Über die Automorphismengruppe extremaler Codes der Längen 96 und 120

Dissertation

zu Erlangung des akademischen Grades

doctor rerum naturalium
(Dr. rer. nat.)

von M. Sc. Javier De la Cruz C.
geb. am 02.04.1977 in Pivijay-Kolumbien

genehmigt durch die Fakultät für Mathematik
der Otto-von-Guericke-Universität Magdeburg.

Gutachter: Prof. Dr. Wolfgang Willems
Prof. Dr. Alfred Wassermann

eingereicht am: 07.12.2011

Verteidigung am: 02.03.2012

Zusammenfassung

Die vorliegende Arbeit untersucht die Automorphismengruppe selbstdualer extremaler Codes der Längen 96 und 120. Im ersten Teil der Arbeit wird bewiesen, dass ein Automorphismus eines selbstdualen extremalen $[96, 48, 20]$-Codes der Ordnung 3 keine oder 6 Fixpunkte hat und ein Automorphismus der Ordnung 5 genau 6. Hat ferner kein Automorphismus der Ordnung 3 einen Fixpunkt, so ist die Automorphismengruppe entweder auflösbar und ihre Ordnung ist 15, 30, 240, 480 oder Teiler von $2^5 3$, $2^5 5$, oder die Automorphismengruppe ist die einfache Gruppe A_5. Weiterhin können die Fälle $|\mathrm{Aut}(C)| = 20$ oder $|\mathrm{Aut}(C)| = 40$ nicht auftreten.

Für Automorphismen auf selbstdualen $[120, 60, 24]$-Codes beweisen wir, dass ungerade Primzahlordnung p höchstens für $p = 3$, 5 ,7, 19, 23 oder 29 auftritt, die jeweilige Zyklen-Struktur durch 3-$(40; 0)$, 5-$(24; 0)$, 7-$(17; 1)$, 19-$(6; 6)$, 23-$(5; 5)$ oder 29-$(4; 4)$ gegeben ist. Die Ordnung der Automorphismengruppe ist $|\mathrm{Aut}(C)| = 2^a \cdot 3^b \cdot 5^c \cdot 7^d \cdot 19^e \cdot 23^f \cdot 29^g$, wobei $a \in \mathbb{N}_0$ und $b, c, d, e, f, g \in \{0, 1\}$ ist. Ist σ ein Automorphismus eines selbstdualen $[120, 60, 24]$-Codes von ungerader zusammengesetzter Ordnung r, so ist $r = 15, 57$ oder 115 und seine Zyklen-Struktur ist $3 \cdot 5$-$(0, 0, 8; 0)$, $3 \cdot 19$-$(2, 0, 2; 0)$ oder $5 \cdot 23$-$(1, 0, 1; 0)$.

In einem weiteren Kapitel zeigen wir, dass der binäre Code $C(\mathcal{D})$ zu einem selbstorthogonalen 5-$(120, 24, 8855)$ Design $\mathcal{D}$ ein selbstdualer und doppeltgerader $[120, 60, d]$-Code mit Minimaldistanz $d = 16$ oder 24 ist. Daher wird ein selbstdualer $[120, 60, 24]$-Code von den Vektoren minimalen Gewichts 24 erzeugt.

Abstract

In this work we study the automorphism group of extremal codes of lengths 96 and 120. First we prove that an automorphism of an extremal $[96, 48, 20]$ code C of order 3 has exactly 6 or no fixed points and an automorphism of order 5 has exactly 6 fixed points. Moreover, if all automorphisms of order 3 are fixed point free then either $\mathrm{Aut}(C)$ is a solvable group and its order is 15, 30, 240, 480 or divides $2^5 3$, $2^5 5$, or $\mathrm{Aut}(C)$ is the alternating group A_5. Furthermore, $|\mathrm{Aut}(C)| = 20$ or $|\mathrm{Aut}(C)| = 40$ cannot occur.

Moreover we prove that the only odd primes that may divide the order of the automorphism group of a putative binary self-dual doubly-even $[120, 60, 24]$ code C are 2, 3, 5, 7, 19, 23 and 29. Moreover, the cyclic structure of an automorphism of these orders is given by 3-$(40; 0)$, 5-$(24; 0)$, 7-$(17; 1)$, 19-$(6; 6)$, 23-$(5; 5)$ and 29-$(4; 4)$. The order of the automorphism group is $|\mathrm{Aut}(C)| = 2^a \cdot 3^b \cdot 5^c \cdot 7^d \cdot 19^e \cdot 23^f \cdot 29^g$, where $a \in \mathbb{N}_0$ and $b, c, d, e, f, g \in \{0, 1\}$. Furthermore, we prove that if σ is an automorphism of C of odd composite order r then $r = 15$, 57 or $r = 115$ and the cyclic structure of an automorphism of these orders are given by $3 \cdot 5$-$(0, 0, 8; 0)$, $3 \cdot 19$-$(2, 0, 2; 0)$ or $5 \cdot 23$-$(1, 0, 1; 0)$.

We also show that the binary code $C(\mathcal{D})$ of length 120 related to a self-orthogonal 5-$(120, 24, 8855)$ design $\mathcal{D}$ is self-dual doubly-even and has minimum distance $d = 24$ (i.e. is extremal) or $d = 16$. Thus a self-dual extremal code $[120, 60, 24]$ code is generated by the vectors of minimal weight 24.

Inhaltsverzeichnis

Einleitung

Lineare binäre selbstduale Codes spielen in der Codierungstheorie eine bedeutende Rolle. So haben der erweiterte binäre Golay-Code sowie einige quadratische Reste-Codes ihren Ursprung in diesem Bereich. Gleason, Pierce und Turyn bewiesen in ihren Arbeiten (siehe [54] und [4]), dass, wenn $r \mid \mathrm{wt}(v)$ für alle Vektor eines binären selbstdualen Codes C, so ist $r = 2$ oder $r = 4$. Man spricht hier von einem doppeltgeraden Code, wenn $r = 4$ ist.

Ab Paragraph 1.2 der vorliegenden Arbeit betrachten wir, wenn nicht anders vermerkt, nur lineare binäre Codes. In [25] wurde bewiesen, dass für C selbstdual und doppeltgerade das homogene Gewichtspolynom von C ein Polynom mit rationalen Koeffizienten in $x^8 + 14x^4y^4 + y^8$ und $x^4y^4(x^4 - y^4)^4$ ist. Das bedeutet, dass die Längen von binären selbstdualen doppeltgeraden Codes durch 8 teilbar sind. Ein binärer selbstdualer doppeltgerader Code heißt Typ II Code. Die selbstdualen Codes, die nicht doppeltgerade sind, nennen wir Typ I Codes. Mallows und Sloane haben in [41] gezeigt, dass ein binärer selbstdualer doppeltgerader (Typ II) Code der Länge n eine Minimaldistanz $d \leq 4\lfloor n/24 \rfloor + 4$ hat. Rains verdeutlicht in [51], dass für selbstduale binäre Codes mit einer Länge von $24 \nmid n + 2$ im Allgemeinen auch die obige Schranke gilt, ohne Voraussetzung einer Doppelgeradigkeit. Gerade Rains begründet, dass, wenn C ein selbstdualer binärer Code mit einer Länge von n ist, demnach $d \leq 4\lfloor n/24 \rfloor + 4$ ergibt, ausgenommen wenn $n \equiv 22 \mod 24$ ist, wobei $d \leq 4\lfloor n/24 \rfloor + 6$. Ein selbstdualer Code, der auf diese Schranke trifft, wird als extremal bezeichnet.

Mallows und Sloane zeigen in [41], dass es keine extremalen Codes für große Längen n gibt. Allerdings gaben sie hierbei keine exakte Beschränkung an. Ma bewies in [39], dass keine extremalen doppeltgeraden Codes der Länge $n \geq 3984$ existieren, da der Koeffzient $A_{4m+8} < 0$ für $m = \lfloor n/24 \rfloor \geq 166$. Für die minimalen Längen ist bekannt, dass ein doppeltgerader extremaler Code für die Länge 8, zwei für die Länge 16, einer für die Länge 24, fünf für die Länge 32 und einer für die Länge 48 existieren. Alle haben einen Automorphismus von ungerader Primzahlordnung. Der größte extremale doppeltgerade Code, der bis dato konstruiert wurde, hat die Länge $n = 136$, welcher ein doppeltzirkulanter Code ist [43]. Daher gibt es eine große Lücke zwischen der Schranke und dem was gebaut wurde.

Rains bewies in [51], dass jeder selbstduale (extremale) $[24m, 12m, 4m+4]$-Code doppeltgerade ist (d.h. sind von Typ II). Zhang bewies in [63], welche Codes die Länge $n = 24m \leq 3672$ haben. Es ist bekannt, dass die doppeltgeraden extremalen Codes die größte Anzahl der Fehler zwischen den selbstdualen doppeltgeraden Codes korrigieren. Weiterhin wurde von Assmus und Mattson gezeigt [3], dass, wenn die Länge durch 24 teilbar ist, die Träger der Vektoren eines konstanten Gewichts ein 5-Design bilden. Deshalb sind doppeltgerade extremale Codes der Länge $n = 24m$ aus geometrischer Sicht von besonderer Bedeutung. Trotz ihrer Bedeutung und obwohl die Schranke ($n = 24m < 3672$) für die Länge erheblich groß ist, sind nur zwei selbstduale extremale $[24m, 12m, 4m + 4]$-Codes bekannt: der Golay $[24, 12, 8]$-Code und der bekannte quadratische $[48, 24, 12]$-Reste-Code. Beide mit einer nicht

trivialen Automorphismengruppe [45], [40], [32], [38], [33]. Nichtsdestotrotz, der erste zu untersuchende Fall ist $m = 3$. Bereits 1972 hat Sloane in [53] die Frage nach der Existenz eines extremalen $[72, 36, 16]$-Codes gestellt. Trotz der vielfachen Versuche eine Nicht-Existenz oder eine Konstruktion zu finden, bleibt die Antwort bis heute offen. Für eine mögliche Konstruktion könnte ein nicht-trivialer Automorphismus nützlich sein. Die ersten Arbeiten von Conway, Pless, Thompson, Huffman und Yorgov begründen, dass die einzigen möglichen teilbaren Primfaktoren in der Ordnung der Automorphismengruppe die Zahlen 2, 3, 5 oder 7 sein können [14], [47], [50], [35]. Ähnlich ist man früher vorgegangen, als man versuchte, die Existenz einer projektiven Ebene der Ordnung 10 nachzuweisen, von der wir heute wissen, dass sie nicht existiert.

Die Zyklen-Struktur der Automorphismen dieser Ordnungen wurde von Bouyuklieva, Dontcheva, van Zanten und Dodunekov in [9], [8] und [19] untersucht. Die Elemente der Ordnung 2 und 3 haben keine Fixpunkte und die der Ordnung 5 und 7 exakt zwei. 2006 Bouyuklieva, O'Brien und Willems bewiesen in [10], dass die Automorphismengruppe auflösbar ist. Im Jahre 2011 zeigten O'Brien und Willems in [13], dass die Ordnung der Automorphismengruppe kleiner oder gleich 36 ist. Die kürzlich von Feulner und Nebe in [24] verwendete Darstellungstheorie sowie das Kombinieren der Ergebnisse aus [44] und [13] und von Yankov in [57] beweisen: Die Automorphismengruppe eines binären selbstdualen $[72, 36, 16]$-Codes hat Ordnung 5, 10 (Diedergruppe) oder r mit $r \mid 24$.

Der Schwerpunkt dieser Arbeit liegt in der Untersuchung der Automorphismengruppe für die Fälle $m = 4$ und $m = 5$, also die extremalen $[96, 48, 20]$- und $[120, 60, 24]$-Codes. Hierfür verwenden wir die entwickelten Ideen und Methoden von Conway, Pless und Huffman in [14], [33], wo die Untercodes $F_\sigma(C)$ (sowie der zusammengezogene Code $\pi(F_\sigma(C))$) und $E_\sigma(C)$ definiert sind, für einen selbstdualen Code C mit einem Automorphismus σ von ungerader Primzahlordnung. Diese ermöglichen die Zerlegung des Codes $C = F_\sigma(C) \oplus E_\sigma(C)$. In gleicher Weise verwenden wir Erweiterungen dieser Arbeiten von Yorgov in [58], [59]. In diesen Arbeiten werden hinreichende und notwendige Bedingungen für die Existenz eines selbstdualen Codes mit einem Automorphismus von ungerader Primzahlordnung gegeben sowie für die Äquivalenz von zwei selbstdualen Codes mit einem gleichen Automorphismus.

Die vorliegende Arbeit besteht aus vier Kapiteln. Im ersten Paragraphen von **Kapitel 1** erfolgt eine kurze Beschreibung von Definitionen, Bemerkungen und bekannten Ergebnissen, die während dieser Arbeit verwendet werden. Zudem werden auch einige neue Ergebnisse im Paragraphen 1.4 und 1.6 vorgestellt, wie das Lemma 1.4.8, Lemma 1.4.9, Lemma 1.6.3 und der Satz 1.6.4. Dieser Satz ist von besonderer Bedeutung, weil er zeigt, dass ein binärer selbstdualer Code mit Minimaldistanz d keinen Automorphismus vom Typ p-$(c; f)$ hat, wobei p eine ungerade Primzahl, $c = f$ und $p + c < d$ ist. Es ist möglich, die Primzahl 11 als einen möglichen Teiler aus der Ordnung der Automorphismengruppe von einem extremalen Code der Länge 120 auszuschließen.

In **Kapitel 2** werden die möglichen Automorphismengruppen eines selbstdualen $[96, 48, 20]$-Codes untersucht. Im Paragraph 2.1.1 werden die Typen 3-$(24; 24)$, 3-$(26; 18)$ und 5-$(16; 16)$ für einen Automorphismus der Ordnung 3 oder 5 ausgeschlossen und mit theoretischen Argumenten gezeigt, dass in jedem Fall $F_\sigma(C)$ nicht existiert. Im Paragraph 2.1.2 wird anhand vom Frobenius Lemma die Struktur der Automorphismengruppe analysiert. Als Hauptergebnis dieses Kapitels erhalten wir:

Hauptsatz 2.1.2 *Sei C ein extremaler Code der Länge* 96.

1. *Falls σ ein Automorphismus von C der Primzahlordnung p ist, dann ist seine Zyklen-Struktur gegeben durch*

p	*Anzahl der p-Zyklen*	*Anzahl der Fixpunkte*
2	48	0
3	30, 32	6, 0
5	18	6

2. *Ist σ ein Automorphismus von C von ungerader zusammengesetzter Ordnung r, so ist $r = 9, 15$ oder 45 und seine Zyklen-Struktur ist $9\text{-}(0, 10; 6)$, $9\text{-}(1, 10; 3)$, $9\text{-}(2, 10; 0)$, $3 \cdot 5\text{-}(0, 0, 6; 6)$, $3 \cdot 5\text{-}(2, 0, 6; 0)$, $3^2 \cdot 5\text{-}(0, 0, 0, 2; 6)$, $3^2 \cdot 5\text{-}(1, 0, 0, 2; 3)$ oder $3^2 \cdot 5\text{-}(2, 0, 0, 2; 0)$.*

3. *Falls alle Automorphismen der Ordnung 3 keine Fixpunkte haben, so ist die Automorphismengruppe auflösbar oder die Automorphismengruppe ist die einfache Gruppe A_5. Insbesondere ist $|\mathrm{Aut}(C)| \leq 480$. Weiterhin können die Fälle $|\mathrm{Aut}(C)| = 20$ oder $|\mathrm{Aut}(C)| = 40$ nicht auftreten.*

In **Kapitel 3** wird der Fall $m = 5$ untersucht, also ein selbstdualer $[120, 60, 24]$-Code. Im Abschnitt 3.1 beweisen wir, dass die einzigen ungeraden Primzahlen, die die Ordnung der Automorphismengruppen teilen, 3, 5, 7, 19, 23 und 29 sind. Der Ausschluss aller anderen Primzahlen erfolgt in theoretischer Form mit Ausnahme von 59. Für diese werden computergestützte Kalkulationen verwendet, basierend auf den Methoden von Yorgov in [58] und [59]. Hierbei wird auch deutlich, dass alle Automorphismen von ungerader Primzahlordnung nur einen möglichen Typ aufweisen. Insbesondere in Zusammenarbeit mit Stefka Bouyuklieva konnten wir beweisen, dass Automorphismen der Ordnung 3 keine Fixpunkte haben. Als Hauptsatz im Paragraph 3.1 erhalten wir:

Hauptsatz 3.1.2 *Sei C ein extremaler Code der Länge 120.*

1. *Falls σ ein Automorphismus von C der Primzahlordnung p ist, dann ist seine Zyklen-Struktur gegeben durch*

p	*Anzahl der p-Zyklen*	*Anzahl der Fixpunkte*
2	48, 60	24, 0
3	40	0
5	24	0
7	17	1
19	6	6
23	5	5
29	4	4

2. *Die Ordnung der Automorphismengruppe ist $|\mathrm{Aut}(C)| = 2^a \cdot 3^b \cdot 5^c \cdot 7^d \cdot 19^e \cdot 23^f \cdot 29^g$, wobei $a \in \mathbb{N}_0$ und $b, c, d, e, f, g \in \{0, 1\}$ ist.*

3. *Ist σ ein Automorphismus von C von ungerader zusammengesetzter Ordnung r, so ist $r = 15$, 57 oder 115 und die Zyklen-Struktur von σ ist $3 \cdot 5\text{-}(0, 0, 8; 0)$, $3 \cdot 19\text{-}(2, 0, 2; 0)$ oder $5 \cdot 23\text{-}(1, 0, 1; 0)$.*

Obwohl es nicht einfach ist, die Primzahlen 19 und 29 aufgrund der Größe des Codes auszuschließen, präsentieren wir im Paragraph 3.2 die mögliche Erzeugermatrix eines extremalen Codes der Länge 120 mit einem Automorphismus dieser Ordnung. Hierbei verwenden wir Resultate aus den Arbeiten [35] und [59]. Mit diesen Resultaten wurden neue selbstduale doppeltgerade Codes für die Länge 120 gefunden.

Wie schon erwähnt, besteht eine interessante Verbindung zwischen den extremalen Codes der Länge $24m$ sowie 5-Designs. Insbesondere wird in [30] und [29] bewiesen, dass für $m = 3$ und für $m = 4$ die Existenz eines extremalen $[24m, 12m, 4m + 4]$-Codes C gleichwertig zur Existenz eines selbstorthogonalen 5-$(24m, 4m + 4, \binom{5m-2}{m-1})$ Designs $\mathcal{D}$ ist. Im Paragraph 3.3 beweisen wir das folgende Hauptergebnis:

Hauptsatz 3.3.1 *Sei $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ ein selbstorthogonales 5-$(120, 24, 8855)$ Design. Dann ist der Code $C(\mathcal{D})$ zum Design $\mathcal{D}$ ein selbstdualer und doppeltgerader $[120, 60, d]$-Code mit Minimaldistanz d gleich 16 oder 24.*

Leider war es nicht möglich, die Distanz $d = 16$ auszuschließen und damit die Äquivalenz zwischen der Existenz eines orthogonalen 5-$(120, 24, 8855)$ Designs $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ und eines extremalen $[120, 60, d]$-Codes C zu begründen. Nichtsdestotrotz haben wir als Ergebnis des Hauptsatzes 3.3.2, dass ein selbstdualer $[120, 60, 24]$-Code von Vektoren des minimalen Gewichts 24 erzeugt wird. Im Paragraph 3.4 werden einige konkrete Berechnungen durchgeführt, um notwendige Bedingungen für die Existenz eines selbstdualen $[120, 60, 24]$-Codes herbeizuführen. Solche sind schon für die Länge 72 und 96 in [20] und [6] hergeleitet.

Schließlich konstruieren wir in **Kapitel 4** neue selbstduale Codes. Konkret wird im Paragraphen 4.1 gezeigt, dass mindestens 24 nicht-äquivalente doppeltgerade selbstduale $[120, 60, 20]$-Codes mit einem Automorphismus der Ordnung 59 existieren und mindestens 23 mit einem Automorphismus der Ordnung 29. Die Untersuchungen im Paragraphen 4.2 führen zu folgendem Ergebnis:

Hauptsatz 4.2.1 *Es gibt nur drei extremale $[60, 30, 12]$-Codes C vom Typ I mit einem Automorphismus der Ordnung 29.*

Danksagung

Zunächst möchte ich Gott für seine Kraft und den Beistand danken, die es erst möglich machten, diese Arbeit zu vollenden.

Ferner danke ich Professor Willems für die Möglichkeit, mit ihm zusammenzuarbeiten, für seine konstruktiven Gespräche und seine Unterstützung.

Ich danke Stefka Bouyuklieva für ihre Unterstützung und die Beweisideen zu verschiedenen Ergebnissen. Auch möchte ich Ralph August für die einführenden Hilfestellungen im Umgang mit dem Programm MAGMA danken.

Für die orthographische Korrektur dieser Arbeit danke ich Jeannette Polte und Matthias Henze.

Ganz besonders danke ich meiner großen Liebe Arleth Sugey, für ihre stets bedingungslose Unterstützung und das grenzenlose Vertrauen in meine Arbeit. Tatsächlich war mein Aufenthalt in Deutschland an ihrer Seite deutlich einfacher.

Meinen Eltern danke ich für ihre Ratschläge, Unterstützung und die Kraft während meiner Studien.

Ich danke Ismael Gutierrez für sein Vertrauen in meine Person sowie für den Kontakt zu Professor Willems.

Zu guter Letzt bedanke ich mich bei meiner Familie und meinen Freunden Jorge Robinson und Michael für die hilfreichen Ratschläge und motivierenden Worte während der letzten drei Jahre.

Kapitel 1

Grundbegriffe und vorbereitende Resultate

1.1 Selbstduale Codes und Gewichtspolynome

1.1.1 Definition. Ein *linearer* $[n,k]$*-Code* C über K ist ein Unterraum des K-Vektorraums K^n der Dimension k, wobei K ein endlicher Körper und $n \in \mathbb{N}$ ist. Ist $v \in C$, so heißt v ein *Codewort* von C. Für ein Codewort $v = (v_1, \ldots, v_n) \in C$ setzen wir $\mathrm{wt}(v) = |\{i \mid v_i \neq 0\}|$ und nennen $\mathrm{wt}(v)$ das *Gewicht von* v. Das minimale Gewicht aller Differenzen zweier verschiedener Codeworte heißt die Minimaldistanz d von C. Wir sprechen dann auch von einem linearen $[n,k,d]$-Code. Wir nennen C einen binären $[n,k,d]$-Code, falls $K = \mathbb{F}_2$ ist.

Den Träger von $v = (v_1, \ldots, v_n) \in K^n$ definieren wir durch $\mathrm{supp}(v) = \{i \mid v_i \neq 0\}$. Insbesondere ist $\mathrm{wt}(v) = |\mathrm{supp}(v)|$.

Im Vektorraum K^n definiert man das innere Produkt der Vektoren $v = (v_1, \ldots, v_n)$ und $u = (u_1, \ldots, u_n)$ durch $v \cdot u := v_1u_1 + \ldots + v_nu_n$. Für einen gegebenen linearen Code C definiert man den dualen Code von C als

$$C^\perp := \{v \in K^n \mid v \cdot u = 0, \text{ für alle } u \in C\}.$$

Man spricht von einem selbstdualen Code, wenn $C = C^\perp$. Ist $C \subseteq C^\perp$, so nennen wir C einen selbstorthogonalen Code.

Der Beweis des folgenden Lemmas ist trivial.

1.1.2 Lemma. *Sei C ein binärer Code der Länge n. Weiterhin sei $0 \neq v, u \in C$ und*

$$S_{v,u} :=\mid \mathrm{supp}(v) \cap \mathrm{supp}(u) \mid .$$

1. *Ist C mit Minimaldistanz d und $v \neq u$ mit $\mathrm{wt}(v) = \mathrm{wt}(u) = d$, so ist $S_{v,u} \leq d/2$.*
2. *$S_{v,u} \geq \mathrm{wt}(u) + \mathrm{wt}(v) - n$.*

1.1.3 Definition. Sei C ein Code der Länge n. Für $i = 0, \ldots, n$ bezeichnen wir mit

$$A_i = |\{c \mid c \in C, \mathrm{wt}(c) = i\}|$$

die Anzahl der Codeworte vom Gewicht i. Weiterhin nennen wir $A_0, \ldots, A_n$ die Gewichtsverteilung und das ganzzahlige Polynom

$$W_C(z) = W(z) = \sum_{i=0}^{n} A_i z^i = \sum_{c \in C} z^{\mathrm{wt}(c)} \in \mathbb{Z}[z]$$

das *Gewichtspolynom von C*. Wir nennen

$$W_C(x,y) = W(x,y) = x^n W(\frac{y}{x}) = \sum_{i=0}^{n} A_i x^{n-i} y^i \in \mathbb{Z}[x,y]$$

das *homogene Gewichtspolynom von C* in den Variablen x, y.

Zentral in der Untersuchung von linearen Codes sind die folgenden Indentitäten:

1.1.4 Satz. ([34, Chap. 7, Theorem 7.1.3]) **(MacWilliams-Identitäten)** *Sei C ein $[n,k]$-Code über $\mathbb{F}_q$ mit dem Gewichtspolynom $W_C(z) = \sum_{i=0}^{n} A_i z^i$. Sei $W_{C^\perp}(z) = \sum_{i=0}^{n} A_i^\perp z^i$ das Gewichtspolynom von $C^\perp$. Dann gelten für alle $r = 0, \ldots, n$ die Identitäten*

$$\sum_{i=0}^{n-r} \left(\begin{array}{c} n-i \\ r \end{array} \right) A_i = q^{k-r} \sum_{j=0}^{r} \left(\begin{array}{c} n-j \\ r-j \end{array} \right) A_j^\perp.$$

Aus 1.1.4 folgt durch Rechnung

1.1.5 Satz. ([56, Kap. 3, Satz 3.7.2 (a)]) *Sei C ein $[n,k,d]$-Code über $\mathbb{F}_q$ und $d^\perp$ die Minimaldistanz von $C^\perp$. Weiterhin sei $A_0, A_1, \ldots, A_n$ die Gewichtsverteilung von C. Dann gilt für alle $r = 1, \ldots, d^\perp$*

$$A_{n-d^\perp+r} = (-1)^r r \binom{d^\perp}{r} \sum_{j=d}^{n-d^\perp} \binom{n-j}{d^\perp} \frac{A_j}{n-j-d^\perp+r} +$$

$$\binom{n}{d^\perp - r} \sum_{i=0}^{r-1} (-1)^i \binom{n-d^\perp+r}{i} (q^{k-d^\perp+r-i} - 1).$$

Insbesondere ist die Gewichtsverteilung durch die Parameter $n, k, d, d^\perp, q$ und $A_d, \ldots, A_{n-d^\perp}$ eindeutig bestimmt.

Einige Gleichungen äquivalent zu den MacWilliams Identitäten sind die folgenden:

1.1.6 Satz. ([48, Chap. 8, Theorem 85]) **(Pless Power Moments)** *Sei C ein $[n,k]$-Code über $\mathbb{F}_q$. Weiterhin sei $A_0, A_1, \ldots, A_n$ die Gewichtsverteilung von C und $B_0, B_1, \ldots, B_n$ die Gewichtsverteilung von $C^\perp$. Dann gilt*

$$\sum_{j=0}^{n} j^r A_j = \sum_{j=0}^{\min\{n,r\}} (-1)^j B_j \left[\sum_{\nu=j}^{r} \nu! S(r,\nu) q^{k-\nu} (q-1)^{\nu-j} \binom{n-j}{n-\nu} \right]$$

für $0 \leq r$, wobei $S(r,\nu) = \frac{1}{\nu!} \sum_{i=0}^{\nu} (-1)^{\nu-i} \binom{\nu}{i} i^r$ ist.

1.1.7 Definition. Sei C ein linearer $[n,k]$-Code über $\mathbb{F}_q$, mit Koordinaten-Menge $S := \{1,2,\ldots,n\}$ und $T := \{T_1, T_2, \ldots, T_p\}$ eine Partition von S mit $n_u := |T_u|$. Für einen Vektor $v \in \mathbb{F}_q^n$ setzen wir

$$W_T(v) := (|\mathrm{supp}(v) \cap T_1|, \ldots, |\mathrm{supp}(v) \cap T_p|)$$

und nennen $W_T(v)$ das *T-Gewicht von v*.

Sei $W(T)$ die Menge aller möglichen Gewichte in Bezug auf die Partition T, d.h.

$$W(T) := \{\mathbf{i} \in \mathbb{N}^p \mid i_u \leq n_u \ \forall u\}.$$

Die Kardinalität von $W(T)$ ist $N(T) := \prod_{u=1}^{p}(n_u + 1)$.

Weiterhin sei $A_{\mathbf{i}}(T) := |\{v \in C \mid W_T(v) = \mathbf{i}\}|$ und $B_{\mathbf{i}}(T) := |\{v \in C^\perp \mid W_T(v) = \mathbf{i}\}|$. Der Vektor $((A_{\mathbf{i}}(T)))_{\mathbf{i}\in W(T)}$ der Länge $N(T)$ heißt die *Gewichtsverteilung des Codes in Bezug auf die Partition T*. Ist $p = 2$, sprechen wir von der *Split-Gewichtsverteilung*.

Der folgende Satz gibt die MacWilliams Identitäten in Bezug auf die Split-Gewichtsverteilung eines linearen Codes C an.

1.1.8 Satz. ([23]) *Sei C ein linearer $[n,k]$-Code über $\mathbb{F}_q$. Ist $T := (T_1, T_2)$ eine Partition seiner Koordinaten mit $(|T_1|, |T_2|) = (n_1, n_2)$, so ist*

$$B_{(\mathbf{i}_1,\mathbf{i}_2)} = \frac{1}{q^k} \sum_{\mathbf{w}_2=0}^{n_2} \sum_{\mathbf{w}_1=0}^{n_1} A_{(\mathbf{w}_1,\mathbf{w}_2)} \mathcal{K}_{\mathbf{i}_1}(\mathbf{w}_1, n_1) \mathcal{K}_{\mathbf{i}_2}(\mathbf{w}_2, n_2),$$

wobei $\mathcal{K}_{\mathbf{s}}(x,\gamma) = \sum_{j=0}^{s} \binom{\gamma-x}{s-j}\binom{x}{j}(-1)^j(q-1)^{s-j}$ für alle $s = 0, 1, \ldots, \gamma$.

1.1.9 Definition. Sei $1 < r \in \mathbb{N}$. Ein Code C heißt *r-dividierbar*, falls für alle $c \in C$ die Bedingung $r \mid \mathrm{wt}(c)$ gilt.

Gleason, Pierce und Turyn bewiesen (siehe [54] und [4]), dass für jeden r-dividierbaren binären selbstdualen Code $r = 2$ oder $r = 4$ ist.

1.1.10 Definition. Ein binärer 4-dividierbarer Code heißt *doppeltgerade*. Ein doppeltgerader Code ist immer ein selbstorthogonaler Code. Ist C ein binärer selbstorthogonaler Code, so ist C ein 2-dividierbarer Code. Wenn C binär und nicht doppeltgerade ist, so heißt C *einfachgerade*.

Ein selbstdualer und doppeltgerader Code heißt *Typ II Code*. Die selbstdualen Codes, die nicht doppeltgerade sind, nennen wir *Typ I Codes*.

Im Jahre 1971 bewies Gleason in [25] den folgenden Satz.

1.1.11 Satz. ([25], [5]) **(Gleason)** *Sei C ein binärer Code.*

1. *Ist C selbstdual, so ist das homogene Gewichtspolynom von C ein Polynom mit rationalen Koeffizienten in*

$$x^2 + y^2 \ \text{ und } \ x^8 + 14x^4y^4 + y^8, \ \text{ oder in}$$

$$x^2 + y^2 \ \text{ und } \ x^2y^2(x^2 - y^2)^2.$$

2. *Ist C selbstdual und doppeltgerade, so ist das homogene Gewichtspolynom von C ein Polynom mit rationalen Koeffizienten in*

$$x^8 + 14x^4y^4 + y^8 \text{ und } x^4y^4(x^4 - y^4)^4, \text{ oder in}$$

$$x^8 + 14x^4y^4 + y^8 \text{ und } x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}.$$

Unmittelbar folgt aus 1.1.11 das folgende Korollar

1.1.12 Korollar. (Gleason) *Ein binärer selbstdualer und doppeltgerader Code hat eine durch 8 teilbare Länge.*

1.2 Der Schatten eines Codes

Das Schatten-Konzept für binäre selbstduale Codes wurde von Conway und Sloane in [16] eingeführt, um obere Schranken für das minimale Gewicht von einfachgeraden selbstdualen Codes herzuleiten.

Im Folgenden betrachten wir ausschließlich binäre Codes C.

1.2.1 Definition. Sei C ein selbstdualer Code und sei C_0 die Menge der Codeworte von C, deren Gewicht durch 4 teilbar ist, und sei $C_2 := C \backslash C_0$. Der *Schatten von C* ist die Menge S, die aus allen Codewörtern v mit folgender Eigenschaft besteht:

$$v \cdot u = 0, \text{ für alle } u \in C_0$$

und

$$v \cdot u = 1, \text{ für alle } u \in C_2.$$

Wenn C ein Typ II Code ist, dann ist $C_2 = \emptyset$ und $S = C$. Im Allgemeinen bezeichnen wir für einen selbstdualen binären Code C die Menge

$$S := \begin{cases} C_0^{\perp} \backslash C, & \text{wenn } C \text{ einfachgerade ist} \\ C, & \text{wenn } C \text{ doppeltgerade ist} \end{cases}$$

als den Schatten von C.

1.2.2 Lemma. *Sei C ein selbstdualer einfachgerader Code und sei C_0 die Menge der Codeworte von C, deren Gewicht durch 4 teilbar ist. Dann ist C_0 der einzige lineare Untercode vom Index 2 in C.*

Beweis. Da $|\mathrm{supp}(u) \cap \mathrm{supp}(v)| \equiv u \cdot v \mod 2$ ist, ist $\varphi : C \to \mathbb{F}_2$ mit $\varphi(u) := \frac{1}{2}\mathrm{wt}(u)$ eine lineare Funktion auf C mit Kern C_0. ∎

Nach dem obigen Lemma gibt es für einen selbstdualen einfachgeraden Code C vier Untercodes C_0, C_1, C_2, C_3 so dass $C_0^{\perp} = C_0 \cup C_1 \cup C_2 \cup C_3$, wobei $C = C_0 \cup C_2$ und $S = C_1 \cup C_3$ der Schatten von C ist.

Der folgende Satz von Conway und Sloane gibt verschiedene Eigenschaften des Gewichtspolynoms des Schattens eines Typ I Codes an.

1.2.3 Satz. ([16]) **(Conway und Sloane)** *Sei S der Schatten eines selbstdualen $[n, n/2, d]$-Codes C vom Typ I.*

1. *Ist das Gewichtspolynom von C gegeben durch*

$$W_C(x,y) = \sum_{j=0}^{\lfloor n/8 \rfloor} a_j (x^2+y^2)^{\frac{n}{2}-4j} (x^2y^2(x^2-y^2)^2)^j,$$

so ist das Gewichtspolynom des Schattens

$$W_S(x,y) = \sum_{j=0}^{\lfloor n/8 \rfloor} (-1)^j a_j 2^{\frac{n}{2}-6j} (xy)^{\frac{n}{2}-4j} (x^4-y^4)^{2j}.$$

2. *Ist $W_S(x,y) = \sum_{i=0}^{n} B_i x^{n-i} y^i$ das Gewichtspolynom des Schattens, so ist:*

   (a) $B_i = B_{n-i}$ *für alle* i.

   (b) $B_i = 0$, *außer* $i \equiv \frac{n}{2} \mod 4$.

   (c) $B_0 = 0$.

   (d) $B_i \leq 1$, *für* $i < d/2$.

   (e) *höchstens ein* B_i *ungleich Null für* $i < (d+4)/2$.

1.3 Extremale Codes

Mittels Invariantentheorie haben Mallows und Sloane in [41] gezeigt, dass ein binärer selbstdualer und doppeltgerader Code der Länge n eine Minimaldistanz $d \leq 4\lfloor n/24 \rfloor + 4$ hat. Dabei bedeutet $\lfloor x \rfloor$ die größte ganze Zahl kleiner oder gleich x. Unter Ausnutzung weiterer Ideen konnte Rains in [51] zeigen, dass die obige Abschätzung auch ohne die Voraussetzung der Doppeltgeradigkeit gilt, sofern $24 \nmid n+2$.

Zusammenfassend haben wir den folgenden Satz:

1.3.1 Satz. ([41], [51]) **(Mallows-Sloane, Rains)** *Sei C ein binärer und selbstdualer $[n,k,d]$-Code. Dann gilt*

$$d \leq 4\lfloor n/24 \rfloor + 4, \text{ falls } n \not\equiv 22 \mod 24$$

und

$$d \leq 4\lfloor n/24 \rfloor + 6, \text{ falls } n \equiv 22 \mod 24.$$

1.3.2 Definition. Ein binärer selbstdualer $[n,k,d]$-Code heißt ein *extremaler Code, wenn Gleichheit in 1.3.1 gilt.*

Mallows und Sloane haben in [41] gezeigt, dass es keine extremalen Codes für große n gibt. Allerdings gaben sie keine explizite Schranke an. Ma bewies in [39], dass es keine extremalen doppeltgeraden Codes der Länge $n \geq 3984$ gibt, da der Koeffizient $A_{4m+8} < 0$ für $m = \lfloor n/24 \rfloor \geq 166$. Der größte extremale doppeltgerade Code, der konstruiert wurde, ist von der Länge $n = 136$ und ein doppeltzirkulanter Code (siehe [43], [52, Chap. 12]). Daher gibt es eine große Lücke zwischen der Schranke und was konstruiert wurde.

Extremale Codes, deren Länge durch 24 teilbar sind, sind aus geometrischer Sicht von besonderem Interesse. Rains bewies in [51], dass jeder selbstduale extremale $[24m, 12m, 4m+4]$-Code doppeltgerade ist. Der größte dieser Codes, der bekannt ist, ist der extremale doppeltgerade $[48, 24, 12]$-Code, der zu den sogenannten quadratischen Restklassen-Codes gehört. Ma bewies in [39], dass die extremalen doppeltgeraden $[24m, 12m, 4m + 4]$-Codes Länge $n = 24m \leq 3744$ haben. Ein Jahr später reduzierte Zhang [63] die Schranke bis $n \leq 3672$. Im Jahr 2002 hat Duursma [22] das gleiche Ergebnis durch einen kürzeren Beweis gezeigt. Obwohl diese Schranke groß ist, ist sie die beste, die man bis heute kennt.

1.4 Automorphismengruppen von Codes.

1.4.1 Definition. Eine G-Menge ist eine Menge X, die mit einer Gruppe G eine Verknüpfung $* : X \times G \longrightarrow X$ besitzt, für die gilt:

- $x * 1_G = x$ für alle $x \in X$, wobei 1_G das neutrale Element der Gruppe ist.
- $x * (gh) = (x * g) * h$ für alle $g, h \in G$ und alle $x \in X$.

Wir schreiben einfach xg statt $x * g$.

Ist X eine G-Menge und $x \in X$, so wird die *G-Bahn von x* definiert durch $O(x) = \{xg \mid g \in G\} \subseteq X$ und der *Stabilisator von x in G* ist die Untergruppe

$$G_x = \{g \in G \mid xg = x\} \leq G.$$

Es gilt $|O(x)| = \frac{|G|}{|G_x|}$. Weiterhin, falls $\mathrm{Fix}(g)$ die Anzahl der Elemente $x \in X$ bezeichnet, welche unter der Wirkung von $g \in G$ fixiert werden, so ist die Anzahl der $t(G)$ Bahnen nach dem Frobenius Lemma (siehe [36, 1A.6, p.7]) gleich

$$t(G) = t = \frac{1}{|G|} \sum_{g \in G} \mathrm{Fix}(g).$$

Ferner ist für $H \leq G$ *der Normalisator von H in G* definiert durch

$$N_G(H) = \{\sigma \in G \mid \sigma H \sigma^{-1} = H\}.$$

Für ein Element $\tau \in G$ der Ordnung p schreiben wir τ_p und $N_G(\tau_p)$ für $N_G(\langle \tau_p \rangle)$. Ist $|G| = p^s m$, wobei p eine Primzahl ist und p nicht m teilt, so haben die *p-Sylowuntergruppen* von G die Ordnung p^s. Für ein festes p bezeichnet $\mathrm{Syl}_p(G)$ die Menge der p-Sylowuntergruppen von G und $n_p(G) = |\mathrm{Syl}_p(G)|$ ihre Anzahl. Dann wissen wir, dass $n_p(G) = \frac{|G|}{|N_G(S)|}$ ist, wobei $S \in \mathrm{Syl}(G)$. Weiterhin ist $n_p(G) \equiv 1 \mod p$ (siehe [36, Cor. 1.17]).

Das folgende Lemma wird in Kapitel 2 benötigt.

1.4.2 Lemma. ([36, 1E.2 p. 38.]) *Sei $|G| = pqr$, wobei $p < q < r$ Primzahlen sind. Dann ist $n_r(G) = 1$.*

1.4.3 Definition. Seien $C \leq \mathbb{F}_2^n$ ein binärer Code, $\sigma \in S_n$ eine Permutation und $v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$. Wir setzen $v\sigma := (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$ und nennen die Codes $C\sigma$ und C *äquivalente Codes*.

Wir nennen σ einen *Automorphismus* von C, falls $C\sigma = C$. Die Menge $\mathrm{Aut}(C)$, die aus allen Automorphismen von C besteht, ist eine Gruppe und heißt die *Automorphismengruppe* von C.

Ein bekanntes Ergebnis ist, dass die Automorphismengruppen von zwei äquivalenten Codes konjugiert sind. Das heißt, es existiert $\rho \in S_n$ mit

$$\mathrm{Aut}(C) = \rho \mathrm{Aut}(C')\rho^{-1}. \tag{1.1}$$

Im Folgenden betrachten wir den Typ eines Automorphismus, wobei die Ordnung eine Primzahl oder die Multiplikation von zwei Primzahlen ist. Allerdings kann dies analog für mehr als zwei Primzahlen erweitert werden.

1.4.4 Definition. Sei C ein binärer Code der Länge n.

1. Sei $\sigma \in \mathrm{Aut}(C)$ der Ordnung p, wobei p eine Primzahl ist. Wir sagen, dass σ *vom Typ* p-$(c; f)$ ist, falls σ genau c p-Zyklen und f Fixpunkte hat.

2. Sei $\sigma \in \mathrm{Aut}(C)$ der Ordnung $p \cdot r$, wobei p und r Primzahlen sind. Wir sagen, dass σ *vom Typ* $p \cdot r$-$(s_1, s_2, s_3; f)$ ist, falls $n = s_1 p + s_2 r + s_3 pr + f$ und σ genau s_1 p-Zyklen, s_2 r-Zyklen, s_3 $p \cdot r$-Zyklen und f Fixpunkte hat.

Sei C ein binärer Code mit einem Automorphismus von ungerader Primzahlordnung vom Typ p-$(c; f)$. Mit $\Omega_1, \ldots, \Omega_c$ bezeichnen wir die p-Zyklen und mit $\Omega_{c+1}, \ldots, \Omega_{c+f}$ die f Fixpunkte.

Wenn $\sigma \in \mathrm{Aut}(C)$ von Ordnung p ist, so können wir ohne Beschränkung der Allgemeinheit annehmen, dass σ von der Form

$$\sigma = (1, 2, \ldots, p)(p+1, p+2, \ldots, 2p) \ldots ((c-1)p+1, (c-1)p+2, \ldots, cp) \tag{1.2}$$

ist.

1.4.5 Lemma. ([19]) *Sei C ein binärer Code der Länge n.*

1. *Falls C einen Automorphismus σ vom Typ $p \cdot r$-$(s_1, s_2, s_3; f)$ hat, wobei p und r verschiedene Primzahlen mit $n = s_1 p + s_2 r + s_3 pr + f$ sind, dann ist σ^r ein Automorphismus vom Typ p-$(s_1 + s_3 r; s_2 r + f)$ und σ^p ist ein Automorphismus vom Typ r-$(s_2 + s_3 p; s_1 p + f)$.*

2. *Falls C einen Automorphismus σ vom Typ p^2-$(s_1, s_2; f)$ hat, wobei $n = s_1 p + s_2 p^2 + f$ ist, dann ist σ^p ein Automorphismus vom Typ p-$(s_2 p; s_1 p + f)$.*

Als Folge von Lemma 1.4.5 (2) haben wir das folgende Korollar:

1.4.6 Korollar. *Sei C ein binärer Code und sei p eine feste Primzahl. Wenn für alle möglichen Automorphismen des Typs p-$(c; f)$ gilt, dass $c \not\equiv 0 \bmod p$ ist, so gibt es keinen Automorphismus der Ordnung p^2.*

Der folgende Satz, der eine Verallgemeinerung eines Ergebnisses in [9] ist, erlaubt unter bestimmten Bedingungen die p-Sylowuntergruppen von $\mathrm{Aut}(C)$ anzugeben.

1.4.7 Satz. *Sei C ein binärer Code der Länge n. Ist p-$(c; f)$ der einzige Typ für einen Automorphismus $\sigma \in \mathrm{Aut}(C)$ der Primzahlordnung p mit $c \not\equiv 0 \mod p$ und $f < p$, so ist $p^2 \nmid |\mathrm{Aut}(C)|$.*

BEWEIS. Angenommen, dass p^2 die Ordnung der Automorphismengruppe von C teilt. Dann gibt es eine abelsche Untergruppe N der Ordnung p^2. Falls $N = \langle\delta\rangle$, so ist δ ein Element von $\mathrm{Aut}(C)$ der Ordnung p^2. Da $c \not\equiv 0 \mod p$ ist, folgt nach Korollar 1.4.6, dass C keinen Automorphismus der Ordnung p^2 hat. Deshalb ist $N = \langle\sigma\rangle\langle\theta\rangle$, $\langle\sigma\rangle \cap \langle\theta\rangle = \langle 1\rangle$ und $\sigma\theta = \theta\sigma$, wobei σ und θ Automorphismen der Ordnung p sind. Da jeder Automorphismus der Ordnung p einen Typ der Form p-$(c; f)$ hat, können wir o.B.d.A. annehmen, dass

$$\sigma = \underbrace{(1, 2, \ldots, p)}_{\Omega_1}\underbrace{(p+1, p+2, \ldots, 2p)}_{\Omega_2}\ldots\underbrace{((c-1)p+1, (c-1)p+2, \ldots, cp)}_{\Omega_c}$$

ist. Wir wissen, dass

$$\sigma = \theta^{-1}\sigma\theta = (1\theta, 2\theta, \ldots, p\theta), \ldots, (((c-1)p+1)\theta, (c-1)p+2)\theta, \ldots, (cp)\theta)$$

und $\langle\theta\rangle$ auf der Menge der Zyklen $\{\Omega_1, \ldots, \Omega_c\}$ mit Bahnen der Länge p und 1 wirkt. Da $c \not\equiv 0 \mod p$ ist, gilt $\Omega_i\theta = \Omega_i$ für mindestens ein $i \in \{1, \ldots, c\}$.

Sei $\Omega_j\theta = \Omega_j = (((j-1)p+1)\theta, (j-1)p+2)\theta, \ldots, jp\theta)$. Ist $((j-1)p+1)\theta = (j-1)p+1$, so erhalten wir, dass $k\theta = k$ für $k = (j-1)p+1, (j-1)p+2, \ldots, jp$ ist, was ein Widerspruch ist, da C keinen Automorphismus der Ordnung p mit p Fixpunkten hat.

Somit ist $((j-1)p+1)\theta = t$ für einige $(j-1)p+1 < t \leq jp$ und $\Omega_j\theta = \Omega_j\sigma^{t-1}$. Dann fixiert $\theta^{-1}\sigma^{t-1}$ die Punkte $(j-1)p+1, (j-1)p+2, \ldots, jp$. Aber $\theta^{-1}\sigma^{t-1}$ hat Ordnung p, ein Widerspruch. ∎

1.4.8 Lemma. *Sei C ein binärer Code der Länge n, so dass jeder Automorphismus der Ordnung p keine Fixpunkte hat. Ist $|\mathrm{Aut}(C)| = p^a m$, so ist $a \leq max\,\{r : p^r \mid n\}$.*

BEWEIS. Angenommen, $p^a \mid |\mathrm{Aut}(C)|$ und $a > max\,\{r : p^r \mid n\}$. Dann gibt es eine Untergruppe $H \leq \mathrm{Aut}(C)$ mit $|H| = p^a$. Die Untergruppe H wirkt auf der Menge $X = \{1, \ldots, n\}$ und da alle Automorphismen $\sigma \in H$ keine Fixpunkte haben, ist $|O(x)| = p^a$ für alle Bahnen $O(x)$, $x \in X$. Somit ist $|O(x)| = p^a \mid n$, ein Widerspruch. ∎

1.4.9 Lemma. *Sei C ein binärer Code der Länge n und seien $p \neq q$ Primzahlen. Sei τ_p ein Element von $G = \mathrm{Aut}(C)$ der Ordnung p. Wir nehmen an, dass jeder Automorphismus der Ordnung p genau $f > 0$ Fixpunkte hat und jeder Automorphismus der Ordnung q keine Fixpunkte. Ist $q^s = \max\{q^l \mid 1 \leq q^l \leq f\}$, so ist $q^{s+1} \nmid |N_G(\tau_p)|$.*

BEWEIS. Angenommen $q \mid |N_G(\tau_p)|$. Dann gibt es $Q \in \mathrm{Syl}_q(N_G(\tau_p))$ mit $|Q| = q^r$ und $q^{r+1} \nmid |N_G(\tau_p)|$. Da τ_p f Fixpunkte hat, schreiben wir o.B.d.A $(x)\tau_p = x$ für $1 \leq x \leq f$. Falls $g \in Q$, dann gibt es $i \in \mathbb{Z}$, so dass $(y)g\tau_p g^{-1} = (y)\tau_p^i$ für alle $1 \leq y \leq n$. Somit ist $((x)g)\tau_p = (x)g$ für alle $1 \leq x \leq f$. Das heißt $(x)g$, ist ein Fixpunkt von τ_p und daher gilt $(x)g \in \{1, \ldots, f\}$.

Sei Q_x der Stabilisator von x in Q für $x \in \{1, \ldots, f\}$. Da alle Elemente von Q Ordnung q^r haben, haben keine Fixpunkte. Dann ist $|Q_x| = 1$ und $|O_x| = \frac{|Q|}{|Q_x|} = |Q|$. Nach Definition ist $O_x = \{xg \mid g \in Q\}$ und weiterhin $xg \in \{1, \ldots, f\}$ für alle $g \in Q$. Deswegen gilt $|Q| = |O_x| \leq f$ und damit $1 \leq q^r \leq f$. Daher erhalten wir $q^r \leq q^s$, und somit $q^{s+1} \nmid |N_G(\tau_p)|$. ∎

1.5 Selbstduale Codes mit einem Automorphismus von ungerader Primzahlordnung

Sei C ein binärer Code mit einem Automorphismus σ wie in (1.2) von ungerader Primzahlordnung vom Typ p-$(c; f)$. Seien $\Omega_1, \ldots, \Omega_c$ die p-Zyklen und $\Omega_{c+1}, \ldots, \Omega_{c+f}$ die f Fixpunkte.

Nachfolgend definieren wir zwei interessante Untercodes von C mittels eines Automorphismus σ von ungerader Primzahlordnung.

1.5.1 Definition. Sei C ein binärer $[n, k]$-Code und $\sigma \in \mathrm{Aut}(C)$. Wir setzen

$$F_\sigma(C) := \{v \in C \mid v\sigma = v\}$$

und $E_\sigma(C) := \{v \in C | \, \mathrm{wt}(v|\Omega_i) \equiv 0 \bmod 2, i = 1, \ldots, c + f\}$, wobei $v|\Omega_i$ die Einschränkung von v über Ω_i ist.

Man beachte, dass genau dann $v \in F_\sigma(C)$ ist, wenn $v \in C$ und v konstant auf den Zyklen ist.

1.5.2 Satz. ([33]) *Sei $\pi : F_\sigma(C) \to (\mathbb{F}_2)^{c+f}$, wobei $(\pi(v))_i = v_j$ für $j \in \Omega_i$ und $i = 1, \ldots, c+f$.*

1. *Ist C ein selbstdualer Code, so ist $\pi(F_\sigma(C))$ ein selbstdualer Code der Länge $n-c(p-1)$.*
2. *Ist C ein selbstdualer doppeltgerader Code und $p \equiv 1 \bmod 4$ oder $f = 0$, so ist $\pi(F_\sigma(C))$ doppeltgerade.*

1.5.3 Korollar. *Sei C ein selbstdualer doppeltgerader Code. Ist $p \equiv 1 \mod 4$ und $p \not\equiv 1 \bmod 8$, so ist c gerade.*

Beweis. Wegen 1.1.12 und 1.5.2 gilt $n - c(p-1) \equiv 0 \bmod 8$. Da $n \equiv 0 \mod 8$ und $p - 1 \not\equiv 0 \bmod 8$, ist $c \equiv 0 \mod 2$.

1.5.4 Lemma. *Sei C ein binärer $[n, k]$-Code mit einem Automorphismus σ der Ordnung p und Gewichtspolynom $W_C(y) = \sum A_i y^i$. Ist $A_i^F := |\{v \in C \mid v \in F_\sigma(C) \text{ und } \mathrm{wt}(v) = i\}|$, so ist $A_i \equiv A_i^F \bmod p$.*

Beweis. Wir wissen, dass

$$|O(v)| = \begin{cases} 1, & \text{wenn } v \in F_\sigma(C) \\ p, & \text{wenn } v \notin F_\sigma(C) \end{cases}$$

ist. Es folgt $C = F_\sigma(C) \cup C'$, wobei C' die Elemente in C sind, die nicht unter σ festbleiben. Also $A_i = A_i^F + px_i$ für geeignete $x_i \in \mathbb{N}_0$. ∎

1.5.5 Definition. Sei p eine Primzahl. Mit $s(p)$ bezeichnen wir

$$\min\{s \in \mathbb{N} \mid p \mid (2^s - 1)\}.$$

In [33] gab Huffman die folgende Zerlegung eines binären Codes mit einem Automorphismus von ungerader Primzahlordnung. Diese werden wir viele Male in dieser Arbeit verwenden. Teile der Aussage sind bereits im Satz von Maschke (1898) (siehe [1, Chap. 5, p. 116]) enthalten.

1.5.6 Lemma. ([33]) *Sei C ein $[n,k,d]$-Code und $\sigma \in \mathrm{Aut}(C)$. Dann gilt:*

1. $C = F_\sigma(C) \oplus E_\sigma(C)$.
2. *Ist C ein selbstdualer Code, so ist $\dim E_\sigma(C) = \frac{(p-1)c}{2}$. Weiterhin teilt $s(p)$ die Dimension von $E_\sigma(C)$. Insbesondere gilt: Ist C ein selbstdualer Code und 2 eine primitive Wurzel* mod p*, so ist c gerade.*

Wegen 1.5.6 können wir annehmen, dass die Erzeugermatrix von C die Gestalt

$$\mathrm{gen}(C) = \begin{pmatrix} X & Y \\ Z & 0 \end{pmatrix} \begin{matrix} \} \text{ gen } F_\sigma(C) \\ \} \text{ gen } E_\sigma(C) \end{matrix} \tag{1.3}$$

hat.

Wenn wir die Matrizen $\mathrm{gen}(F_\sigma(C))$ und $\mathrm{gen}(E_\sigma(C))$ kennen, können wir den Code C finden. Später werden wir sehen, dass wir mit Hilfe von 1.5.10 für einige Längen n alle selbstdualen $[n,k,d]$-Codes mit einem Automorphismus σ finden können.

Statt Codes als Unterräume in $\mathbb{F}_2^p$ aufzufassen, können wir diese auch als Unterräume in $R_p := \mathbb{F}_2[x]/\langle x^p - 1\rangle$ lesen, wobei wir den Vektor $v = (v_0, v_1, \ldots, v_{p-1}) \in \mathbb{F}_2^p$ mit dem Polynom $v(x) = v_0 + v_1 x + \ldots + v_{p-1}x^{p-1}$ identifizieren.

1.5.7 Lemma. ([33]) *Sei $P := \{v(x) \in R_p \mid \mathrm{wt}(v(x)) \equiv 0 \mod 2\}$.*

1. *P ist ein zyklischer Code mit $\mid P \mid = 2^{p-1}$ und Erzeugerpolynom $x - 1$.*
2. *P ist ein Unterring von $\mathbb{F}_2[x]/\langle x^p - 1\rangle$ mit Identität $e(x) = x + x^2 + \ldots + x^{p-1}$.*
3. *Ist $p \in \mathbb{P}$ und $1 + x + \ldots + x^{p-1}$ irreduzibel in $\mathbb{F}_2[x]$, so ist P ein Körper. Weiterhin ist*

$$\beta(x)p(x) \equiv xp(x) \mod (x^p - 1)$$

für $p(x) \in P$, wobei $\beta(x) := 1 + x^2 + x^3 + \ldots + x^{p-1}$ ist. Das heißt, dass die Multiplikation mit $\beta(x)$ einer zyklischen Translation in P entspricht.

Der Beweis des folgenden Lemmas ist trivial.

1.5.8 Lemma. *Sei $p \in \mathbb{P}$, so dass $1 + x + \ldots + x^{p-1}$ irreduzibel in $\mathbb{F}_2[x]$ ist und $\beta(x)$ wie in 1.5.7. Dann gilt:*

1. *$x^t e(x) \equiv \beta(x)^t \mod (x^p - 1)$ für alle $0 \le t \le p-1$ und $\mathrm{ord}(xe(x)) = \mathrm{ord}(\beta(x)) = p$.*
2. *Sind $q(x) \in P$ mit $\mathrm{ord}(q(x)) = m$ und $(p,m) = 1$, so ist $\mathrm{ord}(xq(x)) = pm$.*
3. *$H = \langle \beta(x) \rangle$ ist die einzige Untergruppe der Ordnung p in $P \backslash \{0\}$.*
4. *$\beta(x), \beta(x)^2, \ldots, \beta(x)^{p-1}$ sind die einzigen Elemente der Ordnung p in $P\backslash\{0\}$ und $H = \langle \beta(x)^i \rangle$, $i = 1, 2, \ldots, p-1$.*

Mit $E_\sigma(C)^*$ bezeichnen wir den Code, der aus $E_\sigma(C)$ durch Streichung der f Fixpunkte gewonnen wird. Weiterhin definieren wir die Abbildung

$$\varphi : E_\sigma(C)^* \to P^c$$

durch $(\varphi(v))_i = v_0 + v_1 x + \ldots + v_{p-1}x^{p-1} \in P$ für $i = 1, 2, \ldots, c$ und $v \in E_\sigma(C)^*$ mit $v|\Omega_i = (v_0, v_1, \ldots, v_{p-1})$.

$\varphi(E_\sigma(C)^*)$ ist ein P-Untermodul des P-Moduls P^c (siehe [58]). Insbesondere: Falls C ein selbstdualer Code und $1 + x + x^2 + \ldots + x^{p-1}$ irreduzibel über $\mathbb{F}_2[x]$ ist, so ist $\varphi(E_\sigma(C)^*)$ ein $[c, c/2]$-Code über dem Körper P (siehe [33]). Beachte, dass die Dimension des Codes $\varphi(E_\sigma(C)^*)$ über dem Körper P gleich $c/2$ ist. Daher muss c gerade sein, was im Einklang mit Lemma 1.5.6 (2) steht.

1.5.9 Bemerkung. Sei $w = (w_1, \ldots, w_c)$ ein Zeilenvektor von $\mathrm{gen}(\varphi(E_\sigma(C)^*))$. Ist $1 + x + x^2 + \ldots + x^{p-1}$ irreduzibel über $\mathbb{F}_2[x]$, so ist $[(\varphi^{-1}(w))_i]$ eine $(p-1) \times p$-Zirkulanten-Matrix in $\mathrm{gen}(E_\sigma(C)^*)$.

Der nächste Satz enthält notwendige und hinreichende Bedingungen um festzustellen, wann ein binärer Code mit einem Automorphismus von ungerader Ordnung selbstdual ist.

1.5.10 Satz. ([58]) **(Huffman-Yorgov)** *Sei $1+x+x^2+\ldots+x^{p-1}$ ein irreduzibles Polynom in $\mathbb{F}_2[x]$. C ist genau dann ein selbstdualer Code, wenn*

1. *$\pi(F_\sigma(C))$ selbstdual ist.*
2. *$\varphi(E_\sigma(C)^*)$ ist selbstdual über P, bezüglich des Skalarproduktes $u \cdot v := \sum_{i=0}^{c} u_i v_i^{2^{\frac{p-1}{2}}}$, wobei $u = (u_1, \ldots, u_c)$, $v = (v_1, \ldots, v_c) \in P^c$.*

Mit Hilfe von Satz 1.5.10 und Lemma 1.5.6 ist es möglich, für einige Längen n und für bestimmte Werte von p und c alle selbstdualen Codes mit einem Automorphismus σ vom Typ p-$(c; f)$ zu finden. Viele dieser Codes sind äquivalent. Der folgende Satz liefert hinreichende und notwendige Bedingungen um festzustellen, wann solche Codes äquivalent sind.

1.5.11 Satz. ([59]) **(Yorgov)** *Sei σ ein Automorphismus der selbstdualen Codes C und C^* von der gleichen Länge und vom Typ p-$(c; f)$, wie in (1.2) definiert, mit*

$$p > (c + (c^2 + 4f)^{1/2})/2.$$

Dann gilt: Die Codes C und C^* sind genau dann äquivalent, wenn der Code C^* mittels einer der folgenden Operationen aus C abgeleitet werden kann:

1. *Substitution $x \to x^t$ in $\varphi(E_\sigma(C)^*)$, wobei t eine ganze Zahl ist und $1 \le t \le p-1$.*
2. *Multiplikation der j-ten Koordinate von $\varphi(E_\sigma(C)^*)$ mit x^{t_j}, wobei t_j eine ganze Zahl ist, $0 \le t_j \le p-1$, $j = 1, 2, \ldots, c$.*
3. *Permutation der ersten c Zyklen von C.*
4. *Permutation der letzten f Koordinaten von C.*

Die folgenden Sätze bieten Hilfsmittel, um die Typen von Automorphismen von Codes zu beschreiben.

1.5.12 Satz. ([58]) *Sei C ein selbstdualer $[n, n/2, d]$-Code mit einem Automorphismus vom Typ p-$(c; f)$, wobei p eine ungerade Primzahl ist. Setzen wir*

$$g(k) := \lceil d/2^0 \rceil + \lceil d/2^1 \rceil + \ldots + \lceil d/2^{k-1} \rceil,$$

wobei $\lceil d/2^i \rceil = min\{k \in \mathbb{Z} \mid d/2^i \leq k\}$ ist, so gilt:

1. *Ist $pc \geq g((p-1)c/2)$. Falls $d \leq 2^{(p-1)c/2-2} - 2$ ist, so ist $pc > g((p-1)c/2)$.*
2. *Ist $f > c$, so gilt $f \geq g((f-c)/2)$. Falls $d \leq 2^{(f-c)/2-2} - 2$ ist, so ist $f > g((f-c)/2)$.*

1.5.13 Satz. ([11]) *Sei C ein selbstdualer Code, $\sigma \in \mathrm{Aut}(C)$ vom Typ p-$(c; f)$ und $p \geq 3$. Ist $s(p)$ gerade, so ist c gerade.*

Aus Satz 1.5.13 folgt, dass c gerade ist, falls 2 eine primitive Wurzel modulo p ist. Dies wurde bereits im Lemma 1.5.6 (2) erwähnt.

1.5.14 Satz. ([11]) *Ist C ein extremaler selbstdualer Code der Länge $24m+2r$, $0 \leq r \leq 11$, $m \geq 2$ und $\sigma \in \mathrm{Aut}(C)$ vom Typ p-$(c; f)$, wobei $p \geq 5$, so ist $c \geq f$.*

1.6 Das Balance Prinzip für den Untercode $\pi(F_\sigma(C))$

Sei $\sigma \in \mathrm{Aut}(C)$ vom Typ p-$(c; f)$ wie in (1.2). Sei π_1 der Untercode von $\pi(F_\sigma(C))$, der aus allen Codewörtern besteht, die in den ersten c Koordinaten ihren Träger haben und sei π_2 der Untercode von $\pi(F_\sigma(C))$, der aus allen Codewörtern besteht, die in den letzte f Koordinaten ihren Träger haben. Dann hat $\pi(F_\sigma(C))$ eine Erzeugermatrix von folgender Form

$$\mathrm{gen}(\pi(F_\sigma(C))) = \begin{pmatrix} A & O \\ O & B \\ D & E \end{pmatrix}, \tag{1.4}$$

wobei $(A\,O)$ eine Erzeugermatrix von π_1, $(O\,B)$ eine Erzeugermatrix von π_2 und O hierbei die Nullmatrix angemessener Größe ist. Mit dieser Bemerkung erhalten wir

1.6.1 Lemma. ([34, Chap. 9, Theorem 9.41]) *Ist $k_1 = dim(\pi_1)$ und $k_2 = dim(\pi_2)$, so gilt:*

1. *(Balance Prinzip) $k_1 - \frac{c}{2} = k_2 - \frac{f}{2}$.*
2. *$rank(D) = rank(E) = \frac{c+f}{2} - k_1 - k_2$.*
3. *Sei $\mathcal{A}$ der Code der Länge c, welcher von A erzeugt wird, $\mathcal{A}_D$ der Code der Länge c, der von den Zeilen von A und D erzeugt wird, $\mathcal{B}$ der Code der Länge f, der durch B erzeugt wird, und $\mathcal{B}_E$ der Code der Länge f, der von den Zeilen von B und E erzeugt wird. Dann ist $\mathcal{A}^\perp = \mathcal{A}_D$ und $\mathcal{B}^\perp = \mathcal{B}_E$.*

Das folgende Lemma, dessen Beweis trivial ist, wird nützlich, wenn wir mit dem Code $\mathcal{A}$ arbeiten.

1.6.2 Lemma. *Sei $\mathcal{A}$ ein binärer $[n, k]$-Code mit dualer Distanz 1. Dann gilt $\mathcal{A} = (0 \mid \mathcal{A}_1)$, wobei $\mathcal{A}_1$ ein binärer $[n-1, k]$-Code ist und $\mathcal{A}^\perp = (0 \mid \mathcal{A}_1^\perp) \cup (1 \mid \mathcal{A}_1^\perp)$.*

1.6.3 Lemma. *Sei C ein binärer selbstdualer $[n, n/2, d]$-Code und $\sigma \in \mathrm{Aut}(C)$ vom Typ p-$(c; f)$ mit $c = f < d$. Dann hat $\pi(F_\sigma(C))$ eine Erzeugermatrix der Form $(I_c \mid E')$, wobei I_c die Einheitsmatrix der Größe c und E' eine quadratische Matrix der Größe c ist*

Beweis. Wir schreiben $\mathrm{gen}(\pi(F_\sigma(C)))$ wie in (1.4). Da $c = f < d$ ist, gilt $k_2 = 0$ und dann ist $B = 0$. Andererseits gilt wegen des Balance Prinzips und $c = f$, dass $k_1 = 0$ und damit $A = 0$.

Deshalb gilt

$$\mathrm{gen}(\pi(F_\sigma(C))) = (D \mid E),$$

wobei, wegen Lemma 1.6.1 (2), $\mathrm{rank}(D) = c$ ist.
Da D eine $c \times c$ Matrix ist, ist D eine invertierbare Matrix. Deshalb ist

$$D^{-1}\mathrm{gen}(\pi(F_\sigma(C))) = (I_c \mid E')$$

eine Erzeugermatrix von $\pi(F_\sigma(C))$. ∎

Mit Hilfe des folgenden Satzes können wir bestimmte Typen eines Automorphismus von ungerader Primzahlordnung ausschließen.

1.6.4 Satz. *Sei C ein binärer selbstdualer $[n, n/2, d]$-Code. Dann hat C keinen Automorphismus vom Typ p-$(c; f)$, wobei p eine ungerade Primzahl, $c = f$ und $p + c < d$ ist.*

Beweis. Da $p+c < d$ ist, also $c < d$, folgt wegen Lemma 1.6.3, dass $\mathrm{gen}(\pi(F_\sigma(C))) = (I_c \mid E')$ ist. Sei $v_1 = (e_1|h_1)$ die erste Zeile von $(I_c \mid E')$. Wir erhalten

$$\mathrm{wt}(\pi^{-1}(v_1)) = \mathrm{wt}(\pi^{-1}(e_1|h_1)) = p + \mathrm{wt}(h_1).$$

Da $\mathrm{wt}(h_1) \leq f = c$ ist, gilt $\mathrm{wt}(\pi^{-1}(v_1)) \leq p + c < d$. Dies ist ein Widerspruch. ∎

1.7 Codes und Designs

1.7.1 Definition. Sei $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ eine Inzidenzstruktur. Wir nennen $\mathcal{D}$ ein t-(v, k, λ)-Design, wobei t, v, k, λ nicht-negative ganze Zahlen sind, falls

- $|\mathcal{P}| = v$
- Jeder Block $B \in \mathcal{B}$ inzidiert mit genau k Punkten.
- Je t verschiedene Punkte inzidieren mit genau λ Blöcken.

In unserem Fall definieren wir die Inzidenz $\mathcal{I}$ als:

$$(p, B) \in \mathcal{I} \leftrightarrow p \in B.$$

Daher ist ein t-(v, k, λ) Design $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ eine Kollektion $\mathcal{B}$ von k-elementigen Teilmengen (Blöcken) einer Menge $\mathcal{P}$ von Punkten, so dass jede t-elementige Teilmenge von P in genau λ-Blöcken enthalten ist.

1.7.2 Lemma. ([2, Chap. 1, Theorem 1.2.1]) *Sei $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ ein t-(v, k, λ) Design und $0 \leq i \leq t$. Dann ist die Anzahl λ_i der Blöcke, die mit i verschiedenen Punkten inzidieren, unabhängig von den i Punkten und wird gegeben durch*

$$\lambda_i = \lambda \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}}.$$

Insbesondere ist $\mathcal{D}$ ein i-(v, k, λ_i) Design für alle i mit $1 \leq i \leq t$.

1.7.3 Bemerkung. Ist $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ ein t-(v, k, λ) Design, so ist die Anzahl aller Blöcke

$$b := \lambda_0 = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}.$$

Wenn wir $r := \lambda_1$ setzen, dann erhalten wir den bekannte Ausdruck $bk = vr$.

1.7.4 Definition. Sei $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ ein Design, mit $|\mathcal{P}| = v$ und $|\mathcal{B}| = b$.

1. Wenn wir die Punkte $\{p_1, p_2, \ldots, p_v\}$ und die Blöcke $\{B_1, B_2, \ldots, B_b\}$ numerieren, so wird die Inzidenzmatrix von $\mathcal{D}$ als eine $b \times v$ Matrix $A = (a_{ij})$ definiert durch:

$$a_{ij} = \begin{cases} 1, & \text{wenn } (p_j, B_i) \in \mathcal{I} \\ 0, & \text{wenn } (p_j, B_i) \notin \mathcal{I}. \end{cases}$$

2. Der Code $C(\mathcal{D})$ über $\mathbb{F}_2$, der durch die Zeilen der Inzidenzmatrix erzeugt wird, heißt *Code zum Design* $\mathcal{D} = (\mathcal{P}, \mathcal{B})$. Seine Dimension ist der 2-rank vom $\mathcal{D}$.

Obwohl es verschiedene Inzidenzmatrizen für ein Design gibt, sind die Codes, die durch sie erzeugt werden, äquivalent.

1.7.5 Definition. ([55], [42]) Sei $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ ein t-(v, k, λ) Design.

1. Wir nennen
$$R := \{0 \leq i < k \mid \exists\, B, B' \in \mathcal{B},\ B \neq B',\ |B \cap B'| = i\}$$
die Block-Schnittzahlen vom Design $\mathcal{D}$.

   Wenn $i \equiv k \bmod 2$ für alle $i \in R$ gilt, sagen wir, dass $\mathcal{D}$ ein selbstorthogonales Design ist.

2. Wenn $S \subseteq \mathcal{P}$ eine s-elementige Teilmenge ist, definiert man die Schnittzahlen von S in $\mathcal{D}$ als
$$n_i^S := |\{B \in \mathcal{B} \mid |B \cap S| = i\}|, \text{ für } 0 \leq i \leq s.$$
   Insbesondere, wenn $S \in \mathcal{B}$ ist, das heißt, wenn S ein Block ist, so ist n_i^S die Anzahl der verschiedenen Blöcke ungleich S, die in i Punkten zusammentreffen.

Im Jahr 1971 bewies Mendelsohn [42] das folgende Egebnis. Es beschreibt einen wichtigen Zusammenhang zwischen den Schnittzahlen einer Teilmenge $S \subseteq \mathcal{P}$ untereinander:

1.7.6 Satz. ([42], [7]) **(Mendelsohn)** *Sei $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ ein t-(v, k, λ) Design und sei $S \subseteq \mathcal{P}$ mit $|S| = s$. Dann gilt für $j = 0, 1, \ldots, t$:*

$$\sum_{i=j}^{s} \binom{i}{j} n_i^S = \binom{s}{j} \lambda_j.$$

Der folgende berühmte Satz zeigt eine interessante Beziehung zwischen Codierungstheorie und Designtheorie.

1.7.7 Satz. ([3], [2, Chap. 2, Theorem 2.11.2]) **(Assmus-Mattson)** *Sei C ein binärer Code mit Minimaldistanz d und Minimaldistanz $d^\perp$ von $C^\perp$. Angenommen, es gibt ein $t \in \mathbb{N}$ mit $0 < t < d$, so dass für*

$$A_{C^\perp}(1, y) = \sum_{i=0}^{n} A_i y^i$$

höchstens $d - t$ Koeffizienten von $A_1, A_2, \ldots, A_{n-t}$ ungleich Null sind. Dann bilden für alle i mit $d \leq i \leq n$ die Träger der Vektoren vom Gewicht i in C ein t-Design. In ähnlicher Weise bilden für alle j mit $d^\perp \leq j \leq n - t$ die Träger der Vektoren vom Gewicht j in $C^\perp$ ein t-Design.

Kapitel 2

Selbstduale $[96, 48, 20]$-Codes

2.1 Über die Ordnung der Automorphismengruppe eines selbstdualen $[96, 48, 20]$-Codes

Extremale Codes, deren Länge durch 24 teilbar ist, sind aus geometrischer Sicht von besonderem Interesse, da die Codeworte von einem festen Gewicht ungleich 0 nach Assmus und Mattson [3] ein 5-Design bilden. Trotzdem kennt man nur zwei Beispiele, den $[24, 12, 8]$-Golay-Code und einen $[48, 24, 12]$-Code, die zu den sogenannten quadratischen Restklassen-Codes gehören. Nicht-triviale Automorphismen können hilfreich sein, um die Existenz von Codes größerer Länge zu untersuchen.

Die Existenz extremaler Codes ist eine der zentralen Fragen der Codierungstheorie. Bereits 1972 hat Sloane in [53] die Frage nach der Existenz eines extremalen Codes der Länge 72 gestellt. Sie ist trotz vieler Anstrengungen bis heute offen. Unter bestimmten Voraussetzungen können wir nach Lemma 1.5.6 (1) einen selbstdualen binären Code mit einem Automorphismus von ungerader Ordnung konstruieren.

In [14], [47], [35], [50] und [24] wurde bewiesen, dass für einen selbstdualen $[72, 36, 16]$-Code C als ungerade Primzahlen in der Ordnung der Automorphismengruppe nur 3 und 5 vorkommen können. Auf gleiche Weise wurde in [61] und [17] bewiesen, dass für einen selbstdualen $[96, 48, 20]$-Code C nur 3 und 5 vorkommen können. Im Detail wissen wir

Code	Existenz	$G = \mathrm{Aut}(C)$	(mögliche) Primzahlen in $\lvert G\rvert$	Referenz
[24,12,8]	ext. Golay	M_{24}	2,3,5,7,11,23	[45], [40]
[48,24,12]	ext. QR	$\mathrm{PSL}(2, 47)$	2,3,23,47	[32], [38], [33]
[72,36,16]	?	$\lvert G\rvert \leq 24$	2,3,5	[60], [8], [13], [24]
[96,48,20]	?	Keine bekannte Schranke für $\lvert G\rvert$	2,3,5	[61], [17], [8]

Mit Blick auf die Tabelle ist es natürlich, die folgenden Fragen zu stellen:

2.1.1 Fragen. Angenommen, ein selbstdualer $[96, 48, 20]$-Code C existiert. Ist die Automorphismengruppe auflösbar? Ist es möglich, eine obere Schranke für die Ordnung der Automorphismengruppe zu finden?

Ziel dieses Kapitels ist, eine Antwort auf diese Fragen zu geben. Unserer wichtigstes Resultat in dieser Hinsicht ist das folgende:

2.1.2 Hauptsatz. *Sei C ein extremaler Code der Länge 96.*

1. *Falls σ ein Automorphismus von C der Primzahlordnung p ist, dann ist seine Zyklen-Struktur gegeben durch*

p	*Anzahl der p-Zyklen*	*Anzahl der Fixpunkte*
2	48	0
3	$30, 32$	$6, 0$
5	18	6

2. *Ist σ ein Automorphismus von C von ungerader zusammengesetzter Ordnung r, so ist $r = 9, 15$ oder 45 und seine Zyklen-Struktur ist 9-$(0, 10; 6)$, 9-$(1, 10; 3)$, 9-$(2, 10; 0)$, $3 \cdot 5$-$(0, 0, 6; 6)$, $3 \cdot 5$-$(2, 0, 6; 0)$, $3^2 \cdot 5$-$(0, 0, 0, 2; 6)$, $3^2 \cdot 5$-$(1, 0, 0, 2; 3)$ oder $3^2 \cdot 5$-$(2, 0, 0, 2; 0)$.*

3. *Falls alle Automorphismen der Ordnung 3 keine Fixpunkte haben, so ist die Automorphismengruppe auflösbar oder die Automorphismengruppe ist die einfache Gruppe A_5. Insbesondere ist $|\mathrm{Aut}(C)| \leq 480$. Weiterhin können die Fälle $|\mathrm{Aut}(C)| = 20$ oder $|\mathrm{Aut}(C)| = 40$ nicht auftreten.*

2.1.1 Typen von Automorphismen

In [61], [17] und [8] wurde bewiesen, dass für einen $[96, 48, 20]$-Code C als Primzahlen in der Ordnung der Automorphismengruppe nur 2, 3 und 5 vorkommen können und die Automorphismen folgende Zyklen-Struktur haben.

p	Anzahl der p-Zyklen	Anzahl der Fixpunkte
2	48	0
3	$24, 26, 30, 32$	$24, 18, 6, 0$
5	$16, 18$	$16, 6$

Wir werden in diesem Abschnitt die Möglichkeiten der Zyklen-Struktur reduzieren, das heißt, einige Typen für Automorphismen der Ordnung 3 und 5 ausschließen und im folgenden Abschnitt die Automorphismengruppe untersuchen.

2.1.3 Lemma. *Sei C ein selbstdualer $[96, 48, 20]$-Code. Dann hat C keinen Automorphismus der Ordnung 3 vom Typ 3-$(24; 24)$.*

Beweis. Angenommen $\sigma \in \mathrm{Aut}(C)$ ist vom Typ 3-$(24; 24)$. Wir betrachten eine Erzeugermatrix für den selbstdualen Code $\pi(F_\sigma(C))$ in Form von (1.4). Da $c = f$ ist, erhalten wir $k_1 = k_2$ nach dem Balance Prinzip (siehe Lemma 1.6.1 (1)). Weiterhin ist $\mathcal{B}$ ein doppeltgerader $[24, k_2, d']$-Code mit $d' = 20$ oder $d' = 24$.

Falls $k_2 \geq 2$ ist, so enthält offenbar $\pi(F_\sigma(C))$ und deshalb auch C einen Vektor mit Gewicht kleiner oder gleich 8, ein Widerspruch. Deswegen ist $k_1 = k_2 \leq 1$.

Wenn $k_2 = k_1 = 0$ ist, ist D nach Lemma 1.6.1 (2) eine invertierbare Matrix. Deshalb erhalten wir

$$\mathrm{gen}(\pi(F_\sigma(C))) = (I_{24} \mid E).$$

Sei $(e_i \mid v_i)$ die i-te Zeile von E für $i = 1, \ldots, 24$. Da $\mathrm{wt}(\pi^{-1}(e_i \mid v_i)) = 3 + \mathrm{wt}(v_i) \geq 20$ ist, gilt dann $\mathrm{wt}(v_i) = 17$ oder 21. Falls $\mathrm{wt}(v_i) = 17$ und $\mathrm{wt}(v_j) = 21$, so gilt

$$S_{v_i,v_j} = |\operatorname{supp}(v_i) \cap \operatorname{supp}(v_j)| \geq 14,$$

und deshalb $\mathrm{wt}(\pi^{-1}(e_i + e_j \mid v_i + v_j)) = 6 + \mathrm{wt}(v_i + v_j) \leq 16$, ein Widerspruch.

Wenn beide $\mathrm{wt}(v_i) = 21$ und $\mathrm{wt}(v_j) = 21$ sind, so ist

$$S_{v_i,v_j} = |\operatorname{supp}(v_i) \cap \operatorname{supp}(v_j)| \geq 18.$$

Somit gilt $\mathrm{wt}(\pi^{-1}(e_i + e_j \mid v_i + v_j)) = 6 + \mathrm{wt}(v_i + v_j) \leq 12$, abermals ein Widerspruch.

Deshalb gilt $\mathrm{wt}(v_i) = 17$ für alle $i = 1, \ldots, 24$. Offensichtlich ist $S_{v_i,v_j} \geq 10$ und $v_i \neq v_j$ für $i \neq j$. Auf der anderen Seite erhalten wir für $x = (e_i \mid v_i)$ und $y = (e_j \mid v_j)$, dass $S_{x,y} = S_{v_i,v_j}$, und Lemma 1.1.2 führt zu $S_{x,y} \leq 10$. Somit ist $S_{v_i,v_j} = 10$ für alle $i \neq j$ mit $i, j \in \{1, \ldots, 24\}$. Insbesondere haben die Vektoren $v_i \neq v_j$ keine gleiche 0-Koordinate. Deshalb ist die Dimension von $\mathrm{gen}(\pi(F_\sigma(C)))$ höchstens 3, ein Widerspruch.

Falls $k_2 = 1$, so hat $\pi(F_\sigma(C))$ eine Erzeugermatrix der Form

$$\begin{pmatrix} a & 0 \ldots 0 \\ 0 \ldots 0 & b \\ D & E \end{pmatrix},$$

wobei $\mathrm{wt}(b) = 20$ oder 24. Da C doppeltgerade ist, gilt $\mathrm{wt}(a) \in \{8, 12, 16, 20, 24\}$. Angenommen, $\mathrm{wt}(a) = 24$, das heißt, a ist der Vektor der Länge 24 mit ausschließlich 1-Einträgen. Also gibt es $z \in \mathcal{A}^\perp$ mit $\mathrm{wt}(z) = 2$ und $(z \mid u) \in \pi(F_\sigma(C))$ mit $\mathrm{wt}(u) \geq 14$. Ist $\mathrm{wt}(b) = 24$, so folgt

$$\mathrm{wt}(\pi^{-1}((z \mid u) + (0 \mid b))) \leq 6 + 10 = 16,$$

ein Widerspruch. Somit ist $\mathrm{wt}(b) = 20$. Wenn $\mathbf{1}$ der Vektor der Länge 96 mit ausschließlich 1-Einträgen ist, erhalten wir

$$\mathrm{wt}(\pi^{-1}(a \mid b) + \mathbf{1}) \leq 4,$$

ebenfalls ein Widerspruch. Damit ist $\mathrm{wt}(a) \leq 20$. Daher muss der Vektor a mindestens vier Nullen enthalten. Somit gibt es mindestens vier Vektoren der Form $z_i = (0, 0, \ldots, 1, \ldots, 0, 0) \in \mathbb{F}_2^{24}$, die orthogonal zu a sind. Nach Lemma 1.6.1 (3) erhalten wir wieder $z_i \in \mathcal{A}^\perp = \mathcal{A}_D$. Der Widerspruch folgt nun wie im Fall $k_2 = 0$. ∎

2.1.4 Lemma. *Sei C ein selbstdualer $[96, 48, 20]$-Code. Dann hat C keinen Automorphismus der Ordnung 3 vom Typ 3-$(26; 18)$.*

Beweis. Sei $\sigma \in \mathrm{Aut}(C)$ vom Typ 3-$(26; 18)$. Wir betrachten wieder eine Erzeugermatrix von $\pi(F_\sigma(C))$ der Form (1.4). Da $f = 18 < 20$ ist, erhalten wir $k_2 = 0$ und wegen des Balance Prinzips (siehe Lemma 1.6.1) ist $k_1 = 4$. Deshalb hat $\pi(F_\sigma(C))$ eine Erzeugermatrix der Form

$$\begin{pmatrix} A & 0 \\ D & E \end{pmatrix}.$$

Man beachte, dass $\mathcal{A}$ ein doppeltgerader $[26, 4, d^*]$-Code mit $d^* \geq 8$ ist. Weiterhin zeigt die Tabelle [27], dass die duale Distanz $(d^*)^\perp$ von $\mathcal{A}$ entweder 1 oder 2 ist.

Zunächst betrachten wir den Fall $(d^*)^\perp = 1$. Wir beobachten, dass es keine zwei Codewörter $a_1, a_2 \in \mathcal{A}^\perp$ beide mit Gewicht 1 gibt. Falls doch, so ist $(a_i \,|\, b_i) \in \pi(F_\sigma(C))$ mit $\mathrm{wt}(b_i) = 17$. Es folgt

$$0 \neq c = \pi^{-1}(a_1 + a_2 \,|\, b_1 + b_2) \in C$$

mit $\mathrm{wt}(c) \leq 8$, ein Widerspruch.
Somit enthält A eine Null-Spalte, wenn die duale Distanz $(d^*)^\perp = 1$ ist. Wenn diese Spalte entfernt wird, erhalten wir einen doppeltgeraden $[25, 4, \geq 8]$-Code A' mit dualer Distanz von mindestens 2. $A'^\perp$ hat Länge 25 und Dimension 21. Die Tabelle in [27] zeigt, dass seine Minimaldistanz höchstens 2 beträgt. Deshalb enthält $\mathcal{A}^\perp$ Codewörter des Gewichts 2.

Nun wählen wir $a_i \in \mathcal{A}^\perp$ vom Gewicht i für $i = 1, 2$. Somit gibt es Vektoren $(a_i \,|\, b_i) \in \pi(F_\sigma(C))$ mit $\mathrm{wt}(b_1) = 17$ und $\mathrm{wt}(b_2) = 14$ oder 18. Folglich ist

$$\mathrm{wt}(\pi^{-1}(a_1 + a_2 \,|\, b_1 + b_2)) \leq 9 + 5 < 20,$$

ein Widerspruch.

Nun sei $(d^*)^\perp = 2$. Angenommen $a_1, a_2 \in \mathcal{A}^\perp$, mit $a_1 \neq a_2$ und $\mathrm{wt}(a_1) = \mathrm{wt}(a_2) = 2$. Daher gibt es Vektoren $(a_i \,|\, b_i) \in \pi(F_\sigma(C))$ mit $\mathrm{wt}(b_i) = 14$ oder 18 für $i = 1, 2$. Insbesondere ist $\mathrm{wt}(b_1 + b_2) \leq 8$. Falls $\mathrm{wt}(a_1 + a_2) = 2$, so gilt

$$\mathrm{wt}(\pi^{-1}(a_1 + a_2 \,|\, b_1 + b_2)) = 6 + \mathrm{wt}(b_1 + b_2) \leq 6 + 8 < 20,$$

ein Widerspruch. Somit ist $\mathrm{wt}(a_1 + a_2) = 4$. Da

$$\mathrm{wt}(\pi^{-1}(a_1 + a_2 \,|\, b_1 + b_2)) = 12 + \mathrm{wt}(b_1 + b_2) \geq 20,$$

erhalten wir $\mathrm{wt}(b_1 + b_2) = 8$ und $\mathrm{wt}(b_i) = 14$ für $i = 1, 2$.
Es gibt höchstens vier Vektoren b_i, die diese Bedingungen erfüllen. Deshalb gibt es höchstens vier Vektoren $a_i \in \mathcal{A}^\perp$ mit $\mathrm{wt}(a_i) = 2$.

Bezeichne die exakte Anzahl mit $s \leq 4$. Als Nächstes punktieren wir den Code $\mathcal{A}$ unter dem Träger des Vektors $a_1 + \ldots + a_s$. Wir erhalten entweder einen $[26 - 2s, 4, \geq 2]$-Code oder einen $[18, 3, \geq 2]$-Code (falls $s = 4$ und $a_1 + \ldots + a_s \in \mathcal{A}$ ist). Nennen wir diesen Code $\mathcal{A}'$. Sei $0 \neq v \in \mathcal{A}'^\perp$. Wenn $\mathrm{wt}(v) = 1$ ist, dann können wir Nullen an die Stellen von $\mathrm{supp}(a_1 + \ldots + a_s)$ einfügen, um einen Vektor des Gewichts 1 in $\mathcal{A}^\perp$ zu bekommen, ein Widerspruch. Wenn $\mathrm{wt}(v) = 2$ ist, dann führt dieselbe Konstruktion zu einem Vektor des Gewichts 2 in $\mathcal{A}^\perp$ ungleich a_i für $i = 1, \ldots, s$, ein erneuter Widerspruch. Dies zeigt, dass die minimale Distanz von $\mathcal{A}'^\perp$ mindestens 3 ist. Auf der anderen Seite zeigt die Tabelle [27], dass die minimale Distanz irgendeines $[26 - 2s, 22 - 2s]$-Codes für $s = 1, \ldots, 4$ und irgendeines $[18, 15]$-Codes höchstens 2 ist, was den Beweis vervollständigt. ∎

2.1.5 Lemma. *Sei C ein selbstdualer $[96, 48, 20]$-Code. Dann hat C keinen Automorphismus der Ordnung 5 vom Typ 5-$(16; 16)$.*

Beweis. Man beachte, dass $p = 5 \equiv 1 \bmod 4$ ist. Somit ist nach 1.5.2 (2) der Vektorraum $\pi(F_\sigma(C))$ ein selbstdualer doppeltgerader $[32, 16, d_\pi]$-Code. Darüber hinaus ist $c = f = 16 < d$. Nach Lemma 1.6.3 hat $\pi(F_\sigma(C))$ eine Erzeugermatrix der Form

$$\mathrm{gen}(\pi(F_\sigma(C))) = (I_{16} \mid E').$$

Falls $x = (1, 0, 0, \ldots, 0 \mid x')$ und $y = (0, 1, 0, \ldots, 0 \mid y')$ die erste bzw. die zweite Zeile von $(I_{16} \mid E')$ bezeichnen, so ist

$$\mathrm{wt}(\pi^{-1}(x)) = \mathrm{wt}(\pi^{-1}(1, 0, 0, \ldots, 0 \mid x')) = 5 + \mathrm{wt}(x') \geq 20.$$

Deshalb ist $15 \leq \mathrm{wt}(x') \leq 16$. Da C und $\pi(F_\sigma(C))$ doppeltgerade sind, erhalten wir $\mathrm{wt}(x') = 15$. Ebenso gilt $\mathrm{wt}(y') = 15$. Dann ist $\mathrm{wt}(x' + y') \leq 2$ und somit

$$\mathrm{wt}(\pi^{-1}(x + y)) = \mathrm{wt}(\pi^{-1}(1, 1, 0, \ldots, 0 \mid x' + y')) = 2 \cdot 5 + \mathrm{wt}(x' + y') \leq 12,$$

ein Widerspruch. ∎

Wegen den vorherigen Ergebnissen gilt der folgende Satz

2.1.6 Satz. *Sei C ein extremaler Code der Länge 96. Dann hat ein Automorphismus von C der Ordnung 3 keine oder 6 Fixpunkte und einen Automorphismus der Ordnung 5 genau 6.*

2.1.7 Bemerkung. Sei C ein selbstdualer $[96, 48, 20]$-Code und sei $\sigma \in \mathrm{Aut}(C)$ vom Typ 3-$(30; 6)$. Dann ist $\pi(F_\sigma(C))$ ein selbstdualer $[36, 18, d_\pi]$-Code. Nach Satz 1.3.1 haben wir $d_\pi \leq 8$. Wenn wir $d_\pi = x + y$ schreiben, wobei x die Anzahl der Einsen in den ersten c Koordinaten eines Vektors mit minimalem Gewicht ist und y die Anzahl der Einsen in den letzten Koordinaten, so ist $x + y \leq 8$ und $3x + y \geq 20$. Dies erzwingt $x \geq 6$, $y = 0$ und $d_\pi = 8$. Deswegen ist $\pi(F_\sigma(C))$ ein selbstdualer $[36, 18, 8]$-Code. Nach [16] gibt es zwei mögliche Gewichtspolynome für $\pi(F_\sigma(C))$:

$$W_{36,1}(y) = 1 + 225y^8 + 2016y^{10} + \ldots$$

und

$$W_{36,2}(y) = 1 + 289y^8 + 1632y^{10} + \ldots$$

Wir betrachten eine Erzeugermatrix für $\pi(F_\sigma(C))$ der Form (1.4). Da $f = 6 < 20$ ist, gilt dann $k_2 = 0$. Nach dem Balance Prinzip, haben wir $k_1 = 12$. Dann hat $\pi(F_\sigma(C))$ eine Erzeugermatrix der Form

$$\begin{pmatrix} A & 0 \\ D & E \end{pmatrix}.$$

Beachte, dass $\mathcal{A}$ ein doppeltgerader $[30, 12, d^*]$ mit $d^* = 8$ oder $d^* = 12$ ist. Wenn die duale Distanz $(d^*)^\perp \leq 4$ wäre, dann gilt $\mathrm{wt}(\pi^{-1}(a|b)) \leq 12 + \mathrm{wt}(b) \leq 12 + 6 < 20$ für einen Vektor $(a|b) \in \pi(F_\sigma(C))$, ein Widerspruch. Deswegen $(d^*)^\perp \geq 5$. Auf der anderen Seite zeigt die Tabelle [27], dass die minimale Distanz irgendeines $[30, 18]$-Codes höchstens 6 ist. Daher ist $(d^*)^\perp = 5$ oder 6. Man kann zeigen, dass $(d^*)^\perp = 5$ und

$$W_{\mathcal{A}}(y) = 1 + 75y^8 + 1360y^{12} + 2175y^{16} + 480y^{20} + 5y^{24},$$

$$W_{\mathcal{A}^\perp}(y) = 1 + 36y^5 + 155y^6 + 600y^7 + 1425y^8 + 2580y^9 + \ldots$$

ist.

Sei $\sum A_i^F y^i$ und $\sum A_i^\pi y^i$ das Gewichtspolynom von $F_\sigma(C)$ und $\pi(F_\sigma(C))$. Andererseits sei $T := \{T_1, T_2\}$ eine Partition von $S := \{1, \ldots, 36\}$, wobei $T_1 = \{1, \ldots, 30\}$ und $T_2 =$

$\{31,\ldots,36\}$ ist. Sei $((A_{\mathbf{i}}(T)))_{\mathbf{i}\in W(T)}$ die Split-Gewichtsverteilung des Codes $\pi(F_\sigma(C))$, wobei, wie in der Definition 1.1.7, $A_{\mathbf{i}} = A_{(x,y)} := |\{(v|u) \in \pi(F_\sigma(C)) \mid \mathrm{wt}(v) = x \text{ und } \mathrm{wt}(u) = y\}|$ ist.

Dann ist $A^F_{20} = A_{(5,5)} + A_{(6,2)}$ und $A^\pi_8 = A_{(6,2)} + A_{(8,0)}$. Deshalb ist

$$A^F_{20} = A_{(5,5)} + (A^\pi_8 - A_{(8,0)}) = \begin{cases} 36 + (225 - 75) = 186 \equiv 0 \mod 3 \\ 36 + (289 - 75) = 250 \equiv 1 \mod 3. \end{cases}$$

Nach Lemma 1.5.4 gilt $A_{20} \equiv A^F_{20} \mod 3$ und da $A_{20} = 3217056 \equiv 0 \mod 3$ ist (siehe [41]), ist $W_{36,1}$ das Gewichtspolynom von $\pi(F_\sigma(C))$. Daher ist $A^F_{20} = 186$ und der Untercode $F_\sigma(C)$ hat

$$W_{F_\sigma(C)}(y) = 186y^{20}+680y^{24}+2730y^{28}+8040y^{32}+18640y^{36}+30600y^{40}+11160y^{44}+49295y^{48}+\ldots$$

als Gewichtspolynom, was in Einklang mit Lemma 1.5.4 steht.

2.1.8 Lemma. *Sei C ein selbstdualer $[96, 48, 20]$-Code und sei p eine ungerade Primzahl. Falls σ ein Automorphismus vom Typ p^2-$(s_1, s_2; f)$ ist, so ist $p = 3$ und seine Zyklen-Struktur wird gegeben durch 9-$(0, 10; 6)$, 9-$(1, 10; 3)$ oder 9-$(2, 10; 0)$.*

Beweis. Nach dem Korollar 1.4.6 gibt es keinen Automorphismus der Ordnung 25, da jeder Automorphismus der Ordnung 5 einen Typ der Form 5-$(18; 6)$ hat. Deshalb ist $p = 3$ und σ^3 ein Automorphismus vom Typ 3-$(3s_2; 3s_1 + f)$, nach Lemma 1.4.5. Somit ist $(3s_2, 3s_1 + f) \in \{(30, 6), (32, 0)\}$. Dann ist $3s_2 = 30$ und $3s_1 + f = 6$. Da $s_1 \in \{0, 1, 2\}$ ist, erhalten wir die behauptete Zyklen-Struktur. ∎

2.1.9 Lemma. *Ist C ein selbstdualer $[96, 48, 20]$-Code, so hat C keinen Automorphismus der Ordnung 27.*

Beweis. Sei σ ein Automorphismus der Ordnung 3^3 vom Typ 3^3-$(s_1, s_2, s_3; f)$, wobei $3s_1 + 9s_2 + 27s_3 + f = 96$ ist. Dann hat σ^3 den Typ 3^2-$(3s_2, 3s_3; 3s_1 + f)$ und nach Lemma 2.1.8 wissen wir, dass $(3s_2, 3s_3, 3s_1 + f)$ ein Element von $\{(0, 10, 6), (1, 10, 3), (2, 10, 0)\}$ ist. Dafür gibt es aber keine ganzzahligen Lösungen. ∎

2.1.10 Lemma. *Ist σ ein Automorphismus der Ordnung $3{\cdot}5$, so hat σ den Typ $3{\cdot}5$-$(0, 0, 6; 6)$ oder $3 \cdot 5$-$(2, 0, 6; 0)$.*

Beweis. Sei σ ein Automorphismus vom Typ $3{\cdot}5$-$(s_1, s_2, s_3; f)$, wobei $3s_1+5s_2+15s_3+f = 96$ ist. Dann gibt es einen Automorphismus vom Typ 3-$(s_1+5s_3, 5s_2+f)$ und 5-$(s_2+3s_3; 3s_1+f)$. Dann ist $(s_1 + 5s_3, 5s_2 + f) \in \{(30, 6), (32, 0)\}$ und $(s_2 + 3s_3; 3s_1 + f) \in \{(18, 6)\}$. Somit hat σ den Typ $3 \cdot 5$-$(0, 0, 6; 6)$ oder $3 \cdot 5$-$(2, 0, 6; 0)$. ∎

2.1.11 Lemma. *Ist σ ein Automorphismus der Ordnung $3^2 \cdot 5$, so hat σ den Typ $3^2 \cdot 5$-$(0, 0, 0, 2; 6)$, $3^2 \cdot 5$-$(1, 0, 0, 2; 3)$ oder $3^2 \cdot 5$-$(2, 0, 0, 2; 0)$.*

Beweis. Sei σ ein Automorphismus vom Typ $3^2 \cdot 5$-$(s_1, s_2, s_3, s_4, s_5; f)$, wobei $96 = 3s_1 + 5s_2 + 9s_3 + 15s_4 + 45s_5 + f$ ist. Dann hat σ^3 Typ $3 \cdot 5$-$(3s_2, s_3 + 3s_4, 3s_5; 3s_1 + f)$. Nach dem Lemma 2.1.10, wissen wir, dass $(3s_2, s_3 + 3s_4, 3s_5, 3s_1 + f) \in \{(0, 0, 6, 6), (2, 0, 6, 0)\}$ ist. Es folgt die Behauptung. ∎

Zusammenfassend haben wir den folgenden Satz bewiesen:

2.1.12 Satz. *Sei C ein extremaler Code der Länge 96.*

1. *Ist σ ein Automorphismus von C von ungerader zusammengesetzter Ordnung r, so ist $r = 9, 15$ oder 45 und seine Zyklen-Struktur ist 9-$(0, 10; 6)$, 9-$(1, 10; 3)$, 9-$(2, 10; 0)$, $3 \cdot 5$-$(0, 0, 6; 6)$, $3 \cdot 5$-$(2, 0, 6; 0)$, $3^2 \cdot 5$-$(0, 0, 0, 2; 6)$, $3^2 \cdot 5$-$(1, 0, 0, 2; 3)$ oder $3^2 \cdot 5$-$(2, 0, 0, 2; 0)$.*

2. *Falls alle Automorphismen von C der Ordnung 3 keine Fixpunkte haben, so gibt es keine Automorphismen ungerader Ordnung größer als 5 ungleich 15.*

2.1.2 Die Struktur der Automorphismengruppe

In diesem Abschnitt wird die Struktur der Automorphismengruppe eines selbstdualen doppeltgeraden $[96, 48, 20]$-Codes unter der Annahme untersucht, dass jeder Automorphismus der Ordnung 3 keine Fixpunkte hat. Diese Annahme ist berechtigt, da für $n = 48, 72, 120$ ein Element der Ordnung 3 fixpunktfrei operiert (siehe [33], [9] und Satz 3.1.10).

Im Folgenden sei C ein selbstdualer $[96, 48, 20]$-Code, G seine Automorphismengruppe und alle Elemente $\sigma \in G$ der Primzahlordnung seien vom Typ 2-$(48; 0)$, 3-$(32; 0)$ oder 5-$(18; 6)$. Also ist $|G| = 2^a 3^b 5^c$, wobei $a, b, c \geq 0$. Nach Satz 1.4.7 ist $3^2 \nmid |\mathrm{Aut}(C)|$ und somit $b \in \{0, 1\}$. Weiterhin gilt nach Lemma 1.4.8, dass $a \in \{0, \ldots, 5\}$.

2.1.13 Lemma. *Ist $|G| = 2^a 3^b 5$, mit $0 \leq a \leq 5$, $b \in \{0, 1\}$, so ist $|O(x)| = 2^a 3^b 5$ oder $|O(x)| = 2^a 3^b$ für alle $x \in \{1, \ldots, 96\}$.*

Beweis. Da die nicht-trivialen Automorphismen mit Fixpunkten Ordnung 5 haben, ist $|G_x| = 1$ oder 5. Wir wissen, dass $|O(x)| = \frac{|G|}{|G_x|}$ ist. Daher folgt die Behauptung. ∎

2.1.14 Lemma. *Die Ordnung von G teilt $2^a 3^b 5^c$, wobei $a \in \{0, 1, \ldots, 5\}$ und $b, c \in \{0, 1\}$ ist.*

Beweis. Wir wissen bereits $a \in \{0, 1, \ldots, 5\}$ und $b \in \{0, 1\}$. Um $c \leq 1$ zu beweisen, nehmen wir an, dass $5 \mid |G| = 2^a 3^b 5^c$. Zur Berechnung der Anzahl der t Bahnen der Wirkung von G auf den 96 Koordinaten von C verwenden wir das Cauchy-Frobenius Lemma. Nach Satz 2.1.12 (2) gibt es nur Automorphismen, deren Ordnung 3, 5, 15 oder gerade ist. Somit haben, abgesehen von der Identität, nur Elemente der Ordnung 5 Fixpunkte. Daher ist

$$\mathrm{Fix}(g) = \begin{cases} 0, & \text{wenn } \mathrm{ord}(g) \text{ gerade ist;} \\ 0, & \text{wenn } \mathrm{ord}(g) = 3, 15 \text{ ist;} \\ 6, & \text{wenn } \mathrm{ord}(g) = 5 \text{ ist.} \end{cases}$$

Dann gilt

$$\begin{aligned} t &= \tfrac{1}{2^a 3^b 5^c} \left(96 + \textstyle\sum_{\mathrm{ord}(g)=5} 6\right) \\ &= \tfrac{1}{2^a 3^b 5^c} \left(6 \cdot 16 + 6y\right), \end{aligned}$$

wobei $y \in \mathbb{N}_0$. Falls $G_5 = \{g \in G \mid g^5 = 1\}$ und $|G|_5 = 5^c$ ist, teilt $5^c = |G|_5$ die Anzahl $|G_5| = y + 1$ nach ([26], Remark 15.10). Deswegen ist $y + 1 = 5^c z$ mit $z \in \mathbb{N}_0$. Folglich ist

$$t = \frac{1}{2^a 3^b 5^c} 6(15 + (y + 1)) = \frac{1}{2^a 3^b 5^c} 6(15 + 5^c z),$$

also

$$2^a 3^b 5^c \cdot t = 6(15 + 5^c z)$$

und wir erhalten $c \leq 1$. ∎

Sei τ_5 ein Element der Ordnung 5 von G und $\mathrm{N}_G(\tau_5)$ der Normalisator von $\langle \tau_5 \rangle$ in G.

2.1.15 Lemma. *Gilt* $15 \mid |G|$ *und* $3 \nmid |\mathrm{N}_G(\tau_5)|$, *so ist* $|G| = 60$. *Insbesondere ist* A_5 *die einzige Automorphismengruppe die möglicherweise auftreten kann.*

Beweis. Wir haben $2^3 \nmid |\mathrm{N}_G(\tau_5)|$ nach Lemma 1.4.9. Folglich ist $|\mathrm{N}_G(\tau_5)| = 2^x \cdot 5$, wobei $0 \leq x \leq 2$, nach Lemma 2.1.14. Da $\langle \tau_5 \rangle \in \mathrm{Syl}_5(G)$ ist, ist

$$n_5(G) = |G : \mathrm{N}_G(\tau_5)| = \frac{2^a \cdot 3 \cdot 5}{2^x \cdot 5} = 2^{a-x} \cdot 3 \equiv 1 \mod 5.$$

Die einzigen Möglichkeiten für (a, x) sind

$$(1,0), (2,1), (3,2), (5,0).$$

Weiterhin ist die Anzahl der Bahnen $t = \frac{1}{|G|}(96 + n_5(G) \cdot 4 \cdot 6)$.

Im letzten Fall ($a = 5$ und $x = 0$) haben wir $|G| = 32 \cdot 15 = 480$ und G hat genau $n_5(G) = 96$ 5-Sylowuntergruppen. Dann ist die Anzahl der Bahnen

$$t = \frac{1}{480}(96 + 96 \cdot 4 \cdot 6) = 5.$$

Nach Lemma 2.1.13 erhalten wir, dass die Bahnen von G Länge $2^a \cdot 3 = 96$ haben. Dies widerspricht der Tatsache, dass $t = 5$ ist.

In den anderen Fällen ist die Anzahl $n_5(G)$ der 5-Sylowuntergruppen 6, deshalb ist die Anzahl der Bahnen

$$t = \frac{1}{2^a \cdot 3 \cdot 5}(96 + 6 \cdot 4 \cdot 6) = \frac{2^4}{2^a}.$$

Im Fall $a = 3$ haben wir $t = 2$. Dies kann auch nicht sein, da die Bahnen von G nach Lemma 2.1.13 Länge $2^a \cdot 3 = 24$ haben.

Im Fall $a = 2$ haben wir $|G| = 60$. Wir wissen, dass A_5 die einzige Gruppe mit $n_5 = 6$ ist.

Im Fall $a = 1$ haben wir $|G| = 30 = 2 \cdot 3 \cdot 5$ und $n_5 = 6$, was Lemma 1.4.2 widerspricht. ∎

2.1.16 Lemma. *Gilt* $15 \mid |G|$ *und* $3 \mid |\mathrm{N}_G(\tau_5)|$, *so ist* G *eine auflösbare Gruppe der Ordnung* $|G| = 15$, 30, 240 *oder* 480.

Beweis. Wir wissen, dass

$$n_5(G) = |G : \mathrm{N}_G(\tau_5)| = \frac{2^a \cdot 3 \cdot 5}{2^x \cdot 3 \cdot 5} = 2^{a-x} \equiv 1 \mod 5,$$

wobei $0 \leq a \leq 5$ und $0 \leq x \leq 2$. Die einzigen Möglichkeiten für (a, x) sind

$$(0,0), (1,1), (2,2), (4,0), (5,1).$$

Für die ersten zwei Fälle $a = 0, 1$ ist $|G| = 15, 30$. Es ist bekannt, dass eine Gruppe mit dieser Ordnung auflösbar ist.

Im Fall $a = 2$ ($|G| = 60$) ist die Anzahl $n_5(G)$ der 5-Sylowuntergruppen gleich 1. Die Anzahl der Bahnen ist gegeben durch

$$t = \frac{1}{60}(96 + 6 \cdot 4) = 2.$$

Offensichtlich haben die Bahnen Länge 12 oder 60. Da $12m + 60n = 96$ und $m + n = 2$ keine Lösungen in $\mathbb{N}_0$ haben, kann die Gruppe G nicht als Automorphismengruppe von C existieren.

Im Fall $a = 4$ ist $|G| = 240$ und $n_5(G) = 16$. Mit MAGMA erhalten wir, dass es exakt 8 nicht-auflösbare Gruppen der Ordnung 240 gibt, alle mit $n_5(G) = 6$. Deswegen ist G auflösbar.

Im letzteren Fall $a = 5$ ist $|G| = 480$ und $n_5(G) = 16$. Man bestätigt mit MAGMA, dass es genau 26 nicht-auflösbare Gruppen der Ordnung 480 gibt, alle mit $n_5(G) = 6$. Somit ist G abermals auflösbar. ∎

2.1.17 Bemerkung.

1. Durch MAGMA wissen wir, dass 200 auflösbare Gruppen G der Ordnung 240 existieren, von denen nur zwei $n_5(G) = 16$ haben. Deshalb gibt es nur zwei auflösbare Gruppen der Ordnung 240 als mögliche Automorphismengruppe G.

2. Ähnlich erhalten wir, dass es 1187 auflösbare Gruppen G der Ordnung 480 gibt. Aber nur 7 haben $n_5(G) = 16$. Deshalb gibt es nur 7 auflösbare Gruppen der Ordnung 480 als mögliche Automorphismengruppe G.

2.1.18 Lemma. $|G| \neq 20, 40$.

Beweis. Falls $|G| = 20$ ist, so existiert genau eine 5-Sylowuntergruppe, da $n_5(G) \equiv 1 \mod 5$ und $n_5(G) \mid |G|$. Dann gilt

$$t = \frac{1}{20}(96 + 6 \cdot 4) = 6.$$

Offensichtlich haben die Bahnen Länge 20 oder 4. Aber die Gleichungen $20m + 4n = 96$ und $m + n = 6$ haben keine Lösungen in $\mathbb{N}_0$.

Im Fall $|G| = 40$ ist wieder eine 5-Sylowuntergruppe normal, durch das gleiche Argument wie oben. Die Anzahl der Bahnen ist gegeben durch

$$t = \frac{1}{40}(96 + 6 \cdot 4) = 3.$$

Nun haben die Bahnen Länge 40 oder 8. Da $40m + 8n = 96$ und $m + n = 3$ keine Lösungen in $\mathbb{N}_0$ haben, kann die Gruppe G nicht als Automorphismengruppe von C existieren. ∎

Wir haben zusammenfassend den folgenden Satz bewiesen:

2.1.19 Satz. *Sei C ein selbstdualer $[96, 48, 20]$-Code. Falls alle Automorphismen der Ordnung 3 keine Fixpunkte haben, so ist die Automorphismengruppe entweder auflösbar und ihre Ordnung ist 15, 30, 240, 480 oder Teiler von $2^5 3$, $2^5 5$, oder die Automorphismengruppe ist die einfache Gruppe A_5. Insbesondere ist $|\mathrm{Aut}(C)| \leq 480$. Weiterhin können die Fälle $|\mathrm{Aut}(C)| = 20$ oder $|\mathrm{Aut}(C)| = 40$ nicht auftreten.*

Kapitel 3

Selbstduale $[120, 60, 24]$-Codes

3.1 Über die Ordnung der Automorphismengruppe eines selbstdualen $[120, 60, 24]$-Codes

Wie schon in Kapitel 2 erwähnt, ist die Existenz der extremalen Codes vom Typ II der Länge $24m$ ein zentrales Thema in der Kodierungstheorie. Für den Fall $m = 5$ erhalten wir den extremalen $[120, 60, 24]$-Code vom Typ II. Dieser Code, dessen Existenz bis heute unbekannt ist, wurde wenig erforscht. Wenn dieser Code existieren würde, wäre ein erster Versuch ihn zu konstruieren die Anwendung der Zerlegung des Lemma 1.5.6, welche man durch einen nicht-trivialen Automorphismus von ungerader Ordnung erhält.

Existiert der Code und hat einen Automorphismus ungerader Ordnung, so funktioniert die ganze Suche oft mit Hilfe dieser Methode wenn immer die Untercodes $F_\sigma(C)$ und $E_\sigma(C)$ bestimmt werden können. Wenn dem so ist, erhalten wir den Code, sonst hätten wir gezeigt, dass dieser Code keinen Automorphismus mit dieser Ordnung hat. Für die Fälle $m = 3$ und $m = 4$ hat die Automorphismengruppe nur Elemente kleiner Ordnung. Es ist daher natürlich zu fragen

3.1.1 Frage. Sollte ein selbstdualer $[120, 60, 24]$-Code vom Typ II existieren, welche Primzahlen teilen dann die Ordnung der Automorphismengruppe?

Ziel dieses Kapitels ist es, eine Antwort auf diese Fragen zu geben. In [8] wurde bewiesen, dass ein Automorphismus der Ordnung 2 vom Typ 2-$(48; 24)$ und 2-$(60; 0)$ ist. Wir formulieren zunächst den Hauptsatz dieses Kapitels.

3.1.2 Hauptsatz. *Sei C ein extremaler Code der Länge 120.*

1. *Falls σ ein Automorphismus von C der Primzahlordnung p ist, dann ist seine Zyklen-Struktur gegeben durch*

p	*Anzahl der p-Zyklen*	*Anzahl der Fixpunkte*
2	48, 60	24, 0
3	40	0
5	24	0
7	17	1
19	6	6
23	5	5
29	4	4

2. *Die Ordnung der Automorphismengruppe ist* $|\mathrm{Aut}(C)| = 2^a \cdot 3^b \cdot 5^c \cdot 7^d \cdot 19^e \cdot 23^f \cdot 29^g$, *wobei* $a \in \mathbb{N}_0$ *und* $b, c, d, e, f, g \in \{0, 1\}$ *ist.*

3. *Ist* $\sigma \in \mathrm{Aut}(C)$ *von ungerader zusammengesetzter Ordnung* r, *so ist* $r = 15$, 57 *oder* 115 *und die Zyklen-Struktur von* σ *ist* $3 \cdot 5\text{-}(0, 0, 8; 0)$, $3 \cdot 19\text{-}(2, 0, 2; 0)$ *oder* $5 \cdot 23\text{-}(1, 0, 1; 0)$.

Die möglichen Typen $p\text{-}(c; f)$ von Automorphismen σ eines selbstdualen $[120, 60, 24]$-Codes C mit $p \geq 3$ sind:

Tabelle 3.1: Mögliche Typen von Automorphismen eines selbstdualen $[120, 60, 24]$-Codes.

p	c	f
3	1,2,3,4,5,6,7,8,9,10,	117,114,111,108,105,102,99,96,93,90,
	11,12,13,14,15,16,17,18,19,20,	87,84,81,75,72,69,66,63,60,
	21,22,23,24,25,26,27,28,29,30,	57,54,51,48,45,42,39,36,33,30,
	31,32,33,34,35,36,37,38,39,40	27,24,21,18,15,12,9,6,3,0
5	1,2,3,4,5,6,7,8,9,10,	115,110,105,100,95,90,85,80,75,70,
	11,12,13,14,15,16,17,18,19,20,	65,60,55,50,40,35,30,25,20,
	21,22,23,24	15,10,5,0
7	1,2,3,4,5,6,7,8,9,10,	113,106,99,92,85,78,71,64,57,50,
	11,12,13,14,15,16,17	43,36,29,22,15,8,1
11	1,2,3,4,5,6,7,8,9,10	109,98,87,76,65,54,43,32,21,10
13	1,2,3,4,5,6,7,8,9	107,94,81,68,55,42,29,16,3
17	1,2,3,4,5,6,7	103,86,69,52,35,18,1
19	1,2,3,4,5,6	101,82,63,44,25,6
23	1,2,3,4,5	97,74,51,28,5
29	1,2,3,4	91,62,33,4
31	1,2,3	89,58,27
37	1,2,3	83,46,9
41	1,2	79,38
43	1,2	77,34
47	1,2	73,26
53	1,2	67,14
59	1,2	61,2
61	1	59
67	1	53
71	1	49
73	1	47
79	1	41
83	1	37
89	1	31
97	1	23
101	1	19
103	1	17
109	1	11
113	1	7

3.1.3 Lemma. *Ein selbstdualer* $[120, 60, 24]$*-Code* C *hat keinen Automorphismus vom Typ* $3\text{-}(p; c)$ *mit* c *ungerade.*

Beweis. Da 2 eine primitive Wurzel modulo 3 ist, ist c gerade wegen 1.5.6 (2). ∎

3.1.4 Lemma. *Ein selbstdualer* $[120, 60, 24]$*-Code* C *hat keinen Automorphismus vom Typ* $3\text{-}(2; 114)$, $3\text{-}(4; 108)$, $3\text{-}(6; 102)$, $3\text{-}(8; 96)$, $3\text{-}(10; 90)$, $3\text{-}(12; 84)$, $3\text{-}(14; 78)$, $3\text{-}(16; 72)$, $3\text{-}(18; 66)$, $3\text{-}(20; 60)$, $3\text{-}(22; 54)$, $3\text{-}(24; 48)$, $3\text{-}(26; 42)$ *und* $3\text{-}(28; 36)$.

Beweis. Dies folgt mit 1.5.12 und einer einfachen Rechnung. ∎

Wegen 1.5.14, 3.1.3 und 3.1.4 erhalten wir, dass die möglichen Typen $p\text{-}(c; f)$ von Automorphismen σ von ungerader Primzahlordnung $p \geq 3$ die Folgenden sind:

Tabelle 3.2: Typen von Automorphismen eines selbstdualen $[120, 60, 24]$-Codes.

p	c	f
3	30, 32, 34, 36, 38, 40	30, 24, 18, 12, 6, 0
5	20,21,22,23,24	20,15,10,5,0
7	15,16,17	15,8,1
11	10	10
13	9	3
17	7	1
19	6	6
23	5	5
29	4	4
59	2	2

3.1.1 Automorphismen der Ordnung 3

3.1.5 Lemma. *Sei* C *ein selbstdualer* $[120, 60, 24]$*-Code. Dann hat* C *keinen Automorphismus der Ordnung* 3 *vom Typ* $3\text{-}(30; 30)$.

Beweis. Sei $\sigma \in \mathrm{Aut}(C)$ vom Typ $3\text{-}(30; 30)$. Dann ist $\pi(F_\sigma(C))$ ein selbstdualer $[60, 30, d_\pi]$-Code. Nach Satz 1.3.1 haben wir $d_\pi \leq 12$.

Wir betrachten eine Erzeugermatrix für den selbstdualen Code $\pi(F_\sigma(C))$ in Form von (1.4). Da $c = f$ ist, erhalten wir $k_1 = k_2$, nach dem Balance Prinzip (siehe Lemma 1.6.1).

Bemerke, dass $\mathcal{B}$ ein doppeltgerader $[30, k_2, d']$-Code ist, mit $d' = 24$ oder $d' = 28$. In beiden Fällen ist $k_2 \leq 1$. Sei $d' = 24$ und angenommen, dass u und v zwei Zeilen von B sind, mit $\mathrm{wt}(u) = \mathrm{wt}(v) = 24$. Deswegen haben wir $S_{u,v} \geq 18$ nach Lemma 1.1.2 (2) und daher ist $\mathrm{wt}(\pi^{-1}(0|u + v)) \leq 12$, ein Widerspruch. Falls $\mathrm{wt}(u) = 24$ und $\mathrm{wt}(v) = 28$ sind, dann ist $S_{u,v} \geq 22$ und somit ist $\mathrm{wt}(\pi^{-1}(0|u + v)) \leq 8$, abermals ein Widerspruch. Schließlich, falls $d' = 28$ ist und u und v zwei Zeilen von B mit $\mathrm{wt}(u) = \mathrm{wt}(v) = 28$ sind, dann ist $\mathrm{wt}(\pi^{-1}(0|u + v)) \leq 4$, ein Widerspruch. Somit ist $k_1 = k_2 \leq 1$.

Falls $k_2 = 0$ ist, dann ist $\mathrm{gen}(\pi(F_\sigma(C))) = (I_{30} \mid E)$. Wir bezeichnen die i-te Zeile von E mit $(e_i \mid v_i)$ für $i = 1, \ldots, 30$. Da $\mathrm{wt}(\pi^{-1}(e_i|v_i)) = 3 + \mathrm{wt}(v_i) \geq 24$ ist, gilt dann $\mathrm{wt}(v_i) = 21$,

25 oder 29. Wenn $\mathrm{wt}(v_i) = 29$ und $\mathrm{wt}(v_j) = 29$ sind, dann ist

$$S_{v_i,v_j} = |\operatorname{supp}(v_i) \cap \operatorname{supp}(v_j)| \geq 28$$

und somit

$$\mathrm{wt}(\pi^{-1}(e_i + e_j | v_i + v_j)) = 6 + \mathrm{wt}(v_i + v_j) \leq 8,$$

ein Widerspruch. In allen anderen Fällen erhalten wir ebenfalls einen Widerspruch, außer $\mathrm{wt}(v_i) = 21$ für $i = 1, \ldots, 30$.

Wenn $x = (e_i|v_i)$ und $y = (e_j|v_j)$ ist, dann ist $S_{x,y} = S_{v_i,v_j} \geq 12$. Falls $S_{v_i,v_j} > 12$ ist, erhalten wir

$$\mathrm{wt}(\pi^{-1}(x + y)) \leq 6 + 17 = 23,$$

ein Widerspruch. Folglich ist $S_{v_i,v_j} = 12$ für alle $i \neq j \in \{1, \ldots, 30\}$. Daher haben zwei Vektoren $v_i \neq v_j$ keine gleiche 0-Koordinate. Deswegen ist die Dimension von $\mathrm{gen}(\pi(F_\sigma(C))$ höchstens 3, ein Widerspruch.

Falls $k_2 = 1$ ist, dann hat $\pi(F_\sigma(C))$ eine Erzeugermatrix der Form

$$\begin{pmatrix} a & 0 \ldots 0 \\ 0 \ldots 0 & b \\ D & E \end{pmatrix},$$

wobei $\mathrm{wt}(b) = 24$ oder 28 ist. Da C doppeltgerade ist, gilt $\mathrm{wt}(a) \in \{8, 12, 16, 20, 24, 28\}$. Angenommen, dass $\mathrm{wt}(a) = 28$ ist. Dann ist $\mathrm{wt}(\pi^{-1}(a|b)) \geq 108$, was bedeutet, dass $(a|b)$ der Vektor mit ausschließlich 1-Einträgen ist, was $\mathrm{wt}(a) = 28$ widerspricht. Daher ist $\mathrm{wt}(a) \leq 24$. Folglich enthält a in mindestens sechs Positionen eine 0. Somit gibt es mindestens sechs Vektoren der Form $z_i = (0, 0, \ldots, 1, \ldots, 0, 0) \in \mathbb{F}_2^{30}$, die orthogonal zu a sind. Nach Lemma 1.6.1 (3) erhalten wir $z_i \in \mathcal{A}^\perp = \mathcal{A}_D$. Der Widerpruch folgt nun wie im Fall $k_2 = 0$. ∎

3.1.6 Lemma. *Sei C ein selbstdualer $[120, 60, 24]$-Code. Dann hat C keinen Automorphismus der Ordnung 3 vom Typ 3-$(38; 6)$.*

Beweis. Angenommen, dass $\sigma \in \mathrm{Aut}(C)$ vom Typ 3-$(38; 6)$ ist. Dann ist $\pi(F_\sigma(C))$ ein selbstdualer $[44, 22, d_\pi]$-Code. Nach Satz 1.3.1 haben wir $d_\pi \leq 8$. Wenn wir $d_\pi = x + y$ schreiben, wobei x die Anzahl der Einsen in den ersten 38 Koordinaten eines Vektors mit minimalem Gewicht ist und y die Anzahl der Einsen in den letzten Koordinaten, so ist $x + y \leq 8$ und $3x + y \geq 24$. Dies zwingt $x \geq 8$, $y = 0$ und gilt $d_\pi = 8$. Deswegen ist $\pi(F_\sigma(C))$ ein selbstdualer $[44, 22, 8]$-Code.

Nach [16] gibt es zwei mögliche Gewichtspolynome für $\pi(F_\sigma(C))$:

$$W_{44,1}(y) = 1 + (44 + 4\beta)y^8 + (976 - 8\beta)y^{10} + \ldots$$

für $10 \leq \beta \leq 122$ und

$$W_{44,2}(y) = 1 + (44 + 4\beta)y^8 + (1232 - 8\beta)y^{10} + (10241 - 20\beta)y^{12} + \ldots$$

für $0 \leq \beta \leq 154$.

Wir betrachten eine Erzeugermatrix für $\pi(F_\sigma(C))$ der Form (1.4). Da $f < 24$ ist, gilt $k_2 = 0$ und wegen des Balance Prinzips ist $k_1 = 16$. Somit hat $\pi(F_\sigma(C))$ eine Erzeugermatrix der Form

$$\begin{pmatrix} A & 0 \\ D & E \end{pmatrix}.$$

Der Code $\mathcal{A}$ ist ein doppeltgerader $[38, 16, d']$-Code mit $d' \geq 8$. Da $d_\pi = 8$ ist, gibt es einen Vektor $(u|w) \in \pi(F_\sigma(C))$ mit $\mathrm{wt}(u|w) = 8$ und es gilt $3\mathrm{wt}(u) + \mathrm{wt}(w) \geq 24$. Daraus folgt $\mathrm{wt}(u) = 8$ und $\mathrm{wt}(w) = 0$ und somit $d' = 8$.

Seien $W_\mathcal{A} = \sum A_i y^i$ und $W_{\pi(F_\sigma(C))} = \sum A_i^\pi y^i$ die Gewichtspolynome der Codes $\mathcal{A}$ beziehungsweise $\pi(F_\sigma(C))$. Dann ist $A_8 = A_8^\pi$. Deswegen ist $A_{36} = 0$, denn wenn $(u|0) \in \pi(F_\sigma(C))$, mit $\mathrm{wt}(u) = 36$, dann ist

$$\mathrm{wt}(\pi^{-1}(u + \mathbf{1}|\mathbf{1})) \leq 6 + 6 < 24,$$

wobei $\mathbf{1}$ der Vektor mit ausschließlich 1-Einträgen der angemessenen Länge ist, also ein Widerpruch.

Ist andererseits $a \in \mathcal{A}^\perp$, so gibt es einen Vektor $(a|b) \in \pi(F_\sigma(C))$ mit $3\mathrm{wt}(a) + \mathrm{wt}(b) \geq 24$ und $\mathrm{wt}(b) \leq 6$. Somit ist $\mathrm{wt}(a) \geq 6$. Schließlich ist $\mathcal{A}$ ein doppeltgerader $[38, 16, 8]$-Code mit dualer Distanz $d'^\perp \geq 6$.

Sei

$$W_\mathcal{A}(y) = 1 + A_8 y^8 + A_{12} y^{12} + \ldots + A_{32} y^{32}$$

und

$$W_{\mathcal{A}^\perp}(y) = 1 + A_6^\perp y^6 + A_7^\perp y^7 + \ldots$$

Nach dem Satz 1.1.5 und einer Rechnung in MAPLE finden wir, dass

$$A_{12} = 2808 - 6A_8, \ldots, A_{28} = 632 - 6A_8,\ A_{32} = -27 + A_8$$

ist. Widerum mit Hilfe von MAPLE und MacWilliams-Identitäten (siehe Satz 1.1.4) erhalten wir

$$A_6^\perp = 4A_8 - 87,\ A_7^\perp = 480 - 8A_8,\ A_8^\perp = 660 + 4A_8,\ A_9^\perp = 1920,\ A_{10}^\perp = 7952 - 24A_8, \ldots$$

Da $A_7^\perp = 480 - 8A_8 \geq 0$ ist, gilt $A_8 = A_8^\pi = 44 + 4\beta \leq 60$. Deswegen ist $0 \leq \beta \leq 4$ und $W_{44,2}$ das Gewichtspolynom von $\pi(F_\sigma(C))$.

Wie in der Definition 1.1.7 sei

$$A_\mathbf{i} = A_{(x,y)} := |\{(v|u) \in \pi(F_\sigma(C)) \mid \mathrm{wt}(v) = x \text{ und } \mathrm{wt}(u) = y\}|.$$

Da $\mathbf{1} \in \pi(F_\sigma(C))$, ist $A_{(x,y)} = A_{(38-x,6-y)}$.

Dann erhalten wir

$$A_{12}^\pi = A_{(12,0)} + A_{(10,2)} + A_{(8,4)} + A_{(6,6)}$$

mit $A_{(12,0)} = A_{12} = 2808 - 6A_8 = 2544 - 24\beta$,
$A_{(10,2)} = (A_{(10,2)} + A_{(10,6)}) - A_{(10,6)} = A_{10}^\perp - A_{(28,0)} = A_{10}^\perp - A_{28} = 7320 - 18A_8 = 6528 - 72\beta$,
$A_{(8,4)} = (A_{(8,4)} + A_{(8,0)}) - A_{(8,0)} = A_8^\perp - A_8 = 660 + 3A_8 = 792 + 12\beta$ und
$A_{(6,6)} = A_{(32,0)} = A_{32} = -27 + A_8 = 17 + 4\beta$.

Somit ist $A_{12}^\pi = 9881 - 80\beta = 10241 - 20\beta$, und daher $\beta < 0$, ein Widerspruch. ∎

3.1.7 Lemma. *Sei C ein selbstdualer $[120, 60, 24]$-Code. Dann hat C keinen Automorphismus der Ordnung 3 vom Typ 3-$(32; 24)$.*

Beweis. Angenommen $\sigma \in \mathrm{Aut}(C)$ vom Typ 3-$(32; 24)$. Wie zuvor betrachten wir eine Erzeugermatrix für $\pi(F_\sigma(C))$ der Form (1.4). Nach dem Balance Prinzip (siehe Lemma 1.6.1) gilt $k_1 = k_2 + 4$. Da $f = d = 24$ ist, gilt dann $k_2 = 0$ oder 1.

- Sei $k_2 = 0$. Dann ist $k_1 = 4$ und $\pi(F_\sigma(C))$ hat eine Erzeugermatrix der Form

$$\begin{pmatrix} A & 0 \\ D & E \end{pmatrix}.$$

Der Code $\mathcal{A}$ ist ein doppeltgerader $[32, 4, d']$-Code mit $d' \geq 8$. Deswegen ist $\mathcal{A}^\perp$ ein $[32, 28, d'^\perp]$-Code. Mit Blick auf die Code-Tabelle [27] sehen wir, dass die duale Distanz $d(\mathcal{A}^\perp) = d'^\perp = 1$ oder 2 ist.

Wir betrachten zunächst den Fall $d(\mathcal{A}^\perp) = 1$. Sei $a_1 \in \mathcal{A}^\perp$ mit $\mathrm{wt}(a_1) = 1$. Dann gibt es einen Vektor $(a_1|b_1) \in \pi(F_\sigma(C))$ mit $b_1 \in \mathbb{F}_2^{24}$. Da $\mathrm{wt}(\pi^{-1}(a_1|b_1)) = 3 + \mathrm{wt}(b_1) \geq 24$ ist, gilt dann $\mathrm{wt}(b_1) = 21$. Nach Lemma 1.6.2, ist $\mathcal{A} = (0 \mid \mathcal{A}_1)$ und $\mathcal{A}^\perp = (0 \mid \mathcal{A}_1^\perp) \cup (1 \mid \mathcal{A}_1^\perp)$. Der Code $\mathcal{A}_1^\perp$ hat Parameter $[31, 27]$ und nach den Code-Tabellen [27] ist die Minimaldistanz 1 oder 2.

Wenn $d(\mathcal{A}_1^\perp) = 1$ ist, dann gibt es (bis auf Äquivalenz) einen Vektor $(0, 1, 0, \ldots, 0|b_2) \in \pi(F_\sigma(C))$ mit $\mathrm{wt}(b_2) = 21$. Aber dann ist

$$\mathrm{wt}(\pi^{-1}((a_1|b_1) + (0, 1, 0, \ldots, 0|b_2))) \leq 6 + 6 < 24,$$

ein Widerspruch.

Wenn $d(\mathcal{A}_1^\perp) = 2$ ist, dann gibt es (bis auf Äquivalenz) einen Vektor

$$(0, 1, 1, \ldots, 0|b_2) \in \pi(F_\sigma(C))$$

mit $\mathrm{wt}(b_2) = 18$ oder 22. Aber dann erhalten wir wieder

$$\mathrm{wt}(\pi^{-1}((a_1|b_1) + (0, 1, 1, 0, \ldots, 0|b_2))) \leq 9 + \mathrm{wt}(b_1 + b_2) \leq 18 < 24,$$

ein Widerspruch.

Betrachten wir nun den Fall $d(\mathcal{A}^\perp) = 2$. Seien

$$W_\mathcal{A}(y) = 1 + A_8 y^8 + A_{12} y^{12} + A_{16} y^{16} + A_{20} y^{20} + A_{24} y^{24} + A_{28} y^{28} + A_{32} y^{32}$$

und

$$W_{\mathcal{A}^\perp}(y) = 1 + B_2 y^2 + B_3 y^3 + \ldots$$

die Gewichtspolynome vom Code $\mathcal{A}$ bzw. seines dualen Codes $\mathcal{A}^\perp$. Da $k_2 = 0$ ist, gilt dann $A_{32} = 0$.

Weiterhin ist $B_2 \neq 0$. Angenommen, dass a_1, $a_2 \in \mathcal{A}^\perp$ mit $a_1 \neq a_2$ und $\mathrm{wt}(a_1) = \mathrm{wt}(a_2) = 2$ ist. Dann gibt es Vektoren $(a_i|b_i) \in \pi(F_\sigma(C))$ mit $\mathrm{wt}(b_i) = 18$ oder 22 für $i = 1, 2$. Da $b_1, b_2 \in \mathbb{F}_2^{24}$ ist, gilt $\mathrm{wt}(b_1 + b_2) \leq 12$.

Wenn $\mathrm{wt}(a_1 + a_2) = 2$ ist, dann gilt

$$\mathrm{wt}(\pi^{-1}(a_1 + a_2|b_1 + b_2)) = 6 + \mathrm{wt}(b_1 + b_2) \leq 6 + 12 < 24,$$

ein Widerspruch.

Deshalb ist $\mathrm{wt}(a_1 + a_2) = 4$. Da

$$\mathrm{wt}(\pi^{-1}(a_1 + a_2|b_1 + b_2)) = 12 + \mathrm{wt}(b_1 + b_2) \geq 24$$

ist, erhalten wir $\mathrm{wt}(b_1+b_2)\geq 12$. Daher ist $\mathrm{wt}(b_1+b_2)=12$ und $\mathrm{wt}(b_i)=18$. Folglich ist $B_2\leq 4$.

Wenn wir die ersten Pless Power Moments vom Code $\mathcal{A}$ berechnen, erhalten wir nach Satz 1.1.6

$$\begin{cases} A_8+A_{12}+A_{16}+A_{20}+A_{24}+A_{28} & =15\\ 8A_8+12A_{12}+16A_{16}+20A_{20}+24A_{24}+28A_{28} & =8.32\\ 8^2A_8+12^2A_{12}+16^2A_{16}+20^2A_{20}+24^2A_{24}+28^2A_{28} & =4\cdot 32\cdot 33+8B_2 \end{cases}$$

$$\begin{cases} A_8+A_{12}+A_{16}+A_{20}+A_{24}+A_{28} & =15\\ 2A_8+3A_{12}+4A_{16}+5A_{20}+6A_{24}+7A_{28} & =64\\ 8A_8+18A_{12}+32A_{16}+50A_{20}+72A_{24}+98A_{28} & =16\cdot 33+B_2 \end{cases}$$

$$\begin{cases} A_8+A_{12}+A_{16}+A_{20}+A_{24}+A_{28} & =15\\ 2A_8+3A_{12}+4A_{16}+5A_{20}+6A_{24}+7A_{28} & =64\\ -4A_8+8A_{16}+20A_{20}+36A_{24}+56A_{28} & =16\cdot 9+B_2 \end{cases}$$

Nach der letzten Gleichung ist 4 Teiler von B_2. Deshalb haben wir $B_2=4$.

$$\begin{cases} A_8+A_{12}+A_{16}+A_{20}+A_{24}+A_{28} & =15\\ -A_8+A_{16}+2A_{20}+3A_{24}+4A_{28} & =19\\ -A_8+2A_{16}+5A_{20}+9A_{24}+14A_{28} & =4\cdot 9+1=37 \end{cases}$$

$$\begin{cases} A_8+A_{12}+A_{16}+A_{20}+A_{24}+A_{28} & =15\\ -A_8+A_{16}+2A_{20}+3A_{24}+4A_{28} & =19\\ A_8+A_{20}+3A_{24}+6A_{28} & =-1 \end{cases}$$

Die letzte Gleichheit ist nicht möglich und wir erhalten wieder einen Widerspruch.

- Sei $k_2=1$. Dann ist $k_1=5$ und $\mathcal{A}$ ein doppeltgerader $[32,5,d']$-Code mit $d'\geq 8$. Deshalb ist $\mathcal{A}^\perp$ ein $[32,27,d'^\perp]$-Code. Nach der Code-Tabelle [27] wissen wir, dass die duale Minimaldistanz $d(\mathcal{A}^\perp)=d'^\perp\leq 2$ ist. Daher gibt es einen Vektor $(a|b)\in\pi(F_\sigma(C))$ mit $\mathrm{wt}(a)\leq 2$ und $\mathrm{wt}(b)\geq 18$. Da $k_2=1$ ist, ist der Vektor $(0,\ldots,0|\mathbf{1})\in\pi(F_\sigma(C))$. Aber dann ist
$$\mathrm{wt}(\pi^{-1}(a|b+\mathbf{1}))\leq 6+6<24,$$
ein Widerspruch. ∎

3.1.8 Lemma. *Sei C ein selbstdualer $[120,60,24]$-Code. Dann hat C keinen Automorphismus der Ordnung 3 vom Typ 3-$(36;12)$.*

Beweis. Sei σ ein Automorphismus der Ordnung 3 vom Typ 3-$(36;12)$. Dann ist $\pi(F_\sigma(C))$ ein selbstdualer $[48,24,\geq 8]$-Code. Nehmen wir eine Erzeugermatrix für $\pi(F_\sigma(C))$ der Form (1.4). Da $f=12<24$ ist, gilt $k_2=0$ und wegen des Balance Prinzips ist $k_1=12$. Somit ist

$$\mathrm{gen}(\pi(F_\sigma(C)))=\begin{pmatrix} A & O\\ D & I_{12}\end{pmatrix}. \tag{3.1}$$

Der Code $\mathcal{A}$ ist ein doppeltgerader $[36,12,d']$- Code mit $d'\geq 8$. Wenn $a\in\mathcal{A}^\perp$ ist, dann gibt es einen Vektor $(a|b)\in\pi(F_\sigma(C))$ mit $3\mathrm{wt}(a)+\mathrm{wt}(b)\geq 24$ und $\mathrm{wt}(b)\leq 12$. Somit ist

$\mathrm{wt}(a) \geq 4$. Daher ist $\mathcal{A}$ ein doppeltgerader $[36, 12, d']$-Code mit $d' \geq 8$ und dualer Distanz $d'^{\perp} \geq 4$.

Sei $\sum_{i=0}^{48} A_i^{\pi} y^i$ das Gewichtspolynom von $\pi(F_\sigma(C))$ und wie in der Definition 1.1.7,

$$A_{\mathbf{i}} = A_{(x,y)} := |\{(v|u) \in \pi(F_\sigma(C)) \mid \mathrm{wt}(v) = x \text{ und } \mathrm{wt}(u) = y\}|.$$

Da die Erzeugermatrix von $\mathrm{gen}(\pi(F_\sigma(C)))$ die Untermatrix $(D \mid I_{12})$ enthält, ist $A_{(x,1)} \neq 0$ für einige $1 \leq x \leq 36$. Da C doppeltgerade ist, gilt $3x+1 \equiv 0 \mod 4$. Deswegen ist $x+1 \not\equiv 0 \mod 4$. Da $A_{(x,1)} \neq 0$ ist, ist auch $A_{x+1}^{\pi} \neq 0$. Wegen $x+1 \not\equiv 0 \mod 4$ gibt es Vektoren in $\pi(F_\sigma(C))$, die durch 4 nicht teilbar sind. Somit ist $\pi(F_\sigma(C))$ ein einfachgerader $[48, 24, d']$-Code mit $d' = 8$ oder $d' = 10$.

Dann haben wir

$$W_{\pi(F_\sigma(C))} = \sum_{j=0}^{6} a_j (1+y^2)^{24-4j} (y^2(1-y^2)^2)^j = \sum_{i=0}^{48} A_i^{\pi} y^i,$$

nach Satz 1.2.3. Da $A_i^{\pi} = 0$ für $1 \leq i < 8$ ist, haben wir $a_0 = 1$, $a_1 = -24$, $a_2 = 156$, $a_3 = -272$ und $a_4 = A_8^{\pi} + 54$. Sei S der Schatten von $\pi(F_\sigma(C))$ und $W_S(y) = \sum B_i y^i$ das Gewichtspolynom vom Schatten. Nach Satz 1.2.3 erhalten wir auch

$$W_S(y) = \sum_{j=0}^{6} (-1) a_j 2^{24-6j} y^{24-4j} (1-y^4)^{2j} = \sum_{i=0}^{48} B_i y^i,$$

wobei $B_0 = \frac{1}{4096} a_6$, $B_4 = -\frac{1}{64} a_5 - \frac{3}{1024} a_6$. Da $B_0 = 0$ ist, gilt $a_5 = -64 B_4$ und $a_6 = 0$. Damit haben wir

$$a_0 = 1,\ a_1 = -24,\ a_2 = 156,\ a_3 = -272,\ a_4 = A_8^{\pi} + 54,\ a_5 = -64 B_4 \text{ und } a_6 = 0.$$

Mit $a := A_8^{\pi}$ und $b := B_4$ erhalten wir

$$\begin{aligned}\sum_{i=0}^{48} A_i^{\pi} y^i =& 1 + a y^8 + (768 - 64b) y^{10} + (8592 - 8a + 384b) y^{12} + (57600 - 704b) y^{14} + \\ & (267831 + 28a - 256b) y^{16} + (871168 + 2496b) y^{18} + (1997040 - 56a - 2432b) y^{20} + \\ & (3264768 - 1728b) y^{22} + (3841680 + 70a + 4608b) y^{24} + \ldots\end{aligned}$$

und

$$\begin{aligned}\sum_{i=0}^{48} B_i y^i =& b y^4 + (a + 54 - 10b) y^8 + (16976 - 8a + 45b) y^{12} + (536040 + 28a - 120b) y^{16} + \\ & (3993648 - 56a + 210b) y^{20} + (7683780 + 70a - 252b) y^{24} + \ldots\end{aligned}$$

Weiterhin ist $A_{(32,0)} = b$. In der Tat, sei S_4 die Menge, die aus Vektoren von S des Gewichts 4 besteht. Sei $R := \{(v|u) \in \pi(F_\sigma(C)) \mid \mathrm{wt}(v) = 32 \text{ und } \mathrm{wt}(u) = 0\}$ und definiere die Injektion $\phi : R \longrightarrow \mathbb{F}_2^{48}$ durch $\phi(v|0) := (v + \mathbf{1}|0)$. Zunächst beweisen wir, dass $\phi(R) \subseteq S_4$ ist. Sei $(v|0) \in R$ und $z = (v + \mathbf{1}|0)$. Dann ist $\mathrm{wt}(z) = 4$ und $z \notin \pi(F_\sigma(C))$. Weiterhin sei

$c = (u|w) \in \pi(F_\sigma(C))$ mit $4 \mid \mathrm{wt}(c)$. Da $(v|0) \in \pi(F_\sigma(C))$ ist und $\pi(F_\sigma(C))$ selbstdual, ist $c \cdot (v|0) = 0$. Somit ist $(u|w) \cdot (v|0) = 0$, und wir haben $u \cdot v = 0$. Angenommen o.B.d.A., dass

$$\begin{aligned}(v|0) &= \overbrace{111\ldots1}^{\mathrm{supp}(v)}0000\,|0\\ (u|w) &= \qquad u_1 \quad u_2 \quad |w\end{aligned}$$

ist. Da $u \cdot v = 0$ ist, erhalten wir $\mathrm{wt}(u_1) \equiv 0 \mod 2$. Angenommen, $\mathrm{wt}(u_2)$ ist ungerade. Wir wissen, dass $\mathrm{wt}(u) + \mathrm{wt}(w) \equiv 0 \mod 4$ und $3\mathrm{wt}(u) + \mathrm{wt}(w) \equiv 0 \mod 4$ ist. Deswegen gilt $\mathrm{wt}(u_1) + \mathrm{wt}(u_2) + \mathrm{wt}(w) \equiv 0 \mod 4$ und $3\mathrm{wt}(u_1) + 3\mathrm{wt}(u_2) + \mathrm{wt}(w) \equiv 0 \mod 4$. Da $\mathrm{wt}(u_1) = 2n_1$ und $\mathrm{wt}(u_2) = 2n_2 + 1$ mit $n_1, n_2 \in \mathbb{N}_0$, haben wir $2 \equiv 0 \mod 4$, ein Widerspruch. Somit ist $\mathrm{wt}(u_2)$ gerade. Dann ist

$$z \cdot c = (v + \mathbf{1}|0) \cdot (u|w) = v \cdot u + \mathbf{1} \cdot u = \mathbf{1} \cdot u = 0.$$

Das heißt, z ist ein Vektor vom Gewicht 4 im Schatten von $\pi(F_\sigma(C))$.

Wir zeigen nun, dass $\phi : R \longrightarrow S_4$ surjektiv ist. Sei $z = (v|w) \in S_4$. Wenn $c \in \mathcal{A}$ ist, dann ist $(c|0) \in \pi(F_\sigma(C))$. Deswegen ist $0 = (v|w) \cdot (c|0) = v \cdot c$ und es gilt $v \in \mathcal{A}^\perp$. Da $d(\mathcal{A}^\perp) \geq 4$ ist, ist $\mathrm{wt}(v) = 4$ und $z = (v|0)$. Weiterhin ist $(v|\mathbf{1}) \in \pi(F_\sigma(C))$. Somit gilt $(v + \mathbf{1}|0) \in R$ und $\phi(v + \mathbf{1}|0) = (v|0) = z$.

Nun berechnen wir die Split-Gewichtsverteilung $A_{(x,y)}$ für $0 \leq x \leq 36$ und $0 \leq y \leq 12$. Dafür verwenden wir die folgenden Einschränkungen:

- Falls $x + y$ ungerade ist, so ist $A_{(x,y)} = 0$
- Falls $3x + y \not\equiv 0 \mod 4$ ist, so ist $A_{(x,y)} = 0$
- Falls $0 < x + y < 8$ oder $40 < x + y < 48$ ist, so ist $A_{(x,y)} = 0$
- Falls $0 < 3x + y < 24$ oder $96 < 3x + y < 120$ ist, so ist $A_{(x,y)} = 0$

Weiterhin verwenden wir die folgenden Ausdrücke

- $A_{(0,0)} = 1$ und $A_{(x,y)} = A_{(36-x,12-y)}$
- $A_{(32,0)} = b$
- $\sum_{i=0}^{36} A_{(i,0)} = 2^{12}$
- $\sum_{i=0}^{\min\{12,j\}} A_{(j-i,i)} = A_j^\pi$ für $0 \leq j \leq 24$. Insbesondere ist $A_{(8,0)} = A_8^\pi$,

und wir erhalten
$A_{(9,5)} = 57600 - 704b - A_{(13,1)} - A_{(11,3)} - A_{(29,5)} - A_{(31,3)}$
$A_{(10,6)} = 267831 + 28a - 257b - A_{(16,0)} - A_{(14,2)} - A_{(12,4)} - A_{(28,4)} - A_{(30,2)}$
$A_{(13,5)} = 871168 + 2496b - A_{(17,1)} - A_{(15,3)} - A_{(25,5)} - A_{(27,3)} - A_{(29,1)}$
$A_{(14,6)} = 1992945 - 55a - 2431b - A_{(18,2)} - A_{(16,4)} + A_{(16,0)} - A_{(24,4)} - A_{(26,2)} + A_{(12,0)} + A_{(24,0)}$
$A_{(17,5)} = 3264768 - 1728b - A_{(21,1)} - A_{(19,3)} - A_{(21,5)} - A_{(23,3)} - A_{(25,1)}$
$A_{(18,6)} = 3841680 + 70a + 4608b - 2A_{(24,0)} - 2A_{(22,2)} - 2A_{(20,4)}$

Wir berechnen (siehe Satz 1.1.8)

$$A_{(r,0)} = \frac{1}{2^{24}} \sum_{v=0}^{12} \sum_{w=0}^{36} A_{(w,v)} \mathcal{K}_r(w, 36) \mathcal{K}_0(v, 12),$$

und

$$A_{(r,1)} = \frac{1}{2^{24}} \sum_{v=0}^{12} \sum_{w=0}^{36} A_{(w,v)} \mathcal{K}_r(w, 36) \mathcal{K}_1(v, 12),$$

für $0 \leq r \leq 36$, wobei $\mathcal{K}_{\mathbf{s}}(x, \gamma) = \sum_{j=0}^{s} \binom{\gamma - x}{s - j} \binom{x}{j} (-1)^j$ für alle $s = 0, 1, \ldots, \gamma$ ist.

Durch mehrfache Substitutionen finden wir $A_{(28,0)} = -a - 4b$ und $A_{(30,2)} = -162 + 18b - 12a$, was unmöglich ist. ∎

3.1.9 Lemma. *Sei C ein selbstdualer $[120, 60, 24]$-Code. Dann hat C keinen Automorphismus der Ordnung 3 vom Typ 3-$(34; 18)$.*

Beweis. Sei σ ein Automorphismus der Ordnung 3 vom Typ 3-$(34; 18)$. Dann ist $\pi(F_\sigma(C))$ ein selbstdualer $[52, 26, \geq 8]$-Code. Wir betrachten eine Erzeugermatrix für $\pi(F_\sigma(C))$ der Form (1.4). Da $f = 12 < 24$ ist, folgt $k_2 = 0$ und $k_1 = 8$. Dann ist

$$\operatorname{gen}(\pi(F_\sigma(C))) = \begin{pmatrix} A & O \\ D & I_{18} \end{pmatrix}. \tag{3.2}$$

Der Code $\mathcal{A}$ ist ein doppeltgerader $[34, 8, d']$-Code mit $d' \geq 8$. Ist $a \in \mathcal{A}^\perp$, so gibt es einen Vektor $(a|b) \in \pi(F_\sigma(C))$ mit $3\operatorname{wt}(a) + \operatorname{wt}(b) \geq 24$ und $\operatorname{wt}(b) \leq 18$. Somit ist $\operatorname{wt}(a) \geq 2$. Daher ist $\mathcal{A}$ ein doppeltgerader $[36, 12, d']$-Code mit $d' \geq 8$ und dualer Distanz $d'^\perp \geq 2$.

Sei $W_{\pi(F_\sigma(C))} = \sum A_i^\pi y^i$ das Gewichtspolynom von $\pi(F_\sigma(C))$, S sein Schatten und $W_S(y) = \sum B_i y^i$ das Gewichtspolynom vom Schatten. Ist $a := A_8^\pi$, $e := B_2$ und $b := B_6$, so erhalten wir

$$\begin{aligned}\sum_{i=0}^{52} A_i^\pi y^i =& 1 + ay^8 + (442 + 2a - 16b - 192e)y^{10} + (6188 - 7a + 64b + 1792e)y^{12} + \\ & (53040 - 16a - 10240e)y^{14} + (308958 + 20a - 320b + 40192e)y^{16} + \\ & (1270360 + 56a + 320b - 98560e)y^{18} + (3754569 - 28a + 576b + 130816e)y^{20} + \\ & (8065616 - 112a - 1024b - 34816e)y^{22} + (12707500 + 14a - 320b - 172800e)y^{24} + \\ & (14775516 + 140a + 1440b + 287616e)y^{26} + \ldots\end{aligned}$$

und

$$\begin{aligned}\sum_{i=0}^{52} B_i y^i =& ey^2 + by^6 + (4a + 884 - 10b - 54e)y^{10} + (106080 - 32a + 45b + 320e)y^{14} + \\ & (2540720 + 112a - 120b - 945e)y^{18} + (16131232 - 224a + 210b + 1728e)y^{22} + \\ & (29551032 + 280a - 252b - 2100e)y^{26} + \ldots\end{aligned}$$

Ähnlich wie im vorherigen Lemma können wir beweisen, dass $A_{(32,0)} = e$ ist.

Nun berechnen wir die Split-Gewichtsverteilung $A_{(x,y)}$ für $0 \leq x \leq 34$ und $0 \leq y \leq 18$. Dafür verwenden wir Einschränkungen wie im vorherigen Lemma und berechnen

$$A_{(r,i)} = \frac{1}{2^{26}} \sum_{v=0}^{18} \sum_{w=0}^{34} A_{(w,v)} \mathcal{K}_r(w, 34) \mathcal{K}_i(v, 18),$$

für $0 \leq i \leq 2$ und $0 \leq r \leq 34$.

Durch mehrfache Einschränkungen und Substitutionen finden wir

$$A_{(9,1)} = -22a - 4A_{(12,0)} + 34,$$

$$A_{(31,3)} = -476 - 16e + 20a + 8A_{(12,0)} + 2A_{(16,0)}$$

und

$$A_{(20,0)} = 663 - 10a - 6A_{(12,0)} - 3A_{(16,0)} + 3e.$$

Dann ist $3A_{(31,3)} + 2A_{(20,0)} + 3A_{(9,1)} = -42e - 26a$. Somit ist $a = e = 0$ und $0 = A_{(9,1)} = 34 - 4A_{(12,0)}$, ein Widerspruch. ∎

Wegen den vorherigen Ergebnissen gilt der folgende Satz

3.1.10 Satz. *Ein Automorphismus eines selbstdualen* $[120, 60, 24]$*-Codes der Ordnung* 3 *hat keine Fixpunkte.*

Nach einer Tabelle in einer Arbeit von Mallows und Sloane (siehe [41]) sind die Gewichtskoeffizienten eines selbstdualen $[120, 60, 24]$-Codes gegeben durch folgendes Lemma.

3.1.11 Lemma. *Die Koeffizienten des Gewichtspolynoms eines selbstdualen* $[120, 60, 24]$*-Codes* C *sind:*

$A_0 = A_{120} = 1$
$A_{24} = A_{96} = 39703755$
$A_{28} = A_{92} = 6101289120$
$A_{32} = A_{88} = 475644139425$
$A_{36} = A_{84} = 18824510698240$
$A_{40} = A_{80} = 397450513031544$
$A_{44} = A_{76} = 4630512364732800$
$A_{48} = A_{72} = 30531599026535880$
$A_{52} = A_{68} = 116023977311397120$
$A_{56} = A_{64} = 257257766776517715$
$A_{60} = 335200280030755776$

3.1.12 Bemerkung. Sei $\sigma \in \mathrm{Aut}(C)$ von der Ordnung 3. Dann ist σ vom Typ 3-$(40; 0)$. Wegen Satz 1.5.2 ist $\pi(F_\sigma(C))$ ein selbstdualer $[40, 20, 8]$-Code. Da σ keine Fixpunkte hat, ist $\pi(F_\sigma(C))$ doppeltgerade. Nach [16] ist das Gewichtspolynom von $\pi(F_\sigma(C))$ gleich

$$W_{\pi(F_\sigma(C))}(y) = 1 + 285y^8 + 21280y^{12} + 239970y^{16} + 525504y^{20} + \ldots$$

Dann erhalten wir

$$W_{F_\sigma(C)}(y) = 1 + 285y^{24} + 21280y^{36} + 239970y^{48} + 525504y^{60} + \ldots,$$

was im Einklang mit Lemma 1.5.4 ist wegen Lemma 3.1.11.

3.1.2 Automorphismen der Ordnung 5

3.1.13 Lemma. *Ein selbstdualer* $[120, 60, 24]$*-Code* C *hat keinen Automorphismus vom Typ* 5-$(21; 15)$ *oder* 5-$(23; 5)$.

Beweis. Wegen $5 \equiv 1 \mod 4$ und $5 \not\equiv 1 \mod 8$ ist c gerade (siehe Korollar 1.5.3). ∎

3.1.14 Lemma. *Ein selbstdualer* $[120, 60, 24]$*-Code* C *hat keinen Automorphismus vom Typ* 5-$(20; 20)$.

Beweis. Da $c = f = 20$ und $c = 20 < 24 = d$ ist, erhalten wir mit Lemma 1.6.3

$$\text{gen}(\pi(F_\sigma(C))) = (I_{20} \mid E'), \tag{3.3}$$

wobei E' eine Matrix der Größe 20×20 ist. Sei $v_1 = (1, 0, 0, \ldots, 0 \mid x_1)$ die erste und $v_2 = (0, 1, 0, \ldots, 0 \mid x_2)$ die zweite Zeile von $(I_{20} \mid E')$. Dann folgt

$$\text{wt}(\pi^{-1}(v_1)) = \text{wt}(\pi^{-1}(1, 0, 0, \ldots, 0 \mid x_1)) = 5 + \text{wt}(x_1) \geq 24.$$

Deshalb ist $19 \leq \text{wt}(x_1) \leq 20$. Da C und $\pi(F_\sigma(C))$ doppeltgerade Codes sind, ist $\text{wt}(x_1) = 19$. Auf die gleiche Weise erhalten wir $\text{wt}(x_2) = 19$. Dementsprechend ist $\text{wt}(x_1 + x_2) \leq 2$.

Also

$$\text{wt}(\pi^{-1}(v_1 + v_2)) = \text{wt}(\pi^{-1}(1, 1, 0, \ldots, 0 \mid x_1 + x_2)) = 2 \cdot 5 + \text{wt}(x_1 + x_2) \leq 12,$$

ein Widerspruch. ∎

3.1.15 Lemma. *Sei* C *ein selbstdualer* $[120, 60, 24]$*-Code. Dann hat* C *keinen Automorphismus der Ordnung* 5 *vom Typ* 5-$(22; 10)$.

Beweis. Angenommen, $\sigma \in \text{Aut}(C)$ ist vom Typ 5-$(22; 10)$. Dann ist $\pi(F_\sigma(C))$ ein selbstdualer $[32, 16, d_\pi]$-Code. Weiterhin ist $\pi(F_\sigma(C))$ doppeltgerade, wegen 1.5.2 (2), da $p \equiv 1 \mod 4$ ist. Gemäß Satz 1.3.1 haben wir $d_\pi \leq 8$. Wenn wir $d_\pi = x + y$ schreiben, wobei x die Anzahl der Einsen in den ersten 22 Koordinaten eines Vektors mit minimalem Gewicht ist und y die Anzahl der Einsen in den letzten Koordinaten, so folgt $x + y \leq 8$ und $5x + y \geq 24$. Dies erzwingt $x \geq 4$ und $d_\pi = 8$. Daher ist $\pi(F_\sigma(C))$ ein extremaler selbstdualer und doppeltgerader Code der Länge 32. Nach ([52], p. 262) gibt es (bis auf Isometrie) genau fünf solcher Codes, welche mit $C81$ (erweiterter quadratischer residualer Code), $C82$ (Reed-Muller Code), $C83$, $C84$ und $C85$ bezeichnet sind. Um zu beweisen, dass keiner dieser Codes als $\pi(F_\sigma(C))$ auftreten kann, gehen wir wie folgt vor:

Sei C_0 einer dieser Codes. Wir wissen nicht, welche Koordinaten zu den Fixpunkten von σ gehören. Wir kennen lediglich die Anzahl - nämlich 10. Deswegen wählen wir alle möglichen 10-elementigen Teilmengen von $1, \ldots, 32$ und benutzen sie als Koordinaten der Fixpunkte. Für jeden Fall konstruieren wir $\pi^{-1}(C_0)$ und berechnen die minimale Distanz mit MAGMA. Es stellt sich heraus, dass alle kleiner als 24 sind. Deshalb können keine der fünf extremalen doppeltgeraden Codes der Länge 32 als $\pi(F_\sigma(C))$ auftreten, ein Widerspruch. ∎

3.1.16 Bemerkung. Es ist möglich, die Berechnung im letzten Beweis zu beschleunigen, indem man die Tatsache ausnutzt, dass die Automorphismengruppen von $C81$ und $C82$ 2-fach transitiv sind. Dadurch können wir die ersten beiden Koordinaten in jeder 10-elementigen Menge festsetzen. Die anderen Automorphismengruppen sind nur transitiv (durch MAGMA). In diesen Fällen kann nur eine Koordinate festgesetzt werden.

Wegen der vorherigen Ergebnisse gilt der folgende Satz:

3.1.17 Satz. *Ein Automorphismus eines selbstdualen* $[120, 60, 24]$*-Codes der Ordnung* 5 *hat keine Fixpunkte.*

3.1.18 Bemerkung. Sei $\sigma \in \mathrm{Aut}(C)$ von der Ordnung 5. Dann ist σ vom Typ 5-$(24; 0)$. Wegen Satz 1.5.2 ist $\pi(F_\sigma(C))$ ein selbstdualer $[24, 12]$-Code. Weiterhin, da $5 - 1 \equiv 0 \mod 4$ ist, ist $\pi(F_\sigma(C))$ ein selbstdualer doppeltgerader $[24, 12]$-Code. Also wissen wir nach [49], dass $\pi(F_\sigma(C))$ äquivalent zu A_{24}, B_{24}, C_{24}, D_{24}, E_{24}, F_{24} oder G_{24} ist. Da $f = 0$ ist, ist jeder Vektor in $\pi(F_\sigma(C))$ vom Gewicht 4 ein Vektor in $F_\sigma(C)$ vom Gewicht 20. Dementsprechend ist die einzige Möglichkeit $\pi(F_\sigma(C)) \sim G_{24}$ und das Gewichtspolynom von $F_\sigma(C)$ ist

$$W_{F_\sigma(C)}(y) = 1 + 759y^{40} + 2576y^{60} + 759y^{80} + y^{120}.$$

3.1.3 Automorphismen der Ordnung 7

3.1.19 Lemma. *Sei* C *ein selbstdualer* $[120, 60, 24]$*-Code. Dann hat* C *keinen Automorphismus der Ordnung* 7 *vom Typ* 7-$(15; 15)$.

Beweis. Sei $\sigma \in \mathrm{Aut}(C)$ vom Typ 7-$(15; 15)$. Dann gilt $c = f = 15$ und $p + c = 7 + 15 < 24 = d$. Wegen Satz 1.6.4 gibt es keinen Automorphismus mit diesen Parametern. ∎

3.1.20 Lemma. *Sei* C *ein selbstdualer* $[120, 60, 24]$*-Code. Dann hat* C *keinen Automorphismus der Ordnung* 7 *vom Typ* 7-$(16; 8)$.

Beweis. Sei σ ein Automorphismus vom Typ 7-$(16; 8)$. Dann ist $\pi(F_\sigma(C))$ ein selbstdualer $[24, 12, d_\pi]$-Code. Wegen des Satzs 1.3.1 ergibt sich $d_\pi \leq 8$. Falls $d_\pi = x + y$, wobei x die Anzahl der Nicht-Null-Einträge der ersten 16 Koordinaten und y diejenige der letzten 8 Koordinaten ist, dann ist $x + y \leq 8$ und $7x + y \geq 24$. Deswegen ist $x \geq 3$ und $d_\pi = 4$, 6 oder 8.

Insgesamt gibt es 30 selbstduale $[24, 12, d_\pi]$-Codes (siehe [49], [15]), einen mit $d_\pi = 8$, einen mit $d_\pi = 6$ und 28 mit $d_\pi = 4$.

Wenn $d_\pi = 8$ ist, dann ist $\pi(F_\sigma(C))$ der Golay Code. Das Gewichtspolynom des Golay Codes ist $1 + 759y^8 + 2576y^{12} + 759y^{16} + y^{24}$. Wir wissen, dass ein Vektor in $F_\sigma(C)$ vom Gewicht 28 nur von Vektoren von $\pi(F_\sigma(C))$ mit Gewicht 4 und 10 geformt werden kann, da $28 = 4 \cdot 7 + 0$ und $28 = 3 \cdot 7 + 7$ ist. Deshalb hat $F_\sigma(C)$ keine Codewörter des Gewichts 28. Dies jedoch widerspricht der Tatsache, dass die Anzahl A_{28} (siehe Lemma 3.1.11) der Codewörter von C mit Gewicht 28, $A_{28} = 6101289120 \equiv 3 \mod 7$ erfüllt.

Falls $d_\pi = 6$ ist, dann ist $\pi(F_\sigma(C))$ der Code Z_{24} (siehe [15], Tabelle E). Für diesen Fall betrachten wir alle Möglichkeiten für die 8 Fixpunkte und konstruieren $\pi^{-1}(Z_{24})$. In allen Fällen finden wir durch Berechnung mit MAGMA einen Vektor, dessen Gewicht kleiner als 24 oder nicht durch 4 teilbar ist.

Somit verbleibt der Fall $d_\pi = 4$. Man führe sich nun die folgende Tatsache vor Augen:

Wenn ein Vektor von $\pi(F_\sigma(C))$ ein Gewicht von 4 hat, dann korrespondieren alle nicht Null-koordinaten zu Zyklen, da C Minimaldistanz 24 hat. Falls daher $\pi(F_\sigma(C))$ die Komponenten d_n oder e_n hat (für die Bezeichnung siehe [49]), so sind die zugehörigen Koordinaten Zyklen. Durch diese Beobachtung stellen wir leicht fest, dass σ weniger als 8 Fixpunkte hat, es sei denn $\pi(F_\sigma(C))$ ist vom Typ X_{24} oder Y_{24}. Der Fall $\pi(F_\sigma(C)) = X_{24}$ kann nicht auftreten, da es einen Vektor vom Gewicht 30 in C ergibt.

Der letzte Fall, Y_{24} wurde mit MAGMA genau wie Z_{24} ausgeschlossen. ∎

Wegen der vorherigen Ergebnisse gilt folgender Satz

3.1.21 Satz. *Ist C ein selbstdualer $[120, 60, 24]$-Code, so ist ein Automorphismus der Ordnung 7 vom Typ 7-$(17; 1)$.*

3.1.22 Definition. [33] Ein *Duo* ist ein Paar von Koordinaten eines Codes. Ein *Cluster* für einen Code ist eine Menge von disjunkten Duos, so dass die Vereinigung zweier verschiedener Duos den Träger eines Codes mit Gewicht vier bildet.

3.1.23 Bemerkung. Sei $\sigma \in \mathrm{Aut}(C)$ vom Typ 7-$(17; 1)$. Wegen Satz 1.5.2 ist $\pi(F_\sigma(C))$ ein selbstdualer $[18, 9]$-Code. Nach [46] wissen wir, dass $\pi(F_\sigma(C))$ äquivalent ist zu

$$C_2^9,\ C_2^5 \oplus A_8,\ C_2^3 \oplus B_{12},\ C_2^3 \oplus D_{14},\ C_2 \oplus E_{16},\ C_2 \oplus A_8^2,\ C_2 \oplus F_{16},\ H_{18} \text{ oder } I_{18}.$$

Wenn $\pi(F_\sigma(C))$ als direkten Summanden C_2 hat, so gibt es einen Vektor in $F_\sigma(C)$ vom Gewicht 8 oder 14, ein Widerspruch. Deshalb sind H_{18} und I_{18} die einzigen Möglichkeiten.

Ein Vektor vom Gewicht 4 in $\pi(F_\sigma(C))$ ist ein Vektor vom Gewicht 4, 10, 16, 22 oder 28 in $F_\sigma(C)$. Da C ein doppeltgerader Code mit $d = 24$ ist, ist nur 28 möglich. Das heißt, alle Koordinaten ungleich Null dieses Vektors sind Zyklen. Wir wissen, dass

$$\mathrm{gen}(H_{18}) = \begin{pmatrix}
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\\
1&0&1&0&1&0&1&0&1&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&1&0&1&0&1&0&1&0&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{pmatrix}$$

ist.

Dann sind $M_1 = \{\{1, 2\}, \{3, 4\}, \{5, 6\}\}$, $M_2 = \{\{7, 8\}, \{9, 10\}, \{11, 12\}\}$ und $M_3 = \{\{13, 14\}, \{15, 16\}, \{17, 18\}\}$ Cluster von $\mathrm{gen}(H_{18})$. Daher kann keine Koordinate ein Fixpunkt sein.

Dementsprechend ist $\pi(F_\sigma(C)) \sim I_{18}$, wobei

$$\mathrm{gen}(I_{18}) = \begin{pmatrix}
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&1&0&1&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{pmatrix}.$$

Da $M_4 = \{\{1, 2\}, \{3, 4\}, \{5, 6\}, \{7, 8\}, \{9, 10\}\}$ und $M_5 = \{\{12, 13\}, \{14, 15\}, \{16, 17\}\}$ Cluster von I_{18} sind, sind die 11-te und die 18-te die einzigen möglichen Koordinaten für

Fixpunkte. Wenn die 18-te Koordinate ein Fixpunkt wäre, so gibt es einen Vektor vom Gewicht 22, ein Widerspruch. Deshalb ist die 11-te Koordinate der einzige Fixpunkt und wir erhalten

$$\mathrm{gen}(F_\sigma(C)) = \left(\begin{array}{cccccccccccccccc|c} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & 1 \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & 1 \end{array}\right)$$

wobei **1** und **0** ein Vektor der Länge 7 mit den Einträgen alle 1 und 0 ist. Deshalb ist das Gewichtspolynom von $F_\sigma(C)$

$$W_{F_\sigma(C)}(y) = 1 + 17y^{28} + 51y^{36} + 187y^{56} + 187y^{64} + 51y^{84} + 17y^{92} + y^{120}.$$

3.1.4 Automorphismen der Ordnung 11

3.1.24 Satz. *Ein selbstdualer* $[120, 60, 24]$*-Code* C *hat keinen Automorphismus der Ordnung* 11*.*

Beweis. Sei $\sigma \in \mathrm{Aut}(C)$ der Ordnung 11. Dann gilt $c = f = 10$ nach Tabelle 3.2. Deswegen ist $p + c = 11 + 10 < 24 = d$. Wegen Satz 1.6.4 gibt es keinen Automorphismus mit diesen Parametern. ∎

3.1.5 Automorphismen der Ordnung 13

3.1.25 Satz. *Ein selbstdualer* $[120, 60, 24]$*-Code* C *hat keinen Automorphismus der Ordnung* 13*.*

Beweis. Ist σ ein Automorphismus der Ordnung 13, so ist er vom Typ 13-$(9; 3)$ nach Tabelle 3.2. Da $13 \equiv 1 \mod 4$ und $13 \not\equiv 1 \mod 8$ ist c gerade wegen 1.5.3, ein Widerspruch. ∎

3.1.6 Automorphismen der Ordnung 17

3.1.26 Satz. *Ein selbstdualer* $[120, 60, 24]$*-Code* C *hat keinen Automorphismus der Ordnung* 17*.*

Beweis. Falls σ ein Automorphismus der Ordnung 17 ist, dann hat er Typ 17-$(7; 1)$ nach Tabelle 3.2. Da $s(17) = 8$ gerade ist, ist die Anzahl der Zyklen c gerade wegen 1.5.13, ein Widerspruch zu $c = 7$. ∎

3.1.27 Bemerkung. Im Beweis von 3.1.26 kann man weder 1.5.3 noch 1.5.6 (2) anwenden.

3.1.7 Automorphismen der Ordnung 59

3.1.28 Satz. *Ein selbstdualer* $[120, 60, 24]$*-Code* C *hat keinen Automorphismus der Ordnung* 59.

Beweis. Sei $\sigma \in \mathrm{Aut}(C)$ vom Typ 59-$(2;2)$. Wegen Satz 1.5.2 ist $\pi(F_\sigma(C))$ ein selbstdualer $[4,2]$-Code. Nach [46] wissen wir, dass $\pi(F_\sigma(C)) = C_2 \oplus C_2$. Somit ist

$$\mathrm{gen}(\pi(F_\sigma(C))) = \left(\begin{array}{cc|cc} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{array}\right).$$

Deshalb können wir

$$\mathrm{gen}(F_\sigma(C)) = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 1 \end{array}\right)$$

wählen, wobei $\mathbf{1}$ der Vektor mit ausschließlich 1-Einträgen und $\mathbf{0}$ der Nullvektor der Länge 59 ist.

Da $s(59) = 58$ ist, gibt es nur zwei zyklotomische Klassen mod 59 über $\mathbb{F}_2$. Deshalb ist die Zerlegung von $x^{59} - 1$ in irreduzible Polynome in $\mathbb{F}_2[x]$ gleich

$$x^{59} - 1 = (x+1)(1 + x + x^2 + \ldots + x^{58}).$$

Wir erhalten mit Lemma 1.5.7, dass $P = \langle x - 1\rangle \subseteq \mathbb{F}_2[x]/\langle x^{59} - 1\rangle$ ein Körper mit der Identität $e(x) = x + x^2 + \ldots + x^{58}$ ist.

Nach Satz 1.5.10 gilt dann, dass $\varphi(E_\sigma(C)^*)$ ein selbstdualer $[2,1]$-Code über dem Körper P mit dem Skalarprodukt

$$u \cdot v = u_1(x)v_1(x)^{2^{29}} + u_2(x)v_2(x)^{2^{29}}$$

ist.

Deshalb wird $\varphi(E_\sigma(C)^*)$ von einem Vektor $(m(x), n(x)) \in P^2$ erzeugt. Aufgrund der Orthogonalitätsbedingung erhalten wir $m(x) \neq 0 \neq n(x)$. Dann wird $\varphi(E_\sigma(C)^*)$ auch durch $(e(x), m(x)^{-1}n(x))$ erzeugt, also

$$\mathrm{gen}(\varphi(E_\sigma(C)^*)) = (e(x), a(x)),$$

wobei $e(x) = x + x^2 + \ldots + x^{58}$ die Identität von P ist und $0 \neq a(x) \in P$.

Man bestätigt mit MAGMA, dass $\alpha(x) = x^{55} + x^{51} + x^{50} + x^{48} + x^{42} + x^{39} + x^{35} + x^{29} + x^{23} + x^{20} + x^{10} + x^9 + x^3 + x$ ein primitives Element im Körper P ist. Da P ein Körper mit $|P| = 2^{58}$ ist, erhalten wir $a(x) = \alpha(x)^t$ für ein t mit $0 \leq t \leq 2^{58} - 2$.

Deshalb gilt

$$\mathrm{gen}(\varphi(E_\sigma(C)^*)) = (e(x), \alpha(x)^t),$$

wobei $0 \leq t \leq 2^{58} - 2$ ist.

Es gibt viele Werte für t und damit viele Codes. Wir reduzieren nun die Anzahl der Möglichkeiten. Aufgrund der Orthogonalitätsbedingung erhalten wir

$$(e(x), a(x)) \cdot (e(x), a(x)) = e(x) + \alpha(x)^{(2^{29}+1)t} = 0.$$

Also gilt $e(x) = \alpha(x)^{(2^{29}+1)t}$, $0 \leq t \leq 2^{58} - 2$. Da $\alpha(x)$ ein primitives Element von P ist, ist $\mathrm{ord}(\alpha(x)) = 2^{58} - 1$. Weiterhin gilt $2^{58} - 1 \mid (2^{29} + 1)t$, das heißt $(2^{29} + 1)t \equiv 0 \bmod (2^{58} - 1)$. Daher ist $t \equiv 0 \mod (2^{29} - 1)$ und wir erhalten

$$a(x) = \alpha(x)^t = \alpha(x)^{k(2^{29}-1)} = (\alpha(x)^{(2^{29}-1)})^k,$$

für eine ganze Zahl k.

Wegen

$$\mathrm{ord}(\alpha(x)^{(2^{29}-1)}) = \frac{\mathrm{ord}(\alpha(x))}{(\mathrm{ord}(\alpha(x)), 2^{29}-1)} = \frac{2^{58}-1}{2^{29}-1} = 2^{29}+1$$

können wir nun $a(x) = (\alpha(x)^{(2^{29}-1)})^k$ für eine ganze Zahl k mit $0 \leq k \leq 2^{29}$ annehmen. Damit haben wir die Möglichkeiten reduziert.

Setzen wir $\delta(x) := \alpha(x)^{2^{29}-1}$, so erhalten wir $a(x) = \delta(x)^k$ mit $0 \leq k \leq 2^{29}$. Nach Lemma 1.5.6 gilt dann

$$\mathrm{gen}(C) = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 1 \\ \hline [\mathrm{e(x)}] & [\delta(x)^k] & 0 & 0 \end{array}\right), \tag{3.4}$$

wobei $\mathbf{1}$ und $\mathbf{0}$ Vektoren der Länge 59 mit den Koordinaten alle 1 bzw. alle 0 sind. Ferner sind $[e(x)]$, $[\delta(x)^k]$ zirkulante 58×59-Matrizen und $0 \leq k \leq 2^{29}$. Dies liefert $2^{29}+1$ Codes, von denen einige äquivalent sein können.

Sei $\beta(x) = 1+x^2+\ldots+x^{58}$. Da $1+x+\ldots+x^{58}$ irreduzibel in $\mathbb{F}_2[x]$ ist, folgt nach 1.5.8, dass $H = \langle\beta(x)\rangle$ die einzige Untergruppe der Ordnung 59 in $P\backslash\{0\}$ ist und $\beta(x), \beta(x)^2, \ldots, \beta(x)^{58}$ die einzigen Elemente der Ordnung 59 sind.

Wegen

$$\mathrm{ord}(\delta(x)^{\frac{2^{29}+1}{59}}) = \frac{2^{29}+1}{(\frac{2^{29}+1}{59}, 2^{29}+1)} = 59$$

erhalten wir $\langle\delta(x)^{\frac{2^{29}+1}{59}}\rangle = \langle\beta(x)\rangle$. Deshalb ist $\langle\beta(x)\rangle \leq \langle\delta(x)\rangle$.

Wir wissen, dass $\langle\delta(x)\rangle/\langle\beta(x)\rangle = \langle\delta(x)\langle\beta(x)\rangle\rangle$ ist. Da $|\langle\delta(x)\rangle/\langle\beta(x)\rangle| = \frac{|\langle\delta(x)\rangle|}{|\langle\beta(x)\rangle|} = \frac{2^{29}+1}{59}$ gilt, ist

$$\langle\delta(x)\rangle/\langle\beta(x)\rangle = \{\langle\beta(x)\rangle, \delta(x)\langle\beta(x)\rangle, \delta(x)^2\langle\beta(x)\rangle, \ldots, \delta(x)^{\frac{2^{29}+1}{59}-1}\langle\beta(x)\rangle\},$$

d.h. $\langle\delta(x)\rangle = \cup_{i=0}^{\frac{2^{29}+1}{59}-1} \delta(x)^i\langle\beta(x)\rangle$.

Mit der folgenden Bemerkung erhalten wir eine signifikante Reduktion. Seien $g(x)$, $c(x)$ zwei Vertreter der gleichen Nebenklasse von $\langle\beta(x)\rangle$ in $\langle\delta(x)\rangle$ und seien C_1 und C_2 die Codes, die $(e(x), g(x))$ und $(e(x), c(x))$ in der Erzeugermatrix (3.4) enthalten. Da $g(x), c(x) \in \delta(x)^i\langle\beta(x)\rangle$ für $0 \leq i \leq \frac{2^{29}+1}{59} - 1$, gilt $g(x) = \beta(x)^t c(x)$ für ein $0 \leq t \leq 58$. Wegen 1.5.8 (1) ist $x^t e(x) \equiv \beta(x)^t \mod (x^{59}-1)$. Deshalb erhalten wir C_2 aus C_1 nach einer Multiplikation der zweiten Koordinate von $\varphi(E_\sigma(C)^*)$ mit x^t für $0 \leq t \leq 58$. Es folgt wegen 1.5.11 (2), dass C_1 und C_2 äquivalent sind.

Daher müssen wir jetzt nur noch $\frac{2^{29}+1}{59} = 9099507$ Codes mit der Erzeugermatrix

$$\mathrm{gen}(C) = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 1 \\ \hline [\mathrm{e(x)}] & [\delta(x)^t] & 0 & 0 \end{array}\right)$$

analysieren.

Die Anzahl der Möglichkeiten lässt sich allerdings noch weiter verringern. Seien C_1 und C_2 Codes, die $(e(x), \delta(x)^i)$ und $(e(x), \delta(x)^{2i})$ in der Erzeugermatrix enthalten. Wenn wir die Substitution $x \to x^2$ auf $(e(x), \delta(x)^i) \in \varphi(E_\sigma(C)^*)$ anwenden, dann erhalten wir

$$(e(x^2), \delta(x^2)^i) = (e(x), \delta(x)^{2i}).$$

Somit können wir C_2 aus C_1 durch die Substitution $x \to x^2$ erhalten. Daher sind C_2 und C_1 äquivalente Codes nach 1.5.11 (1).

Wir wissen, dass die Operation $t \to 2t$ die Menge $\mathbb{Z}_{9099507}$ in Bahnen unterteilt. Diese Bahnen sind $O(t) = \{t2^n \mod 9099507 \mid n \in \mathbb{Z}\}$, wobei $t \in \mathbb{Z}_{9099507}$. Wegen der vorangegangenen Bemerkung wissen wir, dass, wenn t_1, t_2 in der gleichen Bahn liegen, die zugehörigen Codes äquivalent sind. Mit MAGMA erhalten wir, dass die Anzahl der Bahnen 156889 ist. Wir haben mit MAGMA auch einen Vertreter t' für jede dieser Bahnen berechnet. Somit bleiben nur noch Codes mit der Erzeugermatrix

$$\mathrm{gen}(C) = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 1 \\ \hline [\mathrm{e(x)}] & [\alpha(x)^{(2^{29}-1)t'}] & 0 & 0 \end{array}\right)$$

zu untersuchen, wobei t' ein Vertreter der 156889 Bahnen ist.

Mittels MAGMA haben wir in jedem Code ein Codewort vom Gewicht kleiner als 24 gefunden. Deshalb hat ein selbstdualer $[120, 60, 24]$-Code C keinen Automorphismus σ der Ordnung 59. ∎

Wir haben zusammenfassend den folgenden Satz bewiesen:

3.1.29 Satz. *Sei C ein selbstdualer Code der Länge 120. Falls σ ein Automorphismus von C von ungerader Primzahlordnung p ist, so ist $p = 3, 5, 7, 19, 23$ oder 29 und seine Zyklen-Struktur gegeben durch folgende Tabelle*

p	*Anzahl der p-Zyklen*	*Anzahl der Fixpunkte*
3	40	0
5	24	0
7	17	1
19	6	6
23	5	5
29	4	4

3.1.30 Satz. *Sei C ein selbstdualer $[120, 60, 24]$-Code und p eine ungerade Primzahl. Dann gilt $p^2 \nmid |\mathrm{Aut}(C)|$.*

Beweis. Sei p eine ungerade Primzahl. Nach Satz 3.1.29 hat ein Automorphismus σ der Ordnung p nur Typ p-$(c; f)$ mit $c \not\equiv 0 \mod p$ und $f < p$. Dann gilt $p^2 \nmid |\mathrm{Aut}(C)|$, nach Satz 1.4.7. ∎

3.1.8 Automorphismen von ungerader zusammengesetzter Ordnung

3.1.31 Satz. *Sei C ein selbstdualer $[120, 60, 24]$-Code und sei $\sigma \in \mathrm{Aut}(C)$ von Ordnung $p \cdot q$, wobei p und q zwei verschiedene Primzahlen sind. Dann ist die Ordnung gleich $3 \cdot 5$, $3 \cdot 19$ oder $5 \cdot 23$ und die Zyklen-Struktur von σ ist $3 \cdot 5$-$(0, 0, 8; 0)$, $3 \cdot 19$-$(2, 0, 2; 0)$ oder $5 \cdot 23$-$(1, 0, 1; 0)$.*

Beweis.

- Angenommen, σ ist ein Automorphismus vom Typ $3 \cdot 5\text{-}(s_1, s_2, s_3; f)$, wobei $120 = 3s_1 + 5s_2 + 15s_3 + f$. Nach Lemma 1.4.5 gibt es auch Automomorphismen vom Typ $3\text{-}(s_1 + 5s_3; 5s_2 + f)$ und Typ $5\text{-}(s_2 + 3s_3; 3s_1 + f)$. Wegen Satz 3.1.29 gilt

$$s_1 + 5s_3 = 40, \quad 5s_2 + f = 0, \quad s_2 + 3s_3 = 24 \text{ und } 3s_1 + f = 0.$$

  Daher hat σ nur Typ $3 \cdot 5\text{-}\ (0, 0, 8; 0)$

- Sei σ ein Automorphismus vom Typ $3{\cdot}19\text{-}(s_1, s_2, s_3; f)$, wobei $120 = 3s_1{+}19s_2{+}57s_3{+}f$. Nach Lemma 1.4.5 hat C auch Automorphismen vom Typ $3\text{-}(s_1 + 19s_3; 19s_2 + f)$ und $19\text{-}(s_2 + 3s_3; 3s_1 + f)$. Wegen Satz 3.1.29 gilt

$$s_1 + 19s_3 = 40, \quad 19s_2 + f = 0, \quad s_2 + 3s_3 = 6 \text{ und } 3s_1 + f = 6.$$

  Daher hat σ Typ $3 \cdot 19\text{-}(2, 0, 2; 0)$.

- Falls σ ein Automorphismus vom Typ $5 \cdot 23\text{-}(s_1, s_2, s_3; f)$ ist, wobei $120 = 5s_1 + 23s_2 + 115s_3 + f$ ist, dann hat C Automorphismen vom Typ $5\text{-}(s_1 + 23s_3; 23s_2 + f)$ und Typ $23\text{-}(s_2 + 5s_3; 5s_1 + f)$. Wegen Satz 3.1.29 gilt

$$s_1 + 23s_3 = 24, \quad 23s_2 + f = 0, \quad s_2 + 5s_3 = 5 \text{ und } 5s_1 + f = 5.$$

  Daher ist σ vom $5 \cdot 23\text{-}(1, 0, 1; 0)$.

- Angenommen, dass C ein Automorphismus σ vom Typ $3 \cdot 7\text{-}(s_1, s_2, s_3; f)$ ist, wobei $120 = 3s_1{+}7s_2{+}21s_3{+}f$ ist. Dann gibt es Automorphismen vom Typ $3\text{-}(s_1{+}7s_3; 7s_2{+}f)$ und $7\text{-}(s_2 + 3s_3; 3s_1 + f)$. Wegen Satz 3.1.29 erhalten wir

$$s_1 + 7s_3 = 40, \quad 7s_2 + f = 0, \quad s_2 + 3s_3 = 17 \text{ und } 3s_1 + f = 1,$$

  was keine Lösungen in $\mathbb{N}_0$ hat.

- Angenommen nun, dass C ein Automorphismus σ vom Typ $7 \cdot 5\text{-}(s_1, s_2, s_3; f)$ ist, wobei $120 = 7s_1 + 5s_2 + 35s_3 + f$ ist. Nach Lemma 1.4.5 hat C auch Automorphismen vom Typ $7\text{-}(s_1 + 5s_3; 5s_2 + f)$ und $5\text{-}(s_2 + 7s_3; 7s_1 + f)$. Wegen Satz 3.1.29 erhalten wir $s_1 + 5s_3 = 17$, $5s_2 + f = 1$, $s_2 + 7s_3 = 24$ und $7s_1 + f = 0$. Dies System hat wieder keine Lösung in $\mathbb{N}_0$ hat. ∎

In ähnlicher Weise findet man in den Fällen $3 \cdot 23$, $3 \cdot 29$, $5 \cdot 19$, $5 \cdot 29$, $7 \cdot 19$, $7 \cdot 23$, $7 \cdot 29$, $19 \cdot 23$, $19 \cdot 29$ und $23 \cdot 29$ ebenfalls keine Lösungen in $\mathbb{N}_0$.

Nach Satz 3.1.30 gibt es keinen Automorphismus der Ordnung p^2 für alle Primzahlen $p \geq 3$. Deswegen haben wir zusammenfassend den folgenden Satz bewiesen

3.1.32 Satz. *Sei C ein selbstdualer Code der Länge 120. Ist σ ein Automorphismus von C von ungerader zusammengesetzter Ordnung r, so ist $r = 15$, 57 oder 115 und die Zyklen-Struktur von σ ist $3 \cdot 5\text{-}(0, 0, 8; 0)$, $3 \cdot 19\text{-}(2, 0, 2; 0)$ oder $5 \cdot 23\text{-}(1, 0, 1; 0)$.*

3.1.9 Die Ordnung der Automorphismengruppe G im Fall 19, 23, $29 \nmid |G|$ und fixpunktfreien Operation von Involutionen

Nach 3.1.29 und 3.1.30 ist die Ordnung der Automorphismengruppe $G = \mathrm{Aut}(C)$ eines selbstdualen $[120, 60, 20]$-Codes C gegeben durch $|G| = 2^a \cdot 3^b \cdot 5^c \cdot 7^d \cdot 19^e \cdot 23^f \cdot 29^g$, wobei $a \in \mathbb{N}_0$ und $b, c, d, e, f, g \in \{0, 1\}$ ist.

Wie in den Fällen $n = 72$ und $n = 96$ vermuten wir, dass $|G|$ nur kleine Primteiler hat, d.h. die Primzahlen nur 2, 3, 5, 7. Wir vermuten auch, dass die Involutionen keine Fixpukte haben. Wenn wir dies annehmen, so hat $|G|$ kein Element ungerader Ordnung größer als 7 ungleich 15 und $|G| = 2^a 3^b 5^c 7^d$ mit $a \in \mathbb{N}_0$ und $0 \leq b, c, d \leq 1$. Ferner ist $a \leq 3$ wegen 1.4.8.

Zur Berechnung der Anzahl der Bahnen der Wirkung von G auf 120 Koordinaten von C verwenden wir wieder das Cauchy-Frobenius Lemma

$$t = \frac{1}{|G|} \sum_{g \in G} \mathrm{Fix}(g).$$

Wegen unserer Annahme haben wir

$$\mathrm{Fix}(g) = \begin{cases} 0, & \text{wenn } \mathrm{ord}(g) \text{ gerade ist;} \\ 0, & \text{wenn } \mathrm{ord}(g) = 3, 5 \text{ oder } 15 \text{ ist;} \\ 1, & \text{wenn } \mathrm{ord}(g) = 7 \text{ ist.} \end{cases}$$

3.1.33 Satz. *Die Ordnung der Automorphismengruppe vom Code C ist 7, 56 oder ein Teiler von 120.*

Beweis. Sei $|G| = 2^a 3^b 5^c 7$. Dann ist

$$t = \frac{1}{2^a 3^b 5^c 7}(120 + \sum_{|g|=7} 1) = \frac{1}{2^a 3^b 5^c 7}(120 + 6n_7).$$

Nach Lemma 1.4.9 haben wir $|N_G(\tau_7)| = 7$. Da $n_7 = \frac{|G|}{|N_G(\tau_7)|} = \frac{2^a 3^b 5^c 7}{7} = 2^a 3^b 5^c$ ist, erhalten wir

$$t = \frac{120}{2^a 3^b 5^c 7} + \frac{6}{7},$$

was nur die ganzzahligen Lösungen

$$(0, 0, 0), (3, 0, 0), (0, 1, 1), (3, 1, 1)$$

für (a, b, c) hat.

Im Fall $(a, b, c) = (0, 1, 1)$ ist $|G| = 105$. Mit MAGMA erhalten wir, dass zwei Gruppen G der Ordnung 105 existieren, alle mit $|N_G(\tau_7)| = 105 \neq 7$.

Im letzteren Fall $(a, b, c) = (3, 1, 1)$ ist $|G| = 840$. Man bestätigt mit MAGMA, dass es genau 186 Gruppen der Ordnung 840 gibt, alle mit $|N_G(\tau_7)| = 105, 840 \neq 7$.

Daher ist $|G| = 7$ oder 56.

Sei $|G| = 2^a 3^b 5^c$. Dann hat die Gruppe G kein Element der Ordnung 7 und $t = \frac{120}{2^a 3^b 5^c}$. Daher ist $|G|$ ein Teiler von 120. ∎

3.1.34 Bemerkung. 1. Mit darstellungstheoretische Argumenten können weitere Gruppen ausgeschlossen werden, etwa $\mathrm{SL}(2,5)$.

2. Mittels MAGMA sehen wir, dass 13 Gruppen G der Ordnung 56 existieren, von denen nur eine $|N_G(\tau_7)| = 7$ erfüllt. Deshalb gibt es nur eine Gruppe der Ordnung 56 als mögliche Automorphismengruppe G.

3.2 Über die Struktur extremaler $[120, 60, 24]$-Codes C mit einem Automorphismus der Ordnung 29 oder 19

Aufgrund der Größe eines selbstdualen $[120, 60, 24]$-Codes ist es nicht einfach, die Primzahlen 29, 19 und 23 auszuschließen. In diesem Abschnitt analysieren wir die Struktur eines Codes mit einem Automorphismus der Ordnung 29 bzw. 19. Dies benutzen wir später um einen selbstdualen doppeltgeraden $[120, 60, 20]$-Code zu konstruieren. Hierbei verwenden wir Resultate aus den Arbeiten [35] und [59]. Die Struktur eines selbstdualen $[120, 60, 24]$-Codes mit einem Automorphismus der Ordnung 23 ist in [62] von Yorgova und Wassermann studiert worden, um neue selbstduale doppeltgerade $[120, 60, 20]$-Codes zu konstruieren mit einem Automorphismus mit dieser Ordnung.

3.2.1 Automorphismen der Ordnung 29

Sei C ein selbstdualer $[120, 60, 24]$-Code und σ ein Automorphismus der Ordnung 29. Nach Satz 3.1.2 ist σ vom Typ 29-$(4; 4)$. Dann ist $\pi(F_\sigma(C))$ ein selbstdualer $[8, 4]$-Code. Da $29-1 \equiv 0 \bmod 4$ ist, ist $\pi(F_\sigma(C))$ ein selbstdualer doppeltgerader $[8, 4]$-Code über $\mathbb{F}_2$. Also wissen wir nach [46], dass $\pi(F_\sigma(C)) \sim A_8$ oder $\pi(F_\sigma(C)) \sim C_2^4$, wobei:

$$\mathrm{gen}(A_8) = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \tag{3.5}$$

$$\mathrm{gen}(C_2^4) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Da C_2^4 nicht doppeltgerade ist, ist $\pi(F_\sigma(C)) \sim A_8$. Wir wissen jedoch nicht, welche Spalten den Fixpunkten entsprechen.

Sei $\sum A_i y^i$ und $\sum A_i^F y^i$ das Gewichtspolynom von C bzw. $F_\sigma(C)$. Nach 1.5.4 ist $A_{32} \equiv A_{32}^F \bmod 29$. Wegen 3.1.11 wissen wir, dass $A_{32} = 475644139425 \equiv 4 \bmod 29$ ist. Deshalb gibt es $4 \bmod 29$ Vektoren von $F_\sigma(C)$ mit Gewicht 32.

Für jedes $v \in \{u \in C \mid u \in F_\sigma(C) \text{ und } \mathrm{wt}(u) = 32\}$ ist das Gewicht $\mathrm{wt}(v)$ von der Form $\mathrm{wt}(v) = 29 \cdot 1 + 3$. Damit ist $\mathrm{wt}(\pi(v)) = 4$.
Angenommen $v_1, v_2 \in \{u \in C \mid u \in F_\sigma(C) \text{ und } \mathrm{wt}(u) = 32\}$ stimmen in den Koordinaten eines Zyklus überein. Dann ist $\mathrm{wt}(v_1 + v_2) \leq 2$. Deshalb gibt es genau 4 Vektoren in $F_\sigma(C)$

mit $\mathrm{wt}(v) = 32$. Diese sind in $\pi(F_\sigma(C))$ linear unabhängig und bis auf Permutationen der letzten vier Spalten ist:

$$\mathrm{gen}(\pi(F_\sigma(C))) = \left(\begin{array}{cccc|cccc} 1&0&0&0&0&1&1&1\\ 0&1&0&0&1&0&1&1\\ 0&0&1&0&1&1&0&1\\ 0&0&0&1&1&1&1&0 \end{array}\right). \tag{3.6}$$

(Man kann mit MAGMA überprüfen, dass die Codes, die durch die Matrizen 3.5 und 3.6 erzeugt werden, äquivalent sind.)

Dementsprechend erhalten wir:

$$\mathrm{gen}(F_\sigma(C)) = \left(\begin{array}{cccc|cccc} \mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&0&1&1&1\\ \mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&1&0&1&1\\ \mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&1&1&0&1\\ \mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&1&1&1&0 \end{array}\right), \tag{3.7}$$

wobei $\mathbf{1}$ und $\mathbf{0}$ ein Vektor der Länge 29 mit den Koordinaten alle 1 und alle 0 sind.

Daher ist

$$W_{F_\sigma(C)}(y) = 1 + 4y^{32} + 6y^{60} + 4y^{88} + y^{120}.$$

3.2.1 Lemma. *Sei* $L := \{(i,j)(i+4,j+4) \in S_8 \mid 1 \le i \le 4 \text{ und } 1 \le j \le 4\}$. *Dann ist* $L \subseteq \mathrm{Aut}(\pi(F_\sigma(C)))$.

Beweis. Wegen der Symmetrie der Matrix (3.6) erhalten wir, dass, wenn v eine Zeile von (3.6) ist und $\rho \in L$, dann ist $\rho(v)$ auch eine Zeile von (3.6). ∎

3.2.2 Korollar. *Sei* $\mathrm{gen}(C) = \left(\begin{array}{c|c} X & Y \\ \hline Z & O \end{array}\right)$ *und* $\mathrm{gen}(C') = \left(\begin{array}{c|c} X & Y \\ \hline \xi(Z) & O \end{array}\right)$, *wobei* $(X \mid Y)$ *die Matrix in* (3.7) *ist,* O *die Nullmatrix von geeigneter Größe,* $(Z \mid O) = \mathrm{gen}(E_\sigma(C))$ *und* $\xi \in S_4$ *eine Permutation der* 29*-Zyklen. Dann sind* $C \sim C'$.

Beweis. Offensichtlich wegen 3.2.1. ∎

Da andererseits $s(29) = 28$ ist, ist die Zerlegung von $x^{29} - 1$ in irreduzible Polynome in $\mathbb{F}_2[x]$ gleich $x^{29} - 1 = (x+1)(1 + x + x^2 + \ldots + x^{28})$. Nach Satz 1.5.10 gilt dann, dass $\varphi(E_\sigma(C)^*)$ ein selbstdualer $[4,2]$-Code über dem Körper $P = \langle x+1\rangle \subseteq \mathbb{F}_2[x]/\langle x^{29}-1\rangle$ mit dem Skalarprodukt

$$u \cdot v = u_1 v_1^{2^{14}} + u_2 v_2^{2^{14}} + u_3 v_3^{2^{14}} + u_4 v_4^{2^{14}} \tag{3.8}$$

ist.

3.2.3 Lemma. $\varphi(E_\sigma(C)^*)$ *ist ein selbstdualer* $[4,2,3]$*-Code über* $P \cong \mathbb{F}_{2^{28}}$.

Beweis. $\varphi(E_\sigma(C)^*)$ kann Minimaldistanz 1, 2 oder 3 über P haben.

1. $\varphi(E_\sigma(C)^*)$ hat keinen Vektor von Gewicht 1.

   Sei $v \in \varphi(E_\sigma(C)^*)$ mit $\mathrm{wt}(v) = 1$. Wegen 3.2.2 können wir annehmen, dass $v = (v_1, 0, 0, 0)$ mit $v_1 \in P\backslash\{0\}$. Wenn wir v mit $(x+1)v_1^{-1}$ multiplizieren, dann ist $v = (x+1, 0, 0, 0)$. Deshalb haben wir einen Widerspruch, weil $\mathrm{wt}(\varphi^{-1}(v)) = 2 < 24$ ist.

2. $\varphi(E_\sigma(C)^*)$ hat keinen Vektor vom Gewicht 2.

   Sei $v \in \varphi(E_\sigma(C)^*)$ mit $\mathrm{wt}(v) = 2$. Wegen des Korollars 3.2.2 können wir annehmen, dass $v = (v_1, v_2, 0, 0)$ mit $v_1, v_2 \in P\backslash\{0\}$.

   Sei M der P-Vektorraum, der von v erzeugt wird. Das heißt $M := \{(uv_1, uv_2, 0, 0) \mid u \in P\}$ und $\dim_{\mathbb{F}_2} M = 28$.

   $W := \varphi^{-1}(M) \subseteq E_\sigma(C)^*$ ist ein Code über dem Körper $\mathbb{F}_2$ mit $\dim_{\mathbb{F}_2}(W) = 28$. Da

   $$24 = d(C) \leq d(E_\sigma(C)) = d(E_\sigma(C)^*) \leq d(W),$$

   ist W ein $[116, 28, d']$-Code über $\mathbb{F}_2$ mit $d' \geq 24$.

   Sei $W^* \subseteq \mathbb{F}_2^{58}$ der Code, der von W durch Streichung der letzten 58 Koordinaten gewonnen wird. Dann ist W^* ein $[58, 28, d'']$-Code mit $d'' = d' \geq 24$.
   Deshalb gilt

   $$\lceil(\frac{d''}{2^0})\rceil + \lceil(\frac{d''}{2^1})\rceil + \ldots + \lceil(\frac{d''}{2^{27}})\rceil \geq$$
   $$\lceil\frac{24}{1}\rceil + \lceil\frac{24}{2}\rceil + \lceil\frac{24}{4}\rceil + \lceil\frac{24}{8}\rceil + \lceil\frac{24}{16}\rceil + \lceil\frac{24}{32}\rceil + \ldots + \lceil\frac{24}{2^{27}}\rceil =$$
   $$24 + 12 + 6 + 3 + 2 + (22 + 1)1 = 70 > 58.$$

   Wegen der Griesmer-Schranke haben wir einen Widerspruch.

   Dementsprechend ist $\varphi(E_\sigma(C)^*)$ ein selbstdualer $[4, 2, 3]$-Code über P mit dem Skalarprodukt

   $$v \cdot u = v_1 u_1^{2^{14}} + \ldots + v_4 u_4^{2^{14}},\ \forall v, u \in \varphi(E_\sigma(C)^*).$$

■

Insbesondere ist $\varphi(E_\sigma(C)^*)$ ein MDS-Code. Daher sind in der Erzeugermatrix von $\varphi(E_\sigma(C)^*)$ je $k = 2$ Spalten linear unabhängig. Deshalb können wir

$$\mathrm{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} \alpha^{t_1} & 0 & \alpha^{t_3} & \alpha^{t_5} \\ 0 & \alpha^{t_2} & \alpha^{t_4} & \alpha^{t_6} \end{pmatrix}$$

wählen, wobei α ein primitives Element von P und $0 \leq t_i \leq 2^{28} - 2$ ist.

Andererseits wissen wir, dass $2^{28} - 1 = (2^{14} + 1)(2^{14} - 1)$. Sei $\phi = \alpha^{2^{14}+1}$ und $\delta = \alpha^{2^{14}-1}$. Dann ist $\mathrm{ord}(\phi) = 2^{14} - 1 = 3 \times 43 \times 127$ und $\mathrm{ord}(\delta) = 2^{14} + 1 = 5 \times 29 \times 113$. Da $(\mathrm{ord}(\phi), \mathrm{ord}(\delta)) = 1$, gilt

$$\mathrm{ord}(\phi\delta) = \mathrm{ord}(\phi) \cdot \mathrm{ord}(\delta) = 2^{28} - 1 = \mathrm{ord}(\alpha).$$

Deshalb ist $\phi\delta$ ein weiteres primitives Element des Körpes P. Damit erhalten wir:

$$\mathrm{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} (\phi\delta)^{i_1} & 0 & (\phi\delta)^{i_3} & (\phi\delta)^{i_5} \\ 0 & (\phi\delta)^{i_2} & (\phi\delta)^{i_4} & (\phi\delta)^{i_6} \end{pmatrix},$$

wobei $0 \leq i_1, i_2, i_3, i_4, i_5, i_6 \leq 2^{28} - 2$ ist.

Wir multiplizieren die erste Zeile mit $\delta^{-i_3}\phi^{-i_1}$ und die zweite Zeile mit $\delta^{-i_4}\phi^{-i_2}$. Dann gilt

$$\mathrm{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} \delta^{s_1} & 0 & \phi^{t_1} & \phi^{t_2}\delta^{s_2} \\ 0 & \delta^{s_3} & \phi^{t_3} & \phi^{t_4}\delta^{s_4} \end{pmatrix}, \tag{3.9}$$

wobei $0 \leq s_1, s_2, s_3, s_4 \leq 2^{14},\ 0 \leq t_1, t_2, t_3, t_4 \leq 2^{14} - 2$.

Wir erhalten viele mögliche Werte für t_i, s_i und damit viele mögliche Codes. Deshalb wollen wir die Anzahl der Möglichkeiten reduzieren.

Wir wissen, dass $\langle\delta\rangle/\langle\beta\rangle = \langle\delta\langle\beta\rangle\rangle$ ist, wobei $\beta(x) = 1 + x^2 + x^3 + \ldots + x^{28}$. Nehmen wir als Transversale von $\langle\beta\rangle$ in $\langle\delta\rangle$ die Menge $\{e, \theta, \ldots, \theta^{(5\times 13)-1}\}$, wobei $e(x) = x + x^2 + \ldots + x^{28}$ die Identität von P ist und $\theta = \delta^{29}$ (Man könnte auch wie in Satz 3.1.28 als Transversale die Menge $\{e, \delta, \ldots, \delta^{(5\times 13)-1}\}$ wählen).

Seien $g(x)$, $c(x)$ zwei Vertreter der gleichen Nebenklasse von $\langle\theta\rangle$ in $\langle\delta\rangle$ und seien C_1 und C_2 die Codes, die aus $g(x)$ und $c(x)$ in der Matrix (3.9) abgeleitet werden. Deshalb ist $g(x) = \beta(x)^t c(x)$ für $0 \leq t \leq 28$. Da $x^t e(x) \equiv \beta(x)^t \mod (x^{29} - 1)$ ist, erhalten wir den Code C_2 aus dem Code C_1 nach einer Multiplikation der j-ten Koordinate von $\varphi(E_\sigma(C)^*)$ mit x^t, für $0 \leq t \leq 28$ und $0 \leq j \leq 4$. Dann folgt wegen 1.5.11, dass C_1 und C_2 äquivalent sind.

Daher können wir annehmen, dass

$$\operatorname{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} \theta^{l_1} & 0 & \phi^{t_1} & \phi^{t_2}\theta^{l_2} \\ 0 & \theta^{l_3} & \phi^{t_3} & \phi^{t_4}\delta^{s_5} \end{pmatrix}, \tag{3.10}$$

wobei $0 \leq l_1, l_2, l_3 \leq (5 \times 113) - 1,\ 0 \leq t_1, t_2, t_3, t_4 \leq 2^{14} - 2$ und $0 \leq s_5 \leq 2^{14}$.

Da andererseits die Zeilen der Matrix (3.10) orthogonal bzg. des Skalarproduktes (3.8) sind, erhalten wir

$$(0, \theta^{l_3}, \phi^{t_3}, \phi^{t_4}\delta^{s_5}) \cdot (\theta^{l_1}, 0, \phi^{t_1}, \phi^{t_2}\theta^{l_2}) = \phi^{t_3}\phi^{2^{14}t_1} + \phi^{t_4}\delta^{s_5}\phi^{2^{14}t_2}\theta^{2^{14}l_2} = 0.$$

Wegen $\phi^{2^{14}-1} = e$ und $\theta^{2^{14}+1} = (\theta^{5\times 113})^{29} = e$ erhalten wir $\phi^{2^{14}} = \phi$ und $\theta^{2^{14}} = \theta^{-1}$. Deshalb ist

$$\phi^{t_3+t_1} + \phi^{t_4+t_2}\delta^{s_5}\theta^{-l_2} = 0$$
$$\phi^{t_3+t_1-t_4-t_2} = \delta^{s_5}\theta^{-l_2}.$$

Somit $\operatorname{ord}(\phi^{t_3+t_1-t_4-t_2}) = \operatorname{ord}(\delta^{s_5}\theta^{-l_2})$. Weiterhin wissen wir, dass

$$\operatorname{ord}(\phi^{t_3+t_1-t_4-t_2}) \mid \operatorname{ord}(\phi) = 2^{14} - 1 = 3 \times 43 \times 127$$

und

$$\operatorname{ord}(\delta^{s_5}\theta^{-l_2}) \mid \operatorname{ord}(\delta) = 2^{14} + 1 = 5 \times 29 \times 113.$$

Da $(\operatorname{ord}(\phi), \operatorname{ord}(\delta)) = 1$, gilt $\operatorname{ord}(\phi^{t_3+t_1-t_4-t_2}) = \operatorname{ord}(\delta^{s_5}\theta^{-l_2}) = 1$, d.h

$$\phi^{t_3+t_1-t_4-t_2} = \delta^{s_5}\theta^{-l_2} = e.$$

Also ist $\phi^{t_3+t_1} = \phi^{t_4+t_2}$ und $\delta^{s_5} = \theta^{l_2}$. Somit ist

$$t_4 - t_3 \equiv t_1 - t_2 \mod (2^{14} - 1) \text{ und } \delta^{s_5} = \theta^{l_2},$$

und daher

$$\operatorname{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} \theta^{l_1} & 0 & \phi^{t_1} & \phi^{t_2}\theta^{l_2} \\ 0 & \theta^{l_3} & \phi^{t_3} & \phi^{t_4}\theta^{l_2} \end{pmatrix}, \tag{3.11}$$

wobei $0 \leq l_1, l_2, l_3 \leq (5 \times 113) - 1,\ 0 \leq t_1, t_2, t_3, t_4 \leq 2^{14} - 2$ mit

$$t_4 - t_3 \equiv t_1 - t_2 \mod (2^{14} - 1). \tag{3.12}$$

Wenn wir andererseits jede Zeile in (3.11) mit sich selbst multiplizieren, dann erhalten wir

$$(\theta^{l_1}, 0, \phi^{t_1}, (\phi^{t_2}\theta^{l_2})) \cdot (\theta^{l_1}, 0, \phi^{t_1}, (\phi^{t_2}\theta^{l_2})) = \theta^{(2^{14}+1)l_1} + \phi^{(2^{14}+1)t_1} + (\phi^{(2^{14}+1)t_2}\theta^{(2^{14}+1)l_2}) = 0.$$

Da $\theta^{(2^{14}+1)} = e$, ist $\phi^{(2^{14}+1)t_1} + \phi^{(2^{14}+1)t_2} = e$ und mit $\phi^{(2^{14}+1)} = \phi^2$ erhalten wir

$$\phi^{2t_1} + \phi^{2t_2} = e.$$

Wegen $(\phi^{t_1} + \phi^{t_2})^2 = \phi^{2t_1} + \phi^{2t_2}$ ist

$$\phi^{t_1} + \phi^{t_2} = e. \tag{3.13}$$

In gleicher Weise bekommen wir

$$\phi^{t_3} + \phi^{t_4} = e. \tag{3.14}$$

Wir haben die Paare (t_1, t_2), (t_3, t_4), die die Bedingungen (3.13) und (3.14) erfüllen, mit MAGMA berechnet. Ist M die Menge, die die Paare $(t_1, t_2), (t_3, t_4)$ enthält, so ist $|M| = 8192$.

Wir haben mit MAGMA gezeigt, dass es für die Gültigkeit der Bedingungen (3.12), (3.13) und (3.14) notwendig ist, dass $t_1 = t_4$ und $t_2 = t_3$ gilt.

Deshalb erhalten wir

$$\varphi(E_\sigma(C)^*) = \begin{pmatrix} \theta^{l_1} & 0 & \phi^{t_1} & \phi^{t_2}\theta^{l_2} \\ 0 & \theta^{l_3} & \phi^{t_2} & \phi^{t_1}\theta^{l_2} \end{pmatrix},$$

wobei $0 \le l_1, l_2, l_3 \le (5 \times 113) - 1$ ist und $\{t_1, t_2\} \in M$.

Wenn wir die Substitution $x \to x^2$ anwenden, dann erhalten wir äquivalente Codes durch die Operation $(l_1, l_2, l_3, t_1, t_2) \to (2l_1, 2l_2, 2l_3, 2t_1, 2t_2)$. Die Operation $(t_1, t_2) \to (2t_1, 2t_2)$ unterteilt die Menge M in Bahnen. Diese Bahnen sind

$$O(t_1, t_2) = \{(t_1 2^n \bmod (2^{14} - 1),\ t_2 2^n \bmod (2^{14} - 1)) \mid n \in \mathbb{Z}\}.$$

Sei M' die Menge der Vertreter. Wir finden durch Berechnung mit MAGMA, dass die Anzahl der Vertreter 595 ist.

Andererseits erhalten wir ebenfalls mit MAGMA, dass $\alpha(x) = x^{13} + x^{12} + x^6 + x^5 + x^4 + x^2$ ein primitives Element des Körpes P ist.

Zusammenfassend haben wir den folgenden Satz bewiesen:

3.2.4 Satz. *Ein selbstdualer doppeltgerader* $[120, 60, 24]$*-Code* C *mit einem Automorphismus* σ *der Ordnung* 29 *hat Erzeugermatrix*

$$\mathrm{gen}(C) = \left(\begin{array}{cccc|cccc} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 1 & 1 & 1 \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & 1 & 0 & 1 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & 1 & 1 & 0 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & 1 & 1 & 1 & 0 \\ \hline [\theta^{l_1}] & [\,0\,] & [\phi^{t_1}] & [\phi^{t_2}\theta^{l_2}] & 0 & 0 & 0 & 0 \\ [\,0\,] & [\theta^{l_3}] & [\phi^{t_2}] & [\phi^{t_1}\theta^{l_2}] & 0 & 0 & 0 & 0 \end{array}\right),$$

wobei $\mathbf{1}$ *der Vektor mit ausschließlich* 1*-Einträgen und* $\mathbf{0}$ *der Nullvektor der Länge* 29 *ist,* $\alpha = x^{13} + x^{12} + x^6 + x^5 + x^4 + x^2$ *ein primitives Element des Körpers* P *ist,* $\phi = \alpha^{2^{14}+1}$, $\theta = \alpha^{29(2^{14}-1)}$, $0 \le l_1, l_2, l_3 \le (5 \times 113) - 1$ *ist und* $\{t_1, t_2\} \in M'$ *mit* $|M'| = 595$.

3.2.2 Automorphismen der Ordnung 19

Sei C ein selbstdualer $[120, 60, 24]$-Code und $\sigma \in \mathrm{Aut}(C)$ mit $\mathrm{ord}(\sigma) = 19$. Dann ist σ vom Typ 19-$(6; 6)$. Wegen Satz 1.5.2 ist $\pi(F_\sigma(C))$ ein binärer selbstdualer $[12, 6]$-Code. Also wissen wir nach [46], dass $\pi(F_\sigma(C)) \sim B_{12}$, $\pi(F_\sigma(C)) \sim C_2^6$ oder $\pi(F_\sigma(C)) \sim C_2^2 \oplus A_8$ ist, wobei

$$\mathrm{gen}(B_{12}) = \begin{pmatrix} 1&1&1&1&0&0&0&0&0&0&0&0\\ 0&0&1&1&1&1&0&0&0&0&0&0\\ 0&0&0&0&1&1&1&1&0&0&0&0\\ 0&0&0&0&0&0&1&1&1&1&0&0\\ 0&0&0&0&0&0&0&0&1&1&1&1\\ 0&1&0&1&0&1&0&1&0&1&0&1 \end{pmatrix} \tag{3.15}$$

$$\mathrm{gen}(C_2^6) = \begin{pmatrix} 1&1&0&0&0&0&0&0&0&0&0&0\\ 0&0&1&1&0&0&0&0&0&0&0&0\\ 0&0&0&0&1&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&1&0&0&0&0\\ 0&0&0&0&0&0&0&0&1&1&0&0\\ 0&0&0&0&0&0&0&0&0&0&1&1 \end{pmatrix} \tag{3.16}$$

$$\mathrm{gen}(C_2^2 \oplus A_8) = \begin{pmatrix} 1&1&0&0&0&0&0&0&0&0&0&0\\ 0&0&1&1&0&0&0&0&0&0&0&0\\ 0&0&0&0&1&1&1&1&0&0&0&0\\ 0&0&0&0&0&0&1&1&1&1&0&0\\ 0&0&0&0&0&0&0&0&1&1&1&1\\ 0&0&0&0&0&1&0&1&0&1&0&1 \end{pmatrix} \tag{3.17}$$

- C_2^6 kann nicht auftreten, weil jeder Vektor von $\mathrm{gen}(C_2^6)$ in $F_\sigma(C)$ das Gewicht 2, 20 oder 38 hat.

- Analysieren wir nun $C_2^2 \oplus A_8$. Seien $v_1, \ldots, v_6$ die Zeilenvektoren von $\mathrm{gen}(C_2^2 \oplus A_8)$. In diesem Fall haben wir zwei Cluster:
  $M_1 = \{\{1, 2\}, \{3, 4\}\}$
  $M_2 = \{\{5, 6\}, \{7, 8\}, \{9, 10\}, \{11, 12\}\}$

  Da es keine Vektoren in $F_\sigma(C)$ mit dem Gewicht 2 und 20 gibt, sind die Koordinaten von M_1 keine Fixpunkte.
  Daher sind die ersten vier Koordinaten Zyklen. Die anderen zwei Zyklen liegen in M_2. Wenn diese in dem gleichen Duo liegen, dann werden einige Vektoren v_3, v_4 oder v_5 vom Gewicht 4 in $F_\sigma(C)$ sein, ein Widerspruch. Wenn diese in verschiedenen Duos liegen, dann werden v_3, v_4 oder v_5 oder die Summe von ihnen vom Gewicht 4 in $F_\sigma(C)$ sein, ein Widerspruch.

Dementsprechend ist $\pi(F_\sigma(C)) \sim B_{12}$. Jedoch wissen wir immer noch nicht, welche Spalten der Matrix (3.15) den 19-Zyklen und den Fixpunkten entsprechen.

Nach 1.5.4 ist $|\{v \in F_\sigma(C) \mid \mathrm{wt}(v) = 24\}| \equiv A_{24} \mod 19$. Wegen 3.1.11 wissen wir, dass $A_{24} = 39703755 \equiv 6 \mod 19$ ist. Deshalb gibt es $6 \mod 19$ Vektoren von $F_\sigma(C)$ mit Gewicht 24.
Ist $v \in F_\sigma(C)$, so ist v konstant auf den Zyklen. Für $v \in \{v \in C \mid v \in F_\sigma(C) \text{ und } \mathrm{wt}(v) = 24\}$ ist das Gewicht daher von der Form $\mathrm{wt}(v) = 19 \cdot 1 + 5$. Das heißt v ist nur 1 in einem Zyklus und auf fünf Fixpunkten. Damit ist $\mathrm{wt}(\pi(v)) = 6$.

Angenommen $v_1, v_2 \in \{v \in C \mid v \in F_\sigma(C) \text{ und } \mathrm{wt}(v) = 24\}$ treffen in den Koordinaten eines Zyklus zusammen. Dann ist $\mathrm{wt}(v_1 + v_2) \leq 2$. Deshalb ist $v_1 = v_2$ und es gibt genau 6 Vektoren in $F_\sigma(C)$ mit $\mathrm{wt}(v) = 24$. Diese sind in $\pi(F_\sigma(C))$ linear unabhängig und bis auf Permutation der letzten sechs Spalten ist:

$$\mathrm{gen}(\pi(F_\sigma(C))) = \left(\begin{array}{cccccc|cccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{array}\right). \tag{3.18}$$

(Man kann mit MAGMA überprüfen, dass die Codes, die durch die Matrizen (3.15) und (3.18) erzeugt werden, äquivalent sind).

Dementsprechend erhalten wir:

$$\mathrm{gen}(F_\sigma(C)) = \left(\begin{array}{cccccc|cccccc} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 1 & 1 & 1 & 1 & 1 \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 & 0 & 1 & 1 & 1 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 & 1 & 0 & 1 & 1 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & 1 & 1 & 1 & 0 & 1 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & 1 & 1 & 1 & 1 & 0 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & 1 & 1 & 1 & 1 & 1 & 0 \end{array}\right),$$

wobei **1** und **0** Vektoren der Länge 19 mit den Koordinaten alle 1 bzw. 0 sind.

Deshalb haben wir

$$W_{F_\sigma(C)}(y) = 1 + 6y^{24} + 15y^{40} + 20y^{60} + 15y^{80} + 6y^{96} + y^{120}.$$

Da andererseits $s(19) = 18$ ist, gibt es nur zwei zyklotomische Klassen mod 19 über $\mathbb{F}_2$. Deshalb ist die Zerlegung von $x^{19} - 1$ in irreduzible Polynome in $\mathbb{F}_2[x]$ gleich

$$x^{19} - 1 = (x + 1)(1 + x + x^2 + \ldots + x^{18}).$$

Damit erhalten wir nach Lemma 1.5.7, dass P ein Körper mit Identität $e(x) = x+x^2+\ldots+x^{18}$ ist. Nach Satz 1.5.10 gilt dann, dass $\varphi(E_\sigma(C)^*)$ ein selbstdualer $[6, 3]$-Code über dem Körper $P \cong \mathbb{F}_{2^{18}}$ mit dem Skalarprodukt

$$u \cdot v = u_1 v_1^{2^9} + \ldots + u_6 v_6^{2^9}$$

ist.

Ähnlich wie im Fall $p = 29$ können wir beweisen, dass $\varphi(E_\sigma(C)^*)$ ein $[6, 3, 4]$-Code über P ist. Deshalb haben wir den folgenden Satz:

3.2.5 Satz. *Ein selbstdualer* $[120, 60, 24]$*-Code* C *mit einem Automorphismus* σ *der Ordnung*

19 *hat Erzeugermatrix*

$$\mathrm{gen}(C) = \left(\begin{array}{cccccc|cccccc} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 1 & 1 & 1 & 1 & 1 \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 & 0 & 1 & 1 & 1 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 & 1 & 0 & 1 & 1 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & 1 & 1 & 1 & 0 & 1 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & 1 & 1 & 1 & 1 & 0 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & 1 & 1 & 1 & 1 & 1 & 0 \\ \hline [\,e\,] & [\,0\,] & [\,0\,] & [\alpha^{t_1}] & [\alpha^{t_2}] & [\alpha^{t_3}] & 0 & 0 & 0 & 0 & 0 & 0 \\ [\,0\,] & [\,e\,] & [\,0\,] & [\alpha^{t_4}] & [\alpha^{t_5}] & [\alpha^{t_6}] & 0 & 0 & 0 & 0 & 0 & 0 \\ [\,0\,] & [\,0\,] & [\,e\,] & [\alpha^{t_7}] & [\alpha^{t_8}] & [\alpha^{t_9}] & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right),$$

wobei $\mathbf{1}$ *der Vektor mit ausschließlich* 1*-Einträgen und* $\mathbf{0}$ *der Nullvektor der Länge* 19 *ist,* $e(x) = x + x^2 + \ldots + x^{18}$ *die Identität von* P*,* α *ein primitives Element im* P *und* $0 \leq t_i \leq 2^{18} - 2$*.*

3.3 5-Designs von extremalen Codes der Länge $24m$

Es gibt eine wichtige Verbindung zwischen Codierungstheorie und Geometrie, vor allem mit der Designtheorie, aufgrund des bekannten Satzes von Assmus-Mattson. Dieses Kapitel analysiert die Beziehung zwischen den 5-Designs und extremalen Codes der Länge teilbar durch $24m$. Insbesondere analysieren wir ein 5-Design für den Fall $m = 5$.

Sei C ein binärer selbstdualer extremaler $[24m, 12m, 4m + 4]$-Code. Wir setzen $\mathcal{P} = \{1, \ldots, 24m\}$ und definieren die Blöcke $B \in \mathcal{B}$ als die Träger von Codewörtern mit minimalem Gewicht. Wegen Assmus-Mattsons Satz 1.7.7 ist $\mathcal{D}_C = (\mathcal{P}, \mathcal{B})$ ein selbstorthogonales 5-$(24m, 4m + 4, \lambda)$ Design mit

$$\binom{24m}{5}\lambda = A_d\binom{d}{5},$$

wobei A_d die Anzahl der Codewörter mit minimalem Gewicht $d = 4m + 4$ bezeichnet. Das Design $\mathcal{D}_C$ heißt *das assoziierte Design des Codes* C. Da

$$A_d = \frac{\binom{24m}{5}\binom{5m-2}{m-1}}{\binom{d}{5}}$$

ist, ist

$$\lambda = \binom{5m-2}{m-1},$$

nach [40, Chap. 19, § 4, Theorem 13]. Deshalb führt ein binärer selbstdualer extremaler Code der Länge $n = 24m$ zu einem selbstorthogonalen

$$5\text{-}(24m, 4m + 4, \binom{5m-2}{m-1})$$

Design.

Umgekehrt, angenommen $\mathcal{D}$ sei ein selbstorthogonales 5-$(24m, 4m + 4, \binom{5m-2}{m-1})$ Design. Wir untersuchen nun den Code $C(\mathcal{D})$, das heißt, den Code zum Design $\mathcal{D}$. Offenbar ist $C(\mathcal{D})$ selbstorthogonal, da $\mathcal{D}$ selbstorthogonal ist.

Wir zeigen, dass $C(\mathcal{D})$ selbstdual ist. Sei $c^\perp \in C(\mathcal{D})^\perp$ mit $\mathrm{wt}(c^\perp) = w$ und S der Träger von $c^\perp$, also $|S| = w$. Falls

$$\lambda_j = \lambda \frac{\binom{24m-j}{5-j}}{\binom{4m+4-j}{5-j}} \tag{3.19}$$

ist, dann ist

$$\sum_{i=0}^{\lfloor \frac{w}{2} \rfloor} \binom{2i}{j} n_{2i}^S = \lambda_j \binom{w}{j} \qquad (j = 0, 1, \ldots, 5), \tag{3.20}$$

nach Satz 1.7.6. Wenn wir beweisen können, dass das lineare Gleichungssystem (3.20) nur Lösungen $n_{2i} \in \mathbb{N}_0$ hat, wenn $4 \mid w$, so ist $C(\mathcal{D})^\perp$ doppeltgerade. Dies bedeutet, dass

$$C(\mathcal{D})^\perp \subseteq (C(\mathcal{D})^\perp)^\perp = C(\mathcal{D})$$

ist. Daher ist $C(\mathcal{D})$ selbstdual.

Diese Methode funktioniert für $m = 1, \ldots, 25$, außer wenn $m = 7, 13, 14, 15$ und 23 ist. In den Ausnahmefällen versagt die Methode, da es mögliche Lösungen $n_{2i} \in \mathbb{N}_0$ von (3.20) gibt für alle $w \equiv 2 \bmod 4$.

Beachte, für $m = 1$ gibt es genau einen binären extremalen Code, nämlich der erweiterte $[24, 12, 8]$-Golay-Code und genau ein 5-$(24, 8, 1)$ Design $\mathcal{D}$, ein Steiner-System, wobei der zugehörige Code $C(\mathcal{D})$ der binäre erweiterte Golay-Code ist (siehe [45, Theorem 5] und [2, Theorem 8.6.2]). Für $m = 2$ gibt es wieder genau einen binären extremalen Code, nämlich den binären verlängerten quadratische $[48, 24, 12]$-Reste-Code [32] und genau ein selbstorthogonales 5-$(48, 12, 8)$ Design $\mathcal{D}$ ([31, Theorem 1.1]), wobei der zugehörige Code $C(\mathcal{D})$ der binäre erweiterte quadratische Reste-Code der Länge 48 ist.

Im Fall $m = 3$ und $m = 4$ kennen wir nicht die Existenz, weder der binär extremalen selbstdualen Codes der Längen 72 oder 96 noch die selbstorthogonalen 5-$(72, 16, 78)$ oder 5-$(96, 20, 816)$ Designs. Doch nach [30] und [29] sind die Codes $C(\mathcal{D})$ zum Design $\mathcal{D}$ extremal.

3.3.1 Der Fall $m = 5$

Für $m = 5$ bilden die Träger der Vektoren vom Gewicht 24 in einem extremalen $[120, 60, 24]$-Code ein 5-$(120, 24, 8855)$ Design mit $b := \lambda_0 = 39703755$, $r := \lambda_1 = 7940751$, $\lambda_2 = 1534767$, $\lambda_3 = 286143$, $\lambda_4 = 51359$ und $\lambda = \lambda_5 = 8855$. In diesem Fall haben wir den folgenden Satz:

3.3.1 Hauptsatz. *Sei $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ ein selbstorthogonales 5-$(120, 24, 8855)$ Design. Dann ist $C(\mathcal{D})$ ein selbstdualer und doppeltgerader $[120, 60, d]$-Code mit Minimaldistanz d gleich 16 oder 24.*

Beweis. Sei A die Inzidenzmatrix des Designs $\mathcal{D}$ und seien $v_i, v_{i'}$ zwei Zeilenvektoren von A, die den Blöcken $B_i, B_{i'}$ entsprechen. Da das Design selbstorthogonal ist, gilt $|B_i \cap B_{i'}| \equiv 24 \bmod 2$. Deshalb ist $|B_i \cap B_{i'}|$ gerade und dann ist $v_i \cdot v_{i'} = 0$. Somit ist $C(\mathcal{D})$ ein selbstorthogonaler Code. Weiterhin, da die Zeilenvektoren von A doppeltgerade sind, folgt, dass $C(\mathcal{D})$ ein doppeltgerader Code ist.

Es bleibt zu zeigen: $C(\mathcal{D})^{\perp} \subseteq C(\mathcal{D})$. Sei $c^{\perp} \in C(\mathcal{D})^{\perp}$ mit $\mathrm{wt}(c^{\perp}) = w$ und $S := \mathrm{supp}(c^{\perp})$. Deshalb erhalten wir nach dem Gleichungssystem (3.20)

$$\sum_{i=0}^{\lfloor \frac{w}{2} \rfloor} \begin{pmatrix} 2i \\ j \end{pmatrix} n_{2i} = \lambda_j \begin{pmatrix} w \\ j \end{pmatrix}, \text{ für } j = 0, 1, ..., 5. \tag{3.21}$$

(In (3.21) haben wir einfach n_{2i} statt n_{2i}^{S} geschrieben).

Da $n_{2i} = 0$ für $2i > 24$ ist, hat das Gleichungssystem (3.21) die Gestalt

$$x \cdot L = b \tag{3.22}$$

mit

$$x = (n_0,\, n_2,\, n_4,\, n_6,\, n_8,\, n_{10},\, n_{12},\, n_{14},\, n_{16},\, n_{18},\, n_{20},\, n_{22},\, n_{24}),$$

$$L = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 \\ 1 & 4 & 6 & 4 & 1 & 0 \\ 1 & 6 & 15 & 20 & 15 & 6 \\ 1 & 8 & 28 & 56 & 70 & 56 \\ 1 & 10 & 45 & 120 & 210 & 252 \\ 1 & 12 & 66 & 220 & 495 & 792 \\ 1 & 14 & 91 & 364 & 1001 & 2002 \\ 1 & 16 & 120 & 560 & 1820 & 4368 \\ 1 & 18 & 153 & 816 & 3060 & 8568 \\ 1 & 20 & 190 & 1140 & 4845 & 15504 \\ 1 & 22 & 231 & 1540 & 7315 & 26334 \\ 1 & 24 & 276 & 2024 & 10626 & 42504 \end{pmatrix}$$

$$\text{und } \; b = \left(\lambda_0, \;\; \lambda_1 \tbinom{w}{1}, \;\; \lambda_2 \tbinom{w}{2}, \;\; \lambda_3 \tbinom{w}{3}, \;\; \lambda_4 \tbinom{w}{4}, \;\; \lambda_5 \tbinom{w}{5} \right), \text{ wobei}$$

$\lambda_0 = 39703755$, $\lambda_1 = 7940751$, $\lambda_2 = 1534767$, $\lambda_3 = 286143$, $\lambda_4 = 51359$ und $\lambda_5 = 8855$ ist. Aus dem Gleichungssystem (3.22) erhält man:

$$n_{10} = \beta_{10} - 6n_{12} - 21n_{14} - 56n_{16} - 126n_{18} - 252n_{20} - 462n_{22} - 792n_{24}\,,$$

wobei

$$\beta_{10} = \frac{1}{32 \times 8 \times 3}(1771w^5 - 120428w^4 + 3253580w^3 - 41174416w^2 + 204795264w)$$

ist.

Mit MAPLE folgt, dass, falls $w \not\equiv 0 \mod 4$ ist, $\beta_{10} \notin \mathbb{Z}$ und wir haben einen Widerspruch. Deshalb ist $w \equiv 0 \bmod 4$, das heißt $C(\mathcal{D})^{\perp}$ ist doppeltgerade und $C(\mathcal{D})$ ist selbstdual.

Andererseits, sei $c \in C^{\perp}(\mathcal{D}) = C(\mathcal{D})$ mit $\mathrm{wt}(c) = w$. Wegen (3.21) erhalten wir :

$$\sum_{i=0}^{\lfloor \frac{w}{2} \rfloor} 2_i n_{2i} = \lambda_1 w \;\text{ und }\; \sum_{i=0}^{\lfloor \frac{w}{2} \rfloor} \binom{2i}{2} n_{2i} = \lambda_2 \binom{w}{2}.$$

Daher folgt

$$2\sum_{i=0}^{\lfloor \frac{w}{2} \rfloor} \binom{2i}{2} n_{2i} - \sum_{i=0}^{\lfloor \frac{w}{2} \rfloor} 2in_{2i} = 2\lambda_2 \binom{w}{2} - \lambda_1 w$$

$$\sum_{i=0}^{\lfloor \frac{w}{2} \rfloor} [2i(2i-1)n_{2i} - 2in_{2i}] = \lambda_2 w(w-1) - \lambda_1 w$$

$$\sum_{i=0}^{\lfloor \frac{w}{2} \rfloor} 2i(2i-2)n_{2i} = w((w-1)\lambda_2 - \lambda_1).$$

Da $2i(2i-2)n_{2i} \geq 0$ ist für alle $i = 0, ..., \lfloor \frac{w}{2} \rfloor$, gilt

$$\sum_{i=0}^{\lfloor \frac{w}{2} \rfloor} 2i(2i-2)n_{2i} = w((w-1)\lambda_2 - \lambda_1) \geq 0.$$

Dementsprechend ist

$$w \geq \frac{\lambda_1 + \lambda_2}{\lambda_2} > 6.$$

Deshalb ist die Minimaldistanz d gleich 8, 12, 16, 20 oder 24.

- d kann nicht 8 sein, denn für $w = 8$ hat das Gleichungssystem $x \cdot L = b$ in (3.22) mit

  $$b = (39703755, 63526008, 42973476, 16024008, 3595130, 495880)$$

  keine nichtnegative ganzzahlige Lösung.

- d kann nicht 12 sein, denn für $w = 12$ hat das Gleichungssystem $x \cdot L = b$ in (3.22) mit

  $$b = (39703755, 95289012, 101294622, 62951460, 25422705, 7013160)$$

  keine nichtnegative ganzzahlige Lösung.

- d kann nicht 20 sein.

  Für $w = 20$ hat zumindest das Gleichungssystem $x \cdot L = b$ in (3.22) mit

  $$b = (39703755, 158815020, 291605730, 326203020, 248834355, 137287920)$$

  die nichtnegative ganzzahlige Lösung

  $$x = (574140, 10214100, 18892755, 8752800, 1200300, 69660, 0, 0, 0, 0, 0, 0, 0).$$

  Angenommen $d = 20$. Dann ist $C(\mathcal{D})$ ein selbstdualer doppeltgerader $[120, 60, 20]$-Code. Wegen 1.1.11 ist

  $$W_{C(\mathcal{D})}(x, y) = \sum_{i=0}^{5} a_i (x^8 + 14x^4y^4 + y^8)^{15-3i} (x^4y^4(x^4 - y^4)^4)^i,$$

mit $a_i \in \mathbb{Z}$ für $i = 0, \ldots, 5$. Also gilt

$$\begin{aligned} W(y) =& a_0 + (210a_0 + a_1)y^4 + (20595a_0 + 164a_1 + a_2)y^8 + (1251460a_0 + 12282a_1 + \\ & 118a_2 + a_3)\, y^{12} + (52705485a_0 + 554740a_1 + 6085a_2 + 72a_3 + a_4)\, y^{16} + \\ & (1630086822a_0 + 16800251a_1 + 178456a_2 + 2004a_3 + 26a_4 + a_5)\, y^{20} + \\ & (38263749615a_0 + 358399128a_1 + 322864a_2 + 25272a_3 + 39a_4 - 20a_5)y^{24} + \ldots \\ =& A_0 + A_{20}y^{20} + A_{24}y^{24} + \ldots \end{aligned}$$

Ein Koeffizientenvergleich liefert das Gleichungssystem:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 210 & 1 & 0 & 0 & 0 \\ 20595 & 164 & 1 & 0 & 0 \\ 1251460 & 12282 & 118 & 1 & 0 \\ 52705485 & 554740 & 6085 & 72 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

welches den Vektor $(a_0, a_1, a_2, a_3, a_4) = (1, -20, 13845, -305950, 1571490)$ als Lösung hat. Dann gilt $A_{20} = 492372 + a_5 > 0$ und $A_{24} = 29856315 - 20a_5$. Da $-a_5 < 492372$ ist, folgt

$$A_{24} = 29856315 - 20a_5 < 29856315 + 9847440 = 39703755.$$

Daher haben wir einen Widerspruch, denn die Inzidenzmatrix $A = \text{gen}(C(\mathcal{D}))$ hat 39703755 Zeilenvektoren mit Gewicht 24. ∎

3.3.2 Bemerkung. Der Code $C(\mathcal{D})$ kann einen Vektor c mit Gewicht 16 haben, da in diesem Fall das Gleichungssystem (3.22) nichtnegative Lösungen hat. Wenn $d = 16$ ist, dann ist $n_{14} = n_{16} = 0$, da sonst die Vektorsumme $v + c$ ein Gewicht kleiner als 24 hätte, wobei v ein Zeilenvektor der Erzeugernmatrix mit Gewicht 24 ist. Daher haben die Lösungen des Gleichungssystems einen einzigen freien Parameter und sind gegeben durch $n_0 = 1599377 + n_{12}$, $n_2 = 17248920 - 6n_{12}$, $n_4 = 16427320 + 15n_{12}$, $n_6 = 4325776 - 20n_{12}$, $n_8 = 66690 + 15n_{12}$ und $n_{10} = 35672 - 6n_{12}$.

3.3.3 Korollar. *Sei C ein selbstdualer $[120, 60, 24]$-Code. Dann wird C durch die Vektoren des Gewichts 24 erzeugt.*

Beweis. Sei $M = \{v \in C \mid \text{wt}(v) = 24\}$. Wegen des Satzes von Assmus-Mattson bilden die Träger der Vektoren von M ein 5-$(120, 24, 8855)$ Design $\mathcal{D}$. Nach 3.3.1 ist $C(\mathcal{D})$ ein selbstdualer Code mit $\text{gen}(\mathcal{C}(\mathcal{D})) = A$, wobei A die Inzidenzmatrix von $\mathcal{D}$ ist. Da die Menge der Zeilenvektoren von A gleich M ist, gilt $\langle M \rangle = C(\mathcal{D}) \subseteq C$. Deshalb ist $\langle M \rangle^\perp \supseteq C^\perp$. Da $\langle M \rangle$ und C selbstdual sind, folgt $\langle M \rangle = C$. ∎

3.3.2 Automorphismengruppe

Es ist wohlbekannt, dass die Automorphismengruppe des binären erweiterten Golay-Codes mit der Automorphismengruppe des assoziierten 5-$(24, 8, 1)$ Designs übereinstimmt; es ist die Mathieu-Group M_{24}. Das gleiche geschieht mit dem binären erweiterten quadratischen Reste-Code der Länge 48 und des assoziierten selbstorthogonalen 5-$(48, 12, 8)$ Designs. Die Gruppe ist $\text{PSL}(2, 47)$. Im Allgemeinen haben wir:

3.3.4 Satz. *Sei C ein binärer selbstdualer extremaler $[24m, 12m, 4m+4]$-Code mit assoziiertem selbstorthogonalen 5-$(24m, 4m+4, \binom{5m-2}{m-1})$ Design $\mathcal{D}_C$. Ist $C(\mathcal{D}_C)^\perp = C(\mathcal{D}_C)$, so ist*

$$\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D}_C).$$

Beweis. Die Bedingung $C(\mathcal{D}_C)^\perp = C(\mathcal{D}_C)$ bedeutet, dass C von der Menge $S = \{v_1, \ldots, v_s\}$, die aus allen Vektoren mit minimalem Gewicht $d = 4m+4$ besteht, erzeugt wird.

Sei $\sigma \in \mathrm{Aut}(\mathcal{D}_C)$. Für $c = \sum_{i=1}^{s} \alpha_i v_i \in C$ setzen wir $\sigma(c) = \sum_{i=1}^{s} \alpha_i \sigma(v_i)$. Beachte, dass dies wohldefiniert ist, da σ die Koordinaten $\{1, \ldots, 24m\}$ permutiert. Es ist klar, dass $\sigma(v_i) \in S \subseteq C$ für alle i. Also ist $\sigma(c) \in C$. Dies beweist $\sigma \in \mathrm{Aut}(C)$.

Umgekehrt, sei $\sigma \in \mathrm{Aut}(C)$. Da σ eine Permutation auf S bewirkt, induziert es eine Permutation auf den Blöcken, was $\sigma \in \mathrm{Aut}(\mathcal{D}_C)$ beweist. ∎

3.3.5 Bemerkung.

Nach Satz 3.3.1 und den Rechnungen, die wir im vorherigen Abschnitt erwähnt haben, gilt $C(\mathcal{D})^\perp = C(\mathcal{D})$ für alle selbstorthogonalen 5-$(24m, 4m+4, \binom{5m-2}{m-1})$ Designs $\mathcal{D}$ mit $m = 1, \ldots, 25$ außer eventuelle $m = 7, 13, 14, 15, 23$. Deshalb ist für diese m die Automorphismengruppe eines binären extremalen $[24m, 12m, 4m+4]$-Code C gleich der Automorphismengruppe des assoziierten Designs $\mathcal{D}_C$.

3.3.6 Satz. *Sei $\mathcal{D}$ ein selbstorthogonales 5-$(24m, 4m+4, \binom{5m-2}{m-1})$ Design mit $C(\mathcal{D})$ ein extremaler $[24m, 12m, 4m+4]$-Code. Dann ist* $\mathrm{Aut}(\mathcal{D}) = \mathrm{Aut}(C(\mathcal{D}))$.

Beweis. Es ist klar, dass $\mathrm{Aut}(\mathcal{D}) \subseteq \mathrm{Aut}(C(\mathcal{D}))$.

Bleibt zu beweisen $\mathrm{Aut}(C(\mathcal{D})) \subseteq \mathrm{Aut}(\mathcal{D})$. Sei $\sigma \in \mathrm{Aut}(C(\mathcal{D}))$ und B_i ein Block (man kann es auch als einen Zeilenvektor der Erzeugermatrix von $C(\mathcal{D})$ betrachten). Wegen Bemerkung 1.7.3 ist die Anzahl der Blöcke $b = \binom{5m-2}{m-1} \frac{\binom{24m}{5}}{\binom{4m+4}{5}}$. Wenn A_d die Anzahl der Vektoren vom Gewicht $d = 4m+4$ in $C(\mathcal{D})$ ist, dann ist $A_d = b$ (siehe [40, Chap. 19, § 4, Theorem 13]), da $C(\mathcal{D})$ extremal ist. Somit ist jeder Vektor mit minimalem Gewicht d von $C(\mathcal{D})$ ein Zeilenvektor der Erzeugermatrix ist, d.h. ein Block. Da $\mathrm{wt}(\sigma(B_i)) = d$ und $\sigma(B_i) \in C(\mathcal{D})$, ist $\sigma(B_i)$ ein Block.

3.3.7 Bemerkung. Da $C(\mathcal{D})$ extremal ist für $m = 3$ und $m = 4$, ist die Automorphismengruppe eines selbstorthogonalen 5-$(72, 16, 78)$ oder 5-$(96, 20, 816)$ Designs $\mathcal{D}$ die Automorphismengruppe des extremalen Codes $C(\mathcal{D})$ zum Design $\mathcal{D}$. Falls alle Automorphismen der Ordnung 3 eines extremalen $[96, 48, 20]$-Code keine Fixpunkte haben, so ist die Automorphismengruppe auflösbar oder die Automorphismengruppe ist die einfache Gruppe A_5 (siehe Satz 2.1.19).

Sei $\mathcal{D}$ ein selbstorthogonales 5-$(24m, 4m+4, \binom{5m-2}{m-1})$ Design und $C(\mathcal{D})$ der Code zum Design $\mathcal{D}$. Es ist natürlich zu fragen:

Frage 1 Ist $C(\mathcal{D})^\perp = C(\mathcal{D})$?

Frage 2 Ist $C(\mathcal{D})$ ein selbstdualer extremaler $[24m, 12m, 4m+4]$-Code?

Beachte, eine bejahende Antwort auf die Frage 1 impliziert, dass die Automorphismengruppe eines extremalen Codes der Länge 24 gleich der Automorphismengruppe des assoziierten 5-Designs ist. Eine bejahende Antwort der Frage 2 besagt, dass die Existenz eines

extremalen $[24m, 12m, 4m+4]$-Codes äquivalent zu der Existenz eines selbstorthogonalen 5-$(24m, 4m+4, \binom{5m-2}{m-1})$ Designs ist.

3.4 Einige notwendige Bedingungen für die Existenz eines binären selbstdualen $[120, 60, 24]$-Codes

Im Folgenden zeigen wir einige Bedingungen für die Existenz eines selbstdualen $[120, 60, 24]$-Codes. Ähnliche Bedingungen sind in [20] und [6] hergeleitet für den selbstdualen $[72, 36, 16]$-Code und den $[96, 48, 20]$-Code.

Zuerst betrachte einen extremalen $[118, 59, 22]$-Code C (vom Typ I). Wegen 1.2.3 erhalten wir, dass

$$W_C(y) = \sum_{j=0}^{14} a_j (1+y^2)^{59-4j} (y^2(1-y^2)^2)^j,$$

mit $a_j \in \mathbb{Z}$ für $j = 0, ..., 14$. Also gilt

$$\begin{aligned} W_C(y) =& a_0 + (59a_0 + a_1)y^2 + (1711a_0 + 53a_1 + a_2)y^4 + (32509a_0 + 1376a_1 + 47a_2 + a_3)y^6 + \\ & (455126a_0 + 23320a_1 + 1077a_2 + 41a_3 + a_4)y^8 + \dots \\ =& A_0 + A_{22}y^{22} + A_{24}y^{24} + \dots \end{aligned}$$

Eine Rechnung liefert $a_0 = 1$, $a_1 = -59$, $a_2 = 1416$, $a_3 = -17877$, $a_4 = 128679$, $a_5 = -538375$, $a_6 = 1291628$, $a_7 = -1713124$, $a_8 = 1187434$, $a_9 = -400374$ und $a_{10} = 0$.

Wenn wir diese Werte in $W_S(y) = \sum_{j=0}^{14} (-1)^j a_j 2^{59-6j} y^{59-4j} (1-y^4)^{2j}$ einsetzen, erhalten wir

$$\begin{aligned} W_S(y) =& \frac{1}{33554432} a_{14} y^3 + (-\frac{1}{524288} a_{13} - \frac{7}{8388608} a_{14}) y^7 + (\frac{189}{16777216} a_{14} + \frac{1}{8192} a_{12} + \\ & \frac{13}{262144} a_{13}) y^{11} + (-\frac{819}{8388608} a_{14} - \frac{1}{128} a_{11} - \frac{325}{524288} a_{13} - \frac{3}{1024} a_{12}) y^{15} + \\ & (\frac{325}{65536} a_{13} + \frac{69}{2048} a_{12} + \frac{11}{64} a_{11} + \frac{20475}{33554432} a_{14}) y^{19} + \\ & (-\frac{231}{128} a_{11} - \frac{7475}{262144} a_{13} - \frac{12285}{4194304} a_{14} - \frac{253}{1024} a_{12} + 12811968) y^{23} + \dots \end{aligned}$$

Sei $W_S(y) = \sum_{i=0}^{118} B_i y^i$. Nach 1.2.3 (2) ist $B_i \in \{0, 1\}$ für $i = 3, 7$ und höchstens ein B_i ist ungleich Null für $i \leq 11$. Daher gibt es vier Möglichkeiten:

1. Ist $B_3 = 1$, $B_7 = 0$, $B_{11} = 0$, so ist $a_{14} = 33554432$, $a_{13} = -14680064$, $a_{12} = 2867200$. Da $B_{15} = -2576 - \frac{1}{128} a_{11} \geq 0$ ist, folgt $B_{19} = 44275 + \frac{11}{164} a_{11} < 0$, ein Widerspruch.

2. Ist $B_3 = 0$, $B_7 = 1$, $B_{11} = 0$, so ist $a_{14} = 0$, $a_{13} = -524288$, $a_{12} = 212992$. Da $B_{15} = -299 - \frac{1}{128} a_{11} \geq 0$ ist, folgt $B_{19} = 4576 + \frac{11}{164} a_{11} < 0$. Deshalb erhalten wir einen Widerspruch.

3. Ist $B_3 = 0$, $B_7 = 0$, $B_{11} \neq 0$, so ist $a_{14} = a_{13} = 0$ und $a_{12} > 0$. Dann hat das Ungleichungsesystem $B_{15} = \frac{1}{-128} a_{11} - \frac{3}{1024} a_{12} \geq 0$ und $B_{19} = \frac{69}{2048} a_{12} + \frac{11}{64} a_{11} \geq 0$ keine Lösung, also wieder ein Widerspruch.

Somit ist $B_3 = 0$, $B_7 = 0$, $B_{11} = 0$ und wir erhalten $a_{14} = a_{13} = a_{12} = a_{11} = 0$. Also hat der Schatten Minimaldistanz 23 und wir können die Gewichtspolynome W_C und W_S berechnen (siehe Tabelle 3.3 und 3.4).

Tabelle 3.3: Gewichtspoynom eines selbstduales $[118, 59, 22]$-Codes.

i	A_i
22 96	1534767
24 94	25357020
26 92	323009424
28 90	3577030288
30 88	33041945820
32 86	255009210885
34 84	1660986238080
36 82	9190790517376
38 80	43420813336368
40 78	175902467952336
42 76	613510461769920
44 74	1848313759032000
46 72	4823479510074576
48 70	10929799315381752
50 68	21547310072116608
52 66	37017173713636224
54 64	55486969304739115
56 62	72637487089840296
58 60	83095867738716768

3.4.1 Lemma. *Sei C_0 die Menge der Codeworte von einem selbstdualen $[118, 59, 22]$-Code, deren Gewicht durch 4 teilbar ist. Dann bilden die Träger der Vektoren von festem Gewicht in C_0 und in $C_0^\perp$ jeweils ein 3 Design.*

Beweis. Da C_0 ein $[118, 58, 24]$-Code ist und $C_0^\perp = C \cup S$, ist $C_0^\perp$ ein $[118, 60, 22]$-Code. Ist $W_{C_0}(x, y) = \sum_{i=0}^{118} A_i x^{118-i} y^i$, so erhalten wir $|\{i \mid A_i \neq 0,\ 0 < i \leq 115\}| = 19 \leq d(C_0^\perp) - 3$. Deshalb bilden, nach dem Satz von Assmus-Mattson, die Träger der Vektoren vom Gewicht i in $C_0^\perp$ und in C_0 ein 3 Design. ∎

3.4.2 Frage. In einem selbstdualen $[118, 59, 22]$-Code bilden die Träger der Vektoren von minimalem Gewicht 22 ein 3-$[118, 22, 8885]$ Design $\mathcal{D}$. Wir haben die Frage: Ist $C(\mathcal{D})$ ein selbstdualer $[118, 59, 22]$-Code, wenn $\mathcal{D}$ ein selbstorthogonales 3-$[118, 22, 8885]$ Design ist?

3.4.3 Definition.

1. Zwei selbstduale Codes der Länge n heißen *Nachbarn*, falls sein Durchschnitt ein Code der Dimension $\frac{n}{2} - 1$ ist.
2. Wenn C und $C^\perp$ die gleichen Gewichtspolynome haben, so spricht man von *formal selbstdualen Codes.*

Tabelle 3.4: Gewichtspolynom der Schatten eines selbstdualen $[118, 59, 22]$-Codes.

i	B_i
23 95	12811968
27 91	2201249408
31 87	187592982720
35 83	7972733942784
39 79	178129081470720
43 75	2168688143930880
47 71	14778320201079552
51 67	57459493525644288
55 63	129133310381938304
59	169008544553322240

3. Falls C ein $[n, n/2, d]$ selbstdualer Code mit $d > 2$ ist, wähle zwei Koordinaten und betrachte den $(\frac{n}{2} - 1)$-dimensionalen Untercode C' von C mit entweder in beiden Positionen 0 oder in beiden eine 1. Lässt man beide Koordinaten von C' weg, erhält man einen selbstdualen Code C'^* der Länge $n - 2$; C'^* heißt *das Kind von* C und C heißt *Parent von* C'^*.

3.4.4 Lemma. ([37]) *Ist C ein Kind vom Typ I eines extremalen Parent vom Typ II mit Schatten $S = C_1 \cup C_3$, so ist $W_{C_1}(y) = W_{C_3}(y)$.*

3.4.5 Lemma. ([37]) *Sei C ein selbstdualer $[24m-2, 12m-1, 4m+2]$-Code, dessen Schatten ein minimales Gewicht $4m+3$ hat. Dann ist C ein Kind eines extremalen $[24m, 12m, 4m+4]$-Codes vom Typ II.*

3.4.6 Lemma. ([21], [20]) *Für festes m ist die Existenz eines einfachgeraden $[24m-2, 12m-1, 4m+2]$-Codes, dessen Schatten minimales Gewicht $4m+3$ hat, äquivalent zu der Existenz eines extremalen $[24m, 12m, 4m+4]$-Codes.*

Da der Schatten eines selbstdualen $[118, 59, 22]$-Codes Minimaldistanz 23 hat, ist die Existenz eines selbstdualen $[120, 60, 24]$-Codes äquivalent zur Existenz eines selbstdualen $[118, 59, 22]$-Codes C (Im Allgemeinen ist nach [51] die Existenz eines extremalen Codes der Länge $24m$ äquivalent zu der Existenz eines selbstdualen $[24m - 2, 12m - 1, 4m + 2]$-Code). Nach Lemma 3.4.1 bilden die Träger der Vektoren vom Gewicht k im Schatten S von C ein 3-$(118, k, \lambda)$ Design. Daher gilt, wenn ein $[118, 59, 22]$-Code existiert und sein Schatten das Gewichtspolynom $W_S(y) = \sum_{i=0}^{118} B_k y^k$ hat, so müssen die Koeffizienten des Schattens die Teilbarkeitsbedingung $\frac{(k-i)!}{k!}\frac{118!}{(118-i)!} \mid B_k$ erfüllen, da die Terme $\lambda_i = B_K \frac{k!}{(k-i)!}\frac{(118-i)!}{118!} \in \mathbb{N}_0$ sind. Leider erfüllen alle Koeffizienten B_k (siehe Tabelle 3.5) diese Bedingung.

3.4.7 Lemma. ([6]) *Sei C ein binärer Code vom Typ I der Länge n mit Schatten $S = C_1 \cup C_3$, wobei C_0 der Untercode ist, der aus allen Vektoren von C mit Gewicht teilbar durch 4 besteht. Angenommen, dass $n \equiv 2 \mod 4$ ist. Sei C^* ein Code der Länge $n + 2$, den man aus $C_0^\perp$ durch folgende Erweiterung erhält:*

$$(0, 0, C_0), (1, 0, C_2), (0, 1, C_1), (1, 1, C_3).$$

Tabelle 3.5: Parameter des 3-Designs.

k	$\lambda_0 = B_k$	λ_1	λ_2	$\lambda_3 = \lambda$
23	12811968	2497248	469568	85008
27	2201249408	503675712	9327328	24122400
31	187592982720	49282902240	12636641600	3159160400
35	7972733942784	2364793966080	687205084160	195497998080
39	178129081470720	58873170994560	19121200835840	6099003714880
43	2168688143930880	790284662618880	283691930170880	100270423594880
47	14778320201079552	5886280080091008	2314263963112704	897774813276480
51	57459493525644288	24834187879727616	10612900803302400	4483035684153600
55	129133310381938304	60189254839039040	27779656079556480	12692429070831840
59	169008544553322240	84504272276661120	41891006769626880	20584374016109760
63	129133310381938304	68944055542899264	36534456783416704	19212085032658784
67	57459493525644288	32625305645916672	18404018569491456	10312596612215040
71	14778320201079552	8892040120988544	5320024004010240	3164497036868160
75	2168688143930880	1378403481312000	871810748864000	548639522992000
79	178129081470720	119255910476160	79503940317440	52774167279680
83	7972733942784	5607939976704	3930351094784	2744469298944
87	187592982720	138310080480	101663819840	74495040400
91	2201249408	1697573696	1305825920	1001883680
95	12811968	10314720	8287040	6643920

Ist $W_{C_1}(y) = W_{C_3}(y)$, so ist C^* ein formal selbstdualer Code mit Gewichtspolynom

$$W_{C_0}(y) + y(W_{C_1}(y) + W_{C_2}(y)) + y^2 W_{C_3}(y).$$

3.4.8 Lemma. *Ist C ein $[118, 59, 22]$-Code vom Typ I, so ist der Code C^* im vorhergehenden Lemma formal selbstdual.*

Beweis. Wegen Lemma 3.4.5 ist C ein Kind eines selbstdualen $[120, 60, 24]$-Codes. Deshalb ist C^* formal selbstdual, nach Lemma 3.4.4. ∎

Das Gewichtspolynom des Codes C^* ist gegeben in der Tabelle 3.6. Dieses berechnet sich nach Lemma 3.4.7, dem Gewichtspolynom des $[118, 59, 22]$-Codes vom Typ I und seines Schattens, die in den Tabellen 3.3 und 3.4 gegeben sind. Zusammenfassend haben wir das folgende Ergebnis:

3.4.9 Satz. *Wenn es keine linearen $[120, 60, 23]$-Codes mit Gewichtspolynom wie in der Tabelle 3.6 gibt, dann gibt es keinen selbstdualen $[120, 60, 24]$-Code.*

Sei C ein selbstdualer $[120, 60, 24]$-Code und $u \in \mathbb{F}_2^{120}$ mit $\mathrm{wt}(u) = 4$. Dann ist $D := C \cap \langle u \rangle^\perp$ ein selbstorthogonaler $[120, 59]$-Code. Weiterhin ist $N := \langle D, u \rangle$ ein selbstdualer doppeltgerader $[120, 60, 4]$-Code. Da $\dim(N \cap C) = 59$ ist, haben wir, dass N ein Nachbar von C ist. Der Code N hat nur einen Vektor mit Gewicht 4. Um die Anzahl der Vektoren mit Gewicht 20 zu bestimmen, genügt es, die Anzahl der Vektoren $w \in C$ mit Gewicht 24

und $|\mathrm{supp}(w) \cap \mathrm{supp}(u)| = 4$ zu berechnen. Da die Vektoren von C mit Gewicht 24 ein 5-Design bilden, ist diese Zahl gleich $\lambda_4 = 51359$, wobei λ_4 die Anzahl der Blöcke ist, die mit 4 verschiedenen Punkten inzidieren.

Wenn $\sum A_i y^i$ das Gewichtspolynom von N ist, dann ist $A_0 = 1$, $A_4 = 1$, $A_8 = 0$, $A_{12} = 0$, $A_{16} = 0$ und $A_{20} = 51359$. Dann, mit Hilfe von Satz 1.1.11, erhalten wir das Gewichtspolynom des Codes N. Zusammenfassend haben wir das folgendes Ergebnis gezeigt:

3.4.10 Satz. *Wenn es keine selbstdualen doppeltgeraden* $[120, 60, 4]$*-Codes mit Gewichtspolynom wie in der Tabelle 3.7 gibt, dann gibt es keinen selbstdualen* $[120, 60, 24]$*-Code.*

Tabelle 3.6: Gewichtspolynom des formal selbstdualen $[120, 60, 23]$-Codes.

Gewicht	Gewichtsverteilung	Gewicht	Gewichtsverteilung
0	1	61	84504272276661120
23	1534767	63	72637487089840296
24	31763004	64	120053624495708267
25	6405984	65	64566655190969152
27	323009424	67	37017173713636224
28	4677654992	68	50277056834938752
29	1100624704	69	28729746762822144
31	33041945820	71	10929799315381752
32	348805702245	72	12212639610614352
33	93796491360	73	7389160100539776
35	1660986238080	75	1848313759032000
36	13177157488768	76	1697854533735360
37	3986366971392	77	1084344071965440
39	43420813336368	79	175902467952336
40	264967008687696	80	132485354071728
41	89064540735360	81	89064540735360
43	613510461769920	83	9190790517376
44	2932657830997440	84	5647353209472
45	1084344071965440	85	3986366971392
47	4823479510074576	87	255009210885
48	18318959415921528	88	126838437180
49	7389160100539776	89	93796491360
51	21547310072116608	91	3577030288
52	65746920476458368	92	1423634128
53	28729746762822144	93	1100624704
55	55486969304739115	95	25357020
56	137204142280809448	96	7940751
57	64566655190969152	97	6405984
59	83095867738716768		
60	167600140015377888		

Tabelle 3.7: Gewichtspolynom des selbstdualen doppeltgeraden Nachbar $[120, 60, 4]$-Codes.

i	A_i
0 120	1
4 116	1
20 100	51359
24 96	43481179
28 92	6539254776
32 88	494044041905
36 84	19178964940125
40 80	400399951557816
44 76	4639015235035296
48 72	30526043817770504
52 68	115980280893408771
56 64	257259077150523955
60	335272511326715600

Kapitel 4

Neue selbstduale Codes C mit nicht-trivialen Automorphismen

4.1 Selbstduale und doppeltgerade $[120, 60, 20]$-Codes

Wir wissen, dass die Minimaldistanz d von einem selbstdualen Code der Länge 120 kleiner oder gleich 24 ist. Die Existenz eines selbstdualen $[120, 60, 24]$-Codes ist bis heute, wie bereits mehrfach erwähnt, eine offene Frage. Man ist daran interessiert, Codes mit der höchst möglichen Minimaldistanz zu finden. In [62] wurden 26 selbstduale $[120, 60, 20]$-Codes mit einem Automorphismus der Ordnung 23 gefunden. Wir werden 24 weitere nicht-äquivalente $[120, 60, 20]$-Codes mit einem Automorphismus der Ordnung 59 sowie 23 mit einem Automorphismus der Ordnung 29 konstruieren.

Das Gewichtpolynom eines selbstdualen doppeltgeraden $[120, 60, 20]$-Codes ist

$$W_C(1, y) = 1 + (492372 + \beta)y^{20} + (29856315 - 20\beta)y^{24} + \dots$$

4.1.1 Satz. *Es gibt mindestens* 24 *selbstduale doppeltgerade* $[120, 60, 20]$*-Codes* C *mit einem Automorphismus* σ *der Ordnung* 59*.*

Beweis. Mittels der Erzeugermatrix in 3.1.28 finden wir für gewisse t' (siehe Tabelle 4.1) neue nicht-äquivalente selbstduale doppeltgerade $[120, 60, 20]$-Codes mit einen Automorphismus σ der Ordnung 59. ∎

4.1.2 Satz. *Es gibt mindestens* 23 *selbstduale doppeltgerade* $[120, 60, 20]$*-Codes* C *mit einem Automorphismus* σ *der Ordnung* 29*.*

Beweis. Existiert ein selbstdualer $[120, 60, 24]$-Code, der einen Automorphismus der Ordnung 29 hat, so hat er eine Erzeugermatrix wie in 3.2.4. Wir finden durch Berechnung mit MAGMA 23 neue nicht-äquivalente selbstduale doppeltgerade $[120, 60, 20]$-Codes mit einem Automorphismus σ der Ordnung 29 (siehe Tabelle 4.2). ∎

Bei Codes der Länge $24m$ ist in dem Fall $m = 3$ die Existenz eines $[72, 36, 14]$-Codes vom Typ I ein offenes Problem ([34, Research Problem 9.3.6]). Für $m = 5$ ist auch nicht die Existenz eines $[120, 60, 22]$-Codes vom Typ I bekannt. Wir haben im Allgemeinen das folgende Ergebnis bewiesen

4.1.3 Satz. *Ein* $[120, 60, d]$*-Code vom Typ* I *hat keinen Automorphismus der Ordnung* 59*, für alle* $d \geq 4$*.*

Tabelle 4.1: Neue $[120, 60, 20]$-Codes vom Typ II mit einen Automorphismus der Ordnung 59.

t'	A_{20}	β	t'	A_{20}	β
51	103368	-389004	8317	97704	-394668
63	107616	-384756	8811	96996	-395376
103	96642	-395730	203425	104784	-387588
181	99828	-392544	203731	102306	-390066
287	107262	-385110	203801	103014	-389358
361	106908	-385464	203805	91686	-400686
665	101244	-391128	396325	103722	-388650
681	98058	-394314	397141	105138	-387234
779	100536	-391836	397397	101952	-390420
7503	100890	-391482	400309	102660	-389712
7521	101598	-390774	789641	98412	-393960
7607	99474	-392898	8357499	105020	-387352

BEWEIS. Die Erzeugermatrix eines selbstdualen $[120, 60, d \geq 4]$-Codes C mit einem Automorphismus σ der Ordnung 59 ist gleich

$$\mathrm{gen}(C) = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 1 \\ \hline [\mathrm{e(x)}] & [\alpha(x)^{(2^{29}-1)t}] & 0 & 0 \end{array}\right), \tag{4.1}$$

wobei t Vertreter der 156889 Bahnen sind und $\alpha(x) = x^{55} + x^{51} + x^{50} + x^{48} + x^{42} + x^{39} + x^{35} + x^{29} + x^{23} + x^{20} + x^{10} + x^9 + x^3 + x$ ist.

Wir finden durch Berechnung mit MAGMA, dass stehts $\mathrm{wt}((e(x), \alpha(x)^{(2^{29}-1)t})) \equiv 0 \mod 4$ für alle t. Da C selbstdual ist, ist C vom Typ II. ∎

4.2 Extremale $[60, 30, 12]$-Codes vom Typ I mit einem Automorphismus der Ordnung 29

In [41] wurde das Gewichtspolynom eines selbstdualen einfachgeraden $[60, 30, 12]$-Codes berechnet, jedoch unvollständig, weil in [28] Gulliver und Harada einen Code für $\beta = 10$ konstruierten, der nicht in dieser Liste war.

Es gibt zwei mögliche Gewichtspolynome:

$$W_1(y) = 1 + (2555 + 64\beta)y^{12} + (33600 - 384\beta)y^{14} + \ldots$$

für $0 \leq \beta \leq 10$ und

$$W_2(y) = 1 + 3451y^{12} + 24128y^{14} + \ldots$$

In [18] wurde ein Code mit einem Automorphismus der Ordnung 7 für $\beta = 7$ konstruiert. Wir werden einen $[60, 30, 12]$-Code mit einem Automorphismus der Ordnung 29 konstruieren.

Tabelle 4.2: Neue $[120, 60, 20]$-Codes vom Typ II mit einen Automorphismus der Ordnung 29.

l_1	l_2	l_3	t_1	t_2	A_{20}
3	5	1	5469	9024	95874
200	200	1	4187	15205	97962
5	342	1	8144	15977	98310
200	4	5	6540	9071	98484
200	1	4	896	13285	98658
342	2	565	5903	10368	99006
5	342	4	3921	16257	99180
342	342	3	8131	13840	99528
1	4	4	6647	12854	99702
2	342	565	7846	8062	99876
1	565	5	5903	10368	100050
1	200	1	160	15186	100224
342	565	2	1477	9154	100398
5	3	1	7805	10339	100572
565	5	200	5903	10368	100746
2	4	4	10138	14404	100920
565	1	4	6647	12854	101094
1	342	200	4817	15454	101268
4	2	1	3701	4776	101790
2	2	200	1379	6536	101964
200	1	565	1338	5711	102486
4	5	5	6647	12854	102834
3	4	5	5469	9024	104226

4.2.1 Hauptsatz. *Es gibt nur drei extremale* $[60, 30, 12]$*-Codes* C *vom Typ I mit einem Automorphismus der Ordnung* 29*.*

Beweis. Sei $\sigma \in \mathrm{Aut}(C)$ der Ordnung 29. Dann gilt $c = 2$ und $f = 2$. In ähnlicher Weise wie in dem Satz 3.1.28 erhalten wir:

$$\mathrm{gen}(C) = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 1 \\ \hline [\mathrm{e(x)}] & [\alpha(x)^{(2^{14}-1)t}] & 0 & 0 \end{array}\right), \tag{4.2}$$

wobei $\alpha(x) = x^{13} + x^{12} + x^6 + x^5 + x^4 + x^2$ ein primitives Element von $P = \langle x + 1\rangle \subseteq \mathbb{F}_2[x]/\langle x^{29} - 1\rangle$ ist und $t \in \mathbb{Z}_{565}$.
Die Operation $t \to 2t$ unterteilt die Menge $\mathbb{Z}_{565}$ in Bahnen. Mit MAGMA haben wir gezeigt, dass die Anzahl der Bahnen 21 ist. Die Vertreter sind

$$\{1, 3, 5, 7, 9, 13, 15, 17, 19, 23, 25, 27, 29, 39, 41, 45, 47, 49, 51, 81, 113\}.$$

Ebenfalls mit MAGMA haben wir für

$$t \in \{1, 3, 5, 7, 9, 13, 17, 19, 23, 25, 27, 29, 39, 41, 47, 49, 81, 113\}$$

ein Codewort vom Gewicht kleiner als 12 gefunden. Für 15, 45 und 51 sind die Codes nicht äquivalent und haben einen Automorphismus σ der Ordnung 29. Für alle 3 Codes gilt $|\mathrm{Aut}(C)| = 2 \times 29$ und das Gewichtspolynom ist:

$$\begin{aligned} W_C(y) =& 1 + 3451y^{12} + 24128^{14} + 336081y^{16} + 1469952y^{18} + 8556856y^{20} + 24907520y^{22} + \\ & 68747400y^{24} + 130023936y^{26} + 190791667y^{28} + 224019840y^{30} + 190791667y^{32} + \\ & 130023936y^{34} + 68747400^{36} + 24907520y^{38} + 8556856y^{40} + 1469952y^{42} + \\ & 336081y^{44} + 24128^{46} + 3451y^{48} + y^{60}. \end{aligned}$$

Ferner gilt

$$\begin{aligned} W_{C_1}(y) =& y^2 + 319^{10} + 39672y^{14} + 1981309y^{18} + \ldots \\ W_{C_3}(y) =& 24128y^{14} + 1469952y^{18} + \ldots, \end{aligned}$$

wobei $S = C_1 \cup C_3$ der Schatten ist. ∎

Literaturverzeichnis

[1] J.L. Alperin, R.B. Bell, Groups and Representations, Springer-Verlag, New York, 1995.

[2] E.F. Assmus, Jr. and J.D. Key, Designs and Their Codes, Cambridge University Press.

[3] E.F. Assmus, Jr. and H.F. Mattson Jr., New 5-designs, *J. Combin. Theory* **6** (1969), 122-151.

[4] E.F. Assmus, Jr., H.F. Mattson, J.r., and R.J. Turyn, Research to develop the algebraic theory of codes, Air Force Cambridge Res. Labs., Bedford, MA, Report AFCRL-67-0365, June 1967.

[5] E.R. Berlekamp, F.J. MacWilliams, and N.J.A. Sloane, Gleason's theorem on self-dual codes, *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 409-414, 1972.

[6] K. Betsumiya, M. Harada, Formally Self-Dual Codes Related to Type II Codes, *Appl. Algebra Eng. Commun. Comput.* **14**(2)(2003), 81-88.

[7] A. Betten, Schnittzahlen von Designs, Bayreuther Mathematische Schriften, Heft 58, 2000.

[8] S. Bouyuklieva, On the automorphisms of order 2 with fixed points for the extremal self-dual codes of length 24m, *Des. Codes and Crypt.* **25** (2002), 5-13.

[9] S. Bouyuklieva, On the Automorphism Group of a Doubly-Even $(72, 32, 16)$ Code, *IEEE Trans. Inform. Theory* **50** (2004), 544-547.

[10] S. Bouyuklieva, E.A. O'Brien and W. Willems, The automorphism group of a binary self-dual doubly-even $[72, 36, 16]$ code is solvable, *IEEE Trans. Inform. Theory* **52** (2006), 4244-4248.

[11] S. Bouyuklieva, A. Malevich and W. Willems, Automorphisms of extremal self-dual codes, *IEEE Trans. Inform. Theory* **56** (2010), 2091-2096.

[12] R.A. Brualdi, V. Pless, Weight enumerators of self-dual codes, *IEEE Trans. Inform. Theory* **37**(4) (1991), 1222-1225.

[13] E.A. O'Brien and W. Willems, On the automorphism group of a binary self-dual doubly-even [72,36,16] code, *IEEE Trans. Inform. Theory* **57** (2011), 4445-4451.

[14] J.H. Conway and V. Pless, On primes dividing the group order of a doubly-even $[72, 36, 16]$ code and the group order order of a quaternary $[24, 12, 10]$ code, Discrete Math., pp. 143-156, 1982.

[15] J.H. Conway, V. Pless, and N.J.A. Sloane, The binary self-dual codes of length up to 32:A revised enumeration, J. Comb. Theory, Ser. A, vol. **60** 1992, 183-195.

[16] J.H. Conway and N.J.A. Sloane, A New Upper Bound on the Minimal Distance of Self-Dual Codes, *IEEE Trans. Inform. Theory*, Vol **36**, No. 6, NOVEMBER 1990.

[17] R. Dontcheva, On the Doubly-Even Self-Dual Codes of Length 96, *IEEE Trans. Inform. Theory*, Vol **48**, No. 2, FEBRUARY 2002.

[18] R. Dontcheva, M. Harada, Some Extremal Self-Dual Codes with an Automorphism of Order 7, *Appl. Algebra Eng. Comm. Computing*, vol. 14 (2003), 75-79. **50** (2004), 311-318.

[19] R. Dontcheva, A.J. van Zanten, and S. Dodunekov, Binary Self-Dual Codes With Automorphisms of Composite Order, *IEEE Trans. Inform. Theory* **50** (2004), 311-318.

[20] S.T. Dougherty, The Search for the $[24k, 12k, 4k+4]$ Extremal Type II Code, Scranton, PA 18510 November 29, 2006.

[21] S.T. Dougherty, M. Harada, New extremal self-dual codes of length 68, *IEEE Trans. Inform. Theory* IT-45 (1999) 2133-2136.

[22] I.M. Duursma, Extremal weight enumerators ans ultraspherical polynomials, *Discrete Math*, **268**, 103-127 (2002).

[23] M. El-Khamy and R. J. McEliece, The partition weight enumerator of MDS codes and its applications, submitted to International Symposium on Information Theory (ISIT) 2005.

[24] T. Feulner, G. Nebe, The automorphism group of an extremal $[72, 36, 16]$ code does not contain Z_7, $Z_3 \times Z_3$, or D_{10}. (preprint, arXiv:1110.6012v1)

[25] A.M. Gleason, Weight polynomials of codes and the MacWilliams identities, *Actes Congrès Intern. de Math.*, Gauthier-Villars, Paris, 1971, vol. 3, pp. 211-215.

[26] R. Gow, B. Huppert, R. Knörr, O. Manz and W. Willems, *Representation theory in arbitrary characteristic,* Casa Editrice Dott. Antonio Milani, Padua 1993.

[27] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, online available at `http://www.codetables.de`

[28] T.A. Gulliver, M. Harada, Weight enumerators of extremal singly-even [60,30,12] codes, *IEEE Trans. Inform. Theory* **42**, 658-659 (1996).

[29] M. Harada, Remark on a 5-design related to a putative extremal doubly-even self-dual [96, 48, 20] code. To appear.

[30] M. Harada, M. Kitazume and A. Munemasa, On a 5-design related to an extremal doubly even self-dual code of length 72, J. Combin. Theory Ser. A, **107**, (2004), 143-146.

[31] M. Harada, A. Munemaza and V.D. Tonchev, A characterization of designs related to an extremal doubly-even self-dual code of length 48, *Annals of Combinatorics* **5** (2005), 189-198.

[32] S.K. Houghten, C.W.H. Lam, L.H. Thiel and J.A. Parker, The extended quadratic residue code is the only $(48, 24, 12)$ self-dual doubly-even code, *IEEE Trans. Inform. Theory* **48** (2003), 53-59.

[33] W.C. Huffman, Automorphisms of Codes with Applications to Extremal Doubly Even Codes of Length 48, *IEEE Trans. Inform. Theory* IT-28,(1982)511-521.

[34] W.C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge 2003.

[35] W.C. Huffman and V. Yorgov, A $[72, 36, 16]$ doubly-even code does not have an automorphism of order 11, *IEEE Trans. Infor. Theory*, **33**, pp. 749-752, 1987.

[36] I.M. Isaacs, *Finite group theory,* Graduate Studies in Math, Vol. 92, AMS, Providence 2008.

[37] G.T. Kennedy and V.S. Pless, A coding theoretic approach to extending designs, *Discrete Appl. Math.* **142** (1995), pp. 155-168.

[38] J.S. Leon, V. Pless and N.J.A. Sloane, Duadic codes, *IEEE Trans. Inform. Theory* **30** (1984), 709-714.

[39] X. Ma, Nonexistence of extremal doubly even self-dual codes with large length, *Discrete Math.* **185**, 265-274 (1998).

[40] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes. North-Holland, Amsterdam, 1977.

[41] C.L. Mallows, N.J.A. Sloane, An upper bound for self-dual codes, Information and Control 22 (1973), 188-200.

[42] N.S. Mendelsohn, Intersection numbers of t-Designs, Studies in Pure Mathematics, p.p. 145-150, Academic Press, London, 1971.

[43] E.H. Moore, Double circulant codes and related algebraic structures. Ph.D. dissertation, Dartmouth College, 1976.

[44] G. Nebe, An extremal $[72, 36, 16]$ binary code has no automorphism group containing $Z_2 \times Z4$, Q_8, or Z_{10}. (preprint, arXiv:1109.1680)

[45] V. Pless, On the uniqueness of the Golay codes, *J. Comb. Theory* **5** (1968), 215-228.

[46] V. Pless, A classification of self-orthogonal codes over $GF(2)$, *Discr. Math.*, vol. **3**, pp. 209-246, 1972.

[47] V. Pless, 23 does not divide the order of the group of a $[72, 36, 16]$ doubly-even code, *IEEE Trans. Inform. Theory*, **28**, pp. 113-117, 1982.

[48] V. Pless, An Introduction to the Theory of Error-Correcting Codes. New York: Wiley, 1982.

[49] V. Pless and N.J.A. Sloane, On the classification and enumeration of self-dual codes, *J. Comb. Theory*, Ser. A, **18** (1975), 313-335.

[50] V. Pless and J.g. Thompson, 17 does not divide the order of the group of a $[72, 36, 16]$ doubly-even code. *IEEE Trans. Inform. Theory*, **28**, pp. 537-541, 1982.

[51] E.M. Rains, Shadow Bounds for Self-Dual Codes, *IEEE Trans. Inform. Theory*, **44**, pp. 134 - 139, 1998.

[52] E.M. Rains and N.J.A. Sloane, Self-dual codes, in Handbook of coding theory, Volume **1**, Elsevier 1998, 177-294.

[53] N.J.A. Sloane, Is there a $[72, 36]$, $d = 16$ self-dual code? *IEEE Trans. Inform. Theory*, **19**, pp. 251, 1973.

[54] N.J.A. Sloane, Relations between combinatorics and other parts of mathematics, *Proc. Symposia Pure Math.* **34** (1979), 273-308.

[55] V.D. Tonchev, A characterization of designs related to the Witt system S(5, 8, 24), Mathematische Zeitschrift Vol. **191** (1986) pp. 225-230.

[56] W. Willems, Codierungstheorie, Walter de Gruyter, Berlin. New York 1999.

[57] N. Yankov, A putative doubly even $[72, 36, 16]$ code does not have an automorphism of order 9, *IEEE Trans. Inform. Theory* (to appear).

[58] V.Y. Yorgov, Binary self-dual codes with automorphisms of odd order, Probl. Pered. Inform. vol. **19**, pp. 11-24, 1983. Russian.

[59] V.Y. Yorgov, A method for Constructing Inequivalent Self-Dual Codes with Applications to Length 56, *IEEE Trans. Inform. Theory* IT-**33**, (1987) 77-82.

[60] V.Y. Yorgov, On the automorphism group of a putative code, *IEEE Trans. Inform. Theory* Vol. **52**, No. 4, APRIL 2006.

[61] V.Y. Yorgov, A. Shterev, and N. Ziapkov, A [96, 48, 20] doubly-even self-dual code does not have automorphism of order 47 and 31, In Int. Workshop ACCT, leningrad, U.S.S.R., 1990, PP. 191-194.

[62] R. Yorgova, A. Wassermann, Binary self-dual codes with automorphisms of order 23, *Des. Codes and Cryptography* **48** (2008), pp. 155-164.

[63] S. Zhang, On the nonexistence of extremal self-dual codes, *Discrete Appl. Math.*, V. **91**, pp. 277-286, 1999.