = h(X)$  gelten.  $\square$

Es existiert also eine 1-1-Korrespondenz zwischen den zyklischen Codes von  $\mathbb{F}_q^n$  und den normierten Teilern von  $X^n - 1 \in \mathbb{F}_q[X]$ .

Beispiel:  $X^6 - 1 \in F_2[X]$ .

$$X^6 - 1 = (1 + X)^2(1 + X + X^2)^2$$

$$1, 1 + X, 1 + X + X^2, (1 + X)^2, (1 + X)(1 + X + X^2), (1 + X)^2(1 + X + X^2), \\ (1 + X + X^2)^2, (1 + X)(1 + X + X^2)^2, (1 + X)^2(1 + X + X^2)^2$$

sind alle Teiler von  $X^6 - 1$  über  $\mathbb{F}_2$ . Es existieren also 9 verschiedene zyklische Codes.

Z.B. zu  $(1 + X + X^2)^2 = (1 + X^2 + X^4)$  gehört

$$C = \{000000, 101010, 010101, 111111\}.$$

**Hilfssatz 25** Habe  $X^n - 1 \in \mathbb{F}_q[X]$  die Faktorisierung

$$X^n - 1 = \prod_{i=1}^r p_i^{e_i}(X),$$

mit paarweise verschiedenen über  $\mathbb{F}_q$  irreduziblen Polynomen  $p_i(X)$ ,  $i = 1, \dots, r$ . Dann existieren

$$\prod_{i=1}^r (e_i + 1)$$

zyklische Codes der Länge  $n$  über  $\mathbb{F}_q$ .

**Satz 19** Sei  $g(X)$  Generatorpolynom des zyklischen Codes  $C$ , so gilt

$$\dim(C) = n - \text{grad}(g).$$

Beweis: Setze  $k := n - \text{grad}(g)$ . Die Menge

$$A := \{c(X)g(X) : c(X) \in \mathbb{F}_q[X]/(X^n - 1), \text{grad}(c) \leq k - 1\}$$

hat  $q^k$  Elemente. Weiterhin läßt sich jedes Codewort  $a(X)g(X)$  mit  $a(X) \in \mathbb{F}_q[X]/(X^n - 1)$  als

$$a(X)g(X) = u(X)(X^n - 1) + v(X)$$

mit  $\text{grad}(v) < n$  schreiben und  $g(X)$  teilt  $v(X)$ , d.h.  $v(X) = b(X)g(X)$  für ein Polynom  $b(X)$  mit  $\text{grad}(b) \leq k - 1$ . Wir haben also  $(g) = A$  und  $\dim(C) = k$ .  $\square$

**Satz 20** Sei  $g(X) = g_0 + g_1X + \dots + g_{n-k}X^{n-k}$  Generatorpolynom des zyklischen Codes  $C$  der Länge  $n$ , dann ist

$$G = \begin{pmatrix} g(X) \\ Xg(X) \\ \vdots \\ X^{k-1}g(X) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & 0 \\ \vdots & \vdots & & & & & & \vdots \\ 0 & 0 & \dots & 0 & g_0 & g_1 & \dots & g_{n-k} \end{pmatrix}$$

Generatormatrix von  $C$ .

Beweis: Die Polynome  $g(X), Xg(X), \dots, X^{k-1}g(X)$  bilden eine Basis von  $\pi(C)$ .  $\square$

**Definition 31** Sei  $h(X) = h_0 + h_1X + \dots + h_kX^k$ ,  $h_k \neq 0$ . Dann heißt das Polynom

$$h_R(X) := X^k h(1/X) = h_k + h_{k-1}X + \dots + h_0X^k$$

das reziproke Polynom von  $h(X)$ .

**Satz 21** Ist  $g(X)$  Generatorpolynom eines zyklischen  $[n, k]$ -Codes  $C$  und setze  $h(X) := (X^n - 1)/g(X) = h_0 + \dots + h_kX^k$ . Dann ist  $h_0^{-1}h_R(X)$  Generatorpolynom von  $C^\perp$ .

Beweis: Sei  $g(X) = g_0 + g_1X + \dots + g_{n-1}X^{n-1}$  und  $h(X) = h_0 + h_1X + \dots + h_{n-1}X^{n-1}$  und somit  $h_R(X) = h_k + h_{k-1}X + \dots + h_0X^k$ . (Wir haben  $g_{n-k+1} = \dots = g_{n-1} = 0$  und  $h_{k+1} = \dots = h_{n-1} = 0$ .) In  $\mathbb{F}_q[X]/(X^n - 1)$  gilt:

$$\begin{aligned} 0 &= X^n - 1 = g(X)h(X) \\ &= (g_0h_0 + g_1h_{n-1} + \dots + g_{n-1}h_1) + (g_0h_1 + g_1h_0 + \dots + g_{n-1}h_2)X + \dots \\ &\quad + (g_0h_{n-1} + g_1h_{n-2} + \dots + g_{n-1}h_0)X^{n-1}. \end{aligned}$$

Koeffizientenvergleich liefert, dass  $(h_{n-1}, \dots, h_0)$  orthogonal zu allen Zeilen der zu  $g(X)$  gehörenden Generatormatrix ist, d.h.  $(h_{n-1}, \dots, h_0) \in C^\perp$  bzw. in Polynomschreibweise  $X^{n-k-1}h_R(X) \in C^\perp$ . Genauso erhält man  $h_0^{-1}X^i h_R(X) \in C^\perp$ ,  $i = 0, 1, \dots, n - k - 1$ , und diese linear unabhängigen Polynome bilden wegen  $\dim(C^\perp) = n - k$  eine Basis von  $C^\perp$ . D.h.  $h_0^{-1}h_R(X)$  ist Generatorpolynom von  $C^\perp$ .  $\square$

**Definition 32** Das Polynom  $h_0^{-1}h_R(X)$  wird Kontrollpolynom von  $C$  genannt.

Beispiel: Sei  $C$  der binäre Code der Länge 7 mit Generatorpolynom  $g(X) = 1 + X^2 + X^3$ . Dann ist  $h(X) = (X^7 - 1)/g(X) = 1 + X^2 + X^3 + X^4$  und  $h_R(X) = 1 + X + X^2 + X^4$ . Die Kontrollmatrix ist

$$H = \begin{pmatrix} 1110100 \\ 0111010 \\ 0011101 \end{pmatrix}.$$

$C$  ist der  $[7, 4]$ -Hamming Code.

## Decodierung

Wir können aus einer Kontrollmatrix der Form

$$H' = \begin{pmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_0 & 0 & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_0 \end{pmatrix}$$

durch elementare Zeilenoperationen eine Kontrollmatrix der Form  $H = (E_{n-k}|A)$  bekommen.

**Satz 22** Sei  $H = (E_{n-k}|A)$  eine Kontrollmatrix des zyklischen Codes  $C$  über  $\mathbb{F}_q$  und  $g(X)$  ein Generatorpolynom von  $C$ . Dann ist das Syndrom  $S(v(X))$  des Polynoms  $v(X) \in \mathbb{F}_q[X]/(X^n - 1)$  das eindeutig bestimmte Polynom  $r(X)$  mit

$$v(X) = g(X)u(X) + r(X), \quad \text{grad}(r) < \text{grad}(g).$$

Beweis: Wir identifizieren die  $i$ te Spalte von  $A$  mit einem Polynom  $a_i(X)$  vom Grad kleiner als  $n - k$  und schreiben

$$A = (a_0(X), a_1(X), \dots, a_{k-1}(X)).$$

$G = (-A^T|E_k)$  ist Generatormatrix von  $C$  und somit  $X^{n-k+i} - a_i(X) \in C$ , d.h.

$$a_i(X) = X^{n-k+i} - q_i(X)g(X), \quad i = 0, 1, \dots, k-1,$$

für ein  $q_i(X)$ . Sei  $v(X) = v_0 + v_1X + \dots + v_{n-1}X^{n-1}$  dann gilt

$$\begin{aligned} S(v(X)) &= v_0 + v_1X + \dots + v_{n-k-1}X^{n-k-1} + v_{n-k}a_0(X) + \dots + v_{n-1}a_{k-1}(X) \\ &= v(X) - \left( \sum_{j=0}^{k-1} v_{n-k+j}q_j(X) \right) g(X). \end{aligned}$$

Die Behauptung folgt, da der Grad von  $S(v(X))$  höchstens  $n - k - 1 < \text{grad}(g)$  ist.  $\square$

Beispiel: Sei  $C$  der  $[7, 4]$ -Hamming Code mit Generatorpolynom  $g(X) = 1 + X^2 + X^3$ . Wir erhalten eine Kontrollmatrix der Form  $H = (E_3|A)$  mit

$$A = \begin{pmatrix} 1110 \\ 0111 \\ 1101 \end{pmatrix}.$$

Sei  $\mathbf{v} = 0110110$ . Das zugehörige Syndrom ist  $\mathbf{s} = \mathbf{v}H^T = 010$ . Andererseits gilt

$$v(X) = X + X^2 + X^4 + X^5 = X^2g(X) + X$$

und  $S(v(X)) = X$ .

**Hilfssatz 26** Ist das Gewicht von  $S(v(X))$  höchstens  $\lfloor (d(C) - 1)/2 \rfloor$ , so wird nach Maximum-Likelihood Decodierung  $v(X)$  zu  $v(X) - S(v(X))$  decodiert.

Beweis: Wegen  $v(X) = g(X)u(X) + S(v(X))$  gilt  $v(X) - S(v(X)) \in C$ , d.h.  $v(X)$  und  $S(v(X))$  liegen in derselben Nebenklasse von  $C$ . Wegen  $w(S(v(X))) \leq \lfloor (d(C) - 1)/2 \rfloor$  ist  $S(v(X))$  Nebenklassenführer nach Hilfssatz 17.  $\square$

**Hilfssatz 27** Sei  $s(X) = s_0 + s_1X + \dots + s_{n-k-1}X^{n-k-1}$  das Syndrom von  $v(X)$ , so ist das Syndrom von  $Xv(X)$  gleich  $Xs(X) - s_{n-k-1}g(X)$ .

Beweis: Sei  $v(X) = q(X)g(X) + s(X)$  und somit

$$Xv(X) = Xq(X)g(X) + Xs(X) = (Xq(X) + s_{n-k-1})g(X) + (Xs(X) - s_{n-k-1}g(X)).$$

Die Behauptung folgt nach Satz 22, da der Grad von  $Xs(X) - s_{n-k-1}g(X)$  kleiner als der Grad von  $g(X)$  ist.  $\square$

Beispiel: Wir setzen das Beispiel vor den beiden Hilfssätzen fort. Die Syndrome von  $Xv(X)$  und  $X^2v(X)$  sind  $X^2$  und  $X^3 - g(X) = 1 + X^2$ .

Algorithmus:

1. Berechne die Syndrome  $s_i(X)$  von  $X^i v(X)$ ,  $i = 1, 2, \dots$
2. Finde  $m$ , so dass das Gewicht von  $s_m(X)$  höchstens  $\lfloor (d(C) - 1)/2 \rfloor$  ist.
3. Berechne  $e(X)$  mit  $\text{grad}(e) < n$  und  $X^{n-m}s_m(X) = (X^n - 1)q(X) + e(X)$ .
4. Decodiere  $v(X)$  zu  $v(X) - e(X)$ .

**Hilfssatz 28** Sind bei der Übermittlung eines Wortes maximal  $\lfloor (d(C) - 1)/2 \rfloor$  Fehler aufgetreten, sind wenigstens  $k$  zyklisch aufeinanderfolgende Zeichen richtig übermittelt worden und ist  $v(X)$  das empfangene Wort, so existiert ein  $s_m(X)$  mit Gewicht höchstens  $\lfloor (d(C) - 1)/2 \rfloor$  und der Algorithmus liefert das gesendete Wort  $v(X) - e(X)$ .

Beweis: Nach Voraussetzung hat  $e(X)$  wenigstens  $k$  zyklisch aufeinanderfolgende Koeffizienten gleich 0 und Gewicht höchstens  $\lfloor (d(C) - 1)/2 \rfloor$ . Daher existiert ein  $m$ , so dass  $s_m(X) = X^m e(X) \in \mathbb{F}_q[X]/(X^n - 1)$  höchstens den Grad  $n - k - 1$  hat. Dieses Polynom erfüllt aber dann  $X^m v(X) = X^m g(X)q(X) + s_m(X)$  und ist daher Syndrom von  $X^m v(X)$ .

Wegen  $v(X) = g(X)q(X) + X^{n-m}s_m(X)$  sind  $v(X)$  und  $e(X)$  in derselben Nebenklasse und  $e(X)$  ist wegen der Gewichtsbedingung ein Nebenklassenführer.  $\square$

## Aufgaben

1. Zeige, dass der Ring der ganzen Zahlen  $\mathbb{Z}$  ein Hauptidealring ist.
2. a) Zeige, dass  $X^6 + X^3 + 1$  ein über  $\mathbb{F}_2$  irreduzibler Teiler von  $X^9 - 1$  ist.  
b) Bestimme aus der Faktorisierung von  $X^9 - 1$  über  $\mathbb{F}_2$  die Anzahl der binären zyklischen Codes der Länge 9.  
c) Gib zu jedem dieser Codes Generator- und Kontrollpolynom an.
3. Sei  $g(X) = X^4 + X + 1$  Generatorpolynom eines binären zyklischen Codes  $C$  der Länge 15. Bestimme die Dimension von  $C$  und gib eine Generator- und eine Kontrollmatrix von  $C$  an.

# Kapitel 9

## BCH-Codes

### Minimalpolynome

**Definition 33** Ein Minimalpolynom eines Elementes  $\alpha \in \mathbb{F}_{q^m}$  über  $\mathbb{F}_q$  ist ein normiertes Polynom  $0 \neq f(X) \in \mathbb{F}_q[X]$  kleinsten Grades mit  $f(\alpha) = 0$ .

**Hilfssatz 29** Das Minimalpolynom von  $\alpha \in \mathbb{F}_{q^m}$  über  $\mathbb{F}_q$  existiert, ist eindeutig und irreduzibel über  $\mathbb{F}_q$ .

Beweis: Ein Element  $\alpha \in \mathbb{F}_{q^m}$  ist Nullstelle von  $X^{q^m} - X$ , woraus die Existenz folgt.

Seien  $M_1(X)$  und  $M_2(X)$  zwei Minimalpolynome von  $\alpha$ . Dann gilt  $M_1(X) = M_2(X)u(X) + r(x)$  mit einem  $r(X)$  vom Grad kleiner  $\text{grad}(M_2)$ . Wegen  $r(\alpha) = M_1(\alpha) - M_2(\alpha)u(\alpha) = 0$  muss  $r(X) = 0$  nach Definition des Minimalpolynoms gelten. D.h.  $M_2(X)$  teilt  $M_1(X)$  und analog erhält man, dass  $M_1(X)$  auch  $M_2(X)$  teilt, woraus  $M_1(X) = M_2(X)$  folgt.

Sei das Minimalpolynom  $M(X)$  von  $\alpha$  reduzibel über  $\mathbb{F}_q$ , d.h. es existieren nicht konstante Polynome  $f(X), g(X) \in \mathbb{F}_q[X]$  mit  $M(X) = f(X)g(X)$ . Dann gilt  $M(\alpha) = f(\alpha)g(\alpha)$  und daher  $f(\alpha) = 0$  oder  $g(\alpha) = 0$  im Widerspruch zur Minimalität des Grades von  $M(X)$ .  $\square$

Sei  $f(X)$  ein normiertes Polynom über  $\mathbb{F}_q$  mit  $f(\alpha) = 0$ , so ist das Minimalpolynom  $M(X)$  von  $\alpha$  ein Teiler von  $f(X)$  und daher  $\text{grad}(M) \leq \text{grad}(f)$ .

Falls  $M(\alpha) = 0$  für ein irreduzibles normiertes Polynom  $M(X) \in \mathbb{F}_q[X]$  gilt, so ist  $M(X)$  Minimalpolynom von  $\alpha$ .

Beispiele: 1.  $X - a$  ist Minimalpolynom von  $a \in \mathbb{F}_q$  über  $\mathbb{F}_q$ .

2.  $\mathbb{F}_9 = \mathbb{F}_3/(x^2 + 1)$ :  $X^2 + 1$  ist Minimalpolynom von  $x$  und  $2x$ ,  $X^2 + X + 2$  ist Minimalpolynom von  $x + 1$  und  $2x + 1$  und  $X^2 + 2X + 2$  ist Minimalpolynom  $x + 2$  und  $2x + 2$ .

**Definition 34** Seien  $n$  und  $q$  teilerfremd. Die  $i$ te Kreisteilungsklasse von  $q$  modulo  $n$  ist

$$C_i := \{iq^j \in \mathbb{Z}_n : j = 0, 1, \dots\}.$$

Beispiel: Kreisteilungsklassen von 2 modulo 15:

$$\begin{aligned} C_0 &= \{0\}, C_1 = \{1, 2, 4, 8\} (= C_2 = C_4 = C_8), \\ C_3 &= \{3, 6, 12, 9\} (= C_6 = C_9 = C_{12}), C_5 = \{5, 10\} (= C_{10}), \\ C_7 &= \{7, 14, 13, 11\} (= C_{11} = C_{13} = C_{14}). \end{aligned}$$

**Satz 23** Sei  $\alpha$  ein primitives Element von  $\mathbb{F}_{q^m}$ . Dann ist das Minimalpolynom  $M^{(i)}(X)$  von  $\alpha^i$  über  $\mathbb{F}_q$  gleich

$$M^{(i)}(X) = \prod_{j \in C_i} (X - \alpha^j),$$

wobei  $C_i$  die  $i$ te Kreisteilungsklasse von  $q$  modulo  $q^m - 1$  ist.

Beweis: Da  $i \in C_i$  ist  $\alpha^i$  Nullstelle von  $M^{(i)}$ .

Sei  $M^{(i)}(X) = a_0 + a_1X + \dots + a_dX^d$ . Dann gilt

$$a_0^q + a_1^qX + \dots + a_d^qX^d = \prod_{j \in C_i} (X - \alpha^{jq}) = \prod_{j \in C_i} (X - \alpha^j) = M^{(i)}(X).$$

Koeffizientenvergleich liefert  $a_l^q = a_l$ , d.h.  $a_l \in \mathbb{F}_q$ .  $M^{(i)}(X)$  ist also ein Polynom über  $\mathbb{F}_q$ .

Da  $\alpha$  primitives Element ist, sind alle Nullstellen von  $M^{(i)}(X)$  verschieden. Sei jetzt  $f(X) \in \mathbb{F}_q[X]$  ein Polynom mit  $f(\alpha^i) = 0$  und  $j \in C_i$ , d.h.  $j$  ist von der Form  $j = iq^l + k(q^m - 1)$ . Daher gilt

$$f(\alpha^j) = f(\alpha^{iq^l}) = f(\alpha^i)^{q^l} = 0.$$

Daher ist  $M^{(i)}(X)$  ein Teiler von  $f(X)$ .

Die drei Schritte ergeben, dass  $M^{(i)}(X)$  Minimalpolynom von  $\alpha^i$  ist.  $\square$

Beispiel: Sei  $\rho$  ein primitives Element von  $\mathbb{F}_4$ , so ist  $C_1 = \{1, 2\} = C_2$  und  $M^{(1)}(X) = M^{(2)}(X) = (X - \rho)(X - \rho^2) = \rho^3 + (\rho + \rho^2)X + X^2$ . Da  $\rho$  Nullstelle von  $X^3 - 1$  ist aber  $\rho \neq 1$ , ist  $\rho$  auch Nullstelle von  $(X^3 - 1)/(X - 1) = X^2 + X + 1$ . Es gilt also  $\rho^3 = 1$  und  $\rho^2 = \rho + 1$ , woraus  $M^{(1)}(X) = X^2 + X + 1$  folgt.

## BCH-Codes

**Definition 35** Sei  $\alpha$  ein primitives Element von  $\mathbb{F}_{q^m}$  und sei  $M^{(i)}(X)$  das Minimalpolynom von  $\alpha^i$  über  $\mathbb{F}_q$ . Ein BCH-Code (Bose/Chaudhuri/Hocquenghem-Code) über  $\mathbb{F}_q$  der Länge  $n = q^m - 1$  mit vorgegebenem Abstand  $\delta$  ist ein zyklischer Code mit Generatorpolynom

$$g(X) := \text{kgV}(M^{(a)}(X), M^{(a+1)}(X), \dots, M^{(a+\delta-2)}(X)).$$

Im Fall  $a = 1$  heißt solch ein Code BCH-Code im engeren Sinn.

## Dimension

**Satz 24** Die Dimension eines BCH-Codes über  $\mathbb{F}_q$  der Länge  $q^m - 1$  mit vorgegebenem Abstand  $\delta$  ist mindestens  $q^m - 1 - m(\delta - 1)$ .

Beweis: Sei  $S := \bigcup_{i=a}^{a+\delta-2} C_i$ . Dann gilt

$$g(X) = \prod_{i \in S} (X - \alpha^i)$$

und die Dimension des zyklischen Codes ist gleich

$$n - \text{grad}(g) = q^m - 1 - |S| = q^m - 1 - \left| \bigcup_{i=a}^{a+\delta-2} C_i \right| \geq q^m - 1 - \sum_{i=a}^{a+\delta-2} |C_i|.$$

Wegen  $C_i \subseteq \{i, qi, \dots, q^{m-1}i\}$  gilt  $|C_i| \leq m$ , woraus die Behauptung folgt.  $\square$

## Minimalgewicht

**Satz 25** Ein BCH-Code mit vorgegebenem Abstand  $\delta$  hat Minimalabstand mindestens  $\delta$ .

Beweis: Sei  $C$  ein BCH-Code. Angenommen, der Minimalabstand  $d$  von  $C$  wäre kleiner als  $\delta$ . Dann gäbe es ein Codewort  $c(X) = c_0 + c_1X + \dots + c_{n-1}X^{n-1} \in C$  mit Gewicht  $d$  kleiner als  $\delta$ . Dann wäre  $c(X) = u(X)g(X)$  und  $c(\alpha^i) = 0$  für  $i = a, \dots, a + \delta - 2$ . Seien  $c_{l_1}, \dots, c_{l_d}$  die von Null verschiedenen Koeffizienten von  $c(X)$ , so schreibt sich dieses Gleichungssystem als

$$\alpha^{il_1}c_{l_1} + \dots + \alpha^{il_d}c_{l_d} = 0, \quad i = a, \dots, a + d - 1 (\leq a + \delta - 2).$$

Die Determinante der Koeffizientenmatrix (Vandermonde-Matrix)  $(\alpha^{il_j})$  ist

$$\prod_{j=1}^d \alpha^{al_j} \prod_{k>k'} (\alpha^{l_k} - \alpha^{l_{k'}}) \neq 0.$$

Daher hat das Gleichungssystem die eindeutige Lösung  $c_{l_1} = \dots = c_{l_d} = 0$  im Widerspruch zu  $c(X) \neq 0$ .  $\square$

Beispiel: Sei  $\alpha$  eine Nullstelle von  $1 + X + X^3 \in \mathbb{F}_2[X]$  und  $C$  der BCH-Code der Länge 7 mit  $\delta = 4$ ,  $a = 0$  und Generatorpolynom

$$g(X) = \text{kgV}(M^{(0)}(X), M^{(1)}(X), M^{(2)}(X)) = 1 + X^2 + X^3 + X^4.$$

Dann gilt  $w(C) = 4$ .

( $C$  ist identisch mit dem BCH-Code mit  $\delta = 3$ .)

## Reed-Solomon Codes

**Definition 36** Sei  $\alpha$  ein primitives Element von  $\mathbb{F}_q$ ,  $a \geq 0$  und  $2 \leq \delta \leq q - 2$ . Ein BCH-Code der Länge  $n = q - 1$  mit Generatorpolynom

$$g(X) = (X - \alpha^{a+1})(X - \alpha^{a+2}) \cdots (X - \alpha^{a+\delta-1})$$

heißt Reed-Solomon Code.

**Satz 26** Die Reed-Solomon Codes sind MDS-Codes.

Beweis: Wir müssen  $\dim(C) = n - w(C) + 1$  zeigen. Der Grad von  $g(X)$  ist  $\delta - 1$  und somit  $\dim(C) = n - \delta + 1 = q - \delta$ . Weiterhin gilt  $w(C) \geq \delta$  und  $w(C) \leq n - \dim(C) + 1 = \delta$  nach der Singleton-Schranke, also  $w(C) = \delta$ , woraus die Behauptung folgt.  $\square$

## Aufgaben

1. Bestimme die Kreisteilungsklassen von 2 modulo 31.
2. Bestimme für alle binären BCH-Codes im engeren Sinne der Länge 31 Dimension und untere Schranken für das Minimalgewicht.
3. Zeige, dass der duale Code eines Reed-Solomon Codes wieder ein Reed-Solomon Code ist.

# Kapitel 10

## Quadratische Reste Codes

Sei  $p > 2$  eine Primzahl und  $g$  ein primitives Element von  $\mathbb{F}_p$ .

**Definition 37** Ein Element  $r \in \mathbb{F}_p^*$  heißt quadratischer Rest modulo  $p$ , wenn  $r = g^{2i}$  für eine ganze Zahl  $i$ . Anderenfalls heißt  $r$  quadratischer Nichtrest modulo  $p$ .

Die Definition ist unabhängig von der Wahl des primitiven Elementes  $g$ .

Sei

$$Q = \{g^{2i} : i = 0, 1, \dots, (p-3)/2\}$$

die Menge der quadratischen Reste modulo  $p$  und

$$N = \{g^{2i+1} : i = 0, 1, \dots, (p-3)/2\}$$

die Menge der quadratischen Nichtreste modulo  $p$ .

Sei  $l$  eine Primzahl, die quadratischer Rest modulo  $p$  ist. Wähle  $m \geq 1$  so, dass  $l^m - 1$  durch  $p$  teilbar ist. Sei  $\vartheta$  ein primitives Element von  $\mathbb{F}_{l^m}$  und  $\alpha = \vartheta^{(l^m-1)/p}$ . Dann ist die Ordnung von  $\alpha$  gleich  $p$ .

**Hilfssatz 30** Die Polynome

$$g_Q(X) = \prod_{r \in Q} (X - \alpha^r)$$

und

$$g_N(X) = \prod_{n \in N} (X - \alpha^n)$$

sind aus  $\mathbb{F}_l[X]$  und es gilt

$$X^p - 1 = (X - 1)g_Q(X)g_N(X).$$

Beweis: Sei  $g_Q(X) = a_0 + a_1X + \dots + a_kX^k$  mit  $a_i \in \mathbb{F}_{l^m}$  und  $k = (p-1)/2$ . Dann gilt

$$a_0^l + a_1^lX + \dots + a_k^lX^k = \prod_{r \in Q} (X - \alpha^{lr}) = \prod_{r \in Q} (X - \alpha^r) = g_Q(X)$$

und die Koeffizienten von  $g_Q(X)$  sind aus  $\mathbb{F}_l$ . Genauso zeigt man  $g_N(X) \in \mathbb{F}_l[X]$ . Wir haben

$$X^p - 1 = \prod_{i=0}^{p-1} (X - \alpha^i)$$

und die zweite Behauptung folgt wegen  $\mathbb{F}_p = \{0\} \cup Q \cup N$ . □

Beispiel: Sei  $p = 7$ ,  $l = 2$  und  $\alpha$  Nullstelle von  $1 + X + X^3 \in \mathbb{F}_2[X]$ . Dann gilt

$$g_Q(X) = (X - \alpha)(X - \alpha^2)(X - \alpha^4) = 1 + X + X^3$$

und

$$g_N(X) = (X - \alpha^3)(X - \alpha^5)(X - \alpha^6) = 1 + X^2 + X^3.$$

**Definition 38** Seien  $p$  und  $l$  Primzahlen, so dass  $l$  quadratischer Rest modulo  $p$  ist, und  $m \geq 1$  so gewählt, dass  $l^m - 1$  durch  $p$  teilbar ist. Sei  $\vartheta$  ein primitives Element von  $\mathbb{F}_{l^m}$  und  $\alpha = \vartheta^{(l^m-1)/p}$ . Die zyklischen Codes der Länge  $p$  über  $\mathbb{F}_l$  mit Generatorpolynom  $g_Q(X)$  und  $g_N(X)$  heißen quadratische Reste Codes.

Die Dimension der quadratischen Reste Codes ist  $(p+1)/2$ .

**Hilfssatz 31** Die quadratischen Reste Codes  $C_Q = (g_Q(X))$  und  $C_N = (g_N(X))$  der Länge  $p$  über  $\mathbb{F}_l$  sind äquivalent.

Beweis: Sei  $m$  ein quadratischer Nichtrest modulo  $p$ . Dann gilt  $N = mQ$  und  $g_N(X) = g_Q(X^m)$ . D.h. ist  $c(X) = c_0 + c_1X + \dots + c_{p-1}X^{p-1} \in C_Q$ , so ist  $c'(X) = c(X^m) = c_0 + c_1X^m + c_2X^{2m} + \dots + c_{p-1}X^{(p-1)m} \in C_N$ . Da mit  $i$  auch  $im$  alle Elemente von  $\mathbb{F}_p$  durchläuft, durchlaufen in  $\mathbb{F}_l[X]/(X^p - 1)$  die Monome  $X^{im}$ ,  $i = 0, \dots, p-1$ , genau die Monome  $X^i$ ,  $i = 0, \dots, p-1$ . D.h. man bekommt  $c'(X)$  durch eine fixe Koordinatenpermutation aus  $c(X)$ . □

**Satz 27** Ein Codewort  $c(X)$  eines quadratischen Reste Codes der Länge  $p$  mit  $c(1) \neq 0$  hat Gewicht  $w > p^{1/2}$ .

Beweis: Sei  $m \in N$ , dann ist  $c(X)c(X^m) \in C_Q \cap C_N$ . D.h. für ein  $a \in \mathbb{F}_l$  gilt

$$c(X)c(X^m) = ag_Q(X)g_N(X) = a(1 + X + \dots + X^{p-1}).$$

Wegen  $c(1) \neq 0$  ist  $a \neq 0$  und  $c(X)c(X^m)$  hat Gewicht  $p$ . Da  $c(X)$  und  $c(X^m)$  dasselbe Gewicht  $w$  haben, hat  $c(X)c(X^m)$  höchstens das Gewicht  $w^2$  und es gilt

$w^2 \geq p$ . Da  $p$  keine Quadratzahl ist, kann keine Gleichheit gelten.  $\square$

Für binäre quadratische Reste Codes kann man zeigen, dass ein Wort mit geradem Gewicht kein minimales Gewicht haben kann und das Minimalgewicht somit größer als  $\sqrt{p}$  ist.

Beispiel: (Golay-Codes)

Der binäre quadratische Restecode der Länge 23 heißt (*binärer*) *Golay Code*. Der ternäre ( $l = 3$ ) quadratische Restecode der Länge 11 heißt *ternärer Golay Code*. Man kann zeigen, dass die Golay-Codes perfekt sind, d.h. beim binären Golay Code gilt  $d = 7$  und beim ternären  $d = 5$ .

## Aufgaben

1. Zeige, dass 2 genau dann ein quadratischer Rest modulo  $p$  ist, wenn  $p \equiv \pm 1 \pmod{8}$  ist.
2. Für welche Längen  $p < 50$  gibt es binäre quadratische Reste Codes.
3. Bestimme das Minimalgewicht des binären quadratischen Restecodes der Länge 7.

# Kapitel 11

## Goppa Codes

### Verallgemeinerte Reed-Solomon Codes

**Satz 28** Sei  $\alpha$  ein primitives Element von  $\mathbb{F}_q$  und  $2 \leq \delta \leq q - 1$ . Der Reed-Solomon Code mit Generatorpolynom

$$g(X) = (X - \alpha)(X - \alpha^2) \dots (X - \alpha^{\delta-1})$$

ist gleich

$$C := \{(f(1), f(\alpha), \dots, f(\alpha^{q-2})) : f(X) \in \mathbb{F}_q[X], \text{grad}(f) < q - \delta\}.$$

Beweis: Offensichtlich ist  $C$  ein Vektorraum.

Der Vektor  $\mathbf{c} = (f(1), f(\alpha), \dots, f(\alpha^{q-2})) \in C$  läßt sich mit dem Polynom

$$c(X) = \sum_{i=0}^{q-2} f(\alpha^i) X^i \in \mathbb{F}_q[X]/(X^{q-1} - 1)$$

identifizieren. Wir müssen zeigen, dass  $g(X)$  ein Teiler von  $c(X)$  ist, d.h.

$$c(\alpha) = c(\alpha^2) = \dots = c(\alpha^{\delta-1}) = 0.$$

Für  $1 \leq k \leq q - 2$  gilt

$$\sum_{i=0}^{q-2} \alpha^{ik} = \frac{\alpha^{k(q-1)} - 1}{\alpha^k - 1} = 0.$$

Mit  $f(X) = \sum_{j=0}^{q-\delta-1} f_j X^j$  ergibt das für  $1 \leq l \leq \delta - 1$ :

$$c(\alpha^l) = \sum_{i=0}^{q-2} f(\alpha^i) \alpha^{il} = \sum_{j=0}^{q-\delta-1} f_j \left( \sum_{i=0}^{q-2} \alpha^{i(j+l)} \right) = 0.$$

Somit ist  $C$  eine Teilmenge des Reed-Solomon Codes.

Die Abbildung  $f \mapsto (f(1), f(\alpha), \dots, f(\alpha^{q-2}))$  der Polynome vom Grad kleiner  $q - \delta$  in  $C$  ist injektiv. (Der Kern ist trivial, da  $f \neq 0$  höchstens  $q - \delta - 1$  Nullstellen haben kann.) Offensichtlich ist diese Abbildung dann bijektiv und die Dimension von  $C$  gleich  $q - \delta$ , was mit der Dimension des Reed-Solomon Codes übereinstimmt.  $\square$

**Definition 39** Sei  $n \leq q$  und  $\alpha = (\alpha_1, \dots, \alpha_n)$  mit verschiedenen Elementen  $\alpha_i \in \mathbb{F}_q$ ,  $1 \leq i \leq n$ . Sei  $\mathbf{v} = (v_1, \dots, v_n) \in (\mathbb{F}_q^*)^n$ . Für  $k \leq n$  ist der verallgemeinerte Reed-Solomon Code  $GRS_k(\alpha, \mathbf{v})$  definiert als

$$\{(v_1 f(\alpha_1), v_2 f(\alpha_2), \dots, v_n f(\alpha_n)) : f(X) \in \mathbb{F}_q[X], \text{grad}(f) < k\}.$$

**Satz 29** Der verallgemeinerte Reed-Solomon Code  $GRS_k(\alpha, \mathbf{v})$  ist ein MDS-Code.

Beweis: Die Länge ist offensichtlich  $n$  und analog zum Beweis von Satz 28 kann man zeigen, dass die Dimension  $k$  ist. Wir müssen zeigen, dass der Minimalabstand  $n - k + 1$  ist.

Ist  $f(X)$  nicht das Nullpolynom, so hat es höchstens  $\text{grad}(f) < k$  Nullstellen, das zugehörige Codewort hat also Gewicht mindestens  $n - k + 1$  und die Singleton-Schranke liefert das Ergebnis.  $\square$

## Alternantencodes

**Hilfssatz 32 (Unterkörpercodes)** Sei  $C$  ein  $[N, K, D]$ -Code über  $\mathbb{F}_{q^m}$ . Dann ist der Unterkörpercode

$$C' := C|_{\mathbb{F}_q} := C \cap \mathbb{F}_q^N$$

ein  $[n, k, d]$ -Code mit

$$n = N \quad \text{und} \quad k \geq mK - (m - 1)N.$$

Falls  $k \geq 1$  gilt  $d \geq D$ .

Beweis: Der Unterkörpercode ist ein Linearcode über  $\mathbb{F}_q$ , da  $C$  und  $\mathbb{F}_q^N$  Vektorräume über  $\mathbb{F}_q$  sind. Die Länge  $n = N$  ist klar. Für die Dimension gilt

$$\begin{aligned} \dim(C') &= \dim(C \cap \mathbb{F}_q^N) = \dim(C) + \dim(\mathbb{F}_q^N) - \dim(C + \mathbb{F}_q^N) \\ &\geq \dim(C) + \dim(\mathbb{F}_q^N) - \dim(\mathbb{F}_{q^m}^N) = mK + N - mN, \end{aligned}$$

wobei alle Dimensionen als Dimension des Vektorraums über  $\mathbb{F}_q$  zu verstehen sind. Im Fall  $C' \neq \{0\}$  gilt schließlich  $d \geq D$ , da  $C' \subseteq C$ .  $\square$

**Definition 40** Ein Unterkörpercode

$$A_k(\alpha, \mathbf{v}) := GRS_k(\alpha, \mathbf{v})|_{\mathbb{F}_q}$$

eines verallgemeinerten Reed-Solomon Codes über  $\mathbb{F}_{q^m}$  heißt Alternantencode.

**Hilfssatz 33** Der Alternantencode  $A_k(\alpha, \mathbf{v})$  ist ein  $[n, k', d]$ -Code mit

$$mk - (m - 1)n \leq k' \leq k \quad \text{und} \quad d \geq n - k + 1.$$

Beweis: Nach Satz 29 gilt für den verallgemeinerten Reed-Solomon Code  $d = n - k + 1$  und die Behauptung folgt aus Hilfssatz 32.  $\square$

## Goppa Codes

**Definition 41** Sei  $g(Z)$  ein nicht konstantes Polynom in  $\mathbb{F}_{q^m}[Z]$  und  $L := \{\alpha_1, \dots, \alpha_n\}$  eine Teilmenge von  $\mathbb{F}_{q^m}$ , die keine Nullstelle von  $g(Z)$  enthält. Für  $\mathbf{c} = (c_1, \dots, c_n) \in \mathbb{F}_q^n$  sei

$$R_{\mathbf{c}}(Z) := \sum_{i=1}^n \frac{c_i}{Z - \alpha_i}.$$

Der Code

$$\Gamma(L, g) := \{\mathbf{c} \in \mathbb{F}_q^n : R_{\mathbf{c}}(Z) = 0 \in \mathbb{F}_{q^m}[Z]/(g(Z))\}$$

heißt Goppa Code.

Bemerkungen: 1. Wir können  $R_{\mathbf{c}}(Z)$  als Polynom auffassen:

$$R_{\mathbf{c}}(Z) = - \sum_{i=1}^n c_i \frac{g(Z) - g(\alpha_i)}{Z - \alpha_i} g(\alpha_i)^{-1} \in \mathbb{F}_{q^m}[Z]/(g(Z)).$$

Da dieses Polynom kleineren Grad als  $g(Z)$  hat, gilt  $\mathbf{c} \in \Gamma(L, g)$  genau dann, wenn das Polynom  $R_{\mathbf{c}}(Z) = 0$  ist.

2. Goppa Codes sind Linearcodes.

**Hilfssatz 34** Für ein nicht konstantes Polynom  $g(Z)$  vom Grad  $t$  gilt

$$\Gamma(L, g) = \{\mathbf{c} \in \mathbb{F}_q^n : \mathbf{c}H^T = \mathbf{0}\}$$

mit

$$H = \begin{pmatrix} g(\alpha_1)^{-1} & \cdots & g(\alpha_n)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \cdots & \alpha_n g(\alpha_n)^{-1} \\ \vdots & & \vdots \\ \alpha_1^{t-1} g(\alpha_1)^{-1} & \cdots & \alpha_n^{t-1} g(\alpha_n)^{-1} \end{pmatrix}.$$

Beweis: Setze  $g(Z) = \sum_{i=0}^t g_i Z^i$ . Nach der Bemerkung 1 gilt  $\mathbf{c} = (c_1, \dots, c_n) \in \Gamma(L, g)$  genau dann, wenn

$$\sum_{i=1}^n c_i \frac{g(Z) - g(\alpha_i)}{Z - \alpha_i} g(\alpha_i)^{-1} = 0,$$

d.h.

$$\mathbf{c} \in \Gamma(L, g) \Leftrightarrow \mathbf{c}H^T = \mathbf{0}$$

mit

$$\begin{aligned} & H' \\ = & \begin{pmatrix} g_t g(\alpha_1)^{-1} & \cdots & g_t g(\alpha_n)^{-1} \\ (g_{t-1} + \alpha_1 g_t) g(\alpha_1)^{-1} & \cdots & (g_{t-1} + \alpha_n g_t) g(\alpha_n)^{-1} \\ \vdots & & \vdots \\ (g_1 + \alpha_1 g_2 + \cdots + \alpha_1^{t-1} g_t) g(\alpha_1)^{-1} & \cdots & (g_1 + \alpha_n g_2 + \cdots + \alpha_n^{t-1} g_t) g(\alpha_n)^{-1} \end{pmatrix} \\ = & \begin{pmatrix} g_t & 0 & \cdots & 0 \\ g_{t-1} & g_t & \cdots & 0 \\ g_{t-2} & g_{t-1} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ g_1 & g_2 & \cdots & g_t \end{pmatrix} \begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \alpha_1^2 & \cdots & \alpha_n^2 \\ \vdots & & \vdots \\ \alpha_1^{t-1} & \cdots & \alpha_n^{t-1} \end{pmatrix} \begin{pmatrix} g(\alpha_1)^{-1} & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & g(\alpha_n)^{-1} \end{pmatrix}. \end{aligned}$$

Die erste Matrix auf der rechten Seite ist invertierbar und Multiplikation beider Seiten mit dem Inversen dieser Matrix ergibt  $\mathbf{c}H^T = \mathbf{0}$ .  $\square$

**Satz 30** *Der Goppa-Code  $\Gamma(L, g)$  ist der Alternantencode*

$$\Gamma(L, g) = GRS_{n-t}(\alpha, \mathbf{v})|_{\mathbb{F}_q},$$

wobei  $t := \text{grad}(g)$  und  $\mathbf{v} = (v_1, \dots, v_n)$  mit  $v_i = g(\alpha_i) / \prod_{j \neq i}^n (\alpha_i - \alpha_j)$ ,  $1 \leq i \leq n$ .

Beweis: Der Alternantencode ist im Goppacode enthalten, wenn

$$v_1 g(\alpha_1)^{-1} f(\alpha_1) + \cdots + v_n g(\alpha_n)^{-1} f(\alpha_n) = 0$$

für alle Polynome  $f(Z)$  vom Grad kleiner  $n - t$ . Jedes dieser Polynome ist eindeutig durch  $n - 1$  Stützstellen definiert (Lagrange Interpolation):

$$f(Z) = \sum_{i=1}^n f(\alpha_i) \prod_{j \neq i} \frac{Z - \alpha_j}{\alpha_i - \alpha_j}.$$

Wegen  $\text{grad}(f) \leq n - 2$  verschwindet der Koeffizient bei  $Z^{n-1}$ :

$$0 = \sum_{i=1}^n \frac{f(\alpha_i)}{\prod_{j \neq i} (\alpha_i - \alpha_j)} = v_1 g(\alpha_1)^{-1} f(\alpha_1) + \cdots + v_n g(\alpha_n)^{-1} f(\alpha_n).$$

Der verallgemeinerte Reed-Solomon Code hat Kontrollmatrix  $H$ . Daher kann es keinen größeren Code mit dieser Eigenschaft geben und es gilt Gleichheit.  $\square$

**Korollar 1** *Der Goppa-Code  $\Gamma(L, g)$  ist ein  $[n, k, d]$ -Code mit*

$$k \geq n - m \text{grad}(g) \quad \text{und} \quad d \geq \text{grad}(g) + 1.$$

Beispiel: Sei  $q = 2$ ,  $g(Z) = Z$  und  $L = \mathbb{F}_{2^m}^*$ . Dann gilt

$$\Gamma(L, g) = \{\mathbf{c} \in \mathbb{F}_2^{2^m-1} : \mathbf{c}H^T = \mathbf{0}\}$$

mit

$$H = (1, \alpha, \alpha^2, \dots, \alpha^{2^m-2}),$$

wobei  $\alpha$  ein primitives Element von  $\mathbb{F}_{2^m}$  ist. D.h. es handelt sich um einen binären Hamming-Code.

# Kapitel 12

## Überdeckungsradius

**Definition 42** Der Überdeckungsradius  $\rho(C)$  eines Codes  $C \subseteq A^n$  ist

$$\rho(C) := \max_{\mathbf{x} \in A^n} \min_{\mathbf{c} \in C} d(\mathbf{x}, \mathbf{c}).$$

**Hilfssatz 35**  $C$  ist genau dann perfekt, wenn  $d(C) = 2\rho(C) + 1$ .

Allgemein gilt  $\rho(C) \geq \lfloor d(C)/2 \rfloor$ .

Beweis: Sei  $d := d(C)$ .  $C$  ist genau dann perfekt, wenn

$$\bigcup_{\mathbf{c} \in C} K_{\lfloor (d-1)/2 \rfloor}(\mathbf{c}) = A^n,$$

d.h. zu jedem  $\mathbf{x} \in A^n$  gibt es genau ein  $\mathbf{c} \in C$  mit  $\mathbf{x} \in K_{\lfloor (d-1)/2 \rfloor}(\mathbf{c})$ . (Dies ist nur möglich, wenn  $d$  ungerade ist.) Der maximale Abstand von  $\mathbf{x} \in A^n$  zu  $C$  ist  $(d-1)/2$  und daher  $\rho(C) = (d-1)/2$ .

Allgemein gilt

$$\bigcup_{\mathbf{c} \in C} K_{\lfloor (d-1)/2 \rfloor}(\mathbf{c}) \subseteq A^n = \bigcup_{\mathbf{c} \in C} K_{\rho(C)}(\mathbf{c}),$$

woraus die zweite Behauptung folgt, da die Inklusion echt ist, wenn  $d$  gerade ist.  $\square$

Beispiel: Sei  $C = \langle (11 \dots 1) \rangle$  Binärcode der Länge  $n$ . Dann ist  $\rho(C) = \lfloor n/2 \rfloor$  und  $d(C) = n$ .

**Hilfssatz 36** Ist  $C$  ein selbstorthogonaler aber nicht selbstdualer Code, so gilt  $\rho(C) \geq d(C^\perp)$ .

Beweis: Wegen  $C \subsetneq C^\perp$  existiert ein  $\mathbf{c} \in C^\perp \setminus C$ , das somit mindestens den Abstand  $d(C^\perp)$  zu jedem Codewort aus  $C$  hat.  $\square$

**Hilfssatz 37** Sei  $C$  ein  $[n, k]$ -Code und  $H$  eine Kontrollmatrix von  $C$ . Der Überdeckungsradius  $\rho(C)$  ist die kleinste ganze Zahl, so dass jeder  $n - k$ -dimensionale Vektor Linearkombination von höchstens  $\rho(C)$  Spalten von  $H$  ist.

Beweis: Jedes  $\mathbf{y} \in \mathbb{F}_q^{n-k}$  lässt sich als  $\mathbf{y} = \mathbf{x}H^T$  mit einem  $\mathbf{x} \in \mathbb{F}_q^n$  schreiben. Sei  $\mathbf{c} \in C$  ein Codewort mit minimalem Abstand  $d(\mathbf{x}, \mathbf{c}) = r \leq \rho(C)$  und seien  $x_{i_1}, \dots, x_{i_r}$  die Koordinaten von  $\mathbf{x}$ , die nicht mit den Koordinaten von  $\mathbf{c}$  übereinstimmen. Wegen  $\mathbf{c}H^T = \mathbf{0}$  gilt

$$\mathbf{y} = \mathbf{x}H^T = (\mathbf{x} - \mathbf{c})H^T = (x_{i_1} - c_{i_1})\mathbf{s}_{i_1} + \dots + (x_{i_r} - c_{i_r})\mathbf{s}_{i_r},$$

wobei  $\mathbf{s}_i$  die  $i$ te Spalte von  $H$  und  $c_i$  die  $i$ te Koordinate von  $\mathbf{c}$  ist. Jedes  $\mathbf{y} \in \mathbb{F}_q^{n-k}$  ist also Linearkombination von höchstens  $\rho(C)$  Spalten von  $H$ .

Ist umgekehrt  $\mathbf{y} \in \mathbb{F}_q^{n-k}$  Linearkombination von  $r$  Spalten von  $H$ , so existiert  $\mathbf{x} \in \mathbb{F}_q^n$  mit  $\mathbf{y} = \mathbf{x}H^T$  und  $d(\mathbf{x} + \mathbf{c}, \mathbf{c}) = r$  für alle  $\mathbf{c} \in C$ . Lässt sich jedes  $\mathbf{y}$  als Linearkombination von höchstens  $r$  Spalten von  $H$  schreiben, so gilt  $\rho(C) \leq r$ .  $\square$

Sei  $g(X) \in \mathbb{F}_q[X]$  Minimalpolynom eines Elementes  $\alpha$  der Ordnung  $n$  und  $m$  die Ordnung von  $q$  modulo  $n$ , d.h.  $\alpha \in \mathbb{F}_{q^m}$ . Dann hat der zyklische Code mit Generatorpolynom  $g(X)$  die Kontrollmatrix

$$H = (1, \alpha, \alpha^2, \dots, \alpha^{n-1}),$$

wobei die Elemente in  $\mathbb{F}_{q^m}$  als  $m$ -dimensionale Spalten aufgefasst werden.

**Satz 31** *Ist  $g(X) \in \mathbb{F}_q[X]$  Minimalpolynom eines Elementes der Ordnung  $n$  und  $m$  die Ordnung von  $q$  modulo  $n$ , so gilt für den zyklischen Code mit Generatorpolynom  $g(X)$ :*

$$\rho(C) \leq m.$$

Beweis: Die ersten  $m$  Spalten von  $H$  bilden eine Basis von  $\mathbb{F}_{q^m}$  über  $\mathbb{F}_q$  und jedes Element aus  $\mathbb{F}_{q^m}$  ist Linearkombination von höchstens  $m$  Basiselementen. Die Behauptung folgt dann aus Hilfssatz 37.  $\square$

**Satz 32** *Ist  $g(X) \in \mathbb{F}_q[X]$  Minimalpolynom eines Elementes der Ordnung  $n$  und  $m$  die Ordnung von  $q$  modulo  $n$ , so gilt für den zyklischen Code mit Generatorpolynom  $g(X)$ :*

$$\rho(C) \leq \frac{q^m - 1}{n}.$$

Beweis: Sei  $\alpha$  Nullstelle von  $g(X)$ . Wir zeigen, dass jedes Element von  $\mathbb{F}_q^*$  als Summe von höchstens  $(q^m - 1)/n$  Elementen aus  $S := \{1, \alpha, \dots, \alpha^{n-1}\}$  darstellbar ist. Sei

$$S_l := \{\alpha_1 + \dots + \alpha_l \neq 0 : \alpha_1, \dots, \alpha_l \in S\}, \quad l = 1, 2, \dots$$

Ist  $\eta \in S_l \setminus S_{l-1}$  so auch  $\alpha\eta$  für alle  $\alpha \in S$ . Damit gilt entweder  $S_l = S_{l-1} = \mathbb{F}_q^*$  oder  $|S_l| \geq |S_{l-1}| + n$ . Also gilt  $S_l = \mathbb{F}_q^*$  oder  $|S_l| \geq ln$  und somit  $S_{(q^m-1)/n} = \mathbb{F}_q^*$ . Die Behauptung folgt dann aus Hilfssatz 37.  $\square$

Beispiele:

1. Für  $q = 2$  und  $n = 3$  gilt  $m = 2$ . Ist  $\alpha$  ein Element der Ordnung 3, so ist jedes Element von  $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$  Linearkombination von einem Element aus  $\{1, \alpha, \alpha^2\}$  und der Überdeckungsradius ist 1. Satz 31 liefert  $\rho(C) \leq 2$  und Satz 32  $\rho(C) \leq 1$ .
2. Für  $q = 2$  und  $n = 9$  ist  $m = 6$  und Satz 31 liefert die obere Schranke 6, während Satz 32 nur  $\rho(C) \leq 7$  liefert.

# Literaturverzeichnis

- [1] E.R. Berlekamp, Algebraic Coding Theory, McGraw-Hill Book Co., New York, 1968.
- [2] D. Jungnickel, Codierungstheorie, Spektrum Akademischer Verlag GmbH, Heidelberg, 1995.
- [3] S. Ling und C. Xing, An Introduction to Coding Theory, Springer, New York, 2004.  
<http://www.math.nus.edu.sg/~ma3218/>
- [4] J.H. van Lint, Introduction to Coding Theory, Springer, New York, 1982.