Codes und Codegitter

Katharina Distler

27. April 2015

Inhaltsverzeichnis

1 Codes 4

2 Codegitter 14

Einleitung

Die folgende Seminararbeit behandelt das Konzept von Codes und Codegittern. Da sie bei der Informationsübertragung eine wichtige Rolle spielen, werden insbesondere fehlerkorrigierende Codes betrachtet. Bei jeder Art der Kommunikation kann es passieren, dass es beim Übertragen einer Nachricht zu Störungen kommt. Dies motiviert das Kodieren einer Nachricht mit gewissen Zusatzinformationen, sodass im Prozess der Dekodierung mögliche Übertragungsfehler gefunden und korrigiert werden können. Das Entwerfen solcher fehlerkorrigierender Codes ist das Thema der Codierungstheorie. Das Hauptproblem dabei ist möglichst effiziente Codes zu finden.

Codes stehen im Zusammenhang zu Gittern, da sich geeignete Gitter definieren lassen, sodass sich die Eigenschaften des Codes auf das zugehörige Gitter „übertragen“. Dies hat den Vorteil das sich bestimmte Eigenschaften besser über Gitter nachrechnen lassen als über den Code.

Im ersten Kapitel werden zunächst Codes definiert und ihre wichtigsten Eigenschaften untersucht, durch Beispiele wie den Binäre Wiederholungscode und den besonders effizienten Hammingcode werden diese dann veranschaulicht. Im zweiten Kapitel werden dann Codegitter definiert und der Zusammenhang von Codes zu Codegittern untersucht. Abschließend wird aus dem erweiterten Hammingcode das E_8-Gitter konstruiert.

Die Seminararbeit basiert auf den Abschnitten 1.2 und 1.3 des Buchs „Lattices and Codes“ von Wolfgang Ebeling. Dieses Buch beinhaltet Mitschriften der von Friedrich Hirzebruch gehaltenen Vorlesung im Jahr 1988/89.

1 Codes

Dieses Kapitel gibt eine kurze Einführung in die Codierungstheorie. Es werden Codes definiert und ihre wichtigsten Eigenschaften untersucht. Anhand von Beispielen wie dem Binären Wiederholungscode und dem Hammingcode wird das Hauptproblem der Codierungstheorie deutlich: Effizienz.

Mathematisch ist eine Nachricht eine endliche Sequenz von Symbolen eines Alphabets, wofür man einen endlichen Körper $\mathbb{F}_q$ mit $q = p^r$ (p Primzahl) Elementen verwendet. Aus naheliegenden Gründen wählt man in der Kommunikation- und Computertechnologie meistens den Körper $\mathbb{F}_2$ mit den Elementen Null und Eins. Jedes dieser Elemente nennt man ein "Bit".

Kodieren kann als injektive Abbildung $f : \mathbb{F}_q^k \to \mathbb{F}_q^n$ mit $n > k > 0$ gesehen werden. Das Bild dieser Abbildung f, $f(\mathbb{F}_q^k) =: C \subset \mathbb{F}_q^n$ heißt ein Code der Länge n.

Definition 1.1 *Ein* ***Code*** C *der Länge* n *ist eine nichtleere echte Teilmenge des* $\mathbb{F}_q^n$. *Die Elemente von* C *heißen* ***Codewörter*** *und* n *die* ***Wortlänge*** *von* C.

Bemerkung 1.2 *Sei* C *ein Code.*
C *heißt trivial, wenn* $|C| = 1$. *Falls* $q = 2$, *bzw.* $q = 3$, *heißt* C *Binärcode, bzw. Trinärcode.*

Beispiel 1.3

$$\begin{array}{c} \textit{Nachricht} \\ \longrightarrow \\ a \in \mathbb{F}_q^k \end{array} \quad \boxed{\textit{Kodierer}} \quad \begin{array}{c} \longrightarrow \\ f(a) \in C \end{array} \quad \boxed{\textit{Kanal}} \quad \begin{array}{c} \longrightarrow \\ b \end{array} \quad \boxed{\textit{Dekodierer}} \quad \begin{array}{c} \textit{dekodierte Nachricht} \\ \longrightarrow \\ g(b) \in C \end{array}$$

Als erstes wird die Nachricht kodiert. Sie verlässt den Kodierer als Codewort $f(a)$ *des Codes* C *und wird über den Kanal zum Dekodierer geschickt. Hierbei kann es zu Störungen*

kommen, was die Nachricht verfälschen würde. Um solche Fehler zu finden, verwendet man einen Code mit möglichst verschiedenen Codewörtern. Der Dekodierer vergleicht dann das erhaltene Wort mit den einzelnen Codewörtern und wählt hiervon das Ähnlichste aus.

Beispiel 1.4 ***Binärer Wiederholungscode der Länge 3***

Sei $q = 2$, $k = 1$, $n = 3$ *und* $C = \{(0,0,0), (1,1,1)\} \subset \mathbb{F}_2^3$.
Die zu übertragenden Information sind: „Ja“ $(= (1,1,1))$ *oder „Nein“* $(= (0,0,0))$.

Falls der Dekodierer $(0,1,0)$ *empfängt, wird angenommen, dass „Nein“ übertragen wurde, da* $(0,1,0)$ *sich nur an einer Stelle von* $(0,0,0)$ *unterscheidet, von* $(1,1,1)$ *allerdings an zwei. Daher wird die Ausgabe des Dekodierers „Nein“ sein.*

Dieser Code kann also einen Fehler korrigieren, d.h. wenn es einen Übertragungsfehler an höchstens einer Stelle gibt, wird dieser gefunden und korrigiert.

Definition 1.5 *Sei* $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$.

1. *Das* ***Gewicht*** *von* x *ist*

$$w(x) := |\{x_i \mid x_i \neq 0, i \in \underline{n}\}|,$$

   also die Anzahl der von Null verschiedenen x_i.

2. *Für* $x, y \in \mathbb{F}_q^n$, *ist der (Hamming-)****Abstand*** $d(x,y)$ *von* x *und* y *definiert durch*

$$d(x,y) := w(x-y).$$

3. *Für einen nichttrivialen Code* C *heißt*

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

   der ***minimale Abstand*** *des Codes* C.

4. *Ein Code der Wortlänge* n *mit* M *Codewörtern und minimalem Abstand* d *heißt* (n, M, d)*-Code.*

Beispiel 1.6 *Der Wiederholungscode der Länge 3 ist ein* $(3, 2, 3)$*-Code.*

Ein Code mit minimalem Abstand d kann exakt t Fehler korrigieren, wobei t durch

$$d = \begin{cases} 2t+1 & d \text{ ungerade} \\ 2(t+1) & d \text{ gerade} \end{cases}$$

definiert ist.

Um eine korrekte Informationsübertragung sicherzustellen, interessiert man sich besonders für Codes mit möglichst großem minimalen Abstand d.

Beispiel 1.7 *Der minimale Abstand des Wiederholungscodes beträgt 3.*
Ein Nachteil des Codes ist allerdings, dass er für die Übertragung einer 1-bit Information drei Bits benötigt. Somit ist er „verschwenderisch".

Hier erkennt man das grundlegende Problem der Codierungstheorie:
Um einen möglichst großen minimalen Abstand zu erreichen, benötigt man ein großes Alphabet oder lange Codewörter. Beides führt allerdings zu unnötig hohem Rechenaufwand, welcher unerwünscht ist.
Aus diesem Grund führt man neben dem minimalen Abstand eine weitere Größe ein.

Definition 1.8 *Die* ***Informationsrate*** R *eines Codes* C *in* $\mathbb{F}_q^n$ *ist definiert durch*

$$R := \frac{\log_q |C|}{\log_q |\mathbb{F}_q^n|}.$$

Hierbei steht $|C|$ *bzw.* $|\mathbb{F}_q^n|$ *für die Anzahl der Codewörter bzw. aller möglichen Wörter.*

Folgerung 1.9 *Falls* C *ein Binärcode ist, kann die Zahl* $\log_2 |C|$ *als die minimale Anzahl an Bedingungen interpretiert werden, welche benötigt werden, um jedes Codewort eindeutig zu identifizieren.*

Beispiel 1.10 *Der Wiederholungscode der Länge 3 hat die Informationsrate* $R = \frac{1}{3}$.

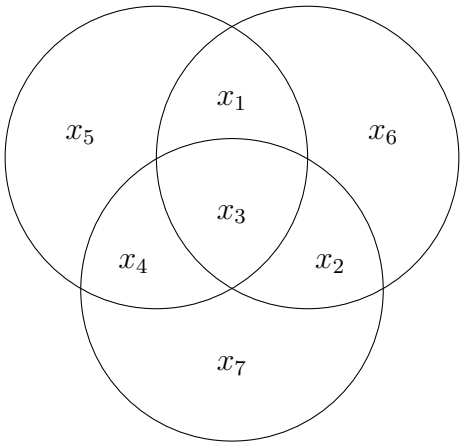
Jetzt kann man ein Hauptproblem der klassischen Codierungstheorie formulieren:
Finde Codes, die sowohl einen möglichst großen minimalen Abstand, als auch eine möglichst große Infomationsrate besitzen.

Beispiel 1.11 ***Der Hammingcode***

Der vermutlich erste effizientere fehlerkorrigierende Code ist der Hammingcode. Er ist ein Binärcode der Länge 7, der durch die Abbildung

$$\begin{array}{ccc} \mathbb{F}_2^4 & \to & \mathbb{F}_2^7 \\ (x_1, x_2, x_3, x_4) & \mapsto & (x_1, x_2, x_3, x_4, x_5, x_6, x_7) \end{array}$$

definiert ist, wobei x_5, x_6 und x_7 so bestimmt werden, dass die Summe von je vier Elementen eines Kreises Null ergibt.



Hier kann man drei linear unabhängige Gleichungen in $\mathbb{F}_2^7$ ablesen:

$$\begin{aligned} x_1 + x_3 + x_4 + x_5 &= 0 \\ x_1 + x_2 + x_3 + x_6 &= 0 \\ x_2 + x_3 + x_4 + x_7 &= 0 \end{aligned}$$

Die Lösungsmenge des Systems heißt H und ist ein 4-dimensionaler Untervektorraum des $\mathbb{F}_2^7$.

Definition 1.12 *Ein **linearer Code** C ist ein Untervektorraum des $\mathbb{F}_q^n$. Wenn C Dimension k und minimalen Abstand d hat, nennt man C auch einen $[n,k,d]_q$-Code.*

Bemerkung 1.13 *Da bei einem linearen Code für $x, y \in C$ auch $x - y \in C$ gilt, ist der minimale Abstand gleich dem Minimum der Gewichte der Codewörter ungleich 0.*

Definition 1.14 *Eine Sequenz*

$$\mathcal{V}_0 \xrightarrow{f_1} \mathcal{V}_1 \xrightarrow{f_2} \mathcal{V}_2 \xrightarrow{f_3} \ldots \xrightarrow{f_n} \mathcal{V}_n$$

*von K-Vektorräumen $\mathcal{V}_i$ und Vektorraumhomomorphismen f_i heißt **exakt**, falls* $\mathrm{Bild}(f_i) = \mathrm{Kern}(f_{i+1})$, $i = 1, \ldots, n-1$.

Betrachte die Vektoren des $\mathbb{F}_q^n$ als Spaltenvektoren. Dann ist ein linearer Code definiert durch eine exakte Sequenz

$$0 \to \mathbb{F}_q^k \xrightarrow{A} \mathbb{F}_q^n \xrightarrow{B} \mathbb{F}_q^{n-k} \to 0,$$

wobei A und B lineare Abbildungen sind. Die Exaktheit der Sequenz ist äquivalent zu den drei Bedingungen $\mathrm{Rang}(A) = k$, $BA = 0$ und $\mathrm{Rang}(B) = n - k$. Um nun den Code C, der über diese exakte Sequenz definiert ist, zu erhalten, gibt es 2 Möglichkeiten:

1. $C = A(\mathbb{F}_q^k) \subset \mathbb{F}_q^n$.
   Die lineare Abbildung A ist durch eine $(n \times k)$-Matrix A gegeben, deren Spalten eine Basis von C bilden. Gewöhnlich betrachtet man allerdings die transponierte Matrix $G = A^{\mathrm{tr}}$, auch **Erzeugermatrix** genannt. Die Zeilen dieser $(n \times k)$-Matrix bilden eine Basis für C.

2. $C = \mathrm{Kern}(B)$, d.h. es gilt $x \in C$ genau dann, wenn $Bx = 0$ ist.
   Die lineare Abbildung B ist durch eine $((n-k) \times n)$-Matrix B gegeben. Die Zeilen dieser Matrix B geben die Relationen an, die C definieren. Die Matrix B heißt auch **Prüfmatrix** oder **Parity-Check-Matrix**. Für jedes $x \in \mathbb{F}_q^n$ nennt man $Bx \in \mathbb{F}_q^{n-k}$ das **Syndrom** von x. Die Codewörter von C sind über das Syndrom $0 \in \mathbb{F}_q^{n-k}$ charakterisiert.

Beispiel 1.15 *In Beispiel* 1.11 *wurde der Hammingcode über*

$$H = \mathrm{Kern} \underbrace{\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}}_{=: B \in F_2^{3\times 7}}.$$

definiert. Die zugehörige Erzeugermatrix ist

$$G := A^{\mathrm{tr}} := \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \in \mathbb{F}_2^{4\times 7}.$$

Angenommen, das Wort $(1,1,0,0)$ *soll versendet werden. Codieren ergibt*

$$(1,1,0,0)\cdot G = (1,1,0,0,1,0,1)$$

Beim Senden treten nun Störungen auf, und der Empfänger erhält

$$x := (1,1,0,1,1,0,1).$$

Dann ist das Syndrom $Bx^{\mathrm{tr}} = (1,0,1)^{\mathrm{tr}}$*, also gilt* $x \notin C$*. Daraus folgt, dass*

$$x = c + e$$

für ein $c \in C$ *und einen Fehlervektor* $0 \neq e \in \mathbb{F}_2^7$ *ist. Es ist*

$$Bx^{\mathrm{tr}} = Bc^{\mathrm{tr}} + Be^{\mathrm{tr}} = Be^{\mathrm{tr}},$$

gesucht ist also ein $e \in \mathbb{F}_q^7$ *mit minimalem Gewicht und* $Be^{\mathrm{tr}} = (1,0,1)^{\mathrm{tr}}$*. Dieses* e *ist eindeutig und durch*

$$e = (0,0,0,1,0,0,0)$$

gegeben. Also ist das gesuchte Wort

$$x - e = (1,1,0,0,1,0,1).$$

Sei C nun ein linearer Code, der durch eine exakte Sequenz definiert ist. Aus der Linearen Algebra weiß man, dass eine lineare Abbildung $\phi : \mathcal{V} \to \mathcal{W}$, zwischen zwei Vektorräumen $\mathcal{V}$ und $\mathcal{W}$, eine duale Abbildung $\phi^* : \mathcal{W}^* \to \mathcal{V}^*$ induziert. Falls $\mathcal{V}$ und $\mathcal{W}$ endlich erzeugt sind, kann man sie nach Wahl der Basen mit ihren korrespondierenden Dualräumen $\mathcal{V}^*$ und $\mathcal{W}^*$ identifizieren.
Deshalb induziert die Sequenz von oben eine duale Sequenz:

$$0 \to \mathbb{F}_q^{n-k} \xrightarrow{B^{\mathrm{tr}}} \mathbb{F}_q^n \xrightarrow{A^{\mathrm{tr}}} \mathbb{F}_q^k \to 0.$$

Definition 1.16 *Der **duale Code** $C^\perp$ wird durch diese exakte Sequenz definiert, d.h.*

$$C^\perp := B^{\mathrm{tr}}(\mathbb{F}_q^{n-k}).$$

Wenn C k-dimensional ist, ist $C^\perp$ $(n-k)$-dimensional.

Sei Φ eine symmetrische Bilinearform definiert durch

$$\Phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q,\ (x,y) \mapsto \sum_{i=1}^{n} x_i y_i.$$

Lemma 1.17 *Sei C ein linearer Code. Dann gilt*

$$C^\perp = \{y \in \mathbb{F}_q^n \mid \Phi(x,y) = 0 \text{ für alle } x \in C\}.$$

Beweis Nach Definition ist $y \in C^\perp$ genau dann, wenn $A^{\mathrm{tr}}y = 0$ ist. Dies ist aber äquivalent zu $\Phi(A^{\mathrm{tr}}y, z) = 0$ für alle $z \in \mathbb{F}_q^k$. Es gilt:

$$\Phi(A^{\mathrm{tr}}y, z) = (A^{\mathrm{tr}}y)^{\mathrm{tr}}z = y^{\mathrm{tr}}Az = \Phi(y, Az)$$

für alle $z \in \mathbb{F}_q^k$. Daraus folgt nun, dass x genau dann ein Element von $C^\perp$ ist, wenn $\Phi(x,y) = 0$ für alle $y \in C = A(\mathbb{F}_q^k)$ gilt. □

Definition 1.18 *Ein linearer Code C heißt **selbstdual**, wenn $C = C^\perp$ ist.*

Bemerkung 1.19 *Sei C ein linearer Code und $n := \dim(C) + \dim(C^\perp)$. C ist genau dann selbstdual, wenn $\dim(C) = \frac{n}{2}$ und $C \subset C^\perp$ ist.*

Bemerkung 1.20 *Es gilt $C \subset C^\perp$ genau dann, wenn $\Phi(x,y) = 0$ für alle $x, y \in C$.*

Definition 1.21 *Ein Binärcode C heißt **doppelt gerade**, wenn das Gewicht $w(x)$ aller Codewörter $x \in C$ durch 4 teilbar ist.*

Folgerung 1.22 *Ein doppelt gerader linearer Code erfüllt $C \subset C^\perp$.*

Beweis Seien $x, y \in C$. Es gilt $\Phi(x,x) \equiv w(x) \pmod 2$ und

$$w(x+y) = w(x) + w(y) - 2|\{i \mid x_i = y_i = 1\}| \equiv 0 \pmod 4.$$

Daraus folgt, dass alle Summanden w in $4\,\mathbb{Z}$ liegen, woraus $\Phi(x,y) = 0$ folgt. □

Satz 1.23 *Die Symmetrische Gruppe S_n operiert auf $\mathbb{F}_q^n$ durch Permutation der Einträge.*

$$\begin{array}{ccc} S_n \times \mathbb{F}_q^n & \to & \mathbb{F}_q^n \\ (\sigma, (a_1, \ldots, a_n)) & \mapsto & (a_{\sigma^{-1}(1)}, \ldots, a_{\sigma^{-1}(n)}) \end{array}$$

Definition 1.24

1. *Zwei Codes C und C' über $\mathbb{F}_q^n$ heißen **äquivalent**, wenn beide Wortlänge n haben und ein $\sigma \in S_n$ existiert mit $\sigma(C) = C'$.*

2. *Die Automorphismengruppe $\mathrm{Aut}(C)$ eines Codes C ist definiert durch*

$$\mathrm{Aut}(C) := \{\sigma \in S_n \mid \sigma(C) = C\}.$$

Definition 1.25 *Eine (endliche) Menge M mit einer Teilmenge $G \subseteq \mathrm{Pot}(M)$ heißt **projektive Ebene**, falls gilt:*

1. *Zu je zwei verschiedenen Elementen aus M gibt es genau eine Menge aus G, die beide Elemente enthält.*

2. *Je zwei Mengen aus G haben einen einelementigen Durchschnitt.*

3. *Es gibt vier Elemente in M, von denen je drei nicht in einer Menge aus G liegen.*

Die Elemente aus M heißen Punkte, die Menge aus G heißen Geraden.

Satz 1.26 *Zu jeder endlichen projektiven Ebene (M, G) gibt es eine natürliche Zahl $n \in \mathbb{Z}_{\geq 2}$, genannt die **Ordnung** der projektiven Ebene, so dass gilt:*

1. *Jede Gerade hat $n + 1$ Punkte.*

2. *Durch jeden Punkt gehen genau $n + 1$ Geraden.*

3. *Es gibt insgesamt $n^2 + n + 1$ Punkte.*

4. *Es gibt insgesamt $n^2 + n + 1$ Geraden.*

Beispiel 1.27 ***Hammingcode*** **H**

Der Hammingcode besitzt $2^4 = 16$ *Codewörter:*

0000000	*1000110*
0001101	*1001011*
0010111	*1010001*
0011010	*1011100*
0100011	*1100101*
0101110	*1101000*
0110100	*1110010*
0111001	*1111111*

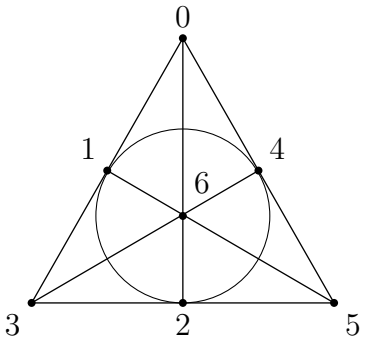
Man sieht, dass das minimale Gewicht 3 ist. H ist also ein $[7, 4, 3]_2$*-Code.*
Es gibt ein Wort des Gewichts 0, sieben Wörter des Gewichts 3, sieben des Gewichts 4 und eins des Gewichts 7. Die Informationsrate R beträgt $\frac{4}{7}$*.*

Wenn man den Wiederholungscode mit dem selben minimalen Abstand wie den Hammingcode für eine 4-bit-Übertragung nutzen würde, müsste man jedes 4-bit-Wort dreimal wiederholen. Die Informationsrate dieses Codes beträgt $\frac{4}{12}$*. Somit ist die Informationsrate des Hammingcodes* $\frac{12}{7} \approx 1.71$*-mal so groß. In der gleichen Zeit überträgt der Hammingcode also* 71% *mehr Informationen als der Wiederholungscode.*

Als eine Menge von Erzeugern von H kann man die sieben Codewörter des Gewichts 3 nehmen. Diese entsprechen sieben 3-elementigen Teilmengen einer 7-elementigen Menge mit der Eigenschaft, dass zwei Teilmengen immer genau ein gemeinsames Element haben. Sie entsprechen den Geraden einer projektiven Ebene der Ordnung 2:

$$\mathbb{P}_2(\mathbb{F}_2) = \mathbb{F}_2^2 \cup \mathbb{F}_2 \cup \{\infty\}$$

Die sieben Punkte und sieben Geraden dieser Ebene bilden die ***Fano-Ebene*** *mit der Inzidenzmatrix:*



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

Eine (4×7)-Teilmatrix der Inzidenzmatrix ist eine Erzeugermatrix von H.

Die Automorphismengruppe des Hammingcodes ist die Automorphismengruppe der projektiven Ebene $\mathbb{P}_2(\mathbb{F}_2)$ und ist isomorph zu der Gruppe $\mathrm{GL}_3(\mathbb{F}_2)$. Diese ist eine einfache Gruppe der Ordnung 168.

Der Hammingcode ist nicht selbstdual, kann aber zu einem selbstdualen Code der Länge 8 erweitert werden.

Definition 1.28 *Sei $C \subset \mathbb{F}_2^n$ ein Binärcode der Länge n. Man betrachte die Abbildung*

$$\begin{array}{rccc} I: & \mathbb{F}_2^n & \to & \mathbb{F}_2^{n+1} \\ & (x_1, \ldots, x_n) & \mapsto & (x_1, \ldots, x_n, x_1 + \cdots + x_n). \end{array}$$

*Der Code $\tilde{C} := I(C)$ heißt der **erweiterte Code** von C.*

Bemerkung 1.29 *Durch die Erweiterung des Codes C zu $\tilde{C}$ bekommt man einen weiteren Parity-Check des Codes C.*

Beispiel 1.30 *Der erweiterte Code $\tilde{H} = I(H)$ des Hammingcodes heißt der **erweiterte Hammingcode**. Er ist ein $[8, 4, 4]_2$-Code mit einem Codewort des Gewichts 0, 14 des Gewichts 4 und einem des Gewichts 8.*

Der erweiterte Hammingcode ist somit nach Bemerkung 1.19 selbstdual und doppelt gerade.

2 Codegitter

In diesem Abschnitt werden Codegitter definiert und der Zusammenhang zwischen einem Code und seinem zugehörigen Gitter untersucht. Mit Hilfe des erweiterten Hammingcodes wird abschließend dann ein gerades, unimodulares, 8-dimensionales Gitter konstruiert: Das E_8-Gitter.

Aus linearen Binärcodes will man nun Gitter konstruieren. Dazu wird das Standardgitter $\mathbb{Z}^n \subset \mathbb{R}^n$ und der Gruppenhomomorphismus

$$\begin{array}{rccc} \rho: & \mathbb{Z}^n & \to & (\mathbb{Z}/2\,\mathbb{Z})^n = \mathbb{F}_2^n \\ & (a_1, \ldots, a_n) & \mapsto & (a_1 \bmod 2, \ldots, a_n \bmod 2) \end{array}$$

betrachtet.

Bemerkung 2.1 *Sei C ein $[n,k,d]_2$-Code. Da $\mathbb{F}_2^n/C$ isomorph zu $\mathbb{F}_2^{n-k}$ ist, ist C eine Untergruppe des Index*

$$|\,\mathbb{F}_2^n/C| = 2^{n-k}$$

von $\mathbb{F}_2^n$.

Das Urbild von C, $\rho^{-1}(C)$, ist somit eine Untergruppe des Index 2^{n-k} von $\mathbb{Z}^n$. Insbesondere ist $\rho^{-1}(C)$ ein freier $\mathbb{Z}$-Modul von Rang n und folglich ein Gitter in $\mathbb{R}^n$. Es gilt

$$\det(\rho^{-1}(C)) \;=\; |\,\mathbb{Z}^n/\rho^{-1}(C)|^2 \det(\mathbb{Z}^n) \;=\; 2^{2n-2k}.$$

Definition 2.2 *Sei C ein linearer Binärcode. Dann heißt*

$$\Gamma_C := \frac{1}{\sqrt{2}}\rho^{-1}(C)$$

das zu C gehörige Gitter.

Satz 2.3 *Sei C ein linearer Binärcode und Γ_C das zugehörige Gitter.*

1. *Es gilt $C \subset C^\perp$ genau dann, wenn Γ_C ein ganzes Gitter ist.*

2. *C ist genau dann doppelt gerade, wenn Γ_C ein gerades Gitter ist.*

3. *C ist genau dann selbstdual, wenn Γ_C unimodular ist.*

BEWEIS Seien dazu $x, y \in \Gamma_C$. Dann sind x und y darstellbar als

$$x = \frac{1}{\sqrt{2}}(c + 2z),\ y = \frac{1}{\sqrt{2}}(c' + 2z')$$

für geeignete $c, c' \in \{0,1\}^n$, die Codewörter aus C repräsentieren, und geeignete $z, z' \in \mathbb{Z}^n$. Um die Notation zu vereinfachen, identifiziert man im weiteren Verlauf des Beweises $\mathbb{F}_2^n$ mit der Teilmenge $\{0,1\}^n$ des $\mathbb{Z}^n$ und schreibt $c, c' \in C$. Daraus folgt, dass

$$\Phi(x,x) = \tfrac{1}{2}(\Phi(c,c) + 4\Phi(c,z) + 4\Phi(z,z))$$

und

$$\begin{aligned}\Phi(x,y) &= \tfrac{1}{2}(\Phi(x+y,x+y) - \Phi(x,x) - \Phi(y,y)) \\ &\equiv \tfrac{1}{4}(\Phi(c+c',c+c') - \Phi(c,c) - \Phi(c',c')) \pmod{\mathbb{Z}} \\ &\equiv \tfrac{1}{2}\Phi(c,c') \pmod{\mathbb{Z}}\end{aligned}$$

gilt. Es folgt, dass $\Phi(x,y)$ genau dann ganzzahlig für alle $x, y \in \Gamma_C$ ist, wenn $\Phi(c,c')$ eine gerade ganze Zahl für alle $c, c' \in C$ ist. Deshalb ist Γ_C genau dann ein ganzes Gitter, wenn $C \subset C^\perp$ ist. Es folgt auch, dass $\Phi(x,x) \in 2\,\mathbb{Z}$ ist, genau dann wenn $\Phi(c,c) \in 4\,\mathbb{Z}$ für alle $c \in C$ ist, was bedeutet, dass Γ_C genau dann gerade ist, wenn C doppelt gerade ist.
Aus der Definition von Γ_C folgt, dass

$$\det(\Gamma_C) = (\tfrac{1}{2})^n \det(\rho^{-1}(C)) = 2^{n-2k}$$

gilt. Also ist $\det(\Gamma_C) = 1$ genau dann, wenn $k = \frac{n}{2}$ ist. C ist somit genau dann selbstdual, wenn Γ_C unimodular ist, das heißt das Gitter ist ganzzahlig mit Determinante 1. □

Beispiel 2.4 ***Konstruktion des $\mathbf{E_8}$-Gitters aus dem erweiterten Hammingcode***

Nach Satz 2.3 ist $\Gamma_{\tilde{H}}$ ein gerades unimodulares Gitter im $\mathbb{R}^8$, dessen Basis im Folgenden konstruiert wird.

Dazu betrachtet man als erstes die sieben Zeilen der Inzidenzmatrix der Fano-Ebene, die den Hammingcode erzeugen, und definiert aus diesen die Vektoren

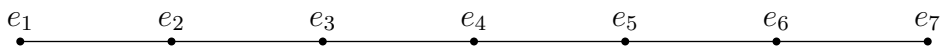
$$f_1 := \frac{1}{\sqrt{2}}(0,1,1,0,1,0,0,1)$$
$$f_2 := \frac{1}{\sqrt{2}}(0,0,1,1,0,1,0,1)$$
$$f_3 := \frac{1}{\sqrt{2}}(0,0,0,1,1,0,1,1)$$
$$f_4 := \frac{1}{\sqrt{2}}(1,0,0,0,1,1,0,1)$$
$$f_5 := \frac{1}{\sqrt{2}}(0,1,0,0,0,1,1,1)$$
$$f_6 := \frac{1}{\sqrt{2}}(1,0,1,0,0,0,1,1)$$
$$f_7 := \frac{1}{\sqrt{2}}(1,1,0,1,0,0,0,1)$$

so, dass $\Phi(f_i, f_i) = 2$ *ist für alle* $i \in \underline{7}$. *Da sich je zwei Geraden der* $\mathbb{P}_2(\mathbb{F}_2)$ *in genau einem Punkt schneiden, gilt auch* $\Phi(f_i, f_j) = 1$ *für alle* $i, j \in \underline{7}$, $i \neq j$. *Setze*

$$e_1 = f_1,\ e_2 = f_2 - f_1,\ e_3 = f_3 - f_2,\ e_4 = f_4 - f_3,$$
$$e_5 = f_5 - f_4,\ e_6 = f_6 - f_5,\ e_7 = f_7 - f_6.$$

Dann ist $\Phi(e_i, e_i) = 2$ *für alle* $i \in \underline{7}$ *und* $\Phi(e_i, e_j) \in \{0, -1\}$ *für alle* $i, j \in \underline{7}$, $i \neq j$.

Um die Matrix $(\Phi(e_i, e_j))_{1 \leq i,j \leq 7}$ *zu beschreiben, assoziiert man einen Graphen mit diesen Elementen wie folgt:*
Jeder Vektor e_i *wird durch einen Knoten repräsentiert. Für* $i \neq j$ *verbindet man diese Knoten genau dann mit einer Kante, wenn* $\Phi(e_i, e_j) = -1$ *ist.*



Dieser Graph heißt ***Coxeter-Dynkin Diagramm****. Die Vektoren* $e_1, \ldots, e_7$ *sind linear unabhängig.*
Man betrachte nun die Gerade durch die Punkte 2, 3 und 5 der Fano-Ebene als die Gerade durch den unendlich fernen Punkt und bildet davon das Komplement. Man ordnet den

Punkten also folgende Gewichte zu:

$$\begin{aligned} 0 &\mapsto -1 \\ 1 &\mapsto -1 \\ 4 &\mapsto 1 \\ 6 &\mapsto -1. \end{aligned}$$

Hieraus bekommt man nun den Vektor

$$e_8 := \frac{1}{\sqrt{2}}(-1,-1,0,0,1,0,-1,0) \in \Gamma_{\tilde{H}},$$

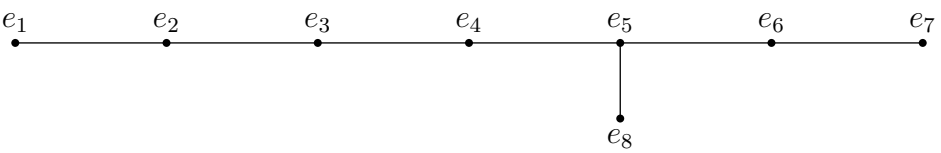
welcher linear unabhängig zu den Vektoren $e_1,\dots,e_7$ ist und $\Phi(e_8,e_8) = 2$ erfüllt. Aus der Konstruktion der Vektoren folgt jetzt, dass

$$\Phi(e_8,f_i) = \begin{cases} 0 & \text{für } i \in \{1,2,3,4\} \\ -1 & \text{für } i \in \{5,6,7\} \end{cases}$$

ist, woraus sich die Matrix

$$(\Phi(e_i,e_j))_{1\le i,j\le 8} = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 2 \end{pmatrix}$$

ergibt. Insbesondere ist die Determinante dieser Matrix gleich 1, woraus nun folgt, dass die Vektoren $e_1,\dots,e_8$ eine Gitterbasis bilden. An dieser Basis kann man das Coxeter-Dynkin Diagramm zu den Vektoren $\{e_1,\dots,e_8\}$ ablesen:



Nach Konstruktion erzeugt also die Basis $E = (e_1,\dots,e_8)$ das Gitter $\Gamma_{\tilde{H}}$, auch **$\mathbf{E_8}$-*Gitter*** *genannt.*

Abschließend betrachtet man noch die Anzahl der kürzesten Vektoren des E_8-Gitters. Da der erweiterte Hammingcode $\tilde{H}$ ein doppelt gerader Code und E_8 somit ein gerades Gitter ist, kann kein Vektor der Länge 1 existieren. Die konstruierten Basisvektoren haben Quadratlänge 2, dies ist somit die Länge der kürzesten Vektoren. Man sucht also die Anzahl der Vektoren $x \in \Gamma_{\tilde{H}}$ für die $\Phi(x,x) = 2$ gilt. Diese ist allerdings gleich der Anzahl der Vektoren $y \in \rho^{-1}(\tilde{H})$ mit $\Phi(y,y) = 4$. Man kann y aber auch als $c + 2z$ mit $c \in \tilde{H}$ und $z \in \mathbb{Z}^n$ schreiben. Dass es für $\Phi(y,y) = 4$ 14 Möglichkeiten gibt, weiß man bereits aus dem Beispiel 1.30. In jedem dieser 14 Codewörter kann man aber einige 1en auch durch -1en ersetzten. Da jedes der 14 c's vier Einsen enthält, ergibt das $4^2 = 16$ Möglichkeiten. Für den Fall, dass c der Nullvektor ist, gilt $\Phi(y,y) = 4\Phi(z,z)$. Es gibt $8 \cdot 2$ $z \in \mathbb{Z}^n$ für die $\Phi(z,z) = 1$ ist.
Insgesamt ergibt das

$$14 \cdot 16 + 8 \cdot 2 = 240$$

kürzeste Vektoren in E_8.

Lemma 2.5 *Es existiert eine Untergruppe von $\mathrm{Aut}(\Gamma_C)$, die isomorph zu dem semidirekten Produkt von $(\mathbb{Z}/2\mathbb{Z})^n$ und $\mathrm{Aut}(C)$ ist.*

Beweis Man zeige zunächst, dass zu $(\mathbb{Z}/2\mathbb{Z})^n$ und $\mathrm{Aut}(C)$ isomorphe Untergruppen von $\mathrm{Aut}(\Gamma_C)$ existieren.

Sei dazu g ein Element aus $\mathrm{Aut}(C)$, d.h. insbesondere aus S_n. Dann induziert g einen $\mathbb{Z}$-Modulautomorphismus $\overline{g}$ auf $\mathbb{Z}^n$ durch Permutation der Einträge:

$$\begin{array}{rccc} \overline{g}: & \mathbb{Z}^n & \to & \mathbb{Z}^n \\ & (x_1, \ldots, x_n) & \mapsto & (x_{g^{-1}(1)}, \ldots, x_{g^{-1}(n)}). \end{array}$$

Es gilt $\overline{g}(\Gamma_C) = \Gamma_C$, da

$$\begin{aligned} \overline{g}(\Gamma_C) &= \overline{g}\left(\frac{1}{\sqrt{2}}\rho^{-1}(C)\right) \\ &= \frac{1}{\sqrt{2}}\overline{g}(\rho^{-1}(C)) \\ &= \frac{1}{\sqrt{2}}\rho^{-1}(g(C)) \\ &= \frac{1}{\sqrt{2}}\rho^{-1}(C) = \Gamma_C \end{aligned}$$

d.h. $\overline{g}$ lässt Γ_C fest. Die Abbildung $\overline{g} : \Gamma_C \to \Gamma_C$ ist bijektiv, wohldefiniert und $\mathbb{Z}$-additiv und es gilt

$$\Phi(\overline{g}(V), \overline{g}(W)) = \Phi(V, W)$$

für alle V und W aus Γ_C. Somit ist $\overline{g}$ ein Gitterautomorphismus von Γ_C. Es folgt insgesamt, dass

$$\begin{array}{rccc} \phi: & \mathrm{Aut}(C) & \to & \mathrm{Aut}(\Gamma_C) \\ & g & \mapsto & \overline{g} \end{array}$$

ein Gruppenmonomorphismus ist. Die Untergruppe Bild(ϕ) von Aut(Γ_C) ist also isomorph zu Aut(C).

Man definiert nun

$$\begin{array}{rccc} \psi: & (\mathbb{Z}/2\mathbb{Z})^n & \to & \mathrm{Aut}(\Gamma_C) \\ & (\overline{a_1}, \ldots, \overline{a_n}) & \mapsto & (\Gamma_C \to \Gamma_C, (v_1, \ldots, v_n) \mapsto (v_1', \ldots, v_n'), v_i' := (-1)^{a_i} v_i), \end{array}$$

wobei ohne Einschränkung $(a_1, \ldots, a_n) \in \{0, 1\}^n$ angenommen wird. Zu zeigen ist, dass diese Abbildung wohldefiniert ist. Sei dazu $\overline{a} = (\overline{a_1}, \ldots, \overline{a_n}) \in (\mathbb{Z}/2\mathbb{Z})^n$ und $(v_1, \ldots, v_n)$ ein beliebiger Gittervektor. Dann gilt

$$\rho(\sqrt{2}v) = \rho(\sqrt{2}\psi(\overline{a})(v_1, \ldots, v_n)),$$

da ein Vorzeichenwechsel mod 2 gerechnet nichts verändert. Also gilt

$$\psi(\overline{a})(v_1, \ldots, v_n) \in \Gamma_C.$$

Außerdem ist $\psi(\overline{a})$ bijektiv, $\mathbb{Z}$-additiv und es gilt

$$\Phi(\psi(\overline{a})(V), \psi(\overline{a})(W)) = \Phi(V, W)$$

für alle Gittervektoren V und W, da sich das Vorzeichen an den jeweils gleichen Stellen ändert. Also ist ψ eine wohldefinierte Abbildung. Insgesamt ist ψ ein Gruppenmonomorphismus und die Untergruppe Bild(ψ) von Aut(Γ_C) ist isomorph zu $(\mathbb{Z}/2\mathbb{Z})^n$.

Seien nun G und H Untergruppen von Aut(Γ_C), wobei G isomorph zu Aut(C) und H isomorph zu $(\mathbb{Z}/2\mathbb{Z})^n$ ist. Zu zeigen ist, dass H von G normalisiert wird. Seien dazu

$g \in G$ und $h \in H$. Dann existiert ein $\sigma \in \mathrm{Aut}(C)$ und ein $(\overline{a_1}, \ldots, \overline{a_n}) \in (\mathbb{Z}/2\,\mathbb{Z})^n$ mit $\phi(\sigma) = g$ und $\psi((\overline{a_1}, \ldots, \overline{a_n})) = h$. Es folgt

$$\begin{aligned} ghg^{-1} &= \phi(\sigma) \circ \psi((\overline{a_1}, \ldots, \overline{a_n})) \circ \phi(\sigma)^{-1} \\ &= \phi(\sigma) \circ \psi((\overline{a_1}, \ldots, \overline{a_n})) \circ \phi(\sigma^{-1}) \\ &= \psi((\overline{a_{\sigma^{-1}(1)}}, \ldots, \overline{a_{\sigma^{-1}(n)}})), \end{aligned}$$

da

$$\begin{aligned} &(\phi(\sigma) \circ \psi((\overline{a_1}, \ldots, \overline{a_n})) \circ \phi(\sigma)^{-1})(v_1, \ldots, v_n) \\ &\quad = (\phi(\sigma) \circ \psi((\overline{a_1}, \ldots, \overline{a_n})))(v_{\sigma(1)}, \ldots, v_{\sigma(n)}) \\ &\quad = \phi(\sigma)((-1)^{a_i} v_{\sigma(1)}, \ldots, (-1)^{a_n} v_{\sigma(n)}) \\ &\quad = ((-1)^{a_{\sigma^{-1}(1)}} v_{\sigma^{-1}(\sigma(1))}, \ldots, ((-1)^{a_{\sigma^{-1}(n)}} v_{\sigma^{-1}(\sigma(n))}) \\ &\quad = \psi((\overline{a_{\sigma^{-1}(1)}}, \ldots, \overline{a_{\sigma^{-1}(n)}}))(v_1, \ldots, v_n) \end{aligned}$$

für alle Gittervektoren $(v_1, \ldots, v_n)$ gilt. Also liegt ghg^{-1} in H. Da G auf H durch innere Automorphismen operiert, folgt die Behauptung. □