Codes und Invariantentheorie

von

Annika Günther

Diplomarbeit in Mathematik

vorgelegt der

Fakultät für Mathematik, Informatik und Naturwissenschaften
der Rheinisch-Westfälischen Technischen Hochschule Aachen

im
September 2006

angefertigt im
Lehrstuhl D für Mathematik

bei
Prof. Dr. G. Nebe

Inhaltsverzeichnis

Vorwort

Ein Code im klassischen Sinne ist ein Untervektorraum von $\mathbb{F}^N$, wobei $\mathbb{F}$ ein endlicher Körper ist. Da Codes zur Nachrichtenübertragung benutzt werden, sind Codes mit guten fehlerkorrigierenden Eigenschaften von besonderem Interesse. Dies sind häufig die selbstdualen Codes. Aus Eigenschaften von Codes wiederum, wie zum Beispiel der Selbstdualität, ergeben sich Invarianzeigenschaften der zugehörigen Gewichtszähler. Dies sind Polynome, die als Information die Häufigkeiten der verschiedenen Gewichtsverteilungen in C enthalten und damit auch Informationen über seine fehlerkorrigierenden Eigenschaften. Ein berühmtes Ergebnis der Codierungstheorie ist der Satz von Gleason aus dem Jahr 1970. Dieser Satz besagt, dass Gewichtszähler doppelt gerader binärer selbstdualer Codes in dem Polynomring liegen, der von den Gewichtszählern p_{e_8} des Hamming-Codes der Länge 8 sowie $p_{g_{24}}$ des Golay-Codes der Länge 24 erzeugt wird.

In dem Buch [5] entwickeln G. Nebe, E.M. Rains und N.J.A. Sloane das Konzept des Typs eines Codes über Form-Ringe und ihre Darstellungen. Einerseits ermöglichen diese Strukturen die Modellierung von Codes mit bestimmten Eigenschaften; die selbstdualen doppelt geraden binären Codes etwa sind in dieser Sprache die Typ 2_{II}^E Codes. Auch die sehr allgemeine Klasse der $\mathbb{F}_q$-linearen Codes über dem endlichen Körper $\mathbb{F}_q$ findet ihre Entsprechung - dies sind genau die Codes vom Typ q^{lin}. Auf der anderen Seite liefert eine Darstellung ρ einer Form-Struktur eine komplexe Matrixgruppe $\mathcal{C}(\rho)$, die Clifford-Weil-Gruppe, unter der die Gewichtszähler von Codes des Typs ρ invariant sind. Die Darstellung ρ stellt also einen Zusammenhang her zwischen Eigenschaften von Codes des Typs ρ einerseits und Invarianzeigenschaften der zugehörigen Gewichtszähler andererseits. Im Fall der doppelt geraden selbstdualen binären Codes, also der Typ 2_{II}^E-Codes etwa ergibt sich eine komplexe Matrixgruppe, deren Invariantenring erzeugt wird von p_{e_8} und $p_{g_{24}}$. Resultate wie der Satz von Gleason lassen sich also auf immer die gleiche Weise mit Hilfe dieser Theorie beweisen.

Gleichzeitig liefert die Kenntnis des Invariantenrings von $\mathcal{C}(\rho)$ einen Überblick über mögliche Gewichtszähler von Codes des Typs ρ. Mit Hilfe der Invariantentheorie lassen sich daher etwa obere Schranken an das Minimalgewicht von Codes herleiten, welches sich aus dem Gewichtszähler ablesen lässt und gleichzeitig ein Maßstab für die fehlerkorrigierenden Eigenschaften ist.

Gewisse Typen ρ von Codes erlauben die Definition eines Schattens. Ist $C \leq \mathbb{F}^N$, so ist dies ein Teilraum von $\mathbb{F}^N$, dessen Gewichtszähler durch Variablensubstitution aus dem Gewichtszähler von C hervorgeht. Diese Substitution geht aus der Darstellung ρ hervor. Man kann also durch Anwenden der Schattentransformation prüfen, ob ein Element des Invariantenrings von $\mathcal{C}(\rho)$ der Gewichtszähler eines Codes vom Typ ρ ist. Das entstehende Polynom muss als Gewichtszähler eines Teilraums von $\mathbb{F}^N$ in Frage kommen; zum Beispiel dürfen keine negativen Koeffizienten auftauchen. Diese Vorgehensweise wird im letzten Teil dazu benutzt, bessere obere Schranken an das Minimalgewicht zu finden.

Nun zum Inhalt: Nach einer Einführung in die Codierungstheorie und die Invariantentheorie führt das dritte Kapitel die Sprache der Form-Ringe ein, deren Darstellungen den Typ eines Codes definieren. Darauf aufbauend wird im vierten Kapitel die eingangs erwähnte endliche komplexe Matrixgruppe $\mathcal{C}(\rho)$, die Clifford-Weil-Gruppe, konstruiert. Im sechsten Kapitel wird die Struktur dieser Gruppe untersucht und im siebten Kapitel wird der Hauptsatz von [5] bewiesen, der besagt, dass der Invariantenring von $\mathcal{C}(\rho)$ von den Gewichtszählern von Codes vom Typ ρ erzeugt wird. Hierbei konzentrieren wir uns auf den wichtigen Fall, dass der zugrundeliegende Ring ein Matrixring über einem

endlichen Körper ist. Dies vereinfacht viele Beweise und ermöglicht einen vollständigen Beweis des Hautsatzes in diesem Fall. Im achten Kapitel wird der Hauptsatz am Beispiel von Codes über $\mathbb{F}_4 \oplus \mathbb{F}_4 u$ illustriert; dort finden wir auch Codes, die den entsprechenden Invariantenring erzeugen. Im letzten Kapitel erhalten wir durch gleichzeitiges Betrachten der Gewichtszähler des Codes und seines Schattens (der im fünften Kapitel eingeführt wird) neue bessere Schranken an den Minimalabstand Euklidisch selbstdualer Codes über $\mathbb{F}_4$.

Für die verallgemeinert doppelt geraden Codes über $\mathbb{F}_4$ geben wir bis zur Länge 32 alle extremalen Gewichtszähler an. Für die Rechnungen wurden die Computeralgebrasysteme MAGMA ([2]) und MAPLE ([3]) benutzt.

1 Codes und ihre Gewichtszähler

In diesem Kapitel möchte ich einige Grundbegriffe einführen und motivieren.

Definition 1.1. *Ist A eine endliche Menge, so nennt man eine Teilmenge $C \subseteq A^N$ einen Code. Man nennt A das Alphabet des Codes C.*

In dieser Definition wird von dem Code C noch recht wenig Struktur verlangt. Als klassische Codes sind Untervektorräume des K-Vektorraums K^N bekannt, wobei K ein endlicher Körper ist. Das Alphabet K besitzt in diesem Fall eine Gruppenstruktur.

Codes werden zur Nachrichtenübertragung gebraucht. Nach ihrer Übermittlung müssen die Codeworte decodiert werden; zuvor jedoch müssen eventuelle Übertragungsfehler korrigiert werden. Dies geschieht durch Ermittlung des Codeworts, welches in einem im Folgenden präzisierten Sinne den geringsten Abstand zum übermittelten Codewort aufweist.

Definition 1.2. *Seien A eine endliche Menge und $C \subseteq A^N$ ein Code. Für $c, c' \in C$ seien*

$$d(c, c') := |\{i \in \{1, \dots, n\} \mid c_i \neq c'_i\}|$$

der Hamming-Abstand von c und c' sowie

$$d(C) := \min\{d(c, c') \mid c, c' \in C, c \neq c'\}$$

der Minimalabstand von C.

Bemerkung 1.3. *Der Minimalabstand von C bestimmt die fehlerkorrigierenden Eigenschaften von C: Es gelten*

(i) $d(C) - 1$ *ist die Anzahl der Fehler, die C erkennt.*

(ii) $\left\lceil \frac{d(C)-1}{2} \right\rceil$ *ist die Anzahl der Fehler, die C korrigiert.*

Hat ein Code C gute fehlerkorrigierende Eigenschaften, so wird er schlicht als gut bezeichnet.

Ist das Alphabet A von C eine endliche abelsche Gruppe und $C \leq A^N$, so lassen sich die fehlerkorrigierenden Eigenschaften mit Hilfe des Begriffs des Minimalgewichts erfassen.

Definition und Bemerkung 1.4. *(Minimalgewicht eines Codes.) Es seien A eine abelsche Gruppe und $C \leq A^N$ eine Untergruppe.*

(i) Es sei $c = (c_1, \dots, c_N) \in C$. Dann heißt

$$\mathrm{wt}(c) := \{i \in \{1, \dots, n\} \mid c_i \neq 0\}$$

das Gewicht von c.

(ii) Man nennt $\mathrm{wt}(C) := \min\{\mathrm{wt}(c) \mid c \in C,\ c \neq 0\}$ *das Minimalgewicht von C.*

(iii) Wegen $d(c, c') = \mathrm{wt}(c - c')$ für $c, c' \in C$ gilt

$$d(C) = \mathrm{wt}(C).$$

Im Folgenden seien stets A eine endliche abelsche Gruppe und $C \leq A^N$.
Das Minimalgewicht von C lässt sich aus seinem vollständigen Gewichtszähler ablesen.

Definition 1.5. *Für $c \in C$ und $a \in A$ sei $n_a(c) := |\{i \in \{1, \ldots, n\} \mid c_i = a\}|$. Dann heißt*

$$\mathrm{cwe}(C) := \sum_{c \in C} \prod_{a \in A} x_a^{n_a(c)} \quad \in \mathbb{C}[x_a \mid a \in A]$$

der vollständige Gewichtszähler von C.

Der vollständige Gewichtszähler eines Codes $C \leq A^N$ ist ein homogenes Polynom vom Grad N.

Definition 1.6. *Es seien R ein Ring und $p \in R[x_1, \ldots, x_n]$. Gilt für zwei Monome $x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$ und $x_1^{b_1} \cdot \ldots \cdot x_n^{b_n}$ mit nicht verschwindenden Koeffizienten in p, dass $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i =: N$ ist, so nennt man p homogen vom Grad N. Mit $R[x_1, \ldots, x_n]_N$ bezeichnen wir die Menge aller homogenen Polynome in $R[x_1, \ldots, x_n]$ vom Grad N.*

Im Folgenden wird der volle Gewichtszähler eines Codes C eingeführt, der als eine direkte Kopie von C angesehen werden kann. Dazu benötigen wir noch eine Definition.

Definition 1.7 (Gruppenring). *Seien R ein Ring und G eine endliche Gruppe. Es bezeichne RG den freien R-Modul auf $(b_g \mid g \in G)$. Mit der Multiplikation $b_g b_h := b_{gh}$ für alle $g, h \in G$ wird RG zu einer R-Algebra, dem sogenannten Gruppenring von G über R.*

Definition 1.8. *Der volle Gewichtszähler von C ist definiert durch*

$$\mathrm{fwe}(C) := \sum_{c \in C} b_c \ \in \mathbb{C}A^N.$$

Der vollständige Gewichtszähler $\mathrm{cwe}(C)$ geht aus $\mathrm{fwe}(C)$ gewissermaßen durch Vergessen der Anordnung der Koordinaten hervor. Dies wir im Folgenden präzisiert.

Definition und Bemerkung 1.9. *Definieren wir eine Abbildung*

$$\mathrm{Sym}: \ \mathbb{C}[A^N] \to \mathbb{C}[x_a \mid a \in A], \quad b_{(a_1, \ldots, a_N)} \mapsto \prod_{i=1}^N x_{a_i},$$

so ist Sym *ein $\mathbb{C}$-Vektorraumhomomorphismus, welcher* $\mathrm{fwe}(C)$ *auf* $\mathrm{cwe}(C)$ *abbildet.*

Die Eigenschaften eines Codes spiegeln sich in Invarianzeigenschaften seines Gewichtszählers unter gewissen linearen Transformationen wieder. Sei etwa K ein endlicher Körper und $C \leq K^N$ ein K-Teilraum, der mit seinem Orthogonalraum bezüglich des Euklidischen Skalarprodukts

$$< x, y >= \sum_{i=1}^N x_i y_i, \ x = (x_1, \ldots, x_N), \ y = (y_1, \ldots, y_N)$$

übereinstimmt. Dann ist $N = 2\dim(C)$ gerade (siehe dazu Bemerkung 3.20) und als homogenes Polynom vom Grad N ist $\mathrm{cwe}(C) \in \mathbb{C}[x_k \mid k \in K]$ dann invariant unter der Transformation

$$x_k \mapsto -x_k, \ k \in K.$$

Lineare Transformationen werden beschrieben durch die Operation gewisser komplexer Matrizen. Die Operation einer komplexen Matrixgruppe auf $\mathbb{C}[x_a \mid a \in A]$ wird im Folgenden definiert.

Definition und Bemerkung 1.10. *Ist $G \leq \mathrm{GL}_n(\mathbb{C})$, so induziert jedes $g \in G$ einen $\mathbb{C}$-Algebrenautomorphismus von $\mathbb{C}[x_1, \ldots, x_n]$ durch*

$$p \cdot g(x_1, \ldots, x_n) = p(g(x_1), \ldots, g(x_n)),$$

für $p \in \mathbb{C}[x_1, \ldots, x_n]$, wobei

$$g(x_j) = \sum_{i=1}^{n} g_{ij} x_i,\ j \in \{1, \ldots, n\}.$$

Diese linearen Transformationen auf $\mathbb{C}[x_a \mid a \in A]$ sind Ringhomorphismen, welche in gewisser Weise mit speziellen Automorphismen von $\mathbb{C}A^N$ korrespondieren. Dies beschreibt das folgende Lemma.

Lemma 1.11. *Es sei $T : \mathbb{C}[x_a \mid a \in A] \to \mathbb{C}[x_a \mid a \in A]$ ein Ringhomomorphismus. Wir definieren Funktionen f_a für $a \in A$ durch*

$$T(x_a) = \sum_{v \in A} f_a(v) x_v.$$

Ist $\tilde{T} : \mathbb{C}A^N \to \mathbb{C}A^N$ ein $\mathbb{C}$-Vektorraumhomomorphismus mit

$$\tilde{T}(b_{\tilde{a}}) = \sum_{\tilde{v} \in A^N} f_{a_1}(v_1) \ldots f_{a_N}(v_N)\ b_{\tilde{v}}$$

für $\tilde{a} = (a_1, \ldots, a_N),\ \tilde{v} = (v_1, \ldots, v_N) \in A^N$, so ist $\mathrm{Sym} \circ \tilde{T} = T \circ \mathrm{Sym}$.

Beweis. Es sei $\tilde{a} = (a_1, \ldots, a_N) \in A^N$. Dann gilt

$$\begin{aligned} \mathrm{Sym}(\tilde{T}(b_{\tilde{a}})) &= \mathrm{Sym}(\sum_{\tilde{v} \in A^N} f_{a_1}(v_1) \ldots f_{a_N}(v_N)\ b_{\tilde{v}}) = \sum_{\tilde{v} \in A^N} \prod_{i=1}^{N} f_{a_i}(v_i) x_{v_i} \\ &= \prod_{i=1}^{N} \sum_{v \in A} f_{a_i}(v) x_v = \prod_{i=1}^{N} T(x_{a_i}) = T(\prod_{i=1}^{N} x_{a_i}) = T(\mathrm{Sym}(b_{\tilde{a}})). \end{aligned}$$

□

In den folgenden Kapiteln werden aus den Eigenschaften eines Codes C häufig zunächst Invarianzeigenschaften seiner direkten Kopie $\mathrm{fwe}(C)$ hergeleitet - die entsprechenden Automorphismen von $\mathbb{C}V$ haben dabei immer die in Lemma 1.11 beschriebene Gestalt. Lemma 1.11 liefert in diesen Fällen ein allgemeines Prinzip, um die Invarianzeigenschaften von $\mathrm{fwe}(C)$ auf $\mathrm{cwe}(C)$ zu übertragen.

Mehr Informationen über den Code erhält man, indem man höhere Gewichtszähler betrachtet.

Definition 1.12. *Es sei $C \leq A^N$ ein Code und $m \in \mathbb{N}$. Sind $c^{(1)}, \ldots, c^{(m)} \in C$ sowie $v = (v^{(1)}, \ldots, v^{(m)}) \in A^m$, so definieren wir*

$$a_v(c^{(1)}, \ldots, c^{(m)}) := |\{i \in \{1, \ldots, N\} \mid c_i^{(1)} = v^{(1)}, \ldots, c_i^{(m)} = v^{(m)}\}|.$$

Dann heißt

$$\mathrm{cwe}_m(C) := \sum_{c^{(1)}, \ldots, c^{(m)} \in C} \prod_{v \in A^m} x_v^{a_v(c^{(1)}, \ldots, c^{(m)})} \in \mathbb{C}[x_v \mid v \in A^m]$$

der Geschlecht-m-Gewichtszähler von C.

In $\mathrm{cwe}_m(C)$ gehen also die Spalten der Matrizen $A^{m\times N}$ ein, deren Zeilen Codeworte sind.

Beispiel 1.13. *Es sei $i_2 \leq \mathbb{F}_2^2$ der Code mit Erzeugermatrix $A := (1\ 1)$; das heißt, die Zeilen von A erzeugen i_2 als $\mathbb{F}_2$-Vektorraum. Dann ist $i_2 = \{(0,0),(1,1)\}$, $\mathrm{fwe}(i_2) = b_{(0,0)} + b_{(1,1)}$, $\mathrm{cwe}(i_2) = x_0^2x_1^2$ und*

$$\mathrm{cwe}_2(i_2) = x_{00}^2 + x_{11}^2 + x_{10}^2 + x_{01}^2.$$

In Beispiel 1.13 lässt sich bereits die folgende allgemeine Tatsache beobachten.

Bemerkung 1.14. *Es sei $C \leq \mathbb{F}_q^N$ ein Code und auch ein $\mathbb{F}_q$-Vektorraum. Die Dimension von C als $\mathbb{F}_q$-Vektorraum sei m. Dann ist C durch $\mathrm{cwe}_m(C)$ eindeutig bestimmt bis auf Permutation der Koordinaten.*

Beweis. Es seien $c_1,\dots,c_m \in C$ mit $c_i = (c_i^{(1)},\dots,c_i^{(N)})$ für $i = 1,\dots,N$. Dann bildet $(c_1,\dots,c_m)$ genau dann eine Basis von C, wenn die Matrix $(c_i^{(j)})_{ij}$ den Rang m hat. Wegen $\dim(C) = m$ existiert ein Monom $\prod_{i=1}^N x_{v_i}$ mit $v_i = (v_i^{(1)},\dots,v_i^{(m)})$ für $i = 1,\dots,N$ mit nicht verschwindendem Koeffizienten in $\mathrm{cwe}_m(C)$, so dass die Matrix $A := (v_i^{(j)})_{ij}$ den Rang m hat. Dann bilden die Spalten von A eine Basis von C. □

2 Invariantenringe

Im vorigen Kapitel haben wir beispielhaft gesehen, dass Gewichtszähler von Codes invariant sind unter gewissen linearen Transformationen, die von den Eigenschaften der Codes abhängen. Später werden wir diesen Zusammenhang mit Hilfe des Begriffs der Darstellung eines Form-Rings spezifizieren, indem wir feststellen, dass die Gewichtszähler im Invariantenring der komplexen Matrixgruppe $\mathcal{C}(\rho)$ liegen, der Clifford-Weil-Gruppe, welche wiederum durch die Eigenschaften der Codes bestimmt wird. In diesem Kapitel beschäftigen wir uns mit der Struktur solcher Invariantenringe. Die Kenntnis dieser Struktur verschafft einen Überblick über mögliche Gewichtszähler von Codes, was besonders im Hinblick auf das maximal mögliche Minimalgewicht interessant ist. Die Sätze in diesem Kapitel finden sich in [10].

Definition 2.1 (Invariantenring einer Matrixgruppe). *Ist $G \leq \mathrm{GL}_n(\mathbb{C})$, so heißt*

$$\mathrm{Inv}(G) := \{p \in \mathbb{C}[x_1,\dots,x_n] \mid p\cdot g = p \text{ für alle } g \in G\}$$

der Invariantenring von G.

Gemäß 1.10 ist $\mathrm{Inv}(G)$ tatsächlich ein Ring. Weiter erhält die Operation von G auf $\mathbb{C}[x_1,\dots,x_n]$ die Eigenschaft der Homogenität in dem Sinne, dass für $p \in \mathbb{C}[x_1,\dots,x_n]$, p homogen vom Grad N die Transformation $p\cdot g$ für $g \in G$ ebenfalls homogen vom Grad N ist. Daher gilt

$$\mathrm{Inv}(G) = \oplus_{N=0}^{\infty} \mathrm{Inv}(G)_N,$$

wobei

$$\mathrm{Inv}(G)_N = \mathbb{C}[x_1,\dots,x_n]_N \cap \mathrm{Inv}(G) = \{p \in \mathrm{Inv}(G) \mid p \text{ homogen vom Grad } N$$

2.1 Die Cohen-Macaulay-Eigenschaft

Definition 2.2. *Sei R eine graduierte $\mathbb{C}$-Algebra mit Krull-Dimension n. Die Menge $\{\theta_1, \ldots, \theta_n\} \subset H(R_+)$ heißt homogenes Parametersystem für R, falls R endlich erzeugt ist als $\mathbb{C}[\theta_1, \ldots, \theta_n]$-Modul. Insbesondere sind dann $\theta_1, \ldots, \theta_n$ algebraisch unabhängig.*

Das Noethersche Normalisierungslemma besagt, dass ein solches homogenes Parametersystem für jede graduierte $\mathbb{C}$-Algebra R existiert.

Satz 2.3. *Es seien R eine graduierte $\mathbb{C}$-Algebra und $\theta_1, \ldots, \theta_n$ ein homogenes Parametersystem für R. Dann sind die folgenden beiden Bedingungen äquivalent.*

(i) R ist ein freier $\mathbb{C}[\theta_1, \ldots, \theta_n]$-Modul, das heißt, es existieren $\eta_1, \ldots, \eta_t \in R$ mit

$$R = \oplus_{i=1}^{t} \eta_i \mathbb{C}[\theta_1, \ldots, \theta_n].$$

(ii) Ist $\phi_1, \ldots, \phi_n$ ein homogenes Parametersystem für R, so ist R frei als $\mathbb{C}[\phi_1, \ldots, \phi_n]$-Modul.

Bemerkung 2.4. *In Satz 2.3 können wir annehmen, dass $\eta_1, \ldots, \eta_t$ homogen sind.*

Man sagt, dass eine graduierte $\mathbb{C}$-Algebra R die Cohen-Macaulay-Eigenschaft besitzt, falls sie einer und damit beiden Bedingungen aus Satz 2.3 genügt.

Eine Darstellung von R wie in Satz 2.3 (i) heißt dann Hironaka-Zerlegung von R. Aus einer Hironaka-Zerlegung von R läßt sich die Hilbert-Reihe von R, welche im nächsten Abschnitt definiert wird, unmittelbar ablesen.

Definition und Bemerkung 2.5. *Ist $G \leq \mathrm{GL}_n(\mathbb{C})$ eine endliche komplexe Matrixgruppe, so hat $\mathrm{Inv}(G)$ die Cohen-Macaulay-Eigenschaft. Mit den Bezeichnungen von Satz 2.3 heißen dann $\theta_1, \ldots, \theta_n$ die primären Invarianten und $\eta_1, \ldots, \eta_n$ die sekundären Invarianten von $\mathrm{Inv}(G)$.*

2.2 Die Hilbertreihe eines Invariantenrings

Definition 2.6. *Es sei $R = R_0 \oplus R_1 \oplus R_2 \oplus \ldots$ eine graduierte $\mathbb{C}$-Algebra. Für $i \in \mathbb{N}$ sei $n_i := \dim_{\mathbb{C}}(R_i)$. Dann heißt die formale Potenzreihe*

$$H(R, z) := \sum_{i=0}^{\infty} n_i z^i$$

die Hilbertreihe von R.

Die Hilbertreihe des Invariantenrings einer endlichen komplexen Matrixgruppe lässt sich auch direkter durch die Gruppe selbst beschreiben.

Definition 2.7. *Es sei G eine endliche komplexe Matrixgruppe. Die formale Potenzreihe*

$$Molien(G, z) := \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(id - zg)}$$

heißt die Molienreihe von G.

Satz 2.8 (Molien). *Es sei G eine endliche komplexe Matrixgruppe und R der Invariantenring von G. Dann gilt*

$$Molien(G, z) = H(R, z).$$

Satz 2.9. *Es sei R eine graduierte Cohen-Macaulay-Algebra mit einer Hironaka-Zerlegung wie in Satz 2.3. Dann ist die Hilbertreihe von R gegeben durch*

$$H(R,z) = \frac{z^{\deg(\eta_1)} + \ldots + z^{\deg(\eta_t)}}{(1-z^{\deg(\theta_1)}) \cdot \ldots \cdot (1-z^{\deg(\theta_n)})}.$$

Existieren Codes $C_1^p, \ldots, C_n^p, C_1^s, \ldots, c_t^s$ vom Typ ρ mit

$$\mathrm{Inv}_{\mathbb{C}[x_v \mid v \in V]}(\mathcal{C}(rho)) = \mathrm{cwe}(C_1^s)[\mathrm{cwe}(C_1^p), \ldots, \mathrm{cwe}(C_n^p)] + \ldots + \mathrm{cwe}(C_t^s)[\mathrm{cwe}(C_1^p), \ldots, \mathrm{cwe}(C_n^p)],$$

so schreiben wir auch

$$\mathrm{Inv}_{\mathbb{C}[x_v \mid v \in V]}(\mathcal{C}(\rho)) = \frac{C_1^s, \ldots, C_t^s}{C_1^p, \ldots, C_n^p}.$$

Folgender Zusammenhang besteht zwischen der Ordnung einer Gruppe und ihren Invarianten.

Satz 2.10. *Es sei G eine endliche Gruppe. In einer Hironaka-Zerlegung wie in Satz 2.3 seien $d_1, \ldots, d_n$ die Grade der primr̈en Invarianten. Ist t die Anzahl der sekundären Invarianten, so gilt*

$$t = \frac{d_1 d_2 \ldots d_n}{|G|}.$$

3 Der Typ eines Codes

In diesem Kapitel wird der in dem Buch [5] entwickelte theoretische Rahmen vorgestellt, der es ermöglicht, die vielgestaltigen Eigenschaften linearer Codes durch die Begriffe der Isotropie und der Selbstdualität zu erfassen. Diese Begriffe werden immer bezüglich einer Darstellung gebildet; dies ist eine Datenstruktur, welche geeignet ist, die Eigenschaften linearer Codes zu modellieren. Eigenschaften von Codes werden also indirekt durch algebraische Objekte beschrieben, denen eine gewisse Struktur gemeinsam ist.

Darstellungen wiederum sind Konkretisierungen allgemeinerer Objekte, der Form-Ringe. Zu einem Form-Ring gibt es verschiedene Darstellungen, die Codes verschiedener Längen oder auch, wie in Abschnitt 3.3, Codes mit unterschiedlichen Eigenschaften modellieren können.

Die abstraktere Betrachtungsweise durch Form-Ringe ermöglicht die Definition der Witt-Gruppe (siehe [5]) sowie der hyperbolischen counitären Gruppe $\mathcal{U}(R,\Phi)$ in Kapitel 6. Die Betrachtung von $\mathcal{U}(R,\Phi)$ erleichtert die Bestimmung des Isomorphietyps der in der Einleitung erwähnten Gruppe $\mathcal{C}(\rho)$, da diese eine projektive Darstellung von $\mathcal{U}(R,\Phi)$ ist. Mit Hilfe der Darstellungen wiederum lässt sich $\mathcal{C}(\rho)$ allgemein beschreiben; dies geschieht in Kapitel 4.

3.1 Form-Ringe

Definition 3.1. *Ein Quadrupel (R, M, ψ, Φ) heißt Form Ring, falls die folgenden sechs Bedingungen erfüllt sind.*

a) *R ist ein Ring.*

b) *M ist ein $R \otimes R$-Rechtsmodul mit Automorphismus $\tau : M \to M$, so dass $\tau(m)(r \otimes s) = \tau(m(s \otimes r))$ für alle $m \in M, r, s \in R$ und $\tau^2 = id_M$.*

c) *$\psi : R_R \to M_{1\otimes R}$ ist ein R-Modulisomorphismus, so dass $\epsilon := \psi^{-1}(\tau(\psi(1))) \in R^*$.*

d) *Φ ist ein R-qModul, d.h. Φ ist eine abelsche Gruppe und es gibt eine Abbildung $[\ ] : R \to \mathrm{End}_{\mathbb{Z}}(\Phi)$ mit*

   (i) $[1] = id$

   (ii) $[r][s] = [r \cdot s]$

   (iii) $[r + s + t] + [r] + [s] + [t] = [r + s] + [t + s] + [r + t]$

   für alle $r, s, t \in R$.

e) *Es existieren Abbildungen $\lambda : \Phi \to M, \{\!\{\ \}\!\} : M \to \Phi$ mit*

$$\{\!\{\tau(m)\}\!\} = \{\!\{m\}\!\}, \quad \tau(\lambda(\phi)) = \lambda(\phi) \quad \textit{und} \quad \lambda(\{\!\{m\}\!\}) = m + \tau(m)$$

   für alle $m \in M$ und $\phi \in \Phi$.

f) *Es gilt $\phi[r + s] = \phi[r] + \phi[s] + \{\!\{\lambda(\phi)(r \otimes s)\}\!\}$ für alle $\phi \in \Phi$ und $r, s \in R$.*

Ein Morphismus von Form-Ringen besteht aus einem Tripel von Abbildungen, das mit diesen Strukturen verträglich ist. Speziell für Isomorphismen ergibt sich

Definition 3.2 (Isomorphismen von Form-Ringen). *Es seien $\mathcal{R}_1 = (R_1, M_1, \psi_1, \Phi_1)$ sowie $\mathcal{R}_2 = (R_2, M_2, \psi_2, \Phi_2)$ zwei Form-Ringe; weiter seien τ_i, λ_i und $\{\!\{\ \}\!\}_i$ für $i = 1, 2$ wie in Definition 3.1. Die Form-Ringe $\mathcal{R}_1$ und $\mathcal{R}_2$ heißen isomorph, falls ein Tripel (f_R, f_M, f_Φ) existiert, welches den folgenden neun Bedingungen genügt:*

(i) $f_R : R_1 \to R_2$ *ist ein Ringisomorphismus.*

(ii) $f_M : M_1 \to M_2$ *ist ein Isomorphismus abelscher Gruppen.*

(iii) $f_\Phi : \Phi_1 \to \Phi_2$ *ist ein Isomorphismus abelscher Gruppen.*

(iv) Es gilt $f_M(m(r \otimes s)) = f_M(m)(f_R(r) \otimes f_R(s))$ *für alle* $m \in M_1$ *und* $r, s \in R_1$.

(v) Es gilt $f_\Phi(\phi[r])) = f_\Phi(\phi)[f_R(r)]$ *für alle* $\phi \in \Phi_1$ *und* $r \in R_1$.

(vi) Es gilt $f_M(\tau_1(m)) = \tau_2(f_M(m))$ *für alle* $m \in M_1$ *und* $r, s \in R$.

(vii) Es gilt $f_M(\psi_1(r)) = \psi_2(f_R(r))$ *für alle* $r \in R_1$.

(viii) Es gilt $f_M(\lambda_1(\phi)) = \lambda_2(f_\Phi(\phi))$ *für alle* $\phi \in \Phi_1$.

(ix) Es gilt $f_\Phi(\{\!\{m\}\!\}_1) = \{\!\{f_M(m)\}\!\}_2$ *für alle* $m \in M_1$.

Beispiel 3.3 (Reskalieren von Form-Ringen). *Es seien $\mathcal{R} = (R, M, \psi, \Phi)$ ein Form-Ring und $a \in R^*$. Wir definieren einen $1 \otimes R$-Modulhomomorphismus*

$$\psi^a : R \to M,\ s \mapsto \psi(as).$$

Dann ist $\mathcal{R}^a := (R, M, \psi^a, \Phi)$ ebenfalls ein Form-Ring, welcher isomorph ist zu $\mathcal{R}$. Man nennt $\mathcal{R}^a$ die Reskalierung von $\mathcal{R}$ bezüglich a.

Für jeden Form-Ring $\mathcal{R} = (R, M, \psi, \Phi)$ lässt sich ein Antiautomorphismus ^{J} von R folgendermaßen konstruieren:

Definition und Bemerkung 3.4. *Die Abbildung*

$$^J :\ R \to R,\ r \mapsto \psi^{-1}(\psi(1)(r \otimes 1))$$

ist ein Antiautomorphismus von R.

Dass ^{J} tatsächlich ein Antiautommorphismus ist, wird im Folgenden zusammen mit weiteren Rechenregeln in Form-Ringen bewiesen.

Bemerkung 3.5. *[Einige Rechenregeln in Form-Ringen] Für den Antiautomorphismus ^{J} von R gelten*

(i) $\psi(r)(s \otimes t) = \psi(s^J r t)$ *für alle* $r, s, t \in R$,

(ii) $(rs)^J = s^J r^J$ *für alle* $r, s \in R$,

(iii) $\tau(\psi(r)) = \psi(r^J \epsilon)$ *für alle* $r \in R$,

(iv) $\epsilon^J r^{J^2} \epsilon = r$ *für alle* $r \in R$,

(v) $\epsilon^J \epsilon = 1$,

(vi) $\beta(r^{-J} v, v') = \beta(v, r v')$ *für alle* $r \in R,\ v, v' \in V$.

Beweis.

zu (i): $\psi(r)(s\otimes t)=\psi(r)(s\otimes 1)(1\otimes t)=\psi(1)(s\otimes 1)(1\otimes rt)=\psi(s^J)(1\otimes rt)=\psi(s^Jrt)$

zu (ii): Wir zeigen $\psi((rs)^J)=\psi(s^Jr^J)$; da ψ ein Isomorphismus ist, folgt dann $(rs)^J=s^Jr^J$ für alle $r,s\in R$. Es ist

$$\begin{aligned}\psi((rs)^J) &= \psi(\psi^{-1}(\psi(1)(rs\otimes 1)))=\psi(1)(rs\otimes 1)=\psi(1)(r\otimes 1)(s\otimes 1)\\ &\overset{(i)}{=} \psi(r^J)(s\otimes 1)\overset{(i)}{=}\psi(s^Jr^J).\end{aligned}$$

zu (iii): $\tau(\psi(r))=\tau(\psi(1)(1\otimes r))=(\tau(\psi(1)))(r\otimes 1)=\psi(\epsilon)(r\otimes 1)\overset{3.5(i)}{=}\psi(r^J\epsilon)$

zu (iv): Es ist $\psi(r)=\tau(\tau(\psi(r)))\overset{(iii)}{=}\tau(\psi(r^J\epsilon))\overset{(iii)}{=}\psi((r^J\epsilon)^J\epsilon)\overset{(ii)}{=}\psi(\epsilon^Jr^{J^2}\epsilon)$. Die Behauptung folgt nun, da ψ ein Isomorphismus ist.

zu (v): Nach (iv) ist $\epsilon^J1^{J^2}\epsilon=1$. Aus $1^{J^2}=1$ folgt $\epsilon^J\epsilon=1$.

zu (vi): Es ist $\beta(r^{-J}v,v')=\rho_M(\psi(1)(r^{-J}\otimes 1))(v,v')=\rho_M(\psi(r))(v,v')=\beta(v,rv')$.

□

Bemerkung 3.6. *Mit den Bezeichnungen von Definition 3.1 besagt Teil (v) von Bemerkung 3.5, dass ϵ stets ein Linksinverses in R besitzt. Ist R endlich, so ergibt sich daraus $\epsilon\in R^*$, das heißt, diese Forderung ist dann in Definition 3.1(c) entbehrlich.*

Beweis. Wir betrachten die Abbildung $m_\epsilon: R\to R$. Nach Bemerkung 3.5(v) ist m_ϵ injektiv, denn für $x,y\in R$ folgt aus $\epsilon x=\epsilon y$, dass $\epsilon^J\epsilon x=\epsilon^J\epsilon y$, also $x=y$. Wegen $|R|<\infty$ ist m_ϵ auch surjektiv. □

Beispiel 3.7. *Ist $\mathcal{R}=(R,M,\psi,\Phi)$ ein Form-Ring mit ^{J} wie in Definition und Bemerkung 3.4 und $\mathcal{R}^a$ die Reskalierung von $\mathcal{R}$ bezüglich $a\in R^*$, so ist der Antiautomorphismus $^{J^a}$ von $\mathcal{R}^a$ gegeben durch*

$$r^{J^a}=a^{-1}r^Ja$$

für $r\in R$. Denn es ist

$$r^{J^a}=(\psi^a)^{-1}(\psi^a(1)(r\otimes 1))=a^{-1}\psi^{-1}(\psi(a)(r\otimes 1))=a^{-1}\psi^{-1}(\psi(1)(r\otimes 1))a.$$

In Kapitel 4 werden wir besonders die folgenden speziellen Idempotente betrachten.

Definition 3.8. *Seien R ein Ring und ^{J} ein Antiautomorphismus von R. Ein Idempotent $e\in R$ heißt symmetrisch bezüglich ^{J} genau dann, wenn gilt*

$$eR\cong e^JR$$

als R-Rechtsmoduln. Ein Idempotent, welches nicht Summe anderer nichttrivialer Idempotente ist, heißt primitiv.

Beispiel 3.9. *Es sei speziell R ein Matrixring über einem endlichen Körper K, also $R=K^{n\times n}$, und es sei ^{J} ein (Anti-) Automorphismus von K. Durch*

$$^{J^{(n)}}: R\to R,\ (r_{ij})\mapsto(r_{ji}^J)$$

erhalten wir einen Antiautomorphismus von R. Dann sind alle primitiven symmetrischen Idempotente bezüglich $^{J^{(n)}}$ konjugiert zu $e_1:=\mathrm{diag}(1,0,\ldots,0)$. Denn bekanntlich sind Idempotente diagonalisierbar mit Eigenwerten 0 und 1; mit der Definition von Primitivität folgt die Behauptung.

Bemerkung 3.10. *Sei R ein Ring. Ein Idempotent $e \in R$ ist genau dann symmetrisch bezüglich des Antiautomorphismus' J von R, wenn Elemente $u_e \in eRe^J, v_e \in e^J Re$ existieren mit $u_e v_e = e$ und $v_e u_e = e^J$.*

Beweis. Ist $\psi : eR \to e^J R$ ein R-Rechtsmodulisomorphismus, so definieren wir $v_e := \psi(e)$ sowie $u_e := \psi^{-1}(e^J)$. Diese Elemente haben die gewünschten Eigenschaften:

$$v_e e = \psi(e)e = \psi(e^2) = \psi(e) = v_e$$

$$u_e e^J = \psi^{-1}(e^J)e^J = \psi^{-1}(e^J e^J) = \psi^{-1}(e^J) = u_e$$

$$v_e u_e = \psi(e)u_e = \psi(eu_e) = \psi(u_e) = e^J$$

$$u_e v_e = \psi^{-1}(e^J)v_e = \psi^{-1}(e^J v_e) = \psi^{-1}(v_e) = e.$$

Umgekehrt wird durch $\psi : eR \to e^J R, e \mapsto v_e$ ein Isomorphismus von R-Rechtsmoduln definiert, da $\psi(eu_e r) = e^J r, r \in R$. □

Die folgende Bemerkung motiviert den Begriff der Darstellung eines Form-Rings. In einem Form-Ring $\mathcal{R} = (R, M, \psi, \Phi)$ haben M und Φ eine ähnliche Struktur wie die im Folgenden beschriebenen Bilinearformen bzw. quadratische Abbildungen - diese Abbildungen eigenen sich dazu, die Eigenschaften der Selbstdualität bzw. der Isotropie von Codes zu beschreiben (siehe Definition 3.16). Eine Darstellung von $\mathcal{R}$ besteht dementsprechend aus Morphismen von $\mathcal{R}$, welche $\mathcal{R}$ so konkretisieren, dass Eigenschaften von Codes modelliert werden können.

Bemerkung 3.11. *Seien R ein Ring, V ein R-Linksmodul und A eine abelsche Gruppe.*

a) Die Gruppe

$$\mathrm{Bil}(V, A) := \{\beta : V \times V \to A | \beta \text{ ist } \mathbb{Z} - \text{bilinear}\}$$

ist ein $R \otimes_{\mathbb{Z}} R$-Rechtsmodul durch

$$\beta(r \otimes s)(v, w) := \beta(rv, sw) \text{ für alle } \beta \in \mathrm{Bil}(V, A),\ v, w \in V.$$

Die Abbildung $\tau : \mathrm{Bil}(V, A) \to \mathrm{Bil}(V, A)$, definiert durch

$$\tau(\beta(v, w)) := \beta(w, v) \text{ für alle } \beta \in \mathrm{Bil}(V, A),\ v, w \in V$$

ist ein Automorphismus von $\mathrm{Bil}(V, A)$ mit $\tau^2 = id_{\mathrm{Bil}(V,A)}$.

b) Die Gruppe $\mathrm{Quad}_0(V, A)$ der quadratischen Abbildungen von V nach A, welche genau die Abbildungen $\phi : V \to A$ enthält mit

$$\phi(v+w+u)+\phi(v)+\phi(w)+\phi(u) = \phi(v+u)+\phi(w+u)+\phi(v+w) \text{ für alle } u, v, w \in V$$

ist ein R-qModul durch

$$\phi[r](v) := \phi(rv) \text{ für alle } \phi \in \mathrm{Quad}_0(V, A),\ r \in R,\ v \in V.$$

Aus der definierenden Eigenschaft der Gruppe $\mathrm{Quad}_0(V, A)$ ergibt sich für $\phi \in \mathrm{Quad}_0(V, A)$, dass $\phi(0) = 0$.

c) Die Abbildungen $\lambda : \mathrm{Quad}_0(V,A) \to \mathrm{Bil}(V,A)$ *und* $\{\!\{\ \}\!\} : \mathrm{Bil}(V,A) \to \mathrm{Quad}_0(V,A)$*, definiert durch*

$$\lambda(\phi)(v,w) = \phi(v+w) - \phi(v) - \phi(w) \text{ für alle } \phi \in \mathrm{Quad}_0(V,A),\ v,w \in V,$$

$$\{\!\{\beta\}\!\}(v) = \beta(v,v) \text{ für alle } \beta \in \mathrm{Bil}(V,A),\ v \in V,$$

haben die Eigenschaften, dass

$$\{\!\{\tau(m)\}\!\} = \{\!\{m\}\!\}, \quad \tau(\lambda(\phi)) = \lambda(\phi)$$

sowie

$$\lambda(\{\!\{m\}\!\}) = m + \tau(m), \quad \phi[r+s] - \phi[r] - \phi[s] = \{\!\{\lambda(\phi)(r \otimes s)\}\!\}$$

für alle $m \in \mathrm{Bil}(V,A)$, $\phi \in \mathrm{Quad}_0(V,A)$ *und* $r,s \in R$*. Man nennt* $(\mathrm{Bil}(V,A), \mathrm{Quad}_0(V,A))$ *mit* $\tau, \{\!\{\ \}\!\}$ *und* λ *wegen obiger Eigenschaften ein quadratisches Paar über* R*.*

3.2 Darstellungen von Form-Ringen

Definition 3.12. *Sei* $\mathcal{R} = (R, M, \psi, \Phi)$ *ein Form-Ring. Ein Quadrupel* $\rho = (V, \rho_M, \rho_\Phi, \beta)$ *heißt Darstellung von* $\mathcal{R}$*, falls*

a) V *ist ein* R*-Linksmodul,*

b) $\rho_M : M \to \mathrm{Bil}(V,A)$ *(*A *eine abelsche Gruppe) ist* $R \otimes R$*-Modulhomomorphismus mit* $\rho_M(\tau(m))(v,w) = \rho_M(m)(w,v)$ *für alle* $m \in M, v, w \in V$*,*

c) $\rho_\Phi : \Phi \to \mathrm{Quad}_0(V,A)$ *ist* R*-qModulhomomorphismus,*

d) $\{\!\{\rho_M(m)\}\!\} = \rho_\Phi(\{\!\{m\}\!\})$ *für alle* $m \in M$ *und* $\rho_M(\lambda(\phi)) = \lambda(\rho_\Phi(\phi)))$ *für alle* $\phi \in \Phi$*,*

e) $\beta := \rho_M(\psi(1))$ *ist nichtsingulär, das heißt,* $v \mapsto \beta(v,\cdot), V \to \mathrm{Hom}(V,A)$ *ist ein Isomorphismus.*

Die Darstellung ρ *heißt endlich, falls* $|V| < \infty$ *und* $A = \mathbb{Q}/\mathbb{Z}$*.*

Im Folgenden bezeichne stets $\mathcal{R} = (R, M, \psi, \Phi)$ einen Form-Ring sowie $\rho = (V, \rho_M, \rho_\Phi, \beta)$ eine Darstellung von $\mathcal{R}$.

Wir kommen zu einer der grundlegendsten Definitionen:

Definition 3.13. *Ein Code* C *in* ρ *ist ein* R*-Untermodul von* V*.*

Zu einem Code C in ρ lässt sich sein dualer Code definieren.

Definition 3.14. *Ist* C *ein Code, so bezeichnet*

$$C^\perp = \{v \in V \mid \beta(v,c) = 0 \text{ für alle } c \in C\}$$

den dualen Code von C*.*

Bemerkung 3.15. *Ist* C *ein Code, so ist*

$$C^\perp = \{v \in V \mid \rho_M(m)(v,c) = 0 \text{ für alle } c \in C,\ m \in M\}.$$

Denn für $v_1, v_2 \in V$ *gilt*

$$\rho_M(m)(v_1,v_2) = \rho_M(\psi(\psi^{-1}(m)))(v_1,v_2) = \rho_M(\psi(1)(1 \otimes \psi^{-1}(m)))(v_1,v_2) = \beta(v_1, \psi^{-1}(m)v_2).$$

Ist nun $v_2 \in C$*, so ist auch* $\psi^{-1}(m) \in C$*, da* C *ein* R*-Teilmodul von* V *ist. Daraus folgt* $\beta(v_1, \psi^{-1}(m)v_2) = 0$*.*

Die eingangs erwähnten Eigenschaften der Selbstdualität und der Isotropie eines Codes lassen sich nun durch ρ folgendermaßen beschreiben:

Definition 3.16. *Es sei $C \leq V$ ein Code.*

(i) C heißt selbstorthogonal, falls $C \subseteq C^{\perp}$.

(ii) C heißt selbstdual, falls $C = C^{\perp}$.

(iii) C heißt isotrop, falls C selbstorthogonal ist und $\rho_\Phi(\phi)(c) = 0$ ist für alle $c \in C, \phi \in \Phi$.

Auch auf der abstrakten Ebene der Form-Ringe ist in gewisser Weise erkennbar, wie Eigenschaften von Codes in den zugehörigen Darstellungen modelliert werden können.

Bemerkung 3.17. *Es seien $\mathcal{R} = (R, M, \psi, \Phi)$ mit $\{\!\{\ \}\!\}$ und λ ein Form-Ring und $\rho = (V, \rho_M, \rho_\Phi, \beta)$ eine Darstellung von $\mathcal{R}$.*

(i) Ist $\{\!\{\ \}\!\}$ surjektiv, so ist ein selbstorthogonaler Code in ρ auch isotrop in ρ.

(ii) Ist λ surjektiv, so ist ein isotroper Code in ρ auch selbstorthogonal in ρ.

Beweis.

zu (i): Es seien $c \in C$ und $\phi = \{\!\{m\}\!\} \in \Phi, m \in M$. Dann gilt

$$\rho_\Phi(\{\!\{m\}\!\})(c) = \{\!\{\rho_M(m)\}\!\}(c) = \rho_M(m)(c,c) = \{\!\{\beta\}\!\}[m](c).$$

zu (ii): wie (i).

□

Aus einer Darstellung kann man weitere Darstellungen desselben Form-Rings konstruieren.

Definition 3.18. *a) Durch $\overline{\rho} := (V, -\rho_M, -\rho_\Phi, -\beta)$ erhält man wieder eine Darstellung von $\mathcal{R}$; $\overline{\rho}$ heißt die zu ρ konjugierte Darstellung.*

b) Für $N \in \mathbb{N}$ ist $N\rho := (V^N, \rho_M^N, \rho_\Phi^N, \beta^N)$ eine Darstellung von $\mathcal{R}$; hierbei sind ρ_M^N und ρ_Φ^N definiert durch

$$\rho_M^N(m)(v,w) = \sum_{i=1}^{N} \rho_M(m)(v_i, w_i), \qquad \rho_\Phi^N(\phi)(v) = \sum_{i=1}^{N} \rho_\Phi(\phi)(v_i)$$

für $v, w \in V^N,\ v = (v_1, \ldots, v_N),\ w = (w_1, \ldots, w_N)$.

In unserem Kontext ist die Darstellung $N\rho$ von besonderer Bedeutung, da sie es erlaubt, Codes mit unterschiedlicher Länge, aber ähnlichen Eigenschaften durch Variation der Darstellung zu modellieren. Auf diese Weise können wir nun den Typ eines Codes definieren:

Definition 3.19. *Ein Code der Länge N vom Typ ρ ist ein selbstdualer isotroper Code in $N\rho$.*

3.3 Beispiele von Typen von Codes

Zunächst eine Bemerkung, mit deren Hilfe sich in gewissen Fällen die Selbstdualität eines Codes nachweisen lässt.

Bemerkung 3.20. *Es seien K ein endlicher Körper und V ein endlich-dimensionaler K-Vektorraum sowie $\beta : V \times V \to \mathbb{Q}/\mathbb{Z}$ eine nichtsinguläre Bilinearform. Dann gilt*

$$dim_K(C^{\perp,\beta}) = dim_K(V) - dim_K(C).$$

Denn da β nichtsingulär ist, ist $V \cong Hom(V, \mathbb{Q}/\mathbb{Z})$ via $v \mapsto \beta(v, \cdot)$. Insbesondere ist die Abbildung $\psi : V \to Hom(C, \mathbb{Q}/\mathbb{Z}),\ v \mapsto \beta(v, \cdot)\big|_C$ ein Epimorphismus. Wegen $\mathrm{Kern}(\psi) = C^{\perp,\beta}$ folgt die Behauptung aus dem Homomorphiesatz für Gruppen.

3.3.1 q^{lin}

Wir wollen allgemeine lineare Codes über dem endlichen Körper $\mathbb{F}_q$ in der Sprache der Form-Ringe und ihrer Darstellungen modellieren.

Sei dazu

$$\mathcal{R}(q^{\mathrm{lin}}) := (\mathbb{F}_q \oplus \mathbb{F}_q, \mathbb{F}_q \oplus \mathbb{F}_q, \mathrm{id}, \{\!\{\mathbb{F}_q \oplus \mathbb{F}_q\}\!\}),$$

wobei $\{\!\{\mathbb{F}_q \oplus \mathbb{F}_q\}\!\} \cong \mathbb{F}_q$ und $q = p^f$ eine Primzahl ist. Eine Darstellung von $\mathcal{R}$ mit den gewünschten Eigenschaften ist gegeben durch $\rho(q^{\mathrm{lin}}) := (V, \rho_M, \rho_\Phi, \beta)$, wobei $V := \mathbb{F}_q \oplus \mathbb{F}_q$, $\rho_M(a, b) := m_{a,b}$ mit

$$m_{a,b}((x_1, y_1), (x_2, y_2)) := \frac{1}{p} \mathrm{Tr}_{\mathbb{F}_q|\mathbb{F}_p}(x_1 a y_2 + y_1 b x_2).$$

Hierbei bezeichne $\mathrm{Tr}_{\mathbb{F}_q|\mathbb{F}_p}$ die Spur von $\mathbb{F}_q$ in seinen Primkörper $\mathbb{F}_p$, den wir mit $\mathbb{Z}/p\mathbb{Z}$ identifizieren. Ist C ein Code der Länge N in $\rho(q^{\mathrm{lin}})$, so hat C als $\mathbb{F}_q \oplus \mathbb{F}_q$-Untermodul von $(\mathbb{F}_q \oplus \mathbb{F}_q)^N$ die Form $C = C_1 \oplus C_2$, wobei $C_1 = (1, 0)C \leq (1, 0)(\mathbb{F}_q \oplus \mathbb{F}_q)^N$ und $C_2 = (0, 1)C \leq (0, 1)(\mathbb{F}_q \oplus \mathbb{F}_q)^N$. Wir schreiben $c = (c_1, c_2)$ für $c \in C$ mit $c = c_1 + c_2$, $c_1 \in C_1, c_2 \in C_2$. Dann ist

$$\rho_M^N(m_{a,b})((c_1, c_2), (c_1', c_2')) = \sum_{i=1}^{N} (c_{1i} a c_{2i}' + c_{2i} b c_{1i}').$$

Es bezeichne $(\cdot, \cdot)$ das Euklidische Skalarprodukt auf $\mathbb{F}_q \times \mathbb{F}_q$, das heißt, $(a, b) = ab$ für $a, b \in \mathbb{F}_q$. Ist $(c, c') = 0$ für alle $c \in C_1$ und $c' \in C_2$, so ergibt sich aus obiger Gleichung die Selbstorthogonalität von C. Ebenso gilt, dass C selbstdual ist, falls $C_1 = C_2^\perp$ und damit auch $C_1^\perp = C_2$. Durch geeignete Wahl der a, b erhält man auch die Umkehrungen dieser Aussagen, da

$$\rho_M^N(m_{1,0})((c_1, c_2), (c_1', c_2')) = \sum_{i=1}^{N} c_{1i} c_{2i}'.$$

Im Folgenden werden die beiden Typen von Codes eingführt, mit denen wir uns in Kapitel 9 beschäftigen werden. Auch in Kapitel 5 werden diese Codes wieder aufgegriffen und bezüglich des dort eingeführten Begriffs des Schattens untersucht.

3.3.2 q_I^E

Euklidisch selbstduale Codes über $\mathbb{F}_q,\ q = 2^f$:

Diese Codes lassen sich modellieren durch den Form-Ring $\mathcal{R}(q_I^E) = (\mathbb{F}_q, \mathbb{F}_q, id, \mathbb{F}_q)$ mit $\{\,\} = \tau = id_{\mathbb{F}_q}$ und $\lambda = 0$. Die zugehörige Darstellung $\rho(q_I^E) = (\mathbb{F}_q, \rho_M, \rho_\Phi, \beta)$ ist definiert durch

$$\rho_M(m)(x,y) = \beta(1 \otimes m)(x,y) = \beta(x, my) := \frac{1}{2}\operatorname{Tr}_{\mathbb{F}_q|\mathbb{F}_2}(mxy)$$

für alle $m, x, y \in \mathbb{F}_q$. Die Abbildung ρ_Φ ist damit gemäß Bemerkung 3.17 wegen der Surjektivität von $\{\,\}$ bereits bestimmt, das heißt, es ist $\rho_\Phi(\Phi) =< \{\beta\} >=< \rho_\Phi(1) >$ als $\mathbb{F}_q$-qModul.

Codes vom Typ q_I^E enthalten den Einsvektor $\mathbf{1}$. Denn das Quadrieren ist ein Galois-Automorphismus von $\mathbb{F}_q$, und daher gilt

$$\beta(c,c) = \frac{1}{2}\operatorname{Tr}_{\mathbb{F}_q|\mathbb{F}_2}(c^2) = \frac{1}{2}\operatorname{Tr}_{\mathbb{F}_q|\mathbb{F}_2}(c) = \beta(1,c)$$

für alle $c \in C$.

Die selbstdualen (und damit auch isotropen) Codes in $N\rho(q_I^E)$ sind tatsächlich genau die euklidisch selbstdualen Codes in $\mathbb{F}_q$. Denn bezeichnen wir mit $(\cdot,\cdot) : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q$ das Euklidische Skalarprodukt auf $\mathbb{F}_q$, so gilt für einen Code $C \leq \mathbb{F}_q^N$ offensichtlich $C^{\perp,(\cdot,\cdot)} \subseteq C^{\perp,\beta}$. Da sowohl $(\cdot,\cdot)$ als auch β nichtsingulär sind, folgt aus Dimensionsgründen $C^{\perp,(\cdot,\cdot)} = C^{\perp,\beta}$.

3.3.3 q_{II}^E

Euklidisch selbstduale verallgemeinert doppelt-gerade Codes über $\mathbb{F}_q, q = 2^f$

Diese Codes sind zum Beispiel von Quebbemann in [8] und in [6] betrachtet worden. Für die Einführung dieses Typs benötigen wir die folgenden wohlbekannten Lemmata aus der Zahlentheorie.

Lemma 3.21. *Seien $n \in \mathbb{N}$ und K ein Körper mit $char(K) \nmid n$. Es bezeichne $\phi_m(x) \in \mathbb{Z}[x]$ für $m \in \mathbb{N}$ das m-te Kreisteilungspolynom. Genau dann ist $\zeta \in K$ eine primitive n-te Einheitswurzel, wenn $\phi_n(\zeta) = 0$ ist.*

Beweis. Wir führen den Beweis durch Induktion nach n und benutzen, dass

$$\phi_n(x) = \frac{x^n - 1}{\prod\limits_{\substack{d|m \\ d \neq m}} \phi_d(x)}.$$

"⇒": Ist $\zeta \in K$ eine primitive n-te Einheitswurzel, so ist ζ eine Nullstelle von $x^n - 1$, aber nach Induktionsvoraussetzung keine Nullstelle von $\phi_d(x)$ für $d|n, d \neq n$ - man beachte, dass $char(K) \nmid d$. Daher ist ζ Nullstelle von $\phi_n(x)$.

"⇐": Sei $\zeta \in K$ mit $\phi_n(\zeta) = 0$. Wegen $\phi_n(x) \big| x^n - 1$ ist ζ eine n-te Einheitswurzel. Angenommen, ζ ist nicht primitiv. Dann existiert nach Induktionsvoraussetzung ein $d \in \mathbb{N}$ mit $d|n,\ d \neq n$, so dass $\phi_d(\zeta) = 0$. Wegen $x^n - 1 = \prod_{d|n} \phi_d(x)$ ist ζ doppelte Nullstelle von $x^n - 1$, also auch Nullstelle von $(x^n - 1)' = nx^{n-1}$. Dies führt aber auf $\zeta = 0$, im Widerspruch zu der Tatsache, dass ζ eine n-te Einheitswurzel ist. □

Das folgende Lemma findet sich in [7] auf Seite 135. Im Folgenden bezeichne $\mathbb{Z}_p$ den Ring der ganzen p-adischen Zahlen und $\mathbb{Q}_p$ dessen Quotientenkörper.

Lemma 3.22 (Henselsches Lemma). *Es sei $f(x) \in \mathbb{Z}_p[x]$ mit $f(x) \not\equiv 0 \mod p$. Besitzt $f(x)$ modulo p ein Zerlegung*

$$\overline{f}(x) = \overline{g}(x)\overline{h}(x) \quad \in \mathbb{F}_p[x]$$

in teilerfremde Polynome $\overline{g}, \overline{h} \in \mathbb{F}_p[x]$, so besitzt $f(x)$ eine Zerlegung

$$f(x) = g(x)h(x) \quad \in \mathbb{Z}_p[x]$$

mit $\deg(g) = \deg(\overline{g})$ *sowie*

$$g(x) \equiv \overline{g}(x) \mod p \text{ und } h(x) \equiv \overline{h}(x) \mod p.$$

Lemma 3.23. *Es sei $q = 2^f,\ f \in \mathbb{N}$, und es sei $\zeta_{q-1} \in \overline{\mathbb{Q}_2}$ eine primitive $(q-1)$-te Einheitswurzel. Weiter sei $\mathbb{F}_q$ der Körper mit q Elementen. Dann ist*

$$\mathbb{F}_q \cong \mathbb{Z}_2[\zeta_{q-1}]/2\mathbb{Z}_2[\zeta_{q-1}].$$

Beweis. Es bezeichne $\mu(x) \in \mathbb{Z}_2[x]$ das Minimalpolynom von ζ_{q-1}, und es sei $\overline{\mu}(x) \in \mathbb{F}_2[x]$ die Reduktion von μ modulo 2. Wir zeigen, dass ein $\omega_0 \in \mathbb{F}_q$ mit Minimalpolynom $\overline{\mu}(x)$ existiert, welches die multiplikative Gruppe von $\mathbb{F}_q$ erzeugt. Wie in Lemma 3.21 bezeichne $\phi_m(x)$ für $m \in \mathbb{N}$ das m-te Kreisteilungspolynom. Wegen Lemma 3.21 gilt dann $\mu(x) \mid \Phi_{q-1}(x)$ in $\mathbb{Q}_2[x]$ und also auch in $\mathbb{Z}_2[x]$.

Nun sei $h(x) := x^{q-1} - 1 \in \mathbb{Z}_2[x]$. Wir betrachten gemäß 3.21 die Reduktion

$$\overline{h}(x) = \overline{\phi_{q-1}}(x) \prod_{\substack{d|(q-1),\\ d\neq q-1}} \overline{\phi}_d(x),$$

welche über $\mathbb{F}_q^*$ vollständig in Linearfaktoren zerfällt. Aus dem Henselschen Lemma ergibt sich, dass $\overline{\mu}(x) \in \mathbb{F}_2[x]$ irreduzibel ist, woraus die Existenz von ω_0 folgt - man beachte, dass ω_0 nach Lemma 3.21 eine primitive $(q-1)$-te Einheitswurzel ist.

Nun ist

$$\mathbb{F}_q = \mathbb{F}_2[\omega_0] \cong \mathbb{F}_2[x]/(\overline{\mu(x)}) \cong \mathbb{Z}_2[x]/(2, \mu(x)) \cong \mathbb{Z}_2[\zeta_{q-1}]/2\mathbb{Z}_2[\zeta_{q-1}]$$

□

Wir wollen Codes mit den folgenden Eigenschaften modellieren.

Definition 3.24. *Ein Code $C \leq \mathbb{F}_q^N$ heißt doppelt-gerade, falls für alle $c = (c_1, \ldots, c_N) \in C$ die Bedingungen*

$$(i) \quad \sum_{i=1}^{N} c_i = 0 \quad \text{und} \quad (ii) \quad \sum_{i<j} c_i c_j = 0$$

erfüllt sind.

Um die Eigenschaften euklidisch selbstdualer doppelt-gerader Codes über $\mathbb{F}_q$ in der Sprache der Form-Ringe und ihrer Darstellungen zu erfassen, betrachten wir den Form-Ring

$$\mathcal{R}(q_{II}^E) = (\mathbb{F}_q, \mathbb{F}_q, id, \mathcal{O}/4\mathcal{O}),$$

wobei $\mathcal{O} = \mathbb{Z}_2[\zeta_{2^f-1}]$. Gemäß Lemma 3.23 ist $\mathbb{F}_q = \mathcal{O}/2\mathcal{O}$. Ist ω_0 wie im Beweis von Lemma 3.23, so wird ω_0 unter der dort angegebenen Isomorphismenkette auf $\zeta_{q-1} + 2\mathcal{O}$ abgebildet. Quadrate von Elementen aus $\mathbb{F}_q$ kann man also als Elemente von $\Phi = \mathcal{O}/4\mathcal{O}$

auffassen vermöge der wohldefinierten Abbildung $x + 2\mathcal{O} \mapsto x^2 + 4\mathcal{O}$. Durch $\phi[\omega_0] := (\zeta_{q-1}^2 + 4\mathcal{O})\phi$ für $\phi \in \mathcal{O}/4\mathcal{O}$ wird $\mathcal{O}/4\mathcal{O}$ zu einem $\mathbb{F}_q$-qModul.

Die zugehörige Darstellung ist gegeben durch

$$\rho(q_{II}^E) = (\mathbb{F}_q, \rho_M, \rho_\Phi, \beta),$$

wobei ρ_M wie beim Typ qE definiert ist durch

$$\rho_M(m)(x, y) = \frac{1}{2} \operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(mxy)$$

für $m, x, y \in \mathbb{F}_q$.

Nun ist $\mathcal{O}/4\mathcal{O}$ eine freier $\mathbb{Z}/4\mathbb{Z}$-Modul (siehe Bemerkung 4.9) und offensichtlich auch $\mathbb{Z}/4\mathbb{Z}$-Algebra, weshalb die Linksmultiplikation mit x ist für jedes $x \in \mathcal{O}/4\mathcal{O}$ einen $Z/4Z$-Modulhomomorphismus von $\mathcal{O}/4\mathcal{O}$ darstellt. Dessen Spur wird im Folgenden mit $\operatorname{Tr}_{\mathcal{O}/4\mathcal{O}\big|\mathbb{Z}/4\mathbb{Z}}(x)$ bezeichnet. Nun können wir die quadratischen Abbildungen definieren durch

$$\rho_\Phi(a)(x) = \frac{1}{4} \operatorname{Tr}_{\mathcal{O}/4\mathcal{O}\big|\mathbb{Z}/4\mathbb{Z}}(ax^2)$$

für $a \in \mathcal{O}/4\mathcal{O}$ und $x \in \mathbb{F}_q$.

Die Abbildungen $\{\,\}$ und λ sind gegeben durch

$$\{\,\} : \mathbb{F}_q \to \mathcal{O}/4\mathcal{O},\ m \mapsto 2m^2, \quad \lambda : \mathcal{O}/4\mathcal{O} \to \mathbb{F}_q,\ \phi \mapsto \phi + 2\mathcal{O}/4\mathcal{O}.$$

Da λ surjektiv ist, impliziert die Isotropie eines Codes in $N\rho(q_{II}^E)$ gemäß Bemerkung 3.17 seine Selbstorthogonalität.

Um zu zeigen, dass es sich hier tatsächlich um die selbstdualen verallgemeinert doppelt geraden Codes handelt, betrachten wir zunächst einmal genauer die quadratischen Formen dieses Typs, welche, wie wir eben gesehen haben, die maßgeblichen Eigenschaften solcher Codes modellieren. Lemma 3.25 stellt zwischen den quadratischen Formen des Typs $\rho(q_I^E)$ einerseits und $\rho(q_{II}^E)$ andererseits einen hilfreichen Zusammenhang her.

Lemma 3.25. *Für die quadratischen Abbildungen $\rho_{\Phi(q_I^E)}(1)$ bzw. $\rho_{\Phi(q_{II}^E)}(1)$ der Darstellungen $\rho(q_I^E)$ bzw. $\rho(q_{II}^E)$ gilt*

$$2\rho_{\Phi(q_{II}^E)}(1) = \rho_{\Phi(q_I^E)}(1).$$

Beweis. Als $\mathbb{Z}/4\mathbb{Z}$-Modul ist $\mathcal{O}/4\mathcal{O}$ frei auf den Erzeugern $(1 + 4\mathcal{O}, \zeta_{q-1} + 4\mathcal{O}, \ldots, \zeta_{q-1}^{f-1} + 4\mathcal{O})$ - siehe dazu auch Bemerkung 4.9. Gemäß Lemma 3.23 ist

$$\mathcal{O}/4\mathcal{O}/2\mathcal{O}/4\mathcal{O} \cong \mathcal{O}/2\mathcal{O} \cong \mathbb{F}_q.$$

Daher ergibt sich, dass

$$\operatorname{Tr}_{\mathcal{O}/4\mathcal{O}\big|\mathbb{Z}/4\mathbb{Z}}(v^2) \mod 2 = \operatorname{Tr}_{\mathbb{F}_q\big|\mathbb{F}_2}(v^2) \in \mathbb{Z}/2\mathbb{Z}$$

für alle $v \in \mathbb{F}_q$. Daraus folgt aber

$$\frac{1}{2} \operatorname{Tr}_{\mathcal{O}/4\mathcal{O}\big|\mathbb{Z}/4\mathbb{Z}}(v^2) = \frac{1}{2} \operatorname{Tr}_{\mathbb{F}_q\big|\mathbb{F}_2}(v^2) \in \mathbb{Q}/\mathbb{Z},$$

woraus die Behauptung folgt. □

Daraus folgt nun

Satz 3.26. *Die Codes vom Typ $\rho(q_{II}^E)$ sind genau die selbstdualen verallgemeinert doppelt geraden Codes.*

Beweis. Wegen Bemerkung 3.20 genügt es, sich im Beweis auf den Nachweis der Eigenschaften (i) und (ii) aus Beispiel 3.3.3 bzw. der Isotropie von C zu beschränken.

Sei $C \leq V^N$ ein Code vom Typ $\rho(q_{II}^E)$. Da $\mathbb{F}_q^2 = \mathbb{F}_q$ ist und Quadrate von Elementen von $\mathbb{F}_q$ als Elemente von $\mathcal{O}/4\mathcal{O}$ aufgefasst werden können, können wir die Gleichung

$$(\sum_{i=1}^{N} c_i)^2 = \sum_{i=1}^{N} c_i^2 + 2\sum_{i<j} c_i c_j \tag{1}$$

über $\mathcal{O}/4\mathcal{O}$ betrachten. Aus der Isotropie von C ergibt sich, dass

$$\rho^N_{\Phi(q_{II}^E)}(a^2)(c) = \frac{1}{4}\operatorname{Tr}_{\mathcal{O}/4\mathcal{O}\big|\mathbb{Z}/4\mathbb{Z}}(a^2\sum_{i=1}^{N} c_i^2) = 0$$

für alle $c \in C$ und $a \in \mathbb{F}_q$. Mit Lemma 3.25 erhalten wir daraus, dass

$$0 = \rho_{\Phi(q_{II}^E)}(1)(a^2\sum_{i=1}^{N} c_i^2) = \frac{1}{2}\rho_{\Phi(q_I^E)}(1)(a^2\sum_{i=1}^{N} c_i^2) = \frac{1}{2}\beta(a^2, \sum_{i=1}^{N} c_i^2)$$

für alle $c \in C$ und $a \in \mathbb{F}_q$. Da β nichtsingulär ist und $char(\mathbb{F}_q) = 2$, folgt

$$\sum_{i=1}^{N} c_i^2 = 0 = (\sum_{i=1}^{N} c_i)^2 \in \mathbb{F}_q,$$

also auch $\sum_{i=1}^{N} c_i = 0 \in \mathbb{F}_q$, womit wir die Eigenschaft (i) aus Beispiel 3.3.3 nachgewiesen haben. Die Gleichung (1) ergibt dann

$$2\sum_{i<j} c_i c_j = 0 \in \mathcal{O}/4\mathcal{O}.$$

Da $\mathcal{O}$ ein Integritätsbereich ist, folgt, dass

$$\sum_{i<j} c_i c_j = 0 \in \mathcal{O}/2\mathcal{O} \cong \mathbb{F}_q.$$

Dies entspricht Eigenschaft (ii) aus Beispiel 3.3.3.

Ist umgekehrt $C \leq \mathbb{F}_q^N$ ein verallgemeinert doppelt gerader Code, so lautet wegen der Eigenschaften (i) und (ii) von C die Gleichung 1

$$\sum_{i=1}^{N} c_i^2 = 0 \ \in \mathcal{O}/4\mathcal{O}.$$

Daraus ergibt sich

$$\rho_\Phi^N(\phi)(c) = \sum_{i=1}^{N} \rho_\Phi(\phi)(c_i) = \sum_{i=1}^{N} \frac{1}{4}\operatorname{Tr}(\phi c_i^2) = \frac{1}{4}\operatorname{Tr}(\sum_{i=1}^{N} \phi c_i^2) = 0$$

für alle $\phi \in \mathcal{O}/4\mathcal{O}$. Als isotroper Code ist C in $N\rho(q_{II}^E)$ auch selbstorthogonal und damit wegen Bemerkung 3.20 sogar selbstdual, also vom Typ $\rho(q_{II}^E)$. □

4 Invarianzeigenschaften und die Clifford-Weil-Gruppe

Gewichtszähler von Codes eines Typs ρ sind invariant unter gewissen linearen Transformationen, die sich aus den Eigenschaften dieser Codes ergeben. Maßgeblich sind hier die Eigenschaft R-Modul zu sein sowie die Isotropie und die Selbstdualität von C.

Diese Eigenschaften entsprechen je einer Klasse von Automorphismen von $\mathbb{C}V$ und somit je einer Klasse von Erzeugern der zugehörigen komplexen Matrixgruppe, der Clifford-Weil-Gruppe. Die den ersten beiden Eigenschaften entsprechenden Transformationen sind relativ offensichtlich. Um die der Selbstdualität von C entsprechende Transformation zu finden, benutzen wir eine partielle MacWilliams-Identität (Satz 4.4), zu deren Beweis Hilfsmittel aus der Darstellungstheorie benötigt werden.

4.1 Invarianzeigenschaften von Gewichtszählern

Definition 4.1. *Ist G eine endliche abelsche Gruppe, so heißt*

$$\widehat{G} = \{\chi : G \to \mathbb{C}^* | \chi(a+b) = \chi(a)\chi(b) \text{ für alle } a, b \in G\}$$

die Charaktergruppe von G.

Definition 4.2. *Es bezeichne $\mathbb{C}^G = \{f : G \to \mathbb{C}\}$ den $\mathbb{C}$-Vektorraum der komplexwertigen Funktionen auf G. Dann erhalten wir ein Hermitesches positiv definites Skalarprodukt $< >_G$ auf $\mathbb{C}^G \times \mathbb{C}^G$ durch*

$$< f, h >_G := \frac{1}{|G|} \sum_{g \in G} f(g)\overline{h(g)}.$$

Den folgenden Satz werden wir öfter verwenden, um die Invarianz von $\mathrm{fwe}(C)$ unter bestimmten linearen Transformationen herzuleiten. Er beinhaltet in vereinfachter Form die wohlbekannten Orthogonalitätsrelationen.

Satz 4.3. *Es ist*

a) $|\widehat{G}| = |G|$ *und*

b) $\widehat{G}$ *bildet eine Orthonormalbasis des $\mathbb{C}$-Vektorraums $\mathbb{C}^G = \{f : G \to \mathbb{C}\}$ bezüglich des Skalarprodukts $< , >_G$.*

Beweis. Im Folgenden seien $n := |G|$ und $\widehat{G} = \{\widehat{g_1}, \ldots, \widehat{g_k}\}$.

zu a): Betrachtet man die Darstellung

$$G = < g_1 > \times < g_2 > \times \ldots \times < g_m >,\ g_1, \ldots g_m \in G$$

von G als direktes Produkt zyklischer Untergruppen, so ist $\widehat{g} \in \widehat{G}$ eindeutig bestimmt durch $(\widehat{g}(g_1), \ldots, \widehat{g}(g_m))$. Ist $d_i := | < g_i > |, i = 1, \ldots, m$, so sind als Wahlen der $\widehat{g}(g_i)$ genau die d_i-ten Einheitswurzeln möglich, falls $i \in \{1, \ldots, m\}$. Also ist $|\widehat{G}| = d_1 \ldots d_m = |G|$.

zu b): Es genügt zu zeigen, dass $\widehat{G}$ ein Orthonormalsystem bezüglich $<>_G$ ist, da zum einen $dim_{\mathbb{C}}(\mathbb{C}^G) = |G|$ ist und sich zum anderen für jede lineare Abhängigkeit $(\lambda_1, \ldots, \lambda_n) \in \mathbb{C}^n$ von $\widehat{G}$ aus der Orthonormalitätseigenschaft

$$\begin{aligned} 0 &= < \lambda_1\widehat{g_1} + \ldots + \lambda_n\widehat{g_n}, \lambda_1\widehat{g_1} + \ldots + \lambda_n\widehat{g_n} > \\ &= |\lambda_1|^2 + \ldots + |\lambda_n|^2 \end{aligned}$$

ergibt. Bezeichnet $\mathbf{1} : G \to \mathbb{C},\ g \mapsto 1$ für alle $g \in G$ den trivialen Charakter von G, so genügt es wegen

$$\widehat{g}\overline{\widehat{h}} = \mathbf{1} \Leftrightarrow \widehat{g} = \widehat{h},\ \widehat{g}, \widehat{h} \in \widehat{G}$$

zu zeigen, dass

$$< \widehat{g}, 1 >_G = \begin{cases} 1, & \widehat{g} = \mathbf{1} \\ 0 & \text{sonst} \end{cases} \quad \text{für alle } \widehat{g} \in \widehat{G}.$$

Sei dazu $\widehat{g} \in \widehat{G}, \widehat{g} \neq \mathbf{1}$; dann existiert ein $j \in \{1, \ldots, m\}$ mit $\widehat{g}(g_j) \neq 1$. Definiert man

$$G_j :=< g_1 > \times \ldots < g_{j-1} > \times < g_{j+1} > \times \ldots \times < g_m > \leq G,$$

so ist

$$G/G_j \cong < g_j > \text{ und } G = \bigcup_{i=0}^{d_j - 1} g_j^i + G_j.$$

Daraus ergibt sich

$$< \widehat{g}, 1 >_G = \frac{1}{|G|} \underbrace{\sum_{i=0}^{d_j-1} \widehat{g}(g_j)^i}_{=0} \sum_{g \in G_j} \widehat{g}(g) = 0.$$

□

Satz 4.4 (Partielle MacWilliams-Identität). *Es seien $\mathcal{R} = (R, M, \psi, \Phi)$ ein Form-Ring, $\rho = (V, \rho_M, \rho_\Phi, \beta)$ eine endliche Darstellung von $\mathcal{R}$ und $C \leq V$ ein R-Teilmodul. Seien weiter e ein symmetrisches Idempotent bezüglich der durch τ auf M induzierten Involution ^{J} auf R und u_e, v_e wie in 3.10. Dann gilt*

$$\mathrm{fwe}(C^\perp) = \frac{1}{|eC|} \sum_{v \in (1-e)C^\perp} \sum_{w \in eV} \sum_{c \in eC} \exp(2\pi i \beta(w, v_e c)) b_{w+(1-e)v}.$$

Beweis. Wir zerlegen $C^\perp$ mit Hilfe der orthogonalen Idempotente e und $1 - e$ in

$$C^\perp = (1-e)C^\perp \oplus eC^\perp = (1-e)C^\perp \oplus (eC)^{\perp, \beta_e}$$

und erhalten

$$\mathrm{fwe}(C^\perp) = \sum_{v \in (1-e)C^\perp} \sum_{w \in (eC)^{\perp, \beta_e}} b_w b_v.$$

Den zweiten Summanden wollen wir mit Hilfe der Orthogonalität der Charaktere umschreiben; betrachten wir dazu den Charakter

$$\chi_w :\ eC \to \mathbb{C}^*,\ c \mapsto \exp(2\pi i \beta_e(w, c)).$$

Es gilt $\chi_w = \mathbf{1}$ genau dann, wenn $w \in (eC)^{\perp, \beta_e}$, und damit gilt

$$\sum_{c \in eC} \exp(2\pi i \beta(w, v_e c)) = \sum_{c \in eC} \exp(2\pi i \beta_e(w, c)) = |eC| < \chi_w, \mathbf{1} >= \begin{cases} |eC|, & w \in (eC)^{\perp, \beta_e} \\ 0, & \text{sonst} \end{cases}$$

Daraus ergibt sich

$$\sum_{w \in (eC)^{\perp, \beta_e}} b_w = \frac{1}{|eC|} \sum_{w \in eV} \sum_{c \in eC} \exp(2\pi i \beta(w, v_e c)) b_w,$$

womit die Behauptung bewiesen ist. □

Folgerung 4.5. *In der Situation von Satz 4.4 betrachten wir den Fall, dass C selbstdual ist. Dazu beobachten wir zunächst für $c \in eC$ und $v \in (1-e)C$, dass $(1-e)(c+v) = (1-e)v$ sowie $v_e(c+v) = v_e c$, wegen $v_e \in e^J Re$.*

Satz 4.4 besagt dann, dass

$$\mathrm{fwe}(C) = \frac{1}{|eC|} \sum_{c \in C} \sum_{w \in eV} \exp(2\pi i \beta(w, v_e c)) b_{w+(1-e)c}.$$

Das heißt, bezeichnet H den $\mathbb{C}$-Vektorraumautomorphismus von $\mathbb{C}V$, welcher definiert ist durch

$$b_v \mapsto \sum_{w \in e} \exp(2\pi i \beta(w, v_e v)) b_{w+(1-e)v},$$

so ist $H(\mathrm{fwe}(C)) = \mathrm{fwe}(C)$.

4.2 Die Clifford-Weil-Gruppe einer Darstellung

Definition 4.6 (Clifford-Weil-Gruppe). *Seien $\mathcal{R} = (R, M, \psi, \Phi)$ ein Form-Ring und $\rho = (V, \rho_M, \rho_\Phi, \beta)$ eine endliche Darstellung von $\mathcal{R}$. Die zugehörige Clifford-Weil-Gruppe $\mathcal{C}(\rho) \leq \mathrm{GL}_{|V|}(\mathbb{C})$ ist definiert durch*

$$\mathcal{C}(\rho) = < m_r, d_\phi, h_{e,u_e,v_e} | r \in R^*, \phi \in \Phi, e \in R \text{ symm. Idempotent}, e = u_e v_e, e^J = v_e u_e >,$$

wobei $m_r, d_\phi, h_{e,u_e,v_e} \in Aut(\mathbb{C}V)$ definiert sind durch

$$m_r(b_v) = b_{rv}, \qquad d_\phi(b_v) = \exp(2\pi i \rho_\Phi(\phi)(v)) b_v$$

sowie

$$h_{e,u_e,v_e}(b_v) = \frac{1}{|eV|^{1/2}} \sum_{w \in eV} \exp(2\pi i \beta(w, v_e v)) b_{w+(1-e)v}.$$

Satz 4.7. *Ist C ein selbstdualer isotroper Code vom Typ ρ, so gilt $g(\mathrm{fwe}(C)) = \mathrm{fwe}(C)$ für alle $g \in \mathcal{C}(\rho)$.*

Beweis. Es genügt, dies für die Erzeuger von $\mathcal{C}(\rho)$ zu zeigen. Für $r \in R^*$ operiert m_r auf $\mathbb{C}V$ durch Permutation der Basisvektoren. Da $C \leq V$ ein R-Untermodul von V ist, ist $\mathrm{fwe}(C)$ invariant unter m_r.

Die $d_\phi,\ \phi \in \Phi$, operieren diagonal auf $\mathbb{C}V$ und lassen genau die isotropen Vektoren $v \in V$ invariant.

Die Invarianz von $\mathrm{fwe}(C)$ unter h_{e,u_e,v_e} schließlich ergibt sich aus Folgerung 4.5 □

Für den vollständigen Gewichtszähler erhalten wir

Folgerung 4.8. *Ist C ein selbstdualer isotroper Code in $N\rho$, so ist $\mathrm{cwe}(C) \in \mathrm{Inv}_{\mathbb{C}[x_v \mid v \in V]}(\mathcal{C}(\rho))$.*

Beweis. Wir zeigen die Invarianz von $\mathrm{cwe}(C)$ unter den Erzeugern von $\mathcal{C}(\rho)$ mit Hilfe von Lemma 1.11. Im Fall der m_r können wir das Lemma mit

$$f_a(v) = \begin{cases} 1, & v = ra \\ 0, & \text{sonst} \end{cases} \qquad \text{für } a, v \in V$$

verwenden, da $r(v_1, \ldots, v_N) = (rv_1, \ldots, rv_N)$ für $r \in R$ und $v = (v_1, \ldots, v_N) \in V^N$. Für die d_ϕ liefert das Lemma mit

$$f_a(v) = \begin{cases} \exp(2\pi i \rho_\Phi(\phi)(v)), & v = a \\ 0, & \text{sonst} \end{cases} \qquad \text{für } a, v \in V$$

die gewünschte Aussage, da $\rho_\Phi^N(\phi)(v) = \sum_{i=1}^N \rho_\Phi(\phi)(v_i)$ für alle $v = (v_1, \ldots, v_N) \in V^N$ sowie $\phi \in \Phi$. Bei den h_{e,u_e,v_e} schließlich betrachten wir die Funktionen

$$f_a(v) = |eV|^{-\frac{1}{2}} \exp(2\pi i \beta(v, v_e a)) \quad \text{für } a, v \in V;$$

der Vorfaktor $|eV|^{-\frac{1}{2}}$ ergibt sich hierbei aus $|eV^N| = |(eV)^N| = |eV|^N$, da $\mathrm{cwe}(C)$ homogen vom Grad N ist. □

4.3 Beispiele für Clifford-Weil-Gruppen: Typ $\rho(4_I^E)$ und Typ $\rho(4_{II}^E)$

Nun wollen wir zu den in Kapitel 3.3 eingeführten Darstellungen $\rho(q_I^E)$ und $\rho(q_{II}^E)$ für $q = 4$ explizit Erzeuger der zugehörigen Clifford-Weil-Gruppen bestimmen. In beiden Fällen lässt sich die Clifford-Weil-Gruppe von drei Elementen erzeugen. Dies liegt unter anderem an der einfachen Erzeugtheit der jeweiligen q-Moduln, die hier für $\rho(q_{II}^E)$ nachgewiesen wird:

Bemerkung 4.9. *[Die Struktur von $\mathcal{O}/4\mathcal{O}$]*

Es ist $\mathcal{O}/4\mathcal{O} =< 1 >$ als $\mathbb{F}_q$-qModul. Denn bezeichnet $\mu(x) \in \mathbb{Z}_2[x]$ das Minimalpolynom von ζ_{q-1} und $\overline{\mu}(x)$ dessen Reduktion modulo 4, so gilt

$$\mathbb{Z}_2[\zeta_{q-1}]/4\mathbb{Z}_2[\zeta_{q-1}] \cong \mathbb{Z}/4\mathbb{Z}[x]/(\overline{\mu}(x))$$

via

$$\sum_{i=0}^{d-1} a_i \zeta_{q-1}^i + 4\mathbb{Z}_2[\zeta_{q-1}] \mapsto \sum_{i=0}^{d-1} (a_i^1 + 2a_i^2) x^i + (\overline{\mu}(x)),$$

wobei $a_i = \sum_{j=1}^{\infty}) a_i^{(j)} 2^{j-1} \in \mathbb{Z}_2$, $a_i^{(j)} \in \{0, 1\}$ für $i = 1, \ldots, n$. Daher erhalten wir aus der Tatsache, dass

$$\mathbb{Z}/4\mathbb{Z}[x]/(\overline{\mu}(x)) =< 1 + (\overline{\mu}(x)), x + (\overline{\mu}(x)), \ldots, x^{f-1} + (\overline{\mu}(x)) >$$

als $\mathbb{Z}$-Modul, dass

$$\mathcal{O}/4\mathcal{O} =< 1 + 4\mathcal{O}, \zeta_{q-1} + 4\mathcal{O}, \ldots, \zeta_{q-1}^{f-1} + 4\mathcal{O} >$$

als abelsche Gruppe. Ist nun ω_0 der im Beweis von Lemma 3.23 definierte Erzeuger von $\mathbb{F}_q^*$, so gilt gemäß Beispiel 3.3.3, dass

$$\phi[\omega_0] = (\zeta_{q-1}^2 + 4\mathcal{O})\phi \text{ für } \phi \in \mathcal{O}/4\mathcal{O}.$$

Daraus ergibt sich, dass

$$\{1 + 4\mathcal{O}, \zeta_{q-1} + 4\mathcal{O}, \ldots, \zeta^{f-1} + 4\mathcal{O}\} \subseteq < 1 >_{\mathbb{F}_q - qModul},$$

womit die Behauptung bewiesen ist.

Die einfache Erzeugtheit der q-Moduln wird nun auf die Elemente der Clifford-Weil-Gruppe übertragen.

Bemerkung 4.10. *Mit den Bezeichnungen von 4.6 gilt*

$$d_{\phi_1+\phi_2} = d_{\phi_1} d_{\phi_2} \text{ und } d_{\phi[r]} = m_{r^{-1}} d_\phi m_r$$

für alle $r \in R$ sowie $\phi_1, \phi_2 \in \Phi$.

Beispiel 4.11. *Wir bestimmen Erzeuger der Clifford-Weil-Gruppe für die Darstellung $\rho(q_I^E)$ des Form-Rings $\mathcal{R}(q_I^E)$. Wegen Bemerkung 4.10 wird $\mathcal{C}(\rho(q_I^E))$ erzeugt von m_w, d_1 und $h_{1,1,1}$, wobei $w \in \mathbb{F}_q$ eine primitive $(q-1)$te Einheitswurzel bezeichne. Im Fall $q = 4$ sind diese Matrizen explizit*

$$m_w = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, d_\phi = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

sowie

$$h_{1,1,1} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix}.$$

Als Isomorphietyp von $\mathcal{C}(\rho(4_I^E))$ erhalten wir die Gruppe

$$\mathcal{C}(\rho(4_I^E)) \cong (D_8 Y D_8).S_3$$

der Ordnung $2^6 \cdot 3$.

Die Molien-Reihe von $\mathcal{C}(\rho(4_I^E))$ (siehe Kapitel 2) ist gegeben durch

$$\frac{1+t^{16}}{(1-t^2)(1-t^4)(1-t^6)(1-t^8)}.$$

Beispiel 4.12. *Auch hier gibt es gemäß Bemerkung 4.10 drei Erzeuger. Wir verwenden Lemma 3.25, um diese im Fall $q = 4$ explizit zu berechnen. Sind m_ω und $h_{1,1,1}$ wie in Beispiel 4.11, so ist*

$$\mathcal{C}(\rho(q_{II}^E)) =< m_\omega, h_{1,1,1}, d_\phi >,$$

wobei

$$d_\phi = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & i \end{pmatrix}.$$

Es gilt

$$\mathcal{C}(\rho(4_{II}^E)) \cong (Z_4 \mathbf{Y} D_8 \mathbf{Y} D_8).A_5,$$

wie man mit [2] nachrechnet. Es gilt $|\mathcal{C}(\rho)| = 2^8 \cdot 3 \cdot 5$. Die Molienreihe dieser Gruppe ist

$$\frac{1+t^{40}}{(1-t^4)(1-t^8)(1-t^{12})(1-t^{20})}.$$

4.4 Höhere Clifford-Weil-Gruppen

Bisher haben wir von der Clifford-Weil-Gruppe $\mathcal{C}(\rho)$ einer Darstellung ρ gesprochen; tatsächlich können wir für jede natürliche Zahl $n \in \mathbb{N}$ eine *Geschlecht-n-Clifford-Weil-Gruppe* $\mathcal{C}_n(\rho)$ zu ρ definieren. Die bisher behandelte Gruppe $\mathcal{C}(\rho)$ ordnet sich hier mit $n = 1$ ein. Auch im Folgenden schreiben wir stets $\mathcal{C}(\rho)$ für $\mathcal{C}_1(\rho)$.

Um $\mathcal{C}_n(\rho)$ definieren zu können, variieren wir zunächst den zugrunde liegenden Form-Ring.

Definition und Bemerkung 4.13. *Seien $\mathcal{R} = (R, M, \psi, \Phi)$ ein Form-Ring und $n \in \mathbb{N}$. Dann ist das Quadrupel $\mathrm{Mat}_n(R, M, \psi, \Phi) := (R^{n\times n}, M^{n\times n}, \psi^{n\times n}, \Phi^{(n)})$ mit den Abbildungen $\lambda^{(n)}$, $\{\!\{\ \}\!\}^{(n)}$ sowie $\tau^{(n)}$ wieder ein Form-Ring, wobei*

$$\Phi^{(n)} = \left\{ \begin{pmatrix} \phi_1 & m_{12} & \dots & m_{1n} \\ & & & \vdots \\ & & \ddots & m_{n-1,n} \\ & & & \phi_n \end{pmatrix} | \phi_i \in \Phi, m_{ij} \in M, i, j = 1, \dots, n \right\}.$$

Die Involution $\tau^{(n)} : M^{n\times n} \to M^{n\times n}$ ist hierbei definiert durch

$$\tau^{(n)}((m_{ij})_{i,j=1\dots n}) = (\tau(m_{ji}))_{j,i=1\dots n},$$

und die Strukturabbildungen $\lambda^{(n)} : \Phi^{(n)} \to M^{n\times n}$ bzw. $\{\!\{\ \}\!\}^{(n)} : M^{n\times n} \to \Phi^{(n)}$ sind gegeben durch

$$\lambda^{(n)}(\phi) = \begin{pmatrix} \lambda(\phi_1) & m_{12} & \dots & m_{1n} \\ \tau(m_{12}) & & & \vdots \\ \vdots & & \ddots & m_{n-1,n} \\ \tau(m_{1n}) & \dots & \tau(m_{n-1,n}) & \lambda(\phi_n) \end{pmatrix}$$

bzw.

$$\{\!\{(m_{ij})_{i,j=1\dots n}\}\!\}^{(n)} \begin{pmatrix} \{\!\{m_{11}\}\!\} & m_{12} + \tau(m_{21}) & \dots & m_{1n} + \tau(m_{n1}) \\ & & \ddots & \vdots \\ & \ddots & & m_{n-1,n} + \tau(m_{n,n-1}) \\ & & & \{\!\{m_{nn}\}\!\} \end{pmatrix}.$$

Auf $M^{n\times n}$ erhalten wir eine $R^{n\times n} \otimes R^{n\times n}$-Modulstruktur, indem wir $X(A \otimes B)$ für $A, B \in R^{n\times n}$ und $X \in M^{n\times n}$ als Interpretation des formalen Matrixprodukts $A^{J^{(n)}} X B$ auslegen - man interpretiert das Produkt $a^J x b$ als $x(a \otimes b)$ für $x \in M$ und $a, b \in R$. Motiviert wird das durch Bemerkung 3.5.

Konkret heißt das

$$(X(A \otimes B))_{ij} = \sum_{l,k=1}^{n} X_{kl}(A_{ki} \otimes B_{lj}).$$

Auf $\Phi^{(n)}$ liefert ebenfalls die Imitation von Matrixmultiplikation eine $R^{n\times n}$-qModul-Struktur. Man erhält

$$\phi[A]_{ij} = \begin{cases} \sum_{k=1}^{n} \phi_{kk}[A_{ki}] + \sum_{1\le k<l\le n} \{\!\{\phi_{kl}(A_{ki} \otimes A_{li})\}\!\}, & i = j \\ \sum_{k=1}^{n} \lambda(\phi_{kk})(A_{ki} \otimes A_{kj}) + \sum_{1\le k<l\le n} \phi_{kl}(A_{li} \otimes A_{kj}) + \tau(\phi_{lk})(A_{ki} \otimes A_{lj}), & i < j \end{cases}$$

Im Fall $n = 2$, mit dem wir uns in Abschnitt 6.1 noch beschäftigen werden, lautet diese Vorschrift explizit

$$\begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix} \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right] = \begin{pmatrix} \phi_1' & m' \\ & \phi_2' \end{pmatrix},$$

wobei

$$\begin{aligned}\phi_1' &= \phi_1[a] + \phi_2[c] + \{\!\{ m(a \otimes c) \}\!\}, \\ \phi_2' &= \phi_1[b] + \phi_2[d] + \{\!\{ m(b \otimes d) \}\!\}\end{aligned}$$

und

$$m' = \lambda(\phi_1)(a \otimes b) + m(a \otimes d) + \lambda(\phi_2)(c \otimes d) + \tau(m)(c \otimes b).$$

Die Antiautomorphismen auf $K^{n\times n}$ für den endlichen Körper K lassen sich relativ leicht beschreiben.

Satz 4.14. *Es seien K ein endlicher Körper und ^{J} ein Antiautomorphismus von $K^{n\times n}$. Für $X \in K^{n\times n}$ sei X^t die Transponierte von X. Dann gibt es einen Isomorphismus $\overline{\ }: K \to K$ sowie $A \in \mathrm{GL}_n(K)$ mit*

$$X^J = A\overline{X}^t A^{-1}$$

für alle $X \in K^{n\times n}$.

Beweis. Ist $A \in K^{n\times n}$ zentral, so ist auch $A^J \in Z(K^{n\times n})$, denn für $X \in K^{n\times n}$ gilt

$$A^J X = (X^{-J} A)^J = (AX^{-J})^J = XA^J.$$

Wegen $Z(K^{n\times n}) = \{\alpha I_n \mid \alpha \in K\}$ können wir dann einen Isomorphismus $\overline{\ }: K \to K$ definieren durch $\overline{\alpha} I_n := (\alpha I_n)^J$ für $\alpha \in K$.

Dann ist ${}^{\tilde{J}}: \ K^{n\times n} \to K^{n\times n}, X \mapsto \overline{X}^t$ ein Antiautomorphismus auf $K^{n\times n}$. Daraus folgt, dass

$$\phi := {}^J \circ {}^{\tilde{J}} \in \mathrm{Aut}_K(K^{n\times n}).$$

Nach dem Satz von Skolem-Noether (siehe [9], Cor. 7.23(i)) existiert ein $A \in \mathrm{GL}_n(K)$ mit $\phi(X) = AXA^{-1}$ für alle $X \in K^{n\times n}$ - damit haben $\overline{\ }$ und A die gewünschten Eigenschaften. □

Nun wollen wir uns mit den Darstellungen des Form-Rings $\mathrm{Mat}_n(\mathcal{R})$ beschäftigen, falls $R = K$ ein endlicher Körper ist. Die folgenden Resultate sind in [5] in Abschnitt 4.5 bereits allgemeiner mit Hilfe der Morita-Theorie für Form-Ringe bewiesen worden.

Satz 4.15. *Seien $\mathcal{R} = (K, M, \psi, \Phi)$ ein Form-Ring über dem Körper K und $n \in \mathbb{N}$. Dann ist jede endliche Darstellung ρ von $\mathrm{Mat}_n(\mathcal{R})$ von der Form*

$$\rho = K^{n\times 1} \otimes_K \rho_0$$

für eine endliche Darstellung $\rho_0 = (V_0, \rho_M, \rho_\Phi, \beta)$ von $\mathcal{R}$.

Das heißt, es gilt

$$\rho = (V_0^n, \rho_{M^{n\times n}}, \rho_{\Phi^{(n)}}, \beta^{(n)}),$$

wobei die Abbildungen $\rho_{M^{n\times n}}, \rho_{\Phi^{(n)}}$ und $\beta^{(n)}$ definiert sind durch

$$\rho_{M^{n\times n}}((m_{ij}))(x, y) = \sum_{i,j=1}^{n} \rho_M(m_{ij})(x_i, y_j),$$

$$\rho_{\Phi^{(n)}}\left(\begin{pmatrix} \phi_1 & & m_{ij} \\ & \ddots & \\ & & \phi_n \end{pmatrix}\right)(x) = \sum_{i=1}^{n} \phi_i(x_i) + \sum_{i<j} m_{ij}(x_i, x_j)$$

sowie

$$\beta^{(n)}(x,y) = \sum_{i=1}^{n} \beta(x_i, y_i)$$

für alle $x = (x_1, \ldots, x_n)$ *und* $y = (y_1, \ldots, y_n) \in V_0^N$ *sowie* $(m_{ij}) \in M^{n\times n}$.

Beweis. Es sei $\rho = (V, \rho_{M^{n\times n}}, \rho_{\Phi^{(n)}}, \beta^n)$ eine endliche Darstellung von $\mathrm{Mat}_n(\mathcal{R})$. Dann ist V isomorph zu $K^{n\times m}$ als $K^{n\times n}$-Linksmodul, was eine Zerlegung von V in n Kopien von $K^{1\times m}$ (als Teilräume) induziert. Setzen wir $V_0 := K^{1\times m}$, so ist also V_0^n ein $K^{n\times n}$-Modul durch übliche Matrixmultiplikation und als solcher isomorph zu V.

Um nachzuweisen, dass $\rho_{M^{n\times n}}$ und $\rho_{\Phi^{(n)}}$ von der gewünschten Form sind, werden wir Objekte von $\mathcal{R}$ in $\mathrm{Mat}_n(\mathcal{R})$ einbetten. Es sei etwa

$$(m(k,l))_{ij} := \begin{cases} m, & i = k, j = l \\ 0, & \text{sonst} \end{cases} \in M^{n\times n}$$

für $k, l \in \{1, \ldots, n\}$ sowie $m \in M$. Entsprechend seien $v(k)$ und $\phi(k,k)$ definiert für $k \in \{1, \ldots, n\}$ und $v \in V_0, \phi \in \Phi$. Elemente von M können auf diese Weise auch in $\Phi^{(n)}$ eingebettet werden; wir schreiben $m^\Phi(k,l)$ für $k, l \in \{1, \ldots, n\}, k < l$.

Es seien $e_1, \ldots, e_n$ wie in Beispiel 3.9. Dann gilt nach Bemerkung 3.5

$$\begin{aligned} (m(k,l))_{i,j=1}^n (e_k \otimes e_l) &= \psi(\psi^{-1}((m(k,l))_{i,j=1}^n))(e_k \otimes e_l) \\ &= \psi(e_k \psi^{-1}((m(k,l))_{i,j=1}^n) e_l) \\ &= (m(k,l))_{i,j=1}^n \end{aligned}$$

für $m \in M$ und somit

$$\begin{aligned} \rho_{M^{n\times n}}((m_{ij})_{i,j=1}^n)(x,y) &= \sum_{k,l=1}^{n} \rho_{M^{n\times n}}((m_{kl}(k,l)))(x,y) \\ &= \sum_{k,l=1}^{n} \rho_{M^{n\times n}}((m_{kl}(k,l))(e_k \otimes e_l))(x,y) \\ &= \sum_{k,l=1}^{n} \rho_{M^{n\times n}}((m_{kl}(k,l)))(e_k x, e_l y) \end{aligned}$$

für $x = (x_1, \ldots, x_n)$ und $y = (y_1, \ldots, y_n) \in V_0^n$.

so können wir einen $K \otimes K$-Rechtsmodulhomomorphismus $\rho_M : M \to \mathrm{Bil}(V_0, \mathbb{Q}/\mathbb{Z})$ definieren durch

$$\rho_M(m)(x,y) := \rho_{M^{n\times n}}((m(1,1)))(x(1), y(1)),$$

Wir zeigen, dass dann für $k, l \in \{1, \ldots, n\}$ gilt, dass

$$\rho_M(m)(x,y) = \rho_{M^{n\times n}}((m(k,l)))(e_k x(k), e_l y(l)).$$

Seien dazu $P_{1k}, P_{1l} \in K^{n\times n}$ die Permutationsmatrizen, welche durch Vertauschung der ersten mit der k-ten bzw. mit der l-ten Zeile aus der Einheitsmatrix des $K^{n\times n}$ hervorgehen.

Dann gilt

$$\begin{aligned} \rho_M(m)(x,y) &= \rho_{M^{n\times n}}(m(1,1))(x(1), y(1)) \\ &= \rho_{M^{n\times n}}(m(l,k)(P_{1l} \otimes P_{1k}))(x(1), y(1)) \\ &= \rho_{M^{n\times n}}(m(l,k))(P_{1l} x(1), P_{1k} y(1)) \\ &= \rho_{M^{n\times n}}(m(l,k))(x(l), y(k)) \end{aligned}$$

Somit ist $\rho_{M^{n\times n}}$ von der gewünschten Form.

Für $\rho_{\Phi^{(n)}}$ gehen wir ähnlich vor; es ist

$$\rho_{\Phi^{(n)}}(\begin{pmatrix} \phi_1 & & m_{ij} \\ & \ddots & \\ & & \phi_n \end{pmatrix}) = \sum_{i=1}^{n} \rho_{\Phi^{(n)}}(\phi_i(i)) + \sum_{i<j} \rho_{\Phi^{(n)}}(m_{ij}^{\Phi}(i,j)).$$

Wir beobachten, dass $\{\!\{m(i,j)\}\!\}^n = m^{\Phi}(i,j)$ für $m \in M$ und $i < j$. Daraus ergibt sich

$$\begin{aligned} \rho_{\Phi^{(n)}}(\{\!\{m(i,j)\}\!\}^n)(x) &= \{\!\{\rho_{M^{n\times n}}(m(i,j))\}\!\}(x) = \rho_{M^{n\times n}}(m(i,j))(x,x) \\ &= \rho_{M^{n\times n}}(m(i,j))(e_i x, e_j x) = \rho_{M^{n\times n}}(m(i,j))(x(i),x(j)) \end{aligned}$$

Für $\phi \in \Phi$ und $x \in V_0$ definieren wir

$$\rho_{\Phi}(\phi)(x) := \rho_{\Phi^{(n)}}(\phi(1,1))(x(1)).$$

Gemäß Definition 4.13 ist $\phi(i,i)[P_{1i}] = \phi(1,1)$, und damit gilt

$$\rho_{\Phi}(\phi)(x) = \rho_{\Phi^{(n)}}(\phi(i,i)[P_{1i}])(x(1)) = \rho_{\Phi^{(n)}}(\phi(i,i))(P_{1i}x(1)) = \rho_{\Phi^{(n)}}(\phi(i,i))(x(i)).$$

Damit ergibt sich aus (4.4), dass

$$\rho_{\Phi^{(n)}}(\begin{pmatrix} \phi_1 & & m_{ij} \\ & \ddots & \\ & & \phi_n \end{pmatrix}) = \sum_{i=1}^{n} \rho_{\Phi}(\phi_i) + \sum_{i<j} \rho_M(m_{ij}).$$

□

Wir erhalten Strukturaussagen über alle Form-Ringe über Matrix-Ringen endlicher Körper.

Satz 4.16. *Es sei $\mathcal{R} = (R, M, \psi, \Phi)$ ein Form-Ring, wobei $R = K^{n\times n}$ ein Matrix-Ring über dem endlichen Körper K sei. Dann existiert ein Form-Ring $\mathcal{R}_0 = (R_0, M_0, \psi_0, \Phi_0)$, so dass $R_0 \cong K$ und*

$$\mathcal{R} \cong \mathrm{Mat}_n(\mathcal{R}_0).$$

Beweis. Es sei $\mathcal{R} = (K^{n\times n}, M, \psi, \Phi)$ mit der Involution τ, dem Antiautomorphismus ^{J} sowie den Abbildungen $\{\!\{\ \}\!\}$ und λ eine Form-Struktur auf $K^{n\times n}$. Nach Satz 4.14 existieren ein $A \in \mathrm{GL}_n(K)$ und ein Antiautomorphismus $\ : K \to K$ mit $X^J = A\overline{X}^{tr}A^{-1}$ für alle $X \in K^{n\times n}$. Nach Reskalierung von $\mathcal{R}$ mit A (siehe Beispiel 3.3) können wir also annehmen, dass $^J = {}^t$; insbesondere könne wir annehmen, dass die primitiven Idmepotente $e_1 = \mathrm{diag}(1,0,\ldots,0), \ldots, e_n = \mathrm{diag}(0,\ldots,0,1)$ (siehe Beispiel 3.9) invariant sind unter ^{J}.

Nun definieren wir einen Form-Ring $\mathcal{R}_0 = (R_0, M_0, \psi_0, \Phi_0)$ durch

$$R_0 := eK^{n\times n}e,\ \psi_0 := \psi|_{R_0},\ M_0 := \psi_0(R_0) \text{ und } \Phi_0 := \Phi[e].$$

Insbesondere gehe der Antiautomorphismus $^J_{R_0}$ von R_0 durch Einschränkung von ^{J} auf R_0 hervor. Wir zeigen, dass $\mathcal{R} \cong \mathrm{Mat}_n(\mathcal{R}_0)$ ist. Seien dazu die Bezeichnungen wie in Definition 3.2.

Da $R_0 = eK^{n\times n}e \cong K$ ist, wählen wir f_R als den offensichtliche Isomorphismus von $K^{n\times n}$ nach $\mathrm{Mat}_n(R_0)$, das heißt,

$$f_R : K^{n\times n} \to R_0^{n\times n},\ X = \sum_{i,j=1}^{n} e_i X e_j \mapsto \sum_{i,j=1}^{n} (P_{1i}e_i X e_j P_{1j})(i,j).$$

Wegen Bedingung (vii) aus Definition 3.2 ist dann f_M eindeutig bestimmt als

$$f_M : M \to M_0^{n\times n},\ m \mapsto \psi_0^{n\times n}(f_R(\psi^{-1}(m))).$$

Ist $e_i = \mathrm{diag}(0,\ldots,0,1,0,\ldots,0)$ wie in Beispiel 3.9 für $i = 1,\ldots,n$, so gilt für $\phi \in \Phi$ nach Definition 3.1 (vi) wegen $e_1 + \ldots + e_n = 1$

$$\phi = \sum_{i=1}^{n} \phi[e_i] + \sum_{i<j} \{\!\{ \lambda(\phi)(e_i \otimes e_j) \}\!\}.$$

Dies bestimmt f_Φ teilweise, da

$$f_\Phi(\{\!\{ \lambda(\phi)(e_i \otimes e_j) \}\!\}) = \{\!\{ f_M(\lambda(\phi)(e_i \otimes e_j)) \}\!\}$$

für $i,j \in \{1,\ldots,n\}$ mit $i < j$. Mit den Bezeichnungen aus Bemerkung 4.15 definieren wir

$$f_\Phi(\phi[e_i]) := \phi[e_i][P_{1i}][e_1](i,i) \in \Phi_0^{(n)}.$$

Nun wollen wir noch nachprüfen, dass das Tripel (f_R, f_M, f_Φ) den Bedingungen aus Definition 3.2 genügt. Dazu beobachten wir zunächst, dass

$$\begin{aligned} f_R(r^J) &= \sum_{i,j=1}^{n} (P_{1i}e_i r^J e_j P_{1j})(i,j) = \sum_{i,j=1}^{n} (P_{1i}e_i r e_j P_{1j})^J(j,i) \\ &= \sum_{i,j=1}^{n} (P_{1i}e_i r e_j P_{1j})^{J_{R_0}}(j,i) = \left(\sum_{i,j=1}^{n} (P_{1i}e_i r e_j P_{1j})(i,j) \right)^{J_{R_0^{n\times n}}} \\ &= f_R(r)^{J_{R_0^{n\times n}}}. \end{aligned}$$

Damit erhalten wir

$$\begin{aligned} f_M(m(r\otimes s)) &= f_M(\psi(\psi^{-1}(m))(r\otimes s)) = f_M(\psi(r^J x s)) \\ &= \psi_0^{n\times n}(f_R(r^J\psi^{-1}(m)s)) = \psi_0^{n\times n}(f_R(r)^J f_R(\psi^{-1}(m))f_R(s)) \\ &= \psi_0^{n\times n}(f_R(\psi^{-1}(m)))(f_R(r)\otimes f_R(s)) = f_M(m)(f_R(r)\otimes f_R(s)). \end{aligned}$$

□

Bemerkung 4.17. *Es seien $\mathcal{R} = (R, M, \psi, \Phi)$ ein Form-Ring und $\rho = (V, \rho_M, \rho_\Phi, \beta)$ eine endliche Darstellung von $\mathcal{R}$. Weiter sei $C \le V^N$ ein Code vom Typ ρ. Mit $C(n) \le V^{N\times n}$ bezeichnen wir die abelsche Gruppe von Matrizen, deren Zeilen Elemente von C sind. Durch Matrixmultiplikation wird $C(n)$ zu einem $R^{n\times n}$-Teilmodul von $V^{n\times n}$.*

Dann ist $C(n)$ ein Code vom Typ $K^{n\times 1}\otimes_K \rho$; es gilt sogar, dass alle Codes vom Typ $K^{n\times 1}\otimes_K \rho$ von dieser Form sind.

Nun können wir höhere Gewichtszähler als gewöhnliche Gewichtszähler ausdrücken.

Bemerkung 4.18. *Mit den Bezeichnungen aus Bemerkung 4.17 gilt*

$$\mathrm{cwe}_n(C) = \mathrm{cwe}(C(n)).$$

Definieren wir nun die höheren Clifford-Weil-Gruppen, ergibt sich daraus sofort Bemerkung 4.20.

Definition 4.19. *Ist ρ eine Darstellung eines Form-Rings über dem Körper K, so heißt*

$$\mathcal{C}_n(\rho) := \mathcal{C}(K^{n\times 1} \otimes_K \rho)$$

die Geschlecht-n-Clifford-Weil-Gruppe von ρ.

Bemerkung 4.20. *Mit den Bezeichnungen von Bemerkung 4.17 gilt*

$$\mathrm{cwe}_n(C) \in \mathrm{Inv}(\mathcal{C}_n(\rho)).$$

5 Der Schatten eines Codes

Im vorigen Kapitel haben wir gesehen, dass sich aus den zu der Darstellung ρ gehörigen quadratischen Formen $\rho_\Phi(\phi),\ \phi \in \Phi$, gewisse Invarianzeigenschaften der Gewichtszähler von Codes vom Typ ρ ergeben.

Betrachten wir nun zwei Form-Ringe $\mathcal{R}_I = (R, M, \psi, \Phi_I)$ und $\mathcal{R}_{II} = (R, M, \psi, \Phi_{II})$, wobei $\Phi_I \subsetneq \Phi_{II}$; es seien ρ_I und ρ_{II} endliche Darstellungen von $\mathcal{R}_I$ bzw. $\mathcal{R}_{II}$, wobei ρ_I aus ρ_{II} hervorgehe durch Einschränkung auf $\mathcal{R}_I$. Da durch ρ_{II} mehr quadratische Formen definiert werden, hat $\mathcal{C}(\rho_{II})$ den kleineren Invariantenring; insbesondere ergeben sich aus der Invariantentheorie für Codes vom Typ ρ_{II} bessere obere Schranken an das Minimalgewicht.

Man nennt (ρ_I, ρ_{II}) ein Schattenpaar, denn für einen selbstorthogonalen Code C in $N\rho_I$ lassen sich mit Hilfe von Φ_{II} Schatten von C definieren. Dies sind Restklasse nach $C^\perp$, deren Gewichtszähler durch Variablensubstitution aus dem Gewichtszähler von C hervorgehen. Die offensichtliche Bedingung, dass die Koeffizienten im Gewichtszähler eines Schattens nicht-negative ganze Zahlen sind, liefert eine Verschärfung der oberen Schranken an das Minimalgewicht von Codes vom Typ ρ_I.

5.1 Einführung des Schattens

Definition und Bemerkung 5.1. *[Schatten eines selbstorthogonalen Codes] Sei $\rho = (V, \rho_M, \rho_\Phi, \beta)$ eine Darstellung eines Form-Rings und $C \leq V^N$ ein selbstorthogonaler Code in $N\rho$. Dann gelten*

(i) Die Abbildung $\rho_\Phi^N(\phi) :\ C \mapsto \mathbb{Q}/\mathbb{Z}$ ist für $\phi \in \Phi$ ein Homomorphismus abelscher Gruppen.

(ii) Es sei

$$S_\phi(C) = \{v \in V^N \mid \beta^N(v, c) = \rho_\Phi^N(\phi)(c) \text{ für alle } c \in C\}$$

der ϕ-Schatten von C, für $\phi \in \Phi$. Dann ist $S_\phi(C)$ für $\phi \in \Phi$ eine Restklasse nach dem dualen Code $C^\perp$, die nur von der Restklasse $\phi + \{\!\{M\}\!\} \in \Phi + \{\!\{M\}\!\}$ abhängt.

Beweis.

zu (i): Für $c, c' \in C$ gilt

$$\rho_\Phi^N(\phi)(c + c') - \rho_\Phi^N(\phi)(c) - \rho_\Phi^N(\phi)(c') = \lambda(\rho_\Phi^N(\phi))(c, c') = \rho_M^N(\lambda(\phi))(c, c') = 0.$$

zu (ii): Wir zeigen zunächst, dass $S_\phi(C) \neq \emptyset$ ist: Nach (i) ist $\rho_\Phi^N(\phi)$ linear auf C. Als solcher lässt $\rho_\Phi^N(\phi)$ sich zu einem Homomorphismus $\psi :\ V \mapsto \mathbb{Q}/\mathbb{Z}$ auf V fortsetzen. Da β nichtsingulär ist, existiert ein $v \in V$ mit $\beta(v, \cdot) = \psi$ für alle $v \in V$. Insbesondere gilt $v \in S_\phi(C)$.
Ist $v \in S_\phi(C)$ und ist $c' \in C^\perp$, so ist $v + c' \in S_\phi(C)$, da

$$\beta^N(v + c', c) = \beta^N(v, c) + \beta^N(c', c) = \beta^N(v, c) = \rho_\Phi^N(\phi)(c)$$

für alle $c \in C$.
Umgekehrt ergibt sich für $v, v' \in S_\phi(C)$, dass $v - v' \in C^\perp$, denn für $c \in C$ ist

$$\beta^N(v - v', c) = \beta^N(v, c) - \beta^N(v', c) = \rho_\Phi^N(c) - \rho_\Phi^N(c) = 0.$$

Es bleibt zu zeigen, dass $S_\phi(C)$ nur von der Restklasse $\phi + \{\!\{M\}\!\} \in \Phi + \{\!\{M\}\!\}$ abhängt, das heißt, dass $S_\phi(C) = S_{\phi+\{\!\{m\}\!\}}(C)$ für $m \in M$. Seien dazu $m \in M$ und $c \in C$. Dann ist

$$\rho_\phi^N(\{\!\{m\}\!\})(c) = \{\!\{\rho_M^N(m)\}\!\}(c) = \rho_M^N(m)(c,c) = \beta(c,mc) = 0,$$

wobei die letzte Gleichheit aus der Selbstorthogonalität von C folgt.

Da

$$\rho_\phi^N : \Phi \to \mathrm{Quad}_0(V,A)$$

ein Gruppenhomomorphismus ist, gilt $\rho_\phi^N(\phi + \{\!\{M\}\!\})(c) = \rho_\phi^N(\phi)(c)$ für alle $c \in C$. Aus der Definition von $S_\phi(C)$ folgt nun die Behauptung.

□

Bemerkung 5.2. *Ist C ein isotroper Code in $N\rho$, $\phi \in \Phi$, so ist $S_\phi(C) = C^\perp$. Ist C zusätzlich selbstdual, so ist $S_\phi(C) = C$.*

5.2 Das Schattenpaar $(\rho(q_I^E), \rho(q_{II}^E))$

Die in Kapitel 3 eingeführten Darstellungen $\rho(q_I^E)$ und $\rho(q_{II}^E)$ von $\mathcal{R}(q_I^E)$ bzw. $\mathcal{R}(q_{II}^E)$ bilden ein Schattenpaar.

Ein selbstdualer isotroper Code C in $N\rho(q_I^E)$ ist auch selbstdual als Code in $N\rho(q_{II}^E)$, ist in dieser Darstellung aber nicht notwendig isotrop. Daher kann man die Darstellung $\rho(q_{II}^E)$ benutzen, um nicht-triviale Schatten von C zu konstruieren (vgl. 5.2):

Fasst man C als Code in $N\rho(q_{II}^E)$ auf, so ist $S_\phi(C) \neq \emptyset$ für $\phi \in \Phi$; dies folgt mit dem Argument aus 5.1 (ii) wegen $\beta_{\rho(q_{II}^E)} = \beta_{\rho(q_I^E)}$.

In Kapitel 4 haben wir gesehen, dass die einfache Struktur der q-Moduln sich in gewisser Weise auf die Clifford-Weil-Gruppe überträgt. Ähnliches gilt auch für die Schatten. Das folgende Lemma zeigt, dass sich im Fall der einfachen Erzeugtheit des q-Moduls alle Schatten $S_\phi(C)$ für $\phi \in \Phi$ aus einem einzigen Schatten berechnen lassen.

Lemma 5.3. *Es sei C ein selbstorthogonaler Code in ρ. Weiter seien ϕ, ϕ_1 und $\phi_2 \in \Phi$ sowie $r \in R^*$. Dann gelten*

(i) $S_{\phi[r]}(C) = (r^J)^{-1} S_\phi(C)$,

(ii) $S_{\phi_1+\phi_2}(C) = S_{\phi_1}(C) + v_0$ *für jedes* $v_0 \in S_{\phi_2}(C)$.

Beweis.

zu (i): Da die Abbildung ρ_ϕ ein R-qModulhomomorphismus ist, gilt

$$\begin{aligned} S_{\phi[r]}(C) &= \{v \in V \mid \beta(v,c) = \rho_\Phi(\phi[r])(c) \text{ für alle } c \in C\} \\ &= \{v \in V \mid \beta(v,c) = \rho_\Phi(\phi)(rc) \text{ für alle } c \in C\}. \end{aligned}$$

Mit Hilfe von 3.5 (v) erhalten wir

$$\begin{aligned} S_{\phi[r]}(C) &= \{v \in V \mid \beta(v,r^{-1}c) = \rho_\Phi(\phi)(c) \text{ für alle } c \in C\} \\ &= \{v \in V \mid \beta(r^J v,c) = \rho_\Phi(\phi)(c) \text{ für alle } c \in C\} \\ &= (r^J)-1 S_\phi(C). \end{aligned}$$

zu (ii): Da C selbstorthogonal ist, ist $\rho_\Phi(\phi_2)$ linear auf C; daher existiert ein $v_0 \in V$ mit $\rho_\Phi(\phi_2)(c) = \beta(v_0, c)$ für alle $c \in C$. Nach dieser Wahl gilt auch $v_0 \in S_{\phi_2}(C)$, und es ist

$$\begin{aligned} S_{\phi_1+\phi_2}(C) &= \{v \in V \mid \beta(v,c) = \rho_\Phi(\phi_1)(c) + \rho_\Phi(\phi_2)(c) \text{ für alle } c \in C\} \\ &= \{v \in V \mid \beta(v - v_0, c) = \rho_\Phi(\phi_1)(c) \text{ für alle } c \in C\} \\ &= S_{\phi_2}(C) + v_0. \end{aligned}$$

□

Euklidisch selbstduale Codes $C \leq \mathbb{F}_q^N,\ q = 2^f$, lassen sich mit Hilfe einer invertierbaren Abbildung $\Delta : \mathbb{F}_q^N \to \mathbb{F}_2^N$ in euklidisch selbstduale binäre Codes (Typ $\rho(2_I^E)$) transformieren. Diese Transformation vertauscht mit der Bildung gewisser Schatten, so dass der Schatten eines Codes C vom Typ $\rho(q_I^E)$ durch Transformation eines Schattens von $\Delta(C) \leq \mathbb{F}_2^N$ berechnet werden kann. Die Schatten eines binären selbstdualen Codes (eines Typ $\rho(2_I^E)$-Codes) wiederum lassen sich relativ leicht beschreiben.

Lemma 5.4. *Sei $q = 2^f,\ f \in \mathbb{N}$, und sei $C \leq \mathbb{F}_q^N$ vom Typ $\rho(q_I^E)$. Sei weiter $(b_1, \ldots, b_f)$ eine $\mathbb{F}_2$-Orthonormalbasis von $\mathbb{F}_q$ bezüglich der Spurbilinearform, das heißt, $\mathrm{Tr}_{\mathbb{F}_q|\mathbb{F}_2}(b_i b_j) = \delta_{ij}\ \beta(q_{II}^E)$. Es sei im Folgenden abkürzend $\mathrm{Tr} := \mathrm{Tr}_{\mathbb{F}_q|\mathbb{F}_2}$. Wir definieren einen $\mathbb{F}_2$-Vektorraumisomorphismus*

$$\Delta : \mathbb{F}_q^N \to \mathbb{F}_2^{fN},\ (v_1, \ldots, v_N) \mapsto (v_1^{(1)}, \ldots, v_1^{(f)}, \ldots, v_N^{(1)}, \ldots, v_N^{(f)}),$$

falls $v_i = v_i^{(1)} b_1 + \ldots + v_i^{(f)} b_f$ für $i \in \{1, \ldots, N\}$.

Dann gelten

(i) $\beta(q_{II}^E)(\Delta^{-1}(v), \Delta^{-1}(c)) = \beta(2_{II}^E)(v, c)$ *für alle* $v \in \mathbb{F}_2^{fN},\ c \in \Delta(C)$,

(ii) $\rho_{\Phi(q_{II}^E)}(1)(\Delta^{-1}(c)) = \rho_{\Phi(2_{II}^E)}(1)(c)$ *für alle* $c \in \Delta(C)$.

Aus (i) folgt insbesondere, dass $\Delta(C)$ ein binärer selbstdualer Code der Länge fN ist, falls $C \leq \mathbb{F}_{2^f}^N$ ein Euklidisch selbstdualer Code ist.

Beweis.

zu (i): Da $(b_1, \ldots, b_f)$ als $\mathbb{F}_2$-Orthonormalbasis von $\mathbb{F}_q$ bezüglich Tr gewählt war, ergibt sich

$$\begin{aligned} \beta(q_{II}^E)(\Delta^{-1}(v), \Delta^{-1}(c)) &= \tfrac{1}{2} \textstyle\sum_{i=1}^N \mathrm{Tr}((\Delta^{-1}(v))_i, (\Delta^{-1}(c))_i) \\ &= \tfrac{1}{2} \textstyle\sum_{i=1}^N \mathrm{Tr}(v_{f(i-1)+1} c_{f(i-1)+1} b_1^2 + \ldots + v_{fi} c_{fi} b_f^2) \\ &= \tfrac{1}{2} \textstyle\sum_{i=1}^N v_{f(i-1)+1} c_{f(i-1)+1} + \ldots + v_{fi} c_{fi} = \tfrac{1}{2} \textstyle\sum_{i=1}^{fN} v_i c_i = \beta(2_{II}^E)(v, c). \end{aligned}$$

zu (ii): Es ist

$$\begin{aligned} \rho_{\Phi(q_{II}^E)}(1)(\Delta^{-1}(c)) &= \tfrac{1}{2} \rho_{\Phi(q_I^E)}(1)(\Delta^{-1}(c)) = \tfrac{1}{2} \beta(q_I^E)(\Delta^{-1}(v), \Delta^{-1}(c)) \\ &= \tfrac{1}{2} \beta(q_{II}^E)(\Delta^{-1}(v), \Delta^{-1}(c)) \overset{(i)}{=} \tfrac{1}{2} \beta(2_{II}^E)(c, c) = \rho_{\Phi(2_{II}^E)}(1)(c). \end{aligned}$$

□

Beispiel 5.5 (Berechnung von Schatten beim Typ 2_I^E). *Es sei C ein selbstorthogonaler Code in $N\rho(2_I^E)$, also ein binärer Code, welcher selbstorthogonal ist bezüglich des Euklidischen Skalarprodukts.*

Den zu dem Form-Ring $\mathcal{R}(2_{II}^E)$. gehörigen $\mathbb{F}_2$-qModul $\mathbb{Z}/4\mathbb{Z}$ wollen wir im Folgenden mit Φ_{II} bezeichnen.

Um für $\phi_{II} \in \Phi_{II}$ den Schatten $S_{\phi_{II}}(C)$ zu berechnen, überlegen wir uns zunächst, wie die Restklassengruppe $\Phi_{II}/\{\mathbb{F}_2\}$ aussieht (vgl. 5.1(ii)); es ist

$$\Phi_{II}/\{\mathbb{F}_2\} = \mathbb{Z}/4\mathbb{Z}/2\mathbb{Z}/4\mathbb{Z},$$

und daher ist

$$S_0(C) = S_2(C) \qquad \text{und } S_1(C) = S_3(C).$$

Berechnen wir also $S_0(C)$ und $S_1(C)$: Gemäß 3.11(b) ist $\rho^N_{\Phi_{II}}(0)(c) = 0$ für alle $c \in C$; daher ist

$$S_0(C) = \{v \in V^N \mid \beta^N(v,c) = 0 \text{ für alle } c \in C\} = C^\perp.$$

Der Schatten $S_1(C)$ lässt sich auch anders beschreiben. Betrachten wir den maximalen isotropen Untercode von C, welcher zunächst für allgemeine Form-Ringe und Codes C definiert sei durch

$$C_0 := \{c \in C \mid \rho^N_\Phi(\phi)(c) = 0 \text{ für alle } \phi \in \Phi\}.$$

Als Schnitt der Kerne der Gruppenhomomorphismen $\rho^N_\Phi(\phi),\ \phi \in \Phi$, ist C_0 tatsächlich eine Untergruppe von C. C_0 ist auch ein R-Modul, da $\rho^N_\Phi(\phi)(rc) = \rho^N_\Phi(\phi[r])(c)$ für $r \in R,\ c \in C$, und die Isotropie von C_0 ergibt sich sofort aus seiner Definition.

Sei nun wieder C ein selbstorthogonaler Code in $N\rho(2_{II}^E)$. In diesem Fall ist

$$C_0 = \{c \in C \mid \operatorname{wt}(c) \equiv 0 \mod 4\},$$

und dies ist eine Untergruppe vom Index 2 in C, denn für $c, c' \in C - C_0$ gilt

$$\operatorname{wt}(c+c') = \operatorname{wt}(c) + \operatorname{wt}(c') - 2\sum_{i=1}^N c_i c_i' \equiv 0 \mod 4,$$

also $c + c' \in C_0$.

Mit diesem Wissen können wir nun zeigen, dass $S_1(C) = C_0^\perp - C_0$ ist. Die Inklusion $S_1(C) \subseteq C_0^\perp - C^\perp$ ergibt sich sofort aus der Definition von $S_1(C)$. Ist umgekehrt $v \in C_0^\perp - C^\perp$, so ist zu zeigen, dass v für alle $c \in C$ der Gleichung $\beta^N(v,c) = \rho^N_{\Phi_{II}}(1)(c)$ genügt.

Für $c \in C_0$ ist dies klar. Sind $c, c' \in C - C_0$, so ist, wie wir oben gesehen haben, $c + c' \in C_0$, und aus $v \in C_0^\perp$ folgt dann $\beta(v,c) = \beta(v,c')$. Weiter existiert wegen $v \notin C^\perp$ ein $c \in C$ mit $\beta(v,c) = \frac{1}{2} = \rho^N_{\Phi_{II}}(1)(c)$, und diese letzte Gleichung gilt dann für alle $c' \in C - C_0$.

Beispiel 5.6. *Es sei $C \leq \mathbb{F}_4^4$ der selbstduale Code mit Erzeugermatrix*

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

Die Erzeugermatrix von $\Delta(C) \leq \mathbb{F}_2^8$ ergibt sich zu

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

Es gilt

$$v \in S_1(\Delta(C)) \Leftrightarrow \beta^8(v,c) = \rho_\Phi^8(1)(c) \text{ für alle } c \in \Delta(c).$$

Da $\rho_\Phi^8(1)$ linear ist auf $\Delta(C)$ und die Zeilen der Erzeugermatrix von $\Delta(C)$ diesen als abelsche Gruppe erzeugen, müssen wir diese Bedingung nur für die Erzeuger überprüfen, was auf ein Kongruenzgleichungssystem führt: Es ist $v = (v_1, \ldots, v_8) \in S_1(\Delta(C))$ genau dann, wenn

$$\begin{array}{ll} v_1 + v_2 + v_3 + v_4 + v_5 + v_6 + v_7 + v_8 \equiv 0 & \mod 2 \\ v_1 + v_3 + v_5 + v_7 \equiv 0 & \mod 2 \\ v_5 + v_6 + v_7 + v_8 \equiv 0 & \mod 2 \\ v_5 + v_7 \equiv 1 & \mod 2. \end{array}$$

Dies wird beispielsweise von $(1,1,0,0,1,0,0,1) \in \mathbb{F}_2^8$ erfüllt, daher ist

$$S_1(\Delta(C)) = (1,1,0,0,1,0,0,1) + \Delta(C).$$

Die Rücktransformation ergibt

$$S_1(C) = (1,0,w,w^2) + C.$$

5.3 Der Gewichtszähler des Schattens

Der vollständige Gewichtszähler des Schattens ergibt sich durch Variablensubstitution aus dem Gewichtszähler des Codes. Um das zu zeigen, betrachten wir zunächst eine lineare Transformation des vollen Gewichtszählers.

Satz 5.7. *Ist $C \leq V^N$ ein selbstorthogonaler Code in $N\rho$, so gilt*

$$\mathrm{fwe}(S_\phi(C)) = \frac{1}{|C|} \sum_{c \in C} \sum_{w \in V^N} \exp(2\pi i(\beta^N(w,c) - \rho_\Phi^N(\phi)(c)))b_w.$$

Beweis. Da C selbstorthogonal ist, ist gemäß Definition und Bemerkung 5.1 (i) ρ_Φ^N linear auf C; daher wird durch

$$\chi_{\phi,w} : \ C \to \mathbb{C}, \ c \mapsto \exp(2\pi i(\beta^N(w,c) - \rho_\Phi^N(\phi)(c)))$$

ein Charakter von C definiert. Dies ist genau dann der triviale Charakter $\mathbf{1}_C$, wenn $w \in S_\phi(C)$ ist, und deshalb ist

$$< \chi_{\phi,w}, \mathbf{1}_C >_C = \frac{1}{|C|} \sum_{c \in C} \exp(2\pi i(\beta^N(w,c) - \rho_\Phi^N(\phi)(c))) = \begin{cases} 1, & w \in S_\phi(C) \\ 0, & \text{sonst.} \end{cases}$$

□

Satz 5.8. *Definieren wir auf $\mathbb{C}[x_v \mid v \in V]_N$ einen $\mathbb{C}$-Algebrenhomomorphismus T_ϕ durch*

$$T_\phi(x_v) = \sum_{w \in V} \exp(2\pi i(\beta(v,w) - \rho_\Phi(\phi)(v)))x_w,$$

so gilt

$$\mathrm{cwe}(S_\phi(C)) = \frac{1}{|C|} T_\phi(\mathrm{cwe}(C)).$$

Beweis. Dies ergibt sich wegen Satz 5.7 aus Lemma 1.11 mit $T = T_\phi$ sowie

$$f_v(w) = \exp(2\pi i(\beta(v,w) - \rho_\Phi(\phi)(v))), \;\; \tilde{T} = \sum_{w \in V^N} \exp(2\pi i(\beta^N(w,c) - \rho_\Phi^N(\phi)(c))).$$

□

Bemerkung 5.9. *Es sei C ein Code vom Typ $\rho(q_I^E)$. Nach Lemma 5.3 ist $S_{r^2}(C) = rS_1(C)$ für $\phi \in \Phi$ und $r \in \mathbb{F}_q^*$. Es sei $m_r \in \mathbb{F}_2^{q \times q}$ die Matrix, welche die Linksmultiplikation mit r beschreibt. Dann gilt*

$$\mathrm{cwe}(S_{r^2}(C)) = \mathrm{cwe}(S_1(C))m_r,$$

das heißt, $\mathrm{cwe}(S_{r^2}(C))$ geht durch Permutation der Variablen aus $\mathrm{cwe}(S_1(C))$ hervor.

6 Die Struktur der Clifford-Weil-Gruppe

Im Folgenden bezeichne $\mathcal{R} = (R, M, \psi, \Phi)$ einen Form-Ring; es sei dabei stets R ein Matrixring über einem endlichen Körper K. Diese Annahme vereinfacht die in diesem Kapitel behandelten Aussagen und Beweise; alle Sätze und Lemmata lassen sich jedoch auch über allgemeinen Ringen R beweisen.

6.1 Die hyperbolische counitäre Gruppe $U(R, \Phi)$

Definition 6.1. *Sei $\mathcal{R} = (R, M, \psi, \Phi)$ ein Form-Ring. Dann heißt*

$$P(R, \Phi) := R^* \ltimes \Phi = \{(r, \phi) | r \in R^*, \phi \in \Phi\}$$

mit der Multiplikation

$$(r_1, \phi_1)(r_2, \phi_2) := (r_1 r_2, \phi_1[r_1] + \phi_2)$$

die parabolische Gruppe von (R, Φ).

Definition 6.2. *Sei $\mathcal{R} = (R, M, \psi, \Phi)$ ein Form-Ring und sei $f \in R$. Dann heißt*

$$U(f, (R, \Phi)) := \{(r, \phi) \in P(R, \Phi) | r^J f r - f = \psi^{-1}(\lambda(\phi))\} \leq P(R, \Phi)$$

die counitäre Gruppe von R. Ist speziell $f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in R^{2\times 2}$, so heißt

$$U(R, \Phi) := U(f, \mathrm{Mat}_2(R, \Phi))$$

die hyperbolische counitäre Gruppe von $\mathcal{R}$.

Bemerkung 6.3. *$U(R, \Phi)$ enthält genau die Elemente $\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix}\right)$ von $P(\mathrm{Mat}_2(R, \Phi))$ mit*

$$\begin{pmatrix} c^J a & c^J b \\ d^J a - 1 & d^J b \end{pmatrix} = (\psi^{2\times 2})^{-1}(\lambda^{(2)}(\begin{pmatrix} \lambda(\phi_1) & m \\ \tau(m) & \lambda(\phi_2) \end{pmatrix}).$$

Definition 6.4. *Wir definieren einen Gruppenhomomorphismus $\pi : U(R, \Phi) \to \mathrm{GL}_2(R)$ durch*

$$\pi(\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix}\right)) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Der Kern und das Bild von π haben oft eine sehr schöne Struktur.

Bemerkung 6.5. *Es sei $\mathcal{R} = (R, M, \psi, \Phi)$ mit λ ein Form-Struktur. Dann gilt $\mathrm{Kern}(\pi) \cong \lambda \oplus \lambda$.*

Beweis. Es gilt

$$\mathrm{Kern}(\pi) = \left\{\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix}\right) \in U(R, \Phi)\right\}.$$

Gemäß Bemerkung 3.5 ist die definierende Bedingung dieser Menge äquivalent damit, dass $\lambda(\phi_1) = \lambda(\phi_2) = m = 0$ ist. □

Beispiel 6.6 ($\mathrm{Bild}(\pi)$ **beim Typ** $q_{II}^E,\ q=2^f$**).** *Es seien p eine ungerade Primzahl. Es sei dann $\mathcal{R}=(R,M,\psi,\Phi):=\mathrm{Mat}_n(\mathcal{R}_0)$, wobei $\mathcal{R}_0$ der Form-Ring des Typs q_{II}^E sei (siehe Abschnitt 3.3.3. Dann ist $\Phi=\{\!\{M\}\!\}=\{m+m^t\mid m\in\mathbb{F}_q^{n\times n}\}=:\mathrm{Sym}_n(\mathbb{F}_q)$ die Menge der symmetrischen Matrizen in $\mathbb{F}_q^{n\times n}$. Nun enthält* $\mathrm{Bild}(\pi)$ *genau die Matrizen* $\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\mathrm{GL}_{2n}(\mathbb{F}_q)$*, für die die Matrix*

$$X:=\begin{pmatrix} a^t & b^t\\ c^t & d^t\end{pmatrix}\begin{pmatrix} 0 & 0\\ I_n & 0\end{pmatrix}\begin{pmatrix} a & b\\ c & d\end{pmatrix}-\begin{pmatrix} 0 & 0\\ I_n & 0\end{pmatrix}$$

symmetrisch ist. Diese Bedingung ist äquivalent mit $X-X^t=0$, das heißt

$$\begin{pmatrix} a^t & b^t\\ c^t & d^t\end{pmatrix}\begin{pmatrix} 0 & -I_n\\ I_n & 0\end{pmatrix}\begin{pmatrix} a & b\\ c & d\end{pmatrix}=\begin{pmatrix} 0 & -I_n\\ I_n & 0\end{pmatrix}.$$

Daraus folgt $\mathrm{Bild}(\pi)\cong\mathrm{Sp}_{2n}(\mathbb{F}_q)$.

Die folgende Tabelle gibt das Bild von π für verschiedene Form-Ringe an. Hierbei ist $\mathrm{Ev}_n(K)=\{A\in\mathrm{Sym}_n\mid 2|A_{ii},\ i=1,\dots,n\}$.

R	J	ϵ	$\mathrm{Bild}(\pi)$
$\mathbb{F}_q^{n\times n}\oplus\mathbb{F}_q^{n\times n}$	$(r,s)^J=(s^t,r^t)$	1	$\mathrm{GL}_{2n}(\mathbb{F}_q)$
$\mathbb{F}_{q^2}^{n\times n}$	$r^J=(r^q)^t$	1	$U_{2n}(\mathbb{F}_{q^2})$
$\mathbb{F}_q^{n\times n},\ q=p^m,\ p>2$	$r^J=r^t$	1	$\mathrm{Sp}_{2n}(\mathbb{F}_q)$
$\mathbb{F}_q^{n\times n},\ q=p^m,\ p>2$	$r^J=r^t$	-1	$O_{2n}^+(\mathbb{F}_q)$
$\mathbb{F}_q^{n\times n},\ q=p^m,\ p=2$	$\psi^{-1}(\lambda(\Phi))=\mathrm{Sym}_n(\mathbb{F}_q)$		$\mathrm{Sp}_{2n}(\mathbb{F}_q)$
$\mathbb{F}_q^{n\times n},\ q=p^m,\ p=2$	$\psi^{-1}(\lambda(\Phi))=\mathrm{Ev}_n(\mathbb{F}_q)$		$O_{2n}^+(\mathbb{F}_q)$

Satz 6.7. *Die Abbildung*

$$d:\ \ P(R,\Phi)\to U(R,\Phi),\qquad (r,\Phi)\mapsto\left(\begin{pmatrix} r^{-J} & r^{-J}\psi^{-1}(\lambda(\phi))\\ 0 & r\end{pmatrix},\begin{pmatrix} 0 & 0\\ & \phi\end{pmatrix}\right)$$

ist ein Gruppenmonomorphismus.

Bemerkung 6.8. *Ist $e\in R$ ein symmetrisches Idempotent und sind $u_e,v_e\in R$ wie in Bemerkung 3.10, so ist*

$$H_{e,u_e,v_e}:=\left(\begin{pmatrix} 1-e^J & v_e\\ -\epsilon^{-1}u_e^J & 1-e\end{pmatrix},\begin{pmatrix} 0 & \psi(-\epsilon e)\\ & 0\end{pmatrix}\right)\in U(R,\Phi).$$

Der folgende Satz wird in [5], Abschnitt 5.2.1, für allgemeinere Ringe R gezeigt.

Satz 6.9. *Es sei $\mathcal{R}=(R,M,\psi,\Phi)$ ein Form-Ring. Dann gilt*

$$U(R,\Phi)=<d(P(R,\Phi),H_{e,u_e,v_e})\ \big|\ e\in R\text{ symmetrisches Idempotent}\ >.$$

Der Satz 6.13 stellt eine Verschärfung dieses Satzes dar, falls speziell $R=K^{n\times n}$ ist mit dem endlichen Körper K. Dieser Satz ist das Ziel der folgenden drei Bemerkungen.

Bemerkung 6.10. *Es seien $e \in R$ ein symmetrisches Idempotent bezüglich ^{J} sowie u_e und v_e wie in Bemerkung 3.10; weiter sei $r \in R^*$. Setzen wir $d := rer^{-1}$ sowie $u_d := ru_er^J$ und $v_d := r^{-J}v_er^{-1}$, so ist das Idempotent d ebenfalls symmetrisch bezüglich ^{J} und u_d, v_d haben bezüglich d die in Bemerkung 3.10 geforderten Eigenschaften. Weiter gilt*

$$d((r,0))H_{e,u_e,v_e}d((r^{-1},0)) = H_{d,u_d,v_d}.$$

Beweis. Zuerst weisen wir die in Bemerkung 3.10 geforderten Eigenschaften bei u_d und v_d nach; diese ergeben sich aus den entsprechenden Eigenschaften von u_e und v_e, da

$$\begin{aligned}
&du_d = rer^{-1}ru_er^J = ru_er^J = u_d, \quad u_dd^J = ru_er^Jr^{-J}e^Jr^J = ru_er^J = u_d,\\
&d^Jv_d = r^{-J}e^Jr^Jr^{-J}v_er^{-1} = r^{-J}v_er^{-1} = v_d, \quad v_dd = r^{-J}v_er^{-1}rer^{-1} = r^{-J}v_er^{-1} = v_d,\\
&u_dv_d = ru_er^Jr^{-J}v_er^{-1} = rer^{-1} = d, \quad v_du_d = r^{-J}v_er^{-1}ru_er^J = r^{-J}e^Jr^J = d^J.
\end{aligned}$$

Nun berechnen wir das Produkt $d((r,0))H_{e,u_e,v_e}d((r^{-1},0))$ mit Hilfe der Rechenregeln in Definition 6.1

Konjugation von $\pi(H_{e,u_e,v_e})$ mit $\pi(d(r,0))$ ergibt

$$\begin{pmatrix} r^{-J} & 0 \\ 0 & r \end{pmatrix}\begin{pmatrix} 1-e^J & v_e \\ -\epsilon^{-1}u_e^J & 1-e \end{pmatrix}\begin{pmatrix} r^J & 0 \\ 0 & r^{-1} \end{pmatrix} = \begin{pmatrix} 1-d^J & r^{-J}v_er^{-1} \\ -r\epsilon^{-1}u_e^Jr^J & 1-d \end{pmatrix} = \pi(H_{d,u_d,v_d}).$$

Unter der Konjugation ergibt sich gemäß Definition und Bemerkung 4.13

$$\begin{pmatrix} 0 & \psi(-\epsilon e) \\ & 0 \end{pmatrix}\left[\begin{pmatrix} r^J & 0 \\ 0 & r^{-1} \end{pmatrix}\right] = \begin{pmatrix} 0 & \psi(-r^{J^2}\epsilon er^{-1}) \\ 0 & 0 \end{pmatrix}$$

Nach Bemerkung 3.5 ist

$$\psi(-r^{J^2}\epsilon er^{-1}) = \psi(-r^{J^{(2)}}\epsilon er^{-1}) = \psi(\epsilon rer^{-1}) = \psi(\epsilon d),$$

woraus die Behauptung folgt. □

Es genügt also, sich auf Vetreter der Konjugiertenklassen symmetrischer Idempotente zu beschränken, um $U(R,\Phi)$ zu erzeugen; diese kann man so wählen, dass sie die Form $\mathrm{diag}(d_1,\ldots,d_n)$ haben mit $d_i \in \{0,1\}$ für $i = 1,\ldots,n$. Insbesondere kann man wegen Bemerkung 4.16 annehmen, dass diese Idempotente invariant sind unter ^{J}, woraus sich erneut eine Vereinfachung ergibt:

Bemerkung 6.11. *Es $e \in R$ ein Idempotent, welches invariant ist unter ^{J}; weiter seien u_e und v_e wie in Bemerkung 3.10. Dann existiert ein $T \in U(R,\Phi)$ mit $TH_{e,u_e,v_e} = H_{e,e,e}$.*

Beweis. Es ist

$$\pi(H_{e,u_e,v_e})^{-1} = \pi(H_{e,-\epsilon^{-1}u_e^J,-v_e^J\epsilon}) = \begin{pmatrix} 1-e^J & -v_e^J\epsilon \\ u_e & 1-e \end{pmatrix}.$$

Setzen wir $T_1 := \pi(H_{e,e,e})\pi(H_{e,-\epsilon^{-1}u_e^J,-v_e^J\epsilon})$, so ist

$$T_1 = \begin{pmatrix} 1-e+u_e & 0 \\ 0 & \epsilon^{-1}v_e^J\epsilon+1-e \end{pmatrix} \in \pi(d(P(R,\Phi))),$$

da $(\epsilon^{-1}v_e^J\epsilon+1-e)^{-J} = (\epsilon^Jv_e^{J^2}\epsilon+1-e)^{-1} = (v_e+1-e)^{-1} = 1-e+u_e$. Nach Konstruktion von T_1 gilt $T_1\pi(H_{e,u_e,v_e}) = \pi(H_{e,e,e})$. Daher besitzt $T := (T_1,0) \in d(P(R,\Phi))$ die gewünschte Eigenschaft. □

Die folgende Bemerkung zeigt, dass unter diesen Vertretern sogar nur die primitiven Idempotente benötigt werden.

Bemerkung 6.12. *Sind $e_1, e_2 \in R$ orthogonale Idempotente, welche invariant sind unter ^{J}, so gilt*

$$H_{e_1,e_1,e_1} H_{e_2,e_2,e_2} = H_{e_1+e_2,e_1+e_2,e_1+e_2}.$$

Beweis. Wir erhalten wegen der Orthogonalität von e_1 und e_2

$$\pi(H_{e_1,e_1,e_1})\pi(H_{e_2,e_2,e_2}) \begin{pmatrix} 1-(e_1+e_2) & e_1+e_2 \\ -\epsilon^{-1}(e_1+e_2) & 1-(e_1+e_2) \end{pmatrix} = \pi(H_{e_1+e_2,e_1+e_2,e_1+e_2})$$

Für die zweite Komponente ergibt sich

$$\begin{aligned} &\begin{pmatrix} 0 & \psi(-\epsilon e_1) \\ & 0 \end{pmatrix} \left[\begin{pmatrix} 1-e_2 & e_2 \\ -\epsilon^{-1}e_2 & 1-e_2 \end{pmatrix} \right] \\ &= \begin{pmatrix} \{\!\{\psi((1-e_1)(e_2e_1))\}\!\} & \psi(-(1-e_1)e_2\epsilon = \tau(\psi(e_1\epsilon^2 e_2 e_1)) \\ & \{\!\{\psi(-e_1\epsilon e_2)\}\!\} \end{pmatrix} \\ &= \begin{pmatrix} 0 & \psi(-e_2\epsilon) \\ & 0 \end{pmatrix}, \end{aligned}$$

woraus sich die Behauptung ergibt. □

Da die primitiven Idempotente gemäß 3.9 konjugiert zueinander sind, erhalten wir mit den Bemerkungen 6.10 und 6.11 den folgenden Satz.

Satz 6.13. *Es seien $R = K^{n\times n}$ und $\mathcal{R} = (R, M, \psi, \Phi)$ ein Form-Ring. Dann ist*

$$U(R,\Phi) =< d(P(R,\Phi)), H_{e,e,e} >,$$

wobei $e = \mathrm{diag}(1, 0, \ldots, 0)$.

Zum Beweis benötigen wir

Lemma 6.14. *a) Ist $x := \left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \begin{pmatrix} \phi_1 & \mu \\ & \phi_2 \end{pmatrix} \right) \in U(R,\Phi)$, so gilt*

(i) $\gamma^J\alpha = \alpha^J\epsilon\gamma,\ \delta^J\beta = \beta^J\epsilon\delta,\ \gamma^J\beta = \alpha^J\epsilon\delta - \epsilon,\ \beta^J\epsilon\gamma = \delta^J\alpha - 1,$

(ii) $\alpha\beta^J = \beta\epsilon^J\alpha^J,\ \gamma\delta^J = \delta\epsilon^J\gamma^J,\ \alpha\delta^J = 1 + \beta\epsilon^J\gamma^J,\ \delta\epsilon^J\alpha^J = \epsilon^J + \gamma\beta^J.$

b) Ist $x \in U(R,\Phi)$ von der Form

$$x = \left(\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}, \begin{pmatrix} 0 & m \\ & \phi \end{pmatrix} \right) \text{ mit } \alpha, \beta, \delta \in R,\ m \in M,\ \phi \in \Phi,$$

so ist $x \in d(P(R,\Phi))$.

Beweis.

a) (i) Für $y := \begin{pmatrix} \gamma^J\alpha & \gamma^J\beta \\ \delta^J\alpha - 1 & \delta^J\beta \end{pmatrix}$ gilt wegen $x \in U(R,\Phi)$

$$y = \left(\psi^{2\times 2}\right)^{-1} \left(\lambda^{2\times 2}\left(\begin{pmatrix} \phi_1 & \mu \\ & \phi_2 \end{pmatrix} \right)\right).$$

Da $\psi^{2\times 2}(y) \in \text{Bild}(\lambda^{2\times 2})$, folgt

$$\begin{aligned}
\psi^{2\times 2}(y) &= \tau^{(2)}(\psi^{2\times 2}(y)) \\
&= \begin{pmatrix} \tau(\psi(\gamma^J \alpha)) & \tau(\psi(\gamma^J \beta)) \\ \tau(\psi(\delta^J \alpha - 1)) & \tau(\psi(\delta^J \beta)) \end{pmatrix} \\
&= \psi^{2\times 2}(\begin{pmatrix} \alpha^J \gamma^{J^2} \epsilon & \beta^J \gamma^{J^2} \epsilon \\ \alpha^J \delta^{J^2} \epsilon - \epsilon & \beta^J \delta^{J^2} \epsilon \end{pmatrix}) \\
&= \psi^{2\times 2}(\begin{pmatrix} \alpha^J \epsilon \gamma & \beta^J \epsilon \gamma \\ \alpha^J \epsilon \delta - \epsilon & \beta^J \epsilon \delta \end{pmatrix}).
\end{aligned}$$

Da $\psi^{2\times 2}$ ein Isomorphismus ist, folgt die Behauptung.

(ii) Im Folgenden sei $g := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Wegen $x \in U(R, \Phi)$ gilt nach Definition

$$\underbrace{g^{J_2} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} g - \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}}_{=:M_1} = \underbrace{\left(\psi^{2\times 2}\right)^{-1} (\lambda^{2\times 2}(\begin{pmatrix} \phi_1 & \mu \\ & \phi_2 \end{pmatrix}))}_{=:M_2}$$

Wenn man auf beide Seiten dieser Gleichung den Antiautomorphismus J_2 anwendet und anschließend von rechts mit ϵ_2 multipliziert, erhält man einerseits

$$\begin{aligned}
M_1^{J_2} \epsilon_2 &= \left[g^{J_2} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \underbrace{g^{J_2^2}}_{=\epsilon_2 g \epsilon_2^{J_2}} - \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right] \epsilon_2 \\
&= g^{J_2} \begin{pmatrix} 0 & \epsilon \\ 0 & 0 \end{pmatrix} g - \begin{pmatrix} 0 & \epsilon \\ 0 & 0 \end{pmatrix}.
\end{aligned}$$

Andererseits ist $M_2^{J_2} \epsilon_2 = \left(\psi^{2\times 2}\right)^{-1} (\tau^{(2)}(\psi^{2\times 2}(M_2)))$; wegen $\psi^{2\times 2}(M_2) \in \text{Bild}(\lambda^{2\times 2})$ ist $\tau^{(2)}(\psi^{2\times 2}(M_2)) = \psi^{2\times 2}(M_2)$, das heißt, es ist $M_2^{J_2} \epsilon_2 = M_2$.
Insgesamt erhalten wir die Gleichung

$$\begin{aligned}
& g^{J_2} \begin{pmatrix} 0 & \epsilon \\ 0 & 0 \end{pmatrix} g - \begin{pmatrix} 0 & \epsilon \\ 0 & 0 \end{pmatrix} = g^{J_2} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} g - \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \\
\Leftrightarrow \quad & \begin{pmatrix} 0 & -\epsilon \\ 1 & 0 \end{pmatrix} = g^{J_2} \begin{pmatrix} 0 & -\epsilon \\ 1 & 0 \end{pmatrix} g \\
\Leftrightarrow \quad & g \begin{pmatrix} 0 & 1 \\ -\epsilon^{-1} & 0 \end{pmatrix} g^{J_2} = \begin{pmatrix} 0 & 1 \\ -\epsilon^{-1} & 0 \end{pmatrix} g \\
\Leftrightarrow \quad & \begin{pmatrix} \alpha\beta^J - \beta\epsilon^J \alpha^J & \alpha\delta^J - \beta\epsilon^J \gamma^J \\ \gamma\beta^J - \delta\epsilon^J \alpha^J & \gamma\delta^J - \delta\epsilon^J \gamma^J \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -\epsilon^J & 0 \end{pmatrix}.
\end{aligned}$$

Aus der letzten Ungleichung lässt sich die Behauptung ablesen.

b) Aus der Definition von $U(R, \Phi)$ ergibt sich unmittelbar $0^J \cdot \beta = \psi^{-1}(m)$, also ist $m = 0$. Nachzuweisen sind nun noch die Gleichungen $\delta^J = \alpha$ sowie $\alpha\psi^{-1}(\lambda(\phi)) = \beta$; beachte, dass $\alpha, \delta \in R^*$ wegen $\pi(x) \in R^{2\times 2^*}$. Nun gilt nach (a)(i) $\delta^J \alpha - 1 = 0$, woraus $\delta^{-J} = \alpha$ folgt. Nach Definition von $U(R, \Phi)$ gilt weiter $\psi^{-1}(\lambda(\phi)) = \delta^J \beta$; wegen $\delta^J = \alpha$ ist dies äquivalent zu $\alpha\psi^{-1}(\lambda(\phi)) = \beta$.

□

Beweis. [von Satz 6.13] Sei $\mathcal{G} :=< d(P(R,\Phi)), H_{e,e,e} >$ mit $e = \mathrm{diag}(1,0,\ldots,0)$. Aus den beiden vorangegangenen Sätzen folgt $\mathcal{G} \leq U(R,\Phi)$. Sei nun

$$x := \left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \begin{pmatrix} \phi_1 & \mu \\ & \phi_2 \end{pmatrix} \right) \in U(R,\Phi).$$

Wir nehmen zunächst an, dass $\delta \in R^*$. Nach Lemma 6.14 ist dann

$$g := \left(\begin{pmatrix} \delta^{-J} & \beta \\ 0 & \delta \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ & \phi_2 \end{pmatrix} \right) \in d(P(R,\Phi)).$$

Es ist

$$g^{-1} = \left(\begin{pmatrix} \delta^J & -\delta^J\beta\delta^{-1} \\ 0 & \delta^{-1} \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ & -\phi_2[\delta^{-1}] \end{pmatrix} \right)$$

und

$$\pi(g^{-1}x) = \begin{pmatrix} 1 & 0 \\ \delta^{-1}\gamma & 1 \end{pmatrix}.$$

Setzen wir nun $H := H_{1,1,1} = \left(\begin{pmatrix} 0 & 1 \\ -\epsilon^{-1} & 0 \end{pmatrix}, \begin{pmatrix} 0 & \psi(-\epsilon) \\ & 0 \end{pmatrix} \right) \in \mathcal{G} \leq U(R,\Phi)$, so ist $Hg^{-1}xH^{-1}$ von der Form

$$Hg^{-1}xH^{-1} = \left(\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}, \begin{pmatrix} 0 & * \\ & * \end{pmatrix} \right) \in U(R,\Phi).$$

Nach Lemma 6.14 gilt dann sogar $Hg^{-1}xH^{-1} \in d(P(R,\Phi)) \leq \mathcal{G}$. Dies bedeutet aber $x \in \mathcal{G}$, das heißt, $\mathcal{G}$ enthält alle Elemente $x \in U(R,\Phi)$ mit $\delta \in R^*$.

Sei nun $\delta \in R$ beliebig.
Wir können annehmen, dass δ ein symmetrisches Idempotent bezüglich J ist, sogar, dass $\delta^J = \delta$ ist, denn nach dem Elementarteilersatz existieren $u_1, u_2 \in R^*$, so dass

$$u_1\delta u_2 = \mathrm{diag}(1,\ldots,1,0,\ldots,0),$$

und es ist

$$d(u_1,0)\ x\ d(u_2,0) = \left(\begin{pmatrix} * & * \\ u_1\delta u_2 & * \end{pmatrix}, \begin{pmatrix} * & * \\ & * \end{pmatrix} \right) \in U(R,\Phi).$$

Das Idempotent $e := 1-\delta$ erfüllt ebenfalls $e^J = e$, ist also insbesondere symmetrisch bezüglich J. Weiter haben $\alpha_e := -\epsilon^J\gamma^J e$ und $\beta_e := \beta e$ die Eigenschaften

$$\begin{array}{lcl} e\alpha_e & = & -(1-\delta)\epsilon^J\gamma^J(1-\delta) = -\epsilon^J\gamma^J + \delta\epsilon^J\gamma^J + \epsilon^J\gamma^J\delta - \delta\epsilon^J\gamma^J\delta \\ & \overset{\delta\epsilon^J\gamma^J = \gamma\delta^J}{=} & -\epsilon^J\gamma^J + \gamma\delta^J + \epsilon^J\gamma^J\delta - \gamma\delta^J\delta = -\epsilon^J\gamma^J(1-\delta) = \alpha_e, \\ e^J\beta_e & = & (1-\delta)\beta(1-\delta) = \beta - \delta\beta - \beta\delta + \delta\beta\delta \\ & \overset{\delta^J\beta = \beta^J\epsilon\delta}{=} & \beta - \beta^J\epsilon\delta - \beta\delta + \beta^J\epsilon\delta = \beta(1-\delta) = \beta_e, \end{array}$$

woraus sich weiter ergibt, dass

$$\begin{array}{lcl} \alpha_e\beta_e & = & -\epsilon^J\gamma^J\beta_e = -\epsilon^J\gamma^J\beta + \epsilon^J\gamma^J\beta\delta \\ & \overset{\gamma^J\beta = \alpha^J\epsilon\delta - \epsilon}{=} & -\epsilon^J\alpha^J\epsilon\delta + 1 + (\epsilon^J\alpha^J\epsilon\delta - 1)\delta = 1 - \delta = e \end{array}$$

und

$$\begin{aligned}\beta_e\alpha_e &= \beta\alpha_e = -\beta\epsilon^J\gamma^J(1-\delta)\\ &= (\alpha\delta^J-1)(1-\delta) = 1-\delta = e^J.\end{aligned}$$

Somit ist $H_{e,\alpha_e,\beta_e} \in \mathcal{G}$, und Rechtsmultiplikation mit $\pi(H^{-1}_{e,\alpha_e,\beta_e})$ liefert

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} \delta & -\beta_e^J\epsilon \\ \alpha_e & \delta \end{pmatrix} = \begin{pmatrix} * & * \\ * & d \end{pmatrix},$$

wobei $d = -\gamma\beta_e^J\epsilon + \delta = -\gamma\beta^J + \gamma\delta\beta^J + \delta$. Im Folgenden werden wir zeigen, dass $d \in R^*$ ist.
Dazu beobachten wir zunächst, dass

$$\begin{aligned}d\delta &= -\gamma\beta^J\delta + \gamma\delta\beta^J\delta + \delta = -\gamma(\delta^J\beta)^J + \gamma\delta(\delta^J\beta)^J + \delta\\ &= -\gamma(\beta^J\epsilon\delta)^J + \gamma\delta(\beta^J\epsilon\delta)^J + \delta = \delta\end{aligned}$$

sowie

$$\begin{aligned}(1-\delta)d &\quad (1-\delta)(-\gamma\beta^J + \gamma\delta\beta^J + \delta) = -\gamma\beta^J + \gamma\delta\beta^J + \delta + \delta\gamma\beta^J - \delta\gamma\delta\beta^J - \delta\\ &\overset{\gamma\beta^J = \delta\epsilon^J\alpha^J - \epsilon^J}{=} -\delta\epsilon^J\alpha^J + \epsilon^J + \gamma\delta\beta^J + \delta\epsilon^J\alpha^J - \delta\epsilon^J - \delta\gamma\delta\beta^J\\ &\overset{\gamma\delta^J = \delta\epsilon^J\gamma^J}{=} \delta\epsilon^J\gamma^J\beta^J - \delta\epsilon^J\gamma^J\beta^J + \epsilon^J - \delta\epsilon^J = (1-\delta)\epsilon^J.\end{aligned}$$

Nun können wir zeigen, dass $\epsilon - \delta(d\epsilon - 1) = d^{-1}$, denn es ist

$$\begin{aligned}d(\epsilon - \delta(d\epsilon-1)) &= d\epsilon - d\delta(d\epsilon-1) = d\epsilon - \delta(d\epsilon-1)\\ &= d\epsilon - \delta d\epsilon + \delta = (1-\delta)d\epsilon + \delta\\ &= 1 - \delta + \delta = \delta.\end{aligned}$$

Es ist also $d \in R^*$; da wir diesen Fall anfangs schon behandelt haben, ist der Beweis des Satzes erbracht. □

6.2 $\mathcal{C}(\rho)$ als projektive Darstellung von $U(R,\Phi)$

Satz 6.15. *Es sei $\rho = (V, \rho_M, \rho_\Phi, \beta)$ eine endliche Darstellung von $\mathcal{R}$ und es sei $e = \mathrm{diag}(1,0,\ldots,0) \in R$. Dann ist*

$$p : U(R,\Phi) \to \mathcal{C}(\rho)/\mathbb{C}^*I_{|V|},\ d((r,\phi)) \mapsto m_r d_\phi \cdot \mathbb{C}^*I_{|V|},\ H_{e,e,e} \mapsto h_{e,e,e}\cdot\mathbb{C}^*I_{|V|}$$

ein Gruppenhomomorphismus, der eine projektive Darstellung $\rho_p : U(R,\Phi) \to \mathcal{C}(\rho)$ von $U(R,\Phi)$ liefert.

Beweis. Wir müssen nachweisen, dass p wohldefiniert ist; es muss also oBdA für a, b sowie $a', b' \in U(R,\Phi)$ mit $ab = a'b'$ gezeigt werden, dass $p(a)p(b)p(b')^{-1}p(a')^{-1} \in \mathbb{C}^*I_{|V|}$.

Dazu konstruiert man eine Gruppe $\mathcal{E}(V) \leq \mathrm{GL}_n(\mathcal{C})$ mit der Eigenschaft $C_{\mathrm{GL}_n(\mathbb{C})}(\mathcal{E}(V)) = \mathbb{C}^*I_{|V|}$ Die komplexe Matrixgruppe $\mathcal{C}(\rho)$ operiert auf $\mathcal{E}(V)$ durch Konjugation. Wir müssen also zeigen, dass die Elemente $p(a)p(b)p(b')^{-1}p(a')^{-1}$ trivial auf $\mathcal{E}(V)$ operieren, oder, anders ausgedrückt, dass $p(a)p(b)$ operiert wie $p(b')p(a')$. Die Operation von $U(R,\Phi)$ auf $\mathcal{E}(V)$, die auf den Erzeugern von $U(R,\Phi)$ definiert ist durch

$$x(v) := p(x)^{-1}vp(x),\ x \in d(P(R,\Phi)) \cup \{H_{e,e,e}\},$$

muss also wohldefiniert sein. Dazu zeigen wir, dass diese Operation mit einer weiteren, nicht nur auf Erzeugern definierten Operation von $U(R,\Phi)$ auf $\mathcal{E}(V)$ übereinstimmt.

Man erhält die Gruppe $\mathcal{E}(V)$ als Spezialfall der (nichtabelschen) Gruppe $E(f,V)$, $f \in R$, die definiert ist durch

$$E(f,V) = V \times \mathcal{Q}/\mathcal{Z}, (x_1,q_1)+(x_2,q_2) = (x_1+x_2, q_1+q_2+\beta(f\,x_2,x_1)).$$

Es operiert $U(f,(R,\Phi))$ auf $E(f,V)$ durch

$$(x,q)[(u,\phi)] = (ux, q+\rho_\Phi(\phi)(x)),\ u \in R^*,\ \phi \in \Phi,\ x \in V,\ q \in \mathbb{Q}/\mathbb{Z}.$$

Setzt man nun speziell

$$\mathcal{E}(\mathcal{V}) := E(\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, V \times V) = (V \times V) \times \mathbb{Q}/\mathbb{Z}$$

mit

$$((z_1,x_1),q_1)+((z_2,x_2),q_2) = ((z_1+z_2, x_1+x_2), q_1+q_2+\beta(x_2,z_1)),$$

so operiert $U(R,\Phi)$ entsprechend auf $\mathcal{E}(V)$. Um eine Operation von $\mathcal{C}(\rho)$ auf $\mathcal{E}(V)$ definieren zu können, betrachten wir die Darstellung $\mathcal{E}(V) \to \mathrm{GL}_{|V|}(\mathbb{C})$, die durch folgende (lineare) Operation von $\mathcal{E}(V)$ auf $\mathbb{C}V$ induziert wird:

$$((z,x),q)b_v = \exp(2\pi i(q+\beta(v,z)))b_{v+x}.$$

Man beachte, dass diese Darstellung treu ist, da β nichtsingulär ist.
Nun operiert $\mathcal{C}(\rho)$ durch Konjugation auf $\mathcal{E}(V)$.
Die folgenden Rechnungen zeigen, dass die beiden auf $\mathcal{E}(V)$ definierten Operationen übereinstimmen:

Es gilt $(m_r d_\phi)((z,x),q)(m_r d_\phi)^{-1}(b_v)$

$$\begin{aligned}
&= (m_r d_\phi)((z,x),q)\exp(-2\pi i\rho_\Phi(\phi)(r^{-1}v))b_{r^{-1}v} \\
&= (m_r d_\phi)\exp(2\pi i(q+\beta(r^{-1}v,z)-\rho_\Phi(\phi)(r^{-1}v)))b_{r^{-1}v+x} \\
&= \exp(2\pi i(\rho_\Phi(\phi)(r^{-1}v+x)+q+\beta(r^{-1}v,z)-\rho_\Phi(\phi)(r^{-1}v)))b_{v+rx} \\
&= \exp(2\pi i(q+\rho_\Phi(\phi)(x)+\beta(r^{-1}v,z)+\rho_M(\lambda(\phi))(r^{-1}v,x)))b_{v+rx} \\
&= \exp(2\pi i(q+\rho_\Phi(\phi)(x)+\beta(v,r^{-J}z)+\beta(r^{-1}v,\psi^{-1}(\lambda(\phi))x)))b_{v+rx} \\
&= \exp(2\pi i(q+\rho_\Phi(\phi)(x)+\beta(v,r^{-J}z+r^{-J}\psi^{-1}(\lambda(\phi))x)))b_{v+rx} \\
&= ((r^{-J}z+r^{-J}\psi^{-1}(\lambda(\phi))x, rx), q+\rho_\Phi(\phi)(x))(b_v) \\
&= ((z,x),q)[d(r,\phi)](b_v).
\end{aligned}$$

Sei nun $y_e^N := ((z,x),q)[H_{e,e,e}]$. Dann ist

$$\begin{aligned}
y &= ((z,x),q)[\left(\begin{pmatrix} 1-e & e \\ -\epsilon^{-1}e & 1-e \end{pmatrix}, \begin{pmatrix} 0 & \psi(-\epsilon e) \\ & 0 \end{pmatrix}\right)] \\
&= \left(\begin{pmatrix} 1-e & e \\ -\epsilon^{-1}e & 1-e \end{pmatrix}\begin{pmatrix} z \\ x \end{pmatrix}, q+\rho_\Phi(\begin{pmatrix} 0 & \psi(-\epsilon e) \\ & 0 \end{pmatrix})(z,x)\right) \\
&= \left(((1-e)z+ex, -\epsilon^{-1}ez+(1-e)x), q-\beta(z,\epsilon ex)\right); \qquad (2)
\end{aligned}$$

in der oben definierten Darstellung von $\mathcal{E}(V)$ entspricht dies

$$y_e^N := b_v \mapsto \exp(2\pi i(q-\beta^N(z,\epsilon ex)+\beta^N(v,z)-\beta^N(v,ez)+\beta^N(v,ex)))\ b_{v+x-ex-\epsilon^{-1}ez}.$$

Da $V = V_0^N$ ist, werden wir alle anderen Fälle auf den Fall $N = 1$ zurückführen.

Ist $N = 1$ und $e = 1$, so lautet (2)

$$y_1^1 = b_v \mapsto \exp(2\pi i(q - \beta(z, \epsilon x) + \beta(v, x)))\ b_{v-\epsilon^{-1}z}.$$

Nun ist
$h_{1,1,1}((z,x),q)\ h_{1,1,1}^{-1}(b_v)$

$$\begin{aligned}
&= && h_{1,1,1}((z,x),q)|V|^{-\frac{1}{2}} \sum_{w' \in V} \exp(-2\pi i\beta(v,w'))\ b_{w'} \\
&= && h_{1,1,1}|V|^{-\frac{1}{2}} \sum_{w' \in V} \exp(2\pi i(q + \beta(w',z) - \beta(v,w')))\ b_{w'+x} \\
&= && |V|^{-1} \sum_{w \in V} \exp(2\pi i(q + \beta(w,x))) \\
& && \sum_{w' \in V} \exp(2\pi i(\beta(w',z) - \beta(v,w') + \beta(w,w')))\ b_w \\
&\overset{w \leftrightarrow w - \epsilon^{-1}z}{=} && |V|^{-1} \sum_{w \in V} \exp(2\pi i(q - \beta(\epsilon^{-1}z,x) + \beta(w,x))) \\
& && \sum_{w' \in V} \exp(2\pi i(\beta(w',z) + \beta(w-v,w') + \beta(-\epsilon^{-1}z,w')))\ b_{w-\epsilon^{-1}z} \\
&\overset{\epsilon^{-J} = \epsilon}{=} && |V|^{-1} \sum_{w \in V} \exp(2\pi i(q - \beta(z,\epsilon x) + \beta(w,x))) \\
& && \sum_{w' \in V} \exp(2\pi i(\beta(w-v,w') \underbrace{\beta(w',z) - \beta(z,\epsilon w')}_{=0 \text{ nach } (*)}))\ b_{w-\epsilon^{-1}z} \\
&= && |V|^{-1} \sum_{w \in V} \exp(2\pi i(q - \beta(z,\epsilon x) + \beta(w,x))) \underbrace{\sum_{w' \in V} \exp(2\pi i\beta(w-v,w'))}_{= \begin{cases} 0, & w \neq v \\ |V|, & w = v \end{cases}}\ b_{w-\epsilon^{-1}z} \\
&= && \exp(2\pi i(q - \beta(z,\epsilon x) + \beta(v,x)))\ b_{v-\epsilon^{-1}z} \\
&= && y(b_v)
\end{aligned}$$

Zu $(*)$: Es gilt
$\beta(z, \epsilon w')$

$$\begin{aligned}
&= \rho_M(\psi(1)(1 \otimes \epsilon))(z,w') \\
&= \rho_M(\psi(1^J\epsilon))(z,w') && \text{(da } \psi(r)(s \otimes t) = \psi(s^J rt) \text{ für alle } r,s,t \in R\text{)} \\
&= \rho_M(\tau(\psi(1)))(z,w') && \text{(da } \tau(\psi(r)) = \psi(r^J\epsilon) \text{ für alle } r,s,t \in R\text{)} \\
&= \rho_M(\psi(1))(w',z) \\
&= \beta(w',z).
\end{aligned}$$

Sei nun $e = \mathrm{diag}(1, 0, \ldots, 0)$.

Wir definieren einen $\mathbb{C}$-Vektorraumhomomorphismus

$$\mathrm{Ext} : \mathbb{C}V_0 \to V, \quad b_v \mapsto b_{(v,0,\ldots,0)}.$$

Mit Hilfe von Ext können wir dann y_e^N durch y_1^1 ausdrücken, da

$$\begin{aligned} y_e^N(b_v) &= \exp(2\pi i(q-\beta^N(z,\epsilon ex)+\beta^N(v,(1-e)z)+\beta^N(v,ex)))\, b_{v+x-ex-\epsilon^{-1}ez} \\ &= \exp(2\pi i(q-\beta(z_1,\epsilon x_1)+\beta(v_1,x_1)))\exp(2\pi i\beta^N((1-e)v,(1-e)z)) \\ &\quad \mathrm{Ext}(b_{v_1-\epsilon^{-1}z_1})b_{(1-e)v}b_{(1-e)x} \end{aligned} \tag{3}$$

Mit $c := \exp(2\pi i\beta((0,v_2,\ldots,v_N),(0,z_2,\ldots,z_N)))b_{(0,v_2,\ldots,v_N)}b_{(0,x_2,\ldots,x_N)}$ ergibt sich

$$y_e^N = c\cdot \mathrm{Ext}(y_1^1(b_{v_1})).$$

Dann gilt für $v=(v_1,\ldots,v_N)\in V$, dass

$$\begin{aligned} h_{e,e,e}(b_v) &= |eV|^{-\frac{1}{2}}\sum_{w\in eV}\exp(2\pi i\beta(w,ev))b_{(1-e)v+w} \\ &= |V_0|^{-\frac{1}{2}}\sum_{w\in V_0}\exp(2\pi i\beta(w,v_1))b_{(w,0,\ldots,0)}b_{(0,v_2,\ldots,v_N)} \\ &= \mathrm{Ext}(\tilde{h}_{1,1,1}(b_{v_1}))b_{(0,v_2,\ldots,v_N)} \end{aligned} \tag{4}$$

mit $\tilde{h}_{1,1,1}:\mathbb{C}V_0\to\mathbb{C}V_0$. Ebenso gilt $h_{e,e,e}^{-1}(b_v)=\mathrm{Ext}(\tilde{h}_{1,1,1}^{-1}(b_{v_1}))b_{(0,v_2,\ldots,v_N)}$.

Wir müssen also herausfinden, was unter der Operation von $\mathcal{E}(V)$ mit Produkten von Elementen von $\mathbb{C}V$ passiert. Wir stellen fest, dass

$$\begin{aligned} ((z,x),q)(b_vb_w)=((z,x),q)(b_{v+w}) &= \exp(2\pi i(q+\beta(v+w,z)))b_{v+w+x} \\ &= \exp(2\pi i(q+\beta(v,z)))b_{v+x}\exp(2\pi i\beta(w,z))b_w \\ &= ((z,x),q)(b_v)\exp(2\pi i\beta(w,z))b_w \end{aligned} \tag{5}$$

für $v,w\in V$.

Weiter beobachten wir, dass

$$\begin{aligned} ((z,x),q)(\mathrm{Ext}(b_{v_1})) &= \exp(2\pi i(q+\beta^N((v_1,0,\ldots,0),z)))b_{(v_1+x_1,x_2,\ldots,x_N)} \\ &= \exp(2\pi i(q+\beta(v_1,z_1)))\,\mathrm{Ext}(b_{v_1+x_1})b_{(0,x_2,\ldots,x_N)} \\ &= \mathrm{Ext}(((z_1,x_1),q)(b_{v_1}))b_{(0,x_2,\ldots,x_N)} \end{aligned} \tag{6}$$

Aus den Gleichungen (5) und (6) erhalten wir

$$\begin{aligned} ((z,x),q)h_{e,e,e}^{-1}(b_v) &= c\cdot((z,x),q)(\mathrm{Ext}(\tilde{h}_{1,1,1}^{-1}(b_{v_1}))) \\ &= c\cdot\mathrm{Ext}(((z_1,x_1),q)(\tilde{h}_{1,1,1}^{-1}(b_{v_1}))). \end{aligned} \tag{7}$$

Als nächstes stellt sich also die Frage, wie $h_{e,e,e}$ Produkte $b_vb_w\in\mathbb{C}V$ abbildet, wobei $v\in eV$ und $w\in(1-e)V$. Dazu ergibt sich

$$\begin{aligned} h_{e,e,e}(b_vb_w) &= h_{e,e,e}(b_{v+w}) \\ &= |V_0|^{-\frac{1}{2}}\sum_{w'\in eV}\exp(2\pi i\beta(w',e(v+w)))b_{(1-e)(v+w)+w'} \\ &= |V_0|^{-\frac{1}{2}}\sum_{w'\in eV}\exp(2\pi i\beta(w',ev))b_{(1-e)(v+w')}b_{(1-e)w} \\ &= h_{e,e,e}(b_v)b_{(1-e)w}. \end{aligned} \tag{8}$$

Außerdem hat die Verknüpfung $h_{e,e,e} \circ \mathrm{Ext}$ wegen (4) die nützliche Eigenschaft

$$h_{e,e,e}(\mathrm{Ext}(b_{v_1})) = \mathrm{Ext}(\tilde{h}_{1,1,1}(b_{v_1})).$$

Indem wir (7), (8) und (6.2) benutzen, erhalten wir

$$\begin{aligned} h_{e,e,e}((z,x),q)h_{e,e,e}^{-1}(b_v) &= c \cdot h_{e,e,e}(\mathrm{Ext}(((z_1,x_1),q)(\tilde{h}_{1,1,1}^{-1}(b_{v_1})))) \\ &= c \cdot \mathrm{Ext}(\tilde{h}_{1,1,1}((z_1,x_1),q)\tilde{h}_{1,1,1}^{-1}(b_{v_1})) \end{aligned}$$

und insgesamt

$$h_{e,e,e}((z,x),q)h_{e,e,e}^{-1}(b_v) = c \cdot \mathrm{Ext}(y(b_{v_1})).$$

Wegen Gleichung (6.2) ist damit nachgewiesen, dass die beiden Operationen übereinstimmen. □

6.3 Eine hinreichende Bedingung für die Endlichkeit von $\mathcal{C}(\rho)$

Folgerung 6.16. *Es sei $\rho = (V, \rho_M, \rho_\Phi, \beta)$ eine endliche Darstellung von $\mathcal{R}$. Ist $N \in \mathbb{N}$ und existiert ein selbstdualer isotroper Code $C \leq V^N$ vom Typ ρ, so gilt*

$$|\mathcal{C}(\rho)| \mid N \cdot |U(R,\Phi)|;$$

insbesondere ist dann $\mathcal{C}(\rho)$ endlich.

Beweis. Es sei p die im vorigen Satz definierte Abbildung. Bezeichnen wir mit $S(\rho) := \mathbb{C}^* \cdot \mathbb{I}_{|V|} \cap \mathcal{C}(\rho)$ die Skalarmatrizen von $\mathcal{C}(\rho)$, so ist $p : U(R,\Phi) \to \mathcal{C}(\rho)/S(\rho)$ ein Epimorphismus; es gilt also $\mathcal{C}(\rho)\big||U(R,\Phi)| \cdot |S(\rho)|$. Ist p der Gewichtszähler eines selbstdualen isotropen Codes der Länge N vom Typ ρ, so ist p homogen vom Grad N und invariant unter $\mathcal{C}(\rho)$; insbesondere gilt für $S := s \cdot \mathcal{I}_{|V|} \in S(\rho)$

$$p(x) = p[S](X) = p(sX) = s^N p(X).$$

Damit gilt $S(\rho) \leq \zeta_N \cdot \mathcal{I}_{|V|}$, wobei ζ_N eine primitive N-te Einheitswurzel ist. Es folgt $|S(\rho)|\big|N$ und daher $|\mathcal{C}(\rho)| \mid N \cdot |U(R,\Phi)|$. □

7 Die Invarianten der Clifford-Weil-Gruppe

Wie im vorigen Kapitel bezeichne stets $\mathcal{R} = (R, M, \psi, \Phi)$ einen Form-Ring, wobei R ein Matrixring sei über dem endlichen Körper K. Weiter sei $\rho = (V, \rho_M, \rho_\Phi, \beta)$ eine endliche Darstellung von $\mathcal{R}$. Wir nehmen weiterhin an, dass ein isotroper selbstdualer Code in ρ existiert.

In Abschnitt 7.1 wird gezeigt, dass die Gewichtszähler isotroper Codes in $N\rho$ den $\mathbb{C}$-Vektorraum der Invarianten von $P(\rho) \leq \mathcal{C}(\rho)$ erzeugen.

Darauf aufbauend wird in Abschnitt 7.2 gezeigt, dass wir ein Erzeugendensystem des $\mathbb{C}$-Vektorraums der Invarianten von $\mathcal{C}(\rho)$ erhalten, wenn wir von den isotropen Codes zusätzlich die Selbstdualität verlangen. Dies ist die Aussage des Hauptsatzes in dem Buch [5] für den Spezialfall $R = K^{n\times n}$.

Per Definition wird $\mathcal{C}(\rho)$ erzeugt von den Elementen von $P(\rho)$ sowie den h_{e,u_e,v_e} (siehe Bemerkung 3.10), wobei e die symmetrischen Idempotente von R bezüglich ^{J} durchläuft. In Abschnitt 4 haben wir bereits gesehen, dass die Matrizen h_{e,u_e,v_e} in Bezug auf Invarianzeigenschaften von p_C mit der Selbstdualität von C korrespondieren. Entsprechendes können wir auch in diesem Kapitel beobachten.

Aus dem Beweis des Hauptsatzes in 7.2 können wir im Körperfall außerdem folgern, dass ein einziges der h_{e,u_e,v_e}, nämlich $h_{e,e,e}$ mit $e = \mathrm{diag}(1, 0, \ldots, 0)$, genügt, um $\mathcal{C}(\rho)$ zu erzeugen.

7.1 Die Invarianten der Untergruppe $P(\rho) \leq \mathcal{C}(\rho)$

Abkürzend schreiben wir $p_C := \mathrm{fwe}(C) = \sum_{v\in C} b_v$. Weiter seien

$$D :=< d_\phi \mid \phi \in \Phi >,\ M :=< m_r \mid r \in R^* > \leq \mathcal{C}(\rho).$$

Dann ist $P(\rho) =< D, M >$.

Definition 7.1. *Sei $C \leq V$ ein Code. Wir definieren $\mu_C := \sum_{\{v\in V | Rv=C\}} b_v$.*

Man beachte, dass $\mu_C = 0$ ist, falls C nicht von einem einzigen Element von V erzeugt wird. Zwei Vektoren $v, w \neq 0 \in K^{n\times 1}$ können durch eine Element aus $\mathrm{GL}_n(K)$ ineinander überführt werden. Wird also C von einem einzigen Element von V erzeugt und ist $C \neq 0$, so folgt

Bemerkung 7.2. *Existiert ein $v \in V$ mit $C = Rv$, so ist $\mu_C = \sum_{r\in R^*} b_{rv}$.*

Mit Hilfe von Bemerkung 7.2 können wir nun den folgenden Satz beweisen.

Satz 7.3. *Die Familie $A := (\mu_C | C \leq V, C = Kv$ für ein $v \in V$ mit $\rho_\Phi(\phi)(v) = 0$ für alle $\phi \in \Phi)$ bildet eine Basis von $\mathrm{Inv}_{\mathbb{C}V}(P(\rho))$.*

Beweis. Sei zunächst $b = \sum_{j\in J} \beta_j b_{v_j} \in \mathrm{Inv}_{\mathbb{C}V}(P(\rho))$ mit einer geeigneten endlichen Indexmenge J. Da insbesondere $b \in \mathrm{Fix}_{\mathbb{C}V}(D)$, gilt

$$\sum_{j\in J} \beta_j b_{v_j} = \sum_{j\in J} \beta_j \exp(2\pi i \rho_\Phi(\phi)(v_j)) b_{v_j},$$

also $\rho_\Phi(\phi)(v_j) = 0$ für alle $j \in J$ mit $\beta_j \neq 0$. Ebenso folgt wegen $b \in \mathrm{Fix}_{\mathbb{C}V}(M)$, dass $\beta_j = \beta_{j'}$ ist, falls $v_j = kv_{j'}$ für ein $k \in K^*$. Also ergibt sich b als Linearkombination von Summen von K-Bahnen auf isotropen Vektoren, womit gezeigt ist, dass A ein Erzeugendensystem von $\mathbb{C}V^{P(\rho)}$ bildet. Die lineare Unabhängigkeit ergibt sich aus der Disjunktheit verschiedener solcher Bahnen. □

Folgerung 7.4. *Es ist* $\mathrm{Inv}_{\mathbb{C}V}(P(\rho)) =< p_C | C \leq V$ *isotroper Code in* $\rho >$.

Beweis.

" $\subseteq$ " Ist $\mu_C \in A$, so ist $\mu_C = p_C$.
Weiter ist dann C isotrop, da$\rho_\Phi(\phi)(rc) = \rho_\Phi(\phi[r])(c) = 0$ für alle $r \in R$.

" $\supseteq$ " Ist $C \leq V$ isotrop, so ist $p_C = \sum_{D \leq C,\ D = Kv \text{ für ein } v \in V} \mu_D$.

□

Mit Hilfe des allgemeinen Prinzips der Symmetrisierung erhalten wir aus diesem Ergebnis auch Erzeuger des $\mathbb{C}$-Vektorraums

$$\mathrm{Inv}_{P(\rho)}(\mathbb{C}[V]) = \{f \in \mathbb{C}\,[x_v \,|v \in V] \;\big|\; f(gx) = f(x) \text{ für alle } g \in P(\rho)\}.$$

Satz 7.5 (Prinzip der Symmetrisierung). *Seien G, H endliche Gruppen. Seien weiter W ein $\mathbb{C}(G \times H)$-Modul sowie M_G, M_H einfache $\mathbb{C}G$- bzw. $\mathbb{C}H$-Moduln. Bezeichnet man für einen Ring R und einen R-Modul M sowie einen einfachen R-Modul E mit*

$$M(E) := \sum_{U \leq_R M:\, U \cong_R E} U$$

die E-homogenen Komponenten von M, so gilt

$$(W(M_G))(M_H) = (W(M_H))(M_G).$$

Beweis. Da die Ringe $\mathbb{C}(G \times H)$ und $\mathbb{C}G \otimes_{\mathbb{C}} \mathbb{C}H$ isomorph sind, kann man auf W eine $\mathbb{C}G$-Modulstruktur definieren vermöge

$$xw := (x \otimes_{\mathbb{C}} 1_{\mathbb{C}H})w \text{ für alle } x \in \mathbb{C}G, w \in W.$$

Nach dem Struktursatz von Wedderburn ist $\mathbb{C}G \cong \oplus_{i=1}^{k} \mathbb{C}^{n_i \times n_i}$ mit $k \in \mathbb{N}, n_i \in \mathbb{N}$ für $i = 1, \ldots, k$. Als einfacher $\mathbb{C}G$-Linksmodul ist M_G isomorph zu $\mathbb{C}^{n_i \times 1}$ für ein $i \in \{1, \ldots, k\}$; weiter ist $W \cong_{\mathbb{C}G} \oplus_{j \in J} M_j^{n_j}$, wobei $J \subseteq \{1, \ldots, k\}, n_j \in \mathbb{N}$ für $j \in J$ und die $M_j, j \in J$, einfache $\mathbb{C}G$-Moduln sind.
Definiert man nun $e_i := \left(0_{\mathbb{C}^{n_1 \times n_1}}, \ldots, 0_{\mathbb{C}^{n_{i-1} \times n_{i-1}}}, E_{n_i}, 0_{\mathbb{C}^{n_{i+1} \times n_{i+1}}}, \ldots, 0_{\mathbb{C}^{n_k \times n_k}}\right)$, so ist offenbar

$$e_i W = M_i^{n_i}.$$

Weiter ist

$$e_i W(M_i) = \sum_{\substack{U \leq_{\mathbb{C}G} W \\ U \cong_{\mathbb{C}G} M_i}} e_i U = \sum_{\substack{U \leq_{\mathbb{C}G} W \\ U \cong_{\mathbb{C}G} M_i}} U = W(M_i),$$

weshalb in der Inklusionskette

$$W(M_i) = e_i W(M_i) \subseteq e_i W = M_i^{n_i} \subseteq W(M_i)$$

überall die Gleichheit gilt. Insgesamt ergibt sich

$$W(M_G) = e_i W.$$

Man beachte, dass das Idempotent e_i nicht von der Wahl des $\mathbb{C}G$-Moduls W abhängt.
Nun vertauschen die oben definierten Operationen von G bzw. H auf W; jedes $h \in H$

induziert also einen Isomorphismus von $\mathbb{C}G$-Moduln. Daher ist $W(M_G)$ ein $\mathbb{C}H$-Modul. Sei nun $e_j \in \mathbb{C}H$ ein Idempotent mit $W(M_G)(M_H) = e_j e_i W \leq \mathbb{C}H$. Dann ist

$$\begin{aligned} W(M_G)(M_H) &= e_j e_i W = (1_{\mathbb{C}G} \otimes_{\mathbb{C}} e_j)(e_i \otimes 1_{\mathbb{C}H})W = (e_i \otimes 1_{\mathbb{C}H})(1_{\mathbb{C}G} \otimes_{\mathbb{C}} e_j)W \\ &= e_i e_j W = W(M_H)(M_G). \end{aligned}$$

□

Folgerung 7.6. *Es ist*

$$\mathrm{Inv}_{\mathbb{C}V}(P(\rho)) =< \mathrm{cwe}(C) \mid C \leq V^N \textit{ isotroper Code in } N\rho >_{\mathbb{C}-VR} .$$

Beweis. Die symmetrische Gruppe $S_N =: H$ operiert trivial auf $\mathbb{C} =: M_H$ und auf $\mathbb{C}V^N =: W$ durch

$$\pi(b_{(v_1,\ldots,v_N)}) = b_{(v_{\pi^{-1}(1)},\ldots,v_{\pi^{-1}(N)})} \text{ für alle } v = (v_1,\ldots,v_N) \in V^N \text{ und } \pi \in S_N;$$

durch lineare Fortsetzung dieser Operationen wird $\mathbb{C}V^N$ zu einem $\mathbb{C}S_N$-Modul und $\mathbb{C}$ zu einem einfachen $\mathbb{C}S_N$-Modul. Die Gruppe $P(N\rho)$ operiert ebenfalls auf W durch

$$m_r(b_{(v_1,\ldots,v_N)}) = b_{(rv_1,\ldots,rv_N)}, \quad d_\phi(b_{(v_1,\ldots,v_N)}) = \prod_{j=1}^{N} \exp(2\pi i \rho_\Phi(\phi)(v_j)) b_{(v_1,\ldots,v_N)}$$

für $(v_1,\ldots,v_N) \in V^N$. Diese diagonale Operation von $P(N\rho)$ auf W vertauscht mit der Operation von S_N auf W, so dass W auch eine $\mathbb{C}(P(N\rho) \times S_N)$- Struktur erhält.
Ist O ein Vertretersystem der Bahnen von S_N auf V^N, so ist $(\sum_{\pi \in S_N} \pi(b_v) \mid v \in O)$ eine Basis des $\mathbb{C}$-Vektorraums $W(M_H)$. Denn ist $U \leq_{\mathbb{C}S_N} \mathbb{C}V^N$ mit $U \cong_{\mathbb{C}S_N} \mathbb{C}$, so existiert wegen $\mathbb{C} =< 1 >$ als $\mathbb{C}S_N$-Modul ein $x \in \mathbb{C}V^N$ mit $U = \{cx \mid c \in \mathbb{C}\}$; da die Operation von S_N auf $\mathbb{C}$ trivial definiert war, gilt $\pi(x) = x$. Daher sind alle Elemente von U und damit auch von W im Erzeugnis von $\sum_{\pi \in S_N} \pi(b_v \mid v \in O)$ enthalten. □

7.2 Der Hauptsatz

Lemma 7.7. *Es seien $e := \mathrm{diag}(1,0,\ldots,0) \in R$ und $h := h_{e,e,e} \in \mathbb{C}V$; nach den Bemerkungen 4.16 und 4.15 können wir annehmen, dass $V = V_0^n$ für einen K-Vektorraum V_0. Weiter sei $X_P := \frac{1}{|P(\rho)|} \sum_{g \in P(\rho)} g \in \mathrm{End}(\mathrm{Inv}_{\mathbb{C}V}(\mathcal{C}(\rho)))$. Nach Bemerkung 4.17 erhalten wir jeden isotropen Code $C \leq V$ durch $C = C_0(m)$ mit $C_0 \leq V_0$. Ist $C \leq V_0$ isotrop, so gilt*

$$(X_p h)(p_{C(m)}) = \sum_{C' \leq C^\perp, C' =< C, x >_{R_0} \textit{ für ein } x \in V_0} n_{C'} p_{C'(m)},$$

wobei $n_C = 1$ genau dann gilt, wenn $C = C^\perp$.

Beweis. Es ist

$$\begin{aligned} h(p_{C(m)}) &= \frac{|eC(m)|}{|eV|^{\frac{1}{2}}} \sum_{c \in (1-e)C(m)} \sum_{w \in eC(m)^{\perp,\beta_e}} b_{w+c} = \frac{|C|}{|V_0|^{\frac{1}{2}}} \sum_{c \in C(m-1)} \sum_{w \in C^\perp} b_{w+c} \\ &= |C^\perp/C|^{-\frac{1}{2}} p_{C^\perp \oplus C(m-1)}. \end{aligned}$$

Damit erhalten wir

$$(X_P\ h)(p_{C(m)}) = |C^\perp/C|^{-\frac{1}{2}}|P(\rho)|^{-1} \sum_{\substack{u\in \mathrm{GL}_m(K),\\ \phi\in\Phi}} \sum_{\substack{c_1\in C^\perp\\ c_2,\ldots,c_m\in C}} \exp(2\pi i \rho_{\Phi_0}(\phi_1)(c_1)) e_{u\cdot(c_1,\ldots,c_m)},$$

denn ist $\phi = \begin{pmatrix} \phi_1 & & m_{ij} \\ & \ddots & \\ & & \phi_m \end{pmatrix} \in \Phi = \Phi_0^{(m)}$, so folgt wegen der Isotropie von C

$$\rho_\Phi(\phi)(c_1,\ldots,c_m) = \sum_{i=1}^m \rho_{\Phi_0}(\phi_i)(c_i) + \sum_{i<j} \rho_{M_0}(m_{ij})(c_i,c_j) = \rho_{\Phi_0}(\phi_1)(c_1).$$

Nun ist $\sum_{\phi\in\Phi} \exp(2\pi i \rho_{\Phi_0}(\phi_1)(c_1)) = \frac{|\Phi|}{|\Phi_0|} \sum_{\phi_1\in\Phi_0} \exp(2\pi i \rho_{\Phi_0}(\phi_1)(c_1))$. Da weiter $|P(\rho)| = |\mathrm{GL}_m(K)||\Phi|$, erhalten wir mit $a := |C^\perp/C|^{-\frac{1}{2}}|\mathrm{GL}_m(K)|^{-1}|\Phi_0|^{-1}$

$$(X_P\ h)(p_{C(m)}) = a \sum_{u\in\mathrm{GL}_m(K)} \sum_{\substack{c_1\in C^\perp\\ c_2,\ldots,c_m\in C}} \left(\sum_{\phi_1\in\Phi_0} \exp(2\pi i \rho_{\Phi_0}(\phi_1)(c_1)) \right) e_{u\cdot(c_1,\ldots,c_m)^t}.$$

Definieren wir nun für $v \in V_0$ den Charakter $\chi_v :\ \Phi_0 \to \mathbb{C}^*,\ \phi \mapsto \exp(2\pi i \rho_{\Phi_0}(\phi)(v))$, so gilt $\chi_v = 1$ genau dann, wenn v isotrop ist. Mit den Orthogonalitätsrelationen ergibt sich

$$(X_P\ h)(p_{C(m)}) = |C^\perp/C|^{-\frac{1}{2}}|\mathrm{GL}_m(K)|^{-1} \sum_{\substack{c_1\in C^\perp\\ c_1\text{isotrop}}} \sum_{c_2,\ldots,c_m\in C} \sum_{u\in\mathrm{GL}_m(K)} e_{u\cdot(c_1,\ldots,c_m)^{tr}}.$$

Sei nun O ein Vertretersystem von $C^\perp/C$ und $O' \subset O$ bestehe aus den isotropen Restklassen. Wir beobachten, dass

$$\sum_{\substack{c_1\in C^\perp\\ c_1\text{isotrop}}} e_{u\cdot(c_1,\ldots,c_m)^{tr}} = \sum_{c_1\in O'} \sum_{x\in C} e_{u\cdot(c_1,0,\ldots,0)^{tr}} e_{u\cdot(x,c_2,\ldots,c_m)^{tr}}.$$

In obiger Summation über $\mathrm{GL}_m(K)$ können wir bei $e_{u\cdot(x,c_2,\ldots,c_m)^{tr}}$ auf die Multiplikation mit u verzichten, so dass sich $(X_P\ h)(p_{C(m)})$ zu

$$\begin{aligned} & |C^\perp/C|^{-\frac{1}{2}}|\mathrm{GL}_m(K)|^{-1} \sum_{c_1\in O'} \sum_{x,c_2,\ldots,c_m\in C} \sum_{u\in\mathrm{GL}_m(K)} e_{u\cdot(c_1,0,\ldots,0)^{tr}} e_{(x,c_2,\ldots,c_m)^{tr}} \\ = \ & |C^\perp/C|^{-\frac{1}{2}}|\mathrm{GL}_m(K)|^{-1} \sum_{c_1\in O'} \sum_{u\in\mathrm{GL}_m(K)} e_{u\cdot(c_1,0,\ldots,0)^{tr}} p_{C(m)} \end{aligned}$$

ergibt.

Nun wollen wir die Koeffizienten $n_{C'} \in \mathbb{C}$ berechnen. Es ist

$$\begin{aligned} (X_P\ h)(p_{C(m)}) &= \frac{|\mathrm{GL}_m(K)|^{-1}}{|C^\perp/C|^{1/2}} \sum_{c_1\in O'} \sum_{u\in\mathrm{GL}_m(K)} e_{u\cdot(c_1,0,\ldots,0)^{tr}} p_{C(m)} \\ &= \left(\underbrace{\frac{1}{|C^\perp/C|^{1/2}}\mu_0 + \frac{|\mathrm{GL}_m(K)|^{-1}}{|C^\perp/C|^{1/2}} \sum_{0\neq v\in O'} \mu_{<(v,0,\ldots,0)^{tr}>_{R^{m\times m}}}}_{=:\nu} \right) p_{C(m)} \end{aligned}$$

Wir wollen nun über $\mathcal{D} := \{D \leq V \mid D =< (v,0,\ldots,0)^{tr} >$ für ein isotropes $v \in V_0, v \neq 0\}$ summieren und erhalten

$$\nu = \underbrace{\frac{1}{|C^\perp/C|^{1/2}}\mu_0}_{=:n_0'} + \sum_{D\in\mathcal{D}} \underbrace{\frac{|\operatorname{GL}_m(K)|^{-1}}{|C^\perp/C|^{1/2}} \sharp\{c \in O' \mid <(c,0,\ldots,0)>= D\}}_{=:n_D'} \mu_D.$$

Wegen $\mu_0 = p_0$ und $p_D - p_0 = \mu_D$ für $D \leq V,\ D \neq \{0\}$ erhalten wir

$$\nu = \underbrace{\left(\frac{1}{|C^\perp/C|^{1/2}} - \sum_{D\in\mathcal{D}} n_D'\right)}_{=n_C} p_0 + \sum_{D\in\mathcal{D}} n_D' p_D$$

Da $\sum_{D\in\mathcal{D}} n_D' = \frac{|\operatorname{GL}_m(K)|^{-1}}{|C^\perp/C|^{1/2}}\ (|O'|-1)$, können wir n_C berechnen als

$$n_C = \frac{1}{|C^\perp/C|^{1/2}}\left(1 - \frac{|O'|-1}{|\operatorname{GL}_m(K)|}\right),$$

das heißt,

$$n_C = 1 \Leftrightarrow \underbrace{1 - \frac{|O'|-1}{|\operatorname{GL}_m(K)|}}_{\leq 1} = \underbrace{|C^\perp/C|^{1/2}}_{\geq 1} \Leftrightarrow C = C^\perp.$$

□

Lemma 7.8. *Es seien W ein endlich-dimensionaler $\mathbb{C}$-Vektorraum und $(P,\leq)$ eine endliche partiell geordnete Menge, so dass durch $E := (w_p \mid p \in P)$ ein Erzeugendensystem von W gegeben ist. Weiter sei A ein Endomorphismus von W mit der Eigenschaft, dass für $p,q \in P$ Elemente $c_{pq} \in \mathbb{C}$ gewählt werden können mit*

$$A(w_p) = \sum_{p\leq q} c_{pq} w_q \qquad (*)$$

Gilt mit dieser Wahl nun $c_{pp} = 1$ genau für die maximalen Elemente p in $(P,\leq)$, so ist

$$Fix_W(A) = \{w \in W \mid A(w) = w\} =< w_p \in E \mid p \text{ maximal in } (P,\leq) >_{\mathbb{C}-VR}.$$

Beweis. Wir können oBdA annehmen, dass E linear unabhängig ist, denn andernfalls gilt die Aussage des Lemmas für eine linear unabhängige Teilfamilie von E: Sei zunächst $\leq'$ eine lineare Fortsetzung von $\leq$ zu einer Totalordnung auf P, so dass für jedes maximale Element p und jedes nicht maximale Element q von $(P,\leq)$ gilt, dass $q \leq' p$. Ist dann $\sum_{p\in P} a_p w_p = 0$ mit $a_p \in \mathbb{C},\ p \in P$, so existiert wegen der Endlichkeit von P ein bezüglich $\leq'$ minimales Element $p_0 \in P$ mit der Eigenschaft, dass $a_{p_0} \neq 0$. Es ist $< w_p \mid p \in P \setminus \{p_0\} >=< w_p \mid p \in P >$. Ist p_0 maximal bezüglich $\leq$, so ist p_0 nach Konstruktion von $\leq'$ Linearkombination anderer maximaler Elemente von P bezüglich $\leq$, das heißt, es ist

$$< w_p \mid p \text{ maximal in } (P,\leq) >=< w_p \mid p \neq p_0, p \text{ maximal in } \in (P,\leq) > .$$

Streichen wir auf diese Weise weitere Elemente von E, so erhalten wir nach endlich vielen Schritten eine linear unabhängige Teilfamilie $< w_p \mid p \in P' >,\ P' \subset P$, so dass $A(w_p) = \sum_{p\leq q} c_{pq} w_q$ für alle $p \in P \cap P'$.

Wegen $(*)$ sind die maximalen Elemente von $(P, \leq)$ fix unter A. Für das charakteristische Polynom μ_A von A gilt wegen $(*)$: $\mu_A(t) = \prod_{p \in P}(t - c_{pp})$, das heißt, in der Ungleichungskette

$$\sharp\{p \in P \mid c_{pp} = 1\} = \dim < w_p \mid p \text{ maximal in } (P, \leq) > \leq dim(E_1(A)) = Fix_W(A)$$

steht auf der linken Seite die algebraische Vielfachheit $\nu_{alg}(1)$ und auf der rechten Seite die geometrische Vielfachheit $\nu_{geo}(1)$ des Eigenwerts 1 von A. Wegen $\nu_{geo}(1) \leq \nu_{alg}(1)$ gilt dort überall die Gleichheit, womit die Behauptung bewiesen ist. □

Lemma 7.9. *Es sei $e = \mathrm{diag}(1, 0, \ldots, 0)$. Dann ist*

$$\mathrm{Fix}_{\mathbb{C}V^N}(< R^* \ltimes \Phi, h_{e,e,e} >) =< \mathrm{fwe}(C) \;\big|\; C = C^\perp \textit{ isotroper Code in } N\rho >_{\mathbb{C}-VR} .$$

Beweis. Wir benutzen Lemma 7.8 mit $W = \mathbb{C}V$ und

$$P = \{C \leq V^N \mid C \text{ isotroper Code in } N\rho\};$$

nach Folgerung 7.6 ist $(w_p \mid p \in P)$ ein Erzeugendensystem von W. Die Inklusion definiert eine Halbordnung auf P. Die maximalen Elemente bezüglich dieser Halbordnung sind genau die isotropen selbstdualen Codes in $N\rho$, da der Witt-Index als Dimension eines maximalen isotropen Teilraums von V^N wohldefiniert ist - vergleiche [4]. □

Daraus erhalten wir sofort als Folgerung

Folgerung 7.10. *Es gilt*

$$\mathrm{Fix}_{\mathbb{C}V}(\mathcal{C}(\rho)) =< \mathrm{fwe}(C) \;\big|\; C = C^\perp \textit{ isotroper Code in } \rho >_{\mathbb{C}-VR} .$$

Durch Symmetrisieren erhalten wir den Hauptsatz.

Satz 7.11 (Hauptsatz). *Es gilt*

$$\mathrm{Inv}(\mathcal{C}(\rho)) =< \mathrm{cwe}(C) \;\big|\; C = C^\perp \textit{ isotroper Code in } \rho >_{\mathbb{C}-VR} .$$

Aus Lemma 7.9 und dem Hauptsatz ergeben sich Konsequenzen für die Erzeuger von $\mathcal{C}(\rho)$; es gilt nämlich

Folgerung 7.12. *Es seien $R = K^{n\times n}$ mit einem endlichen Körper K, $\mathcal{R}$ ein Form-Ring über R und ρ eine Darstellung von $\mathcal{R}$. Weiter sei $e := \mathrm{diag}(1, 0, \ldots, 0) \in K^{n\times n}$. Dann gilt*

$$\mathcal{C}(\rho) =< m_r, d_\phi, h_{e,e,e} \;\big|\; r \in R^*, \phi \in \Phi > .$$

Beweis. Es sei $\mathcal{G} :=< R^* \ltimes \Phi, h_{e,e,e} >\leq \mathcal{C}(\rho)$. Aus Lemma 7.9 und dem Hauptsatz erhalten wir durch Symmetrisieren, dass

$$\mathrm{Inv}(\mathcal{G}) = \mathrm{Inv}(\mathcal{C}(\rho)).$$

Nach Satz 2.10 ist daher $|\mathcal{G}| = |\mathcal{C}(\rho)|$, also $\mathcal{G} = \mathcal{C}(\rho)$. □

8 Ein Beispiel: Codes über $\mathbb{F}_4 \oplus \mathbb{F}_4 u$

Wir betrachten Codes über dem nichtkommutativen Ring $R := \mathbb{F}_4 \oplus \mathbb{F}_4 u$, wobei $u^2 = 0$ und $ua = a^2 u$ für alle $a \in \mathbb{F}_4$, das heißt, es gilt

$$(a' + b'u)(a + bu) = a'a + (a'b + b'a^2)u$$

für alle $a, b, a', b' \in \mathbb{F}_4$. Solche Codes wurden zum Beispiel in [1] im Zusammenhang mit Quaternionengittern betrachtet. Auf R ist eine Involution gegeben durch $\overline{a + bu} = a - bu$, und man erhält ein Skalarprodukt $(\ ,\ )$ auf $R \times R$ durch

$$((a' + b'u), (a + bu)) = a'a + (b'a^2 - ab')u.$$

Die bezüglich $(\ ,\ )$ selbstdualen Codes in R^N wollen wir nun in der Sprache der Form-Ringe und ihrer Darstellungen ausdrücken.

Dabei gehen wir von der konkreteren Sichtweise der Darstellungen aus.

Wir definieren einen Form-Ring $\mathcal{R} = (R, M, \psi, \Phi)$ wie folgt. Es sei $m_0 : R \times R \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ die Bilinearform mit

$$m_0(a + bu, a' + b'u) := \frac{1}{2} \operatorname{Tr}_{\mathbb{F}_4 \big| \mathbb{F}_2}(ab' - a'b).$$

Dann erhalten wir einen $R \otimes R$-Rechtsmodul M durch $M := m_0(1 \otimes R) \leq \mathrm{Bil}(R, \mathbb{Q}/\mathbb{Z})$ mit der Modulstruktur

$$m_0(r_1 \otimes r_2)(x, y) := m_0(r_1 x, r_2 y).$$

Eine Involution $\tau : M \to M$ ist dann gegeben durch $\tau(m)(x, y) := m(y, x)$. Durch $\psi : R_R \to M_{1 \otimes R},\ 1 \mapsto m_0$ wird ein R-Modulisomorphismus definiert. Weiter ist $\Phi := \{\!\{M\}\!\} \leq \mathrm{Quad}_0(R, \mathbb{Q}/\mathbb{Z})$ ein R-qModul, wobei $\{\!\{m\}\!\}(x) := m(x, x)$. Dadurch ist $\lambda : \Phi \to M$ eindeutig bestimmt als $\lambda(\{\!\{m\}\!\}) = m + \tau(m)$.

Die Identität ist dann eine Darstellung von $\mathcal{R}$.

Es sei $m_\omega \leq \mathrm{GL}_{16}(\mathbb{C})$ die Matrix der Rechtsmultiplikation mit ω auf R. Dann operiert $S :=< m_\omega >$ auf $\mathbb{C}R$ durch Permutation der Basisvektoren mit sechs Bahnen; ein Vertretersystem dieser Operation ist gegeben durch $Rep := \{0, 1, u, 1 + u, \omega + u, \omega^2 + u\}$. Da die Operationen von S und $\mathcal{C}(\rho)$ miteinander vertauschen, erhalten wir durch Einschränkung eine Operation von $\mathcal{C}(\rho)$ auf $\mathrm{Fix}_{\mathbb{C}^{16}}(S)$. Dies induziert eine Darstellung $\Delta : \mathcal{C}(\rho) \to \mathrm{GL}_6(\mathbb{C})$ von $\mathcal{C}(\rho)$. Definieren wir nun auf natürliche Weise eine Abbildung

$$\mathrm{Sym}_{Rep} : \mathbb{C}[x_r \mid r \in R] \to \mathbb{C}[x_r \mid r \in Rep],$$

so folgt aus Satz 7.5, dass

$$\mathrm{Inv}(\Delta(\mathcal{C}(\rho))) = \mathrm{Sym}_{Rep}(\mathrm{Inv}(\mathcal{C}(\rho))).$$

Setzen wir $\mathcal{C}^6(\rho) := \Delta(\mathcal{C}(\rho))$, so ergibt sich die Molienreihe von $\mathcal{C}^6(\rho)$ zu

$$\frac{1 + t^5 + t^8 + t^{13}}{(1 - t)(1 - t^2)^2(1 - t^4)^2(1 - t^6)}.$$

Es gibt eine Hironaka-Zerlegung von $\mathrm{Inv}_{\mathbb{C}[x_r \mid r \in Rep]}$ durch Gewichtszähler von Codes des Typs ρ. Die Gewichtszähler wurden mit Hilfe von MAGMA ([2]) ermittelt. Addition und Multiplikation in $\mathbb{F}_4 \oplus \mathbb{F}_4 u$ können als Abbildungen von $\mathbb{F}_4 \oplus \mathbb{F}_4 u \times \mathbb{F}_4 \oplus \mathbb{F}_4 u$ in sich selbst aufgefasst und so in MAGMA implementiert werden; auf diese Weise lässt sich der

Gewichtszähler aus einer vollständigen Liste der Codeworte ermitteln. Die Hironaka-Zerlegung ist nun

$$\mathrm{Inv}_{\mathbb{C}[x_r \mid r \in Rep]}(\mathcal{C}^6(\rho)) = \frac{1, C_5, C_8, C_5 \oplus C_8}{C_1, V_2, C_2, V_4, C_4, V_6}.$$

Hierbei sei für $N \in 2\mathbb{N}$

$$V_N :=< \mathbf{1}, (0, u, 0, \ldots, 0, u), (0, 0, u, 0, \ldots, 0, u), \ldots, (0, \ldots, 0, u, u) >,$$

und weiter $C_1 :=< (u) >$, $C_2 :=< (1 + u, \omega + u) >$, $C_4 :=< (1, \omega, \omega + u, \omega + \omega u), (0, u, 0, u), (0, 0, u, u) >$ sowie $C_5 :=< (1, 1, 1, 1, 0), (0, 1, \omega, \omega^2, 1), (u, u, 0, 0, u) >$. Der Code C_8 hat die Erzeugermatrix $(I_4|A)$, wobei

$$A = \begin{pmatrix} \omega u & 1 & \omega + \omega u & \omega^2 \\ \omega u & 1 + u & \omega^2 + \omega u & \omega + u \\ \omega u & 1 + \omega u & 1 & 1 \\ 1 + \omega u & \omega u & 0 & 0 \end{pmatrix}.$$

9 Extremale Codes vom Typ 4_I^E und 4_{II}^E

9.1 Bestimmung extremaler Gewichtszähler

Ziel ist die Bestimmung des maximal möglichen Minimalgewichts $d(N)$ von Codes der Länge N vom Typ $\rho(4_I^E)$ bzw. $\rho(4_{II}^E)$. Die Gewichtszähler solcher Codes sind Invarianten von $\mathcal{C}(\rho)$ mit $\rho = \rho(4_I^E)$ bzw. $\rho = \rho(4_{II}^E)$, die einigen zusätzlichen Bedingungen genügen. Ein Teil dieser Bedingungen ist derart, dass die Invarianten, welche diesen Bedingungen genügen, einen $\mathbb{Z}$-Teilmodul von $\mathrm{Inv}_{\mathbb{C}[x_v \mid v\in\mathbb{F}_4]}(\mathcal{C}(\rho))$ bilden. Dass diese Bedingungen erfüllt sind, lässt sich a priori sicherstellen.

Eine weitere Bedingung an die Gewichtszähler, die Nichtnegativität der Koeffizienten, lässt sich mit Hilfe linearer Programmierung prüfen. Gewichtszähler werden hier mit ganzzahligen Punkten in Polyedern identifiziert.

Schließlich liefert die Dimension des $\mathbb{F}_2$-rationalen Untercodes eine weitere Bedingung an die so ermittelten möglichen Gewichtszähler.

9.1.1 Einige Bedingungen a priori

Ist $C \leq \mathbb{F}_4^N$ ein Euklidisch selbstdualer Code mit Minimalabstand $d(C) \geq d$, so gilt $x^d \mid \mathrm{cwe}(C)(1,x,x,x) - 1$. Wir bestimmen also eine Basis des $\mathbb{Q}$-Vektorraums

$$\mathcal{T}_{N,\rho}(d) := \{p \in \mathrm{Inv}_{\mathbb{C}[x_v \mid v\in\mathbb{F}_4]}(\mathcal{C}(\rho)) \;\big|\; x^d \mid p(1,x,x,x)-1\} \leq \mathrm{Inv}_{\mathbb{C}[x_v \mid v\in\mathbb{F}_4]}(\mathcal{C}(\rho))_N,$$

der alle vollständigen Gewichtszähler selbstdualer isotroper Codes C in $N\rho$ mit Minimalgewicht $d(C) \geq d$ enthält.

Es gilt also

$$\mathrm{cwe}(C)(x_0,x_1,x_\omega,x_{\omega^2}) \in \mathbb{Z}[x_0,x_1,x_\omega,x_{\omega^2}] \cap \mathcal{T}_{N,\rho}(d).$$

Ist $\rho = \rho(4_I^E)$, so erhalten wir durch den Gewichtszähler $\mathrm{cwe}(S(C))$ des Schattens S eines möglichen Codes C in $N\rho$ mit Minimalgewicht $d(C) \geq d$ weitere Bedingungen. Gemäß Abschnitt 5.3 existiert ein Ringhomomorphismus $T_S : \mathbb{C}[x_v \mid v \in \mathbb{F}_4] \to \mathbb{C}[x_v \mid v \in \mathbb{F}_4]$, welcher $\mathrm{cwe}(C)$ auf $\mathrm{cwe}(S(C))$ abbildet. Daraus erhalten wir

$$T_S(\mathrm{cwe}(C)) \in \mathbb{Z}[x_0,x_1,x_\omega,x_{\omega^2}] \cap T_S(\mathcal{T}_{N,\rho}(d)).$$

Man beachte, dass wir uns auf die Bedingungen beschränken können, welche durch $S_1(C)$ gegeben sind. Denn gemäß Bemerkung 5.9 ist $T_{S_{r^2}} = m_r \circ T_{S_1}$, falls $r \in \mathbb{F}_4^*$ ist und $m_r \in \mathbb{F}_2^{4\times 4}$ die Linksmultiplikation mit r beschreibt. Die zu T_{S_1} gehörige Matrix ist gegeben durch

$$M(T_{S_1}) = \begin{pmatrix} 1 & -1 & -i & -i \\ 1 & -1 & i & i \\ 1 & 1 & i & -i \\ 1 & 1 & -i & i \end{pmatrix}.$$

Es sei $(t_1,\ldots,t_k)$ mit $t_i \in \mathbb{Z}[x_0,x_1,x_\omega,x_{\omega^2}]_N,\ i = 1,\ldots,k$ eine $\mathbb{Q}$-Basis von $\mathcal{T}_{N,\rho}(d)$. Da T_{S_1} ein Ringhomomorphismus ist, ist dann $(T_{S_1}(t_1),\ldots,T_{S_1}(t_k))$ eine Basis von $T_{S_1}(\mathcal{T}_{N,\rho}(d))$. Um die jeweiligen Koeffizienten unterscheiden zu können, schreiben wir das Tupel $(t_i, T_{S_1}(t_i))$ als $t_i(X) + T_{S_1}(t_i)(Y) \in \mathbb{Q}[x_0,\ldots,x_{\omega^2},y_0,\ldots,y_{\omega^2}]$ für $i = 1,\ldots,k$. Entsprechend sei

$$\mathcal{TS}_{N,\rho}(d) :=< p(x) + T_{S_1}(p)(y) \mid p \in \mathcal{T}_{N,\rho}(d) > .$$

Ist C ein Code der Länge N mit Minimalgewicht $d(C) \geq d$, so gilt also

$$(\mathrm{cwe}(C)(X), \mathrm{cwe}(S_1(C))(Y)) \in \mathcal{TS}_{N,\rho}(d) \cap \mathbb{Z}[x_0, \ldots, x_{\omega^2}, y_0, \ldots, y_{\omega^2}].$$

Wir wollen eine Ganzheitsbasis von $\mathcal{T}_{N,\rho}(d)$ bzw. von $\mathcal{TS}_{N,\rho}(d)$ bestimmen, um die ganzzahligen Polynome in $\mathcal{T}_{N,\rho}(d)$ leichter ermitteln zu können. Dazu benötigen wir

Lemma 9.1. *Es sei V der $\mathbb{Q}$-Vektorraum, welcher erzeugt wird von den Spalten von $A \in \mathbb{Q}^{n\times k},\ k \leq n$. Ist $c \in \mathbb{N}$ mit $cA \in \mathbb{Z}^{n\times k}$, so existieren nach dem Elementarteileralgorithmus eine Permutationsmatrix P, eine Matrix*

$$D = \begin{pmatrix} d_1 & 0 & \ldots & 0 \\ 0 & d_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \ldots & 0 & d_k \\ 0 & \ldots & & 0 \\ \vdots & & & \vdots \\ 0 & \ldots & & 0 \end{pmatrix} \in \mathbb{Z}^{n\times k}$$

sowie $Q \in \mathrm{GL}_k(\mathbb{Z})$ mit $cA = PDQ$. Wir definieren eine Matrix $\widetilde{D} := \mathrm{diag}(\widetilde{d_1}, \ldots, \widetilde{d_k})$ durch

$$\widetilde{d_i} := \begin{cases} d_i^{-1}, & d_i \neq 0 \\ 0, & d_i = 0. \end{cases}$$

Eine Ganzheitsbasis von V ist dann gegeben durch die Spalten von $I(A) := cAQ^{-1}\widetilde{D}$.

Beweis. Es seien $\lambda_1, \ldots, \lambda_k \in \mathbb{Q}$, so dass $A\ (\lambda_1, \ldots, \lambda_k)^t \in \mathbb{Z}^k$. Dann ist $(\lambda_1, \ldots, \lambda_k)^t$ eine $\mathbb{Z}$-Linearkombination der Spalten von $cQ^{-1}\widetilde{D}$. □

Zur Bestimmung einer Ganzheitsbasis wenden wir Lemma 9.1 auf die Koeffizientenmatrix $A \in \mathbb{Q}^{n\times k},\ k \leq n$, einer $\mathbb{Q}$-Basis von $\mathcal{T}_{N,\rho}(d)$ bzw. von $\mathcal{TS}_{N,\rho}(d)$ an.

Ist C ein Code vom Typ $\rho(4_I^E)$ oder $\rho(4_{II}^E)$, so sind die Monomkoeffizienten von $\mathrm{cwe}(C)$ bei Monomen der Form $x_0^a x_1^b x_\omega^b x_{\omega^2}^b, a \in \mathbb{N}_0, b \in \mathbb{N}$, durch drei teilbar, da C ein $\mathbb{F}_4$-Vektorraum ist. Es sei $\widetilde{\mathcal{T}}_{N,\rho}(d)$ der $\mathbb{Z}$-Untermodul von $\mathcal{T}_{N,\rho}(d)$, welcher die Polynome enthält, die dieser Bedingung genügen. Weiter seien mit $i_1, \ldots, i_n$ die Indizes der Zeilen von A bezeichnet, welche für Monome der Form $x_0^a x_1^b x_\omega^b x_{\omega^2}^b$ stehen. Wir definieren eine Matrix $B := \mathrm{diag}(b_1, \ldots, b_n)$ durch

$$b_i := \begin{cases} \frac{1}{3}, & i \in \{i_1, \ldots, i_n\}, \\ 0, & \text{sonst.} \end{cases}$$

Ist dann $\widetilde{A} := BA$, so bilden nach Lemma 9.1 die Spalten von $I(\widetilde{A})$ eine Ganzheitsbasis von $\widetilde{\mathcal{T}}_{N,\rho}(d)$.

9.1.2 Nichtnegativität der Koeffizienten

Ist $C \leq \mathbb{F}_4^N$ ein Euklidisch selbstdualer Code, so haben $\mathrm{cwe}(C)$ und $\mathrm{cwe}(S_\phi(C))$ natürlich nichtnegative Koeffizienten. Weiter ist in $\mathrm{cwe}(C)$ der Koeffizient bei den Monomen x_0^N sowie x_1^N gleich 1. Aus einer Ganzheitsbasis von $\mathcal{T}_{N,\rho}(d)$ bzw. von $\mathcal{TS}_{N,\rho}(d)$ ergibt sich daher ein lineares Ungleichungssystem, also ein Problem der Form $A(x_1, \ldots, x_n)^t \geq b$ mit $A \in \mathbb{Q}^{k\times n}, b \in \mathbb{Z}^k$. Wir sind an den ganzzahligen Lösungen dieses Systems interessiert.

Mit Hilfe von [3] lassen sich diese durch Minimieren und Maximieren der Zielfunktionen $x_i,\ i \in \{1, \ldots, n\}$ sukzessive ermitteln. Da im Vorhinein unklar ist, wie oft dies geschehen muss, ist hierfür ein rekursiver Funktionsaufbau notwendig.

9.1.3 Der $\mathbb{F}_2$-rationale Untercode

Ist $C \leq \mathbb{F}_4^N$ ein Euklidisch selbstdualer Code, so gilt

$$\mathrm{cwe}(C)(1,1,0,0) = 2^i \text{ für ein } i \in \{1,\ldots,\frac{N}{2}\}.$$

Dies folgt mit

Definition 9.2. *Für einen Code $C \leq \mathbb{F}_4^N$ heißt*

$$C' := \{(c_1,\ldots,c_N) \in C \mid c_i \in \mathbb{F}_2 \textit{ für } i = 1,\ldots,n\} \leq \mathbb{F}_2^N$$

der $\mathbb{F}_2$-rationale Untercode von C.

Offenbar ist C' selbstorthogonal; daher ist $\dim_{\mathbb{F}_2}(C') \leq \frac{N}{2}$. Nun ist $\mathrm{cwe}(C)(1,1,0,0) = |C'|$.

9.2 Kurze Darstellung extremaler Gewichtszähler

Die folgenden Überlegungen dienen einer übersichtlichen lesbaren Darstellung von Elementen von $\mathrm{Inv}_{\mathcal{C}(\rho(4_I^E))}(\mathbb{C}[x_v \mid v \in \mathbb{F}_4])_N$.

Wir werden feststellen, dass mögliche extremale Gewichtszähler Euklidisch selbstdualer Codes in vielen Fällen invariant sind unter Permutation der Variablen $\{x_v \mid v \in \mathbb{F}_4\}$.

Diese Eigenschaft entspricht der Invarianz unter der komplexen Matrixgruppe $\mathcal{S} \leq \mathrm{GL}_4(\mathbb{C})$, wobei $\mathcal{S}$ das Bild der durch die Operation von S_4 auf $\{1,\ldots,4\}$ induzierten Darstellung ρ_{S_4} von S_4 bezeichne. Ist $p \in \mathrm{Inv}_{\mathcal{S}}(\mathbb{C}[x_v \mid v \in \mathbb{F}_4])_N$, so besitzen alle Monome in $\mathbb{C}[x_v \mid v \in \mathbb{F}_4]_N$, welche durch Permutation der Variablen x_v , $v \in \mathbb{F}_4$, auseinander hervorgehen, den gleichen Koeffizienten in p. Um p zu beschreiben, genügt dann die Angabe eines Koeffizienten pro Bahn von $\mathcal{S}$ auf der Menge der Monome in $\mathbb{C}[x_v \mid v \in \mathbb{F}_4]$, und die Bahnen entsprechen den Partitionierungen von N in vier nichtnegative ganze Zahlen. Die Summe $\sum_{\pi \in S_4}(x_0^a x_1^b x_\omega^c x_{\omega^2}^d)\pi$ wird dargestellt durch $[a,b,c,d]$, wobei $a \geq b \geq c \geq d$ und wir Nullen in den Quadrupeln weglassen.

Beispiel 9.3. *Sei $C \leq \mathbb{F}_4^N$ der Euklidisch selbstduale Code mit Erzeugermatrix*

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

Der vollständige Gewichtszähler p von C ist gegeben durch

$$\begin{aligned} p(x_0,x_1,x_\omega,x_{\omega^2}) \;=\; & x_0^8 + 14x_0^4x_1^4 + 14x_0^4x_\omega^4 + 14x_0^4x_{\omega^2}^4 + 168x_0^2x_1^2x_\omega^2x_{\omega^2}^2 \\ & + x_1^8 + 14x_1^4x_\omega^4 + 14x_1^4x_{\omega^2}^4 + x_\omega^8 + 14x_\omega^4x_{\omega^2}^4 + x_{\omega^2}^8. \end{aligned}$$

Wegen $p(x_0,x_1,x_\omega,x_{\omega^2}) = p(x_0,x_1,x_{\omega^2},x_\omega)$ lässt p sich darstellen als

$$1[8] + 168[2,2,2,2] + 14[4,4].$$

Bemerkung 9.4. *Ist $C \leq \mathbb{F}_4^N$ ein Euklidisch selbstdualer Code, so ist* $\mathrm{cwe}(C)$ *invariant unter der Operation der komplexen Matrixgruppe*

$$\mathcal{P} :=< M, T >$$

auf $\mathbb{C}[x_v \mid v \in \mathbb{F}_4]$, wobei die Erzeugermatrizen gegeben sind durch $M = \rho_{S_4}((2\ 3\ 4))$ und $\rho_{S_4}((1\ 2)(3\ 4))$. Es gilt $\mathcal{P} \cong A_4$.

Beweis. Gemäß Beispiel 4.11 ist $M \in \mathcal{C}(\rho(4_I^E))$, woraus sich nach Satz 4.7 die Invarianz von $\mathrm{cwe}(C)$ unter M ergibt.

In Beispiel 3.3.2 wurde gezeigt, dass C den Einsvektor $\mathbf{1}$ enthält; daher ist

$$\psi : C \to C, \quad c \mapsto \mathbf{1} + c$$

eine bijektive Abbildung. Bezüglich des $\mathbb{C}$-Vektorraumhomomorphismus' $\mathrm{Sym} : \mathbb{C}V^N \to \mathbb{C}[x_v \mid v \in \mathbb{F}_4]$ (siehe Definition 1.9) hat ψ die Eigenschaft

$$\mathrm{Sym}(\psi(c)) = \mathrm{Sym}(c)T.$$

Wegen $\mathrm{fwe}(C) = \mathrm{fwe}(\psi(C))$ erhalten wir

$$\mathrm{cwe}(C) = \mathrm{Sym}(\mathrm{fwe}(C)) = \mathrm{Sym}(\mathrm{fwe}(\psi(C))) = \sum_{c \in C} \mathrm{Sym}(\psi(c)) = \sum_{c \in C} \mathrm{Sym}(c)T = \mathrm{cwe}(C)T.$$

□

Folgerung 9.5. *Ist $p \in \mathrm{Inv}(\mathcal{C}(\rho(4_I^E)))$, so ist p invariant unter der in Bemerkung 9.4 definierten Matrixgruppe $\mathcal{P}$.*

Beweis. Nach dem Hauptsatz 7.11 wird $\mathrm{Inv}_{\mathcal{C}(\rho(4_I^E))}(\mathbb{C}\,[x_v \mid v \in \mathbb{F}_4])$ als $\mathbb{C}$-Vektorraum erzeugt von den vollständigen Gewichtszählern Euklidisch selbstdualer Codes der Länge N über $\mathbb{F}_4$. Diese sind gemäß Bemerkung 9.4 invariant unter $\mathcal{P}$. Da $\mathcal{P}$ auf $\mathbb{C}\,[x_v \mid v \in \mathbb{F}_4]$ durch $\mathbb{C}$-Algebrenautomorphismen operiert, ergibt sich daraus die Invarianz von p unter $\mathcal{P}$. □

Bemerkung 9.6. *Es gilt $M = \rho_{S_4}((1\ 2\ 3))$ und $T = \rho_{S_4}((1\ 2)(3\ 4))$. Definieren wir*

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \in \mathrm{GL}_4(\mathbb{C}),$$

so ist $Q = \rho_{S_4}((3\ 4))$. Wegen $S_4 =< (1\ 2\ 3), (1\ 2)(3\ 4), (3\ 4) >$ folgt

$$\mathcal{S} =< M, T, Q > .$$

Ist also für $p \in \mathrm{Inv}_{\mathcal{S}}(\mathbb{C}[x_v \mid v \in \mathbb{F}_4])_N$ die Invarianz unter Q gegeben, so ist p wegen Folgerung 9.5 invariant unter $\mathcal{S}$ und kann wie eingangs beschrieben mit Hilfe der Partitionierungen von N dargestellt werden.

Bemerkung 9.7. *Die Permutationsmatrix Q ist durch den Galois-Automorphismus $x \mapsto x^2 \in \mathcal{G}al_{\mathbb{F}_2}(\mathbb{F}_4)$ induziert. Ist also der Code C invariant unter der Galois-Gruppe von $\mathbb{F}_4$, so ist auch* $\mathrm{cwe}(C) \in \mathrm{Inv}(\mathcal{S})$.

Als Folgerung erhalten wir die folgende Bemerkung, die es uns für kleine Längen erspart, die Invarianz unter $\mathcal{S}$ zu überprüfen.

Bemerkung 9.8. *Ist $p \in \mathrm{Inv}(\mathcal{C}(\rho(4_{II}^E)))$ mit $\deg(p) \leq 16$, so ist p invariant unter $\mathcal{S}$, da in einer Hironaka-Zerlegung alle primären und sekundären Invarianten dieses Grades invariant unter Q sind.*

9.3 Eigenschaften der Invarianten von $\mathcal{C}(\rho(4_I^E))$

Satz 9.9. *Es sei $p(x_0, x_1, x_\omega, x_{\omega^2}) \in \mathrm{Inv}_{\mathcal{C}(\rho(4_I^E))}(\mathbb{C}[x_v \mid v \in \mathbb{F}_4])_N$. Ist $x_0^a x_1^b x_\omega^c x_{\omega^2}^d$ ein Monom in $\mathbb{C}[x_v \mid v \in \mathbb{F}_4]_N$, dessen Koeffizient in p nicht verschwindet, so gilt $c + d \in 2\mathbb{N}$.*

Beweis. Sei zunächst $p = \mathrm{cwe}(C)$ für einen Euklidisch selbstdualen Code $C \leq \mathbb{F}_4^N$, und sei $c \in C$. Weiter sei die Funktion $n_a,\ a \in \mathbb{F}_4$, wie in Definition 1.5; dann ist $c + d = n_\omega(c) + n_{\omega^2}(c)$.

Angenommen, es gilt $n_\omega(c) + n_{\omega^2}(c) \notin 2\mathbb{N}$. Dann folgt wegen $\omega + \omega^2 = 1$

$$< c, c >= \underbrace{\omega^2 + \ldots + \omega^2}_{n_\omega - \text{mal}} + \underbrace{\omega + \ldots + \omega}_{n_{\omega^2} - \text{mal}} + \underbrace{1 + \ldots + 1}_{n_1 - \text{mal}} \in \{\omega + 1, \omega^2 + 1\},$$

im Widerspruch zur Selbstdualität von C.

Für beliebiges $p \in \mathrm{Inv}_{\mathcal{S}}(\mathbb{C}[x_v \mid v \in \mathbb{F}_4])_N$ folgt die Aussage des Satzes aus dem Hauptsatz 7.11. □

9.4 Maximales Minimalgewicht von Codes vom Typ $\rho(4_I^E)$ und Typ $\rho(4_{II}^E)$

Die folgende Tabelle listet die mit dieser Methode erhaltenen Schranken an das maximale Minimalgewicht von Codes des Typs 4_I^E bzw. 4_{II}^E für die verschiedenen Längen N solcher Codes auf. Bei $N = 24$ tritt der erste offene Fall auf; man kann nachweisen, dass es für diese Länge keinen Code C gibt mit $d(C) \geq 10$, kennt aber andererseits keinen Code der Länge 24 mit Minimalgewicht 9. Es existiert jedoch ein Typ 4_{II}^E-Code mit Minimalgewicht 8. Die Einträge in den Zeilen, welche für größere Längen stehen, sind ebenso zu verstehen.

	Typ 4_I^E	Typ 4_{II}^E	
Länge	d	d	extremale Gewichtszähler
2	2		
4	3	3	1
6	3		
8	4	4	1
10	4		
12	6	6	1
14	6		
16	6	6	2
18	7		
20	8	8	4
22	8		
24	8-9	8-9	2
26	8-9		
28	9-10	9-10	1030
30	10-12		
32	10-12	10-12	41

9.5 Klassifizierung extremaler Gewichtszähler

9.5.1 Quadratische Restcodes

Quadratische Restcodes sind spezielle zyklische Codes. Hier machen wir noch einmal von dem klassischen Begriff eines Codes als Untervektorraum von $\mathbb{F}_q^N$ Gebrauch, falls $\mathbb{F}_q$ ein endlicher Körper ist (siehe Vorwort).

Definition 9.10. *Es sei $C \leq \mathbb{F}_q^N$ ein Code. Gilt für $c = (c_1, \ldots, c_N) \in C$, dass auch $(c_N, c_1, \ldots, c_{N-1}) \in C$, so heißt C zyklisch.*

Die zyklischen Codes entsprechen den Idealen von $\mathbb{F}_q[x]/(x^N - 1)$, also Teilern des Polynoms $x^N - 1$.

Bemerkung 9.11. *(i) Wir definieren einen $\mathbb{F}_q$-Vektorraumisomorphismus $\phi : \mathbb{F}_q^N \to \mathbb{F}_q[x]/(x^N - 1)$ durch*

$$\phi((a_1, \ldots, a_N)) = a_1 + a_2 x + \ldots + a_n x^{N-1} + (x^N - 1).$$

Ein Code $C \leq \mathbb{F}_q^N$ ist genau dann zyklisch, wenn $\phi(C) \leq \mathbb{F}_q[x]/(x^N - 1)$ ein Ideal ist.

(ii) Es sei $I \trianglelefteq \mathbb{F}_q[x]/(x^N - 1)$ ein Ideal. Dann existiert ein Polynom $g \in \mathbb{F}_q[x]$, so dass $g(x) \big| (x^N - 1)$ und $I = (g) + (x^N - 1)$. Ist $\deg(g) = d$ und $g(x) = a_d x^d + \ldots + a_1 x + a_0$, so können wir einen zyklischen Code C definieren durch die Erzeugermatrix

$$\begin{pmatrix} a_d & a_{d-1} & \ldots & & a_0 & 0 & \ldots & & 0 \\ 0 & a_d & a_{d-1} & \ldots & & a_0 & 0 & \ldots & 0 \\ & & & & \ldots & & & & \\ 0 & \ldots & 0 & a_d & a_{d-1} & \ldots & & & a_0 \end{pmatrix} \in \mathbb{F}_q^{N-d \times N}.$$

Dann ist $\phi(C) = I$.

Definition 9.12. *Sind das Polynom g und der zyklische Code C wie in Bemerkung 9.11(ii), so heißt g das Erzeugerpolynom von C.*

Nun können wir die quadratischen Restcodes einführen.

Definition und Bemerkung 9.13. *Es seien p eine ungerade Primzahl und ζ eine primitive p-te Einheitswurzel in einer Körpererweiterung $\widetilde{\mathbb{F}}$ von $\mathbb{F}_2$. Wir betrachten das Polynom*

$$g := \prod_{a \in (\mathbb{F}_p^*)^2} (x - \zeta^a) \in \widetilde{\mathbb{F}}[x].$$

Dann liegt g in $\mathbb{F}_4[x]$, und es gilt $g(x) | (x^p - 1)$. Mit $\mathbf{QR}(\widetilde{\mathbb{F}}, p) \leq \widetilde{\mathbb{F}}^p$ bezeichnen wir den zyklischen Code in $\widetilde{\mathbb{F}}^p$ mit Erzeugerpolynom g, den quadratischen Restcode zur Primzahl p.

Ist $\mathbb{F}$ ein endlicher Körper und $C \leq \mathbb{F}^N$ ein Code (im klassischen Sinne), so erhalten wir mit Hilfe folgender Konstruktion aus C einen Code $\widetilde{C}$ der Länge $N+1$ mit $\dim(C) = \dim(\widetilde{C})$.

Definition und Bemerkung 9.14. *Es sei $\mathbb{F}$ ein endlicher Körper und $C \leq \mathbb{F}^N$ ein Code. Indem wir $c = (c_1, \ldots, c_N) \in C$ ersetzen durch $(c_1, \ldots, c_N, \sum_{i=1}^N c_i)$, erhalten wir einen Code $\widetilde{C} \leq \mathbb{F}^{N+1}$, welcher selbstdual ist bezüglich des in Kapitel 1 eingeführten Euklidischen Skalarprodukts. Es gilt $\dim(\widetilde{C}) = \dim(C)$. Wir nennen $\widetilde{C}$ den Erweiterungscode von C.*

Bemerkung 9.15. *Mit den Bezeichnungen von Definition und Bemerkung 9.13 sei* $C := \mathbf{QR}(\widetilde{\mathbb{F}}, p)$ *ein quadratischer Restcode.*

(i) Der Code C *enthält den Einsvektor* $\mathbf{1}$*.*

(ii) Die Bezeichnungen seien wie in Definition und Bemerkung 9.13, und es sei $p \equiv 3 \mod 4$*. Dann ist* $h(x) := (1-x)g(x)$ *ein Erzeugerpolynom von* $C^\perp$*.*

(iii) Es sei wieder $p \equiv 3 \mod 4$*. Dann ist der Erweiterungscode* $\widetilde{C}$ *von* C *selbstdual.*

Beweis.

zu (i): Es ist $\phi(\mathbf{1}) = 1 + x + \ldots + x^{p-1}$. Für das Erzeugerpolynom $g(x)$ von C gilt gemäß Definition und Bemerkung 9.13, dass $g(x) \big| (x^p - 1)$ sowie $(x-1) \nmid g(x)$. Daher gilt $\phi(\mathbf{1}) = \frac{x^p-1}{x-1} \in (g(x))$, also $\mathbf{1} \in C$.

zu (ii): Für ein Polynom $q(x) = \sum_{i=0}^{p-1} a_i x^i \in \mathbb{F}[x]$ bezeichnen wir mit $\mathrm{rev}(q)(x) = x^{p-1} q(x^{-1}) = \sum_{i=0}^{p-1} a_i x^{N-i}$ das Polynom, bei dem die Koeffizienten von q in umgekehrter Reihenfolge auftreten. Nun sei $r(x) = \frac{x^N-1}{g(x)} = (x-1) \prod_{a \notin (\mathbb{F}_p^*)^2} (x - \zeta^a)$. Zunächst zeigen wir, dass $\mathrm{rev}(r)(x)$ ein Erzeugerpolynom von $C^\perp$ ist. Dazu seien $c = (c_1, \ldots, c_p) \in C$ und $c' = (c'_1, \ldots, c'_p) \in \mathbb{F}^p$. Nun gilt

$$\phi(c)\,\mathrm{rev}(\phi(c')) = (\sum_{i=0}^{p-1} c_i x^i)(\sum_{j=0}^{p-1} c'_j x^{p-1-j}) + (x^p - 1) = \sum_{i,j=0}^{p-1} c_i c'_j x^{p+i-j-1} + (x^p - 1).$$

Nun gilt $\sum_{i=0}^{p-1} c_i c'_i = 0$ genau dann, wenn der Koeffizient in $\widetilde{\phi(c)\phi(c')}$ bei x^{p-1} verschwindet. Dies ist der Fall für $\mathrm{rev}(\phi(c')) \in (r(x))$, da $g(x)r(x) = 0 \mod (x^p - 1)$. Da offenbar $\mathrm{rev}(\ )$ eine Bijektion von $\mathbb{F}[x]/(x^p-1)$ ist mit $\mathrm{rev} \circ \mathrm{rev} = \mathrm{id}$, erhalten wir $(\mathrm{rev}(r(x))) \subseteq \phi(C^\perp)$. Betrachten wir nun die Dimension der Ideale $(\overline{g(x)})$ und $(\overline{\mathrm{rev}(r(x))})$ als $\mathbb{F}_q$-Vektorräume. Ist $d := \dim((\overline{g(x)}))$, so ist $\dim((\overline{\mathrm{rev}(r(x))})) = N - (N-d) - 1 = d - 1$. Wir erhalten $\dim((\overline{g(x)})) + \dim((\overline{\mathrm{rev}(r(x))})) = N$. Daraus folgt $(\mathrm{rev}(r(x))) = \phi(C^\perp)$.

Nun zeigen wir, dass $(\mathrm{rev}(r(x))) = ((x-1)g(x))$, also dass $h(x)$ ebenfalls ein Erzeugerpolynom von $C^\perp$ ist. Durch elementares Nachrechnen stellen wir fest, dass rev ein Isomorphismus von $\widetilde{F}[x]$ ist. Daher ist

$$\mathrm{rev}(r(x)) = \mathrm{rev}((x-1) \prod_{a \notin (\mathbb{F}_p^*)^2} (x - \zeta^a)) = (1-x) \prod_{a \notin (\mathbb{F}_p^*)^2} (-\zeta^a x + 1).$$

Wegen $p \equiv 3 \mod 4$ gilt $x \in (\mathbb{F}_p^*)^2$ genau dann, wenn $-x \notin (\mathbb{F}_p^*)^2$. Wir erhalten

$$\begin{aligned} \mathrm{rev}(r(x)) &= (x-1) \prod_{a \notin (\mathbb{F}_p^*)^2} \zeta^a (x - \zeta^{-a}) \\ &= (x-1) \prod_{a \notin (\mathbb{F}_p^*)^2} \zeta^a \prod_{a \in (\mathbb{F}_p^*)^2} (x - \zeta^a). \end{aligned}$$

Dem entnehmen wir, dass $h(x)$ durch Multiplikation mit einem invertierbaren Element von $\widetilde{\mathbb{F}}$ aus $\mathrm{rev}(r(x))$ hervorgeht; daher ist $(\mathrm{rev}(r(x))) = (h(x))$.

zu (iii): Aus (ii) erhalten wir, dass

$$C^\perp = \{c = (c_1, \ldots, c_p) \in C \mid \sum_{i=1}^{p} c_i = 0\}.$$

Bezeichnen wir mit $E_{p+1} \leq \mathbb{F}^p$ den von $\mathbf{1}$ erzeugten $\widetilde{\mathbb{F}}$-Vektorraum, so folgt daraus

$$\widetilde{C} = \widetilde{C^\perp} \oplus E_{p+1}.$$

Daher ist $\widetilde{C}$ selbstorthogonal. Weiter gilt wegen $\dim(C) = 1 + \dim(C^\perp)$

$$\dim(\widetilde{C}^\perp) = p+1-\dim(\widetilde{C}) = p+1-\dim(C) = p-\dim(C^\perp) = \dim(C) = \dim(\widetilde{C}),$$

und daher ist $\widetilde{C}$ sogar selbstdual.

□

Satz 9.16. *Es seien $\mathbb{F} = \mathbb{F}_q, q = 2^f$, eine Körper und p eine Primzahl mit $p \equiv 3 \pmod 4$. Dann ist der erweiterte quadratische Restcode $\widetilde{C} := \widetilde{\mathbf{QR}}(\mathbb{F}, p)$ ein Code vom Typ $\rho(q_{II}^E)$.*

Beweis. Die Selbstdualität von $\widetilde{C}$ wurde in Bemerkung 9.15 gezeigt. Nun wollen wir die Bedingungen aus Definition 3.24 nachweisen. Ist $C := \mathbf{QR}(\mathbb{F}, p)$, so schreiben wir wie im Beweis von Bemerkung 9.15(iii)

$$\widetilde{C} = \widetilde{C^\perp} \oplus E_{p+1}.$$

Da $p + 1 \cong 0 \pmod 4$ und, wie im Beweis von Bemerkung 9.15 gezeigt wurde, $C^\perp = \{c = (c_1, \ldots, c_p) \in C \mid \sum_{i=1}^{p} c_i = 0\}$ ist, ist Bedingung (i) offensichtlich erfüllt. Zum Nachweis von Bedingung (ii) berechnen wir für $c = (c_1, \ldots, c_p) \in C^\perp$

$$\sum_{i=1}^{p} c_i \sum_{j=1} c_j + \sum_{1 \leq i < j \leq p} c_i c_j = \sum_{i=1}^{p} c_i^2 = 0.$$

□

Die folgenden Listen enthalten Koeffizienten $(c_1, \ldots, c_n)$, so dass $q = c_1 p_1 + \ldots + c_n p_n$ ein möglicher Gewichtszähler eines Codes $C \leq \mathbb{F}_4^N$ vom Typ 4_{II}^E mit Minimalgewicht d ist. Es existiert kein Code der Länge N dieses Typs mit größerem Minimalgewicht als d. Im Folgenden bezeichnen wir mit $\omega \in \mathbb{F}_4$ einen Erzeuger von $\mathbb{F}_4^*$.

9.5.2 Typ 4_{II}^E, Länge 4, $d = 3$

Der einzige Gewichtszähler ist gegeben durch

$$p_1 := 1[4] + 12[1, 1, 1, 1]$$

wird durch den Code mit Erzeugermatrix A realisiert, wobei

$$A := \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & w & w^2 \end{pmatrix}.$$

9.5.3 Typ 4_{II}^{E}, Länge 16, $d = 6$

Die möglichen Gewichtszähler sind

$$\mathrm{cwe}(Pr(Q_{20})) = q_1 := p_1 + 113p_2,\ q_2 := p_1 + 125p_2,$$

wobei der Code $Pr(Q_{20})$ die Erzeugermatrix I_8, A hat mit

$$\begin{pmatrix} 0 & 0 & \omega^2 & 0 & \omega & 1 & \omega^2 & 0 \\ \omega^2 & 0 & 1 & 1 & 1 & 1 & \omega & \omega^2 \\ 1 & 0 & 1 & \omega & 1 & 1 & 0 & \omega \\ \omega & 1 & 1 & \omega & 0 & 1 & \omega & \omega \\ 0 & \omega^2 & 1 & \omega & 0 & 1 & 1 & 1 \\ \omega & \omega & \omega^2 & 1 & \omega^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \omega & \omega & \omega^2 & \omega^2 \\ \omega^2 & \omega & \omega & 0 & 1 & 0 & \omega^2 & 0 \end{pmatrix}$$

Es ist $\mathrm{cwe}(Pr(Q_{20}))(1,1,0,0) = 2^2$ und $q_2(1,1,0,0) = 2^4$.

Gewichtsverteilung	p_1	p_2
$[16]$	1	0
$[10,2,2,2]$	-284	4
$[9,5,1,1]$	564	-4
$[7,3,3,3]$	5608	-8
$[6,6,2,2]$	1108	12
$[5,5,5,1]$	4380	-12
$[4,4,4,4]$	13990	10
$[8,4,4]$	-2	2
$[8,8]$	-111	1

9.6 Typ 4_{II}^{E}, Länge 20, $d = 8$

Es gibt vier mögliche Gewichtszähler. Diese lassen sich parametrisieren durch

$$q_i = p_1 + (-345 + 48\sum_{j=0}^{i-1} 4^{-j})p_2,\ i = 0, \ldots, 3.$$

Es gilt

$$q_i(1,1,0,0) = 2^{7-2i},\ i = 0, \ldots, 3.$$

Es ist $q_3 = \mathrm{cwe}(Q_{20})$.

Die Polynome p_1 und p_2 sind hierbei wie folgt.

Gewichtsverteilung	p_1	p_2
$[20]$	1	0
$[11,3,3,3]$	48	-16
$[10,6,2,2]$	6804	12
$[9,9,1,1]$	1508	4
$[9,5,5,1]$	72	-24
$[8,4,4,4]$	96291	108
$[7,7,3,3]$	18480	-80
$[6,6,6,2]$	79500	100
$[5,5,5,5]$	115560	-216
$[12,4,4]$	849	2
$[8,8,4]$	1701	3
$[12,8]$	-282	-1

9.6.1 Typ 4_{II}^{E}, Länge 24, $d = 9$

Hier gibt es zwei Kandidaten für Gewichtszähler, welche durch die untenstehende Tabelle beschrieben werden. Es ist $p_1(1,1,0,0) = 2^4$ und $p_2(1,1,0,0) = 2^2$.

Gewichtsverteilung	p_1	p_2
$[24]$	1	1
$[15,3,3,3]$	2280	2376
$[14,6,2,2]$	2652	2508
$[13,9,1,1]$	192	264
$[13,5,5,1]$	6456	6600
$[12,4,4,4]$	88602	88242
$[11,7,3,3]$	80472	81048
$[10,10,2,2]$	11184	10824
$[10,6,6,2]$	158604	157740
$[9,9,5,1]$	37392	37752
$[9,5,5,5]$	944232	945384
$[8,8,4,4]$	633642	632742
$[7,7,7,3]$	768912	770352
$[6,6,6,6]$	2196096	2193840
$[12,8,4]$	1422	1386
$[8,8,8]$	8157	8085
$[12,12]$	14	2

9.6.2 Typ 4_{II}^{E}, Länge 28, $d = 10$

Parameter	Dimension des $\mathbb{F}_2$-rationalen Untercodes
$p_1 - 63p_2$	7
$p_1 - 15p_2 + ip_3,\ i = 0, \ldots, 288$	5
$p_1 - 3p_2 + ip_3,\ i = 0, \ldots, 360$	3
$p_1 + ip_3,\ i = 0, \ldots, 378$	1

Gewichtsverteilung	p_1	p_2	p_3
$[28]$	1	0	0
$[18, 6, 2, 2]$	1638	4	-2
$[17, 9, 1, 1]$	0	0	1
$[17, 5, 5, 1]$	3276	-16	6
$[16, 4, 4, 4]$	62244	26	6
$[15, 7, 3, 3]$	78624	-16	-12
$[14, 10, 2, 2]$	13104	-10	6
$[14, 6, 6, 2]$	201474	96	-10
$[13, 13, 1, 1]$	756	12	-2
$[13, 9, 5, 1]$	65520	-44	8
$[13, 5, 5, 5]$	1677312	-344	6
$[12, 8, 4, 4]$	1630629	241	46
$[11, 11, 3, 3]$	321048	-56	-32
$[11, 7, 7, 3]$	3000816	-448	-12
$[10, 10, 6, 2]$	958230	258	-20
$[10, 6, 6, 6]$	13433238	1356	-114
$[9, 9, 9, 1]$	371280	-120	15
$[9, 9, 5, 5]$	9562644	-924	6
$[8, 8, 8, 4]$	11548719	881	66
$[7, 7, 7, 7]$	28167984	-1904	96
$[16, 8, 4]$	819	5	-2
$[12, 12, 4]$	4095	1	0
$[12, 8, 8]$	24570	12	-2
$[16, 12]$	0	-1	0

9.6.3 Typ 4_{II}^{E}, Länge 32, $d = 12$

Parameter	Dimension des $\mathbb{F}_2$-rationalen Untercodes
$p_1 + 2p_3$	2
$p_1 + 3ip_2 + (62 - 6i)p_3,\ i = 0, \ldots, 10$	6
$p_1 + (48 + 3i)p_2 + (158 - 6i)p_3,\ i = 0, \ldots, 20$	8
$p_1 + (240 + 3i)p_2 + (542 - 6i)p_3,\ i = 0, \ldots, 7$	10

Gewichtsverteilung	p_1	p_2	p_3
$[32]$	1	0	0
$[20, 4, 4, 4]$	41416	-38	16
$[19, 7, 3, 3]$	47616	80	-32
$[18, 10, 2, 2]$	7440	-74	24
$[18, 6, 6, 2]$	134912	-92	48
$[17, 13, 1, 1]$	496	16	-8
$[17, 9, 5, 1]$	66960	64	-24
$[17, 5, 5, 5]$	1548512	48	-112
$[16, 8, 4, 4]$	2018968	-213	172
$[15, 11, 3, 3]$	518816	432	-144
$[15, 7, 7, 3]$	4977856	208	-320
$[14, 14, 2, 2]$	38192	-180	56
$[14, 10, 6, 2]$	2156112	-360	216
$[14, 6, 6, 6]$	30224256	1252	576
$[13, 13, 5, 1]$	205840	176	-56
$[13, 9, 9, 1]$	1174528	80	-96
$[13, 9, 5, 5]$	30035280	-1216	-504
$[12, 12, 4, 4]$	7418424	-388	340
$[12, 8, 8, 4]$	52332960	2217	768
$[11, 11, 7, 3]$	20394528	-192	-624
$[11, 7, 7, 7]$	191801216	-7728	-1504
$[10, 10, 10, 2]$	10256784	26	408
$[10, 10, 6, 6]$	143811728	6092	1160
$[9, 9, 9, 5]$	171038160	-7840	-1080
$[8, 8, 8, 8]$	370384156	14712	1786
$[20, 8, 4]$	1488	-1	0
$[16, 12, 4]$	3224	-17	4
$[16, 8, 8]$	24180	-6	6
$[12, 12, 8]$	115320	-17	12
$[20, 12]$	0	1	0
$[16, 16]$	0	0	1

Literatur

[1] C. Bachoc. Applications of coding theory to the construction of modular lattices. *Journal of Combinatorial Theory*, (A 78):92–119, 1997.

[2] John J. Cannon and Wieb Basma, editors. *Handbook of Magma Functions*. Sydney: School of Mathematics and Statistics, University of Sydney, 2.12 edition, 2005. siehe `http://magma.maths.usyd.edu.au/magma/`.

[3] Waterloo Maple Inc. Maple 8. www.maplesoft.com.

[4] M.A. Knus. *Quadratic and Hermitian Forms over Rings*. Springer-Verlag, 1991.

[5] G. Nebe, E.M.Rains, and N.J.A. Sloane. *Self-Dual Codes and Invariant Theory*. Springer-Verlag, 2006.

[6] G. Nebe, H.-G. Quebbemann, E.M.Rains, and N.J.A. Sloane. Complete weight enumerators of generalized doubly-even self-dual codes. *Finite Fields and Their Applications*, (10):540–550, 2004.

[7] J. Neukirch. *Algebraische Zahlentheorie*. Springer-Verlag, 1992.

[8] H.-G. Quebbemann. On even codes. *Discrete Mathematics*, (98):29–34, 1991.

[9] I. Reiner. *Maximal Orders*. Academic Press, 1975.

[10] B. Sturmfels. *Algorithms in Invariant Theory*. Springer-Verlag, 1993.