# Der Golay-Code und das Leech-Gitter

**Vortrag zum Seminar „Gitter und Codes“**

Nils Malte Pawelzik

12.05.2015

# Inhaltsverzeichnis

# Einleitung

Ziel dieses Vortrags ist es den Golay-Code zu konstruieren und dessen Eindeutigkeit als $(23, 2^{12}, 7)$-Code zu zeigen. Dafür werden wir die Eindeutigkeit eines $(24, 2^{12}, 8)$-Codes zeigen, den erweiterten Golay-Code als ein Beispiel eines solchen Codes konstruieren und dann aus diesem den Golay-Code erhalten, indem eine Koordinatenposition gelöscht wird.
Abschließend werden wir mithilfe des Code-Gitters des erweiterten Golay-Codes das Leech-Gitter als Beispiel eines geraden unimodularen wurzellosen Gitters in $\mathbb{R}^{24}$ konstruieren.

Der Vortrag und diese Ausarbeitung basieren auf dem Kaptiel 2.8 des Buchs *Lattices and Codes* [1].

Zunächst werden wir aber den Begriff eines Designs einführen, da sich mithilfe der Eindeutigkeit eines Design-Typen die Eindeutigkeit eines $(24, 2^{12}, 8)$-Codes folgern lässt.

# 1 Designs

## 1.1 Elementare Eigenschaften eines Designs und die Eindeutigkeit eines $2$-$(11, 5, 2)$-Designs

Beginnen wir also mit der Definition eines Designs.

**Definition 1.1** *Sei $S$ eine Menge mit $v$ Elementen und sei $\mathfrak{B}$ eine nicht-leere Menge von $k$-elementigen Teilmengen (die wir als **Blöcke** bezeichnen) mit der Eigenschaft, dass alle $t$- elementigen Teilmengen von $S$ in genau $\lambda$ Blöcken enthalten sind mit $v \geq k > 0$ und $0 \leq t \leq k$.*
*Dann nennen wir das Tupel ($S$,$\mathfrak{B}$) ein $t$-**Design**, genauer ein $t$-$(v, k, \lambda)$ **Design**. Die Elemente von $S$ werden als **Punkte** des Designs bezeichnet.*

Wir benötigen einige elementare Aussagen aus der Design-Theorie, wobei wir zunächst folgenden Satz zeigen.

**Satz 1.2** *Für ein $t$-$(v, k, \lambda)$ Design und eine Menge $S_j$ von $j$ Punkten, mit $0 \leq j \leq t$, gilt für die Anzahl $\lambda_j$ der Blöcke, die $S_j$ enthalten, folgende Gleichheit:*

$$\lambda_j \binom{k-j}{t-j} = \binom{v-j}{t-j} \lambda.$$

BEWEIS Basierend auf $S_j$ lassen sich auf zwei Arten eine $t$-elementige Menge und ein Block, der Obermenge der Erweiterung ist, erhalten.

1. Als erstes wählt man einen der $\lambda_j$ Blöcke, die $S_j$ enthalten, und wählt aus den $k-j$ noch nicht in $S_j$ enthaltenen Punkten $t-j$ Punkte aus diesem Block aus.

   Damit erhält man also
   $$\lambda_j \binom{k-j}{t-j}$$
   mögliche Wahlen.

2. Anderseits kann man zunächst $t-j$ Punkte aus den $v-j$ Punkten, die noch nicht in $S_j$ enthalten sind, auswählen. Die somit erhaltene $t$-elementige Menge ist nach Definition 1.1 also in $\lambda$ Blöcken enthalten, aus denen man nun einen auswählt.

   Also bieten sich
   $$\binom{v-j}{t-j}\lambda$$
   Möglichkeiten auszuwählen.

Dabei lassen sich die Wahlen jeweils auch auf die entsprechend andere Art erhalten, indem man die Auswahlschritte vertauscht. Also erhält man:

$$\lambda_j \binom{k-j}{t-j} = \binom{v-j}{t-j}\lambda.$$

■

Insbesondere folgt damit, dass $\lambda_j$ unabhängig von der speziellen Wahl von $S_j$ ist. Außerdem ist $\lambda_0$ die Anzahl der Blöcke, da jeder Block die leere Menge enthält, und wird mit $b$ bezeichnet. Ebenso bezeichnet man $\lambda_1$, also die Anzahl der Blöcke, die einen bestimmten Punkt enthalten, mit $r$.

Um Designs kompakt darstellen zu können, definieren wir zwei Begriffe.

**Definition 1.3** *Für ein $t$-$(v,k,\lambda)$ Design lässt sich mit einer Abzählung der Punkte des Designs jedem Block ein* ***charakteristischer Vektor*** *aus $\{0,1\}^{1\times v}$ zuweisen, der angibt welche Punkte der Block enthält.*

*Die charakteristischen Vektoren lassen sich mit einer Abzählung der Blöcke zu einer* ***Inzidenzmatrix*** *des Designs aus $\{0,1\}^{b\times v}$ zusammensetzen, indem man die Zeilenvektoren untereinander anordnet.*

Weitere Möglichkeiten der Inzidenzmatrix wollen wir zunächst in einem Beispiel betrachten.

**Beispiel 1.4** *Sei für ein $t$-$(v,k,\lambda)$ Design eine Inzidenzmatrix $M$ gegeben.*
*Dann lassen sich die Punkte des Designs ihrer Abzählung entsprechend mit den Einheitsvektoren $e_1, \dots e_v \in \{0,1\}^{v\times 1}$ identifizieren. Somit gibt $Me_j \in \{0,1\}^{b\times 1}$ an, welche Blöcke diesen Punkt enthalten, für $1 \leq j \leq v$. Insbesondere liefert $(Me_i)^{tr}(Me_j)$ also die Anzahl der Blöcke, die beide Punkte enthalten, für $0 \leq i,j \leq v$.*

*Entsprechend erhält man für $0 \leq i \leq b$ und den $i$-ten Einheitsvektor $e_i \in \{0,1\}^{b\times 1}$ mit $e_i^{tr}M$ den charakteristischen Vektor des $i$-ten Blocks.*

*Insbesondere ergibt Rechts-Multiplikation mit dem Eins-Vektor die Anzahl der Elemente der Blöcke, da ihre charakteristischen Vektoren die Zeilen von $M$ bilden. Ebenso liefert die Links-Multiplikation der Eins-Zeile die Anzahl der Blöcke, die die jeweiligen Punkte enthalten, da die charakteristischen Vektoren aufsummiert werden.*

Mit diesen Betrachtungen lässt sich der Beweis des nächsten Lemmas kürzer formulieren.

**Lemma 1.5** *In einem 2-$(v,k,\lambda)$-Design mit $b = v$ und $k = r$ haben zwei unterschiedliche Blöcke genau $\lambda$ gemeinsame Punkte.*

Beweis Sei $M$ eine Inzidenzmatrix des Designs. Wie in Beispiel 1.4 gesehen, lässt sich die Bedingung, dass jeweils zwei verschieden Punkte in $\lambda$ Blöcken liegen, bezüglich $M$ umformulieren:
Für $i,j \in \{1,\dots,v\}$ gilt

$$\left(M^{tr}M\right)_{ij} = (Me_i)^{tr}(Me_j) = \begin{cases} r & \text{für } i = j \\ \lambda & \text{für } i \neq j \end{cases},$$

da ein 2-$(v,k,\lambda)$ Design gegeben ist.

Damit folgt mit der Voraussetzung $k = r$ schon

$$M^{tr}M = (k-\lambda)I_v + \lambda J_v$$

mit den $v \times v$ Eins- bzw. Einheitsmatrizen.

Entsprechend erhält man mit den Voraussetzungen $k = r$ und $b = v$, dass

$$J_v M = rJ_v = kJ_v = MJ_v$$

gilt. $M$ kommutiert also mit $J_v$.

Betrachten wir die Vektoren $x_i := e_1 - e_i$, für $i = 2,\dots,v$, so gilt

$$M^{tr}Mx_i = \left((k-\lambda)I_v + \lambda J_v\right) x_i = (k-\lambda)x_i.$$

Nach Voraussetzung gilt $k = r$ und nach Satz 1.2 gilt $r(k-1) = (v-1)\lambda$. Dabei gilt $k \neq v$, da mit der Voraussetzung ansonsten gelten müsste $k = v = b = 1$, was nach Definition der Annahme eines 2-Designs widersprechen würde. Somit gilt $(k - \lambda) \neq 0$. Also hat $M^{tr}M$ insbesondere $v - 1$ linear unabhängige Eigenvektoren zu einem Wert $\neq 0$.
Betrachtet man nun noch den 1-Vektor $\mathbf{1}$, so gilt $M^{tr}M\ \mathbf{1} = ((k + (v-1) \cdot \lambda)\ \mathbf{1}$. Dabei ist $v$ nach Definition eines 2-Designs $\geq 1$, und somit ist auch $\mathbf{1}$ ein Eigenvektor zu einem Wert $\neq 0$. Insgesamt folgt damit die Invertierbarkeit von $M^{tr}M$.

Insbesondere erhält man

$$0 \neq \det(M^{tr}M) = \det(M^{tr})\det(M) = (\det(M))^2$$

mit Ergebnissen der Linearen Algebra. Damit ist also auch $M$ invertierbar. Mit der oben gezeigten Identität gilt also

$$\begin{aligned} M^{tr} &= ((k-\lambda)I_v + \lambda J_v)M^{-1} = (k-\lambda)M^{-1} + \lambda J_v M^{-1} \\ &= M^{-1}(k-\lambda) + M^{-1}M\lambda J_v M^{-1} = M^{-1}(k-\lambda) + M^{-1}\lambda J_v M M^{-1} \\ &= M^{-1}(k-\lambda) + M^{-1}\lambda J_v = M^{-1}((k-\lambda)I_v + \lambda J_v), \end{aligned}$$

da $M$ mit $J_v$ kommutiert. Hiermit folgt, dass $M$ auch mit $M^{tr}$ kommutiert, also

$$MM^{tr} = (k-\lambda)I_v + \lambda J_v.$$

Also gilt analog zu den Betrachtungen über die Aussagen über zwei Punkte unter Verwendung der Einheitszeilen, dass damit folgt, dass zwei unterschiedliche Blöcke jeweils $\lambda$ gemeinsame Punkte haben. ∎

Damit können wir nun die Eindeutigkeitsaussage zeigen, die wir im zweiten Kapitel zum Beweis der Eindeutigkeit eines $(24, 2^{12}, 8)$-Codes verwenden werden.

**Satz 1.6** *Es existiert (bis auf Umbennenung oder Umordnung) genau ein* 2-$(11, 5, 2)$ *Design*

Beweis Anwendung von Satz 1.2 ergibt:

$$b\binom{5-0}{2-0} = \binom{11-0}{2-0}2 \quad bzw. \quad r\binom{5-1}{2-1} = \binom{11-1}{2-1}2.$$

Damit ergeben sich die Werte

$$b = \frac{110}{10} = 11 \quad bzw. \quad r = \frac{20}{4} = 5.$$

Somit sind die Voraussetzungen von Lemma 1.5 gegeben. Also haben zwei unterschiedliche Blöcke eines solchen Designs stets 2 Schnittpunkte.

Wir wollen nun über die Inzidenzmatrix die Existenz und Eindeutigkeit eines solchen Designs zeigen. Ohne Beschränkung der Allgemeinheit können wir davon ausgehen, dass der charakteristische Vektor des ersten Blocks durch $(1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0)$ gegeben ist, da wir ansonsten die Anordnung der Punkte entsprechend permutieren können.
Für die 2-elementigen Teilmengen einer 5-elementigen Menge gibt es $\binom{5}{2} = 10$ Möglichkeiten. Damit korrespondieren die übrigen Blöcke zu den 2-elementigen Teilmengen der ersten 5 Punkte aufgrund der Schnittbedingung. Ebenfalls ohne Einschränkung kann man annehmen, dass deren charakteristische Vektoren in der Inzidenzmatrix lexikographisch angeordnet sind, da man ansonsten die Abzählung der Blöcke entsprechend permutieren kann.

Damit erhalten wir für die Inzidenzmatrix die Form

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

mit $X \in \{0,1\}^{10\times 6}$, sodass die Eigenschaften des Designs erfüllt werden.
Also lässt sich zunächst die erste Zeile von $X$ auf $\begin{pmatrix}1 & 1 & 1 & 0 & 0 & 0\end{pmatrix}$ festlegen, da sich die Punkte ansonsten umordnen lassen und der Block insgesamt noch drei Punkte enthalten muss. Da der erste und zweite Block schon einen gemeinsamen Punkt haben, lässt sich dann die zweite Zeile von $X$ auf $\begin{pmatrix}1 & 0 & 0 & 1 & 1 & 0\end{pmatrix}$ setzen, da man sonst auch hier innerhalb der ersten drei und der letzten drei Punkte umordnen kann.
Fährt man so fort erhält man für die ersten vier Zeilen folgende Belegung:

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

Für die fünfte Zeile ergeben sich dann die Möglichkeiten $\begin{pmatrix}0 & 1 & 0 & 0 & 1 & 1\end{pmatrix}$ und $\begin{pmatrix}0 & 0 & 1 & 1 & 0 & 1\end{pmatrix}$. Danach sind die restlichen Zeilen aber jeweils eindeutig, womit man

insgesamt als mögliche Inzidenzmatrizen

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

und die transponierte Matrix erhält. Man erhält die Transponierte jedoch indem man jeweils die Spalten 4 und 5, 7 und 8, und 9 und 10 und die korrespondierenden Zeilen miteinander vertauscht.
Also erhält man bis auf Umordnung der Punkte bzw. Umordnung der Blöcke nur ein Design, womit der Satz gezeigt ist. ∎

Damit haben wir alle im Weiteren benötigten Aussagen über Designs gezeigt.

# 2 Der Golay Code

Wir beginnen nun mit der Betrachtung von Codes, wobei wir zunächst wieder eine Eindeutigkeitsaussage herleiten wollen.

## 2.1 Die Eindeutigkeit eines $(24, 2^{12}, 8)$-Codes

Bevor wir damit beginnen definieren wir den Begriff eines perfekten Codes. Ein solcher Code liefert eine disjunkte Überdeckung des $\mathbb{F}_2^n$ und wird damit beim Beweis der Eindeutigkeit ein Abzählverfahren ermöglichen.

**Definition 2.1** *Ein Code $C \subset \mathbb{F}_2^n$ mit minimalem Abstand $d = 2e+1$, für $e \in \mathbb{N}_0$, wird* ***perfekter Code*** *genannt, falls eine der folgenden äquivalenten Bedingungen erfüllt ist:*

*(i) Für jedes $x \in \mathbb{F}_2^n$ existiert genau ein Codewort $c$, für das $d(c,x) \leq e$ gilt.*

*(ii)* $|C|(1 + \binom{n}{1} + \cdots + \binom{n}{e}) = 2^n$.

Dabei wollen wir kurz beweisen, dass diese Bedingungen wirklich äquivalent sind. Außerdem wird einsichtig, inwiefern dies eine Überdeckung beschreibt.

BEWEIS Für $c \in C$ sei

$$K_c := \{x \in \mathbb{F}_2^n \,|d(x,c) \leq e\}$$

die Menge der Elemente, die von $c$ mit $\leq e$ Vertauschungen von 0 und 1 erreichbar sind.

Es existieren $\binom{n}{j}$ Möglichkeiten, für $0 \leq j \leq e$, $c$ an $j$ Stellen zu verändern. Somit ergibt sich:

$$|K_c| = \sum_{j=0}^{e} \binom{n}{j}.$$

Gäbe es für $c, c' \in C$ mit $c \neq c'$ ein $x \in (K_c \cap K_{c'})$, so würde für dieses nach Definition $d(x,c) \leq e$ und $d(x,c') \leq e$ gelten, womit auch $d(c,c') \leq 2e$ gelten müsste, was ein Widerspruch wäre. Somit gilt für $c, c' \in C$ mit $c \neq c'$ schon $K_c \cap K_{c'} = \emptyset$.

Mit diesen Betrachtungen folgt also

$$\left| \bigcup_{c \in C} K_c \right| = |C| \left( \sum_{j=0}^{e} \binom{n}{j} \right)$$

Damit ergibt sich der Äquivalenzbeweis wie folgt:
Gilt $|C|(1 + \binom{n}{1} + \cdots + \binom{n}{e}) = 2^n$, dann ist dies äquivalent zu

$$\left| \bigcup_{c \in C} K_c \right| = 2^n = |\,\mathbb{F}_2^n\,|.$$

Nach Definition ist dies wiederum äquivalent zu $\bigcup_{c \in C} K_c = \mathbb{F}_n^2$, was mit der oben gezeigten Disjunktheit wiederum äquivalent zu der Aussage ist, dass für alle $x \in \mathbb{F}_2^n$ genau ein $c \in C$ existiert mit $x \in K_c$, also $d(x,c) \leq e$. ∎

Bevor wir mithilfe der Überdeckungseigenschaft den Beweis der Eindeutigkeits-Aussage führen, wollen wir noch eine praktische Bemerkung über die Gewichte und das Standardskalarprdokut einfügen.

**Bemerkung 2.2** *Sei $n \in \mathbb{N}$. Dann lässt sich das Standardskalarprodukt über $\mathbb{R}$ auf den $\mathbb{F}_2^n$ erweitern mit*

$$\Phi : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{R},\ \Phi(x,y) := \sum_{i=1}^{n} \tilde{x}_i \cdot \tilde{y}_i,$$

*wobei $\tilde{x}$ und $\tilde{y}$ die Identifikationen von $x$ und $y$ in $\{0,1\}^{n\times 1}$ seien.*
*Da $\Phi$ nun unter anderem die gemeinsamen Gewichtsstellen zählt, gilt für $x, y \in \mathbb{F}_2^n$*

$$d(x,y) = w(x) + w(y) - 2\Phi(x,y)$$

*beziehungsweise aufgrund der Identifizierung*

$$x \cdot y = \Phi(x,y) + 2\,\mathbb{Z}\,.$$

Kommen wir nun zum Beweis der Eindeutigkeit eines $(24, 2^{12}, 8)$-Codes.

**Satz 2.3** *Sei $C$ ein binärer $(24, 2^{12}, 8)$-Code, der $0$ enthält. Dann ist $C$ ein doppelt gerader, selbst-dualer, linearer $[24, 12, 8]$-Code und es existiert bis auf Äquivalenz höchstens ein solcher Code.*

Beweis Sei $C$ ein solcher Code. Wir löschen eine beliebige Koordinatenposition, was man als Punktieren bezeichnet. Damit erhalten wir einen $(23, 2^{12}, 7)$-Code $C_0$.
Dabei verringert sich die Länge durch das Löschen der Position und die Anzahl der Codewörter bleibt gleich, da für $C$ nach Voraussetzung $d > 1$ gilt. Dass sich der minimale Abstand bei $C_0$ verringert, lässt sich folgendermaßen sehen:
Wir definieren ähnlich zum Beweis zu (2.1) für $c \in C_0$

$$K_c^j := \{x \in \mathbb{F}_2^{23} \,|d(x,c) \leq j\} \;\text{ für } j \in \mathbb{N}_0\,.$$

Für alle $c, c' \in C_0$ gilt schon $K_c^3 \cap K_{c'}^3 = \emptyset$, weil nur eine Koordinatenposition entfernt wurde und somit $d > 6$ gilt und der Abstand eine Metrik ist. Würde $d = 8$ gelten, könnten die 3-Sphären noch nicht den kompletten $\mathbb{F}_2^{23}$ überdecken. Wie im Beweis zu 2.1 gesehen, würde damit

$$|\,\mathbb{F}_2^{23}\,| > \Big|\bigcup_{c\in C_0} K_c^3\Big| = |C|\left(\sum_{j=0}^{3}\binom{23}{j}\right) = 2^{12}\cdot 2^{11} = 2^{23}$$

folgen, was ein Widerspruch ist.
Also gilt $d = 7$, womit $C_0$ ein $(23, 2^{12}, 7)$-Code und insbesondere perfekt ist , da wie eben gesehen Bedingung (ii) aus Definition 2.1 erfüllt ist.
Somit bilden die 3-Sphären um die Codewörter eine disjunkte Überdeckung des $\mathbb{F}_2^{23}$. Also liegen alle Elemente des $\mathbb{F}_2^{23}$ mit Gewicht $\leq 3$ schon in der Sphäre um $0 \in C_0$. Somit müssen die Elemente mit Gewicht 4 in den Sphären um die Codewörter mit Gewicht 7 liegen. Da man durch Ersetzen dreier Einsen durch 0 aus Codewörtern des Gewichts 7 Elemente mit Gewicht 4 erhalten kann, gilt $A_7 = \binom{23}{4}/\binom{7}{3} = 253$. Nun enthalten die Sphären um diese Wörter jeweils $\binom{7}{2}$ Elemente mit Gewicht 5, somit gilt $A_8 = [\binom{23}{5} - A_7\binom{7}{2}]/\binom{8}{3} = 506$. Von einem Wort mit Gewicht 7 erreicht man Elemente

mit Gewicht 6 durch Löschen einer Eins oder durch hinzufügen einer Eins und Löschen zweier weiterer. Von Wörtern mit Gewicht 8 erreicht man Elemente mit Gewicht 6 durch Löschen zweier Einsen. Also gilt $A_9 = [\binom{23}{6} - A_7\binom{7}{1} - A_7\binom{7}{2}\binom{23-7}{1} - A_8\binom{8}{2}]/\binom{9}{3} = 0$. Iteriert man dieses Inklusions-Exklusions-Prinzip (eine Implementierung des Verfahrens befindet sich im Anhang, siehe 4.1) erhält man folgende Koeffizienten ungleich 0:

$$A_0 = A_{23} = 1 \qquad A_7 = A_{16} = 253$$
$$A_8 = A_{15} = 506 \qquad A_{11} = A_{12} = 1288.$$

Angenommen es existiert ein Wort in $C$, dessen Gewicht $w$ nicht durch 4 teilbar ist. Punktiert man $C$ passend, existiert in $C_0$ also ein Wort mit Gewicht $w$ bzw. $w-1$, wobei dies nicht kongruent zu 0 oder $-1$ mod 4 ist. Dies ist jedoch ein Widerspruch zur eben gezeigten Gewichtsverteilung. Also sind die Gewichte aller Wörter durch 4 teilbar und insbesondere ergibt sich folgende Gewichtsverteilung, aus der des punktierten Codes, für $C$:

$$A_0 = A_{24} = 1 \quad A_8 = A_{16} = 759 \quad A_{12} = 2576.$$

Wählt man einen beliebiges $u \in C_0$ und betrachtet anstatt der Gewichte den Abstand zu diesem Wort, erhält man mit dem gleichen Zählprinzip die eben gesehene Gewichtsverteilung wieder als Abstandsverteilung zu $u$. Aus analoger Betrachtung folgt dann, dass alle Abstände in $C$ durch 4 teilbar sind.

Wie in Bemerkung 2.2 gesehen gilt für $u, v \in C$ schon

$$d(u,v) = w(u) + w(v) - 2\Phi(u,v).$$

Da der Abstand, wie eben gesehen, durch 4 teilbar ist, gilt $u \cdot v = 0 + 2\,\mathbb{Z}$. Damit gilt nach Definition $C \subset C^\perp$.
Dabei ist $C^\perp$ ein Vektorraum und somit gilt $\langle C\rangle \subset C^\perp$. Da $|C| = 2^{12}$, gilt schon $\dim\langle C\rangle \geq 12$, womit (wie im ersten Vortrag gesehen) auch gilt $\dim C^\perp = 24 - \dim\langle C\rangle \leq 12$ und somit $|C^\perp| \leq 2^{12}$.
Insgesamt gilt also $C = C^\perp$, womit $C$ ein doppelt gerader $[24, 12, 8]$-Code ist.

Sei $u \in C$ mit Gewicht 12, dann existiert ein $\overline{u} \in C$ mit Gewicht 12, sodass $u + \overline{u} = \mathbf{1}$, also der Einsvektor, da $C$ linear ist und nach der oben erhaltenen Gewichtsverteilung $\mathbf{1} \in C$ gilt.
Punktiert man $C$ an allen Koordinatenpositionen an denen Gewicht von $u$ liegt, so erhält man einen linearen Code $C_u$. Dann hat $C_u$ Wortlänge 12.
Sei $x \in C$, dann ist $x + u \in C$, da $C$ linear ist. Die Wörter sind nach der Punktierung identisch, und da $x$ beliebig gewählt war, folgt $|C_u| \leq 2^{11}$. Angenommen es existieren $x, x' \in C$ mit $x \neq x'$, die durch die Punktierung identisch werden, mit Differenzvektor $x + x' =: v \neq u$. Dann muss das Gewicht von $v$ auf den gelöschten Koordinaten liegen und $w(v) \geq 8$ gelten, da $d = 8$ für $C$ gilt. Damit gilt aber auch $0 < d(v,w) \leq 4$, was ein

Widerspruch zum Minimalabstand 8 ist. Also gilt $|C_u| = 2^{11}$ und somit $\dim C_u = 11$. Außerdem haben alle Wörter in $C_u$ gerades Gewicht, da für $x \in C$ und das entsprechende $\tilde{x} \in C_u$

$$w(\tilde{x}) + 2\,\mathbb{Z} = \Phi(x, \overline{u}) + 2\,\mathbb{Z} = x \cdot \overline{u} = 0$$

gilt, da $C$ selbstdual ist.

Damit ist $C_u$ aufgrund der Kardinalitätsgleichheit schon der Code, der aus allen Vektoren des $\mathbb{F}_2^{12}$ besteht, die gerades Gewicht haben. Für einen solchen Code ist

$$\left(\begin{array}{c|c} (1^{11})^{tr} & I_{11} \end{array}\right)$$

eine Generatormatrix, wobei $a^n$ den Zeilenvektor, der $n$-mal $a$ enthält, darstellt. Wählt man bis auf Äquivalenz $u = (1^{12}\ 0^{12})^{tr}$, ergibt sich aus Dimensionsgründen, das $C$ eine Generatormatrix folgender Form hat

$$\left(\begin{array}{c|c|c|c} 1^{11} & 1 & 0 & 0^{11} \\ \hline A & (0^{11})^{tr} & (1^{11})^{tr} & I_{11} \end{array}\right)$$

mit $A \in \mathbb{F}_2^{11\times 11}$, da sich die zwölfte Spalte ausräumen lässt.
Die Matrix $A$ muss dabei folgende Eigenschaften erfüllen, die aus $d = 8$ folgen:

(i) Jede Zeile hat Gewicht $\geq 6$

(ii) Zwei unterschiedliche Zeilen haben Abstand $\geq 6$

Dabei müssen die Zeilen gleichzeitig Gewicht $\geq 6$ und Abstand $\geq 5$ zu $1^{11}$ haben, somit gilt schon, dass jede Zeile Gewicht 6 hat. Außerdem muss für alle $i, j \in \underline{11}$ mit $i \neq j$ für die entsprechenden Zeilen $A_i, A_j$ gelten $4|(d(A_i, A_j)+2)$, da $C$ doppelt gerade ist. Somit gilt

$$d(A_i, A_j) \in \{6, 10\} \text{ für alle } i, j \in \{1, \ldots, 11\} \text{ mit } i \neq j.$$

Angenommen es gilt $d(A_i, A_j) = 10$ für $i, j \in \underline{11}$, dann gilt $w(A_i + A_j) = 10$. Somit gilt $d(1^{11}, A_i + A_j) = 1$, was ein Widerspruch ist, da der Abstand von $u$ zur Summe der beiden Zeilen der kompletten Generatormatrix dann $4 < d = 8$ wäre. Also gilt

$$d(A_i, A_j) = 6 \text{ für alle } i, j \in \{1, \ldots, 11\} \text{ mit } i \neq j.$$

Sei $A'$ die Identifizierung von $A$ in $\{0, 1\}^{11\times 11}$, dann erhält man unter Verwendung von Bemerkung 2.2 folgende Gleichheiten:

$$A'(A')^{tr} = 3I_{11} + 3J_{11} \quad \text{und} \quad A'J_{11} = 6J_{11}.$$

Somit gilt für $J_{11} - A'$ wiederum

$$\begin{aligned}(J_{11} - A')(J_{11} - A')^{tr} &= (J_{11} - A')(J_{11}^{tr} - (A')^{tr}) = J_{11}J_{11} - J_{11}(A')^{tr} - A'J_{11} - A'(A')^{tr} \\ &= 11J_{11} - (A'J_{11})^{tr} - 6J_{11} + 3I_{11} + 3J_{11} \\ &= 3I_{11} + 8J_{11} - 6J_{11} = 3I_{11} + 2J_{11}.\end{aligned}$$

Also ist $J_{11} - A'$ die Inzidenzmatrix eines 2-$(11, 5, 2)$-Designs. Somit folgt die Eindeutigkeit von $C$ mit Satz 1.6. ∎

## 2.2 Konstruktion des erweiterten Golay-Codes über den Hexacode

Wir wollen nun einen solchen Code konstruieren. Wir beginnen mit dem **Hexacode**, der ein $[6, 3, 4]$-Code über $\mathbb{F}_4 = \{0, 1, \omega, \overline{\omega}\}$, mit $\omega^2 = \omega + 1 = \overline{\omega}$, ist.
Die Wörter erhalten wir nach folgender Formel:

$$(a, b, c, f(1), f(\omega), f(\overline{\omega})), \quad \text{wobei} \quad f(x) := ax^2 + bx + c \quad \text{für} \quad a, b, c \in \mathbb{F}_4\,.$$

Entsprechend erhalten wir eine Generatormatrix mit

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

Nun wollen wir Aussagen über die Gewichte und Abstände des Codes zeigen.

**Lemma 2.4** *Der Hexacode hat Minimalabstand* 4 *und kein Wort von Gewicht* 5.

Beweis Da der Hexacode $C$ linear ist, ist die erste Aussage äquivalent dazu, dass ein $c \in C$ existiert mit $w(c) = 4$ und kein $c' \in C \setminus \{0\}$ existiert mit $w(c') < 4$.
Betrachtet man die Bildungsvorschrift der Wörter so erhält man die Wörter aus $C \setminus \{0\}$ durch Verwendung von Koeffizienten $(a, b, c) \in \mathbb{F}_4^3$ mit $(a, b, c) \neq 0$. Also erhält man in Kombination mit den Nullstellen des Polynoms folgende Gewichte für $(a, b, c) \neq (0, 0, 0)$:

| $a$ | $b$ | $c$ | $f = ax^2 + bx + c$ | Gewicht |
|---|---|---|---|---|
| $\neq 0$ | $\neq 0$ | $\neq 0$ | Irreduzibel oder zwei verschiedene NST | 4 oder 6 |
| $\neq 0$ | $\neq 0$ | $= 0$ | 0 als NST und eine weitere | 4 |
| $\neq 0$ | $= 0$ | $\neq 0$ | eine NST $\neq 0$, da Wurzeln in $\mathbb{F}_4$ eind. | 4 |
| $\neq 0$ | $= 0$ | $= 0$ | keine NST außer 0, da $\mathbb{F}_4$ Körper | 4 |
| $= 0$ | $\neq 0$ | $\neq 0$ | eine NST $\neq 0$ | 4 |
| $= 0$ | $\neq 0$ | $= 0$ | 0 ist einzige NST | 4 |
| $= 0$ | $= 0$ | $\neq 0$ | keine NST | 4 |

Somit folgen schon die zu zeigenden Aussagen. ∎

Auf Grundlage des Hexacodes wollen wir nun einen binären linearen Code $\tilde{G}$, den wir als den **erweiterten Golay-Code** bezeichnen werden, der Länge 24 konstruieren. Dabei stellen wir aus Gründen der Übersichtlichkeit die Wörter dieses Codes als als Matrizen aus $\{0,1\}^{4\times 6}$ dar, wobei man aus dieser Repräsentation die Codewörter zeilenweise ablesen kann.
Dabei müssen die Wörter folgenden Bedingungen genügen:

(A) Die Spaltensummen und die erste Zeilensumme sind entweder alle gerade oder ungerade.

(B) Bezeichnet man mit $r_i$ die $i$-te Zeile, für $1 \leq i \leq 4$, dann ist $r_2 + \omega r_3 + \overline{\omega} r_4$ ein Wort des Hexacodes.

Ein Codewort von $\tilde{G}$ erhält man dann in folgender Weise:

(i) Wähle eine Wort des Hexacodes.

(ii) Wähle die Parität der ersten Zeile.

(iii) Wähle 5 Spalten, sodass sie die Paritäts-Bedingung erfüllen und (B) genügen. Dabei ergeben die Spalten aus $\{0,1\}^{4\times 1}$ jeweils das angegeben Element von $\mathbb{F}_4$, wenn man die gewichtete Summe aus (B) berechnet:

$$\begin{array}{cccccccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \begin{pmatrix}0\\0\\0\\0\end{pmatrix} & \begin{pmatrix}1\\0\\0\\0\end{pmatrix} & \begin{pmatrix}0\\1\\1\\1\end{pmatrix} & \begin{pmatrix}1\\1\\1\\1\end{pmatrix} & \begin{pmatrix}0\\1\\0\\0\end{pmatrix} & \begin{pmatrix}1\\1\\0\\0\end{pmatrix} & \begin{pmatrix}0\\0\\1\\1\end{pmatrix} & \begin{pmatrix}1\\0\\1\\1\end{pmatrix} \\ \omega & \omega & \omega & \omega & \overline{\omega} & \overline{\omega} & \overline{\omega} & \overline{\omega} \\ \begin{pmatrix}0\\0\\1\\0\end{pmatrix} & \begin{pmatrix}1\\0\\1\\0\end{pmatrix} & \begin{pmatrix}0\\1\\0\\1\end{pmatrix} & \begin{pmatrix}1\\1\\0\\1\end{pmatrix} & \begin{pmatrix}0\\0\\0\\1\end{pmatrix} & \begin{pmatrix}1\\0\\0\\1\end{pmatrix} & \begin{pmatrix}0\\1\\1\\0\end{pmatrix} & \begin{pmatrix}1\\1\\1\\0\end{pmatrix} \end{array}$$

.

(iv) Aufgrund der Parität ist dann der erste Eintrag der sechsten Spalte schon eindeutig festgelegt und somit mit den weiteren Bedingungen auch die komplette Spalte.

**Satz 2.5** *Der* ***erweiterte Golay-Code*** $\tilde{G}$ *ist ein* $[24, 12, 8]$*-Code.*
*Insbesondere ist* $\tilde{G}$ *bis auf Äquivalenz eindeutig.*

BEWEIS Die Wörter von $\tilde{G}$ werden als Matrizen aus $\{0,1\}^{4\times 6}$ repräsentiert, also lassen sie sich auch mit Elementen aus $\mathbb{F}_2^{24}$ identifizieren. Somit ist $\tilde{G}$ ein binärer Code der Länge 24.
Seien $g, h \in \tilde{G}$, dann sind für $g$ und $h$ die Bedingungen (A) und (B) erfüllt. Dabei sind die Paritäten der Zeilen bzw. Spaltensummen linear und somit erfüllt $g+h$ die Bedingung (A). Seien $r_2, r_3, r_4$ bzw. $r'_2, r'_3, r'_4$ die 2-ten bis 4-ten Zeilen der Matrixrepräsentation von $g$ bzw. $h$. Dann gilt

$$\begin{aligned}&(r_2 + r'_2) + \omega(r_3 + r'_3) + \overline{\omega}(r_4 + r'_4)\\ =&(r_2 + \omega r_3 + \overline{\omega} r_4) + (r'_2 + \omega r'_3 + \overline{\omega} r'_4),\end{aligned}$$

was Element des Hexacodes ist, da dieser linear ist. Somit ist auch für $g+h$ (B) erfüllt. Insgesamt gilt also, dass $\tilde{G}$ ein linearer Code.

Also lässt sich die Dimension des Codes über die Freiheitsgrade bzw. Wahlmöglichkeiten der Konstruktion herleiten.
In (i) lässt sich jedes der $4^3 = 2^6$ Elemente des Hexacodes wählen.
Schritt (ii) bietet $2 = 2^1$ Möglichkeiten.
Aufgrund der Paritätsbedingung lässt sich in (iii) für jede der fünf Spalten zwischen zwei Spalten wählen, die beide die gleiche Parität besitzen und in der gewichteten Summe das gleiche Element des $\mathbb{F}_4$ ergeben. Somit ergeben sich $2^5$ Wahlen.
Da im letzten Schritt keine Wahlmöglichkeit mehr besteht, ergibt sich insgesamt, dass $\tilde{G}$ die Dimension $6 + 1 + 5 = 12$ besitzt.

Also ist noch zu zeigen, dass $\tilde{G}$ Minimalabstand 8 hat. Da $\tilde{G}$ linear ist, ist dies äquivalent dazu, dass das minimale Gewicht ungleich 0 in $\tilde{G}$ schon 8 beträgt.
Betrachtet man die Matrix

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

dann erfüllt diese (A) und (B). Somit existiert ein Wort in $\tilde{G}$ mit Gewicht 8.
Betrachten wir nun die Konstruktionsvorschrift:
Wählt man bei (ii) gerade und bei (i) 0 erhält man entweder 0 oder ein Wort mit Gewicht $\geq 8$, da sich die 0 in der gewichteten Spaltensumme und gerader Spaltensumme nur mit der Einsspalte erreichen lässt.
Wählt man bei (ii) gerade und bei (i) ein Wort ungleich 0, so hat das Wort aus dem Hexacode nach Lemma 2.4 mindestens Gewicht 4 und somit haben alle so konstruierten Wörter von $\tilde{G}$ bereits Gewicht $\geq 4 \cdot 2 = 8$.
Wählt man in (ii) ungerade, folgt sofort, dass keine Nullspalte existieren kann. Also erhällt man Wörter mit Gewichten $\geq 6$. Gewicht 6 ließe sich nur erreichen, indem man die eine 1 in der ersten Zeile einträgt und auf die 5 weiteren Spalten jeweils eine 1

außerhalb der ersten Spalte verteilt. Die gewichtete Spaltensumme würde dann aber mit Gewicht 5 kein Wort des Hexacodes darstellen, wie in Lemma 2.4 gesehen. Gewicht 7 ist aufgrund der Paritätswahl auch nicht möglich. Also haben alle so konstruierten Wörter wieder Gewicht $\geq 8$.

Insgesamt haben wir also gezeigt, dass der erweiterte Golay-Code eine $[24, 12, 8]$-Code ist. Damit folgt die Eindeutigkeit mit Satz 2.3. ∎

## 2.3 Konstruktion des erweiterten Golay-Codes mithilfe eines Ikosaeders

Alternativ lässt sich der erweiterte Golay-Code mithilfe eines Ikosaeders konstruieren. Aufgrund seiner Symmetrie lässt sich ohne Beschränkung der Allgemeinheit eine Ecke als Ausgangspunkt bestimmen. Man nummeriere davon ausgehende zunächst die fünf Ecken die über eine Kante mit dem Ausgangspunkt verbunden sind, dann die fünf über zwei Kanten verbundenen und schließlich den letzten gegenüberliegenden zwölften Punkt. Damit lässt sich der Ikosaeder als Graph darstellen:

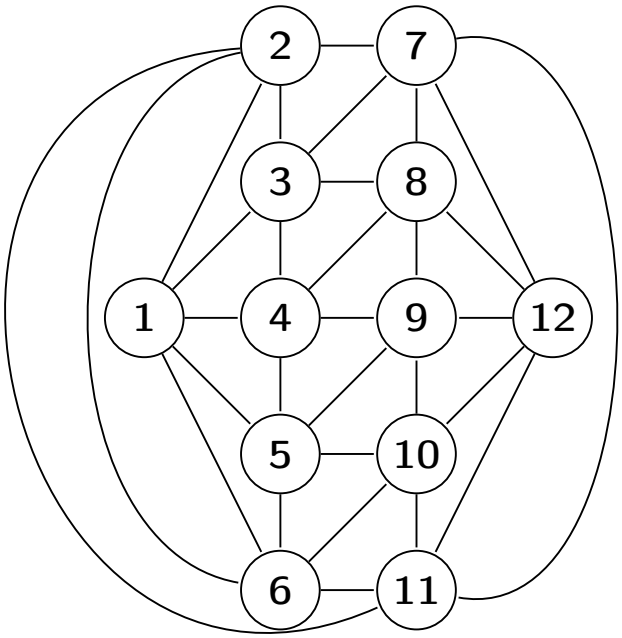


Abbildung 1: Darstellung des Ikosaeders als Graphen

Mit $A$ bezeichnen wir die Matrix, die man erhält, wenn man die Adjazenzmatrix des Graphen in $\mathbb{F}_2^{12\times 12}$ identifiziert.
Da die Adjazenzmatrix eines ungerichteten Graphen symmetrisch ist, gilt dies auch für $A$. Somit gilt für $i, j \in \{1, \dots, 12\}$ auch

$$\begin{aligned}(AA)_{i,j} = (AA^{tr})_{i,j} &= (A_{\_,i}) \cdot (A_{\_,j}) = \Phi(A_{\_,i}, A_{\_,j}) + 2\,\mathbb{Z} \\ &= \begin{cases} 0 + 2\,\mathbb{Z} & \text{, falls } i \neq j \\ 1 + 2\,\mathbb{Z} & \text{, falls } i = j \end{cases},\end{aligned}$$

da $\Phi$ das Skalarprodukt der Spalten der Adjazenzmatrix bildet und man am Graphen ablesen kann, dass zwei ungleiche Knoten stets eine gerade Anzahl an Knoten besitzen zu denen sie beide verbunden sind.
Also ist $A \in \mathrm{GL}_{12}(\mathbb{F}_2)$ und insbesondere selbstinvers.

Betrachten wir nun den Code den wir mit folgender Generatormatrix erhalten

$$M := \left(\begin{array}{c|c} I_{12} & J_{12} + A \end{array}\right)$$

Dann erzeugt uns dies einen Code der Länge 24 mit Dimension 12.
Außerdem gilt mit der Symmetrie von $A$ und da $A$ selbstinvers ist

$$\begin{aligned}MM^{tr} &= I_{12} + (J_{12} + A)(J_{12} + A)^{tr} \\ &= I_{12} + J_{12}^2 + J_{12}A + (J_{12}A)^{tr} + A^2 \\ &= I_{12} + I_{12} = 0.\end{aligned}$$

Damit ist der generierte Code aus Dimensionsgründen schon selbstdual. Darüber hinaus gilt nach Betrachtung des Graphen bereits, dass jede Zeile von $A$ Gewicht 5 besitzt. Somit besitzt jede Zeile von $M$ Gewicht 8, womit ein doppelt gerader Code vorliegt.

Um zu zeigen, dass wir (bis auf eventuelle Umordnung) wieder den Golay-Code konstruiert haben, ist also noch zu zeigen, dass Minimalabstand 8 gilt. Aus dem eben Gezeigten folgt schon, dass nur Minimalabstand 4 oder 8 möglich ist.
Da der Code linear ist, reicht es wieder minimale Gewichte von Wörtern ungleich 0 zu betrachten.
Ein Wort mit Gewicht 4 müsste eine Linearkombination von höchstens vier Zeilen der Generatormatrix sein, da diese die $I_{12}$ enthält. Wie oben gesehen haben keine der Zeilen Gewicht 4 und eine Linearkombination von vier Zeilen mit Gewicht 4 würde eine nichttriviale Linearkombination der 0 aus den Zeilen von $A$ erfordern, was nicht möglich ist, da $A$ invertierbar ist.
Eine Linearkombination aus zwei Zeilen mit Gewicht 4 würde eine Linearkombination von zwei Zeilen von $A$ mit Gewicht 2 bedingen. Führt man dies auf den Ikosaeder zurück müsste es zwei Ecken geben, für die es nur zwei Ecken gibt, die nur mit jeweils einer

der beiden mit einer Kante verbunden sind. Aufgrund der Symmetrie kann man alle möglichen Fälle durch die Betrachtung der Knoten 1 und 4 bzw. 1 und 9 bzw. 1 und 12 im Graphen aus der Abbildung abdecken, für die diese Aussage stets falsch ist.
Dreier-Linearkombinationen mit Gewicht 4 würden für den Ikosaeder bedeuten, dass bei Wahl von drei verschiedenen Ecken nur genau eine Ecke existiert, die mit einer geraden Anzahl von diesen drei Ecken verbunden ist. Sind die drei Ecken unverbunden, ist dies falsch. Sind nur zwei der Ecken verbunden, so lässt sich dies aufgrund der Symmetrie auf die Fälle der Knoten 1 und 4 mit 7 bzw. 12 zurückführen, für die die Aussage jeweils nicht gilt. Liegt eine Ecke zwischen den beiden anderen, lässt sich dies so drehen, dass die Ecken dem Knoten 1 und zwei Knoten die über eine Kante mit 1 verbunden sind. Damit wären aber die Knoten 1 und 12 mit einer geraden Anzahl der drei Kanten verbunden.

Insgesamt folgt also, dass ein $[24, 12, 8]$-Code erzeugt wird.

## 2.4 Konstruktion des Golay-Codes aus dem erweiterten Golay-Code

Nun wollen wir den Golay-Code aus dem erweiterten Golay-Code durch Punktieren erhalten. Da wir auch hier die Eindeutigkeit bis auf Äquivalenz zeigen wollen, ist es nötig zu zeigen, dass die Wahl der Koordinatenposition bei der Punktierung beliebig ist. Dazu betrachten wir die Automorphismengruppe des erweiterten Golay-Codes.

**Proposition 2.6** *Die Automorphismengruppe des erweiterten Golay-Codes $\tilde{G}$ operiert transitiv auf den 24 Koordinatenpositionen.*

BEWEIS Betrachtet man die Generatormatrix von $\tilde{G}$ aus der Konstruktion aus dem Ikosaeder so gilt:

$$\begin{pmatrix} J_{12} + A & I_{12} \end{pmatrix} \begin{pmatrix} I_{12} & J_{12} + A \end{pmatrix}^{tr} = (J_{12} + A) + (J_{12} + A) = 0$$

Da der Code selbstdual ist, sind also beide Matrizen Generatormatrizen von $\tilde{G}$.
Die Symmetriegruppe des Ikosaeders operiert transitiv auf den 12 Ecken und somit folgt, dass auch die Automorphismengruppe des erweiterten Golay-Codes transitiv auf den 12 ersten bzw. auf den 12 zweiten Koordinatenpositionen operiert. Da diese insgesamt miteinander vertauschbar sind, wie oben gesehen, folgt die Transitivität auf den gesamten 24 Koordinatenpositionen. ∎

Kommen wir nun zum Golay-Code.

**Korollar 2.7** *Sei $C$ ein binärer Code, der die 0 enthält, mit Wortlänge 23, Minimalabstand 7 und $|C| = 2^{12}$. Dann ist $C$ der binäre **Golay-Code** $G$.*

BEWEIS Sei $C$ ein solcher Code. Für alle $u, v \in C$ mit $d(u,v) = 7$ gilt dann wie in Bemerkung 2.2 gesehen

$$7 = d(u,v) = w(u) + w(v) - \underbrace{2\Phi(u,v)}_{\in 2\,\mathbb{Z}}.$$

Also hat eines der Wörter gerades Gewicht und eines ungerades Gewicht. Somit erhalten wir durch Hinzufügen eines Paritäts-Bit einen $(24, 2^{12}, 8)$-Code, also nach Satz 2.3 den erweiterten Golay-Code.

Also erhält man $C$ aus $\tilde{G}$ durch Punktieren einer Koordinatenposition. Nach Proposition 2.6 operiert die Automorphismengruppe des Golay-Codes jedoch transitiv auf den Koordinatenposition, womit alle Wahlen der Punktierungspositionen äquivalent sind. ∎

Insbesondere haben wir im Beweis zu Satz 2.3 schon die Koeffizienten der Gewichtszähler bestimmt. Für $G$ bzw. $\tilde{G}$ erhällt man also folgende Gewichtszähler:

$$\begin{aligned} W_G(X,Y) =& X^{23} + 253X^{16}Y^7 + 506X^{15}Y^8 + 1288X^{12}Y^{11} \\ & 1288X^{11}Y^{12} + 506X^8Y^{15} + 253X^7Y^{16} + Y^{23} \end{aligned}$$

$$W_{\tilde{G}}(X,Y) = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24}.$$

Diese werden uns im letzten Kapitel noch hilfreich sein.

# 3 Das Leech-Gitter

Kommen wir nun zum letzten Kapitel der Ausarbeitung.

## 3.1 Ein unimodulares gerades Gitter der Dimension 24 ohne Wurzeln

In diesem Abschnitt wollen wir mithilfe des eben konstruierten erweiterten Golay-Codes ein unimodulars gerades Gitter ohne Wurzeln erhalten. Dazu verwenden wir wieder die Reduktionsabbildung mod 2

$$\rho : \mathbb{Z}^{24} \to \mathbb{F}_2^{24}.$$

Zunächst werden wir das Gitter $\Gamma_{\tilde{G}} = \frac{1}{\sqrt{2}}\rho^{-1}(\tilde{G})$ betrachten und definieren zur besseren Übersichtlichkeit $\Gamma := \rho^{-1}(\tilde{G})$.

**Bemerkung 3.1** *Das Gitter $\Gamma_{\tilde{G}}$ ist ein gerades unimodulares Gitter. Für $\Gamma_{\tilde{G}}$ haben wir folgende Koeffizienten der Theta-Reihe*

$$a_1 = 48 \quad \textit{und} \quad a_2 = 195408.$$

BEWEIS Nach Aussagen des ersten Vortrags folgt die Unimodularität von $\Gamma_{\tilde{G}}$ direkt aus der Selbstdualität von $\tilde{G}$. Ebenso ist $\Gamma_{\tilde{G}}$ ist ein gerades Gitter, da $\tilde{G}$ ein doppelt gerader Code ist.

Nach Definition korrespondieren die Wurzeln von $\Gamma_{\tilde{G}}$ zu den Vektoren der Länge 4 aus $\Gamma$. Dabei existieren in $\mathbb{Z}^{24}$ für Vektoren der Länge 4 nur zwei Möglichkeiten. Entweder ist dies ein mit $\pm 2$ skalierter Einheitsvektor oder die Summe vier unterschiedlicher positiver oder negativ skalierter Einheitsvektoren. Dabei werden Erstere durch $\rho$ auf 0 abgebildet und Letztere werden von $\rho$ auf Elemente mit Gewicht 4 abgebildet und sind somit nicht in $\Gamma$ enthalten. Damit enthällt $\Gamma$ insgesamt $2 \cdot \binom{24}{1} = 48$ Vektoren der Länge 4 und somit folgt

$$a_1 = 48.$$

Nach einer Aussage des vorangegangenen Vortrags gilt aber auch schon

$$a_2 = 196560 - 24a_1 = 195048.$$

Dies lässt sich auch mit analoger Argumentation wie für $a_1$ erschließen. ∎

Somit ist $\Gamma_{\tilde{G}}$ noch nicht das gewünschte Gitter, da es noch Wurzeln enthält.
Um das Leech-Gitter zu definieren betrachten wir zunächst $\Gamma$ und eine Zerlegung von $\Gamma$ mithilfe einer Reduktionsabbildung.

**Bemerkung 3.2** *Die Abbildung*

$$\alpha : \Gamma \to \mathbb{F}_2, x \mapsto \left( \frac{1}{2} \sum_{i=1}^{24} x_i \right) + 2\,\mathbb{Z}$$

*ist ein wohldefinierter Homomorphismus.*
*Insbesondere lässt sich mit $N := \alpha^{-1}(1)$ und $A := \alpha^{-1}(0)$ das Gitter $\Gamma$ disjunkt zerlegen, also*

$$\Gamma = A \uplus N.$$

BEWEIS Sei $G'$ die Identifizierung von $\tilde{G}$ in $\mathbb{Z}^{24}$. Dann lässt sich jedes $x \in \Gamma$ darstellen als $x = c + 2y$ mit $c \in G'$ und $y \in \mathbb{Z}^{24}$.
Nach Satz 2.3 ist $\tilde{G}$ ein doppelt gerader Code, damit gilt also

$$\sum_{\mathrm{i}=1}^{24} c_i \in 4\,\mathbb{Z}\,.$$

Somit folgt also insbesondere

$$\sum_{\mathrm{i}=1}^{24} x_i \in 2\,\mathbb{Z},$$

da $\sum_{\mathrm{i}=1}^{24} 2y_i \in 2\,\mathbb{Z}$. Damit ist die Abbildung $\alpha$ ein wohldefinierter Homomorphismus, da sie offenbar $\mathbb{Z}$-linear ist. Die Zerlegung folgt nach Definition von $\alpha$. ∎

Die Mengen $A$ und $N$ wollen wir zunächst etwas genauer betrachten.

**Bemerkung 3.3** *Es gilt:*

*i) $A$ ist ein volles Teilgitter von $\Gamma$ von Index 2 und enthält keine Vektoren der Quadratlänge 4.*

*ii) Die Quadratlängen aller Element von $\left(\frac{1}{2}\cdot \boldsymbol{1} + N\right)$ sind durch 4 teilbar. Dabei bezeichnet $\boldsymbol{1} \in \mathbb{Z}^{24}$ den 1-Vektor.*

Beweis
Zu i) :

Für alle $i \in \{1, \ldots, 24\}$ gilt $4 \cdot e_i \in A$. Somit ist $A$ als Kern von $\alpha$ eine volles Teilgitter von $\Gamma$. Mit dem Homomorphiesatz folgt, dass $A = \mathrm{Kern}(\alpha)$ Index 2 in $\Gamma$ hat.
Im Beweis zu Bemerkung 3.1 haben wir bereits die Form der Vektoren von $\Gamma$ mit Quadratlänge 4 gesehen. Nach Definition von $\alpha$ werden diese auf $1 + 2\,\mathbb{Z}$ abgebildet. Also liegen keine Vektoren dieser Länge in $A$.

Zu ii) :

Sei $x \in \left(\frac{1}{2}\cdot \mathbf{1} + N\right)$, dann existiert ein $c$ aus der Identifizierung von $\tilde{G}$ und ein $y \in \mathbb{Z}^{24}$ mit $\sum y_i$ ungerade, sodass gilt

$$x = \frac{1}{2}\cdot \mathbf{1} + c + 2\cdot y.$$

Es gilt nach Wahl von $c$ und $y$ schon $\sum_{\mathrm{i}=1}^{24} x_i \equiv 2\sum_{\mathrm{i}=1}^{24} y_i \pmod 4$, da $\tilde{G}$ ein doppelt gerader Code ist und $\sum_{\mathrm{i}=1}^{24} \frac{1}{2}\mathbf{1}_i = 12 \equiv 0 \pmod 4$. Somit gilt auch $\frac{1}{2}\sum_{\mathrm{i}=1}^{24} x_i \equiv \sum_{\mathrm{i}=1}^{24} y_i \pmod 2$ und damit insbesondere $2\sum_{\mathrm{i}=1}^{24} y_i \equiv 2 \pmod 4$, also gilt:

$$\begin{aligned}
(x,x) &= \left(\frac{1}{2}\cdot \mathbf{1} + c + 2\cdot y, \frac{1}{2}\cdot \mathbf{1} + c + 2\cdot y\right) \\
&= \frac{1}{4}(\mathbf{1},\mathbf{1}) + \underbrace{(\mathbf{1},c)}_{\in 4\,\mathbb{Z}} + 2\cdot(\mathbf{1},y) + \underbrace{4\cdot(c,y)}_{\in 4\,\mathbb{Z}} + \underbrace{(c,c)}_{\in 4\,\mathbb{Z}} + \underbrace{4\cdot(y,y)}_{\in 4\,\mathbb{Z}} \\
&\equiv 6 + 2\cdot(\mathbf{1},y) \pmod 4 \\
&\equiv 6 + 2\cdot\left(\sum_{\mathrm{i}=1}^{24} y_i\right) \equiv 0 \pmod 4.
\end{aligned}$$

∎

Mithilfe der beiden Mengen aus Bemerkung 3.2 definieren wir nun das Leech-Gitter.

**Definition 3.4** *Das* ***Leech-Gitter*** *ist das Gitter*

$$\Lambda_{24} := \frac{1}{\sqrt{2}} \left( A \cup \left( \frac{1}{2}\boldsymbol{1} + N \right) \right).$$

Nun wollen wir zeigen, dass $\Lambda_{24}$ das gewünschte unimodulare ganze Gitter ist, was die Aussage des nächsten Lemmas ist. Vorher wollen wir kurz Argumente aus der Einführung von Gittern aufgreifen, da diese Aussagen die Unimodularität liefern.

**Bemerkung 3.5** *Sei $L \subset \mathbb{R}$ ein volles Gitter und $L'$ ein volles Teilgitter. Dann gilt bekanntermaßen:*

$$\operatorname{vol}(\mathbb{R}^n / L') = \operatorname{vol}(\mathbb{R}^n / L) \cdot |L/L'| \tag{1}$$

$$\operatorname{vol}(\mathbb{R}^n / L^{\#}) = \frac{1}{\operatorname{vol}(\mathbb{R}^n / L)} \tag{2}$$

$$L^{\#} \subset (L')^{\#} \tag{3}$$

*Damit erhält man also direkt*

$$|L/L'| = \frac{\operatorname{vol}(\mathbb{R}^n / L')}{\operatorname{vol}(\mathbb{R}^n / L)} = \frac{\operatorname{vol}(\mathbb{R}^n / L^{\#})}{\operatorname{vol}(\mathbb{R}^n / (L')^{\#})} = |(L')^{\#} / L^{\#}|.$$

*Ist $L''$ wiederum ein volles Teilgitter von $L'$, dann ergibt sich mit Gleichung* (1)*:*

$$|L/L''| = \frac{\operatorname{vol}(\mathbb{R}^n / L'')}{\operatorname{vol}(\mathbb{R}^n / L)} = \frac{\operatorname{vol}(\mathbb{R}^n / L'')}{\operatorname{vol}(\mathbb{R}^n / L')} \cdot \frac{\operatorname{vol}(\mathbb{R}^n / L')}{\operatorname{vol}(\mathbb{R}^n / L)} = |L/L'| \cdot |L'/L''|.$$

Zeigen wir nun also die Eigenschaften des Leech-Gitters.

**Lemma 3.6** *Das Leech-Gitter $\Lambda_{24}$ ist ein gerades unimodulares Gitter, das keine Wurzeln enthällt.*

Beweis Zunächst ist zu zeigen, dass $\left(A \cup \left(\frac{1}{2}\mathbf{1} + N\right)\right)$ ein Gitter ist. Wählt man $x, y \in \left(\frac{1}{2}\mathbf{1} + N\right)$, so gilt $x + y \in A$, da $\alpha$ ein Homomorphismus ist und $\alpha(\mathbf{1}) = 0$. Wählt man $x \in A$ und $y \in \left(\frac{1}{2}\mathbf{1} + N\right)$, so exisitiert ein $y' \in N$ mit $y = \frac{1}{2} \cdot \mathbf{1} + y'$. Dann gilt wieder mit der Homomorphie von $\alpha$ schon $x + y' \in N$ und somit $x + y \in \left(\frac{1}{2}\mathbf{1} + N\right)$.
Nach Bemerkung 3.3 ist $A$ ein Gitter und somit gilt insgesamt, was zu zeigen war.

Also ist auch $\Lambda_{24}$ ein Gitter und insbesondere ein gerades Gitter, was direkt aus den Aussagen aus Bemerkung 3.3 folgt.

In 3.3 i) haben wir außerdem gesehen, dass $A$ ein Teilgitter von Index 2 von $\Gamma$ ist, womit auch $\frac{1}{\sqrt{2}}A$ ein Teilgitter von Index 2 von $\Gamma_{\tilde{G}}$ ist. Da $\frac{1}{2}\cdot\mathbf{1}$ kein Vektor aus $A$ ist und nach Bemerkung 3.2 schon $A$ und $N$ eine disjunkte Zerlegung von $\Gamma$ bilden, hat $\frac{1}{\sqrt{2}}A$ Index 2 in $\Lambda_{24}$. Dabei ist $\Gamma_{\tilde{G}}$ nach Bemerkung 3.1 unimodular und somit gilt dies auch für $\Lambda_{24}$ mi den Aussagen von Bemerkung 3.5.

Mit Bemerkung 3.3 folgt sofort, dass $\frac{1}{\sqrt{2}}A$ keine Wurzeln enthält.
Betrachtet man $\left(\frac{1}{2}\mathbf{1}+\mathbb{Z}^{24}\right)\supseteq\left(\frac{1}{2}\mathbf{1}+N\right)$, so sieht man, dass die kürzest möglichen Vektoren die Form $\left(\pm\frac{1}{2},\ldots,\pm\frac{1}{2}\right)$ und somit Länge 6 haben. Insgesamt folgt also, dass $\Lambda_{24}$ keine Wurzeln enthält. ∎

Also erfüllt $\Lambda_{24}$ alle Anforderungen, womit wir mithilfe des erweiterten Golay-Codes ein Gitter der gewünschten Form konstruiert haben.

Abschließend wollen wir noch die Anzahl der Vektoren der Länge 4 aus $\Lambda_{24}$ ermitteln, die somit die kürzesten Vektoren des Gitters sind. Diese korrespondieren zu den Vektoren der Länge 8 aus $A$ und $\left(\frac{1}{2}\mathbf{1}+N\right)$. Diese lassen sich aber leicht über ihre Form (bis auf Permutation) charakterisieren.

Betrachtet man zunächst $A$, so haben die Vektoren der Länge 8 die Form $(\pm1)^8(0)^{16}$ oder $(\pm2)^2(0)^{22}$. Erstere werden durch $\rho$ auf Wörter mit Gewicht 8 reduziert und liegen im Kern von $\alpha$, also lässt sich aus dem Gewichtszähler von $\tilde{G}$ ablesen, dass es $759\cdot2^7=97152$ Vektoren dieser Form in $A$ gibt. Alle $\binom{24}{2}\cdot2^2=1104$ aus $\mathbb{Z}^{24}$ mit der zweiten Form sind in $A$ enthalten.

Im Beweis zum letzten Lemma haben wir bereits die Form der Vektoren der Länge 6 gesehen. Also müssen die Vektoren der Länge 8 in $\left(\frac{1}{2}\mathbf{1}+N\right)$ von der Form $(\pm\frac{1}{2})^{23}(\pm\frac{3}{2})^1$ sein. Dabei zerfallen die Vektoren in einen Anteil aus $N$ und $\frac{1}{2}\cdot\mathbf{1}$. Um einen Eintrag $\pm\frac{3}{2}$ zu erhalten, muss man einen Eintrag des Anteils aus $N$ auf 1 oder $-2$ setzen. Der Vektor muss im Urbild von $1+2\,\mathbb{Z}$ unter $\alpha$ liegen, was im ersten Fall einen Vektor mit gerader Anzahl an Einträgen ungleich 0 benötigt, wobei einer die 1 ist und alle anderen $-1$ als Wert haben müssen, im zweiten Fall braucht man einen entsprechenden Vektor mit ungerader Länge. Also kann man mithilfe des Gewichtszählers von $\tilde{G}$ die Anzahl berechnen:

$$2\cdot(1\cdot24+759\cdot8+2576\cdot12+759\cdot16)=98304.$$

Fasst man dies nun zusammen, erhält man insgesamt folgende Tabelle

| Typ | | Anzahl |
|---|---|---|
| $(\pm1)^80^{16}$ | aus $A$ | 97152 |
| $(\pm2)^20^{22}$ | aus $A$ | 1104 |
| $(\pm\frac{1}{2})^{23}(\pm\frac{3}{2})^1$ | aus $\left(\frac{1}{2}\mathbf{1}+N\right)$ | 98304 |
| | | 196560 |

Damit kann man auch wieder sehen, dass $\Lambda_{24}$ keine Wurzeln enthält.

Insgesamt haben wir in dieser Ausarbeitung also den Golay-Code über den erweiterten Golay-Code erhalten und deren Eindeutigkeit gezeigt.
Das Leech-Gitter ließ sich darauf basierend dann konstruieren.

# 4 Anhang

## 4.1 Implementierung des Abzählverfahrens

Das im Beweis zu Satz 2.3 vorgestellte Abzählverfahren lässt sich einfach, wie hier zum Beispiel in Java, als Programm implementieren. Der Code dient der Überprüfung der angegeben Koeffizienten des Gewichtszählers.

```
public class KoeffCNull{
  public static void main (String[] args){
    long[] koeff = new long[24];

    //Initialisierung, da 0 in C0 vertreten ist
    koeff[0]=1;
    for(int i = 1; i < koeff.length; i++){
      koeff[i] = 0;
    }

    //Beginn bei 7, da Minimalabstand = 7
    for(int i = 7; i < koeff.length; i++){
      int v = i-3;
      //Gesamtanzahl der Woerter mit Gewicht v
      koeff[i] = binomial(23,v);

      //Abzug der schon Ueberdeckten Woerter
      for(int j= i-6; j<i; j++){
        switch((j-v)){
          case 3:
            koeff[i] -= koeff[j] * binomial(j,3);
            break;
          case 2:
            koeff[i] -= koeff[j] * binomial(j,2);
            break;
          case 1:
            koeff[i] -= koeff[j] * j + koeff[j] * (23-j) * binomial(j,2);
            break;
          case 0:
            koeff[i] -= koeff[j] + koeff[j] * j *(23-j);
            break;
          case -1:
            koeff[i] -= koeff[j] * (23-j) + koeff[j] * (j) * binomial(23-j,2);
            break;
          case -2:
            koeff[i] -= koeff[j] * binomial(23-j,2);
            break;
          case -3:
            koeff[i] -= koeff[j] * binomial(23-j,3);
            break;
          default:
            koeff[i] += 0;
        }

      }
      //Anzahl der Woerter von Gewicht i
      koeff[i] = koeff[i] /(binomial(i,3));
    }
    for(int i = 0; i < koeff.length; i++){
      if(koeff[i] != 0){
        System.out.println("A[" + i + "] = " + koeff[i]);
      }
    }
  }

  //Binomialkoeffizient
  private static long binomial (int n, int k){
    if (k>n-k)
          k=n-k;
      long b=1;
      for (int i=1, m=n; i<=k; i++, m--)
        b=b*m/i;
      return b;
  }
}
```

# Literatur

[1] Ebeling, Wolfgang, *Lattices and Codes*, Springer Fachmedien Wiesbaden, 2012