Universität Bayreuth Fakultät für Mathematik, Physik und Informatik

Dissertation

Geometrische Konstruktionen linearer Codes über Galois-Ringen der Charakteristik 4 von hoher homogener Minimaldistanz

Michael Kiermaier

2012

Für meinen Vater
1954 – 2001

Vorwort

Die vorliegende Dissertation entstand in den Jahren 2006 bis 2012 an der Universität Bayreuth unter der Betreuung von Herrn Prof. Dr. Kerber. Für seine beständige Unterstützung und das mir vom ersten Augenblick an entgegengebrachte Vertrauen gebührt ihm mein tiefer Dank.

Weiter bedanke ich mich bei Herrn Prof. Dr. Laue, Axel Kohnert, Alfred Wassermann, Stephan Elsenhans, Sascha Kurz, Johannes Zwanzger und Thomas Feulner für die konstruktive und stets unkomplizierte Zusammenarbeit. Meine Stelle wurde teilweise aus dem DFG-Projekt WA 1666/4 finanziert, das Axel Kohnert und Alfred Wassermann beantragt hatten.

Ein besonderer Dank gilt meinem langjährigen Lehrer Thomas Honold, der mich als Betreuer meiner Diplomarbeit zum Thema der linearen Codes über endlichen Ringen gebracht hat. Mit seinem unerschöpflichen Wissen war er mir stets ein wertvoller Ansprechpartner. Nicht unerwähnt bleiben soll auch seine großzügige Einladung an die Zhejiang Universität in Hangzhou, China, die mir im März und April 2010 sechs unvergessliche und wissenschaftlich sehr fruchtbare Wochen bescherte.

Nicht zuletzt möchte ich mich bei meiner Familie für ihre Unterstützung bedanken: bei meiner Mutter, meinem leider viel zu früh verstorbenen Vater und besonders bei meiner Ehefrau Julia, deren dreißigsten Geburtstag ich mir als Abgabetermin für die Dissertation gesetzt hatte, den ich auch auf den Tag genau einhalten konnte.

Bayreuth, im November 2012 *Michael Kiermaier*

Inhaltsverzeichnis

1. Einleitung

Fehlerkorrigierende Codes werden heute in nahezu jeder Form der Informationsübertragung und -speicherung eingesetzt. Prominente Beispiele sind CD-Spieler, WLAN sowie die Kommunikation mit Weltraumsonden.

In der Codierungstheorie werden fehlerkorrigierende Codes wie folgt mathematisch modelliert: Ein *Blockcode* $\mathcal{C}$ der Länge n ist eine Teilmenge von Γ^n, wobei das *Alphabet* Γ eine endliche Menge ist. Für die Anwendungen sind die *binären* Blockcodes mit $\#\Gamma = 2$ von besonderem Interesse.[1] Die *Hamming-Distanz* zweier Codewörter ist die Anzahl der Positionen, an denen sie sich unterscheiden, und die *Minimaldistanz* d eines Blockcodes $\mathcal{C}$ ist das Minimum über die Hamming-Distanzen aller Paare verschiedener Codewörter in $\mathcal{C}$. Man bezeichnet dann $\mathcal{C}$ als einen $(n, \#\mathcal{C}, d)_{\#\Gamma}$-*Code*. Eine wichtige Klasse sind die *linearen Codes* über endlichen Körpern: Hier ist $\Gamma = \mathbb{F}_q$ ein endlicher Körper und $\mathcal{C}$ ein Untervektorraum des $\mathbb{F}_q$-Vektorraums $\mathbb{F}_q^n$. Gute Fehlerkorrektureigenschaften von $\mathcal{C}$ entsprechen einem möglichst kleinen Parameter n sowie möglichst großen Parametern $\#\mathcal{C}$ und d.

1.1. Geschichte der linearen Codes über Ringen

Im Jahr 1967 hielt John Robinson, Elektrotechniker an der University of Iowa, USA, einen Einführungsvortrag für Schüler über Codierungstheorie [4, S. 68]. Er illustrierte seinen Vortrag mit dem folgenden offenen Forschungsproblem: Der nach dem damaligen Wissensstand größte bekannte binäre Blockcode der Länge 16 und Minimaldistanz 6 war ein linearer binärer Code der Größe 128. Man wusste, dass kein größerer linearer binärer Code dieser Länge und Minimaldistanz existiert. Für allgemeine binäre Blockcodes der Länge 16 und Minimaldistanz 6 war nach den bekannten oberen Schranken jedoch noch eine Größe von bis zu 256 Codewörtern denkbar.

Überraschenderweise gelang es dem Schüler Alan W. Nordstrom aufgrund des Vortrags, einen nichtlinearen binären $(16, 2^8, 6)_2$-Blockcode zu konstruieren.[2] Dieser Code hat eine höhere Minimaldistanz als jeder *lineare* binäre Code gleicher Länge und Größe, weshalb wir ihn als *BTL-Code* (*better than linear*) bezeichnen. Er wurde 1967 in einer gemeinsamen Arbeit von Nordstrom und Robinson veröffentlicht [114] und 1969 nochmals

[1] In dieser Arbeit bezeichnet das Symbol # die Mächtigkeit einer Menge oder Multimenge oder auch das Gewicht einer Partition.

[2] Tatsächlich handelte es sich sowohl in Robinsons Vortrag als auch bei dem von Nordstrom gefundenen Code um binäre Blockcodes der Länge 15 und Minimaldistanz 5. Durch Anhängen eines Paritätsbits entsprechen diese Codes jedoch eindeutig den binären Blockcodes der Länge 16 und Minimaldistanz 6.

unabhängig von den beiden Russen Semakov und Zinoviev gefunden [122]. Aufgrund etlicher weiterer bemerkenswerter Eigenschaften und seiner vergleichsweise kleinen Parameter ist der *Nordstrom-Robinson-Code* der heute wohl prominenteste BTL-Code.

Bereits im Originalartikel wurde von Nordstrom und Robinson die Frage nach einer größeren Klasse verwandter nichtlinearer Codes aufgeworfen. Eine solche Klasse wurde 1969 in Form der unendlichen Serie der *Preparata-Codes* [118] mit den Parametern

$$(2^{k+1},\ 2^{2^{k+1}-2(k+1)},\ 6)_2$$

und eine weitere 1972 durch die unendliche Serie der *Kerdock-Codes* mit den Parametern

$$(2^{k+1},\ 2^{2(k+1)},\ 2^k - 2^{\frac{k-1}{2}})_2$$

angegeben [80], dabei ist jeweils $k \geq 3$ eine ungerade Zahl. Beide Serien von Codes enthalten mit $k = 3$ den Nordstrom-Robinson-Code als ihren kleinsten Vertreter. Die Kerdock- und Preparata-Codes haben ausgezeichnete Fehlerkorrektureigenschaften. Im Jahr 1977 wurde im Standardwerk [108] als Research Problem (15.4) die Frage gestellt, ob die Kerdock- und Preparata-Codes sämtlich BTL-Codes sind. Für die Preparata-Codes konnte die Frage 1993 positiv beantwortet werden [14]. Die Kerdock-Codes sind besser als alle *bekannten* vergleichbaren linearen Codes (*BTKL-Codes*, *better than known linear*), die Frage nach der BTL-Eigenschaft ist jedoch nach wie vor offen.[3][4]

Im Jahr 1975 wurden in [31] die *Delsarte-Goethals-Codes* mit den Parametern

$$(2^{k+1},\ 2^{2(k+1)+kt},\ 2^k - 2^{\frac{k-1}{2}+t})_2$$

($k \geq 3$ ungerade und $t \in \{0, \ldots, (k-1)/2\}$) als eine Verallgemeinerung der Kerdock-Codes (Spezialfall $t = 0$) angegeben. Für $t = 1$ sind alle Delsarte-Goethals-Codes BTKL, für $t \geq 2$ scheinen sie im Hinblick auf die Fehlerkorrektureigenschaften weniger interessant zu sein. Im Jahr 1976 wurden in [45] (Vorankündigung ohne Beweise 1974 in [44]) die zu den Preparata-Codes verwandten *Goethals-Codes* mit den Parametern

$$(2^{k+1},\ 2^{2^{k+1}-3k-2},\ 8)_2$$

($k \geq 3$ ungerade) vorgestellt. Abgesehen vom kleinsten Fall $k = 3$ sind alle Goethals-Codes BTKL.

Aleksandr A. Nechaev fand im Jahr 1989 heraus, dass sich die zweifach punktierten Kerdock-Codes durch $\mathbb{Z}_4$-lineare Rekursionsgleichungen darstellen lassen. Die beiden Forschergruppen A. Roger Hammons Jr. und P. Vijay Kumar sowie A. R. Calderbank, N. J. A. Sloane und Patrick Solé arbeiteten zunächst unabhängig voneinander und bündelten schließlich 1994 ihre Resultate im Artikel [52]: Alle Kerdock-, Preparata-, Goethals-

[3] Aus der Nichtexistenz linearer binärer Codes mit den Parametern der Preparata-Codes folgt über die MacWilliams-Identität, dass kein linearer binärer Code mit dem Hamming-Gewichtszähler der Kerdock-Codes existiert. Die Existenz eines linearen binären Codes mit lediglich derselben Länge, Größe und Minimaldistanz wie die Kerdock-Codes ist damit aber noch nicht ausgeschlossen.

[4] Während BTL eine harte mathematische Eigenschaft eines Blockcodes ist, spiegelt BTKL nur den aktuellen Wissensstand wieder.

und Delsarte-Goethals-Codes sind Bilder von $\mathbb{Z}_4$-linearen Codes (d.h. von Untermoduln des $\mathbb{Z}_4$-Moduls $\mathbb{Z}_4^n$) unter der sogenannten Gray-Abbildung. Diese Ergebnisse waren so bemerkenswert, dass der Artikel 1995 von der *IEEE Information Theory Society* mit dem *Information Theory Paper Award* ausgezeichnet wurde. Außerdem fanden die Resultate Eingang in das Heft des Jahres 1994 der Reihe *What's Happening in the Mathematical Sciences* der American Mathematical Society, die jährlich in allgemeinverständlicher Sprache einen Abriss über die wichtigsten Neuentwicklungen in der mathematischen Forschung gibt [25]. Diese Erfolge waren der Auslöser einer regen Forschungstätigkeit auf dem Gebiet der linearen Codes über dem Ring $\mathbb{Z}_4$ und bald auch über allgemeineren endlichen Ringen. Es wurde eine Fülle von strukturtheoretischen Aussagen über ringlineare Codes veröffentlicht. Erstaunlicherweise wurden jedoch – trotz der nun zur Verfügung stehenden neuen Konstruktionsmethode als Gray-Bild eines $\mathbb{Z}_4$-linearen Codes – kaum neue binäre Blockcodes konstruiert.

Bis zum Beginn der Untersuchung von ringlinearen Codes an der Universität Bayreuth waren keine neuen BTL-Parameter als Gray-Bild eines $\mathbb{Z}_4$-linearen Codes gefunden worden, die sich nicht trivial aus bereits bekannten BTL-Parametern ableiten lassen.[5] Die bis dahin neu gefundenen BTKL-Parameter von Gray-Bildern $\mathbb{Z}_4$-linearer Codes beschränken sich auf wenige Einzelfälle (vgl. [54]): Die Parameter $(64, 2^{32}, 14)_2$ vom *quaternary Reed-Muller-Code* $\mathrm{QRM}(2, 5)$ aus [52, Sec. V-D][6] sowie nochmals vom nicht zu $\mathrm{QRM}(2, 5)$ isomorphen (siehe hierzu [24]) erweiterten $\mathbb{Z}_4$-linearen QR-Code der Länge 32 [117], [21, Th. 4.2]; die Parameter $(96, 2^{48}, 18)_2$ vom erweiterten $\mathbb{Z}_4$-linearen QR-Code der Länge 48 [117];[7] die Parameter $(64, 2^{37}, 12)_2$ vom Calderbank-McGuire-Code aus [20]; sowie die Parameter $(92, 2^{24}, 28)_2$ und $(84, 2^{13}, 34)_2$ aus Example 1 und 7 in [3].[8]

Im Jahr 2009 wurde die Situation von Marcus Greferath in einem Übersichtsartikel über ringlineare Codes mit der Formulierung *„[...] the still unsolved problem of the construction of large families of ring-linear codes of high quality"* sehr deutlich dargestellt [48, S. 219].

[5] Beispielsweise hat das Gray-Bild des $\mathbb{Z}_4$-linearen Codes aus [3, Ex. 4] die BTL-Parameter $(30, 2^8, 28)_2$. Diese Parameter lassen sich aber auch durch Verkürzen des $\mathbb{Z}_4$-Urbilds des Kerdock-Codes mit $k = 5$ ableiten.

[6] Der „Hensel lift of the extended binary three-error-correcting BCH code" aus [21] ist als $\mathbb{Z}_4$-linearer Code isomorph zu $\mathrm{QRM}(2, 5)$, siehe [41]. Die Isomorphie wird auch durch den Algorithmus aus [39] bestätigt.

[7] An dieser Stelle sei darauf hingewiesen, dass der symmetrisierte Gewichtszähler des erweiterten $\mathbb{Z}_4$-linearen QR-Codes der Länge 48 in [117] sowie der Lee-Gewichtszähler in [9] nicht korrekt sind, siehe [87].

[8] Die Parameter der restlichen Beispiele in [3] sind entweder nicht BTKL aufgrund von seitdem neu gefundenen $\mathbb{F}_2$-linearen Codes, oder sie lassen sich durch (wiederholtes) Punktieren und/oder Verkürzen trivial aus den Kerdock-Codes herleiten bzw. im Fall von Example 3 sogar verbessern.

1.2. Ringlineare Codes und Hjelmslev-Geometrien

In Kapitel 2 werden die benötigten Grundlagen über ringlineare Codes bereitgestellt. Für die Klasse der Grundringe beschränken wir uns der Einfachheit halber auf Galois-Ringe R der Kettenlänge 2, die für die später folgenden Konstruktionen und Resultate ausreichen. Die Darstellung hält sich eng an die geometrische Sichtweise, die – grob gesprochen – einen R-linearen Code mit Punkten in einer projektiven Geometrie über R identifiziert. Die Hyperebenen der Geometrie entsprechen dann den Codewörtern, und die Gewichte der Codewörter lassen sich durch Schnitteigenschaften der Hyperebenen mit den gewählten Punkten ausdrücken. Auf diese Art erhält man einen basisfreien Zugang zur Codierungstheorie.[9]

Für herkömmliche lineare Codes ist dieser Ansatz beispielsweise in [35] beschrieben. Unsere Situation ist von den Arbeiten [65, 69, 71] abgedeckt, wo allgemeiner lineare Codes über endlichen Kettenringen mit projektiven Hjelmslev-Geometrien in Verbindung gebracht werden. Die geometrische Sichtweise ermöglicht uns die Untersuchung und Konstruktion ringlinearer Codes mit Hilfe geometrischer Methoden.

1.3. Entstehung dieser Arbeit

Im Jahr 2009 modifizierte Johannes Zwanzger seinen ursprünglich für herkömmliche lineare Codes geschriebenen Algorithmus [131] für die Suche nach linearen Codes über endlichen Kettenringen. Damit gelang es ihm, zwei binäre Codes mit den neuen BTL-Parametern $(58, 2^7, 28)_2$ und $(114, 2^8, 56)_2$ als Gray-Bilder $\mathbb{Z}_4$-linearer Codes zu finden. Im Anschluss wurde im Rahmen des DFG-Projekts WA 1666/4 zusammen mit Johannes Zwanzger der Ansatz aus [13, 95] benutzt, um eine Suche nach linearen Codes über endlichen Kettenringen mit vorgeschriebenen Automorphismen durchzuführen. Insbesondere über dem Ring $\mathbb{Z}_4$ ergaben sich etliche neue BTL- und BTKL-Codes. Diese Resultate sind online zugänglich [88] und teilweise Inhalt der Dissertation von Johannes Zwanzger [132].

Die auf diese Weise neu gefundenen Codes wurden einer rechnergestützten Analyse hinsichtlich diverser geometrischer oder kombinatorischer Eigenschaften unterzogen. Bei manchen Codes zeichnete sich dabei eine deutliche Struktur ab, die nun als zusätzliche Information umgekehrt wieder in die Computersuche eingebracht werden konnte, um damit nach ähnlich aufgebauten Codes – etwa mit einer größeren Länge, in höherer Dimension oder über einem größeren Grundring – in zuvor nicht mehr zugänglichen Parameterbereichen zu suchen. Durch Erfolge und Misserfolge kristallisierten sich auf diese Weise immer deutlichere Strukturmerkmale heraus, die es einerseits erlaubten, mit einer weiter spezialisierten Suche in noch größere Parameterbereiche vorzudringen, und andererseits allmählich zu Vermutungen über unendliche Serien von Codes und deren Parameter führten.

[9] Betrachtet man Codewörter als Koordinatenvektoren von Vektoren in R^n, so hängt das Gewicht eines Codeworts von der gewählten Basis ab (üblicherweise ist die Standardbasis ausgewählt). Schnittzahlen zwischen Punktmengen und Hyperebenen sind dagegen basisunabhängig.

Tabelle 1.4.1.: Gray-Bilder spezieller Codes der in dieser Arbeit konstruierten Serien

Beispiel	Code	Gray-Bild	Status	Kommentar
3.1.16	$\mathcal{T}_{2,5,2}$	$(248, 2^{10}, 120)_2$	BTKL	unveröffentlicht
3.1.19	$\mathcal{T}_{4,3,0}$	$(84, 4^6, 60)_4$	BTKL	[55]
3.2.7	$\mathcal{T}^*_{2,5,0}$	$(372, 2^{10}, 184)_2$	BTL	[91, 92]
3.2.9	$\mathcal{T}^*_{4,3,0}$	$(504, 4^6, 376)_4$	BTKL	[85]
3.2.12	$\hat{\mathcal{K}}^*_{3+1}$	$(114, 2^8, 56)_2$	BTL	[132, 89, 91, 92]
3.2.13	$\hat{\mathcal{K}}^*_{5+1}$	$(1988, 2^{12}, 992)_2$	BTL	[89, 91, 92]
3.3.9	$\hat{\mathcal{S}}_{2,3}$	$(58, 2^7, 28)_2$	BTL	[132, 90, 91]
3.3.10	$\hat{\mathcal{S}}_{2,4}$	$(244, 2^9, 120)_2$	BTKL	[91, 92]

1.4. Vier neue unendliche Serien ringlinearer Codes

In Kapitel 3 werden nun insgesamt vier neue unendliche Serien von R-linearen Codes vorgestellt, nämlich die beiden 3-Parameter-Serien $\mathcal{T}_{q,k,s}$ und $\mathcal{T}^*_{q,k,s}$, die 2-Parameter-Serie $\hat{\mathcal{S}}_{q,k}$ und über dem Ring $\mathbb{Z}_4$ die 1-Parameter-Serie $\hat{\mathcal{K}}^*_{k+1}$. Dabei ist $q = 2^r$ und $R = \mathrm{GR}(4, r)$ ein Galois-Ring der Charakteristik 4. Die Arbeit schließt in Kapitel 4 mit einer Diskussion offener und neu aufgeworfener Fragen.

Die vier neuen Serien haben hervorragende Fehlerkorrektureigenschaften: In den Parameterbereichen, wo ein Vergleich mit den Codetabellen möglich ist, sind alle Gray-Bilder der Codes der vier Serien BTL oder BTKL. Eine Übersicht ist in Tabelle 1.4.1 gegeben. Dort nicht aufgeführt sind Codes, deren Parameter sich trivial aus den Kerdock-Codes ableiten lassen.

Obwohl das Auffinden der einzelnen Codeserien erst durch massiven Computereinsatz ermöglicht wurde, sind die in dieser Arbeit gegebenen Beweise ihrer Parameter letztlich völlig computerfrei. Hierfür erwies sich die geometrische Sichtweise als sehr fruchtbar.

Jede dieser Konstruktionen baut auf die eine oder andere Weise auf der Teichmüller-Menge in einem Galois-Ring der Charakteristik 4 auf. Diese Teichmüller-Menge hat eine reiche kombinatorische Struktur (siehe z.B. [8, Sect. III], [59, Sect. VI] oder Satz 3.1.5), wodurch sich Codes mit sehr wenigen Gewichten und hoher Minimaldistanz ergeben. Teichmüller-Mengen existieren auch in ungerader Charakteristik sowie allgemeiner in jedem Kettenring der Kettenlänge 2, so dass sich die Konstruktionen prinzipiell auch über diesen Ringen durchführen lassen. Im allgemeinen Fall verhält sich die Teichmüller-Menge jedoch völlig anders als in einem Galois-Ring der Charakteristik 4, infolgedessen sich uninteressante Codes mit schlechter Minimaldistanz ergeben. Neben der Tatsache, dass bisher kein einziger BTL- oder BTKL-Code in ungerader Charakteristik oder über einem allgemeineren Kettenring bekannt ist, ist dies der Grund für die Beschränkung auf Galois-Ringe der Charakteristik 4.[10]

[10] Z.B. liegt auch den Kerdock-Codes eine Teichmüller-Menge zugrunde, weshalb diese Codes bisher nur in Charakteristik 4 betrachtet wurden.

Im Folgenden werden noch genauere Einzelheiten zu den vier Serien angegeben.

Verallgemeinerte Teichmüller-Codes

Aufbauend auf den Untersuchungen von Thomas Honold [59] wird in Abschnitt 3.1 entschieden, unter welchen Umständen eine die Teichmüller-Gruppe des Galois-Rings $S = \mathrm{GR}(4, kr)$ umfassende echte Untergruppe $\Sigma < S^*$ durch die Partition

$$\{\{0\},\ 2S \setminus \{0\},\ \Sigma,\ S^* \setminus \Sigma\}$$

ein symmetrisches Translationsschema $\mathcal{A}_\Sigma$ auf $(S, +)$ induziert (Satz 3.1.5), und unter welchen Bedingungen eine solche Gruppe Σ die Einheitengruppe R^* eines Galois-Teilrings $R = \mathrm{GR}(4, r)$ von S enthält (Lemma 3.1.2). Bei der Charakterisierung spielen symmetrische Bilinearformen über $\mathbb{F}_2$ eine wichtige Rolle. Die resultierenden Familien von Gruppen Σ und Translationsschemata $\mathcal{A}_\Sigma$ zerfallen in zwei Typen I und II. Die Translationsschemata vom Typ II sind bereits bekannt [76, Th. 9]. Die für die Codierungstheorie interessanteren Translationsschemata vom Typ I scheinen im Wesentlichen neu zu sein (Bemerkung 3.1.6(d)).

Von den Gruppen Σ erhalten wir zwei Serien von Punktmengen $\mathfrak{T}_{q,k,s}$ (Typ I) und $\mathfrak{U}_{q,k,s}$ (Typ II) in der projektiven Hjelmslev-Geometrie $\mathrm{PHG}(R^k)$ mit $k \geq 3$ und

$$s \in \begin{cases} \{0, 2, 4, \ldots, (k-1)r\} & \text{falls k ungerade,} \\ \{r, r+2, r+4, \ldots, (k-1)r\} & \text{falls k gerade,} \end{cases}$$

die für $s \neq (k-1)r$ nur zwei verschiedene Schnittzahlen mit den Hyperebenen aufweisen (Satz 3.1.8). Die von den Punktmengen $\mathfrak{U}_{q,k,s}$ mit $s \neq (k-1)r$ induzierten R-linearen Codes haben nur zwei von Null verschiedene Gewichte (sind also *two-weight codes*) und erzeugen stark reguläre Graphen (Satz 3.1.12). Die Punktmengen $\mathfrak{T}_{q,k,s}$ verallgemeinern die Teichmüller-Punktmengen aus [59] und induzieren R-lineare Codes $\mathcal{T}_{q,k,s}$. Diese Codes verallgemeinern die Teichmüller-Codes ($s = 0$), welche wiederum die verkürzten $\mathbb{Z}_4$-linearen Kerdock-Codes ($s = 0, q = 2$) und die von den Hyperovalen in [67] induzierten Codes ($s = 0, k = 3$) als Spezialfälle enthalten. Im Fall $s = 1, q = 2$ erhalten wir Codes mit den Parametern der zweifach verkürzten $\mathbb{Z}_4$-linearen Kerdock-Codes, und im Fall $s = (k-1)r$ erhalten wir die Simplex-Codes $\mathrm{Sim}(k, R)$ [65, Sec. 6.1], siehe auch Abschnitt 2.4.1. Das Gray-Bild von $\mathcal{T}_{q,k,s}$ hat die Parameter (Satz 3.1.10)

$$\left(2^s q \cdot \frac{q^k - 1}{q - 1},\quad q^{2k},\quad 2^s q^k - 2^{s/2} q^{\frac{k-1}{2}}\right)_q.$$

Die für diese Konstruktion benötigten Grundlagen über symmetrische Bilinearformen in endlichdimensionalen $\mathbb{F}_2$-Vektorräumen und über symmetrische Assoziationsschemata werden in den Anhängen A und B bereitgestellt.

Dualisierte verallgemeinerte Teichmüller-Codes

Durch Dualisieren der Punktmengen $\mathfrak{T}_{q,k,s}$ mit $s \neq (k-1)r$ in der projektiven Hjelmslev-Geometrie $\mathrm{PHG}(R^k)$ ergeben sich Punktmengen $\mathfrak{T}^*_{q,k,s}$, die wieder nur zwei verschiedene Schnittzahlen mit den Hyperebenen aufweisen. Die erzeugten Codes $\mathcal{T}^*_{q,k,s}$ verallgemeinern die bereits in [92] veröffentlichten Codes $\mathcal{T}^*_{q,k}$ (Spezialfall $s = 0$). Das Gray-Bild von $\mathcal{T}^*_{q,k,s}$ hat die Parameter (Satz 3.2.3(b))

$$\left(\frac{1}{2}\frac{q^k-1}{q-1}\left(q^k - 2^{s/2}q^{\frac{k+1}{2}}\right),\quad 2^k,\quad \frac{1}{2}q^{k-1}\left(q^k - 2^{s/2}q^{\frac{k+1}{2}} - 1\right)\right)_q.$$

Im Fall $s = (k-1)r-2$ stimmen die Spektren von $\mathfrak{T}_{q,k,(k-1)r-2}$ und $\mathfrak{T}^*_{q,k,(k-1)r-2}$ überein, so dass $\mathfrak{T}_{q,k,(k-1)r-2}$ eine formal selbstduale Punktmenge ist (Satz 3.2.5).

Dualisierte Kerdock-Codes

Eine ähnliche Konstruktion kann für die zu den $\mathbb{Z}_4$-linearen Kerdock-Codes $\mathcal{K}_{k+1}$ gehörenden Punktmengen $\mathfrak{K}_{k+1}$ mit ungeradem $k \geq 3$ durchgeführt werden. Die Berechnung des symmetrisierten Gewichtszählers des resultierenden Codes $\mathcal{K}^*_{k+1}$ wird durch die Formel in [70] ermöglicht. Die Codes $\mathcal{K}^*_{k+1}$ lassen sich hier noch durch Konstruktion X mit einem Wiederholungscode geeigneter Länge zu den Codes $\hat{\mathcal{K}}^*_{k+1}$ verbessern. Diese Konstruktion wurde bereits in [92] veröffentlicht. Das Gray-Bild von $\hat{\mathcal{K}}^*_{k+1}$ hat die Parameter (Satz 3.2.11)

$$\left(2^{2k+1} - 2^{k+1} + 2^{\frac{k-1}{2}},\quad 2^{2k+2},\quad 2^{2k} - 2^k\right)_2.$$

Verlängerte Simplex-Codes

Wir untersuchen, wie die $(q-1)$-fache Wiederholung der Simplex-Codes $\mathrm{Sim}(R,k)$ mit $k \geq 3$ durch Anhängen einer Torsionszeile an die Generatormatrix vergrößert werden kann. Dazu wird der zusätzlichen Zeile eine Punktmenge $\mathfrak{k}$ in $\mathrm{PHG}(R^k)$ zugeordnet. Der symmetrisierte Gewichtszähler des vergrößerten Codes $\mathrm{SimAug}(\mathfrak{k})$ kann dann in Abhängigkeit vom Spektrum der Punktmenge $\mathfrak{k}$ berechnet werden (Satz 3.3.2). Anschließend wird analysiert, welche der Punktmengen $\mathfrak{T}_{q,k,s}$ und $\mathfrak{T}^*_{q,k,s}$ die beste Minimaldistanz des vergrößerten Codes liefern (Lemma 3.3.4). Wie im Fall der Codes $\mathcal{K}^*_{k+1}$ lassen sich die resultierenden Codes noch durch Konstruktion X mit einem Wiederholungscode geeigneter Länge zu den Codes $\hat{\mathcal{S}}_{q,k}$ verbessern. Diese Konstruktion verallgemeinert die bereits in [90] veröffentlichten Codes, welche den Spezialfall $k = 3$ bilden. Das Gray-Bild von $\hat{\mathcal{S}}_{q,k}$ hat die Parameter (Satz 3.3.6 und Satz 3.3.7)

$$\begin{cases} \left(2^{2k} - 2^k + 2^{\lceil\frac{k-1}{2}\rceil},\quad 2^{2k+1},\quad 2^{2k-1} - 2^{k-1}\right)_2 & \text{falls } q = 2, \\ \left(q^{2k} - q^k + q^{k-1} - q^{k-2},\quad q^{2k+1},\quad q^{2k} - q^{2k-1} - q^k + q^{k-1}\right)_q & \text{falls } q \geq 4. \end{cases}$$

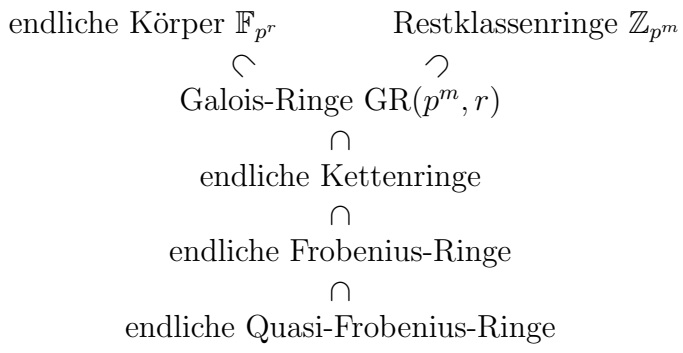
2. Grundlagen

2.1. Galois-Ringe

In diesem Abschnitt werden die Grundringe der später betrachteten ringlinearen Codes vorgestellt.[11] Details findet man beispielsweise in [109, 112].

In [109, S. 307] sind zwei Gründe für die Bedeutung der Galois-Ringe aufgeführt: Zum einen bilden sie eine Oberklasse sowohl der endlichen Körper als auch der Restklassenringe der ganzen Zahlen modulo einer Primzahlpotenz. Dies ermöglicht eine einheitliche Behandlung gewisser kombinatorischer Fragestellungen über diesen beiden Ringklassen (in unserem Fall ist das natürlich die Codierungstheorie). Zum anderen sind die Galois-Ringe wichtige Grundbausteine in der Theorie der endlichen Ringe.

Viele Eigenschaften der Galois-Ringe sind in ihrer Idealstruktur – einer Kette – begründet. Daher überrascht es nicht, dass sich etliche Resultate ohne Mühe auf die endlichen Kettenringe ausweiten lassen, also auf endliche Ringe, deren Verband der Linksideale (und dann auch Rechtsideale) eine Kette ist.[12] Die endlichen Kettenringe sind in der Klasse der endlichen Frobenius-Ringe enthalten, und diese wiederum in der Klasse der endlichen Quasi-Frobenius-Ringe, die von vielen Codierungstheoretikern als die größte noch für die Codierungstheorie taugliche Ringklasse angesehen wird. Die Einordnung in die Hierarchie endlicher Ringe ist an folgendem Diagramm veranschaulicht:



Definition 2.1.1 *Sei p eine Primzahl, m eine positive ganze Zahl und $f \in \mathbb{Z}_{p^m}[X]$ ein normiertes Polynom vom Grad $r \geq 1$, so dass sein Bild modulo p in $\mathbb{F}_p[X]$ irreduzibel ist. Der Ring $\mathbb{Z}_{p^m}[X]/(f)$ heißt* Galois-Ring $\mathrm{GR}(p^m, r)$ *der Charakteristik p^m vom Rang r.*

[11] Unter einem Ring verstehen wir einen nicht zwingend kommutativen Ring mit Einselement.

[12] Alternativ lassen sich die endlichen Kettenringe als die endlichen lokalen Hauptidealringe charakterisieren.

Die Ordnung dieses Galois-Rings ist $\#\,\mathrm{GR}(p^m, r) = p^{mr}$. Unter vorgegebenen Parametern p, r und m hängt die Definition bis auf Ringisomorphie nicht von der genauen Wahl des Polynoms f ab ([98, Satz 8]). Die Galois-Ringe umfassen zwei wichtige Klassen endlicher Ringe: Die endlichen Körper $\mathbb{F}_{p^r} = \mathrm{GR}(p, r)$ und die Restklassenringe der ganzen Zahlen modulo einer Primzahlpotenz $\mathbb{Z}_{p^m} = \mathrm{GR}(p^m, 1)$. Im Folgenden sind die Bezeichner p, m, r, $q = p^r$ und $R = \mathrm{GR}(p^m, r)$ wie in Definition 2.1.1 fest vorgegeben.

Bemerkung 2.1.2 Die Galois-Ringe tauchen erstmals 1924 unter dem Namen *Grundringe* bei Krull auf [98, §4]. Sie wurden 1966 von Janusz [78, S. 476] und 1969 von Raghavendran [119, Sec. 3.1] offenbar unabhängig voneinander neu entdeckt und von beiden Autoren aufgrund der starken Verwandtschaft zu den endlichen Körpern *Galois-Ringe* genannt. Der oben eingeführte Bezeichner GR(Charakteristik, Rang) ist von Janusz übernommen. Raghavendran benutzt denselben Bezeichner GR, allerdings mit den Parametern GR(Ordnung, Charakteristik). In der Literatur sind heute beide Varianten üblich, wobei erstere die häufigere zu sein scheint.

2.1.1. Wahl des definierenden Polynoms

Für die explizite Darstellung von endlichen Körpern $\mathbb{F}_{p^r}$ hat man das Problem, dass es im Allgemeinen viele verschiedene irreduzible Polynome vom Grad r über $\mathbb{F}_p$ gibt. Leider ist keine glatte mathematische Charakterisierung bekannt, die auf eindeutige Weise ein „schönes" Polynom auswählt. In aktuellen Computeralgebrasystemen wie Magma [10] werden hierfür die *Conway-Polynome* $f_{p^r} \in \mathbb{F}_p[X]$ benutzt. Diese werden rekursiv definiert: Das Conway-Polynom f_{p^r} ist das lexikographisch kleinste normierte primitive Polynom vom Grad r, das für alle echten Teiler s von r die Teilbarkeitseigenschaft $f_{p^s}(X) \mid f_{p^r}(X^{(p^r-1)/(p^s-1)})$ (*Norm-Kompatibilität*) erfüllt.[13]

Ist jedoch einmal eine Wahl für die definierenden Polynome der endlichen Körper getroffen, so ist der Schritt zu den Galois-Ringen nicht mehr schwierig: Für das definierende Polynom f von $\mathrm{GR}(p^m, r)$ bietet es sich an, den *Hensel-Lift* nach $\mathbb{Z}_{p^m}[X]$ des definierenden Polynoms $f_{p^r} \in \mathbb{F}_p[X]$ von $\mathbb{F}_{p^r}$ zu benutzen, also das eindeutig bestimmte normierte Polynom $f \in \mathbb{Z}_{p^m}[X]$ mit $f \mid X^{p^r-1} - 1$, dessen Bild modulo Rp mit f_{p^r} übereinstimmt (siehe z.B. [127]). Der Hensel-Lift kann effizient berechnet werden [22, Th. 1], [132, Sec. 1.3]. Im Fall $p = 2$ ist die *Methode von Gräffe* (benannt nach dem Mathematiker Karl Heinrich Gräffe) gut geeignet, siehe [126, Appendix V] und [52, Sec. III-A]. Neben dieser eindeutigen Auswahl des Polynoms f ergibt sich auch der Vorteil, dass im Fall eines primitiven Ausgangspolynoms f_{p^r} jede Nullstelle des Hensel-Lifts f ein Erzeuger der Teichmüller-Gruppe T^* (s.u.) ist. In der aktuellen Implementierung der Galois-Ringe in Magma wird leider nicht der Hensel-Lift, sondern der „naive" Lift von $\mathbb{F}_p[X]$ nach $\mathbb{Z}_{p^m}[X]$ benutzt.

[13] Laut [121] stammt die Idee, Norm-kompatible Polynome zur Darstellung der endlichen Körper zu benutzen, von J. H. Conway. Die exakte Definition der Conway-Polynome wurde 1990 von R. A. Parker in einem Vortrag mit dem Titel *Finite fields and Conway polynomials* im IBM Scientific Center in Heidelberg gegeben.

2.1.2. Eigenschaften

Der Galois-Ring $R = \mathrm{GR}(p^m, r)$ ist ein lokaler kommutativer Ring. Das eindeutige maximale Ideal ist das Hauptideal Rp. Der zugehörige *Restklassenkörper* R/Rp ist isomorph zu $\mathbb{F}_q$ mit $q = p^r$. Des Weiteren ist R ein Hauptidealring, und sein Idealverband bildet die Kette

$$\{0\} = Rp^m \subset Rp^{m-1} \subset \ldots \subset Rp^1 \subset Rp^0 = R.$$

Aus diesem Grund bezeichnen wir m auch als die *Kettenlänge* von R.

Die *Höhe* $h(x)$ eines Elements $x \in R$ ist die größte ganze Zahl $s \leq m$ mit $x \in Rp^s$. Es gilt $h(x) \in \{0, \ldots, m\}$. Zwei Ringelemente haben genau dann dieselbe Höhe, wenn sie assoziiert sind. Das einzige Ringelement von Höhe 0 ist das Nullelement, und die Ringelemente von Höhe m sind genau die Einheiten. Die Größe eines Ideals Rx schreibt sich unter Zuhilfenahme der Höhe als $\#(Rx) = q^{m-h(x)}$.

Einheiten und die p-adische Entwicklung

Die Einheitengruppe $R^* = R \setminus Rp$ hat die Ordnung $\#R^* = \#R - \#(Rp) = q^{m-1}(q-1)$. Weil q^{m-1} und $q-1$ teilerfremd sind und R^* abelsch ist, gibt es als Hall-Untergruppen von R^* genau eine Untergruppe T^* der Ordnung $q-1$ und genau eine Untergruppe H der Ordnung q^{m-1}. Die Untergruppe T^* ist zyklisch und heißt *Teichmüller-Gruppe*. Wählt man das definierende Polynom f von R als den Hensel-Lift eines primitiven Polynoms in $\mathbb{F}_p[X]$ vom Grad r, so ist $X + (f)$ ein Erzeuger von T^*. Weiter heißt $T = T^* \cup \{0\}$ die *Teichmüller-Menge* in R. Sie bildet ein multiplikativ abgeschlossenes Vertretersystem des Restklassenkörpers. Jedes Element $x \in R$ lässt sich eindeutig in der *p-adischen Entwicklung* $\sum_{i=0}^{m-1} t_i p^i$ mit Koeffizienten $t_i \in T$ schreiben. Ein Ideal Rp^i besteht genau aus den Elementen, für die in der p-adischen Entwicklung alle Koeffizienten bis einschließlich zum $(i-1)$-ten gleich 0 sind.

Weiter ist $H = 1 + Rp$ die Menge der *Haupteinheiten* (engl. *principal units*) von R. Die Untergruppen T^* und H sind in R^* komplementär. Genauer gilt:

Fakt 2.1.3 ([119, Th. 9]) *Es gilt $R^* = T^* \cdot H \cong T^* \times H$, dabei ist $T^* \cong \mathbb{Z}_{p^r-1}$ und*

$$H \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_{2^{m-1}}^{r-1} & \text{falls } p = 2 \text{ und } m \geq 3, \\ \mathbb{Z}_{p^{m-1}}^r & \text{sonst.} \end{cases}$$

Automorphismen und Galois-Teilringe

Wir definieren den *verallgemeinerten Frobenius-Automorphismus* von R mit Hilfe der p-adischen Entwicklung als

$$\phi : R \to R, \quad \sum_{i=0}^{m-1} t_i p^i \mapsto \sum_{i=0}^{m-1} t_i^p p^i.$$

Fakt 2.1.4 ([119, Prop. 2]) *Die Automorphismengruppe $\mathrm{Aut}(R)$ von R ist zyklisch von Ordnung r und wird vom verallgemeinerten Frobenius-Automorphismus erzeugt.*

Ein Galois-Ring $R = \mathrm{GR}(p^m, r)$ ist genau dann isomorph zum Teilring eines anderen Galois-Rings $S = \mathrm{GR}(c, s)$, wenn die Charakteristiken übereinstimmen (d.h. $c = p^m$) und r ein Teiler von s ist. In dieser Situation enthält S genau einen zu R isomorphen Teilring, welcher in perfekter Analogie zur Galois-Theorie über endlichen Körpern aus den Fixpunkten des Automorphismus $\phi^{s/r}$ von S besteht. In p-adischer Entwicklung sind dies alle Elemente, deren Koeffizienten Repräsentanten von Elementen in $\mathbb{F}_{q^r}$ sind. Betrachten wir R in S eingebettet, so ist die Teichmüller-Gruppe T^* von R eine Untergruppe der Teichmüller-Gruppe U^* von S, und R ist das Ring-Erzeugnis von T^* in S.

Auf diese Weise ist der Galois-Ring $S = \mathrm{GR}(p^m, rk)$ für jede positive ganze Zahl k ein freier R-Modul vom Rang k, so dass wir die Elemente von S mit Vektoren in R^k identifizieren dürfen. Diese Identifikation liefert einen R-Modulisomorphismus $R^k \cong S_R$,[14] der die Vektoren in R^k mit einer zusätzlichen multiplikativen Struktur versieht.

Anders als mancherorts behauptet (beispielsweise [119, Prop. 1] oder [109, Lemma XVI.7]) ist im Allgemeinen nicht jeder Teilring eines Galois-Rings selbst wieder ein Galois-Ring [81]. Beispielsweise bilden im Galois-Ring $\mathrm{GR}(4, 2)$ der Ordnung 16 die Elemente mit der 2-adischen Entwicklung $t_0 + 2t_1$ mit $t_0 \in \{0, 1\}$, $t_1 \in T$ einen Teilring der Ordnung 8, während der einzige echte Galois-Teilring $\mathrm{GR}(4, 1)$ die Ordnung 4 hat.

2.1.3. Gestutzte Witt-Vektoren

Ernst Witt gab 1937 eine Arithmetik an, die der Menge der Folgen (den *Witt-Vektoren*) über einem Körper K der Charakteristik p eine kommutative Ringstruktur $W(K)$ der Charakteristik 0 aufprägt [128]. Der *Witt-Ring* $W(\mathbb{F}_p)$ ist isomorph zum Ring der ganzen p-adischen Zahlen. Beschränkt man sich auf die ersten m Komponenten der Witt-Vektoren, so erhält man einen Teilring von $W(K)$, den Ring der *gestutzten Witt-Vektoren* $W_m(K)$ der Charakteristik p^m.

Für uns sind die gestutzten Witt-Vektoren aufgrund der Isomorphie $W_m(\mathbb{F}_{p^r}) \cong \mathrm{GR}(p^m, r)$ von Interesse [119, Th. 7]. Ein Isomorphismus $\mathrm{GR}(p^m, r) \to W_m$ bildet ein Element $a \in \mathrm{GR}(p^m, r)$ im Wesentlichen auf die Koeffizientenfolge seiner p-adischen Entwicklung ab [67, Th. 11]. In $R = W_m(\mathbb{F}_{p^r})$ ist das Nullelement durch $(0, \ldots 0)$ gegeben, das Einselement durch $(1, 0, \ldots, 0)$ und das Element p durch $(0, 1, 0, \ldots, 0)$. Die Teichmüller-Elemente haben die Form $(*, 0, \ldots, 0)$, und ein Element $(\alpha, 0, \ldots, 0)$ ist genau dann ein Erzeuger der Teichmüller-Gruppe, wenn $\alpha \in \mathbb{F}_{p^r}$ ein primitives Element ist. Die Haupteinheiten haben die Form $(1, *, \ldots, *)$. Für $i \in \{0, \ldots, m\}$ besteht das Ideal Rp^i aus allen Elementen von R, bei denen die ersten i Komponenten gleich 0 sind. Insbesondere ist ein Element genau dann invertierbar, wenn seine erste Komponente in $\mathbb{F}_{p^r}$ invertierbar ist. Für einen Teiler s von r besteht der eindeutige zu $\mathrm{GR}(p^m, s)$ isomorphe Teilring von R aus allen Elementen, deren Einträge im Teilkörper $\mathbb{F}_{p^s}$ von $\mathbb{F}_{p^r}$ liegen.

[14] Der Index R im Ausdruck S_R verdeutlicht, dass in diesem Moment S als ein R-Modul aufgefasst wird.

Die Arithmetik der Witt-Vektoren ist im Allgemeinen ziemlich kompliziert, weshalb wir uns hier auf den später benötigten Spezialfall $p = m = 2$ beschränken: Für $\mathbf{a} = (a_0, a_1), \mathbf{b} = (b_0, b_1) \in W_2(\mathbb{F}_{2^r})$ ist

$$\mathbf{a} + \mathbf{b} = (a_0 + b_0,\ a_1 + b_1 + a_0 b_0) \quad \text{und} \quad \mathbf{a} \cdot \mathbf{b} = (a_0 b_0,\ a_1 b_0^2 + b_1 a_0^2).$$

Weiter gilt

$$-\mathbf{a} = (a_0,\ a_0^2 + a_1) \quad \text{und} \quad \mathbf{a}^{-1} = (a_0^{-1},\ a_0^{-4} a_1) \text{ falls } a_0 \neq 0.$$

2.1.4. Endlich erzeugte Moduln über einem Galois-Ring

Im Folgenden werden die wichtigsten Struktursätze für endlich erzeugte R-Moduln diskutiert. Weil R endlich ist, ist ein R-Modul genau dann endlich erzeugt, wenn er endlich ist.

So wie die Galois-Ringe als eine Verallgemeinerung sowohl der endlichen Körper als auch der ganzzahligen Restklassenringe modulo einer Primzahlpotenz aufgefasst werden können, ist die Theorie der endlich erzeugten R-Moduln eine Verallgemeinerung sowohl der Theorie der endlichdimensionalen Vektorräume über endlichen Körpern als auch der Theorie der endlichen abelschen p-Gruppen.[15]

Die Theorie kann ohne Probleme noch auf die endlichen Kettenringe ausgeweitet werden, siehe hierzu [65, 69]. Möchte man noch allgemeiner über endlichen Frobenius-Ringen Codierungstheorie betreiben, so steht man vor dem Problem, dass keine einheitliche Beschreibung der endlich erzeugten Moduln bekannt ist.

Partitionen

Unter einer *Partition* λ verstehen wir eine schwach monoton fallende Folge $(\lambda_i)_{i \in \mathbb{N}}$ mit Koeffizienten $\lambda_i \in \mathbb{N}$,[16] in der nur endlich viele Einträge von Null verschieden sind. Die Nulleinträge werden bei der Angabe einer Partition üblicherweise weggelassen. Besteht keine Verwechslungsgefahr mit den üblichen Potenzen, so wird eine Partition

$$(\underbrace{a_0, \ldots, a_0}_{t_0 \text{ mal}}, \underbrace{a_1, \ldots, a_1}_{t_1 \text{ mal}}, \ldots).$$

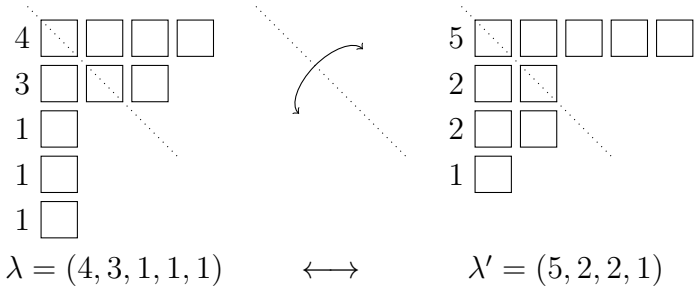
auch in *Exponentialschreibweise* als $(a_0^{t_0} a_1^{t_1} \ldots)$ geschrieben. Auf die Exponentialschreibweise dürfen die gewohnten Potenzrechenregeln angewendet werden. Beispielsweise beschreiben die Ausdrücke $(4^1 3^1 1^3)$, $(1^3 3^1 4^1)$, $(4 \cdot 3 \cdot 1^3)$, $(4^1 3^1 2^0 1^3)$ und $(0^3 1^1 4^1 3^1 1^2)$ alle die Partition $(4, 3, 1, 1, 1)$.

Die Anzahl der Partitionsglieder ungleich Null heißt *Länge* $\ell(\lambda)$ von λ, und das größte Folgenglied λ_0 heißt *Höhe*. Weiter heißt die Zahl $\#\lambda = \sum_{i \in \mathbb{N}} \lambda_i \in \mathbb{N}$ das *Gewicht* von λ. Die Partitionen vom Gewicht $n \in \mathbb{N}$ entsprechen genau den Möglichkeiten, die Zahl n in positive ganzzahlige Summanden zu zerlegen, wobei nicht nach der Reihenfolge der Summanden unterschieden wird.

[15] Die endlich erzeugten Moduln über dem Galois-Ring $\mathbb{Z}_{p^m}$ sind genau die endlichen abelschen p-Gruppen vom Exponent höchstens p^m.

[16] In dieser Arbeit ist $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Abbildung 2.1.: Ferrers-Diagramm einer Partition und ihrer konjugierten Partition



Oft ist es günstig, eine Partition in einem sogenannten *Ferrers-Diagramm* zu veranschaulichen. Hierzu wird jede Komponente λ_i von λ als eine Zeile von λ_i Kästchen dargestellt, die linksbündig untereinandergesetzt werden. Das Gewicht $\#\lambda$ ist dann die Gesamtzahl der Kästchen im Diagramm. Spiegelt man das Ferrers-Diagramm einer Partition λ entlang der Diagonale von links oben nach rechts unten, so entsteht wieder ein Ferrers-Diagramm, siehe Abbildung 2.1. Die zugehörige Partition wird als die *konjugierte Partition* λ' von λ bezeichnet. Offenbar ist $(\lambda')' = \lambda$ und $\#\lambda = \#\lambda'$. Formal lässt sich λ' auch definieren als die Partition

$$(\#\{j \in \mathbb{N} \mid \lambda_j > i\})_{i \in \mathbb{N}}$$

Es gilt $\ell(\lambda') = \lambda_0$ und $\ell(\lambda) = (\lambda')_0$. Mit Hilfe der konjugierten Partition ergibt sich die Exponentialschreibweise als $\left(\prod_{i=1}^{\infty} i^{\lambda'_{i-1}-\lambda'_i}\right)$.

Für zwei Partitionen λ und μ schreiben wir $\lambda \leq \mu$, wenn $\lambda_i \leq \mu_i$ für alle $i \in \mathbb{N}$ gilt. Damit ist auf der Menge aller Partitionen eine Halbordnung definiert, die sogar einen distributiven Verband bildet, den sogenannten *Young-Verband*. Anschaulich bedeutet $\lambda \leq \mu$, dass das Ferrers-Diagramm von λ im Ferrers-Diagramm von μ enthalten ist. Es ist $\lambda \leq \mu$ genau dann, wenn $\lambda' \leq \mu'$.

Der konjugierte Umriss

Es gilt folgende Verallgemeinerung des Hauptsatzes über endliche abelsche Gruppen:

Fakt 2.1.5 ([109, S. 310, Th. XVI.2]) *Es sei M ein endlich erzeugter R-Modul. Dann existiert genau eine Partition λ der Höhe höchstens m mit*

$$M \cong Rp^{m-\lambda_0} \oplus \ldots \oplus Rp^{m-\lambda_{\ell(\lambda)-1}}.$$

Die Partition λ aus Fakt 2.1.5 heißt *Umriss* (engl. *shape*, siehe [64, Def. 2] und [65, Def. 2.1]) $\mathrm{shp}(M)$ von M. Als trennende Invariante auf den endlich erzeugten R-Moduln ist der Umriss eine direkte Verallgemeinerung des Dimensionsbegriffs der linearen Algebra über Körpern. In vielen Fragestellungen erscheint es natürlicher, nicht den Umriss λ, sondern den konjugierten Umriss $\mathrm{cshp}(M) = \mathrm{shp}(M)' = \lambda'$ zu betrachten. Ist beispielsweise R ein endlicher Körper und M ein endlich erzeugter R-Vektorraum, so hat M

genau dann die R-Dimension n, wenn M als R-Modul den konjugierten Umriss (n) der Länge 1 hat. Aus diesem Grund werden wir im Folgenden konsequent den konjugierten Umriss anstelle des Umrisses benutzen.

Es gilt $\#M = q^{\#\operatorname{cshp}(M)} = q^{\#\operatorname{shp}(M)}$. Der R-Modul M ist genau dann frei, wenn $\operatorname{cshp}(M) = (k^m)$ mit $k \in \mathbb{N}$ gilt. In diesem Fall ist k der Rang von M.

Für zwei Partitionen λ und μ ist der *verallgemeinerte Gauß-Koeffizient* definiert als

$$\begin{bmatrix}\lambda\\ \mu\end{bmatrix}_q = \prod_{i=0}^{\infty}\left(q^{\mu_{i+1}(\lambda_i-\mu_i)} \cdot \begin{bmatrix}\lambda_i-\mu_{i+1}\\ \mu_i-\mu_{i+1}\end{bmatrix}_q\right).$$

Dabei bezeichnet für $n \in \mathbb{Z}$, $k \in \mathbb{N}$

$$\begin{aligned}\begin{bmatrix}n\\ k\end{bmatrix}_q &= \begin{cases}\prod_{i=0}^{k-1} \frac{q^{n-i}-1}{q^{i+1}-1} & \text{falls } n \geq 0\\ 0 & \text{falls } n < 0\end{cases}\\ &= \begin{cases}0 & \text{falls } k > n,\\ 1 & \text{falls } k \in \{0, n\},\text{[17]}\\ \frac{(q^n-1)(q^{n-1}-1)\cdot\ldots\cdot(q^{n-k+1}-1)}{(q-1)(q^2-1)\cdot\ldots\cdot(q^k-1)} & \text{falls } k \in \{1,\ldots,n-1\}\end{cases}\end{aligned}$$

den herkömmlichen Gauß-Koeffizienten, der im Fall $n \geq 0$ die Anzahl der Unterräume der Dimension k in einem n-dimensionalen $\mathbb{F}_q$-Vektorraum angibt. Für $\mu \not\leq \lambda$ wird einer der herkömmlichen Gauß-Koeffizienten in der Definition von $\begin{bmatrix}\lambda\\ \mu\end{bmatrix}_q$ gleich Null, so dass sich in diesem Fall $\begin{bmatrix}\lambda\\ \mu\end{bmatrix}_q = 0$ ergibt.

Auch hier bietet es sich an, natürliche Zahlen a mit der Partition (a) der Länge 1 zu identifizieren, denn für Partitionen $\lambda = (n)$ und $\mu = (k)$ stimmt der verallgemeinerte Gauß-Koeffizient mit dem üblichen Gauß-Koeffizienten überein.

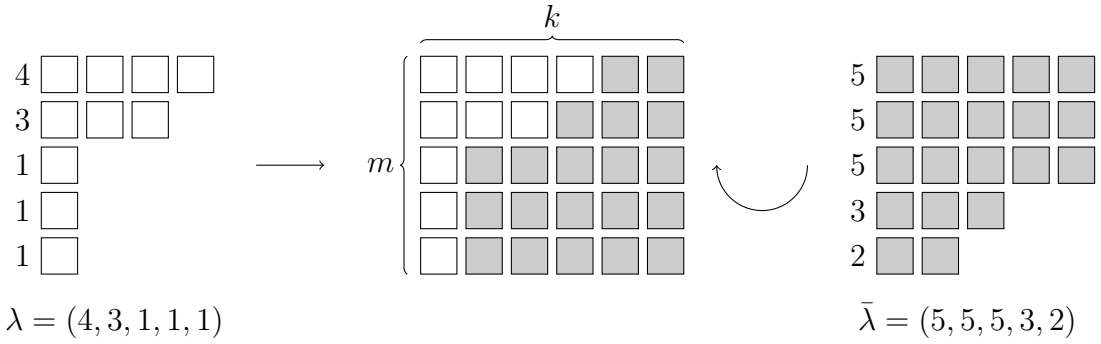
Bemerkung 2.1.6 Die Definition des verallgemeinerten Gauß-Koeffizienten in [86] weicht von der obigen insofern ab, als die Eingabepartitionen λ und μ durch ihre konjugierten Partitionen ersetzt wurden. Um die herkömmlichen Gauß-Koeffizienten einzubetten, muss man dann aber n mit der Partition (1^n) identifizieren. Die obige Definition wurde gewählt, weil zum einen die Identifikation von n mit (n) natürlicher erscheint und man zum anderen innerhalb der Definition ohne eine „Verdrehung" von λ bzw. μ zu λ' bzw. μ' auskommt.

Die vorgenommene Definition der verallgemeinerten Gauß-Koeffizienten wird durch die folgende Aussage gerechtfertigt:

Fakt 2.1.7 ([65, Th. 2.4]) *Seien λ und μ zwei Partitionen. Ein R-Modul vom konjugierten Umriss λ enthält genau dann einen Untermodul vom konjugierten Umriss μ, wenn $\mu \leq \lambda$ ist. Genauer ist die Anzahl der Untermoduln vom konjugierten Umriss μ gegeben durch den verallgemeinerten Gauß-Koeffizienten $\begin{bmatrix}\lambda\\ \mu\end{bmatrix}_q$.*

[17] Im Fall $k = 0$ steht ein leeres Produkt.

Abbildung 2.2.: Ferrers-Diagramm des komplementären konjugierten Umrisses



Bemerkung 2.1.8

(a) Für die Galois-Ringe $R = \mathbb{Z}_{p^m}$ zählt Fakt 2.1.7 genau die Untergruppen vom Typ μ einer endlichen abelschen p-Gruppe vom Typ λ. Dieses Resultat wurde laut [15, S. 22] im Jahr 1948 unabhängig voneinander in drei Artikeln publiziert, auf Englisch [130], auf Französisch [33] (durch Möbius-Inversion auf dem Untergruppenverband, siehe auch [26]) und auf Russisch [36].

(b) Die den verallgemeinerten Gauß-Koeffizienten zugrundeliegende Fragestellung lässt sich noch verfeinern: Gibt man zusätzlich zu λ und μ noch eine dritte Partition ν vor, so sei $g^{\lambda}_{\mu\nu}(q)$ die Anzahl der Untermoduln N eines endlichen R-Moduls M vom Umriss λ, für die $\mathrm{shp}(N) = \mu$ und $\mathrm{shp}(M/N) = \nu$ ist. Im Jahr 1959 definierte Philip Hall diese Zahlen in der Situation von endlichen abelschen p-Gruppen M und zeigte, dass $g^{\lambda}_{\mu\nu}$ ein Polynom in p mit ganzzahligen Koeffizienten ist [51]. Aus diesem Grund werden die Polynome $g^{\lambda}_{\mu\nu}$ heute als *Hall-Polynome* bezeichnet, tatsächlich tauchten diese Polynome samt der zugehörigen Hall-Algebra bereits 1901 bei Ernst Steinitz auf [123]. Als ein Spezialfall der Resultate von [106] gelten diese Ergebnisse auch für endlich erzeugte R-Moduln. Insbesondere ist es legitim, in der obigen Situation die Anzahl $g^{\lambda}_{\mu\nu}$ nur mit der Zahl q zu parametrisieren und nicht mit dem Ring R. Offenbar gilt $\sum_{\nu} g^{\lambda}_{\mu\nu}(q) = \begin{bmatrix} \lambda' \\ \mu' \end{bmatrix}_q$, d.h. die Hall-Polynome verfeinern die Information der verallgemeinerten Gauß-Koeffizienten. Allerdings sind die Hall-Polynome deutlich schwieriger explizit zu berechnen als die verallgemeinerten Gauß-Koeffizienten, siehe z.B. [110].

Sei nun ein freier R-Modul M_R vom Rang k fest als Umgebungsraum vorgegeben und die *Graßmann-Varietät* $\mathcal{G}(M_R, \lambda)$ definiert als die Menge aller Untermoduln von M_R eines vorgegebenen konjugierten Umrisses λ. Nach Fakt 2.1.7 gilt

$$\#\mathcal{G}(M_R, \lambda) = \begin{bmatrix} (k^m) \\ \lambda \end{bmatrix}_q .$$

Im Fall $\lambda \leq (k^m)$ definieren wir weiter den *komplementären konjugierten Umriss* $\bar{\lambda}$ anschaulich durch dasjenige Ferrers-Diagramm, das – um 180 Grad gedreht – das

Ferrers-Diagramm von λ zum Ferrers-Diagramm des konjugierten Umrisses (k^m) des Umgebungsraum R^k, also zu einem $(m \times k)$-Rechteck ergänzt. In Abbildung 2.2 ist ein Beispiel mit $m = 5$ und $k = 6$ zu sehen. Formal ist der komplementäre konjugierte Umriss definiert als

$$\bar{\lambda} = (k - \lambda_{m-i-1})_{i \in \{0,\ldots,m-1\}}.$$

Für jeden R-Modul $M \leq R^k$ vom konjugierten Umriss λ hat der Faktormodul R^k/M den konjugierten Umriss $\bar{\lambda}$.

Für zwei Vektoren $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in R^n$ ist das *Standardskalarprodukt* wie üblich erklärt als

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i.$$

Für eine beliebige Teilmenge $M \subseteq R^n$ definieren wir den *orthogonalen* (auch: *dualen*) Untermodul als

$$M^\perp = \{\mathbf{x} \in R^n \mid \mathbf{x} \cdot \mathbf{y} = 0 \text{ für alle } \mathbf{y} \in M\}.$$

Man prüft nach, dass $M^\perp$ tatsächlich ein Untermodul von R^m ist.

Fakt 2.1.9 ([64, Th. 3], [65, Th. 3.1]) *Sei $M \leq R^n$. Es gilt:*

(a) $\mathrm{cshp}(M^\perp) = \overline{\mathrm{cshp}(M)}$.

(b) $(M^\perp)^\perp = M$.

(c) $\perp$ *induziert einen Verbandsantiautomorphismus auf dem Verband aller Untermoduln von R^n. Insbesondere gilt*

$$(U + V)^\perp = U^\perp \cap V^\perp \quad \textit{und} \quad (U \cap V)^\perp = U^\perp + V^\perp$$

für alle Untermoduln U und V von R^n.

Mit Fakt 2.1.7 folgt daraus unmittelbar:

Fakt 2.1.10 ([57, Prop. 1]) *Seien λ und μ zwei Partitionen kleiner gleich (k^m). Ein R-Modul vom konjugierten Umriss λ ist in genau $\begin{bmatrix} \bar{\lambda} \\ \bar{\mu} \end{bmatrix}_q$ Untermoduln von R^k vom konjugierten Umriss μ enthalten.*

2.2. Lineare Codes über Galois-Ringen der Kettenlänge 2

Es wird nun ein Abriss über die Codierungstheorie über Galois-Ringen der Kettenlänge 2 gegeben. Die Theorie kann ohne Probleme auf endliche Kettenringe beliebiger Kettenlänge verallgemeinert werden [65, 69], für die späteren Anwendungen ist die hier beschriebene Situation jedoch ausreichend. Die traditionelle Codierungstheorie über endlichen Körpern wird als bekannt vorausgesetzt, hierzu sei auf die Lehrbücher [53, 75, 5] verwiesen.

Im Folgenden ist immer p eine Primzahl, r eine positive ganze Zahl, $q = p^r$ und R der Galois-Ring $\mathrm{GR}(p^2, r)$. Weiter seien für $i \in \{0, 1\}$ Vertretersysteme R_i von R/Rp^i mit $0 \in R_i$ vorgegeben. Es gilt stets $R_0 = \{0\}$, und eine natürliche Wahlmöglichkeit für R_1 ist beispielsweise die Teichmüller-Menge von R. Die Ordnung von R ist $\#R = q^2$. Das einzige nichttriviale Ideal Rp hat die Größe $\#(Rp) = q$.

Definition 2.2.1 *Eine Teilmenge $\mathcal{C}$ von R^n mit $n \in \mathbb{N}$ heißt* Blockcode *der Länge n über R. Wenn $\mathcal{C}$ ein Untermodul des R-Moduls R^n ist, heißt $\mathcal{C}$ auch R-*linearer *Code.*

Nach Fakt 2.1.5 wird der Isomorphietyp eines R-lineareren Codes $\mathcal{C}$ als R-Modul durch den konjugierten Umriss $\mathrm{cshp}(\mathcal{C}) = (\lambda_0, \lambda_1)$ beschrieben. Anstelle von λ_0 und λ_1 werden hierfür auch gerne die beiden Zahlen $k_1 = \lambda_1$ und $k_2 = \lambda_0 - \lambda_1$ angegeben, d.h. $\mathrm{cshp}(\mathcal{C}) = (k_1 + k_2, k_1)$. Es gilt $\#\mathcal{C} = q^{\lambda_0+\lambda_1} = q^{2k_1+k_2}$, und $\mathcal{C}$ ist als R-Modul genau dann frei, wenn $\lambda_0 = \lambda_1$ ist, bzw. dazu äquivalent wenn $k_2 = 0$ ist. Das Ferrers-Diagramm von $\mathrm{cshp}(\mathcal{C})$ ist dann ein $(2 \times k_1)$-Rechteck.

Ein Vektor $\mathbf{v} \in R^n$ ($n \in \mathbb{N}$) über R heißt *torsionsfrei* (auch: *fett*, siehe z.B. [65, 69]), wenn die Abbildung $R \to R^n$, $a \mapsto a\mathbf{v}$ injektiv ist, d.h. wenn wenigstens eine Komponente von $\mathbf{v}$ eine Einheit ist. Andernfalls heißt $\mathbf{v}$ *Torsionsvektor*. Die Menge aller Torsionsvektoren in R^n ist gegeben durch $(Rp)^n$, und für $\mathbf{v} \in (Rp)^n$ ist das Ergebnis der Skalarmultiplikation $a\mathbf{v}$ mit $a \in R$ bereits durch die Restklasse von a mod Rp bestimmt. Die Multiplikation mit p als Abbildung $R \to R$ ist ein Homomorphismus von R-Moduln, Kern und Bild der Abbildung ist Rp. Der Homomorphiesatz liefert also einen Isomorphismus von R-Moduln $\varphi : R/Rp \to Rp$. Durch koordinatenweises Fortsetzen erhalten wir mit $R/Rp \cong \mathbb{F}_q$ einen Isomorphismus von R-Moduln $\mathbb{F}_q^n \to (Rp)^n$, den wir wieder mit φ bezeichnen, und der den Untermodul $(Rp)^n$ aller Torsionsvektoren mit der Struktur eines $\mathbb{F}_q$-Vektorraums versieht. Insbesondere ist ein R-linearer Code mit $k_1 = 0$ ein Untermodul von $(Rp)^n$ und damit als herkömmlicher $\mathbb{F}_q$-linearer Code uninteressant.

2.2.1. Generatormatrizen

Sei im Folgenden wieder $\mathcal{C}$ ein R-linearer Code vom konjugierten Umriss $(k_1 + k_2, k_1)$. Der Code $\mathcal{C}$ ist der Zeilenraum einer Matrix $\mathbf{G} \in R^{(k_1+k_2)\times n}$, in der die oberen k_1 Zeilen torsionsfrei und die unteren k_2 Zeilen vom Nullvektor verschiedene Torsionsvektoren sind. Jede solche Matrix heißt *Generatormatrix* von $\mathcal{C}$. Die Abbildung $R^{k_1} \times R_1^{k_2} \to \mathcal{C}$, $\mathbf{x} \mapsto \mathbf{xG}$ ist eine Bijektion, und $\mathbf{x}$ wird *Informationsvektor* des Codeworts $\mathbf{xG}$ genannt. Ein Code heißt *fett* (auch: *regulär*, siehe z.B. [16]), wenn die Projektionsabbildung auf jede Koordinate surjektiv ist. Ein Code ist genau dann fett, wenn eine (und dann jede) Generatormatrix des Codes ausschließlich aus torsionsfreien Spalten besteht.

Bis auf eine Koordinatenpermutation hat jeder R-lineare Code $\mathcal{C}$ eine *systematische Generatormatrix* der Bauart (siehe [28, Gleichung (2)] für $R = \mathbb{Z}_4$, [22, Gleichung (1)] für $R = \mathbb{Z}_{p^m}$ und [115, Prop. 3.2] für endliche kommutative Kettenringe)

$$\begin{pmatrix} \mathbf{I}_{k_1} & \mathbf{A} & \mathbf{B} \\ \mathbf{0}_{k_2\times k_1} & p\mathbf{I}_{k_2} & p\mathbf{C} \end{pmatrix} \tag{2.1}$$

mit $\mathbf{A} \in R_1^{k_1 \times k_2}$, $\mathbf{B} \in R^{k_1 \times (n-(k_1+k_2))}$ und $\mathbf{C} \in R_1^{k_2 \times (n-(k_1+k_2))}$. Das Symbol $\mathbf{I}_a$ bezeichnet die $a \times a$ Einheitsmatrix und $\mathbf{0}_{a \times b}$ die $a \times b$ Nullmatrix.

Der Nachteil der systematischen Generatormatrix ist jedoch, dass sie den Ausgangscode nur bis auf eine Koordinatenpermutation darstellt. Dies könnte natürlich durch Rückpermutation der Koordinaten behoben werden. Aber da es mehrere Möglichkeiten für die Ausgangspermutation geben kann, ist die resultierende Matrix dann im Allgemeinen nicht eindeutig.

Abhilfe schafft bei Codes über endlichen Körpern die *reduzierte Zeilenstufenform* (engl. *row echelon form*). Diese kann auf R-lineare Codes verallgemeinert werden:

Definition 2.2.2 *Eine Matrix über R heißt in* reduzierter Zeilenstufenform*, wenn gilt: In jeder Zeile i gibt es genau ein* Pivot-Element p^{h_i} *mit $h_i \in \{0, 1\}$. Sind $i < j$ zwei Zeilenindizes, so gilt $h_i \leq h_j$, und im Fall $h_i = h_j$ steht das Pivot-Element der i-ten Zeile weiter links als das der j-ten Zeile. Die Einträge rechts von jedem Pivot-Element p^{h_i} liegen in Rp^{h_i}, die Einträge links sogar in Rp^{h_i+1}.*[18] *Die Einträge ober- und unterhalb eines Pivot-Elements p^{h_i} liegen stets in R_{h_i}.*

Mit anderen Worten: In der reduzierten Zeilenstufenform gibt es für ein Pivot-Element die beiden Möglichkeiten 1 und p. Beim zeilenweisen Durchschreiten der Matrix folgen zuerst die Pivot-Elemente gleich 1 in aufsteigender Reihenfolge ihrer Spaltenpositionen aufeinander. Danach folgen die Pivot-Elemente p, wieder in aufsteigender Reihenfolge ihrer Spaltenpositionen. Ist ein Pivot-Element gleich 1, so ist links davon alles in Rp und ober- und unterhalb davon alles gleich 0. Ist ein Pivot-Element gleich p, so ist links und unterhalb davon alles gleich 0, rechts davon alles in Rp und oberhalb davon alles in R_1. (Dass unterhalb alles gleich 0 ist liegt daran, dass in diesen Zeilen nur Pivot-Elemente p folgen und diese weiter rechts liegen.)

Durch eine Variante des Gauß-Algorithmus und anschließendem Wegstreichen der Nullzeilen kann jede Matrix über R mit elementaren Zeilenumformungen effizient in diese Zeilenstufenform transformiert werden:

Fakt 2.2.3 (vgl. [109, S. 329, Exercise XVI.7] und [40]) *Jeder R-lineare Code hat genau eine Generatormatrix in reduzierter Zeilenstufenform.*

Die eindeutige Generatormatrix von $\mathcal{C}$ in reduzierter Zeilenstufenform heißt *kanonische Generatormatrix*. Eine kanonische Generatormatrix ist bis auf eine Spaltenpermutation systematisch. Damit können Aussagen über systematische Generatormatrizen in der Regel durch Umkehrung der Spaltenpermutation auch auf kanonische Generatormatrizen angewendet werden. Aufgrund der Eindeutigkeit ist die kanonische Generatormatrix hervorragend zur Darstellung von Codes in Computeralgebrasystemen geeignet. Das einzige Computeralgebrasystem mit einer nennenswerten Unterstützung für ringlineare Codes ist momentan Magma [10]. Leider wird dort eine andere, nicht eindeutige Normalform für die Generatormatrizen benutzt.

[18] Bei „rechts von" bzw. „links von" sind nur die Einträge in der gleichen Zeile gemeint, bei „oberhalb" und „unterhalb" nur die Einträge in der gleichen Spalte.

Beispiel 2.2.4 Als Anwendung der reduzierten Zeilenstufenform überlegen wir uns die kanonischen Generatormatrizen aller Untermoduln von R^3 vom konjugierten Umriss $(2,1)$. In der ersten Zeile einer reduzierten Zeilenstufenform muss das Pivot-Element 1 stehen, für dessen Position es drei Möglichkeiten gibt. Für die Position des Pivot-Elements p in der zweiten Zeile verbleiben noch zwei Möglichkeiten. Entsprechend der 6 verschiedenen Positionen der beiden Pivot-Elemente ergeben sich die folgenden Möglichkeiten für die reduzierte Zeilenstufenform:

$$q^4 \text{ mal } \begin{pmatrix} \boxed{1} & R_1 & R \\ 0 & \boxed{p} & Rp \end{pmatrix}, \quad q^3 \text{ mal } \begin{pmatrix} 0 & \boxed{1} & R \\ \boxed{p} & 0 & Rp \end{pmatrix}, \quad q^2 \text{ mal } \begin{pmatrix} 0 & Rp & \boxed{1} \\ \boxed{p} & Rp & 0 \end{pmatrix},$$
$$q^3 \text{ mal } \begin{pmatrix} \boxed{1} & R & R_1 \\ 0 & 0 & \boxed{p} \end{pmatrix}, \quad q^2 \text{ mal } \begin{pmatrix} Rp & \boxed{1} & R_1 \\ 0 & 0 & \boxed{p} \end{pmatrix}, \quad q \text{ mal } \begin{pmatrix} Rp & 0 & \boxed{1} \\ 0 & \boxed{p} & 0 \end{pmatrix}.$$

Dabei sind genau die q^4 Generatormatrizen der ersten Bauart systematisch. Wir erläutern exemplarisch für die dritte Matrix den linken oberen Eintrag x: Weil x links vom Pivot-Element 1 steht, gilt $x \in Rp$, und weil x oberhalb vom Pivot-Element p steht, gilt $x \in R_1$. Mit $Rp \cap R_1 = \{0\}$ folgt nun $x = 0$.

Unter Benutzung von Fakt 2.2.3 sehen wir durch Addition der einzelnen Anzahlen, dass es genau $q^4 + 2q^3 + 2q^2 + q$ Unterräume von R^3 vom konjugierten Umriss $(2,1)$ gibt. Diese Anzahl ist nach Fakt 2.1.7 auch durch den verallgemeinerten Gauß-Koeffizienten $\begin{bmatrix} (3,3) \\ (2,1) \end{bmatrix}_q$ gegeben. Es gilt tatsächlich

$$\begin{bmatrix} (3,3) \\ (2,1) \end{bmatrix}_q = q \cdot \begin{bmatrix} 2 \\ 1 \end{bmatrix}_q \cdot \begin{bmatrix} 3 \\ 1 \end{bmatrix}_q = q(q+1)(q^2+q+1) = q^4 + 2q^3 + 2q^2 + q.$$

Bemerkung 2.2.5

(a) Zur Untersuchung von Untergruppen endlicher abelscher Gruppen wurde 1933 von Birkhoff in [6] eine Matrixnormalform benutzt, für eine Weiterentwicklung und übersichtliche Darstellung siehe [15]. Damit ist eine Normalform über den Galois-Ringen $R = \mathbb{Z}_{p^m}$ gegeben.

(b) Im Jahr 1955 wurde von L. E. Fuller eine entsprechende Normalform über Faktorringen eines kommutativen Hauptidealbereichs nach einem Ideal angegeben [40]. Die Galois-Ringe sind hierin als Spezialfall enthalten. In [109, S. 329, Exercise XVI.7] wurde das Resultat von Fuller für Galois-Ringe formuliert. In der dortigen Normalform sind die Matrizen stets quadratisch, indem zusätzliche Nullzeilen durch Pivot-Elemente 0 erlaubt werden. Weiter sind die Zeilen so sortiert, dass die Pivot-Elemente auf der Diagonale liegen. Unsere Definition wurde dagegen so gewählt, dass wie in der systematischen Form zuerst die torsionsfreien Zeilen und dann die Torsionszeilen aufeinander folgen.

(c) Die diskutierte reduzierte Zeilenstufenform lässt sich unmittelbar auf endliche, nicht zwingend kommutative Kettenringe beliebiger Kettenlänge verallgemeinern. Damit steht auch für diese allgemeinere Klasse von Codes eine eindeutige und effizient zu berechnende Generatormatrix zur Verfügung.

2.2.2. Gewichte, Distanzen und die Gray-Abbildung

Gewichte

Für einen Vektor $\mathbf{c} = (c_1, \ldots, c_n) \in R^n$ bezeichne

$$a_i(\mathbf{c}) = \#\{c_i \mid h(c_i) = i\}$$

die Anzahl der Komponenten von $\mathbf{c}$ der Höhe $i \in \{0, 1, 2\}$. Diese drei Werte werden im *symmetrisierten Gewicht* (auch: *integral weight* [113]; *type* [64, Def. 5], [65, S. 8])

$$w_{\text{sym}} : R^n \to \mathbb{N}^3, \quad \mathbf{c} \mapsto (a_0(\mathbf{c}), a_1(\mathbf{c}), a_2(\mathbf{c}))$$

zusammengefasst. Das *Hamming-Gewicht* ist wie üblich definiert als die Größe des Trägers eines Codeworts, d.h.

$$w_{\text{Ham}} : R^n \to \mathbb{N}, \quad \mathbf{c} \mapsto a_0(\mathbf{c}) + a_1(\mathbf{c}).$$

Weiter wird das *homogene Gewicht* definiert als

$$w_{\text{hom}} : R^n \to \mathbb{N}, \quad \mathbf{c} \mapsto (q-1)a_0(\mathbf{c}) + qa_1(\mathbf{c}).$$

Für $R = \mathbb{Z}_4$ ist das homogene Gewicht besser unter dem Namen *Lee-Gewicht* w_{Lee} bekannt.

Bemerkung 2.2.6

(a) Anhand der Definitionen erkennt man, dass das Hamming- und das homogene Gewicht durch das symmetrisierte Gewicht festgelegt sind. In diesem Sinne ist das symmetrisierte Gewicht feiner als die anderen beiden Gewichte.

(b) Als eine Verfeinerung des symmetrisierten Gewichts wird gelegentlich das *vollständige Gewicht*

$$R^n \to \mathbb{N}^R, \quad \mathbf{c} \mapsto (\#\{i \in \{1, \ldots, n\} \mid \mathbf{c}_i = x\})_{x \in R}$$

betrachtet. Im Gegensatz zu den oben definierten Gewichten ist das vollständige Gewicht jedoch nicht invariant unter (semi-)linearen Codeisometrien (vgl. Abschnitt 2.2.3). Der Begriff *symmetrisiertes Gewicht* leitet sich daraus ab, dass es aus dem vollständigen Gewicht durch „Symmetrisieren" hervorgeht, indem assoziierte Ringelemente als gleichwertig aufgefasst werden.

(c) Die Idee hinter dem homogenen Gewicht ist, dass sich für die beiden vom Nullideal verschiedenen Ideale $I \in \{R, Rp\}$ von R dasselbe von Null verschiedene *Durchschnittsgewicht*

$$\frac{1}{\#I} \sum_{a \in I} w_{\text{hom}}(a)$$

ergibt [27]. Fordert man weiter $w_{\text{hom}}(0) = 0$ und dass w_{hom} auf den Klassen von assoziierten Ringelementen konstant ist, so ist das homogene Gewicht bis auf Skalierung eindeutig festgelegt. In der oben angegebenen Definition wurde die Skalierung so gewählt, dass sich stets ganzzahlige homogene Gewichte ergeben. Das Durchschnittsgewicht ist dann $q - 1$.

Distanzen

Jedes dieser Gewichte $w \in \{w_{\mathrm{sym}}, w_{\mathrm{Ham}}, w_{\mathrm{hom}}, w_{\mathrm{Lee}}\}$ hat eine zugehörige Distanzfunktion (d_{sym}, d_{Ham}, d_{hom} oder d_{Lee}), die ein Paar $(\mathbf{c}, \mathbf{c}')$ von Codewörtern auf $w(\mathbf{c}-\mathbf{c}')$ abbildet. Weiter werden alle in einem Code $\mathcal{C}$ auftretenden Gewichte im jeweiligen *Gewichtszähler*

$$w(\mathcal{C}) = \sum_{\mathbf{c}\in\mathcal{C}} X^{w(\mathbf{c})}$$

zusammengefasst. Im Fall des symmetrisierten Gewichts ist dabei X als der Vektor $\mathbf{X} = (X_0, X_1, X_2)$ zu lesen, d.h.

$$w_{\mathrm{sym}}(\mathcal{C}) = \sum_{\mathbf{c}\in\mathcal{C}} \mathbf{X}^{w_{\mathrm{sym}}(\mathbf{c})} = \sum_{\mathbf{c}\in\mathcal{C}} X_0^{a_0(\mathbf{c})} X_1^{a_1(\mathbf{c})} X_2^{a_2(\mathbf{c})}.$$

In der Schreibweise

$$w(\mathcal{C}) = \sum_{\omega} A_\omega X^\omega$$

gibt der Koeffizient A_ω die Anzahl der Codewörter $\mathbf{c} \in \mathcal{C}$ mit $w(\mathbf{c}) = \omega$ an. Dabei läuft in der Summe ω über $\mathbb{N}$ bzw. im Fall des symmetrisierten Gewichtszählers über $\mathbb{N}^3$.

Am symmetrisierten Gewichtszähler können einige Parameter des Codes abgelesen werden: Zum einen ist $w_{\mathrm{sym}}(\mathcal{C})$ ein homogenes Polynom, dessen Grad mit der Länge n von $\mathcal{C}$ übereinstimmt, und durch die Gleichungen

$$w_{\mathrm{sym}}(\mathcal{C})(1,1,1) = \#\mathcal{C} = q^{\lambda_0+\lambda_1}, \qquad w_{\mathrm{sym}}(\mathcal{C})(0,1,1) = q^{\lambda_0}$$

ist der konjugierte Umriss $\mathrm{cshp}(\mathcal{C}) = (\lambda_0, \lambda_1)$ festgelegt. Weiter gilt

$$w_{\mathrm{sym}}(\mathcal{C})(X,X,1) = w_{\mathrm{Ham}}(\mathcal{C}), \quad w_{\mathrm{sym}}(\mathcal{C})(X^{q-1}, X^q, 1) = w_{\mathrm{hom}}(\mathcal{C}), \quad w_{\mathrm{sym}}(\mathcal{C})(0,0,1) = 1.$$

Der Übersichtlichkeit halber werden wir umfangreichere symmetrisierte Gewichtszähler in Form einer Tabelle angeben. Jede Zeile entspricht dabei einem Monom und listet den zugehörigen Koeffizienten (Spalte „#Codewörter") und die Exponenten der einzelnen Polynomvariablen X_i (Spalte „ω_i") auf. Außerdem wird in der Regel für jedes symmetrisierte Gewicht ein Bezeichner (Spalte „Typ") und das zugehörige homogene bzw. Lee-Gewicht (Spalte „w_{hom}" oder „w_{Lee}") mit angegeben, siehe z.B. Tabelle 2.4.1. In noch größeren Fällen wie z.B. in Tabelle 2.4.3 werden diese Einträge für jedes einzelne Monom jeweils zeilenweise untereinander geschrieben.

Für die drei Distanzen $d \in \{d_{\mathrm{Ham}}, d_{\mathrm{hom}}, d_{\mathrm{Lee}}\}$ und einen R-linearen Code $\mathcal{C}$ wird weiter die zugehörige Minimaldistanz $d(\mathcal{C})$ definiert als die kleinste Distanz, die zwischen zwei verschiedenen Codewörtern in $\mathcal{C}$ auftritt. Aufgrund der Linearität sind R-lineare Codes *distanzhomogen*, d.h. die Zahlen $A_i(\mathbf{c}) = \#\{\mathbf{c}' \in \mathcal{C} \mid d(\mathbf{c}, \mathbf{c}') = i\}$ mit $i \in \mathbb{N}$ sind von der Wahl von $\mathbf{c} \in \mathcal{C}$ unabhängig. Insbesondere ist die Minimaldistanz bereits durch das kleinste positive Gewicht unter den Codewörtern von $\mathcal{C}$ gegeben.

Die Gray-Abbildung

Das Hamming-Gewicht spielt für R-lineare Codes keine große Rolle. Denn für jedes torsionsfreie Codewort $\mathbf{c}$ eines R-linearen Codes $\mathcal{C}$ mit $k_1 \geq 1$ gilt $p\mathbf{c} \in C \setminus \{\mathbf{0}\}$ und $w_{\mathrm{Ham}}(\mathbf{c}) \geq w_{\mathrm{Ham}}(p\mathbf{c})$, so dass die minimale Hamming-Distanz von $\mathcal{C}$ bereits durch den Teilcode aller Torsionsvektoren bestimmt ist. Dieser hat eine $\mathbb{F}_q$-lineare Struktur.[19]

Für die Fehlerkorrektur ist das homogene Gewicht wesentlich besser geeignet. Der Grund dafür ist die Existenz einer distanzerhaltenden injektiven Abbildung

$$(R^n,\ d_{\mathrm{hom}}) \quad \to \quad (\mathbb{F}_q^{qn},\ d_{\mathrm{Ham}}),$$

der *verallgemeinerten Gray-Abbildung*.[20] Mit der Gray-Abbildung ist es möglich, R-lineare Codes hoher homogener Minimaldistanz in – im Allgemeinen nichtlineare – Blockcodes der q-fachen Länge und derselben minimalen Hamming-Distanz zu übersetzen.

Die wichtigsten Parameter eines R-linearen Codes $\mathcal{C}$ sind also seine Länge n, seine Größe $\#\mathcal{C}$ und seine homogene Minimaldistanz $d_{\mathrm{hom}}(\mathcal{C})$. Diese Parameter werden in der Notation

$$(n,\ \#\mathcal{C},\ d_{\mathrm{hom}}(\mathcal{C}))_R$$

kompakt zusammengefasst. Wollen wir anstelle der Größe präziser den konjugierten Umriss von $\mathcal{C}$ angeben, so benutzen wir wie für herkömmliche $\mathbb{F}_q$-lineare Codes eckige Klammern, um die R-lineare Struktur herauszustellen.[21] Die Parameter von $\mathcal{C}$ schreiben sich dann als

$$[n,\ \mathrm{cshp}(\mathcal{C}),\ d_{\mathrm{hom}}(\mathcal{C})]_R.$$

Durch die Parameter erhalten wir eine Halbordnung auf der Menge der R-linearen Codes: Ein $(n, s, d)_R$-Code ist hinsichtlich seiner Fehlerkorrektureigenschaften mindestens so gut wie ein $(n', s', d')_R$-Code, wenn gleichzeitig $n \leq n'$, $s \geq s'$ und $d \geq d'$ erfüllt sind. Die bezüglich dieser Halbordnung maximalen Codes sind von besonderem Interesse.

Bemerkung 2.2.7

(a) In [52] wurde eine Isometrie[22] $\phi : (\mathbb{Z}_4, d_{\mathrm{Lee}}) \to (\mathbb{F}_2^2, d_{\mathrm{Ham}})$ angegeben mit der Abbildungsvorschrift

$$0 \mapsto (0,0), \quad 1 \mapsto (0,1), \quad 2 \mapsto (1,1), \quad 3 \mapsto (1,0).$$

Weil die Werte $\phi(0)$, $\phi(1)$, $\phi(2)$, $\phi(3)$ den Raum $\mathbb{F}_2^2$ in der Reihenfolge des binären Gray-Codes durchlaufen, wurde die Abbildung ϕ als *Gray map* bezeichnet.

[19] Diesen $\mathbb{F}_q$-linearen Code werden wir weiter unten mit $\mathcal{C}^{(2)}$ bezeichnen.

[20] Der Zusatz „verallgemeinert" wird im Folgenden meist weglassen.

[21] Ein $(n, s, d)_q$-Code $\mathcal{C}$ ist ein nicht zwingend linearer Code der Länge n, Größe s und minimaler Hamming-Distanz d über einem q-nären Alphabet. Ist $\mathcal{C}$ darüber hinaus $\mathbb{F}_q$-linear, so kann wegen $s = q^{\dim(\mathcal{C})}$ die Angabe der Größe s durch die $\mathbb{F}_q$-Dimension von $\mathcal{C}$ ersetzt werden: Der Code $\mathcal{C}$ wird dann auch als $[n, \dim(\mathcal{C}), d]_q$-Code bezeichnet. Die eckigen Klammern signalisieren also, dass $\mathcal{C}$ ein $\mathbb{F}_q$-linearer Code ist, und dass der zweite Parameter nicht die Größe, sondern die Dimension von $\mathcal{C}$ angibt.

[22] Sind X, Y und Z Mengen mit Abbildungen $d : X \times X \to Z$ und $d' : Y \times Y \to Z$, so verstehen wir unter einer *Isometrie* $\phi : (X, d) \to (Y, d')$ eine bijektive Abbildung $\phi : X \to Y$ mit $d'(\phi(x), \phi(x')) = d(x, x')$ für alle $x, x' \in X$. Linearität wird für eine Isometrie nicht gefordert.

(b) Das homogene Gewicht wurde in [27] als eine Verallgemeinerung des Lee-Gewichts auf die Restklassenringe $\mathbb{Z}_k$ eingeführt; für den Fall $k = p^2$ mit p prim findet sich dort auch eine verallgemeinerte Gray-Abbildung.

(c) Ein in unserer Situation der Galois-Ringe der Länge 2 passendes homogenes Gewicht mit zugehöriger verallgemeinerter Gray-Abbildung γ_* wurde in [113] angegeben. Die Abbildungsvorschrift von γ_* lässt sich im Wesentlichen so beschreiben: Wir identifizieren die Elemente von R mit ihrer p-adischen Entwicklung $a_0 + a_1 p$, wobei a_0 und a_1 Elemente der Teichmüller-Menge von R sind, und bezeichnen die Reduktion von a_i modulo p mit $\bar{a}_i \in \mathbb{F}_q$. Sei

$$\mathbf{G} = \begin{pmatrix} b_1 & b_2 & \dots & b_q \\ 1 & 1 & \dots & 1 \end{pmatrix},$$

wobei $b_1, b_2, \dots, b_q$ die Elemente des endlichen Körpers $\mathbb{F}_q$ durchläuft. Die Abbildung

$$(R, d_{\mathrm{hom}}) \to (\mathbb{F}_q^q, d_{\mathrm{Ham}}), \quad a_0 + a_1 p \mapsto (\bar{a}_0, \bar{a}_1)\mathbf{G}$$

ist eine distanzerhaltende injektive Abbildung. Koordinatenweises Anwenden liefert nun eine verallgemeinerte Gray-Abbildung.

Diese Abbildung kann als Konkatenation mit dem von $\mathbf{G}$ erzeugten $\mathbb{F}_q$-linearen Code – ein MDS-Code mit den Parametern $[q, 2, q-1]_q$ – aufgefasst werden. Weil dieser Code ein Reed-Solomon-Code ist, wurde γ_* in [113] *Reed-Solomon map* genannt.

(d) Der von $\mathbf{G}$ erzeugte Code lässt sich auch als q-närer Reed-Muller-Code $\mathrm{RM}_q(1,1)$ erster Ordnung beschreiben.[23] Diese Sichtweise erlaubt eine Verallgemeinerung für allgemeine Kettenringe beliebiger Kettenlänge m: Durch Konkatenation mit dem Reed-Muller-Code $\mathrm{RM}_q(m-1,1)$ erhält man auf ähnliche Weise eine verallgemeinerte Gray-Abbildung [49] (siehe [23] für den Spezialfall der Kettenringe $\mathbb{Z}_{2^m}$). Weitere Verallgemeinerungen des homogenen Gewichts und der Gray-Abbildung findet man in [73, 50].

(e) Die verallgemeinerte Gray-Abbildung ist genau für den kleinsten Grundring $\mathbb{Z}_4$ eine Isometrie. Für größere Galois-Ringe ist die verallgemeinerte Gray-Abbildung nicht mehr surjektiv.

(f) Weil die verallgemeinerte Gray-Abbildung distanzerhaltend ist, ist mit einem R-linearen Code $\mathcal{C}$ auch sein Gray-Bild stets distanzhomogen.

BTL- und BTKL-Codes

Unser Ziel wird sein, durch Gray-Bilder R-linearer Codes nichtlineare Blockcodes über $\mathbb{F}_q$ zu konstruieren, deren Parameter $\mathbb{F}_q$-linear nicht realisierbar sind. Wir nennen einen R-linearen Code $\mathcal{C}$ *BTL* (*better than linear*), wenn sein Gray-Bild nachweislich eine höhere

[23] Das Symbol $\mathrm{RM}_q(m,r)$ bezeichnet den $\mathbb{F}_q$-linearen Reed-Muller-Code der Länge q^m und der Ordnung r. Der Code $\mathrm{RM}_q(m,r)$ hat die Parameter $[q^m, m+1, q^m - q^{m-r}]_q$.

Minimaldistanz hat als jeder vergleichbare (d.h. gleiche Länge und Größe) $\mathbb{F}_q$-lineare Code. Hat das Gray-Bild eine höhere Minimaldistanz als jeder bekannte vergleichbare $\mathbb{F}_q$-lineare Code, so nennen wir den Code $\mathcal{C}$ *BTKL* (*better than known linear*). Während BTL eine harte mathematische Eigenschaft eines ringlinearen Codes ist, beschreibt BTKL lediglich den aktuellen Kenntnisstand: Ein BTKL-Code ist ein Kandidat für einen BTL-Code.

Das folgende Beispiel belegt, dass es tatsächlich BTL-Codes gibt:

Beispiel 2.2.8 Der aufgrund seiner relativ kleinen Parameter, seiner Entdeckungsgeschichte und vieler interessanter Eigenschaften wohl prominenteste ringlineare Code ist der von der (sowohl systematischen als auch kanonischen) Generatormatrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 1 & 3 & 1 & 2 \end{pmatrix}$$

erzeugte $\mathbb{Z}_4$-lineare *Oktacode* $\mathcal{O}$. Der Oktacode hat den symmetrisierten Gewichtszähler

$$w_{\mathrm{sym}}(\mathcal{O}) = X_2^8 + 112X_0^4X_1X_2^3 + 14X_1^4X_2^4 + 16X_0^8 + 112X_0^4X_1^3X_2 + X_1^8$$

und den Lee-Gewichtszähler

$$w_{\mathrm{Lee}}(\mathcal{O}) = 1 + 112X^6 + 30X^8 + 112X^{10} + X^{16}.$$

Damit ist der Oktacode ein $(8, 2^8, 6)_{\mathbb{Z}_4}$-Code bzw. genauer ein $[8, (4, 4), 6]_{\mathbb{Z}_4}$-Code.

Die minimale Lee-Distanz ist $d_{\mathrm{Lee}}(\mathcal{O}) = 6$, und das Gray-Bild ist demzufolge ein binärer $(16, 2^8, 6)_2$-Code, der *Nordstrom-Robinson-Code* [114]. Weil ein linearer binärer $[16, 8]_{\mathbb{F}_2}$-Code bestenfalls die Minimaldistanz 5 hat, handelt es sich bei dem Oktacode um einen BTL-Code.

2.2.3. Lineare und semilineare Isometrien

Dieser Abschnitt hat die strukturerhaltenden Abbildungen von R-linearen Codes zum Inhalt. Zur Theorie der Gruppenoperationen siehe z.B. [79].

Lineare Isometrien

Zu einem Vektor $\mathbf{v} \in R^n$ definieren wir die Diagonalmatrix $\mathrm{diag}(\mathbf{v}) \in R^{n\times n}$ mit der Diagonale $\mathbf{v}$. Weiter definieren wir zu einer Permutation $\sigma \in S_n$ die Permutationsmatrix $\mathbf{P}_\sigma \in \mathrm{GL}(n, R)$ als diejenige Matrix, deren Eintrag an der Position (i, j) durch $\delta_{i,\sigma(j)}$ gegeben ist, wobei δ das Kronecker-Delta bezeichnet. Die Abbildung $S_n \to \mathrm{GL}(n, R)$, $\sigma \mapsto \mathbf{P}_\sigma$ ist ein Gruppenmonomorphismus.[24]

Eine Abbildung $f : R^n \to R^n$ heißt *monomial*, wenn es einen *Permutationsanteil* $\sigma \in S_n$ und einen *Skalierungsanteil* $\mathbf{v} \in (R^*)^n$ gibt mit $f(\mathbf{c}) = \mathrm{diag}(\mathbf{v})\mathbf{P}_\sigma\mathbf{c}$ für alle

[24] Permutationen sind Abbildungen, operieren also von links.

$\mathbf{c} \in R^n$. Permutations- und Skalierungsanteil einer monomialen Abbildung sind eindeutig festgelegt. Die Menge aller monomialen Abbildungen bildet eine zum Kranzprodukt $R^* \wr S_n$ isomorphe Gruppe, die wir die *monomiale Gruppe* $\mathrm{Mon}(n, R)$ auf R^n nennen. In der Kranzproduktschreibweise entspricht die S_n-Komponente dem Permutationsanteil, und die R^*-Komponenten (n Stück) bilden zusammen den Skalierungsanteil. Die Gruppenstruktur von R^* ist durch Fakt 2.1.3 festgelegt. Monomiale Abbildungen sind linear. Die zugehörigen Abbildungsmatrizen $\mathrm{diag}(\mathbf{v})\mathbf{P}_\sigma$ bilden eine die Permutationsmatrizen umfassende Untergruppe der $\mathrm{GL}(n, R)$. In der Codierungstheorie werden Vektoren meist als Zeilenvektoren aufgefasst; die monomiale Abbildung f schreibt sich dann als $\mathbf{c} \mapsto \mathbf{c}\mathbf{P}_{\sigma^{-1}} \mathrm{diag}(\mathbf{v})$.

Nach [129, Prop. 6.1] sind die linearen Isometrien $(R^n, d_{\mathrm{Ham}}) \to (R^n, d_{\mathrm{Ham}})$ gerade die monomialen Abbildungen auf R^n, die wir deshalb auch als die *linearen Codeisometrien* auf R^n bezeichnen. Von den Eigenschaften des Hamming-Gewichts wird hierfür nur benötigt, dass es invariant unter Multiplikation mit Einheiten ist, und dass es ein Gewicht gibt, das genau von den Vektoren der Bauart $\lambda\mathbf{e}$ mit einer Einheit $\lambda \in R^*$ und einem Einheitsvektor $\mathbf{e}$ angenommen wird. Weil diese Eigenschaften auch auf w_{hom} und w_{sym} zutreffen, sind die linearen Codeisometrien auch genau die linearen Isometrien $(R^n, d_{\mathrm{hom}}) \to (R^n, d_{\mathrm{hom}})$ und auch genau die linearen Isometrien $(R^n, d_{\mathrm{sym}}) \to (R^n, d_{\mathrm{sym}})$.

Semilineare Isometrien

Weiter definieren wir die *semilinearen Codeisometrien* auf R^n durch die Menge aller Abbildungen $f \circ \rho$, wobei $f \in \mathrm{Mon}(n, R)$ eine monomiale Abbildung auf R^n ist und $\rho \in \mathrm{Aut}(R)$ einen Ringautomorphismus von R bezeichnet, der komponentenweise auf R^n angewendet wird. Auch hier ist der *Monomialanteil* f und der *Automorphismenanteil* ρ durch die semilineare Abbildung $f \circ \rho$ eindeutig festgelegt. Die semilinearen Codeisometrien bilden eine Gruppe, die die monomialen Abbildungen als Normalteiler enthalten. Genauer ist die Gruppe der semilinearen Codeisometrien ein semidirektes Produkt $\mathrm{Mon}(n, R) \rtimes_\theta \mathrm{Aut}(R)$, wobei der definierende Homomorphismus $\theta : \mathrm{Aut}(R) \to \mathrm{Aut}(\mathrm{Mon}(n, R))$ gegeben ist durch

$$\theta(\rho) \quad = \quad (\mathbf{c} \mapsto \mathrm{diag}(\mathbf{v})\mathbf{P}_\sigma \mathbf{c}) \;\mapsto\; (\mathbf{c} \mapsto \mathrm{diag}(\rho(\mathbf{v}))\mathbf{P}_\sigma \mathbf{c}).$$

Nach Fakt 2.1.4 bilden die semilinearen Codeisometrien also eine zu $(R^* \wr S_n) \rtimes \mathbb{Z}_r$ isomorphe Untergruppe von $\Gamma\mathrm{L}(R_R^n)$.[25] Mit Hilfe des Hauptsatzes der projektiven Hjelmslev-Geometrie (siehe Abschnitt 2.3.1) kann man sich überlegen, dass die semilinearen Codeisometrien genau die Isometrien $(R^n, w_{\mathrm{Ham}}) \to (R^n, w_{\mathrm{Ham}})$ sind, die Untermoduln von R^n wieder auf Untermoduln vom gleichen konjugierten Umriss abbilden. Wie zuvor kann hier anstelle von w_{Ham} auch wieder w_{hom} oder w_{sym} benutzt werden.

Die Gruppe G der (semi-)linearen Codeisometrien operiert auf R^n und damit auch auf der Menge der Untermoduln von R^n und partitioniert diese in Bahnen. Zwei R-lineare

[25] Die *semilineare Gruppe* $\Gamma\mathrm{L}(R_R^n)$ besteht aus allen *R-semilinearen* Abbildungen $R^n \to R^n$, d.h. aus allen Abbildungen f, für die ein Automorphismus $\rho \in \mathrm{Aut}(R)$ existiert mit $f(\mathbf{v}+\mathbf{w}) = f(\mathbf{v}) + f(\mathbf{w})$ und $f(\lambda\mathbf{v}) = \rho(\lambda) f(\mathbf{v})$ für alle Vektoren $\mathbf{v}, \mathbf{w} \in R^n$ und alle Skalare $\lambda \in R$.

Codes heißen nun *(semi-)linear isometrisch* (auch: *isomorph*, *äquivalent*), wenn sie unter der Operation von G in der gleichen Bahn liegen. Sind zwei Codes $\mathcal{C}$ und $\mathcal{D}$ semilinear isometrisch, so schreiben wir $\mathcal{C} \cong \mathcal{D}$. Die (semi-)lineare *Automorphismengruppe* eines Codes $\mathcal{C}$ ist der Stabilisator von $\mathcal{C}$ unter der Operation von G.

Isometrische Codes stimmen in vielen codierungstheoretischen Eigenschaften überein, sie haben beispielsweise dieselben Gewichtszähler. Zur Untersuchung von Isometriefragen auf $\mathbb{Z}_4$-linearen Codes ist der Algorithmus von Thomas Feulner in [39] sehr nützlich. Dort wird der Ansatz für herkömmliche lineare Codes aus [38] auf die Situation der $\mathbb{Z}_4$-linearen Codes angepasst. Der Algorithmus berechnet aus einer Generatormatrix die Automorphismengruppe und eine kanonische Form des davon erzeugten Codes.

2.2.4. Dualität

Der orthogonale Untermodul $\mathcal{C}^\perp$ im Sinne von Abschnitt 2.1.4 heißt der *duale Code* von $\mathcal{C}$. Hat $\mathcal{C}$ den konjugierten Umriss $\operatorname{cshp}(\mathcal{C}) = \lambda = (\lambda_0, \lambda_1) = (k_1 + k_2, k_1)$, so hat nach Fakt 2.1.9(a) der duale Code den konjugierten Umriss $\operatorname{cshp}(\mathcal{C}^\perp) = \bar{\lambda}$. In der Schreibweise $\operatorname{cshp}(\mathcal{C}^\perp) = (k_1^\perp + k_2^\perp, k_1^\perp)$ gilt $k_1^\perp = n - (k_1 + k_2)$ und $k_2^\perp = k_2$.

Ist $\mathcal{C}$ der Zeilenraum einer systematischen Generatormatrix wie in Gleichung (2.1), so ist eine Generatormatrix von $\mathcal{C}^\perp$ gegeben durch

$$\begin{pmatrix} (\mathbf{AC} - \mathbf{B})^\top & -\mathbf{C}^\top & \mathbf{I}_{k_1^\perp} \\ -p\mathbf{A}^\top & p\mathbf{I}_{k_2} & \mathbf{0}_{k_2 \times k_1^\perp} \end{pmatrix}. \tag{2.2}$$

(Siehe [28, Gleichung (3)] für $R = \mathbb{Z}_4$, [22, Gleichung (3)] für $R = \mathbb{Z}_{p^m}$ und [115, Th. 3.10] für endliche kommutative Kettenringe.) Diese Generatormatrix ist bis auf eine Permutation der Koordinaten wieder systematisch.

Im Fall $\mathcal{C} \leq \mathcal{C}^\perp$ heißt $\mathcal{C}$ *selbstorthogonal*, im Fall $\mathcal{C} \cong \mathcal{C}^\perp$ *isodual* und im Fall $\mathcal{C} = \mathcal{C}^\perp$ *selbstdual*. Selbstdualität und Selbstorthogonalität sind im Allgemeinen nicht invariant unter (semi)-linearen Codeisometrien. Um die Selbstorthogonalität zu erhalten, müssen beide Gruppen auf Skalierungsanteile $\mathbf{v} = (v_1, \ldots, v_n)$ mit der Eigenschaft $v_i^2 = 1$ für alle $i \in \{1, \ldots, n\}$ eingeschränkt werden.

Die symmetrisierten Gewichtszähler von $\mathcal{C}$ und $\mathcal{C}^\perp$ können durch die MacWilliams-Transformation ineinander umgerechnet werden:

Fakt 2.2.9 (MacWilliams-Transformation [113, Prop. 3]) *Sei $\mathcal{C}$ ein R-linearer Code. Mit der Variablensubstitution*

$$\begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 1 \\ -q & q-1 & 1 \\ q^2 - q & q-1 & 1 \end{pmatrix} \begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix}$$

gilt

$$w_{\text{sym}}(\mathcal{C}^\perp)(X_0, X_1, X_2) = \frac{w_{\text{sym}}(\mathcal{C})(Y_0, Y_1, Y_2)}{w_{\text{sym}}(\mathcal{C})(1, 1, 1)}.$$

Die Variablensubstitution aus Fakt 2.2.9 wird MacWilliams-Transformation genannt. Bleibt der symmetrisierte Gewichtszähler eines (nicht notwendig linearen) Codes $\mathcal{C}$ über R unter dieser Transformation unverändert, so heißt $\mathcal{C}$ *formal selbstdual*. Isoduale Codes sind stets auch formal selbstdual.

2.2.5. Radikalcode und Torsionscode

Wir betrachten die Multiplikation mit p als eine Abbildung auf $\mathcal{C}$: Sei $\mu_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$, $\mathbf{c} \mapsto p\mathbf{c}$. Die Abbildung $\mu_{\mathcal{C}}$ ist ein Homomorphismus von R-Moduln, und es gilt

$$\mathrm{im}(\mu_{\mathcal{C}}) \leq \ker(\mu_{\mathcal{C}}) \leq (Rp)^n.$$

Definition 2.2.10 *Sei $\mathcal{C}$ ein R-linearer Code. Wir definieren den* Radikalcode $\mathcal{C}^{(1)}$ *und den* Torsionscode $\mathcal{C}^{(2)}$ *durch*

$$\mathcal{C}^{(1)} = \varphi^{-1}(\mathrm{im}(\mu_{\mathcal{C}})) \qquad \textit{und} \qquad \mathcal{C}^{(2)} = \varphi^{-1}(\ker(\mu_{\mathcal{C}})).$$

Dabei bezeichnet $\varphi : \mathbb{F}_q^n \to (Rp)^n$ den im Zusammenhang mit Torsionsvektoren auf Seite 18 eingeführten Isomorphismus von R-Moduln.

Radikal- und Torsionscode sind beide $\mathbb{F}_q$-linear. Der Radikalcode $\mathcal{C}^{(1)}$ stimmt mit dem Bild modulo Rp von $\mathcal{C}$ überein, und der Torsionscode $\mathcal{C}^{(2)}$ ist das φ^{-1}-Bild aller Torsionsvektoren in $\mathcal{C}$. Ist der Code $\mathcal{C}$ durch eine systematische Generatormatrix wie in Gleichung (2.1) gegeben, so erhalten wir systematische Generatormatrizen von $\mathcal{C}^{(1)}$ und $\mathcal{C}^{(2)}$ als

$$\begin{pmatrix} \mathbf{I}_{k_1} & \bar{\mathbf{A}} & \bar{\mathbf{B}} \end{pmatrix} \in \mathbb{F}_q^{k_1 \times n} \qquad \text{und} \qquad \begin{pmatrix} \mathbf{I}_{k_1} & \mathbf{0}_{k_1 \times k_2} & \bar{\mathbf{B}} - \bar{\mathbf{A}}\bar{\mathbf{C}} \\ \mathbf{0}_{k_2 \times k_1} & \mathbf{I}_{k_2} & \bar{\mathbf{C}} \end{pmatrix} \in \mathbb{F}_q^{(k_1+k_2) \times n}, \tag{2.3}$$

wobei für eine Matrix $\mathbf{M}$ über R die durch eintragsweise Reduktion modulo Rp entstehende Matrix über $\mathbb{F}_q$ mit $\bar{\mathbf{M}}$ bezeichnet wird.

Fakt 2.2.11 *Sei $\mathcal{C}$ ein R-linearer Code und* $\mathrm{cshp}(\mathcal{C}) = (\lambda_0, \lambda_1) = (k_1 + k_2, k_1)$. *Es gilt:*

(a) $\dim_{\mathbb{F}_q}(\mathcal{C}^{(1)}) = \lambda_1 = k_1$ *und* $\dim_{\mathbb{F}_q}(\mathcal{C}^{(2)}) = \lambda_0 = k_1 + k_2$.

(b) $\mathcal{C}^{(1)} \leq \mathcal{C}^{(2)}$ *mit Gleichheit genau dann, wenn $\mathcal{C}$ ein freier Code ist.*

(c) $(\mathcal{C}^{\perp})^{(1)} = (\mathcal{C}^{(2)})^{\perp}$ *und* $(\mathcal{C}^{\perp})^{(2)} = (\mathcal{C}^{(1)})^{\perp}$.

(d) Ist $\mathcal{C}$ ein selbstorthogonaler Code, so ist auch $\mathcal{C}^{(1)}$ selbstorthogonal. Im Fall $R = \mathbb{Z}_4$ ist $\mathcal{C}^{(1)}$ zusätzlich doppeltgerade, d.h. alle auftretenden Hamming-Gewichte sind Vielfache von 4.

(e) Ist $\mathcal{C}$ ein selbstdualer Code, so ist $\mathcal{C}^{(1)} = (\mathcal{C}^{(2)})^{\perp}$ und $\mathcal{C}^{(2)} = (\mathcal{C}^{(1)})^{\perp}$.

(f) Es gilt $(q-1)d_{\mathrm{Ham}}(\mathcal{C}^{(1)}) \leq d_{\mathrm{hom}}(\mathcal{C}) \leq q d_{\mathrm{Ham}}(\mathcal{C}^{(2)})$.

Bemerkung 2.2.12

(a) Die Codes $\mathcal{C}^{(1)}$ und $\mathcal{C}^{(2)}$ wurden für $R = \mathbb{Z}_4$ in [28] eingeführt. Dort finden sich alle Aussagen von Fakt 2.2.11 bis auf Teil (c) und Teil (f). In [115] wurde mit den Codes $\overline{(C : \gamma^i)}$ eine Verallgemeinerung für allgemeine kommutative Kettenringe angegeben, die unsere Situation der Galois-Ringe der Kettenlänge 2 abdeckt. Die Codes $\overline{(C : \gamma^i)}$ hängen eng mit der Ulm-Kaplansky-Reihe zusammen, siehe [69, Rem. 3.1].

(b) Mit Hilfe unserer Vorarbeiten ist Fakt 2.2.11 nicht schwer zu beweisen: Wir können o.E. annehmen, dass $\mathcal{C}$ durch eine systematische Generatormatrix wie in Gleichung (2.1) erzeugt wird (denn Dualität ist invariant unter Permutationsäquivalenz). Die einzelnen Aussagen lassen sich nun ausgehend von den abgeleiteten Generatormatrizen in den Gleichungen (2.2) und (2.3) leicht nachrechnen.

(c) Ein freier selbstdualer $\mathbb{Z}_4$-linearer Code $\mathcal{C}$ hat stets eine durch 8 teilbare Länge, denn für diesen ist nach Fakt 2.2.11 (b), (d) und (e) $\mathcal{C}^{(1)} = \mathcal{C}^{(2)}$ ein selbstdualer doppeltgerader $\mathbb{F}_2$-linearer Code. Solche $\mathbb{F}_2$-linearen Codes werden auch *selbstduale Codes vom Typ II* genannt und existieren nur für durch 8 teilbare Längen.

2.2.6. Modifikationen R-linearer Codes

Punktieren, Verkürzen, Residuum

Zu einer Teilmenge $I \subseteq \{1, \ldots, n\}$ bezeichne $\complement I = \{1, \ldots, n\} \setminus I$ die komplementäre Koordinatenmenge und $\pi_I : R^n \to R^{\#I}, (c_1, \ldots, c_n) \mapsto (c_i)_{i \in I}$ den Restriktionshomomorphismus auf die Koordinaten in I.[26]

Definition 2.2.13 *Sei $\mathcal{C}$ ein R-linearer Code der Länge n und $I \subseteq \{1, \ldots, n\}$. Der in I* punktierte Code *(engl.* punctured code*) ist gegeben durch $P_I(\mathcal{C}) = \pi_{\complement I}(\mathcal{C})$, und der in I* verkürzte Code *(engl.* shortened code*) ist gegeben durch $S_I(\mathcal{C}) = \pi_{\complement I}(\mathcal{C} \cap \ker(\pi_I))$. Weiter ist zu einem Codewort $\mathbf{c} \in \mathcal{C}$ der* residuelle Code in $\mathbf{c}$ *(engl.* residual code*) gegeben durch den in* $\mathrm{supp}(\mathbf{c})$ *punktierten Code* $\mathrm{res}_{\mathbf{c}}(\mathcal{C}) = P_{\mathrm{supp}(\mathbf{c})}(\mathcal{C})$.

Fakt 2.2.14 *Sei $\mathcal{C}$ ein R-linearer Code der Länge n und der homogenen Minimaldistanz d.*

(a) Sei $I \subseteq \{1, \ldots, n\}$. Es gilt $P_I(\mathcal{C})^\perp = S_I(\mathcal{C}^\perp)$ und $S_I(\mathcal{C})^\perp = P_I(\mathcal{C}^\perp)$.

(b) Für alle $a \in \{1, \ldots, n\}$ gilt: Ist $d > q$, so ist der in a punktierte Code $P_{\{a\}}(\mathcal{C})$ ein R-linearer Code mit den Parametern

$$[n-1,\ \mathrm{cshp}(\mathcal{C}),\ \geq d-q]_R.$$

[26] Üblicherweise werden die restringierten Codewörter nicht mit der Koordinatenmenge I indiziert, sondern mit $\{1, \ldots, \#I\}$.

(c) *Für alle* $a \in \{1, \ldots, n\}$ *gilt: Der in* a *verkürzte Code* $S_{\{a\}}(\mathcal{C})$ *ist ein* R*-linearer Code mit den Parametern*

$$\left(n-1, \quad \frac{\#\mathcal{C}}{\#\pi_{\{a\}}(\mathcal{C})}, \quad \geq d\right)_R .$$

(d) *Sei* $\mathbf{c} \in \mathcal{C}$ *ein Codewort mit* $(q-1)w_{\mathrm{Ham}}(\mathbf{c}) < d$*. Dann ist der residuelle Code* $\mathrm{res}_{\mathbf{c}}(\mathcal{C})$ *in* $\mathbf{c}$ *ein* R*-linearer Code mit den Parametern*

$$\left(n - w_{\mathrm{Ham}}(\mathbf{c}), \quad \frac{\#\mathcal{C}}{\#(R\mathbf{c})}, \quad \geq d - (q-1)w_{\mathrm{Ham}}(\mathbf{c})\right)_R .$$

Beweis. Die Teile (b) und (c) sind klar. Teil (d) wurde in [17, Cor. 1] bewiesen. □

Konstruktion X

Ähnlich wie für herkömmliche lineare Codes über Körpern (z.B. [108, Ch. 18, §7.1]) lässt sich die Konstruktion X auch für R-lineare Codes formulieren:

Definition 2.2.15 *Seien* $\mathcal{C}_1$ *und* $\mathcal{C}_2$ *zwei* R*-lineare Codes der Länge* n *mit den homogenen Minimaldistanzen* d_1 *und* d_2 *und* $\mathcal{C}_1 \leq \mathcal{C}_2$*. Sei weiter ein* R*-linearer* Hilfscode *(engl:* auxiliary code*)* $\mathcal{A}$ *von Länge* n_a*, homogener Minimaldistanz* d_a *und konjugiertem Umriss* $\mathrm{cshp}(\mathcal{A}) = \mathrm{cshp}(\mathcal{C}_2/\mathcal{C}_1)$ *gegeben. Nach Fakt 2.1.5 existiert ein* R*-Modul-Isomorphismus* $\varphi : \mathcal{C}_2/\mathcal{C}_1 \to \mathcal{A}$*. Wir definieren die* Konstruktion X *aus* $\mathcal{C}_1 \leq \mathcal{C}_2$ *mit dem Hilfscode* $\mathcal{A}$ *als den* R*-linearen Code*

$$\hat{\mathcal{C}} \quad = \quad \{(\mathbf{c},\ \varphi(\mathbf{c}+\mathcal{C}_1)) \mid \mathbf{c} \in \mathcal{C}_2\}$$

der Länge $n + n_a$ *und der Größe* $\#\mathcal{C}_2$*.*

Bemerkung 2.2.16

(a) Die Konstruktion X hängt neben den Codes $\mathcal{C}_1$, $\mathcal{C}_2$ und $\mathcal{A}$ auch vom gewählten Isomorphismus φ ab. Somit können im Allgemeinen mehrere Isomorphietypen von Codes als Konstruktion X aus $\mathcal{C}_1 \leq \mathcal{C}_2$ mit dem Hilfscode $\mathcal{A}$ konstruiert werden.

(b) Üblicherweise wird die Konstruktion X dazu benutzt, um ausgehend von zwei Codes $\mathcal{C}_1 \leq \mathcal{C}_2$ von hoher Minimaldistanz d_1 bzw. d_2 einen weiteren guten Code $\hat{\mathcal{C}}$ zu konstruieren. Hierzu sucht man nach einem möglichst kurzen Hilfscode $\mathcal{A}$ vom konjugierten Umriss $\mathrm{cshp}(\mathcal{C}_2/\mathcal{C}_1)$ und von Minimaldistanz $d_a = d_2 - d_1$. Die Wahl von φ ist dann uninteressant, weil nach Fakt 2.2.17 die Minimaldistanz des Codes $\hat{\mathcal{C}}$ bereits festgelegt ist. Aus diesem Grund werden für die Konstruktion X in der Regel die Codes $\mathcal{C}_1$, $\mathcal{C}_2$ und $\mathcal{A}$, aber nicht der Homomorphismus φ angegeben.

(c) Tatsächlich ist der durch Konstruktion X entstehende Code $\hat{\mathcal{C}}$ bereits durch die R-lineare Abbildung

$$\rho : \mathcal{C}_2 \to R^{n_a}, \quad \mathbf{c} \mapsto \varphi(\mathbf{c}+\mathcal{C}_1)$$

festgelegt. Ausgehend von ρ erhält man $\mathcal{C}_2$ als den Definitionsbereich und die anderen beiden Codes als $\mathcal{C}_1 = \ker(\rho)$ und $\mathcal{A} = \mathrm{im}(\rho)$ zurück. Durch Anwenden des Homomorphiesatzes auf ρ rekonstruiert man schließlich den Isomorphismus $\varphi : \mathcal{C}_2/\mathcal{C}_1 \to \mathcal{A}$.

Fakt 2.2.17 *Ein durch Konstruktion X aus $\mathcal{C}_1 \leq \mathcal{C}_2$ mit dem Hilfscode $\mathcal{A}$ gewonnener Code $\hat{\mathcal{C}}$ ist ein R-linearer Code mit den Parametern*

$$\left[n + n_a,\ \mathrm{cshp}(\mathcal{C}_2),\ \hat{d}\right]_R,$$

wobei $\min(d_1, d_2 + d_a) \leq \hat{d} \leq d_1$ *gilt.*

Der Beweis lässt sich völlig analog zur Situation von Codes über endlichen Körpern führen:

Beweis. Weil φ eine lineare Abbildung ist, ist $\hat{\mathcal{C}}$ ein R-linearer Code und als R-Modul isomorph zu $\mathcal{C}_2$. Die homogene Minimaldistanz von $\hat{\mathcal{C}}$ kann also als das minimale homogene Gewicht von $\hat{\mathcal{C}}$ berechnet werden. Jedes Codewort von $\hat{\mathcal{C}}$ hat die Form $\hat{\mathbf{c}} = (\mathbf{c},\ \varphi(\mathbf{c}+\mathcal{C}_1))$ mit $\mathbf{c} \in \mathcal{C}_2$.

(i) Ist $\mathbf{c} \in \mathcal{C}_1$, so ist $\varphi(\mathbf{c} + \mathcal{C}_1) = \mathbf{0}$. Wenn $\mathbf{c}$ das Nullwort ist, so ist auch $\hat{\mathbf{c}}$ das Nullwort. Andernfalls ist $w_{\mathrm{hom}}(\hat{\mathbf{c}}) = w_{\mathrm{hom}}(\mathbf{c}) \geq d_1$. Für die Codewörter $\mathbf{c} \in \mathcal{C}_1$ von minimalem Gewicht gilt $w_{\mathrm{hom}}(\hat{\mathbf{c}}) = d_1$.

(ii) Ist $\mathbf{c} \notin \mathcal{C}_1$, so ist $\mathbf{c} \neq \mathbf{0}$ und $\varphi(\mathbf{c} + \mathcal{C}_1) \neq \mathbf{0}$ und es folgt

$$w_{\mathrm{hom}}(\hat{\mathbf{c}}) = w_{\mathrm{hom}}(\mathbf{c}) + w_{\mathrm{hom}}(\varphi(\mathbf{c} + \mathcal{C}_1)) \geq d_2 + d_a. \qquad \square$$

2.3. Projektive Hjelmslev-Geometrie

Die Hjelmslev-Geometrie geht zurück auf den Artikel [56] aus dem Jahr 1916, in dem der dänische Mathematiker Johannes Hjelmslev eine „Geometrie der Wirklichkeit" vorstellte, in der sich zwei verschiedene Geraden in mehreren Punkten schneiden können und demzufolge die Verbindungsgerade zweier verschiedener Punkte nicht immer eindeutig ist.

Dieser Abschnitt hat die benötigten Grundlagen der projektiven Hjelmslev-Geometrie über Galois-Ringen der Kettenlänge 2 zum Inhalt. Wir richten uns dabei nach [65, 69, 71], wo die projektive Hjelmslev-Geometrie allgemeiner über endlichen Kettenringen beschrieben wird. Im Folgenden ist wieder p eine Primzahl, r eine positive ganze Zahl, R der Galois-Ring $\mathrm{GR}(p^2, r)$, $q = p^r$ die Ordnung seines Restklassenkörpers und $k \geq 2$.

2.3.1. Definitionen

Sei M_R ein freier R-Modul vom Rang k. Der Verband aller Untermoduln von M_R wird mit $\mathrm{PHG}(M_R)$ bezeichnet und heißt die *projektive Hjelmslev-Geometrie* der *Dimension* $k-1$ über R. Bis auf Isomorphie hängt der Verband $\mathrm{PHG}(M_R)$ nur von R und dem Rang k von M_R ab. Die freien Untermoduln vom Rang 1 heißen *Punkte*, diejenigen vom Rang 2 *Geraden* und diejenigen vom Rang $k-1$ *Hyperebenen* von $\mathrm{PHG}(M_R)$. Die Menge aller Punkte, Geraden bzw. Hyperebenen wird mit $\mathcal{P} = \mathcal{G}(M_R, (1,1))$, $\mathcal{L} = \mathcal{G}(M_R, (2,2))$ bzw. $\mathcal{H} = \mathcal{G}(M_R, (k-1, k-1))$ bezeichnet, zur Notation siehe Abschnitt 2.1.4. Wir werden die geometrische Sprechweise der Inzidenz benutzen, die Inzidenzrelation auf den Objekten von $\mathrm{PHG}(M_R)$ ist die Inklusion von Mengen.

Koordinatenvektoren

Nach Fakt 2.1.5 gilt $M_R \cong R_R^k$, so dass wir im Folgenden M mit R^k identifizieren dürfen. Sei $x \in \mathcal{P}$ ein Punkt und $H \in \mathcal{H}$ eine Hyperebene. Ein Vektor $\mathbf{v} \in R^k$ mit $x = R\mathbf{v}$ heißt *Koordinatenvektor* des Punkts x. Analog dazu heißt ein Vektor $\mathbf{v} \in R^k$ mit $H = \mathbf{v}^\perp$ *Koordinatenvektor* der Hyperebene H. Offenbar hat jeder Punkt und jede Hyperebene genau $\#R^* = q(q-1)$ Koordinatenvektoren, und wenn $\mathbf{v}$ ein Koordinatenvektor eines Punkts oder einer Hyperebene ist, so ist die Menge aller Koordinatenvektoren durch $R^*\mathbf{v}$ gegeben. Die als Koordinatenvektoren eines Punkts oder einer Hyperebene auftretenden Vektoren sind genau die torsionsfreien Vektoren in R^k. Jedem Punkt x und jeder Hyperebene H wird willkürlich ein fest gewählter Koordinatenvektor $\kappa(x)$ bzw. $\kappa(H)$ zugewiesen. Beispielsweise kann man unter den möglichen Koordinatenvektoren immer denjenigen Vektor auswählen, dessen erster invertierbarer Eintrag gleich 1 ist.

Multimengen

Wie üblich ist eine *Multimenge* $\mathfrak{M}$ über einer endlichen Grundmenge X eine Abbildung $X \to \mathbb{N}$, die jedem Element $x \in X$ eine *Vielfachheit* (auch *Multiplizität*) $\mathfrak{M}(x)$ zuordnet. Die Multiplizität $\mathfrak{M}(x)$ gibt an, wie oft die Multimenge $\mathfrak{M}$ das Element x enthält. Die *Mächtigkeit* $\#\mathfrak{M} = \sum_{x \in X} \mathfrak{M}(x)$ ist die Anzahl der Elemente von $\mathfrak{M}$, die entsprechend ihrer Vielfachheit gezählt werden. Weiter bezeichnen wir die Menge $\{x \in X \mid \mathfrak{M}(x) \neq 0\}$ als den *Träger* von $\mathfrak{M}$. Ist $S \subseteq X$, so können wir S durch die charakteristische Funktion

$$\chi_S : X \to \mathbb{N}, \quad x \mapsto \begin{cases} 1 & \text{falls } x \in X, \\ 0 & \text{falls } x \notin X \end{cases}$$

auch als eine Multimenge auf X auffassen.

Kollineationen

Ein Verbandsisomorphismus zwischen zwei Hjelmslev-Geometrien wird auch als *Kollineation* bezeichnet; die beiden Geometrien heißen dann *isomorph*. Aus der Diskussion in Abschnitt 2.3.2 geht hervor, dass eine Kollineation bereits durch die Bilder der Punkte

festgelegt ist. Deshalb dürfen wir eine Kollineation zwischen zwei Hjelmslev-Geometrien auch als eine Abbildung zwischen den beiden zugehörigen Punktmengen auffassen.

Die Gruppe der Verbandsautomorphismen von $\mathrm{PHG}(M_R)$ heißt auch *Kollineationsgruppe* von $\mathrm{PHG}(M_R)$. In perfekter Analogie zu den herkömmlichen desargueschen projektiven Geometrien ist nach dem Hauptsatz der projektiven Hjelmslev-Geometrie [96] die Kollineationsgruppe von $\mathrm{PHG}(M_R)$ durch die Gruppe $\mathrm{P\Gamma L}(k, R)$ gegeben.

Die Operation der Kollineationsgruppe von $\mathrm{PHG}(M_R)$ induziert einen Isomorphiebegriff auf den Multimengen von Punkten in $\mathrm{PHG}(M_R)$: Zwei Multimengen $\mathfrak{k}$ und $\mathfrak{k}'$ von Punkten heißen *isomorph*, wenn sie in derselben Bahn unter dieser Gruppenoperation liegen, d.h. wenn eine Kollineation $f : \mathcal{P} \to \mathcal{P}$ existiert mit $\mathfrak{k} \circ f = \mathfrak{k}'$. In diesem Fall schreiben wir $\mathfrak{k} \cong \mathfrak{k}'$. Der Stabilisator von $\mathfrak{k}$ unter der Operation der Kollineationsgruppe wird als die *Kollineationsgruppe* oder *Automorphismengruppe* von $\mathfrak{k}$ bezeichnet.

Der zu $\mathrm{PHG}(M_R)$ duale Verband ist die *duale Hjelmslev-Geometrie*. Beim Übergang zur dualen Geometrie wird die Rolle der Punkte und Hyperebenen vertauscht. Nach Fakt 2.1.9(c) sind $\mathrm{PHG}(M_R)$ und die zu $\mathrm{PHG}(M_R)$ duale Hjelmslev-Geometrie isomorph.

Teilräume

Ein Untermodul U von M_R ist genau dann mit mindestens einem Punkt inzident, wenn $\mathrm{cshp}(U)_1 \neq 0$ ist. In dieser Situation ist U durch die Menge $\mathfrak{k}_U$ der mit U inzidenten Punkte eindeutig festgelegt, so dass wir U mit $\mathfrak{k}_U$ identifizieren dürfen. Die Punktmenge $\mathfrak{k}_U$ heißt dann *Teilraum* von $\mathrm{PHG}(M_R)$ vom *konjugierten Umriss* $\mathrm{cshp}(\mathfrak{k}_U) = \mathrm{cshp}(U)$. Ist U ein freier Modul, so heißt $\mathfrak{k}_U$ auch *Hjelmslev-Teilraum*. Punkte, Geraden und Hyperebenen sind Hjelmslev-Teilräume von $\mathrm{PHG}(M_R)$ vom konjugierten Umriss $(1, 1)$, $(2, 2)$ bzw. $(k - 1, k - 1)$. Der *Spann* einer Multimenge $\mathfrak{k}$ von Punkten in $\mathrm{PHG}(M_R)$ ist der kleinste Teilraum von $\mathrm{PHG}(M_R)$, der alle Punkte aus dem Träger von $\mathfrak{k}$ enthält.

Nachbarn

Anders als in der herkömmlichen projektiven Geometrie kann es in $\mathrm{PHG}(R^k)$ passieren, dass zwei verschiedene Punkte durch mehr als eine Gerade verbunden sind. In diesem Fall heißen die beiden Punkte *Nachbarn*. Auf duale Weise erhalten wir auch einen Nachbarschaftsbegriff auf den Hyperebenen. Für zwei Koordinatenvektoren $\mathbf{v}$ und $\mathbf{w} \in R^k$ sind die beiden Punkte $R\mathbf{v}$ und $R\mathbf{w}$ genau dann Nachbarn, wenn die beiden Hyperebenen $\mathbf{v}^\perp$ und $\mathbf{w}^\perp$ Nachbarn sind. Dies ist genau dann der Fall, wenn $p(\mathbf{v} - \mathbf{w}) = \mathbf{0}$ ist.

Damit erkennt man, dass die Nachbarrelation eine Äquivalenzrelation ist, welche die Punktmenge $\mathcal{P}$ in *Punktklassen* und die Menge der Hyperebenen $\mathcal{H}$ in *Hyperebenenklassen* partitioniert. Die Punktklasse eines Punkts x werden wir mit $[x]$ und die Hyperebenenklasse einer Hyperebene H mit $[H]$ bezeichnen. Punkt- und Hyperebenenklassen[27] sind Teilräume von $\mathrm{PHG}(R^k)$ vom konjugierten Umriss $\mathrm{cshp}([x]) = (k, 1)$ bzw. $\mathrm{cshp}([H]) = (k, k - 1)$. Weiter heißt der Punkt x *Nachbar* der Hyperebene H, wenn H

[27] An dieser Stelle identifizieren wir wie üblich $[H]$ mit der Menge aller Punkte, die in irgendeiner Hyperebene in $[H]$ enthalten sind.

einen zu x benachbarten Punkt enthält oder dazu äquivalent, wenn $[x]$ in $[H]$ enthalten ist.

Affine Hjelmslev-Geometrie

Für einen Untermodul U von M_R und $\mathbf{v} \in M_R$ heißt $A = \mathbf{v} + U$ ein *affiner Teilraum* von R^k. In dieser Darstellung ist der Untermodul U eindeutig festgelegt. Der *konjugierte Umriss* $\mathrm{cshp}(A)$ von A ist definiert als der konjugierte Umriss von U. Betrachtet man den Verband aller affinen Teilräume von M_R, so gelangt man zur *affinen Hjelmslev-Geometrie* $\mathrm{AHG}(M_R)$. Die *Punkte* der affinen Hjelmslev-Geometrie sind die affinen Unterräume vom konjugierten Umriss $() = (0, 0)$, d.h. jeder Punkt hat die Form $\{\mathbf{v}\}$ und kann mit seinem affinen Koordinatenvektor $\mathbf{v}$ identifiziert werden. Die *Geraden* von $\mathrm{AHG}(M_R)$ sind die affinen Unterräume vom konjugierten Umriss $(1, 1)$ und die *Hyperebenen* die affinen Unterräume vom konjugierten Umriss $(k-1, k-1)$.

Wie in der herkömmlichen projektiven Geometrie kann $\mathrm{AHG}(R^k)$ in $\mathrm{PHG}(R^{k+1})$ eingebettet werden: Die durch $\mathbf{v} \mapsto R(1, \mathbf{v})$ induzierte *Standardeinbettung* $\mathrm{AHG}(R^k) \to \mathrm{PHG}(R^{k+1})$ ist injektiv und inzidenzerhaltend. Das Bild eines affinen Teilraums von R^k vom konjugierten Umriss (λ_0, λ_1) ist ein Untermodul von R^{k+1} vom konjugierten Umriss $(\lambda_0 + 1, \lambda_1 + 1)$. Insbesondere werden Punkte auf Punkte, Geraden auf Geraden und Hyperebenen auf Hyperebenen abgebildet. Das Bild der Punktmenge von $\mathrm{AHG}(R^k)$ ist das Komplement der *unendlich fernen* Hyperebenenklasse $(p, 0, \ldots, 0)^\perp$ in der Punktmenge von $\mathrm{PHG}(R^{k+1})$.

2.3.2. Punkt-Geraden-Inzidenzen

Wir haben uns bei der obigen Definition zweckmäßigerweise auf Hjelmslev-Geometrien beschränkt, die über Galois-Ringen koordinatisierbar sind. Allgemeiner werden Hjelmslev-Geometrien synthetisch über Axiome an die Punkt-Geraden-Inzidenzen definiert; siehe z.B. [93, 2, 97] sowie [104] für affine Hjelmslev-Ebenen.

Tatsächlich reicht in unserer Situation der projektiven Hjelmslev-Geometrien über einem Galois-Ring der Länge 2 die Inzidenzrelation $I \subseteq \mathcal{P} \times \mathcal{L}$ zwischen der Punktmenge $\mathcal{P}$ und der Geradenmenge $\mathcal{L}$ aus, um den Untermodulverband von M_R schrittweise zu rekonstruieren: Man überprüft, dass die folgenden inzidenzgeometrischen Beschreibungen gelten:

- Eine Punktmenge $\mathfrak{k}$ ist ein Hjelmslev-Teilraum genau dann, wenn $\mathfrak{k}$ für alle $x, y \in \mathfrak{k}$ auch eine Verbindungsgerade von x und y enthält. Weiter ist $\mathfrak{k}$ ein Teilraum genau dann, wenn für alle $x, y \in \mathfrak{k}$ der Schnitt aller Verbindungsgeraden von x und y in $\mathfrak{k}$ enthalten ist.

- Der Spann von $\mathfrak{k}$ ist der Schnitt aller $\mathfrak{k}$ umfassenden Teilräume von $\mathrm{PHG}(M_R)$.[28]

[28] In [65, 69, 71] wird der Spann (engl. *closure*, *hull*) als der Schnitt aller $\mathfrak{k}$ umfassenden *Hjelmslev*-Teilräume definiert. Hierbei hat man aber das Problem, dass eine Hyperebenenklasse nicht als Spann auftreten kann.

- Den konjugierten Umriss $\mathrm{cshp}(\mathfrak{k}) = (\lambda_0, \lambda_1)$ eines Hjelmslev-Teilraums $\mathfrak{k}$ erhält man wie folgt: Die Zahl λ_0 ist die minimale Mächtigkeit einer $\mathfrak{k}$ aufspannenden Teilmenge von $\mathfrak{k}$. Für Hjelmslev-Teilräume ist wegen $\lambda_1 = \lambda_0$ der konjugierte Umriss damit bereits festgelegt. Für allgemeine Teilräume erhält man λ_1 als den größtmöglichen konjugierten Umriss (λ_1, λ_1) eines in $\mathfrak{k}$ enthaltenen Hjelmslev-Teilraums.

Auf diese Weise liefern die Punkt-Geraden-Inzidenzen alle Untermoduln von M_R, für die der zugehörige Teilraum mindestens einen Punkt enthält, also alle Untermoduln vom konjugierten Umriss (λ_0, λ_1) mit $\lambda_1 \neq 0$. Da $\perp$ eine inklusionsumkehrende Bijektion auf dem Untermodulverband ist, können weiter die Untermoduln vom konjugierten Umriss $(\lambda_0, 0)$ mit $\lambda_0 \in \{0, \ldots, k-1\}$ samt der zugehörigen Inklusionsbeziehungen aus den bereits beschriebenen Untermoduln vom konjugierten Umriss $(k, k-\lambda_0)$ abgeleitet werden. Vom letzten verbleibenden konjugierten Umriss $(k, 0)$ gibt es genau einen Untermodul U, dessen Inklusionsbeziehung zu einem weiteren Untermodul N bereits durch $\mathrm{cshp}(N)$ festgelegt ist. Damit ist die Rekonstruktion des Untermodulverbands vollständig.

Mit dieser Argumentation sehen wir auch, dass ein Verbandsisomorphismus zwischen zwei Hjelmslev-Geometrien bereits durch die Bilder der Punkte festgelegt ist und dass eine Bijektion zwischen zwei Hjelmslev-Geometrien bereits dann einen Verbandsisomorphismus induziert, wenn sie die Punkt-Geraden-Inzidenzen erhält. Der in Abschnitt 2.3.1 erklärte Kollineationsbegriff stimmt also mit dem in der synthetischen Geometrie üblichen Kollineationsbegriff überein.

2.3.3. Inzidenzanzahlen

Mit Hilfe von Fakt 2.1.7 lassen sich viele Inzidenzanzahlen leicht berechnen. In unserer Situation der Kettenlänge 2 treten nur konjugierte Umrisse der Länge 2 auf. Für diese hat der verallgemeinerte Gauß-Koeffizient die Form

$$\begin{bmatrix}(\lambda_0, \lambda_1)\\(\mu_0, \mu_1)\end{bmatrix}_q = q^{\mu_1(\lambda_0-\mu_0)} \cdot \begin{bmatrix}\lambda_0 - \mu_1\\ \mu_0 - \mu_1\end{bmatrix}_q \cdot \begin{bmatrix}\lambda_1\\ \mu_1\end{bmatrix}_q.$$

Damit erhalten wir

$$\#\mathcal{P} = \#\mathcal{H} = \begin{bmatrix}(k,k)\\(1,1)\end{bmatrix}_q = \begin{bmatrix}(k,k)\\(k-1,k-1)\end{bmatrix}_q = q^{k-1} \cdot \frac{q^k - 1}{q-1}.$$

Es gibt insgesamt

$$\begin{bmatrix}(k,k)\\(k,1)\end{bmatrix}_q = \begin{bmatrix}(k,k)\\(k,k-1)\end{bmatrix}_q = \frac{q^k - 1}{q-1}$$

Punkt- und Hyperebenenklassen, und jede Punkt- bzw. Hyperebenenklasse enthält

$$\begin{bmatrix}(k,1)\\(1,1)\end{bmatrix}_q = \begin{bmatrix}(k,k-1)\\(k-1,k-1)\end{bmatrix}_q = q^{k-1}$$

Punkte bzw. Hyperebenen. Weiter enthält jede Hyperebene genau

$$\begin{bmatrix}(k-1,k-1)\\(1,1)\end{bmatrix}_q = q^{k-2} \cdot \frac{q^{k-1} - 1}{q-1}$$

Punkte und dual dazu geht durch jeden Punkt dieselbe Anzahl an Hyperebenen. Die Anzahl der Punkte in einer Hyperebenenklasse ist

$$\begin{bmatrix}(k,k-1)\\(1,1)\end{bmatrix}_q = q^{k-1}\cdot\frac{q^{k-1}-1}{q-1}.$$

Damit erhalten wir eine Bestätigung für die Anzahl der Punkte in affinen Hjelmslev-Geometrien, denn das Komplement einer Hyperebenenklasse ist das Bild von $\mathrm{AHG}(R^{k-1})$ unter der Standardeinbettung und enthält genau

$$q^{k-1}\cdot\frac{q^k-1}{q-1} - q^{k-1}\cdot\frac{q^{k-1}-1}{q-1} = q^{2(k-1)}$$

Punkte.

2.3.4. Verbindung zur Codierungstheorie

Sei $\mathcal{C}$ ein fetter R-linearer Code, der frei vom Rang k ist. Dann bestehen die Spalten einer Generatormatrix $\mathbf{G}$ ausschließlich aus torsionsfreien Vektoren. Die Spalten sind also Koordinatenvektoren von Punkten in $\mathrm{PHG}(R^k)$, und die auf diese Art definierte Multimenge von Punkten wird mit $\mathrm{pts}(\mathcal{C})$ bezeichnet. Bis auf das Anwenden einer Kollineation ist diese Definition unabhängig von der Wahl der Generatormatrix $\mathbf{G}$. Weil $\mathcal{C}$ frei ist, ist der Spann von $\mathrm{pts}(\mathcal{C})$ die gesamte Geometrie $\mathrm{PHG}(R^k)$.

Sei nun umgekehrt $\mathfrak{k}$ eine Multimenge von Punkten in $\mathrm{PHG}(R^k)$, welche die volle Geometrie $\mathrm{PHG}(R^k)$ aufspannt. Durch spaltenweises Eintragen (entsprechend der Vielfachheit in $\mathfrak{k}$) von Koordinatenvektoren der Punkte in $\mathfrak{k}$ erhalten wir eine $(k\times\#\mathfrak{k})$-Matrix $\mathbf{G}$ über R. Der von $\mathfrak{k}$ erzeugte R-lineare Code $\mathrm{cde}(\mathfrak{k})$ ist nun der Zeilenraum von $\mathbf{G}$. Er ist ein fetter Code, der frei ist vom Rang k. Bis auf lineare Äquivalenz von Codes ist diese Definition unabhängig von der Wahl der Koordinatenvektoren und der Reihenfolge der Spalten in $\mathbf{G}$.

Diese beiden Zuweisungen sind im folgenden Sinne zueinander invers: Für alle Multimengen von Punkten $\mathfrak{k}$ in $\mathrm{PHG}(R^k)$, welche die volle Geometrie aufspannen, gilt die Isomorphie

$$\mathrm{pts}(\mathrm{cde}(\mathfrak{k}))\cong\mathfrak{k},$$

und für alle fetten R-linearen Codes $\mathcal{C}$, die frei vom Rang k sind, gilt die semilineare Isometrie

$$\mathrm{cde}(\mathrm{pts}(\mathcal{C}))\cong\mathcal{C}.$$

Typ und Spektrum

Sei nun $\mathfrak{k}$ eine Multimenge von Punkten in $\mathrm{PHG}(R^k)$. Für $S\subseteq\mathcal{P}$ setzen wir $\mathfrak{k}(S)=\sum_{x\in S}\mathfrak{k}(x)$. Insbesondere ist dann $\#\mathfrak{k}=\mathfrak{k}(\mathcal{P})$.

Für eine Hyperebene H bezeichne

$$a_2(H)=\mathfrak{k}(H),\qquad a_1(H)=\mathfrak{k}([H]\setminus H),\qquad a_0(H)=\mathfrak{k}(\mathcal{P}\setminus[H]).$$

Es ist also $a_2(H)$ die Anzahl der auf H liegenden Punkte in $\mathfrak{k}$, $a_1(H)$ die Anzahl der zu H benachbart, aber nicht auf H liegenden Punkte von $\mathfrak{k}$ und $a_0(H)$ die Anzahl der Punkte in $\mathfrak{k}$, die von H „weit entfernt" (d.h. nicht benachbart) sind. Dabei wird jeder Punkt entsprechend seiner Vielfachheit in $\mathfrak{k}$ gezählt. Wir nennen

$$\mathbf{a}_{\mathfrak{k}}(H) = (a_0(H), a_1(H), a_2(H)) \in \mathbb{N}^3$$

den $\mathfrak{k}$-*Typ* der Hyperebene H. Weiter heißt das Zählpolynom

$$\operatorname{spec}(\mathfrak{k}) = \sum_{H\in\mathcal{H}} \mathbf{X}^{\mathbf{a}_{\mathfrak{k}}(H)} = \sum_{H\in\mathcal{H}} X_0^{a_0(H)} X_1^{a_1(H)} X_2^{a_2(H)} \in \mathbb{Z}[X_0, X_1, X_2]$$

das *Spektrum* von $\mathfrak{k}$. In der Schreibweise

$$\operatorname{spec}(\mathfrak{k}) = \sum_{\omega\in\mathbb{N}^3} A_\omega \mathbf{X}^\omega$$

gibt ein Koeffizient A_ω die Anzahl der Hyperebenen vom $\mathfrak{k}$-Typ ω in $\mathrm{PHG}(R^k)$ an. Wie bei den Gewichtszählern werden wir Spektren meist in Form einer Tabelle angeben.

Aus geometrischer Sicht entsprechen die Codewörter des Codes $\mathcal{C}$ den Hyperebenen in $\mathrm{PHG}(R^k)$. Präziser zeigt für torsionsfreie Vektoren $\mathbf{x} \in R^n$ die Gleichung

$$w_{\mathrm{sym}}(\mathbf{xG}) = \mathbf{a}_{\mathrm{pts}(\mathcal{C})}(\mathbf{x}^\perp),$$

dass eine Hyperebene H den $q(q-1)$ Codewörtern $\mathbf{xG}$ entspricht, deren Informationsvektoren $\mathbf{x}$ Koordinatenvektoren von H sind. Ist weiter $\mathbf{x} \neq \mathbf{0}$ ein Torsionsvektor, dann ist $\mathbf{x} = p\mathbf{y}$ mit einem torsionsfreien Vektor $\mathbf{y}$ und $w_{\mathrm{sym}}(\mathbf{xG}) = (0, \omega_0, \omega_1 + \omega_2)$ mit $(\omega_0, \omega_1, \omega_2) = \mathbf{a}_{\mathrm{pts}(\mathcal{C})}(\mathbf{y}^\perp)$. Daran erkennen wir, dass das Spektrum von $\mathfrak{k}$ das geometrische Gegenstück des symmetrisierten Gewichtszählers von $\mathcal{C}$ ist:

Fakt 2.3.1 ([65, Th. 5.2], [69, Th. 5.2])

(a) Sei $\mathcal{C}$ ein fetter R-linearer Code, der frei vom Rang k ist. Dann spannt $\mathrm{pts}(\mathcal{C})$ *die volle Geometrie* $\mathrm{PHG}(R^k)$ *auf. Das Spektrum von* $\mathrm{pts}(\mathcal{C})$ *ist gegeben durch*

$$\operatorname{spec}(\mathrm{pts}(\mathcal{C})) = \frac{1}{q(q-1)} f,$$

wobei f die Summe aller durch X_0 teilbaren Terme in $w_{\mathrm{sym}}(\mathcal{C})$ bezeichnet.

(b) Sei $\mathfrak{k}$ eine Multimenge von Punkten in $\mathrm{PHG}(R^k)$*, welche die volle Geometrie aufspannt. Dann ist der Code* $\mathrm{cde}(\mathfrak{k})$ *fett und frei vom Rang k. Der symmetrisierte Gewichtszähler von* $\mathrm{cde}(\mathfrak{k})$ *ist gegeben durch*

$$w_{\mathrm{sym}}(\mathrm{cde}(\mathfrak{k})) = X_2^n + q(q-1)\operatorname{spec}(\mathfrak{k})(X_0, X_1, X_2) + \frac{q-1}{q^{k-1}} \operatorname{spec}(\mathfrak{k})(X_1, X_2, X_2).$$

Geometrische Interpretation von Codemodifikationen

Sei $\mathfrak{k}$ eine Multimenge von Punkten in $\mathrm{PHG}(R^k)$, die die volle Geometrie aufspannt. Für den Code $\mathrm{cde}(\mathfrak{k})$ lassen sich die Modifikationen aus Abschnitt 2.2.6 wie folgt interpretieren:

- *Punktieren*: Sei x ein Punkt im Träger von $\mathfrak{k}$. Sei i eine zu x gehörende Koordinate von $\mathrm{cde}(\mathfrak{k})$. Wenn auch $\mathfrak{k} - \chi_{\{x\}}$ noch die volle Geometrie aufspannt, so ist $P_{\{i\}}(\mathrm{cde}(\mathfrak{k})) \cong \mathrm{cde}(\mathfrak{k} - \chi_{\{x\}})$, d.h. das Punktieren von $\mathrm{cde}(\mathfrak{k})$ in der zu x gehörenden Koordinate entspricht dem Reduzieren der Vielfachheit von x in $\mathfrak{k}$ um 1.

- *Verkürzen*: Sei wieder x ein Punkt im Träger von $\mathfrak{k}$ und i eine zu x gehörende Koordinate von $\mathrm{cde}(\mathfrak{k})$. Die Projektionsabbildung $\mathrm{PHG}(R^k) \to \mathrm{PHG}(R^k/x)$, $U \mapsto U + x$ ist surjektiv und inzidenzerhaltend. Auf diese Weise entsprechen die Punkte von $\mathrm{PHG}(R^k/x)$ eindeutig den mit x inzidenten Geraden in $\mathrm{PHG}(R^k)$. Wenn der Träger von $\mathfrak{k} - \chi_{\{x\}}$ keinen zu x benachbarten Punkt enthält (insbesondere darf x in $\mathfrak{k}$ nur mit Multiplizität 1 enthalten sein), so sei $\mathfrak{k}_x$ die Multimenge in $\mathrm{PHG}(R^k/x)$, die durch *Zentralprojektion* von $\mathfrak{k}$ auf x entsteht. Dabei werden alle Punkte in $\mathfrak{k}$, die auf derselben Geraden L durch x liegen, zu einem Punkt $x + L$ in $\mathrm{PHG}(R^k/x) \cong \mathrm{PHG}(R^{k-1})$ zusammengefasst. Die Vielfachheit dieses Punkts in $\mathfrak{k}_x$ ist die Summe der Vielfachheiten aller zusammengefassten Punkte in $\mathfrak{k}$. Dann ist $\#\mathfrak{k}_x = \#\mathfrak{k} - 1$ und es gilt $S_{\{i\}}(\mathrm{cde}(\mathfrak{k})) \cong \mathrm{cde}(\mathfrak{k}_x)$, d.h. das Verkürzen von $\mathrm{cde}(\mathfrak{k})$ in der zu x gehörenden Koordinate entspricht der Zentralprojektion von $\mathfrak{k}$ auf x.

- *Residuum*: Sei nun $H = \mathbf{y}^\perp$ eine Hyperebene und $\mathbf{c} = \mathbf{yG}$ ein zugehöriges Codewort in $\mathrm{cde}(\mathfrak{k})$. Wir fassen die auf H liegenden Punkte von $\mathfrak{k}$ als eine Multimenge in $\mathrm{PHG}(R^{k-1})$ auf. Ist die Voraussetzung von Fakt 2.2.14(d) erfüllt, d.h. $(q-1)w_{\mathrm{Ham}}(\mathbf{c}) < d_{\mathrm{hom}}(\mathrm{cde}(\mathfrak{k}))$, so spannt $\mathfrak{k}_H$ die volle Geometrie $\mathrm{PHG}(R^{k-1})$ auf und es gilt $\mathrm{cde}(\mathfrak{k}_H) \cong \mathrm{res}_{\mathbf{c}}(\mathrm{cde}(\mathfrak{k}))$. Der Übergang von $\mathrm{cde}(\mathfrak{k})$ zum residuellen Code in $\mathbf{c}$ entspricht also dem Einschränken von $\mathfrak{k}$ auf die zu $\mathbf{c}$ gehörende Hyperebene.

Arcs

Ist $\mathfrak{k}$ eine Multimenge von Punkten in $\mathrm{PHG}(M_R)$, so ist $\mathfrak{k}$ ein *u-Arc* (auch: *$(\#\mathfrak{k}, u)$-Arc*), wenn jede Hyperebene von $\mathrm{PHG}(M_R)$ höchstens u Punkte aus $\mathfrak{k}$ enthält[29] und die Zahl u minimal ist mit dieser Eigenschaft (d.h. es existiert eine Hyperebene, die genau u Punkte aus $\mathfrak{k}$ enthält).

Die Existenz eines herkömmlichen $\mathbb{F}_q$-linearen $[n, k, d]_{\mathbb{F}_q}$-Codes ist äquivalent zur Existenz eines $(n, n-d)$-Arcs in der projektiven Geometrie $\mathrm{PG}(\mathbb{F}_q^k)$ der Dimension $k-1$ über $\mathbb{F}_q$. Dementsprechend ist man daran interessiert, zu einer vorgegebenen Zahl u einen möglichst großen u-Arc in $\mathrm{PG}(\mathbb{F}_q^k)$ zu finden.

Für R-lineare Codes gibt es keine direkte Entsprechung zwischen großen Arcs und Codes hoher homogener Minimaldistanz. Die Suche nach großen Arcs bildet eine separate Fragestellung, die intensiv untersucht wurde. Ergebnisse finden sich beispielsweise in [55,

[29] Auch hier werden die Punkte in $\mathfrak{k}$ wieder entsprechend ihrer Vielfachheit gezählt.

103, 66, 67, 82, 60, 85, 83, 102, 63, 84, 7, 62, 61]. Eine verwandte Fragestellung ist die Suche nach Punktmengen mit nur 2 Schnittzahlen (engl. *two-intersection set*), siehe [94, 59]. Die Suche nach großen Arcs ist jedoch auch für die Codierungstheorie über R relevant. Denn zum einen liefern große Arcs mit wenigen Schnittzahlen oder vielen Symmetrien häufig auch gute Codes, und zum anderen trägt die Untersuchung von großen Arcs zu einem besseren Verständnis der Kombinatorik der projektiven Hjelmslev-Geometrien bei, das der Analyse und Konstruktion R-linearer Codes zugutekommt.

2.4. Beispiele R-linearer Codes

Es sei wieder $R = \mathrm{GR}(p^2, r)$ ein Galois-Ring der Kettenlänge 2 und $q = p^r$.

2.4.1. Simplex-Codes

Dieser Abschnitt folgt [65, Sec. 6.1], wo die R-linearen Simplex-Codes eingeführt wurden. Sei im Folgenden $\mathcal{P}$ die Punktmenge der Hjelmslev-Geometrie $\mathrm{PHG}(R^k)$ mit $k \geq 2$. Wir berechnen das Spektrum von $\mathcal{P}$: Mit den Anzahlen aus Abschnitt 2.3.3 sehen wir, dass es in $\mathrm{PHG}(R^k)$ genau $q^{k-1} \cdot \frac{q^k-1}{q-1}$ Hyperebenen gibt, und dass jede Hyperebene H genau $q^{k-2} \cdot \frac{q^{k-1}-1}{q-1}$ Punkte von $\mathcal{P}$ enthält. Weiter liegen genau

$$q^{k-1} \cdot \frac{q^{k-1}-1}{q-1} - q^{k-2} \cdot \frac{q^{k-1}-1}{q-1} = q^{k-2}(q^{k-1}-1)$$

Punkte aus $\mathcal{P}$ benachbart, aber nicht innerhalb von H, und die verbleibenden $q^{2(k-1)}$ Punkte der Geometrie liegen nicht benachbart zu H. Somit ergibt sich

$$\mathrm{spec}(\mathcal{P}) = q^{k-1} \cdot \frac{q^k-1}{q-1} X_0^{q^{2(k-1)}} X_1^{q^{k-2}(q^{k-1}-1)} X_2^{q^{k-2} \cdot \frac{q^{k-1}-1}{q-1}}.$$

Der k-dimensionale *Simplex-Code* über R ist nun definiert als $\mathrm{Sim}(k, R) = \mathrm{cde}(\mathcal{P})$. Die Punktmenge $\mathcal{P}$ spannt offensichtlich die komplette Geometrie auf. So ist $\mathrm{Sim}(k, R)$ ein freier, fetter R-linearer Code vom Rang k. Weil $\mathrm{Sim}(k, R)$ ein freier Code ist, stimmen Torsions- und Radikalcode überein, und es ergibt sich die q^{k-1}-fache Wiederholung des herkömmlichen Simplex-Codes $\mathrm{Sim}(k, \mathbb{F}_q)$.

Mit Hilfe von Fakt 2.3.1 berechnen wir die Parameter:

Fakt 2.4.1 ([65, Sec. 6.1])

(a) Der Simplex-Code $\mathrm{Sim}(k, R)$ *hat die Parameter*

$$\left[q^{k-1} \cdot \frac{q^k-1}{q-1}, \quad (k, k), \quad q^{2k-1} - q^{k-1} \right]_R.$$

Tabelle 2.4.1 zeigt den symmetrisierten Gewichtszähler von $\mathrm{Sim}(k, R)$.

Tabelle 2.4.1.: Symmetrisierter Gewichtszähler des Simplex-Code $\mathrm{Sim}(k, R)$

Typ	#Codewörter	ω_0	ω_1	ω_2	w_{hom}
S	$q^k(q^k-1)$	$q^{2(k-1)}$	$q^{k-2}(q^{k-1}-1)$	$q^{k-2}\cdot\frac{q^{k-1}-1}{q-1}$	$q^{2k-1}-q^{k-1}$
pS	q^k-1	0	$q^{2(k-1)}$	$q^{k-1}\cdot\frac{q^{k-1}-1}{q-1}$	q^{2k-1}
0	1	0	0	$q^{k-1}\cdot\frac{q^k-1}{q-1}$	0

(b) Das Gray-Bild von $\mathrm{Sim}(k, R)$ *hat die Parameter*

$$\left(q^k\cdot\frac{q^k-1}{q-1},\quad q^{2k},\quad q^{2k-1}-q^{k-1}\right)_q$$

und den Hamming-Gewichtszähler

$$1 \quad + \quad q^k(q^k-1)X^{q^{2k-1}-q^{k-1}} \quad + \quad (q^k-1)X^{q^{2k-1}}.$$

Bemerkung 2.4.2

(a) Das Gray-Bild von $\mathrm{Sim}(k, R)$ hat hervorragende Parameter, als $\mathbb{F}_q$-linearer Code wäre es Griesmer-optimal. Andererseits ist $\mathrm{Sim}(k, R)$ kein BTL-Code, denn mit den MacDonald-Codes aus [116] existiert stets ein $\mathbb{F}_q$-linearer Code mit denselben Parametern.[30] Als eine weitere Konstruktionsmöglichkeit kann man die Simplex-Konstruktion über dem Kettenring $\mathbb{F}_q[X]/(X^2)$ durchführen; die verallgemeinerten Gray-Bilder solcher Codes sind stets linear. Tatsächlich sind alle linearen Codes mit den entsprechenden Parametern zu den MacDonald-Codes isomorph [124, Th. 2.1]. Ein kurzer Beweis über geometrisches Dualisieren findet sich in [35, Prop. 5]. Zur Darstellung allgemeinerer MacDonald-Codes über endlichen Kettenringen siehe [64, Th. 11] und [65, Th. 6.1].

(b) Das Beispiel der Simplex-Codes belegt, dass die Konstruktionsmethode „Gray-Bilder R-linearer Codes" – unabhängig vom Parameter q – prinzipiell in der Lage ist, sehr gute Blockcodes zu generieren.

2.4.2. Teichmüller-Codes und Kerdock-Codes

Es sei $p = 2$. Wir betrachten die Ringerweiterung $R = \mathrm{GR}(4, r) \subseteq S = \mathrm{GR}(4, rk)$ mit $k \geq 3$ ungerade. Für die Teichmüller-Gruppen U^* von R und T^* von S gilt $U^* \leq T^*$ und $[T^* : U^*] = (q^k-1)/(q-1)$. Vermöge der R-Modul-Isomorphie $S \cong R^k$ können wir ein Vertretersystem von T^*/U^* als eine Menge von $(q^k-1)/(q-1)$ Vektoren in R^k auffassen. Weil alle solchen Elemente in S^* liegen, hat jeder dieser Vektoren mindestens einen invertierbaren Eintrag, d.h. jeder Vektor ist der Koordinatenvektor eines

[30] Die Codes werden in [116] auf Seite 108 mit M_m bezeichnet. Die dortigen Parameter k und m müssen in unserer Schreibweise auf $2k$ und k gesetzt werden. Für den binären Fall $q = 2$ wurden die Codes bereits in [107] als *Type 13*-Codes eingeführt.

Punkts in PHG(R^k). Die durch diese Koordinatenvektoren gegebene Punktmenge heißt *Teichmüller-Punktmenge* $\mathfrak{T}_{q,k}$. Da je zwei Vektoren in derselben Nebenklasse von T^*/U^* denselben Punkt beschreiben, ist $\mathfrak{T}_{q,k}$ unabhängig von der Wahl des Vertretersystems.

Betrachtet man die Teichmüller-Menge $T = T^* \cup \{0\}$ als eine Menge von q^k affinen Koordinatenvektoren, so erhält man eine Teilmenge der Punktmenge von AHG(R^k). Das Bild dieser Punktmenge in PHG(R^{k+1}) unter der Standardeinbettung heißt *Kerdock-Punktmenge* $\mathfrak{K}_{q,k+1}$.

Sowohl $\mathfrak{T}_{q,k}$ als auch $\mathfrak{K}_{q,k+1}$ spannen jeweils die komplette Punktmenge der Umgebungsgeometrie PHG(R^k) bzw. PHG(R^{k+1}) auf. Die erzeugten Codes $\mathcal{T}_{q,k} = \mathrm{cde}(\mathfrak{T}_{q,k})$ und $\mathcal{K}_{q,k} = \mathrm{cde}(\mathfrak{K}_{q,k})$ heißen *Teichmüller-Codes* bzw. *Kerdock-Codes*.

Bemerkung 2.4.3

(a) Der Name Teichmüller-Punktmenge (*Teichmüller set*) stammt aus [55, 68], [59, Ex. II.3]. Sie enthalten mit $\mathfrak{T}_{q,3}$ die Hyperovale aus [67] als Spezialfall. Der naheliegende Bezeichner *Teichmüller-Codes* für die erzeugten Codes wurde in [91, 92] eingeführt. Die Teichmüller-Codes fassen die verkürzten $\mathbb{Z}_4$-linearen Kerdock-Codes ($q = 2$) und die von den Hyperovalen in [67] kommenden Codes ($k = 3$) in einer allgemeineren Codeklasse zusammen. Das Spektrum der Teichmüller-Punktmengen und der symmetrisierte Gewichtszähler der Teichmüller-Codes lassen sich aus [59, Ex. II.3] ableiten.

In Abschnitt 3.1 werden wir die Teichmüller-Punktmengen und -Codes verallgemeinern und erhalten damit einen zusätzlichen Parameter s. Spektrum und symmetrisierte Gewichtszähler ergeben sich dann auch als der Spezialfall $s = 0$ aus den Sätzen 3.1.8 und 3.1.10.

(b) Unter den Kerdock-Codes verstand man zunächst die von Kerdock in [80] eingeführten nichtlinearen binären Blockcodes. In [111, 52] wurde gezeigt, dass sich diese bis auf eine Koordinatenpermutation als Gray-Bild der $\mathbb{Z}_4$-linearen Kerdock-Codes $\mathcal{K}_{2,k+1}$ darstellen lassen. Diese $\mathbb{Z}_4$-linearen Kerdock-Codes werden wir im Folgenden einfacher mit $\mathcal{K}_{k+1}$ und die zugehörigen Punktmengen mit $\mathfrak{K}_{k+1}$ bezeichnen. In [99] wurden die Codes $\mathcal{K}_{k+1}$ auf die Codes $\mathcal{K}_{q,k+1}$ über beliebigen Galois-Ringen der Charakteristik 4 verallgemeinert.

(c) Im $\mathbb{Z}_4$-linearen Fall gilt $\#U^* = 1$, und damit erhält man den Teichmüller-Code $\mathcal{T}_{2,k}$ durch Verkürzen des Kerdock-Codes $\mathcal{K}_{k+1}$ an der zum Teichmüller-Element 0 gehörenden Position. Weil nach [52, Sec. V-E] die Automorphismengruppe der $\mathbb{Z}_4$-linearen Kerdock-Codes transitiv (sogar doppelt transitiv) auf den Positionen operiert, führt auch das Verkürzen an jeder anderen Position zum Code $\mathcal{T}_{2,k}$.

(d) Im vorliegenden Fall der geraden Charakteristik hat die Teichmüller-Menge T eine reiche kombinatorische Struktur (siehe. z.B. [8, Sec. III], [59, Sec. VI], wir werden diese Aussagen in Abschnitt 3.1 verallgemeinern), wodurch sich Codes mit sehr wenigen Gewichten und hoher Minimaldistanz ergeben und ein allgemeiner Beweis der Eigenschaften ermöglicht wird. Prinzipiell sind die genannten Konstruktionen

Tabelle 2.4.2.: Spektrum der Kerdock-Punktmenge $\mathfrak{K}_{q,k+1}$

Typ	#Hyperebenen	ω_0	ω_1	ω_2
H_{++}	$\frac{1}{2}\frac{q^k-1}{q-1}(q^k+q^{\frac{k+1}{2}})$	q^k-q^{k-1}	$q^{k-1}-q^{k-2}-(q^{\frac{k-1}{2}}-q^{\frac{k-3}{2}})$	$q^{k-2}+(q^{\frac{k-1}{2}}-q^{\frac{k-3}{2}})$
H_{+}	$\frac{1}{2}(q^k-1)(q^k-q^{\frac{k+1}{2}})$	q^k-q^{k-1}	$q^{k-1}-q^{k-2}-q^{\frac{k-3}{2}}$	$q^{k-2}+q^{\frac{k-3}{2}}$
H_0	q^k	q^k	0	0
H_{-}	$\frac{1}{2}(q^k-1)(q^k+q^{\frac{k+1}{2}})$	q^k-q^{k-1}	$q^{k-1}-q^{k-2}+q^{\frac{k-3}{2}}$	$q^{k-2}-q^{\frac{k-3}{2}}$
H_{--}	$\frac{1}{2}\frac{q^k-1}{q-1}(q^k-q^{\frac{k+1}{2}})$	q^k-q^{k-1}	$q^{k-1}-q^{k-2}+(q^{\frac{k-1}{2}}-q^{\frac{k-3}{2}})$	$q^{k-2}-(q^{\frac{k-1}{2}}-q^{\frac{k-3}{2}})$

auch in ungerader Charakteristik durchführbar. Hier verhält sich T jedoch ziemlich chaotisch und die erzeugten Codes erscheinen aufgrund vieler verschiedener Gewichte und einer schlechten Minimaldistanz uninteressant.

(e) Durch Punktieren an der Position des Teichmüller-Elements 0 entsteht aus dem Kerdock-Code $\mathcal{K}_{q,k+1}$ der *punktierte Kerdock-Code* $\dot{\mathcal{K}}_{q,k+1}$. An dieser Stelle sei angemerkt, dass die Parameter in [113, Th. 4] für den punktierten Kerdock-Code fehlerhaft sind: Demzufolge hätte der Code $\dot{\mathcal{K}}_{4,3+1}$ nur die homogene Minimaldistanz 176. Tatsächlich hat das Gray-Bild aber die BTKL-Parameter $(252, 4^8, 177)_4$. Auch operiert die Automorphismengruppe im Allgemeinen nicht mehr transitiv auf den Positionen: Punktieren von $\mathcal{K}_{4,3+1}$ an jeder anderen Position liefert einen Code der minimalen homogenen Distanz 176.

Fakt 2.4.4

(a) Die Kerdock-Punktmenge $\mathfrak{K}_{q,k+1}$ ist in einer affinen Teilgeometrie von $\mathrm{PHG}(R^{k+1})$ *enthalten. Jede Punktklasse dieser affinen Teilgeometrie enthält genau einen Punkt von $\mathfrak{K}_{q,k+1}$. Tabelle 2.4.2 zeigt das Spektrum von $\mathfrak{K}_{q,k+1}$.*

(b) Der Kerdock-Code $\mathcal{K}_{q,k+1}$ ist ein fetter, freier Code vom Rang $k+1$ mit den Parametern

$$\left[q^k, \quad (k+1, k+1), \quad (q-1)(q^k-q^{\frac{k-1}{2}})\right]_R.$$

Tabelle 2.4.3 zeigt den symmetrisierten Gewichtszähler von $\mathcal{K}_{q,k+1}$.

Beweis. Der symmetrisierte Gewichtszähler von $\mathcal{K}_{q,k+1}$ kann aus dem vollständigen Gewichtszähler in [100, Th. 1] abgeleitet werden. Satz 2.3.1(a) liefert das Spektrum von $\mathfrak{K}_{q,k+1}$. Nach Konstruktion sind die Punkte von $\mathfrak{K}_{q,k+1}$ im Bild von $\mathrm{AHG}(R^k)$ unter der Standardeinbettung enthalten. Weil die Elemente der Teichmüller-Menge T ein Vertretersystem des Restklassenkörpers $\mathbb{F}_{q^k}$ von S bilden, liegen keine zwei Punkte in derselben Punktklasse. Damit enthält jede Punktklasse der affinen Teilgeometrie genau einen Punkt der Kerdock-Punktmenge, und der Spann von $\mathfrak{K}_{q,k+1}$ ist die volle Geometrie $\mathrm{PHG}(R^{k+1})$. □

Tabelle 2.4.3.: Symmetrisierter Gewichtszähler des Kerdock-Codes $\mathcal{K}_{q,k+1}$

Typ H_{++}	#Cw.	$\frac{1}{2}(q^k-1)(q^{k+1}+q^{\frac{k+3}{2}})$
	ω_0	q^k-q^{k-1}
	ω_1	$q^{k-1}-q^{k-2}-(q^{\frac{k-1}{2}}-q^{\frac{k-3}{2}})$
	ω_2	$q^{k-2}+(q^{\frac{k-1}{2}}-q^{\frac{k-3}{2}})$
	w_{hom}	$q^{k+1}-q^k-(q^{\frac{k+1}{2}}-q^{\frac{k-1}{2}})$
Typ H_{+}	#Cw.	$\frac{1}{2}(q-1)(q^k-1)(q^{k+1}-q^{\frac{k+3}{2}})$
	ω_0	q^k-q^{k-1}
	ω_1	$q^{k-1}-q^{k-2}-q^{\frac{k-3}{2}}$
	ω_2	$q^{k-2}+q^{\frac{k-3}{2}}$
	w_{hom}	$q^{k+1}-q^k-q^{\frac{k-1}{2}}$
Typ H_0	#Cw.	$q^{k+1}(q-1)$
	ω_0	q^k
	ω_1	0
	ω_2	0
	w_{hom}	$q^{k+1}-q^k$
Typ H_{-}	#Cw.	$\frac{1}{2}(q-1)(q^k-1)(q^{k+1}+q^{\frac{k+3}{2}})$
	ω_0	q^k-q^{k-1}
	ω_1	$q^{k-1}-q^{k-2}+q^{\frac{k-3}{2}}$
	ω_2	$q^{k-2}-q^{\frac{k-3}{2}}$
	w_{hom}	$q^{k+1}-q^k+q^{\frac{k-1}{2}}$
Typ H_{--}	#Cw.	$\frac{1}{2}(q^k-1)(q^{k+1}-q^{\frac{k+3}{2}})$
	ω_0	q^k-q^{k-1}
	ω_1	$q^{k-1}-q^{k-2}+(q^{\frac{k-1}{2}}-q^{\frac{k-3}{2}})$
	ω_2	$q^{k-2}-(q^{\frac{k-1}{2}}-q^{\frac{k-3}{2}})$
	w_{hom}	$q^{k+1}-q^k+(q^{\frac{k+1}{2}}-q^{\frac{k-1}{2}})$
Typ $pH_{\pm}$	#Cw.	$q(q^k-1)$
	ω_0	0
	ω_1	q^k-q^{k-1}
	ω_2	q^{k-1}
	w_{hom}	$q^{k+1}-q^k$
Typ pH_0	#Cw.	$q-1$
	ω_0	0
	ω_1	q^k
	ω_2	0
	w_{hom}	q^{k+1}
Typ 0	#Cw.	1
	ω_0	0
	ω_1	0
	ω_2	q^k
	w_{hom}	0

Tabelle 2.4.4.: Spektrum der Kerdock-Punktmenge $\mathfrak{K}_{k+1}$ über $\mathbb{Z}_4$

Typ	#Hyperebenen	ω_0	ω_1	ω_2
H_+	$2^{2k} - 2^k$	2^{k-1}	$2^{k-2} - 2^{\frac{k-3}{2}}$	$2^{k-2} + 2^{\frac{k-3}{2}}$
H_0	2^k	2^k	0	0
H_-	$2^{2k} - 2^k$	2^{k-1}	$2^{k-2} + 2^{\frac{k-3}{2}}$	$2^{k-2} - 2^{\frac{k-3}{2}}$

Tabelle 2.4.5.: Symmetrisierter Gewichtszähler des $\mathbb{Z}_4$-linearen Kerdock-Codes $\mathcal{K}_{k+1}$

Typ	#Codewörter	ω_0	ω_1	ω_2	w_{Lee}
H_-	$2^{2k+1} - 2^{k+1}$	2^{k-1}	$2^{k-2} - 2^{\frac{k-3}{2}}$	$2^{k-2} + 2^{\frac{k-3}{2}}$	$2^k - 2^{\frac{k-1}{2}}$
H_0	2^{k+1}	2^k	0	0	2^k
H_+	$2^{2k+1} - 2^{k+1}$	2^{k-1}	$2^{k-2} + 2^{\frac{k-3}{2}}$	$2^{k-2} - 2^{\frac{k-3}{2}}$	$2^k + 2^{\frac{k-1}{2}}$
$2H_\pm$	$2^{k+1} - 2$	0	2^{k-1}	2^{k-1}	2^k
$2H_0$	1	0	2^k	0	2^{k+1}
0	1	0	0	2^k	0

Bemerkung 2.4.5 Im Fall $q = 2$ reduziert sich die Anzahl der symmetrisierten Gewichte von $\mathcal{K}_{2,k+1} = \mathcal{K}_{k+1}$ wie auch die Anzahl der Typen im Spektrum von $\mathfrak{K}_{2,k+1}$ gegenüber dem allgemeinen Fall jeweils um zwei. Denn in den beiden Tabellen fallen jeweils die Typen H_+ und H_{++} sowie die Typen H_- und H_{--} zusammen. Außerdem vereinfachen sich die Ausdrücke in den Tabellen deutlich, so dass wir für den Fall $R = \mathbb{Z}_4$ bequemlichkeitshalber das Spektrum nochmals in Tabelle 2.4.4 sowie den symmetrisierten Gewichtszähler nochmals in Tabelle 2.4.5 auflisten.

3. Konstruktionen

3.1. Verallgemeinerte Teichmüller-Codes

In [59, Th. V.7] wurde bewiesen, dass eine Teichmüller-Punktmenge über $R = \mathrm{GR}(4, r)$ in der projektiven Hjelmslev-Geometrie $\mathrm{PHG}(R^k)$ für ungerades k nur zwei Schnittzahlen mit den Hyperebenen zulässt.

Dieses Resultat soll nun verallgemeinert werden. Wir werden durch das Kombinieren mehrerer paarweise disjunkter Teichmüller-Punktmengen zwei neue Serien von Punktmengen in $\mathrm{PHG}(R^k)$ mit zwei Schnittzahlen konstruieren. Die erste Serie $\mathfrak{T}_{q,k,s}$ verallgemeinert die Teichmüller-Punktmengen und erzeugt R-lineare Codes $\mathcal{T}_{q,k,s}$ mit hervorragenden Parametern. In diesen Codes sind die Teichmüller-Codes sowie die Simplex-Codes als Spezialfälle enthalten. Die zweite Serie $\mathfrak{U}_{q,k,s}$ erzeugt R-lineare Codes $\mathcal{U}_{q,k,s}$ mit nur zwei von Null verschiedenen Gewichten.

In [59] wurde der Nachweis der Schnitteigenschaften über ein symmetrisches Translationsschema auf der additiven Gruppe eines Galois-Rings S der Charakteristik 4 geführt. Das dort betrachtete Translationsschema wird von einer bestimmten Obergruppe der Teichmüller-Gruppe T^* von S induziert. In Satz 3.1.5 wird allgemein entschieden, unter welchen Umständen eine T^* umfassende echte Untergruppe von S^* ein symmetrisches Translationsschema auf $(S, +)$ induziert. Der wesentliche Schritt besteht in Lemma 3.1.4, einer Verallgemeinerung von [59, Lemma VI.1]. Der Nachweis dieses Lemmas kann in weiten Teilen wie in [59] geführt werden. Eine Stelle bereitet jedoch zusätzliche Schwierigkeiten. Die hierfür benötigten Aussagen werden in Lemma 3.1.1 und 3.1.2 vorbereitet und erfordern eine Untersuchung von symmetrischen Bilinearformen über $\mathbb{F}_2$.

3.1.1. Unterräume vom Typ I und II

Die in diesem Abschnitt benötigten Definitionen und Grundlagen über symmetrische Bilinearformen in endlichdimensionalen $\mathbb{F}_2$-Vektorräumen finden sich in Anhang A.

Zwei der rang-extremalen Typen von Unterräumen einer Bilinearform $B_{t,t}$ mit $t \in \mathbb{N}$ spielen in den folgenden Untersuchungen eine wichtige Rolle: Ein Unterraum U von $B_{t,t}$ heiße

- vom *Typ I*, falls $\mathrm{Rad}(U) = \{\mathbf{0}\}$, d.h. falls $\mathrm{rk}(U) = \dim(U)$.
  (mit anderen Worten: Die eingeschränkte Bilinearform $B|_{U\times U}$ ist nicht ausgeartet.)

- vom *Typ II*, falls $\mathrm{Rad}(U) = U^\perp$, d.h. falls $\mathrm{rk}(U) = 2\dim(U) - t$.
  (mit anderen Worten: $U^\perp$ besteht nur aus isotropen Vektoren.)

Unterräume vom Typ I existieren für alle Dimensionen $0, \ldots, t$ und Unterräume vom Typ II für die Dimensionen $\lceil t/2 \rceil, \ldots, t$.

Lemma 3.1.1 *Sei V ein t-dimensionaler $\mathbb{F}_2$-Vektorraum mit der Bilinearform $B_{t,t}$. Sei weiter U ein Unterraum von V und $\sigma = \dim(U)$. Für $\mathbf{v} \in V$ bezeichnen wir die Anzahl der Lösungen $(\mathbf{x}, \mathbf{y}) \in (U \setminus \{\mathbf{0}\}) \times U$ der Gleichung $\mathbf{x} \perp (\mathbf{y} + \mathbf{v})$ mit $N_\mathbf{v}$. Die Zahl $N_\mathbf{v}$ ist genau dann für alle $\mathbf{v} \in V \setminus U$ gleich, wenn U vom Typ I oder vom Typ II ist. In diesem Fall gilt*

$$N_\mathbf{v} = \begin{cases} 2^{2\sigma-1} - 2^{\sigma-1} & \text{falls } U \text{ vom Typ I,} \\ 2^{2\sigma-1} - 2^{\sigma} & \text{falls } U \text{ vom Typ II.} \end{cases}$$

Beweis. Sei $B = B_{t,t}$. Wegen $B(\mathbf{x}, \mathbf{y} + \mathbf{v}) = B(\mathbf{x}, \mathbf{y}) + B(\mathbf{x}, \mathbf{v})$ sind die Vektorpaare $(\mathbf{x}, \mathbf{y}) \in (U \setminus \{\mathbf{0}\}) \times U$ zu zählen, für die $B(\mathbf{x}, \mathbf{y}) = B(\mathbf{x}, \mathbf{v})$ ist. Ist $\mathbf{x} \notin \operatorname{Rad}(U)$, so gibt es stets $\#U/2$ Vektoren $\mathbf{y}$ mit $B(\mathbf{x}, \mathbf{y}) = B(\mathbf{x}, \mathbf{v})$. Dies ergibt $(\#U - \#\operatorname{Rad}(U))(\#U/2)$ Lösungspaare mit $\mathbf{x} \notin \operatorname{Rad}(U)$. Ist $\mathbf{x} \in \operatorname{Rad}(U)$, so ist immer $B(\mathbf{x}, \mathbf{y}) = 0$. Für ein Lösungspaar $(\mathbf{x}, \mathbf{y})$ muss also $B(\mathbf{x}, \mathbf{v}) = 0$ gelten, d.h. $\mathbf{x} \in (\operatorname{Rad}(U) \cap \mathbf{v}^\perp) \setminus \{\mathbf{0}\}$. Folglich gibt es $(\#(\operatorname{Rad}(U) \cap \mathbf{v}^\perp) - 1)\#U$ Lösungspaare mit $\mathbf{x} \in \operatorname{Rad}(U)$.

Damit $N_\mathbf{v}$ für alle $\mathbf{v} \in V \setminus U$ gleich ist, muss also für alle $\mathbf{v} \in V \setminus U$ der Unterraum $\operatorname{Rad}(U) \cap \mathbf{v}^\perp$, bzw. dazu äquivalent der Unterraum

$$(\operatorname{Rad}(U) \cap \mathbf{v}^\perp)^\perp = \operatorname{Rad}(U)^\perp + \langle \mathbf{v} \rangle = U + U^\perp + \langle \mathbf{v} \rangle$$

stets dieselbe Dimension haben. Hierfür gibt es zwei Möglichkeiten:

(i) Für alle $\mathbf{v} \in V \setminus U$ ist $\mathbf{v} \in U + U^\perp$. Dies ist äquivalent zu $U + U^\perp = V$, d.h. $\operatorname{Rad}(U) = U \cap U^\perp = \{\mathbf{0}\}$ und weiter U vom Typ I. Mit $\operatorname{rk}(U) = \sigma$ ergibt sich

$$N_\mathbf{v} = (\#U - 1)\frac{\#U}{2} + 0 = 2^{2\sigma-1} - 2^{\sigma-1}.$$

(ii) Für alle $\mathbf{v} \in V \setminus U$ ist $\mathbf{v} \notin U + U^\perp$. Dies ist äquivalent zu $U^\perp \subseteq U$, d.h. $\operatorname{Rad}(U) = U \cap U^\perp = U^\perp$ und weiter U vom Typ II. Mit $\operatorname{rk}(U) = 2\sigma - t$ ergibt sich

$$N_\mathbf{v} = (\#U - \#U^\perp)\frac{\#U}{2} + \#U\left(\frac{\#U^\perp}{2} - 1\right) = 2^{2\sigma-1} - 2^{\sigma}.$$

□

Lemma 3.1.2 *Seien k und r positive ganze Zahlen, $q = 2^r$, $\sigma \in \{0, \ldots, kr\}$ und die Spurform auf dem $\mathbb{F}_2$-Vektorraum $\mathbb{F}_{q^k}$ vorgegeben.*

(a) Der $\mathbb{F}_2$-Vektorraum $\mathbb{F}_{q^k}$ hat genau dann einen $\mathbb{F}_q$ umfassenden Unterraum U der Dimension σ vom Typ I, wenn gilt:

$$\sigma \in \begin{cases} \{r, r+2, r+4, \ldots, kr\} & \text{falls } k \text{ ungerade,} \\ \{2r, 2r+2, 2r+4, \ldots, kr\} & \text{falls } k \text{ gerade.} \end{cases}$$

(b) Der $\mathbb{F}_2$-Vektorraum $\mathbb{F}_{q^k}$ hat genau dann einen $\mathbb{F}_q$ umfassenden Unterraum U der Dimension σ vom Typ II, wenn gilt:

$$\sigma \in \left\{ \left\lceil \frac{k}{2} \right\rceil r,\ \left\lceil \frac{k}{2} \right\rceil r + 1,\ \ldots,\ kr \right\}.$$

Beweis. Ist $f = \mathrm{Tr}_{\mathbb{F}_2}$ die Spur auf $\mathbb{F}_{q^k}$ sowie $g = \mathrm{Tr}_{\mathbb{F}_2}$ die Spur auf $\mathbb{F}_q$, so gilt wegen $(2^r)^i \equiv 1 \pmod{2^r - 1}$ für alle $x \in \mathbb{F}_q$

$$f(x) = \sum_{i=0}^{kr-1} x^{2^i} = \sum_{i=0}^{k-1} \sum_{j=0}^{r-1} x^{2^{ri+j}} = \sum_{i=0}^{k-1} \sum_{j=0}^{r-1} (x^{(2^r)^i})^{2^j} = \sum_{i=0}^{k-1} \sum_{j=0}^{r-1} x^{2^j} = k \cdot g(x).$$

Daraus folgt

$$\mathrm{rk}(\mathbb{F}_q) = \begin{cases} 0 & \text{falls } k \text{ gerade,} \\ r & \text{falls } k \text{ ungerade.} \end{cases}$$

Die Bedingung $U \geq \mathbb{F}_q$ ist äquivalent zu $U^\perp \leq \mathbb{F}_q^\perp$. Wegen $1 \in \mathbb{F}_q$ ist $\mathbb{F}_q^\perp$ alternierend. Mit der obigen Rangaussage ist $\mathbb{F}_q^\perp$ also vom Typ $A_{(k-1)r,(k-1)r}$ für k ungerade bzw. $A_{(k-1)r,(k-2)r}$ für k gerade.

Im Fall von Typ I ist $U^\perp$ wegen $1 \in U$ vom Typ $A_{(kr-\sigma,kr-\sigma)}$. Ein solcher Unterraum von $\mathbb{F}_q^\perp$ existiert für ungerades k genau dann, wenn $\sigma \geq r$ und $kr - \sigma$ gerade ist (also $\sigma - r$ gerade); und für gerades k genau dann, wenn $\sigma \geq 2r$ und σ gerade ist.

Im Fall von Typ II ist $U^\perp$ wegen $1 \in U$ vom Typ $A_{(kr-\sigma,0)}$. Ein solcher Unterraum von $\mathbb{F}_q^\perp$ existiert für ungerades k genau dann, wenn $\frac{1}{2}(k-1)r \geq kr - \sigma$, d.h. $\sigma \geq r(k+1)/2$; und für gerades k genau dann, wenn $(k-2)r - 2(\sigma - r) \leq 0$, d.h. $\sigma \geq kr/2$. □

3.1.2. Symmetrische Translationsschemata auf $(\mathrm{GR}(4,t),+)$

Die im Folgenden benötigten Grundlagen zur Theorie der Assoziationsschemata finden sich in Anhang B.

In diesem Abschnitt sei t eine positive ganze Zahl, $S = \mathrm{GR}(4,t)$ ein Galois-Ring der Charakteristik 4 und T^* die Teichmüller-Gruppe von S. Zu einer Untergruppe $\Sigma \leq S^*$ sei $\bar{\Sigma} = S^* \setminus \Sigma$. Im Fall $\Sigma \neq S^*$ definieren wir die Partition

$$\mathcal{A}_\Sigma = \{\{0\}, 2S \setminus \{0\}, \Sigma, \bar{\Sigma}\}$$

von S. Wir wollen allgemein die Frage beantworten, unter welchen Umständen $\mathcal{A}_\Sigma$ für $T^* \leq \Sigma < S^*$ ein symmetrisches Translationsschema auf $(S,+)$ ist. Um der Anforderung $-\Sigma = \Sigma$ zu genügen, muss hierfür sicher $-1 \in \Sigma$ gelten.

Bezeichnet $H = 1 + 2S$ die Haupteinheiten von S (siehe S. 11), so gilt $S^* = T^* \cdot H \cong T^* \times H$. Nach Fakt 2.1.3 ist H eine elementarabelsche Gruppe der Form $\mathbb{Z}_2^t$. Folglich gibt es eine Bijektion zwischen den T^* umfassenden Untergruppen Σ von S^* und den $\mathbb{F}_2$-Untervektorräumen von H. Zur Angabe einer expliziten Bijektion identifizieren wir weiterhin S mit dem Ring der gestutzten Witt-Vektoren $W_2(\mathbb{F}_{2^t})$, siehe Abschnitt 2.1.3.

Die Abbildung $\rho : (\mathbb{F}_{2^t}, +) \to (H, \cdot)$, $x \mapsto (1, x)$ ist dann ein Gruppenhomomorphismus, und jede T^* umfassende Untergruppe Σ hat die Form $\Sigma_U = T^* \cdot \rho(U) \cong T^* \times \rho(U)$, wobei U ein Untervektorraum des $\mathbb{F}_2$-Vektorraums $\mathbb{F}_{2^t}$ ist. Weil sich -1 in den gestutzten Witt-Vektoren als $(1, 1)$ schreibt, übersetzt sich die Bedingung $-1 \in \Sigma_U$ in $\mathbb{F}_2 \subseteq U$. Es gilt $\#\Sigma_U = \#U \cdot \#T^* = 2^\sigma \cdot (2^t - 1)$ mit $\sigma = \dim_{\mathbb{F}_2}(U)$.

Lemma 3.1.3 *Sei U ein Untervektorraum des $\mathbb{F}_2$-Vektorraums $\mathbb{F}_{2^t}$. Es gilt*

$$\Sigma_U = \{(\gamma_0, \gamma_1) \in W_2(\mathbb{F}_{2^t}) \mid \gamma_0 \in \mathbb{F}_{2^t}^*, \gamma_1 \in \mathbb{F}_{2^t}, \gamma_1/\gamma_0^2 \in U\}.$$

Beweis. Wegen $\Sigma_U = T^* \cdot \rho(U)$ haben die Elemente von Σ_U die Form $(\alpha, 0) \cdot (1, u) = (\alpha, u\alpha^2)$ mit $u \in U$ und $\alpha \in \mathbb{F}_{2^t}^*$. □

Im Folgenden betrachten wir den $\mathbb{F}_2$-Vektorraum $\mathbb{F}_{2^t}$ zusammen mit der Spurform $B : (x, y) \mapsto \mathrm{Tr}_{\mathbb{F}_2}(xy)$.

Lemma 3.1.4 *Sei U ein echter Untervektorraum des $\mathbb{F}_2$-Vektorraums $\mathbb{F}_{2^t}$ mit $\mathbb{F}_2 \subseteq U$ und sei $\sigma = \dim(U)$. Sei weiter für alle $\gamma \in S$ die Lösungsanzahl*

$$n_\gamma = \#\{(A, B) \in \Sigma_U \times \Sigma_U \mid A + B = \gamma\}$$

definiert. Die Zahl n_γ ist genau dann nur vom Partitionsteil $P \in \mathcal{A}_{\Sigma_U}$ mit $\gamma \in P$ abhängig, wenn einer der folgenden beiden Fälle eintritt:

(i) U ist vom Typ I. In diesem Fall gilt

$$n_\gamma = \begin{cases} 2^\sigma(2^t - 1) & \text{falls } \gamma = 0, \\ 2^\sigma(2^\sigma - 1) & \text{falls } \gamma \in 2S \setminus \{0\}, \\ 2^\sigma(2^\sigma - 2) & \text{falls } \gamma \in \Sigma_U, \\ 2^{2\sigma} & \text{falls } \gamma \in \bar{\Sigma}_U. \end{cases}$$

(ii) U ist vom Typ II. In diesem Fall gilt

$$n_\gamma = \begin{cases} 2^\sigma(2^t - 1) & \text{falls } \gamma = 0, \\ 2^\sigma(2^\sigma - 1) & \text{falls } \gamma \in 2S \setminus \{0\}, \\ 2^\sigma(2^\sigma + 2^{t-\sigma} - 3) & \text{falls } \gamma \in \Sigma_U, \\ 2^\sigma(2^\sigma - 1) & \text{falls } \gamma \in \bar{\Sigma}_U. \end{cases}$$

Mit der Vorarbeit von Lemma 3.1.1 kann der Beweis nun ähnlich wie in [59, Lemma VI.1] geführt werden.

Beweis. Wir schreiben γ als den gestutzten Witt-Vektor (γ_0, γ_1) und $A = (\alpha, a')$, $B = (\beta, b')$. Mit der Arithmetik der gestutzten Witt-Vektoren über einem Grundkörper der Charakteristik 2 ist die Anzahl der Lösungen des Gleichungssystems

$$\alpha + \beta = \gamma_0 \qquad\qquad a' + b' + \alpha\beta = \gamma_1$$

mit $(\alpha, a'), (\beta, b') \in \Sigma_U$ zu bestimmen. Mit der Substitution $a' = \alpha^2 a$ und $b' = \beta^2 b$ ist dies äquivalent zu

$$\alpha + \beta = \gamma_0 \tag{3.1}$$
$$\alpha^2 a + \beta^2 b + \alpha\beta = \gamma_1 \tag{3.2}$$

mit $\alpha, \beta \in \mathbb{F}_{2^t}^*$ und $a, b \in U$.

Im Fall $\gamma_0 = 0$ (d.h. $\gamma \in 2S$) können wir weiter umformen zu

$$\alpha = \beta \qquad \text{und} \qquad \alpha^2(a + b + 1) = \gamma_1.$$

Für $\gamma_1 = 0$ (d.h. $\gamma = 0$) muss wegen $\alpha \neq 0$ die Gleichheit $a + b + 1 = 0$ gelten. D.h. α kann beliebig in $\mathbb{F}_{2^t}^*$ und a beliebig in U gewählt werden, und $\beta = \alpha$ und $b = 1 + a$ sind dann eindeutig festgelegt. Wegen $1 \in U$ ist $b \in U$. Für $\gamma = 0$ ergeben sich also $(\#\mathbb{F}_{2^t}^*) \cdot \#U = (2^t - 1) \cdot 2^\sigma$ Lösungen. Ist $\gamma_1 \neq 0$ (d.h. $\gamma \in 2S \setminus \{0\}$), so durchläuft γ_1/α^2 mit α ganz $\mathbb{F}_{2^t}^*$, d.h. für genau $\#U - 1$ Werte von α ist $\gamma_1/\alpha^2 \in U$. Für diese α kann nun $a \in U$ beliebig gewählt werden, und $b = \gamma_1/\alpha^2 + a + 1 \in U$ ist dann festgelegt. Folglich gibt es für $\gamma \in 2S \setminus \{0\}$ genau $(\#U - 1)\#U = 2^\sigma(2^\sigma - 1)$ Lösungen.

Sei nun also $\gamma_0 \neq 0$ (d.h. $\gamma \in S^*$). Gleichung (3.1) ist äquivalent zu $\beta = \gamma_0 + \alpha$, und die Bedingung $\alpha, \beta \neq 0$ ist äquivalent zu $\alpha \in \mathbb{F}_{2^t} \setminus \{0, \gamma_0\}$. Einsetzen in Gleichung (3.2) liefert

$$\alpha^2(a + b + 1) + \alpha\gamma_0 + \gamma_0^2 b = \gamma_1.$$

Die Substitution $\alpha' = \alpha/\gamma_0$ und $u = a + b + 1$ liefert

$$u(\alpha')^2 + \alpha' = \gamma_1/\gamma_0^2 + b, \tag{3.3}$$

und die Bedingung $\alpha \in \mathbb{F}_{2^t} \setminus \{0, \gamma_0\}$ übersetzt sich in $\alpha' \in \mathbb{F}_{2^t} \setminus \mathbb{F}_2$. Folglich ist n_γ die Anzahl der Lösungen $(\alpha', u, b) \in (\mathbb{F}_{2^t} \setminus \mathbb{F}_2) \times U \times U$ der Gleichung (3.3). Wir unterscheiden zwei Fälle:

Ist $u = 0$, so hat die Gleichung (3.3) $\#U - 2$ Lösungen falls $\gamma \in \Sigma_U$ (denn hier ist nach Lemma 3.1.3 $\gamma_1/\gamma_0^2 \in U$ und demnach müssen die Fälle $\alpha' = \gamma_1/\gamma_0^2 + b \in \{0, 1\}$ ausgeschlossen werden) und $\#U$ Lösungen falls $\gamma \in \bar{\Sigma}_U$.

Sei also $u \neq 0$. Zunächst überlegen wir uns die Anzahl der „verbotenen" Lösungen mit $\alpha' \in \mathbb{F}_2$. Mit $(\alpha')^2 = \alpha'$ vereinfacht sich Gleichung (3.3) zu

$$(u + 1)\alpha' - b = \gamma_1/\gamma_0^2.$$

Die linke Seite liegt in U, und die rechte Seite liegt nach Lemma 3.1.3 genau dann in U, wenn $\gamma \in \Sigma_U$ ist. D.h. für $\gamma \in \bar{\Sigma}_U$ gibt es keine verbotene Lösung. Für $\gamma \in \Sigma_U$ gibt es die verbotenen Lösungen $\alpha' = 0$, $u \in U \setminus \{0\}$, $b = \gamma_1/\gamma_0^2$ und $\alpha' = 1$, $u \in U \setminus \{0\}$, $b = u + 1 + \gamma_1/\gamma_0^2$, insgesamt also $2(\#U - 1)$ Stück.

Wir multiplizieren nun Gleichung (3.3) mit u und gelangen zu

$$(u\alpha')^2 + u\alpha' = u(\gamma_1/\gamma_0^2 + b). \tag{3.4}$$

Die Abbildung $f : \mathbb{F}_{2^t} \to \mathbb{F}_{2^t}, x \mapsto x^2+x$ ist ein Homomorphismus von $\mathbb{F}_2$-Vektorräumen. Es gilt $\mathrm{im}(f) = V_0$, wobei $V_0 = \{x \in \mathbb{F}_{2^t} \mid \mathrm{Tr}_{\mathbb{F}_2}(x) = 0\}$ die Menge aller isotropen Vektoren in $\mathbb{F}_{2^t}$ bezeichnet.[31] Wegen $\mathrm{codim}_{\mathbb{F}_{2^t}}(V_0) = 1$ hat also jedes Element in V_0 zwei Urbilder unter f, und die Elemente außerhalb von V_0 haben kein Urbild.

Ist $\gamma \in \Sigma_U$, so durchläuft $v = \gamma_1/\gamma_0^2 + b$ mit b ganz U. Es gilt $uv \in V_0$ genau dann, wenn $B(u, v) = 0$ ist. Dies ist wegen $u \neq 0$ genau

$$(\#\operatorname{Rad}(U) - 1)\#U + (\#U - \#\operatorname{Rad}(U))(\#U/2) = 1/2\#U(\#U + \#\operatorname{Rad}(U) - 2)$$

mal der Fall. Jede dieser Möglichkeiten für u und b lässt sich mit genau 2 Werten von $\alpha' \in \mathbb{F}_{2^t}$ zu einer Lösung von Gleichung (3.4) ergänzen. Dabei wurden allerdings die verbotenen Lösungen mit $\alpha' \in \{0, 1\}$ mitgezählt. Abziehen dieser $2(\#U - 1)$ Lösungen und Zusammenfassen mit der Lösungsanzahl $\#U - 2$ für $u = 0$ liefert nun

$$n_\gamma = \#U(\#U + \#\operatorname{Rad}(U) - 3) = \begin{cases} 2^\sigma(2^\sigma - 2) & \text{falls } \mathrm{rk}(U) = \sigma, \\ 2^\sigma(2^\sigma + 2^{t-\sigma} - 3) & \text{falls } \mathrm{rk}(U) = 2\sigma - t. \end{cases}$$

Ist $\gamma \notin \Sigma_U$, so gibt uns Lemma 3.1.1 Auskunft über die Anzahl der $u \in U \setminus \{0\}$, $b \in U$ mit $B(u, b + \gamma_1/\gamma_0^2) = 0$. Damit erhalten wir, dass n_γ nur für Unterräume U vom Typ I oder II für alle $\gamma \in \Sigma_U$ identisch ist. In diesem Fall gilt

$$\begin{aligned} n_\gamma &= \begin{cases} 2 \cdot (2^{2\sigma-1} - 2^{\sigma-1}) + 2^\sigma & \text{falls } \mathrm{rk}(U) = \sigma, \\ 2 \cdot (2^{2\sigma-1} - 2^\sigma) + 2^\sigma & \text{falls } \mathrm{rk}(U) = 2\sigma - t \end{cases} \\ &= \begin{cases} 2^{2\sigma} & \text{falls } \mathrm{rk}(U) = \sigma, \\ 2^\sigma(2^\sigma - 1) & \text{falls } \mathrm{rk}(U) = 2\sigma - t. \end{cases} \end{aligned}$$

□

Satz 3.1.5 *Sei U ein echter Untervektorraum des $\mathbb{F}_2$-Vektorraums $\mathbb{F}_{2^t}$ und sei $\sigma = \dim(U)$. Die Partition $\mathcal{A}_{\Sigma_U}$ ist genau dann ein symmetrisches Translationsschema auf $(S, +)$ mit 3 Klassen, wenn U vom Typ I oder II ist und $\mathbb{F}_2$ enthält.*

Beweis. Damit $\mathcal{A}_{\Sigma_U}$ ein symmetrisches Translationsschema ist, müssen die Klassen abgeschlossen unter Negation sein. Dies ist äquivalent zu $\mathbb{F}_2 \subseteq U$. Weiter darf die Lösungsanzahl n_γ aus Lemma 3.1.4 nur vom Partitionsteil $P \in \mathcal{A}_{\Sigma_U}$ mit $\gamma \in P$ abhängen. Aufgrund von Lemma 3.1.4 ist U also vom Typ I oder vom Typ II.

Dass unter dieser Bedingung $\mathcal{A}_{\Sigma_U}$ tatsächlich ein symmetrisches Translationsschema ist, lässt sich völlig analog zum Beweis von [59, Th. V.7] zeigen. □

[31] $\{0\} \to V_0 \xrightarrow{\iota} \mathbb{F}_{2^t} \xrightarrow{f} \mathbb{F}_{2^t} \xrightarrow{\mathrm{Tr}} \mathbb{F}_2 \to \{0\}$ ist eine exakte Sequenz.

Bemerkung 3.1.6

(a) Als Spezialfall $q = 2$ von Lemma 3.1.2 erhalten wir die folgenden notwendigen und hinreichenden Bedingungen für die Existenz eines passenden U:

- Für Typ I:
$$\sigma \in \begin{cases} \{1, 3, \ldots, t-2\} & \text{falls } t \text{ ungerade} \\ \{2, 4, \ldots, t-2\} & \text{falls } t \text{ gerade} \end{cases}$$
- Für Typ II:
$$\sigma \in \left\{ \left\lceil \frac{t}{2} \right\rceil, \left\lceil \frac{t}{2} \right\rceil + 1, \ \ldots, \ t-1 \right\}$$

(b) Die Translationsschemata vom Typ II sind bereits bekannt: Man erhält sie als Fusionsschemata der amorphen symmetrischen Translationsschemata in [76, Th. 9], siehe hierzu auch [105, S. 84].

(c) Für Typ II ist n_γ für alle $\gamma \in S \setminus (\Sigma_U \cup \{0\})$ gleich. Wegen $-\Sigma_U = \Sigma_U$ ist also Σ_U eine partielle Differenzenmenge in $(S, +)$. Damit sind die Mengen Σ_U vom Typ II in den in [74] beschriebenen partiellen Differenzenmengen enthalten.[32]

(d) Translationsschemata vom Typ I mit $\sigma \in \{1, 2\}$ wurden bereits in [105, Th. 13 u. 14] angegeben. Aus [59, Th. V.7] erhält man Translationsschemata vom Typ I mit $\sigma \mid t$ und t/σ ungerade, indem man die dortigen Bezeichner r und k auf σ und t/σ setzt. Die restlichen Fälle vom Typ I scheinen bisher nicht bekannt gewesen zu sein. Das kleinste neue Beispiel ist demnach das durch $t = 5$ und $\sigma = 3$ gegebene Translationsschema auf der Gruppe $(\mathbb{Z}_4^5, +)$ der Ordnung 1024.

3.1.3. Punktmengen in $\mathrm{PHG}(R^k)$ mit zwei Schnittzahlen

Im Folgenden seien $r \geq 1$ und $k \geq 2$ ganze Zahlen, $t = rk$, $R = \mathrm{GR}(4, r)$, $S = \mathrm{GR}(4, rk)$ und $q = 2^r$. Für einen Unterraum U des $\mathbb{F}_2$-Vektorraums $\mathbb{F}_{q^k}$ wollen wir die Gruppe Σ_U als Punktmenge in $\mathrm{PHG}(S_R)$ auffassen. Hierzu muss Σ_U projektiv abgeschlossen über R sein, d.h. für jedes $x \in \Sigma_U$ gilt $R^* x \subseteq \Sigma_U$. Mit der Gruppenstruktur bedeutet dies gerade, dass Σ_U die Einheitengruppe R^* umfasst. Nach Lemma 3.1.3 ist das genau dann der Fall, wenn für alle $\gamma_0 \in \mathbb{F}_q^*$ und $\gamma_1 \in \mathbb{F}_q$ das Element γ_1/γ_0^2 in U liegt, d.h. genau dann, wenn U den Körper $\mathbb{F}_q$ enthält. In diesem Fall bezeichnen wir die von Σ_U in $\mathrm{PHG}(S_R)$ induzierte Punktmenge mit

$$\mathrm{pts}(\Sigma_U) = \{Rx \mid x \in \Sigma_U\}.$$

Für die Dimension $\sigma = \dim_{\mathbb{F}_2}(U)$ gilt $\sigma \geq r$. Im Folgenden soll anstelle von σ die Kodimension $s = \dim_{\mathbb{F}_2}(U) - r \in \{0, \ldots, (k-1)r\}$ von $\mathbb{F}_q$ in U benutzt werden.

[32] In der Notation von [74] ist $s(2, t) = \lceil t/2 \rceil$ (folgt aus [74, Lemma 5.2]), und damit ergeben sich für $p = 2$ partielle Differenzenmengen mit den Parametern $(v, k, \lambda, \mu) = (p^{2t}, r(p^t - 1), p^t + r^2 - 3r, r^2 - r)$ aus $r \in \{2^{\lceil t/2 \rceil}, 2 \cdot 2^{\lceil t/2 \rceil}, 3 \cdot 2^{\lceil t/2 \rceil}, \ldots, 2^t\}$ Nebenklassen der Teichmüller-Gruppe.

Lemma 3.1.7 *Sei U ein $\mathbb{F}_q$ umfassender Unterraum des $\mathbb{F}_2$-Vektorraums $\mathbb{F}_{q^k}$, und sei $s = \dim(U) - r$. Es gilt*

$$\#\operatorname{pts}(\Sigma_U) = 2^s \cdot \frac{q^k - 1}{q - 1},$$

und in jeder Punktklasse von $\mathrm{PHG}(S_R)$ liegen 2^s Punkte von $\operatorname{pts}(\Sigma_U)$. Insbesondere spannt $\operatorname{pts}(\Sigma_U)$ die gesamte Geometrie $\mathrm{PHG}(S_R)$ auf. Die Gruppe $G = \Sigma_U/R^*$ induziert durch $g \cdot Rx = R(gx)$ eine Kollineationsgruppe auf $\mathrm{PHG}(S_R)$. G operiert transitiv auf der Menge der Punktklassen und auf der Menge der Hyperebenenklassen und scharf transitiv auf $\operatorname{pts}(\Sigma_U)$.

Beweis. Es ist $\#\operatorname{pts}(\Sigma_U) = \#\Sigma_U/(\#R^*) = 2^{\dim(U)}(q^k-1)/(q(q-1)) = 2^s(q^k-1)/(q-1)$. Für jedes Element $g \in S^*$ ist $S \to S, x \mapsto gx$ eine R-lineare Bijektion. Folglich ist $\mathrm{PHG}(S_R) \to \mathrm{PHG}(S_R)$, $Rx \mapsto R(gx)$ eine Kollineation. Daraus folgen die Aussagen über G, die Transitivität auf der Menge der Punkt- bzw. Hyperebenenklassen erhält man mit $T^* \leq \Sigma_U$. Insbesondere enthält jede der $\frac{q^k-1}{q-1}$ Punktklassen von $\mathrm{PHG}(S_R)$ gleichviele Elemente von $\operatorname{pts}(\Sigma_U)$, nämlich 2^s Stück. □

Sei wieder U ein $\mathbb{F}_q$ umfassender Untervektorraum des $\mathbb{F}_2$-Vektorraums $\mathbb{F}_{q^k}$ und $s = \dim(U) - r$. Wir bezeichnen $\operatorname{pts}(\Sigma_U)$ mit $\mathfrak{T}_{q,k,s}$, falls U vom Typ I ist, und mit $\mathfrak{U}_{q,k,s}$, falls U vom Typ II ist. Aufgrund der Isomorphie $S_R \cong R_R^k$ dürfen wir im Folgenden $\mathfrak{T}_{q,k,s}$ und $\mathfrak{U}_{q,k,s}$ als Punktmengen in $\mathrm{PHG}(R^k)$ auffassen. Sei weiter $\mathcal{T}_{q,k,s} = \operatorname{cde}(\mathfrak{T}_{q,k,s})$ und $\mathcal{U}_{q,k,s} = \operatorname{cde}(\mathfrak{U}_{q,k,s})$. Im Fall $s = 0$ gibt es für U nur die einzige Möglichkeit $U = \mathbb{F}_q$ und für $s = (k-1)r$ nur die Möglichkeit $U = \mathbb{F}_{q^k}$. Im Allgemeinen gibt es zu vorgegebenen Parametern q, k und s jedoch mehrere Möglichkeiten für die Wahl eines passenden Unterraums U, und die davon erzeugten Punktmengen bzw. Codes sind im Allgemeinen nicht alle isomorph, vgl. Beispiele 3.1.16 und 3.1.17. Die Symbole $\mathfrak{T}_{q,k,s}$, $\mathfrak{U}_{q,k,s}$, $\mathcal{T}_{q,k,s}$ und $\mathcal{U}_{q,k,s}$ sind also als Bezeichner für eine beliebige auf die oben beschriebene Weise erzeugte Punktmenge bzw. für einen beliebigen solchen Code zu verstehen.

Satz 3.1.8 *Es seien $r \geq 1$ und $k \geq 2$ ganze Zahlen und $q = 2^r$.*

(a) Es sei

$$s \in \begin{cases} \{0, 2, 4, \ldots, (k-1)r\} & \text{falls } k \text{ ungerade,} \\ \{r, r+2, r+4, \ldots, (k-1)r\} & \text{falls } k \text{ gerade.} \end{cases}$$

Die Punktmenge $\mathfrak{T}_{q,k,s}$ spannt die gesamte Geometrie $\mathrm{PHG}(R^k)$ auf. Im Fall $s \neq (k-1)r$ treten genau zwei verschiedene Schnittzahlen mit den Hyperebenen von $\mathrm{PHG}(R^k)$ auf. Das Spektrum ist in Tabelle 3.1.1 angegeben.

(b) Es sei

$$s \in \left\{ \left\lfloor \frac{k-1}{2} \right\rfloor r,\ \left\lfloor \frac{k-1}{2} \right\rfloor r + 1,\ \ldots,\ (k-1)r \right\}.$$

Die Punktmenge $\mathfrak{U}_{q,k,s}$ spannt die gesamte Geometrie $\mathrm{PHG}(R^k)$ auf. Im Fall $s \neq (k-1)r$ treten genau zwei verschiedene Schnittzahlen mit den Hyperebenen von $\mathrm{PHG}(R^k)$ auf. Das Spektrum ist in Tabelle 3.1.2 angegeben.

Tabelle 3.1.1.: Spektrum der Punktmenge $\mathfrak{T}_{q,k,s}$

Typ	#Hyperebenen	ω_0	ω_1	ω_2
H_-	$\frac{1}{2}\frac{q^k-1}{q-1}\left(q^{k-1}-2^{s/2}q^{\frac{k-1}{2}}\right)$	$2^s q^{k-1}$	$2^s q^{k-2}+2^{s/2}q^{\frac{k-3}{2}}$	$2^s\frac{q^{k-2}-1}{q-1}-2^{s/2}q^{\frac{k-3}{2}}$
H_+	$\frac{1}{2}\frac{q^k-1}{q-1}\left(q^{k-1}+2^{s/2}q^{\frac{k-1}{2}}\right)$	$2^s q^{k-1}$	$2^s q^{k-2}-2^{s/2}q^{\frac{k-3}{2}}$	$2^s\frac{q^{k-2}-1}{q-1}+2^{s/2}q^{\frac{k-3}{2}}$

Tabelle 3.1.2.: Spektrum der Punktmenge $\mathfrak{U}_{q,k,s}$

Typ	#Hyperebenen	ω_0	ω_1	ω_2
H_-	$\frac{q^k-1}{q-1}(q^{k-1}-2^s)$	$2^s q^{k-1}$	$2^s q^{k-2}$	$2^s\frac{q^{k-2}-1}{q-1}$
H_+	$\frac{q^k-1}{q-1}2^s$	$2^s q^{k-1}$	$(2^s-1)q^{k-2}$	$2^s\frac{q^{k-2}-1}{q-1}+q^{k-2}$

Beweis. Im Fall $s=(k-1)r$ ist $\mathfrak{T}_{q,k,s}=\mathfrak{U}_{q,k,s}$ die komplette Punktmenge von $\mathrm{PHG}(R^k)$ mit nur einer Schnittzahl mit den Hyperebenen, deren Spektrum in Abschnitt 2.4.1 berechnet wurde. Sei im Folgenden also $s\neq(k-1)r$. Wir halten uns bei der Berechnung der Schnittzahlen eng an die Vorgehensweise in [59, Th. V.7(ii)].

Für Typ I ist die Aussage von Lemma 3.1.4(i) äquivalent zur Gleichung

$$\chi_{\Sigma_U}^2=2^\sigma(2^\sigma-2)\chi_{\Sigma_U}+2^{2\sigma}\chi_{\bar{\Sigma}_U}+2^\sigma(2^\sigma-1)\chi_{2S\setminus\{0\}}+2^\sigma(2^t-1)\chi_{\{0\}} \tag{3.5}$$

in der Gruppenalgebra $\mathbb{C}[(S,+)]$. Sei $\psi: S\to\mathbb{C}^*$ ein auf $2S$ nichttrivialer Charakter von $(S,+)$. Für eine Teilmenge $M\subseteq S$ benutzen wir die Schreibweise $\psi(M)=\sum_{x\in M}\psi(x)$. Es gilt $\psi(S)=0$ und $\psi(2S)=0$. Daraus folgt $\psi(\bar{\Sigma}_U)=-\psi(\Sigma_U)$ und $\psi(2S\setminus\{0\})=-1$. Anwenden von ψ auf Gleichung (3.5) liefert

$$\psi(\Sigma_U)^2=2^\sigma(2^\sigma-2)\psi(\Sigma_U)-2^{2\sigma}\psi(\Sigma_U)-2^\sigma(2^\sigma-1)+2^\sigma(2^t-1).$$

Auflösen nach $\psi(\Sigma_U)$ ergibt

$$\psi(\Sigma_U)=-2^\sigma\pm2^{\frac{\sigma+t}{2}}.$$

Nach [59, Lemma V.4] treten zwischen $\mathfrak{T}_{q,k,s}$ und den Hyperebenen von $\mathrm{PHG}(R^k)$ somit nur die beiden Schnittzahlen

$$s_\pm=\#(\mathfrak{T}_{q,k,s}\cap H)=\frac{1}{q^2}\left(\psi(\Sigma_U)+2^s\frac{q^k-q}{q-1}\right)=2^s\frac{q^{k-2}-1}{q-1}\pm2^{s/2}\cdot q^{(k-3)/2}.$$

auf. Wir bezeichnen die Anzahl der Hyperebenen mit Schnittzahl s_- bzw. s_+ mit n_- bzw. n_+. Es gilt

$$\begin{aligned}n_-+n_+&=\#\text{Hyperebenen in }\mathrm{PHG}(R^k),\\ n_-s_-+n_+s_+&=\#\mathfrak{T}_{q,k,s}\cdot\#\text{Hyperebenen durch einen Punkt von }\mathrm{PHG}(R^k),\end{aligned}$$

wobei die zweite Gleichung durch doppeltes Abzählen der Menge

$$\{(x,H)\mid x\in\mathfrak{T}_{q,k,s},\ H\text{ Hyperebene in }\mathrm{PHG}(R^k),\ x\in H\}$$

entsteht. Mit Hilfe der Formeln aus Abschnitt 2.3.3 bestimmt man aus diesen beiden Gleichungen die Zahlen n_- und n_+. Weil nach Lemma 3.1.7 jede Punktklasse von $\mathrm{PHG}(R^k)$ gleich viele Punkte von $\mathfrak{T}_{q,k,s}$ enthält, lassen sich die noch fehlenden Werte des Spektrums von $\mathfrak{T}_{q,k,s}$ nun problemlos aus den Zahlen s_+ und s_- berechnen.

Für Typ II berechnet man das Spektrum von $\mathfrak{U}_{q,k,s}$ auf die gleiche Art. Die dabei auftretenden Zwischenergebnisse sind

$$\begin{aligned}\chi^2_{\Sigma_U} &= 2^\sigma(2^\sigma + 2^{t-\sigma} - 3)\chi_{\Sigma_U} + 2^\sigma(2^\sigma - 1)\chi_{\bar{\Sigma}_U} + 2^\sigma(2^\sigma - 1)\chi_{2S\setminus\{0\}} + 2^\sigma(2^t - 1)\chi_{\{0\}},\\ \psi(\Sigma_U) &= -2^\sigma + \frac{1 \pm 1}{2}2^t \quad \text{und}\\ s_\pm &= 2^s\frac{q^{k-2} - 1}{q - 1} + \frac{1 \pm 1}{2}q^{k-2}.\end{aligned}$$

□

Bemerkung 3.1.9

(a) Die Punktmengen $\mathfrak{T}_{q,k,s}$ und $\mathfrak{U}_{q,k,s}$ enthalten etliche bereits bekannte Punktmengen als Spezialfälle: Für ungerades k ist $\mathfrak{T}_{q,k,0} = \mathfrak{T}_{q,k}$ die Teichmüller-Punktmenge. In verschiedenen Situationen wurden Punktmengen betrachtet, bei denen jede Punktklasse ein Hyperebenen-Segment (d.h. im ebenen Fall $k = 3$ ein Geradensegment) enthält, so dass deren Richtungen jede Hyperebenenklasse in $\mathrm{PHG}(R^k)$ genau einmal treffen. Solche Punktmengen können als $\mathfrak{U}_{q,k,r(k-2)}$ realisiert werden. Weiter ist $\mathfrak{T}_{4,3,2}$ der maximale $(84, 6)$-Arc in der projektiven Hjelmslev-Ebene über $\mathrm{GR}(4, 2)$ aus [85]. Die Punktmenge $\mathfrak{T}_{q,k,r(k-1)} = \mathfrak{U}_{q,k,r(k-1)}$ besteht aus allen Punkten von $\mathrm{PHG}(R^k)$.

(b) Die Punktmengen $\mathfrak{T}_{q,k,s}$ haben sehr gute Parameter als Arcs. Die bereits erwähnten Hyperovale und der $(84, 6)$-Arc in $\mathrm{PHG}(\mathrm{GR}(4, 2)^3)$ sind Arcs von maximal möglicher Größe. Für $k = 4$ und $s = r$ ergibt sich ein $(q^4 + q^3 + q^2 + q,\ q^2 + 2q)$-Arc im projektiven Hjelmslev-Raum über $\mathrm{GR}(4, r)$, im kleinsten Fall $q = 2$ ist das ein $(30, 8)$-Arc in $\mathrm{PHG}(\mathbb{Z}_4^4)$. Dieser Arc hat maximal mögliche Größe, denn in [7] finden sich die Schranken $23 - 30$. Ein $(30, 8)$-Arc ließe sich auch in der Form $\mathrm{pts}(\mathcal{C})$ konstruieren, wobei $\mathcal{C}$ eine doppelte Verkürzung des Kerdock-Codes $\mathcal{K}_{2,3+1}$ oder der Code aus [3, Ex. 4] ist.

Satz 3.1.10 *Seien $r \geq 1$ und $k \geq 2$ ganze Zahlen, $q = 2^r$ und*

$$s \in \begin{cases}\{0, 2, 4, \ldots, (k-1)r\} & \text{falls } k \text{ ungerade,}\\ \{r, r+2, r+4, \ldots, (k-1)r\} & \text{falls } k \text{ gerade.}\end{cases}$$

Der Code $\mathcal{T}_{q,k,s}$ ist ein freier R-linearer Code vom Rang k mit den Parametern

$$\left[2^s \cdot \frac{q^k - 1}{q - 1},\quad (k, k),\quad 2^s q^k - 2^{s/2} q^{\frac{k-1}{2}}\right]_R.$$

Der homogene Gewichtszähler von $\mathcal{T}_{q,k,s}$ ist in Tabelle 3.1.3 angegeben.

Tabelle 3.1.3.: Homogener Gewichtszähler des Codes $\mathcal{T}_{q,k,s}$

Typ	#Codewörter	w_{hom}
0	1	0
H_+	$\frac{1}{2}(q^k-1)(q^k+2^{s/2}q^{\frac{k+1}{2}})$	$2^sq^k-2^{s/2}q^{\frac{k-1}{2}}$
$2H$	q^k-1	2^sq^k
H_-	$\frac{1}{2}(q^k-1)(q^k-2^{s/2}q^{\frac{k+1}{2}})$	$2^sq^k+2^{s/2}q^{\frac{k-1}{2}}$

Tabelle 3.1.4.: Homogener Gewichtszähler des Codes $\mathcal{U}_{q,k,s}$

Typ	#Codewörter	w_{hom}
0	1	0
H_+	$2^s(q^{k+1}-q)$	$2^sq^k-q^{k-1}$
$H_-, 2H$	$q^{2k}-2^s(q^{k+1}-q)-1$	2^sq^k

Beweis. Der homogene Gewichtszähler und die Parameter von $\mathcal{T}_{q,k,s}$ können problemlos mit Fakt 2.3.1 aus dem Spektrum von $\mathfrak{T}_{q,k,s}$ in Satz 3.1.8(a) berechnet werden. □

Bemerkung 3.1.11 Die Codes $\mathcal{T}_{q,k,s}$ verallgemeinern die von den Teichmüller-Punktmengen induzierten Codes ($s=0$), welche wiederum die verkürzten $\mathbb{Z}_4$-linearen Kerdock-Codes ($s=0, q=2$) und die von den Hyperovalen in [67] induzierten Codes ($s=0, k=3$) als Spezialfälle enthalten. Im Fall $s=(k-1)r$ erhalten wir die Simplex-Codes $\text{Sim}(k,R)$ [65, Sec. 6.1], siehe auch Beispiel 2.4.1. Im Fall $s=1, q=2$ erhalten wir Codes mit den Parametern der zweifach verkürzten $\mathbb{Z}_4$-linearen Kerdock-Codes. Diese Codes $\mathcal{T}_{q,k,1}$ sind im Allgemeinen aber nicht zu den doppelt verkürzten Kerdock-Codes isomorph, vgl. Beispiel 3.1.15.[33]

Satz 3.1.12 *Seien $r \geq 1$ und $k \geq 2$ ganze Zahlen, $q=2^r$ und*

$$s \in \left\{ \left\lfloor \frac{k-1}{2} \right\rfloor r,\ \left\lfloor \frac{k-1}{2} \right\rfloor r+1,\ \ldots,\ (k-1)r \right\}.$$

(a) Der Code $\mathcal{U}_{q,k,s}$ ist ein freier R-linearer Code vom Rang k mit den Parametern

$$\left[2^s \cdot \frac{q^k-1}{q-1},\quad (k,k),\quad 2^sq^k-q^{k-1} \right]_R.$$

Der homogene Gewichtszähler von $\mathcal{U}_{q,k,s}$ ist in Tabelle 3.1.4 angegeben.

[33] Die Automorphismengruppe eines $\mathbb{Z}_4$-linearen Kerdock-Codes operiert nach [52, Sec. V-E] zweifach transitiv auf den Positionen, so dass alle durch doppeltes Verkürzen enstehenden Codes isomorph sind.

(b) *Für $s \neq (k-1)r$ hat der $\mathcal{U}_{q,k,s}$ genau zwei von Null verschiedene homogene Gewichte $w_1 < w_2$. Bezeichnet man zwei Codewörter $\mathbf{c}$ und $\mathbf{c}'$ mit $w_{\mathrm{hom}}(\mathbf{c}-\mathbf{c}') = w_1$ als benachbart, so entsteht ein Graph G auf der Knotenmenge $\mathcal{U}_{q,k,s}$. Dieser Graph ist stark regulär mit den Parametern*

$$(N, K, \lambda, \mu) \quad = \quad \left(q^{2k}, \quad 2^s q(q^k-1), \quad q^k + 2^s q(2^s q - 3), \quad 2^s q(2^s q - 1)\right).$$

Beweis. Der homogene Gewichtszähler und die Parameter von $\mathfrak{U}_{q,k,s}$ ergeben sich mit Fakt 2.3.1 wieder aus dem Spektrum von $\mathfrak{U}_{q,k,s}$ in Satz 3.1.8(b).

Wir sehen, dass $\mathcal{U}_{q,k,s}$ fett und projektiv ist (d.h. die zugehörige Multimenge $\mathfrak{U}_{q,k,s}$ ist eine Menge) und nur zwei von Null verschiedene homogene Gewichte hat. Nach [16, Th. 5.5] ist G stark regulär. Die Parameter von G werden mit den dort angegebenen Formeln berechnet. □

Bemerkung 3.1.13

(a) Die Codes $\mathcal{U}_{q,k,s}$ überschneiden sich im Fall $s \geq (k-2)r$ mit der Konstruktion in [101] (der Spezialfall $k = 3$ findet sich bereits in [16, Prop. 6.6]), in der dortigen Notation müssen dafür q und s Zweierpotenzen sein. Vermutlich können die partiellen Differenzenmengen in [74] benutzt werden, um eine Klasse von Codes mit zwei Schnittzahlen anzugeben, welche die Codes $\mathcal{U}_{q,k,s}$ sowie die Codes aus [101] als Spezialfall enthält. Da die homogene Minimaldistanz der Codes $\mathcal{U}_{q,k,s}$ jedoch nicht besonders gut ist, soll dieser Frage hier nicht weiter nachgegangen werden.

(b) Für herkömmliche lineare Codes wurde der Zusammenhang zwischen Codes mit nur zwei verschiedenen Gewichten (engl.: *two-weight codes*) und stark regulären Graphen erstmals in [29] beobachtet, siehe auch [19]. In [16, 58] wurde diese Theorie auf two-weight Codes über endlichen Frobenius-Ringen ausgeweitet, weitere Ergebnisse hierzu finden sich in [18]. Zur allgemeinen Theorie stark regulärer Graphen siehe z.B. [43, Sec. 10].

(c) Die Parameter der stark regulären Graphen G aus Satz 3.1.12 sind nicht neu. Jedes orthogonale Array $\mathrm{OA}(q^k, 2^s q)$ erzeugt einen stark regulären Graphen mit denselben Parametern [43, Sec. 10.4].

3.1.4. Beispiele

Im Folgenden diskutieren wir einige konkrete Fälle der Codes $\mathcal{T}_{q,k,s}$. Für Isomorphietests wurde der Algorithmus aus [39] verwendet, alle weiteren Berechnungen wurden im Computeralgebrasystem Magma [10] realisiert.

Beispiel 3.1.14 (Heptacode) Der eindeutige Code $\mathcal{T}_{2,3,0}$ hat die Parameter $[7, (3,3), 6]_{\mathbb{Z}_4}$ und den symmetrisierten Gewichtszähler

$$X_2^7 + 42X_0^4X_1X_2^2 + 7X_1^4X_2^3 + 14X_0^4X_1^3.$$

$\mathcal{T}_{2,3,0}$ ist bis auf Isomorphie der einzige $(7, 2^6, 6)_{\mathbb{Z}_4}$-Code [39]. Er ist isomorph zur Verkürzung des $\mathbb{Z}_4$-linearen Oktacodes (Beispiel 2.2.8) an beliebiger Position.

Das Gray-Bild ist ein nichtlinearer Code mit den BTL-Parametern $(14, 2^6, 6)_2$ und dem Hamming-Gewichtszähler

$$1 + 42X^6 + 7X^8 + 14X^{10}.$$

Damit ist $\mathcal{T}_{2,3,0}$ der kürzeste $\mathbb{Z}_4$-lineare BTL-Code. Es ist auch kein $\mathbb{Z}_4$-linearer BTKL-Code kleinerer Größe oder kleinerer Minimaldistanz bekannt. Aus diesem Grund drängt es sich auf, diesen bemerkenswerten Code mit dem noch nicht vergebenen Namen *Heptacode* zu adeln.

Beispiel 3.1.15 Es gibt 4 passende Unterräume U zur Erzeugung eines Codes $\mathcal{T}_{2,4,1}$. Die resultierenden Codes sind alle isomorph, das Symbol $\mathcal{T}_{2,4,1}$ legt also einen bis auf Isomorphie eindeutigen $\mathbb{Z}_4$-linearen Code fest. Eine mögliche Generatormatrix ist

$$\begin{pmatrix}
1&0&0&0&1&2&1&3&1&2&3&1&2&3&1&0&0&1&1&1&3&0&2&2&0&3&3&2&0&1\\
0&1&0&0&1&1&0&1&0&2&0&1&1&3&0&2&1&3&3&2&0&1&1&2&2&1&3&3&1&2\\
0&0&1&0&1&1&0&0&1&2&2&2&1&1&1&1&2&3&1&3&1&3&3&1&1&0&0&2&2&0\\
0&0&0&1&2&2&1&0&0&1&1&0&0&2&2&0&2&1&1&1&1&1&1&1&1&1&1&1&1&2
\end{pmatrix}.$$

Dieser Code ist fett und hat die Parameter $[30, (4, 4), 28]_{\mathbb{Z}_4}$ und den symmetrisierten Gewichtszähler

$$X_2^{30} + 180X_0^{16}X_1^6X_2^8 + 15X_1^{16}X_2^{14} + 60X_0^{16}X_1^{10}X_2^4.$$

Das Gray-Bild hat die Parameter $(60, 2^8, 28)_2$ und ist damit ein BTL-Code [12, Th. 3]. Der Hamming-Gewichtszähler ist

$$1 + 180X^{28} + 15X^{32} + 60X^{36}.$$

Der Code aus [3, Ex. 4] ist zu $\mathcal{T}_{2,4,1}$ isomorph.

Doppeltes Verkürzen des $\mathbb{Z}_4$-linearen Kerdock-Codes $\mathcal{K}_{5+1}$ in zwei beliebigen Koordinaten liefert einen nicht zu $\mathcal{T}_{2,4,1}$ isomorphen Code mit denselben Parametern und demselben symmetrisierten Gewichtszähler. Eine mögliche Generatormatrix ist

$$\begin{pmatrix}
1&0&0&0&1&1&2&3&1&0&2&0&2&1&1&1&3&2&3&3&0&3&1&0&2&2&0&1&3&1\\
0&1&0&0&1&0&2&0&2&0&1&2&0&2&0&1&2&3&3&1&3&1&1&1&1&3&1&3&1&2\\
0&0&1&0&0&1&1&0&1&2&2&1&1&3&1&2&2&3&1&1&1&3&3&1&1&2&2&0&0&0\\
0&0&0&1&0&0&1&1&1&1&0&0&1&1&2&2&1&1&2&0&1&1&1&2&2&1&1&1&1&2
\end{pmatrix}.$$

Im Jahr 2009 wurde von Johannes Zwanzger durch ein heuristisches Suchverfahren ein weiterer $[30, (4, 4), 28]_{\mathbb{Z}_4}$-Code mit der Generatormatrix

$$\begin{pmatrix}
1&0&0&0&1&1&1&2&1&1&0&1&1&0&1&1&1&0&1&1&2&2&2&1&1&2&1&0&0&2\\
0&1&0&0&2&1&3&1&0&1&1&2&3&2&2&0&1&1&0&1&0&1&1&1&1&0&2&1&2&1\\
0&0&1&0&0&0&0&2&1&3&1&3&3&1&1&2&2&2&0&0&1&1&3&1&3&1&1&3&2&2\\
0&0&0&1&1&3&2&3&3&0&3&2&3&1&3&2&1&2&1&2&1&2&1&1&2&2&2&2&1&3
\end{pmatrix}$$

gefunden. Im Gegensatz zu den vorherigen beiden Codes hat dieser Code zwei identische Spalten.[34] Der symmetrisierte Gewichtszähler ist

$$X_2^{30} + 182X_0^{16}X_1^6X_2^8 + 15X_1^{16}X_2^{14} + 56X_0^{16}X_1^{10}X_2^4 + 2X_0^{16}X_1^{14},$$

und das Gray-Bild hat den Hamming-Gewichtszähler

$$1 + 182X^{28} + 15X^{32} + 56X^{36} + 2X^{44}.$$

Mit den eben genannten Gewichtszählern existiert schließlich noch ein vierter Isomorphietyp: Kürzlich wurde in [72, Ex. 3] ein nicht freier $[30, (5, 3), 28]_{\mathbb{Z}_4}$-Code durch Vergrößerung des Simplex-Codes $\mathrm{Sim}(3, \mathbb{Z}_4)$ um zwei nicht freie Zeilen konstruiert. Der Code hat zwei Torsionsspalten, ist also nicht fett. Eine mögliche Generatormatrix ist

$$\begin{pmatrix}
1&0&0&1&1&0&0&0&2&3&1&1&3&1&0&3&2&0&1&3&3&1&2&2&2&3&1&1&0&2\\
0&1&0&1&1&1&3&1&0&1&2&1&0&0&1&1&2&3&1&1&2&2&1&0&1&1&0&2&0&2\\
0&0&1&0&0&0&1&1&1&1&1&1&1&2&0&0&1&1&1&1&1&1&1&1&2&2&2&2&2&0\\
0&0&0&2&0&2&0&2&2&2&0&0&2&2&2&0&2&2&0&0&0&0&2&2&2&0&0&0&2&0\\
0&0&0&0&2&2&2&0&2&2&2&0&0&2&0&0&0&2&2&2&0&0&2&0&0&0&2&2&0&2
\end{pmatrix}.$$

Beispiel 3.1.16 Zur Erzeugung eines Codes $\mathcal{T}_{2,5,2}$ gibt es 20 Möglichkeiten für den Unterraum U. Je 5 dieser Unterräume liefern zueinander isomorphe Codes, d.h. es gibt 4 Isomorphietypen von Codes $\mathcal{T}_{2,5,2}$. Jeder solche Code ist fett mit den Parametern $[124, (5, 5), 120]_{\mathbb{Z}_4}$ und dem symmetrisierten Gewichtszähler

$$X_2^{124} + 744X_0^{64}X_1^{28}X_2^{32} + 31X_1^{64}X_2^{60} + 248X_0^{64}X_1^{36}X_2^{24}.$$

Das Gray-Bild hat die Parameter $(248, 2^{10}, 120)_2$ und den Hamming-Gewichtszähler

$$1 + 744X^{120} + 31X^{128} + 248X^{136}.$$

Die Codes $\mathcal{T}_{2,5,2}$ sind BTKL: Die Internetseite [46] zeigt für die größtmögliche Minimaldistanz eines $[248, 10]_{\mathbb{F}_2}$-Codes das Intervall 119–120, die untere Schranke stammt aus [37]. Die obere Schranke erhält man so: Gäbe es einen linearen $[248, 10, 121]_{\mathbb{F}_2}$-Code, so durch das Bilden des Residuums in einem Codewort von minimalem Gewicht auch einen $[127, 9, 61]_{\mathbb{F}_2}$-Code,[35] durch erneutes Bilden des Residuums in einem Codewort von minimalem Gewicht einen $[66, 8, 31]_{\mathbb{F}_2}$-Code und durch Anhängen eines Paritätsbits schließlich einen $[67, 8, 32]_{\mathbb{F}_2}$-Code im Widerspruch zu [34, Th. 2.3].

Beispiel 3.1.17 Zur Erzeugung eines Codes $\mathcal{T}_{2,6,1}$ gibt es 16 Wahlmöglichkeiten für den Unterraum U. Bezüglich der Isomorphieklassen der erzeugten Codes zerfallen diese 16

[34] Die angegebene Matrix wurde unverändert von der Programmausgabe von Johannes Zwanzger übernommen. Dort sind die achte und die letzte Spalte identisch.

[35] Sollte die Minimaldistanz des Residuums > 61 sein, so kann dieser Code durch Nullsetzen einer oder mehrerer im Träger eines Codeworts von minimalem Gewicht enthaltenen Position zu einem $[127, 9, 61]_{\mathbb{F}_2}$-Code modifiziert werden.

Möglichkeiten in die Partition $(6, 6, 3, 1)$. Es gibt also vier Isomorphietypen von Codes $\mathcal{T}_{2,6,1}$. Eine der beiden zu einem Partitionseintrag 6 gehörenden Isomorphieklassen enthält auch den Code aus [3, Ex. 4]. Jeder Code $\mathcal{T}_{2,6,1}$ ist fett und hat die Parameter $[126, (6, 6), 120]_{\mathbb{Z}_4}$ und den symmetrisierten Gewichtszähler

$$X_2^{126} + 2520X_0^{64}X_1^{28}X_2^{34} + 63X_1^{64}X_2^{62} + 1512X_0^{64}X_1^{36}X_2^{26}.$$

Die Gray-Bilder haben die Parameter $(252, 2^{12}, 120)_2$ und den Hamming-Gewichtszähler

$$1 + 2520X^{120} + 63X^{128} + 1512X^{136}.$$

Die Internetseite [46] zeigt für die größtmögliche Minimaldistanz eines $[252, 12]_{\mathbb{F}_2}$-Codes das Intervall 118–120. Damit sind die Codes $\mathcal{T}_{2,6,1}$ BTKL. Die obere Schranke erhält man durch die Betrachtung des Residuums in einem Codewort von minimalem Gewicht und der oberen Schranke 60 an die Minimaldistanz eines $[131, 11]_{\mathbb{F}_2}$-Codes aus [77]. Ein weiterer, nicht in den 4 Isomorphieklassen von $\mathcal{T}_{2,6,1}$ enthaltener Code mit demselben symmetrisierten Gewichtszähler ist der doppelt verkürzte Kerdock-Code $\mathcal{K}_{7+1}$.

Beispiel 3.1.18 Zur Erzeugung eines Codes $\mathcal{T}_{2,6,3}$ gibt es 80 Wahlmöglichkeiten für den Unterraum U. Bezüglich der Isomorphieklassen der erzeugten Codes zerfallen diese 80 Möglichkeiten in die Partition $(6^{13}2^1)$, es gibt also 14 Isomorphietypen von Codes $\mathcal{T}_{2,6,3}$. Jeder Code $\mathcal{T}_{2,6,3}$ ist fett und hat die Parameter $[504, (6, 6), 496]_{\mathbb{Z}_4}$ und den symmetrisierten Gewichtszähler

$$X_2^{504} + 3024X_0^{256}X_1^{120}X_2^{128} + 63X_1^{256}X_2^{248} + 1008X_0^{256}X_1^{136}X_2^{112}.$$

Die Gray-Bilder haben die Parameter $(1008, 2^{12}, 496)_2$ und den Hamming-Gewichtszähler

$$1 + 3024X^{496} + 63X^{512} + 1008X^{528}.$$

Dieser Code ist leider zu lang, um ihn direkt mit den Tabellen für lineare Codes vergleichen zu können.

Beispiel 3.1.19 Wegen $s = 0$ ist der Unterraum $U = \mathbb{F}_4$ und damit der Code $\mathcal{T}_{4,3,0}$ eindeutig. Er hat die Parameter $[21, (3, 3), 60]_{\mathrm{GR}(4,2)}$ und den symmetrisierten Gewichtszähler

$$X_2^{21} + 2520X_0^{16}X_1^3X_2^2 + 63X_1^{16}X_2^5 + 1512X_0^{16}X_1^5.$$

Das Gray-Bild hat die Parameter $(84, 4^6, 60)_4$ und den Hamming-Gewichtszähler

$$1 + 2520X^{60} + 63X^{64} + 1512X^{68}.$$

Die Internetseite [46] zeigt für die größtmögliche Minimaldistanz eines $[84, 6]_{\mathbb{F}_4}$-Codes das Intervall 59–60. Damit ist $\mathcal{T}_{4,3,0}$ ein BTKL-Code. Er wurde erstmals in [55] angegeben. Dort wurde der Code als das Erzeugnis eines Hyperovals in $\mathrm{PHG}(\mathrm{GR}(4, 2)^3)$ realisiert.

Für die Erzeugung von $\mathcal{T}_{4,3,0}$ wird ein zweidimensionaler $\mathbb{F}_2$-Vektorraum U von $\mathbb{F}_{2^6}$ benutzt. Die gleiche Situation liegt bei dem Code $\mathcal{T}_{2,6,1}$ aus Beispiel 3.1.17 vor. Hierdurch erklärt sich die Ähnlichkeit zwischen den Gewichtszählern der beiden Codes.

3.2. Geometrisches Dualisieren

Im Abschnitt 2.3 haben wir gesehen, dass jede Hjelmslev-Geometrie PHG(R^k) zu ihrer dualen Geometrie isomorph ist. Ist also eine Multimenge $\mathfrak{k}$ von Punkten in PHG(R^k) vorgegeben, so können wir anhand des $\mathfrak{k}$-Typs bestimmte Hyperebenen der Geometrie (evtl. mehrfach) auswählen und wieder als eine Multimenge von Punkten in PHG(R^k) interpretieren. Auf diese Weise erhalten wir die *dualisierte* Punktmenge.

Die Auswahl der Hyperebenen wird durch eine *Dualisierungsfunktion* τ realisiert. Sei dazu $\Omega = \{\mathbf{a}_\mathfrak{k}(H) \mid H \in \mathcal{H}\} \subset \mathbb{N}^3$ die Menge aller $\mathfrak{k}$-Typen. Eine Dualisierungsfunktion τ ist dann eine Abbildung $\Omega \to \mathbb{N}$, die einer Hyperebene vom Typ ω die Multiplizität $\tau(\omega)$ zuweist. Damit definiert τ eine Multimenge $\mathfrak{k}^\tau$ von Hyperebenen in der dualen Geometrie, die wir als die dualisierte Multimenge von Punkten in der Ausgangsgeometrie PHG(R^k) auffassen.

Wir nennen eine Multimenge $\mathfrak{k}$ von Punkten *selbstdual*, wenn eine Dualisierungsfunktion τ existiert mit $\mathfrak{k}^\tau \cong \mathfrak{k}$,[36] und *formal selbstdual*, wenn eine Dualisierungsfunktion τ existiert mit $\mathrm{spec}(\mathfrak{k}) = \mathrm{spec}(\mathfrak{k}^\tau)$. Selbstduale Punktmengen sind auch formal selbstdual.

Für *lineare* Dualisierungsfunktionen, d.h. $\tau((\omega_0, \omega_1, \omega_2)) = \alpha + \beta\omega_1 + \gamma\omega_2$ mit $\alpha, \beta, \gamma \in \mathbb{Q}$,[37] hängt das Spektrum der dualisierten Punktmenge nur vom ursprünglichen Spektrum und der Verteilung der Punkte auf die Punktklassen ab:

Fakt 3.2.1 ([70, Th. 2]) *Der $\mathfrak{k}^\tau$-Typ einer Hyperebene $x \in \mathcal{P}$ der dualen Geometrie ist*

$$\mathbf{a}_{\mathfrak{k}^\tau}(x) = (b_0, b_1, b_2)$$

mit

$$\begin{aligned}
b_0 &= \alpha q^{2k-2} + \beta \cdot \#\mathfrak{k} \cdot q^{2k-4}(q-1) + \gamma \cdot \#\mathfrak{k} \cdot q^{2k-4} \\
&\quad - \left(\beta q^{2k-4}(q-1) + \gamma q^{2k-4}\right) \mathfrak{k}([x]), \\
b_1 &= \alpha q^{k-2}(q^{k-1}-1) + \beta \cdot \#\mathfrak{k} \cdot q^{k-3}(q^{k-2}-1)(q-1) + \gamma \cdot \#\mathfrak{k} \cdot q^{k-3}(q^{k-2}-1) \\
&\quad + \left(\beta q^{k-3}(q^k - 2q^{k-1} + q^{k-2} - 1) + \gamma q^{k-3}(q^{k-1} - q^{k-2} + 1)\right) \mathfrak{k}([x]) \\
&\quad - (\gamma - \beta) q^{2k-4} \mathfrak{k}(x), \\
b_2 &= \alpha q^{k-2} \cdot \frac{q^{k-1}-1}{q-1} + \beta \cdot \#\mathfrak{k} \cdot q^{k-3}(q^{k-2}-1) + \gamma \cdot \#\mathfrak{k} \cdot q^{k-3} \cdot \frac{q^{k-2}-1}{q-1} \\
&\quad + \left(\beta q^{k-3}(q^{k-1} - q^{k-2} + 1) + \gamma q^{k-3}(q^{k-2}-1)\right) \mathfrak{k}([x]) \\
&\quad + (\gamma - \beta) q^{2k-4} \mathfrak{k}(x).
\end{aligned}$$

Aus Sicht der Codierungstheorie wählt die Dualisierungskonstruktion für jedes symmetrisierte Gewicht $\omega = (\omega_0, \omega_1, \omega_2)$ mit $\omega_0 \neq 0$ eine Menge X von projektiven Vertretern

[36] Gleichheit kann an dieser Stelle nicht gefordert werden, denn die Identifizierung der dualen Geometrie mit der Ausgangsgeometrie ist nur bis auf einen Isomorphismus festgelegt.

[37] Zunächst nennt man eine Dualisierungsfunktion der Form $\tau((\omega_0, \omega_1, \omega_2)) = \alpha'\omega_0 + \beta'\omega_1 + \gamma'\omega_2$ linear. Mit $\#\mathfrak{k} = \omega_0 + \omega_1 + \omega_2$ kann τ dann aber durch $\tau((\omega_0, \omega_1, \omega_2)) = (\alpha' \#\mathfrak{k}) + (\beta' - \alpha')\omega_1 + (\gamma' - \alpha')\omega_2$ auf die angegebene Form gebracht werden.

der Informationswörter der Codewörter in cde($\mathfrak{k}$) vom symmetrisierten Gewicht ω aus und setzt je $\tau(\omega)$ Kopien von jedem Vektor in X als Spalten in eine Generatormatrix $\mathbf{G}^*$. Der Zeilenraum von $\mathbf{G}^*$ ist der Code cde($\mathfrak{k}^\tau$).

Diese Dualisierungskonstruktion soll nun auf die Codes $\mathcal{T}_{q,k,s}$ und die $\mathbb{Z}_4$-linearen Kerdock-Codes $\mathcal{K}_{k+1}$ angewendet werden.

3.2.1. Dualisierte verallgemeinerte Teichmüller-Codes

In diesem Abschnitt seien ganze Zahlen $r \geq 1$, $k \geq 2$, $q = 2^r$ und

$$s \in \begin{cases} \{0, 2, 4, \ldots, (k-1)r\} & \text{falls k ungerade,} \\ \{r, r+2, r+4, \ldots, (k-1)r\} & \text{falls k gerade} \end{cases}$$

vorgegeben. Das Spektrum der Punktmenge $\mathfrak{T}_{q,k,s}$ ist laut Satz 3.1.8 in Tabelle 3.1.1 angegeben. Wir bezeichnen die beiden auftretenden Typen wie dort mit H_- und H_+. Es sei nun eine Dualisierungsfunktion τ definiert durch $\tau(H_-) = 1$ und $\tau(H_+) = 0$, d.h. τ wählt genau die Hyperebenen vom Typ H_- aus. Sei $\mathfrak{T}^*_{q,k,s} = \mathfrak{T}^\tau_{q,k,s}$. Im Fall $s = (k-1)r$ ist $\mathfrak{T}^*_{q,k,(k-1)r}$ die leere Menge. Für $s \neq (k-1)r$ spannt $\mathfrak{T}^*_{q,k,s}$ die volle Punktmenge von PHG(R^k) auf (das werden wir in Satz 3.2.3(a) zeigen), so dass wir an dieser Stelle bereits $\mathcal{T}^*_{q,k,s} = \text{cde}(\mathfrak{T}^*_{q,k,s})$ definieren.

Lemma 3.2.2 *In jeder Hyperebenenklasse von* PHG(R^k) *gibt es* $\frac{1}{2}\left(q^{k-1} - 2^{s/2} q^{\frac{k-1}{2}}\right)$ *Hyperebenen vom Typ* H_- *und* $\frac{1}{2}\left(q^{k-1} + 2^{s/2} q^{\frac{k-1}{2}}\right)$ *Hyperebenen vom Typ* H_+. *Durch einen Punkt in* $\mathfrak{T}_{q,k,s}$ *gehen*

$$\begin{aligned} n_-(\mathfrak{T}_{q,k,s}) &= \frac{1}{2}\left(q^{k-2}\frac{q^{k-1}-1}{q-1} - 2^{s/2} q^{\frac{k-1}{2}} \frac{q^{k-2}-1}{q-1} - \frac{q^{\frac{k-1}{2}}}{2^{s/2}} q^{k-2} \right) \\ &= \frac{1}{2}\left(\frac{q^{\frac{k-1}{2}}}{2^{s/2}} - 1 \right)\left(2^{s/2} q^{\frac{k-1}{2}} \frac{q^{k-2}-1}{q-1} - q^{k-2} \right) \end{aligned}$$

Hyperebenen vom Typ H_- *und*

$$\begin{aligned} n_+(\mathfrak{T}_{q,k,s}) &= \frac{1}{2}\left(q^{k-2}\frac{q^{k-1}-1}{q-1} + 2^{s/2} q^{\frac{k-1}{2}} \frac{q^{k-2}-1}{q-1} + \frac{q^{\frac{k-1}{2}}}{2^{s/2}} q^{k-2} \right) \\ &= \frac{1}{2}\left(\frac{q^{\frac{k-1}{2}}}{2^{s/2}} + 1 \right)\left(2^{s/2} q^{\frac{k-1}{2}} \frac{q^{k-2}-1}{q-1} + q^{k-2} \right) \end{aligned}$$

Hyperebenen vom Typ H_+.

Durch einen Punkt außerhalb von $\mathfrak{T}_{q,k,s}$ gehen

$$n_-(\complement\mathfrak{T}_{q,k,s}) = \frac{1}{2}\left(q^{k-2}\frac{q^{k-1}-1}{q-1} - 2^{s/2}q^{\frac{k-1}{2}}\frac{q^{k-2}-1}{q-1}\right)$$

Hyperebenen vom Typ H_- und

$$n_+(\complement\mathfrak{T}_{q,k,s}) = \frac{1}{2}\left(q^{k-2}\frac{q^{k-1}-1}{q-1} + 2^{s/2}q^{\frac{k-1}{2}}\frac{q^{k-2}-1}{q-1}\right)$$

Hyperebenen vom Typ H_+.

Beweis. Laut Satz 3.1.8(a) gibt es $\frac{1}{2}\frac{q^k-1}{q-1}\left(q^{k-1} - 2^{s/2}q^{\frac{k-1}{2}}\right)$ Hyperebenen vom Typ H_-. Nach Lemma 3.1.7 operiert $\mathrm{Aut}(\mathfrak{T}_{q,k,s})$ transitiv auf der Menge der Hyperebenenklassen. Weil es insgesamt $\frac{q^k-1}{q-1}$ Hyperebenenklassen gibt, folgen daraus die behaupteten Anzahlen der Hyperebenen vom Typ H_- bzw. H_+ innerhalb einer Hyperebenenklasse.

Die Anzahlen $n_-(\mathfrak{T}_{q,k,s})$, $n_+(\mathfrak{T}_{q,k,s})$, $n_-(\complement\mathfrak{T}_{q,k,s})$ und $n_+(\complement\mathfrak{T}_{q,k,s})$ lassen sich nun wie in [59, Sec. IV] durch doppeltes Abzählen aus dem aus Satz 3.1.8(a) bekannten Spektrum von $\mathfrak{T}_{q,k,s}$ berechnen. □

Satz 3.2.3

(a) Die Punktmenge $\mathfrak{T}^*_{q,k,s}$ enthält $\frac{1}{2}\frac{q^k-1}{q-1}\left(q^{k-1} - 2^{s/2}q^{\frac{k-1}{2}}\right)$ Punkte. Für $s \neq (k-1)r$ spannt $\mathfrak{T}^*_{q,k,s}$ die volle Punktmenge der Geometrie $\mathrm{PHG}(R^k)$ auf und hat nur zwei verschiedene Schnittzahlen mit den Hyperebenen. Das Spektrum von $\mathfrak{T}^*_{q,k,s}$ ist in Tabelle 3.2.1 angegeben.

(b) Der Code $\mathcal{T}^*_{q,k,s}$ hat die Parameter

$$\left[\frac{1}{2}\frac{q^k-1}{q-1}\left(q^{k-1} - 2^{s/2}q^{\frac{k-1}{2}}\right),\quad (k,k),\quad q^k - 2^{s/2}q^{\frac{k+1}{2}} - 1\right]_R$$

und den in Tabelle 3.2.2 angegebenen homogenen Gewichtszähler.

Beweis. Die Anzahl der Punkte in $\mathfrak{T}^*_{q,k,s}$ ist die Anzahl der Hyperebenen vom $\mathfrak{T}_{q,k,s}$-Typ H_- aus 3.2.2. Nach Lemma 3.2.2 enthält $\mathfrak{T}^*_{q,k,s}$ für $s \neq (k-1)r$ Punkte aus jeder Punktklasse und spannt folglich die volle Geometrie $\mathrm{PHG}(R^k)$ auf. Aus der Anzahl der Punkte pro Punktklasse ergeben sich die ω_0-Einträge in Tabelle 3.2.1. Die ω_2-Einträge sind die Werte $n_-(\mathfrak{T}_{q,k,s})$ und $n_-(\complement\mathfrak{T}_{q,k,s})$ aus Lemma 3.2.2. Mit $\omega_0 + \omega_1 + \omega_2 = \#\mathfrak{T}^*_{q,k,s}$ folgen nun auch die ω_1-Einträge. Die Anzahl-Einträge sind nichts anderes als die Größe der Punktmenge $\mathfrak{T}_{q,k,s}$ bzw. ihres Komplements.

Über Fakt 2.3.1 berechnet man nun den symmetrisierten Gewichtszähler von $\mathcal{T}^*_{q,k,s}$ und daraus weiter den homogenen Gewichtszähler und die Parameter. □

Bemerkung 3.2.4 Die Serie $\mathcal{T}^*_{q,k,s}$ verallgemeinert die Serie der dualisierten Teichmüller-Codes $\mathcal{T}^*_{q,k}$ aus [91, 92], diese bilden den Spezialfall $s = 0$.

Tabelle 3.2.1.: Spektrum der dualisierten Punktmenge $\mathfrak{T}^*_{q,k,s}$

Typ H^*_-	#Hyperebenen	$2^s \dfrac{q^k-1}{q-1}$
	ω_0	$\dfrac{1}{2}q^{k-1}\left(q^{k-1}-2^{s/2}q^{\frac{k-1}{2}}\right)$
	ω_1	$\dfrac{1}{2}q^{k-2}\left(q^{k-1}-1-2^{s/2}q^{\frac{k-1}{2}}+\dfrac{q^{\frac{k-1}{2}}}{2^{s/2}}\right)$
		$=\dfrac{1}{2}q^{k-2}\left(\dfrac{q^{\frac{k-1}{2}}}{2^{s/2}}-1\right)\left(2^{s/2}q^{\frac{k-1}{2}}+1\right)$
	ω_2	$\dfrac{1}{2}\left(q^{k-2}\dfrac{q^{k-1}-1}{q-1}-2^{s/2}q^{\frac{k-1}{2}}\dfrac{q^{k-2}-1}{q-1}-\dfrac{q^{\frac{k-1}{2}}}{2^{s/2}}q^{k-2}\right)$
		$=\dfrac{1}{2}\left(\dfrac{q^{\frac{k-1}{2}}}{2^{s/2}}-1\right)\left(2^{s/2}q^{\frac{k-1}{2}}\dfrac{q^{k-2}-1}{q-1}-q^{k-2}\right)$
Typ H^*_+	#Hyperebenen	$(q^{k-1}-2^s)\dfrac{q^k-1}{q-1}$
	ω_0	$\dfrac{1}{2}q^{k-1}\left(q^{k-1}-2^{s/2}q^{\frac{k-1}{2}}\right)$
	ω_1	$\dfrac{1}{2}q^{k-2}\left(q^{k-1}-1-2^{s/2}q^{\frac{k-1}{2}}\right)$
	ω_2	$\dfrac{1}{2}\left(q^{k-2}\dfrac{q^{k-1}-1}{q-1}-2^{s/2}q^{\frac{k-1}{2}}\dfrac{q^{k-2}-1}{q-1}\right)$

Tabelle 3.2.2.: Homogener Gewichtszähler von $\mathcal{T}^*_{q,k,s}$

Typ	#Codewörter	w_{hom}
0	1	0
H^*_+	$q(q^k-1)(q^{k-1}-2^s)$	$\frac{1}{2}q^{k-1}\left(q^k-2^{s/2}q^{\frac{k+1}{2}}-1\right)$
$2H^*$	q^k-1	$\frac{1}{2}q^{k-1}\left(q^k-2^{s/2}q^{\frac{k+1}{2}}\right)$
H^*_-	$q(q^k-1)2^s$	$\frac{1}{2}q^{k-1}\left(q^k-2^{s/2}q^{\frac{k+1}{2}}-1+\frac{q^{\frac{k-1}{2}}}{2^{s/2}}\right)$

Tabelle 3.2.3.: Spektrum der selbstdualen Punktmenge $\mathfrak{T}_{q,k,(k-1)r-2}$

Typ	#Hyperebenen	ω_0	ω_1	ω_2
H_-	$\frac{1}{4}q^{k-1}\frac{q^k-1}{q-1}$	$\frac{1}{4}q^{2k-2}$	$\frac{1}{4}q^{2k-3}+\frac{1}{2}q^{k-2}$	$\frac{1}{4}q^{k-1}\frac{q^{k-2}-1}{q-1}-\frac{1}{2}q^{k-2}$
H_+	$\frac{3}{4}q^{k-1}\frac{q^k-1}{q-1}$	$\frac{1}{4}q^{2k-2}$	$\frac{1}{4}q^{2k-3}-\frac{1}{2}q^{k-2}$	$\frac{1}{4}q^{k-1}\frac{q^{k-2}-1}{q-1}+\frac{1}{2}q^{k-2}$

Satz 3.2.5 *Die Punktmenge $\mathfrak{T}_{q,k,s}$ ist genau für $s \in \{(k-1)r-2, (k-1)r\}$ formal selbstdual. Das Spektrum der formal selbstdualen Punktmenge $\mathfrak{T}_{q,k,(k-1)r-2}$ ist in Tabelle 3.2.3 angegeben.*

Beweis. Im Fall $s = (k-1)r$ ist $\mathfrak{T}_{q,k,s}$ die komplette Punktmenge von $\mathrm{PHG}(R^k)$, diese ist offensichtlich selbstdual. Sei also $s < (k-1)r$ und $\mathfrak{T}_{q,k,s}$ formal selbstdual. Weil es nach Satz 3.1.8(a) nur zwei verschiedene $\mathfrak{T}_{q,k,s}$-Typen gibt, gibt es für die Dualisierungsfunktion nur die beiden Möglichkeiten $\tau(H_-) = 0, \tau(H_+) = 1$ und $\tau(H_-) = 1, \tau(H_+) = 0$.

Im ersten Fall erhalten wir aus

$$\#\mathfrak{T}_{q,k,s} = \#\mathfrak{T}^{\tau}_{q,k,s} = \#\text{Hyperebenen vom Typ } H_+$$

und dem Spektrum in Satz 3.1.8(a) die Gleichung

$$2^s - \frac{1}{2}q^{k-1} - 2^{s/2}q^{\frac{k-1}{2}} = 0$$

und weiter $s = (k-1)r$, Widerspruch.

Im zweiten Fall erhalten wir genauso

$$2^s + \frac{1}{2}q^{k-1} - 2^{s/2}q^{\frac{k-1}{2}} = 0$$

und weiter $s = (k-1)r-2$. Die Dualisierungsfunktion stimmt hier mit der in Satz 3.2.3(a) betrachteten überein. Einsetzen in das in Satz 3.1.8(a) bzw. in Satz 3.2.3(a) angegebene Spektrum zeigt, dass $\mathfrak{T}_{q,k,(k-1)r-2}$ wirklich dasselbe Spektrum hat wie $\mathfrak{T}^*_{q,k,(k-1)r-2}$ und dieses durch das Spektrum in Tabelle 3.2.3 gegeben ist. □

Bemerkung 3.2.6 Eine Untersuchung mit dem Algorithmus aus [39] zeigt, dass in den formal selbstdualen Fällen $\mathfrak{T}_{2,3,0}$ (bis auf Isomorphie 1 Punktmenge, vgl. Beispiel 3.1.14), $\mathfrak{T}_{2,4,1}$ (1 Punktmenge, vgl. Beispiel 3.1.15), $\mathfrak{T}_{2,5,2}$ (4 Punktmengen, vgl. Beispiel 3.1.16) und $\mathfrak{T}_{2,6,3}$ (14 Punktmengen, vgl. Beispiel 3.1.18) jede Punktmenge zu ihrer dualisierten Punktmenge isomorph ist. Damit liegt die Vermutung nahe, dass die Punktmengen $\mathfrak{T}_{q,k,(k-1)r-2}$ sogar selbstdual sind.

Beispiel 3.2.7 Der Code $\mathcal{T}^*_{2,5,0}$ hat die Parameter $[186, (5,5), 184]_{\mathbb{Z}_4}$ und den symmetrisierten Gewichtszähler

$$X_2^{186} + 930X_0^{96}X_1^{44}X_2^{46} + 31X_1^{96}X_2^{90} + 62X_0^{96}X_1^{60}X_2^{30}.$$

Das Gray-Bild ist ein $(372, 2^{10}, 184)_2$-Code mit dem Hamming-Gewichtszähler

$$1 + 930X^{184} + 31X^{192} + 62X^{216}.$$

Dieser Code ist BTL, denn gäbe es einen linearen $[372, 10, 184]_{\mathbb{F}_2}$-Code, so über das Residuum in einem Codewort von minimalem Gewicht auch einen $[188, 9, 92]_{\mathbb{F}_2}$-Code. Ein solcher Code existiert nach [77] jedoch nicht.

Der Code $\mathcal{T}^*_{2,5,0}$ wurde als dualisierter Teichmüller-Code bereits in [91, 92] veröffentlicht.

Beispiel 3.2.8 Wie von den Codes $\mathcal{T}_{2,6,1}$ in Beispiel 3.1.17 gibt es auch von den Codes $\mathcal{T}^*_{2,6,1}$ genau 4 Isomorphietypen. Sie haben die Parameter $[756, (6, 6), 752]_{\mathbb{Z}_4}$ und den symmetrisierten Gewichtszähler

$$X_2^{756} + 3780X_0^{384}X_1^{184}X_2^{188} + 63X_1^{384}X_2^{372} + 252X_0^{384}X_1^{216}X_2^{156}.$$

Das Gray-Bild ist stets ein $(1512, 2^{12}, 752)_2$-Code mit dem Hamming-Gewichtszähler

$$1 + 3780X^{752} + 63X^{768} + 252X^{816}.$$

Dieser Code ist leider zu lang, um ihn direkt mit den Tabellen für lineare Codes vergleichen zu können. Einen fünften Isomorphietyp mit demselben symmetrisierten Gewichtszähler erhält man durch Dualisieren einer doppelten Verkürzung des Kerdock-Codes $\mathcal{K}_{7+1}$.

Beispiel 3.2.9 Der Code $\mathcal{T}^*_{4,3,0}$ hat die Parameter $[126, (3, 3), 376]_{\mathrm{GR}(4,2)}$ und den symmetrisierten Gewichtszähler

$$X_2^{126} + 3780X_0^{96}X_1^{22}X_2^{8} + 63X_1^{96}X_2^{30} + 252X_0^{96}X_1^{30}.$$

Das Gray-Bild ist ein $(504, 4^6, 376)_4$-Code mit dem Hamming-Gewichtszähler

$$1 + 3780X^{376} + 63X^{384} + 252X^{408}.$$

Dieser Code ist BTKL: Das Residuum eines $\mathbb{F}_4$-linearen $[504, 6, 376]_{\mathbb{F}_4}$-Codes in einem Codewort von minimalem Gewicht wäre ein $[128, 5, \geq 94]_{\mathbb{F}_4}$-Code. Der Internetseite [46] zufolge ist ein solcher Code nicht bekannt, für die größtmögliche Minimaldistanz eines $[128, 5]_{\mathbb{F}_4}$-Codes verbleibt das Intervall 93–94. Die untere Schranke entsteht durch dreifaches Verkürzen des $[131, 5, 96]_{\mathbb{F}_4}$-Codes in [11, Th. 11]. Die obere Schranke erhält man so: Gäbe es einen $[128, 5, 95]_{\mathbb{F}_4}$-Code, so durch das Residuum in einem Codewort von minimalem Gewicht auch einen $[33, 4, 23]_{\mathbb{F}_4}$-Code und durch Verkürzen weiter einen $[32, 4, 22]_{\mathbb{F}_4}$-Code im Widerspruch zu [47, Th. 3.3(vi)].

Als der von einem maximalen $(126, 8)$-Arc in $\mathrm{PHG}(\mathrm{GR}(4, 2)^3)$ erzeugte Code wurde $\mathcal{T}^*_{4,3,0}$ bereits in [85, Sec. 5] veröffentlicht.

3.2.2. Dualisierte Kerdock-Codes

Wir wollen nun die $\mathbb{Z}_4$-linearen Kerdock-Codes $\mathcal{K}_{k+1}$ mit ungeradem $k \geq 3$ auf ähnliche Weise dualisieren. Das Spektrum der $\mathbb{Z}_4$-linearen Kerdock-Punktmenge $\mathfrak{K}_{k+1}$ ist in Tabelle 2.4.4 angegeben. Die Hyperebenen zerfallen in die drei $\mathfrak{K}_{k+1}$-Typen H_-, H_0 und H_+. Wir definieren eine Dualisierungsfunktion τ durch $\tau(H_+) = 0$, $\tau(H_0) = 0$ und $\tau(H_-) = 1$. Sei weiter $\mathfrak{K}^*_{k+1} = \mathfrak{K}^\tau_{k+1}$ und $\mathcal{K}^*_{k+1} = \mathrm{cde}(\mathfrak{K}^*_{k+1})$.

Satz 3.2.10 ([92, Lemma 4]) *Die Punktmenge $\mathfrak{K}^*_{k+1}$ spannt die gesamte Punktmenge von $\mathrm{PHG}(\mathbb{Z}_4^{k+1})$ auf. Tabelle 3.2.4 zeigt das Spektrum von $\mathfrak{K}^*_{k+1}$.*

Der Code $\mathcal{K}^*_{k+1}$ hat die Parameter

$$\left[2^{2k} - 2^k, \quad (k+1, k+1), \quad 2^{2k} - 2^k - 2^{\frac{k-1}{2}}\right]_{\mathbb{Z}_4}.$$

Tabelle 3.2.7 zeigt den symmetrisierten Gewichtszähler von $\mathcal{K}^*_{k+1}$. Die Codewörter der Typen H^*_0, $2H^*_0$, $2H^*_{\mathfrak{K}}$ und 0 bilden zusammen einen $\mathbb{Z}_4$-linearen Teilcode $\mathcal{C}_1$ mit den Parametern

$$\left[2^{2k} - 2^k, \quad (k+1, k), \quad 2^{2k} - 2^k\right]_{\mathbb{Z}_4}.$$

Beweis. Die Dualisierungsfunktion τ ist linear, denn es gilt $\tau((\omega_0, \omega_1, \omega_2)) = \alpha + \beta\omega_1 + \gamma\omega_2$ mit

$$\alpha = 0, \quad \beta = \frac{1 + 2^{\frac{k-1}{2}}}{2^k} \quad \text{und} \quad \gamma = \frac{1 - 2^{\frac{k-1}{2}}}{2^k}.$$

Das Spektrum von $\mathfrak{K}^*_{k+1}$ kann nun mit Fakt 3.2.1 berechnet werden. Hierbei gibt es nach Fakt 2.4.4(a) drei Möglichkeiten für das Paar $(\mathfrak{K}_{k+1}(x), \mathfrak{K}_{k+1}([x]))$: Für die 2^k Punkte $x \in \mathfrak{K}_{k+1}$ ist $\mathfrak{K}_{k+1}(x) = \mathfrak{K}_{k+1}([x]) = 1$. Es ergibt sich der Typ $H^*_{\mathfrak{K}}$ in Tabelle 3.2.4. Für die $2^k(2^k - 1) = 2^{2k} - 2^k$ Punkte x in der unendlich fernen Hyperebene gilt $\mathfrak{K}_{k+1}(x) = \mathfrak{K}_{k+1}([x]) = 0$. Diese ergeben den Typ H^*_0. Die verbleibenden $2^{2k} - 2^k$ Punkte x erfüllen $\mathfrak{K}_{k+1}(x) = 0$ und $\mathfrak{K}_{k+1}([x]) = 1$ und ergeben den Typ $H^*_{\complement\mathfrak{K}}$. Das auf diese Weise berechnete Spektrum zeigt, dass $\mathfrak{K}^*_{k+1}$ die volle Punktmenge aufspannt, denn andernfalls gäbe es eine Hyperebenenklasse, die alle Punkte enthält, und diese hätte den $\mathfrak{K}^*_{k+1}$-Typ $(0, *, *)$.

Wir können also Fakt 2.3.1 benutzen, um den symmetrisierten Gewichtszähler von $\mathcal{K}^*_{k+1}$ aus dem Spektrum abzuleiten. Die $\mathbb{Z}_4$-Linearität des Teilcodes $\mathcal{C}_1$ folgt daraus, dass die Hyperebenen H^*_0 nach Fakt 2.4.4(a) eine Hyperebenenklasse in $\mathrm{PHG}(R^{k+1})$ bilden. Die restlichen Aussagen über $\mathcal{C}_1$ sind klar. □

Der Teilcode $\mathcal{C}_1$ aus Satz 3.2.10 erlaubt es uns, den Code $\mathcal{K}^*_{k+1}$ noch zu verbessern: Wir wenden Konstruktion X (siehe Abschnitt 2.2.6) auf die Codes $\mathcal{C}_1 < \mathcal{K}^*_{k+1}$ mit dem Wiederholungscode $\{\mathbf{0}, (2, \ldots, 2)\}$ der Länge $2^{\frac{k-3}{2}}$ als Hilfscode an und nennen den resultierenden Code $\hat{\mathcal{K}}^*_{k+1}$.[38] Der Code $\hat{\mathcal{K}}^*_{k+1}$ entsteht aus $\mathcal{K}^*_{k+1}$, indem den Codewörtern in $\mathcal{C}_1$ insgesamt $2^{\frac{k-3}{2}}$ Nullsymbole angehängt werden und den restlichen Codewörtern dieselbe Anzahl an 2-Symbolen.

[38] Für diesen sehr kleinen Hilfscode ist der aus der Konstruktion X resultierende Code sogar bis auf Isomorphie eindeutig festgelegt. Der verlängerte Code $\hat{\mathcal{K}}^*_{k+1}$ ist eine Verbesserung von $\mathcal{K}^*_{k+1}$ in dem Sinne, dass der Ausgangscode $\mathcal{K}^*_{k+1}$ trivial durch Verkürzen aus $\hat{\mathcal{K}}^*_{k+1}$ zurückgewonnen werden kann.

Tabelle 3.2.4.: Spektrum der dualisierten Kerdock-Punktmenge $\mathfrak{K}^*_{k+1}$

Typ	#Hyp.	ω_0	ω_1	ω_2
$H^*_{\mathbb{C}\mathfrak{K}}$	$2^{2k}-2^k$	$2^{2k-1}-2^{k-1}$	$2^{2k-2}-2^{k-2}-2^{\frac{k-3}{2}}$	$2^{2k-2}-2^{k-2}+2^{\frac{k-3}{2}}$
H^*_0	$2^{2k}-2^k$	2^{2k-1}	$2^{2k-2}-2^{k-1}$	$2^{2k-2}-2^{k-1}$
$H^*_{\mathfrak{K}}$	2^k	$2^{2k-1}-2^{k-1}$	$2^{2k-2}+2^{\frac{3k-3}{2}}-2^{k-2}-2^{\frac{k-3}{2}}$	$2^{2k-2}-2^{\frac{3k-3}{2}}-2^{k-2}+2^{\frac{k-3}{2}}$

Tabelle 3.2.5.: Symmetrisierter Gewichtszähler von $\mathcal{K}^*_{k+1}$

Typ $H^*_{\mathbb{C}\mathfrak{K}}$	#Codewörter	$2^{2k+1}-2^{k+1}$
	ω_0	$2^{2k-1}-2^{k-1}$
	ω_1	$2^{2k-2}-2^{k-2}-2^{\frac{k-3}{2}}$
	ω_2	$2^{2k-2}-2^{k-2}+2^{\frac{k-3}{2}}$
	w_{Lee}	$2^{2k}-2^k-2^{\frac{k-1}{2}}$
Typ H^*_0	#Codewörter	$2^{2k+1}-2^{k+1}$
	ω_0	2^{2k-1}
	ω_1	$2^{2k-2}-2^{k-1}$
	ω_2	$2^{2k-2}-2^{k-1}$
	w_{Lee}	$2^{2k}-2^k$
Typ $H^*_{\mathfrak{K}}$	#Codewörter	2^{k+1}
	ω_0	$2^{2k-1}-2^{k-1}$
	ω_1	$2^{2k-2}+2^{\frac{3k-3}{2}}-2^{k-2}-2^{\frac{k-3}{2}}$
	ω_2	$2^{2k-2}-2^{\frac{3k-3}{2}}-2^{k-2}+2^{\frac{k-3}{2}}$
	w_{Lee}	$2^{2k}-2^k+2^{\frac{3k-1}{2}}-2^{\frac{k-1}{2}}$
Typ $2H^*_0$	#Codewörter	2^k-1
	ω_0	0
	ω_1	2^{2k-1}
	ω_2	$2^{2k-1}-2^k$
	w_{Lee}	2^{2k}
Typ $2H^*_{\mathfrak{K}}$	#Codewörter	2^k
	ω_0	0
	ω_1	$2^{2k-1}-2^{k-1}$
	ω_2	$2^{2k-1}-2^{k-1}$
	w_{Lee}	$2^{2k}-2^k$
Typ 0	#Codewörter	1
	ω_0	0
	ω_1	0
	ω_2	$2^{2k}-2^k$
	w_{Lee}	0

Satz 3.2.11 ([92, Th. 5]) *Der Code $\hat{\mathcal{K}}^*_{k+1}$ hat die Parameter*

$$\left[2^{2k} - 2^k + 2^{\frac{k-3}{2}}, \quad (k+1, k+1), \quad 2^{2k} - 2^k\right]_{\mathbb{Z}_4}.$$

Tabelle 3.2.6 zeigt den Lee-Gewichtszähler und Tabelle 3.2.7 den symmetrisierten Gewichtszähler von $\hat{\mathcal{K}}^*_{k+1}$.

Beweis. Direkt aus Satz 3.2.10. □

Beispiel 3.2.12

Der Code $\hat{\mathcal{K}}^*_{3+1}$ hat die Parameter $[57, (4,4), 56]_{\mathbb{Z}_4}$ und den symmetrisierten Gewichtszähler

$$X_2^{57} + (112X_0^{32}X_1^{12}X_2^{13} + 112X_0^{28}X_1^{14}X_2^{15} + 8X_1^{28}X_2^{29}) + 7X_1^{32}X_2^{25} + 16X_0^{28}X_1^{22}X_2^7.$$

Eine mögliche Generatormatrix ist

$$\begin{pmatrix} 1111\,0222\,0222\,0222\,1111\,1111\,1111\,0222\,0222\,0222\,0222\,1111\,1111\,1111\,2 \\ 2022\,1111\,2022\,2022\,1313\,2022\,2022\,1111\,1111\,2022\,1111\,2022\,1331\,3131\,2 \\ 2202\,2202\,1111\,2202\,2202\,1133\,2202\,1133\,2202\,1111\,3131\,1313\,2202\,1331\,2 \\ 2220\,2220\,2220\,1111\,2220\,2220\,1313\,2220\,1133\,3113\,3113\,1133\,1133\,2220\,2 \end{pmatrix}.$$

Das Gray-Bild hat die Parameter $(114, 2^8, 56)_2$ und den Hamming-Gewichtszähler

$$1 + 232X^{56} + 7X^{64} + 16X^{72}.$$

Dieser Code ist BTL: Gäbe es einen $\mathbb{F}_2$-linearen $[114, 8, 56]_{\mathbb{F}_2}$-Code, so auch das Residuum in einem Codewort von minimalem Gewicht, also einen $[58, 7, \geq 28]_{\mathbb{F}_2}$-Code im Widerspruch zu [125, Th. 3.7]. Ein $(58, 2^7, 28)_2$-Code lässt sich jedoch als Gray-Bild eines $\mathbb{Z}_4$-linearen Codes realisieren, siehe Beispiel 3.3.9.

Der Code $\hat{\mathcal{K}}^*_{3+1}$ wurde zuerst 2009 von Johannes Zwanzger gefunden (siehe auch [132]) und bereits in [89, 91, 92] computerfrei beschrieben.

Beispiel 3.2.13 Der Code $\hat{\mathcal{K}}^*_{5+1}$ hat die Parameter $[994, (6,6), 992]_{\mathbb{Z}_4}$ und den symmetrisierten Gewichtszähler

$$X_2^{994} + (1984X_0^{512}X_1^{240}X_2^{242} + 1984X_0^{496}X_1^{248}X_2^{250} + 32X_1^{496}X_2^{498}) + 31X_1^{512}X_2^{482} + 64X_0^{496}X_1^{312}X_2^{186}.$$

Das Gray-Bild hat die Parameter $(1988, 2^{12}, 994)_2$ und den Hamming-Gewichtszähler

$$1 + 4000X^{992} + 31X^{1024} + 64X^{1120}.$$

Dieser Code ist BTL: Durch einen aufwendigen Computerbeweis wurde von Alfred Wassermann und Johannes Zwanzger nachgewiesen, dass kein linearer $[1988, 12, 994]_{\mathbb{F}_2}$-Code existiert, dieses Resultat wurde bislang nicht veröffentlicht.

Der Code $\hat{\mathcal{K}}^*_{5+1}$ wurde bereits in [89, 91, 92] veröffentlicht.

Tabelle 3.2.6.: Lee-Gewichtszähler von $\hat{\mathcal{K}}_{k+1}^*$

Typ	#Codewörter	w_{Lee}
0	1	0
$H_{\mathbb{C}\mathfrak{K}}^*, H_0^*, 2H_{\mathfrak{K}}^*$	$2^{2k+2} - 3 \cdot 2^k$	$2^{2k} - 2^k$
$2H_0^*$	$2^k - 1$	2^{2k}
$H_{\mathfrak{K}}^*$	2^{k+1}	$2^{2k} + 2^{\frac{3k-1}{2}} - 2^k$

Tabelle 3.2.7.: Symmetrisierter Gewichtszähler von $\hat{\mathcal{K}}_{k+1}^*$

Typ $H_{\mathbb{C}\mathfrak{K}}^*$	#Codewörter	$2^{2k+1} - 2^{k+1}$
	ω_0	$2^{2k-1} - 2^{k-1}$
	ω_1	$2^{2k-2} - 2^{k-2}$
	ω_2	$2^{2k-2} - 2^{k-2} + 2^{\frac{k-3}{2}}$
	w_{Lee}	$2^{2k} - 2^k$
Typ H_0^*	#Codewörter	$2^{2k+1} - 2^{k+1}$
	ω_0	2^{2k-1}
	ω_1	$2^{2k-2} - 2^{k-1}$
	ω_2	$2^{2k-2} - 2^{k-1} + 2^{\frac{k-3}{2}}$
	w_{Lee}	$2^{2k} - 2^k$
Typ $H_{\mathfrak{K}}^*$	#Codewörter	2^{k+1}
	ω_0	$2^{2k-1} - 2^{k-1}$
	ω_1	$2^{2k-2} + 2^{\frac{3k-3}{2}} - 2^{k-2}$
	ω_2	$2^{2k-2} - 2^{\frac{3k-3}{2}} - 2^{k-2} + 2^{\frac{k-3}{2}}$
	w_{Lee}	$2^{2k} - 2^k + 2^{\frac{3k-1}{2}}$
Typ $2H_0^*$	#Codewörter	$2^k - 1$
	ω_0	0
	ω_1	2^{2k-1}
	ω_2	$2^{2k-1} - 2^k + 2^{\frac{k-3}{2}}$
	w_{Lee}	2^{2k}
Typ $2H_{\mathfrak{K}}^*$	#Codewörter	2^k
	ω_0	0
	ω_1	$2^{2k-1} - 2^{k-1}$
	ω_2	$2^{2k-1} - 2^{k-1} + 2^{\frac{k-3}{2}}$
	w_{Lee}	$2^{2k} - 2^k$
Typ 0	#Codewörter	1
	ω_0	0
	ω_1	0
	ω_2	$2^{2k} - 2^k + 2^{\frac{k-3}{2}}$
	w_{Lee}	0

3.3. Vergrößerte und verlängerte Simplex-Codes

Wir haben in Abschnitt 2.4.1 gesehen, dass die R-linearen Simplex-Codes hervorragende Fehlerkorrektureigenschaften aufweisen. Im Folgenden wird nun die Frage untersucht, wie die $\mathbb{Z}_4$-linearen Simplex-Codes um einen zu $2\mathbb{Z}_4$ isomorphen direkten Summanden vergrößert werden können, so dass die Minimaldistanz dabei möglichst groß bleibt. Die Konstruktion lässt sich für alle Galois-Ringe der Länge 2 (auch solche ungerader Charakteristik) durchführen, wenn die $(q-1)$-fache Wiederholung des Simplex-Codes als Ausgangscode genommen wird.

Definition 3.3.1 *Sei $\mathfrak{k}$ eine Punktmenge in* $\mathrm{PHG}(R^k)$*. Wir definieren eine Matrix $\mathbf{G} \in R^{(k+1)\times q^{k-1}(q^k-1)}$ wie folgt: Für jeden Punkt x in* $\mathrm{PHG}(R^k)$ *werden $q-1$ Kopien des Koordinatenvektors $\kappa(x)$ spaltenweise in die ersten k Zeilen von $\mathbf{G}$ eingetragen. Ist $x \in \mathfrak{k}$, so werden die zugehörigen $q-1$ Einträge in der $(k+1)$-ten Zeile alle auf 0 gesetzt. Andernfalls werden die $q-1$ Elemente von R^*p jeweils einmal eingetragen. Den von $\mathbf{G}$ erzeugten Code bezeichnen wir mit* $\mathrm{SimAug}(\mathfrak{k})$ (vergrößerter Simplex-Code, augmented Simplex code)*.*

Satz 3.3.2 *Sei $\mathfrak{k}$ eine echte Teilmenge der Punktmenge $\mathcal{P}$ von* $\mathrm{PHG}(R^k)$*. Im Fall $R = \mathbb{Z}_4$ sei $\mathfrak{k}$ keine Hyperebenenklasse. Sei weiter* $\mathrm{spec}(\mathfrak{k}) = \sum_{\psi\in\mathbb{N}^3} A_\psi \mathbf{X}^\psi$ *das Spektrum von $\mathfrak{k}$.*

Dann ist die Matrix $\mathbf{G}$ aus Definition 3.3.1 eine Generatormatrix von $\mathrm{SimAug}(\mathfrak{k})$*. Der Code* $\mathrm{SimAug}(\mathfrak{k})$ *hat den konjugierten Umriss $(k+1, k)$ und den in Tabelle 3.3.1 gezeigten symmetrisierten Gewichtszähler. Dabei sind die beiden Typen H_ψ und pH_ψ für jeden auftretenden $\mathfrak{k}$-Typ ψ auszuwerten.*[39] *Die $(q-1)$-fache Wiederholung des Simplex-Codes* $\mathrm{Sim}(k, R)$ *ist ein Teilcode von* $\mathrm{SimAug}(\mathfrak{k})$ *vom Index q.*

Beweis. Die ersten k Zeilen erzeugen eine $(q-1)$-fache Wiederholung des Simplex-Codes $\mathrm{Sim}(k, R)$, insbesondere ist das Erzeugnis frei vom Rang k. Angenommen, die $(k+1)$-te Zeile $\mathbf{c}$ von $\mathbf{G}$ ist in diesem Teilcode $\mathcal{C}$ enthalten. Weil $\mathbf{c}$ ein Torsionsvektor ist, wäre dann $\varphi^{-1}(\mathbf{c})$ im Torsionscode $\mathcal{C}^{(2)}$ enthalten,[40] einer $(q-1)q^{k-1}$-fachen Wiederholung des Simplex-Codes $\mathrm{Sim}(k, \mathbb{F}_q)$.

Nach Voraussetzung existiert ein Punkt x, der nicht in $\mathfrak{k}$ enthalten ist. An den zugehörigen Positionen hat $\varphi^{-1}(\mathbf{c})$ die $q-1$ paarweise verschiedenen Einträge $\varphi^{-1}(R^*p)$. Im Fall $q \neq 2$, d.h. $R \neq \mathbb{Z}_4$, ist das ein Widerspruch. Sei also $R = \mathbb{Z}_4$. Die Codewörter des Simplex-Codes $\mathrm{Sim}(k, \mathbb{F}_2)$ sind das Nullwort sowie die charakteristischen Vektoren der affinen Teilebenen von $\mathrm{PG}(\mathbb{F}_2^k)$. Demnach ist $\mathfrak{k}$ im Widerspruch zur Voraussetzung entweder die volle Punktmenge oder das Komplement einer affinen Teilebene von $\mathrm{PHG}(\mathbb{Z}_4^k)$, also eine Hyperebenenklasse.

Jedes Codewort $\mathbf{c} \in \mathrm{SimAug}(\mathfrak{k})$ hat einen eindeutigen Informationsvektor $(\mathbf{y}, a)$ mit $\mathbf{c} = (\mathbf{y}, a)\mathbf{G}$, $\mathbf{y} \in R^k$ und $a \in T$, wobei T die Teichmüller-Menge von R bezeichnet. Der

[39] Es kann passieren, dass der Eintrag „#Codewörter" für den Typ pH_ψ für einen festen $\mathfrak{k}$-Typ ψ eine echt rationale Zahl ist. Nach der Summation über alle $\mathfrak{k}$-Typen verbleiben aber nur ganze Zahlen.

[40] Die Abbildung φ wurde in Abschnitt 2.2 definiert.

Tabelle 3.3.1.: Symmetrisierter Gewichtszähler des Codes SimAug($\mathfrak{k}$)

Typ H_ψ	#Codewörter	$(q-1)^2 q A_\psi$
	ω_0	$(q-1)q^{2k-2}$
	ω_1	$(q-1)q^{k-2}(q^{k-1}-1) - ((q-1)\psi_2 - \psi_1)$
	ω_2	$q^{k-2}(q^{k-1}-1) + ((q-1)\psi_2 - \psi_1)$
	w_{hom}	$(q-1)q^{k-1}(q^k-1) - q((q-1)\psi_2 - \psi_1)$
Typ pH_ψ	#Codewörter	$\frac{1}{q^{k-1}}(q-1)^2 A_\psi$
	ω_0	0
	ω_1	$q^{k-1}(q^k - q^{k-1} - 1) - ((q-1)(\psi_1+\psi_2) - \psi_0)$
	ω_2	$q^{2(k-1)} + ((q-1)(\psi_1+\psi_2) - \psi_0)$
	w_{hom}	$(q-1)q^{k-1}(q^k-1) - q^{k-1} + q((q-1)(\psi_1+\psi_2) - \psi_0)$
Typ $0'$	#Codewörter	$q-1$
	ω_0	0
	ω_1	$q^{k-1}(q^k-1) - (q-1)\#\mathfrak{k}$
	ω_2	$(q-1)\#\mathfrak{k}$
	w_{hom}	$q^k(q^k-1) - (q-1)q\#\mathfrak{k}$
Typ S	#Codewörter	$q^k(q^k-1)$
	ω_0	$(q-1)q^{2k-2}$
	ω_1	$(q-1)q^{k-2}(q^{k-1}-1)$
	ω_2	$q^{k-2}(q^{k-1}-1)$
	w_{hom}	$(q-1)q^{k-1}(q^k-1)$
Typ pS	#Codewörter	$q^k - 1$
	ω_0	0
	ω_1	$(q-1)q^{2k-2}$
	ω_2	$q^{k-1}(q^{k-1}-1)$
	w_{hom}	$(q-1)q^{2k-1}$
Typ 0	#Codewörter	1
	ω_0	0
	ω_1	0
	ω_2	$q^{k-1}(q^k-1)$
	w_{hom}	0

Teilcode $\mathcal{C}$ besteht genau aus den Codewörtern mit einem Eintrag $a = 0$ im Informationsvektor. Dies ergibt die Typen S, pS und 0 in Tabelle 3.3.1. Sei also $a \neq 0$. Das an den mit einem Punkt x assoziierten $q-1$ Positionen stehende Teilwort von $\mathbf{c}$ bezeichnen wir mit $\mathbf{c}_x$. Zur blockweisen Berechnung von $w_{\mathrm{sym}}(\mathbf{c})$ überlegen wir uns die Formel

$$w_{\mathrm{sym}}(\mathbf{c}_x) = \begin{cases} (q-1)w_{\mathrm{sym}}(\mathbf{y} \cdot \kappa(x)) & \text{falls } x \in \mathfrak{k}, \\ \sum_{a \in R^*p} w_{\mathrm{sym}}(\mathbf{y} \cdot \kappa(x) + a) & \text{falls } x \notin \mathfrak{k}. \end{cases} \tag{3.6}$$

Wir unterscheiden nun 3 Fälle:

(i) Der Vektor $\mathbf{y}$ ist torsionsfrei:
Sei H die Hyperebene $\mathbf{y}^\perp$ und $(\psi_0, \psi_1, \psi_2) = \mathbf{a}_{\mathfrak{k}}(H)$ der $\mathfrak{k}$-Typ von H. Es ergeben sich die folgenden 6 Fälle für das symmetrisierte Gewicht von $\mathbf{c}_x$; der Exponent gibt jeweils an für wie viele Punkte x der entsprechende Fall auftritt:

	$x \in H$	$x \in [H] \setminus H$	$x \in \mathcal{P} \setminus [H]$
$x \in \mathfrak{k}$	$(0, 0, q-1)^{\psi_2}$	$(0, q-1, 0)^{\psi_1}$	$(q-1, 0, 0)^{\psi_0}$
$x \notin \mathfrak{k}$	$(0, q-1, 0)^{\#H-\psi_2}$	$(0, q-2, 1)^{\#([H]\setminus H)-\psi_1}$	$(q-1, 0, 0)^{\#(\mathcal{P}\setminus[H])-\psi_0}$

Wir erklären exemplarisch den Eintrag im Fall $x \notin \mathfrak{k}$, $x \in [H] \setminus H$: Die Anzahl $\#([H] \setminus H) - \psi_1$ solcher Punkte x folgt direkt aus der Definition des Typs. Wegen $x \notin \mathfrak{k}$ benutzen wir den zweiten Fall in Formel (3.6), und wegen $x \in [H] \setminus H$ gilt $\mathbf{y} \cdot \kappa(x) \in R^*p$. Damit ist $\mathbf{y} \cdot \kappa(x) + a$ genau im Fall $a = -\mathbf{y} \cdot \kappa(x)$ gleich 0, in den anderen $(q-2)$ Fällen ergibt sich jeweils ein Element aus R^*p. Dies zeigt $w_{\mathrm{sym}}(\mathbf{c}_x) = (0, q-2, 1)$.

Auf diese Art erhalten wir den Typ H_ψ in Tabelle 3.3.1. Die Anzahl der Codewörter folgt dabei so: Je $q(q-1)$ Informationsvektoren $\mathbf{y}$ definieren dieselbe Hyperebene $H = \mathbf{y}^\perp$, und für die Wahl von $a \in T \setminus \{0\}$ gibt es $q-1$ Möglichkeiten. Damit repräsentiert jede Hyperebene H je $q(q-1)^2$ Codewörter.

(ii) Der Vektor $\mathbf{y}$ ist ein Torsionsvektor, aber nicht der Nullvektor:
Es existiert ein torsionsfreier Vektor $\mathbf{z}$ mit $\mathbf{y} = p\mathbf{z}$. Wir bezeichnen die Hyperebene $\mathbf{z}^\perp$ mit H. Ähnlich wie zuvor erhalten wir 4 Fälle für $w_{\mathrm{sym}}(\mathbf{c}_x)$:

	$x \in [H]$	$x \in \mathcal{P} \setminus [H]$
$x \in \mathfrak{k}$	$(0, 0, q-1)^{\psi_1+\psi_2}$	$(0, q-1, 0)^{\psi_0}$
$x \notin \mathfrak{k}$	$(0, q-1, 0)^{\#[H]-(\psi_1+\psi_2)}$	$(0, q-2, 1)^{\#(\mathcal{P}\setminus[H])-\psi_0}$

Dies liefert den Typ pH_ψ in Tabelle 3.3.1. Für die Anzahl der Codewörter ist hier zusätzlich zu beachten, dass für je q^k verschiedene torsionsfreie Vektoren $\mathbf{z}$ die Torsionsvektoren $\mathbf{y} = p\mathbf{z}$ übereinstimmen.

(iii) Der Vektor $\mathbf{y}$ ist der Nullvektor:
Hier sind nur die folgenden beiden Fälle zu unterscheiden:

$x \in \mathfrak{k}$	$(0, 0, q-1)^{\#\mathfrak{k}}$
$x \notin \mathfrak{k}$	$(0, q-1, 0)^{\#(\mathcal{P}\setminus\mathfrak{k})}$

Dies liefert den Typ $0'$ in Tabelle 3.3.1. Die Anzahl der Codewörter ist gegeben durch die Anzahl $q-1$ der Wahlmöglichkeiten für $a \in T \setminus \{0\}$. □

Bemerkung 3.3.3

(a) Sei SimAug($\mathfrak{k}$) ein $[n,(k+1,k),d]_R$-Code. Weil die $(q-1)$-fache Wiederholung des Simplex-Codes Sim(k,R) als Teilcode vom Index q in $\mathcal{C}$ enthalten ist, gilt $d \le d' = (q-1)d_{\hom}(\mathrm{Sim}(k,R))$. Folglich ist es wie für die dualisierten Kerdock-Codes in Abschnitt 3.2.2 möglich, den Code SimAug($\mathfrak{k}$) durch Konstruktion X (siehe Abschnitt 2.2.6) mit dem q-elementigen $(n',q,qn')_R$-Wiederholungscode $R(p,\dots,p)$ der Länge $n' = \lceil (d'-d)/q \rceil$ als Hilfscode zu verlängern, um SimAug($\mathfrak{k}$) zu einem $(n+n',q^{2k+1},d')_R$-Code SimLen($\mathfrak{k}$) (*verlängerter Simplex-Code*, *lengthened Simplex code*) zu verbessern. Führt man diese Konstruktion für verschiedene Punktmengen $\mathfrak{k}$ durch, so haben die resultierenden Codes SimLen($\mathfrak{k}$) alle dieselbe homogene Minimaldistanz d', aber im Allgemeinen verschiedene Längen $n+n'$. Je höher die homogene Minimaldistanz d von SimAug($\mathfrak{k}$) ist, desto kürzer (und damit besser) ist der resultierende Code SimLen($\mathfrak{k}$).

(b) In [72] wurde für den $\mathbb{Z}_4$-linearen Fall eine ähnliche Konstruktion angegeben. Die symmetrisierten Gewichte des Codes SimAug($\mathfrak{k}$) können aus [72, Th. 1] abgelesen werden; allerdings fehlen im Vergleich zu Satz 3.3.2 die Anzahlen der jeweiligen Codewörter bzw. Hyperebenen. Die Codes werden dort pauschal um eine Torsionsspalte verlängert und nicht wie oben diskutiert in Abhängigkeit von d um n' Spalten. Der weiter unten in Beispiel 3.3.10 diskutierte $\mathbb{Z}_4$-lineare BTKL-Code $\hat{S}_{2,4}$ kann damit beispielsweise nicht erzeugt werden, denn dieser erfordert das Anhängen von zwei Torsionsspalten.

Lemma 3.3.4 *Sei $r,k \in \mathbb{N}$, $k \ge 3$ und $q = 2^r$. Sei $\mathfrak{k}$ eine der Punktmengen $\mathfrak{T}_{q,k,s}$ oder $\mathfrak{T}^*_{q,k,s}$ mit*

$$s \in \begin{cases} \{0,2,4,\dots,(k-1)r-2\} & \text{falls } k \text{ ungerade,} \\ \{r,r+2,r+4,\dots,(k-1)r-2\} & \text{falls } k \text{ gerade.} \end{cases}$$

Unter den Möglichkeiten für $\mathfrak{k}$ wird die homogene Minimaldistanz von SimAug($\mathfrak{k}$) *für*

$$\mathfrak{k} = \begin{cases} \mathfrak{T}^*_{2,k,0} & \text{falls } q=2 \text{ und } k \text{ ungerade,} \\ \mathfrak{T}^*_{2,k,1} & \text{falls } q=2 \text{ und } k \text{ gerade,} \\ \mathfrak{T}_{q,k,(k-3)r} & \text{falls } q \ge 4 \end{cases}$$

maximal.

Beweis. Laut Satz 3.1.8(a) gibt es genau zwei verschiedene $\mathfrak{T}_{q,k,s}$-Typen, diese wurden in Tabelle 3.1.1 mit H_- und H_+ bezeichnet. In Tabelle 3.3.1 liefert unter H_ψ der Typ H_+ das kleinere homogene Gewicht von SimAug($\mathfrak{T}_{q,k,s}$), dieses ist

$$w_1(s) = q^{k-1}(q-1)(q^k-1) + q \cdot 2^{s/2}(2^{s/2} - q^{\frac{k-1}{2}}).$$

Für $0 \leq s \leq (k-1)r-4$ gilt

$$w_1(s+2) - w_1(s) = 2^{s/2}q(3 \cdot 2^{s/2} - q^{\frac{k-1}{2}}) \leq 2^{s/2}q\left(\frac{3}{4}q^{\frac{k-1}{2}} - q^{\frac{k-1}{2}}\right) < 0,$$

und damit ist w_1 als Funktion in s streng monoton fallend.

Die Typen H_+ und H_- liefern unter pH_ψ in Tabelle 3.3.1 dasselbe homogene Gewicht

$$w_2(s) = q^{k-1}(q-1)(q^k-1) - q^{k-1} + 2^s q.$$

Dies ist eine streng monoton steigende Funktion in s.

Man überprüft, dass für $s = (k-3)r$ die beiden Gewichte $w_1(s)$ und $w_2(s)$ denselben Wert $q^{2k} - q^{2k-1} - q^k + q^{k-2}$ liefern, und dass dieses Gewicht wirklich die homogene Minimaldistanz von $\mathrm{SimAug}(\mathfrak{T}_{q,k,s})$ ist. Damit ist unter den Punktmengen $\mathfrak{T}_{q,k,s}$ die homogene Minimaldistanz für $s = (k-3)r$ maximal.

Wir betrachten nun die Punktmengen $\mathfrak{T}^*_{q,k,s}$. Nach Satz 3.2.5 stimmt das Spektrum der Punktmenge $\mathfrak{T}^*_{q,k,(k-1)r-2}$ mit dem Spektrum der bereits betrachteten Punktmenge $\mathfrak{T}_{q,k,(k-1)r-2}$ überein, so dass wir im Folgenden $s \leq (k-1)r-4$ voraussetzen dürfen. In $\mathrm{SimAug}(\mathfrak{T}^*_{q,k,s})$ liefert der Typ $0'$ das homogene Gewicht $\frac{1}{2}(q^k-1)(q^k + 2^{s/2}q^{\frac{k+1}{2}})$. Mit $s \leq (k-1)r-4$ können wir dieses Gewicht nach oben abschätzen durch $\frac{5}{8}(q^{2k}-q^k)$. Für $q \geq 4$ ist diese Zahl kleiner als die oben ermittelte homogene Minimaldistanz von $\mathrm{SimAug}(\mathfrak{T}_{q,k,(k-3)r})$. Es verbleibt also, die Punktmengen $\mathfrak{T}^*_{2,k,s}$ zu untersuchen.

Laut Satz 3.2.3(a) gibt es genau zwei verschiedene $\mathfrak{T}^*_{2,k,s}$-Typen, welche in Tabelle 3.2.1 mit H^*_- und H^*_+ bezeichnet wurden. In Tabelle 3.3.1 liefert unter H_ψ der Typ H^*_+ das kleinere homogene Gewicht von $\mathrm{SimAug}(\mathfrak{T}^*_{2,k,s})$, dieses ist

$$w(s) = 2^{2k-1} - 2^{k-1} - 2^{\frac{s+k-1}{2}}.$$

Unter $2H_\psi$ liefern die beiden Typen H^*_- und H^*_+ dasselbe homogene Gewicht. Dieses stimmt mit $w(s)$ überein. Weiter erhalten wir unter $0'$ das homogene Gewicht $2^{2k-1} - 2^{k-1} + (2^k-1)2^{\frac{s+k-1}{2}}$, welches sicher größer als $w(s)$ ist. Die homogene Minimaldistanz von $\mathrm{SimAug}(\mathfrak{T}^*_{2,k,s})$ ist also $w(s)$ und wird für den kleinsten zulässigen Wert von s maximal, d.h. für $s=0$ falls k ungerade und für $s=1$ falls k gerade. Ein Vergleich der resultierenden Minimaldistanz mit der Minimaldistanz von $\mathrm{SimAug}(\mathfrak{T}_{2,k,k-3})$ liefert

$$d_{\hom}(\mathrm{SimAug}(\mathfrak{T}^*_{2,k,s})) - d_{\hom}(\mathrm{SimAug}(\mathfrak{T}_{2,k,k-3})) = w(s) - w_1(k-3) = 2^{k-2} - 2^{\frac{s+k-1}{2}}.$$

Diese Differenz ist genau dann nicht negativ, wenn $s \leq k-3$ ist. Damit ist alles gezeigt.□

Bemerkung 3.3.5 Der Beweis von Lemma 3.3.4 zeigt auch, dass unter den betrachteten Punktmengen $\mathfrak{k}$ die homogene Minimaldistanz von $\mathrm{SimAug}(\mathfrak{k})$ außer in den beiden Fällen $(q,k) \in \{(2,3),(2,4)\}$ *genau* für die angegebenen Punktmengen maximal wird. Bis auf Isomorphie stimmt dies auch in den beiden Sonderfällen. Denn in Bemerkung 3.2.6 haben wir gesehen, dass die eindeutige Punktmenge $\mathfrak{T}_{2,3,0}$ zu $\mathfrak{T}^*_{2,3,0}$ und die eindeutige Punktmenge $\mathfrak{T}_{2,4,1}$ zu $\mathfrak{T}^*_{2,4,1}$ isomorph ist.

Tabelle 3.3.2.: Lee-Gewichtszähler des Codes $\hat{\mathcal{S}}_{2,k}$ für k ungerade

Typ	#Codewörter	w_{hom}
0	1	0
$H_+, 2H, S$	$2^{2k+1} - 3 \cdot 2^k + 1$	$2^{2k-1} - 2^{k-1}$
$2S$	$2^k - 1$	2^{2k-1}
H_-	$2^{k+1} - 2$	$2^{2k-1} - 2^{k-1} + 2^{\frac{3k-3}{2}}$
$0'$	1	$2^{2k-1} - 2^{k-1} + 2^{\frac{3k-1}{2}}$

Tabelle 3.3.3.: Lee-Gewichtszähler des Codes $\hat{\mathcal{S}}_{2,k}$ für k gerade

Typ	#Codewörter	w_{hom}
0	1	0
$H_+, 2H, S$	$2^{2k+1} - 5 \cdot 2^k + 3$	$2^{2k-1} - 2^{k-1}$
$2S$	$2^k - 1$	2^{2k-1}
H_-	$2^{k+2} - 4$	$2^{2k-1} - 2^{k-1} + 2^{\frac{3k-4}{2}}$
$0'$	1	$2^{2k-1} - 2^{k-1} + 2^{\frac{3k}{2}}$

Die im Sinne von Lemma 3.3.4 bestmögliche Erweiterung der $(q-1)$-fachen Wiederholung des Simplex-Codes $\mathrm{Sim}(k, R)$ bezeichnen wir nun mit $\hat{\mathcal{S}}_{q,k}$: Es sei

$$\hat{\mathcal{S}}_{q,k} = \begin{cases} \mathrm{SimLen}(\mathfrak{T}^*_{2,k,0}) & \text{falls } q = 2 \text{ und } k \text{ ungerade,} \\ \mathrm{SimLen}(\mathfrak{T}^*_{2,k,1}) & \text{falls } q = 2 \text{ und } k \text{ gerade,} \\ \mathrm{SimLen}(\mathfrak{T}_{q,k,(k-3)r}) & \text{falls } q \geq 4 \text{ gerade.} \end{cases}$$

Satz 3.3.6

(a) Der Code $\mathrm{SimLen}(\mathfrak{T}^*_{2,k,s})$ *hat die Parameter*

$$\left[2^{2k-1} - 2^{k-1} + 2^{\frac{k-3+s}{2}}, \quad (k+1, k), \quad 2^{2k-1} - 2^{k-1}\right]_{\mathbb{Z}_4}.$$

Tabelle 3.3.4 zeigt den symmetrisierten Gewichtszähler.

(b) Für ungerades $k \geq 3$ *hat* $\hat{\mathcal{S}}_{2,k}$ *die Parameter*

$$\left[2^{2k-1} - 2^{k-1} + 2^{\frac{k-3}{2}}, \quad (k+1, k), \quad 2^{2k-1} - 2^{k-1}\right]_{\mathbb{Z}_4}.$$

Tabelle 3.3.2 zeigt den Lee-Gewichtszähler.

(c) Für gerades $k \geq 4$ *hat* $\hat{\mathcal{S}}_{2,k}$ *die Parameter*

$$\left[2^{2k-1} - 2^{k-1} + 2^{\frac{k-2}{2}}, \quad (k+1, k), \quad 2^{2k-1} - 2^{k-1}\right]_{\mathbb{Z}_4}.$$

Tabelle 3.3.3 zeigt den Lee-Gewichtszähler.

Tabelle 3.3.4.: Symmetrisierter Gewichtszähler des Codes SimLen($\mathfrak{T}^*_{2,k,s}$)

Typ H_+, S	#Codewörter	$(2^k-1)(2^{k+1}-2^{s+1})$
	ω_0	2^{2k-2}
	ω_1	$2^{2k-3}-2^{k-2}$
	ω_2	$2^{2k-3}-2^{k-2}+2^{\frac{k-3+s}{2}}$
	w_{hom}	$2^{2k-1}-2^{k-1}$
Typ H_-	#Codewörter	$(2^k-1)2^{s+1}$
	ω_0	2^{2k-2}
	ω_1	$2^{2k-3}-2^{k-2}+2^{\frac{3k-5-s}{2}}$
	ω_2	$2^{2k-3}-2^{k-2}+2^{\frac{k-3+s}{2}}-2^{\frac{3k-5-s}{2}}$
	w_{hom}	$2^{2k-1}-2^{k-1}+2^{\frac{3k-3-s}{2}}$
Typ $2H_\pm$	#Codewörter	2^k-1
	ω_0	0
	ω_1	$2^{2k-2}-2^{k-2}$
	ω_2	$2^{2k-2}-2^{k-2}+2^{\frac{k-3+s}{2}}$
	w_{hom}	$2^{2k-1}-2^{k-1}$
Typ $0'$	#Codewörter	1
	ω_0	0
	ω_1	$2^{2k-2}-2^{k-2}-2^{\frac{3k-1+s}{2}}$
	ω_2	$2^{2k-2}-2^{k-2}-2^{\frac{3k-3+s}{2}}+2^{\frac{k-3+s}{2}}$
	w_{hom}	$2^{2k-1}-2^{k-1}+2^{\frac{3k-1+s}{2}}$
Typ $2S$	#Codewörter	2^k-1
	ω_0	0
	ω_1	2^{2k-2}
	ω_2	$2^{2k-2}-2^{k-1}+2^{\frac{k-3+s}{2}}$
	w_{hom}	2^{2k-1}
Typ 0	#Codewörter	1
	ω_0	0
	ω_1	0
	ω_2	$2^{2k-1}-2^{k-1}+2^{\frac{k-3+s}{2}}$
	w_{hom}	0

Tabelle 3.3.5.: Homogener Gewichtszähler des Codes $\hat{\mathcal{S}}_{q,k}$ für $q \geq 4$

Typ	#Codewörter	w_{hom}
$H_+, 2H, S$	$\frac{1}{2}q^{2k+1} + q^{2k} - \frac{1}{2}q^{2k-1} + \frac{3}{2}q^{k+1}$ $-2q^k - \frac{1}{2}q^{k-1} - q + 1$	$q^{2k} - q^{2k-1} - q^k + q^{k-1}$
H_-	$\frac{1}{2}q^{2k+1} - q^{2k} + \frac{1}{2}q^{2k-1} - \frac{1}{2}q^{k+1} + q^k - \frac{1}{2}q^{k-1}$	$q^{2k} - q^{2k-1} - q^k + 3q^{k-1}$
$2S$	$q^k - 1$	$q^{2k} - q^{2k-1}$
$0'$	$q - 1$	$q^{2k} - q^{2k-2} - q^k + q^{k-1}$
0	1	0

Beweis. Aus Satz 3.2.3(a) erhalten wir das Spektrum von $\mathfrak{T}^*_{2,k,s}$, und mit Satz 3.3.2 berechnen wir daraus den symmetrisierten Gewichtszähler von $\text{SimAug}(\mathfrak{T}^*_{2,k,s})$. Aus dem Beweis von Lemma 3.3.4 wissen wir, dass $\text{SimAug}(\mathfrak{T}^*_{2,k,s})$ die minimale Lee-Distanz $2^{2k-1} - 2^{k-1} - 2^{\frac{s+k-1}{2}}$ hat. Beim Übergang zu $\text{SimLen}(\mathfrak{T}^*_{2,k,s})$ wird der Code durch Konstruktion X also um $2^{\frac{s+k-3}{2}}$ Symbole verlängert. Die im Simplex-Code liegenden Codewörter werden dabei um Symbole 0, die restlichen Codewörter um Symbole 2 verlängert. Damit berechnet man nun weiter den in Tabelle 3.3.4 angegebenen symmetrisierten Gewichtszähler sowie die Parameter von $\text{SimLen}(\mathfrak{T}^*_{2,k,s})$. Durch Spezialisieren erhält man nun für $s = 0$ die Aussagen in Teil (b), und für $s = 1$ die Aussagen in Teil (c). □

Satz 3.3.7 *Sei $q \geq 4$ eine Zweierpotenz und $k \geq 3$. Der Code $\hat{\mathcal{S}}_{q,k}$ hat die Parameter*

$$\left[q^{2k-1} - q^{k-1} + q^{k-2} - q^{k-3}, \quad (k+1, k), \quad q^{2k} - q^{2k-1} - q^k + q^{k-1}\right]_R .$$

Der symmetrisierte Gewichtszähler ist in Tabelle 3.3.6 und der homogene Gewichtszähler in Tabelle 3.3.5 angegeben.

Beweis. Aus Satz 3.1.8(a) erhalten wir das Spektrum von $\mathfrak{T}_{q,k,(k-3)r}$, und mit Satz 3.3.2 berechnen wir daraus den symmetrisierten Gewichtszähler von $\text{SimAug}(\mathfrak{T}_{q,k,(k-3)r})$. Aus dem Beweis von Lemma 3.3.4 wissen wir, dass $\text{SimAug}(\mathfrak{T}_{q,k,(k-3)r})$ die homogene Minimaldistanz $q^{2k} - q^{2k-1} - q^k + q^{k-2}$ hat. Durch Konstruktion X werden beim Übergang zu $\text{SimLen}(\mathfrak{T}_{q,k,(k-3)r})$ die in der $(q-1)$-fachen Wiederholung des Simplex-Codes liegenden Codewörter also um $q^{k-2} - q^{k-3}$ Symbole 0 verlängert und die restlichen Codewörter um $q^{k-2} - q^{k-3}$ Symbole der Höhe 1. Damit kann weiter der in Tabelle 3.3.6 angegebene symmetrisierte Gewichtszähler von $\hat{\mathcal{S}}_{q,k}$ abgeleitet werden. An diesem liest man schließlich die Parameter und den homogenen Gewichtszähler ab. □

Bemerkung 3.3.8

(a) Die für $q \geq 4$ gemachten Aussagen aus Satz 3.3.7 sind auch im Fall $q = 2$ (d.h. $r = 1$) für die Codes $\text{SimLen}(\mathfrak{T}_{2,k,k-3})$ richtig. Aufgrund von Bemerkung 3.2.6 sind für $k \in \{3, 4\}$ die beiden Codes $\text{SimLen}(\mathfrak{T}_{2,k,k-3})$ und $\hat{\mathcal{S}}_{2,k}$ isomorph. Für $k \geq 5$ ist dies nach Lemma 3.3.4 nicht mehr der Fall, hier sind die Codes $\hat{\mathcal{S}}_{2,k}$ besser.

(b) Die Codes $\hat{\mathcal{S}}_{q,k}$ verallgemeinern die bereits in [90] veröffentlichten Codes, diese bilden den Spezialfall $k = 3$.

Tabelle 3.3.6.: Symmetrisierter Gewichtszähler des Codes $\hat{\mathcal{S}}_{q,k}$ für $q \geq 4$

Typ H_+, S	#Cw.	$\frac{1}{2}q^{2k+1} + q^{2k} - \frac{1}{2}q^{2k-1} + \frac{1}{2}q^{k+1} - q^k - \frac{1}{2}q^{k-1}$
	ω_0	$q^{2k-1} - q^{2k-2}$
	ω_1	$q^{2k-2} - q^{2k-3} - q^{k-1} + q^{k-2}$
	ω_2	$q^{2k-3} - q^{k-3}$
	w_{hom}	$q^{2k} - q^{2k-1} - q^k + q^{k-1}$
Typ H_-	#Cw.	$\frac{1}{2}q^{2k+1} - q^{2k} + \frac{1}{2}q^{2k-1} - \frac{1}{2}q^{k+1} + q^k - \frac{1}{2}q^{k-1}$
	ω_0	$q^{2k-1} - q^{2k-2}$
	ω_1	$q^{2k-2} - q^{2k-3} - q^{k-1} + 3q^{k-2}$
	ω_2	$q^{2k-3} - 2q^{k-2} - q^{k-3}$
	w_{hom}	$q^{2k} - q^{2k-1} - q^k + 3q^{k-1}$
Typ $2H$	#Cw.	$q^{k+1} - q^k - q + 1$
	ω_0	0
	ω_1	$q^{2k-1} - q^{2k-2} - q^{k-1} + q^{k-2}$
	ω_2	$q^{2k-2} - q^{k-3}$
	w_{hom}	$q^{2k} - q^{2k-1} - q^k + q^{k-1}$
Typ $0'$	#Cw.	$q - 1$
	ω_0	0
	ω_1	$q^{2k-1} - q^{2k-3} - q^{k-1} + q^{k-2}$
	ω_2	$q^{2k-3} - q^{k-3}$
	w_{hom}	$q^{2k} - q^{2k-2} - q^k + q^{k-1}$
Typ $2S$	#Cw.	$q^k - 1$
	ω_0	0
	ω_1	$q^{2k-1} - q^{2k-2}$
	ω_2	$q^{2k-2} - q^{k-1} + q^{k-2} - q^{k-3}$
	w_{hom}	$q^{2k} - q^{2k-1}$
Typ 0	#Cw.	1
	ω_0	0
	ω_1	0
	ω_2	$q^{2k-1} - q^{k-1} + q^{k-2} - q^{k-3}$
	w_{hom}	0

3.3.1. Beispiele

Beispiel 3.3.9 Der Code $\hat{S}_{2,3}$ hat die Parameter $[29,(4,3),28]_{\mathbb{Z}_4}$ und den symmetrisierten Gewichtszähler

$$X_2^{29} + (98X_0^{16}X_1^6X_2^7 + 7X_1^{14}X_2^{15}) + 7X_1^{16}X_2^{13} + 14X_0^{16}X_1^{10}X_2^3 + X_1^{22}X_2^7.$$

Eine mögliche Generatormatrix ist

$$\begin{pmatrix}
1\,1\,1\,1 & 0\,2\,2\,0 & 0\,2\,2\,0 & 2\,0\,0\,2 & 1\,1\,1\,1 & 1\,1\,1\,1 & 1\,1\,1\,1 & 0\\
2\,0\,2\,0 & 1\,1\,1\,1 & 2\,0\,2\,0 & 1\,1\,1\,1 & 0\,2\,0\,2 & 3\,1\,1\,3 & 3\,1\,3\,1 & 0\\
2\,2\,0\,0 & 2\,2\,0\,0 & 1\,1\,1\,1 & 3\,3\,1\,1 & 3\,3\,1\,1 & 0\,0\,2\,2 & 3\,1\,1\,3 & 0\\
2\,2\,2\,0 & 2\,2\,2\,0 & 2\,2\,2\,0 & 2\,2\,2\,0 & 2\,2\,2\,0 & 2\,2\,2\,0 & 2\,2\,2\,0 & 2
\end{pmatrix}.$$

Das Gray-Bild hat die Parameter $(58, 2^7, 28)_2$ und den Hamming-Gewichtszähler

$$1 + 105X^{28} + 7X^{32} + 14X^{36} + X^{44}.$$

Dieser Code ist BTL [125, Th. 3.7].

Der Code $\hat{\mathcal{S}}_{2,3}$ wurde zuerst 2009 von Johannes Zwanzger gefunden (siehe auch [132]) und in [90] computerfrei beschrieben.

Beispiel 3.3.10 Der Code $\hat{\mathcal{S}}_{2,4}$ hat die Parameter $[122,(5,4),120]_{\mathbb{Z}_4}$ und den symmetrisierten Gewichtszähler

$$X_2^{122} + (420X_0^{64}X_1^{28}X_2^{30} + 15X_1^{60}X_2^{62}) + 15X_1^{64}X_2^{58} + 60X_0^{64}X_1^{36}X_2^{22} + X_1^{92}X_2^{30}.$$

Das Gray-Bild hat die Parameter $(244, 2^9, 120)_2$ und den Hamming-Gewichtszähler

$$1 + 435X^{120} + 15X^{128} + 60X^{136} + X^{184}.$$

Die Internetseite [46] zeigt für die größtmögliche Minimaldistanz eines $[244, 9]_{\mathbb{F}_2}$-Codes das Intervall 119–120. Damit ist der Code $\hat{\mathcal{S}}_{2,4}$ BTKL. Die obere Schranke 120 erhält man dabei so: Für einen $\mathbb{F}_2$-linearen Code der Dimension 9 und der Minimaldistanz 121 gilt aufgrund der Griesmer-Schranke $n \geq \sum_{i=0}^{8} \lceil 121/2^i \rceil = 245$.

Vier weitere Isomorphieklassen von $\mathbb{Z}_4$-lineare Codes mit denselben Parametern wie $\hat{\mathcal{S}}_{2,4}$ wurden bereits in [91, 92] veröffentlicht. Sie entstehen als zweifaches Residuum des dualisierten Kerdock-Codes $\hat{\mathcal{K}}_{5+1}^*$.

Beispiel 3.3.11 Der Code $\hat{\mathcal{S}}_{2,5}$ hat die Parameter $[498,(6,5),496]_{\mathbb{Z}_4}$ und den symmetrisierten Gewichtszähler

$$X_2^{498} + (1922X_0^{256}X_1^{120}X_2^{122} + 31X_1^{248}X_2^{250}) + 31X_1^{256}X_2^{242} + 62X_0^{256}X_1^{152}X_2^{90} + X_1^{312}X_2^{186}.$$

Das Gray-Bild hat die Parameter $(996, 2^{11}, 496)_2$ und den Hamming-Gewichtszähler

$$1 + 1953X^{496} + 31X^{512} + 62X^{560} + X^{624}.$$

Dieser Code ist leider zu lang, um ihn direkt mit den Tabellen für lineare Codes vergleichen zu können. Die Parameter sehen aber sehr vielversprechend aus: Wenn ein linearer $[996, 11, 496]_{\mathbb{F}_2}$-Code existiert, so über das Residuum in einem Codewort von minimalem Gewicht auch ein $[500, 10, 248]_{\mathbb{F}_2}$-Code und durch nochmaliges Bilden des Residuums in einem Codewort von minimalem Gewicht auch ein $[252, 9, 124]_{\mathbb{F}_2}$-Code. Ein solcher Code wäre laut [46] distanzoptimal.

Beispiel 3.3.12 Der Code $\hat{\mathcal{S}}_{4,3}$ hat die Parameter $[1011, (4, 3), 3024]_{\mathrm{GR}(16,4)}$ und den symmetrisierten Gewichtszähler

$$X_2^{1011} + (11592X_0^{768}X_1^{180}X_2^{63} + 189X_1^{756}X_2^{255}) + 4536X_0^{768}X_1^{188}X_2^{55} + 63X_1^{768}X_2^{243} + 3X_1^{948}X_2^{63}.$$

Das Gray-Bild hat die Parameter $(4044, 4^7, 3024)_4$ und den Hamming-Gewichtszähler

$$1 + 11781X^{3024} + 4536X^{3056} + 63X^{3072} + 3X^{3792}.$$

Auch dieser Code ist leider für einen Tabellenvergleich zu lang. Er wurde bereits in [90] veröffentlicht.

4. Ausblick

In dieser Arbeit wurden vier neue Serien von linearen Codes über Galois-Ringen der Charakteristik 4 konstruiert. Die Qualität der Codes insbesondere im $\mathbb{Z}_4$-linearen Fall wird durch Tabelle 1.4.1 belegt. In allen Fällen, wo ein Tabellenvergleich möglich ist, sind die Codes entweder BTL oder BTKL. Diese Resultate werfen jedoch auch eine Reihe von Fragen auf, die Gegenstand zukünftiger Untersuchungen sein sollten und auf die hier zum Abschluss noch kurz eingegangen wird.

(a) Es ist kein einziger BTL- oder BTKL-Code als Gray-Bild eines ringlinearen Codes in ungerader Charakteristik bekannt. Eine denkbare Erklärung hierfür ist, dass die meisten bekannten BTL- und BTKL-Codes in Charakteristik 4 auf die eine oder andere Weise von Teichmüller-Mengen herrühren, deren Eigenschaften in gerader und ungerader Charakteristik sehr unterschiedlich sind. Andererseits gibt es mit den $\mathbb{Z}_4$-linearen Preparata-Codes unendlich viele BTL-Codes in Charakteristik 4, so dass es wenig wahrscheinlich erscheint, dass beispielsweise über $\mathbb{Z}_9$ kein einziger BTL-Code existiert.

(b) Die nach Hepta- und Oktacode nächstgrößeren[41] bekannten $\mathbb{Z}_4$-linearen BTL-Codes haben die Parameter $[29, 7, 28]_{\mathbb{Z}_4}$ und $[30, 8, 28]_{\mathbb{Z}_4}$. Im ersten Fall ist ein einziger Isomorphietyp bekannt (Beispiel 3.3.9), im zweiten Fall vier Isomorphietypen (Beispiel 3.1.15). Eventuell ist es möglich, alle $\mathbb{Z}_4$-linearen Codes mit diesen Parametern komplett zu klassifizieren.

(c) Um zu entscheiden, ob die neuen Serien als R-lineare Codes optimal sind, wäre eine schlagkräftige Optimalitätstheorie für lineare Codes über Galois-Ringen der Länge 2 oder zumindest für $\mathbb{Z}_4$-lineare Codes wünschenswert. Zwar stehen mit [17] einige obere Schranken zur Verfügung, die aber für die wesentlich allgemeinere Klasse der linearen Codes über endlichen Frobenius-Ringen entwickelt wurden und in unserer Situation nicht richtig greifen. Beispielsweise verfehlen sämtliche Codes der neuen vier Serien knapp die Voraussetzung $(q-1)n < d$ für die verallgemeinerte Plotkin-Schranke [17, Th. 1]. Insbesondere wäre eine Verallgemeinerung der Griesmer-Schranke hilfreich.

(d) In diesem Zusammenhang sollte auch systematisch eine Datenbank für die besten bekannten oberen Schranken für R-lineare Codes kleiner Parameter aufgebaut werden. Ein erster Schritt wurde hierzu von Thomas Feulner mit der Klassifikation in

[41] im Hinblick auf den zu erwartenden Rechenaufwand einer vollständigen Klassifikation

[39, Th. 6.3] gemacht. Zusammen mit den unteren Schranken von den Konstruktionen in [88] ergäbe sich dann eine mit [46] vergleichbare Datenbank für R-lineare Codes.

(e) Wie in Bemerkung 2.4.3(e) diskutiert sind die in [113, Th. 4] angegebenen Parameter der punktierten verallgemeinerten Kerdock-Codes $\dot{\mathcal{K}}_{q,k+1}$ nicht korrekt. Nachdem der Code $\dot{\mathcal{K}}_{4,3+1}$ entgegen der dort gemachten Aussage ein BTKL-Code ist, sollten die Parameter und der symmetrisierte Gewichtszähler von $\dot{\mathcal{K}}_{q,k+1}$ allgemein korrekt bestimmt werden.

(f) Aufgrund von Bemerkung 3.2.6 besteht die Vermutung, dass die Punktmengen $\mathfrak{T}_{q,k,(k-1)r-2}$ nicht nur – wie in Satz 3.2.5 gezeigt – formal selbstdual, sondern sogar selbstdual sind.

(g) Die Dualisierungskonstruktion wurde nur für die $\mathbb{Z}_4$-linearen Kerdock-Codes $\mathcal{K}_{k+1}$ durchgeführt. Für die allgemeinen Kerdock-Codes $\mathcal{K}_{q,k+1}$ im Sinne von [99] ist bisher keine überzeugende Dualisierungsfunktion τ bekannt. Die Dualisierungsfunktion der $\mathbb{Z}_4$-Konstruktion lässt sich jedenfalls nicht direkt übernehmen, weil es im allgemeinen Fall nicht mehr nur 3, sondern 5 verschiedene Typen von Hyperebenen gibt, siehe Fakt 2.4.4 und Tabelle 2.4.2.

(h) Für die Konstruktionen SimAug($\mathfrak{k}$) und SimLen($\mathfrak{k}$) wurde unter den in dieser Arbeit behandelten Punktmengen $\mathfrak{T}_{q,k,s}$ und $\mathfrak{T}^*_{q,k,s}$ die beste Möglichkeit für $\mathfrak{k}$ ausgewählt (Lemma 3.3.4). Gleichwohl ist es keineswegs gesichert, dass nicht andere Punktmengen $\mathfrak{k}$ noch bessere Codes SimAug($\mathfrak{k}$) liefern. Aus dem Gewichtszähler in Tabelle 3.3.1 geht hervor, dass gute Punktmengen $\mathfrak{k}$ weder zu groß noch zu klein sein dürfen und die Punkte einigermaßen homogen auf die Punktklassen und die Hyperebenen verteilt sein sollten. Ein genaueres geometrisches Verständnis dieser Situation wäre jedoch wünschenswert. Für sehr kleine Fälle könnte dieser Frage auch mit einer Computersuche nachgegangen werden.

(i) Die Konstruktionen SimAug($\mathfrak{k}$) und SimLen($\mathfrak{k}$) sind genauso in ungerader Charakteristik durchführbar. Die entscheidende Frage ist natürlich wieder, welche Punktmengen $\mathfrak{k}$ gute Codes liefern.

(j) Die Konstruktion SimAug($\mathfrak{k}$) baut im allgemeinen Fall $q > 2$ auf der $(q-1)$-fachen Wiederholung anstelle eines einzelnen Simplex-Codes auf. Denn bei der Benutzung nur eines einzigen Simplex-Codes ist unklar, welches Element aus R^*p im Fall $x \in \mathfrak{k}$ unterhalb des Koordinatenvektors von x in die Generatormatrix eingetragen werden soll; siehe auch [90, Sec. 3.1]. Es stellt sich also die Frage, ob für $q > 2$ auch ausgehend von einem einzigen Simplex-Code eine Konstruktionsmöglichkeit existiert, so dass Codes von hoher Minimaldistanz entstehen und der symmetrisierte Gewichtszähler von SimAug($\mathfrak{k}$) wie in Satz 3.3.2 wieder nur vom Spektrum von $\mathfrak{k}$ abhängt.

A. Bilinearformen über $\mathbb{F}_2$

In diesem Anhang wird das in Abschnitt 3.1 benötigte Wissen zu symmetrischen Bilinearformen in endlichdimensionalen $\mathbb{F}_2$-Vektorräumen bereitgestellt. Für ein weitergehendes Studium wird auf [120, Ch. 11] verwiesen.

Definitionen

Sei B eine symmetrische Bilinearform auf einem $\mathbb{F}_2$-Vektorraum V der endlichen Dimension n. Im Fall $B(\mathbf{v}, \mathbf{w}) = 0$ schreiben wir auch $\mathbf{v} \perp \mathbf{w}$ und sagen, dass $\mathbf{v}$ auf $\mathbf{w}$ *senkrecht* steht. Weiter ist zu einer Menge $U \subseteq V$ die orthogonale Menge

$$U^\perp = \{\mathbf{v} \in V \mid \mathbf{v} \perp \mathbf{u} \text{ für alle } \mathbf{u} \in U\}$$

definiert. Die orthogonale Menge $U^\perp$ ist ein Unterraum von V. Das *Radikal* $\mathrm{Rad}(B)$ von B ist der Unterraum $V^\perp$, und der *Rang* $\mathrm{rk}(B)$ von B ist die Kodimension $n - \dim(V^\perp)$ des Radikals $V^\perp$ in V. Ist $\mathrm{rk}(B) < n$, so heißt B *ausgeartet*. Für alle Unterräume U gilt $U \leq (U^\perp)^\perp$. Ist B nicht ausgeartet, so gilt sogar $U = (U^\perp)^\perp$ und $\dim(U) + \dim(U^\perp) = n$.

Die Vektoren $\mathbf{v} \in \mathbb{F}_2^n$ mit $\mathbf{v} \perp \mathbf{v}$ heißen *isotrop*. Wegen $\mathrm{char}(\mathbb{F}_2) = 2$ ist $V \to \mathbb{F}_2$, $\mathbf{v} \mapsto B(\mathbf{v}, \mathbf{v})$ eine $\mathbb{F}_2$-lineare Abbildung. Als Kern dieser Abbildung ist die Menge V_0 aller isotropen Vektoren ein Unterraum von V der Kodimension 0 oder 1. Im ersten Fall ist $V_0 = V$ und B heißt *alternierend*. Es gilt stets $\mathrm{Rad}(V) \leq V_0$.

Klassifikation

In [1] (siehe auch [120, Th. 11.14 u. Th. 11.29]) wurden die symmetrischen Bilinearformen auf einem endlich-dimensionalen $\mathbb{F}_2$-Vektorraum V klassifiziert: Zu jedem Rang $r \in \{1, \ldots, n\}$ existiert die nicht alternierende Bilinearform $B_{n,r}$, die nach geeigneter Basiswahl durch die Darstellungsmatrix

$$\begin{pmatrix} \mathbf{I}_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \in \mathbb{F}_2^{n \times n}.$$

beschrieben wird. Für gerades r gibt es außerdem die alternierende Bilinearform $A_{n,r}$ mit der Darstellungsmatrix

$$\begin{pmatrix} \mathbf{J}_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \in \mathbb{F}_2^{n \times n},$$

dabei bezeichnet

$$\mathbf{J}_r = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix} \in \mathbb{F}_2^{r \times r}$$

die um 90 Grad gedrehte Einheitsmatrix.

Die Nullform $A_{n,0}$ ist alternierend. Die Standardbilinearform $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} x_i y_i$ auf $\mathbb{F}_2^n$ ist vom (Isomorphie-)Typ $B_{n,n}$. Eine weitere wichtige Bilinearform vom gleichen Typ $B_{n,n}$ ist die *Spurform* $(x, y) \mapsto \mathrm{Tr}_{\mathbb{F}_2}(xy)$ auf dem $\mathbb{F}_2$-Vektorraum $\mathbb{F}_{2^n}$. Dabei bezeichnet $\mathrm{Tr}_{\mathbb{F}_2}$ die Spurabbildung $\mathbb{F}_{2^n} \to \mathbb{F}_2$, $x \mapsto \sum_{i=0}^{n-1} x^{2^i}$.

Für $B = B_{n,n}$ ist $\dim(V_0^\perp) = 1$, d.h. $V_0^\perp$ enthält neben dem Nullvektor einen einzigen weiteren Vektor $\mathbf{1}$. Unter den Vektoren von V ist $\mathbf{1}$ dadurch ausgezeichnet, genau auf den isotropen Vektoren senkrecht zu stehen. Bezüglich der Standardbilinearform auf $\mathbb{F}_2^n$ ist ein Vektor genau dann isotrop, wenn er eine gerade Anzahl von Einseinträgen aufweist. Somit ist hier $\mathbf{1}$ der Einsvektor $(1, \ldots, 1)$, und wir sehen, dass der Vektor $\mathbf{1}$ genau dann selbst isotrop ist, wenn n gerade ist. Bezüglich der Spurform ist ein Element x genau dann isotrop, wenn $\mathrm{Tr}_{\mathbb{F}_2}(x) = 0$ gilt, und der ausgezeichnete Vektor $\mathbf{1}$ ist das Einselement des Körpers $\mathbb{F}_{2^n}$.

Unterräume

Durch Einschränkung einer vorgegebenen Bilinearform B wird jeder Unterraum U von V zu einem Vektorraum mit Bilinearform $B|_{U\times U}$. In dieser Situation nennen wir U auch einen Unterraum von B, und der Isomorphietyp der eingeschränkten Bilinearform wird als der *Typ* von U bezeichnet. Damit lassen sich beispielsweise die selbstorthogonalen Codes als die Unterräume vom Typ $A_{k,0}$ der Standardbilinearform beschreiben. Wir schreiben abkürzend

$$\mathrm{Rad}(U) = \mathrm{Rad}(B|_{U\times U}) = U \cap U^\perp \quad \text{und} \quad \mathrm{rk}(U) = \mathrm{rk}(B|_{U\times U}) = \mathrm{codim}_U(U \cap U^\perp),$$

und sprechen vom *Radikal* bzw. vom *Rang* von U. Weiter heißt U *alternierend* genau dann, wenn $B|_{U\times U}$ alternierend ist. Dies ist genau dann der Fall, wenn $U \leq V_0$ ist, d.h. wenn $\mathbf{1} \in U^\perp$ gilt.

Für jeden Unterraum U von $B_{n,n}$ gilt

$$\mathrm{Rad}(U^\perp) = U^\perp \cap (U^\perp)^\perp = U \cap U^\perp = \mathrm{Rad}(U).$$

Daraus folgt $\mathrm{rk}(U^\perp) = n - 2\dim(U) + \mathrm{rk}(U)$. Aus $\dim(\mathrm{Rad}(U)) = \dim(U) - \mathrm{rk}(U)$ und $0 \leq \dim(\mathrm{Rad}(U)) \leq \min(\dim(U), \dim(U^\perp))$ folgt

$$\max(0, 2\dim(U) - n) \leq \mathrm{rk}(U) \leq \dim(U),$$

und man überlegt sich anhand passender Darstellungsmatrizen, dass alle Kombinationen aus Dimension $\dim(U) \in \{0, \ldots, n\}$ und Rang $\mathrm{rk}(U)$ im obigen Intervall tatsächlich als Unterräume von U von $B_{n,n}$ auftreten.

Weil Isotropie bei Einschränkung erhalten bleibt, sind die Unterräume einer alternierenden Bilinearform wieder alternierend. Anhand passender Darstellungsmatrizen ist es nicht schwer zu sehen, dass als Unterräume von $A_{n,r}$ genau die Typen $A_{m,s}$ mit s gerade,

$$0 \leq m \leq n \quad \text{und} \quad \max(0, r - 2(n-m)) \leq s \leq \min(r, m)$$

auftreten.

B. Assoziationsschemata

Wir geben im Folgenden die in Abschnitt 3.1 benötigten Grundlagen zur Theorie der symmetrischen Assoziationsschemata an. Eine ausführliche Übersicht über Assoziationsschemata findet man in [42, Ch. 12] sowie mit besonderem Schwerpunkt auf der Anwendung in der Codierungstheorie in [30], [108, Ch. 21] und [32].

Definition

Sei X eine endliche Menge, $n = \#X$ und $\mathcal{A} = \{R_0, \ldots, R_d\}$ eine Partition von $X \times X$ in Relationen $R_i \subseteq X \times X$. Die Partition $\mathcal{A}$ heißt *symmetrisches Assoziationsschema* auf X mit d Klassen, wenn die folgenden Bedingungen erfüllt sind:[42]

- $R_0 = \{(x, x) \mid x \in X\}$ ist die Diagonale von $X \times X$.
- Die Relationen R_i sind sämtlich symmetrisch, d.h. aus $(x, y) \in R_i$ folgt $(y, x) \in R_i$.
- Für alle $i, j, k \in \{0, \ldots, k\}$ existiert eine Zahl $p_{ij}^k \in \mathbb{N}$ derart, dass für alle $x, y \in X$ mit $(x, y) \in R_k$ gilt:

  $$\#\{z \in X \mid (x, z) \in R_i \text{ und } (z, y) \in R_j\} = p_{ij}^k.$$

  Mit anderen Worten: Für alle $i, j \in \{0, \ldots, d\}$ und alle $x, y \in X$ hängt die Anzahl p_{ij}^k der $z \in X$ mit $(x, z) \in R_i$ und $(z, y) \in R_j$ nur von der Zahl $k \in \{0, \ldots, n\}$ mit $(x, y) \in R_k$ ab. Die Zahlen p_{ij}^k werden *Schnittzahlen* des Assoziationsschemas $\mathcal{A}$ genannt.

Die symmetrischen Assoziationsschemata mit 2 Klassen entsprechen genau den stark regulären Graphen.

Bose-Mesner-Algebra

Ist $\mathcal{A} = \{R_0, \ldots, R_d\}$ ein symmetrisches Assoziationsschema, so erzeugen die Inzidenzmatrizen $\mathbf{A}_0, \ldots, \mathbf{A}_d$ von $R_0, \ldots, R_d$ eine Unteralgebra der Matrixalgebra $\mathbb{C}^{n \times n}$, die *Bose-Mesner-Algebra* von $\mathcal{A}$. Die Schnittzahlbediungungen von $\mathcal{A}$ übersetzen sich dabei in die Gleichungen ($i, j, k \in \{0, \ldots, d\}$)

$$\mathbf{A}_i \mathbf{A}_j = \sum_{k=0}^{d} p_{ij}^k \mathbf{A}_k. \tag{B.1}$$

[42] Zur Definition eines allgemeinen Assoziationsschemas ohne den Zusatz „symmetrisch" wird in der Definition Punkt B gegen die schwächere Bedingung ersetzt, dass für jedes i ein j existiert mit $R_j = R_i^\top = \{(y, x) \mid (x, y) \in R_i\}$.

Insbesondere hat die Bose-Mesner-Algebra als $\mathbb{C}$-Vektorraum die Dimension $d+1$.

Über die Bose-Mesner-Algebra lassen sich die symmetrischen Assoziationsschemata wie folgt charakterisieren: Ist $\mathcal{A} = \{R_0, \ldots, R_d\}$ eine Partition von $X \times X$ und sind $\mathbf{A}_i \in \mathbb{C}^{n \times n}$ die zugehörigen Inzidenzmatrizen, so ist $\mathcal{A}$ genau dann ein Assoziationsschema mit d Klassen, wenn die folgenden Bedingungen erfüllt sind:

- $\mathbf{A}_0 = \mathbf{I}_n$
- Die Matrizen $\mathbf{A}_i$ sind sämtlich symmetrisch, d.h. $\mathbf{A}_i = \mathbf{A}_i^\top$.
- Der von den Matrizen $\mathbf{A}_0, \ldots, \mathbf{A}_d$ erzeugte Untervektorraum der $\mathbb{C}$-Algebra $\mathbb{C}^{n \times n}$ ist bereits eine Unteralgebra.

Die Schnittzahlen von $\mathcal{A}$ sind dann durch die Gleichung (B.1) festgelegt.

Symmetrische Translationsschemata

Sei nun $(G, +)$ eine abelsche Gruppe. Wir bezeichnen ein symmetrisches Assoziationsschema $\mathcal{A} = \{R_0, \ldots, R_d\}$ auf G als *symmetrisches Translationsschema* (auch: *symmetrisches Cayley-Schema*) auf $(G, +)$, wenn die Relationen R_i *translationsinvariant* unter G sind, d.h. wenn für alle $i \in \{0, \ldots, d\}$ und alle $g \in G$ gilt: Aus $(x, y) \in R_i$ folgt $(x + g, y + g) \in R_i$. In diesem Fall ist $\mathcal{A}$ bereits durch die Partition $\{G_0, \ldots, G_d\}$ mit $G_i = \{g \in G \mid (g, 0) \in R_i\}$ von G festgelegt: Es gilt $R_i = \{(g, h) \in G \times G \mid g - h \in G_i\}$ (der von R_i beschriebene Graph ist der Cayley-Graph von G_i in G). Aus diesem Grund dürfen wir auch die zugehörige Partition $\{G_0, \ldots, G_d\}$ von G als symmetrisches Translationsschema auf $(G, +)$ bezeichnen.

Fassen wir die charakteristische Funktion χ_H einer beliebigen Teilmenge $H \subseteq G$ als ein Element der $\mathbb{C}$-Gruppenalgebra $\mathbb{C}[G]$ auf (d.h. $\chi_H = \sum_{g \in H} g$), so ist die Bose-Mesner-Algebra eines symmetrischen Translationsschemas $\{G_0, \ldots, G_d\}$ zu der von $\chi_{G_0}, \ldots, \chi_{G_d}$ erzeugten Unteralgebra von $\mathbb{C}[G]$ isomorph. Eine Partition $\{G_0, \ldots, G_d\}$ von G ist genau dann ein symmetrisches Translationsschema auf $(G, +)$, wenn $G_0 = \{0\}$ ist, für alle $i \in \{0, \ldots, n\}$ die Beziehung $-G_i = G_i$ gilt, und der von $\chi_{G_0}, \ldots, \chi_{G_n}$ erzeugte Untervektorraum der $\mathbb{C}$-Gruppenalgebra $\mathbb{C}[G]$ bereits eine Unteralgebra ist.

Die auf entsprechende Weise aus den symmetrischen Translationsschemata resultierenden Unteralgebren von $\mathbb{Z}[G]$ sind auch als *symmetrische Schur-Ringe* bekannt.

Literatur

[1] A. A. Albert. “Symmetric and alternate matrices in an arbitrary field, I”. In: *Transactions of the American Mathematical Society* 43.3 (1938), S. 386–436.

[2] B. Artmann. “Hjelmslev-Ebenen mit verfeinerten Nachbarschaftsrelationen”. In: *Mathematische Zeitschrift* 112.3 (1969), S. 163–180.

[3] N. Aydin und D. K. Ray-Chaudhuri. “Quasi-cyclic codes over $\mathbb{Z}_4$ and some new binary codes”. In: *IEEE Transactions on Information Theory* 48.7 (2002), S. 2065–2069.

[4] E. R. Berlekamp. *Key Papers in the Development of Coding Theory*. New York: IEEE Press, 1974. ISBN: 0-87942-031-6.

[5] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert und A. Wassermann. *Error-Correcting Linear Codes. Classification by Isometry and Applications*. Algorithms and Computation in Mathematics 18. Berlin: Springer, 2006. ISBN: 3-540-28371-4.

[6] G. Birkhoff. “Subgroups of abelian groups”. In: *Proceedings of the London Mathematical Society. Second Series* 38 (1934), S. 385–401.

[7] S. Boev, T. Honold und I. Landjev. “Optimal arcs in Hjelmslev spaces of larger dimension”. In: *Proceedings of the Seventh International Workshop on Coding and Cryptography*. 2011, S. 63–70.

[8] A. Bonnecaze und I. M. Duursma. “Translates of linear codes over $\mathbf{Z}_4$”. In: *IEEE Transactions on Information Theory* 43.4 (1997), S. 1218–1230.

[9] A. Bonnecaze, P. Solé, C. Bachoc und B. Mourrain. “Type II codes over $\mathbb{Z}_4$”. In: *IEEE Transactions on Information Theory* 43.3 (1997), S. 969–976.

[10] W. Bosma, J. Cannon und C. Playoust. “The Magma algebra system. I. The user language”. In: *Journal of Symbolic Computation* 24.3-4 (1997), S. 235–265.

[11] I. Bouyukliev, R. Daskalov und S. Kapralov. “Optimal quaternary linear codes of dimension five”. In: *IEEE Transactions on Information Theory* 42.4 (1996), S. 1228–1235.

[12] I. Bouyukliev, D. B. Jaffe und V. Vavrek. “The smallest length of eight-dimensional binary linear codes with prescribed minimum distance”. In: *IEEE Transactions on Information Theory* 46.4 (2000), S. 1539–1544.

[13] M. Braun, A. Kohnert und A. Wassermann. “Optimal linear codes from matrix groups”. In: *IEEE Transactions on Information Theory* 51.12 (2005), S. 4247–4251.

[14] A. E. Brouwer und L. M. G. M. Tolhuizen. “A sharpening of the Johnson bound for binary linear codes and the nonexistence of linear codes with Preparata parameters”. In: *Designs, Codes and Cryptography* 3 (1993), S. 95–98.

[15] L. M. Butler. *Subgroup Lattices and Symmetric Functions*. Memoirs of the American Mathematical Society 539. American Mathematical Society, 1994. ISBN: 0-8218-2600-X.

[16] E. Byrne, M. Greferath und T. Honold. “Ring geometries, two-weight codes, and strongly regular graphs”. In: *Designs, Codes and Cryptography* 48.1 (2008), S. 1–16.

[17] E. Byrne, M. Greferath, A. Kohnert und V. Skachek. “New bounds for codes over finite Frobenius rings”. In: *Designs, Codes and Cryptography* 57.2 (2010), S. 169–179.

[18] E. Byrne, M. Kiermaier und A. Sneyd. “Properties of codes with two homogeneous weights”. In: *Finite Fields and Their Applications* 18.4 (2012), S. 711–727.

[19] A. R. Calderbank und W. M. Kantor. “The geometry of two-weight codes”. In: *The Bulletin of the London Mathematical Society* 18.2 (1986), S. 97–122.

[20] A. R. Calderbank und G. McGuire. “Construction of a $(64, 2^{37}, 12)$ code via Galois rings”. In: *Designs, Codes and Cryptography* 10 (1997), S. 157–165.

[21] A. R. Calderbank, G. McGuire, P. V. Kumar und T. Helleseth. “Cyclic codes over $\mathbb{Z}_4$, locator polynomials, and Newton’s identities”. In: *IEEE Transactions on Information Theory* 42.1 (1996), S. 217–226.

[22] A. R. Calderbank und N. J. A. Sloane. “Modular and p-adic cyclic codes”. In: *Designs, Codes and Cryptography* 6.1 (1995), S. 21–35.

[23] C. Carlet. “$\mathbb{Z}_{2^k}$-linear codes”. In: *IEEE Transactions on Information Theory* 44.4 (1998), S. 1543–1547.

[24] R. Chapman und P. Solé. “Universal codes and unimodular lattices”. In: *Journal de Théorie des Nombres de Bordeaux* 8 (1996), S. 269–276.

[25] B. Cirpa. “Straightening out nonlinear codes”. In: *What’s Happening in the Mathematical Sciences*. Hrsg. von P. Zorn. Bd. 2. American Mathematical Society, 1994, S. 37–40.

[26] G. Constantine und R. S. Kulkarni. “On a result of S. Delsarte”. In: *Proceedings of the American Mathematical Society* 92.1 (1984), S. 149–152.

[27] I. Constantinescu und W. Heise. “A metric for codes over residue class rings”. In: *Problems of Information Transmission* 33 (1997), S. 208–213.

[28] J. H. Conway und N. J. A. Sloane. “Self-dual codes over the integers modulo 4”. In: *Journal of Combinatorial Theory. Series A* 62.1 (1993), S. 30–45.

[29] P. Delsarte. “Weights of linear codes and strongly regular normed spaces”. In: *Discrete Mathematics* 3.1–3 (1972), S. 47–64.

[30] P. Delsarte. “An algebraic approach to the association schemes of coding theory”. In: *Philips Research Reports* 10 (1973).

[31] P. Delsarte und J.-M. Goethals. “Alternating bilinear forms over GF_q”. In: *Journal of Combinatorial Theory. Series A* 19.1 (1975), S. 26–50.

[32] P. Delsarte und V. I. Levenshtein. “Association schemes and coding theory”. In: *IEEE Transactions on Information Theory* 44.6 (1998), S. 2477–2504.

[33] S. Delsarte. “Fonctions de Möbius Sur Les Groupes Abeliens Finis”. In: *Annals of Mathematics. Second Series* 49.3 (1948), S. 600–609.

[34] S. Dodunekov, T. Helleseth, N. Manev und Ø. Ytrehus. “New bounds on binary linear codes of dimension eight”. In: *IEEE Transactions on Information Theory* 33.6 (1987), S. 917–919.

[35] S. Dodunekov und J. Simonis. “Codes and projective multisets”. In: *Electronic Journal of Combinatorics* 5 (1998), #R37.

[36] P. E. Dyubyuk. “On the number of subgroups of an abelian p-group”. In: *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya* 12.4 (1948), S. 351–378.

[37] Y. Edel und J. Bierbrauer. “Twisted BCH-codes”. In: *Journal of Combinatorial Designs* 5.5 (1997), S. 377–389.

[38] T. Feulner. “The automorphism groups of linear codes and canonical representatives of their semilinear isometry classes”. In: *Advances in Mathematics of Communications* 3.4 (2009), S. 363–383.

[39] T. Feulner. “Canonization of linear codes over $\mathbb{Z}_4$”. In: *Advances in Mathematics of Communications* 5.2 (2011), S. 245–266.

[40] L. E. Fuller. “A canonical set for matrices over a principal ideal ring modulo m”. In: *Canadian Journal of Mathematics* 7 (1955), S. 54–59.

[41] P. Gaborit und M. Harada. “Construction of extremal type II codes over $\mathbb{Z}_4$”. In: *Designs, Codes and Cryptography* 16.3 (1999), S. 257–269.

[42] C. D. Godsil. *Algebraic Combinatorics*. New York: Chapman & Hall, 1993. ISBN: 0-412-04131-6.

[43] C. D. Godsil und G. Royle. *Algebraic Graph Theory*. Graduate Texts in Mathematics 207. New York: Springer, 2001. ISBN: 0-387-95220-9.

[44] J.-M. Goethals. “Two dual families of nonlinear binary codes”. In: *Electronics Letters* 10.23 (1974), S. 471–472.

[45] J.-M. Goethals. “Nonlinear codes defined by quadratic forms over GF(2)”. In: *Information and Control* 31.1 (1976), S. 43–74.

[46] M. Grassl. *Code Tables: Bounds on the parameters of various types of codes*. URL: `www.codetables.de`.

[47] P. P. Greenough und R. Hill. “Optimal linear codes over GF(4)”. In: *Discrete Mathematics* 125.1–3 (1994), S. 187–199.

[48] M. Greferath. “An introduction to ring-linear coding theory”. In: M. Sala, S. Sakata, T. Mora, C. Traverso und L. Perret. *Gröbner Bases, Coding, and Cryptography*. Berlin: Springer, 2009, S. 219–238. ISBN: 978-3-540-93805-7.

[49] M. Greferath und S. E. Schmidt. “Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code.” In: *IEEE Transactions on Information Theory* 45.7 (1999), S. 2522–2524.

[50] M. Greferath und S. E. Schmidt. “Finite-ring combinatorics and MacWilliams’ equivalence theorem”. In: *Journal of Combinatorial Theory. Series A* 92.1 (2000), S. 17–28.

[51] P. Hall. “The algebra of partitions”. In: *Proceedings of the 4th Canadian mathematical congress*. Banff, 1959, S. 147–159.

[52] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane und P. Solé. “The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes”. In: *IEEE Transactions on Information Theory* 40.2 (1994), S. 301–319.

[53] W. Heise und P. Quattrocchi. *Informations- und Codierungstheorie*. 3. Aufl. Berlin: Springer, 1995. ISBN: 3-540-57477-8.

[54] T. Helleseth. “Codes over Z_4”. In: *Computational Discrete Mathematics*. Hrsg. von H. Alt. Lecture Notes in Computer Science 2122. Springer, 2001, S. 47–55.

[55] L. Hemme, T. Honold und I. Landjev. “Arcs in projective Hjelmslev spaces obtained from Teichmüller sets”. In: *Proceedings of the Seventh International Workshop on Algebraic and Combinatorial Coding Theory 2000*. 2000, S. 4–12.

[56] J. Hjelmslev. “Die Geometrie der Wirklichkeit”. In: *Acta Mathematica* 40.1 (1916), S. 35–66.

[57] T. Honold. “Arcs and MDS-like codes over finite chain rings”. In: *Proceedings of the Ninth International Workshop on Algebraic and Combinatorial Coding Theory 2004 (ACCT-2004)*. 2004, S. 223–229.

[58] T. Honold. “Further results on homogeneous two-weight codes”. In: *Proceedings of the Fifth International Workshop on Optimal Codes and related Topics 2007 (OC-2007)*. 2007, S. 80–86.

[59] T. Honold. “Two-intersection sets in projective Hjelmslev spaces”. In: *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems*. 2010, S. 1807–1813. ISBN: 978-963-311-370-7.

[60] T. Honold und M. Kiermaier. “Classification of maximal arcs in small projective Hjelmslev geometries”. In: *Proceedings of the Tenth International Workshop on Algebraic and Combinatorial Coding Theory 2006 (ACCT-2006)*. 2006, S. 112–117.

[61] T. Honold und M. Kiermaier. “The existence of maximal $(q^2, 2)$-arcs in uniform projective Hjelmslev planes over chain rings of odd prime characteristic”. In: *Designs, Codes and Cryptography* (2012). Erscheint demnächst.

[62] T. Honold und M. Kiermaier. "The maximal size of 6- and 7-arcs in projective Hjelmslev planes over chain rings of order 9". In: *Science China. Mathematics* 55.1 (2012), S. 73–92.

[63] T. Honold, M. Kiermaier und I. Landjev. "New arcs of maximal size in projective Hjelmslev planes of order 9". In: *Comptes Rendus de l'Académie Bulgare des Sciences* 63.2 (2010), S. 171–180.

[64] T. Honold und I. Landjev. "Linearly representable codes over chain rings". In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 69.1 (1999), S. 187–203.

[65] T. Honold und I. Landjev. "Linear codes over finite chain rings". In: *Electronic Journal of Combinatorics* 7 (2000), #R11.

[66] T. Honold und I. Landjev. "On arcs in projective Hjelmslev planes". In: *Discrete Mathematics* 231.1–3 (2001), S. 265–278.

[67] T. Honold und I. Landjev. "On maximal arcs in projective Hjelmslev planes over chain rings of even characteristic". In: *Finite Fields and Their Applications* 11.2 (2005), S. 292–304.

[68] T. Honold und I. Landjev. "Caps in projective Hjelmslev spaces over finite chain rings of nilpotency index 2". In: *Innovations in incidence geometry.* 4 (2006), S. 13–25.

[69] T. Honold und I. Landjev. "Linear codes over finite chain rings and projective Hjelmslev geometries". In: *Codes over Rings. Proceedings of the CIMPA Summer School Ankara, Turkey, 18 – 29 August 2008.* Hrsg. von P. Solé. Series on Coding Theory and Cryptology 6. World Scientific, 2009, S. 60–123. ISBN: 978-981-283-768-4.

[70] T. Honold und I. Landjev. "The dual construction for arcs in projective Hjelmslev spaces". In: *Advances in Mathematics of Communications* 5.1 (2011), S. 11–21.

[71] T. Honold und I. Landjev. "Codes over rings and ring geometries". In: *Current research topics in Galois geometry.* Hrsg. von L. Storme und J. de Beule. Mathematics Research Developments. New York: Nova Science Publishers, 2012, S. 161–186. ISBN: 978-1-61209-523-3.

[72] T. Honold und I. Landjev. "Non-free extensions of the simplex codes over a chain ring with four elements". In: *Designs, Codes and Cryptography* (2012). Erscheint demnächst.

[73] T. Honold und A. A. Nechaev. "Weighted modules and representations of codes". In: *Problems of Information Transmission* 35.3 (1999), S. 205–223.

[74] X.-D. Hou, K. H. Leung und Q. Xiang. "New partial difference sets in $\mathbb{Z}_{p^2}^t$ and a related problem about Galois rings". In: *Finite Fields and Their Applications* 7.1 (2001), S. 165–188.

[75] W. C. Huffman und V. S. Pless. *Fundamentals of Error-Correcting Codes.* Cambridge: Cambridge University Press, 2003. ISBN: 0521782805.

[76] T. Ito, A. Munemasa und M. Yamada. “Amorphous association schemes over the Galois rings of characteristic 4”. In: *European Journal of Combinatorics* 12.6 (1991), S. 513–526.

[77] D. B. Jaffe. “Binary linear codes: New results on nonexistence”. 1996. URL: `http://www.math.unl.edu/~djaffe/codes/code.ps.gz`.

[78] G. J. Janusz. “Separable algebras over commutative rings”. In: *Transactions of the American Mathematical Society* 122.2 (1966), S. 461–479.

[79] A. Kerber. *Applied finite group actions*. 2. Aufl. Algorithms and Combinatorics 19. Berlin: Springer, 1999. ISBN: 3-540-65941-2.

[80] A. M. Kerdock. “A class of low-rate nonlinear binary codes”. In: *Information and Control* 20 (1972), S. 182–187.

[81] Y. Al-Khamees. “The intersection of distinct Galois subrings is not necessarily Galois”. In: *Compositio Mathematica* 40.3 (1980), S. 283–286.

[82] M. Kiermaier. “Arcs und Codes über endlichen Kettenringen”. Diplomarbeit. Technische Universität München, 2006.

[83] M. Kiermaier und M. Koch. “New complete 2-arcs in the uniform projective Hjelmslev planes over chain rings of order 25”. In: *Proceedings of the Sixth International Workshop on Optimal Codes and Related Topics 2009*. 2009, S. 206–113.

[84] M. Kiermaier, M. Koch und S. Kurz. “2-arcs of maximal size in the affine and the projective Hjelmslev plane over $\mathbb{Z}_{25}$”. In: *Advances in Mathematics of Communications* 5.2 (2011), S. 287–301.

[85] M. Kiermaier und A. Kohnert. “New arcs in projective Hjelmslev planes over Galois rings”. In: *Proceedings of the Fifth International Workshop on Optimal Codes and Related Topics 2007*. 2007, S. 112–119.

[86] M. Kiermaier und I. Landjev. “Designs in projective Hjelmslev spaces”. In: *Contemporary Mathematics* 579 (2012), S. 111–121.

[87] M. Kiermaier und A. Wassermann. “Minimum weights and weight enumerators of $\mathbb{Z}_4$-linear quadratic residue codes”. In: *IEEE Transactions on Information Theory* 58.7 (2012), S. 4870–4883.

[88] M. Kiermaier und J. Zwanzger. *Online tables of linear codes over finite chain rings*. URL: `codes.uni-bayreuth.de/Linear_Codes_R/`.

[89] M. Kiermaier und J. Zwanzger. “A new series of $\mathbb{Z}_4$-linear codes of high minimum Lee distance derived from the Kerdock codes”. In: *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems*. 2010, S. 929–932. ISBN: 978-963-311-370-7.

[90] M. Kiermaier und J. Zwanzger. “A $\mathbb{Z}_4$-linear code of high minimum Lee distance derived from a hyperoval”. In: *Advances in Mathematics of Communications* 5.2 (2011), S. 275–286.

[91] M. Kiermaier und J. Zwanzger. "New ring-linear codes from geometric dualization". In: *Proceedings of the Seventh International Workshop on Coding and Cryptography*. 2011, S. 111–120.

[92] M. Kiermaier und J. Zwanzger. "New ring-linear codes from dualization in projective Hjelmslev geometries". In: *Designs, Codes and Cryptography* (2012). Erscheint demnächst.

[93] W. Klingenberg. "Projektive und affine Ebenen mit Nachbarelementen". In: *Mathematische Zeitschrift* 60 (1954), S. 384–406.

[94] A. Kohnert. "Sets of type (d_1, d_2) in projective Hjelmslev planes over Galois rings". In: *Algorithmic Algebraic Combinatorics and Gröbner Bases*. Hrsg. von M. Klin, G. A. Jones, A. Jurišić, M. Muzychuk und I. Ponomarenko. Heidelberg: Springer, 2009, S. 269–278. ISBN: 978-3-642-01959-3.

[95] A. Kohnert und J. Zwanzger. "New linear codes with prescribed group of automorphisms found by heuristic search". In: *Advances in Mathematics of Communications* 3.2 (2009), S. 157–266.

[96] A. Kreuzer. "Projektive Hjelmslev-Räume". Diss. Technische Universität München, 1988.

[97] A. Kreuzer. "A system of axioms for projective Hjelmslev spaces". In: *Journal of Geometry* 40.1–2 (1991), S. 125–147.

[98] W. Krull. "Algebraische Theorie der Ringe. II." In: *Mathematische Annalen* 91.1–2 (1924), S. 1–46.

[99] A. S. Kuzmin und A. A. Nechaev. "Linearly representable codes and the Kerdock code over an arbitrary Galois field of characteristic 2". In: *Russian Mathematical Surveys* 49.5 (1994), S. 183–184.

[100] A. S. Kuzmin und A. A. Nechaev. "Complete weight enumerators of generalized Kerdock code and related linear codes over Galois rings". In: *Discrete Applied Mathematics* 111.1–2 (2001), S. 117–137.

[101] I. Landjev und S. Boev. "A family of two-weight ring codes and strongly regular graphs". In: *Comptes Rendus de l'Académie Bulgare des Sciences* 62.3 (2009), S. 297–302.

[102] I. Landjev, S. Boev und T. Honold. "Optimal arcs in Hjelmslev spaces of higher dimension". In: *Proceedings of the Sixth International Workshop on Optimal Codes and Related Topics 2009*. 2009, S. 132–138.

[103] I. Landjev und T. Honold. "Arcs in projective Hjelmslev planes". In: *Discrete Mathematics and Applications* 11.1 (2001), S. 53–70.

[104] H. Lüneburg. "Affine Hjelmslev-Ebenen mit transitiver Translationsgruppe". In: *Mathematische Zeitschrift* 79 (1962), S. 260–288.

[105] J. Ma. "Three-class association schemes on Galois rings in characteristic 4". In: *Graphs and Combinatorics* 23.1 (2007), S. 73–86.

[106] I. G. MacDonald. *Symmetric Functions and Hall Polynomials*. 2. Aufl. Oxford: Oxford University Press, 1995. ISBN: 0-19-853489-2.

[107] J. E. MacDonald. "Design methods for maximum minimum-distance error-correcting codes". In: *IBM Journal of Research and Development* 4.1 (1960), S. 43–57.

[108] F. J. MacWilliams und N. J. A. Sloane. *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977. ISBN: 0-444-85009-0.

[109] B. R. McDonald. *Finite Rings with Identity*. New York: Marcel Dekker, 1974. ISBN: 0-8247-6161-8.

[110] F. Miller Maley. "The Hall polynomial revisited". In: *Journal of Algebra* 184.2 (1996), S. 363–371.

[111] A. A. Nechaev. "Kerdock code in a cyclic form". In: *Discrete Mathematics and Applications* 1.4 (1991), S. 365–384.

[112] A. A. Nechaev. "Finite rings with applications". In: *Handbook of Algebra*. Hrsg. von M. Hazewinkel. Bd. 5. Amsterdam: North-Holland, 2008. Kap. 5, S. 213–320. ISBN: 978-0-444-53101-8.

[113] A. A. Nechaev und A. S. Kuzmin. "Linearly presentable codes". In: *Proceedings of the International Symposium on Information Theory and its Application (ISITA) 1996*. 1996, S. 31–34.

[114] A. W. Nordstrom und J. P. Robinson. "An optimum nonlinear code". In: *Information and Control* 11.5–6 (1967), S. 613–616.

[115] G. H. Norton und A. Sălăgean. "On the structure of linear and cyclic codes over a finite chain ring". In: *Applicable Algebra in Engineering, Communication and Computing* 10 (2000), S. 489–506.

[116] A. M. Patel. "Maximal q-nary linear codes with large minimum distance". In: *IEEE Transactions on Information Theory* 21.1 (1975), S. 106–110.

[117] V. S. Pless und Z. Qian. "Cyclic codes and quadratic residue codes over Z_4". In: *IEEE Transactions on Information Theory* 42.5 (1996), S. 1594–1600.

[118] F. P. Preparata. "A class of optimum nonlinear double-error-correcting codes". In: *Information and Control* 13.4 (1968), S. 378–400.

[119] R. Raghavendran. "Finite associative rings". In: *Compositio Mathematica* 21.2 (1969), S. 195–229.

[120] S. Roman. *Advanced Linear Algebra*. 3. Aufl. Graduate Texts in Mathematics 135. New York: Springer, 2008. ISBN: 978-0-387-72828-5.

[121] A. Scheerhorn. "Trace- and norm-compatible extensions of finite fields". In: *Applicable Algebra in Engineering, Communication and Computing* 3.3 (1992), S. 199–209.

[122] N. V. Semakov und V. A. Zinoviev. "Complete and quasi-complete balanced codes". In: *Problems of Information Transmission* 5.2 (1969), S. 11–13.

[123] E. Steinitz. “Zur Theorie der Abel’schen Gruppen”. In: *Jahresbericht der Deutschen Mathematiker-Vereinigung* 9 (1901), S. 80–85.

[124] F. Tamari. “On linear codes which attain the Solomon-Stiffler bound”. In: *Discrete Mathematics* 49.2 (1984), S. 179–191.

[125] H. C. A. van Tilborg. “The smallest length of binary 7-dimensional linear codes with prescribed minimum distance”. In: *Discrete Mathematics* 33.2 (1981), S. 197–207.

[126] J. V. Uspensky. *Theory of Equations*. New York: McGraw-Hill, 1948.

[127] Z.-X. Wan. *Lectures on finite fields and Galois rings*. World Scientific, 2003. ISBN: 978-981-238-570-3.

[128] E. Witt. “Zyklische Körper und Algebren der Charakteristik p vom Grad pn. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p”. In: *Journal für die Reine und Angewandte Mathematik* 176 (1937), S. 126–140.

[129] J. A. Wood. “Duality for modules over finite rings and applications to coding theory”. In: *American Journal of Mathematics* 121 (1999), S. 555–575.

[130] Y. Yeh. “On prime power abelian groups”. In: *Bulletin of the American Mathematical Society* 54.4 (1948), S. 323–327.

[131] J. Zwanzger. “A heuristic algorithm for the construction of good linear codes”. In: *IEEE Transactions on Information Theory* 54.5 (2008), S. 2388–2392.

[132] J. Zwanzger. “Computergestützte Suche nach optimalen linearen Codes über endlichen Kettenringen unter Verwendung heuristischer Methoden”. Diss. Universität Bayreuth, 2011.