Gitter und Codes über Kettenringen

Der Fakultät für Mathematik, Informatik und Naturwissenschaften der RWTH Aachen University vorgelegte Dissertation zur Erlangung des akademischen Grades eines Doktors der Naturwissenschaften

von

Simon Eisenbarth, M.Sc.

aus

Odenthal

Inhaltsverzeichnis

1 Einleitung **5**

2 Codierungstheorie **11**
2.1 Selbst-duale und extremale Codes 13
2.2 Beispiele von Codes 19
2.3 Klassifikation von Codes mit Automorphismen 20

3 Selbst-duale Codes über Kettenringen **33**
3.1 Codes über Kettenringen 34
3.2 Der Sockel 36
3.3 Selbst-duale Codes 37
3.4 Äquivalenz von Codes 40
3.5 Konstruktion aller selbst-dualen, freien Codes 41
3.6 Anwendungen 43

4 Extremale, ternäre Codes **45**
4.1 Codes der Länge 36 46
4.2 Codes der Länge 48 53

5 Gruppencodes **61**
5.1 Gruppencodes über Körpern 61
5.2 Gruppencodes über Kettenringen 65
5.3 Beispiele 70
5.3.1 Zyklische Codes 70
5.3.2 Diedergruppen 72
5.3.3 Die Alternierende Gruppe A_5 82

6 Extremale Gitter mit Automorphismen **85**
6.1 Geschlechter von Gittern 87
6.2 Hermitesche p-elementare Gitter 89
6.3 Modulare und extremale Gitter 93
6.4 Automorphismen eines Gitters 97
6.4.1 Automorphismen der Ordnung p eines p-elementaren Gitters 98
6.5 Extremale, 3-modulare Gitter der Dimension 24 109
6.6 Extremale, 5-modulare Gitter der Dimension 20 118

Literaturverzeichnis **121**

Kapitel 1

Einleitung

Die Codierungstheorie wurde in dem 1948 erschienenen Paper „A mathematical theory of communication“ von C. Shannon begründet. Daten, die über einen gestörten Kanal gesendet werden sollen, können mit Hilfe sogenannter Codes so kodiert werden, dass der Empfänger mögliche Fehler bei der Übertragung korrigieren kann. Die Suche nach Codes, die möglichst viele Fehler korrigieren können, ohne dabei zu ineffizient zu sein, ist das Hauptproblem der Codierungstheorie. In der klassischen, linearen Codierungstheorie ist ein Code C der Länge n über einem endlichen Körper $\mathbb{F}$ ein linearer Teilraum von $\mathbb{F}^n$. Der Minimalabstand ist das Minimum aller Gewichte $\mathrm{wt}(c)$, $0 \neq c \in C$, und ein Code mit Minimalabstand d kann genau $\left\lfloor \frac{d-1}{2} \right\rfloor$ Fehler korrigieren. Es ist also von Interesse, Codes mit möglichst hohem Minimalabstand zu finden, ohne dass die Dimension zu klein wird. Das Duale eines Codes ist der Orthogonalraum in dem zugrunde liegendem Vektorraum und ein Code, der gleich seinem Dualen ist, heißt selbst-dual. In diesem Fall ist der Gewichtszähler

$$\sum_{c \in C} x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)} \in \mathbb{C}[x, y]$$

invariant unter einer endlichen komplexen Matrixgruppe vom Grad 2. Damit lässt sich für kleine Körper eine obere Schranke für den Minimalabstand beweisen und selbst-duale Codes, welche diese Schranke annehmen, heißen extremal.

Ein klassisches Problem in der Mathematik ist das Kugelpackungsproblem. Hier wird eine Anordnung von Kugeln gleicher Größe gesucht, so dass diese einen Raum möglichst dicht ausfüllen. Falls für die Mittelpunkte u und v von zwei Kugeln $u - v$ und $u + v$ ebenfalls Mittelpunkte sind, spricht man von einer Gitterpackung. Ein Gitter in einem quadratischen Raum ist das ganzzahlige Erzeugnis einer Basis. Das Minimum eines Gitters ist die minimale Norm der Gittervektoren ungleich Null und dieses gibt zusammen mit dem Volumen des Fundamentalbereichs an, wie dicht die Kugelpackung den Raum ausfüllt. Ein Hauptproblem der Gittertheorie ist es, möglichst dichte Gitter zu finden. Die dichtesten Gitter sind in den Dimensionen ≤ 8 und 24 bekannt, in Dimension 3 wurde dies bereits durch Gauß gezeigt und erst 1998 konnte T. Hales durch den Beweis der Keplerschen Vermutung zeigen, dass diese Gitterpackung auch eine der überabzählbar

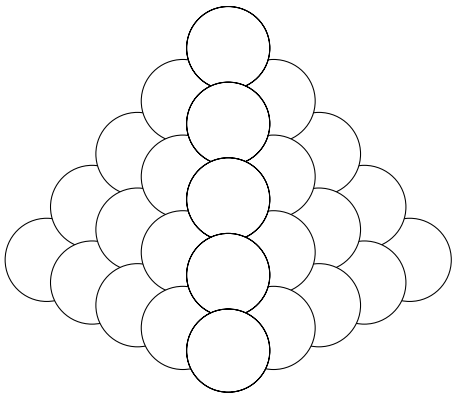


ABBILDUNG 1.1: Die dichteste (Gitter-)Packung in Dimension 3.

vielen besten Kugelpackungen liefert. Ähnliche Resultate wurden kürzlich in Dimension 8 und 24 bewiesen.
Die dichtesten Gitter in Dimension 8 und 24 haben gemeinsam, dass sie sogenannte gerade, unimodulare Gitter sind, d.h. sie definieren positiv definite, reguläre, ganzzahlige quadratische Formen. Für ein solches Gitter der Dimension n lässt sich durch die Theorie der Modulformen für das Minimum die obere Schranke $2 + 2\left\lfloor \frac{n}{24} \right\rfloor$ beweisen, und Gitter, die diese Schranke annehmen, heißen extremal. Da allein das Minimum eines unimodularen Gitters die Dichte bestimmt, definieren die extremalen Gitter die dichteste Kugelpackung unter den geraden, unimodularen Gittern. Motiviert durch die Tatsache, dass einige bekannte Gitter zwar nicht unimodular, aber geometrisch ähnlich zu ihrem Dualen sind, führte H.-G. Quebbemann 1995 den Begriff des p-modularen Gitters ein, diese sind isomorph zu ihrem $\sqrt{p}$-reskalierten Dualen für eine Primzahl p. In diesem Fall ist die Theta-Reihe

$$\sum_{\lambda \in L} q^{\frac{1}{2}(\lambda,\lambda)} \text{ mit } q = e^{2\pi i z}$$

eine Modulform für eine gewisse Untergruppe von $\mathrm{SL}_2(\mathbb{R})$ und falls 24 von $p+1$ geteilt wird, lässt sich wie im unimodularen Fall eine obere Schranke für das Minimum beweisen. Die p-modularen Gitter, welche diese Schranke annehmen, heißen dann ebenfalls extremal. Die extremalen Gitter sind dann von allen p-modularen Gittern einer Dimension die Dichtesten.

Beide Definitionen von Extremalität werden also auf eine ganz ähnliche Weise hergeleitet: steht das Objekt (d.h. der Code oder das Gitter) in Zusammehang mit seinem Dualen, ist die Gewichtsverteilung (d.h. der Gewichtszähler oder die Theta-Reihe) invariant unter einer bestimmten Gruppe, durch diese zusätzliche Struktur lässt sich dann eine obere Schranke für den Minimalabstand bzw. das Minimum beweisen. Die Klassifikation von extremalen Codes und Gittern ist dann eine naheliegendes Fragestellung.

Eine vollständige Klassifikation ist ein endliches Problem, da für jede Länge bzw.

Dimension nur endlich viele extremale Objekte existieren, und ab einer gewissen Schranke keine mehr existieren können (der extremale Gewichtszähler bzw. die extremale Theta-Reihe hätte dann einen negativen Eintrag). Der aktuelle Stand der Forschung ist aber weit von diesen theoretischen Schranken entfernt, allein schon was die Frage der Existenz eines extremalen Objektes betrifft. So ist z.B. bekannt, dass ab Länge 3936 kein binärer, extremaler, doppelt-gerader Code existieren kann, allerdings ist kein solcher Code mit Länge > 136 bekannt. Die Frage nach der Existenz in Länge 72 ist aktuell eines der größten Probleme in der Codierungstheorie. Auch im Fall der ternären, extremalen Codes, wo die Schranke mit 144 noch recht moderat ist, ist kein extremaler Code mit Länge ≥ 68 bekannt.

Die Komplexität einer Klassifikation wächst natürlich stark in der betrachteten Länge bzw. Dimension und die üblichen Beschränkungen von Speicherplatz und Rechenleistung macht diese ab einem gewissen Punkt aussichtslos. Eine Herangehensweise, die sich als sehr ergiebig herausgestellt hat, ist es, zusätzlich Symmetrien zu betrachten, d.h. die Existenz einer Untergruppe der Automorphismengruppe anzunehmen. Damit können zum einen neue extremale Codes oder Gitter gefunden werden, oder die Eindeutigkeit bzw. Nicht-existenz bekannter Objekte plausibilitiert werden. Häufig beschränkt man sich hier auf einen einzelnen Automorphismus von Prim-Ordnung. Der Fall, dass diese Ordnung nicht die Charakteristik des zugrunde liegenden Körpers, bzw. die Modularität des Gitters ist, wird in der Litaratur ausführlich beschrieben und angewendet. Für den Fall, dass beide Primzahlen gleich sind, sind Teilergebnisse in Spezialfällen bekannt, die Entwicklung einer allgemeinen Methodik ist Gegenstand dieser Arbeit.

Sei C ein extremaler, selbst-dualer Code über $\mathbb{F}_p$ mit einem Automorphismus g von Primordnung $q \neq p$. Der Gruppenring $\mathbb{F}_p C_q$ ist halbeinfach und die direkte Summe von Körpererweiterungen von $\mathbb{F}_p$ vom Grad $d = \mathrm{ord}(p \mod q)$, d.h. es gilt

$$\mathbb{F}_p C_q \cong \mathbb{F}_p \oplus \mathbb{F}_{p^d} \oplus \cdots \oplus \mathbb{F}_{p^d}.$$

Dadurch zerfällt C in die direkte Summe von Codes über $\mathbb{F}_{p^d}$ kleinerer Länge. Die Selbst-dualität von C und der Minimalabstand liefern hier Einschränkungen an die möglichen Komponenten. Dies wurde zuerst von V. Pless und J. Conway benutzt, um binäre Codes mit Automorphismen ungerader Ordnung zu betrachten, zusätzlich studierte W. C. Huffman ternäre Codes mit Automorphismen von Prim-Ordnung ≥ 5. Insbesondere bei der Suche nach einem binären, doppelt-geraden, extremalen Code der Länge 72 wurde diese Herangehensweise immer weiter optimiert.

Falls nun g ein Automorphismus von Ordnung p ist, ist C ein $\mathbb{F}_p C_p$-Modul, als Kettenring hat dieser aber keine nicht-triviale Zerlegung. Dies liefert die Hauptmotivation dieser Arbeit, Codes über Kettenringen zu betrachten.

Sei R ein kommutativer, artinscher Kettenring mit maximalem Ideal $\mathfrak{m} = \langle x \rangle$ der

Länge $a+1$. Ein Code C über R der Länge t ist ein R-Teilmodul des freien Moduls R^t. Die Multiplikation mit x definiert die Kette von Teilcodes

$$C \supseteq C^{(1)} := Cx \supseteq C^{(2)} := Cx^2 \supseteq \cdots \supseteq C^{(a)} := Cx^a \supseteq \{0\}.$$

In den Papern [Bou00], [Bou02] und [BW13] wird eine ähnliche Idee für den Spezialfall der binären, selbst-dualen Code mit einem Automorphismus g der Ordnung 2 angewendet (d.h. $R = \mathbb{F}_2C_2$ und $x = (1 + g)$). Das Hauptresultat von [Neb12b] besagt, dass der Code $C \cdot (1 + g)$ kanonisch isomorph zu einem selbst-dualen Code über $\mathbb{F}_2$ ist, genau dann wenn C ein freier $\mathbb{F}_2C_2$-Modul ist. Dieses Ergebnis wird in Kapitel 3 auf die allgemeine Situation übertragen und es wird gezeigt, dass ein selbst-dualer Code C in R^t ein freier R-Modul ist, genau dann wenn $C^{(a)}$ ein (hermitesch) selbst-dualer Code über dem Restklassenkörper $\mathbb{F} = R/\mathfrak{m}$ ist. In diesem Fall wird beschrieben, wie man einen gegebenen Code $C^{(i+1)}$ zu allen zulässigen Codes $C^{(i)}$ liftet. Diese stehen in Bijektion zu (hermitesch) selbst-dualen Codes in einem geeigenetem bilinearen Raum über $\mathbb{F}$. Schließlich wird ein Algorithmus formuliert, um alle freien, selbst-dualen Codes $C^{(0)}$ in R^t (mit hohem Minimalabstand) zu klassifizieren.

In Kapitel 4 wird diese entwickelte Methodik auf ternäre, extremale Codes angewendet. Der Pless-Code P_{36} ist der bisher einzige bekannte solche Code der Länge 36 und nach einem Resultat von W. C. Huffman eindeutig mit einem Automorphismus von Primordnung ≥ 5 ([Huf92]). Es wird gezeigt, dass diese Aussage auch für Ordnung 3 zutrifft. Alle Automorphismen der Ordnung 3 sind fixpunktfrei, daraus folgt, dass die Codes freie $\mathbb{F}_3C_3$-Moduln sind. Mit den Methoden von Kapitel 3 lässt sich also der (eindeutige) Fixcode liften, der einzige extremale Code ist der Pless-Code P_{36}. Im Fall der ternären, extremalen Codes der Länge 48 sind bisher zwei Codes bekannt, der Pless-Code P_{48} und der erweiterte quadratische Restklassen-Code XQ_{47}. Auch hier ist bekannt, dass diese Codes die einzigen solchen Codes mit einem Automorphismus von Primordnung ≥ 5 sind ([Neb12c]). Analog zum Fall der Länge 36 wird gezeigt, dass jeder Automorphismus der Ordnung 3 fixpunktfrei ist und die Codes freie $\mathbb{F}_3C_3$-Moduln sind. Mit den Methoden von Kapitel 3 lässt sich also auch hier wieder theoretisch der (eindeutige) Fixcode zu einem extremalen Code liften. Die Berechnungen sind allerdings zu zeitintensiv, die Eindeutigkeit wird aber unter einem zusätzlichem nicht-trivialen Automorphismus der Ordnung 2 gezeigt. Zusätzlich werden für diese beiden Längen Automorphismen der Ordnung 2 bzw. 4 betrachtet.

Gruppencodes über endlichen Körpern stießen auf Interessen, nachdem S. Berman 1967 gezeigt hat, dass der Reed-Muller-Code der Ordnung $m - l$ gerade die l-te Potenz des Jacobson-Radikals der Gruppenalgebra $\mathbb{F}_2C_2^m$ ist. Später wurden andere bekannte Codes als Gruppencodes identifiziert. In Kapitel 5 werden Gruppencodes über Kettenringen betrachtet. Es wird gezeigt, dass Gruppencodes, welche relativ projektiv für die Untergruppe $\{1\}$ im Sinne der homologischen Algebra sind, in Bijektion zu Ketten von Gruppencodes über

dem Restklassenkörper stehen. Von diesen Ketten lassen sich direkt Eigenschaften des erzeugenden Codes, wie der Minimalabstand oder die Dualität, ablesen.

Viele extremale Gitter wurden von G. Nebe und W. Plesken im Zuge der Klassifikation maximaler, endlicher, rationaler Matrixgruppen entdeckt ([NP95]). Andere Gitter wurden von C. Bachoc mit Hilfe von Zahlenkörpern, Quaternionen und Codes konstruiert (siehe auch [SS99] für einen Übersichtsartikel der Methoden und [Jür15] für den aktuellen Stand der Klassifikation). In [Neb13] wurde ein Langzeitprojekt gestartet, um alle 48-dimensionalen, unimodulare, extremale Gitter mit gegebenen Automorphismen zu klassifizieren und in [Jür15] wurde die Methodik auf den Fall angewendet, dass die Modularität des Gitters und die (Prim-)Ordnung des Automorphismus teilerfremd sind. In Kapitel 6 werden schließlich extremale, p-modulare Gitter mit Automorphismen der Ordnung p untersucht. Die Operation eines solchen Automorphismus liefert eine Zerlegung des zugrunde liegenden quadratischen Raumes in eine Fixpunkt- und zyklotomische Komponente, durch die Projektion bzw. den Schnitt des Gitters mit den beiden Komponenten lassen sich antiisometrische, quadratische, $\mathbb{F}_p$-wertige Räume definieren. Diese bestimmen wie im unimodularen oder teilerfremden Fall den Typ eines Automorphismus und entsprechende extremale Obergitter lassen sich durch die möglichen Antiisometrien bestimmen. Allerdings sind im Gegensatz zum teilerfremden Fall die quadratischen Räume nicht anisotrop, sondern enthalten (isomorphe) maximal total isotrope Teilräume. Diese definieren p-elementare (hermitesche) Gitter und können benutzt werden, um die Fix- und zyklotomischen Teilgitter zu bestimmen. Eine weitere Möglichkeit ist der Übergang zu einem maximalen Obergitter. Als Anwendung dieser Methodik wird gezeigt, dass das einzige bisher bekannte 24-dimensionale, 3-modulare, extremale Gitter das einzige solche Gitter mit einem Automorphismus der Ordnung 3 ist, dies wurde bisher für Prim-Ordnungen ≥ 5 gezeigt. Zusätzlich werden die 20-dimensionalen, 5-modularen, extremalen Gitter mit einem Automorphismus der Ordnung 5 klassifiziert, bis auf Isometrie gibt es genau 97 solche Gitter.

Danksagung

Mein ganz besonderer Dank gilt Prof. Dr. Gabriele Nebe für den Vorschlag dieses interessanten Projektes und die intensive Betreuung. Sie zeigte außerdem großes Interesse an meiner Arbeit und eine ansteckende Begeisterung für das Thema. Außerdem fungierte sie als Sprecherin des Graduiertenkollegs „Experimentelle und konstruktive Algebra“, die mir ein Stipendium während meiner Forschungszeit gewährten und diese somit erst ermöglicht haben.
Außerdem möchte ich Priv.-Doz. Dr. Markus Kirschmer für die viele Hilfe im Computeralgebra-System MAGMA bedanken.
Mein Dank gilt weiterhin dem Lehrstuhl B für Mathematik, ohne deren Server-Infrastruktur die speicherhungrigen Rechnungen in dieser Arbeit nicht möglich gewesen wären.
Zu guter letzt möchte ich mich bei meinen Promotionskollegen Anna Wernz, Henrik Haeger und Christoph Schönnenbeck für die Unterstützung in dieser Zeit bedanken.

Kapitel 2

Codierungstheorie

Fehlerkorrigierende Codes werden benutzt, um Daten, die über einen gestörten Kanal gesendet werden, so zu kodieren, dass der Empfänger mögliche Fehler bei der Übermittlung korrigieren kann. Die Suche nach Codes, die möglichst viele Fehler korrigieren können, ohne dabei zu ineffizient zu sein, ist das Hauptproblem der Codierungstheorie. In der klassischen, linearen Codierungstheorie ist ein Code C der Länge n über einem endlichen Körper $\mathbb{F}$ ein $\mathbb{F}$-linearer Teilraum von $\mathbb{F}^n$. Die Dimension $\dim(C)$ von C ist die Dimension als $\mathbb{F}$-Vektorraum. Für eine Basis $(b_1, \ldots, b_k)$ von C heißt die Matrix

$$\begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} \in \mathbb{F}^{k \times n}$$

Erzeugermatrix. Der Code, der von den Zeilen einer Matrix $G \in \mathbb{F}^{k \times n}$ erzeugt wird, wird mit $\langle G \rangle$ bezeichnet. Das (Hamming-)Gewicht $\mathrm{wt}(c)$ eines Codewortes $c = (c_1, \ldots, c_n) \in C$ ist die Anzahl der Einträge, die nicht Null sind, d.h.

$$\mathrm{wt}(c) := |\{1 \leq i \leq n \mid c_i \neq 0\}|.$$

Dann ist der (Hamming-)Minimalabstand von C

$$d := d(C) := \min\{\mathrm{wt}(c) \mid 0 \neq c \in C\}.$$

Ein Code der Länge n mit Dimension k und Minimalabstand d wird auch als $[n, k, d]$-Code bezeichnet. Zu einem Code mit Basis $(b_1, \ldots, b_k)$ ist der erweiterte Code das Erzeugnis von

$$\begin{pmatrix} b_1 & -\sum_{i=1}^{n} b_{1,i} \\ \vdots & \vdots \\ b_k & -\sum_{i=1}^{n} b_{k,i} \end{pmatrix} \in \mathbb{F}^{k \times (n+1)},$$

d.h. es wird eine Koordinate hinzugefügt, so dass die Summe der Einträge Null ist. Der Gewichtszähler ist das normierte, homogene Polynom

$$\mathrm{we}_C(x, y) = \sum_{c \in C} x^{n - \mathrm{wt}(c)} y^{\mathrm{wt}(c)} \in \mathbb{C}[x, y]$$

und der vollständige Gewichtszähler

$$\mathrm{cwe}_C(x_a \mid a \in \mathbb{F}) := \sum_{c \in C} \prod_{i=1}^{n} x_{c_i} \in \mathbb{C}[x_a \mid a \in \mathbb{F}]$$

unterscheidet zusätzlich zwischen den Körperelementen. Es gilt die Relation $\mathrm{we}_C(x, y) = \mathrm{cwe}_C(x, y, \ldots, y)$. Die monomiale Gruppe vom Grad n von $\mathbb{F}$ ist

$$\mathrm{Mon}_n(\mathbb{F}) := \mathbb{F}^* \wr S_n = (\mathbb{F}^*)^n \rtimes S_n,$$

wobei jedes $\sigma \in \mathrm{Mon}_n(\mathbb{F})$ eine eindeutige Darstellung hat als

$$\sigma = m(\sigma)\pi(\sigma)$$

mit $m(\sigma) = \mathrm{diag}(a_1, \ldots, a_n)$, $a_i \in \mathbb{F}^*$, und $\pi(\sigma) \in S_n$. Diese Gruppe operiert auf $\mathbb{F}^n$ von rechts durch die übliche Matrixmultiplikation bzw. durch Permutation der Koordinaten. Die Permutationen $\pi(\sigma) \in S_n$ werden im weiteren Verlauf der Arbeit je nach Kontext als Permutation auf $\{1, \ldots, n\}$ oder als Permutationsmatrix geschrieben. Die Automorphismengruppe $\mathrm{Aut}(C)$ eines Codes $C \leq \mathbb{F}^n$ ist der Stabilisator von C in $\mathrm{Mon}_n(\mathbb{F})$, also

$$\mathrm{Aut}(C) := \{\sigma \in \mathrm{Mon}_n(\mathbb{F}) \mid c \cdot \sigma \in C \text{ für alle } c \in C\}.$$

Für einen Automorphismus $\sigma \in \mathrm{Aut}(C)$ ist der Fixcode

$$C(\sigma) := \{c \in C \mid c \cdot \sigma = c\}.$$

Sei $\overline{\ } : \mathbb{F} \to \mathbb{F}$ ein selbst-inverser Körperautomorphismus, dann ist

$$x \cdot y := \sum_{i=1}^{n} x_i \overline{y_i}$$

das Standard (hermitesche) innere Produkt auf $\mathbb{F}^n$. Der duale Code $C^\perp$ von C ist definiert als

$$C^\perp := \{v \in \mathbb{F}^n \mid v \cdot c = 0 \text{ für alle } c \in C\},$$

ein linearer Code von Dimension $n - \dim(C)$. Im Fall $C \subseteq C^\perp$ heißt C selbst-orthogonal, im Fall $C = C^\perp$ heißt C selbst-dual.

Satz 2.1 (MacWilliams-Identität, [MS77, Chapter 5]). *Sei $C \leq \mathbb{F}^n$ ein Code mit Gewichtszähler $\mathrm{we}_C(x, y)$, dann ist der Gewichtszähler des dualen Codes $C^\perp$ gleich*

$$\mathrm{we}_{C^\perp}(x, y) = \frac{1}{|C|} \mathrm{we}_C(x + |\mathbb{F}^*|y, x - y).$$

Selbst-duale Codes bilden eine wichtige Klasse von Codes. Zum einen sind viele Beispiele guter Codes (also Codes mit hohem Minimalabstand) selbst-dual, zum anderen sind sie eng mit anderen mathematischen Theorien verbunden.

So konnte zum Beispiel mit Hilfe selbst-dualer Codes gezeigt werden, dass eine projektive Ebene der Ordnung 10 nicht existiert ([LTS89]). Betrachtet man den Gewichtszähler eines selbst-dualen Codes als Element im Invariantenring einer bestimmten Gruppe, lassen sich obere Abschätzungen für den Minimalabstand beweisen (Abschnitt 2.1). Anwendungen finden sich auch in der Theorie der Gitter, Sphärischen Designs, Gruppentheorie und weiteren mehr.

Satz 2.2 ([HP03, Theorem 9.1.3]). *Ein selbst-dualer Code von gerader Länge n über einem Körper $\mathbb{F}$ existiert genau dann, wenn $(-1)^{\frac{n}{2}}$ ein Quadrat in $\mathbb{F}$ ist. Falls n gerade ist und $(-1)^{\frac{n}{2}}$ kein Quadrat in $\mathbb{F}$ ist, dann ist die Dimension eines maximal selbstorthogonalen Codes $\frac{n}{2}-1$. Falls n ungerade ist, ist diese Dimension $\frac{n-1}{2}$.*

Lemma 2.3 (Balance principle, [HP03, Theorem 9.4.1]). *Sei $C = C^{\perp} \leq \mathbb{F}^n$ ein selbst-dualer Code und sei $n = n_1 + n_2$. Dann hat C eine Erzeugermatrix der Form*

$$\begin{pmatrix} B & 0 \\ 0 & D \\ E & F \end{pmatrix} \text{ mit } B \in \mathbb{F}^{k_1 \times n_1},\ D \in \mathbb{F}^{k_2 \times n_2},\ k_3 = \frac{n}{2} - k_1 - k_2 = \operatorname{Rang}(E) = \operatorname{Rang}(F).$$

Definiere

$$\mathcal{B} := \langle \begin{pmatrix} B & 0 \end{pmatrix} \rangle,\ \mathcal{B}^* := \langle B \rangle,\ \mathcal{B}_E := \langle \begin{pmatrix} B \\ E \end{pmatrix} \rangle,\ \mathcal{D}^* := \langle D \rangle \text{ und } \mathcal{D}_F := \langle \begin{pmatrix} D \\ F \end{pmatrix} \rangle.$$

Dann gilt $\mathcal{B}_E^{\perp} = \mathcal{B}^*$ und $\mathcal{D}_F^{\perp} = \mathcal{D}^*$.

2.1 Selbst-duale und extremale Codes

In diesem Abschnitt werden obere Abschätzungen für den Minimalabstand selbst-dualer Codes beschrieben, die die Singleton-Schranke

$$d(C) \leq n - \dim(C) + 1$$

verbessern. Die wichtigste Eigenschaft selbst-dualer Codes über kleinen Körpern ist durch den Satz von Gleason gegeben (Satz 2.5), welcher mit Hilfe der Invariantentheorie bewiesen wird. Als Konsequenz aus dem folgenden Satz von Gleason-Pierce-Ward beschränkt man sich in erster Linie auf die Körper $\mathbb{F}_2$, $\mathbb{F}_3$ und $\mathbb{F}_4$.

Satz 2.4 (Gleason-Pierce-Ward). *Sei $C \leq \mathbb{F}^n$ ein Code der Dimension $\frac{n}{2}$, so dass ein $a \in \mathbb{N}_{\geq 2}$ existiert mit $\operatorname{wt}(c) \equiv 0 \pmod{a}$ für alle $c \in C$. Dann tritt einer der folgenden Fälle ein:*

i) $q = 2$ *und* $a = 2$,

ii) $q = 2$, $a = 4$ *und C ist selbst-dual*,

iii) $q = 3$, $a = 3$ *und C ist selbst-dual*,

iv) $q = 4$, $a = 2$ *und* C *ist hermitesch selbst-dual,*

v) $a = 2$ *und* C *ist isomorph zu einem Code mit Erzeugermatrix* $\begin{pmatrix} I_{\frac{n}{2}} & I_{\frac{n}{2}} \end{pmatrix}$.

Dieser Satz ist eine Verallgemeinerung des Satzes von Gleason-Pierce, welcher die zusätzliche Voraussetzung hat, dass C formal selbst-dual ist, d.h. C und der duale Code $C^\perp$ haben denselben Gewichtszähler. Selbst-duale Codes, welche die Fälle *ii)*, *iii)* bzw. *iv)* erfüllen, heißen Typ II, Typ III, bzw. Typ IV Codes. Es existieren binäre Codes, deren Codewörter alle gerades Gewicht haben, welche aber nicht selbst-dual sind. Die binären Codes, welche selbst-dual, aber keine Typ II Codes sind, heißen Typ I Codes. Der Satz von Gleason-Pierce-Ward liefert nun zusammen mit der MacWilliams-Identität eine wichtige Einschränkung an den Gewichtszähler eines selbst-dualen Codes:
Sei C ein Typ I, Typ II, Typ III, bzw. Typ IV Code über $\mathbb{F}_q$, dann ist der Hamming-Gewichtszähler $\mathrm{we}_C(x, y)$ von C invariant unter der Gruppe

$$G := \langle \begin{pmatrix} 1 & \\ & \omega \end{pmatrix}, \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & 1 \\ q-1 & -1 \end{pmatrix} \rangle \leq \mathrm{GL}_2(\mathbb{C}),$$

wobei ω eine primitive a-te Einheitswurzel ist, mit $a \in \mathbb{N}$ wie in Satz 2.4. Der Gewichtszähler ist also im Invariantenring

$$\mathrm{Inv}(G) := \{p(x, y) \in \mathbb{C}[x, y] \mid p((x, y) \cdot g) = p(x, y) \text{ für alle } g \in G\}$$

von G enthalten. Dieser Invariantenring ist in all diesen Fällen ein Polynomring in algebraisch unabhängigen Gewichtszählern gewisser Codes.

Satz 2.5 (Gleason)**.** *Sei* C *ein selbst-dualer Code von einem der vier Typen. Dann ist der Gewichtszähler* $\mathrm{we}_C(x, y)$ *in dem Polynomring* $\mathbb{C}[p_1, p_2]$ *enthalten, wobei die Polynome* $p_1, p_2 \in \mathbb{C}[x, y]$ *als Gewichtszähler folgender Codes gewählt werden können:*

Typ	p_1	p_2
I	i_2	Hamming-Code h_8
II	Hamming-Code h_8	binärer erweiterter Golay-Code g_{24}
III	Tetracode	ternärer erweiterter Golay-Code
IV	$i_2 \otimes \mathbb{F}_4$	Hexacode

Daraus folgt inbesondere die Aussage von Satz 2.2 für die Typen I, III und IV, denn z.B. im Fall Typ III haben die beiden Polynome p_1 bzw. p_2 den Grad 4 bzw. 8, insbesondere muss also auch der Grad eines Gewichtszählers durch 4 teilbar sein. Für diese Längen existiert aber immer ein selbst-dualer Code, z.B. orthogonale Kopien des Tetracodes von Dimension 4. Damit existiert ein ternärer, selbst-dualer Code der Länge n genau dann, wenn $n \equiv 0 \pmod 4$ ist. Mit derselben Argumentation folgt, dass ein Typ II genau für die Längen $n \equiv 0 \pmod 8$ existiert.

Die Existenz dieser sogenannten Gleason-Polynome wurde in [MS73] und [Mac+78] benutzt, um eine obere Abschätzung für den Minimalabstand von Typ

I bis IV Codes zu zeigen. Sei $\mathbb{Q}[p_1, p_2]_n$ der Vektorraum aller Polynome vom Grad n in der graduierten Algebra $\mathbb{Q}[p_1, p_2]$ und sei $r = r(n) \in \mathbb{N}$ maximal, so dass ein Objekt der Form

$$x^n + \sum_{i=r}^{n} a_i x^{n-i} y^i$$

in $\mathbb{Q}[p_1, p_2]_n$ existiert. Dieser sogenannte extremale Gewichtszähler ist eindeutig und kann konkret angegeben werden, insbesondere ist der höchstmögliche Minimalabstand eines selbst-dualen Codes also gerade r. Das ergibt die folgenden Abschätzungen.

Satz 2.6. *Sei C ein selbst-dualer Code mit Minimalabstand d.*

i) Falls C vom Typ I ist, gilt $d \leq 2\left\lfloor \frac{n}{8} \right\rfloor + 2$.

ii) Falls C vom Typ II ist, gilt $d \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 4$.

iii) Falls C vom Typ III ist, gilt $d \leq 3\left\lfloor \frac{n}{12} \right\rfloor + 3$.

iv) Falls C vom Typ IV ist, gilt $d \leq 2\left\lfloor \frac{n}{6} \right\rfloor + 2$.

Die naheliegende Frage ist nun, welche Codes diese Schranken annehmen und ob diese überhaupt existieren. Eine notwendige Voraussetzung hierfür ist natürlich, dass alle Koeffizienten des extremalen Gewichtszählers nicht-negativ sind. Für die Typen II, III und IV wurde hierfür in [RS98b] untersucht, wann der Koeffizient a_{d+a} des extremalen Gewichtszählers

$$x^n + a_d x^{n-d} y^d + a_{d+a} x^{n-d-a} y^{d+a} + \sum_{i=d+2a}^{n} a_i x^{n-i} y^i$$

negativ wird.

Satz 2.7. *i) Ein Typ II Code mit $d = 4\left\lfloor \frac{n}{24} \right\rfloor + 4$ existiert nicht für $n \geq 3936$.*

ii) Ein Typ III Code mit $d = 3\left\lfloor \frac{n}{12} \right\rfloor + 3$ existiert nicht für $n = 72, 96, 120$ und $n \geq 144$.

iii) Ein Typ IV Code mit $d = 2\left\lfloor \frac{n}{6} \right\rfloor + 2$ existiert nicht für $n \geq 132$.

In [War76] zeigte H. N. Ward, dass ein Typ I Code mit $d = 2\left\lfloor \frac{n}{8} \right\rfloor + 2$ nur für die Längen $n = 2, 4, 6, 8, 12, 14, 22$ und 24 existiert. In [Rai98] konnte E. M. Rains die Abschätzung schließlich für Typ I Codes mit Hilfe des sogenannten Schatten eines Codes erheblich verbessern.

Satz 2.8. *Sei C ein Typ I Code mit Minimalabstand d. Dann gilt*

$$d \leq \begin{cases} 4\left\lfloor \frac{n}{24} \right\rfloor + 4 & \text{falls } n \not\equiv 22 \pmod{24} \\ 4\left\lfloor \frac{n}{24} \right\rfloor + 6 & \text{falls } n \equiv 22 \pmod{24}. \end{cases}$$

Im Fall $n \equiv 0 \pmod{24}$ und $d = 4\left\lfloor \frac{n}{24} \right\rfloor + 4$ ist C bereits ein (extremaler) Typ II Code.

Definition 2.9. *Ein selbst-dualer Code C, dessen Minimalabstand die Abschätzung von Satz 2.6 bzw. Satz 2.8 annimmt, heißt extremal.*

Die nachfolgenden Tabellen verdeutlichen den aktuellen Stand der Klassifikation extremaler Codes und sind für moderate Längen aktualisierte Versionen der Tabellen, welche in [HP03, Table 9.1, Table 9.2 und Table 9.3], angegeben sind. Ein Eintrag der Form d^E bzw. d^O bedeutet, dass die Codes extremal bzw. optimal (d.h. kein Code mit höherem Minimalabstand existiert) sind, ein zusätzlicher Eintrag in Klammern bedeutet, dass bisher nicht bekannt ist, ob ein extremaler Code existiert oder nicht. Für die vollständigen Klassifikationen sind zusätzlich die Referenzen angegeben. Bis auf wenige Ausnahmen folgt die Klassifikation extremaler Codes aus der Klassifikation selbst-dualer Codes.

n	d_{max}	Anzahl	Referenz	n	d_I	Anzahl	Referenz
2	2^O	1	[Ple72]	38	8^E	2744	[Agu+12]
4	2^O	1	[Ple72]	40	8^E	$\sim 10^7$	[BBH13]
6	2^O	1	[Ple72]	42	8^E	≥ 30	
8	2^O	1	[Ple72]	44	8^E	≥ 108	
10	2^O	2	[Ple72]	46	10^E	≥ 1	
12	4^E	1	[Ple72]	48	10^E	≥ 7	
14	4^E	1	[Ple72]	50	10^O	≥ 6	
16	4^E	1	[Ple72]	52	10^O	≥ 499	
18	4^E	2	[Ple72]	54	10^O	≥ 54	
20	4^E	7	[Ple72]	56	12^E	?	
22	6^E	1	[PS75]	58	10^O	≥ 101	
24	6^E	1	[PS75]	60	12^E	≥ 5	
26	6^O	1	[CPS92]	62	12^E	≥ 1	
28	6^O	3	[CPS92]	64	12^E	≥ 5	
30	6^O	13	[CPS92]	66	12^E	≥ 3	
32	8^E	3	[BR02]	68	12^E	≥ 65	
34	6^0	938	[Bil06]	70	14^E	?	
36	8^E	41	[HM12]	72	14^E	?	

TABELLE 2.1: Anzahl der extremalen bzw. optimalen Codes vom Typ I

n	d_{max}	Anzahl	Referenz
8	4^E	1	[Ple72]
16	4^E	2	[Ple72]
24	8^E	1	[PS75]
32	8^E	5	[CPS92]
40	8^E	16470	[BHM12]
48	12^E	1	[Hou+03]
56	12^E	≥ 166	
64	12^E	≥ 3270	
72	$12(16^E)$	?	

TABELLE 2.2: Anzahl der extremalen bzw. optimalen Codes vom Typ II

n	d_{max}	Anzahl	Referenz	n	d_{max}	Anzahl	Referenz
4	3^E	1	[MPS76]	40	12^E	≥ 20	
8	3^E	1	[MPS76]	44	12^E	≥ 8	
12	6^E	1	[MPS76]	48	15^E	≥ 2	
16	6^E	1	[CPS79]	52	15^E	≥ 1	[GO03]
20	6^E	6	[PSW80]	56	15^E	≥ 1	
24	9^E	2	[HM09]	60	18^E	≥ 2	
28	9^E	6931	[HMV09]	64	18^E	≥ 1	
32	9^E	≥ 239		68	$15(18^E)$	?	
36	12^E	≥ 1		72	18^O	≥ 1	

TABELLE 2.3: Anzahl der extremalen bzw. optimalen Codes vom Typ III

n	d_{max}	Anzahl	Referenz	n	d_{max}	Anzahl	Referenz
2	2^E	1	[Mac+78]	18	8^E	1	[BÖ06]
4	2^E	1	[Mac+78]	20	8^E	2	[HM11]
6	4^E	1	[Mac+78]	22	8^E	≥ 46	
8	4^E	1	[Mac+78]	24	8^O	≥ 17	
10	4^E	2	[Mac+78]	26	$8(10^E)$	?	
12	4^O	5	[Mac+78]	28	10^E	≥ 3	
14	6^E	1	[Mac+78]	30	12^E	≥ 1	
16	6^E	4	[CPS79]				

TABELLE 2.4: Anzahl der extremalen bzw. optimalen Codes vom Typ IV

Ab den frühen 1990er Jahren wurden diese vier Typen um weitere Klassen von Codes erweitert. Erst wurden verstärkt Codes über $\mathbb{Z}/4\mathbb{Z}$ untersucht, da gewisse nicht-lineare, binäre Codes als lineare Codes über $\mathbb{Z}/4\mathbb{Z}$ betrachtet werden können. Im späteren Verlauf wurden zusätzlich selbst-duale Codes über $\mathbb{Z}/m\mathbb{Z}$,

additive Codes über $\mathbb{F}_4$, hermitesche Codes über $\mathbb{F}_q$ und weitere Klassen betrachtet ([RS98b]). Für jeden Typ wurde eine MacWilliams-Identität und eine Art Satz von Gleason gezeigt, allerdings wurde in den Beweisen jeder Typ separat betrachtet. In [NRS06] wurde schließlich der Begriff des Typs eines Codes stark verallgemeinert. Hier ist das Alphabet ein Links-R-Modul V mit einer Menge von biadditiven bzw. quadratischen Formen, welche Dualität bzw. zusätzliche Eigenschaften wie doppelt-gerade definieren. Die Codes vom Typ T der Länge N bilden eine Familie von Codes, welche selbst-orthogonal bzgl. einer biadditiven Form und isotrop bzgl. der quadratischen Formen sind. Auf diesen existiert eine verallgemeinerte MacWilliams-Identität und es lässt sich eine komplexe Matrixgruppe angegeben, die Clifford-Weil-Gruppe, unter dieser die betrachteten Gewichtszähler invariant sind. Die Hauptaussage ist nun, dass für eine breite Klasse an Codes (u.a. über jedem endlichen Körper), der Invariantenring dieser Clifford-Weil-Gruppe von den Gewichtszählern der Codes des entsprechenden Typs erzeugt wird, was eine starke Verallgemeinerung des Satz von Gleason ist und die einzelnen Betrachtungen der verschiedenen Typen zusammenführt.

Beispiel 2.10. *Sei $C \leq \mathbb{F}_3^{48}$ ein extremaler Code der Länge 48, d.h. ein selbst-dualer Code mit Minimalabstand 15. Aus der Eindeutigkeit des Hamming-Gewichtszählers folgt, dass C 96 Codewörter mit vollem Gewicht enthält. Falls C das Wort*

$$\boldsymbol{1} = (1, \ldots, 1) \in \mathbb{F}_3^{48}$$

enthält (was nach monomialer Transformation angenommen werden kann), ist der vollständige Gewichtszähler $\mathrm{cwe}_C(x_0, x_1, x_{-1})$ im Invariantenring der Clifford-Weil-Gruppe

$$\mathcal{C}(\rho(3_{\boldsymbol{1}})) = \langle \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \begin{pmatrix} 1 & & \\ & & 1 \\ & 1 & \end{pmatrix}, \begin{pmatrix} 1 & & \\ & \omega & \\ & & \omega \end{pmatrix}, \begin{pmatrix} 1 & & \\ & \omega & \\ & & \omega^2 \end{pmatrix} \rangle \leq \mathrm{GL}_3(\mathbb{C})$$

enthalten ([NRS06, Section 7.4.1]), wobei $\omega \in \mathbb{C}$ eine primitive dritte Einheitswurzel ist. Der $\mathbb{Q}$-Vektorraum aller invarianten Polynome vom Grad 48 mit rationalen Koeffizienten hat Dimension 10. In diesem existiert ein eindeutiges Element, so dass

1) *alle Koeffizienten nicht-negativ sind,*
2) *der Koeffizient von x_0^{48} gleich 1 ist und*
3) *der Koeffizient von allen $x_0^i x_1^j x_{-1}^k$ mit $0 < j + k < 15$ gleich 0 ist.*

Für die 96 Wörter mit vollem Gewicht ergibt sich die Verteilung

$$x_1^{48} + x_{-1}^{48} + 94 \cdot x_1^{24} x_{-1}^{24}.$$

2.2 Beispiele von Codes

In den Klassifikationen von Kapitel 4 sind besonders zwei Familien von Codes von Bedeutung, der quadratische Restklassen-Code und der Pless-Code (siehe auch [MS77, Kapitel 16] und [Ple70]).

Quadratische Restklassen-Codes (QR-Codes)

Die quadratischen Restklassen-Codes („quadratic residue", QR) sind zyklische Codes der Länge p über $\mathbb{F}_l$, wobei l und p Primzahlen sind, so dass l ein quadratischer Rest modulo p ist. Sei $\zeta \in \mathbb{F}_p$ ein primitives Element, dann ist

$$Q := \langle \zeta^2 \rangle \leq \mathbb{F}_p^*$$

die Menge der Quadratischen Rest modulo p und entsprechend ist

$$N := \mathbb{F}_p^* \setminus Q$$

die Menge der quadratischen Nicht-Reste. Sei $\alpha \in \overline{\mathbb{F}_l}$ eine p-te primitive Einheitswurzel und definiere

$$q(x) := \prod_{r \in Q} (x - \alpha^r) \text{ und}$$
$$r(x) := \prod_{n \in N} (x - \alpha^n).$$

Es gilt $q(x), r(x) \in \mathbb{F}_l[x]$ und $x^p - 1 = (x-1)q(x)n(x)$, da Q die Vereinigung von zyklotomischen Klassen modulo p ist.

Definition 2.11. *Die quadratischen Restklassen-Codes $\mathcal{Q}$, $\overline{\mathcal{Q}}$, $\mathcal{N}$ bzw. $\overline{\mathcal{N}}$ sind zyklische Codes der Länge p über $\mathbb{F}_l$ mit Erzeugerpolynomen*

$$q(x),\ (x-1)q(x),\ n(x) \text{ bzw. } (x-1)n(x).$$

Die Codes $\mathcal{Q}$ und $\mathcal{N}$ heißen auch erweiterte QR-Codes, und die Codes $\overline{\mathcal{Q}}$ und $\overline{\mathcal{N}}$ bereinigte QR-Codes. Die Koordinatenpermutation $x \mapsto x^a$, für einen quadratischen Nicht-Rest a, vertauscht $\mathcal{Q}$ und $\mathcal{N}$ bzw. $\overline{\mathcal{Q}}$ und $\overline{\mathcal{N}}$, die Codes sind also äquivalent und von Dimension $\frac{1}{2}(p+1)$ bzw. $\frac{1}{2}(p-1)$. Für den Minimalabstand gilt $d \geq \sqrt{p}$.

So ist zum Beispiel der [7,4,3] Hamming-Code ein QR-Code mit Erzeugerpolynom

$$(x+1)(x^3+x+1),$$

der [23,12,7] binäre Golaycode $\mathcal{G}_{23}$ ist ebenfalls ein QR-Code mit Erzeugerpolynom

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

Bemerkung 2.12. *Seien $\hat{\mathcal{Q}}, \hat{\mathcal{N}}$ die erweiterten Codes von $\mathcal{Q}$ bzw. $\mathcal{N}$. Im Fall $p = 4k-1$ gilt*

$$\mathcal{Q}^{\perp} = \overline{\mathcal{Q}},\ \mathcal{N} = \overline{\mathcal{N}},$$

und $\hat{\mathcal{Q}}$ bzw. $\hat{\mathcal{N}}$ sind selbst-dual, im Fall $p = 4k+1$ gilt

$$\mathcal{Q}^{\perp} = \overline{\mathcal{N}}, \mathcal{N}^{\perp} = \overline{\mathcal{Q}}$$

und $\hat{\mathcal{Q}}^{\perp} = \mathcal{N}$.

Bemerkung 2.13. *Die Automorphismengruppe des erweiterten QR-Codes $\hat{\mathcal{Q}}$ enthält die Gruppe $\mathrm{PSL}_2(p)$.*

Der Pless-Code

Sei p eine Primzahl mit $p \equiv -1 \pmod 6$ und sei $S \in \mathbb{F}_3^{(p+1)\times(p+1)}$ die Matrix

$$S = \begin{pmatrix} 0 & 1 & 1 & \dots & 1 & 1 \\ \epsilon & & & & & \\ \epsilon & & & & & \\ \vdots & & & D & & \\ \epsilon & & & & & \\ \epsilon & & & & & \end{pmatrix},$$

mit $\epsilon = 1$ falls $p = 4k+1$ bzw. $\epsilon = -1$ falls $p = 4k-1$. Die Matrix D ist zirkulant und gegeben durch ihre erste Zeile

$$(0, a_1, \dots, a_{p-1}),$$

wobei $a_i = 1$, falls i ein quadratischer Rest modulo p ist, und -1 sonst.

Definition 2.14. *Der Pless-Code P_{2p+2} ist ein $[2p+2, p+1]$ Code über $\mathbb{F}_3$ mit Erzeugermatrix*

$$\begin{pmatrix} I_{p+1} & S \end{pmatrix}.$$

Dieser Code ist doppelt-zirkulant und selbst-dual.

Bemerkung 2.15. *Die Automorphismengruppe des Codes P_{2p+2} enthält die Gruppe $\mathrm{PSL}_2(p)$.*

Die ersten fünf Pless-Codes haben die Parameter

$$[12, 6, 6],\ [25, 12, 9],\ [36, 18, 12],\ [48, 24, 15] \text{ und } [60, 30, 18],$$

insbesondere sind diese also extremal.

2.3 Klassifikation von Codes mit Automorphismen

Automorphismen spielen bei der Untersuchung von selbst-dualen bzw. extremalen Codes eine wichtige Rolle, da häufig durch die zusätzliche Struktur eine

Klassifikation erst ermöglicht wird. Binäre Codes mit einem Automorphismus von ungerader Primordnung bzw. von Ordnung 2 wurden zuerst in [CP82], [Huf82] und [Ĭor83] bzw. in [Bou96] und [Bou00] untersucht. Insbesondere bei der Suche nach einem binären, extremalen $[72, 36, 16]$-Code wurden hier viele Methoden entwickelt. Die grundlegende Idee ist, dass die Operation einer Gruppe $G \leq \mathrm{Mon}_n(\mathbb{F})$ den Raum $\mathbb{F}^n$ in G-invariante, orthogonale Summen aufspaltet, dadurch reduziert sich die Klassifikation selbst-dualer Codes, für die G in der Automorphismengruppe enthalten ist, auf die Klassifikation von gewissen Teilcodes.

Sei $C \leq \mathbb{F}^n$ ein Code der Länge n und sei $G \leq \mathrm{Aut}(C)$, dann ist C ein Teilmodul des (Rechts-)$\mathbb{F}G$-Moduls $\mathbb{F}^n$. Sei $\hat{} : \mathbb{F}G \to \mathbb{F}G$ der Antialgebrenautomorphismus auf $\mathbb{F}G$, welcher $G \to G, g \mapsto g^{-1}$ $\mathbb{F}$-linear fortsetzt. Für eine Zerlegung

$$1 = f_1 + \cdots + f_t$$

in zentrale Idempotente $f_i \in \mathbb{F}G$ mit $\hat{f}_i = f_i$ gilt

$$\mathbb{F}Gf_i \cong (\mathbb{F}Gf_i)^* \text{ als } \mathbb{F}G\text{-Moduln.}$$

Sei nun $C_i = Cf_i$ für $i = 1, \ldots, t$, dann gilt $\mathbb{F}^n = \mathbb{F}^n f_1 \perp \cdots \perp \mathbb{F}^n f_t$ und $C = C_1 \perp \cdots \perp C_t$ als $\mathbb{F}G$-Moduln und zusätzlich ist für einen selbst-dualen Code C in $\mathbb{F}^n$ der Code C_i selbst-dual in $\mathbb{F}^n f_i$.

Somit können alle solche Codes C klassifiziert werden, in dem alle Kandidaten für die Teilcodes C_i bestimmt und orthogonale Summe gebildet werden.
Im folgenden wird der Spezialfall beschrieben, dass $G = \langle g \rangle$ eine zyklische Gruppe von Primordnung p ist. Als Anwendung werden Codes in einer bestimmten Teilklasse der selbst-dualen doppelt-zyklischen Codes gezählt (Abschnitt 2.3).

Satz 2.16. *Falls p nicht $|\mathbb{F}^*|$ teilt, ist g in $\mathrm{Mon}_n(\mathbb{F})$ konjugiert zu $\pi(g) \in S_n$.*

Beweis. Sei $H \leq \mathrm{Mon}_n(\mathbb{F})$ die Gruppe, die von

$$N := \{\mathrm{diag}(a_1, \ldots, a_n) \mid a_i \in \mathbb{F}^*\}$$

und $\langle g \rangle$ erzeugt wird. Dann ist N ein Normalteiler in H der Ordnung $|\mathbb{F}^*|^n$ und es gilt

$$H/N = \langle \pi(g) + N \rangle.$$

Da p nicht $|\mathbb{F}^*|$ teilt, muss die Ordnung von $\pi(g)$ gleich p sein, insbesondere sind die Ordnungen von N und H/N teilerfremd. Sei nun $U_1 = \langle g \rangle$ und $U_2 = \langle \pi(g) \rangle$, dann gilt $H = NU_1 = NU_2$ und $N \cap U_1 = N \cap U_2 = \{1\}$. Nach dem Satz von Schur-Zassenhaus sind dann U_1 und U_2 in H konjugiert zueinander, daraus folgt die Behauptung. □

Bemerkung 2.17. *Falls p die Ordnung von $\mathbb{F}^*$ teilt, ist g in $\mathrm{Mon}_n(\mathbb{F})$ konjugiert zu*

$$\left(\begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ 1 & & & \end{pmatrix}^t, 1^{n_0}, (\zeta)^{n_1}, \ldots, \left(\zeta^{p-1}\right)^{n_{p-1}} \right),$$

wobei $\zeta \in \mathbb{F}^*$ ein Element der Ordnung p ist.

Bemerkung 2.18. *Im Fall $p \neq \mathrm{char}(\mathbb{F})$ und $g \in S_n$ sei ohne Einschränkung*

$$g = (1, \ldots, p)(p+1, \ldots, 2p) \ldots ((t-1)p+1, \ldots, tp)(tp+1) \ldots (n) \in S_n.$$

Dann gilt $C = C(g) \oplus E$, wobei

$$C(g) = \{c \in C \mid c_1 = \cdots = c_p, c_{p+1} = \cdots = c_{2p}, \ldots, c_{(t-1)p+1} = \cdots = c_{tp}\}$$

der Fixcode von g ist und

$$E = \left\{ c \in C \mid \sum_{i=1}^{p} c_i = \sum_{i=1}^{p} c_{p+i} = \cdots = \sum_{i=1}^{p} c_{(t-1)p+i} = c_{tp+1} = \cdots = c_n = 0 \right\}$$

ist das eindeutige g-invariante Komplement von $C(g)$ in C.

Es tritt also einer der folgenden Fälle ein, die entscheiden, welche Struktur ein Code C zusammen mit einem Automorphismus g hat:

i) p teilt $|\mathbb{F}^*|$,

ii) p teilt $\mathrm{char}(\mathbb{F})$ oder

iii) p teilt weder $|\mathbb{F}^*|$ noch $\mathrm{char}(\mathbb{F})$.

Der Fall p ist teilerfremd zu $\mathrm{char}(\mathbb{F})$ und $|\mathbb{F}^*|$

Sei $g \in \mathrm{Mon}_n(\mathbb{F})$ von Ordnung p, dann kann nach Satz 2.16 ohne Einschränkung angenommen werden, dass $g \in S_n \leq \mathrm{Mon}_n(\mathbb{F})$ gilt. Nach dem Satz von Maschke ist die Gruppenalgebra $\mathbb{F}[g]$ halbeinfach und isomorph zur direkten Summe von gewissen Matrixalgebren über (endlichen) Körpererweiterungen von $\mathbb{F}$, da diese abelsch sein müssen, zerfällt also $\mathbb{F}[g]$ in die direkte Summe von Körpern. Die allgemeine Zerlegungstheorie für Codes wurde von W. C. Huffman in [Huf88] entwickelt und in [Huf90], [Huf91] fortgeführt. Die zentral primitiven Idempotente der Gruppenalgebra $\mathbb{F}[g]$ (welche mit dem Chinesischem Restsatz berechnet werden können) liefern hier eine Zerlegung eines Codes in Teilcodes, die als lineare Codes kleinerer Länge über einer Körpererweiterung von $\mathbb{F}$ betrachtet werden können. Zusätzlich ist das Duale eines direkten Summands wieder ein direkter Summand. Sei

$$x^p - 1 = (x-1) \cdot p_1 \cdots p_m \in \mathbb{F}[x]$$

die Zerlegung von $x^p - 1$ in irreduzible Polynome über $\mathbb{F}[x]$, wobei alle nichttrivialen Faktoren $p_1(x), \ldots, p_m(x)$ denselben Grad $d = |\langle |\mathbb{F}| + p\mathbb{Z}\rangle|$ (d.h. die Ordnung von $|\mathbb{F}|$ in $(\mathbb{Z}/p\mathbb{Z})^*$) haben. Es existieren Polynome $a_0, a_1, \ldots, a_m \in \mathbb{F}[x]$, so dass

$$1 = \underbrace{a_0 \frac{x^p - 1}{x - 1}}_{=:\tilde{e}_0} + \sum_{i=1}^{m} \underbrace{a_i \frac{x^p - 1}{p_i}}_{=:\tilde{e}_i}$$

gilt. Dann sind die zentral primitiven Idempotente $e_0, e_1, \ldots, e_m \in \mathbb{F}G$ gegeben durch

$$e_i = \tilde{e}_i(g)$$

und es gilt $\mathbb{F}Ge_0 \cong \mathbb{F}$, bzw. $\mathbb{F}Ge_i \cong \mathbb{E}$, $i \geq 1$, für eine Körpererweiterung $\mathbb{E}$ vom Grad d von $\mathbb{F}$.

Die natürliche Involution auf $\mathbb{F}G$ ist gegeben durch

$$^- : \mathbb{F}G \to \mathbb{F}G, \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g g^{-1}.$$

Diese operiert auf den Idempotenten $e_0, e_1, \ldots, e_m$, wobei immer $\overline{e_0} = e_0$ gilt.

Bemerkung 2.19. *Es gilt $\overline{e_i} = e_i$ für alle $i \geq 1$, genau dann wenn $d = [\mathbb{E} : \mathbb{F}]$ gerade ist. Ansonsten gilt $\overline{e_i} \neq e_j$, $^-$ operiert also auf den Idempotenten als Involution mit einzigem Fixpunkt e_0.*

Angenommen, g hat t Zykel der Länge p und $f = n - tp$ Fixpunkte. Für einen Code $C = C(g) \oplus E \leq \mathbb{F}^n$ mit $g \in \mathrm{Aut}(C)$ gilt dann

$$C = \underbrace{Ce_0}_{=C(g)} \perp \underbrace{Ce_1 \perp \cdots \perp Ce_m}_{=E}.$$

und Ce_i, $i \geq 1$, kann als Code in $\mathbb{E}^t$ aufgefasst werden, der Fixcode $C(g)$ dann dementsprechend als Code in $\mathbb{F}^{t+f}$. Falls C selbst-dual ist, ist $C(g)$ ein selbstdualer Code in $\mathbb{F}^{t+f}$, insbesondere folgt $\dim_{\mathbb{F}}(C(g)) = \frac{t+f}{2}$. Falls d gerade ist, ist Ce_i ein hermitesch selbst-dualer Code in $\mathbb{E}^t$, im Allgemeinen gilt

$$(Ce_i)^\perp = Ce_j$$

für $\overline{e_i} = e_j$. Insbesondere gilt hier

$$\dim_{\mathbb{F}}(E) = \frac{dmt}{2} = \frac{t(p-1)}{2}.$$

Diese Theorie wurde zuerst von W. C. Huffman benutzt, um extremale Typ IV und Typ III Codes ([Huf90], [Huf91], [Huf92]) moderater Länge mit bestimmten Automorphismen zu klassifizieren, dies wurde danach in vielen anderen Papern aufgegriffen (siehe z.B. [Huf05, Table 2] für eine Auflistung im Fall der extremalen Typ I Codes).

Beispiel: Vierte-Potenz-Restklassen doppelt-zirkulante Codes

Die Konstruktion von Vierte-Potenz-Restklassen doppelt-zirkulante Codes leitet sich aus der von quadratischen Restklassen-Codes ab und wurde in [ZG15] eingeführt. In diesem Beispiel werden als Anwendung der obigen Theorie die selbst-dualen Codes dieser Klasse gezählt. Im folgenden ist p eine ungerade Primzahl und q eine Primpotenz, die teilerfremd zu p ist.

Definition 2.20 ([ZG15, Section II B.]). *Sei p eine ungerade Primzahl, sei s ein primitives Elememt von $\mathbb{F}_p$ und sei $N > 1$ ein Teiler von $p-1$. Dann sind die N-ten zyklotomischen Klassen $C_0, C_1, \ldots, C_{N-1}$ von $\mathbb{F}_p$ definiert als*

$$C_i = \{s^{jN+i} \mid 0 \leq j \leq \tfrac{p-1}{N} - 1\} \text{ für } 0 \leq i \leq N-1.$$

Definition 2.21 ([ZG15, Section II C.]). *Sei p eine ungerade Primzahl der Form $4k+1$ für eine ganze Zahl k und seien C_0, C_1, C_2, C_3 die 4-ten zyklotomischen Klassen. Für Elemente $m_0, m_1, m_2, m_3, m_4 \in \mathbb{F}_p$ ist die Matrix $C_p(m_0, m_1, m_2, m_3, m_4) \in \mathbb{F}_q^{p\times p}$ definiert über*

$$C_p(m_0, m_1, m_2, m_3, m_4)_{ij} = c_{ij},$$

wobei

$$c_{ij} = \begin{cases} m_0, & \text{falls } j = i \\ m_1, & \text{falls } j - i \in C_0 \\ m_2, & \text{falls } j - i \in C_1 \\ m_3, & \text{falls } j - i \in C_2 \\ m_4, & \text{falls } j - i \in C_3. \end{cases}$$

Dann gilt $C_p(1,0,0,0,0) = I_p$ und $C_p(1,1,1,1,1) = J_p$. Definiere zusätzlich

$$\begin{aligned} A_1 &:= C_p(0,1,0,0,0), \\ A_2 &:= C_p(0,0,1,0,0), \\ A_3 &:= C_p(0,0,0,1,0) \text{ und} \\ A_4 &:= C_p(0,0,0,0,1). \end{aligned}$$

Der Code

$$P_p(m_0, m_1, m_2, m_3, m_4) \leq \mathbb{F}_q^{p\times 2p}$$

mit Erzeugermatrix

$$\begin{pmatrix} I_p & m_0 I_p + m_1 A_1 + m_2 A_2 + m_3 A_3 + m_4 A_4 \end{pmatrix} \in \mathbb{F}_q^{p\times 2p}$$

heißt Vierte-Potenz-Restklassen doppelt-zirkulanter Code (im folgenden abgekürzt durch VPRdz-Code)

In [ZG15, Theorem 8] wurde ein Kriterium angegeben, um zu entscheiden, wann ein VPRdz-Code selbst-dual ist. Dies wurde benutzt, um verschiedene Familien von selbst-dualen Codes über endlichen Körpern mit Charakteristik 2 und 3 und

Ordnung ≤ 9 zu konstruieren. Die Beweise bzw. Rechnungen sind hierbei aber sehr technisch, und es werden kaum Struktureigenschaften der Codes benutzt.

Satz 2.22 ([ZG15, Theorem 26])**.** *Die Automorphismengruppe des Codes $P_p(m_0, m_1, m_2, m_3, m_4)$ enthält eine Untergruppe der Ordnung $\frac{p(p-1)}{4}$.*

Diese Gruppe soll nun benutzt werden, um selbst-duale VPRdz-Codes zu zählen.

Sei $\mathcal{V} = (\mathbb{F}_q \oplus \mathbb{F}_q)^{\mathbb{F}_p} \cong \mathbb{F}_q^{2p}$ und sei s ein primitives Element von $\mathbb{F}_p$. Dann operieren

$$\sigma : \mathbb{F}_p \to \mathbb{F}_p, a \mapsto a + 1 \text{ und}$$
$$\mu : \mathbb{F}_p \to \mathbb{F}_p, a \mapsto s \cdot a$$

auf $\mathcal{V}$ und es gilt $\langle \sigma, \mu \rangle \cong \mathrm{Aff}_1(\mathbb{F}_p)$. Sei

$$U = \langle \sigma, \gamma := \mu^4 \rangle \leq \mathrm{Aff}_1(\mathbb{F}_p)$$

von Ordnung $\frac{p(p-1)}{4}$. Ein Element $v \in \mathcal{V}$ wird durch

$$(v(0)_1, v(1)_1, \ldots, v(p-1)_1, v(0)_2, v(1)_2, \ldots, v(p-1)_2)$$

als Vektor in $\mathbb{F}_q^{2p}$ aufgefasst, dann operieren σ und μ auf $\mathbb{F}_q^{2p}$ durch Permutation der Koordinaten.

Lemma 2.23. *Ein Code $C \leq \mathcal{V}$ mit Erzeugermatrix $\begin{pmatrix} I_p & M \end{pmatrix}$ ist genau dann ein VPRdz-Code, wenn σ und γ Automorphismen von C sind, d.h. es gilt $U \leq \mathrm{Aut}(C)$.*

Beweis. Falls C ein VPRdz-Code ist, sind σ und γ Automorphismen von U. Sei nun $C = \langle \begin{pmatrix} I_p & M \end{pmatrix} \rangle \leq \mathcal{V}$ ein Code mit $U \leq \mathrm{Aut}(C)$. Dann wird die erste Zeile

$$(\underbrace{1, 0, \ldots, 0}_{p}, m_0, m_1, \ldots, m_{p-1})$$

der Erzeugermatrix fixiert. Zusätzlich muss für alle $0 \leq i \leq p-1$ gelten, dass $m_i = m_{\gamma(i)}$ ist, also muss $m_i = m_j$ gelten, falls i und j in der selben zyklotomischen Klasse C_k enthalten sind. Durch Anwenden von σ erhält man die restlichen Basisvektoren von C. Dies ist aber gerade die Konstruktion von Definition 2.21. □

Nun werden alle selbst-dualen VPRdz-Codes aufgezählt. Sei $C = \langle \begin{pmatrix} I_p & M \end{pmatrix} \rangle \leq \mathcal{V}$ ein solcher Code.

Bemerkung 2.24. *Der Fixcode $C(\sigma)$ von σ hat die Erzeugermatrix*

$$\begin{pmatrix} 1 & \ldots & 1 & a & \ldots & a \end{pmatrix} \in \mathbb{F}_q^{1 \times 2p}.$$

Da C selbst-dual ist, muss insbesondere $p(a^2 + 1) = 0 \in \mathbb{F}_q$ gelten. Da p und q teilerfremd sind, ist also schon $a^2 = -1$, so ein Element existiert nur in $\mathbb{F}_q$, wenn q eine Potenz von 2 oder wenn $q \equiv 1 \pmod 4$ ist.

Sei

$$\mathbb{F}_q[\sigma] = \mathbb{F}_q \oplus \underbrace{\mathbb{F}_{q^d} \oplus \cdots \oplus \mathbb{F}_{q^d}}_{m \text{ Komponenten}}$$

mit $d = \operatorname{ord}(q \mod p)$ und seien $\mathcal{E} := \{e_0, \ldots, e_m\}$ die zentral primitiven Idempotente von $\mathbb{F}_q[\sigma]$.

Bemerkung 2.25. *Es gilt $(Ce_i)^\perp = C\overline{e_i} \leq \mathcal{V}\overline{e_i}$. Falls $\bar{}$ trivial auf den Idempotenten operiert, ist $Ce_i \leq \mathcal{V}e_i$ selbst-dual mit Erzeugermatrix $\begin{pmatrix} 1 & a \end{pmatrix}$ für ein $a \in \mathbb{F}_{q^d}$ mit $\operatorname{Norm}(a) = -1$.*

Bemerkung 2.26. *Der Automorphismus γ operiert auf den Idempotenten $\mathcal{E}$ mit einzigem Fixpunkt e_0. Es gilt $e_i^\gamma = e_i$ für ein $i \geq 1$, genau dann wenn γ in $\langle \mu^m \rangle$ enthalten ist, genau dann wenn d von $\frac{p-1}{4}$ geteilt wird. Aus der Zerlegung von $\mathbb{F}_q[\sigma]$ folgt $p = md+1$ und mit*

$$\frac{d}{\frac{p-1}{4}} = \frac{4}{m}$$

gilt, dass d von $\frac{p-1}{4}$ geteilt wird, genau dan wenn 4 von m geteilt wird. Sei $\tilde{\gamma} \in S_m$ die Permutation von γ auf $\{e_1, \ldots, e_m\}$. Dann hat $\tilde{\gamma}$ genau t Zykel der Länge $\frac{m}{t}$. Aus $\dim_{\mathbb{F}_q} C(\gamma) = 5$ folgt, dass t ein Teiler von 4 ist. Falls γ trivial operiert, induziert γ einen Automorphismus $\gamma' \in \operatorname{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$. In diesem Fall ist

$$\begin{aligned} 5 = \dim_{\mathbb{F}_q} \mathbb{F}_q^p(\gamma) &= 1 + \sum_{i=1}^{m} \dim_{\mathbb{F}_q}(\mathbb{F}_q^p e_i)(\gamma) \\ &= 1 + \sum_{i=1}^{m} \dim_{\mathbb{F}_q}(\operatorname{Fix}(\gamma')) \\ &= 1 + m|\gamma'|. \end{aligned}$$

Also gilt $|\gamma'| = \frac{4}{m}$ und der Fixkörper ist $\mathbb{F}_{q^{\frac{4}{m}}}$.

Bemerkung 2.27. *Die Anzahl der Elemente $a \in \mathbb{F}_{q^d}$ mit $\operatorname{Norm}(a) = -1$ ist*

$$\begin{cases} q^{\frac{d}{2}} + 1, & \text{falls } d \text{ gerade} \\ 2, & \text{falls } d \text{ ungerade und } q \equiv 1 \pmod 4 \\ 0 & \text{sonst.} \end{cases}$$

Nun werden die Codes $E \leq \mathcal{V}$ gezählt, so dass $C = C(\sigma) \oplus E$ ein selbst-dualer VPRdz-Code ist.

1. Fall: $\bar{}$ und γ operieren trivial (d.h. d ist gerade und $m \mid 4$).
Die Anzahl der selbst-dualen Codes $Ce_i \leq \mathcal{V}e_i$ ist hier die Anzahl der Elemente

$a \in \mathbb{F}_{q^{\frac{4}{m}}}$ mit $\mathrm{Norm}(a) = -1$, also ist die Anzahl insgesamt

$$\begin{cases} q^2+1, & \text{falls } m = 1 \\ (q+1)^2, & \text{falls } m = 2 \\ 2^4 = 16, & \text{falls } m = 4. \end{cases}$$

2. Fall: $^-$ operiert trivial, γ operiert nicht trivial (d.h. d ist gerade und $m \nmid 4$).
Dann hat $\gamma' \in S_m$ genau t Zykel der Länge $\frac{m}{t}$, wobei t ein Teiler von 4 ist. Allerdings muss $\frac{m}{t}$ ungerade sein, sonst würde $\tilde{\gamma}^{\frac{m}{2t}}$ als Involution auf den Idempotenten operieren und d wäre ungerade. Also gilt $t = \nu_2(m)$. Auf jedem der t Zykel gibt es dann $q^{\frac{d}{2}} + 1$ Möglichkeiten für Ce_i, also ist die Anzahl insgesamt

$$\left(q^{\frac{d}{2}} + 1\right)^{\nu_2(m)}.$$

3. Fall: $^-$ operiert nicht trivial, γ operiert trivial (d.h. d ist ungerade und $m \mid 4$).
Da $p - 1 = md$ von 4 geteilt wird und d ungerade ist, wird m von 4 geteilt und es folgt $m = 4$. Teile nun die Idempotente $e_1, \ldots, e_4$ in $\frac{m}{2} = 2$ Paare (i, j) ein, so dass $\overline{e_i} = e_j$ gilt. Da γ trivial operiert, induziert es einen Galoisautomorphismus γ' mit Fixkörper $\mathbb{F}_{q^{\frac{4}{m}}} = \mathbb{F}_q$. Für jedes Paar (i, j) hat (ohne Einschränkung) Ce_i die Erzeugermatrix

$$\begin{pmatrix} 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \end{pmatrix} \text{ oder } \begin{pmatrix} 1 & a \end{pmatrix} \text{ mit } a \in \mathbb{F}_q.$$

Insgesamt ist die Anzahl also

$$(q+3)^2.$$

4. Fall: $^-$ und γ operieren nicht trivial (d.h. d ist ungerade und $m \nmid 4$).
Es gilt $e_i^\gamma = e_j$, genau dann wenn $\overline{e_i}^\gamma = \overline{e_j}$ gilt. Die Ordnung von γ' (gleich $\frac{m}{t}$) teilt die Ordnung von γ (gleich $\frac{p-1}{4}$), also ist

$$\frac{p-1}{4 \cdot \frac{m}{t}} = \frac{mdt}{4m} = \frac{dt}{4}$$

eine ganze Zahl. Da d ungerade und t ein Teiler von 4 ist, folgt bereits $t = 4$ und γ' hat Ordnung $\frac{m}{4}$. Dann liegen e_i und $\overline{e_i}$ genau dann in einer Bahn unter γ, wenn $\frac{m}{4}$ gerade ist. Also hat U vier Bahnen auf $\{e_1, \ldots, e_m\}$ wenn $\frac{m}{4}$ gerade ist, und zwei sonst. Die Anzahl der Codes ist dann insgesamt

$$\begin{cases} (q^d+3)^4, & \text{falls } \frac{m}{4} \text{ gerade} \\ (q^d+3)^2, & \text{falls } \frac{m}{4} \text{ ungerade.} \end{cases}$$

Der Fall p teilt $|\mathbb{F}^*|$

Sei ohne Einschränkung

$$g = \left(\begin{pmatrix} & 1 & & \\ 1 & & & \\ & & \ddots & \\ & & & 1 \\ 1 & & & \end{pmatrix}^t, 1^{n_0}, (\zeta)^{n_1}, \ldots, \left(\zeta^{p-1}\right)^{n_{p-1}} \right)$$

für ein Element $\zeta \in \mathbb{F}^*$ von Ordnung p. Im Fall $t = 0$ (also insbesondere $\pi(g) = 1$) zerfällt C in die orthogonale Summe

$$C = \bigoplus_{\substack{i=0 \\ n_i \neq 0}}^{p-1} \operatorname{Kern}(g - \zeta^i \operatorname{id}).$$

Falls C extremal ist, muss also bereits $n_i = n$ für ein i gelten, dieser Automorphismus ist aber in der Automorphismengruppe von jedem Code enthalten. Die Einschränkung $\pi(g) \neq 1$ ist für extremale Codes also eher technischer Natur.
Sei $C \leq \mathbb{F}^n$ ein selbst-dualer, extremaler Code, so dass g ein Automorphismus von C ist mit $\pi(g) \neq 1$. Dann ist der Fixcode gegeben durch

$$C(g) = \{(\underbrace{c_1, \ldots, c_1}_{p}, \ldots, \underbrace{c_t, \ldots, c_t}_{p}, c_{tp+1}, \ldots, c_{tp+n_0}, 0, \ldots, 0) \in C\}.$$

Definiere die beiden Projektionen

$$\pi_t : C(g) \to \mathbb{F}^t, c \mapsto (c_p, c_{2p}, \ldots, c_{pt}) \text{ und}$$
$$\pi_{n_0} : C(g) \to \mathbb{F}^{n_0}, c \mapsto (c_{pt+1}, \ldots, c_{pt+n_0}).$$

Dann ist

$$C(g)^* := \{(\pi_t(c), \pi_{n_0}(c)) \mid c \in C(g)\}$$

ein Code der Länge $t + n_0$, der selbst-dual bzgl.

$$x \cdot y := p \sum_{i=1}^{t} x_i y_i + \sum_{i=t+1}^{t+n_0} x_i y_i$$

ist, insbesondere ist die Dimension also $\frac{t+n_0}{2}$. Durch die folgenden drei Bemerkungen werden bereits viele mögliche Automorphismen ausgeschlossen:

Bemerkung 2.28. *Angenommen, es gilt $n_0 < d(C)$, dann ist $\operatorname{Kern}(\pi_t)$ ein Code der Länge n_0 (nach Streichung der Nullen) mit Minimalabstand $\geq d(C)$, also gilt bereits $\operatorname{Kern}(\pi_t) = \{0\}$ und π_t ist injektiv. In diesem Fall ist $\pi(C(g))$ ein Code der Länge t, Dimension $\frac{t+n_0}{2}$ und Minimalabstand $\geq \left\lceil \frac{d(C)-n_0}{p} \right\rceil$. Für kleine n_0 ist diese Möglichkeit häufig durch die Schranken in Codetables ([Gra]) ausgeschlossen.*

Bemerkung 2.29. *Es gilt die Abschätzung*

$$d(C) \leq d(C(g)) \leq p \cdot d(\pi_t(C(g))) + n_0.$$

Zusätzlich kann $C(g)$ nach Streichung der letzten $n_1 + \cdots + n_{p-1}$ Stellen (die immer Null sind) als $\frac{t+n_0}{2}$-dimensionaler Code der Länge $pt + n_0$ mit Minimalabstand $\geq d(C)$ aufgefasst werden. Für kleine t ist diese Möglichkeit also wieder häufig durch Codetables ([Gra]) ausgeschlossen.

Bemerkung 2.30. *Es gilt*

$$\pi_t(C(g))^\perp = \pi_t(\mathrm{Kern}(\pi_{n_0})),$$

also existiert ein maximal selbst-orthogonaler Code $\Lambda \leq \mathbb{F}^t$ mit

$$\pi_t(\mathrm{Kern}(\pi_{n_0})) \leq \Lambda \leq \Lambda^\perp \leq \pi_t(C(g)).$$

Dann liefern die Klassifikationen in [HMa] oder die Abschätzungen in [Mey10] einen möglichen Widerspruch.

Der Fall $p = \mathrm{char}(\mathbb{F})$

Zuerst wurden in [Bou96] binäre, selbst-duale Codes mit einem fixpunktfreien Automorphismus der Ordnung 2 untersucht. Mit einer geeigneten Projektion des Fixcodes wurden verschiedene Codes der Länge 64 konstruiert, in [Bou00] wurde diese Konstruktion auf Automorphismen mit Fixpunkten übertragen. Damit wurde dann in [Bou02] gezeigt, dass ein binärer, extremaler Code der Länge $24m$ mit einem Autorphismus der Ordnung 2 mit Fixpunkten nur für $m = 1$ und $m = 5$ existieren kann. In [Neb12b] wurde dies zusammen mit der Klassifikation der binären, extremalen Codes der Länge 36 benutzt, um zu zeigen, dass ein binärer, extremaler Code der Länge 72 ein freier $\mathbb{F}_2C_2$-Modul ist.

Sei $C \leq \mathbb{F}^n$ ein Code der Länge n über einem endlichen Körper der Charakteristik p und sei g ein Automorphismus der Ordnung $q = p^e, e \geq 1$ von C. Dann ist g in $\mathrm{Mon}_n(\mathbb{F})$ konjugiert zu einem Element ohne monomialen Anteil. Angenommen, g hat nur Zykel der Länge q und 1, dann gilt ohne Einschränkung

$$g = (1, 2, \ldots, q)(q+1, \ldots, 2q) \ldots ((t-1)q+1, \ldots, tq) \underbrace{(tq+1) \ldots (n)}_{f},$$

wobei $f := n - tq$ die Anzahl der Fixpunkte von g ist. Der Gruppenring $R := \mathbb{F}[g]$ ist ein artinscher, kommutativer Kettenring mit Idealen

$$\langle (1-g)^i \rangle,\ 0 \leq i \leq q.$$

Es gilt

$$\mathbb{F}^n \cong R^t \oplus \mathbb{F}^f \text{ als } R\text{-Moduln}$$

und der Code C lässt sich mit Lemma 2.3 (mit $n_1 = qt$ und $n_2 = f$) konstruieren als

$$C = \{(x, y) \mid x \in \mathcal{B}_E, y \in \mathcal{D}_F, \psi(x) = y + \mathcal{D}^*\},$$

wobei

$$\mathcal{B}^* \subseteq \mathcal{B}^{*\perp} = \mathcal{B}_E \leq R^t$$

und

$$\mathcal{D}^* \subseteq \mathcal{D}^{*\perp} = \mathcal{D}_F \leq \mathbb{F}^f$$

selbst-orthogonale Codes sind und

$$\psi : \mathcal{B}^{*\perp}/\mathcal{B}^* \to \mathcal{D}^{*\perp}/\mathcal{D}^*$$

eine g-äquivariante Antiisometrie ist.

Lemma 2.31 (siehe [Bou02] für $p = 2$)**.** *Sei $\mathbb{F}^n(g) := \{v \in \mathbb{F}^n \mid v \cdot g = v\}$ und $C(g) = V(g) \cap C$ der Fixcode von g. Definiere*

$$\pi_g : \mathbb{F}^n(g) \to \mathbb{F}^t, (\underbrace{c_1, \ldots, c_1}_{q}, \underbrace{c_2, \ldots, c_2}_{q}, \ldots, \underbrace{c_t, \ldots, c_t}_{q}, x_1, \ldots, x_f) \mapsto (c_1, \ldots, c_t)$$

und

$$\Phi_g : \mathbb{F}^n \to \mathbb{F}^t, (c_1, \ldots, c_n) \mapsto (c_1 + c_2 + \cdots + c_q, \ldots, c_{(t-1)q+1} + \ldots + c_{tq}).$$

Dann ist Φ_g ein g-invarianter Homomorphismus, der

$$v \cdot w = \pi_g(v) \cdot \Phi_g(w) \qquad (\star)$$

für alle $v \in \mathbb{F}^n(g)$ und $w \in \mathbb{F}^n$ erfüllt. Sei $\mathcal{B}$ wie in Lemma 2.3 mit $n_1 = tq$ und sei $\mathcal{B}(g) := C(g) \cap \mathcal{B}$. Dann ist $\Psi_g(C)$ ein selbst-orthogonaler Code mit

$$\Phi_g(C)^\perp = \pi_g(\mathcal{B}(g)) \text{ und } \Phi_g(\mathcal{B})^\perp = \pi_g(C(g)).$$

Beweis. Die Gleichung $(\star)$ folgt durch eine einfache Rechnung, damit gilt

$$\pi_g(\mathcal{B}(g)) \subseteq \Phi_g(C)^\perp \text{ und } \pi_g(C(g)) \subseteq \Phi_g(\mathcal{B})^\perp.$$

Für $c = (c_1, \ldots, c_n) \in C$ erfüllt

$$\begin{aligned} d &:= c \cdot (1 + g + \cdots + g^{q-1}) \\ &= \Big(\underbrace{\sum_{i=1}^{q} c_i, \ldots, \sum_{i=1}^{q} c_i}_{q}, \ldots, \underbrace{\sum_{i=1}^{q} c_{(t-1)q+i}, \ldots, \sum_{i=1}^{q} c_{(t-1)q+i}}_{q}, \underbrace{0, \ldots, 0}_{f} \Big) \in \mathcal{B}(g) \end{aligned}$$

die Gleichung $\pi_g(d) = \Phi_g(c)$, damit ist

$$\Phi_g(\mathcal{B}) \subseteq \Phi_g(C) \subseteq \pi_g(\mathcal{B}(g)) \subseteq \pi_g(C(g)).$$

Sei nun $(d_1, \ldots, d_t) \in \Phi_g(C)^\perp$, dann wird der Vektor

$$v := (\underbrace{d_1, \ldots, d_1}_{q}, \ldots, \underbrace{d_t, \ldots, d_t}_{q}, \underbrace{0, \ldots, 0}_{f}) \in \mathbb{F}^n$$

von g fixiert und die letzten f Koordinaten sind 0. Außerdem ist $v \in C = C^\perp$, da

$$v \cdot c = \pi_g(v) \cdot \Phi_g(c) = 0 \text{ gilt für alle } c \in C.$$

Also ist $v \in \mathcal{B}(g)$ und damit insgesamt $\Phi_g(C)^\perp \subset \pi_g(\mathcal{B}(g))$.
Sei nun $d := (d_1, \ldots, d_t) \in \Phi_g(\mathcal{B})^\perp$. Für jedes $x \in \mathbb{F}^f$ erfüllt das Element

$$v_x := (\underbrace{d_1, \ldots, d_1}_{q}, \ldots, \underbrace{d_t, \ldots, d_t}_{q}, x) \in \mathbb{F}^n(g)$$

dass $\pi_g(v_x) = d$ ist, zusätzlich ist für jedes $b \in \mathcal{B}$ das innere Produkt

$$v_x \cdot b = \pi_g(v_x) \cdot \Phi_g(b) = d \cdot \Phi_g(b) = 0.$$

Da die Projektion von C auf $\mathcal{B}_E$ surjektiv und $\mathcal{B}_E = \mathcal{B}^{*\perp}$ ist, existiert ein Element $x \in \mathbb{F}^f$, so dass $v_x \in C(g)$. Daraus folgt die Behauptung. □

Sei nun g ein fixpunktfreier Automorphismus, d.h. es gilt $n = tq$ und

$$g = (1, \ldots, q)(q+1, \ldots, 2q) \ldots ((t-1)q+1, \ldots, tq).$$

Dann ist $\mathbb{F}^n \cong R^t =: V$ ein freier R-Modul vom Rang t. Im Fall $t = 1$ sind die Codes in V gerade die zyklischen Codes. Auf R ist die natürliche Involution $^- : R \to R$ definiert durch

$$\overline{\sum_{i=0}^{q} \alpha_i g^i} := \sum_{i=0}^{q} \overline{\alpha_i} g^{-1},$$

damit ist

$$\langle \cdot, \cdot \rangle : V \times V \to R, (v, w) \mapsto \sum_{j=1}^{t} v_j \overline{w_j}$$

das Standard hermitesche innere Produkt auf V.

Bemerkung 2.32. *Die Abbildung*

$$\varphi : \mathbb{F}^n \to V, (c_1, \ldots, c_{tq}) \mapsto \left(\sum_{i=1}^{q} c_i g^{i-1}, \ldots, \sum_{i=1}^{q} c_{(t-1)q+i} g^{i-1} \right)$$

ist ein R-Modulisomorphismus, für den gilt

$$c \cdot d = \mathrm{Spur}(\langle \varphi(c), \varphi(d) \rangle),$$

wobei

$$\mathrm{Spur}\left(\sum_{i=0}^{q-1}\alpha_i g^i\right) = \alpha_0.$$

Insbesondere definiert diese Abbildung also eine Bijektion zwischen den selbst-dualen Codes in R^t (bzgl. $\langle\cdot,\cdot\rangle$) und den selbst-dualen Codes $C \leq \mathbb{F}^n$ mit einem Automorphismus $g \in \mathrm{Aut}(C)$.

Für die drei bisher bekannten ternären, extremalen Codes der Länge 36 bzw. 48 gilt, dass die Automorphismen g der Ordnung 3 alle fixpunktfrei sind, außerdem sind diese Code freie R-Moduln. Dies motivierte die Entwicklung der Theorie von selbst-dualen Codes über Kettenringen.

Kapitel 3

Selbst-duale Codes über Kettenringen

In diesem Kapitel wird die Struktur von Codes über Kettenringen untersucht. Auch wenn die Motivation, und sicherlich auch die wichtigste Anwendung, die Klassifikation von selbst-dualen Codes über $\mathbb{F}_p$ mit einem Automorphismus der Ordnung p ist, ist die Theorie so Allgemein wie möglich gehalten. Bedeutung erlangten Kettenringe in der Codierungstheorie, als gewisse nichtlineare binäre Codes mit einem hohem Minimalabstand als das Bild eines linearen $\mathbb{Z}_4$-Codes unter der sogenannten Gray-Map beschrieben werden konnten ([Ham+94]). Zusätzlich sind die Eigenschaften von Kettenringen eng mit denen von Körpern verwandt, es ist also zu erwarten, dass sich auch Strukturen von klassischen linearen Codes übertragen. Außerdem beinhaltet die Klasse von Kettenringen einige wichtige Familien, wie gewisse Restklassenringen der ganzen Zahlen, Galois-Ringe und einige Gruppenringe.
Sei C ein Code über einem artinschen Kettenring R der Länge $a+1$ mit maximalem Ideal $\mathfrak{m} = \langle x \rangle$ und Restklassenkörper $\mathbb{F} = R/\mathfrak{m}$, dann definiert die Multiplikation mit x eine Kette von Teilcodes

$$C \supseteq C^{(1)} := Cx \supseteq C^{(2)} := Cx^2 \supseteq \cdots \supseteq C^{(a)} := Cx^a \supseteq \{0\}.$$

In den Papern [Bou00], [Bou02] und [BW13] wird eine ähnliche Idee für den Spezialfall der binären, selbst-dualen Code mit einem Automorphismus g der Ordnung 2 angewendet. Das Hauptresultat von [Neb12b] ist ein Spezialfall von Satz 3.8, das besagt, dass der Code $C \cdot (1+g)$ kanonisch isomorph zu einem selbst-dualen Code über $\mathbb{F}_2$ ist, genau dann wenn C ein freier $\mathbb{F}_2 C_2$-Modul ist. Im Allgemeinen ist ein selbst-dualer Code C in R^t ein freier R-Modul, genau dann wenn $C^{(a)}$ ein (hermitesch) selbst-dualer Code über dem Restklassenkörper $\mathbb{F}$ ist. In diesem Fall wird beschrieben, wie man einen gegebenen Code $C^{(i+1)}$ zu allen zulässigen Codes $C^{(i)}$ liftet. Diese stehen in Bijektion zu (hermitesch) selbst-dualen Codes in einem geeigenetem bilinearen Raum über $\mathbb{F}$ (Satz 3.14). Dies führt zu einer neuen Methode (Algorithmus 3.18) um alle freien, selbstdualen Codes $C^{(0)}$ (mit hohem Minimalabstand) zu klassifizieren. Damit wird unter anderem gezeigt, dass der Pless-Code P_{36} der einzige ternäre, extremale Code der Länge 36 mit einem Automorphismus der Ordnung 3 ist (Satz 4.6).

Das folgende Kapitel und zusätzlich die Ergebnisse von Satz 4.3 und Satz 4.6 wurden in dem Paper [EN18] veröffentlicht.

3.1 Codes über Kettenringen

Sei wie oben R ein kommutativer, artinscher Kettenring mit 1 und sei $^- : R \to R$ eine Involution, d.h. ein Ring-Automorphismus der Ordnung eins oder zwei. Sei $\mathfrak{m}$ das maximale Ideal von R, dann induziert $^-$ eine Involution auf dem Restklassenkörper $\mathbb{F} = R/\mathfrak{m}$, welche auch mit $^-$ bezeichnet wird. Falls diese Involution die Identität auf dem Restklassenkörper ist, existiert ein $\epsilon \in \{1, -1\}$, so dass $\overline{x} \equiv \epsilon x \pmod{Rx^2}$ gilt für jeden Erzeuger x von $\mathfrak{m}$. Falls $^-$ Ordnung zwei auf $\mathbb{F}$ hat (was dann hermitescher Fall genannt wird), kann nach Hilbert 90 ein Erzeuger x von $\mathfrak{m}$ gewählt werden, so dass $\overline{x} \equiv x \pmod{Rx^2}$ erfüllt ist. Sei nun x ein fest gewählter Erzeuger des maximalen Ideals von R, so dass

$$\overline{x} \equiv \epsilon x \pmod{Rx^2}$$

gilt, mit $\epsilon = 1$ im hermiteschen Fall. Sei $a \in \mathbb{N}_0$ maximal mit $x^a \neq 0$. Dann ist

$$R \supset Rx \supset Rx^2 \supset \cdots \supset Rx^{a+1} = \{0\}$$

die komplette Kette von Idealen in R und alle unzerlegbaren R-Modulen sind von der Form

$$S_b := Rx^b \text{ für ein } 0 \leq b \leq a,$$

wobei $S_0 = R$ der freie Modul von Rang 1 und S_a der eindeutige einfache R-Modul ist. Die Kompositions-Länge (oder Jordan-Hölder-Länge) eines Moduls V wird mit $\ell(V)$ bezeichnet, insbesondere gilt also $\ell(S_b) = a - b + 1$.
Für die Betrachtung von Codes sei $t \in \mathbb{N}$ und sei

$$V := R^t = \{(v_1, \ldots, v_t) \mid v_i \in R\}$$

der freie R-Modul von Rang t mit dem $^-$-hermiteschen innerem Produkt

$$\langle \cdot, \cdot \rangle : V \times V \to R, \langle v, w \rangle := \sum_{j=1}^{t} v_j \overline{w_j}. \tag{1}$$

Definition 3.1. *Ein R-Teilmodul von V heißt Code der Länge t über R. Für einen Code C in V existieren nach dem Satz von Krull-Schmidt-Remak eindeutige $t_0, t_1, \ldots, t_a \in \mathbb{Z}_{\geq 0}$ mit*

$$C \cong S_0^{t_0} \oplus S_1^{t_1} \oplus \cdots \oplus S_a^{t_a}.$$

Das Tupel $(t_0, t_1, \ldots, t_a)$ heißt Typ von C. Der duale Code ist

$$C^\perp := \{v \in V \mid \langle v, w \rangle = 0 \text{ für alle } w \in C\}$$

und C heißt selbst-orthogonal, falls $C \subseteq C^\perp$, bzw. selbst-dual, falls $C = C^\perp$ gilt.

Lemma 3.2. *Sei $C \leq R^t$ ein Code vom Typ $(t_0, t_1, \ldots, t_a)$.*

i) Der Typ von Cx ist $(0, t_0, \ldots, t_{a-1})$.

ii) Der Typ von $C^\perp$ ist $(t - \sum_{i=0}^{a} t_i, t_a, \ldots, t_1)$.

iii) Es gilt $\ell(C) + \ell(C^\perp) = \ell(V)$.

Beweis. Die Aussage von i) ist klar und iii) folgt aus ii). Sei $(t'_0, t'_1, \ldots, t'_a)$ der Typ von $C^\perp$. Als artinscher Ring ist R selbst-injektiv, d.h. es existiert eine kurze exakte Sequenz

$$0 \to C^\perp \to V \to \mathrm{Hom}_R(C, R) \to 0$$

und es ist $\mathrm{Hom}_R(C, R) \cong C$ als R-Moduln. Daraus folgt $C \cong V/C^\perp$. Der Typ von $V/C^\perp = R^t/(\oplus_{b=0}^{a} S_b^{t'_b})$ ist der Typ von

$$\begin{aligned} &\bigoplus_{b=0}^{a} (R/Rx^b)^{t'_b} \oplus R^{t-\sum_{b=0}^{a} t'_b} \\ \cong &\bigoplus_{b=0}^{a} S_{a-b+1}^{t'_b} \oplus S_0^{t-\sum_{b=0}^{a} t'_b}, \end{aligned}$$

also gilt $t_0 = t - \sum_{b=0}^{a} t'_b$ und $t_{a-b+1} = t'_b$ für $1 \leq b \leq a$. □

Lemma 3.3. *Sei $C \subseteq C^\perp \leq V$ ein selbst-orthogonaler Code vom Typ $(t_0, t_1, \ldots, t_a)$. Dann gilt*

$$\sum_{i=0}^{j} t_i \leq t - \sum_{i=0}^{j-a} t_i$$

für alle $j = 0, \ldots, a$ und im Fall $C^\perp x \subseteq C$ ist zusätzlich

$$t - \sum_{i=0}^{a-j} t_i \leq \sum_{i=0}^{j+1} t_i$$

für alle $j = 0, \ldots, a-1$.

Beweis. Falls $C \subseteq C^\perp$ selbst-orthogonal ist, enthält der Modul

$$C^\perp \cong S_0^{t-\sum_{i=0}^{a} t_i} \oplus S_1^{t_a} \oplus \ldots \oplus S_a^{t_1}$$

einen Teilmodul, der isomorph zu $S_0^{t_0} \oplus S_1^{t_1} \oplus \cdots \oplus S_a^{t_a}$ ist. Also folgt

$$\begin{aligned} t_0 &\leq t - \sum_{i=0}^{a} t_i, \\ t_0 + t_1 &\leq t - \sum_{i=0}^{a} t_i + t_a = t - \sum_{i=0}^{a-1} t_i \end{aligned}$$

etc. Analog folgt, falls $C^\perp x \subseteq C$ gilt, dass $S_0^{t_0} \oplus S_1^{t_1} \oplus \cdots \oplus S_a^{t_a}$ einen Teilmodul enthält, der isomorph zu $S_1^{t-\sum_{i=0}^{a} t_i} \oplus S_2^{t_a} \oplus \cdots \oplus S_a^{t_2}$ ist, woraus die anderen Ungleichungen folgen. □

3.2 Der Sockel

Die Multiplikation mit x^a definiert einen Isomorphismus zwischen dem Restklassenkörper $\mathbb{F}$ und dem Sockel von R, womit der Sockel eines Codes $C \leq V$ untersucht werden kann.

Bemerkung 3.4. *Der Isomorphismus*

$$\varphi : \mathbb{F} = R/Rx \to Rx^a = S_a, r + Rx \mapsto rx^a$$

erfüllt

$$\varphi(\overline{r + Rx}) = \overline{r}x^a = \epsilon^a \overline{rx^a},$$

d.h. φ kommutiert oder anti-kommutiert mit den Involutionen auf R und $\mathbb{F}$.

Für einen Code C vom Typ $(t_0, t_1, \ldots, t_a)$ ist der Sockel

$$\mathrm{soc}(C) := \{c \in C \mid cx = 0\} \cong S_a^{t_0+\cdots+t_a}$$

ein Teilraum des Sockels $\mathrm{soc}(V) = Vx^a$ von Dimension $\sum_{i=0}^{a} t_i$.

Bemerkung 3.5. *Sei*

$$v \cdot w := \sum_{i=1}^{t} v_i \overline{w_i}$$

das Standard hermitesche innere Produkt auf $\mathbb{F}^t$. Die Abbildung

$$\pi : \mathrm{soc}(V) = Vx^a \to \mathbb{F}^t, (v_1, \ldots, v_t) \mapsto (\varphi^{-1}(v_1), \ldots, \varphi^{-1}(v_t))$$

ist ein $\mathbb{F}$-linearer Isomorphismus, welcher

$$\pi(vx^a) \cdot \pi(wx^a) = \varphi^{-1}(\langle vx^a, w\rangle) = \epsilon^a \varphi^{-1}(\langle v, wx^a\rangle)$$

für alle $v, w \in V$ erfüllt.

Falls $C \leq V$ ein Code der Länge t über R ist, dann sind Cx^a und $\mathrm{soc}(C)$ Teilcodes von $\mathrm{soc}(V) = Vx^a$.

Lemma 3.6. *Es gilt $(\pi(C^\perp x^a))^\perp = \pi(\mathrm{soc}(C))$.*

Beweis. Sei $(t_0, \ldots, t_a)$ der Typ von C. Dann folgt aus Lemma 3.2, dass

$$\dim(\pi(C^\perp x^a)) = t - \sum_{i=0}^{a} t_i$$

und

$$\dim(\pi(\mathrm{soc}(C))) = \sum_{i=0}^{a} t_i$$

gilt. Also genügt es zu zeigen, dass $\pi(\mathrm{soc}(C))$ in $(\pi(C^\perp x^a))^\perp$ enthalten ist. Seien dafür $s = (s_1, \ldots, s_t) \in \mathrm{soc}(C)$ und $z = (z_1, \ldots, z_t) \in C^\perp$. Dann ist

$$\pi(zx^a) \cdot \pi(s) = \epsilon^a \varphi^{-1}(\langle z, s \rangle) = \epsilon^a \varphi^{-1}(0) = 0$$

und damit $\pi(s) \in (\pi(C^\perp x^a))^\perp$. □

Bemerkung 3.7. *Im Fall $C^\perp x^a \subseteq C$ ist $C^\perp x^a \subseteq \mathrm{soc}(C)$, also ist $\pi(C^\perp x^a)$ ein selbst-orthogonaler Teilcode von $\pi(\mathrm{soc}(V)) = \mathbb{F}^t$ bzgl. des Standard hermiteschen inneren Produkts.*

3.3 Selbst-duale Codes

Von nun an werden selbst-duale Codes $C = C^\perp \leq V$ der Länge t betrachtet. Als Korollar von Lemma 3.2 folgt der folgende Satz (siehe [BW13] und [Neb12b] für den Fall $R = \mathbb{F}_2 C_2$).

Satz 3.8. *Sei $C = C^\perp \leq V$ ein selbst-dualer Code der Länge t.*

i) Der Typ von $(t_0, t_1, \ldots, t_a)$ von C erfüllt $t_1 = t_a$, $t_2 = t_{a-1}, \ldots$ und

$$t_0 = \begin{cases} \frac{t}{2} - \sum_{b=1}^{a/2} t_b & \text{falls } a \text{ gerade} \\ \frac{t - t_{(a+1)/2}}{2} - \sum_{b=1}^{(a-1)/2} t_b & \text{falls } a \text{ ungerade.} \end{cases}$$

ii) Der Code $\pi(Cx^a)$ ist selbst-orthogonal in $(\mathbb{F}, \cdot)$ mit $(\pi(Cx^a))^\perp = \pi(\mathrm{soc}(C))$.

iii) Der Code C ist ein freier R-Modul (d.h. $t_1 = \cdots = t_a = 0$ und $t_0 = t/2$), genau dann wenn $Cx^a = \mathrm{soc}(C)$, genau dann wenn $\pi(Cx^a)$ ein selbst-dualer Code in $(\mathbb{F}^t, \cdot)$ ist.

Beweis. Die erste Aussage folgt direkt aus Lemma 3.2. Es gilt $Cx^a x = \{0\}$, also ist Cx^a im Sockel $\mathrm{soc}(C)$ von C enthalten. Damit folgt die zweite Aussage aus Lemma 3.6. Dann ist $\pi(Cx^a)$ ein selbst-dualer Code in $(\mathbb{F}^t, \cdot)$, genau dann wenn $Cx^a = \mathrm{soc}(C)$ gilt, genau dann wenn beide die gleiche $\mathbb{F}$-Dimension haben. Da die Dimension von $\pi(Cx^a)$ gleich t_0 ist, und die von $\pi(\mathrm{soc}(C))$ gleich $t_0 + t_1 + \cdots + t_a$, sind diese genau dann gleich, wenn $t_1 = \cdots = t_a = 0$ erfüllt ist, d.h. C ist ein freier R-Modul vom Rang $t_0 = t/2$. □

Im folgenden sei C ein selbst-dualer Code von gerader Länge t und vom Typ $(t/2, 0, \ldots, 0)$, d.h. C ist ein freier R-Modul. Dann bilden die Teilcodes

$$C^{(i)} := Cx^i$$

vom Typ $(0^i, t/2, 0^{a-i})$ die folgende Kette:

$$V \supset C^{(a)^\perp} \supset \cdots \supset C^{(1)^\perp} \supset C^\perp = C \supset C^{(1)} \supset \cdots \supset C^{(a)} \supset \{0\}.$$

Lemma 3.9. *Für $0 \leq i \leq a$ gilt $C^{(i)^\perp} = C + Vx^{a+1-i}$. Außerdem ist der Typ von $C^{(i)^\perp}$ gleich $(t/2, 0^{a-i}, t/2, 0^{i-1})$.*

Beweis. Durch eine einfache Rechnung folgt $C + Vx^{a+1-i} \subseteq C^{(i)^\perp}$. Außerdem gilt für die Kompositions-Länge

$$\ell(C^{(i)}) = \ell(S_i^{t/2}) = \tfrac{t}{2}(a - i + 1)$$

und

$$\begin{aligned}\ell(C + Vx^{a+1-i}) &= \ell(C/(Vx^{a+1-i} \cap C)) + \ell(Vx^{a+1-i}) \\ &= \ell(C/C^{(a+1-i)}) + ti \\ &= \tfrac{t}{2}(a + 1 - i) + ti \\ &= \tfrac{t}{2}(a + 1 + i).\end{aligned}$$

Also impliziert

$$\ell(C^{(i)}) + \ell(C + Vx^{a+1-i}) = t(a + 1) = \ell(V)$$

die Gleichheit $\ell(C + Vx^{a+1-i}) = \ell(C^{(i)^\perp})$, daraus folgt die Behauptung. □

Korollar 3.10. *Es gilt $C^{(i)^\perp}x^i = Cx^i + V(x^{a+1-i}x^i) = Cx^i = C^{(i)}$.*

Definition 3.11. *Sei $D \leq Vx^{i+1}$ ein Code vom Typ $(0^{i+1}, t/2, 0^{a-i-1})$ mit $D^\perp x^{i+1} = D$ (dies erfüllt jeder Code $C^{(i+1)}$). Sei*

$$W_i := D^\perp x^i / D \cong \mathbb{F}^t$$

und definiere

$$(\cdot,\cdot)_i : W_i \times W_i \to \mathbb{F}, (cx^i + D, bx^i + D) \mapsto \varphi^{-1}(\langle c, b\rangle x^i).$$

Lemma 3.12. *Das innere Produkt $(\cdot,\cdot)_i$ ist wohldefiniert, nicht-ausgeartet und hermitesch im hermiteschen Fall bzw. ϵ^{i+a}-symmetrisch sonst.*

Beweis. Der Raum W_i ist isomorph zu $\mathbb{F}^t$, da er von der Multiplikation mit x annihiliert wird. Nun wird gezeigt dass das innere Produkt wohldefiniert ist. Für $c, c' \in D^\perp$ gilt

$$cx^i + D = c'x^i + D,$$

genau dann wenn $d \in D^\perp, v \in V$ existieren mit

$$c' = c + dx + vx^{a+1-i}.$$

Für solche $c' = c + dx + vx^{a+1-i}$ und $b' = b + d'x + v'x^{a+1-i}$ ist

$$\begin{aligned}\langle c', b'\rangle x^i &= \langle c + dx + vx^{a+1-i}, b + d'x + v'x^{a+1-i}\rangle x^i \\ &= \langle c, b\rangle x^i + \langle c, d'x\rangle x^i + \langle dx, b\rangle x^i + \langle dx, d'x\rangle x^i \\ &= \langle c, b\rangle x^i,\end{aligned}$$

wobei die erste Gleichung gilt, da $x^{a+1-i}x^i = 0$ ist, die zweite Gleichung gilt, da dxx^i in $D^\perp x^{i+1} = D$ und c, d' in $D^\perp$ enthalten sind, analog gilt $d'x\overline{x}^i \in D^\perp x^{i+1} = D$ und $b, dx \in D^\perp$. Für $c, b \in D^\perp$ gilt

$$(\langle c, b\rangle x^i)x = \langle cx^{i+1}, b\rangle = 0$$

da $cx^{i+1} \in D^\perp x^{i+1} = D$ und $b \in D^\perp$ ist. Also ist $\langle c, b\rangle x^i \in S_a$ und das innere Produkt ist wohldefiniert. Außerdem ist

$$\begin{aligned}(bx^i, cx^i)_i &= \varphi^{-1}(\langle b, c\rangle x^i) = \varphi^{-1}\left(\overline{\langle c, b\rangle}x^i\right) = \varphi^{-1}\left(\overline{\langle c, b\rangle\overline{x^i}}\right) \\ &= \epsilon^a\overline{\varphi^{-1}(\langle c, b\rangle\overline{x^i})} = \epsilon^a\overline{\varphi^{-1}(\langle c, b\rangle\epsilon^i x^i)} = \epsilon^{(i+a)}\overline{\varphi^{-1}(\langle c, b\rangle x^i)} \\ &= \epsilon^{(i+a)}(cx^i, bx^i)_i,\end{aligned}$$

woraus die Symmetrie-Eigenschaft folgt. Für das Radikal sei $bx^i \in D^\perp x^i$, so dass $(cx^i, bx^i)_i = 0$ für alle $c \in D^\perp$ ist. Daraus folgt $\langle c, b\rangle x^i = \langle c, bx^i\rangle = 0$ für alle $c \in D^\perp$, dann gilt aber bereits $bx^i \in D$ und das Radikal ist $\{0\}$ und ist $(\cdot,\cdot)_i$ nicht-ausgeartet. □

Bemerkung 3.13. *Bezüglich $(\cdot,\cdot)_i$ ist*

$$X_i := (D + \mathrm{soc}(V))/D = (D + Vx^a)/D \leq W_i$$

ein maximal isotroper Teilraum von W_i.

Der nächste Satz kann als Verallgemeinerung von Satz 3.8 gesehen werden, da es einen Lift D' von D, d.h. einen selbst-orthogonalen Code, der isomorph zu $S_i^{t/2}$ ist und $D'x = D$ erfüllt, als maximal isotropen Teilraum von W_i identifiziert.

Satz 3.14. *Seien D, W_i und $(\cdot,\cdot)_i$ wie oben. Die Codes $D' \leq Vx^i$ mit $D'x = D$ und $D'^\perp x^i = D'$ sind genau die maximal isotropen Teilräume von D'/D in $(W_i, (\cdot,\cdot)_i)$, die ein Komplement von X_i sind, d.h.*

$$W_i = D'/D \oplus X_i.$$

Beweis. Nach Voraussetzung gilt $D = D'x \subseteq D'$, also ist $D'^\perp \subseteq D^\perp$ und damit

$$D' = D'^\perp x^i \subseteq D^\perp x^i.$$

Daraus folgt $D'/D \leq W_i$. Für $cx^i, bx^i \in D'$ kann ohne Einschränkung angenommen werden, dass $b \in D'^\perp$ gilt, damit ist

$$(cx^i, bx^i)_i = \varphi^{-1}(\langle cx^i, b\rangle) = \varphi^{-1}(0) = 0$$

und D'/D ist ein isotroper Teilraum von W_i. Falls für $b \in D^\perp$ gilt, dass $\langle cx^i, b\rangle = 0$ für alle $c \in D'^\perp$ erfüllt ist, folgt $b \in D'$, also ist D'/D ein maximal isotroper Teilraum von W_i. Insbesondere ist also $D'/D \cong \mathbb{F}^{t/2}$. Aus

$$D'x = D \cong S_{i+1}^{t/2}$$

folgt die Isomorphie $D' \cong S_i^{t/2}$, also ist

$$\mathrm{soc}(V) \cap D' \cong S_a^{t/2} \cong \mathrm{soc}(V) \cap D.$$

Dann ist $\mathrm{soc}(V) \cap D' = \mathrm{soc}(V) \cap D$ und $D'/D \cap X_i = \{0\}$, was eine Richtung des Satzes beweist.
Sei nun $Y \leq W_i$ ein isotropes Komplement von X_i, und sei D' das Urbild von Y in $D^\perp x^i$. Dann ist $D' \leq Vx^i$ und

$$D'x = (D' + \mathrm{soc}(V))x = D^\perp x^i x = D.$$

Dies impliziert, dass der Typ von D' gleich $(0^i, t/2, 0^{a-i})$ ist, außerdem, dass $D \subseteq D'$ und $D'^\perp \subseteq D^\perp$ gilt. Da Y maximal isotrop ist, ist

$$D'^\perp x^i + D/D = Y^\perp = Y = D'/D,$$

also $D' = D'^\perp x^i + D$. Aus Lemma 3.2 folgt, dass der Typ von $D'^\perp$ gleich $(t/2, 0^{a-i}, t/2, 0^{i-1})$ ist, und deshalb $D'^\perp x^i \cong D'$, also $D'^\perp x^i = D'$. Daraus folgt die Behauptung. □

3.4 Äquivalenz von Codes

Sei $U(R) := \{r \in R \mid r\overline{r} = 1\}$ die unitäre Gruppe von R. Dann vertauscht die Operation der monomialen Gruppe

$$\mathrm{Mon}_t(R) := \{\mathrm{diag}(u_1, \ldots, u_t)\pi \mid u_i \in U(R), \pi \in S_t\}$$

mit Dualität. Diese Gruppe ist das semidirekte Produkt des Normalteilers der Diagonalmatrizen $U(R)^t$ und der Untergruppe $P_t \cong S_t$ der Permutationsmatrizen. Analog zum Beweis von Satz 2.16 gilt damit das folgende Lemma:

Lemma 3.15. *Sei $g \in \mathrm{Mon}_t(R)$ ein Element von Ordnung s, so dass s und $|U(R)|$ teilerfremd sind. Dann ist g in $\mathrm{Mon}_t(R)$ konjugiert zu einem Element von P_t.*

Zwei Codes $C, D \leq V$ heißen äquivalent, $C \cong D$, wenn ein $g \in \mathrm{Mon}_t(R)$ existiert mit $C \cdot g = D$. Die Automorphismengruppe $\mathrm{Aut}(C)$ ist der Stabilisator von C in $\mathrm{Mon}_t(R)$.

Lemma 3.16. *Der natürliche Epimorphismus induziert einen Epimorphismus*

$$U(R) \to U(\mathbb{F}), u \mapsto u + xR.$$

Beweis. Falls $\mathrm{char}(\mathbb{F}) = 2$ und $^-$ die Identität auf $\mathbb{F}$ ist, dann ist $U(\mathbb{F}) = \{1\}$ und die Abbildung ist offenbar surjektiv. Sei also $\mathrm{char}(\mathbb{F}) \neq 2$ oder $^-$ ist nicht die Identität auf $\mathbb{F}$. Sei $u \in R$, so dass $u\overline{u} = 1 + rx^j$ gilt für ein $r \in R$ mit $\overline{r} \equiv r \pmod{xR}$ und $j \geq 1$. Für die Behauptung muss nun ein $v \in R$ existieren, so dass

$$(u + vx^j)\overline{(u + vx^j)} = 1 + r'x^{j+1}$$

für ein $r' \in R$ erfüllt ist. Dieses v ist die Lösung der Gleichung

$$-r \equiv u\overline{v} + \overline{u}v \pmod{xR}. \qquad (\star)$$

Falls $^-$ die Identität auf $\mathbb{F}$ ist, ist die Lösung gegeben durch $v \equiv \frac{-r}{2u} \pmod{xR}$, da $2u$ eine Einheit ist. Falls $^-$ nicht die Identität auf $\mathbb{F}$ ist, ist $-r + xR$ gleich der Spur eines Elements im Körper $\mathbb{F}$. Da die Spur surjektiv und u eine Einheit ist, existiert solch ein Element v. □

Bemerkung 3.17. *Die monomiale Gruppe $\mathrm{Mon}_t(\mathbb{F})$ vertauscht mit Dualität bzgl. $\cdot$ und $(\cdot,\cdot)_i$. Aus Lemma 3.16 folgt die Existenz eines Gruppenepimorphismus*

$$\mathrm{Mon}_t(R) \to \mathrm{Mon}_t(\mathbb{F}).$$

3.5 Konstruktion aller selbst-dualen, freien Codes

In den bisherigen Abschnitten wurde die Struktur selbst-dualer Codes der Länge t über R, die frei als R-Modul sind, analysiert. Auf eine natürliche Art und Weise kann diese Struktur ausgenutzt werden, um alle diese Codes C iterativ zu konstruieren. Nach Satz 3.8 iii) ist der Sockel $C^{(a)}$ ein (hermitesch) selbst-dualer Code in $\mathbb{F}^t$, alle Möglichkeiten sind hier also durch eine schon bekannte Klassifikation (z.B. [HMb]) gegeben. Dann können die Codes $C^{(i)} = Cx^i, i = a-1, a-2, \ldots, 0$, als selbst-duale Teilmoduln von $W_i \cong \mathbb{F}^t$ konstruiert werden.

Algorithmus 3.18. Eingabe: *R, t und die Involution $^- : R \to R$.*
Ausgabe: *Eine Menge $\mathcal{D}_0 = \{C_1, \ldots, C_h\}$ der Repräsentanten der Äquivalenzklassen der freien, selbst-dualen Codes in $(V, \langle\cdot,\cdot\rangle)$.*
Algorithmus:

0) Bestimme die Menge $\mathcal{D}_a := \{D_1^{(a)}, \ldots, D_{h_a}^{(a)}\}$ der Repräsentanten der Äquivalenzklassen von (hermitesch) selbst-dualen Codes in $(\mathbb{F}, \cdot)$.

1) Für $i = a-1, a-2, \ldots, 0$ sei die Menge $\mathcal{D}_{i+1} := \{D_1^{(i+1)}, \ldots, D_{h_{i+1}}^{(i+1)}\}$ der Repräsentanten der Äquivalenzklassen von Codes $D \leq Vx^{i+1}$ vom Typ $(0^{i+1}, t/2, 0^{a-i-1})$ mit $D^{\perp}x^{i+1} = D$ gegeben.

2) Definiere $\mathcal{D}_i := \{\}$.

3) Für $j = 1, \ldots, h+1$ seien $D := D_j^{(i+1)}$, $W_i := D^{\perp}x^i/D$ wie in Lemma 3.12 und berechne die Menge $\mathcal{Y} := \{D' \leq Vx^i \mid D'x = D, D'^{\perp}x^i = D'\}$ mit Hilfe von Satz 3.14.

4) *Für alle $D' \in \mathcal{Y}$ überprüfe, ob D' äquivalent zu einem Code in $\mathcal{D}_i$ ist. Wenn nicht, füge D' zu $\mathcal{D}$ hinzu.*

5) *Falls $i = 0$, gebe $\mathcal{D}_0$ zurück.*

Für die Berechnung der Menge $\mathcal{Y}$ in Algorithmus 3.18 3) müssen alle isotropen Komplemente von X_i in $(W_i, (\cdot,\cdot)_i)$ berechnet werden. Sei dafür $\tilde{Y}_i$ ein beliebiges Komplement von X_i in W_i. Da W_i nicht-ausgeartet und X_i maximal isotrop in W_i ist, ist der Raum $\tilde{Y}_i$ isomorph zu $\mathrm{Hom}(X_i, \mathbb{F})$. Insbesondere existieren geeignete Basen von X_i bzw. $\tilde{Y}_i$, so dass die Gram-Matrix von $(\cdot,\cdot)_i$ die Form

$$\begin{pmatrix} 0 & I \\ \epsilon^{a+i} I & G \end{pmatrix}$$

hat, wobei G eine ϵ^{a+i}-hermitesche Matrix ist.

Bemerkung 3.19. *Es existiert ein isotropes Komplement Y_i von X_i in W_i, genau dann wenn $G \in \mathcal{H}$ gilt, wobei $\mathcal{H}$ die Menge*

$$\mathcal{H} := \{X + \epsilon^{a+i} \overline{X}^{tr} \mid X \in \mathbb{F}^{t/2 \times t/2}\}.$$

ist.

Die Menge $\mathcal{H}$ ist der Raum aller ϵ^{a+i}-hermiteschen Matrizen, genau dann wenn entweder $\mathrm{char}(\mathbb{F}) \neq 2$ ist oder $\bar{}$ nicht die Identität auf $\mathbb{F}$ nicht. Andernfalls ist G in $\mathcal{H}$ enthalten, genau dann wenn $G_{ii} = 0$ für alle $1 \leq i \leq t/2$ gilt.

Falls der Code D zu einem Code D' liftet, existiert ein isotropes Komplement Y_i von X_i und es existieren Basen B und B' von X_i bzw. Y_i, so dass die Gram-Matrix von $(\cdot,\cdot)_i$ bzgl. der Basis (B, B') von W_i von der Form

$$\begin{pmatrix} 0 & I \\ \epsilon^{a+i} I & 0 \end{pmatrix}$$

ist.

Folgerung 3.20. *Die selbst-dualen Komplemente von X_i in W_i sind genau die Teilräume $\langle B' + AB \rangle$ mit $A \in \mathbb{F}^{t/2 \times t/2}$, so dass*

$$\overline{A}^{\mathrm{tr}} + \epsilon^{a+i} A = 0$$

gilt. Die Menge all dieser Matrizen bildet einen Vektorraum der Dimension d über dem Fixkörper von $\bar{}$ in $\mathbb{F}$, wobei d gegeben ist durch

$\mathrm{char}(\mathbb{F})$	ϵ^{a+i}	$\bar{}$	d
$\neq 2$	1	id	$t(t-2)/8$
beliebig	-1	id	$t(t+2)/8$
beliebig	1	$\neq$ id	$t^2/4$

Beweis. Jedes Komplement von X_i hat eine Basis $B' + AB$ mit $A \in \mathbb{F}^{t/2 \times t/2}$. Diese Basis ist isotrop, genau dann wenn

$$\begin{pmatrix} I & A \end{pmatrix} \begin{pmatrix} 0 & I \\ \epsilon^{a+i} I & 0 \end{pmatrix} \begin{pmatrix} I \\ \overline{A}^{\mathrm{tr}} \end{pmatrix} = \overline{A}^{\mathrm{tr}} + \epsilon^{a+i} A = 0$$

gilt. Die Dimension d ist also die Dimension des Raumes aller schief-symmetrischen, symmetrischen, bzw. schief-hermiteschen Matrizen. □

3.6 Anwendungen

Das Gray-Bild von selbst-dualen $\mathbb{Z}_4$-linearen Codes

Die vorhergehenden Methoden liefern eine Verallgemeinerung der in [Rai00] beschriebenen Schranken für den Minimalabstand von Codes über $R = Z/4\mathbb{Z}$. Die Gray-Abbildung ist definiert durch

$$\Phi : R^t \to \mathbb{F}_2^{2t}, \begin{cases} 0 \mapsto (0,0) \\ 1 \mapsto (1,0) \\ -1 \mapsto (0,1) \\ 2 \mapsto (1,1). \end{cases}$$

Diese Abbildung definiert eine Isometrie zwischen der Lee-Distanz auf R^t und der Hamming-Distanz auf $\mathbb{F}_2^{2t}$, es ist allerdings kein Gruppen-Homomorphismus, insbesondere muss $\Phi(C)$ also kein linearer Code sein. Der folgende Satz ist eine Verallgemeinerung der Ergebnisse aus [Kie13], welche Rains sicher bekannt waren, aber nicht explizit in [Rai00] angegeben wurden.

Satz 3.21. *Sei $m \in \mathbb{N}$ ungerade und sei $C = C^\perp \leq R^{12m}$ ein selbst-dualer, R-linearer Code. Dann hat das Gray-Bild $\Phi(C) \subseteq \mathbb{F}_2^{24m}$ von C den Minimalabstand $\leq 4m$, insbesondere hat $\Phi(C)$ nicht die Parameter eines extremalen Typ II Codes.*

Beweis. Nach Satz 3.8 ii) ist $\pi(2C) \leq \mathbb{F}_2^{12m}$ ein selbst-orthogonaler, binärer Code der Länge $12m$ mit $\pi(2C)^\perp = \pi(\mathrm{soc}(C))$. Da C selbst-dual ist, gilt

$$0 = (c,c) = \sum_{i=1}^{12m} c_i^2 = |\{i \mid c_i \in \{\pm 1\}\}| + 4\mathbb{Z} = \mathrm{wt}(\pi(2c)) + 4\mathbb{Z}$$

für alle $c \in C$. Insbesondere ist also $\pi(2C)$ doppelt-gerade. Da m ungerade ist, also $12m$ kein Vielfaches von 8 ist, ist der Code $\pi(2C)$ nicht selbst-dual. Mit den Schranken aus [Rai00] (für $12m \equiv 12 \pmod{12}$) folgt

$$d(\pi(2C)^\perp) \leq 4\tfrac{m-1}{2} + 2 = 2m.$$

Also enthält das Gray-Bild $\Phi(\mathrm{soc}(C))$ einen Vektor mit Hamming-Gewicht $4m$. □

Automorphismen linearer Codes

Sei $\mathbb{F}$ ein endlicher Körper der Charakteristik p und sei $^- : \mathbb{F} \to \mathbb{F}$ ein selbstinverser Automorphismus. Sei $g \in \mathrm{Mon}_n(\mathbb{F})$ ein Element der Ordnung $q = p^e$, $e \geq 1$, dann ist g in $\mathrm{Mon}_n(\mathbb{F})$ konjugiert zu einem Element in $S_n \leq \mathrm{Mon}_n(\mathbb{F})$. Angenommen, g hat nur Zykel der Länge q und keine Fixpunkte, dann gilt ohne Einschränkung

$$g = (1, \ldots, q)(q+1, \ldots, 2q) \ldots ((t-1)q+1, \ldots, tq)$$

für ein $t \geq 1$, insbesondere ist dann $n = tq$. Wie in Abschnitt 2.3 beschrieben, ist dann $R := \mathbb{F}[g]$ ein kommutativer, artinscher Kettenring mit Idealen

$$Rx^i,\ 0 \leq i \leq q,$$

wobei $x := (1 - g)$. Die natürliche Involution auf R ist

$$^- : R \to R, \overline{\sum_{i=0}^{q-1} \alpha_i g^i} \mapsto \sum_{j=0}^{q-1} \overline{\alpha_i} g^{-i}.$$

Bemerkung 3.22. *Es gilt*

$$x + \overline{x} = (1 - g^{-1}) + (1 - g) = (1 - g)(1 - g^{-1}),$$

daraus folgt

$$\overline{x} = -x + x\overline{x} = -x - x^2 - \cdots - x^{q-1}.$$

Also ist $\epsilon = -1$ in der Notation von Abschnitt 3.1. Im hermiteschen Fall kann ein $u \in \mathbb{F}$ mit $u\overline{u} = -1$ gewählt werden, nachdem x duch ux ersetzt wurde, gilt dann $\overline{x} \equiv x \pmod{Rx^2}$.

Die (hermitesch) selbst-dualen Codes in $\mathbb{F}^n$ mit $g \in \mathrm{Aut}(C)$ stehen in Bijektion zu den selbst-dualen Codes in dem freien Modul $V := R^t$ (Bemerkung 2.32) und mit den Theorien von Abschnitt 3.3 bzw. Algorithmus 3.18 können die Codes klassifiziert werden, die als R-Modul frei sind.

Kapitel 4

Extremale, ternäre Codes

In diesem Kapitel werden die entwickelten Theorien aus Kapitel 3 auf extremale, ternäre Codes der Länge 36 und 48 angewendet.

Der Pless-Code P_{36} ist der bisher einzige bekannte extremale, ternäre Code der Länge 36, die Automorphismengruppe hat Ordnung $19584 = 2^7 \cdot 3^2 \cdot 17$. Nach einem Resultat von W. C. Huffman ist dieser Code der einzige ternäre, extremale Code der Länge 36 mit einem Automorphismus von Primordnung ≥ 5 ([Huf92, Theorem 6]). Im folgenden wird gezeigt, dass dies auch für Automorphismen der Ordnung 3 zutrifft. Alle Automorphismen der Ordnung 3 eines solchen Codes sind fixpunktfrei (Satz 4.3), daraus folgt, dass die Codes freie $\mathbb{F}_3C_3$-Moduln sind (Lemma 4.4). Mit den Methoden von Kapitel 3 lässt sich also der (eindeutige) Fixcode liften, der einzige extremale Code ist der Pless-Code P_{36} (Satz 4.6).

Zusätzlich wird gezeigt, dass der Code P_{36} der einzige ternäre, extremale Code der Länge 36 mit einem nicht-trivialen Automorphismus der Ordnung 2 ist (Satz 4.2). Daraus folgt, dass jeder solche Code der Pless-Code P_{36} ist, oder die Automorphismengruppe ist in $C_8 = \langle g \mid g^4 = -1 \rangle$ enthalten.

Im Fall der ternären, extremalen Codes der Länge 48 sind bisher zwei bekannt, der Pless-Code P_{48} und der erweiterte quadratische Restklassen-Code XQ_{47}. Die Automorphismengruppen sind hier

$$\mathrm{Aut}(P_{48}) \cong C_2 \times \mathrm{SL}_2(23).C_2 \text{ von Ordnung } 2^6 \cdot 3 \cdot 11 \cdot 23$$

bzw.

$$\mathrm{Aut}(XQ_{47}) \cong C_2 \times \mathrm{PSL}_2(47) \text{ von Ordnung } 2^5 \cdot 3 \cdot 23 \cdot 47.$$

Auch hier ist bekannt, dass diese Codes die einzigen extremalen Codes mit einem Automorphismus von Primordnung ≥ 5 sind ([Neb12c]). Analog zum Fall der Länge 36 wird gezeigt, dass jeder Automorphismus der Ordnung 3 eines solchen Codes fixpunktfrei ist (Satz 4.10) und die Codes freie $\mathbb{F}_3C_3$-Moduln sind. Mit den Methoden von Kapitel 3 lässt sich also auch hier wieder theoretisch der (eindeutige) Fixcode zu einem extremalen Code liften. Die Berechnungen sind hier allerdings zu aufwendig, die Eindeutigkeit wird aber unter einem zusätzlichem nicht-trivialen Automorphismus der Ordnung 2 gezeigt, d.h. die

Automorphismengruppen enthält die Gruppe S_3 oder C_6 (Satz 4.12 und Satz 4.13).

Zusätzlich wird die in [Neb12c] gestellte Frage beantwortet, ob jeder Automorphismus σ der Ordnung 4 eines ternären, extremalen Codes der Länge 48 $\sigma^2 = -1$ erfüllt (Satz 4.9).

4.1 Codes der Länge 36

Sei $C \leq \mathbb{F}_3^{36}$ ein ternärer, extremaler Code der Länge 36 und sei σ ein nichttrivialer Automorphismus von C mit Ordnung 2. Dann ist σ konjugiert zu

$$\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^t, 1^{n_0}, (-1)^{n_1} \right).$$

Automorphismen der Ordnung 2

Satz 4.1. *In der Situation oben ist σ konjugiert zu $\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{16}, (-1)^4 \right)$. Solch ein Automorphismus ist in $\mathrm{Aut}(P_{36})$ enthalten.*

Beweis. 1) Ohne Einschränkung gilt $n_0 \leq n_1$, sonst ersetze σ durch $-\sigma$.
2) Es gilt $n_0 - t \in 4\mathbb{Z}$: Betrachte $C(\sigma)^* = (\pi_t(C(\sigma)), \pi_{n_0}(C(\sigma))) \leq \mathbb{F}_3^{t+n_0}$. Dieser Code ist selbst-dual bzgl. des inneren Produkts

$$(x, y) = -\sum_{i=1}^{t} x_i y_i + \sum_{i=t+1}^{t+n_0} x_i y_i,$$

was im ternären Fall nur möglich ist, wenn $n_0 - t$ ein Vielfaches von 4 ist.
3) Es gilt $t+n_0 \in \{12, 14, 16, 18\}$: Der Code $C(\sigma)^* \leq \mathbb{F}_3^{t+n_0}$ hat Dimension $(t+n_0)/2$ (also insbesondere ist $t + n_0$ gerade) und Minimalabstand $\geq \frac{12}{2} = 6$. Aus den Schranken von Codetables ([Gra]) folgt $t + n_0 \geq 12$. Aus $t + n_1 \geq t + n_0$ und $(t + n_1) + (t + n_0) = 36$ folgt außerdem $t + n_0 \leq 18$.
4) Es gilt $t + n_0 \neq 12$:
Die Möglichkeiten für (t, n_0, n_1) sind

t	n_0	n_1
12	0	12
10	2	14
8	4	16
6	6	18
4	8	20
2	10	22
0	12	24

Für $(t, n_0, n_1) = (0, 12, 24)$ gilt $\pi(\sigma) = 1$, was ausgeschlossen ist. Alle anderen Fälle, außer (12,0,12), werden durch Bemerkung 2.28 ausgeschlossen. Sei in diesem Fall

$$\begin{pmatrix} B & 0 \\ 0 & D \\ E & F \end{pmatrix} \in \mathbb{F}_3^{18\times(24+12)}$$

eine Erzeugermatrix von C nach Lemma 2.3. Es muss $d(\mathcal{D}) \geq 12$ gelten, was nur möglich ist, wenn $\dim(\mathcal{D})$ gleich 0 oder 1 ist.
1. Fall: $\dim(\mathcal{D}) = 0$. Dann gilt $\dim(\mathcal{E}) = \dim(\mathcal{F}) = 12$ und damit $\dim(\mathcal{B}) = 6$. Es gilt $C(\sigma) = \mathcal{B}(\sigma)$ (da $n_0 = 0$), also ist $C(\sigma)^* = \pi_t(\mathcal{B}(\sigma)) \leq \mathbb{F}_3^{12}$ selbst-dual mit Minimalabstand ≥ 6 und daher isomorph zu dem einzigen extremalen, ternären Code der Länge 12, XQ_{11}. Dann hat $\mathcal{B}$ die Form $XQ_{11} \otimes \begin{pmatrix} 1 & 1 \end{pmatrix}$ und es gilt

$$E = \begin{pmatrix} 1 & -1 & 0 & \dots & 0 & 0 & 0 \\ & & & \ddots & & & \\ 0 & 0 & 0 & \dots & 0 & 1 & -1 \end{pmatrix} = I_{12} \otimes \begin{pmatrix} 1 & -1 \end{pmatrix} \in \mathbb{F}_3^{12\times 24}.$$

Diese Basisvektoren müssen mit Vektoren von Gewicht 10 verklebt werden. Seien $v, w \in \mathcal{F}$ zwei Codewörter mit Gewicht 10. Angenommen, es gibt eine Stelle, an denen v und w beide 0 sind. Dann sind diese an mindestens 9 gemeinsamen Stellen ungleich 0 und stimmen an mindestens 5 davon überein (nachdem v eventuell durch $-v$ ersetzt wurde). Dann ist aber $v - w$ ein Codewort mit Gewicht ≤ 7, was nach der Verklebung ein Codewort mit Gewicht ≤ 11 liefert. Die Vektoren, die mit E verklebt werden, dürfen also an keiner gemeinsamen Stelle 0 sein. Das ist aber bei 12 Vektoren nicht möglich.
2. Fall: $\dim(\mathcal{D}) = 1$. Dann gilt $\dim(\mathcal{F}) = 10$ und $\dim(\mathcal{B}) = 7$, daraus folgt $B = \begin{pmatrix} XQ_{11} \otimes \begin{pmatrix} 1 & 1 \end{pmatrix} \\ v \end{pmatrix}$ mit einem $v \in \mathbb{F}_3^{24}$. Es gilt

$$\langle \begin{pmatrix} v \\ E \end{pmatrix} \rangle \subseteq \langle \begin{pmatrix} 1 & -1 & 0 & \dots & 0 & 0 & 0 \\ & & & \ddots & & & \\ 0 & 0 & 0 & \dots & 0 & 1 & -1 \end{pmatrix} \rangle,$$

und da $\langle \begin{pmatrix} v \\ E \end{pmatrix} \rangle$ Dimension 11 hat, enthält das Erzeugnis also mindestens 10 Vektoren von Gewicht 2. Der Rest der Argumentation folgt jetzt wie im 1. Fall.
5) Es gilt $t + n_0 \neq 14$:
Die Möglichkeiten für (t, n_0, n_1) sind

t	n_0	n_1
13	1	9
11	3	11
9	5	13
7	7	15
5	9	17
3	11	19
1	13	21

Bemerkung 2.28 schließt alle Fälle außer $(1, 13, 21)$ aus, für diesen Fall liefert Bemerkung 2.29 den Widerspruch.
6) Es gilt $t + n_0 \neq 18$.
Die Möglichkeiten für (t, n_0, n_1) sind

t	n_0	n_1
17	1	1
15	3	3
13	5	5
11	7	7
9	9	9
7	11	11
5	13	13
3	15	15
1	17	17

Die Fälle $(15, 3, 3)$ und $(7, 11, 11)$ werden durch Bemerkung 2.28 ausgeschlossen, der Widerspruch im Fall $(17, 1, 1)$ folgt aus Bemerkung 2.30, alle anderen Fälle werden durch Bemerkung 2.29 ausgeschlossen.
7) Aus $t + n_0 = 16$ folgt $(t, n_0, n_1) = (16, 0, 4)$:
Die Möglichkeiten für (t, n_0, n_1) sind

t	n_0	n_1
16	0	4
14	2	6
12	4	8
10	6	10
8	8	12
6	10	14
4	12	16
2	14	18
0	16	20

Für $(t, n_0, n_1) = (0, 16, 20)$ gilt $\pi(\sigma) = 1$. Die Fälle $(12, 4, 8)$, $(10, 6, 8)$, $(8, 8, 12)$ und $(6, 10, 14)$ werden durch Bemerkung 2.28 ausgeschlossen, zusätzlich wird der Fall $(14, 2, 6)$ durch Bemerkung 2.30 ausgeschlossen, Bemerkung 2.29 liefert

in den Fällen $(4, 12, 16)$ und $(2, 14, 18)$ einen Widerspruch. Der einzige verbliebene Fall ist $(16, 0, 4)$, der Pless-Code P_{36} hat einen Automorphismus dieser Form. □

Satz 4.2. *Sei $C \leq \mathbb{F}_3^{36}$ ein ternärer, extremaler Code der Länge 36 mit einem Automorphismus $\sigma \neq -1$ der Ordnung 2. Dann ist C isomorph zum Pless-Code P_{36}.*

Beweis. Nach Satz 4.1 gilt ohne Einschränkung

$$\sigma = \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{16}, (-1)^4 \right).$$

Aus $n_0 = 0$ folgt, dass π_t injektiv ist und zusätzlich $\pi_t(C(\sigma))$ ein selbst-dualer Code in $\mathbb{F}_3^{16}$ mit Minimalabstand $\geq \left\lceil \frac{12-n_0}{2} \right\rceil = 6$ ist. Aus [CPS79] folgt, dass $\pi_t(C(\sigma))$ isomorph zu dem Code CPS_{16} ist, daher gilt $C(\sigma) = CPS_{16} \otimes \begin{pmatrix} 1 & 1 \end{pmatrix}$. Sei

$$\begin{pmatrix} B & 0 \\ 0 & D \\ E & F \end{pmatrix} \text{ mit } B \in \mathbb{F}_3^{k_1 \times 32},\ D \in \mathbb{F}_3^{k_2 \times 4},\ E \in \mathbb{F}_3^{(18-k_1-k_2)\times 32},\ F \in \mathbb{F}_3^{(18-k_1-k_2)\times 4}$$

eine Erzeugermatrix von C nach Lemma 2.3. Dann folgt sofort $D = 0$ (sonst wäre $d(C) \leq 4$), also folgt

$$B \in \mathbb{F}_3^{14\times 32},\ E \in \mathbb{F}_3^{4\times 32} \text{ und } F \in \mathbb{F}_3^{4\times 4}.$$

Es gilt zusätzlich $C(\sigma) = \mathcal{B}(\sigma)$, also ist

$$B = \begin{pmatrix} CPS_{16} \otimes \begin{pmatrix} 1 & 1 \end{pmatrix} \\ X \otimes \begin{pmatrix} 1 & -1 \end{pmatrix} \end{pmatrix} \text{ mit } X \in \mathbb{F}_3^{6\times 16} \text{ und } \langle X \rangle \leq \langle X \rangle^{\perp}.$$

Daraus folgt, dass

$$\mathcal{B}_E = \mathcal{B}^{\perp} = \left(CPS_{16} \otimes \begin{pmatrix} 1 & 1 \end{pmatrix} \right) \oplus \left(\langle X \rangle^{\perp} \otimes \begin{pmatrix} 1 & -1 \end{pmatrix} \right)$$

gilt, insbesondere ist der Minimalabstand von $\langle X \rangle^{\perp}$) mindestens 4. Es existiert ein selbst-dualer Code D mit $\langle X \rangle \leq D = D^{\perp} \leq \langle X \rangle^{\perp}$ und Minimalabstand ≥ 4, dann gilt bereits $d(D) = 6$ und D ist nach [CPS79] isomorph zu CPS_{16}. Gesucht sind nun alle 6-dimensionalen Teilcodes von CPS_{16}, deren Duales $d \geq 4$ erfüllt. Davon gibt es (unter der Operation von $\mathrm{Aut}(CPS_{16})$) 5 Stück.
Von diesen 5 kommt allerdings nur ein einziger in Frage: Seien $v, w \in \langle X \rangle^{\perp}$ mit Gewicht 4. Dann müssen $v \otimes \begin{pmatrix} 1 & -1 \end{pmatrix}$ und $w \otimes \begin{pmatrix} 1 & -1 \end{pmatrix}$ mit Vektoren $v', w' \in \mathcal{F}$ von Gewicht 4 verklebt werden. Falls $v + w$ Gewicht 4 hat, muss dies auch für $v' + w'$ gelten, dann folgt bereits $v' = w'$ und $v - w$ muss in $\langle X \rangle$ enthalten sein. Von den 5 möglichen Codes gibt es nur einen, der dies für alle möglichen Paare

v, w erfüllt. Sei ab nun $\langle X \rangle$ dieser Code. Gesucht sind alle Matrizen

$$\begin{aligned} &M \in \mathbb{F}_3^{8\times 16},\ \langle M \rangle = CPS_{16}, \\ &N \in \mathbb{F}_3^{10\times 16},\ \langle N \rangle = \langle X \rangle^{\perp} \text{ und} \\ &F \in \mathbb{F}_3^{4\times 4}, \end{aligned}$$

so dass

$$\left(\begin{array}{c|c} M \otimes \begin{pmatrix} 1 & 1 \end{pmatrix} & 0_{14\times 4} \\ N \otimes \begin{pmatrix} 1 & -1 \end{pmatrix} & F \end{array}\right) \in \mathbb{F}_3^{18\times 36}$$

einen extremalen Code erzeugt. Seien M, N beliebige Erzeugermatrizen von CPS_{16} bzw. $\langle X \rangle$, dann wird ein geeignetes Vertretersystem von

$$\{(M \cdot g_1, N \cdot g_2) \mid g_1, g_2 \in \mathrm{Mon}_{16}(\mathbb{F}_3)\}$$

gesucht. Durch die Operation von $\mathrm{Mon}_{36}(\mathbb{F}_3)$ kann $g_1 = 1$ angenommen werden. Außerdem gilt

$$\begin{aligned} &\{\langle M \rangle \oplus \langle N \rangle \cdot g \mid g \in \mathrm{Mon}_{16}(\mathbb{F}_3)\} \\ =&\{\langle M \rangle \oplus \langle N \rangle \cdot g \mid \mathrm{Aut}(\langle N \rangle) \cdot g \in \mathrm{Aut}(\langle N \rangle) \backslash \mathrm{Mon}_{16}(\mathbb{F}_3)\} \\ =&\{\langle M \rangle \oplus \langle N \rangle \cdot g \mid \mathrm{Aut}(\langle N \rangle) \cdot g \cdot \mathrm{Aut}(\langle M \rangle) \in \mathrm{Aut}(\langle N \rangle) \backslash \mathrm{Mon}_{16}(\mathbb{F}_3) / \mathrm{Aut}(\langle M \rangle\}. \end{aligned}$$

Hier reicht es, nur den Permutationsanteil zu betrachten, dann nach Tensorieren mit $\begin{pmatrix} 1 & -1 \end{pmatrix}$ bedeutet ein Vorzeichenwechsel nur eine Permutation von zwei benachbarten Stellen, dies verändert aber $M \otimes \begin{pmatrix} 1 & 1 \end{pmatrix}$ nicht. Sei also

$$^{-} : \mathrm{Mon}_n \to S_n$$

die natürliche Projektion auf S_n, dann sind die Isomorphieklassen von

$$\{\langle M \rangle \oplus \langle N \rangle \cdot g \mid \mathrm{Aut}(\langle N \rangle) \cdot g \cdot \mathrm{Aut}(\langle M \rangle) \in \mathrm{Aut}(\langle N \rangle) \backslash \mathrm{Mon}_{16}(\mathbb{F}_3) / \mathrm{Aut}(\langle M \rangle\}$$

gleich den Isomorphieklassen von

$$\{\langle M \rangle \oplus \langle N \rangle \cdot g \mid \overline{\mathrm{Aut}(\langle N \rangle)} \cdot g \cdot \overline{\mathrm{Aut}(\langle M \rangle)} \in \overline{\mathrm{Aut}(\langle N \rangle)} \backslash S_{16} / \overline{\mathrm{Aut}(\langle M \rangle}\}.$$

Zusätzlich kann angenommen werden, dass die letzten 4 Zeilen von N aus Vektoren mit Gewicht 4 bestehen. Dann gilt $F \in \{\pm 1\}^{4\times 4}$, durch die Operation von $\mathrm{Mon}_4(\mathbb{F}_3)$ kann dann ohne Einschränkung

$$F = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

angenommen werden. Sei nun $\{g_1, \ldots, g_k\}$ ein Vertretersystem der Doppelnebenklassen von

$$\overline{\mathrm{Aut}(\langle N \rangle)} \backslash S_{16} / \overline{\mathrm{Aut}(\langle M \rangle}},$$

und betrachte alle Codes, die von

$$\left(\begin{array}{c|c} M \otimes \begin{pmatrix} 1 & 1 \end{pmatrix} & 0_{14\times 4} \\ N \cdot g_i \otimes \begin{pmatrix} 1 & -1 \end{pmatrix} & F \end{array} \right)$$

erzeugt werden. Es gilt $k = 1.912.082$ und alle so konstruierten extremalen Codes sind isomorph zum Pless-Code P_{36}. □

Automorphismen der Ordnung 3

Für einen ternären, extremalen Code $C = C^\perp \leq \mathbb{F}_3^{36}$ der Länge 36 mit Minimalabstand $d(C) = 12$ und einem Automorphismus $g \in \mathrm{Aut}(C)$ von Ordnung 3 gilt ohne Einschränkung

$$g = (1,2,3)\ldots(3t-2, 3t-1, 3t)(3t+1)\ldots(36)$$

für ein $1 \leq t \leq 12$. Sei $f := 36 - 3t$ die Anzahl der Fixpunkte von g.

Satz 4.3. *Seien C und g wie oben, dann gilt $t = 12$ und $f = 0$.*

Beweis. Seien $\mathcal{B}^*, \mathcal{B}_E \leq \mathbb{F}_3^{3t}$ die Codes nach Lemma 2.3 (mit $n_1 = 3t$ und $n_2 = f$). Diese sind g'-invariant für $g' = (1,2,3)\ldots(3t-2, 3t-1, 3t)$ und können daher als Teilcodes in dem freien Modul $V = \mathbb{F}_3[g']^t$ aufgefasst werden. Es gilt

$$\mathcal{B}^* \subseteq (\mathcal{B}^*)^\perp = \mathcal{B}_E \leq \mathbb{F}_3^{3t} \cong V.$$

Da $\mathcal{B}_E \cdot (1 - g')$ in $\mathcal{B}^*$ enthalten ist, impliziert Lemma 3.3, dass der Typ (t_0, t_1, t_2) von $\mathcal{B}^* \cong S_0^{t_0} \oplus S_1^{t_1} \oplus S_2^{t_2}$ die Ungleichungen

$$\begin{array}{lcl} 2t_0 + 2t_1 + t_2 & \geq & t \\ 2t_0 + t_1 + t_2 & \leq & t \\ 2t_0 + 2t_1 & \leq & t \end{array}$$

erfüllt. Wende nun Lemma 3.6 auf den Code $\mathcal{B}^*$ an. Es gilt $\mathcal{B}_E \cdot (1 - g') \subseteq \mathcal{B}^*$ und $\mathrm{soc}(\mathcal{B}^*) = \mathcal{B}^*(g')$, also folgt aus Lemma 3.6 und Bemerkung 3.7

$$\Phi(\mathcal{B}_E) \subseteq \Phi(\mathcal{B}_E)^\perp = \pi(\mathcal{B}^*(g')).$$

Insbesondere ist $\pi(\mathcal{B}^*(g')) \leq \mathbb{F}_3^t$ das Duale eines selbst-orthogonalen Codes der Länge t, Dimension $t_0 + t_1 + t_2 \geq \frac{t}{2}$ und Minimalabstand $\geq \frac{12}{3} = 4$ und enthält damit das Duale eines maximal selbst-orthogonalen Codes. Aus den Schranken von [Mey10] folgt nun, dass $t = 10$, $t = 11$ oder $t = 12$ gilt, in jedem Fall ist also $f < 12 = d(C)$, also ist $\mathcal{D}^* = 0$ und $\dim(\mathcal{B}^*) = 3t_0 + 2t_1 + t_2 = 18 - f$.
Im Fall $t = 10$ hat der Code $\pi(\mathcal{B}^*(g')) = \Phi(\mathcal{B}_E)^\perp$ mindestens Dimension 6, nach

der Griesmer-Schranke ([HP03, Theorem 2.7.4]) ist Dimension 7 ausgeschlossen. Also gilt $t_0+t_1+t_2 = 6$, zusammen mit den Schranken aus Lemma 3.3 folgt, dass der Typ von $\mathcal{B}^*$ gleich $(1,4,1)$ oder $(2,2,2)$ ist, der Typ von $\mathcal{B}_E$ ist dann dementsprechend $(4,1,4)$ bzw. $(4,2,2)$. Aus [HMa] folgt, dass es fünf maximal selbstorthogonale Code der Länge 10 gibt, von diesen erfüllt nur einer, dass der Minimalabstand des dualen Codes 4 ist. Sei C' dieser Code. Damit ist $\pi(\mathcal{B}^*(g')) = C'^{\perp}$ und $\pi(\mathcal{B}_E^*(g'))$ ist ein Obercode von Dimension 9 oder 8 von $C'^{\perp}$ mit Minimalabstand $\geq \frac{12-f}{3} = 2$. Unter der Operation von $\mathrm{Aut}(C')$ gibt es einen eindeutigen solchen Obercode X von Dimension 8. Dieser Code enthält zwei Elemente $c_1 \neq \pm c_2$ vom Gewicht 2 mit $|\operatorname{supp}(c_1) \cap \operatorname{supp}(c_2)| = 3$. Ohne Einschränkung enthält daher $\mathcal{B}_E^*$ die Elemente

$$x_1 = (c_1 \otimes \begin{pmatrix}1 & 1 & 1\end{pmatrix}, 1^6)$$
$$x_2 = (c_2 \otimes \begin{pmatrix}1 & 1 & 1\end{pmatrix}, 1^e, (-1)^{6-e}) \text{ für ein } e,$$

aber dann hat x_1+x_2 oder x_1-x_2 ein Gewicht von ≤ 11, also ist C nicht extremal. Im Fall $t = 11$, existiert nach [HMa] ein eindeutiger maximal selbst-orthogonaler Code der Länge 11, dessen Duales Minimalabstand ≥ 4 hat. Unter der Operation der Automorphismengruppe existieren zwei Obercodes mit Minimalabstand 1 bzw. 2. Also hat $\pi(\mathcal{B}^*(g'))$ Dimension 6 und mit den Schranken aus Lemma 3.3 ist der Typ von $\mathcal{B}^*$ gleich $(4,1,1)$ und der von $\mathcal{B}_E^*$ ist $(5,1,1)$, also ist $\pi(\mathcal{B}_E^*(g'))$ ein Obercode von $\pi(B^*(g'))$ von Dimension 7. Allerdings haben alle 7-dimensionalen Obercodes von $\pi(B^*(g'))$ einen Minimalabstand von ≤ 2, also gilt $d(C(g)) \leq 9$ und C ist nicht extremal. Also bleibt nur der Fall $t = 12$ und $f = 0$. □

Es müssen also alle extremalen Codes $C \leq \mathbb{F}_3^{36}$ mit

$$g = (1,2,3)\ldots(34,35,36) \in \mathrm{Aut}(C)$$

klassifiziert werden. Da g fixpunktfrei ist, ist $\mathbb{F}_3^{36} = V \cong \mathbb{F}_3[g]^{12}$ ein freier Modul vom Rang 12. Darin ist C ein freier Modul vom Rang 6:

Lemma 4.4. *Nach Satz 3.8 genügt es zu zeigen, dass $\pi(\mathrm{soc}(C))$ ein selbst-dualer Code in $(\mathbb{F}_3^{12}, \cdot)$ ist. Dies ist immer das Duale eines selbst-orthogonalen Codes und hat Minimalabstand ≥ 4. Die die Länge 12 ist, enthält dieser Code also einen selbst-dualen Code, der dann schon den Minimalabstand 6 haben muss. Dieser Code ist eindeutig ([MPS76]) und gerade der erweiterte quadratische Restklassen-Code XQ_{11}. Eine einfache Rechnung in* MAGMA *zeigt, dass kein echter Obercode von XQ_{11} einen Minimalabstand von ≥ 4 hat. Also gilt $\mathrm{soc}(C) = C \cdot (1-g)^2$ und C ist ein freier Modul von Rang 6.*

Folgerung 4.5. *Der Code C enthält den Teilcode $C^{(2)} = XQ_{11} \otimes \begin{pmatrix}1 & 1 & 1\end{pmatrix}$.*

Nun kann Algorithmus 3.18 angewendet werden. Der Zentralisator von g in $\mathrm{Aut}(C^{(2)})$ hat 16 Bahnen auf allen 3^{21} selbst-dualen Komplementen von $X_1 \leq W_1$, welche zu Kandidaten für Codes $C^{(1)}$ mit Minimalabstand ≥ 12 korrespondieren. Für diese 16 Codes wurden alle 3^{15} Komplemente von $X_0 \leq W_0$ überprüft,

bis auf Isomorphie existiert nur ein Code $C^{(0)}$ mit Minimalabstand 12, der Pless-Code P_{36}. Also wurde gezeigt:

Satz 4.6. *Sei $C = C^\perp \leq \mathbb{F}_3^{36}$ ein ternärer, extremaler Code mit einem Automorphismus der Ordnung 3. Dann ist C isomorph zum Pless-Code P_{36}.*

Zusammen mit Satz 4.2 folgt damit:

Satz 4.7. *Sei $C = C^\perp \leq \mathbb{F}_3^{36}$ ein ternärer, extremaler Code. Dann ist C isomorph zum Pless-Code P_{36} oder $\mathrm{Aut}(C)$ ist in $C_8 = \langle g \mid g^4 = -1 \rangle$ enthalten.*

Zusammen mit einem Automorphismus g der Ordnung 8 mit $g^4 = -1$ wird C zu einem sogenannten LCD-Code („linear complementarity dual", d.h. es gilt $C \cap C^\perp = \{0\}$), eine Klassifikation dieser Codes erscheint zu aufwendig.

4.2 Codes der Länge 48

Automorphismen der Ordnung 4

Lemma 4.8 ([Neb12c, Remark 3.7.])**.** *Sei $C \leq \mathbb{F}_3^{48}$ ein ternärer, extremaler Code der Länge 48 und sei $\sigma \in \mathrm{Aut}(C)$ ein Automorphismus der Ordnung 4. Dann gilt $\sigma^2 = -1$ oder σ^2 ist konjugiert zu $\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{24}\right)$.*

In dem Paper wurde angemerkt, dass für die beiden bekannten extremalen Codes der Länge 48, XQ_{47} und P_{48}, jeder solche Automorphismus $\sigma^2 = -1$ erfüllt. Dies stimmt allgemein für extremale Codes der Länge 48:

Satz 4.9. *Sei $C \leq \mathbb{F}_3^{48}$ ein ternärer, extremaler Code der Länge 48 und sei $\sigma \in \mathrm{Aut}(C)$ ein Automorphismus der Ordnung 4. Dann gilt $\sigma^2 = -1$.*

Beweis. Sei $\sigma \in \mathrm{Aut}(C)$, so dass σ^2 zu $\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{24}\right)$ konjugiert ist. Dann gilt ohne Einschänkung

$$\sigma = \left(\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}^{12}\right)$$

und der Code C zerfällt in die direkte Summe

$$C = C(\sigma) \oplus C_-(\sigma) \oplus C_i(\sigma) \oplus C_{-i}(\sigma).$$

Die Codes $C(\sigma)$ und $C_-(\sigma)$ sind der Fix- und Antifixcode von σ. Der Teilcode $C_i(\sigma)$ besteht aus Blöcken der Form $\begin{pmatrix} -a & -b & a & b \end{pmatrix}$, auf diesem operiert σ also als 4. Einheitswurzel (analog für $C_{-i}(\sigma)$). Es gilt

$$C(\sigma) = \langle M \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \rangle \text{ und}$$
$$C_-(\sigma) = \langle M' \otimes \begin{pmatrix} 1 & -1 & 1 & -1 \end{pmatrix} \rangle,$$

wobei die Matrizen $M, M' \in \mathbb{F}_3^{6\times 12}$ selbst-duale Codes in $\mathbb{F}_3^{12}$ mit Minimalabstand $\geq \frac{15}{4}$ erzeugen. Insbesondere sind diese selbst-dualen Codes also extremal und nach [HMb] eindeutig. Die möglichen Erzeugermatrizen von $C(\sigma) \oplus C_-(\sigma)$ sind dann gegeben durch

$$\begin{pmatrix} M \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \\ M' \cdot g \otimes \begin{pmatrix} 1 & -1 & 1 & -1 \end{pmatrix} \end{pmatrix},\ g \in \mathrm{Mon}_{12}(\mathbb{F}_3).$$

Für den Fall, dass $g = \mathrm{diag}(a_1, \ldots, a_{12}), a_i \neq 0$, ohne Permutationsanteil ist, kann auf jeden Block, für den $a_i = -1$ gilt, die Permutation $(1,2)(3,4)$ angewendet werden. Diese Abbildung fixiert $M \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$ und bildet

$$\begin{pmatrix} M \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \\ M' \cdot g \otimes \begin{pmatrix} 1 & -1 & 1 & -1 \end{pmatrix} \end{pmatrix} \text{ auf } \begin{pmatrix} M \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \\ M' \otimes \begin{pmatrix} 1 & -1 & 1 & -1 \end{pmatrix} \end{pmatrix}$$

ab, es reicht es also, nur den Permutationsanteil zu betrachten. Sei

$$^- : \mathrm{Mon}_n(\mathbb{F}) \to S_n$$

die natürliche Projektion, dann ist ein möglicher Code $C(\sigma) \oplus C_-(\sigma)$ isomorph zu einem Code mit Erzeugermatrix der Form

$$\begin{pmatrix} M \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \\ M' \cdot g \otimes \begin{pmatrix} 1 & -1 & 1 & -1 \end{pmatrix} \end{pmatrix}, \overline{\mathrm{Aut}(\langle M' \rangle)} \cdot \overline{g} \cdot \overline{\mathrm{Aut}(\langle M \rangle)} \in \overline{\mathrm{Aut}(\langle M' \rangle)} \backslash S_{12} / \overline{\mathrm{Aut}(\langle M \rangle)}$$

Dies ergibt nur eine Möglichkeit mit Minimalabstand ≥ 15, also ist $C(\sigma) \oplus C_-(\sigma)$ bis auf Isomorphie eindeutig.
Der Teilcode $C_i(\sigma)$ kann als hermitesch selbst-dualer Code in $\mathbb{F}_9^{12}$ aufgefasst werden. Diese sind gegeben durch selbst-duale Codes in $\mathbb{F}_3^{24}$, welche einen Automorphismus haben, der als 4. Einheitswurzel operiert. Die Erzeugermatrix für $C_i(\sigma) \leq \mathbb{F}_3^{48}$ erhält man dann durch die Abbildung

$$\varepsilon : \mathbb{F}_9 \to \mathbb{F}_3^4, a + ib \mapsto \begin{pmatrix} -a & -b & a & b \end{pmatrix}.$$

Insgesamt existieren 417 hermitesch selbst-duale Codes $D \leq \mathbb{F}_9^{12}$, 4 davon erfüllen, dass der Minimalabstand von $\varepsilon(D) + \varepsilon(D) \cdot \sigma$ mindestens 15 ist.
Der Code $C(\sigma) \oplus C_-(\sigma)$ ist bis Isomorphie eindeutig gegeben, eine Erzeugermatrix N kann hier so gewählt werden, dass diese aus 2×4-Blöcken der Form $\begin{pmatrix} a & b & a & b \\ b & a & b & a \end{pmatrix}$ besteht. Alle möglichen Codes C haben nun eine Erzeugermatrix der Gestalt

$$\begin{pmatrix} N \\ \varepsilon(D \cdot g) \\ \varepsilon(D \cdot g) \cdot \sigma \end{pmatrix},\ g \in \langle i \rangle \wr S_{12}.$$

Allerdings gilt

$$\varepsilon(i(a+ib)) = \varepsilon(-b+ia) = \begin{pmatrix} b & -a & -b & a \end{pmatrix} = \varepsilon(a+ib) \cdot \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

und, da $\sigma = \left(\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}^{12} \right)$ in $\mathrm{Aut}(\langle N \rangle)$ enthalten ist, operiert $\langle i \rangle$ trivial auf $\langle N \rangle$. Also reicht es, die Matrizen

$$\begin{pmatrix} N \\ \varepsilon(D \cdot g) \\ \varepsilon(D \cdot g) \cdot \sigma \end{pmatrix}, \; g \cdot \overline{\mathrm{Aut}(\langle N \rangle)} \in S_{12}/\overline{\mathrm{Aut}(\langle N \rangle)}$$

zu betrachten. Kein so konstruierter Code ist extremal. □

Automorphismen der Ordnung 3

Satz 4.10. *Sei $C \leq \mathbb{F}_3^{48}$ ein ternärer, extremaler Code der Länge 48 und sei ohne Einschränkung*

$$g = (1,2,3)\dots(3t-2,3t-1,3t)(3t+1)\dots(48) \in \mathrm{Aut}(C)$$

ein Element von Ordnung 3. Dann hat g keine Fixpunkte, d.h. es gilt $t = 16$ und $f := 38 - 3t = 0$.

Beweis. Sei

$$\begin{pmatrix} B & 0 \\ 0 & D \\ E & F \end{pmatrix}$$

eine Erzeugermatrix von C nach Lemma 2.3 (mit $n_1 = 3t$ und $n_2 = f$). Da der Minimalabstand von C gleich 15 ist, ist der Minimalabstand von $\pi(\mathcal{B}(g)) \leq \mathbb{F}_3^t$ mindestens 5, und da $\pi(\mathcal{B}(g))$ das Duale des selbst-orthogonalen Codes $\Phi(C)$ ist, ist die Dimension von $\pi(\mathcal{B}(g))$ also mindestens $\frac{t}{2}$. Aus den Schranken von Codetables ([Gra]) folgt damit $t \geq 10$.
Im Fall $t = 10$ folgt aus Codetables, dass die Dimension von $\pi(\mathcal{B}(g))$ höchstens 5 ist, also ist sie gleich 5 und der Code wäre selbst-dual in $\mathbb{F}_3^{10}$, was nicht möglich ist.
Im Fall $t = 11$ gilt $f = 15 = d(C)$ und $t + f = 26 < 2\dim(C) - 2 = 28$, ein Widerspruch zu [Huf92, Lemma 5].
Im Fall $t = 12$ folgt aus Codetables, dass die Dimension von $\pi(\mathcal{B}(g))$ höchstens 6 ist, also ist sie gleich 6 und der Code ist selbst-dual in $\mathbb{F}_3^{12}$. Aus den Ungleichungen von Lemma 3.3 folgt, dass $\mathcal{B}$ (als $\mathbb{F}_3[g]$-Modul) isomorph zu S_1^6 ist, damit

ist $\mathcal{B}_E$ nach Lemma 3.2 isomorph zu $S_0^6 \oplus S_2^6$. Es folgt, dass der Fixcode $C(g)$ 12-dimensional und $\pi(C(g))$ ist der komplette Raum $\mathbb{F}_3^{12}$, $C(g)$ hat dann eine Erzeugermatrix der Form

$$\left(\begin{array}{ccc|c} 111 & & & \\ & \ddots & & A \\ & & 111 & \end{array}\right),\ A \in \{\pm 1\}^{12\times 12}.$$

Der Minimalabstand ist dann aber kleiner als 15.
Im Fall $t = 13$ folgt aus Codetables, dass die Dimension von $\pi(\mathcal{B}(g))$ gleich 7 ist, der Code ist das Duale eines maximal selbst-orthogonalen Codes in $\mathbb{F}_3^{13}$. Aus der Klassifikation dieser Code ([HMa]) folgt aber, dass $\pi(\mathcal{B}(g))$ höchstens den Minimalabstand 4 haben kann.
Im Fall $t = 14$ folgt aus Codetables, dass die Dimension von $\pi(\mathcal{B}(g))$ höchstens 8 ist. Da $\mathbb{F}_3^{14}$ keinen selbst-dualen Code enthält, muss sie 8 sein. Dann folgt aus der Klassifikation ([HMa]) wieder, dass der Minimalabstand höchstens 4 ist.
Im Fall $t = 15$ folgt aus Codetables, dass die Dimension von $\pi(\mathcal{B}(g))$ gleich 8 ist. Aus der Klassifikation [HMa] folgt, dass dieser (ohne Einschränkung) die Erzeugermatrix

$$\left(\begin{array}{c|ccccccc} & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ I_8 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right)$$

hat. Aus den Ungleichungen von Lemma 3.3 folgt, dass $\mathcal{B}$ als $\mathbb{F}_3[g]$-Modul isomorph zu $S_0^6 \oplus S_1 \oplus S_2$ ist, also ist $\mathcal{B}_E$ nach Lemma 3.2 isomorph zu $S_0^7 \oplus S_1 \oplus S_2$ und $\pi(\mathcal{B}_E(g))$ ist ein 9-dimensionaler Obercode von $\pi(\mathcal{B}(g))$ mit Minimalabstand $\geq \frac{15-f}{3} = 4$. Davon existiert (unter der Operation der Automorphismengruppe) genau einer:

$$\pi(\mathcal{B}_E(g)) = \pi(\mathcal{B}(g)) + \langle \underbrace{(1,0,0,-1,0,0,0,0,1,0,0,0,0,1,0)}_{=:y} \rangle.$$

Die Vektoren von Gewicht 4 bilden ein Erzeugendensystem von $\pi(\mathcal{B}_E(g))$. Diese können mit $(1,1,1)$ bzw. $(-1,-1,-1)$ verklebt werden, um $C(g)$ zu erhalten (die Vektoren in der Klasse $\pm y + \pi(\mathcal{B}(g))$ werden mit $(\pm 1, \pm 1, \pm 1)$ verklebt). Dann enthält $C(g)$ das Wort

$$\mathbf{1} = (1, \ldots, 1) \in \mathbb{F}_3^{48},$$

aus Beispiel 2.10 folgt nun, dass alle Wörter von C mit vollem Gewicht entweder $\pm\mathbf{1}$ sind oder genauso oft 1 wie -1 enthalten. Dies erfüllt $C(g)$ allerdings nicht. Damit bleibt nur noch der Fall $t = 16$ und g hat keine Fixpunkte. □

Bemerkung 4.11. *Analog zu Lemma 4.4 folgt auch in Länge 48, dass ein ternärer, extremaler Code mit einem Automorphismus g der Ordnung 3 ein freier $\mathbb{F}_3C_3$-Modul ist. In diesem Fall gilt nach [CPS79]*

$$\pi(\mathrm{soc}(C)) = \pi(C(g)) \cong CPS_{16}.$$

Theoretisch lassen sich also mit Algorithmus 3.18 alle ternären, extremalen Codes der Länge 48 mit einem Automorphismus der Ordnung 3 bestimmen, eine vollständige Klassifikation ist hier allerdings zu aufwendig. Die Eindeutigkeit kann aber unter einem zusätzlichem nicht-trivialen Automorphismus der Ordnung 2 gezeigt werden, d.h. die Automorphismengruppen enthält die Gruppe S_3 oder C_6.

Satz 4.12. *Sei $S_3 \cong A \leq \mathrm{Mon}_{48}(\mathbb{F}_3)$. Dann existiert kein ternärer, extremaler Code C der Länge 48 mit $A \leq \mathrm{Aut}(C)$.*

Beweis. Die Gruppe A wird von zwei Elementen σ bzw. g von Ordnung 2 bzw. 3 erzeugt. Falls $\sigma = -1$ gilt, wäre $\langle\sigma\rangle$ ein Normalteiler in A, was nicht möglich ist. Nach Satz 4.10 ist g in $\mathrm{Mon}_{48}(\mathbb{F}_3)$ konjugiert zu einer fixpunktfreien Permutation und σ ist nach [Neb12c] in $\mathrm{Mon}_{48}(\mathbb{F}_3)$ konjugiert zu $\left(\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}^{24}\right)$ oder zu $\left(\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}^{22}, (-1)^2, 1^2\right)$. Letzteres kann mit einer fixpunktfreien Permutation der Ordnung 3 keine Gruppe erzeugen, die isomorph zu S_3 ist, sei also ohne Einschränkung

$$\sigma = (1,2)(3,4)(5,6)\dots(43,44)(45,46)(47,48)$$
$$g = (1,3,5)(2,6,4)\dots(43,45,47)(44,48,46).$$

Es gilt $C = C(\sigma) \oplus C_-(\sigma)$, wobei

$$C(\sigma) = \langle M \otimes \begin{pmatrix}1 & 1\end{pmatrix}\rangle \text{ und}$$
$$C_-(\sigma) = \langle M' \otimes \begin{pmatrix}1 & -1\end{pmatrix}.$$

Die Matrizen $M, M' \in \mathbb{F}_3^{12\times 24}$ erzeugen selbst-duale Codes in $\mathbb{F}_3^{24}$, deren Minimalabstand mindestens $\frac{15}{2}$ sein muss, also sind diese bereits extremal. Dann gibt es bis auf Isomorphie je zwei Möglichkeiten (siehe [HMb]). Sei

$$(a_1, a_2, \dots, a_{24}) \otimes \begin{pmatrix}1 & 1\end{pmatrix} \in C(\sigma),$$

nach Anwenden von g enthält C also das Codewort

$$v := (a_3, a_2, a_1, a_3, a_2, a_1, \dots, a_{24}, a_{23}, a_{22}, a_{24}, a_{23}, a_{22})$$

und es gilt

$$v - v\sigma = (a_3-a_2, a_1-a_3, a_2-a_1, \dots, a_{24}-a_{23}, a_{22}-a_{24}, a_{23}-a_{22}) \otimes \begin{pmatrix}1 & -1\end{pmatrix} \in C_-(\sigma).$$

Insgesamt folgt also

$$\langle M\rangle \cdot \left(\left(\begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}^8 \right) \right) \subseteq \langle M'\rangle.$$

Damit ist bei gegebener Erzeugermatrix M von $C(\sigma)$ ein 8-dimensionaler Teilraum U von $\langle M'\rangle \leq \mathbb{F}_3^{12}$ bekannt. Die 4-dimensionalen Komplemente können in $\langle U\rangle^\perp/\langle U\rangle$ unter der Operation von $\mathrm{Stab}_{\mathrm{Mon}_{24}(\mathbb{F}_3)}(\langle U\rangle)$ bestimmt werden. Kein so konstruierter Code ist extremal. □

Satz 4.13. *Sei $C \leq \mathbb{F}_3^{48}$ ein ternärer, extremaler Code der Länge 48, so dass ein Element g der Ordnung 6 in $\mathrm{Aut}(C)$ mit $g^3 \neq -1$ existiert. Dann ist C isomorph zum Pless-Code P_{48}.*

Beweis. Als Element der Ordnung 3 hat g^2 nach Satz 4.10 keine Fixpunkte, also gilt dies auch für g. Dann kann angenommen werden, dass $\langle g\rangle$ von den beiden Elementen

$$\sigma_1 := g^3 = (1,2)(3,4)(5,6)\dots(47,48)$$
$$\sigma_2 := g^2 = (1,3,5)(2,4,6)\dots(44,46,48)$$

erzeugt wird. Es folgt $C = C(\sigma_1) \oplus C_-(\sigma_1)$ mit

$$C(\sigma_1) = \langle M \otimes \begin{pmatrix} 1 & 1 \end{pmatrix}\rangle \text{ und}$$
$$C_-(\sigma_1) = \langle M' \otimes \begin{pmatrix} 1 & -1 \end{pmatrix}\rangle.$$

Die Matrizen $M, M' \in \mathbb{F}_3^{12\times 24}$ erzeugen selbst-duale Codes in $\mathbb{F}_3^{24}$, da deren Minimalabstand mindestens $\frac{15}{2}$ sein muss, sind diese bereits extremal und es gibt bis auf Isomorphie je zwei Möglichkeiten ([HMb]). Sei

$$v = (a_1,\dots,a_{24}) \otimes \begin{pmatrix} 1 & 1 \end{pmatrix} \in C(\sigma),$$

dann gilt

$$v\cdot\sigma_2 = (a_3,a_1,a_2,\dots,a_{24},a_{22},a_{23}) \otimes \begin{pmatrix} 1 & 1 \end{pmatrix} \in C(\sigma),$$

also ist

$$g' = (1,2,3)\dots(22,23,24)$$

ein Automorphismus von $\mathrm{Aut}(\langle M\rangle)$ (dasselbe gilt analog auch für $\mathrm{Aut}(\langle M'\rangle)$). Die Erzeugermatrizen M und M' können nun so gewählt werden, dass diese Permutation in den Automorphismengruppen enthalten ist (da beide Codes nur eine Konjugiertenklasse von fixpunktfreien Elementen der Ordnung 3 haben, gibt es hierfür insgesamt 4 Möglichkeiten). Dann haben alle zulässigen, extremalen Codes $C \leq \mathbb{F}_3^{48}$ eine Erzeugermatrix der Form

$$\begin{pmatrix} M \otimes \begin{pmatrix} 1 & 1 \end{pmatrix} \\ M'\cdot\rho \otimes \begin{pmatrix} 1 & -1 \end{pmatrix} \end{pmatrix},\ \rho \in \mathrm{Cent}_{\mathrm{Mon}_{24}(\mathbb{F}_3)}(g').$$

Es gilt

$$\mathrm{Cent}_{\mathrm{Mon}_{24}(\mathbb{F}_3)}(g') = \underbrace{\langle -1, (1,2,3)\rangle}_{\leq \mathrm{Mon}_3(\mathbb{F}_3)} \wr S_8 \cong C_6 \wr S_8$$

und für

$$\rho \in \langle -1\rangle \wr S_8 \leq \mathrm{Cent}_{\mathrm{Mon}_{24}(\mathbb{F}_3)}(g')$$

sind die Erzeugnisse der beiden Matrizen $\begin{pmatrix} M \otimes \begin{pmatrix} 1 & 1 \end{pmatrix} \\ M' \cdot \rho \otimes \begin{pmatrix} 1 & -1 \end{pmatrix} \end{pmatrix}$ und $\begin{pmatrix} M \otimes \begin{pmatrix} 1 & 1 \end{pmatrix} \\ M' \otimes \begin{pmatrix} 1 & -1 \end{pmatrix} \end{pmatrix}$ isomorph. Betrachte also die Matrizen

$$\begin{pmatrix} M \otimes \begin{pmatrix} 1 & 1 \end{pmatrix} \\ M' \cdot \rho \otimes \begin{pmatrix} 1 & -1 \end{pmatrix} \end{pmatrix},\ \rho \cdot \langle g'\rangle \in \langle (1,2,3)\rangle \wr S_8 / \langle g'\rangle.$$

Jeder so konstruierte extremale Code ist isomorph zum Pless-Code P_{48}. □

Kapitel 5

Gruppencodes

Gruppencodes stießen auf Interesse, nachdem S. Berman 1967 gezeigt hat, dass der Reed-Muller-Code der Ordnung $m - l$ gerade die l-te Potenz des Jacobson-Radikals der Gruppenalgebra $\mathbb{F}_2 C_2^m$ ist [Ber69][1]. Zusätzlich studierte er zyklische Codes als Ideale in der Gruppenalgebra $\mathbb{F}C_n \cong \mathbb{F}[x]/(x^n - 1)$. Wenig später verallgemeinerte F. J. MacWilliams Eigenschaften zyklischer Codes auf Ideale in abelschen Gruppenalgebren ([Mac70]). Sie war außerdem die erste, die Gruppenalgebren über nicht-abelschen Gruppen betrachtete ([Mac69]).

In diesem Kapitel wird die Struktur von Gruppencodes über Kettenringen untersucht. Die Codes, die relativ projektiv für die Untergruppe $\{1\}$ im Sinne der homologischen Algebra sind, stehen in Bijektion zu Ketten von projektiven Codes über dem Restklassenkörper. Von diesen Ketten lassen sich dann direkt Eigenschaften wie der Minimalabstand oder der duale Code ablesen.

5.1 Gruppencodes über Körpern

Sei $\mathbb{F}$ ein endlicher Körper und $G = \{g_1, \ldots, g_n\}$ eine endliche Gruppe. Ein (Links-/Rechts-/zweiseitiger) Gruppen-Code C von G ist ein (Links-/Rechts-/zweiseitiges) Ideal in in der Gruppenalgebra $\mathbb{F}G$. Die Dimension von C ist die Dimension als $\mathbb{F}$-Vektorraum.

Eine Sortierung der Gruppenelemente definiert einen Isomorphismus

$$\phi : \mathbb{F}G \to \mathbb{F}^n, \sum_{i=1}^{n} a_i g_i \mapsto (a_1, \ldots, a_n)$$

zwischen den beiden $\mathbb{F}$-Vektorräumen $\mathbb{F}G$ und $\mathbb{F}^n$. Für einen Gruppencode $C \leq \mathbb{F}G$ ist dann $\phi(C) \leq \mathbb{F}^n$ ein linearer Code, so dass sich alle relevanten Eigenschaften übertragen. Damit lassen sich lineare Codes als Gruppencodes definieren.

Definition 5.1. *Ein linearer Code C der Länge n über $\mathbb{F}$ ist ein Gruppencode für die Gruppe G (kurz G-Code), falls eine Bijektion $\nu : \{1, \ldots, n\} \to G$ existiert, so dass die*

[1] Das Paper erschien 1967 auf russisch und wurde 1969 übersetzt.

Menge

$$\left\{ \sum_{i=1}^{n} a_i \nu(i) \mid (a_1, \ldots, a_n) \in C \right\}$$

ein Ideal in $\mathbb{F}G$ ist.

Für welche Gruppen G ein gegebener ein linearer Code ein Gruppencode ist, hängt dann von der Automorphismengruppe ab.

Satz 5.2 ([BRS09, Theorem 1.2.]). *Sei C ein linearer Code der Länge n über $\mathbb{F}$ mit Permutations-Automorphismengruppe $\mathrm{PAut}(C) := \mathrm{Aut}(C) \cap S_n$ and sei G eine endliche Gruppe der Ordnung n.*

i) C ist ein Links-G-Code, genau dann wenn $\mathrm{PAut}(C)$ eine transitive Untergruppe der symmetrischen Gruppe S_n enthält, welche isomorph zu G ist.

ii) C ist ein zweiseitiger G-Code, genau dann wenn G isomorph zu einer transitiven Untergruppe H von S_n ist, so dass $H \cup C_{S_n}(H) \subseteq \mathrm{PAut}(C)$ gilt.

Natürlich kann ein Code ein G-Code für verschiedene Gruppen G (der selben Ordnung) sein. Eine interessante Fragestellung ist also, welche Gruppen-Codes sich über besonders „schönen“ Gruppen realisieren lassen, also z.B. zyklische oder abelsche Gruppen.

Satz 5.3 ([BRS09, Theorem 3.1.]). *Eine Gruppe G hat eine abelsche Zerlegung, falls zwei abelsche Untergruppen A und B von G existieren, so dass G das Produkt*

$$G = AB := \{ab : a \in A, b \in B\}$$

ist. In diesem Fall ist jeder zweiseitige G-Code ein Gruppencode für eine abelsche Gruppe.

Insbesondere gilt dies also für jede Metazyklische Gruppe (also Gruppen mit einem Normalteiler, so dass die Faktorgruppe zyklisch ist). Im halbeinfachen Fall war dies bereits in [SL95] gezeigt worden, in Abschnitt 5.3.2 wird gezeigt, dass im Spezialfall der Diedergruppen jeder solche Code zyklisch ist.
In [Pil+12] wurde gezeigt, dass jede Gruppe von Ordnung < 128, mit Ausnahme von $24, 48, 54, 60, 64, 72, 96, 108$ und 120, eine abelsche Zerlegung besitzt. Das kleinste Gegenbeispiel ist die symmetrische Gruppe S_4 von Ordnung 24, hier gaben die Autoren einen zweiseitigen Code über $\mathbb{F}_5 S_4$ an, der kein abelscher Gruppencode ist. In [NS14] wurde ein Ideal in $\mathbb{F}_3 G$ für eine metabelsche Gruppe G der Ordnung $2^6 = 64$ angegeben, das kein abelscher Gruppencode ist. Alle kleineren p-Gruppen habe eine abelsche Zerlegung, also ist dies das kleinste Beispiel für einen nicht-abelschen, nilpotenten Gruppen-Code. Insbesondere wurde die Frage beantwortet, ob jeder nilpotente Gruppen-Code abelsch ist.

Gegenbeispiele lassen sich auch im nicht-halbeinfachen Fall recht einfach konstruieren. Die Gruppe G^2 operiert auf G durch

$$G^2 \times G \to G, ((g_1, g_2), g) \mapsto g_1 g g_2^{-1}.$$

Sei $H \leq S_{|G|}$ die Permutationsdarstellung dieser Operation, dann sind die Ideale von $\mathbb{F}H$ gerade die zweiseitigen Ideale von $\mathbb{F}G$. Damit können nicht-abelsche Codes als zyklische Moduln konstruiert werden.

Lemma 5.4. *Sei G eine Gruppe von Ordnung $|G| < 64$, welche keine abelsche Zerlegung besitzt (also insbesondere $|G| \in \{24, 48, 54, 60\}$). Dann existiert ein zweiseitiges Ideal in $\mathbb{F}_2 G$, welches kein abelscher Code ist.*

Definition 5.5. *Ein Gruppencode $C \leq \mathbb{F}G$ heißt (zentral) projektiv, falls ein (zentrales) Idempotent $e \in \mathbb{F}G$ existiert mit $C = \mathbb{F}Ge$.*

Sei $1 = e_1 + \cdots + e_s \in \mathbb{F}G$ die Zerlegung der $1 \in \mathbb{F}G$ in zentral primitive Idempotente, dann zerfällt $\mathbb{F}G$ in die direkte Summe von unzerlegbaren Teilalgebren

$$\mathbb{F}G = \mathbb{F}Ge_1 \oplus \cdots \oplus \mathbb{F}Ge_s.$$

Falls $\mathrm{char}(\mathbb{F})$ nicht $|G|$ teilt, ist die Gruppenalgebra nach dem Satz von Maschke halbeinfach, und nach dem Satz von Artin-Wedderburn ist jeder einfacher Summand $\mathbb{F}Ge_i$ ein Matrixring über einer (endlichen) Körpererweiterung von $\mathbb{F}$. Die Idempotente lassen sich hier also recht einfach bestimmen:

Bemerkung 5.6. *Sei $\mathbb{E}$ ein endlicher Körper und sei $m^2 = m \in \mathbb{E}^{l \times l}$ eine idempotente Matrix, dann ist m konjugiert zu*

$$\mathrm{Diag}(\underbrace{1, \ldots, 1}_{\mathrm{Rang}(m)}, \underbrace{0, \ldots, 0}_{l - \mathrm{Rang}(m)}).$$

Insbesondere ist die Anzahl aller Idempotente also

$$2 + \sum_{i=1}^{l-1} \frac{|\operatorname{GL}_l(\mathbb{E})|}{|\operatorname{GL}_i(\mathbb{E})| \cdot |\operatorname{GL}_{l-i}(\mathbb{E})|}.$$

Sei I ein Linksideal von $\mathbb{E}^{l \times l}$, dann gilt

$$I = \left\{ \begin{pmatrix} m_1 \\ \vdots \\ m_l \end{pmatrix} \mid m_i \in \mathcal{V} \right\}$$

für einen Vektorraum $\mathcal{V} \leq \mathbb{E}^l$. Da $\mathbb{E}^{l \times l}$ halbeinfach ist, existiert ein Idempotent, welches I erzeugt.

Folgerung 5.7. *Sei $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{E}^{2 \times 2}$ eine idempotente Matrix, dann tritt einer der folgenden Fälle ein:*

i) m ist zentral, also $m = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ oder $m = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

ii) $m = \begin{pmatrix} 0 & c \\ 0 & 1 \end{pmatrix}$, $c \in \mathbb{E}$ *beliebig.*

iii) $m = \begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}$, $c \in \mathbb{E}$ *beliebig.*

iv) $m = \begin{pmatrix} a & \frac{1-a}{c}a \\ c & 1-a \end{pmatrix}$, $c \neq 0, a \in \mathbb{E}$ *beliebig.*

Insgesamt gibt es also 2 zentrale und $|\mathbb{E}|+|\mathbb{E}|+|\mathbb{E}|\cdot(|\mathbb{E}|-1) = |\mathbb{E}|\cdot(|\mathbb{E}|+1)$ *nicht-zentrale Idempotente. Die Anzahl der Ideale ist* $|\mathbb{E}|+3$*, diese werden von den Idempotenten*

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \text{ und } \begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}, \text{ für alle } c \in \mathbb{E},$$

erzeugt.

Im nicht-halbeinfachen Fall sei $\mathfrak{J}_i$ das Jacobson-Radikal von $\mathbb{F}Ge_i$. Dann ist $\mathbb{F}Ge_i/\mathfrak{J}_i \cong \mathbb{E}^{l\times l}$ für eine Körpererweiterung $\mathbb{E}$ von $\mathbb{F}$, und da $\mathfrak{J}_i$ nilpotent ist, können die Idempotente zu Idempotente von $\mathbb{F}Ge_i$ geliftet werden.

Satz 5.8 ([Web16, Theorem 7.3.5])**.** *Sei I ein nilpotentes Ideal eines Rings A und e ein Idempotent in A/I. Dann existiert ein Idempotent $f \in A$ mit $e = f + I$. Falls e primitiv ist, gilt dies auch für jeden Lift f.*

Beweis. Die Behauptung wird gezeigt, indem für alle k induktiv Idempotente $e_k \in A/I^k$ definiert werden, so dass $e_k + I^{k-1}/I^k = e_{k-1}$ gilt, beginnend mit $e_1 = e$. Angenommen $e_{k-1} = r_{k-1} + I^{k-1}$ ist ein Idempotent von A/I^{k-1}. Wähle ein Urbild $a \in A/I^k$ von e_{k-1} mit $a^2 - a \in I^{k-1}/I$, zum Beispiel $a = r_{k-1} + I^k$. Da $(I^{k-1})^2$ in I^k enthalten ist, folgt $(a^2-a)^2 = 0 \in A/I^k$. Definiere $e_k = 3a^2 - 2a^3$. Dann gilt $e_k + I^{k-1} = e_{k-1}$ und außerdem

$$\begin{aligned} e_k^2 - e_k &= (3a^2 - 2a^3)(3a^2 - 3a^3 - 1) \\ &= -(3-2a)(1+2a)(a^2-a)^2 \\ &= 0. \end{aligned}$$

Angenommen, e ist primitiv und f zerfällt in orthogonale Idempotente $f = f_1 + f_2$. Dann zerfällt $e = e_1 + e_2$ in orthogonale Idempotente $e_i = f + I$. Also muss (ohne Einschränkung) $e_1 = 0 \in A/I$ gelten und es folgt $f_1^2 = f_1 \in I$. Als nilpotentes Ideal enthält I aber keine Idempotente $\neq 0$. □

Bemerkung 5.9. *Für ein Idempotent $e = r + \mathfrak{J}_i^{k-1} \in \mathbb{F}Ge_i/\mathfrak{J}_i^{k-1}$ ist die Menge aller Lifts gegeben durch*

$$\{3(r+j)^2 - 2(r+j)^3 + \mathfrak{J}_i^k \mid j \in \mathfrak{J}_i^{k-1}\}.$$

Falls $\mathbb{F}$ Charakteristik 2 hat, reduziert sich das zu

$$\{r^2 + jr + rj + \mathfrak{J}_i^k \mid j \in \mathfrak{J}_i^{k-1}\}.$$

Für ein festes $r \in \mathbb{F}Ge_i$ ist die Abbildung

$$\varphi_r : \mathfrak{J}_i^{k-1}/\mathfrak{J}_i^k \to \mathfrak{J}_i^{k-1}/\mathfrak{J}_i^k, j + \mathfrak{J}_i^k \mapsto rj + jr + \mathfrak{J}_i^k$$

$\mathbb{F}$-linear und das Bild bestimmt gerade alle Lifts von $r + \mathfrak{J}_i^{k-1}$.

Bemerkung 5.10. *Die Bilinearform*

$$(\cdot,\cdot) : \mathbb{F}G \times \mathbb{F}G \to \mathbb{F}, \left(\sum_{i=1}^n a_i g_i, \sum_{i=1}^n b_i g_i\right) \mapsto \sum_{i=1}^n a_i b_i$$

ist symmetrisch, nicht-ausgeartet und G-invariant. Sei C ein Gruppenring-Code in $\mathbb{F}G$, dann ist der duale Code von C definiert als

$$C^\perp := \{v \in \mathbb{F}G \mid (c, v) = 0 \text{ für alle } c \in C\}.$$

Lemma 5.11. *Sei $^* : \mathbb{F}G \to \mathbb{F}G, g \mapsto g^{-1}$ die Konjugation auf $\mathbb{F}G$ und sei $C = \mathbb{F}Ge$ ein projektiver G-Code. Dann gilt $C^\perp = \mathbb{F}G(1 - e^*)$.*

Beweis. Es gilt $e(1 - e) = 0$, also ist $\mathbb{F}G(1 - e^*)$ in $C^\perp$ enthalten. Aus $\dim C^\perp = \dim \mathbb{F}G(1 - e) = \dim \mathbb{F}G(1 - e^*)$ folgt die Gleichheit. □

Satz 5.12 ([Wil02, Corollary 1.3])**.** *Sei $\mathbb{F}$ ein endlicher Körper und sei G eine endliche Gruppe. Dann enthält die Gruppenalgebra $\mathbb{F}G$ einen selbst-dualen Code, genau dann wenn $\mathbb{F}$ Charakteristik 2 hat und die Ordnung von G gerade ist.*

Bemerkung 5.13 ([Wil02, Remark 4.2])**.** *Sei C ein selbst-dualer Gruppencode in $\mathbb{F}G$. Dann ist das Komplement von C kein Ideal, insbesondere wird C nicht von einem Idempotent erzeugt.*

5.2 Gruppencodes über Kettenringen

Sei R ein kommutativer, artinscher Kettenring mit 1 und maximalen Ideal $\mathfrak{m} = \langle\pi\rangle$. Sei $\mathbb{F} := R/\mathfrak{m}$ der Restklassenkörper mit Charakteristik p und sei ℓ die die kleinste natürliche Zahl, so dass $\mathfrak{m}^\ell = \{0\}$ ist. Die Wahl des Erzeugers des maximalen Ideals definiert R-Modul-Isomorphismen

$$\alpha_j : \mathfrak{m}^j/\mathfrak{m}^{j+1} \to \mathbb{F}, \pi^j r + \mathfrak{m}^{j+1} \mapsto r + \mathfrak{m}$$

für $j = 0, \ldots, \ell - 1$. Für eine endliche Gruppe G seien RG und $\mathbb{F}G$ die Gruppenringe über R und $\mathbb{F}$. Dann können die Isomorphismen α_j zu R-Modul-Isomorphismen

$$\alpha_j : \mathfrak{m}^j RG/\mathfrak{m}^{j+1}RG \to \mathbb{F}G$$

erweitert werden, wobei α_0 ein R-Algebren-Isomorphismus ist.

Definition 5.14. *Ein Gruppenring-Code $\mathcal{C}$ über RG ist ein Linksideal in RG. Dieser heißt relativ-projektiv, falls $\mathcal{C}$ relativ-projektiv für die Untergruppe $\{1\}$ von G im Sinne*

der homologischen Algebra ist, d.h. für jede kurze exakte Sequenz

$$0 \to \mathcal{M} \to \mathcal{N} \xrightarrow{\varphi} \mathcal{C} \to 0$$

von RG-Moduln, für welche ein R-Modul-Homomorphismus $\psi : \mathcal{C} \to \mathcal{N}$ mit $\varphi \circ \psi = \mathrm{id}_{\mathcal{C}}$ existiert, gibt es einen RG-Modul-Homomorphismus $\psi' : \mathcal{C} \to \mathcal{N}$ mit $\varphi \circ \psi' = \mathrm{id}_{\mathcal{C}}$. Falls die Sequenz rechts-split als R-Modul ist, ist sie also bereits rechts-split als RG-Modul.

Für einen Körper ist relativ-projektiv äquivalent zu projektiv, allgemein stimmt dies aber nicht (z.B. $R = \mathbb{Z}/4\mathbb{Z}$ und $\mathcal{C} = 2R$).

Bemerkung 5.15. *Da RG als R-Modul frei, also inbesondere projektiv ist, folgt aus [Zim14, Proposition 2.1.6.], dass ein Gruppenring-Code $\mathcal{C}$ über RG genau dann relativ-projektiv ist, wenn die kurze exakte Sequenz*

$$0 \to \mathrm{Kern}(m) \to RG \otimes_R \mathcal{C} \xrightarrow{m} \mathcal{C} \to 0$$

splittet, wobei $m : \lambda \otimes c \mapsto \lambda c$ die Multiplikationsabbildung ist.

Satz 5.16. *Sei*

$$\mathcal{C}_\star \ : \ C_0 \leq C_1 \leq \cdots \leq C_{\ell-1}$$

eine Kette der Länge ℓ von projektiven Gruppenring-Codes über $\mathbb{F}G$ und seien $e_0, \ldots, e_{\ell-1} \in \mathbb{F}G$ die erzeugenden Idempotente. Dann gilt $e_i e_j = e_{\min(i,j)}$. Sei $\epsilon_j \in RG$ ein Idempotent mit $\alpha_0(\epsilon_j) = e_j$, $j = 0, \ldots, \ell - 1$, dann ist

$$\mathcal{C} := \hat{\mathcal{C}}_\star := RG \left(\sum_{j=0}^{\ell-1} \pi^j \epsilon_j \right)$$

ein relativ-projektiver Gruppenring-Code über RG.

Beweis. Nach Bemerkung 5.15 ist $\mathcal{C}$ genau dann relativ projektiv, wenn die kurze exakte Sequenz

$$0 \to \mathrm{Kern}(m) \to RG \otimes_R \mathcal{C} \xrightarrow{m} \mathcal{C} \to 0$$

splittet. Definiere den R-Modul-Homomorphismus

$$h : \mathcal{C} \to RG \otimes_R \mathcal{C}, \sum_{g \in G} r_g g \cdot \sum_{j=0}^{l-1} \pi^j \epsilon_j \mapsto \sum_{g \in G} r_g \cdot g \otimes \sum_{j=0}^{l-1} \pi^j \epsilon_j.$$

Für ein Element $\sum_{g\in G} r_g g \cdot \sum_{j=0}^{l-1} \pi^j \epsilon_j \in \mathcal{C}$ gilt dann

$$\begin{aligned} & m\left(h\left(\sum_{g\in G} r_g g \cdot \sum_{j=0}^{l-1} \pi^j \epsilon_j\right)\right) \\ =& m\left(\sum_{g\in G} r_g \cdot g \otimes \sum_{j=0}^{l-1} \pi^j \epsilon_j\right) \\ =& \sum_{g\in G} r_g \cdot m\left(g \otimes \sum_{j=0}^{l-1} \pi^j \epsilon_j\right) \\ =& \sum_{g\in G} r_g g \cdot \sum_{j=0}^{l-1} \pi^j \epsilon_g. \end{aligned}$$

Daraus folgt $m \circ h = \mathrm{id}_{\mathcal{C}}$ und die Sequenz splittet. □

Allgemein haben relativ-projektive Gruppenring-Code über RG eine solche Struktur:

Satz 5.17. *Sei $\mathcal{C} \leq RG$ ein relativ-projektiver Gruppenring-Code. Dann existieren primitive, orthogonale Idempotente $\epsilon_i \in RG$ und $a_i \in \mathbb{N}_0$, so dass*

$$\mathcal{C} = \bigoplus_{i=1}^{s} \mathfrak{m}^{a_i} RG\epsilon_i$$

gilt.

Beweis. Die Aussage wird mit einer Induktion über $\min\{a \in \mathbb{N} \mid \mathfrak{m}^a\mathcal{C} = \{0\}\}$ bewiesen. Im Fall $a = 1$ ist $\mathcal{C} \leq \mathfrak{m}^\ell RG$ ein relativ-projektiver $RG/\pi RG$-Modul, also projektiv über $\mathbb{F}G$ woraus die Behauptung folgt. Sei nun $a > 1$. Ersetze in diesem Fall R durch $R/\mathfrak{m}^a R$ und RG durch $\mathfrak{m}^{\ell-a}RG$. Dann gilt ohne Einschränkung $a = \ell$ und $C \not\leq \mathfrak{m}RG$. Sei

$$1 = \sum_{i=1}^{k} \epsilon_i$$

die Zerlegung der $1 \in RG$ in orthogonale, primitive Idempotente. Dann gilt

$$\mathcal{C} = \mathcal{C} \cdot 1 \subseteq \bigoplus_{i=1}^{k} RG\epsilon_i.$$

Es existiert ein i, so dass $\mathcal{C}\epsilon_i \not\subseteq \mathfrak{m}RG\epsilon_i$ gilt, sonst wäre $\mathcal{C}$ in $\mathfrak{m}RG$ enthalten. Zu zeigen ist nun, dass $\mathcal{C}\epsilon_i = RG\epsilon_i$ gilt. Da $\mathcal{C}$ relativ-projektiv ist, ist auch $\mathcal{C}\epsilon_i$ nach Bemerkung 5.15 relativ-projektiv, da die kurze exakte Sequenz

$$0 \to \mathrm{Kern}(m) \to \underbrace{RG \otimes_R \mathcal{C}\epsilon_i}_{\cong \oplus_{j=1}^{k} RG\epsilon_j \otimes_R \mathcal{C}\epsilon_i} \xrightarrow{m} \mathcal{C}\epsilon_i \to 0$$

splittet. Dann ist $\overline{\mathcal{C}\epsilon_i}$ ein projektiver Modul in $RG/\mathfrak{m}RG\overline{\epsilon_i} = \mathbb{F}G\overline{\epsilon_i}$ und es muss bereits $\overline{\mathcal{C}\epsilon_i} = \mathbb{F}G\overline{\epsilon_i}$ gelten, da ϵ_i primitiv ist. Damit folgt $\mathcal{C}\epsilon_i = RG\epsilon_i$. Betrachte nun die kurze exakte Sequenz von RG-Moduln

$$0 \to \mathrm{Kern}(\varphi) \to \mathcal{C} \xrightarrow{\varphi} \mathcal{C}\epsilon_i = RG\epsilon_i \to 0,$$

wobei φ die Multiplikation mit ϵ_i ist. Da $RG\epsilon_i$ ein freier R-Modul und zusätzlich relativ-projektiv ist, splittet die Sequenz als R-Modul und damit bereits als RG-Modul. Nach dem Splitting Lemma ist dann $\mathcal{C}$ isomorph zur direkten Summe von $\mathrm{Kern}(\varphi)$ und $RG\epsilon_i$ und die Argumentation lässt sich mit $\mathrm{Kern}(\varphi)$ fortsetzen. □

Lemma 5.18. *Sei $\mathcal{C} \leq RG$ ein relativ-projektiver Gruppenring-Code. Für $0 \leq j \leq \ell - 1$ definiere*

$$C_j := \alpha_j\left(\frac{\mathcal{C} \cap \mathfrak{m}^j RG}{\mathcal{C} \cap \mathfrak{m}^{j+1} RG}\right) \leq \mathbb{F}G.$$

Dann ist

$$\mathcal{C}_\star \ : \ C_0 \leq C_1 \leq \cdots \leq C_{\ell-1}$$

eine Kette von projektiven Gruppenring-Codes über $\mathbb{F}G$.

Beweis. Nach Satz 5.17 existieren primitive, orthogonale Idempotente $\epsilon_i \in RG$ und $a_i \in \mathbb{N}_0$, so dass

$$\mathcal{C} = \bigoplus_{i=1}^{s} \mathfrak{m}^{a_i} RG\epsilon_i$$

gilt. Insbesondere gilt also

$$\mathcal{C} \cap \mathfrak{m}^j RG = RGf_j$$

mit

$$f_j = \sum_{a_i \leq j} \pi^j \epsilon_i + \sum_{a_i > j} \pi^{a_i} \epsilon_i.$$

Damit folgt

$$\alpha_j\left(\frac{\mathcal{C} \cap \mathfrak{m}^j RG}{\mathcal{C} \cap \mathfrak{m}^{j+1} RG}\right) = \mathbb{F}G \underbrace{\left(\sum_{a_i \leq j} \alpha_0(\epsilon_i)\right)}_{=:e_j}$$

Zusätzlich ist $e_i e_j = e_{\min(i,j)}$, also $C_i \leq C_j$ für $i \leq j$. □

Korollar 5.19. *Es gilt $(\hat{\mathcal{C}}_\star)_\star = \mathcal{C}_\star$, also stehen die relativ-projektiven Gruppenring-Codes über RG in Bijektion zu den Ketten von projektiven Gruppenring-Codes über $\mathbb{F}G$ der Länge ℓ.*

Analog zu Gruppencodes über Körpern sei

$$(\cdot,\cdot) : RG \times RG \to R, \left(\sum_{i=1}^{n} a_i g_i, \sum_{i=1}^{n} b_i g_i\right) \mapsto \sum_{i=1}^{n} a_i b_i$$

eine nicht-ausgeartete Bilinearform auf RG. Dann ist der duale Gruppencodes definiert als

$$\mathcal{C}^\perp := \{v \in RG \mid (v, c) = 0 \text{ für alle } c \in \mathcal{C}\}.$$

Lemma 5.20. *Sei $\mathcal{C} \leq RG$ ein relativ-projektiver Gruppenring-Code mit*

$$\mathcal{C}_\star = C_0 \leq \cdots \leq C_{\ell-1}$$

Dann gilt $\mathcal{C}_\star^\perp = C_{\ell-1}^\perp \leq \cdots \leq C_0^\perp$.

Beweis. Die Aussage folgt mit Lemma 5.18. Seien $b_1, \ldots, b_m \in \mathcal{C} \cap \mathfrak{m}^j RG$, so dass $(b_i + \mathcal{C} \cap \mathfrak{m}^{j+1} RG)_{i=1,\ldots,m}$ ein R-Erzeugendensystem von $\frac{\mathcal{C} \cap \mathfrak{m}^j RG}{\mathcal{C} \cap \mathfrak{m}^{j+1} RG}$ ist. Dann gilt

$$\alpha_{\ell-1-j}\left(\frac{\langle b_1, \ldots, b_m\rangle^\perp \cap \mathfrak{m}^{\ell-1-j} RG}{\langle b_1, \ldots, b_m\rangle^\perp \cap \mathfrak{m}^{\ell-j} RG}\right) = C_j^\perp \leq \mathbb{F}G.$$

Daraus folgt die Behauptung. □

Bemerkung 5.21. *Falls ℓ gerade ist, existiert immer ein selbst-dualer relativ-projektiver Gruppenring-Code über RG, zum Beispiel*

$$\mathcal{C}_\star = \{0\} \leq \cdots \leq \{0\} \leq \mathbb{F}G \leq \cdots \leq \mathbb{F}G.$$

Falls ℓ ungerade ist, müsste für solch einen Code gelten

$$\mathcal{C}_\star = C_0 \leq \cdots \leq C_{\frac{\ell-1}{2}} = C_{\frac{\ell-1}{2}}^\perp \leq C_{\frac{\ell-3}{2}}^\perp \leq \cdots \leq C_0^\perp.$$

Allerdings kann nach Bemerkung 5.13 der selbst-duale Code $C_{\frac{\ell-1}{2}}$ nicht von einem Idempotent erzeugt sein. Ein selbst-dualer relativ-projektiver Gruppenring-Code über RG existiert also genau dann, wenn ℓ gerade ist.

Für einen Gruppenring-Code $\mathcal{C} \leq RG$ ist das Hamming-Gewicht eines Codewortes $c = \sum_{i=1}^n c_i g_i \in \mathcal{C}$

$$w_H(c) := |\{c_i \mid c_i \neq 0\}|,$$

und der Hamming-Minimalabstand ist dann

$$d_H(\mathcal{C}) = \min\{w_H(c) \mid 0 \neq c \in \mathcal{C}\}.$$

Satz 5.22. *Sei $\mathcal{C} \leq RG$ ein relativ-projektiver Gruppenring-Code mit*

$$\mathcal{C}_\star : C_0 \leq \cdots \leq C_{\ell-1}$$

Dann gilt $d_H(\mathcal{C}) = d_H(C_{\ell-1})$.

Beweis. Klar ist, dass $d_H(\mathcal{C}) \leq d_H(C_{\ell-1})$ gilt. Angenommen, es existiert ein $0 \neq c \in \mathcal{C}$, so dass $w_H(c) < d_H(C_{\ell-1})$ ist. Sei dann i minimal mit $\mathfrak{m}^i c \in \mathfrak{m}^{\ell-1} RG$. Insbesondere ist dann $\mathfrak{m}^i c \neq 0$ und $w_H(\mathfrak{m}^i c) \leq w_H(c)$. Allerdings folgt dann $\alpha_{\ell-1}(\mathfrak{m}^i c) \in C_{\ell-1}$ und $w_H(\alpha_{\ell-1}(\mathfrak{m}^i c)) = w_H(\mathfrak{m}^i c)$, also

$d_H(C_{\ell-1}) \leq w_H(c) < d_H(C_{\ell-1})$, ein Widerspruch. □

Im Spezialfall $R = \mathbb{Z}/p^l\mathbb{Z}$ ist das euklidische Gewicht eines Codewortes $c = \sum_{i=1}^n c_i g_i \in (\mathbb{Z}/p^l\mathbb{Z})G$ definiert als

$$w_E(c) := \min\left\{\sum_{i=1}^n a_i^2 \mid a_i \in \mathbb{Z}, a_i + p^l\mathbb{Z} = c_i\right\}$$

und der euklidische Minimalabstand ist dann

$$d_E(\mathcal{C}) = \min\{w_E(c) \mid 0 \neq c \in \mathcal{C}\}.$$

Satz 5.23. *Sei $R = \mathbb{Z}/p^l\mathbb{Z}$ und sei $\mathcal{C} \leq RG$ ein relativ-projektiver Gruppenring-Code mit $\mathcal{C}_\star : C_0 \leq \cdots \leq C_{l-1}$. Falls ein $\gamma > 0$ existiert, so dass die Abschätzung $d_E(C_j) \geq \frac{\gamma}{p^{2j}}$ für alle j gilt, folgt $d_E(\mathcal{C}) \geq \gamma$.*

Beweis. Sei $c = \sum_{i=1}^n (c_i + p^l\mathbb{Z})g_i \in \mathcal{C}$ und sei j maximal mit $c \in \mathfrak{m}^j RG$. Dann ist

$$(c_1, \ldots, c_n) = p^j(y_1, \ldots, y_n) \text{ mit } \sum_{i=1}^n (y_i + p\mathbb{Z})g_i \in C_j.$$

Nach Voraussetzung gilt

$$\sum_{i=1}^n y_i^2 \geq d_E(C_j) \geq \frac{\gamma}{p^{2j}},$$

daraus folgt

$$\sum_{i=1}^n c_i^2 = p^{2j}\sum_{i=1}^n y_i^2 \geq p^{2j}\frac{\gamma}{p^{2j}} = \gamma,$$

also insgesamt $d_E(\mathcal{C}) \geq \gamma$. □

5.3 Beispiele

5.3.1 Zyklische Codes

Sei $\mathbb{F}$ ein Körper der Charakteristik p und sei g ein Erzeuger der zyklischen Gruppe C_n mit $n = p^l m$, so dass $p \nmid m$.

Bemerkung 5.24. *Die Idempotente von $\mathbb{F}C_n$ stehen in Bijektion zu den Idempotenten von $\mathbb{F}[C_n/C_{p^l}] \cong \mathbb{F}[g^{p^l}]$, gegeben durch die natürlich Projektion $\mathbb{F}C_n \to \mathbb{F}[C_n/C_{p^l}]$.*

Die Idempotente von $\mathbb{F}C_n$ sind also genau die Idempotente der halbeinfachen Algebra $\mathbb{F}[g^{p^l}]$ und können dementsprechend einfach berechnet werden. Über $\mathbb{C}$

ist die Charaktertafel von C_n

$$\begin{array}{c|ccccc} & \chi_1 & \chi_2 & \chi^3 & \cdots & \chi^n \\ \hline g & 1 & \zeta_n & \zeta_n^2 & \cdots & \zeta_n^{n-1} \end{array}$$

wobei $\zeta_n \in \mathbb{C}$ eine primitive n-te Einheitswurzel ist. Insbesondere existieren also m irreduzible Brauer-Charaktere. Es gilt $C_n \cong C_{p^l} \times C_m$ und die Einschränkung von χ^i auf $C_m \cong C_n/C_{p^l}$ bildet ζ_n auf ζ_m ab. Jeweils p^l n-te Einheitswurzeln bilden auf ein festes ζ_m^i ab, und zwar alle $\zeta_n^{j\cdot m+i}, j = 0, \ldots, p^l - 1$. Damit ist die Zerlegungsmatrix gegeben durch

$$\begin{pmatrix} 1 & & & \\ \vdots & & & \\ 1 & & & \\ & 1 & & \\ & \vdots & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \\ & & & \vdots \\ & & & 1 \end{pmatrix} \begin{matrix} \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} p^l \\ \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} p^l \\ \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} p^l \end{matrix}$$

mit der ensprechenden Cartanmatrix

$$\begin{pmatrix} p^l & & & \\ & p^l & & \\ & & \ddots & \\ & & & p^l \end{pmatrix}.$$

Damit folgt:

Lemma 5.25. *Seien $e_1, \ldots, e_k$ die zentral primitiven Idempotente von $\mathbb{F}C_n$, d.h.*

$$\mathbb{F}C_n = \bigoplus_{i=1}^{k} \mathbb{F}C_n e_i,$$

und für ein festes i sei $\mathfrak{J}_i$ das Jacobson-Radikal von $\mathbb{F}C_n e_i$. Dann ist $\mathfrak{J}_i$ ein Ideal der Länge p^l und es gilt $\mathbb{F}C_n e_i/\mathfrak{J}_i \cong \mathbb{E}_i$, wobei $\mathbb{E}_i$ eine Körperweiterung von $\mathbb{F}$ ist. Als Körper hat $\mathbb{E}_i$ nur die Idempotente 0 und 1, dasselbe gilt für $\mathbb{F}C_n e_i$. Also hat $\mathbb{F}C_n$ insgesamt 2^k Idempotente.

Da jedes Idempotent von $\mathbb{F}C_n$ ein Polynom in g^{p^l} ist, lässt sich die Struktur projektiver zyklischer Codes recht einfach beschreiben:

Bemerkung 5.26. *Sei $\mathbb{F}$ ein Körper der Charakteristik p, sei $n = p^l m$ mit $p \nmid m$ und sei e ein Idempotent in $\mathbb{F}C_n$. Dann ist der Code C, der von e erzeugt wird, die p^l-fache*

direkte Summe eines zyklischen Codes der Länge m über $\mathbb{F}$. Mit der Sortierung

$$(1, g^{p^l}, \ldots, g^{(m-1)p^l}, g, g^{p^l+1}, \ldots, g^{(m-1)p^l+1}, \ldots, g^{p^l-1}, g^{2p^l+(p^l-1)}, \ldots, g^{(m-1)p^l+(p^l-1)})$$

der Gruppenelemente hat C die Erzeugermatrix

$$\mathrm{Diag}(\underbrace{M, \ldots, M}_{p^l \text{ mal}}),$$

wobei M die Erzeugermatrix eines zyklischen Codes über $\mathbb{F}$ der Länge m ist. Für einen relativ-projektiv Code $\mathcal{C} \leq RC_n$ mit zugehöriger Kette

$$\mathcal{C}_\star : C_0 \leq \cdots \leq C_{\ell-1}$$

von projektiven Codes über $\mathbb{F}C_n$ gilt nun $d_H(\mathcal{C}) = d_H(M_{\ell-1})$ mit

$$C_{\ell-1} = \mathrm{Diag}(M_{\ell-1}, \ldots, M_{\ell-1}).$$

Im nicht-teilerfremden Fall kann man also nicht erwarten, besonders gute Codes zu erhalten.

5.3.2 Diedergruppen

F. J. MacWilliams war die erste, die Codes über nicht-abelschen Gruppenalgebren betrachtet hat ([Mac69]). In diesem Paper wurden Elemente in $\mathbb{F}_2 D_{2n}$ konstruiert, so dass das erzeugte Hauptlinksideal ein selbst-dualer Code ist. Allerdings wurde auch angemerkt, dass die Betrachtung weit davon entfernt ist, vollständig zu sein.
Die meisten Paper, die sich mit Codes über $\mathbb{F}D_{2n}$ beschäftigen, setzen vorraus, dass die Gruppenalgebra halbeinfach ist, insbesondere wird also der interessanteste Fall $\mathbb{F} = \mathbb{F}_2$ ausgeschlossen. So wird zum Beispiel in [DFP09] beschrieben, wann die Anzahl der einfachen Komponenten von $\mathbb{F}D_{2n}$ und $\mathbb{Q}D_{2n}$ (beide als halbeinfach vorausgesetzt) gleich sind, in diesen Fällen wurden die minimalen Codes betrachtet, die von zentralen Idempotenten erzeugt werden.

In diesem Abschnitt werden Dieder-Codes untersucht, mit einem starken Fokus auf den modularen Fall $\mathbb{F}_2 D_{2n}$ und Linksideale, die von Idempotente erzeut sind. In [SL95] wurde gezeigt, dass für eine metazyklische Gruppe G von ungerader Ordnung, jedes zentrale Idempotent in $\mathbb{F}_2 G$ einen Code erzeugt, der zu einen abelschen Code über $\mathbb{F}_2$ äquivalent ist. Diese Ergebnis wurde in [BRS09] auf Gruppen der Form $G = AB$ über beliebigen Körpern übertragen, wobei $A, B \leq G$ zwei abelsche Untergruppen von G sind. Im Fall der Diedergruppe D_{2n} stellt sich heraus, dass jeder solche Code zyklisch ist. Andererseits erzeugt jedes (zentrale) Idempotent über einer zyklischen Gruppe einen Code, welcher du einem Dieder-Code isomorph ist, welcher von einem (nicht notwendigerweise zentralem) Idempotent erzeugt wird. Betrachtet man Codes, welche nicht von

einem Idempotent erzeugt wird, existieren zyklische Codes, die einen größeren Minimalabstand haben als alle Dieder-Codes in der entsprechenden Länge und Dimension.

Sei nun $\mathbb{F}$ ein endlicher Körper und $D_{2n} = \langle a, b \mid a^n = b^2 = 1, bab = a^{-1} \rangle$ die Diedergruppe von Ordnung $2n$.

Der halbeinfache Fall

Angenommen, es gilt $\mathrm{char}(\mathbb{F}) \nmid 2n$. Sei

$$x^n - 1 = (x-1) f_1 \cdots f_{n_1} g_1 g_1^* \cdots g_{n_2} g_{n_2}^* \in \mathbb{F}[x]$$

die Zerlegung von $x^n - 1$ in irreduzible Polynome, wobei die f_i selbstkonjugiert sind, und es n_2 Paare von konjugierten Polynomen gibt. Dann gilt

$$\mathbb{F}D_{2n} \cong \mathbb{F} \oplus \cdots \oplus \mathbb{F} \oplus \bigoplus_{i=1}^{n_1} \mathbb{E}_i^{2\times 2} \oplus \bigoplus_{i=1}^{n_2} \mathbb{E}_i'^{2\times 2},$$

wobei die Anzahl der eindimensionalen Summanden zwei ist, falls n ungerade, und vier sonst. Die $\mathbb{E}_i$ (bzw. $\mathbb{E}_i'$) sind Körpererweiterungen von $\mathbb{F}$ vom Grad $\deg(f_i)/2$ (bzw. $\deg(g_i)$). Sei $\delta \in \overline{\mathbb{F}}$ ein Element mit Minimalpolynom f_i (bzw. g_i). Dann ist $\mathbb{E}_i$ (bzw. $\mathbb{E}_i'$) der kleinste Teilkörper von $\mathbb{F}[\delta]$, so dass $\delta + \delta^{-1}$ darin enthalten ist. Im Fall f_i ist dies ein Körper vom Index 2, im Fall g_i gilt Gleichheit. Damit sind die Projektionen auf die entsprechende Komponente gegeben duch

$$\mathbb{F}D_{2n} \to \mathbb{E}_i^{2\times 2}, \begin{cases} a \mapsto \begin{pmatrix} 0 & 1 \\ -1 & \delta + \delta^{-1} \end{pmatrix} \\ b \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{cases}$$

(wobei das Bild von a gerade die Begleitmatrix des Minimalpolynoms von δ über $\mathbb{E}_i$ ist), bzw.

$$\mathbb{F}D_{2n} \to \mathbb{E}_i'^{2\times 2}, \begin{cases} a \mapsto \begin{pmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{pmatrix} \\ b \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \end{cases}$$

Die Projektionen auf die eindimensionalen Komponenten sind gegeben durch $\begin{cases} a \mapsto 1 \\ b \mapsto 1 \end{cases}, \begin{cases} a \mapsto 1 \\ b \mapsto -1 \end{cases}$ und falls n gerade ist zusätzlich noch durch $\begin{cases} a \mapsto -1 \\ b \mapsto 1 \end{cases}, \begin{cases} a \mapsto -1 \\ b \mapsto -1 \end{cases}$. Da $\mathbb{F}D_{2n}$ halbeinfach ist, ist jedes Ideal von einem

Idempotent erzeugt. Diese lassen sich mit Hilfe von Lemma 5.7 bestimmen.

Der Fall $\mathrm{char}(\mathbb{F}) = 2$

Sei $n = 2^l m$ mit m ungerade. Dann gilt $x^n - 1 = (x^m - 1)^{2^l}$ und sei

$$x^m - 1 = (x-1) f_1 \cdots f_{m_1} g_1 g_1^* \cdots g_{m_2} g_{m_2}^* \in \mathbb{F}[x]$$

die Faktorisierung von $x^m + 1$ in irreduzible Polynome. Seien $q_0, \ldots, q_{m_1+m_2} \in \mathbb{F}[x]$ so dass

$$1 = q_0 \cdot \frac{x^m-1}{x-1} + q_1 \cdot \frac{x^m-1}{f_1} + \cdots + q_{m_1} \cdot \frac{x^m-1}{f_{m_1}} + q_{m_1+1} \cdot \frac{x^m-1}{g_1 g_1^*} + \cdots + q_{m_1+m_2} \cdot \frac{x^m-1}{g_{m_2} g_{m_2}^*},$$

dann sind die zentral primitiven Idempotente $e_0, \ldots, e_{m_1+m_2}$ gegeben durch die Auswertung der einzelnen Summanden an a^{2^l}. In jedem Fall gilt $e_0 = \sum_{i=0}^{m-1} a^{2^l i}$ und $\mathbb{F}D_{2n}e_0 = \mathbb{F}D_{22^l}$ (mit $D_{22^0} = C_2$), der Hauptblock von $\mathbb{F}G$.

Betrachte nun die Struktur der übrigen Blöcke. Der Fall n ungerade (d.h. $l = 0$ und $m = n$) unterscheidet sich nicht wesentlich von Charakteristik 0. Die Konjugiertenklassen von D_{2n} sind

$$\{\mathrm{id}\},\ \{a^i, a^{-i}\}_{i=1,\ldots,\frac{n-1}{2}}, b\langle a\rangle,$$

das heißt es gibt eine Konjugiertenklasse mit allen Elementen der Ordnung 2, die Elemente von ungerader Ordnung bilden zusammen $\frac{n-1}{2} + 1$ Konjugiertenklassen, also existieren auch genau so viele irreduzible Brauer-Charaktere.

Über $\mathbb{C}$ ist die Charaktertafel von D_{2n}

	χ_1	χ_2	$\chi^{(1)}$	$\ldots$	$\chi^{(\frac{n-1}{2})}$
a	1	1	$\zeta_n + \zeta_n^{-1}$	$\ldots$	$\zeta_n^{\frac{n-1}{2}} + \zeta_n^{-\frac{n-1}{2}}$
b	1	-1	0	$\ldots$	0

wobei $\zeta_n \in \mathbb{C}$ eine primtive n-te Einheitswurzel ist.

Seien nun $\phi_1, \phi^{(1)}, \ldots, \phi^{(\frac{n-1}{2})}$ die irreduziblen Brauer-Charaktere. Auf den 2-regulären Klassen sind χ_1 und χ_2 gleich dem trivialen Brauer-Charakter ϕ_1. Es gibt keine weitere 1-dimensionale Darstellung, da alle solchen Darstellungen über die Kommutatorfaktorgruppe $D_{2n}/D'_{2n} = C_2$ faktorisieren, diese hat über einem Körper der Charakteristik 2 aber nur die triviale Darstellung. Die 2-dimensionalen Darstellungen bleiben irreduzibel, denn sonst wäre $\phi^{(i)} = 2 \cdot \phi_1$.

Die Zerlegungsmatrix ist also

$$\begin{pmatrix} 1 & & & \\ 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \in \mathbb{Z}^{\left(\frac{n-1}{2}+2\right)\times\left(\frac{n-1}{2}+1\right)},$$

die Cartanmatrix ist dementsprechend

$$\begin{pmatrix} 2 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \in \mathbb{Z}^{\left(\frac{n-1}{2}+1\right)\times\left(\frac{n-1}{2}+1\right)}.$$

Daraus folgt direkt:

Lemma 5.27. *Sei $\mathbb{F}$ ein endlicher Körper mit Charakteristik 2 und sei n ungerade. Sei*

$$x^n - 1 = (x-1)f_1 \cdots f_{n_1} g_1 g_1^* \cdots g_{n_2} g_{n_2}^* \in \mathbb{F}[x]$$

die Faktorisierung über $\mathbb{F}[x]$ in irreduzible Polynome, dann gilt

$$\mathbb{F}D_{2n} \cong \mathbb{F}C_2 \oplus \bigoplus_{i=1}^{n_1} \mathbb{E}_i^{2\times 2} \oplus \bigoplus_{i=1}^{n_2} \mathbb{E}_i'^{2\times 2}.$$

Die Körperweiterungen und die Projektionen auf die entsprechenden Komponenten berechnen sich wie im halbeinfachen Fall. Das Idempotent $e_0 = \sum_{i=0}^{n-1} a^i \in \mathbb{F}D_{2n}$ erzeugt eine Teilalgebra, welche isomorph zu $\mathbb{F}C_2$ ist. Sei $C_2 = \langle g \rangle$, dann ist die Projektion von $\mathbb{F}D_{2n}$ auf $\mathbb{F}C_2$ gegeben durch $\begin{cases} a \mapsto 1 \\ b \mapsto g. \end{cases}$

Bemerkung 5.28. *Sei $\mathbb{F}$ ein endlicher Körper mit Charakteristik 2 und sei n ungerade. Ein Code $C \leq \mathbb{F}D_{2n}$ wird genau dann von einem Idempotent erzeugt, wenn die Dimension von C gerade ist.*

Betrachte nun die Struktur von $\mathbb{F}D_{2n}$ für n gerade. Die Konjugiertenklassen sind hier

$$\{\mathrm{id}\}, \{a^{\frac{n}{2}}\}, \{a^i, a^{-i}\}_{i=1,\ldots,\frac{n-2}{2}}, \{a^i b : i \text{ gerade}\} \text{ und } \{a^i b : i \text{ ungerade}\}.$$

Insgesamt existieren also $\frac{n-2}{2} + 4$ Konjugiertenklassen, davon sind $\frac{m-1}{2} + 1$ von ungerader Ordnung: die triviale Klasse $\{\mathrm{id}\}$ und $\{(a^{2^l})^i, (a^{2^l})^{-i}\}_{i=1,\ldots,\frac{m-1}{2}}$. Insbesondere existieren also $\frac{m-1}{2} + 1$ irreduzible Brauer-Charaktere auf den 2-regulären Klassen.

Über $\mathbb{C}$ ist die Charaktertafel von D_{2n}

	χ_1	χ_2	χ_3	χ_4	$\chi^{(1)}$	$\dots$	$\chi^{(\frac{n-2}{2})}$
a	1	1	-1	-1	$\zeta_n + \zeta_n^{-1}$	$\dots$	$\zeta_n^{\frac{n-2}{2}} + \zeta_n^{-\frac{n-2}{2}}$
b	1	-1	1	-1	0	$\dots$	0

wobei $\zeta_n \in \mathbb{C}$ wieder eine primitive n-te Einheitswurzel ist.
Wie im Fall n ungerade existiert nur ein irreduzibler Brauer-Charakter von Dimension 1, der triviale Charakter $\phi_1 = 1$ (jeder weitere eindimensionaler Charakter müsste über die Kommutatorfaktorgruppe $D_{2n}/D'_{2n} = C_1$ faktorisieren).
Die Gruppe D_{2n} hat den Normalteiler $C_{2n} \cong C_{2^l} \times C_m$. Die Einschränkung von $\chi^{(i)}$ auf $D_{2m} \cong D_{2n}/C_{2^l}$ bildet also ζ_n auf ζ_m ab und genau $\frac{2^l-2}{2}$ 2-dimensionale Charaktere bilden unter dieser Einschränkung auf den trivialen Charakter ϕ_1 ab, und zwar alle $\chi^{(m \cdot i)}, i = 1, \dots, \frac{2^l-2}{2}$. Die übrigen $\frac{n-2}{2} - (2^{l-1} - 1)$ Charaktere werden unter der Abbildung $\zeta_n^i + \zeta_n^{-i} \mapsto \zeta_m^i + \zeta_m^{-i}$ auf die Brauer-Charaktere abgebildet, d.h. $\chi^{(i)} \mapsto \phi^{(i \bmod \frac{m-1}{2})}$, und zwei Charaktere $\chi^{(i)}, \chi^{(j)}$ fallen zusammen, genau dann wenn $i \equiv \pm j \pmod m$. Insgesamt fallen also jeweils

$$\frac{\frac{n-2}{2} - (2^{l-1} - 1)}{\frac{m-1}{2}} = 2^l$$

Charaktere zusammen, die Zerlegungsmatrix ist daher

$$\begin{pmatrix}
1 & & & \\
1 & & & \\
1 & & & \\
1 & & & \\
2 & & & \\
\vdots & & & \\
2 & & & \\
 & 1 & & \\
 & \vdots & & \\
 & 1 & & \\
 & & \ddots & \\
 & & & 1 \\
 & & & \vdots \\
 & & & 1
\end{pmatrix}
\begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix}
\begin{matrix} \\ \\ \\ \\ \\ \\ \\ \} 2^{l-1} - 1 \\ \\ \\ \} 2^l \\ \\ \\ \} 2^l \end{matrix}$$

mit der entsprechenden Cartanmatrix

$$\begin{pmatrix}
2^{l+1} & & & \\
 & 2^l & & \\
 & & \ddots & \\
 & & & 2^l
\end{pmatrix}.$$

Lemma 5.29. *Sei $\mathbb{F}$ ein endlicher Körper mit Charakteristik 2 und sei $n = 2^l m$ mit m ungerade. Dann ist $\mathbb{F}D_{22^l} = \mathbb{F}D_{2n}e_0$ der Hauptblock von $\mathbb{F}D_{2n}$ und enthält als Kettenring nur die trivialen Idempotente. Für ein zentral primitives Idempotent e_i sei $\mathfrak{J}_i$ das Jacobson-Radikal von $\mathbb{F}D_{2n}e_i$, dann gilt $\mathbb{F}D_{2n}e_i/\mathfrak{J}_i \cong \mathbb{E}_i^{2\times 2}$, wobei der Grad Körperweiterung $\mathbb{E}_i$ von der Faktorisierung von $x^m - 1$ bestimmt wird.*

Die Idempotente von $\mathbb{F}D_{2n}e_i$ können also über die Lifts der Idempotente von $\mathbb{F}D_{2n}e_i/\mathfrak{J}_i \cong \mathbb{E}_i^{2\times 2}$ bestimmt werden. In der Notation von Bemerkung 5.9 gilt für den Lift eines nicht-zentralen Idempotents $r + \mathfrak{J}_i^k \in \mathbb{F}D_{2n}e_i/\mathfrak{J}_i^k$

$$\dim_{\mathbb{F}}(\mathrm{Bild}(\varphi_r)) = 2 \cdot [\mathbb{E}_i : \mathbb{F}].$$

Da es in $\mathbb{E}_i^{2\times 2}$ zwei zentrale und $|\mathbb{E}_i| \cdot (|\mathbb{E}_i| + 1)$ nicht-zentrale Idempotente gibt, ist die Anzahl der Idempotente in $\mathbb{F}D_{2n}e_i$ insgesamt

$$\begin{cases} 2, & \text{falls } i = 0 \\ |\mathbb{E}_i| \cdot (|\mathbb{E}_i| + 1) \cdot |\mathbb{F}|^{2\cdot[\mathbb{E}_i:\mathbb{F}]\cdot(2^l-1)} + 2 & \text{sonst.} \end{cases}$$

Bemerkung 5.30. *Falls ein Code C von einem Idempotent $e \in \mathbb{F}D_{2n}$ erzeugt wird, ist die Dimension von C gerade.*

Beispiel 5.31. *Sei $\mathbb{F} = \mathbb{F}_2$, $n \in 4\mathbb{Z}_{\geq 0}$ und bezeichne mit I_n bzw. J_n die Einheitsmatrix bzw. All-Eins-Matrix in $\mathbb{F}_2^{n\times n}$. Dann ist der Code mit Erzeugermatrix $\left(\begin{array}{c|c} I & I + J \end{array}\right)$ ein Gruppencode in $\mathbb{F}_2D_{2n}$, welcher selbst-dual und doppelt gerade ist. Insbesondere ist C also kein zyklischer Code (siehe [ST83]).*

In [TAT15] behaupten die Autoren, dass sich alle Gruppencodes (hier als Rechtsmoduln) über $\mathbb{F}_2D_6$ bzw. $\mathbb{F}_2D_8$ als zyklische Codes realisieren lassen. Diese Aussage ist falsch, wie das folgende Beispiel zeigt:

Beispiel 5.32. *Als Rechtsmodul erzeugt das Element $1 + a + a^2 + b \in \mathbb{F}_2D_8$ einen selbst-dualen, doppelt-geraden Code, insbesondere ist dieser also nicht isomorph zu einem zyklischen Code ([ST83]).*

Sei $n = 2^l m$, m ungerade, und sei

$$\varphi : \mathbb{F}_2D_{2n} \to \mathbb{F}_2C_{2n}, \sum_{0\leq i\leq n-1, 0\leq j\leq 1} a_{ij}a^i b^j \mapsto \sum_{i,j} a_{ij}g^{2i+j}$$

ein Isomorphismus zwischen den beiden Vektorräumen. Sei $e \in \mathbb{F}_2D_{2n}$ ein zentrales Idempotent, dann ist e ein Polynom in a^{2^l}, d.h.

$$e := \sum_{i=0}^{m-1} a_i \left(a^{2^l}\right)^i.$$

Damit gilt

$$\varphi(e) = \varphi(e^2) = \sum_{i=0}^{m-1} a_i \left(g^{2^{l+1}}\right)^{2i} = \left(\sum_{i=0}^{m-1} a_i \left(g^{2^{l+1}}\right)^i\right)^2 = \varphi(e)^2,$$

d.h. $\varphi(e)$ ist ein (zentrales) Idempotent in $\mathbb{F}_2 C_{2n}$. Andererseits ist das Urbild jedes Idempotents in $\mathbb{F}_2 C_{2n}$ ein Idempotent in $\mathbb{F}_2 D_{2n}$, welches nicht notwendigerweise zentral ist. Damit folgt sofort:

Lemma 5.33. *Sei $\mathbb{F}$ ein endlicher Körper der Charakteristik 2 und sei e ein zentrales Idempotent in $\mathbb{F}D_{2n}$. Nach geeigneter Sortierung der Gruppenelemente hat der Code $\mathbb{F}D_{2n}e$ die Erzeugermatrix $\mathrm{Diag}(M, \ldots, M)$, wobei M ein zyklischer Code der Länge m über $\mathbb{F}$ ist. Dieser wird, aufgefasst als Ideal in $\mathbb{F}C_{2n}$, von $\varphi(e)$ erzeugt. Ist andererseits $f \in \mathbb{F}C_{2n}$ ein Idempotent, so ist $\varphi^{-1}(\mathbb{F}C_{2n}f)$ ein Dieder-Code, der von dem (nicht notwendigerweisen zentralem) Idempotent $\varphi^{-1}(f)$ erzeugt wird.*

Insgesamt gibt es also zu jedem projektiven, zentralen Dieder-Code einen projektiven, zyklischen Code, welcher bei gleicher Dimension einen mindestens genauso hohen Minimalabstand hat. Zu jedem solchen zyklischen Code existiert wiederum ein projektiver (eventuell nicht zentraler) Dieder-Code, welcher bei gleicher Dimension einen mindestens genauso hohen Minimalabstand hat.
Für $n = 2^l$ fallen die beiden Klassen der projektiven Dieder- und projektiven zyklischen Codes zusammen, da es jeweils nur die beiden Idempotente 0 und 1 gibt. Für $n = 7$ existiert kein projektiver Dieder-Code, welcher besser als ein projektiver zyklischer Code ist. Für alle anderen $n \leq 20$ gibt es mindestens einen besseren projektiven Dieder-Code.
Die maximalen Minimalabstände über dem Körper $\mathbb{F}_2$ sind in den folgenden Tabelle angegeben. Im Vergleich mit den Werten aus Codetables ([Gra]) stellt sich heraus, dass nur wenig Codes in interessanten Dimensionen den maximal möglichen Minimalabstand annehmen (nach Bemerkung 5.28 und 5.30 kann die Dimension nicht ungerade sein).
Falls man alle (Links-)Ideale betrachtet, und nicht nur die projektiven, sind die Dieder-Codes nicht zwingend besser als die zyklischen Codes, so existiert zum Beispiel ein zyklischer $[28, 3, 16]$-Code, der einzige Dieder-Codes in dieser Dimension hat aber den Minimalabstand 14. Ein weiteres Gegenbeispiel findet sich für $n = 15$. Für allen anderen $n \leq 20$ sind die Dieder-Codes mindestens genauso gut wie die zyklischen Codes, für alle n außer $n \in \{3, 5, 6, 7\}$ existiert ein mindestens einer Dimension ein besserer Dieder-Code. Die Codes nehmen wesentlicher häufiger den generell maximal mal möglichen Minimalabstand an, besonders für $n = 6$ und $n = 12$ und nahezu jeder Dimension.

Bemerkung 5.34. *Für $n \in \{4, 8, 12, 16, 20, 24, 28, 32, 36\}$ existiert ein selbst-dualer, doppelt gerader Code in $\mathbb{F}_2 D_{2n}$ mit dem bisher am höchsten bekannten Minimalabstand, d.h.*

$$d = \begin{cases} 4\lfloor \frac{2n}{24} \rfloor + 4 & n \leq 32 \\ 4\lfloor \frac{2n}{24} \rfloor = 12 & n = 36. \end{cases}$$

Die Nicht-existenz eines selbst-dualen, doppelt-geraden [72,36,16]-Code im Gruppenring $\mathbb{F}_2 D_{72}$ wurde bereits in [OW11] gezeigt.

n/k	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40
1	-																			
2	-	-																		
3	4	2	1																	
4	-	-	-	1																
5	5	4	2	2	1															
6	-	4	-	2	-	1														
7	7	-	4	3	-	2	1													
8	-	-	-	-	-	-	-	1												
9	12	6	4	4	4	2	2	2	1											
10	-	5	-	8	-	4	-	2	-	1										
11	11	-	-	-	8	6	-	-	-	-	1									
12	-	-	-	8	-	-	-	3	-	-	-	1								
13	13	-	-	-	-	8	5	-	-	-	-	2	1							
14	-	7	-	-	-	8	-	5	-	-	-	2	-	1						
15	20	12	12	10	8	8	8	6	5	4	4	2	2	2	1					
16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1				
17	17	-	-	12	10	-	-	8	6	-	-	4	2	-	-	2	1			
18	-	12	-	6	-	8	-	8	-	6	-	3	-	2	-	2	-	1		
19	19	-	-	-	-	-	-	-	8	7	-	-	-	-	-	-	-	2	1	
20	-	-	-	5	-	-	-	8	-	-	-	5	-	-	-	2	-	-	-	1

TABELLE 5.1: Maximaler Minimalabstand der projektiven Dieder-Codes

$\|G\|/k$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	-	-																		
4	-	-	-	-																
6	6	4	2	2	2	1														
8	8	4	4	4	2	2	2	1												
10	10	5	-	4	2	2	-	2	2	1										
12	12	8	6	4	4	4	4	2	2	2	2	1								
14	14	7	-	-	-	4	4	3	-	-	-	2	2	1						
16	16	8	8	8	4	4	4	4	4	4	2	2	2	2	2	1				
18	18	12	6	6	6	4	4	4	4	4	2	2	2	2	2	2	2	1		
20	20	10	10	8	4	4	4	8	4	4	4	4	4	2	2	2	2	2	2	1
22	22	11	-	-	-	-	-	-	-	8	6	6	-	-	-	-	-	-	-	2
24	24	16	12	12	8	8	8	8	8	8	8	8	4	4	4	4	4	4	2	2
26	26	13	-	-	-	-	-	-	-	-	-	8	6	5	-	-	-	-	-	-
28	28	14	14	7	-	8	8	8	6	6	-	8	8	6	6	5	-	4	4	4
30	30	20	10	12	10	12	6	10	8	8	8	8	6	8	6	6	6	5	4	4
32	32	16	16	16	8	8	8	8	8	8	8	8	8	8	8	8	6	4	4	4
34	34	17	-	-	-	-	-	12	10	10	-	-	-	-	-	8	6	6	-	-
36	36	24	18	12	12	12	12	8	8	8	8	8	8	8	8	8	8	8	6	6
38	38	19	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	8	8	7
40	40	20	20	20	10	10	10	16	8	8	8	12	8	8	8	8	8	8	8	8

TABELLE 5.2: Maximaler Minimalabstand aller Dieder-Codes, Teil I

$\lvert G\rvert/k$	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
22	2	1																		
24	2	2	2	1																
26	-	-	-	2	2	1														
28	2	2	-	2	2	2	2	1												
30	4	4	2	2	2	2	2	2	2	1										
32	4	4	4	2	2	2	2	2	2	2	2	1								
34	-	-	-	4	2	2	-	-	-	-	-	2	2	1						
36	4	4	4	4	4	4	4	2	2	2	2	2	2	2	2	1				
38	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	2	1		
40	8	8	6	5	4	4	4	4	4	4	4	4	2	2	2	2	2	2	2	1

TABELLE 5.3: Maximaler Minimalabstand aller Dieder-Codes, Teil II

Sei nun C_0 ein selbst-orthogonaler, projektiver Dieder-Code, dann definiert die Kette

$$\mathcal{C}_\star : C_0 \leq C_0^\perp$$

einen selbst-dualen relativ-projektiven Dieder-Code $\mathcal{C}$ über $\mathbb{Z}/4\mathbb{Z}$ mit Hamming-Minimalabstand $d_H(\mathcal{C}) = d_H(C_0^\perp)$. In [DHS01, Table VII] ist der maximal mögliche Hamming-Minimalabstand aller selbst-dualen Codes über $\mathbb{Z}/4\mathbb{Z}$ angegeben (bis Länge 24), die folgende Tabelle vergleicht diese Werte mit dem maximal möglichen Hamming-Minimalabstand der selbst-dualen relativ-projektiven Dieder-Code.

Länge	10	12	14	16	18	20	22	24	26	28	30	32	36	38	40	42
	2	2	3	3	4	4	6	8								
	2	2	3	1	4	4	6	3	5	5	6	1	6	7	5	8

Besonders für ungerades n liefern die selbst-dualen, relativ-projektiven Dieder-Codes über $\mathbb{Z}/4\mathbb{Z}$ also häufig optimale oder zumindestens gute Codes.

5.3.3 Die Alternierende Gruppe A_5

Die Gruppenalgebra $\mathbb{F}_2A_5$ hat 2 zentral primitive orthogonale Idempotente e_0 und e_1, die beiden zentralen Codes sind dual zueinander, von Dimension 16 bzw. 44 und sind nicht isomorph zu abelschen Codes.
$\mathbb{F}_2A_5$ hat insgesamt $802 \cdot 2752514 = 2207516228$ Idempotente, welche $67 \cdot 3074 = 205958$ verschiedene Codes erzeugen. Die Dimensionen sind alle durch 4 teilbar und die maximalen Minimalabstände sind in der folgenden Tabelle eingetragen, wobei die Zahl in Klammern der allgemein maximal mögliche Minimalabstand für diese Dimension in Länge 60 sind.

k	4	8	12	16	20	24	28
	24 (32)	24 (27)	22 (24)	20 (20-22)	16 (17-20)	14 (16-18)	12 (16-18)

k	32	36	40	44	48	52	56	60
	10 (12-14)	8 (9-11)	6 (8-9)	6 (6-7)	4 (5)	3 (4)	2 (2)	1 (1)

Insgesamt sind die projektiven A_5-Code also in allen Dimensionen sehr nahe an dem maximal möglichen Minimalabständen.

Satz 5.35. *Sei $\mathbb{F}$ ein endlicher Körper, $C \leq \mathbb{F}A_5$ ein zweiseitiger Code und sei $A := \mathrm{PAut}(C)$ die Permutationsgruppe von C. Dann gilt entweder $A = S_{60}$ (insbesondere gilt dann $C = \{0\}$, $C = \mathbb{F}A_5$, $C = \langle\sum_{g\in A_5} g\rangle$ oder $C = \langle\sum_{g\in A_5} g\rangle^\perp$) oder C ist kein abelscher Code.*

Beweis. Der erste Fall ist klar, sei also nun $A \neq S_{60}$. Die Gruppe A enthält eine Untergruppe welche isomorph zu A_5^2 ist, und zwar alle Permutationen die von der Operation

$$A_5^2 \to A_5, ((g_1, g_2), g) \mapsto g_1 g g_2^{-1}$$

induziert werden. Bis auf Konjugation enthält S_{60} drei maximale Untergruppen, welche transitiv und primitiv sind: $\mathrm{PSL}(2,59).C_2$, $A_5^2.C_2^2$ und A_{60}. Allerdings kann A nicht in $\mathrm{PSL}(2,59).C_2$ enthalten sein, da die Ordnung schon nicht von 3600 = $|A_5^2|$ geteilt wird. Falls A in $A_5^2.C_2^2$ enthalten ist, ist C kein abelscher Code, da diese Gruppe keine transitiven, abelschen Untergruppen enthält. Sei also $A \leq A_{60}$. Angenommen es gilt $A = A_{60}$. Dann existiert genau ein weiterer Code $D \neq C$, zu dem C permutationsäquivalent ist. Sei $k = \dim(C) = \dim(D)$, dann gilt nach eventueller Dualisierung ohne Einschränkung $k \leq 30$. Die beiden Codes C und D sind permutationsäquivalent unter der Permutation $(1,2)$, also folgt, dass $C + D$ ein Code mit Permutationsgruppe $\mathrm{PAut}(C + D) = S_{60}$ ist und von Dimension $\leq k + 2 \leq 32$, was nur möglich ist, wenn C bereits von Dimension 0 oder 1 ist, also inbesondere schon $\mathrm{PAut}(C) = S_{60}$ gilt. Also ist A in einer maximalen Untergruppe von A_{60} enthalten, bis auf Konjugation gibt es davon zwei, welche transitiv und primitiv sind: $\mathrm{PSL}(2,59)$ und $A_5 \wr C_2$. Da A_5^2 nicht in $\mathrm{PSL}(2,59)$ enthalten sein kann, gilt $A \leq A_5 \wr C_2$. Diese Gruppe enthält keine transitiven, abelschen Untergruppen, also ist C kein abelscher Code. Daraus folgt insgesamt die Behauptung. □

Korollar 5.36. *Sei $C \leq \mathbb{F}A_5$ ein zweiseitiger Code, dann sind die möglichen Isomorphietypen von $\mathrm{PAut}(C)$ A_5^2, $A_5 \wr C_2$, $A_5.S_5$, $A_5^2.C_2^2$ und S_{60}.*

Kapitel 6

Extremale Gitter mit Automorphismen

In diesem Kapitel werden extremale, p-modulare Gitter mit Automorphismen der Ordnung p untersucht. Die Operation eines solchen Automorphismus liefert eine Zerlegung des zugrunde liegenden quadratischen Raumes in eine Fixpunkt- und zyklotomische Komponente, durch die Projektion bzw. den Schnitt des Gitters mit den beiden Komponenten lassen sich antiisometrische, quadratische, $\mathbb{F}_p$-wertige Räume definieren. Diese bestimmen wie im unimodularen ([Neb13]) oder teilerfremden Fall ([Jür15]) den Typ eines Automorphismus und entsprechende extremale Obergitter lassen sich durch die möglichen Antiisometrien bestimmen. Allerdings sind im Gegensatz zum teilerfremden Fall die quadratischen Räume nicht anisotrop, sondern enthalten (isomorphe) maximal total isotrope Teilräume. Diese definieren p-elementare (hermitesche) Gitter und können benutzt werden, um die Fix- und zyklotomischen Teilgitter zu bestimmen. Als Anwendung dieser Methodik wird gezeigt, dass das einzige bisher bekannte 24-dimensionale, 3-modulare, extremale Gitter das einzige solche Gitter mit einem Automorphismus der Ordnung 3 ist, diese Klassifikation wurde bisher nur für Primordnungen ≥ 5 gezeigt. Zusätzlich werden alle 5-modularen, extremalen Gitter der Dimension 20 mit einem Automorphismus der Ordnung 5 klassifiziert.

Sei $(\mathcal{V}, q)$ ein positiv definiter rationaler quadratischer Raum, das heißt ein Vektorraum über $\mathbb{Q}$ mit einer positiv definiten quadratischen Form

$$q : \mathcal{V} \to \mathbb{Q}$$

und zugehöriger Bilinearform

$$(\cdot, \cdot) := b_q : \mathcal{V} \times \mathcal{V} \to \mathbb{Q}, (x, y) \mapsto q(x + y) - q(x) - q(y).$$

Sei n die Dimension von $\mathcal{V}$, dann ist ein $\mathbb{Z}$-Gitter L in $(\mathcal{V}, q)$ das $\mathbb{Z}$-Erzeugnis

$$L = \oplus_{i=1}^{n} \mathbb{Z} b_i$$

einer Basis $(b_1, \ldots, b_n)$ von $\mathcal{V}$. Das duale Gitter ist

$$L^{\#} := \{v \in \mathcal{V} \mid (v, \lambda) \in \mathbb{Z} \text{ für alle } \lambda \in L\}.$$

Ein Gitter L heißt ganz, falls es in seinem Dualen enthalten ist, bei Gleichheit heißt es unimodular. Ein ganzes Gitter heißt gerade, falls $q(\lambda) = \frac{1}{2}(\lambda, \lambda)$ für alle $\lambda \in L$ ganzzahlig ist. Die Gram-Matrix bzgl. der Basis $(b_1, \ldots, b_n)$ ist die Matrix

$$\mathcal{G}(L) := ((b_i, b_j))_{1 \leq i,j \leq n},$$

die Determinante $\det(L)$ von L die Determinante $\det(\mathcal{G}(L))$ einer Gram-Matrix von L (unabhängig der gewählten Basis) und gleich dem Quadrat $\mathrm{vol}(\mathcal{V} \otimes \mathbb{R})/L)^2$ des Fundamentalbereichs von L. Eine zweite wichtige Invariante ist das Minimum

$$\min(L) := \min\{(\lambda, \lambda) \mid 0 \neq \lambda \in L\}.$$

Die Dichte einer zu L gehörigen Kugelpackung wird bestimmt durch das Minimum und der Determinante des Gitters L und ist gegeben durch

$$\frac{V_n}{2^n}\sqrt{\gamma(L)},$$

wobei V_n das Volumen des n-dimensionalen Einheitsballes und

$$\gamma(L) := \frac{\min(L)}{\det(L)^{\frac{1}{n}}}$$

die Hermitesche Dichte-Funktion ist. Dann sind die dichtesten Gitter in einer gegebenen Dimension gerade die Gitter, welche die Hermitesche Dichte-Funktion γ maximieren. Die dichtesten Gitter sind in den Dimensionen ≤ 8 und zusätzlich in Dimension 24 bekannt ([CK09]). In Dimension 3 wurde dies bereits durch Gauß gezeigt und erst 1998 konnte T. Hales durch den Beweis der Keplerschen Vermutung zeigen, dass diese Gitterpackung auch eine der überabzählbar vielen besten Kugelpackungen liefert ([Hal05]). Ähnliche Resultate wurden kürzlich in Dimension 8 und 24 bewiesen ([Coh+17], [Via17]). Für ein gerades Gitter L definiert die quadratische Form q eine $\mathbb{Q}/\mathbb{Z}$-wertige quadratische Form $\overline{q}$ auf der Diskriminantengruppe $L^{\#}/L$ via

$$\overline{q} : L^{\#}/L \to \mathbb{Q}/\mathbb{Z}, x + L \mapsto q(x) + \mathbb{Z}.$$

Die Stufe eines Gitters L ist die kleinste Zahl $\ell \in \mathbb{N}$, so dass das reskalierte Dualgitter

$${}^{(\ell)}L^{\#} := \sqrt{\ell}L^{\#}$$

wieder ein gerades Gitter ist. Sei ϵ der Exponent der Diskriminantengruppe von L, dann ist ϵ die kleinste Zahl, so dass ${}^{(\epsilon)}L^{\#}$ ein ganzzahliges Gitter ist. Es gilt $\ell \in \{\epsilon, 2\epsilon\}$ und $\ell L^{\#} \subset L$. Zusätzlich haben ϵ, ℓ und $\det(L)$ dieselben Primteiler, und es gilt $\epsilon = \ell$ wenn ℓ quadratfrei ist. Falls ℓ quadratfrei ist, und zusätzlich

$\det(L) = \ell^k$ gilt, ist $L^\#/L$ isomorph zu $(\mathbb{Z}/\ell\mathbb{Z})^k$, d.h. L ist ℓ-elementar.

6.1 Geschlechter von Gittern

Die p-adischen Zahlen $\mathbb{Q}_p$ sind die Vervollständigung der rationalen Zahlen (d.h. der Grenzwert aller Cauchyfolgen in $\mathbb{Q}$) unter der p-adischen Metrik

$$d_p(x, y) := \frac{1}{p^k},$$

wobei p^k die exakte Potenz in der Faktorisierung von $x - y$ ist. Die p-adischen Zahlen $\mathbb{Z}_p$ sind dann der Abschluss von $\mathbb{Z}$ in $\mathbb{Q}_p$. Für ein Gitter L in $(\mathcal{V}, q)$ ist $L_p := \mathbb{Z}_p \otimes_{\mathbb{Z}} L$ ein $\mathbb{Z}_p$-Gitter in $\mathcal{V}_p := \mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{V}$.
Das Lokal-Global-Prinzip für die Darstellung von Zahlen durch quadratische Räume (als Folgerung aus dem Satz von Minkowski-Hesse) sagt aus, dass für ein $t \in \mathbb{Q}^*$ genau dann $t \in q(\mathcal{V})$ gilt, wenn $t \in q(\mathcal{V}_p)$ für alle Primzahlen p gilt, d.h. eine Zahl lässt sich sich durch eine quadratische Form darstellen, genau dann wenn sie sich lokal für alle Primzahlen darstellen lässt. Für $\mathbb{Z}$-Gitter stimmt diese Aussage im Allgemeinen nicht, sie überträgt sich allerdings, wenn man ein Gitter durch ein sogenantes Geschlecht ersetzt. Dieses besteht aus einer (endlichen) Menge von Isomorphieklassen von Gittern und gibt an, „um wie viel“ das Lokal-Global-Prinzip fehlschlägt. Genauer gilt: Sei L ein Gitter in $(\mathcal{V}, q)$ und sei $t \in \mathbb{Q}^*$ mit $t \in q(L_p)$ für alle p. Dann existiert ein Gitter M im Geschlecht von L mit $t \in q(M)$. Das Lokal-Global-Prinzip gilt genau dann für L, wenn das Geschlecht nur aus dieser Isomorphieklasse besteht.

Definition 6.1. *Zwei $\mathbb{Z}$-Gitter L und M liegen im selben Geschlecht, falls sie über allen p-adischen ganzen Zahlen isomorph sind, d.h. es gilt $L_p \cong M_p$ für alle Primzahlen p.*

Da ein Gitter nach Definition positiv definit ist, muss im Gegensatz zu allgemeinen quadratischen Formen nicht die Vervollständigung bei $p = -1$ bzw. $p = \infty$ (je nach Notation) betrachtet werden.
Da aus $L \cong M$ direkt $L_p \cong M_p$ folgt, besteht ein Geschlecht aus Isomorphieklassen von $\mathbb{Z}$-Gittern und da sich die Werte $\det(L)$ und $q(L) \subset \mathbb{Q}$ aus allen $\det(L_p)$ und $\mathbb{Z}_p q(L_p)$ rekonstruieren lassen, ist die Anzahl h dieser Klassen endlich und heißt Klassenzahl des Geschlechts.
Seien $L := L_1, \ldots, L_h$ Repräsentanten dieser Klassen in einem Geschlecht, dann heißt

$$\sum_{i=1}^{h} |\operatorname{Aut}(L_i)|^{-1}$$

das Maß des Geschlechts. Aus dem Satz von Minkowski-Siegel folgt die Gleichung

$$\sum_{i=1}^{h} |\operatorname{Aut}(L_i)|^{-1} = \gamma(\dim(\mathcal{V})) \cdot \prod_p \alpha_p(L, L)^{-1},$$

wobei $\gamma(\dim(\mathcal{V}))$ induktiv definiert ist durch

$$\gamma(0) = 1,\ \gamma(1) = \frac{1}{2},\ \gamma(2) = \frac{1}{2\pi},\ \gamma(n) = \frac{\gamma(n-1)}{n \cdot \rho_n} = \frac{\gamma(n-1)}{n \cdot \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)}}$$

und $\alpha_p(L, L)$ ist die sogenannte lokale Darstellungsdichte, welche sich nur mit lokalen Invarianten und ohne Kenntnisse der Vertreter L_i berechnen lässt ([Kne02, (33.5)]).

Beispiel 6.2 ([Kne02, (35.2)])**.** *Im Fall der unimodularen, geraden Gitter der Dimension m gilt*

$$\alpha_p(L, L) = (1 - p^{-m/2}) \cdot \prod_{j=1}^{m/2-1} (1 - p^{-2j}),$$

also

$$\prod_p \alpha_p(L, L)^{-1} = \zeta(m/2) \cdot \prod_{i=1}^{m/2-1} \zeta(2j).$$

Für $m = 8$ ist das Maß gleich $1/696729600$, was gerade $|\operatorname{Aut}(E_8)|^{-1}$ ist. Also besteht das Geschlecht in diesem Fall nur aus dem Gitter E_8.

Das Geschlechtssymbol

Für ein Geschlecht existiert ein vollständiges System von Invarianten für p-adische Äquivalenz, diese lassen sich zu dem sogenannten Geschlechtssymbol kombinieren, welches ein Geschlecht eindeutig beschreibt (nach [CS99, Kapitel 15, Abschnitt 7]).

Jedes (ganze) Gitter L hat über den p-adischen ganzen Zahlen eine Zerlegung der Form

$$L = (L_0, q_0) \perp (L_p, pq_1) \perp (L_{p^2}, p^2 q_2) \perp \dots$$

wobei die Determinante von jedem (L_{p^i}, q_i) teilerfremd zu p ist. Diese Zerlegung wird auch Jordan-Zerlegung genannt. Für $p \neq 2$ sei nun

$$n_q = \dim(L_q) \text{ und } \epsilon_q = \left(\frac{\det(L_q)}{p}\right),$$

wobei $\left(\text{-}\right)$ das Legendre-Symbol bezeichnet. Das p-adische Symbol ist dann das formale Produkt der Faktoren

$$q^{\epsilon_q n_q}.$$

Zwei Gitter sind über den p-adischen ganzen Zahlen äquivalent, genau dann wenn sie dieselben Invarianten n_q, ϵ_q für jede Potenz q von p haben, genau dann wenn sie dasselbe p-adische Symbol haben ([CS99, Kapitel 15, Theorem 9]). Für $p = 2$ muss zusätzlich zum p-adischen Symbol noch die Parität der 2-adischen Gitter L_q betrachtet werden, dies wird mittels q_{I} bzw. q_{II} unterschieden. Im Fall

der geraden Gitter entfällt dies aber, da die L_q gerade $\mathbb{Z}_2$-Gitter sind. Ein solches Gitter L der Dimension n hat dann ein Geschlechtssymbol der Form

$$\mathrm{II}_n(\dots),$$

wobei die Klammern die p-adischen Symbole enthalten (für alle p die $2\det(L)$ teilen). Ein Geschlecht wird durch das Geschlechtssymbol eindeutig beschrieben. Mit dem Nachbarschafts-Algorithmus von M. Kneser können alle Isomorphieklassen in einem Geschlecht berechnet werden ([Kne02, Abschnitt 28]).

6.2 Hermitesche p-elementare Gitter

Sei E ein CM-Körper, d.h. eine eine total imaginäre quadratische Erweiterung eines total reellen Zahlkörpers K mit Involution $^- : E \to E$. Seien $\mathbb{Z}_K$ bzw. $\mathbb{Z}_E$ die Ganzheitsringe von K bzw. E. Sei $\mathfrak{p}$ ein Primideal in $\mathbb{Z}_K$, dann heißt $\mathfrak{p}$

$$\begin{cases} \text{träge} \\ \text{zerlegt} \\ \text{verzweigt} \end{cases} \quad \text{falls } \mathfrak{p}\mathbb{Z}_E = \begin{cases} \mathfrak{P} \\ \mathfrak{P}\overline{\mathfrak{P}} \text{ und } \mathfrak{P} \neq \overline{\mathfrak{P}} \\ \mathfrak{P}^2 \end{cases}$$

für ein Primideal $\mathfrak{P}$ von $\mathbb{Z}_E$. Die Differente $\mathfrak{D}_E$ von E ist das Inverse des gebrochenen Ideals

$$\mathfrak{D}_E^{-1} := \{a \in E \mid \mathrm{Tr}_{\mathbb{Q}}^E(a\mathbb{Z}_E) \subseteq \mathbb{Z}\}.$$

Sei nun (V, Φ) ein hermitescher Raum über E, d.h V ist ein E-Vektorraum der Dimension $m < \infty$ und $\Phi : V \times V \to E$ ist eine hermitesche Form bzgl. der Involution $^-$ mit

- $\Phi(x + x', y) = \Phi(x, y) + \Phi(x', y)$ für alle $x, x', y \in V$.
- $\Phi(\alpha x, \beta y) = \alpha\Phi(x, y)\overline{\beta}$ für alle $x, y \in V$ und $\alpha, \beta \in E$.
- $\overline{\Phi(x, y)} = \Phi(y, x)$ für alle $x, y \in V$.

Insbesondere folgt damit $\Phi(x, x) = \overline{\Phi(x, x)} \in K$ für alle $x \in V$.
Ein $\mathbb{Z}_E$-Gitter L in V ist ein endlich erzeugter $\mathbb{Z}_E$-Modul in V. Dieser muss nicht frei sein, da $\mathbb{Z}_E$ kein Hauptidealring ist, es existiert allerdings eine sogenannte Pseudobasis ([OMe63, 81:3]), also eine E-Basis $(x_1, \dots, x_n)$ von EL und gebrochene Linksideale $\mathfrak{A}_1, \dots \mathfrak{A}_n$ in $\mathbb{Z}_E$ mit

$$L = \bigoplus_{i=1}^{n} \mathfrak{A}_i x_i.$$

Das Volumenideal

$$\mathfrak{v}(L) := \mathfrak{A}_1\overline{\mathfrak{A}_1} \dots \mathfrak{A}_n\overline{\mathfrak{A}_n} \cdot \det(x_1, \dots, x_n)$$

ist unabhängig von der gewählten Pseudobasis. Sei ohne Einschränkung L ein volles Gitter in V, d.h. es gilt $V = EL$. Dann ist der Rang von L gleich der Dimension von V. Das hermitesche Dualgitter ist

$$L^* := \{x \in V \mid \Phi(x, L) \subseteq \mathbb{Z}_E\}.$$

Ein $\mathbb{Z}_E$-Gitter heißt $\mathfrak{A}$-modular (für ein gebrochenes, zweiseitiges $\mathbb{Z}_E$-Ideal $\mathfrak{A}$), wenn $\mathfrak{A}L^* = L$ gilt. Ein $\mathbb{Z}_E$-modulares Gitter heißt unimodular. Mit der hermiteschen Form Φ lässt sich eine symmetrische Bilinearform

$$\Phi_T : V \times V \to \mathbb{Q}, \Phi_T(x, y) := \mathrm{Tr}_{\mathbb{Q}}^E(\Phi(x, y))$$

definieren. Dann ist Φ_T nicht ausgeartet, genau dann wenn Φ nicht ausgeartet ist, und Φ_T ist positiv definit, genau dann wenn Φ total positiv definit ist. Als $\mathbb{Z}_E$-Modul ist ein Gitter L in V natürlich auch ein endlich erzeugter $\mathbb{Z}$-Modul, das Gitter $L \leq (V, \Phi_T)$ heißt dann Spurgitter von L, für das duale Gitter gilt die Gleichung

$$L^{\#} = \mathfrak{D}_E^{-1} L^*.$$

Für ein $\mathbb{Z}_E$-Ideal $\mathfrak{A}$ ist die Norm $\mathfrak{N}(\mathfrak{A})$ definiert als $|\mathbb{Z}_E/\mathfrak{A}|$, damit gilt für die Determinante des Spurgitters

$$\det(L) = |d_E|^{\dim_E(L)} \cdot \mathfrak{N}(\mathfrak{v}(L)).$$

Sei Ω_K die Menge der endlichen Stellen von K, d.h. die Menge der Primideale von $\mathbb{Z}_K$. Ein Stelle $\mathfrak{p} \in \Omega_K$ heißt dyadisch, falls $\mathfrak{p} \mid 2$, und nicht-dyadisch sonst. Sei $K_\mathfrak{p}$ die Vervollständigung von K an der Stelle $\mathfrak{p}$ und sei $E_\mathfrak{p} := E \otimes_K K_\mathfrak{p}$ die Vervollständigung von E. Für die Differente gilt $\mathfrak{D}_{E_\mathfrak{p}} := (\mathfrak{D}_E)_\mathfrak{p}$.
Für ein $\mathbb{Z}_E$-Gitter L in V ist $L_\mathfrak{p} := L \otimes_{\mathbb{Z}_K} Z_{K_\mathfrak{p}}$ ein $\mathbb{Z}_{E_\mathfrak{p}}$-Gitter in $V_\mathfrak{p} := V \otimes_K K_\mathfrak{p}$. Es gilt $(L^*)_\mathfrak{p} = (L_\mathfrak{p})^*$. Das (hermitesche) Geschlecht des Gitters L ist dann definiert als die Menge aller Gitter L' in V, so dass $L_\mathfrak{p} \cong L'_\mathfrak{p}$ für alle Stellen $\mathfrak{p} \in \Omega_K$ gilt.
Als Gitter über einem lokalen Körper besitzt $L_\mathfrak{p}$, ähnlich wie im Fall der p-adischen $\mathbb{Z}_p$-Gitter, eine Jordan-Zerlegung. Für jede Komponente in dieser Zerlegung ist der Isomorphietyp nur abhängig von der Modularität ([Jac62]). Sei dafür π_K ein uniformisierendes Element von $K_\mathfrak{p}$, d.h. ein Erzeuger des maximalen Ideals von $\mathbb{Z}_{K_\mathfrak{p}}$, und sei π_E ein Erzeuger des maximalen Ideals $\mathfrak{P}$ in $\mathbb{Z}_{E_\mathfrak{p}}$, welches $\mathfrak{p}\mathbb{Z}_{E_\mathfrak{p}}$ enthält und $\bar{}$-invariant ist. Sei

$$\mathbb{H}(i) := \begin{pmatrix} 0 & (\pi_E)^i \\ (\overline{\pi_E})^i & 0 \end{pmatrix}$$

die ($\mathfrak{P}^i$-modulare) hyperbolische Ebene.

Definition 6.3. *Eine Zerlegung $\Lambda = \perp_{i=1}^t \Lambda_i$ eines $\mathbb{Z}_{E_\mathfrak{p}}$-Gitters Λ heißt Jordan-Zerlegung, falls die Teilgitter $\mathfrak{P}^{s_i}$-modular sind mit $s_1 < s_2 < \cdots < s_t$.*

Jedes $\mathbb{Z}_{E_\mathfrak{p}}$-Gitter besitzt eine Jordan-Zerlegung (siehe z.B. [Kir16]).

Lemma 6.4 ([Jac62, Section 7]). *Sei $\mathfrak{p} \in \Omega_K$ eine nicht-verzweigte, nicht-dyadische Stelle, und sei Λ ein $\mathfrak{P}^i$-modulares $\mathbb{Z}_{E_\mathfrak{p}}$-Gitter, dann gilt*

$$\Lambda \cong \langle \pi_K^i, \dots, \pi_K^i \rangle.$$

Lemma 6.5 ([Jac62, Proposition 8.1]). *Sei $\mathfrak{p} \in \Omega_K$ eine verzweigte, nicht-dyadische Stelle, und sei Λ ein $\mathfrak{P}^i$-modulares $\mathbb{Z}_{E_\mathfrak{p}}$-Gitter vom Rang r, dann gilt*

$$\Lambda \cong \begin{cases} \langle \pi_K^{i/2}, \dots, \pi_K^{i/2}, \det(\Lambda)\pi_K^{i(1-r)/2} \rangle & \text{falls } i \text{ gerade} \\ \mathbb{H}(i) \perp \cdots \perp \mathbb{H}(i) & \text{falls } i \text{ ungerade.} \end{cases}$$

Die Determinante $\det(\Lambda)$ ist wohldefiniert modulo $N(E_\mathfrak{p}^*)$, also ein Element von

$$K_\mathfrak{p}^*/N(E_\mathfrak{p}^*) \cong \begin{cases} C_1 & \mathfrak{p} \text{ zerlegt} \\ C_2 & \text{sonst.} \end{cases}$$

Damit wird das lokale Geschlechtssymbol in [Kir16, Abschnitt 8.3] definiert als

$$(s_{1\pm}^{\mathrm{Rang}(\Lambda_1)}, \dots, s_{t\pm}^{\mathrm{Rang}(\Lambda_t)}),$$

wobei der Index $+$ ist, falls $\det(\Lambda_i) \in N(E_\mathfrak{p}^*)$ ist, und $-$ sonst. Im Fall dass $\mathfrak{p}$ zerlegt, ist das Vorzeichen immer $+$, kann also weggelassen werden. Falls $\mathfrak{p}$ träge ist, ist das Vorzeichen $+$, falls $s_i \cdot \mathrm{Rang}(\Lambda_i)$ gerade ist, und $-$ sonst, in diesem Fall kann es also auch weggelassen werden. Das Geschlechtssymbol eines $\mathbb{Z}_E$-Gitters L ist dann das Tupel aller lokalen Geschlechtssymbole für alle Primideale von $\mathbb{Z}_K$, die in E verzweigen oder an denen L lokal nicht unimodular ist.

Sei nun L ein hermitesches $\mathbb{Z}_E$-Gitter, so dass das Spurgitter ein gerades Gitter mit quadratfreier Stufe ℓ ist. Dann gilt $\ell L^\# \subseteq L \subseteq L^\#$ und aus $L^\# = \mathfrak{D}_E^{-1} L^*$ folgt

$$\ell \mathfrak{D}_E^{-1} L^* \subseteq L \subseteq \mathfrak{D}_E^{-1} L^*.$$

Nach Vervollständigung an einer Stelle $\mathfrak{p} \in \Omega_K$ ergibt dies

$$\ell \mathfrak{D}_{E_\mathfrak{p}}^{-1} L_\mathfrak{p}^* \subseteq L_\mathfrak{p} \subseteq \mathfrak{D}_{E_\mathfrak{p}}^{-1} L_\mathfrak{p}^*.$$

Sei nun $p > 2$ eine Primzahl und $E = \mathbb{Q}[\zeta_p]$ der p-te Kreisteilungskörper mit Involution $\bar{} : \zeta_p \mapsto \zeta_p^{-1}$. Der Fixkörper ist $K = \mathbb{Q}[\zeta_p + \overline{\zeta_p}]$. Die Erweiterung E/K ist verzweigt an der Stelle $\mathfrak{p}$ mit $\mathfrak{p} \mid p$ und unverzweigt sonst. Für das Primideal $\mathfrak{P}$ mit $p\mathbb{Z}_E = \mathfrak{P}^{p-1}$ gilt $\mathfrak{D}_E = \mathfrak{P}^{p-2}$ ([Neu92, Theorem 2.6]) und die Diskriminante von E ist

$$d_E = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

In der Jordan-Zerlegung an der Stelle p eines p-elementaren Gitters sind dann p Komponenten möglich, diese sind $\mathfrak{P}^{s_i}$-modular für $s_i \in \{2-p, \dots, 0, 1\}$. Die Elemente π_K bzw. π_E können als $(1-\zeta_p)(1-\overline{\zeta_p})$ bzw. $(1-\zeta_p)$ gewählt werden.

Die Komponenten minimaler Dimension sind diese in der folgenden Tabelle angegeben, wobei Δ ein Erzeuger von $K_p^*/N(E_p^*) \cong C_2$ ist.

$\mathfrak{P}^{2-p}$	$\mathfrak{P}^{2-p+1}$	...	$\mathfrak{P}^{-3}$	$\mathfrak{P}^{-2}$	$\mathfrak{P}^{-1}$	$\mathbb{Z}_{E_p}$	$\mathfrak{P}$
$\mathbb{H}(2-p)$	$\langle \pi_K^{\frac{2-p+1}{2}} \rangle$		$\mathbb{H}(-3)$	$\langle \pi_K^{-1} \rangle$	$\mathbb{H}(-1)$	$\langle 1 \rangle$	$\mathbb{H}(1)$
	$\langle \Delta\pi_K^{\frac{2-p+1}{2}} \rangle$			$\langle \Delta\pi_K^{-1} \rangle$		$\langle \Delta \rangle$	

Bemerkung 6.6. *Für ein Gitter, das an der Stelle p eines der obigen $\mathfrak{P}^i$-modularen Gitter minimaler Dimension ergibt, gilt für die Determinante des Spurgitters*

$$\begin{cases} p^{p-2+i} & \text{falls } i \text{ gerade} \\ p^{p+i} & \text{falls } i \text{ ungerade.} \end{cases}$$

Bemerkung 6.7. *Sei L ein z-dimensionales Gitter über E, so dass das Spurgitter p-elementar mit Determinante p^m ist. Dann gilt*

$$p^m = \det(L) = |d_E|^z \cdot \mathfrak{N}(\mathfrak{v}(L)) = p^{z(p-2)} \cdot \mathfrak{N}(\mathfrak{v}(L)),$$

insbesondere gilt also $\mathfrak{N}(\mathfrak{v}(L)) = |\mathbb{Z}_E/\mathfrak{v}(L)| = p^{m-z(p-2)}$. An der Stelle p folgt damit $\mathfrak{v}(L_p) = \mathfrak{P}^{m-z(p-2)}$. Für die minimalen Komponenten gilt nun $\mathfrak{v}(\mathbb{H}(i)) = \mathfrak{P}^{2i}$ bzw. $\mathfrak{v}(\langle \pi_K^{i/2} \rangle) = \mathfrak{P}^i$. Zusammen mit $\mathfrak{v}(L \perp L') = \mathfrak{v}(L) \cdot \mathfrak{v}(L')$ lässt sich damit die Norm der Jordan-Zerlegung von L_p bestimmen.

Lemma 6.8. *Die Determinante eines $\mathbb{Z}_{E_p}$-Gitters L ist eine Norm.*

Beweis. Sei $\beta := \zeta_p^2 + \overline{\zeta_p}^2 - 2 \in \mathbb{Q}[\zeta + \overline{\zeta_p}]$, dann gilt $\mathbb{Q}[\zeta_p] = \mathbb{Q}[\zeta_p + \overline{\zeta_p}](\sqrt{\beta})$, und $\det(L)$ ist eine Norm, genau dann wenn

$$(\beta, \det(L))_p = 1,$$

wobei $(\cdot,\cdot)_p$ das Hilbert-Symbol an der Stelle p bezeichnet (siehe [OMe63, 63:10]). Nach dem Reziprozitätsgesetzt ([OMe63, 71:18]) gilt

$$(\beta, \det(L))_p = \prod_{q \neq p} (\beta, \det(L))_q,$$

daraus folgt die Behauptung. □

Beispiel 6.9. *(Die 3-elementaren $\mathbb{Z}[\zeta_3]$-Gitter)*
Die Komponenten in kleinster Dimension sind hier

$\mathfrak{P}^{-1}$	$\mathbb{Z}_{E_p}$	$\mathfrak{P}$
$\mathbb{H}(-1)$	$\langle 1 \rangle$	$\mathbb{H}(1)$

.

Nach Bemerkung 6.6 ist die Determinante des Spurgitter eines $\mathbb{Z}[\zeta_3]$-Gitters L von Rang 2, welches an der Stelle 3 isomorph zu $\mathbb{H}(-1)$ ist, 3, nach Bemerkung 6.7 gilt allerdings

$$\det(L) = 3^2 \cdot \mathfrak{N}(\mathfrak{v}(L)) = 3^2 \cdot 3^{-2},$$

ein Widerspruch und ein solches Gitter existiert nicht. Auf diese Weise lassen sich Vertreter der Geschlechter p-elementarer Gitter angegben. Minimale $\mathbb{Z}$-Gitter mit einer hermiteschen $\mathbb{Z}[\zeta_3]$-Struktur, die nach Vervollständigung an der Stelle 3 die möglichen Komponenten liefern, lassen sich folgendermaßen konstruieren:

(1)	Das Gitter A_2
$\mathbb{H}(1) \perp (1) \perp (1)$	Eindeutiges Teilgitter in A_2^4 mit Elementarteiler 3^6
$\mathbb{H}(1) \perp \mathbb{H}(1)$	Eindeutiges Teilgitter in A_2^4 mit Elementarteiler 3^8
$\mathbb{H}(-1) \perp \mathbb{H}(1)$	Gitter im Geschlecht von A_2^4 (von Klassenzahl 2)
$\mathbb{H}(-1) \perp (1) \perp (1)$ und $\mathbb{H}(-1) \perp \mathbb{H}(-1)$	Hermitesche Dualgitter der obigen Gitter

Aus diesen lassen sich dann Vertreter der Geschlechter 3-elementarer (Spur-)Gitter mit gegebener Determinante kombinieren. Für die Geschlecht der 3-modularen Gitter vom Rang z sind diese z.B.

$$\mathbb{H}(1)^a \perp (1)^{z-4a} \perp \mathbb{H}(-1)^a \textit{ mit } a = 0, \ldots, \lfloor z/4 \rfloor .$$

6.3 Modulare und extremale Gitter

Die Eigenschaft einer Extremalität wurde zuerst für unimodulare Gitter definiert und bedeutet, dass das Minimum so groß ist, wie die Theorie der Modulformen es zulässt. Sei L ein gerades, unimodulares Gitter, dann hat die Theta-Reihe

$$\Theta_L(z) := \sum_{\lambda \in L} q^{\frac{1}{2}(\lambda,\lambda)} \text{ mit } q = e^{2\pi i z}$$

des Gitters die Potenzreihenentwicklung

$$\Theta_L(z) = \sum_{m=0}^{\infty} a_m(L) q^m$$

mit

$$a_m(L) := |\{x \in L \mid (x,x) = 2m\}|.$$

Die Theta-Reihe definiert eine holomorphe Funktion auf der oberen Halbebene

$$\mathbb{H} := \{\tau \in \mathbb{C} \mid \Im(\tau) > 0\}$$

und ist eine Modulform vom Gewicht $\frac{n}{2}$ für die Gruppe $\mathrm{SL}_2(\mathbb{Z})$. Außerdem gilt $n \equiv 0 \pmod 8$ ([Ebe13, Theorem 2.1]).
Die Modulformen vom Gewicht k bilden einen $\mathbb{C}$-Vektorraum $\mathcal{M}_k$, wobei die Dimension für ungerades k Null ist. Die Algebra $\mathcal{M}$ aller Modulformen ist eine

graduierte Algebra, d.h. es gilt

$$\mathcal{M} = \bigoplus_{k=0}^{\infty} \mathcal{M}_k$$

und $\mathcal{M}_i \cdot \mathcal{M}_j \subset \mathcal{M}_{i+j}$. Zusätzlich ist $\mathcal{M}$ gerade die Polynomalgebra $\mathbb{C}[E_4, E_6]$ in den normalisierten Eisensteinreihen vom Index 4 und 6. Dies kann benutzt werden, um zu zeigen, dass die Abbildung

$$\mathcal{M}_{\frac{n}{2}} \to \mathbb{C}^d, \sum_{m=0}^{\infty} a_m q^m \mapsto (a_0, \ldots, a_{d-1})$$

für $n \equiv 0 \pmod 8$ ein Isomorphismus ist, wobei die Dimension

$$d = \dim \mathcal{M}_{\frac{n}{2}} = 1 + \left\lfloor \frac{n}{24} \right\rfloor$$

ist.

Satz 6.10 ([MOS75], [Sie69])**.** *Es gilt $a_d > 0$, insbesondere folgt für ein ein gerades, unimodulares Gitter L der Dimension n die Abschätzung*

$$\min(L) \leq 2 + 2 \left\lfloor \frac{n}{24} \right\rfloor .$$

Für nicht-gerade unimodulare Gitter folgt mit ähnlichen Methoden die Abschätzung

$$\min(L) \leq 1 + \left\lfloor \frac{n}{8} \right\rfloor .$$

Allerdings war auch bekannt, dass diese nur von genau 12 solcher Gitter angenommen wird, wobei die höchste Dimension 23 ist. In [CS90] wurde die Abschätzung zu

$$\min(L) \leq \left\lfloor \frac{n+6}{10} \right\rfloor ,$$

für n genügend groß, verbessert. In [RS98a] wurde schließlich dieselbe Abschätzung wie für gerade unimodulare Gitter gezeigt:

Satz 6.11. *Sei L ein unimodulares Gitter der Dimension n, dann gilt*

$$\min(L) \leq 2 + 2 \left\lfloor \frac{n}{24} \right\rfloor ,$$

außer im Fall $n = 23$, hier gilt $\min(L) \leq 3$.

Definition 6.12. *Ein gerades unimodulares Gitter L der Dimension n heißt extremal, falls $\min(L) = 2 + 2\lfloor \frac{n}{24} \rfloor$ gilt.*

Bisher sind 6 extremale unimodulare Gitter in den Sprungdimensionen (d.h. Vielfache von 24) bekannt, das bereits erwähnte Leech-Gitter Λ_{24}, die Gitter P_{48q},

P_{48p}, P_{48n} und P_{48m} in Dimension 48 ([CS99], [Neb98], [Neb14]) und das bisher einzige bekannte extremale Gitter Γ_{72} in Dimension 72 ([Neb12a]).

Der Begriff eines modularen Gitters wurde von H.-G. Quebbemann in [Que95] eingeführt. Motiviert wurde der Begriff dadurch, dass einige bekannte Gitter, wie das Barnes-Wall-Gitter BW_{16} oder das Coxeter-Todd-Gitter K_{12}, zwar nicht unimodular, aber geometrisch ähnlich zu ihrem Dualen Gitter sind.

Definition 6.13. *Sei ℓ eine quadratfreie, natürliche Zahl und sei L ein gerades Gitter der Stufe ℓ. Dann heißt L ℓ-modular, falls L isomorph zum reskalierten Dualgitter ${}^{(\ell)}L^{\#}$ ist. Falls L für jeden Teiler d von ℓ isomorph zum partiellen Dualgitter*

$$L^{\#,d} := L^{\#} \cap \tfrac{1}{d}L$$

ist, heißt L stark ℓ-modular.

Ein stark ℓ-modulares Gitter ist also insbesondere ℓ-modular und falls ℓ eine Primzahl ist, fallen die beiden Begriffe zusammen. Aus

$$\det(L) = \det(\sqrt{\ell}L^{\#}) = \ell^n \det(L)^{-1}$$

folgt $\det(L) = \ell^{\frac{n}{2}}$. Für ein ℓ-modulares Gitter gilt also

$$L^{\#}/L \cong (\mathbb{Z}/\ell Z)^{\frac{n}{2}}.$$

Auf eine ähnliche Weise wie für gerade, unimodulare Gitter lässt sich auch hier eine Abschätzung für das Minimum beweisen ([Que95], [Que97]). Sei ℓ quadratfrei und sei

$$\Gamma_0(\ell) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{\ell} \right\}$$

die Kongruenzuntergruppe von $\mathrm{SL}_2(\mathbb{Z})$ mit Normalisator $\Gamma_*(\ell)$ in $\mathrm{SL}_2(\mathbb{R})$. Falls ℓ eine Primzahl ist, gilt

$$\Gamma_*(\ell) = \Gamma_0(\ell) \cup \Gamma_0(\ell) \cdot t_\ell,$$

wobei

$$t_\ell = \begin{pmatrix} 0 & \frac{1}{\sqrt{\ell}} \\ -\sqrt{\ell} & 0 \end{pmatrix}$$

die Fricke-Involution ist. Für quadratfreies $\ell \in \mathbb{N}$ ist die Faktorgruppe $\Gamma_*(\ell)/\Gamma_0(\ell)$ 2-elementar abelsch und wird von gewissen Atkin-Lehner-Involutionen erzeugt. Sei nun $\sigma_0(\ell)$ die Anzahl der (positiven) Teiler von ℓ und sei $\sigma_1(\ell)$ die Summe dieser Teiler. Falls $\sigma_1(\ell)$ ein Teiler von 24 ist, also

$$\ell \in \{1, 2, 3, 5, 6, 7, 11, 14, 15, 23\},$$

ist die Abbildung

$$\mathcal{M}_{\frac{n}{2}}(\Gamma_*(\ell), \chi_{\frac{n}{2}}) \to \mathbb{C}^{d_\ell}, \sum_{m=0}^{\infty} a_m q^m \mapsto (a_0, \ldots, a_{d_\ell} - 1)$$

ein Isomorphismus und es gilt

$$d_\ell = \dim \mathcal{M}_{\frac{n}{2}}(\Gamma_*(\ell), \chi_{\frac{n}{2}}) = 1 + \left\lfloor \frac{n \cdot \sigma_1(\ell)}{24 \cdot \sigma_0(\ell)} \right\rfloor.$$

Diese Stufen heißen auch Quebbemannsche Stufen. Der Charakter $\chi_{\frac{n}{2}}$ ist auf $\Gamma_0(\ell)$ als $\left(\frac{-\ell}{d_\ell}\right)$ definiert ist und wird mit Hilfe von Gaußschen Summen auf die erzeugenden Atkin-Lehner Involutionen fortgesetzt (im Fall $\ell = 6$ gibt es hier zwei Möglichkeiten, daher unterscheidet man zwischen den Fällen $6a$ und $6b$). Außerdem ist der Koeffizient a_{d_ℓ} für die extremale Modulform positiv, daraus folgt die folgende Abschätzung:

Satz 6.14. *Sei L ein stark ℓ-modulares Gitter der Dimension n, so dass $\sigma_1(\ell)$ ein Teiler von 24 ist. Dann gilt*

$$\min(L) \leq 2 + 2 \left\lfloor \frac{n \cdot \sigma_1(\ell)}{24 \cdot \sigma_0(\ell)} \right\rfloor.$$

und im Fall der Gleichheit heißt L extremal.

Bemerkung 6.15. *Sei ℓ eine Primzahl und $n \equiv 2 \pmod 4$, falls $\ell \equiv 3 \pmod 4$ und $n \equiv 0 \pmod 4$ sonst. Dann gibt es nach [Que95, Theorem 2], genau ein Geschlecht von geraden Gittern der Dimension n, Stufe ℓ und Determinante $\ell^{n/2}$. In diesem existiert mindestens ein ℓ-modulares Gitter.*

ℓ	Geschlechtssymbol für $r \in \mathbb{N}$
1	II_{8r}
2	$\mathrm{II}_{4r}\left(2^{(-1)^r 2r}\right)$
3	$\mathrm{II}_{2r}\left(3^{(-1)^r r}\right)$
5	$\mathrm{II}_{4r}\left(5^{(-1)^r 2r}\right)$
6	$\mathrm{II}_{8r}\left(2^{+4r}3^{+4r}\right)$
$6a$	$\mathrm{II}_{8r-4}\left(2^{+(4r-2)}3^{+(4r-2)}\right)$
$6b$	$\mathrm{II}_{8r-4}\left(2^{-(4r-2)}3^{-(4r-2)}\right)$
7	$\mathrm{II}_{2r}\left(7^{+r}\right)$
11	$\mathrm{II}_{2r}\left(11^{(-1)^r r}\right)$
14	$\mathrm{II}_{4r}\left(2^{+2r}7^{+2r}\right)$
15	$\mathrm{II}_{4r}\left(3^{(-1)^r 2r}5^{(-1)^r 2r}\right)$
23	$\mathrm{II}_{2r}\left(23^{+r}\right)$

TABELLE 6.1: Geschlechtssymbole der Quebbemanschen Geschlechter

Viele extremale Gitter wurden von G. Nebe und W. Plesken im Zuge der Klassifikation maximaler, endlicher, rationaler Matrixgruppen entdeckt ([NP95]). Andere Gitter wurden von C. Bachoc mit Hilfe von Zahlenkörpern, Quaternionen und Codes konstruiert (siehe auch [SS99] für einen Übersichtsartikel). In [Neb13]

wurde ein Langzeitprojekt gestartet, um alle 48-dimensionalen, unimodulare, extremale Gitter mit gegebenen Automorphismen zu klassifizieren. Für den aktuellen Stand der Klassifikation von extremalen, stark ℓ-modularen Gittern siehe [Jür15] oder die entsprechende Tabelle in [NS].

6.4 Automorphismen eines Gitters

Die Automorphismengruppe eines $\mathbb{Z}$-Gitters L in einem quadratischen Raum $(\mathcal{V}, q)$ ist

$$\mathrm{Aut}(L) := \{\sigma \in \mathrm{GL}(\mathcal{V}) \mid L \cdot \sigma = L \text{ und } q(\lambda \cdot \sigma) = q(\lambda) \text{ für alle } \lambda \in L\}.$$

Sei $\sigma \in \mathrm{Aut}(L)$ ein Automorphismus der Ordnung p für eine Primzahl $p > 2$. Dann ist das Minimalpolynom $\mu_\sigma(x)$ von σ ein Teiler von $x^p - 1$, es gilt also entweder $\mu_\sigma = x^p - 1$ oder $\mu_\sigma = \Phi_p$, wobei $\Phi_p := \frac{x^p-1}{x-1} = 1 + x + \cdots + x^{p-1}$ das p-te Kreisteilungspolynom ist. Dadurch zerfällt $\mathcal{V}$ in die orthogonale, direkte Summe $\mathcal{V} = \mathcal{V}_F \perp \mathcal{V}_Z$ mit

$$\mathcal{V}_F := \mathrm{Kern}(\sigma - 1) \text{ und } \mathcal{V}_Z := \mathrm{Kern}(\Phi_p(\sigma)).$$

Der Raum $\mathcal{V}_Z$ wird durch die Multiplikation

$$\zeta_p v = v \cdot \sigma$$

zu einem $\mathbb{Q}[\zeta_p]$-Vektorraum der Dimension $z := \dim_{\mathbb{Q}[\zeta_p]}(\mathcal{V}_Z) = \frac{\dim_{\mathbb{Q}}(\mathcal{V}_Z)}{p-1}$. Sei zusätzlich $f := \dim_{\mathbb{Q}}(\mathcal{V}_F) = n - (p-1)z$. Die Projektionen auf die beiden Räume sind gegeben durch

$$\pi_F : \mathcal{V} \to \mathcal{V}_F, v \mapsto v \cdot \tfrac{1}{p} \cdot (1 + \sigma + \cdots + \sigma^{p-1})$$

bzw.

$$\pi_Z : \mathcal{V} \to \mathcal{V}_Z, v \mapsto v - \pi_F(v).$$

Definition 6.16. *Die Gitter $F(L) := L \cap \mathcal{V}_F$ und $Z(L) := L \cap \mathcal{V}_Z$ heißen σ-Fixgitter bzw. σ-zyklotomisches Teilgitter von L.*

Lemma 6.17 ([Mar03, Proposition 1.3.4])**.** *Es gilt $\pi_F(L^\#) = F(L)^\#$ und $\pi_Z(L)^\# = Z(L)^\#$.*

Diese Zerlegung wurde in [Neb13] benutzt, um den Typ eines Automorphismus σ der Ordnung p eines (extremalen) geraden unimodularen Gitters L zu definieren: das Teilgitter $F(L) \perp Z(L)$ hat Index p^s in L mit $s \leq \min(f, z)$, der Typ von (L, σ) ist dann definiert das Tupel $p - (f, z) - s$. Aus $L = L^\#$ folgt hier

$$\pi_F(L)/F(L) \cong \pi_Z(L)/Z(L) \cong \mathbb{F}_p^s$$

und es gilt $s \equiv z \pmod 2$. Damit wurden alle möglichen Typen von (L, σ) für ein extremales, unimodulares Gitter der Dimension 48 bestimmt. Zusätzlich wurden alle solchen Gitter mit einem Automorphismus der Ordnung m, $\varphi(m) > 24$, klassifiziert. In [Neb14] wurde so ein viertes extremales, unimodulares Gitter der Dimension 48 gefunden. In [Jür15] wurden diese Methoden auf Gitter der Stufe ℓ (ℓ prim) mit einem Automorphismus der Ordnung p angewendet, wobei ℓ und p teilerfremd sind. In diesem Fall gilt

$$F(L)^{\#,p}/F(L) \cong Z(L)^{\#,p}/Z(L) \cong \mathbb{F}_p^s$$

mit $s \leq \min(f, z)$. Mit

$$\det(F(L)) = p^s \cdot \ell^{k_1} \text{ und } \det(Z(L)) = p^s \cdot \ell^{k_\zeta}$$

wurde der Typ hier als $p - (f, z) - (k_1, k_\zeta)$ definiert (in [Neb19b] heißt dieser Typ det-Typ). Die Geschlechter von $F(L)$ und $Z(L)$ sind durch den Typ von (L, σ) eindeutig bestimmt. Damit wurden viele ℓ-modulare Gitter mit einem Automorphismus der Ordnung p klassifiziert.

6.4.1 Automorphismen der Ordnung p eines p-elementaren Gitters

Sei im folgenden L ein p-modulares Gitter (p prim) mit einem Automorphismus $\sigma \in \mathrm{Aut}(L)$ von Ordnung p. Eine einfache Möglichkeit zur Konstruktion von σ-invarianten, extremalen Gittern ist der Übergang zu (maximalen) Obergittern. Deren Geschlecht ist eindeutig ([CS99, Chapter 15, Theorem 13]) und das Maß ist kleiner als das der p-modularen Gitter (siehe auch [Neb19b] für zusammengesetzte Stufen).

Satz 6.18. *Sei L ein p-elementares, gerades Gitter mit einem Automorphismus σ der Ordnung p und sei M ein maximales, gerades $\mathbb{Z}[\sigma]$-Obergitter von L. Dann ist M bereits ein maximales, gerades $\mathbb{Z}$-Gitter in $\mathbb{Q}L$.*

Beweis. Die quadratische Form q_M ist σ-invariant, also ist die Diskrimantengruppe $M^\#/M$ über $\mathbb{Z}[\sigma]$ ein quadratischer Raum. Dieser ist anisotrop, denn jeder isotrope Vektor würde bereits in M liegen. Daraus folgt für einen Teilraum $X \leq M^\#/M$, dass $X \cap X^\perp = \{0\}$ gilt, also ist $M^\#/M$ die direkte Summe von X und $X^\perp$ und damit ein halbeinfacher $\mathbb{F}_p[\sigma]$-Modul. Der einzige einfache $\mathbb{F}_p[\sigma]$-Modul ist allerdings $\mathbb{F}_p$, also ist $M^\#/M$ ein anisotroper $\mathbb{F}_p$-Vektorraum und damit bereits als gerades $\mathbb{Z}$-Gitter maximal. □

Bemerkung 6.19. *Seien L_1, L_2 Gitter mit $L_1/L_2 \cong \mathbb{F}_p^m$ und sei $U \leq \mathrm{Aut}(L_1) \cap \mathrm{Aut}(L_2)$ mit einem $\sigma \in U$ von Prim-Ordnung p. Der Automorphismus σ operiert als $\overline{\sigma} \in \mathrm{GL}_m(\mathbb{F}_p)$ auf L_1/L_2, alle minimalen σ-invarianten Gitter in L_1/L_2 sind dann gegeben durch die eindimensionalen Teilräume von $\mathrm{Kern}(\overline{\sigma} - 1)$. Auf diesen Teilräumen operiert zusätzlich der Normalisator $\mathrm{N}_U(\sigma)$ von σ in U.*

Beispiel 6.20. *Sei L ein 16-dimensionales, 7-modulares, extremales Gitter mit einem Automorphismus σ der Ordnung 7, dann ist L in einem σ-invarianten, unimodularem Gitter enthalten. Es gibt zwei unimodulare Gitter in Dimension 16, diese haben jeweils zwei Konjugiertenklassen von Automorphismen der Ordnung 7 und es lassen sich damit sechs 7-modulare, extremale Gitter mit einem Automorphismus der Ordnung 7 konstruieren. Davon waren fünf bisher nicht bekannt (Einträge 14 bis 18 in der entsprechenden Tabelle in [NS]).*

Sei $R = \mathbb{Z}_p[\sigma] \cong \mathbb{Z}_p C_p$ der Gruppenring der zyklischen Gruppe der Ordnung p über dem Ring der p-adischen ganzen Zahlen. Dieser Ring hat drei unzerlegbare Gitter, den regulären Modul R, den trivialen Modul $\mathbb{Z}_p$ und das irreduzible Gitter $\mathbb{Z}_p[\zeta_p]$ vom Grad $p-1$ ([Rei57]). Als R-Modul ist L_p nach dem Satz von Krull-Schmidt-Remak isomorph zur direkten Summe von unzerlegbaren Gittern, d.h.

$$L_p \cong R^a \oplus \mathbb{Z}_p[\zeta_p]^b \oplus \mathbb{Z}_p^c.$$

Damit lässt sich eine analoge Aussage zum teilerfremden Fall beweisen:

Lemma 6.21. *Es gilt*

$$p\pi_F(L) \perp \pi_Z(L) \cdot (1-\sigma) \subseteq F(L) \perp Z(L) \subseteq L \subseteq \pi_F(L) \perp \pi_Z(L)$$

und L ist ein volles, subdirektes Produkt von $\pi_F(L)$ und $\pi_Z(L)$. Als $\mathbb{F}_p[\sigma]$-Moduln gilt die Isomorphie

$$\pi_F(L)/F(L) \cong \pi_Z(L)/Z(L) \cong \mathbb{F}_p^s$$

mit $s \leq \min(f, z)$.

Beweis. Sei

$$L_p \cong R^a \oplus \mathbb{Z}_p[\zeta_p]^b \oplus \mathbb{Z}_p^c.$$

Das Gitter $F(L)_p$ ist ein Teilgitter der Dimension $a+c$ von L_p und es gilt

$$(\pi_F(L)_p)/(F(L)_p) \cong (\mathbb{Z}_p/p\mathbb{Z}_p)^a \cong \pi_F(L)/F(L) \cong \mathbb{F}_p^s,$$

also folgt $a = s$ und $f = s + c \geq s$. Analog folgt $z = s + b \geq s$. Direkt aus der Definition folgt $p\pi_F(L) \subseteq F(L)$, und da $(1-\sigma)$ den Modul $\pi_Z(L)/Z(L) \cong \mathbb{F}_p^s$ annihiliert, gilt $\pi_Z(L) \cdot (1-\sigma) \subseteq Z(L)$. □

Definition 6.22. *Das Tupel $p-(f,z)-s$ heißt der Typ von (L,σ).*

Ein Gitter $L_p \cong R^a \oplus \mathbb{Z}_p[\zeta_p]^b \oplus \mathbb{Z}_p^c$ hat also den Typ

$$p-(a+c, a+b)-a,$$

insbesondere bestimmt der Typ (L,σ) den Isomorphietyp von L als $\mathbb{Z}_p[\sigma]$-Modul, und L ist ein freier $\mathbb{Z}_p[\sigma]$-Modul, genau dann wenn (L,σ) den Typ $p-(s,s)-s$ hat.

Lemma 6.23. *Die Typen von (L,σ), $(L^\#,\sigma)$ und jedem partiellen Dualgitter $(L^{\#,d},\sigma)$ sind gleich.*

Beweis. Bezüglich der (σ-invarianten) quadratischen Form q gilt $L^\# \cong \mathrm{Hom}_\mathbb{Z}(L,\mathbb{Z})$ und $\mathbb{Z}_p \otimes_\mathbb{Z} L \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p \otimes_\mathbb{Z} L, \mathbb{Z}_p)$. Als $\mathbb{Z}_p[\sigma]$-Modul sind dann $\mathbb{Z}_p \otimes_\mathbb{Z} L$ und $\mathbb{Z}_p \otimes_\mathbb{Z} L^\#$ isomorph, da alle unzerlegbaren direkten Summanden von $\mathbb{Z}_p \otimes_\mathbb{Z} L^\#$ selbst-dual sind. Daraus folgt, dass die Typen von (L,σ) und $(L^\#,\sigma)$ gleich sind. Für das partielle Dualgitter gilt

$$\mathbb{Z}_p \otimes_\mathbb{Z} L^{\#,d} = \begin{cases} \mathbb{Z}_p \otimes_\mathbb{Z} L^\# & \text{falls } p \mid d \\ \mathbb{Z}_p \otimes_\mathbb{Z} L & \text{sonst .} \end{cases}$$

Daraus folgt die Behauptung. □

Folgerung 6.24. *Das Fixgitter $F(L^\#)$ hat Index p^s in $\pi_F(L^\#) = F(L)^\#$. Aus $\det(F(L)) \cdot \det(F(L)^\#) = 1$ folgt damit*

$$\det(F(L)) \cdot \det(F(L^\#)) = p^{2s}$$

und analog

$$\det(Z(L)) \cdot \det(Z(L^\#)) = p^{2s}.$$

Lemma 6.25. *Der größte mögliche Elementarteiler von $F(L)$ bzw. $Z(L)$ ist p^2.*

Beweis. Zu zeigen ist, dass $p^2F(L)^\#$ in $F(L)$ bzw. $p^2Z(L)^\#$ in $Z(L)$ enthalten ist. Die Aussage folgt dann direkt mit $\pi_F(L^\#) = F(L)^\#$, denn es gilt

$$p^2\pi_F(L^\#) = p\pi_F(pL^\#) \subseteq p\pi_F(L) \subseteq F(L).$$

Die entsprechende Aussage für $Z(L)$ folgt analog. □

Bemerkung 6.26. *Im Fall $s = f$ gilt $\pi_F(L) = \frac{1}{p}F(L)$, denn es ist $\pi_F(L)/F(L) \cong \mathbb{F}_p^s$ und $\frac{1}{p}F(L)/F(L) \cong \mathbb{F}_p^f$. Da $L^\#$ ein Teilgitter von $\frac{1}{p}L$ ist, ist in diesem Fall $F(L^\#)$ in*

$$\tfrac{1}{p}F(L) = \pi_F(L) = F(L^\#)^\#$$

enthalten, insbesondere ist also $F(L^\#)$ ein gerades Gitter. Analog gilt im Fall $s = z$ die Gleichheit

$$\pi_Z(L) = Z(L) \cdot (1-\zeta_p)^{-1}.$$

Bis hierhin unterscheidet der Fall, dass die Modularität gleich der Ordnung des Automorphismus ist, nicht sonderlich vom teilerfremden Fall. Die Besonderheit ist, dass die quadratischen Räume $\pi_F(L)/F(L)$ bzw. $\pi_Z(L)/Z(L)$ maximale total isotrope Teilräume enthalten. Diese definieren p-elementare Gitter (insbesondere ist deren Geschlecht als $\mathbb{Z}$-Gitter eindeutig) und können benutzt werden, um alle möglichen Paare $(\pi_F(L), F(L))$ bzw. $(\pi_Z(L), Z(L))$ zu bestimmen.

Berechnung der $(\pi_F(L), F(L))$

Bemerkung 6.27. *Seien*

$$X_F(L) := \pi_F(L) \cap F(L^\#) \text{ und}$$
$$Y_F(L) := \pi_F(L^\#) \cap \frac{1}{p}F(L).$$

Dann sind $X_F(L)$ und ${}^{(p)}Y_F(L)$ gerade, p-elementare Gitter mit

$$X_F(L)^\# := \pi_F(L) + F(L^\#) \text{ und}$$
$$Y_F(L)^\# := p\pi_F(L^\#) + F(L).$$

Zusätzlich gilt

$$Y_F(L)^\# \subseteq X_F(L) \subseteq X_F(L)^\# \subseteq Y_F(L) \subseteq \tfrac{1}{p}Y_F(L)^\#$$

Insbesondere wird p^f von $\det({}^{(p)}Y_F(L)) \cdot \det(X_F(L))$ geteilt.

Lemma 6.28. *Das Gitter $X_F(L)$ ist das Radikal der quadratischen Form*

$$\pi_F(L)/F(L) \to \tfrac{1}{p}\mathbb{Z}/\mathbb{Z} \cong \mathbb{F}_p,$$

da jeder weitere isotrope Vektor von $\pi_F(L)$ ebenfalls in $\pi_F(L)^\# = Z(L^\#)$ liegen würde.

Lemma 6.29. *Mit der Notation von Abbildung 6.1 sind die Elementarteiler von $F(L)$ p^{2x+b+a} und $(p^2)^{s-a-x}$.*

Beweis. Nach Lemma 6.25 ist der größte Elementarteiler p^2. Direkt aus der Definition folgt, dass $Y_F(L)$ das maximale Teilgitter von $F(L)^\# = \pi_F(L^\#)$ ist, so dass $pY_F(L)$ in $F(L)$ enthalten ist, also kommt p^2 gerade mit der Vielfachheit $s-a-x$ vor. Zusammen mit $|\pi_F(L)/F(L)| = p^{2s-a+b}$ folgt daraus die Behauptung. □

Bemerkung 6.30. *1) Es gilt*

$$\det(F(L)) = p^{2s-a+b}$$

und aus $\det(F(L)) = \det(F(L^\#)) \cdot \left(p^{b+s-a}\right)^2$ folgt $\det(F(L^\#)) = p^{-b+a}$, also insbesondere $\det({}^{(p)}F(L^\#)) = p^{f-b+a}$. Damit gilt

$$\det(F(L)) \cdot \det({}^{(p)}F(L^\#)) = p^{2s+f}.$$

Also ist $F(L)$ oder ${}^{(p)}F(L^\#)$ ein Gitter mit Determinante $\leq p^{(2s+f)/2}$ und Minimum $\geq \min(L)$.
2) Analog dazu folgt

$$\det(F(L^\#)) \cdot \det({}^{(1/p)}F(L)) = p^{2s-f}.$$

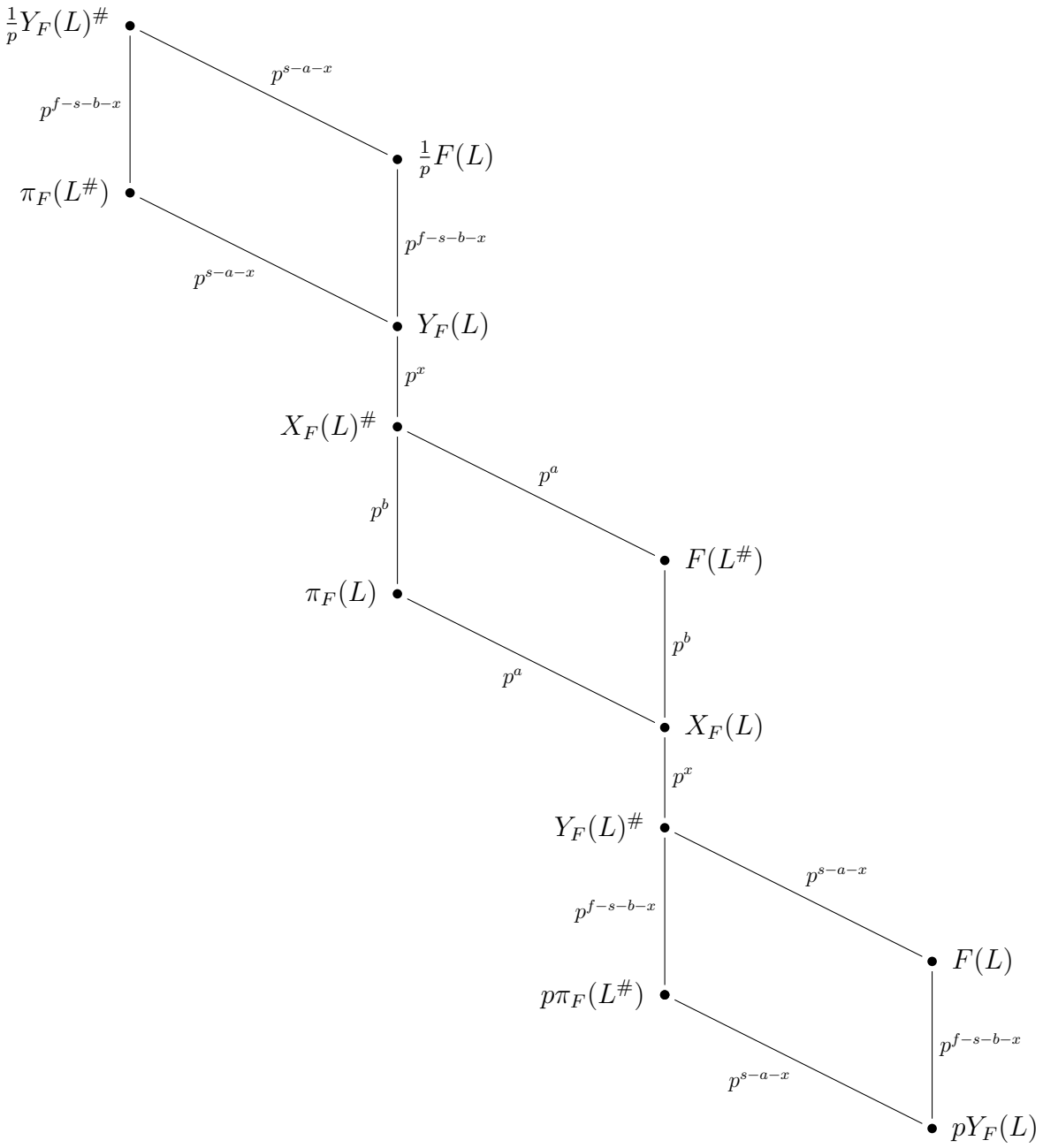


ABBILDUNG 6.1: Verband der Gitter $X_F(L)$ bzw. $Y_F(L)$

Es gilt ${}^{(p)}Y_F(L) = \pi_F({}^{(p)}L^{\#}) \cap F({}^{(1/p)}L)$, also gilt (nachdem eventuell L durch ${}^{(p)}L^{\#}$ ersetzt wurde) nach Bemerkung 6.27 ohne Einschränkung

$$\det(X_F(L)) \leq p^{f/2}$$

Da $X_F(L)$ p-elementar ist, enthält es ein Gitter, welches im Geschlecht der p-modularen Gitter liegt. Davon ausgehend lassen sich erst alle möglichen $F(L^{\#})$ (mit Minimum $\geq \frac{\min(L)}{p}$) bestimmen, in den $\pi_F(L) = F(L^{\#})^{\#}$ muss man schließlich noch alle geeigneten $F(L)$ vom Index p^s berechnen).

Algorithmus 6.31. Eingabe: *Der Typ $p-(f,z)-s$ eines Automorphismus eines p-modularen, extremalen Gitters L.*
Ausgabe: *Repräsentanten der möglichen Paare $(\pi_F(L), F(L))$.*
Algorithmus:

1) *Bestimme Vertreter $U_1, \ldots, U_k$ des Geschlechts der f-dimensionalen p-modularen Gitter.*

2) *Für $i = 1, \ldots, k$ bestimme die Menge $\mathcal{F}_i$ aller möglichen Gitter $F(L^{\#})$ in $U_i^{\#}/U_i$ mit Minimum $\geq \frac{\min(L)}{p}$ und definiere $\mathcal{F} = \cup_{i=1}^{k} \mathcal{F}_i$.*

3) *Sei $d_{min} := \min\{\det(F) \mid F \in \mathcal{F}\}$ und sei Π ein Vertretersystem der Isomorphieklassen aller $F^{\#}$, $F \in \mathcal{F}$, mit $\det(F) \leq \frac{p^{2s-f}}{d_{min}}$.*

4) *Für alle $\pi_F(L) \in \Pi$ sei $X_F(L) := \pi_F(L) \cap \pi_F(L)^{\#}$ und bestimme alle möglichen geraden Gitter $F(L)$ mit $\min(F(L)) \geq \min(L)$ in $X_F(L)/pX_F(L)^{\#}$ vom Index p^{s-a}, wobei p^a der Index $[\pi_F(L) : X_F(L)]$ ist.*

5) *Gebe alle möglichen Paare $(\pi_F(L), F(L))$ aus.*

Beweis. Bis Schritt 2) berechnet der Algorithmus sowohl alle $F(L^{\#})$ also auch alle ${}^{(1/p)}F(L)$, d.h. es gilt $F(L^{\#}), {}^{(1/p)}F(L) \in \mathcal{F}$. Aus

$$\det(F(L^{\#})) \cdot \det({}^{(1/p)}F(L))) = p^{2s-f}$$

folgt die Einschränkung $\det(F) \leq \frac{p^{2s-f}}{d_{\min}}$ in Schritt 4. □

Berechnung der $(\pi_Z(L), Z(L))$

Alle Definitionen und Ergebnisse des vorhergehenden Abschnittes übertragen sich direkt auf den Fall $(\pi_Z(L), Z(L))$, indem F durch Z bzw. f durch $(p-1)z$ ersetzt wird. Insbesondere folgt also wie in Bemerkung 6.30

$$\det(Z(L)) \cdot \det({}^{(p)}Z(L^{\#})) = p^{2s+(p-1)z}.$$

Folgerung 6.32. *Indem man eventuell L durch ${}^{(p)}L^{\#}$ ersetzt, gilt ohne Einschränkung*

$$\det(F(L)) \leq p^{s+f/2} \text{ oder } \det(Z(L)) \leq p^{s+(p-1)z/2}.$$

Durch den Übergang zu dem eindeutigem quadratischem Teilkörper von $\mathbb{Q}(\zeta_p)$ lassen sich im zyklotomischem Fall Teilgitter definieren, die für die Klassifikation der Paare $(\pi_Z(L), Z(L))$ hilfreich sind.

Definition 6.33. *Sei*

$$\delta = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \zeta_p^i$$

die quadratische Gausssumme modulo p. Es gilt $\delta^2 = (-1)^{\frac{p-1}{2}} p$, d.h. δ erzeugt den quadratischen Teilkörper $\mathbb{Q}(\sqrt{\pm p})$ von $\mathbb{Q}(\zeta_p)$. Sei damit

$$\hat{X}_Z(L) := X_Z(L) + X_Z(L)^* = X_Z(L) + X_Z(L)^{\#} \cdot \delta$$

Satz 6.34. *Das Gitter $\hat{X}_Z(L)$ ist ganz und in $Z(L^{\#})$ enthalten.*

Beweis. Es gilt

$$\hat{X}_Z(L) = X_Z(L) + X_Z(L)^{\#} \cdot \delta = (\pi_Z(L) \cap Z(L^{\#})) + \pi_Z(L) \cdot \delta + Z(L^{\#}) \cdot \delta$$

und

$$\hat{X}_Z(L)^{\#} = X_Z(L)^{\#} \cap X_Z(L) \cdot \tfrac{1}{\delta} = (\pi_Z(L) + Z(L^{\#})) \cap \left(\pi_Z(L) \cdot \tfrac{1}{\delta} + Z(L^{\#}) \cdot \tfrac{1}{\delta}\right).$$

Dann ist $\hat{X}_Z(L)$ ein ganzes Gitter, denn es gilt $X_Z(L) \subseteq X_Z(L)^{\#}$, $X_Z(L) \subseteq X_Z(L) \cdot \frac{1}{\delta}$ und $X_Z(L)^{\#} \cdot \delta \subseteq X_Z(L)^{\#}$, zusätzlich ist $X_Z(L)^{\#} \cdot \delta \subseteq X_Z(L) \cdot \frac{1}{\delta}$ äquivalent zu $X_Z(L)^{\#} \subseteq X_Z(L) \cdot \frac{1}{\delta^2} = \frac{1}{p} X_Z(L)$, was erfüllt ist, da $X_Z(L)$ p-elementar ist. Die Projektion $\pi_Z(L)$ ist in $\hat{X}_Z(L)^{\#}$ enthalten, also ist $Z(L^{\#})$ ein Obergitter von $\hat{X}_Z(L)$. □

Lemma 6.35. *Es existiert ein hermitesch unimodulares $\mathbb{Z}[\delta]$-Gitter U mit*

$$\hat{X}_Z(L)^* \subseteq U = U^* \subseteq \hat{X}_Z(L).$$

Beweis. Das Gitter $\hat{X}_Z(L)^*$ ist hermitesch ganzzahlig, also kann U so gewählt werden, dass es an jeder Stelle $\neq p$ mit $\hat{X}_Z(L)$ übereinstimmt, und an der Stelle p ein unimodulares $\mathbb{Z}[\delta]_p$-Obergitter von $\hat{X}_Z(L)_p$ ist. □

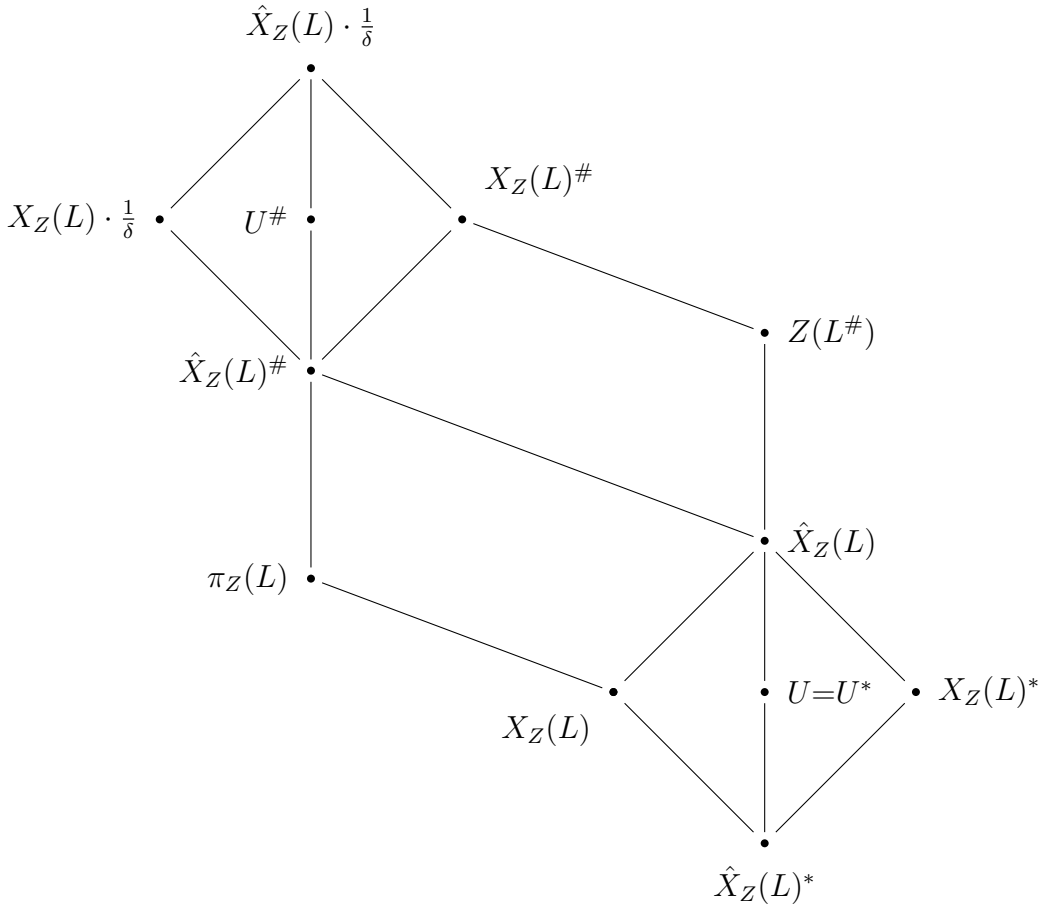


ABBILDUNG 6.2: Verband der definierten Gitter

Bemerkung 6.36. *Die Aussagen gelten analog für* $\hat{Y}_Z(L) = Y_Z(L) + Y_Z(L)^{\#} \cdot \delta$. *In diesem Fall ist* $\hat{Y}_Z(L) \subseteq \frac{1}{p} Z(L)$ *und außerdem* ${}^{(p)}\hat{Y}_Z(L) \cdot \delta \subseteq {}^{(p)}\hat{Y}_Z(L) \subseteq {}^{(p)}\hat{Y}_Z(L)^{\#}$.

Ausgehend von einem hermitesch unimodularen $\mathbb{Z}[\delta]$-Gitter können also erst alle ganzen Obergitter $\hat{X}_Z(L)$ bestimmt werden, mit diesen können dann die möglichen Paare $(\pi_Z(L), Z(L))$ konstruiert werden. In geeigneten Fällen lassen sich auch direkt die hermiteschen Geschlechter der Gitter $X_Z(L)$ bestimmen.

Algorithmus 6.37. Eingabe: *Der Typ $p-(f,z)-s$ eines Automorphismus eines p-modularen, extremalen Gitters L.*
Ausgabe: *Repräsentanten der möglichen Paare $(\pi_Z(L), Z(L))$.*
Algorithmus:

1) *Bestimme Vertreter $U_1, \ldots, U_k$ der Isomorphieklassen hermitesch unimodularer $\mathbb{Z}[\delta]$-Gitter vom Rang z.*

2) *Bestimme die Menge $\hat{\mathcal{X}}_i$ der ganzen Gitter $\hat{X}_Z(L)$ in $U_i^\#/U_i$ und definiere $\hat{\mathcal{X}} = \cup_{i=1}^k \hat{\mathcal{X}}_i$.*

3) *Bestimme für alle $\hat{X} \in \hat{\mathcal{X}}$ die Menge $\mathcal{Z}_X$ der Gitter $Z(L^\#)$ in $\hat{X} \cdot \frac{1}{\delta}/\hat{X}$ mit Minimum $\geq \frac{\min(L)}{p}$ und definiere $\mathcal{Z} := \cup_{X \in \mathcal{X}} \mathcal{Z}_X$.*

4) *Sei $d_{min} = \min\{\det(Z) \mid Z \in \mathcal{Z}\}$ und sei Π ein Vertretersystem der Isomorphieklassen aller $Z^\#, Z \in \mathcal{Z}$ mit $\det(Z) \leq \frac{p^{2s-(p-1)z}}{d_{min}}$.*

5) *Für alle $\pi_Z(L) \in \Pi$ bestimme alle $Z(L)$ in $X_Z(L)/\pi_Z(L) \cdot (1-\zeta_p)$ vom Index p^{s-a}, wobei p^a der Index $[\pi_Z(L) : X_F(L)]$ ist.*

6) *Gebe alle möglichen Paare $(\pi_Z(L), Z(L))$ aus.*

Beweis. Bis Schritt 3) berechnet der Algorithmus sowohl alle $Z(L^\#)$ als auch alle ${}^{(1/p)}Z(L)$, d.h. es gilt $Z(L^\#), {}^{(1/p)}Z(L) \in \mathcal{Z}$. Aus

$$\det(Z(L^\#) \cdot \det({}^{(1/p)}Z(L)) = p^{2s-(p-1)z} \leq 1$$

folgt die Einschränkung $\det(Z) \leq \frac{p^{2s-(p-1)z}}{d_{\min}}$ in Schritt 5. □

Konstruktion von L durch Verklebung

Seien $(\pi_F(L), F(L))$ und $(\pi_Z(L), Z(L))$ zwei mögliche Paare von Gittern, die mit Algorithmus 6.31 bzw. 6.37 berechnet wurden. Ein zugehöriges (extremales) p-modulares Gitter L ist nun gegeben durch eine Antiisometrie der beiden quadratischen Räume

$$(\pi_F(L)/F(L), q_F) \text{ und } (\pi_Z(L)/Z(L), q_Z),$$

d.h. es gilt

$$L = \{(v, \varphi(v)) \in \pi_F(L) \perp \pi_Z(L)\}$$

für einen $\mathbb{F}_p$-Vektorraumisomorphismus

$$\varphi : \pi_F(L)/F(L) \to \pi_Z(L)/Z(L)$$

mit

$$q_F(v) \equiv -q_Z(\varphi(v)) \pmod{\mathbb{Z}} \text{ für alle } v \in \pi_F(L).$$

Bemerkung 6.38. *Die Gitter $X_F(L)$ und $X_Z(L)$ definieren maximal total isotrope Teilräume in $(\pi_F(L)/F(L), q_F)$ bzw. $(\pi_Z(L)/Z(L), q_Z)$. Insbesondere müssen also die Indizes $[\pi_F(L) : X_F(L)]$ und $[\pi_Z(L) : X_Z(L)]$ gleich sein, damit ein solcher Isomorphismus φ existieren kann.*

Sei

$$X(L) := L(L) + (X_F(L) \perp X_Z(L)),$$

dann ist $X(L)$ das maximale, gerade Obergitter von L, so dass

$$\pi_F(L) \perp \pi_Z(L) = \pi_F(X(L)) \perp \pi_Z(X(L))$$

gilt.

Lemma 6.39. *Es gilt $F(X(L)) = X_F(L)$ und $Z(X(L)) = X_Z(L)$.*

Beweis. Sei $l + f + z \in X(L)$, mit $l \in L$, $f \in X_F(L)$ und $z \in X_Z(L)$. Zuerst wird die Aussage für $F(X(L))$ gezeigt. Es gilt $F(X(L)) = \mathrm{Kern}(\pi_Z|_{X(L)})$, also muss gezeigt werden, dass $l + f + z$ in $X_F(L)$ liegt, genau dann wenn $l + f + z$ in $\mathrm{Kern}(\pi_Z|_X)$ enthalten ist. Die Hinrichtung ist klar, da $\pi_Z \circ \pi_F = 0$. Sei also $l + f + z \in \mathrm{Kern}(\pi_Z|_X)$. Es gilt $\pi_Z(l + f + z) = \pi_Z(l) + z$, also folgt $\pi_Z(l) = -z \in X_Z(L)$. Aus $l = \pi_F(l) + \pi_Z(l) = \pi_F(l) - z$ folgt dann $l + f + z = \pi_F(l) + f$. Da l und $\pi_Z(l) = -z$ in $L^\#$ enthalten sind, gilt dies auch für $\pi_F(l)$, insgesamt folgt damit $\pi_F(l) + f \in X_F(L)$. Der Beweis für $Z(X(L))$ verläuft analog. □

Sei

$$N(L) := L \cap (F(X(L)) \perp Z(X(L))) = L \cap (X_F(L) \perp X_Z(L)),$$

dann gilt

$$N(L) = \{(v, \varphi_{|X_F(L) \perp X_Z(L)}(v) \in X_F(L) \perp X_Z(L)\},$$

wobei φ die Antiisometrie ist, die L definiert. Insbesondere ist also $N(L)$ das volle, subdirekte Produkt von $X_F(L)$ und $X_Z(L)$.
Sei a die Dimension von $X_F(L)$ bzw. $X_Z(L)$ in $\pi_F(L)/Z(L)$ bzw. $\pi_Z(L)/Z(L)$. Dann existiert eine Basis $\mathcal{B} = (b_1, \ldots, b_s)$ von $\pi_F(L)/F(L)$, so dass $(b_1, \ldots, b_a)$ eine Basis von $X_F(L)$ in $\pi_F(L)/F(L)$ ist. Die Gram-Matrix bzgl. $\mathcal{B}$ hat dann die Form

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \text{ mit } A \in \mathbb{Z}^{a \times a},\ B \in \mathbb{Z}^{a \times (s-a)},\ C \in \mathbb{Z}^{(s-a) \times a} \text{ und } D \in (\mathbb{Z}/\tfrac{1}{p}\mathbb{Z})^{(s-a) \times (s-a)}.$$

Für eine solche fest gewählte Basis $\mathcal{B}$ sind dann alle möglichen Verklebungen gegeben durch Basen $\mathcal{C} = (c_1, \ldots, c_s)$ von $\pi_Z(L)/Z(L)$, so dass die zugehörige Gram-Matrix äquivalent ist zu $-\begin{pmatrix} A & B \\ C & D \end{pmatrix} \pmod{\mathbb{Z}}$. Die Vektoren $(b_1, c_1), \ldots, (b_a, c_a)$ definieren dann das Teilgitter $N(L)$.

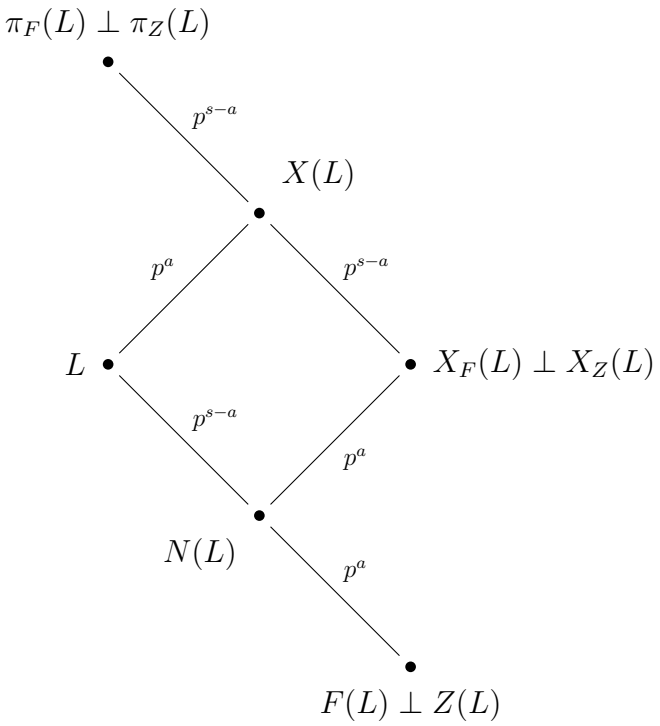


ABBILDUNG 6.3: Verband der definierten Ober- und Teilgitter $X(L)$ und $N(L)$ von L.

Bemerkung 6.40. *Nach dem Satz von Witt operiert (für $p > 2$) die Isometriegruppe von $(\pi_F(L)/F(L), q_F)$ bzw. $(\pi_Z(L)/Z(L), q_Z)$ transitiv auf der Menge der maximal total isotropen Teilräume, damit liegt $N(L)$ charakteristisch in L. Insbesondere kann also erst durch die möglichen Verklebungen $(b_1, c_1), \ldots, (b_a, c_a)$ die Menge aller $N(L)$ bestimmt werden, diese werden dann auf Isomorphie getestet und Vertreter der Isomorphieklassen werden dann weiter zu (extremalen) Gittern L geliftet. Die Isomorphismen müssen hierbei die (hermitesche) Struktur des Raumes $V_1 \perp V_\zeta$ fixieren.*

Der Typ $p - (s, s) - s$

In [Neb19a] werden p-modulare Gitter mit einem Automorphismus σ der Ordnung p untersucht, die als $\mathbb{Z}_p[\sigma]$-Gitter frei sind, d.h. der Typ von (L, σ) ist $p - (s, s) - s$. Die Strukturergebnisse werden in diesem Abschnitt angegeben.

Satz 6.41. *Sei $R := \mathbb{Z}_p[\sigma]$ und $M \cong R^s$ ein freies R-Gitter vom Rang s. Für ein ein freies R-Gitter N mit $pM \subseteq N \subseteq M$ existiert eine R-Basis $(g_1, \ldots, g_s)$ von M und ein $0 \leq k \leq s$, so dass*

$$N = Rg_1 \oplus \cdots \oplus Rg_k \oplus pRg_{k+1} \oplus \cdots \oplus pRg_s$$

gilt.

Satz 6.42. *Sei $p > 2$ ein Primzahl und sei L ein p-modulares Gitter mit einem Automorphismus σ des Typs $p-(s,s)-s$. Dann ist $s = 2t$ gerade und es gilt $F(L)^\#/F(L) \cong (\mathbb{Z}/p\mathbb{Z})^t \oplus (\mathbb{Z}/p^2\mathbb{Z})^t$ und $Z(L)^\#/Z(L) \cong (\mathbb{Z}/p\mathbb{Z})^{(p-1)t} \oplus (\mathbb{Z}/p^2\mathbb{Z})^t$.*

Folgerung 6.43. *Mit den Voraussetzungen von Satz 6.42 gilt $Z(L^\#) = Z(L)^\# \cdot (1-\sigma)$ und*

$$F(L) \subseteq F(L^\#) = p\pi_F(L^\#) = pF(L)^\# \subseteq \tfrac{1}{p}F(L) \subseteq F(L)^\#,$$

wobei der Index jeweils p^t ist. Insbesondere ist ${}^{(1/p)}F(L)$ ein gerades, p-elementares Gitter mit Determinante p^t und Dimension $s = 2t$. Nach [CS99, Kapitel 15, Theorem 13] ist das Geschlecht von $F(L)$ also eindeutig bestimmt.

Satz 6.44. *Im Spezialfall $p = 3$ sei L ein 3-modulares Gitter mit einem Automorphismus σ vom Typs $3-(s,s)-s$. Dann ist $\pi_Z(L) \cap Z(L^\#) =: Y$ ein hermitesch selbst-duales $\mathbb{Z}[\zeta_3]$-Gitter mit*

$$Z(L) \subseteq Y = Y^* \subseteq Z(L^*) = Z(L^\#).$$

Das Geschlecht des hermiteschen $\mathbb{Z}[\zeta_3]$-Gitters $Z(L)$ ist eindeutig durch s bestimmt.

6.5 Extremale, 3-modulare Gitter der Dimension 24

In Dimension 24 ist bisher ein einziges extremales, 3-modulares Gitter bekannt ([Neb98]), sei L_{24} dieses Gitter[1]. Es ist eindeutig mit einem Automorphismus von Prim-Ordnung ≥ 5 ([Jür15, Abschnitt 4.2.5]). Im folgenden werden die entwickelten Methoden benutzt, um den folgenden Satz zu zeigen:

Satz 6.45. *Sei L ein 3-modulares, extremales Gitter der Dimension 24 mit einem Automorphismus der Ordnung 3. Dann ist L isomorph zu L_{24}.*

Sei also L ein 24-dimensionales, 3-modulares, extremales Gitter und sei $\sigma \in \mathrm{Aut}(L)$ ein Automorphismus der Ordnung 3. Indem man eventuell L durch ${}^{(p)}L^\#$ ersetzt, gilt nach Bemerkung 6.30

$$\det(F(L)) \leq 3^{f/2+s} \text{ oder } \det(Z(L)) \leq 3^{z+s}.$$

Da diese beiden Gitter Minimum ≥ 6 haben, sind mit der Cohn-Elkies-Schranke ([CE03]) nur die folgenden Typen möglich:

f	z	s
0	12	0
2	11	2
4	10	4
6	9	$4,5,6$
8	8	$4,5,6,7,8$
10	7	$4,5,6,7$
12	6	$4,5,6$
14	5	$4,5$
16	4	4

[1] Der offizielle Name des Gitters ist eigentlich $\left(\frac{5+\sqrt{13}}{2}\right)L_{24.2}$

Die Automorphismengruppe des bereits bekannten Gitter L_{24} ist von Ordnung $2^5 \cdot 3^2 \cdot 7 \cdot 13$ mit 5 Konjugiertenklassen mit Elementen der Ordnung 3. Zwei davon haben den Typ $3-(0,12)-0$ (insbesondere ist hier L_{24} ein hermitesches Gitter über $\mathbb{Z}[\zeta_3]$, es kann aber nach [Fei78] nicht hermitesch unimodular sein), die anderen drei haben den Typ $3-(8,8)-8$.

Der Fall $f = 16$:

Das Geschlecht der unimodularen $\mathbb{Z}[\zeta_3]$-Gitter vom Rang 4 ist nach [Fei78] einklassig, damit ist das Spurgitter von U gleich A_2^4. Dieses Gitter hat drei ganze Obergitter mit Minimum 2, aus diesen lassen sich insgesamt sieben mögliche Gitter $F(L^\#)$ konstruieren, die vier Isomorphieklassen bilden. Die Determinanten dieser Gitter sind

$$1, 3^2, 3^2 \text{ und } 3^4.$$

Da diese Gitter Kandidaten für $Z(L^\#)$ und ${}^{(1/p)}Z(L)$ sind, folgt aus

$$\det(Z(L^\#)) \cdot \det({}^{(1/p)}Z(L)) = 3^{2s-(p-1)z} = 1,$$

dass $Z(L^\#)$ eindeutig ist. Die einzige Möglichkeit für das Paar $(\pi_Z(L), Z(L))$ ist dann $(E_8, {}^{(3)}E_8)$, insbesondere ist also $\pi_Z(L)$ ein ganzes Gitter und $\pi_F(L)$ muss ein ganzes Gitter mit Minimum ≥ 4 sein. Zusätzlich enthält es ein Gitter, welches im Geschlecht der 3-modularen Gitter der Dimension 16 liegt, davon gibt es sechs mit Minimum ≥ 4 (alle 3-modular und extremal), diese haben aber kein Obergitter mit Minimum 4. Dann ist aber $\pi_F(L)$ ein 3-modulares, extremales Gitter und $F(L^\#) = \pi_F(L)^\#$ hat Minimum $\frac{4}{3}$, ein Widerspruch.

Der Fall $f = 14$:

Es gibt ein unimodulares $\mathbb{Z}[\zeta_3]$-Gitter vom Rang 5 ([Fei78]), dieses hat drei mögliche Obergitter $\hat{X}_Z(L)$. Diese wiederum haben insgesamt sieben Isomorphieklassen von möglichen Gittern $Z(L^\#)$ als Obergitter, die Determinanten sind

$$3, 3^3 \text{ und } 3^5.$$

Dann gilt aber $\det(Z(L^\#)) \cdot \det({}^{(1/p)}Z(L)) > 1$.

Der Fall $f = 12$:

Es gibt zwei unimodulare $\mathbb{Z}[\zeta_3]$-Gitter vom Rang 6, dieses haben neun mögliche Obergitter $\hat{X}_Z(L)$. Diese wiederum haben insgesamt 20 Isomorphieklassen von möglichen Gittern $Z(L^\#)$ als Obergitter, die Determinanten sind

$$1, 3^2, 3^4 \text{ und } 3^6.$$

Also muss die Determinante bereits 1 sein und $s = 6$. Da $Z(L)$ in $\pi_Z(L) \cdot (1-\sigma) = {}^{(3)}\pi_Z(L)$ enthalten ist, muss das Minimum von $\pi_Z(L)$ mindestens 2 sein, davon

gibt es drei Stück und da $z = s$ gilt, ist $Z(L)$ bereits eindeutig dadurch bestimmt. Die minimalen Normen der Restklassen $\pi_Z(L)/Z(L)$ sind

$$(0, 2^{48}, \tfrac{8}{3}^{486}, 4^{194}),\ (0, 2^{66}, \tfrac{8}{3}^{324}, \tfrac{10}{3}^{162}, 4^{176}) \text{ und } (0, 2^{84}, \tfrac{8}{3}^{162}, \tfrac{10}{3}^{324}, 4^{158}).$$

Insbesondere muss das Minimum von $\pi_F(L)$ mindestens 2 sein. Davon gibt es bis auf Isomorphie dreu Stück. Diese haben alle Determinante 1, für zwei hat $X_F(L)$ Index 3^3 in $\pi_F(L)$, für das dritte ist der Index 3. Für das Gitter $\pi_F(L)$ mit Index 3 gilt allerdings, dass alle Restklassen in $\pi_F(L)/3X_F(L)^\#$ die Normen $0, \frac{2}{3} \pmod{\mathbb{Z}}$ haben, diese können alo nicht mit den möglichen $(\pi_Z(L), Z(L))$ verklebt werden. Für die anderen beiden $\pi_F(L)$ lassen sich die Fixgitter $F(L)$ ausrechnen, insgesamt gibt es 2504 Möglichkeiten für $(\pi_F(L), F(L))$. Diese können nicht mit der ersten Möglichkeit für $(\pi_Z(L), Z(L))$ verklebt werden, alle anderen Verklebungen liefern kein extremales, 3-modulares Gitter.

Der Fall $f = 10$:

Es gibt zwei unimodulares $\mathbb{Z}[\zeta_3]$-Gitter vom Rang 7, dieses haben 22 mögliche Obergitter $\hat{X}_Z(L)$. Diese wiederum haben insgesamt 67 Isomorphieklassen von möglichen Gittern $Z(L^\#)$ als Obergitter, die Determinanten sind

$$3^{-1}, 3, 3^3, 3^5 \text{ und } 3^7.$$

Aus

$$\det(Z(L^\#)) \cdot \det({}^{(1/3)}Z(L)) = 3^{2s-14} = \begin{cases} 1 & s = 7 \\ 3^{-2} & s = 6 \\ 3^{-4} & s = 6 \\ 3^{-6} & s = 6 \end{cases}$$

folgt, dass die möglichen Determinanten im Fall $s = 7$ 3^{-1} und 3 sind, im Fall $s = 6$ 3^{-1} und für $s = 5$ und $s = 4$ existieren keine passenden Gitter.
Sei zuerst $s = 7$. Dann existieren 13 mögliche Paare $(\pi_Z(L), Z(L))$, so dass $\pi_Z(L)$ das Minimum ≥ 2 hat, und 257 mögliche Paare $(\pi_F(L), F(L))$. Da L den Index 3^s in $\pi_F(L) \perp \pi_Z(L)$ hat, gilt im Fall $s = 7$, dass $\det(\pi_F(L)) \cdot \det(\pi_Z(L)) = 3^{-2}$ ist. Zusätzlich muss der Index von $X_F(L)$ bzw. $X_Z(L)$ in $\pi_F(L)$ bzw. $\pi_Z(L)$ gleich sein.

Anzahl	Normen	$\det(\pi_Z(L))$	$[\pi_Z(L) : X_Z(L)]$
1	$\left(0, 2, \frac{8}{3}, \frac{10}{3}, 4\right)$	3^{-1}	3^2
1	$\left(0, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}\right)$	3^{-1}	3^3
2	$\left(0, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}\right)$	3^{-1}	3^4
1	$\left(0, 2, \frac{10}{3}, 4, 6\right)$	3	3
1	$\left(0, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}, 6\right)$	3	3^2
1	$\left(0, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}, \frac{16}{3}\right)$	3	3^3
1	$\left(0, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}\right)$	3	3^3
2	$\left(0, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}, 6\right)$	3	3^3
2	$\left(0, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}, \frac{16}{3}\right)$	3	3^4
1	$\left(0, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}, \frac{16}{3}, 6\right)$	3	3^4

Anzahl	Normen	$\det(\pi_F(L))$	$[\pi_F(L) : X_F(L)]$
7	$\left(0, \frac{2}{3}, 2, \frac{8}{3}, 4, \frac{14}{3}, 6, \frac{20}{3}, 8\right)$	3^{-1}	3
10	$\left(0, \frac{2}{3}, 2, \frac{8}{3}, 4, \frac{14}{3}, 6, \frac{20}{3}\right)$	3^{-1}	3
75	$\left(0, \frac{2}{3}, 2, \frac{8}{3}, 4, \frac{14}{3}, 6\right)$	3^{-1}	3
24	$\left(0, \frac{2}{3}, 2, \frac{8}{3}, 4, \frac{14}{3}\right)$	3^{-1}	3
8	$\left(0, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}, \frac{16}{3}, 6\right)$	3^{-1}	3^2
4	$\left(0, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{16}{3}, 6\right)$	3^{-1}	3^2
13	$\left(0, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}, 6\right)$	3^{-1}	3^2
2	$\left(0, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{16}{3}\right)$	3^{-1}	3^2
1	$\left(0, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{16}{3}, 6, 8\right)$	3^{-1}	3^2
4	$\left(0, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}, \frac{16}{3}, 6, 8\right)$	3^{-1}	3^2
3	$\left(0, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}, \frac{16}{3}, 6, 8\right)$	3^{-1}	3^3
1	$\left(0, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{16}{3}, 6\right)$	3^{-1}	3^3
2	$\left(0, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}, \frac{16}{3}, 6\right)$	3^{-1}	3^3
70	$\left(0, \frac{2}{3}, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}\right)$	3^{-3}	3^3
3	$\left(0, \frac{2}{3}, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4\right)$	3^{-3}	3^3
5	$\left(0, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4\right)$	3^{-3}	3^4
1	$\left(0, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}\right)$	3^{-3}	3^4
22	$\left(0, \frac{2}{3}, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}\right)$	3^{-3}	3^4
2	$\left(0, \frac{2}{3}, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4\right)$	3^{-3}	3^4

Dadurch fallen aber bereits die meisten Möglichkeiten weg, so gibt es z.B. 116 Paare $(\pi_F(L), F(L))$ mit $\det(\pi_Z(L)) = 3^{-1}$ und $[\pi_F(L) : X_F(L)] = 3$, aber kein passendes Paar $(\pi_Z(L), Z(L))$. Insgesamt sind nur 169 Verklebungen möglich, diese liefern kein extremales Gitter.
Sei nun $s = 6$. Dann gibt es (bis auf Isomorphie) neun mögliche Gitter $\pi_Z(L)$ mit acht möglichen Paaren $(\pi_Z(L), Z(L))$. Für die Fixgitter gibt es 218 mögliche Paare $(\pi_F(L), F(L))$. In den folgenden zwei Tabellen sind für alle $\pi_Z(L)$ bzw. $\pi_F(L)$ die minimalen Normen in den Restklassen (ohne Vielfachheit), die Determinante und der Index von $X_Z(L)$ bzw. $X_F(L)$ angegeben.

Anzahl	Normen	$\det(\pi_Z(L))$	$[\pi_Z(L) : X_Z(L)]$
1	$\left(0, 2, \frac{10}{3}, 4\right)$	3	3
2	$\left(0, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}\right)$	3	3^2
4	$\left(0, 2, \frac{8}{3}, \frac{10}{3}, 4\right)$	3	3^3
1	$\left(0, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}\right)$	3	3^4

Anzahl	Normen	$\det(\pi_F(L))$	$[\pi_F(L) : X_F(L)]$
115	$\left(0, \frac{2}{3}, 2, \frac{8}{3}, 4, \frac{14}{3}\right)$	3^{-1}	3
14	$\left(0, \frac{2}{3}, 2, \frac{8}{3}, 4\right)$	3^{-1}	3
6	$\left(0, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}\right)$	3^{-1}	3^2
56	$\left(0, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4\right)$	3^{-1}	3^2
4	$\left(0, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4, \frac{14}{3}\right)$	3^{-1}	3^3
23	$\left(0, \frac{4}{3}, 2, \frac{8}{3}, \frac{10}{3}, 4\right)$	3^{-1}	3^3

Daraus folgt, dass nur die 62 Paare mit $[\pi_F(L) : X_F(L)] = 3^2$ in Betracht kommen, diese können aber nicht zu einem extremalen Gitter verklebt werden.

Der Fall $f = 8$:

Sei zuerst $s = 8$. Dies ist neben dem hermiteschen Fall der einzige Typ von Automorphismen der Ordnung 3, die beim Gitter L_{24} vorkommen. Nach Folgerung 6.43 und Satz 6.44 liegen die Gitter $F(L)$ bzw. $Z(L)$ im (hermiteschen) Geschlecht der Gitter $F(L_{24})$ bzw. $Z(L_{24})$. Das Geschlecht von $F(L_{24})$ besteht aus zwei Gittern, beide haben Minimum 6. Das hermitesche Geschlecht von $Z(L_{24})$ besteht aus 103 Gittern, bei diesen muss das Spurgitter Minimum 6 und das Spurgitter des hermitesch Dualen Minimum 2 haben. Dies erfüllen neun Gitter. Für die Projektionen gilt

$$\pi_F(L) = \tfrac{1}{3}F(L) \text{ und } \pi_Z(L) = Z(L) \cdot (1 - \sigma)^{-1},$$

die Radikale $X_F(L)$ bzw. $X_Z(L)$ bilden jeweils 4-dimensionale Teilräume in $\pi_F(L)/F(L)$ bzw. $\pi_Z(L)/Z(L)$. Für beide Möglichkeiten von $F(L)$ existiert eine Basis $(\overline{b_1}, \ldots, \overline{b_8})$ von $\pi_F(L)/F(L)$, so dass die Gram-Matrix die Form

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \text{ mit } A, B, C \in \mathbb{Z}^{4\times 4} \text{ und } \operatorname{diag}(D) = \left(\frac{2}{3}, \frac{2}{3}, \frac{2}{3}, \frac{2}{3}\right)$$

hat. Für 12 der 18 möglichen Kombinationen für $(F(L), Z(L))$ existieren keine $c_5, \ldots, c_8 \in \pi_Z(L)$, so dass das Teilgitter

$$\langle F(L) \perp Z(L), (b_5, \ldots, c_5), \ldots, (b_8, c_8)\rangle \leq L$$

von L Minimum ≥ 6 hat. Für die restlichen sechs Kombinationen werden zuerst alle Verklebungen

$$N(L) = \langle F(L) \perp Z(L), (b_1, c_1), \ldots, (b_4, c_4)\rangle \text{ mit } c_1, \ldots, c_4 \in X_Z(L)$$

bestimmt und in Isomorphieklassen eingeteilt. Zusammen mit den Konjugiertenklassen von passenden Automorphismen (d.h. der Typ ist $3-(8,8)$ und die Elementarteiler von $F(N(L))$ bzw $Z(N(L))$ sind $3^4 9^4$ bzw. $3^8 9^4$) werden diese weiter zu extremalen Gitter L geliftet. Alle so konstruierten Gitter sind isomorph zum Gitter L_{24}.

Betrachte nun also die Fälle mit $s < 8$. Es gibt drei unimodulares $\mathbb{Z}[\zeta_3]$-Gitter vom Rang 8, dieses haben 72 mögliche Obergitter $\hat{X}_Z(L)$. Sei $s = 7$, dann existieren neun Möglichkeiten für $(\pi_F(L), F(L))$. Da L den Index 3^s in $\pi_F(L) \perp \pi_Z(L)$ hat, lassen sich daraus die Möglichkeiten für die Determinanten von $\pi_Z(L)$ berechnen, diese sind in der folgenden Tabelle angegeben:

$\det(\pi_F(L))$	$\det(F(L))$	$\det(X_F(L))$	$\det(\pi_Z(L))$	$\det(X_Z(L))$	$\det(Z(L^\#))$
3^{-4}	3^{10}	3^4	3^2	3^{10}	3^{-2}
3^{-2}	3^{12}	3^2	1	3^4	1
3^{-2}	3^{12}	3^4	1	3^6	1
1	3^{14}	1	3^{-2}	3^{-2}	3^2

Im Fall $\det(Z(L^\#)) = 3^2$ ist $X_Z(L)$ kein ganzes Gitter, also muss die Determinante von $Z(L^\#)$ 1 oder 3^{-2} sein. Im Fall $\det(Z(L^\#)) = 3^{-2}$ existieren bis auf Isomorphie 36 Gitter $\pi_Z(L)$, welche 320 Paare $(\pi_Z(L), Z(L))$ liefern. Im Fall $\det(Z(L^\#)) = 1$ existieren bis auf Isomorphie 57 Gitter $\pi_Z(L)$, welche 75 Paare $(\pi_Z(L), Z(L))$ liefern.
Im Fall $s = 6$ existieren 13 Möglichkeiten für $(\pi_F(L), F(L))$, die Determinanten sind hier

$\det(\pi_F(L))$	$\det(F(L))$	$\det(X_F(L))$	$\det(\pi_Z(L))$	$\det(X_Z(L))$	$\det(Z(L^\#))$
3^{-4}	3^8	3^4	3^4	3^{12}	3^{-4}
3^{-2}	3^{10}	3^2	3^2	3^6	3^{-2}
3^{-2}	3^{10}	3^4	3^2	3^8	3^{-2}
1	3^{12}	1	1	1	1

Kein $\hat{X}_Z(L)$ hat ein Obergitter der Determinante 3^{-4} und Minimum ≥ 2, im Fall $\det(Z(L^\#)) = 1$ existieren 57 Gitter $\pi_Z(L)$, diese enthalten allerdings kein gerades Teilgitter vom Index 3^6 mit Minimum ≥ 6. Im Fall $\det(Z(L^\#)) = 3^{-2}$ existieren 33 mögliche $\pi_Z(L)$ und 348 Paare $(\pi_Z(L), Z(L))$. In allen Fällen liefern die Verklebungen kein extremales Gitter.
Im Fall $s = 4$ bzw. $s = 5$ gilt

$$\det(Z(L^\#)) \cdot \det({}^{(1/3)}Z(L)) = \begin{cases} 3^{-6} & s = 5 \\ 3^{-8} & s = 4. \end{cases}$$

Allerdings wurde bereits gezeigt dass die kleinstmögliche Determinante von $Z(L^\#)$ bzw. ${}^{(1/3)}Z(L)$ 3^{-2} ist, diese Fälle sind also nicht möglich.

Der Fall $f = 6$:

Sei zuerst $s = 6$. Es gibt zwei Möglichkeiten für $(\pi_F(L), F(L))$:

$\det(\pi_F(L))$	$\det(F(L))$	$\det(X_F(L))$	$\det(\pi_Z(L))$	$\det(X_Z(L))$	$\det(Z(L^\#))$
3^{-3}	3^9	3^3	3^3	3^9	3^{-3}
3^{-1}	3^{11}	3	3	3^3	3^{-1}

Das Gitter $X_Z(L)$ ist 3-elementar und ist als $\mathbb{Z}[\zeta_3]_3$-Gitter im Fall $\det(X_Z(L)) = 3^9$ isomorph zu

$$(1)^9,$$
$$\mathbb{H}(1) \perp \mathbb{H}(-1) \perp (1)^5 \text{ oder}$$
$$\mathbb{H}(1) \perp \mathbb{H}(1) \perp \mathbb{H}(-1) \perp \mathbb{H}(-1) \perp (1).$$

bzw. im Fall $\det(X_Z(L)) = 3^3$ isomorph zu

$$\mathbb{H}(-1) \perp \mathbb{H}(-1) \perp \mathbb{H}(-1) \perp (1) \perp (1) \perp (1).$$

Die Maße der Geschlechter sind

$\det(X_Z(L)) = 3^9$	$\det(X_Z(L)) = 3^3$
$3.09 \cdot 10^{-10}$	$2.53 \cdot 10^{-7}$
0.0002	
0.015	

Die hermiteschen Geschlechter liefern $85 + 6$ mögliche $X_Z(L)$, aus welchen sich $1512 + 63$ Paare $(\pi_Z(L), Z(L))$ konstruieren lassen. Keine Verklebung liefert ein extremales Gitter.

Der Fall $s = 5$ funktioniert ähnlich. Es gibt zwei Paare $(\pi_F(L), F(L))$:

$\det(\pi_F(L))$	$\det(F(L))$	$\det(X_F(L))$	$\det(\pi_Z(L))$	$\det(X_Z(L))$	$\det(Z(L^\#))$
3^{-3}	3^7	3^3	3^5	3^{11}	3^{-5}
3^{-1}	3^9	3	3^3	3^5	3^{-3}

Als $\mathbb{Z}[\zeta_3]_3$-Gitter ist $X_Z(L)$ im Fall $\det(X_Z(L)) = 3^{11}$ isomorph zu

$$\mathbb{H}(-1) \perp (1) \perp (1) \perp \mathbb{H}(1) \perp \mathbb{H}(1) \perp (1) \text{ oder}$$
$$\mathbb{H}(1) \perp (1)^7$$

bzw. im Fall $\det(X_Z(L)) = 3^5$ isomorph zu

$$\mathbb{H}(-1) \perp \mathbb{H}(-1) \perp (1)^5 \text{ oder}$$
$$\mathbb{H}(-1) \perp \mathbb{H}(-1) \perp \mathbb{H}(1) \perp \mathbb{H}(-1) \perp (1).$$

Die Maße der Geschlechter sind

$\det(X_Z(L)) = 3^{11}$	$\det(X_Z(L)) = 3^5$
0.0178	$2.311 \cdot 10^{-6}$
$2.53 \cdot 10^{-7}$	0.00018

Die hermiteschen Geschlechter liefern $54 + 11$ mögliche $X_Z(L)$, aus welchen sich $2 + 603$ Paare $(\pi_Z(L), Z(L))$ konstruieren lassen. Keine Verklebung liefert ein extremales Gitter.

Im Fall $s = 4$ gibt es nur ein Paar $(\pi_F(L), F(L))$:

$\det(\pi_F(L))$	$\det(F(L))$	$\det(X_F(L))$	$\det(\pi_Z(L))$	$\det(X_Z(L))$	$\det(Z(L^\#))$
3^{-1}	3^7	3	3^5	3^7	3^{-5}

Als $\mathbb{Z}[\zeta_3]_3$-Gitter ist $X_Z(L)$ isomorph zu

$$\mathbb{H}(-1) \perp \mathbb{H}(-1) \perp \mathbb{H}(1) \perp (1) \perp (1) \perp (1) \text{ oder}$$
$$\mathbb{H}(-1) \perp (1)^7,$$

die Maße der Geschlechter sind 0.0018 bzw. $2.53 \cdot 10^{-7}$. Insgesamt gibt es 54 mögliche $X_Z(L)$, allerdings hat keins ein Obergitter von Determinante 3^{-5} und Minimum ≥ 2.

Die Fälle $f = 0$, $f = 2$ und $f = 4$

In diesen Fällen sind die Paare $(\pi_F(L), F(L))$ zwar eindeutig, die möglichen Paare $(\pi_Z(L), Z(L))$ lassen sich aber nicht sinnvoll berechnen. Es werden also direkt die Teilgitter $N(L)$ konstruiert, welche dann zu einem möglichem extremalen Gitter L geliftet werden können. Für die Fixgitter gilt

	$f = 2$	$f = 4$
$\pi_F(L)$	${}^{(1/3)}A_2$	${}^{(1/3)}A_2 \perp {}^{(1/3)}A_2$
$X_F(L)$	A_2	$A_2 \perp A_2$
$F(L)$	${}^{(3)}A_2$	${}^{(3)}A_2 \perp {}^{(3)}A_2$

Also ist für $f = 0$, $f = 2$ bzw. $f = 4$ $N(L)$ ein Teilgitter von L vom Index 1, 3 bzw. 3^2 mit einem Automorphismus σ vom Typ $3 - (0, 12)$, da ein Element in $\mathrm{Aut}(X_F(L))$ existiert, welches als dritte Einheitswurzel auf $X_F(L)$, aber trivial auf $X_F(L)/F(L)$, operiert. Sei $\delta := (1 - \sigma)$ und sei

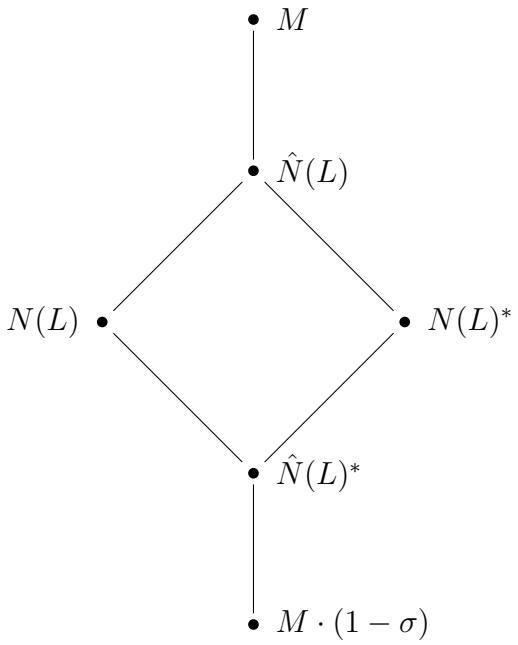
$$\hat{N}(L) := N(L) + N(L)^* = N(L) + N(L)^\# \cdot \delta,$$

dann gilt für das duale Gitter

$$\hat{N}(L)^\# = N(L)^\# \cap N(L) \cdot \frac{1}{\delta}.$$

Analog zum Beweis von Satz 6.34 folgt nun, dass $\hat{N}(L)$ ein ganzes Gitter ist, denn es gilt $N(L) \subseteq N(L)^\#$, $N(L) \subseteq N(L) \cdot \frac{1}{\delta}$ und $N(L)^\# \cdot \delta \subset N(L)^\#$. Zusätzlich ist

$N(L)^{\#} \cdot \delta \subset N(L) \cdot \frac{1}{\delta}$ äquivalent zu $3N(L)^{\#} \subset N(L)$, was erfüllt ist da $N(L)$ 3-elementar ist. Außerdem ist $\hat{N}(L)$ ein gerades Gitter. Es existiert also ein gerades, maximales Obergitter M von $\hat{N}(L)$ mit einem Automorphismus σ. Dieses ist unimodular, hier für gibt es 5 Möglichkeiten (mit jeweils einer Konjugiertenklassen): das Leech-Gitter Λ_{24} und 4 Niemeier-Gitter E_6^4, E_8^3, D_4^6 und A_2^{12} (benannt nach dem Wurzelsystem). Alle $N(L)$ werden nun als σ-invariante Obergitter von $M \cdot (1-\sigma)$ mit Determinante 3^{12}, 3^{14} bzw. 3^{16} konstruiert.



Für die Gitter E_6^4, E_8^3 und Λ_{24} können die Teilgitter $N(L)$ problemlos bestimmt werden, für die Gitter D_4^6 und A_2^{12} ist es sinnvoll zuerst alle Teilgitter mit Determinante 3^{20} und Minimum 6 zu bestimmen (hier gibt es jeweils 54 Stück), und ab dann die Rechnung zu parallelisieren. Die 108 Teilgitter haben im Schnitt rund 10000 Obergitter mit Determinante 3^{16} und einige wenige mit Determinante 3^{14} (mit Minimum 6), extremale Obergitter existieren keine. In den Fällen $f = 2$ bzw. $f = 4$ müssen die $N(L)$ zusätzlich einen Automorphismus vom Typ $3-(2,11)$ bzw. $3-(4,10)$ haben, bzgl. dieser Automorphismen gilt zusätzlich

$$F(L) = F(N(L)) \text{ und } Z(L) = Z(N(L)).$$

Da das Gitter $F(L) \perp Z(L)$ Index 3^s in L hat, gilt für die Determinanten der zyklotomischen Teilgitter

	$f=2$	$f=4$
$\det(\pi_Z(L))$	3^9	3^6
$\det(X_Z(L))$	3^{11}	3^{10}
$\det(Z(L))$	3^{13}	3^{14}

Dadurch kommen bereits die meisten Gitter nicht in Frage. Die verbliebenen Gitter werden in Isomorphieklassen eingeteilt und die Konjugiertenklassen der Automorphismen des entsprechenden Typs betrachtet. Die extremalen Gitter L werden dann als Obergitter von $N(L)$ in $(\frac{1}{3}F(L) \perp Z(L) \cdot (1-\zeta_3)^{-1})/(F(L) \perp Z(L))$ konstruiert. Insgesamt lassen so nur im Fall $f = 0$ extremale Gitter finden, diese sind Teilgitter des Leech-Gitters und isomorph zum bekanntem Gitter L_{24}.

Daraus folgt insgesamt der Beweis von Satz 6.45.

6.6 Extremale, 5-modulare Gitter der Dimension 20

In der Literatur ist bisher kein extremales, 5-modulares Gitter der Dimension 20 bekannt. Die Automorphismen dieser Gitter wurde in [Jür15, Abschnitt 4.2.7.] untersucht, und es wurde gezeigt dass ein solches Gitter keinen Automorphismus mit Primordnung ≥ 7 haben kann. Zusätzlich wurde durch eine heuristische Suche ein Gitter mit Determinante 5^{10} und Minimum 6 gefunden, dieses ist aber nur 5-elementar, und nicht 5-modular. Die Klassifikation dieser Gitter mit einem Automorphismus der Ordnung 5 wurde in [NS] begonnen (hier wurden 72 Gitter gefunden), diese soll nun fertig gestellt werden.

Die maximalen, geraden Obergitter sind 5-elementar mit Determinante 5^2, das entsprechende Geschlecht besteht aus 329 Gittern. Sei M ein solches Gitter, dann können die extremalen Gitter als Obergitter von ${}^{(5)}M^{\#}$ konstruiert werden. Insbesondere muss das Minimum von $M^{\#}$ also mindestens $6/5$ sein, das erfüllen 124 Gitter in dem Geschlecht. Angenommen der Typ von (L, σ) ist $5-(16,1)-1$, dann kann nach Folgerung 6.32 $\det(Z(L)) \leq 5^{s+2z} = 5^3$ angenommen werden. Die Hermitesche Dichte-Funktion des Gitters $Z(L)$ hätte dann Wert

$$\frac{6}{\sqrt[4]{5^3}} \approx 1.79,$$

was gegen die Elkies-Cohn-Schranke von 1.45 verstößt. Insgesamt haben 87 der Obergitter Automorphismen vom Typ ungleich $5-(16,1)$, die Anzahlen der übrigen Typen sind in der folgenden Tabelle angegeben:

Typ	Anzahl
$5-(0,5)$	0
$5-(4,4)$	4
$5-(8,3)$	39
$5-(12,2)$	138

Dass die Gitter keine hermitesche $\mathbb{Z}[\zeta_5]$-Struktur haben können, wurde auch in [Jür15] bemerkt. Für diese 181 Möglichkeiten für (M, σ) können nun alle σ-invarianten, extremalen Gitter L in

$${}^{(5)}M^{\#} \leq L \leq ({}^{(5)}M^{\#})^{\#} = {}^{(1/5)}M$$

berechnet werden. Nur für drei Möglichkeiten existieren extremale Gitter, der Typ von (M, σ) ist in allen Fällen $5 - (4, 4)$.

Satz 6.46. *Es existieren 97 extremale, 5-modulare Gitter L der Dimension 20 mit einem Automorphismus σ der Ordnung 5. Der Typ von (L, σ) ist in allen Fällen $5 - (4, 4) - 4$, insbesondere ist also L als $\mathbb{Z}_5[\sigma]$-Modul frei. Von diesen Gittern ist von vieren die Automorphismengruppe isomorph zu $C_2 \times S_5$, alle anderen Gruppen sind auflösbar.*

Literaturverzeichnis

[Agu+12] Carlos Aguilar-Melchor, Philippe Gaborit, Jon-Lark Kim, Lin Sok und Patrick Solé. „Classification of extremal and s-extremal binary self-dual codes of length 38“. In: *IEEE Trans. Inform. Theory* 58.4 (2012), S. 2253–2262.

[BBH13] Stefka Bouyuklieva, Iliya Bouyukliev und Masaaki Harada. „Some extremal self-dual codes and unimodular lattices in dimension 40“. In: *Finite Fields Appl.* 21 (2013), S. 67–83.

[Ber69] S. D. Berman. „On the theory of group codes“. In: *Cybernetics* 3.1 (1969), 25–31 (1969).

[BHM12] Koichi Betsumiya, Masaaki Harada und Akihiro Munemasa. „A complete classification of doubly even self-dual codes of length 40“. In: *Electron. J. Combin.* 19.3 (2012), Paper 18, 12.

[Bil06] R. T. Bilous. „Enumeration of the binary self-dual codes of length 34“. In: *J. Combin. Math. Combin. Comput.* 59 (2006), S. 173–211.

[BÖ06] Stefka Bouyuklieva und Patric R. J. Östergård. „New constructions of optimal self-dual binary codes of length 54“. In: *Des. Codes Cryptogr.* 41.1 (2006), S. 101–109.

[Bou00] Stefka Bouyuklieva. „A method for constructing self-dual codes with an automorphism of order 2“. In: *IEEE Trans. Inform. Theory* 46.2 (2000), S. 496–504.

[Bou02] Stefka Bouyuklieva. „On the automorphisms of order 2 with fixed points for the extremal self-dual codes of length $24m$“. In: *Des. Codes Cryptogr.* 25.1 (2002), S. 5–13.

[Bou96] Stefka Bouyuklieva. „A method for constructing self-dual codes with application to length 64“. In: *Proceedings of the Fifth International Workshop on Algebraic and Combinatorial Coding Theory (Sozopol, Bulgaria) June 1–7* (1996), S. 81–85.

[BR02] R. T. Bilous und G. H. J. van Rees. „An enumeration of binary self-dual codes of length 32“. In: *Des. Codes Cryptogr.* 26.1-3 (2002). In honour of Ronald C. Mullin, S. 61–86.

[BRS09] José Joaquín Bernal, Ángel del Río und Juan Jacobo Simón. „An intrinsical description of group codes“. In: *Des. Codes Cryptogr.* 51.3 (2009), S. 289–300.

[BW13] Martino Borello und Wolfgang Willems. „Automorphisms of order $2p$ in binary self-dual extremal codes of length a multiple of 24“. In: *IEEE Trans. Inform. Theory* 59.6 (2013), S. 3378–3383.

[CE03] Henry Cohn und Noam Elkies. „New upper bounds on sphere packings. I“. In: *Ann. of Math. (2)* 157.2 (2003), S. 689–714.

[CK09] Henry Cohn und Abhinav Kumar. „Optimality and uniqueness of the Leech lattice among lattices“. In: *Ann. of Math. (2)* 170.3 (2009), S. 1003–1050.

[Coh+17] Henry Cohn, Abhinav Kumar, Stephen D. Miller, Danylo Radchenko und Maryna Viazovska. „The sphere packing problem in dimension 24“. In: *Ann. of Math. (2)* 185.3 (2017), S. 1017–1033.

[CP82] J. H. Conway und V. Pless. „On primes dividing the group order of a doubly-even $(72, 36, 16)$ code and the group order of a quaternary $(24, 12, 10)$ code“. In: *Discrete Math.* 38.2-3 (1982), S. 143–156.

[CPS79] John H. Conway, Vera Pless und Neil J. A. Sloane. „Self-dual codes over $\mathrm{GF}(3)$ and $\mathrm{GF}(4)$ of length not exceeding 16“. In: *IEEE Trans. Inform. Theory* 25.3 (1979), S. 312–322.

[CPS92] J. H. Conway, V. Pless und N. J. A. Sloane. „The binary self-dual codes of length up to 32: a revised enumeration“. In: *J. Combin. Theory Ser. A* 60.2 (1992), S. 183–195.

[CS90] J. H. Conway und N. J. A. Sloane. „A new upper bound for the minimum of an integral lattice of determinant 1“. In: *Bull. Amer. Math. Soc. (N.S.)* 23.2 (1990), S. 383–387.

[CS99] J. H. Conway und N. J. A. Sloane. *Sphere packings, lattices and groups*. Third. Bd. 290. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. Springer-Verlag, New York, 1999, S. lxxiv+703.

[DFP09] Flaviana S. Dutra, Raul A. Ferraz und C. Polcino Milies. „Semisimple group codes and dihedral codes“. In: *Algebra Discrete Math.* 3 (2009), S. 28–48.

[DHS01] Steven T. Dougherty, Masaaki Harada und Patrick Solé. „Shadow codes over $\mathbb{Z}_4$“. In: *Finite Fields Appl.* 7.4 (2001), S. 507–529.

[Ebe13] Wolfgang Ebeling. *Lattices and codes*. Third. Advanced Lectures in Mathematics. A course partially based on lectures by Friedrich Hirzebruch. Springer Spektrum, Wiesbaden, 2013, S. xvi+167.

[EN18] Simon Eisenbarth und Gabriele Nebe. „Self-dual codes over chain rings“. In: *Mathematics in Computer Science* (2018).

[Fei78] Walter Feit. „Some lattices over $\mathbf{Q}(\sqrt{-3})$“. In: *J. Algebra* 52.1 (1978), S. 248–263.

[GO03] Philippe Gaborit und Ayoub Otmani. „Experimental constructions of self-dual codes“. In: *Finite Fields Appl.* 9.3 (2003), S. 372–394.

[Gra] Markus Grassl. *Code Tables: Bounds on the parameters of various types of codes*. http://www.codetables.de.

[Hal05] Thomas C. Hales. „A proof of the Kepler conjecture“. In: *Ann. of Math. (2)* 162.3 (2005), S. 1065–1185.

[Ham+94] A. Roger Hammons Jr., P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane und Patrick Solé. „The $\mathbf{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes“. In: *IEEE Trans. Inform. Theory* 40.2 (1994), S. 301–319.

[HMa] Masaaki Harada und Akihiro Munemasa. *Database of Ternary Maximal Self-Orthogonal Codes*. http://www.math.is.tohoku.ac.jp/~munemasa/research/codes/mso3.htm.

[HMb] Masaaki Harada und Akihiro Munemasa. *Database of Ternary Self-Dual Codes*. http://www.math.is.tohoku.ac.jp/~munemasa/research/codes/sd3.htm.

[HM09] Masaaki Harada und Akihiro Munemasa. „A complete classification of ternary self-dual codes of length 24“. In: *J. Combin. Theory Ser. A* 116.5 (2009), S. 1063–1072.

[HM11] Masaaki Harada und Akihiro Munemasa. „Classification of quaternary Hermitian self-dual codes of length 20“. In: *IEEE Trans. Inform. Theory* 57.6 (2011), S. 3758–3762.

[HM12] Masaaki Harada und Akihiro Munemasa. „Classification of self-dual codes of length 36“. In: *Adv. Math. Commun.* 6.2 (2012), S. 229–235.

[HMV09] Masaaki Harada, Akihiro Munemasa und Boris Venkov. „Classification of ternary extremal self-dual codes of length 28“. In: *Math. Comp.* 78.267 (2009), S. 1787–1796.

[Hou+03] Sheridan K. Houghten, Clement W. H. Lam, Larry H. Thiel und Jeff A. Parker. „The extended quadratic residue code is the only $(48, 24, 12)$ self-dual doubly-even code“. In: *IEEE Trans. Inform. Theory* 49.1 (2003), S. 53–59.

[HP03] W. Cary Huffman und Vera Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003, S. xviii+646.

[Huf05] W. Cary Huffman. „On the classification and enumeration of self-dual codes“. In: *Finite Fields Appl.* 11.3 (2005), S. 451–490.

[Huf82] W. Cary Huffman. „Automorphisms of codes with applications to extremal doubly even codes of length 48“. In: *IEEE Trans. Inform. Theory* 28.3 (1982), S. 511–521.

[Huf88] W. Cary Huffman. „On the $[24, 12, 10]$ quaternary code and binary codes with an automorphism having two cycles“. In: *IEEE Trans. Inform. Theory* 34.3 (1988), S. 486–493.

[Huf90] W. Cary Huffman. „On extremal self-dual quaternary codes of lengths 18 to 28. I“. In: *IEEE Trans. Inform. Theory* 36.3 (1990), S. 651–660.

[Huf91] W. Cary Huffman. „On extremal self-dual quaternary codes of lengths 18 to 28. II“. In: *IEEE Trans. Inform. Theory* 37.4 (1991), S. 1206–1216.

[Huf92] W. Cary Huffman. „On extremal self-dual ternary codes of lengths 28 to 40“. In: *IEEE Trans. Inform. Theory* 38.4 (1992), S. 1395–1400.

[Ĭor83] V. Ĭ. Ĭorgov. „Binary self-dual codes with automorphisms of odd order“. In: *Problemy Peredachi Informatsii* 19.4 (1983), S. 11–24.

[Jac62] Ronald Jacobowitz. „Hermitian forms over local fields“. In: *Amer. J. Math.* 84 (1962), S. 441–465.

[Jür15] Michael Jürgens. „Nicht-Existenz und Konstruktion extremaler Gitter“. Dissertation. Technische Universität Dortmund, 2015.

[Kie13] Michael Kiermaier. „There is no self-dual $\mathbb{Z}_4$-linear code whose gray image has the parameters $(72, 2^{36}, 16)$“. In: *IEEE Trans. Inform. Theory* 59.6 (2013), S. 3384–3386.

[Kir16] Markus Kirschmer. „Definite quadratic and hermitian forms with small class number“. Habilitationsschrift. RWTH Aachen, 2016.

[Kne02] Martin Kneser. *Quadratische Formen*. Revised and edited in collaboration with Rudolf Scharlau. Springer-Verlag, Berlin, 2002, S. viii+164.

[LTS89] C. W. H. Lam, L. Thiel und S. Swiercz. *The Non-existence of Finite Projective Planes of Order 10*. 1989.

[Mac+78] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane und H. N. Ward. „Self-dual codes over $\mathrm{GF}(4)$“. In: *J. Combin. Theory Ser. A* 25.3 (1978), S. 288–318.

[Mac69] Jessie MacWilliams. „Codes and ideals in group algebras“. In: *Combinatorial Mathematics and its Applications (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967)*. Univ. North Carolina Press, Chapel Hill, N.C., 1969, S. 317–328.

[Mac70] F. J. MacWilliams. „Binary codes which are ideals in the group algebra of an Abelian group“. In: *Bell System Tech. J.* 49 (1970), S. 987–1011.

[Mar03] Jacques Martinet. *Perfect lattices in Euclidean spaces*. Bd. 327. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 2003, S. xxii+523.

[Mey10] Annika Meyer. „On dual extremal maximal self-orthogonal codes of type I-IV“. In: *Adv. Math. Commun.* 4.4 (2010), S. 579–596.

[MOS75] C. L. Mallows, A. M. Odlyzko und N. J. A. Sloane. „Upper bounds for modular forms, lattices, and codes“. In: *J. Algebra* 36.1 (1975), S. 68–76.

[MPS76] C. L. Mallows, V. Pless und N. J. A. Sloane. „Self-dual codes over $\mathrm{GF}(3)$“. In: *SIAM J. Appl. Math.* 31.4 (1976), S. 649–666.

[MS73] C. L. Mallows und N. J. A. Sloane. „An upper bound for self-dual codes“. In: *Information and Control* 22 (1973), S. 188–200.

[MS77] F. J. MacWilliams und N. J. A. Sloane. *The theory of error-correcting codes*. North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977, i–ix and 1–762.

[Neb12a] Gabriele Nebe. „An even unimodular 72-dimensional lattice of minimum 8“. In: *J. Reine Angew. Math.* 673 (2012), S. 237–247.

[Neb12b] Gabriele Nebe. „An extremal $[72, 36, 16]$ binary code has no automorphism group containing $Z_2 \times Z_4$, Q_8, or Z_{10}“. In: *Finite Fields Appl.* 18.3 (2012), S. 563–566.

[Neb12c] Gabriele Nebe. „On extremal self-dual ternary codes of length 48“. In: *Int. J. Comb.* (2012), Art. ID 154281, 9.

[Neb13] Gabriele Nebe. „On automorphisms of extremal even unimodular lattices“. In: *Int. J. Number Theory* 9.8 (2013), S. 1933–1959.

[Neb14] Gabriele Nebe. „A fourth unimodular lattice of dimension 48“. In: *Discrete Math.* 331 (2014), S. 133–136.

[Neb19a] Gabriele Nebe. „Automorphisms of p-modular lattices“. In: *preprint* (2019).

[Neb19b] Gabriele Nebe. „Automorphisms of modular lattices“. In: *preprint* (2019).

[Neb98] Gabriele Nebe. „Some cyclo-quaternionic lattices“. In: *J. Algebra* 199.2 (1998), S. 472–498.

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer-Verlag, Berlin, 1992, S. xiii+595.

[NP95] G. Nebe und W. Plesken. „Finite rational matrix groups“. In: *Mem. Amer. Math. Soc.* 116.556 (1995), S. viii+144.

[NRS06] Gabriele Nebe, Eric M. Rains und Neil J. A. Sloane. *Self-dual codes and invariant theory*. Bd. 17. Algorithms and Computation in Mathematics. Springer-Verlag, Berlin, 2006, S. xxviii+430.

[NS] Gabriele Nebe und Neil Sloane. *A Catalogue of Lattices*. `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/index.html`.

[NS14] Gabriele Nebe und Artur Schäfer. „A nilpotent non abelian group code“. In: *Algebra Discrete Math.* 18.2 (2014), S. 268–273.

[OMe63] O. T. O'Meara. *Introduction to quadratic forms*. Die Grundlehren der mathematischen Wissenschaften, Bd. 117. Academic Press, Inc., Publishers, New York; Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963, S. xi+342.

[OW11] E. A. O'Brien und Wolfgang Willems. „On the automorphism group of a binary self-dual doubly even $[72, 36, 16]$ code“. In: *IEEE Trans. Inform. Theory* 57.7 (2011), S. 4445–4451.

[Pil+12] Cristina García Pillado, Santos González, Victor Markov, Consuelo Martínez und Alexandr Nechaev. „When are all group codes of a noncommutative group abelian (a computational approach)?“ In: *Fundam. Prikl. Mat.* 17.2 (2011/12), S. 75–85.

[Ple70] Vera Pless. „On a family of symmetry codes over $\mathrm{GF}(3)$ and related new five-designs“. In: *Combinatorial Structures and their Applications (Proc. Calgary Internat. Conf., Calgary, Alta., 1969)*. Gordon und Breach, New York, 1970, S. 323–326.

[Ple72] Vera Pless. „A classification of self-orthogonal codes over $\mathrm{GF}(2)$“. In: *Discrete Math.* 3 (1972), S. 209–246.

[PS75] Vera Pless und N. J. A. Sloane. „On the classification and enumeration of self-dual codes“. In: *J. Combinatorial Theory Ser. A* 18 (1975), S. 313–335.

[PSW80] Vera Pless, N. J. A. Sloane und Harold N. Ward. „Ternary codes of minimum weight 6 and the classification of the self-dual codes of length 20“. In: *IEEE Trans. Inform. Theory* 26.3 (1980), S. 305–316.

[Que95] H.-G. Quebbemann. „Modular lattices in Euclidean spaces“. In: *J. Number Theory* 54.2 (1995), S. 190–202.

[Que97] H.-G. Quebbemann. „Atkin-Lehner eigenforms and strongly modular lattices“. In: *Enseign. Math. (2)* 43.1-2 (1997), S. 55–65.

[Rai00] Eric Rains. „Bounds for self-dual codes over Z_4“. In: *Finite Fields Appl.* 6.2 (2000), S. 146–163.

[Rai98] Eric M. Rains. „Shadow bounds for self-dual codes“. In: *IEEE Trans. Inform. Theory* 44.1 (1998), S. 134–139.

[Rei57] Irving Reiner. „Integral representations of cyclic groups of prime order“. In: *Proc. Amer. Math. Soc.* 8 (1957), S. 142–146.

[RS98a] E. M. Rains und N. J. A. Sloane. „The shadow theory of modular and unimodular lattices“. In: *J. Number Theory* 73.2 (1998), S. 359–389.

[RS98b] Eric M. Rains und N. J. A. Sloane. „Self-dual codes“. In: *Handbook of coding theory, Vol. I, II*. North-Holland, Amsterdam, 1998, S. 177–294.

[Sie69] Carl Ludwig Siegel. „Berechnung von Zetafunktionen an ganzzahligen Stellen“. In: *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II* 1969 (1969), S. 87–102.

[SL95] Roberta Evans Sabin und Samuel J. Lomonaco. „Metacyclic error-correcting codes“. In: *Appl. Algebra Engrg. Comm. Comput.* 6.3 (1995), S. 191–210.

[SS99] Rudolf Scharlau und Rainer Schulze-Pillot. „Extremal lattices“. In: *Algorithmic algebra and number theory (Heidelberg, 1997)*. Springer, Berlin, 1999, S. 139–170.

[ST83] N. J. A. Sloane und J. G. Thompson. „Cyclic self-dual codes“. In: *IEEE Trans. Inform. Theory* 29.3 (1983), S. 364–366.

[TAT15] Zi Shyuan Tan, Miin Huey Ang und Wen Chean Teh. „Group ring codes over a dihedral group“. In: *Malays. J. Math. Sci.* 9.Special Issue: The 4th International Cryptology and Information Security Conference 2014 (2015), S. 37–52.

[Via17] Maryna S. Viazovska. „The sphere packing problem in dimension 8“. In: *Ann. of Math. (2)* 185.3 (2017), S. 991–1015.

[War76] Harold N. Ward. „A restriction on the weight enumerator of a self-dual code“. In: *J. Combinatorial Theory Ser. A* 21.2 (1976), S. 253–255.

[Web16] Peter Webb. *A Course in Finite Group Representation Theory*. Cambridge University Press, 2016.

[Wil02] Wolfgang Willems. „A note on self-dual group codes“. In: *IEEE Trans. Inform. Theory* 48.12 (2002), S. 3107–3109.

[ZG15] Tao Zhang und Gennian Ge. „Fourth power residue double circulant self-dual codes“. In: *IEEE Trans. Inform. Theory* 61.8 (2015), S. 4243–4252.

[Zim14] Alexander Zimmermann. *Representation Theory: A Homological Algebra Point of View*. Springer International Publishing, 2014.