XI Codierungstheorie

Inhaltsverzeichnis

47 Lineare Codes **1**
47.1 Einführung 1
47.2 Lineare (binäre) Codes 2
47.3 Binäre Hamming Codes als Beispiele für lineare Codes 6

48 Endliche Körper **8**
48.1 Ringe und Ideale 8
48.2 Restklassenringe 10

49 Zyklische Codes **17**
49.1 Ein Codierer für zyklische Codes 20
49.2 Der Minimalabstand zyklischer Codes 21
49.3 Unvollständiges Decodieren von zyklischen Codes 23
49.4 Reed-Solomon Codes 25
49.5 Codes bei CD-Spielern 27

47 Lineare Codes

47.1 Einführung

Definition 47.1 *(i) Ein* Code *C der Länge N über dem (endlichen) Alphabet A ist eine Teilmenge von A^N.*
(ii) Die Informationsrate *von C ist*

$$r(C) := \frac{1}{N}\log_{|A|}(|C|) = \frac{\log(|C|)}{\log(|A^N|)}.$$

(iii) Sind $x, y \in A^N$, so heißt

$$d(x,y) := |\{i \in \{1,\ldots,N\} \mid x_i \neq y_i\}|$$

der Hamming-Abstand *von x und y.*

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

heißt der Minimalabstand *von C.*

Bemerkung: (i) Für den Hamming-Abstand gilt die Dreiecksungleichung:

$$d(x,y) + d(y,z) \geq d(x,z) \text{ für alle } x,y,z \in A^N$$

(ii) $r(C) = \log_{|A|^N}(|C|) =: r$ erfüllt also $|C| = (|A^N|)^r$.
Beispiel: Sei $A = \{a, b, \ldots, z\}$, $N = 3$ und $C := \{(aaa), (bbb), \ldots, (zzz)\}$. Dann ist $r(C) = \frac{1}{3}\log_{26}(26) = \frac{1}{3}$ und $d(C) = 3$. Der Decodierer kann 1 Übertragungsfehler korrigieren und 2 Fehler erkennen.

Definition 47.2 *Sei $C \subseteq A^N$ ein Code. Ein* minimal distance decoder *MDD ist eine Funktion $f : A^N \to C$ mit*

$$d(f(a), a) = \min\{d(c, a) \mid c \in C\} \text{ für alle } a \in A^N.$$

Satz 47.3 *Sei $C \subseteq A^N$ ein Code, $d := d(C)$, f ein MDD für C.*
(i) Für $e < \frac{d}{2}$ kann der MDD e Übertragungsfehler korrigieren.
(ii) Ist die Anzahl e der Übertragungsfehler $e < d$. so erkennt MDD, daß die Übertragung fehlerhaft ist (decodiert aber nicht notwendig zum richtigen Codewort).
Ist also $a \in A^N$ das empfangene Wort beim Senden von $c \in C$ und sind beim Übertragen $d(a, c) = e$ Fehler aufgetreten, so gilt: Ist $e < \frac{d}{2}$, so ist $f(a) = c$. Ist $e < d$, so ist $a = c$ oder $a \notin C$.

Ziel der Codierungstheorie Finde Codes C mit großem Minimalabstand $d(C)$ und großer Informationsrate $r(C)$.

Definition 47.4 *Zwei Codes C, C' heißen* äquivalent, *falls es eine Umordnung σ von $\{1, \ldots, N\}$ gibt, mit $C' = \{(c_{\sigma(1)}, c_{\sigma(2)}, \ldots, c_{\sigma(N)}) \mid (c_1, \ldots, c_N) \in C\}$.*

47.2 Lineare (binäre) Codes

$A = \{0, 1\}$ mit $1 + 1 = 0$. Dann ist A ein Körper und wird auch mit $A = \mathbb{F}_2$ bezeichnet. A ist ein Beispiel eines endlichen Körpers. Wir werden später sehen, daß es zu jeder Primzahlpotenz $q = p^s$ genau einen endlichen Körper mit q Elementen gibt. Dieser wird mit $\mathbb{F}_q$ bezeichnet.

Definition 47.5 *Sei A ein endlicher Körper und $A^N = \{(a_1, \ldots, a_N) \mid a_1, \ldots, a_N \in A\}$ der Standardvektorraum der Dimension N über A. Eine Teilmenge $C \subseteq A^N$ heißt* linearer Code, *falls C ein Untervektorraum von A^N ist ($C \leq A^N$). Ist $A = \mathbb{F}_2$, so nennen wir C einen* linearen binären Code. *Ist $C \leq A^N$ und $(b_1, \ldots, b_k)$ eine A-Basis von C, (die b_i sind Zeilen) so heißt die Matrix $B \in A^{k \times N}$, deren i-te Zeile gerade b_i ist, eine* Erzeugermatrix *von C.*

Bemerkung 47.6 *Ist $C \leq A^N$ ein linearer Code der Dimension k, so ist $|C| = |A|^k$ und $r(C) = \frac{k}{N}$ die Informationsrate von C. C heißt dann auch ein $[N,k]$-Code oder auch $[N,k,d]$-Code, falls $d = d(C)$.*

Bemerkung Ist A ein Körper, $x, y, z \in A^N$, so gilt $d(x,y) = d(x+z, y+z)$.

Satz 47.7 *Für den Minimalabstand eines linearen Codes C gilt: $d(C) = \min\{d(c,0) \mid c \in C\}$, wo $0 \in C$ der Nullvektor ist. Für $c \in C$ heißt $d(c,0) =: w(c)$ auch das* Gewicht *von c.*

Beweis. $d(c,c') = |\{i \mid c_i \neq c'_i\}| = |\{i \mid c_i - c'_i \neq 0\}| = d(c-c', 0) = w(c-c')$. Ist C ein linearer Code, so gilt $c - c' \in C$ falls $c, c' \in C$. □

Beispiel Der erweiterte Hamming Code e_8

Erzeugermatrix:

$$\begin{array}{cccccccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}$$

Code:

$$\begin{array}{cccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}$$

e_8 ist ein $[8,4,4]$-Code. $r(e_8) = \frac{4}{8}$, $d(e_8) = 4$.

Im Vergleich dazu hat der Wiederholungscode mit Erzeugermatrix

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

auch Informationsrate $\frac{1}{2}$ aber kleineren Minimalabstand 2.
Bemerkung: Jeder lineare Code $C \leq A^N$ ist äquivalent zu einem Code mit Erzeugermatrix der Form $(I_k|P_{N-k})$.

Definition 47.8 *Sei A ein Körper.*
(a) Für $x, y \in A^N$ sei $(x, y) := \sum_{i=1}^{N} x_i y_j \in A$ das Skalarprodukt *zwischen x und y.*
(b) Ist $C \leq A^N$ ein linearer Code, so definieren wir

$$C^\perp := \{x \in A^N \mid (x, c) = 0 \text{ für alle } c \in C\}$$

den dualen Code *zu C.*
(c) C heißt selbstdual*, falls $C = C^\perp$.*

Bemerkung 47.9 *(i) Das Skalarprodukt ist symmetrisch, d.h. für alle $x, y \in A^N$ ist $(x, y) = (y, x)$.*
(ii) Für $a_1, a_2 \in A$ und $x, y_1, y_2 \in A^N$ ist $(x, a_1 y_1 + a_2 y_2) = a_1(x, y_1) + a_2(x, y_2)$ d.h. das Skalarprodukt ist linear.
(iii) Für $x \in A^N$ gilt: $x \in C^\perp \Leftrightarrow (x, b_i) = 0$ für alle $1 \leq i \leq k$ für eine Basis $(b_1, \ldots, b_k)$ von C.
(iv) $C^\perp \leq A^N$ ist ein linearer Teilraum.
(v) Für $C \leq A^N$ gilt $(C^\perp)^\perp = C$.

Beweis. (i) Klar aus der Definition. (ii) Nachrechnen, folgt aus dem Distributivgesetz.
(iii) $\Rightarrow$ ist klar, da $b_i \in C$. $\Leftarrow$ Sei $(x, b_i) = 0$ für alle i. Zu $c \in C$ gibt es $a_1, \ldots, a_k \in A$, mit $c = \sum_{i=1}^{k} a_i b_i$. Dann ist $(x, c) = \sum_{i=1}^{k} a_i (x, b_i) = 0$.
(iv) Zu zeigen ist, daß für $a_1, a_2 \in A$ und $x_1, x_2 \in C^\perp$ die Linearkombination $a_1 x_1 + a_2 x_2 \in C^\perp$ liegt. Sei $c \in C$. Dann ist $(a_1 x_1 + a_2 x_2, c) = a_1(x_1, c) + a_2(x_2, c) = 0$.
(v) Klar ist $C \subseteq (C^\perp)^\perp$. Die Gleichheit folgt, da beide Teilräume gemäß dem nächsten Satz die gleiche Dimension haben. □

Beispiel: Für $C = e_8$ gilt $C^\perp = C$.

Satz 47.10 *Sei $C \leq A^N$ ein linearer Code der Dimension $\dim(C) = k$.*
(i) $\dim(C^\perp) = N - k$.
(ii) Ist $(I_k|P_{N-k})$ eine Erzeugermatrix von C, so ist $(-P_{N-k}^{tr}|I_{N-k})$ eine Erzeugermatrix von $C^\perp$.

Beispiel: $A = \mathbb{F}_2$, $N = 6$, $k = 2$, Erzeugermatrix von C:

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

Dann ist $\dim(C^\perp) = 6 - 2 = 4$ und eine Erzeugermatrix von $C^\perp$ ist:

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

Bemerkung Ist B eine Erzeugermatrix von $C^\perp$, so gilt für alle $x \in A^N$:

$$x \in C \Leftrightarrow x \cdot B^{tr} = 0$$

Eine Matrix $H \in A^{N \times N-k}$ mit der Eigenschaft, daß $x \in C \Leftrightarrow x \cdot H = 0$ für alle $x \in A^N$ heißt Prüfmatrix oder Kontrollmatrix für den Code C.
MDD für lineare Codes Sei $C \leq A^N$ ein linearer Code und $H \in A^{N \times (N-k)}$ eine Prüfmatrix für C. Wird das Codewort $c \in C$ gesendet und fügt der Kanal den Fehlervektor e hinzu, so wird der Vektor $c+e$ empfangen. Gilt $(c+e)H = 0$ (z.B. bei $e = 0$), so ist $c + e \in C$ und jeder MDD f wird $c + e$ zu $f(c + e) = c + e$ decodieren. I.a. ist aber $(c+e)H = cH+eH = 0+eH = v \in A^{N-k}$. Bestimmt man nun für jedes $v \in A^{N-k}$ einen Vektor $a := a_v \in A^N$ möglichst kleinem Gewichts (der vermutliche Fehlervektor), mit $aH = v$ so kann man jedes empfangene Wort $x \in A^N$ mit $xA = v$ zu einem Codewort $c = x - a$ decodieren mit $d(c, x) = w(a)$.

Bemerkung 47.11 *Sei $C \leq A^N$ ein linearer Code und $H \in A^{N \times (N-k)}$ eine Prüfmatrix für C.*
(i) Für $x \in A^N$ heißt $xH \in A^{N-k}$ das Syndrom *von x.*
(ii) Ist $a \in A^N$ mit $aH = s$, so ist die Menge aller Vektoren $x \in A^N$ mit demselben Syndrom gleich

$$H^{-1}(s) := \{x \in A^N \mid xH = s\} = \{a + c \mid c \in C\}.$$

(iii) Für $s \in S$ heißt $a_s \in H^{-1}(s)$ ein minimaler Vertreter, *falls $w(a_s) = \min\{w(x) \mid x \in H^{-1}(s)\}$.*
(iv) Es gilt $A^N = \dot{\cup}_{s \in S} H^{-1}(s)$.
(v) Wählt man für jedes $s \in S$ einen minimalen Vertreter a_s, so ist die Funktion $f : A^N \to C$ definiert durch $f(a) := a - a_s$, falls $aH = s$ ist, ein MDD für C.

Beispiel: $C \leq \mathbb{F}_2^6$, Erzeugermatrix G und Prüfmatrix H:

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

Die Menge der Syndrome ist $\mathbb{F}_2^2$ und eine Menge minimaler Vertreter V ist gegeben als:

$$V = \{a_{00} = (0,0,0,0,0,0), a_{10} = (0,1,0,0,0,0), a_{01} = (0,0,1,0,0,0), a_{11} = (1,0,0,0,0,0)\}.$$

47.3 Binäre Hamming Codes als Beispiele für lineare Codes

Definition 47.12 *Sei $N = 2^r - 1$ für ein $r \in \mathbb{N}$. Sei $H \in \mathbb{F}_2^{N \times r}$ eine Matrix, in deren Zeilen gerade alle Vektoren $x_i \neq 0$ von $\mathbb{F}_2^r$ stehen:*

$$H = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_N \end{pmatrix}$$

Der Code C mit Prüfmatrix H heißt Hamming Code *der Länge N.*

Beispiel: $r = 2 \Rightarrow N = 3$ und

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

Der Hamming-Code hat Dimension 1 und Erzeugermatrix $G = (1, 1, 1)$.
$r = 3 \Rightarrow N = 7$ und

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

Der Hamming Code hat Dimension $4 = 7\text{-}3$ und Erzeugermatrix

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

Satz 47.13 *Ist $N = 2^r - 1$, so gibt es bis auf Äquivalenz genau einen Hamming Code $C = H_N = H_N(2)$ der Länge N. Dieser ist von Dimension $\dim(C) = N - r$ und hat Minimalabstand $d(C) = 3$.*

Beweis. Eindeutigkeit: Umordnen der Zeilen der Prüfmatrix H von C liefert zu C äquivalenten Code. $\dim(C) = N - Rang(H) = N - r$. Zum Minimalabstand: Sei wie oben die i-te Zeile von H mit x_i bezeichnet. Ein Wort $c = (c_1, \ldots, c_N)$ liegt genau dann in C, falls $c_1 x_1 + \ldots + c_N x_N = 0$. Ist nun $c \neq 0$, so ist $w(c) \geq 3$, da je 2 Vektoren x_i linear unabhängig sind. $\square$

Bemerkung 47.14 *Ist $C = H_N(2)$ der Hamming Code der Länge $N = 2^r - 1$, so ist $S = \mathbb{F}_2^r$ die Menge der Syndrome von C gerade die Menge der Zeilen der Prüfmatrix H zusammen mit dem Nullvektor. Ist $x_i \in S - \{0\}$ die i-te Zeile von H, so ist der eindeutig bestimmte minimale Vertreter zu x_i gerade der i-te Einheitsvektor $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ (1 an der i-ten Stelle).*

Definition 47.15 *Ein Code $C \subseteq A^N$ heißt* perfekt, *falls es eine Zahl e gibt, so daß zu jedem $a \in A^N$ genau ein $c \in C$ existiert mit $d(a, c) \leq e$.*

Beispiel: (i) $C = A^N$ ist ein perfekter Code mit $e = 0$.
(ii) Ist $A = \mathbb{F}_2$ und N ungerade, so ist der Wiederholungscode $C = \{(0, \ldots, 0), (1, \ldots, 1)\}$ ein perfekter Code mit $e = \frac{N-1}{2}$.
(iii) Der Hamming Code $H_7(2)$ ist ein perfekter Code mit $e = 1$.

Satz 47.16 *Hamming Codes sind perfekte Codes mit $e = 1$.*

Beweis. Sei C der Hamming Code der Länge $N = 2^r - 1$ mit Prüfmatrix H und $a \in \mathbb{F}_2^N$. Dann gilt entweder $aH = 0$ oder $aH = x_i = e_i H$ ist ein Vektor $\neq 0$ in $\mathbb{F}_2^r$ und damit gleich einer Zeile (der i-ten) von H. D.h. entweder $a \in C$, oder $a - e_i \in C$. Da $d(a - e_i, a) = w(e_i) = 1$ ist, gibt es also zu jedem $a \in \mathbb{F}_2^N$ ein $c \in C$ mit $d(a, c) \leq 1$. Die Eindeutigkeit eines solchen c folgt, da $d(C) = 3$ ist. □

Es gilt: Satz
Ist C ein binärer linearer Code mit $e = 1$, so ist C ein Hamming Code.
Ist C ein binärer linearer Code mit $e > 1$, so ist C ein Wiederholungscode, $C = \{(0 \ldots 0), (1 \ldots 1)\}$ oder C ist der binäre Golay Code $\mathcal{G}_{23}$ der Länge 23 und Dimension 12. Es gilt $d(\mathcal{G}_{23}) = 7$ und $\mathcal{G}_{23}$ ist ein perfekter Code mit $e = 3$. Eine Erzeugermatrix für $\mathcal{G}_{23}$ ist (I_{12}, P) mit

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

Definition 47.17 *Sei A ein Körper und $C \subseteq A^N$ ein Code. Dann ist der* erweiterte Code *$\tilde{C} \subseteq A^{N+1}$ definiert als*

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

Satz 47.18 *Sei $C \leq A^N$ ein linearer Code der Dimension k. Dann gilt* $\dim(\tilde{C}) = k$. *Ist G eine Erzeugermatrix und H eine Prüfmatrix für C, so sind*

$$\tilde{G} := (G|g), \quad \tilde{H} := \begin{pmatrix} & & & 1 \\ & H & & \vdots \\ & & & 1 \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

Erzeugermatrix bzw. Prüfmatrix von $\tilde{C}$, wo $g_k := -\sum_{i=1}^{N} G_{ki}$.

Beispiel: (i) Der erweiterte Hamming Code $\widetilde{H_7(2)} = e_8$.
(ii) $C \leq \mathbb{F}_2^5$, Erzeugermatrix $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}$. Der erweiterte Code ist $\tilde{C} \subseteq \mathbb{F}_2^6$ mit Erzeugermatrix $\tilde{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$. Eine Prüfmatrix für C ist $H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Eine Prüfmatrix für $\tilde{C}$ ist entweder $\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ oder

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

Bemerkung 47.19 *Sei $C \leq \mathbb{F}_2^N$ ein linearer binärer Code und $\tilde{C}$ der erweiterte Code. Dann sind die Gewichte $w(\tilde{c}) \in 2\mathbb{Z}$ gerade für alle $\tilde{c} \in \tilde{C}$. Ist also $d(C)$ ungerade, so ist $d(\tilde{C}) = d(C) + 1$.*

48 Endliche Körper

48.1 Ringe und Ideale

Definition 48.1 *Ein* Ring *(kommutativer Ring mit Einselement) $(R, +, \cdot) = R$ ist eine Menge R mit 2 Verknüpfungen $+, \cdot$, die die folgenden Gesetze erfüllen:*
Ak $x + y = y + x$ *(Kommutativgesetz)*
Aa $(x + y) + z = x + (y + z)$ *(Assoziativgesetz)*
An $\exists 0 \in R$, *so daß*
(i) $x + 0 = x$ *für alle* $x \in R$ *und (ii) für alle* $x \in R$ *gibt es ein* $y \in R$ *mit*

$x + y = 0$
Mk $x \cdot y = y \cdot x$ *(Kommutativgesetz)*
Ma $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ *(Assoziativgesetz)*
Mn $\exists 1 \in R$, *so daß* $x \cdot 1 = x$ *für alle* $x \in R$.
AM $x \cdot (y + z) = x \cdot y + x \cdot z$.

Beispiele: (i) Jeder Körper (also z.B. $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{F}_2$) ist ein Ring, wobei in Körpern zusätzlich jedes Element $\neq 0$ ein multiplikatives Inverses hat.
(ii) $\mathbb{Z}$ ist ein Ring. Es gibt in $\mathbb{Z}$ aber z.B. kein Element a mit $2a = 1$.
(iii) Die Menge der Polynome

$$K[x] = \{\sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N}, a_i \in K\}$$

über einem Körper K (oder allgemeiner über einem Ring) ist ein Ring. Auch hier können wir nicht durch alle Elemente $\neq 0$ teilen.

Definition 48.2 *Sei R ein Ring. Eine Teilmenge $I \subseteq R$ heißt ein* Ideal, *falls gilt*
(i) Für alle $a, b \in I$ liegt auch die Summe $a + b \in I$.
(ii) Für alle $a \in I$ und $r \in R$ gilt $ra \in I$.
In Zeichen $I \trianglelefteq R$.

Beispiele: (i) Ist R ein Ring, so ist $\{0\} \subseteq R$ ein Ideal, das Nullideal. Ebenso ist R selbst ein Ideal in R.
(ii) Die Menge der geraden Zahlen bildet ein Ideal in $\mathbb{Z}$, die Menge der ungeraden Zahlen jedoch nicht.
(iii) Ist $n \in \mathbb{Z}$, so bildet die Menge aller durch n teilbaren Zahlen in $\mathbb{Z}$ ein Ideal.

Bemerkung 48.3 *(i) Ist I ein Ideal in einem Ring R, so gilt*

$$I = R \Leftrightarrow 1 \in I.$$

(ii) Ein Körper K hat genau 2 Ideale, $\{0\}$ und K.
(iii) Ist R ein Ring und $a \in R$, so ist die Menge $\{ar \mid r \in R\}$ ein Ideal von R. Dieses wird mit (a) bezeichnet und heißt das von a erzeugte Hauptideal.

Beweis. (i) $I = R \Rightarrow 1 \in I$ ist klar. Zur anderen Richtung. Sei $1 \in I \trianglelefteq R$. Ist $r \in R$, so gilt $r = r \cdot 1 \in I$ und damit $R \subseteq I$, also $R = I$.
(ii) Sei $I \trianglelefteq K$ mit $I \neq \{0\}$. Dann gibt es $k \in I$ mit $k \neq 0$. Da K ein Körper ist, ist k in K invertierbar, d.h. es gibt $k^{-1} \in K$ mit $k^{-1}k = 1$. Damit ist $1 = k^{-1}k \in I$ und daher $I = K$.
(iii) Klar, (i) und (ii) aus Definition 48.2 nachrechnen. □

48.2 Restklassenringe

Definition 48.4 *Sei R ein Ring und I ein Ideal in R. Für $r \in R$ heißt*

$$\overline{r} := r + I := \{r + i \mid i \in I\}$$

die Restklasse *von r nach I. Die Menge der Restklassen nach I wird mit*

$$R/I := \{r + I \mid r \in R\}$$

bezeichnet.

Beispiel: $R = \mathbb{Z}$, $I = (2) = \{2n \mid n \in \mathbb{Z}\}$. $4 + I = I$ Menge der geraden Zahlen, $7 + I = 1 + I$ Menge der ungeraden Zahlen und $\mathbb{Z}/(2)$ hat genau 2 Elemente $\overline{0}, \overline{1}$.

Bemerkung 48.5 *Es gilt $a \in \overline{b} \Leftrightarrow a - b \in I$. Dafür schreiben wir auch $a \equiv b \pmod{I}$, bzw. $a \equiv b \pmod{p}$, falls $I = (p)$ ein Hauptideal ist.*

Satz 48.6 *Ist $I \trianglelefteq R$ ein Ideal in einem Ring R, so wird R/I zu einem Ring durch $\overline{r_1} + \overline{r_2} := \overline{r_1 + r_2}$ und $\overline{r_1} \cdot \overline{r_2} := \overline{r_1 \cdot r_2}$, der* Restklassenring *von R nach I.*

Beweis. Die Ringgesetze folgen aus denen von R. Das Nullelement von R/I ist $\overline{0}$ und das Einselement ist $\overline{1}$. Das einzige, was zu zeigen ist, ist daß die definierten Verknüpfungen nicht von der Wahl von $r_i \in r_i + I$ abhängen. Sei also $r_1' = r_1 + i_1 \in \overline{r_1}$ und $r_2' = r_2 + i_2 \in \overline{r_2}$. Dann ist $\overline{r_1} = \overline{r_1'}$ und $\overline{r_2} = \overline{r_2'}$. Zu zeigen, daß $\overline{r_1 + r_2} = \overline{r_1' + r_2'}$ und $\overline{r_1 \cdot r_2} = \overline{r_1' \cdot r_2'}$.

$$\overline{r_1' + r_2'} = \overline{r_1 + i_1 + r_2 + i_2} = \overline{r_1 + r_2 + (i_1 + i_2)} = \overline{r_1 + r_2}$$

$$\overline{r_1' \cdot r_2'} = \overline{(r_1 + i_1) \cdot (r_2 + i_2)} = \overline{r_1 r_2 + (r_1 i_2 + r_2 i_1 + i_1 i_2)} = \overline{r_1 r_2}$$

□

Beispiel $n \in \mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$.
$n = 2$: $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$.
$n = 3$: $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2} = \overline{-1}\}$ mit $\overline{1} + \overline{2} = \overline{3} = \overline{0}$, $\overline{2} \cdot \overline{2} = \overline{4} = \overline{1}$.
$n = 4$: $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ mit $\overline{2} + \overline{3} = \overline{5} = \overline{1}$, $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$.

Definition 48.7 *Seien $a, b \in \mathbb{Z}$, $a, b \neq 0$. Dann sagen wir a* teilt *b, falls es ein $n \in \mathbb{Z}$ gibt, mit $a \cdot n = b$. Der* größte gemeinsame Teiler *$\mathrm{ggT}(a, b)$ von a und b ist $\max\{d \in \mathbb{N} \mid d$ teilt a und d teilt $b\}$.*

Satz 48.8 *Der größte gemeinsame Teiler d von zwei ganzen Zahlen $a, b \neq 0$ kann mit dem folgenden Algorithmus berechnet werden, mit dem weiter zwei ganze Zahlen x_1, x_2 bestimmt werden mit $d = x_1 a + x_2 b$.*

Idee: Sei $a_1 := a$, $a_2 := b$. a_{n+2} = Rest der Division von a_n durch a_{n+1}:

$$\begin{array}{lllll} a_1 = q_1a_2 + a_3 & \text{mit } |a_3| < |a_2| & \text{falls } a_2 \neq 0 \\ a_2 = q_2a_3 + a_4 & \text{mit } |a_4| < |a_3| & \text{falls } a_3 \neq 0 \\ a_3 = q_3a_4 + a_5 & \text{mit } |a_5| < |a_4| & \text{falls } a_4 \neq 0 \\ a_4 = q_4a_5 + a_6 & \text{mit } |a_6| < |a_5| & \text{falls } a_5 \neq 0 \\ a_5 = q_5a_6 + a_7 & \text{mit } |a_7| < |a_6| & \text{falls } a_6 \neq 0 \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \end{array}$$

Da $|a_i|$ immer kleiner werden, gilt $a_n = 0$ für ein n. Ist z.B. $a_7 = 0$ (und $a_6 \neq 0$), so gilt $a_5 = q_5a_6$, d.h. a_6 teilt a_5, $a_4 = q_4a_5 + a_6 = (q_4q_5 + 1)a_6$, d.h. a_6 teilt a_4, usw., d.h. a_6 teilt a_2 und a_6 teilt a_1. Wir suchen nun $x_1, x_2 \in \mathbb{Z}$ mit $a_6 = x_1a_1 + x_2a_2$. Dann ist $|a_6| = \mathrm{ggT}(a_1, a_2)$ wirklich der größte gemeinsame Teiler von a_1 und a_2, da jede Zahl, die a_1 und a_2 teilt, auch $a_6 = x_1a_1 + x_2a_2$ teilt. Dazu lösen wir rückwärts auf:

$$a_6 = a_4 - q_4a_5 = a_4 - q_4(a_3 - q_3a_4) = (1 + q_4q_3)a_4 - q_4a_3 = (1 + q_4q_3)(a_2 - q_2a_3) - q_4a_3 =$$

$$= (1 + q_4q_3)a_2 - (q_2 + q_4q_3q_2 + q_4)a_3 = (1 + q_4q_3)a_2 - (q_2 + q_4q_3q_2 + q_4)(a_1 - q_1a_2) =$$

$$= -(q_2 + q_4q_3q_2 + q_4)a_1 + (1 + q_4q_3 + q_1q_2 + q_1q_4 + q_4q_3q_2q_1)a_2$$

Algorithmus 48.9 *Euklidischer Algorithmus*
Eingabe: $a, b \in \mathbb{Z}, a, b \neq 0$.
Ausgabe: $d = \mathrm{ggT}(a, b)$ *und* $x, y \in \mathbb{Z}$, *mit* $d = xa + yb$.
0) Setze $x_0 := 1$, $x_1 := 0$, $y_0 := 0$, $y_1 := 1$, $e := 1$.
1) Bestimme $q, r \in \mathbb{Z}$ *mit* $|r| < |b|$ *und* $a = qb + r$.
2) Setze $h := qx_1 + x_0$, $x_0 := x_1$, $x_1 := h$ *sowie* $h := qy_1 + y_0$, $y_0 := y_1$, $y_1 := h$ *und* $e := -e$.
3) Ist $r \neq 0$, *so setze* $a := b$, $b := r$ *und gehe zu 1).*
4) $(r = 0)$. *Setze* $d := b$ *und gib* $d = \mathrm{ggT}(a, b)$ *und* $x := e \cdot x_0$ *und* $y := -e \cdot y_0$ *aus.*

Beispiel: $a = 82$, $b = 24$:
$82 = 3 \cdot 24 + 10$
$24 = 2 \cdot 10 + 4$
$10 = 2 \cdot 4 + 2$
$4 = 2 \cdot 2 + 0$. Also ist $2 = \mathrm{ggT}(82, 24)$ und
$2 = 10 - 2 \cdot 4 = 10 - 2 \cdot (24 - 2 \cdot 10) = 5 \cdot 10 - 2 \cdot 24 = 5 \cdot (82 - 3 \cdot 24) - 2 \cdot 24 = 5 \cdot 82 - 17 \cdot 24$.

Beispiel: $a = 37$, $b = 41$. Gesucht $\overline{37}^{-1} \in \mathbb{Z}/41\mathbb{Z}$. Dazu: 41 ist eine Primzahl, also ist $\mathrm{ggT}(37, 41) = 1$. Suchen mit dem Euklidischen Algorithmus Zahlen $x, y \in \mathbb{Z}$ mit $37x + 41y = 1$. Dann gilt $\overline{37}\overline{x} = \overline{1} - \overline{41y} = \overline{1} \in \mathbb{Z}/41\mathbb{Z}$. Also ist $\overline{x} = \overline{37}^{-1}$.
$41 = 37 + 4$ und $37 = 9 \cdot 4 + 1$. Also ist $1 = \mathrm{ggT}(37, 41) = 37 - 9 \cdot 4 = 37 - 9 \cdot (41 - 37) = 10 \cdot 37 - 9 \cdot 41$, d.h. $\overline{37}^{-1} = \overline{10}$.

Satz 48.10 *Ist $p \in \mathbb{Z}$ eine Primzahl (d.h. $p > 1$ und p ist nur durch 1 und sich selbst teilbar), so ist der Restklassenring $\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$ ein Körper, der (eindeutig bestimmte) Körper mit p Elementen.*

Beweis. Wir wissen schon, daß $\mathbb{Z}/p\mathbb{Z}$ ein Ring ist. D.h. wir müssen nur noch zeigen, daß wir zu jedem Element $\overline{a} \neq \overline{0} \in \mathbb{Z}/p\mathbb{Z}$ ein $\overline{b} \in \mathbb{Z}/p\mathbb{Z}$ finden, mit $\overline{a}\overline{b} = \overline{1}$, d.h. wir müssen die Gleichung $ab = 1 + px$ für jedes $a \notin (p)$ lösen. Da $\overline{a} \neq \overline{0} \in \mathbb{Z}/p\mathbb{Z}$ ist, gilt p teilt nicht a. Also ist $\mathrm{ggT}(a, p) = 1$. Nach dem Euklidischen Algorithmus gibt es Zahlen b, x mit $b \cdot a + x \cdot p = 1$. Also ist $\overline{b}\overline{a} = \overline{1}$ in $\mathbb{F}_p$. □

Bemerkung:
Der Euklidische Algorithmus zeigt, daß alle Ideale in $\mathbb{Z}$ Hauptideale sind, d.h. $\{n\mathbb{Z} \mid n \in \mathbb{N} \cup \{0\}\}$ ist die Menge aller Ideale in $\mathbb{Z}$.
Denn: Sei $I \trianglelefteq \mathbb{Z}$ ein Ideal. Ist $I \neq (0)$, so gibt es $0 \neq a \in I$. Also ist $(a) \subseteq I$. Ist $I \neq (a)$, so gibt es $b \in I - (a)$. Dann ist $d := \mathrm{ggT}(a, b) = xa + yb \in I$ und $(a) \subset (d) \subseteq I$. Da $b \in (d)$ ist, ist das Hauptideal (d) echt grösser als (a). Nach endlich vielen Schritten ist dann $I = (d)$ ein Hauptideal.

Definition 48.11 *Sei $R = K[x]$ der Polynomring über einem Körper K.*
(i) Sind $a, b \in R$, so sagen wir a teilt *b, falls es ein $q \in R$ gibt mit $b = aq$.*
(ii) Ein Polynom $p \in R$ heißt irreduzibel, *falls $d := \mathrm{Grad}(p) \geq 1$ ist und alle Teiler von p entweder Grad 0 oder Grad d haben.*
(iii) Sind $a, b \in R$, $a, b \neq 0$, so heißt das normierte (führender Koeffizient ist 1) Polynom $p \in R$ maximalem Grades, welches beide Polynome a und b teilt der größte gemeinsame Teiler *von a und b, $p := \mathrm{ggT}(a, b)$.*

Beispiel: Bestimme $\mathrm{ggT}(x^2 + 1, x^2 + x + 1)$ in $\mathbb{F}_2[x]$.
$x^2 + x + 1 = (x^2 + 1) + x$
$x^2 + 1 = x \cdot x + 1$
$x = x \cdot 1 + 0$.
Also ist $1 = \mathrm{ggT}(x^2 + 1, x^2 + x + 1) = (x^2 + 1) - x \cdot x = (x^2 + 1) - x(x^2 + x + 1 - (x^2 + 1)) = (1 + x)(x^2 + 1) - x(x^2 + x + 1)$.

Satz 48.12 *Sei K ein Körper und $R := K[x]$ der Ring der Polynome über K. Analog zum Euklidischen Algorithmus 48.9 für ganze Zahlen kann man den größten gemeinsamen Teiler $d = \mathrm{ggT}(a, b) = xa + yb \in R$ ($x, y \in R$), von zwei Polynomen $a, b \in R$, $a, b \neq 0$ berechnen. Dazu ersetzt man in 48.9 den Schritt 1) durch*
1') Bestimme $q, r \in R$ mit $\mathrm{Grad}(r) < Grad(b)$ und $a = qb + r$.

Analog zu Satz 48.10 gilt:

Satz 48.13 *Sei K ein Körper und $R := K[x]$ der Ring der Polynome über K. Ist $p \in R$ irreduzibel, so ist $R/(p)$ ein Körper.*

Beispiel: (i) Sei $K = \mathbb{R}$ und $p(x) = x^2 + 1$. Sei $R := \mathbb{R}[x]/(x^2+1)$. Dann ist R ein 2-dimensionaler Vektorraum über $\mathbb{R}$ mit Basis $(\overline{1}, \overline{x})$. Weiter ist $p(x) \in \mathbb{R}[x]$ irreduzibel. $\overline{x} \in \mathbb{R}[x]/(x^2+1)$ erfüllt $\overline{x}^2 = -\overline{1}$ und $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.
(ii) Sei $K = \mathbb{F}_2$ und $p(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. Dann ist $p(x)$ irreduzibel und $R := \mathbb{F}_2[x]/(p(x))$ ein Körper. R ist ein 2-dimensionaler Vektorraum über $\mathbb{F}_2$ mit Basis $(\overline{1}, \overline{x})$. Elemente von R: $\overline{0}, \overline{1}, \overline{x}, \overline{x}+\overline{1}$. Multiplikationstabelle:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

Beispiel
$K = \mathbb{F}_2[x]/(x^2+x+1)$. Sei $\alpha := \overline{x} \in K$. Dann gilt $\alpha^2 = \alpha + 1$ und jedes Element von K läßt sich eindeutig schreiben als $a_0 + a_1\alpha$ mit $a_0, a_1 \in \mathbb{F}_2$. K ist als Vektorraum also isomorph zu $\mathbb{F}_2^2$. Das Element α ist ein primitives Element von $\mathbb{F}_{2^2}$ und es gilt

$$\begin{array}{rcrcrcl} 0 & = & & & & = & (00) \\ 1 & = & 1 & & & = & (10) \\ \alpha & = & & & \alpha & = & (01) \\ \alpha^2 & = & 1 & + & \alpha & = & (11) \end{array}$$

Beispiel Der Hexacode: Sei $\alpha := \overline{x} \in \mathbb{F}_2[x]/(x^2+x+1) = \mathbb{F}_4$. Der Hexacode $\mathcal{C}_6$ ist der lineare Code der Dimension 3 in $\mathbb{F}_4^6$ mit Erzeugermatrix:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & \alpha^2 & \alpha \\ 0 & 1 & 0 & 1 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Eine Prüfmatrix von $\mathcal{C}_6$ ist

$$H := \begin{pmatrix} 1 & \alpha^2 & \alpha \\ 1 & \alpha & \alpha^2 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Es gilt $r(\mathcal{C}_6) = \frac{1}{2}$ und $d(\mathcal{C}_6) = 4$.

Indem man α durch (01), 1 durch (10) usw. ersetzt erhält man aus dem Code der Länge 6 und Dimension 3 über $\mathbb{F}_4$ einen Code der Länge 12 und Dimension 6, Minimalabstand 4 über $\mathbb{F}_2$ mit Erzeugermatrix:

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

Hauptsatz 48.14 *Sei K ein endlicher Körper. Dann gilt*
(i) Es gibt ein $n \in \mathbb{N}$ mit $n \cdot 1 = 1 + \ldots + 1 = 0$ (n Summanden).
(ii) $\mathrm{char}(K) := \min\{n \in \mathbb{N} \mid n \cdot 1 = 0\}$ *ist eine Primzahl und heißt die* Charakteristik *von K.*
(iii) Ist $p := \mathrm{char}(K)$, so gilt $\mathbb{F}_p = \{0, 1, 2 = 1+1, \ldots, p-1\} \subseteq K$ und K ist ein $\mathbb{F}_p$-Vektorraum. Ist $f := \dim_{\mathbb{F}_p}(K)$, die Dimension von K als $\mathbb{F}_p$-Vektorraum, so gilt $|K| = p^f$.
(iv) Es gibt ein Element $\alpha \in K$, so daß die Menge $K^* := K - \{0\}$ aus den Potenzen von α besteht.

$$K^* = \{\alpha^0 = 1, \alpha, \alpha^2, \ldots, \alpha^{p^f-1}\}$$

Ein solches $\alpha \in K$ heißt primitives Element *von K.*
(v) Je zwei endliche Körper K, K' mit $|K| = |K'|$ sind isomorph, d.h. es gibt eine bijektive Abbildung $\varphi : K \to K'$ mit $\varphi(a+b) = \varphi(a)+\varphi(b)$ und $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ für alle $a, b \in K$. Wir bezeichnen den endlichen Körper mit p^f Elementen als $\mathbb{F}_{p^f}$.
(vi) Für alle $a \in \mathbb{F}_{p^f}$ gilt $a^{p^f} = a$ und $\mathbb{F}_{p^f}$ besteht gerade aus den p^f verschiedenen Nullstellen von $x^{p^f} - x$. Daraus sieht man, daß

$$\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^f} \Leftrightarrow d \text{ teilt } f.$$

(vii) $\mathbb{F}_{p^f} \cong \mathbb{F}_p[x]/(h(x))$, wo $h(x) \in \mathbb{F}_p[x]$ ein irreduzibles, normiertes Polynom vom Grad f ist.

Beweis. (i) $1, 1+1, 1+1+1, \ldots$ sind alles Elemente von K. Da K endlich ist, können diese nicht alle verschieden sein, d.h. es gibt ein $n < m$ mit $n \cdot 1 = m \cdot 1$. Dann ist aber $m - n \in \mathbb{N}$ und $(m-n) \cdot 1 = 0$.
(ii) Sei $n \in \mathbb{N}$ minimal mit $n \cdot 1 = 0$. Ist $n = ab$ mit $a, b \in \mathbb{N}$, $a < n$ und $b < n$, so gilt $a \cdot 1 \neq 0$ und $b \cdot 1 \neq 0$. D.h. es gibt ein $a^{-1} \in K$ mit $a^{-1}(a \cdot 1) = 1$. Also gilt

$$0 = a^{-1}0 = a^{-1}n \cdot 1 = a^{-1}(ab) \cdot 1 = a^{-1}(a \cdot 1)(b \cdot 1) = (b \cdot 1) \neq 0$$

was ein Widerspruch ist. Also gibt es keine solchen Elemente $a, b \in \mathbb{N}$ und n ist eine Primzahl.

(iii) Sei $p := \mathrm{char}(K)$. Dann gilt $M := \{0, 1, 2 \cdot 1, \ldots, (p-1) \cdot 1\} \subseteq K$ und die Elemente von M addieren und multiplizieren sich genauso wie die von $\mathbb{Z}/p\mathbb{Z}$. Also ist $\mathbb{F}_p \subseteq K$. Elemente von K kann man addieren und mit Elementen von $\mathbb{F}_p$ multiplizieren, also ist K ein Vektorraum über $\mathbb{F}_p$.
(iv), (v), (vi) Sind nicht schwierig, brauchen jedoch etwas mehr Vorbereitung.
(vii) Ist $h(x) \in \mathbb{F}_p[x]$ irreduzibel vom Grad f, so ist $\mathbb{F}_p[x]/(h(x))$ ein Körper mit p^f Elementen also isomorph zu $\mathbb{F}_{p^f}$. Es bleibt zu zeigen, daß es zu jedem f ein irreduzibles Polynom $h(x) \in \mathbb{F}_p[x]$ mit $\mathrm{Grad}(h) = f$ gibt. Auch dies ist nicht schwierig (geht durch Abzählen), wird aber hier weggelassen. □

Beispiel
$K = \mathbb{F}_2[x]/(x^4 + x + 1)$. Sei $\alpha := \overline{x} \in K$. Dann gilt $\alpha^4 + \alpha + 1 = 0$ und jedes Element von K läßt sich eindeutig schreiben als $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$ mit $a_0, a_1, a_2, a_3 \in \mathbb{F}_2$. K ist als Vektorraum also isomorph zu $\mathbb{F}_2^4$. Das Element α ist ein primitives Element von $\mathbb{F}_{2^4}$ und es gilt

$$
\begin{array}{lcccccccccl}
0 & = & & & & & & & & = & (0000) \\
1 & = & 1 & & & & & & & = & (1000) \\
\alpha & = & & & \alpha & & & & & = & (0100) \\
\alpha^2 & = & & & & & \alpha^2 & & & = & (0010) \\
\alpha^3 & = & & & & & & & \alpha^3 & = & (0001) \\
\alpha^4 & = & 1 & + & \alpha & & & & & = & (1100) \\
\alpha^5 & = & & & \alpha & + & \alpha^2 & & & = & (0110) \\
\alpha^6 & = & & & & & \alpha^2 & + & \alpha^3 & = & (0011) \\
\alpha^7 & = & 1 & + & \alpha & + & & & \alpha^3 & = & (1011) \\
\alpha^8 & = & 1 & + & & & \alpha^2 & & & = & (1010) \\
\alpha^9 & = & & & \alpha & + & & & \alpha^3 & = & (0101) \\
\alpha^{10} & = & 1 & + & \alpha & + & \alpha^2 & & & = & (1110) \\
\alpha^{11} & = & & & \alpha & + & \alpha^2 & + & \alpha^3 & = & (0111) \\
\alpha^{12} & = & 1 & + & \alpha & + & \alpha^2 & + & \alpha^3 & = & (1111) \\
\alpha^{13} & = & 1 & + & & & \alpha^2 & + & \alpha^3 & = & (1011) \\
\alpha^{14} & = & 1 & + & & & & & \alpha^3 & = & (1001)
\end{array}
$$

Man beachte, daß z.B. auch die Potenzen von α^3 den $\mathbb{F}_2$-Vektorraum K erzeugen, da $1, \alpha^3, \alpha^6, \alpha^9$ also $(1000), (0001), (0011), (0101)$ linear unabhängig sind. Jedoch ist $\beta := \alpha^3$ kein primitives Element von K, da $\beta^5 = (\alpha^3)^5 = \alpha^{15} = 1$ und daher $\{\beta^i\} = \{1, \alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ nur 5 Elemente enhält (und nicht $15 = |K^*|$).
Rechnen in endlichen Körpern. Sei $K = \mathbb{F}_{p^f} = \mathbb{F}_p[x]/(h(x))$ der Körper mit p^f Elementen ($f = \mathrm{Grad}(h)$). Dann ist K ein $\mathbb{F}_p$-Vektorraum und man kann die Elemente in K als f-Tupel

$$a_0 + a_1\overline{x} + \ldots + a_{f-1}\overline{x}^{f-1} \equiv (a_0, a_1, \ldots, a_{f-1}) \in \mathbb{F}_p^f$$

schreiben. In dieser Darstellung ist es einfach, 2 Körperelemente zu addieren, aber schwierig, sie zu multiplizieren. Deshalb benutzt man manchmal eine andere

Darstellung für die Körperelemente durch sogenannte Zech-Logarithmen. Ist $\alpha \in K$ ein primitives Element, so ist

$$K = \{0\} \cup \{1 = \alpha^0, \alpha, \alpha^2, \ldots, \alpha^{p^f-2}\}.$$

Die Multiplikation ist einfach: $\alpha^i \alpha^j = \alpha^{i+j}$, wobei man den Exponenten $i+j$ modulo $p^f - 1$ lesen muß. Zur Berechnung der Summe $\alpha^i + \alpha^j$ benutzt man eine Tabelle: Ist $i \leq j$, so ist

$$\alpha^i + \alpha^j = \alpha^i(1 + \alpha^{j-i})$$

Es genügt also, sich für jede Zahl k das $l \in \{0, \ldots, p^f - 2\}$ zu merken mit $1 + \alpha^k = \alpha^l$ (ist $1 + \alpha^k = 0$, so setzt man z.B. $l = -1$).

Im Beispiel $K = \mathbb{F}_{16}$, α das primitive Element von oben mit $\alpha^4 + \alpha + 1 = 0$ findet man $1 + \alpha^k = \alpha^l$ mit k, l wie folgt:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
l	-1	4	8	14	1	10	13	9	2	7	5	12	11	6	3

Satz 48.15 *Sei $K := \mathbb{F}_{p^f}$ der Körper mit p^f-Elementen und $\mathbb{F}_p := \{0, 1, 2, \ldots, p-1\} \subseteq K$. Dann ist K ein $\mathbb{F}_p$-Vektorraum und die Abbildung $F : K \to K, \alpha \mapsto \alpha^p$ ist eine bijektive $\mathbb{F}_p$-lineare Abbildung mit $F(\alpha\beta) = F(\alpha)F(\beta)$ für alle $\alpha, \beta \in K$. F heißt der* Frobenius-Automorphismus *von K über $\mathbb{F}_p$.*

Beweis. Seien $a, b \in \mathbb{F}_p \subseteq K$ und $\alpha, \beta \in K$. Zu zeigen ist $F(a\alpha + b\beta) = aF(\alpha) + bF(\beta)$. Nun ist

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

mit $\binom{p}{k} = \frac{p!}{k!(p-k)!} \in \mathbb{Z}$. Ist $1 \leq k \leq p-1$, so ist der Zähler von $\frac{p!}{k!(p-k)!}$ durch p teilbar, der Nenner jedoch nicht. Also ist $\binom{p}{k} \in p\mathbb{Z}$ für $1 \leq k \leq p-1$, d.h. $\binom{p}{k} \cdot 1 = 0$ in K. Damit ist

$$(a\alpha + b\beta)^p = (a\alpha)^p + (b\beta)^p = a^p\alpha^p + b^p\beta^p$$

Es genügt also zu zeigen, daß für alle $a \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ die p-te Potenz $a^p = a$ ist. Dazu zeigen wir per Induktion über a, daß für alle $a \in \mathbb{N}$ die p-te Potenz $a^p \equiv a \pmod{p}$ ist:
Für $a = 1$ gilt $1^p = 1$.
$a \Rightarrow a+1$: Es ist $(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \equiv 1 + a^p \pmod{p}$ wie eben. Nach Induktionsvoraussetzung ist $a^p \equiv a \pmod{p}$, also ist $(a+1)^p \equiv 1 + a^p \equiv 1 + a \pmod{p}$. Also ist F eine $\mathbb{F}_p$-lineare Abbildung. Der Kern von F ist $\{\alpha \in \mathbb{F}_{p^f} \mid \alpha^p = 0\} = \{0\}$. Damit ist F injektiv und daher auch bijektiv, aus Dimensionsgründen. Klar ist $F(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = F(\alpha)F(\beta)$. □

Folgerung 48.16 *Ist $\alpha \in \mathbb{F}_{p^f}$ und $h \in \mathbb{F}_p[x]$ mit $h(\alpha) = 0$, so gilt auch $h(F(\alpha)) = 0$.*

Beispiel:
$x^{16} - x = x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1) \in \mathbb{F}_2[x]$.
Ist $\alpha \in \mathbb{F}_{16}$ eine Nullstelle von $x^4 + x + 1$, so sind $\{\alpha^2, \alpha^4, \alpha^8, \alpha^{16} = \alpha\}$ die 4 Nullstellen von $x^4 + x + 1$. Für $\beta := \alpha^3$ gilt $\beta^4 + \beta^3 + \beta^2 + \beta + 1 = 0$ und $\{\beta^2, \beta^4, \beta^8, \beta^{16} = \beta\}$ sind die Nullstellen von $x^4 + x^3 + x^2 + x + 1$. Setzt man $\gamma := \alpha^5$, so gilt $\gamma^2 + \gamma + 1 = 0$ ($\{a_0 + a_1\gamma \mid a_0, a_1 \in \mathbb{F}_2\} \leq \mathbb{F}_{16}$ ist der Teilkörper $\mathbb{F}_4$ von $\mathbb{F}_{16}$) und $\{\gamma^2, \gamma^4 = \gamma\}$ sind die Nullstellen von $x^2 + x + 1$.

49 Zyklische Codes

Im gesamten Abschnitt bezeichnet $q := p^f$ eine Potenz einer Primzahl p und $\mathbb{F}_q$ den Körper mit q Elementen.

Definition 49.1 *Ein linearer Code $C \leq \mathbb{F}_q^N$ heißt* zyklisch, *falls*

$$(c_1, \ldots, c_N) \in C \Rightarrow (c_N, c_1, c_2, \ldots, c_{N-1}) \in C$$

Satz 49.2 *(i) Die Abbildung $\varphi : \mathbb{F}_q^N \to \mathbb{F}_q[x]/(x^N-1)$ definiert durch $(a_1, \ldots, a_N) \mapsto a_1 + a_2\overline{x} + \ldots + a_N\overline{x}^{N-1}$ definiert einen $\mathbb{F}_q$-Vektorraum Isomorphismus.*
(ii) $C \leq \mathbb{F}_q^N$ ist ein zyklischer Code, genau dann wenn $\varphi(C) \trianglelefteq \mathbb{F}_q[x]/(x^N - 1)$ ein Ideal ist.

Beweis. (i) Nachrechnen: Zu zeigen ist, daß die Abbildung $\mathbb{F}_q$-linear und bijektiv ist.
(ii) Es ist $\overline{x}(a_1 + a_2\overline{x} + \ldots + a_N\overline{x}^{N-1}) = a_1\overline{x} + a_2\overline{x}^2 + \ldots + a_N\overline{x}^N$
$= a_1\overline{x} + a_2\overline{x}^2 + \ldots + a_N \cdot 1 = a_N + a_1\overline{x} + a_2\overline{x}^2 + \ldots + a_{N-1}\overline{x}^{N-1}$.
$\varphi(C)$ ist immer ein $\mathbb{F}_q$-Teilvektorraum von $\mathbb{F}_q[x]/(x^N - 1)$. Damit $\varphi(C)$ ein Ideal ist, muß zusätzlich noch $\overline{x}\varphi(c) \in \varphi(C)$ sein für alle $c \in C$. Dies ist nach obiger Rechnung aber genau die Bedingung dafür, daß C ein zyklischer Code ist. □

Im folgenden werden wir stets voraussetzen, daß N nicht durch p teilbar ist. Dann gilt:

$$\mathrm{ggT}(x^N - 1, \frac{d}{dx}(x^N - 1)) = \mathrm{ggT}(x^N - 1, Nx^{N-1}) = \mathrm{ggT}(x^N - 1, x^{N-1}) = 1$$

da $x \cdot x^{N-1} - (x^N - 1) = 1$ ist. D.h. das Polynom $x^N - 1$ hat keine mehrfachen Nullstellen und läßt sich eindeutig schreiben als Produkt

$$x^N - 1 = f_1(x) \cdot \ldots \cdot f_t(x)$$

mit $f_1, \ldots, f_t \in \mathbb{F}_q[x]$ normiert, irreduzibel und paarweise verschieden.

Beispiel
$N = 15,\ q = 2$:

$$x^{15} - 1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1) \in \mathbb{F}_2[x].$$

$N = 6,\ q = 3$:

$$x^6 - 1 = (x-1)^3(x+1)^3 \in \mathbb{F}_3[x].$$

$N = 4,\ q = 3$:

$$x^4 - 1 = (x-1)(x+1)(x^2+1) \in \mathbb{F}_3[x].$$

Diese Faktorisierungen kann man z.B. mit MAPLE berechnen mit dem Befehl

$$\text{Factor}(x^4 - 1) \bmod 3$$

Die Ideale in $\mathbb{F}_q[x]/(x^N - 1)$ sind dann genau die Hauptideale $(f_{i_1 \ldots i_s})$ wo $f_{i_1 \ldots i_s} := \overline{f_{i_1}(x) \cdot \ldots \cdot f_{i_s}(x)}$ für $s \leq t$ und $1 \leq i_1 < i_2 < \ldots < i_s \leq t$. Der Ring hat also genau 2^t Ideale.

Sei $g := f_{i_1} \cdot \ldots \cdot f_{i_s}$ und $d := \text{Grad}(g)$. Dann ist $(\overline{g}) = \{\overline{ag} \mid \overline{a} \in \mathbb{F}_q[x]/(x^N - 1)\}$. Jedes Element $\overline{ag} \in (\overline{g})$ läßt sich schreiben als $\overline{b}\overline{g}$ mit $\text{Grad}(b) \leq N - d - 1$. Dazu sei $h \in \mathbb{F}_q[x]$ mit $gh = x^N - 1$. Dann ist $\text{Grad}(h) = N - d$. Polynomdivision mit Rest liefert $a = a_1 h + b$ mit einem Rest b vom Grad $\leq N - d - 1$. In $\mathbb{F}_q[x]/(x^N - 1)$ gilt dann $\overline{ag} = (\overline{a_1 h + b})\overline{g} = \overline{b}\overline{g}$, da $\overline{h}\overline{g} = 0$ ist. Also ist $(\overline{g}, \overline{xg}, \ldots, \overline{x}^{N-d-1}\overline{g})$. eine Basis von $(\overline{g}) \trianglelefteq \mathbb{F}_q[x]/(x^N - 1)$ und $\dim(\overline{g}) = N - d$.
Beispiel
$N = 4,\ q = 3$:

$$x^4 - 1 = (x-1)(x+1)(x^2+1) \in \mathbb{F}_3[x].$$

$I_{123} = (\overline{(x-1)(x+1)(x^2+1)}) = (0)$,
$I_{12} = (f_{12}) = (\overline{(x-1)(x+1)}) = (\overline{x}^2 - 1)$ hat Dimension 2 und $\mathbb{F}_3$-Basis $(f_{12}, \overline{x} f_{12})$. Denn es ist
$I_{12} = \{(a_0 + a_1\overline{x} + a_2\overline{x}^2 + a_3\overline{x}^3)(\overline{x}^2 - 1) \mid a_0, a_1, a_2, a_3 \in \mathbb{F}_3\} = \{a_0(\overline{x}^2 - 1) + a_1\overline{x}(\overline{x}^2 - 1) + a_2\overline{x}^2(\overline{x}^2 - 1) + a_3\overline{x}^3(\overline{x}^2 - 1) \mid a_0, a_1, a_2, a_3 \in \mathbb{F}_3\}$. Nun ist $\overline{x}^2(\overline{x}^2 - 1) = \overline{x}^4 - \overline{x}^2 = 1 - \overline{x}^2$ und $\overline{x}^3(\overline{x}^2 - 1) = -\overline{x}(\overline{x}^2 - 1)$. Daher ist $I_{12} = \{(a_0 + a_1\overline{x})(\overline{x}^2 - 1) \mid a_0, a_1 \in \mathbb{F}_3\}$.
Der I_{12} entsprechende Code C_{12} hat die Erzeugermatrix

$$\begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$$

Shiftet man die 2. Zeile dieser Matrix noch einmal nach rechts, so erhält man das negative der ersten Zeile.

Die Ergebnisse fassen wir in dem folgenden Satz zusammen:

Satz 49.3 *Sei N nicht durch p teilbar, und $x^N - 1 = f_1(x) \cdot \ldots \cdot f_t(x)$ mit paarweise verschiedenen, normierten, irreduziblen Polynomen $f_1, \ldots, f_t \in \mathbb{F}_q[x]$.*

(i) Setzt man $f_{i_1 \ldots i_s} := \overline{f_{i_1}(x) \cdot \ldots \cdot f_{i_s}(x)}$ *für* $s \leq t$ *und* $1 \leq i_1 < i_2 < \ldots < i_s \leq t$ *so sind die Hauptideale* $(f_{i_1 \ldots i_s})$ *genau die Ideale von* $\mathbb{F}_p[x]/(x^N - 1)$. *Der Ring hat also genau* 2^t *Ideale. Ist* $d_i := \mathrm{Grad}(f_i)$ *der Grad des irreduziblen Faktors* f_i $(d_1 + \ldots + d_t = N)$, *so gilt*

$$\dim(\overline{f_{i_1}(x) \cdot \ldots \cdot f_{i_s}(x)}) = N - (d_{i_1} + \ldots + d_{i_s}).$$

(ii) Das Polynom $g := f_{i_1} \cdot \ldots \cdot f_{i_s}$ *heißt* Erzeugerpolynom *des zyklischen Codes* $C_g := (f_{i_1 \ldots i_s})$. *Ist* $\overline{g} = \sum_{j=0}^{N-k} g_j \overline{x}^j$, *so ist*

$$G_g := \begin{pmatrix} g_0 & g_1 & \ldots & g_{N-k} & 0 & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & g_{N-k-1} & g_{N-k} & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & g_0 & g_1 & \ldots & \ldots & g_{N-k} \end{pmatrix}$$

eine Erzeugermatrix von C_g *und* $k = \dim(C_g)$.
(iii) Ist g *wie in (ii) ein Erzeugerpolynom des zyklischen Codes* C_g, *so heißt das Polynom* $h \in \mathbb{F}_q[x]$ *mit* $gh = x^N - 1$ *ein* Prüfpolynom *von* C_g. *Es gilt* $\mathrm{Grad}(h) + \mathrm{Grad}(g) = N$. *Weiter liegt* $a \in \mathbb{F}_q[x]/(x^N - 1)$ *genau dann in* C_g, *falls* $a\overline{h} = 0$ *ist.*
(iv) Sei h *wie in (iii) ein Prüfpolynom von* C_g. *Ist* $\overline{h} = \sum_{j=0}^{k} h_j \overline{x}^j$, *so ist die Matrix*

$$G'_h := \begin{pmatrix} h_k & h_{k-1} & \ldots & h_0 & 0 & 0 & \ldots & 0 \\ 0 & h_k & \ldots & h_1 & h_0 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & h_k & h_{k-1} & \ldots & \ldots & h_0 \end{pmatrix}$$

eine Erzeugermatrix von $C_g^{\perp}$ *und daher* $(G'_h)^{tr}$ *eine Prüfmatrix von* C_g.

Beweis. (ii) Eine $\mathbb{F}_q$-Basis von C_g ist $\overline{g}, \overline{xg}, \ldots, \overline{x}^{k-1}\overline{g}$, diese Elemente sind genau die Zeilen der Erzeugermatrix.
(iii) Klar ist $\mathrm{Grad}(h) + \mathrm{Grad}(g) = \mathrm{Grad}(hg) = N$. Außerdem gilt für $a \in \mathbb{F}_q[x]/(x^N - 1)$:

$$a\overline{h} = 0 \Leftrightarrow (x^N - 1) \text{ teilt } ah \Leftrightarrow gh \text{ teilt } ah \Leftrightarrow g \text{ teilt } a \Leftrightarrow a \in (\overline{g}) = C_g$$

(iv) $x^N - 1 = gh = (\sum_{j=0}^{N-k} g_j x^j)(\sum_{i=0}^{k} h_i x^i) = \sum_{l=0}^{N}(\sum_{j=0}^{l} g_j h_{l-j})x^l$. Durch Koeffizientenvergleich folgt für $0 < l < N$, daß $\sum_{j=0}^{l} g_j h_{l-j} = 0$. Also stehen die Zeilen von G'_h senkrecht auf denen von G_g. Aus Dimensionsgründen erzeugt also G'_h daher $C_g^{\perp}$. □

Beispiel 49.4 $x^7-1=(x+1)(x^3+x+1)(x^3+x^2+1) \in \mathbb{F}_2[x]$. *Sei* $g := x^3+x+1$. *Dann hat der zyklische Code* $C_g = (\overline{g}) \trianglelefteq \mathbb{F}_2[x]/(x^7-1)$ *Länge 7, Dimension 4 und Erzeugermatrix*

$$G_g := \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Da $h = (x+1)(x^3+x^2+1) = x^4+x^2+x+1$ *findet man eine Erzeugermatrix von* $C_g^\perp$ *als*

$$G'_h := \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Man kann zeigen, daß $C_g = H_7(2)$ *ein Hamming Code ist.*

49.1 Ein Codierer für zyklische Codes

Sei $C \leq \mathbb{F}_q^N$ ein Code der Dimension k mit Erzeugermatrix $G := (I_k, P_{N-k})$. Codierung besteht dann darin, einem Informationswort $u := (u_1, \ldots, u_k) \in \mathbb{F}_q^k$ ein Codewort

$$(c_1, \ldots, c_N) = (u_1, \ldots, u_k, c_{k+1}, \ldots c_N) = uG \in C$$

zuzuordnen. Dabei sind die ersten k Komponenten des Codeworts die Informationssymbole, die anderen $(N-k)$-Komponenten Kontrollsymbole.
Beispiel:
$C \leq \mathbb{F}_2^4$ mit Erzeugermatrix $\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$. Mit C kann man 4 Informationsworte übertragen:
$u_{00} = (00)$ wird codiert zu $(0000) \in C$
$u_{10} = (10)$ wird codiert zu $(1011) \in C$
$u_{01} = (01)$ wird codiert zu $(0101) \in C$
$u_{11} = (11)$ wird codiert zu $(1110) \in C$.

Bei zyklischen Codes kann man die Kontrollsymbole als Rest einer Polynomdivision berechnen:

Satz 49.5 *Sei* $g = \sum_{i=0}^{N-k} g_i x^i \in \mathbb{F}_q[x]$ *ein Teiler von* x^N-1 *und* $C := C_g \trianglelefteq \mathbb{F}_q[x]/(x^N-1)$ *der zyklische Code mit Erzeugerpolynom* g. *Sei* $u := \sum_{i=0}^{k-1} u_i x^i$ *ein Informationswort. Dann gibt es ein eindeutig bestimmtes Polynom* $r = \sum_{i=0}^{N-k-1} r_i x^i \in \mathbb{F}_q[x]$ *mit* $\mathrm{Grad}(r) < N-k = \mathrm{Grad}(g)$, *so daß*

$$ux^{N-k} = gh + r$$

für ein $h \in \mathbb{F}_q[x]$. *Dann ist* $\overline{gh} =$

$$\overline{ux}^{N-k} - \overline{r} = \sum_{i=0}^{k-1} u_i \overline{x}^{N-k+i} - \sum_{i=0}^{N-k-1} r_i \overline{x}^i \equiv (-r_0, -r_1, \ldots, -r_{N-k-1}, u_0, u_1, \ldots, u_{k-1}) \in C_g$$

Bei den zyklischen Codes kommen bei diesem Codierverfahren zunächst die Kontrollsymbole, dann die Informationssymbole. Daher ist es zweckmäßig die Reihenfolge aller Codeworte umzudrehen, also die Worte bzgl. der Basis $(\overline{x}^{N-1}, \overline{x}^{N-2}, \ldots, \overline{x}, 1)$ zu schreiben:
Beispiel $g := x^4 + x + 1 \in \mathbb{F}_2[x]$ teilt $x^{15} - 1 \in \mathbb{F}_2[x]$. Betrachten $C = C_g \trianglelefteq \mathbb{F}_2[x]/(x^{15} - 1)$. Dann ist $C \cong H_{15}(2)$ der Hamming Code der Länge $15 = 2^4 - 1$ und Dimension $15-4 = 11$. Der Codierer ordnet jedem 11-Tupel $(u_{10}, u_9, \ldots, u_0) \in \mathbb{F}_2^{11}$ ein Codewort $(u_{10}, u_9, \ldots, u_0, r_3, r_2, r_1, r_0) \in \mathbb{F}_2^{15}$ zu, wo

$$(\sum_{i=0}^{10} u_i x^i) x^4 = gh + \sum_{i=0}^{3} r_i x^i$$

ist. Ist z.B. $u = (11010011010)$, so kann man die Division mit Rest mechanisch wie folgt durchführen:

$$\begin{array}{cccccccccccccccccc}
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & : & 10011 \\
1 & 0 & 0 & 1 & 1 & & & & & & & & & & & & \\
\cline{1-5}
 & 1 & 0 & 0 & 1 & 0 & & & & & & & & & & & \\
 & 1 & 0 & 0 & 1 & 1 & & & & & & & & & & & \\
\cline{2-6}
 & & & & & 1 & 1 & 1 & 0 & 1 & & & & & & & \\
 & & & & & 1 & 0 & 0 & 1 & 1 & & & & & & & \\
\cline{5-10}
 & & & & & & 1 & 1 & 1 & 0 & 0 & & & & & & \\
 & & & & & & 1 & 0 & 0 & 1 & 1 & & & & & & \\
\cline{6-11}
 & & & & & & & 1 & 1 & 1 & 1 & 0 & & & & & \\
 & & & & & & & 1 & 0 & 0 & 1 & 1 & & & & & \\
\cline{7-12}
 & & & & & & & & 1 & 1 & 0 & 1 & 0 & & & & \\
 & & & & & & & & 1 & 0 & 0 & 1 & 1 & & & & \\
\cline{8-13}
 & & & & & & & & & 1 & 0 & 0 & 1 & 0 & & & \\
 & & & & & & & & & 1 & 0 & 0 & 1 & 1 & & & \\
\cline{9-14}
 & & & & & & & & & & 0 & 0 & 0 & 0 & 1 & 0 &
\end{array}$$

Also ist der Rest x und $c = (110100110100010) \in C$ das zu u gehörende Codewort.

49.2 Der Minimalabstand zyklischer Codes

Der Minimalabstand zyklischer Codes ist im allgemeinen schwer zu bestimmen, man hat jedoch eine untere Schranke:

Eine Nullstelle α von $x^N - 1 \in \mathbb{F}_q[x]$ heißt primitive N-te Einheitswurzel, falls $N = \min\{n \in \mathbb{N} \mid \alpha^n = 1\}$. Man beachte, daß α nicht notwendig in $\mathbb{F}_q$ liegen muß sondern eventuell in einem größeren Körper.

Satz 49.6 *Sei g ein Teiler von $x^N - 1 \in \mathbb{F}_q[x]$ und α eine primitive N-te Einheitswurzel. Sind die r aufeinanderfolgenden Potenzen α^b, α^{b+1}, α^{b+2}, ..., α^{b+r-1} Nullstellen von g, so gilt für den zyklischen Code $C_g := (\overline{g}) \trianglelefteq \mathbb{F}_q[x]/(x^N - 1)$ daß $d(C_g) \geq r + 1$.*

Beweis. Sei $c := \sum_{i=0}^{N-1} c_i \overline{x}^i \in C_g$ ein Codewort vom Gewicht $s \leq r$ und seien $c_{t_1}, \ldots, c_{t_s}$ alle von 0 verschiedenen Einträge von c. Da $c \in C_g$ ein Vielfaches von g ist und $\alpha^b, \ldots, \alpha^{b+r-1}$ Nullstellen von g sind gilt $c(\alpha^b) = c(\alpha^{b+1}) = \ldots = c(\alpha^{b+r-1}) = 0$. D.h. es gilt

$$\begin{array}{ccccccc} c_{t_1}\alpha^{bt_1} & + & \ldots & + & c_{t_s}\alpha^{bt_s} & = & 0 \\ c_{t_1}\alpha^{(b+1)t_1} & + & \ldots & + & c_{t_s}\alpha^{(b+1)t_s} & = & 0 \\ \vdots & & & & \vdots & & \vdots \\ c_{t_1}\alpha^{(b+r-1)t_1} & + & \ldots & + & c_{t_s}\alpha^{(b+r-1)t_s} & = & 0 \end{array}$$

Setzt man

$$H := \begin{pmatrix} \alpha^{bt_1} & \ldots & \alpha^{bt_s} \\ \alpha^{(b+1)t_1} & \ldots & \alpha^{(b+1)t_s} \\ \vdots & \vdots & \vdots \\ \alpha^{(b+s-1)t_1} & \ldots & \alpha^{(b+s-1)t_s} \end{pmatrix}$$

so gilt also insbesondere $H(c_{t_1}, \ldots, c_{t_s})^{tr} = 0$, d.h. c ist im Kern von H. Die Determinante von H ist aber

$$\det(H) = \alpha^{bt_1}\alpha^{bt_2}\cdot\ldots\cdot\alpha^{bt_s} \det \begin{pmatrix} 1 & \ldots & 1 \\ \alpha^{t_1} & \ldots & \alpha^{t_s} \\ (\alpha^{t_1})^2 & \ldots & (\alpha^{t_s})^2 \\ \vdots & \vdots & \vdots \\ (\alpha^{t_1})^{s-1} & \ldots & (\alpha^{t_s})^{s-1} \end{pmatrix} = \alpha^{bt_1}\alpha^{bt_2}\cdot\ldots\cdot\alpha^{bt_s} \prod_{i<j} (\alpha^{t_j} - \alpha^{t_i})$$

nach HMII, 4. Übungsblatt, Aufgabe 2. Da α eine primitive N-te Einheitswurzel ist, ist $\alpha^{t_i} \neq \alpha^{t_j}$ und $\det(H) \neq 0$. Also ist $\mathrm{Ker}(H) = \{0\}$ und $c = 0$. □

Beispiel:
$N = 7$: $x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1) \in \mathbb{F}_2[x]$. Sei $g := x^3+x+1$. Dann ist jede Nullstelle α von g ein primitives Element von $\mathbb{F}_2[x]/(x^3+x+1) = \mathbb{F}_8$ also eine primitive 7-te Einheitswurzel. Da $g \in \mathbb{F}_2[x]$ gilt $0 = F(g(\alpha)) = g(F(\alpha)) = g(\alpha^2)$, für den Frobenius Automorphismus F. Der Code C_g aus Beispiel 49.4 von oben hat also Minimalabstand $\geq 2 + 1 = 3$.
Beispiel:
$N = 23$, $x^{23} - 1 = (x+1)g_1g_2 \in \mathbb{F}_2[x]$ mit

$$g_1 = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$$

$$g_2 = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$$

Sei α eine Nullstelle von g_1. Dann ist $\alpha \neq 1$ und $\alpha^{23} = 1$, d.h. α ist eine primitive 23-te Einheitswurzel. Indem man den Frobenius Automorphismus mehrfach auf α anwendet findet man die Nullstellen

$$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32} = \alpha^9, \alpha^{18}, \alpha^{36} = \alpha^{13}, \alpha^3, \alpha^6, \alpha^{12}$$

von g_1. Insbesondere hat g_1 die 4 aufeinanderfolgenden Nullstellen $\alpha, \alpha^2, \alpha^3, \alpha^4$, also hat $C_g \leq \mathbb{F}_2[x]/(x^{23}-1)$ Minimalabstand ≥ 5. Tatsächlich ist $C_g = \mathcal{G}_{23}$ der Golay-Code der Länge 23 und $d(C_g) = 7$.

Zyklische Codes, für die Satz 49.6 eine gute untere Abschätzung liefern sind die sogenannten BCH-Codes. Das Erzeugerpolynom eines BCH-Codes, ist das Polynom g kleinsten Grades, für das $g(\alpha^b) = \ldots = g(\alpha^{b+r-1}) = 0$ für eine primitive N-te Einheitswurzel α:

Definition 49.7 *Ein* BCH-Code *(Bose, Chandhuri, Hocquenghem) mit* designiertem Minimalabstand δ *über* $\mathbb{F}_q$ *der Länge* N *ist ein zyklischer Code* $C_g \trianglelefteq \mathbb{F}_q[x]/(x^N-1)$ *für den es eine primitive* N*-te Einheitswurzel* α *und* $b \in \mathbb{Z}$ *gibt, so daß* $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$ *Nullstellen von* $g \in \mathbb{F}_q[x]$ *sind und* g *keinen irreduziblen Faktor* h *hat mit* $h(\alpha^b) \neq 0, h(\alpha^{b+1}) \neq 0, \ldots$ *und* $h(\alpha^{b+\delta-2}) \neq 0$.
Ist $N = q^m - 1$ *(also* α *ein primitives Element von* $\mathbb{F}_{q^m}$*), so heißt der BCH-Code* primitiv.

Aus Satz 49.6 folgt direkt:

Bemerkung 49.8 *Ist* C *ein BCH-Code mit designiertem Minimalabstand* δ*, so ist* $d(C) \geq \delta$.

49.3 Unvollständiges Decodieren von zyklischen Codes

Sei C ein BCH-Code der Länge N über $\mathbb{F}_q$ mit designiertem Minimalabstand $\delta = 2t+1$. Dann gibt es zu jedem $a \in \mathbb{F}_q^N$ höchstens ein $c \in C$ mit $d(a,c) \leq t$, da C t Fehler erkennen kann. Wir wollen ein Verfahren angeben, wie man zu einem $a \in \mathbb{F}_q^N$ ein solches $c \in C$ bestimmt, falls es so ein c gibt. Dieses Verfahren nennt man "unvollständige" Decodierung, da der Decodierer im Fall daß mehr als t Fehler aufgetreten sind, keine Antwort gibt.

Sei der Einfachheit halber $C = C_g \trianglelefteq \mathbb{F}_q[x]/(x^N-1)$ ein zyklischer Code der Länge N, $\alpha \in \mathbb{F}_{q^m}$ eine primitive N-te Einheitswurzel (dazu muß N ein Teiler von $q^m - 1$ sein), so daß α, α^2, α^3, ..., α^{2t} Nullstellen von g sind.

Sei

$$c = (c_0, \ldots, c_{N-1}) \equiv c(x) := c_0 + c_1 x + \ldots + c_{N-1} x^{N-1}$$

ein gesendetes Codewort und

$$r = (r_0, \ldots, r_{N-1}) \equiv r(x) := r_0 + r_1 x + \ldots + r_{N-1} x^{N-1}$$

das empfangene Wort. Dann ist der Fehler

$$E = r - c = (r_0 - c_0, \ldots, r_{N-1} - c_{N-1}) = (E_0, \ldots, E_{N-1}) \equiv$$

$$E(x) = r(x) - c(x) = E_0 + E_1 x + \ldots + E_{N-1} x^{N-1}$$

Wir kennen r und wollen daraus c (bzw. E) bestimmen, falls höchstens t Komponenten E_i ungleich 0 sind. Wir definieren nun die unbekannten Größen

$$M := \{i \mid E_i \neq 0\},\ e := |M| = \text{Anzahl der Fehler}$$

$$\sigma(z) := \prod_{i \in M} (1 - \alpha^i z),\ \omega(z) := \sum_{i \in M} E_i \alpha^i z \prod_{j \in M - \{i\}} (1 - \alpha^j z)$$

Kennt man $\sigma(z)$ und $\omega(z)$, so kennt man den Fehler E, denn es ist $E_i \neq 0 \Leftrightarrow \sigma(\alpha^{-i}) = 0$ und dann ist

$$E_i = \frac{-\omega(\alpha^{-i})\alpha^i}{\sigma'(\alpha^{-i})}.$$

Es ist

$$\frac{\omega(z)}{\sigma(z)} = \sum_{i \in M} \frac{E_i \alpha^i z}{1 - \alpha^i z} = \sum_{i \in M} E_i \sum_{l=1}^{\infty} (\alpha^i z)^l = \sum_{l=1}^{\infty} z^l (\sum_{i \in M} E_i (\alpha^i)^l) = \sum_{l=1}^{\infty} z^l E(\alpha^l)$$

Für $1 \leq l \leq 2t$ gilt $E(\alpha^l) = r(\alpha^l)$, da $c(\alpha^l) = 0$ ist für diese l. Somit kennt man die ersten $2t + 1$ Koeffizienten der Potenzreihenentwicklung von $\frac{\omega(z)}{\sigma(z)}$.

Satz 49.9 *Es gibt höchstens ein Paar von Polynomen*

$$\sigma(z) = \sum_{j=0}^{t} \sigma_j z^j,\ \omega(z) = \sum_{j=0}^{t} \omega_j z^j$$

mit $\sigma_0 = 1$, $\omega_0 = 0$ *und* $\text{Grad}(\omega) \leq \text{Grad}(\sigma)(= e) \leq t$, *so daß die Potenzreihenentwicklung von* $\frac{\omega(z)}{\sigma(z)}$ *mit* $\sum_{l=1}^{2t} z^l r(\alpha^l)$ *beginnt.*

Beweis. (als Übung), explizites Ausmultiplizieren ergibt nach Koeffizientenvergleich ein lineares Gleichungssystem mit $2t + 1$ Gleichungen und $2t$ Unbekannten. Die Determinante dieses Gleichungssystems ist $\neq 0$, also hat das System höchstens eine Lösung. □

Die in Satz 49.9 beschriebene Lösung existiert, wenn höchstens t Fehler aufgetreten sind und liefert dann den Fehlervektor E wie oben beschrieben. Als Test sollte man dann noch überprüfen, ob $r - E$ wirklich im Code liegt.
Beispiel:
Sei $g := x^3 + x + 1 \in \mathbb{F}_2[x]$ und $C_g \trianglelefteq \mathbb{F}_2[x]/(x^7 - 1)$ der Code aus Beispiel 49.4. Sei $\alpha \in \mathbb{F}_8$ eine Nullstelle von g. Dann ist auch $g(\alpha^2) = 0$. Sei $r = (1100000) = 1 + x$

ein empfangenes Wort. Wir wollen das Codeswort $c \in C_g$ bestimmen mit $d(r,c)$ minimal, wobei wir annehmen, daß höchstens 1 Fehler aufgetreten ist. Es ist

$$r(\alpha) = 1 + \alpha, \quad r(\alpha^2) = 1 + \alpha^2.$$

Setzen $\omega(z) := \omega_1 z + \omega_0$, $\sigma(z) := \sigma_1 z + 1$. Dann ist

$$\frac{\omega(z)}{\sigma(z)} = \frac{\omega_1 z + \omega_0}{\sigma_1 z + 1} = (1+\alpha)z + (1+\alpha^2)z^2 + \text{ höhere Terme}$$

also

$$\omega_1 z + \omega_0 = (1+\alpha)z + ((1+\alpha^2) + \sigma_1(1+\alpha))z^2$$

und damit

$$\omega_1 = 1+\alpha, \quad \omega_0 = 0, \quad \sigma_1 = (1+\alpha^2)/(1+\alpha) = (1+\alpha^2)\alpha^4 = \alpha^3.$$

Die Nullstelle von $\sigma(z) = \alpha^3 z + 1$ ist $z = \alpha^4 = \alpha^{-3}$. Also ist nur $E_3 \neq 0$ (an der 4. Stelle ist ein Fehler aufgetreten). Wegen $\sigma'(z) = \alpha^3$ ist

$$E_3 = \frac{-\omega(\alpha^4)\alpha^3}{\alpha^3} = \frac{\alpha^3\alpha^4\alpha^3}{\alpha^3} = \alpha^7 = 1.$$

Also ist das richtige Codewort $c = (1101000)$.

49.4 Reed-Solomon Codes

Definition 49.10 *Sei $N = q-1$ und $\alpha \in \mathbb{F}_q$ ein primitives Element von $\mathbb{F}_q$. Ein zyklischer Code mit Erzeugerpolynom*

$$g = (x - \alpha^b)(x - \alpha^{b+1}) \ldots (x - \alpha^{b+r-1}) \in \mathbb{F}_q[x]$$

heißt Reed-Solomon Code *mit Minimalabstand $r+1$.*

Beispiel: $q = 8$, $N = 7$, α eine Nullstelle von $1 + x + x^3$. Dann ist α ein primitives Element von $\mathbb{F}_8$. Sei

$$g = (x + \alpha^5)(x + \alpha^6) = x^2 + \alpha x + \alpha^4 \in \mathbb{F}_8[x].$$

Es gilt

	1	α	α^2
0	0	0	0
1	1	0	0
α	0	1	0
α^2	0	0	1
α^3	1	1	0
α^4	0	1	1
α^5	1	1	1
α^6	1	0	1

Dann ist $\dim(C_g) = 7 - 2 = 5$ und

$$G_g := \begin{pmatrix} \alpha^4 & \alpha & 1 & 0 & 0 & 0 & 0 \\ 0 & \alpha^4 & \alpha & 1 & 0 & 0 & 0 \\ 0 & 0 & \alpha^4 & \alpha & 1 & 0 & 0 \\ 0 & 0 & 0 & \alpha^4 & \alpha & 1 & 0 \\ 0 & 0 & 0 & 0 & \alpha^4 & \alpha & 1 \end{pmatrix}$$

eine Erzeugermatrix von C_g über $\mathbb{F}_8$. Aus C_g erhält man einen $3 \cdot 5 = 15$-dimensionalen Code über $\mathbb{F}_2$ der Länge 21, mit Minimalabstand 3 und Erzeugermatrix

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

Fügt man jedem Tripel aus $\mathbb{F}_{2^3} \equiv \mathbb{F}_2^3$ ein zusätzliches Paritybit hinzu, so erhält man einen Code $\tilde{C}$ der Länge 28, Dimension 15 und weitaus größerem Minimalabstand 6. Die ersten 3 Zeilen der Erzeugermatrix von $\tilde{C}$ sind dann also:

$$\begin{pmatrix} 0110 & 0101 & 1001 & 0000 & 0000 & 0000 & 0000 \\ 1111 & 0011 & 0101 & 0000 & 0000 & 0000 & 0000 \\ 1010 & 1100 & 0011 & 0000 & 0000 & 0000 & 0000 \end{pmatrix}$$

Bemerkung 49.11 *Die praktische Bedeutung der Reed-Solomon-Codes liegt darin, daß sie sich gut zur Korrektur von Fehlerbündeln "burst-errors" eignen. Ist $C \leq \mathbb{F}_{q^m}^{q^m-1}$ ein Reed-Solomon Code über $\mathbb{F}_{q^m}$, mit Dimension $k = q^m - 2t$ der t Fehler korrigieren kann, so erhält man aus C einen linearen Code $C' \leq \mathbb{F}_q^{m(q^m-1)}$ über $\mathbb{F}_q$ der Länge $m(q^m - 1)$ und der Dimension mk. C' kann auch i.a. nur t Fehler korrigieren, was nicht besonders gut ist. Treten aber Fehlerbündel an b aufeinanderfolgenden Stellen des Codes C' auf mit $b \leq m(t-1)+1$, so betreffen diese großen Fehler nur höchstens t Stellen des Codes C und können also korrigiert werden.*

Bemerkung 49.12 *Häufig ist $q = 2^f$ eine 2-er Potenz. Dann kann man aus dem Reed-Solomon Code $C \leq \mathbb{F}_{2^f}^N$, $N = 2^f - 1$ der Dimension $k = N + 1 - d$ und mit Minmalabstand d einen binären linearen Code C' der Länge fN und Dimension fk konstruieren, indem man jedes Element von $\mathbb{F}_{2^f}$ als ein f-Tupel über $\mathbb{F}_2$ schreibt. Dieser Code hat i.a. denselben Minimalabstand d. Ersetzt man jedes Element von $\mathbb{F}_{2^f}$ durch ein $(f+1)$-Tupel von Elementen von $\mathbb{F}_2$, deren Summe 0 ergibt, so erhält man einen Code $\tilde{C}'$ mit Minimalabstand $\geq 2d$, Dimension fk und Länge $(f+1)N$.*

Wegen einfacher Codierung und Decodierung und der Fähigkeit Fehlerbündel zu korrigieren sind die Reed-Solomon Codes von großer praktischer Bedeutung.

49.5 Codes bei CD-Spielern

Die folgende Konstruktion von Codes, das sogenannte Interleaving erhöht die Größe der erkannten Fehlerbündel:

Definition 49.13 *Sei $C \subseteq \mathbb{F}_q^N$ ein Code und $t \in \mathbb{N}$. Durch* Interleaving der Tiefe *t entsteht ein Code $C^{(t)} \subseteq \mathbb{F}_q^{Nt}$ wie folgt: Schreibt man je t Codeworte $c^{(1)}, \ldots, c^{(t)}$ in C als Zeilen einer Matrix:*

$$M = \begin{pmatrix} c_1^{(1)} & c_2^{(1)} & \ldots & c_N^{(1)} \\ c_1^{(2)} & c_2^{(2)} & \ldots & c_N^{(2)} \\ \vdots & \vdots & \ldots & \vdots \\ c_1^{(t)} & c_2^{(t)} & \ldots & c_N^{(t)} \end{pmatrix}$$

so erhält man ein Codewort $(c_1^{(1)}, c_1^{(2)}, \ldots, c_1^{(t)}, c_2^{(1)}, \ldots, c_N^{(t)}) \in C^{(t)}$ indem man die Spalten von M hintereinanderschreibt, also

$$C^{(t)} = \{(c_1^{(1)}, c_1^{(2)}, \ldots, c_1^{(t)}, c_2^{(1)}, \ldots, c_N^{(t)}) \in \mathbb{F}_q^{Nt} \mid c^{(1)}, \ldots, c^{(t)} \in C\}.$$

Beispiel:

$C \leq \mathbb{F}_2^3$ mit Erzeugermatrix $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$. Interleaving der Tiefe 2 macht z.B. aus den beiden Codeworten (110), (101) mit Hilfe der Matrix $M := \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ das Wort $(111001) \in C^{(2)}$. Eine Erzeugermatrix von $C^{(2)}$ ist

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

Bemerkung (i) Ist $C \leq \mathbb{F}_q^N$ ein linearer Code der Dimension k, so ist $C^{(t)} \leq \mathbb{F}_q^{Nt}$ ein linearer Code der Dimension kt.
Eine Basis von $C^{(t)}$ erhält man, indem man alle Matrizen M betrachtet, in denen genau eine Zeile $\neq 0$ ist und diese Zeilen die Basisvektoren von C durchlaufen läßt.
(ii) Erkennt C Fehlerbündel der Länge b, so erkennt $C^{(t)}$ Fehlerbündel der Länge bt.
(iii) Es gilt jedoch $d(C^{(t)}) = d(C)$.

Satz 49.14 *Ist $C_g \trianglelefteq \mathbb{F}_q[x]/(x^N - 1)$ ein zyklischer Code mit Erzeugerpolynom $g = g(x) \mid x^N - 1$ und ist $h(x) := g(x^t)$, dann ist $h(x)$ ein Teiler von $x^{Nt} - 1$ und $C_g^{(t)} = C_h \trianglelefteq \mathbb{F}_q[x]/(x^{Nt} - 1)$.*

Eine Variante: Cross-Interleaving:
Beispiel:
Sei $C_1 := \tilde{H}_7(2)$ der erweiterte Hamming-Code mit Erzeugermatrix

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

Sei $C_2 := C_g \trianglelefteq \mathbb{F}_2[x]/(x^7 - 1)$ der zyklische Code mit Erzeugerpolynom $g := (x+1)(x^3 + x + 1) = (x^4 + x^3 + x^2 + 1)$. Dann ist $\dim(C_2) = 3$ und

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

eine Erzeugermatrix für C_2.

Zum Cross-Interleaving betrachten wir folgende Konstruktion: Wähle 3 (=$\dim(C_2)$) Codeworte aus C_1 als Zeilen einer Matrix z.B.

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

In C_2 gibt es zu jeder Spalte von M_1 genau ein Codewort, das mit den 3 Zahlen beginnt, dieses schreiben wir als Zeile einer Matrix

$$M_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Auf M_2 wenden wir dann Interleaving etwa zur Tiefe 2 an, d.h. wir lesen die Einträge von M_2 in der Reihenfolge $11, 21, 12, 22, 13, 23, ..., 77, 87, 78, 88$ und erhalten so das Codewort

10 01 11 11 10 00 01 00 00 11 00 11 11 11 01 10 11 11 01 00 10 11 11 11 00 00 11 00

der Länge $8 \cdot 7 = 56$.

Definition 49.15 *Seien $C_1 \leq \mathbb{F}_q^{N_1}$ und $C_2 \leq \mathbb{F}_q^{N_2}$ zwei Codes. Sei (I_k, P_{N_2-k}) eine Erzeugermatrix von C_2, $k := \dim(C_2)$ und $t \in \mathbb{N}$ ein Teiler von N_1. Der* Cross-Interleaved *Code $C := CI(C_1, C_2, t) \leq \mathbb{F}_q^{N_1 N_2}$ besteht aus all den Worten in $\mathbb{F}_q^{N_1 N_2}$ die man wie folgt erhält: Man schreibe k Codeworte von C_1 als Zeilen einer Matrix M_1, interpretiere die Spalten von M_1 als Informationsbits für den Code C_2 und schreibe die entsprechenden N_1 Codeworte von C_2 als Zeilen einer Matrix M_2. Auf diese Matrix wendet man dann Interleaving zur Tiefe t an und erhält so ein Codewort von C. Der Code C_1 heißt der* innerer Code *und der Code C_2 der* äußere Code.

Beispiel (Forsetzung).
Die Fehlerkorrektur mit dem Cross-Interleaved Code:
Der äußere Code wird im wesentlichen zur Fehlererkennung (und weniger zur Fehlerkorrektur) benutzt. Er sagt dem inneren Code, wo eventuell Fehler aufgetreten sind, so daß diese dann von C_1 korrigiert werden können.

In unserem Beispiel hat der äußere Code C_2 Minimalabstand 4.

Angenommen, wir empfangen

01 10 00 10 10 00 01 00 01 11 00 11 11 11 01 10 11 11 01 00 10 11 11 11 00 00 11 00

anstelle des obigen Wortes. Durch De-Interleaving der Tiefe 2 erhalten wir die Matrix

$$M_2' = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} & 1 & 1 & 0 & 0 \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & \mathbf{1} & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

(die Fehler sind fett gedruckt).

In den ersten beiden Zeilen stehen Fehlerbündel der Länge 3 bzw. 4. Diese werden vom Code C_2 erkannt. In der 4. Zeile ist ein einzelner Fehler aufgetreten. Den könnte man mit C_2 sogar korrigieren, jedoch begnügt man sich meist mit der Fehlererkennung. C_2 gibt also an C_1 die Matrix

$$M_1' = \begin{pmatrix} - & - & 0 & - & 0 & 1 & 1 & 1 \\ - & - & 0 & - & 1 & 0 & 1 & 1 \\ - & - & 1 & - & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Da der Minimalabstand von C_1 auch 4 ist, gibt es genau eine Art, die fehlenden Positionen (sogenannte Auslöschungen) durch Symbole zu ersetzen, so daß die Zeilen von M_1' Codeworte von C_1 sind. Damit wird das Codewort richtig decodiert.

Beim CD-Spieler verwendet man für den inneren Code einen Code der Länge 28 und Dimension 24 über $\mathbb{F}_{2^8}$ und einen äußeren Code C_2, der Länge 32 und Dimension 28 über $\mathbb{F}_{2^8}$. Beide Codes sind verkürzte Reed-Solomon Codes.

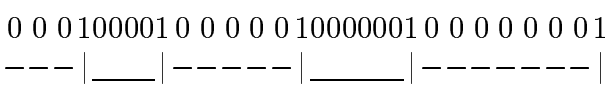
Technische Codierung auf der CD

Auf der CD wird Musik nicht wie auf der Schallplatte als Wellen sondern als Folge von Binärzahlen, die das Tonsignal an festen diskreten Zeiten darstellen, abgespeichert. Bei jeder Signalauswertung wird die Amplitude der Schallwelle gemessen und erhält eine ganze Zahl zwischen 1 und $2^{16}-1$ zugeordnet, die als binäres 16-Tupel geschreiben wird und als Paar von 2 Zahlen in $\mathbb{F}_{2^8}$ aufgefaßt wird. Man gibt pro Signalauswertung 2 Werte an, für jeden Lautsprecher einen. Das Signal wird 44100 mal pro Sekunde ausgewertet. Jede Signalauswertung liefert also 4 Zahlen in $\mathbb{F}_{2^8}$.

Zur Codierung werden 6 aufeinanderfolgende Signalauswertungen zu einem Informationswort $\in \mathbb{F}_{2^8}^{24}$ zusammengefaßt und mit dem inneren Code C_1 zu einem Codewort in $\mathbb{F}_{2^8}^{28}$ codiert. 28 dieser Codeworte werden dann in einer Matrix untereinandergeschrieben, deren Spalten dann als Informationsworte für den äußeren Code C_2 dienen. Dabei wird eine Abwandlung des normalen Interleaving der Tiefe 28 vewendet. Man erhält 28 Codeworte in C_2 der Länge 32 über $\mathbb{F}_{2^8}$. Diese werden nochmals geschickt umgeordnet um später fehlerhafte Daten besser interpolieren zu können.

Zusätzlich wird noch ein weiteres Symbol aus $\mathbb{F}_{2^8}$ angehängt, das Informationen zur Steuerung enthält.

Auf der CD selbst werden die 01-Folgen durch unterschiedliche Tiefen in der spiralförmig laufenden Spur dargestellt, dabei bedeutet eine Höhenänderung eine 1, gleichbleibende Tiefe eine 0:



Die Übergänge können durch den Wechsel der Intensität eines reflektierten Laserstrahls, der die spiralförmige Spur verfolgt erkannt werden. Aus technischen Gründen müssen dabei die Stücke gleicher Höhe eine gewisse Minimallänge haben. Für die Binärtupel bedeutet dies, daß zwischen je zwei Einsen zwischen 2 und 10 Nullen stehen müssen.

Da die Codeworte in C_2, die wir als Folgen von $32 \cdot 8 = 256$ binären Symbolen auffassen können, diese Forderung i.a. nicht erfüllen, werden die Symbole aus $\mathbb{F}_{2^8}$ in Binärfolgen der Länge 14 codiert, die diese Eigenschaft haben. Jede dieser 14-bit Folgen erhält noch 3 zusätzliche Pufferbits, um die nächste Folge anhängen zu können. Dies geschieht mit einer Tabelle.

Anschließend wird noch ein 24-bit Folge für Synchronisationszwecke sowie 3 zusätzliche Pufferbits angehängt, d.h. man hat

$$17 \cdot 33 + 24 + 3 = 588$$

bits um 6 Signalauswertungen zu codieren, d.h. der CD-Spieler muß beim Decodieren

$$(44100 \cdot 588)/6 = 4321800$$

Bits pro Sekunde verarbeiten.

Beim Decodieren wird der Code C_2, der wegen $d(C_2) = 5$ zwei Fehler korrigieren kann, nur zur Fehlerkorrektur eines Fehlers benutzt. Es werden jedoch mit Sicherheit zwei und drei Fehler und mit hoher Wahrscheinlichkeit 4 Fehler erkannt. Diese werden als Auslöschungen für den inneren Code C_1 markiert.

Mit diesem Decodierverfahren können Fehlerbündel von etwa 3000 Audiodaten (Spurlänge $\sim 2,5mm$) korrigiert werden. Durch die zusätzliche Umordnung im Code C_1 gelingt es sogar Fehlerbündel von bis zu 9000 Audiodaten (Spurlänge $\sim 7,7mm$) durch Korrektur und Interpolation auszugleichen.

Literatur

[Bo98] M. Bossert, *Kanalcodierung.* Teubner Verlag Stuttgart, (1998)

[CS93] J. H. Conway, N. J. A. Sloane, *Sphere packings, lattices and groups.* Springer Grundlehren der mathematischen Wissenschaften 290 (3. Ausgabe 1999)

[Ju95] D. Jungnickel, *Codierungstheorie.* Sektrum Akademischer Verlag (1995)

[MS77] F.L. MacWilliams, N. J. A. Sloane, *The theory of Error-Correcting Codes.* North-Holland (1977)

[vL82] J.H. van Lint, *Introduction to Coding Theory.* Springer Graduate Text in Mathematics 86 (3. Ausgabe 1999)

Index

Äquivalenz von Codes, 2

BCH-Code, 23

Charakteristik eines Körpers, 14
Code, 1
Code, äußere, 29
Code, BCH, 23
Code, dualer, 4
Code, erweiterter, 7
Code, Hamming, 6
Code, Hexacode, 13
Code, innere, 29
Code, linearer, 2
Code, linearer binärer, 2
Code, perfekter, 7
Code, Reed-Solomon, 25
Code, zyklisch, 17
Cross-Interleaving, 28, 29

Einheitswurzel, 21
Erzeugermatrix, 2
Erzeugerpolynom, 19

Frobenius Automorphismus, 16

Gewicht, 3
größter gemeinsamer Teiler ganzer Zahlen, 10
größter gemeinsamer Teiler von Polynomen, 12

Hamming Abstand, 1
Hamming Code, 6
Hauptideal, 9
Hexacode, 13

Ideal, 9
Informationsrate, 1
Informationssymbole, 20
Interleaving, 27
irreduzibles Polynom, 12

Kontrollmatrix, 5
Kontrollsymbole, 20

MDD, minimal distance decoder, 2
Minimalabstand eines Codes, 1
minimaler Vertreter, 5

perfekter Code, 7
Prüfmatrix, 5
Prüfpolynom, 19
primitive N-te Einheitswurzel, 21
primitives Element, 14

Reed-Solomon Code, 25
Restklasse, 10
Restklassenring, 10
Ring, 8

selbstdualer Code, 4
Skalarprodukt, 4
Syndrom, 5

Teilbarkeit in ganzen Zahlen, 10
Teilbarkeit von Polynomen, 12

Zech Logarithmen, 16
zyklischer Code, 17