Teil IV

Codes

17

Lineare Codes

Lineare Codes werden in Kommunikationssystemen zur sicheren Übertragung von Nachrichten eingesetzt, etwa in der Telekommunikation und bei der Speicherung von Daten auf Compact Discs. In diesem Kapitel werden die grundlegenden Eigenschaften von linearen Codes behandelt, ein Algorithmus zur Berechnung des Minimalabstands linearer Codes vorgestellt, Schranken zur Abschätzung der Güte linearer Codes diskutiert und ein Verfahren zur Konstruktion guter linearer Codes spezifiziert.

17.1 Linearcodes

Nachrichten werden anhand räumlicher (Funk- oder Kabelstrecken) oder zeitlicher (magnetische, optische oder elektronische Datenträger) Kanäle übertragen. Äußere Einflüsse wie elektromagnetische Wechselwirkungen oder Beschädigungen der Datenträger können dazu führen, dass übertragene Daten gelöscht oder verfälscht werden. Deshalb fügt der Sender den zu übertragenden Daten Redundanz hinzu, damit der Empfänger Fehler in den empfangenen Daten erkennen oder sogar korrigieren kann. Ein allgemeines Datenübertragungsmodell zeigt die Abb. 17.1.

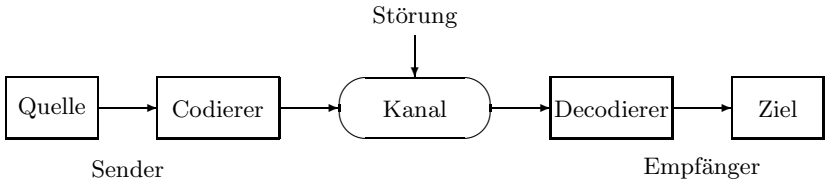

Abb. 17.1. Allgemeines Datenübertragungsmodell.

Blockcodes

Ein (M, n)-*Code* oder *Blockcode* ist eine Menge von M Wörtern der Länge n über $\mathbb{F}_q$. Die Elemente eines Blockcodes heißen *Codewörter*. Ein (M, n)-Code hat die *Informationsrate* $\log_q M/n$. Alle Vektoren werden im Folgenden als Zeilenvektoren geschrieben.

Beispiele 17.1. • Der *binäre Paritätskontrollcode* der Länge $n = k+1$ ist ein $(2^{n-1}, n)$-Code

$$C = \{(a_1, \ldots, a_n) \in \mathbb{F}_2^n \mid a_1 + \cdots + a_n = 0\}. \tag{17.1}$$

An jede Nachricht $(a_1, \ldots, a_{n-1})$ wird ein *Paritätsbit* a_n angehängt, so dass alle Codewörter gerade Parität besitzen. Der *Lochstreifencode* ist von dieser Form.

- Der *binäre dreifache Wiederholungscode* der Länge $n = 3k$ ist ein $(2^k, 3k)$-Code

$$C = \{(a_1, \ldots, a_k, a_1, \ldots, a_k, a_1, \ldots, a_k) \mid a \in \mathbb{F}_2^k\}. \tag{17.2}$$

Linearcodes

Ein *linearer Codierer* ist eine injektive lineare Abbildung $g : \mathbb{F}_q^k \to \mathbb{F}_q^n$. Das Bild eines linearen Codierers g ist also ein k-dimensionaler Unterraum von $\mathbb{F}_q^n$:

$$C = \{g(a) \mid a \in \mathbb{F}_q^k\}. \tag{17.3}$$

Der Blockcode C heißt $[n, k]$-*Code* oder *Linearcode* der Länge n und Dimension k über $\mathbb{F}_q$. Ein $[n, k]$-Code über $\mathbb{F}_q$ enthält q^k Elemente und hat somit die Informationsrate k/n. Die Elemente von $\mathbb{F}_q^k$ heißen *Nachrichten* und die Elemente eines Linearcodes *Codevektoren*.

Eine lineare Abbildung $g : \mathbb{F}_q^k \to \mathbb{F}_q^n$ wird durch Rechtsmultiplikation mit einer $k \times n$-Matrix G über $\mathbb{F}_q$ realisiert

$$g(a) = aG \quad \text{für alle } a \in \mathbb{F}_q^k. \tag{17.4}$$

Die Matrix G wird *Generatormatrix* von C genannt. Jede weitere Generatormatrix G' von C wird durch Linksmultiplikation mit einer regulären $k \times k$-Matrix L erhalten

$$G' = LG. \tag{17.5}$$

Die Matrix L bewirkt elementare Zeilenumformungen von G und induziert somit einen Basiswechsel von C.

Ein linearer Codierer $g : \mathbb{F}_q^k \to \mathbb{F}_q^n$ heißt *systematisch*, wenn die zugehörige Generatormatrix G *kanonisch* ist, d. h., von der Gestalt

$$G = \left(I_k \; A \right), \tag{17.6}$$

wobei I_k die $k \times k$-Einheitsmatrix ist. Ein systematischer Codierer $g : \mathbb{F}_q^k \to \mathbb{F}_q^n$ hängt an jede Nachricht $n - k$ Kontrollstellen an

$$aG = (a, aA), \quad a \in \mathbb{F}_q^k. \tag{17.7}$$

Beispiele 17.2. • Der binäre Paritätskontrollcode der Länge $n = k+1$ ist ein $[n, k]$-Code mit der kanonischen Generatormatrix

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

- Der binäre dreifache Wiederholungscode der Länge $n = 3k$ ist ein $[3k, k]$-Code mit der kanonischen Generatormatrix

$$G = \left(I_k \; I_k \; I_k \right).$$

- Sei C ein binärer $[5, 2]$-Code mit kanonischer Generatormatrix

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

  Der Code C besteht aus den Codevektoren $(00)\,G = 00000$, $(10)\,G = 10110$, $(01)\,G = 01111$ und $(11)\,G = 11001$.

Der duale Code

Sei $\langle , \rangle : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ die *Standard-Bilinearform* auf $\mathbb{F}_q$

$$\langle u, v \rangle = uv^T = \sum_{i=1}^{n} u_i v_i. \tag{17.8}$$

Der *duale Code* eines $[n, k]$-Codes C über $\mathbb{F}_q$ ist der zu C orthogonale Unterraum von $\mathbb{F}_q^n$

$$C^\perp = \{ v \in \mathbb{F}_q^n \mid \forall c \in C \; [vc^T = 0] \}. \tag{17.9}$$

Ein $[n, k]$-Code C heißt *selbstdual*, wenn $C^\perp = C$.

Satz 17.3. *Sei C ein $[n, k]$-Code über $\mathbb{F}_q$. Der duale Code $C^\perp$ ist ein $[n, n-k]$-Code über $\mathbb{F}_q$ und es gilt*

$$(C^\perp)^\perp = C. \tag{17.10}$$

Jede Generatormatrix von $C^\perp$ heißt eine *Kontrollmatrix* von C. Ferner ist nach (17.10) jede Generatormatrix von C auch eine Kontrollmatrix von $C^\perp$.

Satz 17.4. *Sei C ein $[n,k]$-Code über $\mathbb{F}_q$ mit der Kontrollmatrix H. Für jeden Vektor $v \in \mathbb{F}_q^n$ gilt $v \in C$ genau dann, wenn $Hv^T = 0$.*

Beweis. Die Zeilen $h^{(1)}, \ldots, h^{(n-k)}$ von H bilden eine Basis von $C^\perp$, da H eine Generatormatrix von $C^\perp$ ist. Sei $v \in C$. Für jedes $u \in C^\perp$ ist $uv^T = 0$. Dies gilt insbesondere für die Zeilenvektoren von H. Also folgt $Hv^T = 0$.

Sei $Hv^T = 0$, also $h^{(i)}v^T = 0$ für $1 \le i \le n-k$. Da die Zeilenvektoren $h^{(i)}$ eine Basis von $C^\perp$ bilden, ist $wv^T = 0$ für jedes $w \in C^\perp$. Also ist $v \in (C^\perp)^\perp$ und somit wegen (17.10) sogar $v \in C$. □

Lemma 17.5. *Ein $[n,k]$-Code mit kanonischer Generatormatrix $G = \begin{pmatrix} I_k & A \end{pmatrix}$ hat die Kontrollmatrix $H = \begin{pmatrix} -A^T & I_{n-k} \end{pmatrix}$.*

Beispiele 17.6. • Der duale Code des binären $[k+1,k]$-Paritätscodes ist ein $[k+1,1]$-Code mit der Generatormatrix

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

- Der duale Code des binären $[3k,k]$-Wiederholungscodes ist ein $[3k,2k]$-Code mit der Generatormatrix

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

- Der duale Code des binären $[5,2]$-Codes aus 17.2 ist ein $[5,3]$-Code mit der Generatormatrix

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

17.2 Fehlerkorrigierende Linearcodes

Übertragungskanal

In einem gestörten nachrichtentechnischen Kanal können eingespeiste Zeichen in andere Zeichen verwandelt werden. Dabei wird davon ausgegangen, dass die empfangenen Zeichen zufällig (im Sinne von Wahrscheinlichkeiten) von den gesendeten abhängen.

In einem (gedächtnisfreien) *q-nären symmetrischen Kanal* über dem Körper $\mathbb{F}_q$ wird ein Zeichen mit der *Symbolfehlerwahrscheinlichkeit* p in ein anderes Zeichen verwandelt, wobei keines der übrigen $q-1$ Zeichen bevorzugt wird. Die bedingte Wahrscheinlichkeit dafür, dass das Zeichen α in den Kanal eingegeben und das Zeichen β ausgegeben wird, ist

$$P(\beta|\alpha) = \begin{cases} 1-p, \text{ falls } \alpha = \beta, \\ \frac{p}{q-1}, \quad \text{falls } \alpha \neq \beta. \end{cases} \tag{17.11}$$

Im Folgenden wird für den jeweilig zu Grunde liegenden Kanal vorausgesetzt, dass die Wahrscheinlichkeit, ein Zeichen richtig zu übertragen, größer ist als die Wahrscheinlichkeit, es falsch zu übermitteln, also $p < \frac{1}{2}$. Der für die Anwendung wichtigste Kanal ist der *binär symmetrische Kanal* (Abb. 17.2).

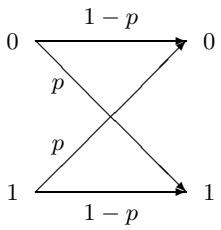

Abb. 17.2. Binär symmetrischer Kanal.

Sei C ein Blockcode der Länge n über $\mathbb{F}_q$. Die bedingte Wahrscheinlichkeit dafür, dass ein Codewort $c \in C$ in den gedächtnislosen Kanal eingegeben und ein Vektor $y \in \mathbb{F}_q^n$ empfangen wird, ist definiert durch

$$P(y|c) = \prod_{i=1}^{n} P(y_i|c_i). \tag{17.12}$$

Der Decodierer sucht zum empfangenen Vektor y ein Codewort, das höchstwahrscheinlich gesendet wurde, also ein Codewort c mit maximaler Übergangswahrscheinlichkeit unter allen Codewörtern

$$P(y|c) = \max\{P(y|c') \mid c' \in C\}. \tag{17.13}$$

Ein solcher Decodierer wird *Maximum-Likelihood-Decodierer*, kurz *ML-Decodierer*, genannt.

Bei der Übertragung eines Codeworts $c \in C$ seien i Fehler aufgetreten. Der *Fehlervektor* $e = y - c$ hat dann i von 0 verschiedene Komponenten und für die Übergangswahrscheinlichkeit gilt

$$P(E = e) = P(y|c) = (\frac{p}{q-1})^i (1-p)^{n-i}. \tag{17.14}$$

Nach der Voraussetzung $p < \frac{1}{2}$ wird die Übergangswahrscheinlichkeit $P(y|c)$ maximal für jedes Codewort c, das sich von y um eine minimale Anzahl von Stellen unterscheidet. Der gestörten Kanal kann als Addierer interpretiert werden, der zum gesendeten Codewort einen zufälligen Fehlervektor addiert (Abb. 17.3).

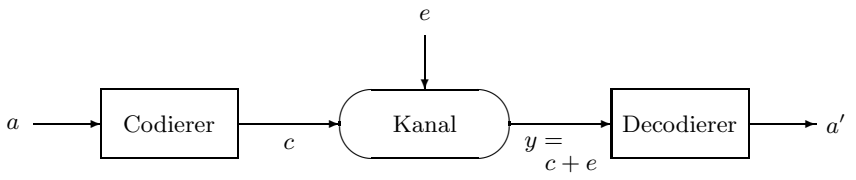

Abb. 17.3. Gestörter Kanal als zufälliger Addierer.

Beispiel 17.7. Sei C der binäre $[5, 2]$-Code aus 17.2. Die Codewörter werden durch einen binär symmetrischen Kanal mit Symbolfehlerwahrscheinlichkeit $p = 1/100$ übertragen.

Das Codewort $c = 10110$ werde in den Kanal eingegeben und das Wort $y = 11110$ empfangen, d. h., bei der Übertragung ist ein Fehler aufgetreten. Die Übergangswahrscheinlichkeiten sind

$$P(y|00000) = P(E = 11110) = p^4(1-p) = \frac{99}{100^5}$$
$$P(y|10110) = P(E = 01000) = p(1-p)^4 = \frac{99^4}{100^5}$$
$$P(y|01111) = P(E = 10001) = p^2(1-p)^3 = \frac{99^3}{100^5}$$
$$P(y|11001) = P(E = 00111) = p^3(1-p)^2 = \frac{99^2}{100^5}.$$

Ein ML-Decodierer ermittelt $c' = 10110$ als den gesendeten Codevektor und liegt damit richtig.

Sei $y = 11111$ der empfangene Vektor, d. h., bei der Übertragung sind zwei Fehler passiert. Die Übergangswahrscheinlichkeiten sind

$$P(y|00000) = P(E = 11111) = p^5 = \frac{1}{100^5}$$
$$P(y|10110) = P(E = 01001) = p^2(1-p)^3 = \frac{99^3}{100^5}$$
$$P(y|01111) = P(E = 10000) = p(1-p)^4 = \frac{99^4}{100^5}$$
$$P(y|11001) = P(E = 00110) = p^2(1-p)^3 = \frac{99^3}{100^5}.$$

Der ML-Decodierer bestimmt $c' = 01111$ als gesendeten Codevektor und begeht somit einen Decodierfehler.

Hamming-Abstand

Ein ML-Decodierer sucht ein Codewort, das sich vom empfangenen Vektor um eine minimale Anzahl von Komponenten unterscheidet. Der *Hamming-Abstand* zwischen zwei Vektoren $u, v \in \mathbb{F}_q^n$ ist die Anzahl der Komponenten, an denen sich u und v unterscheiden

$$d(u, v) = |\{i \mid u_i \neq v_i\}|. \tag{17.15}$$

Satz 17.8. *Der Hamming-Abstand $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{R}$ ist ein Metrik auf $\mathbb{F}_q^n$, d. h. für alle $u, v, w \in \mathbb{F}_q^n$ gilt*

- $d(u, v) = 0$ *genau dann, wenn* $u = v$.
- $d(u, v) = d(v, u)$.
- $d(u, w) \leq d(u, v) + d(v, w)$ *(Dreiecksungleichung).*

Beweis. Die ersten beiden Aussagen folgen direkt aus den Definitionen. Wir beweisen die Dreiecksungleichung. Aus $u_i \neq w_i$ folgt $u_i \neq v_i$ oder $w_i \neq v_i$. Also liefert die i-te Komponente zu $d(u, w)$ den Beitrag 1 und zu $d(u, v) + d(v, w)$ den Beitrag 1 oder 2. □

Korollar 17.9. *Für jede Metrik d auf $\mathbb{F}_q^n$ gilt*

$$d(u, v) \geq 0 \quad \textit{für alle } u, v \in \mathbb{F}_q^n. \tag{17.16}$$

Beweis. Es gilt definitionsgemäß $0 = d(u, u) \leq d(u, v) + d(v, u) = 2d(u, v)$, also $d(u, v) \geq 0$. □

Der Hamming-Abstand zweier Vektoren $u, v \in \mathbb{F}_q^n$ stimmt mit dem Hamming-Gewicht des Differenzvektors überein

$$d(u, v) = \mathrm{wt}(u - v), \tag{17.17}$$

wobei das *Hamming-Gewicht* von $v \in \mathbb{F}_q^n$ die Anzahl der von 0 verschiedenen Komponenten von v ist

$$\mathrm{wt}(v) = |\{i \mid v_i \neq 0\}|. \tag{17.18}$$

Beispielsweise ist $d(1110, 1001) = \mathrm{wt}(1110 - 1001) = \mathrm{wt}(0111) = 3$.

Fehlerkorrigierende Codes

Ein Blockcode C der Länge n über $\mathbb{F}_q$ heißt *t-Fehler-korrigierend*, wenn ein ML-Decodierer garantiert keinen Decodierfehler begeht, sofern bei der Übertragung höchstens t Fehler aufgetreten sind.

Sei C ein t-Fehler-korrigierender Blockcode. Sei c das gesendete Codewort, y der empfangene Vektor und beim Übertragen seien höchstens t Fehler passiert. Dann ist $d(c, y) \leq t$ und für alle übrigen Codewörter c' gilt $d(c', y) > t$. Das gesendete Codewort c ist also das eindeutig bestimmte Codewort mit dem kleinsten Hamming-Abstand zu y. Der empfangene Vektor y liegt in der *abgeschlossenen Kugel vom Radius t* um das gesendete Codewort

$$K_t(c) = \{v \in \mathbb{F}_q^n \mid d(c, v) \leq t\}. \tag{17.19}$$

In der Praxis ist die größte Zahl t von Interesse, für die ein Blockcode t-Fehler-korrigierend ist. Der *Minimalabstand* eines Blockcodes C ist der kleinste Hamming-Abstand zwischen den Codevektoren in C

$$d_C = \min\{d(c, c') \mid c, c' \in C, c \neq c'\}. \tag{17.20}$$

Ist C ein Linearcode, dann stimmt sein Minimalabstand wegen (17.17) mit dem *Minimalgewicht* der von 0 verschiedenen Codevektoren in C überein

$$d_C = \min\{\mathrm{wt}(c) \mid c \in C, c \neq 0\}. \tag{17.21}$$

Satz 17.10. *Ein Blockcode C der Länge n über $\mathbb{F}_q$ ist t-Fehler-korrigierend genau dann, wenn $d_C \geq 2t + 1$.*

Beweis. Ein Blockcode C ist t-Fehler-korrigierend genau dann, wenn die abgeschlossenen Kugeln $K_t(c)$ und $K_t(c')$ vom Radius t um je zwei verschiedene Codewörter c und c' disjunkt sind (Abb. 17.4). Dies ist genau dann der Fall, wenn der Hamming-Abstand zwischen je zwei verschiedenen Codewörtern mindestens $2t + 1$ beträgt. □

Ein $[n, k]$-Code mit dem Minimalabstand d wird als $[n, k, d]$-Code bezeichnet.

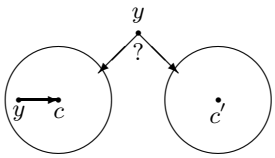

Abb. 17.4. ML-Decodierung.

Beispiele 17.11. • Der binäre $[3k, k]$-Wiederholungscode hat den Minimalabstand $d = 3$ und ist somit 1-Fehler-korrigierend.
- Der binäre $[5, 2]$-Code C aus 17.2 besitzt den Minimalabstand $d = 3$, denn für seine Codevektoren gilt $\mathrm{wt}(00000) = 0$, $\mathrm{wt}(10110) = 3$, $\mathrm{wt}(01111) = 4$ und $\mathrm{wt}(11001) = 3$. Also ist C ebenfalls 1-Fehler-korrigierend.

Satz 17.12. *Sei C ein $[n, k]$-Code über $\mathbb{F}_q$ mit Kontrollmatrix H und sei d eine natürliche Zahl. Sind je $d-1$ Spalten von H linear unabhängig, dann ist $d_C \geq d$.*

Beweis. Seien $h^{(1)}, \ldots, h^{(n)}$ die Spalten von H. Für jedes Codewort $c \in C$ gilt nach Satz 17.4

$$0 = Hc^T = \sum_{i=1}^{n} c_i h^{(i)}.$$

Sind je $d-1$ Spalten von H linear unabhängig, dann kann diese Gleichung nur bestehen, wenn jedes von 0 verschiedene Codewort Hamming-Gewicht $\geq d$ besitzt. □

Korollar 17.13. *Sei C ein $[n, k]$-Code über $\mathbb{F}_q$ mit einer Kontrollmatrix H, in der je $d-1$ Spalten linear unabhängig sind und es d linear abhängige Spalten gibt. Dann hat C den Minimalabstand $d_C = d$.*

Beispiel 17.14. Wir konstruieren einen 1-Fehler-korrigierenden ternären Linearcode der Länge $n \geq 3$. Hierzu betrachten wir alle Vektoren in $\mathbb{F}_3^3$, von denen je zwei linear unabhängig sind. Die folgende Liste von Vektoren besitzt diese Eigenschaft

001 010 011 012 100 110 120
111 121 112 122 101 102

Diese Liste ist ein Vertretersystem der eindimensionalen Unterräume von $\mathbb{F}_3^3$. Wir wählen $n \geq 3$ Vektoren aus dieser Liste und verwenden sie als Spalten einer Matrix. Hat diese Matrix den vollen Rang 3, dann ist sie Kontrollmatrix eines $[n, n-3]$-Codes. Dieser Code hat nach Satz 17.12 den Minimalabstand $d \geq 3$. Beispielsweise ist die Matrix

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

eine Kontrollmatrix eines $[9, 6]$-Codes mit dem Minimalabstand $d = 3$.

Fehlererkennende Codes

In manchen Fällen ist es ausreichend, Fehler zu erkennen und durch Rücksprache zu beheben. Ein ML-Decodierer eines Blockcodes C mit dem Minimalabstand d_C kann bis zu $d_C - 1$ *Fehler erkennen.* Wird nämlich ein Codewort c

gesendet, $y \in \mathbb{F}_q^n$ empfangen und sind höchstens $d_C - 1$ Fehler bei der Übertragung aufgetreten, dann ist $d(c, y) \leq d_C - 1$. Also kann y kein Codewort sein und der Fehler ist erkannt.

Beispiel 17.15. Der binäre $[k+1, k]$-Paritätskontrollcode hat den Minimalabstand $d = 2$ und ist somit 1-Fehler-erkennend. Dieser Fehler wird anhand der Parität des empfangenen Vektors erkannt.

Maximum-Likelihood-Decodierung

Sei C ein $[n, k]$-Code über $\mathbb{F}_q$ mit der Kontrollmatrix H. Die *Syndromabbildung* von C ist

$$\sigma_H : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k} : v \mapsto Hv^T. \tag{17.22}$$

Der Vektor $\sigma_H(v)$ heißt das *Syndrom* von $v \in \mathbb{F}_q^n$. Die Syndromabbildung ist surjektiv, weil H vollen Rang $n - k$ besitzt, und hat nach Satz 17.4 als Kern den Code C.

Der *affine Unterraum von* $\mathbb{F}_q^n$ *durch* $v \in \mathbb{F}_q^n$ *in Richtung* C ist definiert durch

$$v + C = \{v + c \mid c \in C\}. \tag{17.23}$$

Alle Elemente von $v + C$ haben dasselbe Syndrom $s = \sigma_H(v)$, denn für alle $c \in C$ gilt

$$\sigma_H(v + c) = \sigma_H(v) + \sigma_H(c) = \sigma_H(v). \tag{17.24}$$

Satz 17.16. *Die Zuordnung* $\psi : v + C \mapsto \sigma_H(v)$ *liefert eine Bijektion von der Menge aller affinen Unterräume von* $\mathbb{F}_q^n$ *in Richtung* C *auf* $\mathbb{F}_q^{n-k}$.

Jeder minimalgewichtige Vektor in $v + C$ wird *Minimalvektor* von $v + C$ genannt.

Satz 17.17. *Sei* C *ein* t*-Fehler-korrigierender Linearcode über* $\mathbb{F}_q$. *Jeder affine Unterraum von* $\mathbb{F}_q^n$ *in Richtung* C *enthält höchstens einen Vektor mit dem Hamming-Gewicht* $\leq t$.

Beweis. Seien e und e' Elemente von $v + C$ mit dem Hamming-Gewicht $\leq t$. Definitionsgemäß gibt es $c, c' \in C$ mit $e = v + c$ und $e' = v + c'$. Der Differenzvektor $e - e' = c - c'$ liegt in C und hat nach Annahme Hamming-Gewicht $\leq 2t$. Wegen Satz 17.10 hat C Minimalabstand $\geq 2t + 1$. Somit folgt $e - e' = 0$. □

Die Minimalvektoren e eines affinen Unterraums $v + C$ haben definitionsgemäß maximale Übergangswahrscheinlichkeit $P(E = e)$ unter allen Vektoren in $v + C$. Also lässt sich ein ML-Decodierer für C durch Alg. 17.1 spezifizieren. Dieser ML-Decodierer berechnet zum empfangenen Vektor y das Syndrom $s = \sigma_H(y)$, ermittelt den zugehörigen Minimalvektor $e = m(s)$ und liefert den Codevektor $y - e$ zurück.

Algorithmus 17.1 ML-DECODE(C, y)

Eingabe: Linearcode C, empfangener Vektor y
Ausgabe: decodierter Codevektor
1: $s := \sigma_H(y)$ {Syndrom von y}
2: $e := m(s)$ {Minimalvektor in $y + C$}
3: **return** $y - e$

Satz 17.18. *Sei C ein t-Fehler-korrigierender Linearcode über $\mathbb{F}_q$. Der Algorithmus* ML-DECODE$(C, \cdot)$ *decodiert stets richtig, wenn höchstens t Fehler aufgetreten sind.*

Beweis. Sei c ein gesendeter Codevektor und y der empfangene Vektor. Wir nehmen an, dass bei der Übertragung $\leq t$ Fehler aufgetreten sind. Dann hat der Fehlervektor $e = y - c$ Hamming-Gewicht $\leq t$ und ist nach Satz 17.17 der eindeutig bestimmte Minimalvektor von $y + C$. Also decodiert `ML-Decode` richtig. □

Beispiel 17.19. Sei C der binäre $[5, 2, 3]$-Code aus 17.2. Die affinen Unterräume von $\mathbb{F}_2^5$ in Richtung C mitsamt der zugehörigen Minimalvektoren und Syndrome zeigt das so genannte *Standard-Array*

s	$m(s)$	affiner Unterraum
000	00000	00000 10110 01111 11001
110	10000	10000 00110 11111 01001
111	01000	01000 11110 00111 10001
100	00100	00100 10010 01011 11101
010	00010	00010 10100 01101 11011
001	00001	00001 10111 01110 11000
011	01100	01100 11010 00011 10101
101	00101	00101 10011 01010 11100

Der ML-Decodierer kann entweder einen Übertragungsfehler korrigieren (anhand der Syndrome 100, 111, 100, 010, 001) oder zwei Übertragungsfehler erkennen (anhand der Syndrome 011 und 101).

17.3 Linearcodes von gleicher Qualität

Linearcodes mit denselben strukturiellen Eigenschaften werden isomorph genannt. Wir charakterisieren isomorphe Linearcodes und stellen einen Test auf Permutationsisomorphie vor.

Homomorphismen

Seien C und D Linearcodes über $\mathbb{F}$. Eine lineare Abbildung $\phi : C \to D$ heißt ein *Homomorphismus*, wenn $d(\phi(c), \phi(c')) \leq d(c, c')$ für alle $c, c' \in C$. Diese

Bedingung ist nach (17.17) und der Linearität von C und D gleichbedeutend mit $\mathrm{wt}(\phi(c)) \leq \mathrm{wt}(c)$ für alle $c \in C$.

Beispiele 17.20. Sei C ein Linearcode der Länge n über $\mathbb{F}$.

- Jede Linearform $\phi : C \to \mathbb{F}$ ist ein Homomorphismus.
- Ist D ein in C enthaltener Linearcode, dann ist die natürliche Einbettung $\iota : D \to C$ ein Homomorphismus.
- Die inverse Abbildung eines bijektiven Homomorphismus ist nicht notwendig ein Homomorphismus. Beispielsweise wird durch $\phi : 11 \mapsto 10$ ein bijektiver Homomorphismus von $C = \{00, 11\}$ auf $D = \{00, 10\}$ definiert. Die inverse Abbildung ist jedoch kein Homomorphismus.

Ein wichtiger Homomorphismus ist die Projektion. Sei I eine Teilmenge von $\underline{n}$. Die Abbildung $\pi_I : \mathbb{F}^n \to \mathbb{F}^{|I|} : x \mapsto (x_i)_{i \in I}$ heißt *Projektion von $\mathbb{F}^n$ in Richtung I*. Die Einschränkung von π_I auf einen Linearcode C der Länge n über $\mathbb{F}$ ist ein Homomorphismus von C auf $D = \pi_I(C)$, also

$$\pi_I : C \to D : c \mapsto \pi_I(c). \tag{17.25}$$

Beispiel 17.21. Bezeichnet C den binären $[5, 2]$-Code aus 17.2, dann liefert die Projektion π_I im Falle $I = \{3, 4, 5\}$ einen Homomorphismus von C auf $D = \{000, 110, 111, 001\}$.

Eine bijektive lineare Abbildung $\phi : C \to D$ heißt ein *Isomorphismus*, wenn $d(\phi(c), \phi(c')) = d(c, c')$ für alle $c, c' \in C$. Diese Bedingung ist gleichbedeutend mit $\mathrm{wt}(\phi(c)) = \mathrm{wt}(c)$ für alle $c \in C$. Ein Isomorphismus ist also eine *Isometrie*, d. h., eine bijektive lineare Abbildung, die die Hamming-Metrik respektiert. Die inverse Abbildung eines Isomorphismus' $\phi : C \to D$ ist wiederum ein Isomorphismus, denn für alle $u, v \in D$ gilt

$$d(\phi^{-1}(u), \phi^{-1}(v)) = d(\phi(\phi^{-1}(u)), \phi(\phi^{-1}(v))) = d(u, v). \tag{17.26}$$

Zwei Linearcodes C und D heißen *isomorph*, wenn es einen Isomorphismus von C auf D gibt.

Beispiel 17.22. Ein Linearcode C ist isomorph zu jedem Linearcode D, der aus C durch Anhängen einer festen Anzahl von Nullen an jeden Codevektor entsteht. Der Code D enthält dann *Nullspalten*. Ist $D = \{(c, 0) \mid c \in C\}$, dann ist $\phi : C \to D : c \mapsto (c, 0)$ ein Isomorphismus.

Ein Isomorphismus auf C wird *Automorphismus* von C genannt.

Satz 17.23. *Die Menge aller Automorphismen von C bildet mit der Komposition von Abbildungen eine Gruppe.*

Beweis. Die identische Abbildung id_C ist ein Automorphismus von C. Die inverse Abbildung eines Automorphismus von C ist, wie oben gezeigt, ein

Automorphismus von C. Die Komposition zweier Automorphismen ϕ und ϕ' von C ist ebenfalls ein Automorphismus, denn für alle $c, c' \in C$ gilt

$$d((\phi\phi')(c), (\phi\phi')(c')) = d(\phi(\phi'(c)), \phi(\phi'(c'))) = d(\phi(c), \phi(c')) = d(c, c').$$

□

Die Gruppe aller Automorphismen eines Linearcodes C wird als *Automorphismengruppe* von C, kurz $\mathrm{Aut}(C)$, bezeichnet.

Die Automorphismengruppe des vollen Codes $\mathbb{F}^n$

Der volle Code $C = \mathbb{F}^n$ ist ein $[n, n, 1]$-Code. Er hat eine bemerkenswert einfache Automorphismengruppe. Um sie herzuleiten, benötigen wir zwei grundlegende Automorphismen, Permutationen und Konfigurationen.

Jede Permutation σ vom Grad n induziert eine Abbildung $\sigma^* : \mathbb{F}^n \to \mathbb{F}^n$, die die Komponenten der Vektoren in $\mathbb{F}^n$ vertauscht

$$\sigma^*(v) = (v_{\sigma^{-1}(1)}, \ldots, v_{\sigma^{-1}(n)}). \tag{17.27}$$

Die Abbildung σ^* wird durch eine *Permutationsmatrix* vermittelt. Dies ist eine Matrix, die in jeder Zeile und Spalte genau einen Eintrag 1 und sonst lauter Nullen enthält, wobei sich die Einsen an den Stellen $(\sigma^{-1}(i), i)$, $1 \le i \le n$, befinden. Die Abbildung σ^* ist also eine bijektive lineare Abbildung, die das Hamming-Gewicht erhält, mithin ein Automorphismus von $\mathbb{F}^n$ ist.

Beispiel 17.24. Sei $\sigma = (123)$ ein Zykel vom Grad 3. Für jeden Vektor $v \in \mathbb{F}^3$ gilt

$$\sigma^*(v) = (v_3, v_1, v_2) = (v_1, v_2, v_3) \begin{pmatrix} 0\,1\,0 \\ 0\,0\,1 \\ 1\,0\,0 \end{pmatrix}.$$

Jeder Vektor $\alpha \in \mathbb{F}^n$ legt eine komponentenweise Multiplikation auf $\mathbb{F}^n$ fest

$$\alpha^*(v) = (v_1\alpha_1, \ldots, v_n\alpha_n). \tag{17.28}$$

Die Abbildung $\alpha^* : \mathbb{F}^n \to \mathbb{F}^n$ ist linear und wird durch eine Diagonalmatrix mit Diagonaleinträgen $\alpha_1, \ldots, \alpha_n$ vermittelt. Ein Vektor $\alpha \in \mathbb{F}^n$ heißt eine *Konfiguration*, wenn seine Komponenten sämlich von Null verschieden sind. Ist $\alpha \in \mathbb{F}^n$ eine Konfiguration, dann ist die Abbildung α^* bijektiv und erhält das Hamming-Gewicht. Sie ist folglich ein Automorphismus von $\mathbb{F}^n$.

Beispiel 17.25. Sei $\alpha = (2, 1, 2) \in \mathbb{F}_3^3$. Für jeden Vektor $v \in \mathbb{F}_3^3$ gilt

$$\alpha^*(v) = (2v_1, v_2, 2v_3) = (v_1, v_2, v_3) \begin{pmatrix} 2\,0\,0 \\ 0\,1\,0 \\ 0\,0\,2 \end{pmatrix}.$$

Die Komposition einer Permutation und einer Komposition liefert nach Satz 17.23 wiederum einen Automorphismus von $\mathbb{F}^n$

$$\Phi_{\sigma,\alpha}(v) = (\alpha^*\sigma^*)(v) = (v_{\sigma^{-1}(1)}\alpha_1, \ldots, v_{\sigma^{-1}(n)}\alpha_n). \tag{17.29}$$

Die Abbildungsmatrix der zusammengesetzten linearen Abbildung $\Phi_{\sigma,\alpha}$ ist das Produkt der Abbildungsmatrizen von α^* und σ^*. Dieses Produkt ist eine *monomiale Matrix*, eine Matrix, die in jeder Zeile und Spalte genau einen von Null verschiedenen Eintrag enthält. Dementsprechend wird $\Phi_{\sigma,\alpha}$ eine *monomiale Abbildung* auf $\mathbb{F}^n$ genannt.

Beispiel 17.26. Sei $\sigma = (123)$ ein Zykel vom Grad 3 und $\alpha = (2, 1, 2) \in \mathbb{F}_3^3$. Für jeden Vektor $v \in \mathbb{F}_3^3$ gilt

$$\begin{aligned}\Phi_{\sigma,\alpha}(v) &= (v_1, v_2, v_3)\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\begin{pmatrix}2&0&0\\0&1&0\\0&0&2\end{pmatrix} = (v_1, v_2, v_3)\begin{pmatrix}0&1&0\\0&0&2\\2&0&0\end{pmatrix}\\ &= (2v_3, v_1, 2v_2).\end{aligned}$$

Die Komposition zweier monomialer Abbildungen $\Phi_{\sigma,\alpha}$ und $\Phi_{\tau,\beta}$ ist wiederum eine monomiale Abbildung, denn für alle $v \in \mathbb{F}^n$ gilt

$$\begin{aligned}\Phi_{\tau,\beta}\Phi_{\sigma,\alpha}(v) &= \Phi_{\tau,\beta}(v_{\sigma^{-1}(1)}\alpha_1, \ldots, v_{\sigma^{-1}(n)}\alpha_n)\\ &= (v_{\sigma^{-1}(\tau^{-1}(1))}\alpha_{\tau^{-1}(1)}\beta_1, \ldots, v_{\sigma^{-1}(\tau^{-1}(n))}\alpha_{\tau^{-1}(n)}\beta_n)\\ &= (v_{(\tau\sigma)^{-1}(1)}\alpha_{\tau^{-1}(1)}\beta_1, \ldots, v_{(\tau\sigma)^{-1}(n)}\alpha_{\tau^{-1}(n)}\beta_n)\\ &= \Phi_{\tau\sigma,\tau^*(\alpha)\cdot\beta}(v),\end{aligned} \tag{17.30}$$

wobei $\tau^*(\alpha) \cdot \beta = (\alpha_{\tau^{-1}(1)}\beta_1, \ldots, \alpha_{\tau^{-1}(n)}\beta_n)$. Mithin folgt

$$\Phi_{\tau,\beta}\Phi_{\sigma,\alpha} = \Phi_{\tau\sigma,\tau^*(\alpha)\cdot\beta}. \tag{17.31}$$

Daraus kann die inverse Abbildung von $\Phi_{\sigma,\alpha}$ abgeleitet werden. Mit $\tau = \sigma^{-1}$ und $\beta = (\alpha^{-1}_{\tau^{-1}(1)}, \ldots, \alpha^{-1}_{\tau^{-1}(n)})$ gilt

$$\Phi_{\tau,\beta}\Phi_{\sigma,\alpha} = id_{\mathbb{F}^n}. \tag{17.32}$$

Die Menge aller monomialen Abbildungen auf $\mathbb{F}^n$ bildet also eine Gruppe, die *monomiale Gruppe* von $\mathbb{F}^n$. Diese Gruppe wird mit $\mathrm{Mon}_n(\mathbb{F})$ bezeichnet. Sie ist eine Untergruppe der Automorphismengruppe des vollen Codes $\mathbb{F}^n$. Es gilt aber der folgende

Satz 17.27. *Die Automorphismengruppe des vollen Codes $\mathbb{F}^n$ ist die monomiale Gruppe* $\mathrm{Mon}_n(\mathbb{F})$.

Beweis. Es bleibt zu zeigen, dass alle Automorphismen des vollen Codes $\mathbb{F}^n$ monomial sind. Sei ϕ ein Automorphismus von $\mathbb{F}^n$. Wir betrachten die Einheitsbasis von $\mathbb{F}^n$, d. h., die aus den Einheitsvektoren $e^{(i)}$ bestehende Basis von $\mathbb{F}^n$. Da ϕ das Hamming-Gewicht erhält, gilt für jeden Einheitsvektor $e^{(i)}$

$$\mathrm{wt}(\phi(e^{(i)})) = \mathrm{wt}(e^{(i)}) = 1.$$

Das Bild von $e^{(i)}$ ist also ein von Null verschiedenes Vielfaches eines Einheitsvektors. Es gibt also eine Permutation σ vom Grad n und eine Konfiguration $\alpha \in \mathbb{F}^n$, sodass ϕ die Einheitsbasis abbildet auf die Basis

$$\phi(e^{(i)}) = \alpha_{\sigma(i)} e^{(\sigma(i))}, \quad 1 \le i \le n.$$

Da jede lineare Abbildung vollständig festgelegt ist durch die Bilder der Einheitsbasis, ist ϕ monomial. □

Monomiale Abbildungen erhalten das Hamming-Gewicht. Also gilt der folgende

Satz 17.28. *Ist C ein Linearcode der Länge n über $\mathbb{F}$ und ist ϕ ein monomiale Abbildung auf $\mathbb{F}^n$, dann sind C und $\phi(C)$ isomorph.*

Die Automorphismengruppe eines Linearcodes

Satz 17.29. *Jeder Isomorphismus zwischen Linearcodes derselben Länge ist eine monomiale Abbildung.*

Beweis. Seien C und D Linearcodes der Länge n über $\mathbb{F}_q$ und sei $\phi : C \to D$ ein Isomorphismus. Die Codes C und D haben also dieselbe Dimension k.

Wir fassen die Codevektoren von C bzw. D zeilenweise in einer $q^k \times n$-Matrix $M(C)$ bzw. $M(D)$ zusammen. Wir zeigen zuerst, dass beide Matrizen dieselbe Anzahl von Nullspalten enthalten. Bezeichne n_C bzw. n_D die Anzahl der Nullspalten von C bzw. D. Jede Nichtnullspalte von $M(C)$ oder $M(D)$ hat nach dem Gleichverteilungsprinzip $q^{k-1}(q-1)$ von 0 verschiedene Einträge. Mithin folgt

$$\begin{aligned}(n-n_C)q^{k-1}(q-1) &= \sum_{c\in C} \mathrm{wt}(c) = \sum_{c\in C} \mathrm{wt}(\phi(c)) = \sum_{d\in D} \mathrm{wt}(d)\\ &= (n-n_D)q^{k-1}(q-1).\end{aligned}$$

Damit ist $n_C = n_D$ gezeigt.

Wir betrachten die Projektion $\pi_i : C \to \mathbb{F}_q : c \mapsto c_i$, $1 \le i \le n$. Diese Projektion liefert die i-Spalte der Matrix $M(C)$. Ist π_i nicht die Nullabbildung, d. h. die i-te Spalte von $M(C)$ keine Nullspalte, dann ist ihr Kern C_i ein $[n, k-1]$-Code.

Wir zeigen, dass von Null verschiedene Projektionen π_i und π_j linear abhängig sind, d. h. $\pi_i = \kappa\pi_j$ für ein $\kappa \in \mathbb{F}_q^*$, genau dann, wenn $C_i = C_j$. Sei $\pi_i(c) = \kappa\pi_j(c)$ für alle $c \in C$. Dann ist $\pi_i(c) = 0$ gleichbedeutend mit $\pi_j(c) = 0$, d. h. $C_i = C_j$. Umgekehrt seien $c, c' \in C$ mit $c_i \neq 0$ und $c'_i \neq 0$. Dann folgt $\pi_i = \kappa\pi_j$, wobei $\kappa = \frac{c_i}{c_j}$.

Zwei Spalten von $M(C)$ heißen *proportional*, wenn ein $\kappa \in \mathbb{F}_q^*$ existiert, sodass die eine Spalte ein κ-Vielfaches der anderen Spalte ist. Sei die i-te

Nichtnullspalte von $M(C)$ zu den s Spalten $i = i_1, \ldots, i_s$ proportional. Dann hat die Matrix $M(C')$ des Codes $C' = C_i$ genau $s + n_C$ Nullspalten. Nach den obigen Ausführungen hat dann auch die Matrix $M(D')$ von $D' = \phi(C')$ genau $s + n_D$ Nullspalten, und die s Nullspalten von $M(D')$, die von den s Nichtnullspalten $j = j_1, \ldots, j_s$ von $M(D)$ herrühren, sind ebenfalls proportional.

Wir zeigen, dass die i-te Spalte von $M(C)$ und die j-te Spalte von $M(D)$ proportional sind. Dazu wählen wir einen Vektor $v \in C \setminus C'$. Für seinen Bildvektor gilt $\phi(v) \in \phi(C \setminus C') = D \setminus D'$. Da C' ein $(k-1)$-dimensionaler Unterraum von C ist, hat jedes $c \in C$ eine eindeutige Darstellung der Form $c = c' + \kappa v$, wobei $c' \in C'$ und $\kappa \in \mathbb{F}_q$. Für die i-te Komponente von c gilt $c_i = \kappa v_i$. Aus $\phi(c) = \phi(c') + \kappa\phi(v)$ folgt wegen $\phi(c') \in D'$ sofort $\phi(c)_j = \kappa\phi(v)_j$. Mithin sind die beiden Spalten proportional mit dem Proportionalitätsfaktor $\phi(v)_j / v_i$. Damit ist alles bewiesen. □

Als Spezialfall ergibt sich der folgende

Satz 17.30. *Die Automorphismengruppe eines Linearcodes der Länge n über $\mathbb{F}$ ist eine Untergruppe von* $\mathrm{Mon}_n(\mathbb{F})$.

Beispiel 17.31. Der binäre $[n, 1, n]$-Wiederholungscode und der $[n, n-1, 2]$-Paritätskontrollcode haben beide die symmetrische Gruppe S_n als Automorphismengruppe.

Satz 17.32. *Seien C und D zwei $[n, k]$-Codes über $\mathbb{F}$. Sei G eine Generatormatrix von C und H eine Generatormatrix von D. Die Codes C und D sind isomorph genau dann, wenn es Matrizen $L \in \mathrm{Gl}_k(\mathbb{F})$ und $R \in \mathrm{Mon}_n(\mathbb{F})$ gibt, sodass $H = LGR$.*

Beweis. Sei $\phi : C \to D$ ein Isomorphismus. Dieser Isomorphismus wird nach Satz 17.23 durch eine monomiale Matrix $R \in \mathrm{Mon}_n(\mathbb{F})$ vermittelt, also $\phi(c) = cR$ für alle $c \in C$. Die Zeilen $h^{(1)}, \ldots, h^{(k)}$ von H bilden eine Basis von D. Deren Urbilder $h^{(1)}R^{-1}, \ldots, h^{(k)}R^{-1}$ bilden eine Basis von C. Andererseits bilden die Zeilen von G eine Basis von C. Aus dieser Basis wird jede weitere Basis von C durch Linksmultiplikation mit einer regulären Matrix $L \in \mathrm{Gl}_k(\mathbb{F})$ erhalten. Also gibt es eine reguläre Matrix $L \in \mathrm{Gl}_k(\mathbb{F})$ mit $LG = HR^{-1}$.

Umgekehrt seien $L \in \mathrm{Gl}_k(\mathbb{F})$ und $R \in \mathrm{Mon}_n(\mathbb{F})$ mit $LGR = H$. Dann ist LG ebenfalls eine Generatormatrix von C und R vermittelt nach Satz 17.32 einen Isomorphismus von C auf D. □

Beispiel 17.33. Die binären $[5, 2]$-Codes mit den Generatormatrizen

$$G = \begin{pmatrix} 1\,0\,1\,1\,0 \\ 0\,1\,1\,1\,1 \end{pmatrix} \quad \text{und} \quad H = \begin{pmatrix} 0\,1\,1\,1\,1 \\ 1\,0\,1\,1\,0 \end{pmatrix}$$

sind isomorph, denn es gilt

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

Eine Generatormatrix G eines $[n,k]$-Codes C kann durch elementare Zeilenumformungen in eine Matrix überführt werden, deren Spalten die Einheitsvektoren von $\mathbb{F}^k$ enthalten. Diese Matrix lässt sich durch Spaltenvertauschungen auf kanonische Form $H = \begin{pmatrix} I_k & A \end{pmatrix}$ bringen. Elementare Zeilenumformungen entsprechen einer Linksmultiplikation von G mit einer regulären Matrix $L \in \mathrm{Gl}_k(\mathbb{F})$ und Spaltenvertauschungen einer Rechtsmultiplikation mit einer Permutationsmatrix R. Es folgt $H = LGR$. Mit Satz 17.32 ergibt sich der folgende

Satz 17.34. *Jeder Linearcode ist isomorph zu einem Linearcode mit kanonischer Generatormatrix.*

Ein Test für Permutationsisomorphie

Zwei Linearcodes heißen *permutationsisomorph*, wenn es einen Isomorphismus zwischen den Codes gibt, die durch eine Permutationsmatrix vermittelt wird. Sei C ein Linearcode mit Generatormatrix G und D ein Linearcode mit Generatormatrix H. Nach Satz 17.32 sind C und D permutationsisomorph genau dann, wenn es eine reguläre Matrix $L \in \mathrm{Gl}_k(\mathbb{F})$ und eine Permutationsmatrix R gibt, sodass $H = LGR$.

Wir entwickeln einen Test auf Permutationsisomorphie, der auf zwei Beobachtungen fußt. Erstens bildet eine reguläre Matrix $L \in \mathrm{Gl}_k(\mathbb{F})$ je k linear unabhängige Spalten von G auf k linear unabhängige Spalten von HR^{-1} ab. Bezeichne $G_{*,I}$ die $k \times |I|$-Teilmatrix von G, die aus den Spalten mit den Indizes in $I \subseteq \underline{n}$ gebildet wird. Ist $G_{*,I}$ regulär, dann heißt I eine *Informationsmenge* von G. Ist I eine Informationsmenge von G, so ist auch $LG_{*,I}$ regulär und somit eine Informationsmenge von HR^{-1}. Eine reguläre Matrix L bildet also Informationsmengen auf Informationsmengen ab.

Zweitens unterscheiden sich die Matrizen H und HR^{-1} nur um die Spaltenpermutation $R' = R^{-1}$. Wir können diese Permutation vernachlässigen, wenn die Spalten beider Matrizen hinsichtlich einer festen totalen Ordnung sortiert sind. Die zu H gehörende sortierte Matrix wird mit $sort(H)$ bezeichnet. Folglich unterscheiden sich $k \times n$-Matrizen G und H um eine Spaltenpermutation genau dann, wenn $sort(G) = sort(H)$.

Beispiel 17.35. Hinsichtlich der lexikographen Ordnung der Spalten $(0 < 1)$ gilt

$$sort\left(\begin{pmatrix} 1\,0\,1\,1\,0 \\ 0\,1\,1\,1\,1 \\ 1\,0\,1\,0\,1 \end{pmatrix}\right) = \begin{pmatrix} 0\,0\,1\,1\,1 \\ 1\,1\,0\,1\,1 \\ 0\,1\,1\,0\,1 \end{pmatrix}.$$

Algorithmus 17.2 PermIsoTest(C, y)

Eingabe: Generatormatrizen G und H
Ausgabe: true falls permutationsisomorph, false sonst.

```
1: I := Informationsmenge von G
2: for all Informationsmenge J von H do
3:    L := H_{*,J} G_{*,I}^{-1}
4:    if sort(LG) = sort(H) then
5:       return true
6:    end if
7: end for
8: return false
```

Satz 17.36. *Seien C und D zwei $[n, k]$-Codes über $\mathbb{F}$. Sei G eine Generatormatrix von C und H eine Generatormatrix von D. Die Codes C und D sind permutationsisomorph genau dann, wenn* PermIsoTest(G, H) *den Wert* `true` *liefert.*

Beweis. Seien C und D permutationsisomorph. Definitionsgemäß gibt es eine reguläre Matrix $L \in \mathrm{Gl}_k(\mathbb{F})$ und eine Permutationsmatrix R, sodass $LGR = H$. Die Matrix L bildet die Informationsmenge I von G auf eine Informationsmenge J von D ab, die sicherlich in der Laufschleife generiert wird. Die Matrizen LG und H unterscheiden sich um eine Spaltenpermutation, woraus $sort(LG) = sort(H)$ folgt. Also liefert der Algorithmus `true`.

Umgekehrt liefere der Algorithmus `true`. Dann gibt es eine reguläre Matrix $L = H_{*,J} G_{*,I}^{-1}$ mit $sort(LG) = sort(H)$. Somit unterscheiden sich LG und H nur um eine Permutationsmatrix R und es folgt $LGR = H$. Mithin sind C und D permutationsisomorph. □

Beispiel 17.37. Wir betrachten binäre $[5, 2]$-Codes C und D mit Generatormatrizen

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

Eine Informationsmenge von G ist $I = \{1, 2\}$, also $G_{*,I} = I_2$. Die Informationsmengen von H sind $\{1, 3\}$, $\{1, 4\}$, $\{1, 5\}$, $\{2, 3\}$, $\{2, 4\}$, $\{2, 5\}$, $\{3, 5\}$ und $\{4, 5\}$. Für $J = \{2, 3\}$ gilt

$$L = H_{*,J} = \begin{pmatrix} 0\,1 \\ 1\,1 \end{pmatrix}, \quad \text{also} \quad LG = \begin{pmatrix} 0\,1\,0\,1\,1 \\ 1\,1\,1\,1\,0 \end{pmatrix}.$$

Die Matrizen LG und H unterscheiden sich nur um eine Spaltenvertauschung

$$sort(LG) = \begin{pmatrix} 0\,0\,1\,1\,1 \\ 1\,1\,0\,1\,1 \end{pmatrix} = sort(H).$$

Also sind beide Codes permutationsisomorph.

Die Komplexität von PermIsoTest hängt von der Anzahl der Informationsmengen von H ab. Schlimmstenfalls ist jede k-Teilmenge von $\underline{n}$ eine Informationsmenge. Der Code H besitzt dann $\binom{n}{k}$ Informationsmengen. Mithin ist D ein Code vom Geschlecht 0.

17.4 Berechnung des Minimalabstandes

Wir behandeln einen Algorithmus zur Berechnung des Minimalabstands eines Linearcodes. Zunächst stellen wir die Idee des Verfahrens vor. Sei C ein $[n,k]$-Code über $\mathbb{F}_q$. Wir konstruieren eine aufsteigende Folge von Teilmengen des Codes C

$$C_0 = \{0\} \subseteq C_1 \subseteq C_2 \subseteq C_3 \subseteq \ldots \tag{17.33}$$

und berechnen das Minimalgewicht jeder Teilmenge C_i

$$\overline{d}_i = \min\{\mathrm{wt}(c) \mid c \in C_i, c \neq 0\}. \tag{17.34}$$

Die Folge der Gewichte $\overline{d}_i$ ist schwach monoton fallend

$$\overline{d}_1 \geq \overline{d}_2 \geq \overline{d}_3 \geq \ldots. \tag{17.35}$$

Das Minimalgewicht der nicht in C_i liegenden Codevektoren wird nach unten abgeschätzt

$$\underline{d}_i = m(i+1) \leq \min\{\mathrm{wt}(c) \mid c \in C \setminus C_i\}, \tag{17.36}$$

wobei $m > 0$ eine noch festzulegende Konstante ist. Die Folge dieser Schranken ist streng monoton wachsend

$$\underline{d}_1 < \underline{d}_2 < \underline{d}_3 < \ldots. \tag{17.37}$$

Die beiden Folgen kreuzen sich, d. h., es gibt einen kleinsten Index i mit der Eigenschaft $\overline{d}_i \leq \underline{d}_i$. Der Minimalabstand von C ist dann $d_C = \overline{d}_i$ und ein minimalgewichtiger Codevektor liegt in C_i.

Der Algorithmus hat als Eingabe eine kanonische Generatormatrix $G = G_1$ von C

$$G_1 = \left(I_k \; A_1 \right). \tag{17.38}$$

Hat die Blockmatrix A_1 den Rang k, dann wird eine zweite Generatormatrix G_2 berechnet, wobei elementare Zeilenoperationen auf G_1 und Spaltenvertauschungen auf A_1 angewendet werden. Die resultierende Matrix hat die Form

$$G_2 = \left(B_2 \; I_k \; A_2 \right), \tag{17.39}$$

wobei die $k \times k$-Matrix B_2 aus der Einheitsmatrix I_k vermöge elementarer Zeilenoperationen entsteht. Hat auch A_2 den Rang k, wird diese Konstruktion fortgeführt. Seien $G_1, \ldots, G_m$ die auf diese Weise konstruierten Generatormatrizen.

Die Menge C_i besteht aus allen Codevektoren, die durch Nachrichten vom Hamming-Gewicht $\leq i$ vermöge der m Generatormatrizen codierbar sind

$$C_i = \bigcup_{j=1}^{m} \{aG_j \mid a \in \mathbb{F}_q^k,\ \mathrm{wt}(a) \leq i\}. \tag{17.40}$$

Die konstruierten Generatormatrizen erzeugen Linearcodes, die sich von C durch Spaltenvertauschungen unterscheiden. Jede solche Generatormatrix kann in eine Generatormatrix von C durch entsprechende Spaltenvertauschungen übergeführt werden. Eine explizite Konstruktion solcher Matrizen ist nicht notwendig, weil sich der Minimalabstand durch Spaltenvertauschungen nicht ändert.

Schließlich wird das Minimalgewicht der Codevektoren in C_i abgeschätzt. Ein Codevektor $c \in C$ liegt nicht in C_i genau dann, wenn zu jedem $j \in \{1, \ldots, m\}$ eine Nachricht $a^{(j)} \in \mathbb{F}_q^k$ mit dem Hamming-Gewicht $\geq i+1$ existiert, so dass $c = a^{(j)}G_j$. Der Codevektor

$$c = a^{(j)}G_j = a^{(j)} \left(B_j \ I_k \ A_j \right), \quad \mathrm{wt}(a^{(j)}) = i+1, \tag{17.41}$$

hat in den Spalten, an denen die Einheitsmatrix I_k steht, das Hamming-Gewicht $i+1$. Die Einheitsmatrizen I_k unterschiedlicher Generatormatrizen G_j stehen aber an disjunkten Spaltenpositionen. Also hat der Vektor c Hamming-Gewicht $\geq m(i+1)$. Eine untere Schranke für das Minimalgewicht der nicht in C_i liegenden Codevektoren ist also

$$\underline{d}_i = m(i+1). \tag{17.42}$$

Dieses Verfahren wird durch den *Brouwer-Zimmermann-Algorithmus* implementiert (Alg. 17.3). Die Effizienz dieses Algorithmus' hängt von der Anzahl der erzeugbaren Generatormatrizen ab. Je mehr Generatormatrizen erzeugt werden können, desto größer ist untere Schranke und desto schneller terminiert der Algorithmus.

Beispiel 17.38. Sei C ein binärer $[7, 3]$-Code mit der Generatormatrix

$$G_1 = \left(\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right).$$

Im Algorithmus wird noch eine zweite Generatormatrix konstruiert

$$G_2 = \left(\begin{array}{ccc|ccc|c} 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{array}\right).$$

Die Menge C_1 besteht aus den Zeilen der beiden Generatormatrizen und hat somit das Minimalgewicht $\overline{d}_1 = 4$. Die untere Schranke für das Minimalgewicht der nicht in C_1 liegenden Codevektoren ist $\underline{d}_1 = 4$. Folglich ist $d_C = \overline{d}_1 = 4$ der Minimalabstand von C.

Algorithmus 17.3 MINIMALDISTANCE(G)

Eingabe: Generatormatrix $G = G_1 = \left(I_k \; A_1 \right)$ eines Linearcodes C
Ausgabe: Minimalgewicht d von C

1: $m := 1$
2: **while** $\mathrm{rg}(A_m) = k$ **do**
3: bilde $G_{m+1} = \left(B_{m+1} \; I_k \; A_{m+1} \right)$ {aus $G_m = \left(B_m \; I_k \; A_m \right)$ durch elementare Zeilenumformungen und Spaltenvertauschungen von A_m, sodass A_m mit I_k beginnt}
4: $m := m + 1$
5: **end while**
6: $C_0 := \{0\}$
7: $i := 0$
8: **repeat**
9: $i := i + 1$
10: $C_i := C_{i-1} \cup \bigcup_{j=1}^{m} \{aG_j \mid a \in \mathbb{F}_q^k, \mathrm{wt}(a) = i\}$
11: $\overline{d}_i := \min\{\mathrm{wt}(c) \mid c \in C_i, c \neq 0\}$
12: $\underline{d}_i := m * (i + 1)$
13: **until** $\underline{d}_i \geq \overline{d}_i$
14: $d := \overline{d}_i$
15: **return** d

17.5 Schranken

Schranken geben darüber Auskunft, in welcher Weise die Parameter eines Linearcodes voneinander abhängen.

Singleton-Schranke

Satz 17.39. *Für jeden $[n, k]$-Code gilt*

$$d_C \leq n - k + 1. \tag{17.43}$$

Beweis. Sei C ein $[n, k]$-Code. O.B.d.A. besitze C eine kanonische Generatormatrix $G = (I_k \, A)$. Der i-te Einheitsvektor $e^{(i)}$ wird codiert zu $e^{(i)}G = (e^{(i)}, e^{(i)}A)$ und hat somit Hamming-Gewicht $\leq 1 + n - k$. □

Das *Geschlecht* eines $[n, k]$-Codes C ist die Zahl $n-k+1-d_C$. Ein Linearcode vom Geschlecht 0 genügt der Singleton-Schranke mit Gleichheit $d_C = n-k+1$ und wird *Maximum-Distance-Separable-Code (MDS-Code)* genannt.

Drei Linearcodes vom Geschlecht 0 gibt es für jede Länge n und über jedem Alphabet $\mathbb{F}_q$, den $[n, 1, n]$-Wiederholungscode, ein solcher Code hat die Generatormatrix

$$\left(1 \; 1 \; \ldots \; 1 \right),$$

den (vollen) $[n, n, 1]$-Code, ein solcher Code hat die Einheitsmatrix I_n als Generatormatrix, und den $[n, n-1, 2]$-Paritätskontrollcode, ein solcher Code hat die Generatormatrix

$$\left(\begin{array}{c|c} & -1 \\ I_{n-1} & \vdots \\ & -1 \end{array}\right).$$

Diese drei Lineararcodes werden als *triviale Codes* bezeichnet.

Satz 17.40. *Für jeden $[n, k]$-Code C über $\mathbb{F}_q$ sind äquivalent:*

- *C ist vom Geschlecht 0.*
- *In jeder Kontrollmatrix von C sind je $n-k$ Spalten linear unabhängig.*
- *$C^\perp$ ist vom Geschlecht 0.*
- *In jeder Generatormatrix von C sind je k Spalten linear unabhängig.*

Beweis. Nach Satz 17.4 und der Singleton-Schranke sind die ersten beiden Aussagen gleichwertig. Die Kontrollmatrizen von C sind genau die Generatormatrizen von $C^\perp$. Also sind auch die letzten beiden Aussagen äquivalent. Wir zeigen noch, dass die erste und dritte Aussage gleichwertig sind.

Sei C vom Geschlecht 0. Angenommen, $C^\perp$ enthielte einen Vektor $c \neq 0$ vom Hamming-Gewicht $\leq k$. Der Vektor c kann zu einer Basis von $C^\perp$ ergänzt werden, die dann als Zeilen einer Generatormatrix H von $C^\perp$ fungieren. Die zum Vektor c gehörende Zeile hat mindestens $n-k$ Nullen. Somit können nicht je $n-k$ Spalten von H linear unabhängig sein. Nach Satz 17.12 hat C widersprüchlicherweise Minimalabstand $< n-k+1$. Also hat $C^\perp$ den Minimalabstand $d^\perp \geq k+1$. Die Singleton-Schranke liefert für $C^\perp$ aber $d^\perp \leq n-(n-k)+1 = k+1$. Mithin besitzt $C^\perp$ den Minimalabstand $k+1$, d. h. $C^\perp$ ist vom Geschlecht 0. Wegen Satz 17.3 gilt auch die Umkehrung. □

Hamming-Schranke

Satz 17.41. *Für jeden $[n, k, d]$-Code über $\mathbb{F}_q$ gilt*

$$q^k \sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} (q-1)^i \leq q^n. \tag{17.44}$$

Die Gleichheit gilt genau dann, wenn die Vereinigung aller abgeschlossenen Kugeln vom Radius $\lfloor (d-1)/2 \rfloor$ um die Codewörter den gesamten Vektorraum $\mathbb{F}_q^n$ überdeckt.

Beweis. Die Anzahl der Vektoren, die von einem Vektor c den Hammingabstand i haben, ist $\binom{n}{i}(q-1)^i$. Denn es gibt $\binom{n}{i}$ Möglichkeiten, i Komponenten von c auszuwählen, und $(q-1)^i$ Möglichkeiten, diese Komponenten abzuändern. Die linke Seite der Ungleichung ist also die Anzahl der Vektoren in den abgeschlossenen Kugel vom Radius $\lfloor (d-1)/2 \rfloor$ um die Codewörter. Da diese Kugeln disjunkt sind, ist die Summe höchstens $|\mathbb{F}_q^n| = q^n$. □

Ein Linearcode heißt *perfekt*, wenn er die Hamming-Schranke (17.44) mit Gleichheit erfüllt. Zu den perfekten Codes gehören die Hamming-Codes.

Ein *m-ter binärer Hamming-Code* ist ein Linearcode, dessen Kontrollmatrix H_m aus den von 0 verschiedenen Elementen in $\mathbb{F}_2^m$ als Spalten gebildet wird. Das Vertauschen von Spalten liefert einen Code mit denselben Parametern, weshalb von dem m-ten binären Hamming-Code gesprochen wird. Die Kontrollmatrizen der ersten drei binären Hamming-Codes lauten

$$H_1 = \begin{pmatrix} 1 \end{pmatrix},$$
$$H_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$
$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Satz 17.42. *Für jede Zahl $m \geq 2$ ist der m-te binäre Hamming-Code ein perfekter $[2^m - 1, 2^m - m - 1, 3]$-Code.*

Beweis. Die Kontrollmatrix H_m ist eine $m \times (2^m - 1)$-Matrix vom Rang m. Also ist der m-te binäre Hamming-Code ein Linearcode der Länge $n = 2^m - 1$ und Dimension $k = 2^m - m - 1$. Je zwei Spalten von H_m sind voneinander verschieden und somit linear unabhängig über $\mathbb{F}_2$. Die Matrix H_m enthält wegen $m \geq 2$ wenigstens drei linear abhängige Spalten. Nach Satz 17.12 hat der m-te binäre Hamming-Code den Minimalabstand $d = 3$. Dieser Code ist perfekt, weil die Hamming-Schranke nach Satz 10.3 mit Gleichheit erfüllt wird

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

□

Der m-te binäre Hamming-Code C ist 1-Fehler-korrigierend. Nach Satz 17.17 liegen die Einheitsvektoren in verschiedenen affinen Unterräumen von $\mathbb{F}_2^{2^m-1}$ in Richtung C und sind somit Minimalvektoren. Andererseits gibt es genau 2^m Syndrome. Also gibt es außer den Einheitsvektoren und dem Nullvektor keine weiteren Minimalvektoren.

Griesmer-Schranke

Satz 17.43. *Für jeden $[n, k, d]$-Code über $\mathbb{F}_q$ gilt*

$$n \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil. \tag{17.45}$$

Beweis. Der Fall $k = 1$ ist klar. Sei $k \geq 2$ und $N_q(k, d)$ die Länge des kürzesten Linearcodes über $\mathbb{F}_q$ mit Dimension k und Minimalabstand d. Wir zeigen

$$N_q(k, d) \geq d + N_q(k - 1, \lceil d/q \rceil).$$

Sei C ein $[N_q(k, d), k, d]$-Code und $c \in C$ vom Hamming-Gewicht d. Der Vektor c kann zu einer Basis von C ergänzt werden, die dann als Zeilen einer Generatormatrix G von C fungieren. Der Vektor c kann durch Spaltenvertauschung in den Vektor $w = 1 \ldots 10 \ldots 0 = 1^d 0^{n-d}$ transformiert werden. Der resultierende Code besitzt eine Generatormatrix, die w als erste Zeile enthält

$$G = \left(\begin{array}{c|c} 1\ 1\ \ldots\ 1 & 0\ 0\ \ldots\ 0 \\ \hline G_1 & G_2 \end{array} \right),$$

wobei G_1 eine $(k-1) \times d$-Matrix und G_2 eine $(k-1) \times (N_q(k, d) - d)$-Matrix. Wir behaupten, dass G_2 den Rang $k-1$ hat. Andernfalls könnten wir nämlich annehmen, dass die erste Zeile von G_2 aus lauter Nullen bestünde. Die entsprechende Zeile von G_1 müsste dann lauter von 0 verschiedene Elemente enthalten. Durch elementare Zeilenumformungen könnte dann aber noch ein Eintrag der ersten Zeile von G zu 0 gemacht werden. Dieser Codevektor hätte dann widersprüchlicherweise das Gewicht $< d$. Also erzeugt G_2 einen $[N_q(k, d) - d, k - 1, d_2]$-Code C_2.

Sei $c = (c^{(1)}, c^{(2)}) \in C$ mit $c^{(2)} \in C_2$ und $\mathrm{wt}(c^{(2)}) = d_2$. Aus Anzahlgründen gibt es ein $\alpha \in \mathbb{F}_q$, das mindestens $\lceil d/q \rceil$-mal in $c^{(1)}$ vorkommt. Durch Subtrahieren des α-fachen der ersten Zeile w von G folgt

$$d \leq \mathrm{wt}(c - \alpha w) \leq (d - \lceil d/q \rceil) + d_2,$$

also $d_2 \geq \lceil d/q \rceil$ und damit $N_q(k-1, d_2) \geq N_q(k-1, \lceil d/q \rceil)$. Hieraus erhellt sich

$$d + \underbrace{N_q(k-1, d_2)}_{\geq N_q(k-1, \lceil d/q \rceil)} = N_q(k, d).$$

Diese Ungleichung liefert die Behauptung, wenn sie iteriert wird

$$N_q(k, d) \geq \ldots \geq \sum_{i=0}^{k-2} \lceil d/q^i \rceil + \underbrace{N_q(1, \lceil d/q^{k-1} \rceil)}_{= \lceil d/q^{k-1} \rceil} = \sum_{i=0}^{k-1} \lceil d/q^i \rceil.$$

□

Der duale Code des m-ten binären Hamming-Codes heißt *m-ter binärer Simplex-Code*.

Satz 17.44. *Der m-te binäre Simplex-Code ist ein $[2^m - 1, m, 2^{m-1}]$-Code, in dem alle von 0 verschiedenen Codevektoren das Hamming-Gewicht 2^{m-1} haben.*

Beweis. Jede Kontrollmatrix des m-ten binären Hamming-Codes ist eine Generatormatrix des m-ten binären Simplex-Codes. Also ist der m-te binäre Simplex-Code ein Linearcode der Länge $n = 2^m - 1$ und Dimension $k = m$. Die Spalten der Generatormatrix H_m des m-ten binären Simplex-Codes seien mit $h^{(1)}, \ldots, h^{(n)}$ bezeichnet. Dann wird eine Nachricht $a \in \mathbb{F}_2^m$ codiert zum Codewort

$$aH_m = (\langle a, h^{(1)}\rangle, \ldots, \langle a, h^{(n)}\rangle).$$

Die Linearform $\mathbb{F}_2^m \to \mathbb{F}_2 : h \mapsto \langle a, h\rangle$ ist surjektiv für jedes $a \neq 0$. Wenn h den Vektorraum $\mathbb{F}_2^m$ durchläuft, wird jeder Bildwert in $\{0, 1\}$ gleichoft angenommen, also (2^{m-1})-mal. Die Spalten $h^{(i)}$ von H sind die von 0 verschiedenen Vektoren in $\mathbb{F}_2^m$. Mithin besitzt der Codevektor aH_m das Hamming-Gewicht 2^{m-1}. □

Beispielsweise ist der duale Code des binären $[7, 4, 3]$-Hamming-Codes ein $[7, 3, 4]$-Simplex-Code. Die binären Simplex-Codes erreichen die Griesmer-Schranke mit Gleichheit.

Gilbert-Varshamov-Schranke

Satz 17.45. *Seien n, k und d natürliche Zahlen und eine Primzahlpotenz q mit*

$$\sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k}. \tag{17.46}$$

Dann gibt es einen $[n, k]$-Code über $\mathbb{F}_q$ mit dem Minimalabstand $\geq d$.

Beweis. Sei $n = k$. Die Ungleichung ist nur für $d = 1$ erfüllt. Der gesuchte Code ist der $[n, n, 1]$-Code $C = \mathbb{F}_q^n$.

Sei $n - k \geq 1$. Es wird ein $[n, k]$-Code über $\mathbb{F}_q$ anhand einer Kontrollmatrix

$$H = \begin{pmatrix} h^{(1)} & \ldots & h^{(n)} \end{pmatrix}$$

konstruiert, in der je $d - 1$ Spalten linear unabhängig sind. Dieser Code hat dann nach Satz 17.12 Minimalabstand $\geq d$.

Angenommen, eine $(n - k) \times i$-Matrix

$$H = \begin{pmatrix} h^{(1)} & \ldots & h^{(i)} \end{pmatrix},$$

in der je $\min\{i, d-1\}$ Spalten linear unabhängig sind, sei schon konstruiert. Für $i = 1$ braucht nur ein Vektor $h^{(1)} \neq 0$ gewählt zu werden. Jede Linearkombination aus höchstens $l = \min\{i, d-2\}$ der Vektoren $h^{(1)}, \ldots, h^{(i)}$ wird durch die Koeffizienten eindeutig festgelegt. Die Anzahl dieser Linearkombinationen ist

$$\sum_{j=0}^{l} \binom{i}{j} (q-1)^j.$$

Aufgrund der Ungleichung

$$\sum_{j=0}^{l} \binom{i}{j} (q-1)^j \leq \sum_{j=0}^{d-2} \binom{n-1}{j} (q-1)^j < q^{n-k}$$

existiert ein Vektor $h^{(i+1)}$ in $\mathbb{F}_q^{n-k}$, der keine derartige Linearkombination besitzt. Also sind in der um $h^{(i+1)}$ ergänzten $(n-k) \times (i+1)$-Matrix je $\min\{i+1, d-1\}$ Spalten linear unabhängig. □

Jede Schranke besitzt eine diskrete Version für feste Länge n und eine asymptotische Form für n gegen ∞. Letztere ergibt sich jeweils aus der diskreten Version, indem die Schranke als Funktion der Informationsrate $R = k/n$ und der Fehlerkorrekturrate $\lambda = d/n$ geschrieben wird. Auf diese Weise lässt sich die Singleton-Schranke $d \leq n - k + 1$ schreiben als

$$\lambda \leq 1 - R + 1/n. \tag{17.47}$$

Der Übergang $n \to \infty$ ergibt (bei festem R und λ) den asymptotisch zu verstehenden Ausdruck

$$\lambda \leq 1 - R. \tag{17.48}$$

Die asymptotische Version der Singleton-, Hamming- und Gilbert-Varshamov-Schranke für binäre Linearcodes zeigt die Abb. 17.5. Zu jedem binären Linearcode gibt es einen Punkt in diesem Graphen. Linearcodes mit hinreichend großer Länge und hohem Minimalabstand liegen in dem durch Hamming- und Gilbert-Varshamov-Schranke begrenzten Gebiet.

17.6 Modifikation und Kombination

Gute Linearcodes lassen sich oft durch sukzessive Modifikation und Kombination von bekannten Linearcodes erhalten.

Modifikation

Sei C ein $[n, k]$-Code über $\mathbb{F}_q$ mit der Generatormatrix

$$G = \left(g^{(1)} \; g^{(2)} \; \ldots \; g^{(n)} \right). \tag{17.49}$$

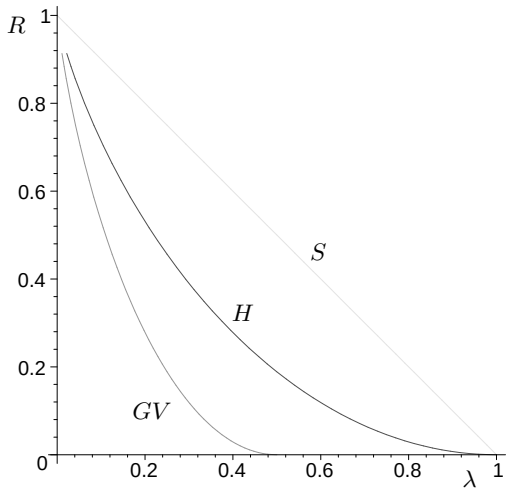

Abb. 17.5. Asymptotische Singleton- (S), Hamming- (H) und Gilbert-Varshamov-Schranke (GV) für binäre Linearcodes.

Der *erweiterte Code* von C entsteht aus C durch Anhängen einer Paritätsstelle

$$\mathrm{Par}(C) = \{(c_1, \ldots, c_n, c_{n+1}) \mid c \in C, c_{n+1} = -\sum_{i=1}^{n} c_i\}. \tag{17.50}$$

Dies ist ein $[n+1, k]$-Code mit der Generatormatrix

$$\left(g^{(1)}\ g^{(2)}\ \ldots\ g^{(n)}\ g^{(n+1)}\right), \quad \text{wobei} \quad g^{(n+1)} = -\sum_{i=1}^{n} g^{(i)}. \tag{17.51}$$

Für den Minimalabstand $P = \mathrm{Par}(C)$ gilt

$$d_C \leq d_P \leq d_C + 1. \tag{17.52}$$

Der erweiterte Code P eines binären Linearcodes C besteht nur aus Vektoren von geradem Gewicht. Ist also d_C ungerade, dann ist $d_P = d_C + 1$.

Beispiel 17.46. Der binäre $[7, 4, 3]$-Hamming-Code wird erzeugt von der Matrix

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

Der erweitere Code ist ein selbstdualer $[8,4,4]$-Code mit der Generatormatrix

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

Der *punktierte Code* von C ist ein Linearcode $\mathrm{Pu}(C)$, der aus C durch Streichen einer (hier der letzten) Komponente entsteht. Dieser Code hat die Generatormatrix

$$\left(g^{(1)}\ g^{(2)}\ \ldots\ g^{(n-1)} \right). \tag{17.53}$$

Beispiel 17.47. Der punktierte Code des $[7,4]$-Hamming-Codes ist ein $[6,4,2]$-Code mit der Generatormatrix

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

Die Generatormatrix von C kann (nach eventueller Zeilenumordnung) geschrieben werden in der Form

$$G = \left(\begin{array}{c|c} * & g_1^{(n)} \\ \hline & 0 \\ G' & \vdots \\ & 0 \end{array}\right). \tag{17.54}$$

Der *verkürzte Code* von C ist ein Linearcode $V(C)$, der von der Matrix G' erzeugt wird. Dieser Code ist also ein $[n-1,k-1]$-Code.

Beispiel 17.48. Der verkürzte Code des $[7,4,3]$-Hamming-Codes ist ein $[6,3,3]$-Code mit der Generatormatrix

$$G' = \begin{pmatrix} 1\,1\,0\,1\,0\,0 \\ 1\,0\,1\,0\,1\,0 \\ 0\,1\,1\,0\,0\,1 \end{pmatrix}.$$

Kombination

Sei C ein $[m,k]$-Code über $\mathbb{F}_q$ mit der Generatormatrix G und sei D ein $[n,l]$-Code über $\mathbb{F}_q$ mit der Generatormatrix H. Die *Summe* $C+D$ von C und D ist der Linearcode über $\mathbb{F}_q$ mit der Generatormatrix

$$\begin{pmatrix} G & 0 \\ 0 & H \end{pmatrix}. \tag{17.55}$$

Für diesen Code gilt

$$C + D = \{(c, d) \mid c \in C, d \in D\}. \tag{17.56}$$

Es handelt sich um einen $[m + n, k + l]$-Code mit dem Minimalabstand $\min\{d_C, d_D\}$, denn für alle $(c, d) \in C + D$ gilt $\mathrm{wt}(c, d) = \mathrm{wt}(c) + \mathrm{wt}(d)$.

Beispiel 17.49. Sei C der binäre $[4, 3, 2]$-Paritätskontrollcode und sei D der binäre $[3, 1, 3]$-Wiederholungscode. Die Summe $C + D$ ist ein binärer $[7, 4, 2]$-Code mit der Generatormatrix

$$\left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}\right).$$

Sei $m = n$. Die *Plotkin-Summe* von C und D über $\mathbb{F}_q$ ist ein Linearcode mit der Generatormatrix

$$\begin{pmatrix} G & G \\ 0 & H \end{pmatrix}. \tag{17.57}$$

Dieser Code wird mit $C \oplus D$ bezeichnet. Es gilt

$$C \oplus D = \{(c, c + d) \mid c \in C, d \in D\}. \tag{17.58}$$

Diese Konstruktion wird auch $u \mid u + v$-Konstruktion genannt, weil alle Codevektoren eben diese Gestalt besitzen.

Satz 17.50. *Sei C ein $[n, k]$-Code über $\mathbb{F}_q$ und D ein $[n, l]$-Code über $\mathbb{F}_q$. Die Plotkin-Summe $C \oplus D$ ist ein $[2n, k + l]$-Code mit dem Minimalabstand $\min\{2d_C, d_D\}$.*

Beweis. Die Aussagen über Länge und Dimension sind klar. Für den Hamming-Abstand zweier Codevektoren $(c, c + d)$ und $(c', c' + d')$ gilt

$$d(c, c') + d(c + d, c' + d') = \mathrm{wt}(c - c') + \mathrm{wt}(c - c' + d - d').$$

Im Falle $d = d'$ ist diese Summe gleich $2d(c, c') \geq 2d_C$. Andernfalls wird sie nach unten abgeschätzt durch

$$\mathrm{wt}(c - c') + \mathrm{wt}(d - d') - \mathrm{wt}(c - c') = \mathrm{wt}(d - d') \geq d_D.$$

□

Beispiel 17.51. Sei C der binäre $[4, 3, 2]$-Paritätscode und D der $[4, 1, 4]$-Wiederholungscode. Die Plotkin-Summe $C \oplus D$ ist ein selbstdualer $[8, 4, 4]$-Code mit der Generatormatrix

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right).$$

Suche nach guten Linearcodes

Für die Praxis werden $[n,k]$-Codes über $\mathbb{F}_q$ mit größtmöglichem Minimalabstand gesucht

$$d_q(n,k) = \max\{d \mid \text{es existiert ein } [n,k,d]\text{-Code über } \mathbb{F}_q\}. \quad (17.59)$$

Ein allgemeines Verfahren zur Berechnung von $d_q(n,k)$ für beliebige n, k und q gibt es (bislang) nicht.

Wir stellen ein Verfahren vor, mit dem Linearcodes modifiziert und kombiniert werden können, um neue, eventuell bessere Linearcodes zu erhalten. Die jeweils berechneten Linearcodes über $\mathbb{F}_q$ werden in einer Tabelle gespeichert. Anfangs ist die Tabelle leer. Sobald ein Code der Länge n über $\mathbb{F}_q$ in die Tabelle eingefügt wird, werden automatisch die trivialen Codes über $\mathbb{F}_q$ bis zur Länge n hinzugefügt. Ein $[n,k]$-Code über $\mathbb{F}_q$ wird eingefügt, wenn sein Minimalabstand entweder größer ist als der Minimalabstand der gespeicherten $[n,k]$-Codes, oder gleich ist dem Minimalabstand der gespeicherten $[n,k]$-Codes und der neue Code zu keinem der gespeicherten Codes isomorph ist. Für das Einfügen von Codes wird eine rekursive Prozedur (Alg. 17.4) benutzt. Diese Routine gewährleistet, dass die Tabelle *invariant* ist unter den verwen-

Algorithmus 17.4 UPDATE(C)

Eingabe: linearer Code C

```
 1: global T {Codetabelle}
 2: if C verbessert T then
 3:    T := T ∪ {C}
 4:    for all Modifikation P von C do
 5:       UPDATE(P)
 6:    end for
 7:    for all Modifikation P von C^⊥ do
 8:       UPDATE(P)
 9:    end for
10: end if
```

deten Modifikationen und unter Dualität. D. h., die Tabelle kann nicht durch Modifizierung oder Dualisierung der gespeicherten Codes verbessert werden. Eine invariante Tabelle lässt sich nur von außen durch das Einfügen neuer Codes verbessern. Invariante Tabellen mit unteren und oberen Schranken für den Minimalabstand wurden zuerst von T. Verhoeff erzeugt.

Hier sind drei neue Linearcodes über $\mathbb{F}_4$, die mit diesem Verfahren gefunden wurden

n	k	d	uS-oS	Spur
36	24	8	7-9	CyP3dP2P2
41	31	7	6-8	CyP3dP2P2P4dP2P2
44	8	27	26-28	CyP3dP2P2

In der Spalte uS-oS wird auf die von A. Brouwer verwaltete Tabelle der besten bekannten Linearcodes verwiesen. Dort sind untere (uS) und obere (oS) Schranken für den Minimalabstand angegeben. Der Spur-Eintrag besagt, dass alle drei Codes aus zyklischen Codes (Cy) durch sukzessives Erweitern (P2), Punktieren (P3) bzw. Verkürzen (P4) hervorgegangen sind. Der Präfix d bezieht sich auf den jeweilig dualen Code.

Selbsttestaufgaben

17.1. Gegeben sei der binäre $[7,3]$-Code C mit der Generatormatrix

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

Bestimme ein Kontrollmatrix von C, den Minimalabstand von C und $C^\perp$ sowie die Minimalvektoren von C und $C^\perp$.

17.2. Zwei Linearcodes C und D der Länge n über $\mathbb{F}_q$ heißen *isomorph*, wenn es eine monomiale Abbildung $\phi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ gibt, so dass $\phi(C) = D$. Eine Abbildung heißt *monomial*, wenn sie durch Linksmultiplikation mit einer $n \times n$-Matrix beschrieben wird, die in jeder Zeile und Spalte genau einen von 0 verschiedenen Eintrag enthält. Zeige, dass isomorphe Linearcodes gleichen Minimalabstand haben.

17.3. Ein Blockcode der Länge n über $\mathbb{F}_q$ heißt *abstandshomogen*, wenn für jedes i, $0 \le i \le n$ die Anzahl $A_i(c) = |\{c' \in C \mid d(c,c') = i\}$ aller Codewörter, die zu einem gegebenen Codewort c den Hamming-Abstand i haben, nicht von dem speziellen Codewort c abhängt. Zeige, dass Linearcodes abstandshomogen sind.

17.4. Beweise den Satz 17.3.

17.5. Bestimme den dualen Code des binären $[5,2]$-Codes aus 17.2.

17.6. Beweise das Lemma 17.5.

17.7. Sei U ein Unterraum eines $\mathbb{F}$-Vektorraums V. Der *Faktorraum* V/U von V nach U ist die Menge aller affinen Unterräume von V in Richtung U. Zeige, dass V/U zusammen mit der Addition $(v+U)+(w+U) := (v+w)+U$ und der Skalarmultiplikation $\kappa(v+U) := (\kappa v)+U$, $u, v \in V$ und $\kappa \in \mathbb{F}$, einen $\mathbb{F}$-Vektorraum bildet.

17.8. Sei $f : V \to W$ eine lineare Abbildung zwischen $\mathbb{F}$-Vektorräumen V und W. Zeige, dass der Kern $U = \ker f$ ein Unterraum von V und das Bild $f(V)$ ein Unterraum von W ist. Zeige, dass $V/U \to f(V) : v+U \mapsto f(v)$ eine bijektive lineare Abbildung ist.

17.9. Zeige, dass für alle $u, v \in \mathbb{F}_2^n$ gilt $\mathrm{wt}(u+v) = \mathrm{wt}(u)+\mathrm{wt}(v)-2\mathrm{wt}(u \cdot v)$, wobei $u \cdot v = (u_1 v_1, \ldots, u_n v_n)$.

17.10. Sei C ein binärer Linearcode. Zeige, dass entweder alle Codevektoren von C gerades Gewicht haben oder die Hälfte gerades und die andere Hälfte ungerades Gewicht besitzen.

17.11. Sei C ein binärer Linearcode. Zeige, dass alle Codevektoren von C entweder mit 0 beginnen oder die Hälfte mit 0 und die andere Hälfte mit 1 anfangen.

17.12. (Gleichverteilungsprinzip) Sei C ein $[n,k]$-Code über $\mathbb{F}_q$ und $1 \leq i \leq n$. Für jedes $\kappa \in \mathbb{F}_q$ sei $\ell_i(\kappa)$ die Anzahl aller Codewörter von C mit i-ter Komponente κ. Zeige, dass entweder $\ell_i(0) = q^k$ oder $\ell_i(\kappa) = q^{k-1}$ für alle $\kappa \in \mathbb{F}_q$.

17.13. Für welche n gibt es ternäre $[n, n-4, 3]$-Codes?

17.14. Sei C ein $[n,k]$-Code über $\mathbb{F}_q$. Die *Automorphismengruppe* von C besteht aus allen monomialen Abbildungen $\phi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ mit $\phi(C) = C$. Zeige, dass die Autommorphismengruppe von $C^\perp$ aus den Transponierten der Automorphismen von C besteht.

17.15. Berechne den Minimalabstand des ternären Linearcodes mit der Generatormatrix

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

17.16. Gegeben sei ein $[5,3]$-Code über $\mathbb{F}_5$ mit folgender Generatormatrix

$$\begin{pmatrix} 1&3&1&0&0 \\ 0&1&3&1&0 \\ 0&0&1&3&1 \end{pmatrix}.$$

Zeige, dass dieser Code das Geschlecht 0 besitzt.

17.17. Überlege, welche Linearcodes durch Punktieren oder Verkürzen des erweiterten binären $[8,4,4]$-Hamming-Codes an ein oder zwei Stellen entstehen.

18

Endliche Körper

In diesem Kapitel wird zuerst die allgemeine Theorie der Körpererweiterungen entwickelt. Auf diese Weise können wir endliche Körper als Erweiterungen der Primkörper $\mathbb{Z}_p$ einführen. Wir zeigen die Existenz und Eindeutigkeit endlicher Körper, diskutieren den Berlekamp-Algorithmus zur Faktorisierung von Polynomen über endlichen Körpern und behandeln eine wichtige Klasse linearer Codes, die so genannten Reed-Solomon-Codes.

18.1 Körperweiterungen

Charakteristik eines Körpers

Lemma 18.1. *Sei $\mathbb{K}$ ein Körper. Für das Einselement in $\mathbb{K}$ gilt entweder $n1 = 1 + \ldots + 1 = 0$ für ein $n \geq 1$ oder $n1 \neq 0$ für alle $n \geq 1$. Im ersten Fall ist die kleinste natürliche Zahl $p > 0$ mit $p1 = 0$ eine Primzahl.*

Beweis. Die beiden Fälle sind klar. Angenommen, es wäre $p \geq 1$ mit $p1 = 0$, aber p nicht prim, mithin $p = ab$ für ganze Zahlen $a, b > 1$. Dann folgt $0 = p1 = (a1)(b1)$. Da $\mathbb{K}$ nullteilerfrei ist, ergibt sich $a1 = 0$ oder $b1 = 0$, was der Minimaliät von p widerspricht. □

Im ersten Fall wird $\mathbb{K}$ als Körper der *Charakteristik p* bezeichnet und im zweiten Fall als Körper der *Charakteristik 0*.

Satz 18.2. *Jeder Körper der Charakteristik $p > 0$ enthält einen zu $\mathbb{Z}_p$ isomorphen Unterkörper.*

Beweis. Sei $\mathbb{K}$ ein Körper der Charakteristik $p > 0$. Für die Menge $\mathbb{P} = \{a1 \mid a \in \mathbb{Z}\}$ aller Vielfachen von 1 in $\mathbb{K}$ gilt nach dem Divisionssatz

$$\mathbb{P} = \{a1 \mid 0 \leq a \leq p - 1\}. \tag{18.1}$$

Für beliebige $a1, b1 \in \mathbb{P}$ gilt $a1 + b1 = c1$, wobei $c = (a + b) \bmod p$, und $(a1)(b1) = d1$, wobei $d = ab \bmod p$. Offenbar bildet $\mathbb{P}$ einen Unterring von $\mathbb{K}$. Zu jedem Element $a1 \neq 0$ in $\mathbb{P}$ gibt es nach dem Satz von Bezout ganze Zahlen s und t mit $sa + tp = 1$. Folglich ist $(s1)(a1) = 1$ in $\mathbb{K}$ und somit $s1$ das Inverse von $a1$. Also ist $\mathbb{P}$ ein Körper. Die Zuordnung $\phi : a \mapsto a1$ liefert einen Isomorphismus von $\mathbb{Z}_p$ auf $\mathbb{P}$. □

Satz 18.3. *Jeder Körper der Charakteristik* 0 *besitzt einen zu* $\mathbb{Q}$ *isomorphen Unterkörper.*

Beweis. Sei $\mathbb{K}$ ein Körper der Charakteristik 0. Die Menge

$$\mathbb{P} = \{\ (a1)(b1)^{-1} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}\} \tag{18.2}$$

bildet einen Unterkörper von $\mathbb{K}$. Die Zuordnung $\phi : \frac{a}{b} \mapsto (a1)(b1)^{-1}$ definiert einen Isomorphismus von $\mathbb{Q}$ auf $\mathbb{P}$. □

Der Körper $\mathbb{Z}_p$ heißt *Primkörper der Charakteristik* $p > 0$ und der Körper $\mathbb{Q}$ *Primkörper der Charakteristik 0.*

Auswertung von Polynomen

Satz 18.4. *Sei* $\mathbb{L}$ *eine Körpererweiterung von* $\mathbb{K}$ *und sei* $\alpha \in \mathbb{L}$. *Die Abbildung* $\eta_\alpha : \mathbb{K}[x] \to \mathbb{L} : f \mapsto f(\alpha)$ *ist ein Homomorphismus.*

Das Bild von η_α, $\mathbb{K}[\alpha] = \{f(\alpha) \mid f \in \mathbb{K}[x]\}$, *ist ein Unterring von* $\mathbb{L}$.

Der Kern von η_α, $\ker(\eta_\alpha) = \{f(\alpha) \mid f \in \mathbb{K}[x]\}$, *ist entweder* $\{0\}$ *oder besteht aus allen Vielfachen eines Polynoms* $g \in \mathbb{K}[x]$, *das minimalen Grad unter allen Polynomen in* $\mathbb{K}[x]$ *besitzt, die* α *als Nullstelle haben.*

Beweis. Nach Satz 16.17 ist η_α ein Homomorphismus und nach 12.10 ist das Bild von η_α ein Unterring von $\mathbb{L}$.

Ist η_α injektiv, dann ist $\ker(\eta_\alpha) = \{0\}$. Andernfalls gibt es ein Polynom $f \neq 0$ in $\mathbb{K}[x]$ mit $f(\alpha) = 0$. Sei $g \in \ker(\eta_\alpha)$ ein Polynom minimalen Grades $n \geq 1$. Für jedes Polynom $f \in \ker(\eta_\alpha)$ gilt nach dem Divisionssatz $f = qg + r$, wobei $q, r \in \mathbb{K}[x]$ und $r = 0$ oder $\operatorname{grad}(r) < n$. Durch Einsetzen von α ergibt sich $0 = f(\alpha) = q(\alpha)g(\alpha) + r(\alpha) = r(\alpha)$. Also ist $r \in \ker(\eta_\alpha)$. Aufgrund der Wahl von g folgt $r = 0$. Somit ist jedes Polynom in $\ker(\eta_\alpha)$ ein Vielfaches von g. Umgekehrt liegt jedes Vielfache von g auch in $\ker(\eta_\alpha)$. □

Sei $\mathbb{L}$ eine Körpererweiterung von $\mathbb{K}$ und sei $\alpha \in \mathbb{L}$. Ist η_α injektiv, so heißt α *transzendent* über $\mathbb{K}$, andernfalls heißt α *algebraisch* über $\mathbb{K}$. Eine algebraische Zahl über $\mathbb{K}$ ist Nullstelle eines von 0 verschiedenen Polynoms über $\mathbb{K}$, während eine Transzendente über $\mathbb{K}$ keiner polynomialen Gleichung mit Koeffizienten aus $\mathbb{K}$ genügt.

Beispiele 18.5. • Jedes Element $\alpha \in \mathbb{K}$ ist algebraisch über $\mathbb{K}$, weil α Nullstelle von $x - \alpha \in \mathbb{K}[x]$ ist.
- Die imaginäre Einheit i ist nach 16.27 eine Wurzel des Polynoms $x^2 + 1$ und somit algebraisch über $\mathbb{Q}$. Die Zahl $\sqrt{2}$ ist algebraisch über $\mathbb{Q}$, weil sie eine Wurzel von $x^2 - 2$ ist.
- Die n-ten Einheitswurzeln sind algebraisch über $\mathbb{Q}$, weil sie nach 16.25 die Nullstellen von $x^n - 1$ sind.
- Die Kreiszahl π und die eulersche Zahl e sind transzendent über $\mathbb{Q}$.

Minimalpolynome

Sei $\mathbb{L}$ eine Körpererweiterung von $\mathbb{K}$ und sei $\alpha \in \mathbb{L}$ algebraisch über $\mathbb{K}$. Nach Satz 18.4 gibt es ein normiertes Polynom minimalen Grades $n \geq 1$ über $\mathbb{K}$, das α als Nullstelle besitzt. Dieses Polynom wird *Minimalpolynom* von α über $\mathbb{K}$ genannt.

Satz 18.6. *Sei $\alpha \in \mathbb{L}$ algebraisch über $\mathbb{K}$.*

- *Das Minimalpolynom von α über $\mathbb{K}$ ist eindeutig bestimmt und irreduzibel über $\mathbb{K}$.*
- *Ist $f \in \mathbb{K}[x]$ irreduzibel, normiert und α eine Wurzel von f, dann ist f das Minimalpolynom von α über $\mathbb{K}$.*

Beweis. Sei g ein Minimalpolynom von α über $\mathbb{K}$. Angenommen, g wäre reduzibel. Dann gibt es Polynome $f, h \in \mathbb{K}[x]$ vom Grad ≥ 1 mit $g = fh$. Durch Einsetzen von α ergibt sich $0 = g(\alpha) = f(\alpha)h(\alpha)$. Da $\mathbb{L}$ nullteilerfrei ist, folgt $f(\alpha) = 0$ oder $h(\alpha) = 0$. O.B.d.A. sei $f(\alpha) = 0$. Nach Satz 18.4 ist f ein Vielfaches von g, hat aber widersprüchlicherweise einen kleineren Grad als g. Sei f ein weiteres Minimalpolynom von α über $\mathbb{K}$. Dann ist f ein Teiler von g und g ein Teiler von f. Nach Lemma 16.4 folgt $\operatorname{grad}(f) = \operatorname{grad}(g)$. Weiter gibt es ein $h \in \mathbb{K}[x]$ mit $f = hg$. Aus Gradgründen ist h ein von 0 verschiedenes Element in $\mathbb{K}$. Da f und g normiert sind, erhellt sich durch Koeffizientenvergleich $h = 1$.

Sei f ein normiertes irreduzibles Polynom über $\mathbb{K}$ mit $f(\alpha) = 0$. Nach Satz 18.4 ist f ein Vielfaches von g. Da aber f irreduzibel ist, müssen f und g assoziiert sein. Also gibt es nach Satz 16.6 ein Element $h \neq 0$ in $\mathbb{K}$ mit $f = hg$. Weil f und g normiert sind, folgt vermöge Koeffizientenvergleich $h = 1$. □

Im Folgenden wird das Minimalpolynom einer algebraischen Zahl α über $\mathbb{K}$ mit m_α bezeichnet.

Beispiele 18.7. • Das Minimalpolynom von $\alpha \in \mathbb{K}$ ist das lineare Polynom $x - \alpha \in \mathbb{K}$.
- Das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$ ist $f = x^2 - 2$, denn f ist normiert, hat $\sqrt{2}$ als Wurzel und ist nach 16.28 irreduzibel über $\mathbb{Q}$. Das Minimalpolynom der imaginären Einheit i über $\mathbb{Q}$ ist $f = x^2 + 1$ nach 16.27 und 16.28.
- Das Minimalpolynom einer n-ten Einheitswurzel über $\mathbb{Q}$ ist ein Teiler von $x^n - 1$ und wird *n-tes Kreisteilungspolynom* genannt.

Endliche Körpererweiterungen

Satz 18.8. *Ist α algebraisch über $\mathbb{K}$, dann ist $\mathbb{K}[\alpha]$ ein Körper.*

Beweis. Nach 18.4 ist $K[\alpha]$ ein Ring. Es bleibt zu zeigen, dass jedes von 0 verschiedene Element in $K[\alpha]$ invertierbar ist. Sei $f \in \mathbb{K}[x]$ mit $f(\alpha) \neq 0$. Nach dem Divisionssatz gibt es Polynome $q, r \in \mathbb{K}[x]$ mit $f = qm_\alpha + r$, wobei $r = 0$ oder $\operatorname{grad}(r) < \operatorname{grad}(m_\alpha)$. Durch Einsetzen von α ergibt sich $f(\alpha) = q(\alpha)m_\alpha(\alpha) + r(\alpha) = r(\alpha)$. Folglich ist $r \neq 0$. Weil m_α irreduzibel ist, müssen r und m_α aus Gradgründen teilerfremd sein. Mithin gibt es nach dem Satz von Bezout Polynome $s, t \in \mathbb{K}[x]$ mit $m_\alpha s + rt = 1$. Durch Einsetzen von α erhellt sich $r(\alpha)t(\alpha) = 1$. Also ist $t(\alpha)$ invers zu $f(\alpha)$. □

Für den Körper $\mathbb{K}[\alpha]$ wird üblicherweise $\mathbb{K}(\alpha)$ geschrieben.

Beispiel 18.9. Die Zahl $\alpha = \sqrt{2}$ hat das Minimalpolynom $x^2 - 2$ über $\mathbb{Q}$. Für die Körpererweiterung $\mathbb{Q}(\sqrt{2})$ von $\mathbb{Q}$ gilt

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Sei $a + bx \in \mathbb{Q}[x]$ mit $a + b\sqrt{2} \neq 0$. Mithilfe des erweiterten euklidischen Algorithmus' folgt

$$\frac{b^2}{a^2 - 2b^2}(x^2 - 2) + \frac{a - bx}{a^2 - 2b^2}(a + bx) = 1.$$

Durch Einsetzen von $\sqrt{2}$ erhellt sich

$$\frac{a - b\sqrt{2}}{a^2 - 2b^2}(a + b\sqrt{2}) = 1.$$

Also ist $\frac{a-b\sqrt{2}}{a^2-2b^2}$ das Inverse von $a + b\sqrt{2}$. Wegen $a + b\sqrt{2} \neq 0$ kann $a^2 - 2b^2$ nicht verschwinden.

Sei $\mathbb{L}$ eine Körpererweiterung von $\mathbb{K}$. Der Körper $\mathbb{L}$ bildet in natürlicher Weise einen $\mathbb{K}$-*Vektorraum:* Die Menge aller Vektoren ist durch die abelsche Gruppe $(\mathbb{L}, +, 0)$ gegeben und die Skalarmultiplikation entspricht der Multiplikation der Elemente in $\mathbb{L}$ (Vektoren) mit den Elementen in $\mathbb{K}$ (Skalare).

Ist $\mathbb{L}$ ein endlich-dimensionaler $\mathbb{K}$-Vektorraum, so wird $\mathbb{L}$ eine *endliche Körpererweiterung* von $\mathbb{K}$ genannt. Die Dimension des $\mathbb{K}$-Vektorraums $\mathbb{L}$ heißt der *Körpergrad von $\mathbb{L}$ über $\mathbb{K}$*, kurz $[\mathbb{L} : \mathbb{K}]$.

Satz 18.10. *Sei α algebraisch über $\mathbb{K}$. Der Körper $\mathbb{K}(\alpha)$ ist eine endliche Körpererweiterung von $\mathbb{K}$. Hat das Minimalpolynom von α über $\mathbb{K}$ den Grad n, dann ist $\mathbb{K}(\alpha)$ ein n-dimensionaler $\mathbb{K}$-Vektorraum mit der $\mathbb{K}$-Basis $B_\alpha = \{1, \alpha, \ldots, \alpha^{n-1}\}$.*

Beweis. Angenommen, α genügt einer Gleichung über $\mathbb{K}$ vom Grad $m < n$

$$f_m\alpha^m + \ldots + f_1\alpha + f_0 = 0, \quad f_i \in \mathbb{K}.$$

Dann ist $f = \sum_{i=0}^{m} f_i x^i$ ein Polynom in $\mathbb{K}[x]$ mit $f(\alpha) = 0$. Nach Satz 18.4 ist f ein Vielfaches von m_α. Aus Gradgründen kann f nur das Nullpolynom sein. Somit ist B_α linear unabhängig über $\mathbb{K}$.

Zu jedem Element $f(\alpha) \neq 0$ in $\mathbb{K}(\alpha)$ gibt es nach dem Beweis von Satz 18.8 ein Polynom $r \neq 0$ in $\mathbb{K}[x]$ vom Grad $< n$ mit $r(\alpha) = f(\alpha)$. Damit ist $f(\alpha)$ als $\mathbb{K}$-Linearkombination der Elemente in B_α darstellbar und somit B_α ein $\mathbb{K}$-Erzeugendensystem von $\mathbb{K}(\alpha)$. □

Beispiele 18.11. • Der Körper $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ ist ein 2-dimensionaler $\mathbb{Q}$-Vektorraum mit der Basis $\{1, \sqrt{2}\}$.

- Der Körper $\mathbb{Q}(i) = \{a+bi \mid a, b \in \mathbb{Q}\}$ ist ein 2-dimensionaler $\mathbb{Q}$-Vektorraum mit der Basis $\{1, i\}$, genannt *Gauss-Zahlkörper*.
- Der *Körper der komplexen Zahlen* $\mathbb{C} = \mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{R}\}$ ist ein 2-dimensionaler $\mathbb{R}$-Vektorraum mit der Basis $\{1, i\}$.
- Der Körper $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$ ist ein 3-dimensionaler $\mathbb{Q}$-Vektorraum mit der Basis $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$, weil die Zahl $\sqrt[3]{2}$ das Minimalpolynom $g = x^3 - 2$ über $\mathbb{Q}$ hat. Die beiden anderen Nullstellen von g sind $\sqrt[3]{2}\, e^{2\pi i/3}$ und $\sqrt[3]{2}\, e^{2\pi i 2/3}$, sie liegen nicht in $\mathbb{Q}(\sqrt[3]{2})$.

Das letzte Beispiel zeigt, dass im Körper $\mathbb{K}(\alpha)$ nicht notwendig alle Nullstellen des Minimalpolynoms von α über $\mathbb{K}$ liegen.

Beispiel 18.12. Der Körper $\mathbb{Q}(\sqrt[3]{2})$ wird so erweitert, dass er alle Wurzeln des Minimalpolynoms $g = x^3 - 2$ von $\sqrt[3]{2}$ über $\mathbb{Q}$ enthält. Nach dem Wurzelsatz ist g durch $x - \sqrt[3]{2}$ teilbar, also

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2).$$

Das Polynom $f = x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2$ ist irreduzibel über $\mathbb{Q}(\sqrt[3]{2})$, weil sonst aus Gradgründen seine Nullstellen in $\mathbb{Q}(\sqrt[3]{2})$ liegen. Der Körper $\mathbb{Q}(\sqrt[3]{2})$ wird um die Nullstelle $\beta = \sqrt[3]{2}\, e^{2\pi i/3}$ von f erweitert

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3}) := \mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{2}e^{2\pi i/3}) = \{a + b\sqrt[3]{2}e^{2\pi i/3} \mid a, b \in \mathbb{Q}(\sqrt[3]{2})\}.$$

Die Elemente von $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3})$ sind also von der Form

$$a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 + (b_0 + b_1\sqrt[3]{2} + b_2(\sqrt[3]{2})^2)\sqrt[3]{2}e^{2\pi i/3}, \quad a_i, b_i \in \mathbb{Q}.$$

Das Polynom f hat die Nullstelle β in $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3})$ und ist somit nach dem Wurzelsatz durch $x-\beta$ teilbar. In der Tat zerfällt f über $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3})$ in Linearfaktoren $f = (x-\beta)(x-\gamma)$ mit $\gamma = \sqrt[3]{2}\, e^{4\pi i/3}$. Demnach liegt auch γ in $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3})$.

Gradformel

Satz 18.13. *Ist $\mathbb{M}$ eine endliche Körpererweiterung von $\mathbb{L}$ und $\mathbb{L}$ eine endliche Körpererweiterung von $\mathbb{K}$, dann ist $\mathbb{M}$ ist eine endliche Körpererweiterung von $\mathbb{K}$ und es gilt*

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{K}]\,. \tag{18.3}$$

Beweis. Ist $\{\alpha_1, \ldots, \alpha_m\}$ eine $\mathbb{L}$-Basis von $\mathbb{M}$ und $\{\beta_1, \ldots, \beta_n\}$ eine $\mathbb{K}$-Basis von $\mathbb{L}$, dann ist $\{\alpha_i\beta_j \mid 1 \le i \le n, 1 \le j \le m\}$ eine $\mathbb{K}$-Basis von $\mathbb{M}$. □

Beispiel 18.14. Für den in 18.12 konstruierten Körper $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3})$ gilt

$$\left[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3}) : \mathbb{Q}\right] = \left[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3}) : \mathbb{Q}(\sqrt[3]{2})\right] \cdot \left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 3{\cdot}2 = 6.$$

18.2 Konstruktion und Eindeutigkeit

Satz 18.15. *Zu jedem endlichen Körper $\mathbb{K}$ gibt es eine Primzahl p und eine natürliche Zahl n mit der Eigenschaft*

$$|\mathbb{K}| = p^n. \tag{18.4}$$

Beweis. Sei $\mathbb{K}$ ein endlicher Körper. Dann hat $\mathbb{K}$ definitionsgemäß Charakteristik $p > 0$. Nach Satz 18.2 enthält $\mathbb{K}$ den Unterkörper $\mathbb{P} = \{a1 \mid 0 \le a \le p-1\}$. Also ist $\mathbb{K}$ ein endlich-dimensionaler $\mathbb{P}$-Vektorraum. Bezeichnet n die Dimension von $\mathbb{K}$ über $\mathbb{P}$, dann hat $\mathbb{K}$ genau $|\mathbb{P}|^n = p^n$ Elemente. □

Konstruktion endlicher Körper

Ein endlicher Körper $\mathbb{K}$ mit p^n Elementen wird anhand eines normierten irreduziblen Polynoms $f = \sum_i f_i x^i \in \mathbb{Z}_p[x]$ vom Grad n konstruiert. Sei α eine Wurzel von f. Wegen Satz 18.6 ist f das Minimalpolynom von α über $\mathbb{Z}_p$. Nach Satz 18.10 ist $\mathbb{K} = \mathbb{Z}_p(\alpha)$ eine endliche Körpererweiterung von $\mathbb{Z}_p$ und ein $\mathbb{Z}_p$-Vektorraum mit der Basis $B_\alpha = \{1, \alpha, \ldots, \alpha^{n-1}\}$. Jedes Element von $\mathbb{K}$ ist eindeutig darstellbar in der Form

$$a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}, \quad a_i \in \mathbb{Z}_p. \tag{18.5}$$

Zwei Körperelemente werden als Vektoren addiert

$$\left(\sum_{i=0}^{n-1} a_i\alpha^i\right) + \left(\sum_{i=0}^{n-1} b_i\alpha^i\right) = \sum_{i=0}^{n-1}(a_i + b_i)\alpha^i \tag{18.6}$$

und als Polynome in α multipliziert

$$\left(\sum_{i=0}^{n-1} a_i \alpha^i\right) \cdot \left(\sum_{i=0}^{n-1} b_i \alpha^i\right) = \sum_{i=0}^{2n-2} \left(\sum_{k=0}^{i} a_k b_{i-k}\right) \alpha^i. \tag{18.7}$$

Die rechte Seite wird in der Basis B_α entwickelt, indem die Potenz α^n mithilfe des Minimalpolynoms von α in der Basis B_α repräsentiert wird

$$\alpha^n = -(f_0 + f_1\alpha + \ldots + f_{n-1}\alpha^{n-1}). \tag{18.8}$$

Auf diese Weise lassen sich alle Potenzen von α in der Basis B_α darstellen.

Beispiel 18.16. Um einen Körper mit vier Elementen zu konstruieren, wird ein irreduzibles Polynom $f = x^2 + x + 1$ vom Grad 2 über $\mathbb{Z}_2$ gewählt. Sei α eine Nullstelle von f, also $\alpha^2 = 1 + \alpha$. Dann ist der gesuchte Körper

$$\mathbb{Z}_2(\alpha) = \{a_0 + a_1\alpha \mid a_0, a_1 \in \mathbb{Z}_2\} = \{0, 1, \alpha, 1 + \alpha\}.$$

Beispielsweise gilt

$$\alpha(1 + \alpha) = \alpha + \alpha^2 = \alpha + (1 + \alpha) = 1 + 2\alpha = 1.$$

Lemma 18.17. *Ist $\mathbb{K}$ ein endlicher Körper mit q Elementen, dann gilt für alle Elemente $\beta \in \mathbb{K}$*

$$\beta^q = \beta. \tag{18.9}$$

Beweis. Nach Korollar 15.36 gilt $\beta^{q-1} = 1$ für alle Elemente β der multiplikativen Gruppe $(\mathbb{K} \setminus \{0\}, \cdot, 1)$. Also gilt $\beta^q = \beta$ für alle Elemente $\beta \neq 0$ in $\mathbb{K}$. Diese Gleichung erfüllt trivialerweise auch das Nullelement. □

Satz 18.18. *Ist $\mathbb{K}$ ein endlicher Körper mit q Elementen, dann gilt*

$$x^q - x = \prod_{\beta \in \mathbb{K}} (x - \beta). \tag{18.10}$$

Beweis. Nach Lemma 18.17 ist jedes $\beta \in \mathbb{K}$ eine Wurzel von $x^q - x$. Nach dem Wurzelsatz wird $x^q - x$ geteilt von

$$\prod_{\beta \in \mathbb{K}} (x - \beta).$$

Beide Polynome haben denselben Grad und sind normiert, mithin sind sie identisch. □

Multiplikative Struktur endlicher Körper

Satz 18.19. *Die multiplikative Gruppe eines endlichen Körpers ist zyklisch.*

Beweis. Sei $\mathbb{K}$ ein endlicher Körper mit p^n Elementen. Sei β ein Element maximaler Ordnung in der multiplikativen Gruppe $(\mathbb{K} \setminus \{0\}, \cdot, 1)$ von $\mathbb{K}$. Wir zeigen, dass für jedes $\gamma \in \mathbb{K}$ mit $\gamma \neq 0$ gilt

$$\operatorname{ord}(\gamma) \mid \operatorname{ord}(\beta). \tag{18.11}$$

Angenommen, es gäbe ein $\gamma \in \mathbb{K}$, so dass $\operatorname{ord}(\gamma)$ kein Teiler von $\operatorname{ord}(\beta)$ wäre. Dann gibt es eine Primzahl q und natürliche Zahlen r, s mit $\operatorname{ord}(\beta) = q^i s$ und $\operatorname{ord}(\gamma) = q^{i+1} r$, so dass q kein Teiler von s ist. Es gilt $(\beta^{q^i})^s = \beta^{q^i s} = 1$ und $(\gamma^r)^{q^{i+1}} = \gamma^{q^{i+1} r} = 1$. Daraus folgt $\operatorname{ord}(\beta^{q^i}) = s$ und $\operatorname{ord}(\gamma^r) = q^{i+1}$. Also sind $\operatorname{ord}(\beta^{q^i})$ und $\operatorname{ord}(\gamma^r)$ teilerfremd. Weil aber die multiplikative Gruppe von $\mathbb{K}$ abelsch ist, folgt

$$\operatorname{ord}(\beta^{q^i}\gamma^r) = [\operatorname{ord}(\beta^{q^i}), \operatorname{ord}(\gamma^r)] = \operatorname{ord}(\beta^{q^i}) \cdot \operatorname{ord}(\gamma^r) = s q^{i+1} = q \cdot \operatorname{ord}(\beta).$$

Dabei ergibt sich die erste Identität aus Abs. 15.5. Also hat $\beta^{q^i}\gamma^r$ widersprüchlicherweise eine größere Ordnung als β.

Sei $l = \operatorname{ord}(\beta)$. Nach (18.11) gilt $\gamma^l = 1$ für jedes $\gamma \neq 0$ in $\mathbb{K}$. Also ist jedes $\gamma \neq 0$ in $\mathbb{K}$ eine Wurzel von $x^l - 1$. Nach dem Wurzelsatz ist $x^l - 1$ ein Vielfaches von

$$g = \prod_{\substack{\gamma \in \mathbb{K} \\ \gamma \neq 0}} (x - \gamma).$$

Ein Gradvergleich ergibt $l \geq \operatorname{grad}(g) = p^n - 1$. Nach Korollar 15.35 ist die Ordnung von β ein Teiler der Ordnung von $(\mathbb{K} \setminus \{0\}, \cdot, 1)$, d. h., l ist ein Teiler von $p^n - 1$. Also folgt $l = p^n - 1$. Somit wird $(\mathbb{K} \setminus \{0\}, \cdot, 1)$ von β erzeugt und ist folglich zyklisch. □

Ein Erzeuger β der multiplikativen Gruppe eines endlichen Körpers $\mathbb{K}$ wird *primitives Element* von $\mathbb{K}$ genannt. Das Minimalpolynom von β über $\mathbb{K}$ heißt ebenfalls *primitiv*.

Beispiel 18.20. Das Polynom $f = x^4 + x + 1 \in \mathbb{Z}_2[x]$ ist irreduzibel über $\mathbb{Z}_2$. Sei α eine Wurzel von f. Die Potenzen von α durchlaufen alle von 0 verschiedenen Elemente von $\mathbb{K} = \mathbb{Z}_2(\alpha)$

$$\begin{array}{lll}
\alpha^0 = 1, & \alpha^5 = \alpha^2 + \alpha, & \alpha^{10} = \alpha^2 + \alpha + 1, \\
\alpha^1 = \alpha, & \alpha^6 = \alpha^3 + \alpha^2, & \alpha^{11} = \alpha^3 + \alpha^2 + \alpha, \\
\alpha^2 & \alpha^7, = \alpha^3 + \alpha + 1, & \alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1, \\
\alpha^3 & \alpha^8, = \alpha^2 + 1, & \alpha^{13} = \alpha^3 + \alpha^2 + 1, \\
\alpha^4 = \alpha + 1, & \alpha^9 = \alpha^3 + \alpha, & \alpha^{14} = \alpha^3 + 1.
\end{array}$$

Also ist f ein primitives Polynom über $\mathbb{Z}_2$.

Das irreduzible Polynom $f = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$ ist nicht primitiv, weil f ein Teiler von $x^5 - 1$ ist und somit jede Wurzel von f eine 5-te Einheitswurzel ist.

Eindeutigkeit endlicher Körper

Satz 18.21. *Je zwei endliche Körper mit p^n Elementen sind isomorph.*

Beweis. Sei $\mathbb{K} = \mathbb{Z}_p(\alpha)$ ein Körper mit p^n Elementen, wobei α ein primitives Element in $\mathbb{K}$ ist. Nach Lemma 18.17 ist α eine Wurzel von $x^{p^n} - x$. Wegen Satz 18.6 ist somit m_α ein Teiler von $x^{p^n} - x$.

Sei $\mathbb{L}$ ein endlicher Körper mit p^n Elementen. Angenommen, es wäre $m_\alpha(\beta) \neq 0$ für alle $\beta \in \mathbb{L}$. Nach Satz 18.18 erhellt sich

$$x^{p^n} - x = \prod_{\beta \in \mathbb{L}} (x - \beta).$$

Da m_α ein Teiler von $x^{p^n} - x$ ist, gibt es ein Polynom $f \in \mathbb{Z}_p[x]$ mit $x^{p^n} - x = m_\alpha f$, also $m_\alpha(\beta) f(\beta) = 0$ für alle $\beta \in \mathbb{L}$. Nach Annahme ist $f(\beta) = 0$ für alle $\beta \in \mathbb{L}$, was nach dem Wurzelsatz aus Gradgründen nicht möglich ist. Also gibt es ein $\beta \in \mathbb{L}$ mit $m_\alpha(\beta) = 0$. Nach Satz 18.6 ist m_α das Minimalpolynom von β über $\mathbb{Z}_p$ und wegen Satz 18.10 ist $\{1, \beta, \ldots, \beta^{n-1}\}$ eine $\mathbb{Z}_p$-Basis von $\mathbb{L}$. Also ist die Abbildung

$$\phi : \mathbb{K} \to \mathbb{L} : a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mapsto b_0 + b_1\beta + \ldots + b_{n-1}\beta^{n-1}$$

ein Isomorphismus der beteiligten additiven Gruppen. Er ist sogar ein Ring-Isomorphismus, weil die Multiplikation in $\mathbb{K}$ und $\mathbb{L}$ durch die Nullstellen α und β desselben irreduziblen Polynoms m_α definiert ist. □

Der bis auf Isomorphie eindeutige endliche Körper mit p^n Elementen wird mit $\mathbb{F}_{p^n}$ bezeichnet und nach Evariste Galois (1811-1832) auch *Galoisfeld* genannt.

Der Verband der Unterkörper

Satz 18.22. *Der Körper $\mathbb{F}_{p^m}$ ist ein Unterkörper von $\mathbb{F}_{p^n}$ genau dann, wenn m ein Teiler von n ist.*

Beweis. Sei m ein Teiler von n, also $n = md$ für eine natürliche Zahl d. In jedem Ring R gilt

$$a^n - 1 = (a^m)^d - 1 = (a^m - 1)(a^{(d-1)m} + \ldots + a^m + 1), \quad a \in R.$$

Im Falle $R = \mathbb{Z}$ folgt aus $m \mid n$ sofort $p^m - 1 \mid p^n - 1$. Im Falle $R = \mathbb{F}_p[x]$ ergibt sich aus $m \mid n$ sofort $x^m - 1 \mid x^n - 1$. Insbesondere folgt aus $p^m - 1 \mid p^n - 1$ sofort $x^{p^m-1} - 1 \mid x^{p^n-1} - 1$. Also ist $\mathbb{F}_{p^m}$ nach Satz 18.18 ein Unterkörper von $\mathbb{F}_{p^n}$.

Sei $\mathbb{F}_{p^m}$ ein Unterkörper von $\mathbb{F}_{p^n}$. Dann ist $\mathbb{F}_{p^n}$ ein Vektorraum über $\mathbb{F}_{p^m}$. Bezeichnet d die Dimension von $\mathbb{F}_{p^n}$ über $\mathbb{F}_{p^m}$, dann ist $p^n = (p^m)^d = p^{md}$ und somit $n = md$. □

Korollar 18.23. *Sei $\mathbb{F}_{p^m}$ ein Unterkörper von $\mathbb{F}_{p^n}$. Ist α ein primitives Element in $\mathbb{F}_{p^n}$, dann besteht der Körper $\mathbb{F}_{p^m}$ aus den Elementen*

$$0, 1, \alpha^u, \alpha^{2u}, \ldots, \alpha^{(p^m-2)u}, \quad u = (p^n - 1)/(p^m - 1).$$

Den Verband der Unterkörper von $\mathbb{F}_{2^{12}}$ zeigt die Abb. 18.1.

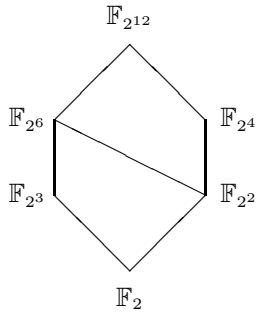

Abb. 18.1. Hasse-Diagramm der Unterkörper von $\mathbb{F}_{2^{12}}$.

18.3 Existenz

Satz 18.24. *Für jede Primzahlpotenz p^n ist $x^{p^n} - x$ das Produkt aller normierten irreduziblen Polynome über $\mathbb{F}_p$, deren Grad n teilt.*

Beweis. Sei $f \in \mathbb{F}_p[x]$ ein normiertes irreduzibles Polynom vom Grad m, das $x^{p^n} - x$ teilt. Nach den Sätzen 16.30 und 18.18 hat f eine Wurzel α in $\mathbb{F}_{p^n}$ und wegen Satz 18.6 ist f das Minimalpolynom von α über $\mathbb{F}_p$. Gemäß Satz 18.10 hat der Körper $\mathbb{F}_p(\alpha)$ genau p^m Elemente, die allesamt folgende Gestalt haben

$$a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1}, \quad a_i \in \mathbb{F}_p.$$

Diese Körperelemente liegen wegen $\alpha \in \mathbb{F}_{p^n}$ in $\mathbb{F}_{p^n}$. Also ist $\mathbb{F}_p(\alpha)$ ein Unterkörper von $\mathbb{F}_{p^n}$. Folglich ist m wegen Satz 18.22 ein Teiler von n.

Sei $f \in \mathbb{F}_p[x]$ ein normiertes irreduzibles Polynom vom Grad m. Sei α eine Nullstelle von f und m ein Teiler von n. Nach Satz 18.6 ist f das Minimalpolynom von α über $\mathbb{F}_p$ und wegen Satz 18.10 hat $\mathbb{F}_p(\alpha)$ genau p^m Elemente. Gemäß Satz 18.22 ist $\mathbb{F}_p(\alpha)$ ein Unterkörper von $\mathbb{F}_{p^n}$. Nach Satz 18.18 ist α eine Wurzel von $x^{p^m} - x$ und somit f wegen Satz 18.4 ein Teiler von $x^{p^m} - x$. Da m ein Teiler von n ist, ist $x^{p^m} - x$ nach dem Beweis von Satz 18.22 ein Teiler von $x^{p^n} - x$. Also ist f auch ein Teiler von $x^{p^n} - x$. □

Beispiel 18.25. Hier sind einige Primfaktorisierungen über $\mathbb{F}_2$:

$$\begin{aligned}
x^2 - x &= x(x-1)\\
x^4 - x &= x(x-1)(x^2+x+1)\\
x^8 - x &= x(x-1)(x^3+x+1)(x^3+x^2+1)\\
x^{16} - x &= x(x-1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)\\
&\quad (x^4+x^3+x^2+x+1).
\end{aligned}$$

Möbius-Funktion

Die *Möbius-Funktion* (A.F. Möbius, 1790-1868) $\mu : \mathbb{N} \to \mathbb{N}_0$ ist definiert durch

$$\mu(n) = \begin{cases} 1 \text{ falls } n = 1, \\ (-1)^k \text{ falls } n \text{ Produkt von } k \text{ paarweise} \\ \quad \text{verschiedenen Primzahlen}, \\ 0 \text{ sonst.} \end{cases} \tag{18.12}$$

Die Möbius-Funktion ist eng verknüpft mit der eulerschen Φ-Funktion.

Lemma 18.26. *Für alle natürlichen Zahlen $n \geq 2$ gilt*

$$\Phi(n) = \sum_{d|n} \mu(d)\frac{n}{d} \quad \textit{und} \quad \sum_{d|n} \mu(d) = 0. \tag{18.13}$$

Beweis. Sei $n = p_1^{e_1} \cdots p_r^{e_r}$ die kanonische Primfaktorisierung von n. Nach Satz 15.8 und der Definition von μ gilt

$$\begin{aligned}
\Phi(n) &= \frac{n}{1} - (\frac{n}{p_1} + \ldots + \frac{n}{p_r}) + (\frac{n}{p_1 p_2} + \ldots + \frac{n}{p_{r-1}p_r}) \pm \ldots + (-1)^r \frac{n}{p_1 \cdots p_r}\\
&= \sum_{\substack{d \\ d|n}} \mu(d)\frac{n}{d}.
\end{aligned}$$

Jeder Teiler von n hat eine Primfaktorzerlegung der Gestalt

$$d = p_1^{f_1} \cdots p_r^{f_r}, \quad 0 \leq f_i \leq e_i.$$

Nach Definition von μ ist $\mu(d) \neq 0$ genau dann, wenn $f_i \in \{0, 1\}$ für alle $1 \leq i \leq r$. Also ist die Anzahl der Teiler d von n mit $\mu(d) \neq 0$, die aus einem Produkt von i Faktoren $p_1, \ldots, p_r$ bestehen, gleich $\binom{r}{i}$. Mit Satz 10.4 folgt

$$\sum_{d|n} \mu(d) = \sum_{\substack{d|n \\ \mu(d)\neq 0}} \mu(d) = 1 - \binom{r}{1} + \binom{r}{2} \pm \ldots + (-1)^r \binom{r}{r} = 0.$$

□

Satz 18.27. (Möbius-Inversion) *Sind $f : \mathbb{N} \to \mathbb{R}$ und $g : \mathbb{N} \to \mathbb{R}$ Abbildungen mit*

$$g(n) = \sum_{\substack{d \\ d|n}} f(d), \tag{18.14}$$

dann gilt

$$f(n) = \sum_{\substack{d \\ d|n}} \mu(d) g(\frac{n}{d}). \tag{18.15}$$

Beweis. Es gilt

$$\begin{aligned}
\sum_{\substack{d \\ d|n}} \mu(d) g(\frac{n}{d}) &= \sum_{\substack{d \\ d|n}} \mu(d) \sum_{\substack{c \\ c|(n/d)}} f(c) \\
&= \sum_{\substack{d \\ d|n}} \sum_{\substack{c \\ c|(n/d)}} \mu(d) f(c) \\
&= \sum_{\substack{c \\ c|n}} f(c) \sum_{\substack{d \\ d|(n/c)}} \mu(d),
\end{aligned}$$

wobei in der letzten Gleichung ausgenutzt wurde, dass die Summation über alle Paare (c, d) mit $d \mid n$ und $c \mid \frac{n}{d}$ der Summation über alle Paare (c, d) mit $c \mid n$ und $d \mid \frac{n}{c}$ entspricht. Nach Lemma 18.26 ist die innere Summe gleich 0 für alle Teiler c von n mit $\frac{n}{c} \geq 2$. Folglich ist

$$\sum_{\substack{c \\ c|n}} f(c) \sum_{\substack{d \\ d|(n/c)}} \mu(d) = f(n) \sum_{\substack{d \\ d|1}} \mu(d) = f(n)\mu(1) = f(n).$$

□

Existenz endlicher Körper

Satz 18.28. *Zu jeder Primzahl p und jeder natürlichen Zahl n gibt es einen endlichen Körper mit p^n Elementen.*

Beweis. Sei $I_p(n)$ die Anzahl der normierten irreduziblen Polynome über $\mathbb{F}_p$ vom Grad n. Aus Satz 18.24 folgt vermöge Gradvergleich

$$p^n = \sum_{\substack{d \\ d|n}} d\, I_p(d). \tag{18.16}$$

Durch Möbius-Inversion ergibt sich

$$I_p(n) = \frac{1}{n} \sum_{\substack{d \\ d|n}} \mu(d) p^{\frac{n}{d}}. \tag{18.17}$$

Die Summe auf der rechten Seite enthält den Term p^n für $d = 1$, womit sich folgende Abschätzung für $I_p(n)$ ergibt

$$I_p(n) \geq \frac{1}{n}(p^n - (p^{n-1} + \ldots + p + 1)) = \frac{1}{n}(p^n - \frac{p^n - 1}{p - 1}). \qquad (18.18)$$

Für jede Primzahl p ist diese rechte Seite positiv und somit $I_p(n) > 0$. Also existiert wenigstens ein normiertes irreduzibles Polynom über $\mathbb{F}_p$ vom Grad n und somit nach Abs. 18.2 ein endlicher Körper mit p^n Elementen. □

Frobenius-Automorphismen

Lemma 18.29. *Eine Primzahl p teilt $\binom{p}{i}$ für jedes $1 \leq i \leq p - 1$.*

Beweis. Sei $1 \leq i \leq p - 1$. Nach Satz 10.2 ist $\binom{p}{i} = \frac{p!}{i!(p-i)!}$. Weil $\binom{p}{i}$ ganz ist, muss $i!(p - i)!$ ein Teiler von $p!$ sein. Da aber p prim ist, sind p und $i!(p - i)!$ teilerfremd, mithin $i!(p - i)!$ ein Teiler von $(p - 1)!$. Also ist p ein Teiler von $\binom{p}{i}$. □

Ein (Ring-)Homomorphismus $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ heißt ein *Automorphismus über* $\mathbb{F}_p$, wenn für alle $\alpha \in \mathbb{F}_p$ gilt $\phi(\alpha) = \alpha$.

Lemma 18.30. *Die Abbildung $\sigma_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} : \alpha \mapsto \alpha^p$ ist ein Automorphismus über $\mathbb{F}_p$ und für alle $\alpha \in \mathbb{F}_{p^n}$ gilt*

$$\alpha^p = \alpha \quad \Longleftrightarrow \quad \alpha \in \mathbb{F}_p. \qquad (18.19)$$

Beweis. Seien $\alpha, \beta \in \mathbb{F}_{p^n}$. Nach dem Binomialsatz und Lemma 18.29 gilt

$$(\alpha + \beta)^p = \alpha^p + \left(\sum_{i=1}^{p-1} \binom{p}{i} \alpha^{p-i}\beta^i\right) + \beta^p = \alpha^p + \beta^p. \qquad (18.20)$$

Weiter ist $(\alpha\beta)^p = \alpha^p\beta^p$ und $1^p = 1$. Folglich ist σ_p ein Homomorphismus.

Sei $\alpha^p = \beta^p$. Wegen (18.20) folgt $(\alpha - \beta)^p = 0$. Da $\mathbb{F}_{p^n}$ nullteilerfrei ist, erhellt sich $\alpha = \beta$. Also ist σ_p injektiv und somit nach Satz 6.8 sogar bijektiv.

Sei $\alpha \in \mathbb{F}_{p^n}$ mit $\alpha^p = \alpha$, d. h., α eine Wurzel von $x^p - x$. Wegen Satz 16.22 hat dieses Polynom höchstens p Wurzeln in $\mathbb{F}_{p^n}$. Nach Satz 18.18 sind aber alle Elemente von $\mathbb{F}_p$ Wurzeln von $x^p - x$. Also gilt $\alpha^p = \alpha$ genau dann, wenn $\alpha \in \mathbb{F}_p$. □

Der Automorphismus α_p wird *Frobenius-Automorphismus* (G. Frobenius, 1848-1917) genannt.

Korollar 18.31. *Ist $\alpha \in \mathbb{F}_{p^n}$ eine Wurzel von $f \in \mathbb{F}_p[x]$, dann ist auch α^p eine Wurzel von f.*

Beweis. Sei $f = \sum_i f_i x^i \in \mathbb{F}_p[x]$. Mit Lemma 18.30 gilt

$$\sigma_p(f(\alpha)) = \sigma_p(\sum_i f_i \alpha^i) = \sum_i f_i \sigma_p(\alpha^i) = \sum_i f_i \sigma_p(\alpha)^i = f(\sigma_p(\alpha)).$$

□

Satz 18.32. *Für das Minimalpolynom von $\alpha \in \mathbb{F}_{p^n}$ über $\mathbb{F}_p$ gilt*

$$m_\alpha = \prod_{i=0}^{t-1} (x - \alpha^{p^i}), \tag{18.21}$$

wobei t die kleinste natürliche Zahl ist mit $\alpha^{p^t} = \alpha$.

Beweis. Sei $f = \sum_i a_i x^i = \prod_{i=0}^{t-1}(x - \alpha^{p^i})$. Jeder Koeffizient a_i ist nach dem Vietaschen Wurzelsatz darstellbar als symmetrisches Polynom in den Wurzeln

$$a_i = (-1)^{t-1-i} s_{t-1-i}.$$

Diese symmetrischen Polynome sind invariant unter dem Frobenius-Automorphismus über $\mathbb{F}_p$ und somit nach Lemma 18.30 Elemente von $\mathbb{F}_p$. Also liegt f in $\mathbb{F}_p[x]$. Nach Korollar 18.31 sind alle Wurzeln von f auch Wurzeln des Minimalpolynoms m_α von α über $\mathbb{F}_p$. Mithin ist f ein Teiler von m_α. Da f normiert ist und m_α irreduzibel, folgt $m_\alpha = f$. □

Beispiel 18.33. Sei α eine Wurzel des primitiven irreduziblen Polynoms $x^4 + x + 1 \in \mathbb{F}_2[x]$. Die zu den Elementen von $\mathbb{F}_{16}$ gehörenden Minimalpolynome sind

$$\begin{aligned}
m_0 &= x \\
m_1 &= x - 1 \\
m_\alpha &= (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8) = x^4 + x + 1 \\
m_{\alpha^3} &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9) = x^4 + x^3 + x^2 + x + 1 \\
m_{\alpha^5} &= (x-\alpha^5)(x-\alpha^{10}) = x^2 + x + 1 \\
m_{\alpha^7} &= (x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11}) = x^4 + x^3 + 1.
\end{aligned}$$

Die Menge aller Automorphismen eines Körpers $\mathbb{F}_{p^n}$ über $\mathbb{F}_p$ bildet eine Gruppe, sie wird *Galoisgruppe* von $\mathbb{F}_{p^n}$ über $\mathbb{F}_p$ genannt.

Satz 18.34. *Die Galoisgruppe von $\mathbb{F}_{p^n}$ über $\mathbb{F}_p$ ist zyklisch von der Ordnung n und wird durch den Frobenius-Automorphismus erzeugt.*

Beweis. Die Potenzen des Frobenius-Automorphismus $\sigma_p^m : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} : \alpha \mapsto \alpha^{p^m}$ sind ebenfalls Automorphismen von $\mathbb{F}_{p^n}$ über $\mathbb{F}_p$. Nach Lemma 18.17 gilt aber $\alpha^{p^n} = \alpha$ für jedes $\alpha \in \mathbb{F}_{p^n}$. Also ist σ_p^n die identische Abbildung und die Potenzen $\sigma_p^0 = id, \sigma_p, \sigma_p^2, \ldots, \sigma_p^{n-1}$ sind paarweise verschieden.

Sei $\tau : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ ein Automorphismus über $\mathbb{F}_p$. Wegen $\tau(1) = 1$ gilt $\tau(k1) = k\tau(1) = k1$ für jedes k-Vielfache von 1. Weil aber $\mathbb{F}_p$ als Primkörper von $\mathbb{F}_{p^n}$ nach dem Beweis von Satz 18.2 aus allen Vielfachen von 1 besteht, folgt $\tau(\beta) = \beta$ für alle $\beta \in \mathbb{F}_p$. Wie in Korollar 18.31 wird gezeigt, dass $\tau(\alpha)$ ebenfalls eine Nullstelle von m_α ist. Somit ist $\tau(\alpha)$ nach Satz 18.32 von der Gestalt α^{p^j}. Da α ein primitives Element in $\mathbb{F}_{p^n}$ ist, folgt $\tau = \sigma_p^j$. □

18.4 Polynom-Faktorisierung

In diesem Abschnitt wird der Berlekamp-Algorithmus zur Faktorisierung von Polynomen über endlichen Körpern präsentiert. Dieser Algorithmus basiert auf dem folgenden

Satz 18.35. *Seien f, g Polynome in $\mathbb{F}_p[x]$ mit $1 \leq \operatorname{grad}(g) < \operatorname{grad}(f)$, so dass f ein Teiler von $g^p - g$ ist. Dann gilt*

$$f = \prod_{\alpha=0}^{p-1} (f, g - \alpha). \tag{18.22}$$

Diese Faktorisierung ist nichttrivial.

Beweis. Nach dem Satz von Fermat gilt für jedes von 0 verschiedene $\alpha \in \mathbb{F}_p$

$$g^p - g = (g - \alpha)(g^{p-1} + \alpha g^{p-2} + \ldots + \alpha^{p-2} g).$$

Somit ist das Polynom $g(g-1) \cdot \ldots \cdot (g-(p-1))$ ein Teiler von $g^p - g$. Weil aber beide Polynome denselben Grad und den gleichen Leitkoeffizienten haben, sind sie identisch

$$g^p - g = g(g-1) \cdot \ldots \cdot (g-(p-1)).$$

Für verschiedene $\alpha, \beta \in \mathbb{F}_p$ sind $g - \alpha$ und $g - \beta$ teilerfremd. Für teilerfremde Polynome h und h' in $\mathbb{F}_p[x]$ gilt aber

$$(f, hh') = (f, h) \cdot (f, h'). \tag{18.23}$$

Nach Voraussetzung ist $f = (f, g^p - g)$, woraus vermöge (18.23) sofort die geforderte Faktorisierung folgt.

Der Grad von $(f, g-\alpha)$ ist wegen $\operatorname{grad}(g-\alpha) < \operatorname{grad}(f)$ kleiner als der Grad von f für jedes $\alpha \in \mathbb{F}_p$. Also gibt es in der obigen Faktorisierung mindestens zwei Faktoren. □

Im Berlekamp-Algorithmus gilt es zu einem zu faktorisierenden Polynom f in $\mathbb{F}_p[x]$ vom Grad n ein Polynom g in $\mathbb{F}_p[x]$ mit $1 \leq \operatorname{grad}(g) < n$ zu finden, so dass f Teiler von $g^p - g$ ist. Denn in diesem Fall liefert die Darstellung (18.22) eine nichttriviale Faktorisierung von f, deren Faktoren mithilfe des euklidischen Algorithmus' berechnet werden können. Auf diesen Faktoren wird das Verfahren solange fortgesetzt, bis f in irreduzible Faktoren zerlegt ist.

Wir müssen noch ein Polynom g mit den angegebenen Eigenschaften aufstellen. Dazu setzen wir $g = g_0 + g_1 x + \ldots + g_{n-1}x^{n-1}$ und erhalten mit Lemma 18.30 und dem Satz von Fermat

$$\begin{aligned} g^p &= g_0^p + g_1^p x^p + \ldots + g_{n-1}^p x^{(n-1)p} \\ &= g_0 + g_1 x^p + \ldots + g_{n-1} x^{(n-1)p}. \end{aligned}$$

Für jedes i, $0 \leq i \leq n-1$, wird das Monom x^{ip} durch f dividiert

$$x^{ip} = q^{(i)} f + r^{(i)}, \quad \text{wobei } r^{(i)} = 0 \text{ oder } \operatorname{grad}(r^{(i)}) < n.$$

Durch Einsetzen in die obige Darstellung von g^p erhellt sich

$$g^p = g_0 r^{(0)} + g_1 r^{(1)} + \ldots + g_{n-1} r^{(n-1)} + qf, \quad q \in \mathbb{F}_p[x].$$

Also ist f ein Teiler von $g^p - g$ genau dann, wenn f ein Teiler von $g_0 r^{(0)} + g_1 r^{(1)} + \ldots + g_{n-1} r^{(n-1)} - (g_0 + g_1 x + \ldots + g_{n-1} x^{n-1})$ ist. Dieses Polynom muss aus Gradgründen 0 sein. Also muss jeder Koeffizient dieses Polynoms verschwinden. Schreiben wir noch

$$r^{(i)} = r_{i0} + r_{i1} x + \ldots + r_{i,n-1} x^{n-1}, \quad r_{ij} \in \mathbb{F}_p,$$

dann erhalten wir ein System von n linearen Gleichungen mit n Unbekannten

$$\begin{aligned} g_0(r_{00} - 1) + \quad g_1 r_{10} \quad + \ldots + \quad g_{n-1} r_{n-1,0} \quad &= 0 \\ g_0 r_{01} \quad + g_1(r_{11} - 1) + \ldots + \quad g_{n-1} r_{n-1,1} \quad &= 0 \\ &\vdots \\ g_0 r_{0,n-1} \quad + \quad g_1 r_{1,n-1} \quad + \ldots + g_{n-1}(r_{n-1,n-1} - 1) &= 0. \end{aligned}$$

In der Sprache der Linearen Algebra hat dieses lineare Gleichungssystem die Form

$$(g_0, \ldots, g_{n-1})(R - I) = (0, \ldots, 0), \tag{18.24}$$

wobei

$$R = \begin{pmatrix} r_{00} & r_{01} & \ldots & r_{0,n-1} \\ r_{10} & r_{11} & \ldots & r_{1,n-1} \\ \vdots & \vdots & & \vdots \\ r_{n-1,0} & r_{n-1,1} & \ldots & r_{n-1,n-1} \end{pmatrix}$$

und $I = I_n$ die $n \times n$-Einheitsmatrix über $\mathbb{F}_p$ ist. Durch Lösen dieses linearen Gleichungssystems erhalten wir ein Polynom g mit den geforderten Eigenschaften.

Beispiel 18.36. Wir betrachten das Polynom $f = x^5 + x^4 + 1 \in \mathbb{F}_2[x]$. Die Division von x^{2i}, $0 \leq i \leq 4$, durch f ergibt

$$\begin{aligned}
x^0 &= 0 \cdot f + 1 \\
x^2 &= 0 \cdot f + x^2 \\
x^4 &= 0 \cdot f + x^4 \\
x^6 &= (x+1) \cdot f + (x^4 + x + 1) \\
x^8 &= (x^3 + x^2 + x + 1) \cdot f + (x^4 + x^3 + x^2 + x + 1),
\end{aligned}$$

also

$$\begin{aligned}
r^{(0)} &= 1 \\
r^{(1)} &= x^2 \\
r^{(2)} &= x^4 \\
r^{(3)} &= x^4 + x + 1 \\
r^{(4)} &= x^4 + x^3 + x^2 + x + 1.
\end{aligned}$$

Die Koeffizienten von $r^{(0)}, \ldots, r^{(4)}$ bilden die Zeilen der Matrix

$$R = \begin{pmatrix} 1\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,1 \\ 1\,1\,0\,0\,1 \\ 1\,1\,1\,1\,1 \end{pmatrix}.$$

Es folgt

$$R - I = \begin{pmatrix} 0\,0\,0\,0\,0 \\ 0\,1\,1\,0\,0 \\ 0\,0\,1\,0\,1 \\ 1\,1\,0\,1\,1 \\ 1\,1\,1\,1\,0 \end{pmatrix}.$$

Das lineare Gleichungssystem (18.24) hat also die Form

$$\begin{aligned}
g_3 + g_4 &= 0 \\
g_1 + g_3 + g_4 &= 0 \\
g_1 + g_2 + g_4 &= 0 \\
g_2 + g_3 &= 0.
\end{aligned}$$

Aus der ersten und letzten Gleichung folgt $g_2 = g_3 = g_4$ und mit der ersten oder zweiten Gleichung ergibt sich $g_1 = 0$. Ferner ist g_0 beliebig wählbar. Die Lösungsmenge des linearen Gleichungssystems ist also

$$\{(\alpha, 0, \beta, \beta, \beta) \mid \alpha, \beta \in \mathbb{F}_2\}.$$

Zu dieser Lösungsmenge gibt es zwei Polynome vom Grad ≥ 1 (wähle $\beta = 1$ und α beliebig), nämlich

$$g = x^4 + x^3 + x^2 \quad \text{und} \quad h = x^4 + x^3 + x^2 + 1.$$

Wir wählen das Polynom g, um eine Faktorisierung von f zu erhalten. Nach Satz 18.35 gilt

$$f = (f, g) \cdot (f, g - 1) = (f, x^4 + x^3 + x^2) \cdot (f, x^4 + x^3 + x^2 + 1).$$

Übrigens liefert das andere Polynom h wegen $h = g - 1$ die gleiche Faktorisierung von f. Mithilfe des euklidischen Algorithmus' erhalten wir

$$(f, x^4 + x^3 + x^2) = x^2 + x + 1 \quad \text{und} \quad (f, x^4 + x^3 + x^2 + 1) = x^3 + x + 1.$$

Daraus folgt

$$f = (x^2 + x + 1)(x^3 + x + 1).$$

Beide Faktoren sind bereits irreduzibel über $\mathbb{F}_2$.

18.5 BCH-Codes

Die BCH-Codes wurden benannt nach ihren Entdeckern, R.C. Bose und D.K. Ray-Chaudhuri (1960) sowie A. Hocquenghem (1959). Sei ξ eine primitive n-te Einheitswurzel in $\mathbb{F}_{q^m}$ sowie $s \geq 0$ und $\delta \geq 1$ ganze Zahlen. Wir betrachten die folgende Matrix über $\mathbb{F}_{q^m}$

$$\begin{aligned} \bar{H} &= \begin{pmatrix} 1 & 1 & \dots & 1 \\ \xi^s & \xi^{s+1} & \dots & \xi^{s+\delta-2} \\ \vdots & \vdots & & \vdots \\ \xi^{(n-1)s} & \xi^{(n-1)(s+1)} & \dots & \xi^{(n-1)(s+\delta-2)} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & \dots & 1 \\ \xi & \xi^2 & \dots & \xi^{\delta-2} \\ \vdots & \vdots & & \vdots \\ \xi^{(n-1)} & \xi^{2(n-1)} & \dots & \xi^{(\delta-2)(n-1)} \end{pmatrix} \begin{pmatrix} 1 & & 0 \\ & \xi & \\ & & \ddots \\ 0 & & \xi^{(n-1)s} \end{pmatrix}. \end{aligned} \tag{18.25}$$

In dieser Matrix wird jeder Eintrag durch das entsprechende m-Tupel einer $\mathbb{F}_q$-Basis von $\mathbb{F}_{q^m}$ ersetzt. Die resultierende transponierte Matrix H kann als Kontrollmatrix eines Linearcodes der Länge n über $\mathbb{F}_q$ angesehen werden. Dieser Code heißt *BCH-Code* mit dem *Entwurfsabstand* δ.

Satz 18.37. (BCH-Schranke) *Jeder BCH-Code der Länge n über $\mathbb{F}_q$ mit dem Entwurfsabstand δ hat den Minimalabstand $d \geq \delta$.*

Beweis. Jede aus δ Spalten gebildete Teilmatrix von $\bar{H}$ ist eine vandermondesche Matrix

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \xi^{j_1} & \xi^{j_2} & \dots & \xi^{j_\delta} \\ \vdots & \vdots & & \vdots \\ \xi^{j_1(n-1)} & \xi_{j_2(n-1)} & \cdots & \xi_{j_\delta(n-1)} \end{pmatrix}$$

mit der Determinante

$$\prod_{i=1}^{\delta-1} \prod_{l=i+1}^{\delta} (\xi^{j_l} - \xi^{j_i}).$$

Diese Determinante ist aufgrund der Wahl von ξ von 0 verschieden. Also sind je δ Spalten von $\bar{H}$ linear unabhängig über $\mathbb{F}_{q^m}$ und somit auch linear unabhängig über $\mathbb{F}_q$. □

Beispiel 18.38. Sei ξ ein primitives Element in $\mathbb{F}_{2^m}$. Der Binärcode der Länge $n = 2^m - 1$, der anhand der Matrix

$$\begin{pmatrix} 1 & \xi & \xi^2 & \dots & \xi^{n-1} \\ 1 & \xi^2 & \xi^4 & \dots & \xi^{2(n-1)} \\ 1 & \xi^3 & \xi^6 & \dots & \xi^{3(n-1)} \\ 1 & \xi^4 & \xi^8 & \dots & \xi^{4(n-1)} \end{pmatrix}$$

als Kontrollmatrix gebildet wird, ist ein BCH-Code mit der Entwurfsdistanz $\delta = 5$.

18.6 Reed-Solomon-Codes

In diesem Abschnitt werden Reed-Solomon-Codes untersucht. Diese Codes werden in Compact-Disc-Systemen für die Codierung von Audiosignalen benutzt.

Lemma 18.39. *Sei $\alpha = (\alpha_1, \dots, \alpha_n)$ eine Folge paarweise verschiedener Elemente in $\mathbb{F}_q$ und $\beta = (\beta_1, \dots, \beta_n)$ eine Folge von 0 verschiedener Elemente in $\mathbb{F}_q$. Sei*

$$G_{k,\alpha,\beta} = \begin{pmatrix} \beta_1 & \beta_2 & \dots & \beta_n \\ \alpha_1\beta_1 & \alpha_2\beta_2 & \dots & \alpha_n\beta_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1}\beta_1 & \alpha_2^{k-1}\beta_2 & \dots & \alpha_n^{k-1}\beta_n \end{pmatrix}. \tag{18.26}$$

In der Matrix $G_{k,\alpha,\beta}$ sind je k Spalten linear unabhängig.

Beweis. Für die Matrix $G_{k,\alpha,\beta}$ gilt

$$G_{k,\alpha,\beta} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_n^{k-1} \end{pmatrix} \begin{pmatrix} \beta_1 & & & 0 \\ & \beta_2 & & \\ & & \ddots & \\ 0 & & & \beta_n \end{pmatrix}.$$

Im ersten Faktor ist jede aus k Spalten gebildete Teilmatrix eine vandermondesche Matrix

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_{j_1} & \alpha_{j_2} & \dots & \alpha_{j_k} \\ \vdots & \vdots & & \vdots \\ \alpha_{j_1}^{k-1} & \alpha_{j_2}^{k-1} & \dots & \alpha_{j_k}^{k-1} \end{pmatrix}$$

mit der Determinante

$$\prod_{i=1}^{k-1} \prod_{l=i+1}^{k} (\alpha_{j_l} - \alpha_{j_i}).$$

Diese Determinante ist aufgrund der Wahl der α_i von 0 verschieden. Also hat $G_{k,\alpha,\beta}$ die geforderte Eigenschaft. □

Ein $[n,k]$-Code über $\mathbb{F}_q$ mit der Generatormatrix (18.26) heißt *k-ter Reed-Solomon-Code* der Länge n über $\mathbb{F}_q$ (bzgl. α und β) und wird mit $\mathrm{RS}_k(\alpha,\beta)$ bezeichnet. Nach Satz 17.40 und Lemma 18.39 gilt der folgende

Satz 18.40. *Der Reed-Solomon-Code $\mathrm{RS}_k(\alpha,\beta)$ der Länge n über $\mathbb{F}_q$ ist ein $[n,k]$-Code mit dem Minimalabstand $d = n-k+1$.*

Beispiel 18.41. Sei ξ ein primitives Element in $\mathbb{F}_8$. Für $\alpha = \beta = (1,\xi,\dots,\xi^6)$ ist der Reed-Solomon-Code $\mathrm{RS}_3(\alpha,\beta)$ ein $[7,3,5]$-Code mit der Generatormatrix

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

Satz 18.42. *Der duale Code des Reed-Solomon-Codes $\mathrm{RS}_k(\alpha,\beta)$ der Länge n über $\mathbb{F}_q$ ist ein Reed-Solomon-Code $\mathrm{RS}_{n-k}(\alpha,\gamma)$ für ein $\gamma \in \mathbb{F}_q^n$.*

Beweis. Sei $k = n-1$. Der duale Code C von $\mathrm{RS}_{n-1}(\alpha,\beta)$ ist 1-dimensional und besteht somit aus allen skalaren Vielfachen eines Vektors $\gamma \in \mathbb{F}_q^n$. Für diesen Vektor gilt $G_{n-1,\alpha,\beta}\gamma^T = 0$, d. h.

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-2} & \alpha_2^{n-2} & \dots & \alpha_n^{n-2} \end{pmatrix} \begin{pmatrix} \beta_1\gamma_1 \\ \vdots \\ \beta_n\gamma_n \end{pmatrix} = 0. \tag{18.27}$$

Angenommen, es wäre $\gamma_i = 0$ für ein $1 \le i \le n$. Dann wird das um die i-te Komponente verkürzte Gleichungssystem betrachtet

$$\begin{pmatrix} 1 & \dots & 1 & 1 & \dots & 1 \\ \alpha_1 & \dots & \alpha_{i-1} & \alpha_{i+1} & \dots & \alpha_n \\ \vdots & & \vdots & \vdots & & \vdots \\ \alpha_1^{n-2} & \dots & \alpha_{i-1}^{n-2} & \alpha_{i+1}^{n-2} & \dots & \alpha_n^{n-2} \end{pmatrix} \begin{pmatrix} \beta_1\gamma_1 \\ \vdots \\ \beta_{i-1}\gamma_{i-1} \\ \beta_{i+1}\gamma_{i+1} \\ \vdots \\ \beta_n\gamma_n \end{pmatrix} = 0.$$

Die Matrix dieses Gleichungssystems ist eine vandermondesche Matrix mit von 0 verschiedener Determinante. Also ist γ widersprüchlicherweise der Nullvektor. Somit besteht γ aus lauter von 0 verschiedenen Komponenten. Es folgt $\mathrm{RS}_{n-1}(\alpha,\beta)^\perp = \mathbb{F}_q\gamma = \mathrm{RS}_1(\alpha,\gamma)$.

Nun zum allgemeinen Fall. Die Produktmatrix $G_{k,\alpha,\beta}G^T_{n-k,\alpha,\gamma}$ besteht aus den Einträgen

$$\sum_{l=1}^{n}(\alpha_l^i\beta_l)(\alpha_l^j\gamma_l) = \sum_{l=1}^{n}\alpha_l^{i+j}\beta_l\gamma_l, \quad 0 \le i \le k-1,\ 0 \le j \le n-k-1.$$

Diese Einträge sind genau die auf der linken Seite von (18.27) vorkommenden Summen und somit aufgrund der Wahl von γ identisch 0. Folglich verschwindet die Produktmatrix. Aus Dimensionsgründen folgt die Behauptung. □

Sei ξ eine primitives Element in $\mathbb{F}_q$ und $n = q-1$. Der Reed-Solomon-Code $\mathrm{RS}_k(\alpha,\beta)$ über $\mathbb{F}_q$ mit $\alpha = (1,\xi,\dots,\xi^{n-1})$ und $\beta = (1,\dots,1)$ heißt *klassischer Reed-Solomon-Code* über $\mathbb{F}_q$ und wird mit RS_k bezeichnet. Der Code RS_k besitzt die Generatormatrix

$$G = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \xi & \dots & \xi^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \xi^{k-1} & \dots & \xi^{(n-1)(k-1)} \end{pmatrix}. \tag{18.28}$$

Ein Linearcode C der Länge n über $\mathbb{F}_q$ heißt *zyklisch*, wenn mit jedem Codevektor $(c_1,c_2,\dots,c_n)$ auch der zyklisch verschobene Vektor $(c_2,\dots,c_n,c_1)$ ein Codevektor ist.

Satz 18.43. *Der klassische Reed-Solomon-Code* RS_k *über* $\mathbb{F}_q$ *ist zyklisch.*

Beweis. Eine Nachricht $a = (a_0,\dots,a_{k-1}) \in \mathbb{F}_q^k$ wird codiert anhand des Codevektors

$$aG = (a(1), a(\xi), \dots, a(\xi^{n-1})),$$

wobei $a(\xi^j)$ die Auswertung des Polynoms $a = \sum_{i=0}^{n-1} a_i x^i$ an der Stelle ξ^j ist.

Für die Nachricht $b = (a_0, a_1\xi, \ldots, a_{k-1}\xi^{k-1})$ gilt

$$bG = (b(1), b(\xi), \ldots, b(\xi^{n-1})) = (a(\xi), a(\xi^2), \ldots, a(\xi^{n-2}), a(1)),$$

wobei wir die Beziehung $\xi^n = \xi^{q-1} = 1$ verwendet haben. □

Beispiel 18.44. Aus dem klassischen $[255, 251, 5]$-Reed-Solomon-Code RS_{251} über $\mathbb{F}_{2^8}$ wird durch Verkürzen ein $[254, 250]$-Code mit dem Minimalabstand $d \geq 5$. Nach der Singleton-Schranke muss $d = 5$ sein, der Code hat also wiederum das Geschlecht 0. Sukzessives Verkürzen liefert $[32, 28, 5]$- und $[28, 24, 5]$-Codes, die in heutigen Compact-Disc-Systemen eingesetzt werden.

Selbsttestaufgaben

18.1. Bestimme das Minimalpolynom von $\alpha = \sqrt[3]{5}e^{2\pi i/3}$ über $\mathbb{Q}$.

18.2. Berechne das Inverse von $a + bi \neq 0$ in $\mathbb{Q}[i]$.

18.3. Konstruiere eine Körpererweiterung von $\mathbb{Q}$, die alle Wurzeln von $x^2 - 2$ und $x^2 - 3$ enthält.

18.4. Eine Körpererweiterung $\mathbb{L}$ von $\mathbb{K}$ heißt *algebraisch*, wenn jedes Element von $\mathbb{L}$ algebraisch über $\mathbb{K}$ ist. Zeige, dass jede endliche Körpererweiterung algebraisch ist.

18.5. Sei $\mathbb{L}$ eine Körpererweiterung $\mathbb{L}$ von $\mathbb{K}$. Zeige, dass

$$A_{\mathbb{L}}(\mathbb{K}) = \{\alpha \in \mathbb{L} \mid \alpha \text{ ist algebraisch über } \mathbb{K}\}$$

eine algebraische Körpererweiterung von $\mathbb{K}$ ist.

18.6. Sei $f \in \mathbb{K}[x]$ irreduzibel über $\mathbb{K}$. Zeige, dass der Restklassenring $\mathbb{K}[x]/f\mathbb{K}[x]$ eine Körpererweiterung von $\mathbb{K}$ ist.

18.7. Sei $f \in \mathbb{K}[x]$ irreduzibel über $\mathbb{K}$ und α einer Wurzel von f. Zeige, dass die Abbildung $\mathbb{K}[x]/f\mathbb{K}[x] \to K(\alpha) : g + f\mathbb{K}[x] \mapsto g(\alpha)$ ein Isomorphismus ist.

18.8. Sei $f \in \mathbb{K}[x]$ mit der Zerlegung $f = f_1^{e_1} \cdots f_n^{e_n}$ in paarweise teilerfremde Potenzen irreduzibler Polynome. Zeige, dass der Ring $\mathbb{K}[x]/f\mathbb{K}[x]$ isomorph ist zum Produktring $\mathbb{K}[x]/f_1^{e_1}\mathbb{K}[x] \times \ldots \times \mathbb{K}[x]/f_n^{e_n}\mathbb{K}[x]$.

18.9. Sei α eine Wurzel des irreduziblen Polynoms $x^3 + x + 1 \in \mathbb{F}_2[x]$. Stelle die Verknüpfungstafeln des Körpers $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ auf.

18.10. Berechne $\mu(d)$ für alle positiven Teiler d von 72.

18.11. Der Vietasche Wurzelsatz (F. Vieta, 1540-1603) besagt, dass für jedes normierte Polynom $f = \sum_{j=0}^{n} f_j x^j$ mit den Wurzeln $\alpha_1, \ldots, \alpha_n$ gilt

$$f_{n-k} = (-1)^k \sum_I \prod_{i \in I} \alpha_i, \quad 1 \leq k \leq n,$$

wobei über alle k-Teilmengen I von $\{1, \ldots, n\}$ summiert wird. Benutze eine Wurzel des irreduziblen Polynoms $x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ und den Vietaschen Wurzelsatz, um alle irreduziblen Teiler von $x^8 - x$ in $\mathbb{F}_2[x]$ zu berechnen.

18.12. Sei β eine Wurzel des irreduziblen Polynoms $x^2 + \alpha x + 1$ über $\mathbb{F}_4$. Dabei sein α eine Wurzel des irreduziblen Polynoms $x^2 + x + 1$ über $\mathbb{F}_2$. Konstruiere den Körper $\mathbb{F}_{16} = \mathbb{F}_4(\beta)$ als Vektorraum über $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$.

18.13. Faktorisiere das Polynom $x^5 + x + 1$ in $\mathbb{F}_2[x]$.

18.14. Beweise die Gleichung (18.23).

18.15. Zeige, dass unter den Voraussetzungen in Abs. 18.4 die Anzahl der verschiedenen irreduziblen Faktoren von $f \in \mathbb{F}_q(x]$ gleich der Dimension des Kerns der Matrix $R - I_n$ ist.

18.16. Gib einen $[27, 23, 5]$-Code über $\mathbb{F}_{32}$ an.