KLEINE EINFÜHRUNG IN DIE KODIERUNGSTHEORIE

VORLESUNG VON B. PAREIGIS IM SS 1998

Inhaltsverzeichnis

Einleitung

Im Sommersemester 1998 habe ich in der Reihe der Fortbildungsveranstaltungen des Mathematischen Instituts der Ludwig-Maxililians-Universität München eine 1-stündige Vorlesung über Kodierungstheorie für Lehrer an Gymnasien in Bayern angeboten.

Es war das Ziel dieser Vorlesung, einen Begriff über die Möglichkeit und die Grenzen von vielen heute verwendeten Kodierungsmöglichkeiten zur Fehlerkorrektur zu vermitteln. Nicht die vielen Probleme der Verschlüsselung von Daten, um Zugriffe von Unbefugten zu vermeiden, sondern die Techniken zur Vermeidung oder Korrektur von Fehlern bei der Übertragung von Daten standen im Mittelpunkt der Vorlesung. Einfache Codes lassen sich schon mit Hilfsmitteln der linearen Algebra erstellen. Die Darstellung dieser Methoden und der Methoden der Fehlerkorrektur standen im Mittelpunkt der Vorlesung. Die moderne Kodierungstheorie verwendet zur Erstellung leistungsfähigerer Codes Hilfsmittel der Zahlentheorie und der algebraischen und arithmetischen Geometrie. Darauf konnte ich wegen der Kürze der Zeit nicht eingehen.

München, im Juli 1998 B. Pareigis

1. Der Satz von Shannon

Bemerkung 1.1. Informationen werden auf die verschiedenste Weise übertragen. Als Beispiele sehen wir Telefon, Funk, Fernsehen, Übertragung von Bildern aus dem Weltall (von den Sonden Mariner oder Voyager), Übertragung mit Hilfe von CD's, militärische Informationsübertragung, das Internet, Bankenverkehr, Codekarten für Bankkunden, aber auch für Telefon oder Zugänge zu Gebäuden, Email, Datenkompression bei Sicherungskopien im Computer, Barcodes, usw. Jeder dieser Übertragungswege hat zunächst einmal die Aufgabe, Information von einem Ort oder Zeitpunkt zu einem anderen zu übertragen. Die abgesandte Information muß korrekt beim Empfänger ankommen. Sie soll während der Übertragung weitgehend frei von äußeren Einflüssen bleiben und je nach Anwendung offen lesbar für jedermann oder aber nur für den Empfänger sein.

Bei der Informationsübertragung entstehen Fehler durch

- zufällige Störungen (Rauschen, Systemfehler),
- willkürliche Verfälschung.

Eine Korrektur kann

- durch Rückfrage erfolgen, falls der Empfänger den Fehler erkennt (Fehlererkennung),
- oder durch Kodierung der Information (zu offenem oder geheimem Text) (Fehlerkorrektur).

Eine Übertragung z.B. per CD oder aus dem Weltall läßt praktisch keine Nachfrage und Wiederholung zu, sie sollte so kodiert werden, daß Fehler nachträglich allein aufgrund der empfangenen Information korrigiert werden können.

Definition 1.2. Wir nehmen an, daß die zu übertragende Information in Form einer Bitfolge, also einer Folge bestehend aus 0 oder 1, gegeben ist. Uns werden in dieser Vorlesung lediglich Fehler interessieren, die durch zufällige Störungen auf dem Informationskanal entstehen. Willkürliche Verfälschungen und systematische Fehler sollen hier nicht studiert werden.

Wir nehmen also für den Informationskanal an, daß

- ein übertragenes Bit 1 mit *fester* Wahrscheinlichkeit p das Bit 0 und mit der Wahrscheinlichkeit $1-p$ das Bit 1 ergibt, und
- ein übertragenes Bit 0 mit *derselben* Wahrscheinlichkeit p das Bit 1 und mit der Wahrscheinlichkeit $1-p$ das Bit 0 ergibt.

Dabei gilt $0 \leq p \leq 1/2$. Wenn $1/2 < p \leq 1$ gilt, dann kann man durch Invertieren der Bits $(0 \mapsto 1, 1 \mapsto 0)$ auf die vorherige Annahme zurückkommen. Der Fall $p = 1/2$ bedeutet offenbar vollständigen Informationsverlust.

Wir nehmen weiterhin an, daß auf dem Kanal jeweils genau ein Bit je Zeiteinheit (z.B. pro Millisekunde) übertragen wird.

Einen solchen Kanal nennt man einen *diskreten, binären, symmetrischen Kanal ohne Speicher* (BSC).

Beispiele 1.3. für Kodierungen:

1) Paritäts-Prüfsumme (Parity Check): Bei einem Computerspeicher verwendet man zur Speicherung von 1 Byte (= 8 Bits) $B = (b_1 \dots b_8)$ ein weiteres Kontrollbit b_9, also 9 Bits, wobei das 9. Kontrollbit wie folgt bestimmt wird: wenn n die Anzahl der Bits eines Bytes ist, die auf 1 gesetzt sind, so ist das

$$\text{Kontrollbit} = \begin{cases} 1, & \text{falls } n \text{ ungerade,} \\ 0, & \text{falls } n \text{ gerade.} \end{cases}$$

Zur Überprüfung testet man, ob für die Summe aller übertragenen 9 Bits gilt

$$\sum_{i=1}^{9} b_i \equiv 0 \mod (2).$$

Wenn diese Bedingung verletzt ist, dann ist sicher bei der Übertragung ein Fehler aufgetreten. Wenn ein einziges Bit falsch übertragen wird, dann wird diese Kontrollbedingung schon verletzt. Eine solche Kodierung kann also einen Fehler (pro übertragenes Byte) erkennen. Dieses Verfahren wird bei vielen PCs verwendet. Wird ein Fehler erkannt, so kann dieser nicht automatisch korrigiert werden, der Computer bleibt also sicherheitshalber stehen.

2) Das Morsealphabet, das mit den Zeichen . (dit) und – (dah) aufgebaut wird. Genauer werden die „Strings" aus den Buchstaben {. (dit), – (dah), _ (kurze Pause), __ (lange Pause)} gebildet. Mit diesen Zeichen können die Buchstaben des Alphabets gebildet werden (z.B. a = .- ; b = -...).

Definition 1.4. Wörterbuch der Kodierung: Ein *Code* ist eine Menge C (von Zeichen, die geeignet ist, Informationen zu speichern und zu übermitteln).

Eine *Chiffre* oder eine *Verschlüsselung* (*Kodierung* oder *Chiffrierung*) ist eine Abbildung $f : C_1 \to C_2$ eines Codes in einen anderen.

Eine *Dechiffrierung* einer Chiffre $f : C_1 \to C_2$ ist eine Abbildung $g : C_2 \to C_1$ mit $gf = \mathrm{id}$.

Die Quelle einer Chiffre $f : C_1 \to C_2$ heißt *Klartext*, ein Element des Klartextes heißt *Nachrichtenwort*.

Ein Element des Bildes einer Chiffre heißt *Codewort*.

Eine Kodierung heißt *lineare Kodierung*, wenn C_1 und C_2 Vektorräume sind und $f : C_1 \to C_2$ eine lineare Abbildung ist.

Ein *Blockcode* ist ein Code, dessen Wörter aus Buchstaben eines Alphabets (typischerweise aus den Bits 0 und 1) zusammengesetzt sind und alle gleiche Länge haben, d. h. aus gleich vielen Buchstaben bestehen.

Wir betrachten hauptsächlich Kodierungen f, die injektiv sind. Falls dies nicht der Fall ist, ist die oben angegebene Bedingung für eine Dekodierung nicht erfüllbar. Es gibt jedoch Beispiele, in denen eine Kodierung mit einer nicht injektiven Abbildung sinnvoll ist, z.B. die Graphik-Kompressions-Protokolle JPEG, GIF und andere.

Beispiele 1.5. für Codes und Kodierungen:

1) Sprachen sind beliebige Mengen (und damit Codes) von „strings" oder Wörtern über einem beliebigen Alphabet A.

2) Das Zahlensystem, d. h. die mit den Ziffern $0, \ldots, 9$ und den Zeichen . und – dargestellten Zahlen, ist ein Code.

3) Die q- und die z-Gruppen in der Morsesprache, das sind Gruppen von drei Buchstaben des (Buchstaben-)Alphabets, die mit q bzw. z beginnen, z.B. qth = Standort, bilden einen Code.

4) Die Barcodes zur Bezeichnung von Waren im Supermarkt sind Codes.

5) Der ISBN-Code (International Standard Book Number), wie z.B. 3-519-02211-7, ist ein Code, wobei die einzelnen Gruppen folgendes bedeuten:

1. 3 = Erscheinungsland
2. 519 = Verlag
3. 02211 = fortlaufende Buchnummer
4. 7 = Prüfnummer (in $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X\}$).

Die Prüfung auf eine korrekte Übertragung (Fehlererkennung) geschieht im Beispiel durch Überprüfung von $10 \cdot 3 + 9 \cdot 5 + 8 \cdot 1 + 7 \cdot 9 + 6 \cdot 0 + 5 \cdot 2 + 4 \cdot 2 + 3 \cdot 1 + 2 \cdot 1 + 1 \cdot 7 \equiv 0 \mod 11$. Die Restklassenberechnung modulo 11 kann durch Bildung der alternierenden Quersumme vorgenommen werden. (http://infoshare1.princeton.edu/katmandu/marc/aut020.html)

6) Beliebiger Text der Umgangssprache kann in einen linearen Code K^n für $K = GF(q)$ übersetzt werden, indem man zunächst den Text jeweils in Gruppen von l Buchstaben und Abstände (und evtl. sonstige Zeichen) zusammenfaßt. Bei der Verwendung von $a, \ldots, z, A, \ldots, Z, \mathit{Zwischenraum}$ sind also 53^l verschiedene solche Textgruppen möglich. Diesen weist man in einer beliebig festzulegenden Weise ebenso viele verschiedene Elemente in K^n zu. Damit bestimmt sich l aus $53^l \leq q^n$ als $l \leq n \cdot \frac{\ln(q)}{\ln(53)}$.

Bemerkung 1.6. Wir werden im folgenden immer Blockcodes verwenden, d. h. die Elemente der beiden Codes einer Kodierung haben alle gleiche Länge, z.B. gleiche Anzahl von Bits. Ein Blockcode der Länge k hat also q^k Wörter, wenn q die Anzahl der Zeichen des verwendeten Alphabets ist, also für $\{0, 1\}$ ist $q = 2$.

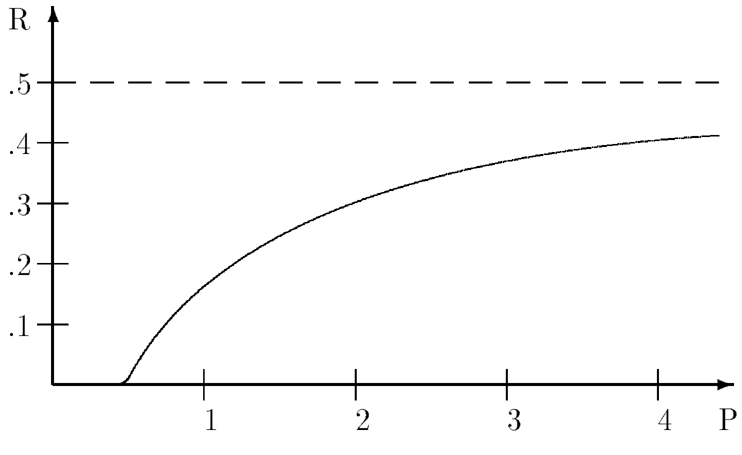
Wir verwenden zur Übertragung einen binären, symmetrischen Kanal (BSC). Wenn eine Kodierung mit Blockcodes $f : C_1 \to C_2$ gegeben ist, wobei C_1 Wörter der Länge k und C_2 Wörter der Länge n besitzt und das verwendete Alphabet $\{0, 1\}$ ist, so werden bei der Übertragung von n Bits, also in n Zeiteinheiten lediglich k Informationsbits übermittelt. Die *Durchsatzrate* der Kodierung ist dann k/n. Weiter ist die *Bit-Fehler-Wahrscheinlichkeit* die Wahrscheinlichkeit, daß ein Bit eines Klartextwortes trotz erfolgter Fehlerkorrektur falsch ankommt.

Wir formulieren jetzt den Satz von Shannon, ohne ihn allerdings zu beweisen. Er dient zum Verständnis der Möglichkeiten der Kodierungstheorie und außerdem als Motivation dafür, möglichst viele verschiedene Kodierungen zu finden und zu studieren.

Theorem 1.7. Der Satz von Shannon (Claude Shannon: A mathematical theory of communication - 1948.) *Sei ein binärer symmetrischer Kanal mit einer Bit-Fehler-Wahrscheinlichkeit* $0 \leq p < \frac{1}{2}$ *gegeben. Dann gibt es eine Zahl* $C > 0$*, die* Kanalkapazität*, so daß es zu jedem* $\varepsilon > 0$ *und zu jeder Durchsatzrate* $0 < R < C$ *einen Blockcode* B *mit Bit-Fehler-Wahrscheinlichkeit* $P(B) < \varepsilon$ *gibt.*

Die Kanalkapazität ist $C = 1 + p\log_2(p) + (1 - p)\log_2(1 - p)$.

Bemerkung 1.8. Der Zusammenhang zwischen Durchsatzrate R und Bit-Fehler-Wahrscheinlichkeit P ist annähernd gegeben durch die folgende Kurve



Alle Punkte im Bereich oberhalb der Kurve sind mit Codes erreichbar, d. h. zu jedem Paar (P, R) oberhalb der Kurve gibt es Codes, deren Durchsatzrate und Bit-Fehler-Wahrscheinlichkeit diesen Wert beliebig genau annähern.

Der Satz von Shannon beruht auf einem reinen Existenzbeweis. Er gibt keine Möglichkeit zur Konstruktion geeigneter Codes an. Der Satz gilt wesentlich allgemeiner, u.a. auch für lineare Codes. Die praktisch verwendeten Blockcodes können sehr lang werden, z.B. 10^{100} mögliche Codewörter.

2. Die Hamming-Metrik

Beispiel 2.1. Der (7,4)-Hamming-Code: Wir verwenden als Codewörter Linearkombinationen der Zeilen-Vektoren von

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

in dem Vektorraum K^7 mit $K := \mathbb{F}_2 = \{0, 1\}$. Die Information ist in den ersten 4 Bits enthalten. Diese können beliebig mit 0 oder 1 besetzt werden. Also haben wir $2^4 = 16$ Codewörter. Die Durchsatzrate ist $4/7 = 0.57$.

Dieser Code hat eine der verblüffendsten Fehlerkorrektur-Möglichkeiten. Wir verwenden die Vektoren

$$\begin{aligned} a &= (0001111), \\ b &= (0110011), \\ c &= (1010101). \end{aligned}$$

Wenn in einem übertragenen Codewort ein Fehler auftritt, z.B. wenn $x = (1011010)$ übertragen wird als $y = (1010010)$ mit einem Fehler im 4. Bit, dann rechne man $\langle y, a\rangle = 1, \langle y, b\rangle = 0, \langle y, c\rangle = 0$ und erhält die Binärzahl 100 oder den Wert 4. Zur Fehlerkorrektur ist nun die 4. Stelle zu korrigieren.

Dieser Code kann grundsätzlich einen Fehler pro Codewort korrigieren. Er hat eine Durchsatzrate von 0.57. Die Bit-Fehler-Wahrscheinlichkeit ergibt wie folgt.

$$q^7 \text{ (keine Fehler) } + 7pq^6 \text{ (ein Fehler) } = 0.4783 + 0.3720 = 0.8503$$

ist die Wahrscheinlichkeit für ein korrekt empfangenes Codewort, also ist die Wort-Fehlerwahrscheinlichkeit 0.1497. Das entspricht einer Bit-Fehler-Wahrscheinlichkeit von 0.0398.

Wir wollen Erkenntnisse über lineare Abbildungen und Matrizen verwenden, um Probleme der linearen Kodierung zu formulieren und zu lösen.

Wir werden in diesem Abschnitt als Grundkörper durchgehend den endlichen Körper $K := GF(q)$ mit q Elementen verwenden. GF ist dabei eine Abkürzung für das Wort Galois-Feld. Man kann zeigen, daß es genau dann einen Körper mit q Elementen gibt, wenn q ein Primzahlpotenz ist, d. h. wenn es eine Primzahl p und eine natürliche Zahl n mit $q = p^n$ gibt. Dieser Körper ist zudem durch die Angabe von q bis auf Isomorphie eindeutig bestimmt.

Wir kennen bisher lediglich die endlichen Körper $GF(p) = \mathbb{Z}/p\mathbb{Z}$ für Primzahlen p. Zunächst werden unsere Anwendungen nur den Körper $\mathbb{Z}/2\mathbb{Z}$ mit zwei Elementen (binäres System der Computer!) benutzen. Daher werden wir die Konstruktion der übrigen Körper $GF(q)$ erst später diskutieren. Wir verweisen den interessierten Leser jedoch jetzt schon auf Lehrbücher der Algebra.

Wir werden im folgenden nur lineare Codes der Form $C = K^n$ mit $K = GF(q)$ verwenden mit der linearen Chiffrierung $f : K^k \to K^n$. Wegen der notwendigen Dechiffrierung wird f immer als Monomorphismus vorausgesetzt.

Eine Kodierung $f : C_1 \to C_2$ bildet den Code C_1 auf eine Teilmenge von C_2 ab. Bei einer Störung der Übertragung von Codewörtern aus C_2 kann es vorkommen, daß ein empfangenes Wort aus C_2 kein Codewort mehr ist, also nicht im Bild von f liegt. Es erhebt sich die Frage beim Empfänger, das Codewort aus dem empfangenen Wort mit Hilfe der Redundanz zurückzugewinnen.

Man kann beweisen, daß bei Verwendung eines binären symmetrischen Kanals das wahrscheinlichste Codewort (maximum likelyhood) gerade durch den kürzesten Abstand der

Hamming-Metrik gegeben ist. Daher sollten die Codewörter möglichst gleichmäßige Abstände im Sinne der Hamming-Metrik besitzen und es sollte der Raum C_2 mit dem Bild von f im Sinne einer möglichst dichten Kugelpackung gefüllt werden.

Definition 2.2. Sei K^n ein linearer Code. Die *Hamming-Metrik* auf K^n ist die Abbildung $d : K^n \times K^n \to \mathbb{N}_0$ mit $d(x, y) :=$ Anzahl der $i \in \{1, \ldots, n\}$ mit $\xi_i \neq \eta_i$. Die Auffassung ist hierbei, daß $d(x, y)$ die Anzahl der Koeffizienten von x angibt, die in y anders (falsch) angegeben werden. Der Wert $d(x, y)$ heißt *Hamming-Abstand* von x und y. Die *Hamming-Gewichtsfunktion* ist die Abbildung $\|.\| : K^n \to \mathbb{N}_0$ mit $\|x\| := d(x, 0)$. Das ist die Anzahl der von Null verschiedenen Komponenten von x.

Definition 2.3. Ein Paar (M, d) heißt *metrischer Raum mit der Metrik* d, wenn M eine Menge und $d : M \times M \to \mathbb{R}$ eine Abbildung sind mit

1) $\forall x, y \in M[d(x, y) = 0 \iff x = y]$,
2) $\forall x, y \in M[d(x, y) = d(y, x)]$,
3) $\forall x, y, z \in M[d(x, z) \leq d(x, y) + d(y, z)]$ (Dreiecksungleichung).

Lemma 2.4. *Die Hamming-Metrik ist eine Metrik auf* K^n*.*

Beweis. folgt unmittelbar aus der Definition. □

Wir vermerken noch eine leicht einzusehende zusätzliche Translationsinvarianz $d(x, y) = d(x+z, y+z)$, die zeigt, daß d durch das Hamming-Gewicht $\|.\|$ schon vollständig bestimmt ist, denn $d(x, y) = \|x - y\|$.

Ein weiteres bekanntes Beispiel für eine Metrik ist der reelle Vektorraum $\mathbb{R}^n$ mit der sogenannten euklidischen Metrik

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (\xi_i - \eta_i)^2}.$$

Lemma 2.5. *Für das Hamming-Gewicht* $\|.\| : K^n \to \mathbb{N}_0$ *gelten*

1) $\|x\| = 0 \iff x = 0$,
2) $\forall \lambda \neq 0 \; [\|\lambda x\| = \|x\|]$,
3) $\|x + y\| \leq \|x\| + \|y\|$.

Beweis. leicht nachzurechnen, da $\|x\|$ die Anzahl der von Null verschiedenen Komponenten von x ist. □

3. Lineare Codes

Bemerkung 3.1. Im folgenden Abschnitt gehen wir von der allgemeinen Vorstellung aus:

$$\boxed{\text{Klartext}} \xrightarrow{\text{Kodierung}} \boxed{\text{Sender}} \xrightarrow{\text{Übertragung/Störung}} \boxed{\text{Empfänger}} \xrightarrow{\text{Decodierung}} \boxed{\text{Klartext}}$$

Es wird also ein Klartext codiert, über eine Informationsleitung zum Empfänger übermittelt, (wobei der Text aufgrund der Kodierung eventuell auch abhörsicher ist,) wird auf der Übertragungsstrecke mit Störungen verschiedener Art verändert und beim Empfänger wieder decodiert. Wir wollen Methoden finden, die Fehler bei der Übertragung zu erkennen und möglichst auch zu korrigieren. Wenn also x ein codiertes ausgesandtes Wort ist und y das empfangene Wort ist, dann soll festgestellt werden, ob es tatsächlich durch die Kodierung entstanden ist oder verändert wurde und ob man daraus das Wort x rekonstruieren kann.

Definition 3.2. Wenn bei einer Kodierung $f : K^k \to K^n$ Fehler an höchstens r Stellen des übertragenen Wortes immer erkannt werden können, so sagen wir, daß die Kodierung *r-fehlerentdeckend* ist. Wenn Fehler an höchstens s Stellen durch die restliche Information im übertragenen Wort korrigiert werden können, so heißt die Kodierung *s-fehlerkorrigierend.*

Bemerkung 3.3. In (1.4) haben wir lineare Kodierungen als lineare Abbildungen $f : C_1 \to C_2$ zwischen zwei Vektorräumen definiert. Für unsere Anwendungen soll f immer injektiv sein. Ohne Einschränkung können wir $C_2 = K^n$ wählen.

Außer einer bijektiven Umschreibung des Codes C_1 verlieren wir nichts, wenn wir C_1 mit dem Bild von f, also einem Untervektorraum $V \subseteq K^n$ identifizieren.

Wenn unser Grundkörper $K = GF(q)$ ist mit q, einer Primzahlpotenz, Elementen, so besitzt die Menge der n-Tupel K^n genau q^n Elemente.

Ein k-dimensionaler Unterraum $V \subseteq K^n$ wird ein (n, k)-*Code* genannt.

Wir betreiben also Theorie von Vektorräumen und Untervektoräumen über einem endlichen Körper $GF(q)$, wenn wir lineare Codes studieren.

Beispiel 3.4. Sei $K = GF(2) = \mathbb{F}_2 = \{0, 1\}$ der Körper mit zwei Elementen. In K^5 betrachten wir den Unterraum

$$\begin{aligned} V = \{&(0\ 0\ 0\ 0\ 0), (1\ 0\ 0\ 1\ 1), (0\ 1\ 0\ 1\ 0), (1\ 1\ 0\ 0\ 1),\\ &(0\ 0\ 1\ 0\ 1), (1\ 0\ 1\ 1\ 0), (0\ 1\ 1\ 1\ 1), (1\ 1\ 1\ 0\ 0)\} \end{aligned}$$

Dieses ist ein 3-dimensionaler Unterraum und definiert einen $(5, 3)$-Code mit $2^3 = 8$ Codewörtern. Wir werden dieses Beispiel als Standardbeispiel weiter verwenden.

Bemerkung 3.5. Sei $V \subseteq K^n$ eine (n, k)-Code und seien $b_1, \ldots , b_k$ eine Basis von V. Dann ist V vollständig bestimmt durch die Angabe dieser Basis oder durch die Matrix $B = \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix}$. Diese Matrix hat wegen der linearen Unabhängigkeit der Zeilen $b_1, \ldots , b_k$ den Zeilenrang k. Die Vektoren aus V sind genau die Linearkombinationen der Zeilen von B. Die Matrix B wird daher auch eine *erzeugende Matrix* für V genannt. Sie ist nicht eindeutig, weil es viele verschiedene Basen für V gibt.

Jede $(k\times n)$-Matrix vom Zeilenrang k mit Vektoren aus V definiert eine erzeugende Matrix für V.

Statt die Liste der Codewörter eines Codes anzugeben, ist es ökonomischer, eine erzeugende Matrix anzugeben. Für einen binären $(50, 30)$-Code hat eine solche Matrix 1500 Einträge, während die Liste der Codewörter mehr als 10^9 Wörter umfassen würde.

Ein erzeugende Matrix B definiert eine injektive lineare Abbildung $B : K^k \ni v \mapsto xB \in K^n$. Diese können wir als zugrunde liegende lineare Kodierung begreifen.

Unser Beispielcode hat beispielsweise folgende zwei erzeugende Matrizen:

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

Bemerkung 3.6. Wir erinnern daran, daß der Zeilenrang einer Matrix B die Maximalzahl linear unabhängiger Zeilen in B ist. Analog ist der Spaltenrang von B die Maximalzahl linear unabhängiger Spalten von B. Man zeigt in der lineare Algebra, daß Zeilenrang$(B) =$ Spaltenrang(B). Weiter ist der (Zeilen- oder Spalten-)Rang einer Matrix gleich der Dimension des Bildraumes von $B : K^r \ni v \mapsto xB \in K^s$. Das Bild wird nämlich von den Zeilenvektoren $b_i = e_iB$ aufgespannt, wobei die e_i die kanonische Basis bilden.

Die Transponierte B^T einer Matrix $B = (b_{ij}|i = 1, \dots, n; j = 1, \dots, k)$ ist die Matrix $B^T = (c_{ij}|i = 1, \dots, k; j = 1, \dots, n)$ mit $c_{ij} = b_{ji}$, also die an der Diagonalen gespiegelte Matrix.

Der Rang von B^T stimmt offenbar mit dem Rang von B überein.

Lemma 3.7. *Sei $V \subseteq K^n$ ein k-dimensionaler Unterraum. Dann ist*

$$V^\perp = \{w \in K^n | \langle v, w\rangle = vw^T = \sum_{i=1}^n \nu_i \omega_i = 0\}$$

ein Untervektorraum der Dimension $n - k$.

Beweis. Sei B eine erzeugende Matrix für V. Offenbar gilt $vw^T = wv^T = 0$ für alle $v \in V$ genau dann, wenn $wB^T = 0$. Da $B^T : K^n \to K^k$ mit $w \mapsto wB^T$ eine lineare Abbildung ist, ist $V^\perp = \mathrm{Ker}(B^T)$, insbesondere also ein Unterraum.

Der Zeilenrang von B ist gleich dem Spaltenrang von B^T gleich dem Zeilenrang von B^T gleich der Dimension des Bildes von B^T. Daher ist die Dimension des Kerns von B^T gleich $n - k$. $\square$

Definition 3.8. Sei $V \subseteq K^n$ ein Code. Dann heißt der Code $V^\perp \subseteq K^n$ *dualer Code* zu V.

Bemerkung 3.9. Seien V ein Code und $V^\perp$ der duale Code. Ist $v \in V$, so gilt $\langle v, w\rangle = 0$ für alle $w \in V^\perp$. Also ist $v \in V^{\perp\perp}$ und daher auch $V \subseteq V^{\perp\perp}$. Da die Dimension $\dim(V^{\perp\perp}) = n - (n - k) = k = \dim(V)$ ist, gilt $V = V^{\perp\perp}$.

Beispiel 3.10. Der duale Code $V^\perp$ zu unserem Beispielcode ist 2-dimensional und durch

$$V^\perp = \{(0\ 0\ 0\ 0\ 0), (1\ 1\ 0\ 1\ 0), (1\ 0\ 1\ 0\ 1), (0\ 1\ 1\ 1\ 1)\}$$

gegeben. Beachte, daß der Vektor $(0\ 1\ 1\ 1\ 1)$ sowohl in V als auch in $V^{\perp\perp}$ liegt, im Gegensatz zum Verhalten einer analogen Konstruktion für das euklidische Skalarprodukt.

Eine erzeugende Matrix ist

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

Definition 3.11. Sei $V \subseteq K^n$ ein Code. Die Transponierte $H = B'^T$ einer erzeugenden Matrix B' des dualen Codes $V^\perp$ heißt *Kontrollmatrix* für V.

Satz 3.12. *Jeder (lineare) Code $V \subseteq K^n$ stimmt überein mit dem Kern einer zugehörigen Kontrollmatrix H.*

Beweis. Ein Vektor v liegt genau dann in $V = V^{\perp\perp}$, wenn $vw^T = 0$ für alle $w \in V^\perp$ genau dann, wenn $vH = 0$ gilt, genau dann wenn er im Kern der Kontrollmatrix H liegt. $\square$

Beispiel 3.13. Eine Kontrollmatrix für unseren Beispielcode ist

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

Die durch die Kontrollmatrix definierten Gleichungen, z.B.

$$\nu_1 1 + \nu_2 1 + \nu_3 0 + \nu_4 1 + \nu_5 0 = 0$$
$$\nu_1 1 + \nu_2 0 + \nu_3 1 + \nu_4 0 + \nu_5 1 = 0$$

kann man als *verallgemeinerte Paritäts-Prüfsummen* auffassen.

Auch der Vektor $(0\ 1\ 1\ 1\ 1)^T$ könnte in einer Kontrollmatrix stehen. Die Gleichung

$$\nu_1 0 + \nu_2 1 + \nu_3 1 + \nu_4 1 + \nu_5 1 = 0$$

bedeutet dann, daß jeder Vektor in V eine gerade Anzahl von Einsen in den Bits 2 bis 5 haben muß.

Bemerkung 3.14. Wir können jetzt einen linearen Code $V \in K^n$ sowohl durch eine erzeugende Matrix B als auch durch eine Kontrollmatrix H vollständig beschreiben. Die wesentlichen Probleme sind jetzt die Dekodierung und die Fehlerkorrektur bzw. Fehlererkennung.

Bei der Dekodierung können wir uns auf den Standpunkt stellen, daß mit der Angabe eines Vektors v im Code V schon alles bekannt ist. Oder aber wir können den Vektor $x \in K^k$ mit $v = xB^T$ suchen.

4. Kontrollmatrizen und Hamming-Metrik

Definition 4.1. Sei $V \subseteq K^n$ ein Code mit einer erzeugenden Matrix B. Das *Hamming-Gewicht* $\|V\| = \|B\|$ von V bzw. von B ist das Minimum der Hamming-Gewichte $\|v\|$ aller $v \in V$ mit $v \neq 0$.

Das Hamming-Gewicht eines Codes V ist damit der minimale Hamming-Abstand zweier verschiedener Vektoren im Code: $d(v_1, v_2) = \|v_1 - v_2\|$.

Satz 4.2. *Sei $V \subseteq K^n$ ein linearer Code mit Kontrollmatrix H. Jede Codewort $v \in V$ von Hamming-Gewicht $r = \|v\|$ definiert eine lineare Abhängigkeitsrelation zwischen r Zeilenvektoren von H. Jede lineare Abhängigkeitsrelation zwischen r Zeilenvektoren von H definiert ein Codewort $v \in V$ vom Hamming-Gewicht $r = \|v\|$.*

Beweis. Sei $H = \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix}$ die Kontrollmatrix mit den Zeilenvektoren h_i. Sei $v = (\nu_1, \ldots, \nu_n)$. Es ist $v \in V$ genau dann, wenn $vH = 0$ genau dann, wenn $\sum \nu_i h_i = 0$. Die Summe hat genau so viele Summanden $\neq 0$, wie v von Null verschiedene Koeffizienten hat, wie das Hamming-Gewicht von v ist. □

Folgerung 4.3. *Sei $V \subseteq K^n$ ein (n,k)-linearer Code vom Hamming-Gewicht $\|V\|$ mit Kontrollmatrix H. Dann sind je $\|V\| - 1$ Zeilenvektoren von H linear unabhängig, und es gibt $\|V\|$ linear abhängige Zeilenvektoren, d. h. $\|V\|$ ist die Minimalzahl von linear abhängigen Zeilenvektoren von H.*

Beweis. Es gibt keinen Vektor $v \in V$, $v \neq 0$ vom Hamming-Gewicht $\|V\| - 1$, daher sind je $\|V\| - 1$ Zeilenvektoren von H linear unabhängig und umgekehrt. Es gibt einen Vektor $v \in V$, $v \neq 0$ vom Hamming-Gewicht $\|V\|$, daher gibt es $\|V\|$ Zeilenvektoren von H, die linear abhängig sind und umgekehrt. □

Folgerung 4.4. *Für jeden (n,k)-linearen Code $V \subseteq K^n$ gilt*

$$\|V\| \leq n - k + 1.$$

Beweis. Der Rang jeder Kontrollmatrix zu V ist $n-k$. Damit sind je $n-k+1$ Zeilenvektoren der Kontrollmatrix linear abhängig. Nach der vorhergehenden Folgerung ist also $\|V\| \leq n - k + 1$. □

Satz 4.5. (Fehlererkennung) *Sei $V \subseteq K^n$ ein (n,k)-linearer Code und sei $x \in K^n$. Wenn es ein $v \in V$ mit $v \neq x$ gibt, so daß $d(v,x) < \|V\|$, dann ist $x \notin V$, d. h. das Wort x ist kein Codewort, also falsch.*

Beweis. folgt unmittelbar aus der Tatsache, daß $\|V\|$ der minimale Hamming-Abstand zwischen zwei verschiedenen Codewörtern in V ist. □

Satz 4.6. (Fehlerkorrektur) *Sei $V \subseteq K^n$ ein (n, k)-linearer Code und sei $x \in K^n$. Wenn es ein $v \in V$ gibt mit $d(v, x) < \frac{1}{2}\|V\|$, dann gilt für alle $v' \in V, v' \neq v: \ d(v, x) < d(v', x)$, d. h. v ist das einzige Element von V mit dem gegebenen Abstand $d(v, x)$ und somit eindeutig durch x bestimmt.*

Beweis. Für $v' \in V$ und $v' \neq v$ gilt $2d(v, x) < \|V\| \leq d(v, v') \leq d(v, x) + d(x, v')$, also $d(v, x) < d(v', x)$. □

Bemerkung 4.7. Wenn bei der Übertragung von v weniger als $\frac{1}{2}\|V\|$ Fehler aufgetreten sind und $x \in K^n$ empfangen wurde, dann ist also $v \in V$ mit $d(v, x) < \frac{1}{2}\|V\|$ das übertragene Element. Somit ist eine linearer Code immer $(\|V\| - 1)$-fehlererkennend und $\frac{1}{2}(\|V\| - 1)$-fehlerkorrigierend. Es kommt also darauf an, Codes V mit möglichst großem Hamming-Gewicht $\|V\|$ zu finden.

Man wird mit den Voraussetzungen des vorhergehenden Satzes $x \in K^n$ als $v \in V$ dekodieren und hat damit die geringstmögliche Anzahl von Änderungen vorgenommen. Damit verwendet die Korrektur den wahrscheinlichsten Fehlerfall in Sinne von „maximum likelihood".

Beispiele 4.8. 1) Paritäts-Prüfungs-Codes: Sei $n \geq 2$ und $k = n - 1$ und $f : K^k \to K^n$ gegeben durch $f(\alpha_1, \ldots, \alpha_{n-1}) = (\alpha_1, \ldots, \alpha_n)$ mit $\alpha_n = -(\alpha_1 + \ldots + \alpha_{n-1})$. Offenbar ist f eine injektive lineare Abbildung. Weiter ist $v \in V = \mathrm{Bi}(f)$ genau dann, wenn $\sum_{i=1}^n \alpha_i = 0$. Wenn $q = 2$ ist, dann wird jede ungerade Anzahl von Fehlern dadurch erkannt, daß $\sum_{i=1}^n \alpha_i = 1$ gilt. Ein gerade Anzahl von Fehlern wird nicht erkannt. Für $v \in V$ und $v \neq 0$ müssen mindestens zwei Koeffizienten von Null verschieden sein, also ist $\|V\| = 2$. Damit kann zwar ein Fehler (und sogar eine ungerade Anzahl von Fehlern) erkannt werden, jedoch ergibt sich keine Möglichkeit zur Korrektur von Fehlern. Diese Kodierungen werden z.B. in PCs verwendet, wenn 8-Bit Worte in 9-Bit Speichern gespeichert werden und das 9. Bit durch die Abbildung f bestimmt wird.

2) Wiederholungscode: Eine einfache Möglichkeit einer sichereren Übertragung auf einer gestörten Übertragungsstrecke ist die dreifache Übertragung jedes einzelnen Wortes. Dabei ist $n = 3m$ und $f : K^k \to K^n$ durch $f(x) = (x, x, x)$ gegeben. Das ist wieder eine linearer Code $V = \mathrm{Bi}(f)$. Man sieht sofort, daß $\|V\| = 3$ ist, also ist dieser Code 2-fehlerentdeckend und 1-fehlerkorrigierend.

Folgerung 4.9. *Sei $V \subseteq K^n$ ein Code mit Kontrollmatrix $H = \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix}$.*

(a) Sei $v \in V$, und seien bei der Übertragung genau t Fehler aufgetreten. Wenn $x \in K^n$ der empfangene Wert ist, dann ist die minimale Anzahl der Koeffizienten $\xi_i \neq 0$, so daß $xH = \sum \xi_i h_i$ gilt, höchstens t.

(b) Sei $v \in V$, seien bei der Übertragung genau t Fehler aufgetreten, und sei $t < \frac{1}{2}\|V\|$. Wenn $x \in K^n$ der empfangene Wert ist, dann gibt es t eindeutig bestimmte Koeffizienten ξ_i mit $xH = \sum \xi_i h_i$. Der Übertragungsfehler ist dann $\sum \xi_i e_i$, und es gilt $v = x - \sum \xi_i e_i$.

Beweis. Mit (a) kann die Anzahl der aufgetretenen Fehler nach unten abgeschätzt werden. Man braucht $v \in V$ nicht zu kennen. Sei $\sum \mu_i e_i$ der Übertragungsfehler, d. h. $x = v + \sum \mu_i e_i$. Dann ist $xH = vH + \sum \mu_i e_i H = \sum \mu_i h_i$. Seien genau t Fehler aufgetreten, so ist die Anzahl der Summanden t. Es ist jedoch möglich, durch andere Wahl der Koeffizienten (weniger Koeffizienten) ξ_i eine andere Linearkombination $\sum \xi_i h_i$ zu erhalten, die mit xH übereinstimmt.

Wenn in (b) weniger als $\frac{1}{2}\|V\|$ Fehler aufgetreten sind, dann ist die minimale Anzahl der Summanden in der Darstellung $xH = \sum \mu_i h_i$ kleiner als $\frac{1}{2}\|V\|$. Wegen (4.3) sind die verwendeten h_i linear unabhängig. Wenn $xH = \sum \lambda_j h_j$ eine weitere Darstellung ist und die Anzahl der Summanden minimal, insbesondere also kleiner als $\frac{1}{2}\|V\|$, ist, dann ist $\sum \mu_i h_i - \sum \lambda_j h_j = 0$ mit weniger als $\|V\|$ Summanden. Die verwendeten h_i sind nach (4.3) linear unabhängig, also stimmen die λ_i mit den μ_i überein, d. h. die Darstellung $xH = \sum \mu_i h_i$ mit weniger als $\frac{1}{2}\|V\|$ Summanden ist eindeutig, und der Fehler ist $x - v = \sum \lambda_i e_i$. Man beachte hier jedoch, daß der Fehler nur unter der Annahme $t < \frac{1}{2}\|V\|$ korrigiert werden konnte. □

Man kann die Minimalzahl von linear abhängigen Zeilenvektoren in H und damit das Hamming-Gewicht von V bestimmen, daher ist es sinnvoll eine beliebige Kontrollmatrix H zu konstruieren und dann aus ihr den Code $V \subseteq K^n$ abzuleiten. Man kann dann H unmittelbar mit einem möglichst großen Minimum an linear abhängigen Vektoren konstruieren. Dann brauchen wir nur noch $V = \mathrm{Ker}(H)$ zu berechnen.

Beispiel 4.10. 1) Sei $K = \mathbb{Z}/11\mathbb{Z}$. Sei die Kontrollmatrix

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

Dann kann man nachrechnen, daß die Minimalzahl von linear abhängigen Zeilenvektoren 4 ist. Eine erzeugende Matrix für den Code $V \subseteq K^7$ gewinnt man aus der Basis des Kerns von H. Sie ist

$$B := \begin{pmatrix} 9 & 1 & 2 & 10 & 0 & 0 & 0 \\ 9 & 2 & 1 & 0 & 10 & 0 & 0 \\ 8 & 2 & 2 & 0 & 0 & 10 & 0 \\ 7 & 5 & 3 & 0 & 0 & 0 & 8 \end{pmatrix}.$$

Diese Kodierung hat das Hamming-Gewicht 4, kann also 3 Fehler erkennen und einen Fehler korrigieren.

2) Sei $K = \mathbb{Z}/2\mathbb{Z}$. Sei die Kontrollmatrix

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

Dann kann man nachrechnen, daß die Minimalzahl von linear abhängigen Zeilenvektoren 3 ist. Eine erzeugende Matrix für den Code $V \subseteq K^7$ ist

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

Diese Kodierung hat das Hamming-Gewicht 3, kann also 2 Fehler erkennen und einen Fehler korrigieren.

5. Systematische Codes

Wir gehen zunächst davon aus, daß bei einer Kodierung $B : K^k \to K^n$ die Informationsbits $v = (\nu_1, \dots, \nu_k)$ durch Anwendung von B auf das ganze Codewort xB „verschmiert" werden und daß in diesem Codewort die Fehlerkontrollbits ebenfalls enthalten sind. Daher sind Codes von spezieller Gestalt etwas einfacher zu behandeln. Wir werden jedoch sehen, daß jeder Code in einen Code der speziellen Gestalt umgewandelt werden kann.

Definition 5.1. Ein *systematischer Code* ist ein Code, der eine erzeugende Matrix, genannt *systematische erzeugende Matrix*, der Form

$$(I_k P) = \begin{pmatrix} 1 & 0 & \dots & 0 & p_{11} & \dots & p_{1,n-k} \\ 0 & 1 & \dots & 0 & p_{21} & \dots & p_{2,n-k} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & p_{k1} & \dots & p_{k,n-k} \end{pmatrix}$$

hat.

Bemerkung 5.2. Eine systematische erzeugende Matrix

$$B = (b_1, \dots, b_n) = (I_k P) = (e_1, \dots, e_k, p_1, \dots, p_{n-k})$$

eines systematischen Codes induziert eine lineare Abbildung $B : K^k \to K^n$ mit $xB = (\xi_1, \dots, \xi_n)B = \sum \xi_i b_i = (\xi_1, \dots, \xi_k, xp_1^T, \dots, xp_{n-k}^T)$. Das Klartextwort $x \in K^k$ ist also der erste Teil des Codewortes xB. Es wird oft die *Menge der Informationssymbole* genannt. Der zweite Teil ist der Fehlerkorrektur vorbehalten und stellt verallgemeinerte Paritäts-Prüfsummen xp_i oder *Redundanzsymbole* dar. Die Elemente von V haben die folgende Form: an den ersten k Stellen stehen beliebige Koeffizienten $\lambda_1, \dots, \lambda_k$. Die weiteren Stellen $\lambda_{k+1}, \dots, \lambda_n$ berechnen sich daraus als

$$\lambda_{k+i} := (\lambda_1, \dots, \lambda_k)p_i = \sum_{j=1}^{k} \lambda_j p_{ji}.$$

Satz 5.3. *Sei $B = (I_k P)$ eine erzeugenden Matrix eines systematischen Codes V. Dann ist $H = \begin{pmatrix} -P \\ I_{n-k} \end{pmatrix}$ eine Kontrollmatrix für V.*

Beweis. Es ist $BH = (I_k P) \begin{pmatrix} -P \\ I_{n-k} \end{pmatrix} = 0$. Da $\mathrm{Rang}(B) = k$ und $\mathrm{Rang}(H) = n - k$, ist V, der von B erzeugte Unterraum der Dimension k, gleich dem $\mathrm{Kern}(H)$, der ja auch die Dimension k hat. $\square$

Beispiel 5.4. Die Matrix $B = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$ ist eine systematische erzeugende Matrix. Die zugehörige Kontrollmatrix ist $H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$. Die Redundanzsymbole ergeben sich als

$$\lambda_4 = \lambda_2 + \lambda_3$$
$$\lambda_5 = \lambda_1 + \lambda_3$$

Der Code hat nach (4.3) das Hamming-Gewicht 2, ist also 1-fehlererkennend, kann aber keine Fehler korrigieren.

Bemerkung 5.5. Elementare Zeilenumformungen sind:

1. Die Addition eines Vielfachen einer Zeile zu einer anderen Zeile und
2. die Multiplikation einer Zeile mit einem Faktor $\alpha \neq 0$.

Wegen $\begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} a+b \\ b \end{pmatrix} \mapsto \begin{pmatrix} a+b \\ -a \end{pmatrix} \mapsto \begin{pmatrix} b \\ -a \end{pmatrix} \mapsto \begin{pmatrix} b \\ a \end{pmatrix}$ läßt sich auch das Vertauschen zweier Zeilen mit elementaren Zeilenoperationen erreichen. Jede elementare Zeilenumformung macht aus einer Basis von V eine neue Basis von V, weil die Zeilenumformungen nicht aus V herausführen und umkehrbar sind, also die Basis erhalten.

Das Gaußsche Eliminationsverfahren zeigt, daß man eine $(k \times n)$-Matrix vom Rang k durch elementare Zeilenumformungen in eine Zeilenstufenform

$$\begin{pmatrix} \alpha & \dots & \alpha & 1 & \alpha & \dots & \alpha & 0 & \alpha & \dots & \dots & \alpha & 0 & \alpha & \dots & \alpha \\ \alpha & \dots & \alpha & 0 & \alpha & \dots & \alpha & 1 & \alpha & \dots & \dots & \alpha & 0 & \alpha & \dots & \alpha \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & & \vdots & \vdots & \vdots & & \vdots \\ \alpha & \dots & \alpha & 0 & \alpha & \dots & \alpha & 0 & \alpha & \dots & \dots & \alpha & 1 & \alpha & \dots & \alpha \end{pmatrix}$$

umwandeln kann, wobei die α's beliebige Koeffizienten sind. Man kann sogar von gewissen α's annehmen, daß sie Null sind.

Durch Permutation der Spalten kann man daraus eine systematische erzeugende Matrix machen. Die Permutation von Spalten bedeutet eine Umschreibung der Zeilenvektoren in K^k durch Permutation ihrer Koeffizienten. Der dann erzielte Code heißt *kombinatorisch äquivalent* zum Ausgangscode. Wir haben damit

Satz 5.6. *Jeder Code ist kombinatorisch äquivalent zu einem systematischen Code.*

6. Standardtafeln und Dekodierung

Es bleibt weiterhin die Frage, wie man ein fehlerhaft übertragenes Codewort jedenfalls in Bezug auf die Informationsbits korrigieren kann, also die Frage der allgemeinen Dekodierung $D : K^n \to K^k$. Wegen der Verwendung der Hamming-Metrik ist hier nicht mit einer linearen Abbildung zu rechnen.

Definition 6.1. Sei $V \subseteq K^n$ ein Code. Eine *Neben- oder Restklassen eines Elements* $x \in K^n$ *bezüglich* V ist die Menge

$$\overline{x} = x + V = \{x + v | v \in V\}.$$

Lemma 6.2. *Für die Nebenklassen gilt*

$$\overline{x} \cap \overline{y} = \emptyset \text{ , wenn } \overline{x} \neq \overline{y};$$
$$\bigcup_{xinK^n} \overline{x} = K^n.$$

Beweis. Die zweite Gleichung ist klar, denn $x = x + 0 \in x + V = \overline{x} \subseteq \bigcup_{yinK^n} \overline{y}$. Wenn zum Beweis der ersten Gleichung gilt, $z \in \overline{x} \cap \overline{y}$, dann gibt es $v_1, v_2 \in V$ mit $z = x + v_1 = y + v_2$. Also ist $y = x + v_1 - v_2 \in x + V = \overline{x}$ und daher $y + v = x + v_1 - v_2 + v \in \overline{x}$, also $\overline{y} \subseteq \overline{x}$. Symmetrisch gilt $\overline{x} \subseteq \overline{y}$ und damit $\overline{x} = \overline{y}$. □

Lemma 6.3. *Je zwei Nebenklassen haben gleich viele Elemente*

Beweis. Die Abbildung $\psi : \overline{x} \ni z \mapsto z + (y - x) \in \overline{y}$ ist bijektiv mit der Umkehrung $\overline{y} \ni z \mapsto z + (x - y) \in \overline{x}$. Tatsächlich ist $\psi(z) = \psi(x + v) = x + v + (y - x) = y + v \in \overline{y}$. □

Definition 6.4. Für einen (n, k)-Code $V \subseteq K^n$ schreiben wir die Elements von K^n in eine Tafel. In der ersten Zeile stehen die Elemente von V. An erster Stelle der Tafel steht die $0 \in V$. Aus jeder Nebenklasse $\overline{x} \in K^n/V$ wählen wir ein Element u aus, einen *Repräsentanten*, und schreiben alle diese Repräsentanten R in die erste Spalte. In die übrigen Felder der Tafel schreiben wir die Summen der links und oben über dem Feld stehenden Elemente $u + v$ mit $u \in R$ und $v \in V$. Eine solche Tafel nennen wir *Standardtafel*. Sie besitzt q^n Elemente ausgeteilt in q^k Spalten und q^{n-k} Zeilen.

Beispiel 6.5. Für unser Beispiel ist

(00000)	(10011)	(01010)	(11001)	(00101)	(10110)	(01111)	(11100)
(10000)	(00011)	(11010)	(01001)	(10101)	(00110)	(11111)	(01100)
(01000)	(11011)	(00010)	(10001)	(01101)	(11110)	(00111)	(10100)
(00100)	(10111)	(01110)	(11101)	(00001)	(10010)	(01011)	(11000)

eine Standardtafel.

Bemerkung 6.6. Zur *Dekodierung* bezüglich des Codes $V \subseteq K^n$ wähle man nun den empfangenen Vektor $y = u + v$ aus der Tafel und dekodiere ihn zu dem in V gelegenen Vektor v. Das ist eine korrekte Dekodierung genau dann, wenn u, der Repräsentant der zugehörigen Nebenklasse, der Fehler bei der Übertragung war.

Man beachte, daß der Hamming-Abstand eines empfangenen Vektors y zu dem am Anfang der Spalte stehenden Vektor $v \in V$ des Codes genau gleich dem Hamming-Gewicht des Differenzvektors $\|u\| = \|y - x\| = d(y, x)$ ist. Daher wählt man als Repräsentanten Vektoren minimalen Hamming-Gewichtes in der entsprechenden Nebenklasse.

Beispiel 6.7. In unserem Beispiel sehen wir, daß genau die Fehler (10000), (01000), (00100) korrigiert werden können.

Die dritte und vierte Zeile des oben gegebenen Beispiels zeigen, daß auch durch die Bedingung minimalen Hamming-Gewichts der Repräsentant noch nicht eindeutig bestimmt ist. Der gegebene Code hat das Hamming-Gewicht 2, kann also auch (global) keine Fehler korrigieren.

Wenn wir jedoch den dualen (5,2)-Code betrachten

$$V^\perp = \{(0\ 0\ 0\ 0\ 0), (1\ 1\ 0\ 1\ 0), (1\ 0\ 1\ 0\ 1), (0\ 1\ 1\ 1\ 1)\}$$

betrachten, dann hat dieser die Kontrollmatrix

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

und damit das Hamming-Gewicht 3, kann also einen Fehler immer (!) korrigieren. Das zeigt auch die zugehörige Standardtafel

(00000)	(11010)	(10101)	(01111)
(00001)	(11011)	(10100)	(01110)
(00010)	(11000)	(10111)	(01101)
(00100)	(11110)	(10001)	(01011)
(01000)	(10010)	(11101)	(00111)
(10000)	(01010)	(00101)	(11111)
(01001)	(10011)	(11100)	(00110)
(01100)	(10110)	(11001)	(00011)

Man kann alle einzeln auftreten Fehler und die Doppelfehler (01001) und (01100) korrigieren.

Bemerkung 6.8. Das Problem bei dieser Dekodierung ist, daß die Tafel eines binären (50,30)-Codes mehr als 10^{15} Einträge hat, in denen man (unsystematisch) nach den empfangenen Wort suchen muß, um es zu dekodieren.

Definition 6.9. Sei $V \subseteq K^n$ ein Code und H eine Kontrollmatrix. Sei $x \in K^n$ ein beliebiger (empfangener) Vektor. Dann heißt

$$s = xH$$

das Syndrom, der Paritäts-Prüfungs-Vektor oder der Kontrollvektor von x.

Lemma 6.10. *$x \in K^n$ ist genau dann ein Codewort, wenn sein Syndrom Null ist.*

Zwei Vektoren x_1 und x_2 sind genau dann in derselben Nebenklasse, wenn ihre Syndrome übereinstimmen.

Insbesondere ist daher das Syndrom einer Nebenklasse eindeutig bestimmt. Weiter haben zwei Nebenklassen dasselbe Syndrom genau dann, wenn sie gleich sind.

Beweis. Dieses ist in wesentlichen der Homomorphiesatz für lineare Abbildungen.

Wir wissen schon $V = \mathrm{Ker}(H)$, also $s = xH = 0$ genau dann, wenn $x \in V$.

x_1 und x_2 sind genau dann in derselben Nebenklasse, wenn $x_1 \in \overline{x_2}$ genau dann, wenn $x_1 = x_2 + v$ für ein $v \in V$ genau dann, wenn $(v =)x_1 - x_2 \in V$ genau dann, wenn $(x_1 - x_2)H = 0$ genau dann, wenn $x_1H = x_2H$ genau dann, wenn die Syndrome von x_1 und x_2 übereinstimmen.

Damit ist klar, daß alle Elemente einer festen Nebenklasse dasselbe Syndrom haben und daß Elemente aus verschiedenen Nebenklassen verschiedene Syndrome haben. Also kann man vom Sydrom einer Nebenklasse sprechen. Die Abbildung, die jeder Nebenklasse ihr Syndrom zuordnet, ist injektiv. □

Bemerkung 6.11. Syndrom-Dekodierung: Das Syndrom eines beliebigen Elements $x \in K^n$ läßt sich leicht ausrechnen, als $s = xH$. Wenn man eine Tafel bildet, in der die ausgewählten Repräsentanten der Nebenklassen (mit minimalem Hamming-Gewicht) neben den Syndromen dieser Repräsentanten stehen, genannt *Syndromtafel*, wenn wir also die Abbildung $\varphi : \{\text{Syndrome}\} \to \{\text{Repräsentanten}\}$ kennen, dann können wir wie folgt dekodieren. Man nehme einen beliebigen (empfangenen) Vektor $x \in K^n$, bilde ihn auf sein Syndrom ab durch xH — dadurch ist die Nebenklasse von x schon bestimmt, bilde den zugehörigen Repräsentanten $u := \varphi(xH)$ und berechne $v := x - u$. Dann hat man einen Vektor $v \in V$ mit der Eigenschaft, daß der Hamming-Abstand $d(x, v) = \|x - v\| = \|u\|$ minimal ist unter den Hamming-Abständen $d(x, v')$ für alle $v' \in V$. Für ein beliebiges $v' \in V$ ist nämlich $(x - v')H = xH - v'H = xH$, d. h. x und $x - v'$ liegen in derselben Nebenklasse und haben damit denselben Repräsentanten u. Damit ist $d(x, v) = \|x - v\| = \|u\| \leq \|x - v'\| = d(x, v')$.

Zur Darstellung von φ : {Syndrome} $\to$ {Repräsentanten} benötigen wir für einen binären (50,30)-Code nur noch 2 Spalten mit je 10^6 Elementen, eine wesentliche Verbesserung gegenüber der Standardtafel mit 10^{15} Einträgen. Darüber hinaus kann man die Syndromeinträge so ordnen, daß sie in lexikographisch aufsteigender Reihenfolge auftreten, wodurch die Suche nach dem entsprechenden Eintrag wesentlich verkürzt wird.

Die Standardtafeln unseres Beispiels für einen Code und seinen dualen Code verringern sich also auf

$$\begin{array}{cc} (00) & (00000) \\ (11) & (10000) \\ (10) & (01000) \\ (01) & (00100) \end{array}$$

bzw.

$$\begin{array}{cc} (000) & (00000) \\ (101) & (00001) \\ (110) & (00010) \\ (001) & (00100) \\ (010) & (01000) \\ (100) & (10000) \\ (111) & (01001) \\ (011) & (01100) \end{array}$$

Die hier diskutierte Methode der Syndromdekodierung ist eine der einfachsten Methoden, die für alle linearen Codes angewendet werden kann. Für große Codes ist jedoch die Sydromtafel immer noch unhandlich groß. Speziellere Codes gestatten elegantere Fehlerkorrektur und Dekodierung.

7. Hamming-Codes

Definition 7.1. Hamming-Codes Sei $m \in \mathbb{N}$ eine natürliche Zahl. Wir bilden eine Matrix mit $2^m - 1$ Zeilen und m Spalten. Die Zeilen mögen aus allen m-Tupeln aus $K = \mathbb{F}_2$ außer der Null bestehen, also aus allen Elementen aus $\mathbb{F}_2^m \setminus \{0\}$. Man beachte, daß jeder Vektor bei der Addition zu sich selbst invers ist, daß also die Summe zweier verschiedener Zeilen nicht die Nullzeile ist. Damit sind je zwei verschiedene Vektoren dieser Matrix linear unabhängig.

Wir betrachten diese Matrix als Kontrollmatrix für einen Code $V = \mathrm{Ker}(H)$. Die Codewörter haben die Länge $2^m - 1$, das Hamming-Gewicht dieses Codes ist $\|V\| = 3$ nach (4.3), V hat die Dimension $2^m - 1 - m$ und jedes Codewort hat m Kontrollbits. Damit haben wir einen $(2^m - 1, 2^m - 1 - m)$-Code konstruiert, der 2-fehlererkennend und 1-fehlerkorrigiernd ist. Sei also $n = 2^m - 1$ und $k = 2^m - 1 - m$. Der (n,k)-Code hat nach (6.4) $2^{n-k} = 2^m$ Nebenklassen und damit $2^m - 1$ korrigierbare Fehler, unter ihnen die Einzelfehler. Da die Länge der Codewörter ebenfalls $2^m - 1$ ist, sind die Repräsentanten kleinsten Hamming-Gewichts genau die Einzelfehler für diesen Code. Dieser Code wird (n,k)-*Hamming-Code* genannt.

Es gilt also

Lemma 7.2. *In einem Hamming-Code sind die Repräsentanten der Nebenklassen kleinsten Hamming-Gewichts genau die Einzelfehler für diesen Code.*

Beispiel 7.3. Der in (2.1) beschriebene Code ist der Hamming-Code zu $m = 3$, $n = 2^3 - 1 = 7$ und $k = n - m = 7 - 3 = 4$. Die Kontrollmatrix ist

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

Sie gehört gemäß (5.3) zu einer systematischen erzeugenden Matrix

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

Satz 7.4. Hamming-Dekodierung *Wenn man bei dem Aufbau der Kontrollmatrix H in die i-te Zeile die Binärzahl für i schreibt, dann ergibt das Syndrom xH für einen Vektor $x \in K^n$ den Binärwert für diejenige Stelle, an der der Einzelfehler aufgetreten ist.*

Beweis. Wenn $v \in V$ übertragen wird und der Einzelfehler bei der Übertragung e_i ist, d. h. an der i-ten Stelle ist, wenn also $v + e_i$ empfangen wird, dann ist das Syndrom $s = (v + e_i)H = e_iH = h_i$ die i-te Zeile von H, also die binäre Darstellung der Zahl i und damit der Fehlerstelle. □

Beispiel 7.5. Eine Kontrollmatrix für einen Code ist nicht eindeutig bestimmt. Wenn wir als Kontrollmatrix

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

wählen, dann ist diese wegen $BH = 0$ Kontrollmatrix für dieselbe erzeugende Matrix B und den dadurch erzeugten Code. Diese Kontrollmatrix erlaubt eine Fehlerkorrektur wie im Beispiel (2.1) mit den Vektoren

$$a = (0001111),$$
$$b = (0110011),$$
$$c = (1010101).$$

Satz 7.6. *Man erhält einen 1-fehlerkorrigierenden Code in K^n, indem man ein minimales m mit $n \leq 2^m - 1$ wählt, eine Kontrollmatrix H wie in (7.4) zum $(2^m - 1, 2^m - 1 - m)$-Hamming-Code bildet und aus dieser Matrix lediglich die ersten n Zeilen verwendet. So erhält man einen $(n, n - m)$-Code, der oft ebenfalls* Hamming-Code *genannt wird.*

Beweis. Die neue Kontrollmatrix H_n erfüllt immer noch die Eigenschaft, daß je zwei verschiedene Zeilen linear unabhängig sind. Weiter sind schon die ersten drei Zeilen linear abhängig. Damit hat der Code V das Hamming-Gewicht $\|V\| = 3$.

Wegen der Bedingung $2^{m-1} \leq n$ kommen alle Vektoren $e_1, \ldots, e_m$ in der Matrix H_n vor. Daher gilt $\mathrm{Rang}(H_n) = m =$ Spaltenzahl von H_n. Somit gilt $\dim(V) = \dim(\mathrm{Ker}(H_n)) = n - \mathrm{Rang}(H_n) = n - m$. □

8. Polynomringe und endliche Körper

Lemma 8.1. *Sei* $K[x]$ *der* K*-Vektorraum mit der abzählbar unendlichen Basis* $1 := x^0, x := x^1, x^2, x^3, \ldots, x^n, \ldots$. *Dann ist* $K[x]$ *ein Ring mit der Multiplikation*

$$(\sum_{i=0}^{m} \alpha_i x^i)(\sum_{j=0}^{n} \beta_j x^j) := \sum_{i=0}^{m} \sum_{j=0}^{n} \alpha_i \beta_j x^{i+j} = \sum_{k=0}^{m+n} (\sum_{l=0}^{k} \alpha_l \beta_{k-l}) x^k.$$

Beweis. Jeder Vektor aus $K[x]$ läßt sich daher in eindeutiger Weise (mit eindeutig bestimmten Koeffizienten) als $\sum_{i=0}^n \alpha_i x^i = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ schreiben. Die oben angegebene Multiplikation ist die bekannte Multiplikation von Polynomen.

Die Addition des Vektorraumes $K[x]$ verwenden wir als Addition des Ringes $K[x]$. Es bleibt die Multiplikation zu untersuchen. Die angegebene Multiplikationsregel reduziert sich auf den Basiselementen zu $x^i x^j = x^{i+j}$.

Die Multiplikation von links mit x_i ergibt auf den Basiselementen $x^i x^j = x^{i+j}$ und läßt sich eindeutig zu einer linearen Abbildung $x^i : K[x] \to K[x]$ fortsetzen als $x^i(\sum_{j=0}^n \beta_j x^j) = \sum_{j=0}^n \beta_j x^{i+j}$, also zu der oben definierten Multiplikation.

Die Multiplikation von rechts mit $\sum_{j=0}^n \beta_j x^j$ ergibt auf den Basiselementen $x^i(\sum_{j=0}^n \beta_j x^j) = \sum_{j=0}^n \beta_j x^{i+j}$ und läßt sich eindeutig zu einer linearen Abbildung $(\sum_{j=0}^m \beta_j x^j) : K[x] \to K[x]$ fortsetzen als $(\sum_{i=0}^m \alpha_i x^i)(\sum_{j=0}^n \beta_j x^j) = \sum_{i=0}^m \alpha_i(\sum_{j=0}^n \beta_j x^{i+j}) = \sum_{i=0}^m \sum_{j=0}^n \alpha_i \beta_j x^{i+j}$, also zu der oben definierten Multiplikation. Damit ist die Multiplikation distributiv.

Das Element $1 := x^0$ ist das Einselement der Multiplikation.

Die Assoziativität ergibt sich aus

$$\begin{aligned}
[(\textstyle\sum_{i=0}^m \alpha_i x^i)(\sum_{j=0}^n \beta_j x^j)](\sum_{k=0}^r \gamma_k x^k) &= [\textstyle\sum_{i=0}^m \sum_{j=0}^n \alpha_i \beta_j x^{i+j}](\sum_{k=0}^r \gamma_k x^k) \\
&= \textstyle\sum_{i=0}^m \sum_{j=0}^n \sum_{k=0}^r \alpha_i \beta_j \gamma_k x^{i+j+k} \\
&= (\textstyle\sum_{i=0}^m \alpha_i x^i)[\sum_{j=0}^n \sum_{k=0}^r \beta_j \gamma_k x^{j+k}] \\
&= (\textstyle\sum_{i=0}^m \alpha_i x^i)[(\sum_{j=0}^n \beta_j x^j)(\sum_{k=0}^r \gamma_k x^k)]
\end{aligned}$$

□

Definition 8.2. Sei $f(x) = \sum_{i=0}^n \alpha_i x^i \neq 0$ ein Polynom. Die eindeutig bestimmte größte Zahl n mit $\alpha_n \neq 0$ heißt der *Grad* des Polynoms $f(x)$. α_n heißt der *höchste Koeffizient* des Polynoms.

Man kann durch Betrachtung der höchsten Koeffizienten einsehen, daß $K[x]$ ein nullteilerfreier Ring ist.

Lemma 8.3. *Die Polynome in* $K[x]$ *vom Grade höchstens* n *bilden einen Vektorraum* P_n *der Dimension* $n+1$.

Beweis. Diese Polynome werden von den linear unabhängigen Polynomen $1, x, x^2, x^3, \ldots, x^n$ erzeugt. □

Theorem 8.4. *Im Polynomring* $K[x]$ *gilt der euklidische Divisionsalgorithmus:*

zu jedem Paar $f, g \in K[x]$ *von Polynomen mit* $g \neq 0$ *gibt es ein eindeutig bestimmtes Paar von Polynomen* $q, r \in K[x]$ *(Quotient und Rest), so daß gilt*

$$f = q \cdot g + r \qquad \textit{und} \qquad \mathrm{Grad}(r) < \mathrm{Grad}(g).$$

Beweis. Wir zeigen zunächst die Eindeutigkeit der Zerlegung. Sei $f = qg + r = q'g + r'$ mit $\mathrm{Grad}(r) < \mathrm{Grad}(g)$ und $\mathrm{Grad}(r') < \mathrm{Grad}(g)$. Dann ist $(q - q')g + (r - r') = 0$. Da auch $\mathrm{Grad}(r - r') < \mathrm{Grad}(g)$ gilt, ist $(q - q')g = 0$. Insbesondere muß der höchste Koeffizient von $(q - q')g$ Null sein, was nur geht, wenn $q - q' = 0$ gilt. Dann ist aber auch $r - r' = 0$ und damit die Eindeutigkeit gezeigt.

Wenn der Grad von f kleiner ist, als der Grad von g, dann setzen wir $q = 0$ und $r = f$. Wenn $\mathrm{Grad}(f) = n+1$ ist und der Satz für Polynome vom Grad n schon bewiesen ist, dann sei $\gamma := \alpha_{n+1}/\beta_k$ der Quotient der höchsten Koeffizienten α_{n+1} von f und β_k von g. Dann ist $f' := f - \gamma g$ ein Polynom vom Grad kleiner oder gleich n. Wir können also schreiben $f' = q'g + r$ mit $\mathrm{Grad}(r) < \mathrm{Grad}(g)$. Also ist $f = (\alpha + q')g + r$ mit $\mathrm{Grad}(r) < \mathrm{Grad}(g)$. □

Folgerung 8.5. *Ein Polynom $f(x)$ in $K[x]$ vom Grad n hat höchstens n verschiedene Nullstellen in K.*

Beweis. Seien $\alpha_1, \ldots, \alpha_k$ paarweise verschiedene Nullstellen von $f(x)$, dann ist $f(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_k) \cdot g(x)$, also $k \leq n$. Nach dem Divisionsalgorithmus ist nämlich $f(x) = (x - \alpha_1) \cdot g_1(x) + \beta_1$. Wenn man für x den Wert α_1 einsetzt, dann erhält man $0 = \beta_1$. Für jede weitere Nullstelle α_i von $f(x)$ ist dann aber $0 = f(\alpha_i) = (\alpha_i - \alpha_1)g(\alpha_i)$, also sind die $\alpha_2, \ldots, \alpha_k$ Nullstellen von $g_1(x)$. Durch Induktion nach dem Grad erhält man die behauptete Aussage. □

Definition 8.6. Vor Polynomen in $K[x]$ können wir wie im reellen Fall Ableitungen bilden, hier *formale Ableitungen* genannt. Wir bilden nämlich die eindeutig bestimmte lineare Abbildung $d/dx : K[x] \to K[x]$, indem wir auf der Basis (x^i) vorschreiben $d/dx(x^i) := ix^{i-1}$ (für $i = 0$ soll $d/dx(x^0) = 0$ gelten).

Lemma 8.7. *Für die formale Ableitung von Polynomen gilt die Produktregel.*

Beweis. Es ist $d/dx(x^i x^j) = (i+j)x^{i+j-1} = ix^{i-1}x^j + jx^i x^{j-1} = d/dx(x^i)x^j + x^i d/dx(x^j)$. Daraus leitet sich wegen der Linearität die Produktregel ab:

$$d/dx(fg) = d/dx(f)g + fd/dx(g).$$

□

Definition 8.8. Sei K ein Körper. Die kleinste Zahl $p > 0$, so daß $1 + \ldots + 1 = 0$ mit genau p Summanden in K gilt, heißt die *Charakteristik* von K. Wenn es keine solche Zahl gibt, so wird die Charakteristik als 0 definiert.

Lemma 8.9. *Wenn K eine Charakteristik $p > 0$ hat, dann ist p eine Primzahl.*

Beweis. Sei $p = qr$ mit $q < p$ und $r < p$, $p, q, r \in \mathbb{N}$. Dann ist $(1 + \ldots + 1)_{q \text{ mal}} \cdot (1 + \ldots + 1)_{r \text{ mal}} = (1 + \ldots + 1)_{qr \text{ mal}} = 0$ in K. Daher ist einer der Faktoren Null, z.B. $(1 + \ldots + 1)_{q \text{ mal}} = 0$ in K im Widerspruch zu $q < p$. Es ist somit einer der Faktoren gleich p, der andere ist 1. Daher ist p eine Primzahl. □

Lemma 8.10. *Sei K ein Körper der Charakteristik $p > 0$.*

1. *Für $\alpha, \beta \in K$ gilt $(\alpha + \beta)^p = \alpha^p + \beta^p$.*
2. *Weiter ist $(x - 1)^p = x^p - 1$ in $K[x]$.*

Beweis. Nach der binomischen Formel ist $(\alpha + \beta)^p = \sum_{i=0}^{p} \binom{p}{i} \alpha^i \beta^{p-i} = \alpha^p + \beta^p$, denn $\binom{p}{i} = \frac{p \cdot \ldots \cdot (p-i+1)}{1 \cdot \ldots \cdot i} \equiv 0 \mod p$, weil p als Primzahl in diesem Bruch nicht gekürzt werden kann. Der Beweis für $(x-1)^p = x^p - 1$ verläuft analog mit denselben Binomialkoeffizienten. □

Lemma 8.11. *Sei K ein endlicher Körper. Dann hat K eine positive Charakteristik $p > 0$.*

Beweis. Die Elemente $1, 1+1, 1+1+1, \ldots$ in K sind nicht alle paarweise verschieden, weil K nur endlich viele Elemente hat. Sei also $(1 + \ldots + 1)_{r \text{ mal}} = (1 + \ldots + 1)_{s \text{ mal}}$ mit $r < s$. Dann können r Summanden 1 gekürzt werden, also gilt $(1 + \ldots + 1)_{(s-r) \text{ mal}} = 0$. Es gibt also mindestens eine positive Zahl $s - r$ mit dieser Eigenschaft. Die kleinste solche Zahl ist dann die positive Charakteristik. □

Definition 8.12. Sei $f \in K[x]$ ein Polynom vom $\mathrm{Grad}(f) > 0$. Das Polynom f heißt *irreduzibel*, wenn für jede Zerlegung $f = gh$ von f in ein Produkt von zwei Polynomen g und h eines der beiden Polynome vom Grad 0, d. h. eine Konstante, ist.

Satz 8.13. *Sei K ein Körper und $f \in K[x]$ ein irreduzibles Polynom. Dann ist die Menge der Nebenklassen $K[x]/(f)$ ein Körper.*

Wenn K q Elemente besitzt und f den Grad n hat, dann hat $K[x]/(f)$ die Dimension n und damit q^n Elemente.

Beweis. Mit (f) bezeichnen wir den Unterraum $\{gf \in K[x] | g \in K[x]\}$. Dieser Unterraum ist ein Ideal, d. h. für jedes Element $h \in K[x]$ und jedes Element $gf \in (f)$ ist auch $h(gf) = (hg)f \in (f)$. Ohne Einschränkung der Allgemeinheit können wir annehmen, daß f höchsten Koeffizienten 1 hat, indem wir das ursprüngliche f mit α_n^{-1} multiplizieren, also f durch $\alpha_n^{-1} f$ ersetzen. Dann ist $(f) = (\alpha_n^{-1} f)$.

Die Menge der Nebenklassen $K[x]/(f)$ bildet eine additive Gruppe durch $\overline{g} + \overline{h} := \overline{g + h}$ und sogar einen Ring durch $\overline{g}\,\overline{h} := \overline{gh}$. Die wichtigste Tatsache, die hierfür nachgewiesen werden muß, ist, daß diese Verknüpfungen von der Auswahl der Repräsentanten der Nebenklassen unabhängig sind.

Diesen Beweis und die Überprüfung der Ringeigenschaft überlassen wir dem Hörer (Leser).

Um nun zu sehen, daß $K[x]/(f)$ ein Körper ist, zeigen wir, daß jedes Element $\overline{g} \neq 0$ ein Inverses unter der Multiplikation besitzt. Dazu betrachten wir die Menge $(g, f) = \{p_1 g + p_2 f | p_1, p_2 \in K[x]\}$. Wir führen die Division $g = qf + r$ durch. Dann ist $\overline{g} = \overline{r} \neq 0$ und $\mathrm{Grad}(r) < \mathrm{Grad}(f)$. Also gibt es in (g, f) ein Element $r = 1g - qf \neq 0$ mit $\mathrm{Grad}(r) < \mathrm{Grad}(f)$.

Sei $s \in (g, f)$, $s \neq 0$ von minimalem Grad. Eine Division mit Rest ergibt $f = qs + t$. Da $t = f - qs \in (g, f)$ und $\mathrm{Grad}(t) < \mathrm{Grad}(s)$ und $s \neq 0$ von minimalem Grad, ist $t = 0$ und daher $f = qs$. Nun ist f irreduzibel und $\mathrm{Grad}(s) < \mathrm{Grad}(f)$, also ist $\mathrm{Grad}(s) = 0$ und $s = \alpha \in K \setminus \{0\}$. Da $s \in (g, f)$ und auch $1 = \alpha^{-1} s \in (g, f)$, gibt es Polynome p_1, p_2 mit $1 = p_1 g + p_2 f$, also $\overline{1} = \overline{p_1 g} + \overline{p_2 f} = \overline{p}_1 \overline{g}$. Damit ist $\overline{p}_1$ Inverses zu $\overline{g}$ und $K[x]/(f)$ ein Körper.

Da jede Linearkombination $\sum_{i=0}^{n-1} \alpha_i x^i$ mit von Null verschiedenen Koeffizienten nicht in (f) liegt, denn Vielfache von f haben höheren Grad, ist $\overline{\sum_{i=0}^{n-1} \alpha_i x^i} = \sum_{i=0}^{n-1} \alpha_i \overline{x^i} \neq \overline{0}$ in $K[x]/(f)$, falls nicht alle Koeffizienten Null sind, d. h. die $\overline{1}, \overline{x}, \overline{x^2}, \ldots, \overline{x^{n-1}}$ sind linear unabhängig. Da aber höhere Potenzen x^{n+i} durch f mit Rest teilbar sind: $x^{n+i} = qf + r$ und daher $\overline{x^{n+i}} = \overline{r} = \overline{\sum_{i=0}^{n-1} \alpha_i x^i}$ für geeignete α_i gilt, bilden die $\overline{1}, \overline{x}, \overline{x^2}, \ldots, \overline{x^{n-1}}$ eine Basis für $K[x]/(f)$. Damit ist $\dim(K[x]/(f)) = n = \mathrm{Grad}(f)$. □

Lemma 8.14. *1) Zu jeder Primzahlpotenz $q = p^n$ gibt es (bis auf Isomorphie) genau einen Körper $GK(q)$ mit q Elementen.*

2) Jede endliche Untergruppe von der multiplikativen Gruppe K^* eines Körpers K ist zyklisch.

3) Sei $K \subseteq L$ eine Körpererweiterung, so daß $\dim_K L < \infty$ gilt. Zu jedem Element $\alpha \in L$ gibt es genau ein irreduzibles Polynom $p(x) \in K[x]$ von höchstem Koeffizienten 1 mit $p(\alpha) = 0$, genannt Minimalpolynom *für α.*

Der Leser sollte die Beweise hierfür in guten Algebralehrbüchern nachlesen.

Lemma 8.15. *Sei $n \in \mathbb{N}$. Dann gibt es ein irreduzibles Polynom $p(x) \in \mathbb{F}_2[x]$ vom Grad n mit Nullstelle $\alpha \in GF(2^n)$, so daß die Ordnung von α in $GF(2^n)^*$ genau $2^n - 1$ ist, also $\alpha^{2^n - 1} = 1$ gilt und $2^n - 1$ die kleinste solche natürliche Zahl ist.*

Beweis. Da $GF(2^n)^*$ eine zyklische Gruppe ist, gibt es ein (erzeugendes) Element $\alpha \in GF(2^n)^*$ von der Ordnung $2^n - 1$. Sei $p(x)$ das Minimalpolynom für α. Da $GF(2^n) = \mathbb{F}_2(\alpha)$, ist $GF(2^n) \cong \mathbb{F}_2[x]/(p(x))$ und $\mathrm{Grad}(p(x)) = n$. □

9. Zyklische Codes

Wir haben bisher fast ausschließlich Codes studiert, deren Hamming-Gewichte klein (z.B. 3 oder 4) waren. Sie sind höchstens 1-fehlerkorrigierend. Mit den zyklischen (Polynom-) Codes erhalten wir Codes mit höherem Hamming-Gewicht.

Bemerkung 9.1. Seien k und n mit $k < n$ gegeben, und sei g ein Polynom vom Grad $n-k$. Dann definiert g die folgende lineare Abbildung $g : P_{k-1} \ni f \mapsto gf \in P_{n-1}$. Wir betrachten die entsprechende lineare Abbildung auf den Koordinatensystemen von Koeffizientenvektoren der Polynome $\widehat{g} : K^k \to K^n$. Wenn $g = \sum_{i=0}^{n-k} \gamma_i x^i$ ist, dann ist die darstellende Matrix von g bezüglich der Basen $1, x, x^2, \ldots, x^{k-1}$ bzw. $1, x, x^2, \ldots, x^{n-1}$ gegeben durch

$$M = \begin{pmatrix}
\gamma_0 & 0 & & \ldots & 0 \\
\gamma_1 & \gamma_0 & 0 & \ldots & 0 \\
\vdots & \ddots & \ddots & & \vdots \\
\vdots & & \ddots & \ddots & \vdots \\
\vdots & & & \gamma_1 & \gamma_0 \\
\vdots & & & & \gamma_1 \\
\gamma_{n-k} & & & & \vdots \\
0 & \gamma_{n-k} & & & \vdots \\
\vdots & & \ddots & & \vdots \\
\vdots & & & \ddots & \vdots \\
0 & \ldots & & 0 & \gamma_{n-k}
\end{pmatrix},$$

wie man sofort aus dem Polynomprodukt

$$gf = \sum_{i=0}^{n-k} \gamma_i x^i \sum_{j=0}^{k-1} \beta_j x^j = \sum_{t=0}^{n-1} (\sum_{j=0}^{k-1} \gamma_{t-j}\beta_j) x^t$$

abliest.

Definition 9.2. Ein Code $V = \mathrm{Bi}(\widehat{g})$, der von einem Polynom g in der Form $\widehat{g} : K^k \to K^n$ mit $\mathrm{Grad}(g) \leq n - k$ erzeugt wird, heißt ein *Polynomcode*.

Definition 9.3. Ein Code $V \subseteq K^n$ heißt *zyklisch*, wenn für alle $x = (\xi_1, \ldots, \xi_n) \in V$ gilt $(\xi_n, \xi_1, \ldots, \xi_{n-1}) \in V$. Also ist jede zyklische Vertauschung eines Codewortes wieder ein Codewort.

Theorem 9.4. *Seien k und n mit $k < n$ gegeben. Sei $g \in P_{n-k}$ vom Grad $n - k$ ein Teiler von $x^n - 1 \in K[x]$. Dann ist der durch g erzeugte Polynomcode ein zyklischer Code. g heißt dann ein* Generatorpolynom *für den zyklischen Code.*

Beweis. Sei $gg' = x^n - 1$. Dann ist $x^n = gg' + 1$. Sei $gf = \alpha_0 + \alpha_1 x + \ldots + \alpha_{n-1} x^{n-1}$ Darstellung eines Codewortes $(\alpha_0, \ldots, \alpha_{n-1})$. Wir multiplizieren diese Gleichung mit x und erhalten $xgf = \alpha_0 x + \alpha_1 x^2 + \ldots + \alpha_{n-1} x^n = \alpha_0 x + \alpha_1 x^2 + \ldots + \alpha_{n-1}(gg' + 1) = \alpha_{n-1} + \alpha_0 x + \alpha_1 x^2 + \ldots + \alpha_{n-1} gg'$ und daraus $\alpha_{n-1} + \alpha_0 x + \alpha_1 x^2 + \ldots + \alpha_{n-2} x^{n-1} = xgf - \alpha_{n-1} gg' = g(xf - \alpha_{n-1} g')$. Da $\mathrm{Grad}(xf - \alpha_{n-1} g') \leq n - 1 - \mathrm{Grad}(g) = k - 1$ gilt, ist also auch $(\alpha_{n-1}, \alpha_0, \ldots, \alpha_{n-2})$ ein Codewort und der Polynomcode zyklisch. □

Bemerkung 9.5. Es gilt auch die Umkehrung des Satzes. Sei $V \subseteq K^n$ ein zyklischer Code. Dann gibt es ein Polynom $g \in P_{n-k}$ mit g teilt $x^n - 1$, das diesen zyklischen Code erzeugt. Wir benötigen den Beweis hier nicht.

Theorem 9.6. *Der durch $g_k := (x-1)^{p-k}$ über $K = GF(q)$ generierte zyklische Code hat die Hamming-Norm $p - k + 1$.*

Beweis. Für $k = 1$ ist $\widehat{g_1} : K^1 \to K^p$ gegeben durch $\widehat{g_1}(\alpha) = \alpha \cdot (x-1)^{p-1}$. Nun ist $(x-1)(x-1)^{p-1} = (x-1)^p = x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \ldots + x + 1)$. Da $K[x]$ nullteilerfrei ist, ist $(x-1)^{p-1} = x^{p-1} + x^{p-2} + \ldots + x + 1$. Damit erhalten wir $g_1 \cdot \alpha = \alpha \cdot (x^{p-1} + x^{p-2} + \ldots + x + 1)$, also $\widehat{g_1}(\alpha) = (\alpha, \ldots, \alpha)$. Offenbar hat diese Kodierung nach Definition die Hamming-Norm p.

Für $k = p$ ist $g_p = 1$, also $\widehat{g_p} : K^p \to K^p$ die identische Abbildung mit der Hamming-Norm 1.

Wir zeigen jetzt $\|\widehat{g}_{k+1}\| < \|\widehat{g}_k\|$ für alle $0 \leq k < p$. Sei $(\alpha_0, \ldots, \alpha_{p-1}) \in \mathrm{Bi}(\widehat{g}_k)$ ein Codewort minimaler Norm, also mit einer minimalen Anzahl von Koeffizienten ungleich Null. Weil wir einen zyklischen Code haben, können wir $\alpha_0 \neq 0$ annehmen. Für $f \neq 0$ gilt $\mathrm{Grad}(g_k f) = \mathrm{Grad}(g_k) + \mathrm{Grad}(f) = (p-k) + \mathrm{Grad}(f) \geq p - k$, also ist auch $\alpha_i \neq 0$ für ein $i > 0$. Dann ist das zugehörige Polynom $\alpha_0 + \alpha_1 x + \ldots + \alpha_{p-1} x^{p-1} = g_k f = (x-1)^{p-k} f$. Wir bilden die formale Ableitung und erhalten $\alpha_1 + 2\alpha_2 x + \ldots + (p-1)\alpha_{p-1} x^{p-2} = (g_k f)' = (p-k)(x-1)^{p-k-1} f + (x-1)^{p-k} f' = (x-1)^{p-(k+1)}((p-k)f + (x-1)f')$. Daher ist $(\alpha_1, 2\alpha_2, \ldots, (p-1)\alpha_{p-1}, 0) \in \mathrm{Bi}(\widehat{g}_{k+1})$ ein Element kleinerer Norm. Damit ist $\|\widehat{g}_{k+1}\| < \|\widehat{g}_k\|$ und

$$1 = \|\widehat{g}_p\| < \|\widehat{g}_{p-1}\| < \ldots < \|\widehat{g}_1\| = p,$$

woraus $\|\widehat{g}_k\| = p - k + 1$ folgt. □

10. Beispiel eines BCH-Codes

Lemma 10.1. *$p_1(x) := x^4 + x + 1$ ist irreduzibel mit Nullstelle $\alpha \in GF(2^4)$ mit der Ordnung $2^4 - 1 = 15$.*

Beweis. $p_1(x)$ hat keine Nullstelle in $\mathbb{F}_2$. Weiter ist $x^2 + x + 1$ das einzige irreduzible Polynom vom Grad 2. Es ist $x^4 + x + 1 = (x^2 + x)(x^2 + x + 1) + 1$. Also ist $p_1(x)$ irreduzibel. Für eine Nullstelle $\alpha \in GF(2^4) = \mathbb{F}_2[x]$ gilt sicher $\alpha^{15} = 1$. Aber es gelten $\alpha^3 \neq 1$, weil $1, \alpha, \alpha^2, \alpha^3$ Basis für $GF(2^4)$ bilden, und $\alpha^5 = \alpha\alpha^4 = \alpha(\alpha + 1) = \alpha^2 + \alpha \neq 1$. Daher ist die Ordnung $|\alpha| = 15$. □

Lemma 10.2. *$p_2(x) := x^4 + x^3 + x^2 + x + 1$ ist irreduzibel mit Nullstelle α^3.*

Beweis. $p_2(x)$ hat keine Nullstelle in $\mathbb{F}_2$. Es ist $x^4 + x^3 + x^2 + x + 1 = x^2(x^2 + x + 1) + (x + 1)$. Damit ist $p_2(x)$ irreduzibel. Weiter ist α^3 Nullstelle von $p_2(x)$, denn es gilt $\alpha^{12} + \alpha^9 + \alpha^6 + \alpha^3 + 1 = (\alpha+1)^3 + \alpha(\alpha+1)^2 + \alpha^2(\alpha+1) + \alpha^3 + 1 = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^3 + \alpha + \alpha^3 + \alpha^2 + \alpha^3 + 1 = 0$. □

Lemma 10.3. *$m(x) := p_1(x)p_2(x)$ hat Nullstellen $\alpha, \alpha^2, \alpha^3, \alpha^4$.*

Beweis. Da $p_1(x)^2 = p_1(x)$ gilt, hat $p_1(x)$ Nullstellen $\alpha, \alpha^2, \alpha^4, \alpha^8$. □

Beispiel 10.4. Ein B.C.H.-Code (R.C.Bose, D.K.Ray-Chaudhuri, A.Hocquenghem 1959/60)

Wir konstruieren Kodierung, Dekodierung und Fehlerkorrektur für einen (15,7)-Code mit Hilfe von $\alpha \in GF(16)$.

Betrachte $f : \mathbb{F}_2^7 \ni (\alpha_{14}, \ldots, \alpha_8) \mapsto \alpha_{14} x^{14} + \ldots + \alpha_8 x^8 \in \mathbb{F}_2[x]_{14} = P_{14}$. Das ist eine lineare Abbildung. Sei $a = (\alpha_{14}, \ldots, \alpha_8)$ zunächst fix. Dann kann man das Polynom $f(a) = p(x)$

schreiben als $p(x) = q(x)m(x) + r(x)$. Wir bilden $s(x) := p(x) - r(x)$. Es sei $s(x)$ die Kodierung von a. Sie ist durch a, α und α^3 eindeutig bestimmt, da $p_1(x)$ das Minimalpolynom von α ist, $p_2(x)$ das Minimalpolynom von α^3 ist, dadurch $m(x)$ eindeutig bestimmt ist, und da die Division mit Rest eindeutig bestimmte $q(x)$ und $r(x)$ ergibt.

Beachte, daß $r(x)$ den Grad < 8 hat und daher die Koeffizienten $\alpha_7, \ldots, \alpha_0$ von $s(x)$ bestimmt, während $f(a)$ die Koeffizienten $\alpha_{14}, \ldots, \alpha_8$ von $s(x)$ bestimmt. Weiter hängt $s(x)$ linear von a ab.

Sei nun $t(x) \in \mathbb{F}_2[x]_{14}$ das empfangene gestörte Polynom und $z(x) := t(x) - s(x)$ das Fehlerpolynom. Es gelten

$$\begin{array}{ll} z(\alpha) = t(\alpha), & \text{weil } s(\alpha) = 0, \\ z(\alpha^2) = t(\alpha^2), & \text{weil } s(\alpha^2) = 0, \\ z(\alpha^3) = t(\alpha^3), & \text{weil } s(\alpha^3) = 0, \\ z(\alpha^4) = t(\alpha^4), & \text{weil } s(\alpha^4) = 0. \end{array}$$

Die Werte $t(\alpha^i)$ sind aber bekannt. Wir setzen

$$S = \begin{pmatrix} t(\alpha) & t(\alpha^2) \\ t(\alpha^2) & t(\alpha^3) \end{pmatrix}$$

Dann betrachten wir folgende Fälle:

1. Es tritt kein Fehler auf. Dann ist $z(x) = 0$, also auch $S = 0$.
2. Es tritt ein Fehler auf. Dann ist $z(x) = x^i$. Dann ist $S = \begin{pmatrix} \alpha^i & \alpha^{2i} \\ \alpha^{2i} & \alpha^{3i} \end{pmatrix}$ und es gilt S hat den Rang 1. Dieses ist die Fehlererkennung. Wir kennen $t(\alpha)$ und alle α^i. Es gibt genau ein i mit $t(\alpha) = \alpha^i$. Dazu muß man die Struktur von $GF(16)$ kennen. Dann ist der Fehler an der i-ten Stelle aufgetreten.
3. Es treten zwei Fehler auf. Das ist genau dann der Fall, wenn $z(x) = x^i + x^j$ für $i \neq j$. Dann ist

$$S = \begin{pmatrix} \alpha^i + \alpha^j & \alpha^{2i} + \alpha^{2j} \\ \alpha^{2i} + \alpha^{2j} & \alpha^{3i} + \alpha^{3j} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \alpha^i & \alpha^j \end{pmatrix} \begin{pmatrix} \alpha^i & 0 \\ 0 & \alpha^j \end{pmatrix} \begin{pmatrix} 1 & \alpha^i \\ 1 & \alpha^j \end{pmatrix}$$

Diese Matrix hat den Rang 2. Damit ist eine 2-Fehlererkennung gegeben.

Zur Fehlerkorrektur beachte, daß für $k = 1, 2, 3, 4$ bekannt sind $t(\alpha^k) = z(\alpha^k)$. Daraus sind i und j zu bestimmen. i, j sind bekannt, wenn von dem Polynom $(x - \alpha^i)(x - \alpha^j) = x^2 + \tau_1 x + \tau_2$ die Koeffizienten $\tau_1 = \alpha^i + \alpha^j$ und $\tau_2 = \alpha^i \alpha^j$ bekannt sind. Denn dann kennt man die Nullstellen und damit die Exponenten.

Wir bestimmen die τ_i aus $t(x)$ wie folgt. Wir kennen den Wert $\tau_1 = \alpha^i + \alpha^j = t(\alpha)$ aus der Matrix S. Weil α^i und α^j Nullstellen des Polynoms sind, gilt

$$\begin{array}{l} \alpha^{2i} + \tau_1 \alpha^i + \tau_2 = 0, \\ \alpha^{2j} + \tau_1 \alpha^j + \tau_2 = 0. \end{array}$$

Multipliziert man die erste der Gleichungen mit α^i und die zweite der Gleichungen mit α^j und addiert die Gleichungen, so erhält man

$$t(\alpha^3) + \tau_1 t(\alpha^2) + \tau_2 t(\alpha) = (\alpha^{3i} + \alpha^{3j}) + \tau_1(\alpha^{2i} + \alpha^{2j}) + \tau_2(\alpha^i + \alpha^j) = 0,$$

wobei die α-Koeffizienten bekannt sind. Diese Gleichung kann man nach τ_2 auflösen und hat damit τ_1, τ_2 bestimmt. Damit ist der gefundene Code 2-fehlerkorrigierend.

Beispiel 10.5. Über dem Körper $GF(64)$ kann man mit Polynomen vom Grad ≤ 12 folgende weitere B.C.H.-Codes ((63,k)-Codes) bestimmen:

30 Bits Information, 6 Fehler korrigierbar,
24 Bits Information, 7 Fehler korrigierbar,
18 Bits Information, 10 Fehler korrigierbar,
16 Bits Information, 11 Fehler korrigierbar,
10 Bits Information, 13 Fehler korrigierbar,
7 Bits Information, 15 Fehler korrigierbar.