Binary $\mathbb{Z}_4$-linear Codes and Sequences

Kalle Ranto

University of Turku,
Department of Mathematics,
FIN-20014 Turku, Finland
E-mail: kara@utu.fi

Turku Centre for Computer Science
TUCS Technical Report No 165
February 1998
ISBN 952-12-0170-3
ISSN 1239-1891

Abstract

We study the basic properties of Galois rings and character sums over them. Galois rings are presented as Witt vector rings. With Galois rings we construct efficient binary non-linear codes, such as Kerdock code and Delsarte-Goethals codes, as images of linear codes over alphabet $\mathbb{Z}_4$. We present also sequence families that are at the moment best known with respect to low maximum correlation.

Keywords: Galois rings, character sums, binary non-linear codes, binary sequences

TUCS Research Group
Coding Theory Group

Contents

1 Introduction

Efficient coding techniques are needed in almost every communication system. Recent computer technology is based on bits, 0 and 1, and therefore the binary codes are the most important in applications.

Codes should have some auxiliary structure so that one can handle them efficiently. Classically a set of binary codewords is viewed as a subset of the vector space $\mathbb{F}_2^m$ where m is the length of codewords and $\mathbb{F}_2$ is the field of two elements, for example 0 and 1. In this representation linearity is a good property, i.e. the set of codewords form a subspace of $\mathbb{F}_2^m$. Linear codes can be encoded easily and linearity implies some nice properties of the code.

Another good class of codes is the cyclic codes for which every cyclic shift of a codeword is also a codeword. This property implies more structure and properties for the code. Cyclic codes can also be viewed as a sequence family which makes them more applicable and interesting.

Most of the good linear binary cyclic codes can easily be described as a trace image of some subset of polynomials in $\mathbb{F}_{2^m}[x]$. The trace of the finite field induces additive characters of this field. This approach allows us to use some number–theoretic results for character sums such as Carlitz–Uchiyama bound to estimate the minimum distance of the code.

There exists very good non–linear binary codes such as Kerdock and Delsarte–Goethals codes which have much more codewords than linear codes with the same length and minimum distance. These codes have duality properties similar to the linear codes and it was expected that these codes have some kind of linearity. The structure of these codes was a mystery for researchers until the year 1994 when Hammons et al. published an article [2] which described these codes as images of linear codes over alphabet $\mathbb{Z}_4$. This kind of binary codes are called $\mathbb{Z}_4$-linear.

As with the binary codes we can view some of these $\mathbb{Z}_4$-codes as trace images of a set of polynomials with coefficients in certain extensions of $\mathbb{Z}_4$. Such extensions are called Galois rings and many structures, for example the trace function and characters, can be defined in Galois rings. Also Carlitz–Uchiyama bound has been generalized to Galois rings [6] and it can be used to estimate the minimum distance of cyclic $\mathbb{Z}_4$-codes.

In a mobile phone network we have many users using the same channel. This can be handled for example by Code–Division–Multiple–Access (CDMA). In CDMA every user has a personal code sequence and all users send message multiplied by the code sequence simultaneously to the channel. The original messages can be separated from the received message if those code sequences have good correlation properties described in Section 6.1.

Shanbhag et al. [11] showed in 1996 that Galois rings can be used to construct sequence families with very good correlation properties. The sequence families they found are the best known at the moment. In Figure 1 on page 38 we see an asymptotic comparison of the best known sequence families. In CDMA applications with many users we need a big family of sequences, i.e. u should be large. Formerly the duals of BCH codes were the best known families for large u, but the Galois ring constructions $Q_1(m, D)$ turned out to be better. For very large u we can see that in the figure the points of the duals of BCH codes lie on a line of slope 2 but taking every third point of the family $Q_1(m, D)$ we get another line of slope

$$\frac{\sqrt{2}\big((D-1)+4\big)-\sqrt{2}(D-1)}{3}=\frac{4}{3}\sqrt{2}$$

which is less than 2. So outside the figure the families $Q_1(m, D)$ are getting better and better in comparison to the duals of BCH codes.

Througout this work we assume that the basic concepts and results of coding theory and the theory of finite fields are known.

Part I

Galois rings

2 Galois fields

In this chapter we recall the basic properties of Galois fields, i.e. finite fields. We give no proofs, but those can be found in any book of basic algebra, for example in [7]. The characters and character sums of finite fields are also studied in [12].

Proposition 2.1. *Every finite field has p^m elements for some prime $p \in \mathbb{P}$ and $m \in \mathbb{N}_0$. On the other hand for every $q = p^m$, $p \in \mathbb{P}$, $m \in \mathbb{N}_0$, there exists a finite field with q elements. Moreover any two finite fields with the same number of elements are isomorphic.*

We can construct a finite field $\mathbb{F}_{p^m}$ with p^m elements as follows:

Let $\mathbb{Z}_p$ be a prime field, $\mathbb{Z}_p[x]$ a ring of polynomials over $\mathbb{Z}_p$ and $p(x) \in \mathbb{Z}_p[x]$ an irreducible polynomial of degree m. Now we get $\mathbb{F}_{p^m}$ as a quotient $\mathbb{Z}_p[x]/\langle p(x)\rangle$, where $\langle p(x)\rangle$ is an ideal generated by $p(x)$.

Proposition 2.2. *For any finite field $\mathbb{F}$ the set of units, i.e. $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$, is a cyclic multiplicative group.*

A generator of $\mathbb{F}^*$ is called a primitive element of $\mathbb{F}$.

Definition 2.3. The *trace map* $\mathrm{Tr}_{\mathbb{F}} : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is defined by the formula

$$\mathrm{Tr}_{\mathbb{F}}(x) = x + x^p + \cdots + x^{p^{m-1}} \qquad \forall x \in \mathbb{F}_{p^m}.$$

The canonical additive character $e_{\mathbb{F}}$ of $\mathbb{F}_{p^m}$ is the mapping

$$e_{\mathbb{F}} : \mathbb{F}_{p^m} \to \mathbb{C}^*, \quad x \mapsto e^{\frac{2\pi i \,\mathrm{Tr}_{\mathbb{F}}(x)}{p}}.$$

Proposition 2.4. *All mappings $x \mapsto e_{\mathbb{F}}(ax)$, where $a \in \mathbb{F}$, are additive characters of $\mathbb{F}$. Moreover these are all additive characters.*

The following relations can be derived easily from the properties of the trace map.

1) $e_{\mathbb{F}}(x + y) = e_{\mathbb{F}}(x) + e_{\mathbb{F}}(y) \qquad \forall x, y \in \mathbb{F}$.

2) $e_{\mathbb{F}}(x^{2^i}) = e_{\mathbb{F}}(x) \qquad \forall x \in \mathbb{F},\ i \in \mathbb{N}_0$.

The next theorem is very elementary in the theory of character sums over finite fields. In addition it can be proved very easily.

Theorem 2.5. *Let $a \in \mathbb{F}_q$. Then*

$$\sum_{x \in \mathbb{F}_q} e_{\mathbb{F}}(ax) = \begin{cases} q & \text{if } a = 0, \\ 0 & \text{otherwise.} \end{cases}$$

For more general character sums we have the famous Weil–Carlitz–Uchiyama bound.

Theorem 2.6 (Carlitz–Uchiyama [1]). *Let $q = p^m$. If $f \in \mathbb{F}_q[x]$ satisfies the condition $f \neq g^p + g + b$ for all $g \in \mathbb{F}_q[x]$ and $b \in \mathbb{F}_q$, then*

$$\left| \sum_{x \in \mathbb{F}_q} e_{\mathbb{F}}\bigl(f(x)\bigr) \right| \leq (\deg f - 1)\sqrt{q}.$$

3 Galois rings and Witt vectors

We present two different constructions of the Galois rings. The first one is normally used in mathematical journals and uses much algebraic theory of rings. The second one is less formal and easier for person familiar with the algebra of finite fields. In this work we use mostly the second construction.

3.1 Galois rings as algebraic extensions

We try to construct a ring which is as much field–like as possible. This is done analogously to the construction of finite fields. For further details of Galois rings we refer interested reader to [9].

Let $\mathbb{Z}_q$ be a prime ring, where $q = p^e$ and $p \in \mathbb{P}$, $\mathbb{Z}_q[x]$ a ring of polynomials over $\mathbb{Z}_q$ and $p(x) \in \mathbb{Z}_q[x]$ a monic polynomial of degree m. Let also $\mu : \mathbb{Z}_q \to \mathbb{Z}_p$ be the reduction map modulo p. This mapping can be naturally extended to $\mathbb{Z}_q[x]$ where we reduce just the coefficients. If polynomial $\mu\big(p(x)\big)$ is irreducible in the ring $\mathbb{Z}_p[x]$, then $\mathbb{Z}_q[x]/\langle p(x)\rangle$ is a ring with q^m elements, characteristic q and as few non–invertible elements as possible. This ring is the Galois ring and it is denoted by $GR(q,m)$. We know in addition that $GR(q,m)$ is a local ring having unique maximal ideal $pGF(q,m)$.

From this point on we concentrate our attention only to the case $q = 2^2 = 4$ which is used in later chapters in coding–theoretic applications.

The units of $GR(4,m)$ have the following multiplicative group structure:

$$G(4,m)^* \simeq \mathbb{Z}_{2^m-1} \times \underbrace{\mathbb{F}_2 \times \cdots \times \mathbb{F}_2}_{m \text{ copies}}.$$

The cyclic subgroup of order $2^m - 1$ with the zero element is called *Teichmüller set* and denoted by $\mathcal{T}^a$. This $\mathcal{T}^a$ is isomorfic to the multiplicative group $\mathbb{F}^*_{2^m}$ with the zero element. Every element of $GR(4,m)$ can be uniquely expressed in the form $a + 2b$ where $a, b \in \mathcal{T}^a$.

3.2 Galois rings as Witt vector rings

Another way to construct the Galois ring $GR(q,m)$, where $q = p^e$, is to consider the elements of $GR(q,m)$ as vectors in $(\mathbb{F}_{p^m})^e$ with suitable addition and multiplication. We are mainly interested in the case $e = 2$ and $p = 2$. It should be noticed that ideas below can be generalized to cases with $e \neq 2$ and $p \neq 2$.

Definition 3.1. Let $W_2(\mathbb{F}_{2^m})$ be the set of ordered pairs $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ with elements in the finite field $\mathbb{F}_{2^m}$ equipped with addition and multiplication as follows:

(i) $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2 + a_1 b_1) \qquad \forall a_1, a_2, b_1, b_2 \in \mathbb{F}_{2^m}$,

(ii) $(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_1^2 b_2 + a_2 b_1^2) \qquad \forall a_1, a_2, b_1, b_2 \in \mathbb{F}_{2^m}$.

We call elements of the set $W_2(\mathbb{F}_{2^m})$ *Witt vectors* and the whole set *Witt vector ring.*

Notation 3.2. From this point on $\mathbb{F}$ is an abbreviation for $\mathbb{F}_{2^m}$ and R is an abbreviation for $W_2(\mathbb{F})$.

It is straightforward to prove the following proposition.

Proposition 3.3. *R is a commutative ring of 4^m elements and characteristic 4. It is also isomorfic to the Galois ring $GR(4, m)$.*

Remark 3.4. If we choose above $m = 1$ we see that $W_2(\mathbb{F}_2)$ is isomorfic to $G(4, 1) = \mathbb{Z}_4$. Isomorfism can be defined as $(0, 0) \mapsto 0$, $(1, 0) \mapsto 1$, $(0, 1) \mapsto 2$ and $(1, 1) \mapsto 3$.

Example 3.5. We calculate a little with the Witt vectors to get some idea of the ring R:

- $2(a_1, a_2) = (a_1, a_2) + (a_1, a_2) = (a_1 + a_1, a_2 + a_2 + a_1^2) = (0, a_1^2)$
- (a_1, a_2) is invertible iff $a_1 \neq 0$: $(a_1, a_2)^{-1} = (a_1^{-1}, a_2 a_1^{-4})$
- $-(a_1, a_2) = 3(a_1, a_2) = (a_1, a_2 + a_1^2)$

From the previous example we see that

$$R^* = \{(a_1, a_2) \in R \mid a_1 \neq 0\},$$

i.e. the set of units of R, is the set of Witt vectors for which the first component is non–zero. On the other hand the set of non–units is the set

$$2R = \{(0, a_2) \in R \mid a_2 \in \mathbb{F}\}.$$

Now the set $\{(a_1, 0) \in R \mid a_1 \in \mathbb{F}\}$ is closed under multiplication. It is isomorphic to the finite field $\mathbb{F}$ as a multiplicative structure and it is called *Teichmüller set* $\mathcal{T}$ (compare with $\mathcal{T}^a$ on page 5). Because of the relation

$$(a_1, 0) + 2(b_1, 0) = (a_1, 0) + (0, b_1^2) = (a_1, b_1^2)$$

every element of the ring R can be uniquely expressed in the form $\alpha + 2\beta$ where $\alpha, \beta \in \mathcal{T}$.

Remark 3.6. Let us take a generator a of $(\mathcal{T}^a)^* \subset GR(4,m)$ and a generator α of $\mathcal{T}^* \subset R$. We can now define an isomorphism between these Teichmüller sets by $a \mapsto \alpha$. Since we have the unique representations $a + 2b$ and $\alpha + 2\beta$ we can extend this isomorphism to an isomorphism from algebraic extension $GR(4,m)$ to the Witt vector ring R.

4 Character sums in Galois rings

In coding–theoretic applications of Galois ring theory estimates for character sums involving a polynomial with coefficients in R are needed. In these applications it is desirable that summation ranges over a multiplicative cyclic group and a natural one in the Galois rings is the Teichmüller set $\mathcal{T}$.

To define characters we need the notion of trace.

4.1 Automorfisms

The construction of the Witt vector ring is functorial in the following sense:

Theorem 4.1. *If $\psi : S \to T$ is a ring homomorfism (*$\mathrm{char}(S) = \mathrm{char}(T) = 2$*), then it induces a ring homomorfism*

$$W_2(\psi) : W_2(S) \to W_2(T),\ (a_1, a_2) \mapsto \big(\psi(a_1), \psi(a_2)\big).$$

Proof. We have

$$\begin{aligned}
W_2(\psi)\big((a_1, a_2) + (b_1, b_2)\big) &= W_2(\psi)\big((a_1 + b_1, a_2 + b_2 + a_1 b_1)\big) \\
&= \big(\psi(a_1 + b_1), \psi(a_2 + b_2 + a_1 b_1)\big) \\
&= \big(\psi(a_1) + \psi(b_1), \psi(a_2) + \psi(b_2) + \psi(a_1)\psi(b_1)\big) \\
&= \big(\psi(a_1), \psi(a_2)\big) + \big(\psi(b_1), \psi(b_2)\big) \\
&= W_2(\psi)\big((a_1, a_2)\big) + W_2(\psi)\big((b_1, b_2)\big)
\end{aligned}$$

and the multiplication property can be proved similarly. □

With this construction we can lift the automorfisms of $\mathbb{F}$ to ring automorphisms of $W_2(\mathbb{F})$.

We know that the Frobenius map $F : \mathbb{F} \to \mathbb{F},\ x \mapsto x^2$ generates all the field automorfisms of $\mathbb{F}$. So the automorfism group of $\mathbb{F}$ contains exactly the mappings F^i where $0 \le i \le m-1$. Lifting these mappings as above we get

$$W_2(F^i) :\ (a_1, a_2) \longmapsto (a_1^{2^i}, a_2^{2^i}).$$

We should notice that $(a_1, a_2)^2 = (a_1^2, a_1^2 a_2 + a_2 a_1^2) = (a_1^2, 0) \neq (a_1^2, a_2^2)$ and hence $(a_1^{2^i}, a_2^{2^i})$ is not generally the same as $(a_1, a_2)^{2^i}$.

The ring of fixed points of $W_2(F^i)$ is clearly the ring $W_2(\mathbb{F}_2) \simeq \mathbb{Z}_4$. So we have as many automorfisms with fixed points in $\mathbb{Z}_4$ as is the degree of extension $GR(4, m)$ over $\mathbb{Z}_4$. This is an analogue to the extension of prime fields and therefore the rings $GR(4, m) \simeq W_2(\mathbb{F})$ are called Galois rings.

4.2 Trace and additive characters

Now we can define a trace map similar to one in the theory of finite fields.

Definition 4.2. We call the mapping

$$\mathrm{Tr} : R \to W_2(\mathbb{F}_2), \quad x \mapsto \sum_{i=0}^{m-1} W_2(F^i)(x)$$

the *trace map* of R.

The above definition is quite uninformative and therefore we write it in a little longer form.

$$\begin{aligned}\mathrm{Tr}\left((a,b)\right) &= \sum_{i=0}^{m-1}(a^{2^i}, b^{2^i}) = \left(\sum_{i=0}^{m-1} a^{2^i}, \sum_{i=0}^{m-1} b^{2^i} + \sum_{0\le i<j\le m-1} a^{2^i}a^{2^j}\right)\\ &= \left(\mathrm{Tr}_{\mathbb{F}}(a), \mathrm{Tr}_{\mathbb{F}}(b) + \sum_{0\le i<j\le m-1} a^{2^i}a^{2^j}\right)\end{aligned}$$

The componentwise trace in the last formula is naturally the usual trace in the finite field $\mathbb{F}$ defined in Definition 2.3. If $a, b \in \mathbb{F}$ have minimal polynomials $x^s + a_1x^{s-1} + a_2x^{s-2} + \cdots + a_s$ and $x^t + b_1x^{t-1} + b_2x^{t-2} + \cdots + b_t$ in $\mathbb{F}_2[x]$, respectively, then $\mathrm{Tr}\left((a,b)\right) = (a_1, b_1 + a_2)$ and clearly $\mathrm{Tr}\left((a,b)\right)$ belongs to the ring $W_2(\mathbb{F}_2)$.

Remark 4.3. As we have seen $W_2(\mathbb{F}_2)$ is isomorphic to $\mathbb{Z}_4$ and usually we interpret the trace map as a mapping $R \to \mathbb{Z}_4$.

Lemma 4.4. *The trace map* $\mathrm{Tr} : R \to \mathbb{Z}_4$ *is* $\mathbb{Z}_4$*-linear.*

Proof. The mapping $W_2(F)$ is linear:

$$\begin{aligned}W_2(F)\big((a_1,a_2)+(b_1,b_2)\big) &= W_2(F)\big((a_1+b_1, a_2+b_2+a_1b_1)\big)\\ &= \big((a_1+b_1)^2, (a_2+b_2+a_1b_1)^2\big) = (a_1^2+b_1^2, a_2^2+b_2^2+a_1^2b_2^2)\\ &= (a_1^2, a_2^2) + (b_1^2, b_2^2) = W_2(F)\big((a_1,a_2)\big) + W_2(F)\big((b_1,b_2)\big).\end{aligned}$$

This implies the additiveness of the trace map. Then $\mathbb{Z}_4$-linearity follows from the fact that $\mathrm{char}(R) = 4$. $\square$

Definition 4.5. The *canonical additive character* of R is the mapping

$$e : R \to \mathbb{C}^*, \quad x \mapsto i^{\mathrm{Tr}(x)}$$

where $\mathrm{Tr}(x)$ is thought as an element of $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

The following proposition can be proved as in the case of finite fields.

Proposition 4.6. *All additive characters of R are of the form*

$$\psi_a : x \mapsto e(ax) \qquad \forall x \in R$$

for some $a \in R$.

We list here the most fundamental properties of the canonical additive character e.

1) $e(x+y) = e(x)e(y) \qquad \forall x, y \in R.$

2) $e\big(W_2(F^i)(x)\big) = e(x) \qquad \forall x \in R,\ 0 \leq i \leq m-1.$

3) $e\big((0,a)\big) = e_{\mathbb{F}}(a) = (-1)^{\mathrm{Tr}_{\mathbb{F}}(a)} \qquad \forall a \in \mathbb{F}.$

4.3 Some simple character sums

Theorem 4.7. *Let $a \in R$. Then the sum*

$$S(a) = \sum_{x \in \mathcal{T}} e(ax)$$

has one of the following moduli

(i) $|S(a)| = 2^m \ \Leftrightarrow\ a = 0,$

(ii) $|S(a)| = 0 \ \Leftrightarrow\ a \in 2R, a \neq 0,$ *i.e. a is a non–zero non–unit,*

(iii) $|S(a)| = 2^{\frac{m}{2}} \ \Leftrightarrow\ a$ *is a unit.*

Proof. Case (i) is clear: $e(0x) = e(0) = 1\ \forall x \in \mathcal{T}$.

In case (ii) $a = (0, a_2)$ for some $a_2 \in \mathbb{F}^*$ and therefore $ax = (0, a_2)(x_1, 0) = (0, a_2 x_1^2)$. This implies that $e(ax) = e_{\mathbb{F}}(a_2 x_1^2) = e_{\mathbb{F}}(\sqrt{a_2} x_1)$ and by Theorem 2.5 the sum vanishes.

Case (iii): Let $a = (a_1, a_2)$, $x = (x_1, 0)$ and $y = (y_1, 0)$. Then

$$\begin{aligned} |S(a)|^2 &= \sum_{x \in \mathcal{T}} e(ax) \overline{\sum_{y \in \mathcal{T}} e(ay)} = \sum_{x,y \in \mathcal{T}} e(ax)\overline{e(ay)} \\ &= \sum_{x,y \in \mathcal{T}} e(ax)e(-ay) = \sum_{x,y \in \mathcal{T}} e\big(a(x-y)\big) \\ &= \sum_{x_1, y_1 \in \mathbb{F}} e\big((a_1, a_2)[(x_1, 0) - (y_1, 0)]\big) \end{aligned}$$

Above we have used the fact: $e(x)e(-x) = e(x-x) = e(0) = 1$, but also $e(x)\overline{e(x)} = |e(x)|^2 = 1$ so $e(-x) = e(x)^{-1} = \overline{e(x)}$. Clearly $(x_1, 0) - (y_1, 0) = (x_1, 0) + (y_1, y_1^2) = (x_1 + y_1, y_1^2 + x_1 y_1) = (x_1 + y_1, y_1(x_1 + y_1))$. As x_1 and y_1 range over $\mathbb{F}$ so does $z = x_1 + y_1$. By substituting $z = x_1 + y_1$ we get

$$\begin{aligned}(a_1, a_2)[(x_1, 0) - (y_1, 0)] &= (a_1, a_2)(z, y_1 z) = (a_1 z, a_2 z^2 + a_1^2 y_1 z)\\ &= (a_1 z, a_2 z^2) + (0, a_1^2 y_1 z).\end{aligned}$$

Hence

$$|S(a)|^2 = \sum_{z, y_1 \in \mathbb{F}} e\big((a_1 z, a_2 z^2)\big) e\big((0, a_1^2 y_1 z)\big) = \sum_{z \in \mathbb{F}} e\big((a_1 z, a_2 z^2)\big) \sum_{y_1 \in \mathbb{F}} e_{\mathbb{F}}(a_1^2 y_1 z)$$

As a is unit we have $a_1 \neq 0$. The latter sum above is therefore 0 unless $z = 0$ when the sum is equal to 2^m. So we have

$$|S(a)|^2 = e\big((0,0)\big) 2^m = 2^m.$$

$\square$

Corollary 4.8. *Let $a, b \in R$. We have same moduli distribution as in Theorem 4.7 for the sum*

$$S(a,b) = \sum_{x \in \mathcal{T}} e(ax + b)$$

Or more exactly $|S(a,b)| = |S(a)|$.

Proof. We have $e(ax+b) = e(ax)e(b)$ and we just take $e(b)$ as a common factor for the sum. We notice that $|e(b)| = 1$ and the claim follows. $\square$

We can say even more about the values of $S(a)$ and this extra information can be used to get more strict bound for the real part of this character sum.

Theorem 4.9. *If $a \in R$ is a unit, then*

(i) $S(a) \in \{\pm 2^{\frac{m}{2}}, \pm i 2^{\frac{m}{2}}\}$, *if* $2 \mid m$, *or*

(ii) $S(a) \in \{\pm 2^{\frac{m-1}{2}} \pm i 2^{\frac{m-1}{2}}\}$, *if* $2 \nmid m$.

In particular, $\big|\Re\big(S(a)\big)\big| \leq 2^{\frac{m-1}{2}}$ when $2 \nmid m$, where $\Re(x)$ denotes the real part of x.

Proof. Clearly $S(a) = u + iv$ where $u, v \in \mathbb{Z}$. By Theorem 4.7 we have

$$u^2 + v^2 = 2^m.$$

If $u = 0$ or $v = 0$ we have the case (i). So suppose that $u \neq 0 \neq v$. We separate the even parts of u and v and get

$$u = 2^s u', \qquad v = 2^t v', \qquad 2 \nmid u',\ 2 \nmid v',\ s, t \in \mathbb{N}_0.$$

If $s > t$, we derive

$$u^2 + v^2 = 2^{2t}(2^{2s-2t}u'^2 + v'^2) = 2^m$$

and therefore 2^m has an odd factor which is absurd. Similarly condition $s < t$ leads to a contradiction. So we must have $s = t$. Now

$$2^m = 2^{2s}(u'^2 + v'^2),$$

i.e. $u'^2 + v'^2$ is a power of 2. On the other hand $(2k+1)^2 = 4k^2 + 4k + 1$ and hence the square of any odd number is congruent to 1 modulo 4. This implies

$$u'^2 + v'^2 \equiv 2 \pmod 4$$

which is possible only in the case $u'^2 + v'^2 = 2$. So we have $u', v' \in \{\pm 1\}$ and the theorem follows. □

Corollary 4.10. *The character sums $S(a, b) = \sum_{x \in \mathcal{T}} e(ax + b)$ get the same values as the sum $S(a)$. In particular, $\left|\Re\big(S(a, b)\big)\right| \leq 2^{\frac{m-1}{2}}$ when $2 \nmid m$.*

Proof. We have as earlier $S(a, b) = e(b)S(a)$ and values of $e(b)$ belong to the set $\{\pm 1, \pm i\}$. The claim follows now straightforwardly from Theorem 4.9. □

We prove now a similar result for certain polynomials of degree 3.

Theorem 4.11. *Let $f(x) = ax + 2bx^3 \in R[x] \setminus \{0\}$ be a polynomial. Then values of the sum*

$$T(a, b) = \sum_{x \in \mathcal{T}} e\big(f(x)\big)$$

satisfy the following conditions:

(i) $T(a, b) \in \{0, \pm 2^{\frac{m}{2}}, \pm i2^{\frac{m}{2}}, \pm 2^{\frac{m}{2}} \pm i2^{\frac{m}{2}}, \pm 2^{\frac{m+2}{2}}, \pm i2^{\frac{m+2}{2}}\}$, *if $2 \mid m$, or,*

(ii) $T(a,b) \in \{0, \pm 2^{\frac{m-1}{2}} \pm i2^{\frac{m-1}{2}}, \pm 2^{\frac{m+1}{2}}, \pm i2^{\frac{m+1}{2}}, \pm 2^{\frac{m+1}{2}} \pm i2^{\frac{m+1}{2}}\}$, *if* $2 \nmid m$.

In particular, $\left|\Re\big(T(a,b)\big)\right| \le 2^{\frac{m+1}{2}}$ *when* $2 \nmid m$.

Proof. We can choose $a = (a_1, a_2^2)$ and $2b = (0, b_2^2)$ because every element of $\mathbb{F}$ can be expressed in the form x^2, $x \in \mathbb{F}$. This simplifies calculations later. Let also $x = (x_1, 0)$ and $y = (y_1, 0)$ and thus we have

$$\begin{aligned} f(x) &= (a_1, a_2^2)(x_1, 0) + (0, b_2^2)(x_1^3, 0) = (a_1 x_1, a_2^2 x_1^2 + b_2^2 x_1^6) \\ &\approx (a_1 x_1, a_2 x_1 + b_2 x_1^3) \end{aligned}$$

where we have used the fact: $e\big((a_1^{2^l}, a_2^{2^m})\big) = e\big((a_1, a_2)\big)$. So these $\approx$-equalities hold only when taking e from both sides. Next we calculate

$$\begin{aligned} f(x) - f(y) &\approx \big(a_1(x_1 + y_1), a_2(x_1 + y_1) + b_2(x_1^3 + y_1^3) + a_1^2 y_1(x_1 + y_1)\big) \\ &= \big(a_1 z, a_2 z + b_2(z^3 + y_1 z^2 + y_1^2 z) + a_1^2 y_1 z\big) \end{aligned}$$

where we subsituted $z = x_1 + y_1$. As usual we separate a part with z's and get

$$\begin{aligned} |T(a,b)|^2 &= \sum_{x,y \in \mathcal{T}} e\big(f(x) - f(y)\big) \\ &= \sum_{z \in \mathcal{T}} e\big((a_1 z, a_2 z + b_2 z^3)\big) \sum_{y_1 \in \mathbb{F}} e_{\mathbb{F}}\big(b_2(y_1 z^2 + y_1^2 z) + a_1^2 y_1 z\big) \\ &= \sum_{z \in \mathcal{T}} e\big((a_1 z, a_2 z + b_2 z^3)\big) \sum_{y_1 \in \mathbb{F}} e_{\mathbb{F}}\big(y_1^2(b_2^2 z^4 + b_2 z + a_1^4 z^2)\big) \qquad (1) \end{aligned}$$

where we have used a relation $e_{\mathbb{F}}(x^{2^i} + y^{2^j}) = e_{\mathbb{F}}(x^{2^i}) e_{\mathbb{F}}(y^{2^j}) = e_{\mathbb{F}}(x) e_{\mathbb{F}}(y) = e_{\mathbb{F}}(x + y)$ for the additive characters of the field $\mathbb{F}$.

In the latter sum we have a polynomial $p(z) = b_2^2 z^4 + b_2 z + a_1^4 z^2$ as a factor of y^2. This polynomial is *linearized* in the sense that $p(u+v) = p(u) + p(v)$ and therefore zeros of this polynomial form a subspace over $\mathbb{F}_2$. This implies that number of zeros of $p(z)$ is 1,2,4 or 2^m in the case that $p(z) \equiv 0$. The last case is possible only if $b_2 = a_1 = 0$ and because $f(x) \not\equiv 0$ we must have $a_2 \neq 0$ and hence the first sum in (1) becomes 0. So we can conclude as usual that

$$|T(a,b)|^2 \in \{0, 2^m, 2 \cdot 2^m, 4 \cdot 2^m\}.$$

We can now complete the proof as in Theorem 4.9 with the relation

$$|T(a,b)|^2 = u^2 + v^2 = 2^{m+i} \quad 0 \le i \le 2, \quad u, v \in \mathbb{Z}.$$

□

Corollary 4.12. *Also values of $\sum_{x\in\mathcal{T}} e(c+ax+2bx^3)$ satisfy the conditions of Theorem 4.11.*

We can do the same things to certain polynomials of degree 5.

Theorem 4.13. *Let $f(x) = ax + 2bx^3 + 2cx^5 \in R[x] \setminus \{0\}$ be a polynomial. Then sum*

$$U(a,b,c) = \sum_{x\in\mathcal{T}} e\big(f(x)\big)$$

has one of the following values:

(i) $U(a,b,c) \in \{0, \pm 2^{\frac{m}{2}}, \pm i2^{\frac{m}{2}}, \pm 2^{\frac{m}{2}} \pm i2^{\frac{m}{2}}, \pm 2^{\frac{m+2}{2}}, \pm i2^{\frac{m+2}{2}}, \pm 2^{\frac{m+2}{2}} \pm i2^{\frac{m+2}{2}}, \pm 2^{\frac{m+4}{2}}, \pm i2^{\frac{m+4}{2}}\}$, *if* $2 \mid m$, *or,*

(ii) $U(a,b,c) \in \{0, \pm 2^{\frac{m-1}{2}} \pm i2^{\frac{m-1}{2}}, \pm 2^{\frac{m+1}{2}}, \pm i2^{\frac{m+1}{2}}, \pm 2^{\frac{m+1}{2}} \pm i2^{\frac{m+1}{2}}, \pm 2^{\frac{m+3}{2}}, \pm i2^{\frac{m+3}{2}}, \pm 2^{\frac{m+3}{2}} \pm i2^{\frac{m+3}{2}}\}$, *if* $2 \nmid m$.

In particular, $\big|\Re\big(U(a,b,c)\big)\big| \le 2^{\frac{m+3}{2}}$ *when* $2 \nmid m$.

Proof. Let $a = (a_1, a_2^2)$, $2b = (0, b_2^2)$, $2c = (0, c_2^2)$, $x = (x_1, 0)$ and $y = (y_1, 0)$. By using same tricks as in Theorem 4.11 we get

$$\begin{aligned} f(x) &= (a_1, a_2^2)(x_1, 0) + (0, b_2^2)(x_1^3, 0) + (0, c_2^2)(x_1^5) \\ &= (a_1x_1, a_2^2x_1^2 + b_2^2x_1^6 + c_2^2x_1^{10}) \\ &\approx (a_1x_1, a_2x_1 + b_2x_1^3 + c_2x_1^5) \end{aligned}$$

and

$$\begin{aligned} &f(x) - f(y) \\ &\approx \big(a_1(x_1+y_1), a_2(x_1+y_1) + b_2(x_1^3+y_1^3) + c_2(x_1^5+y_1^5) + a_1^2y_1(x_1+y_1)\big) \\ &\qquad = \big(a_1z, a_2z + b_2(z^3 + z^2y_1 + zy_1^2) + c_2(z^5 + z^4y_1 + zy_1^4) + a_1^2y_1z\big) \end{aligned}$$

where $(z+y_1)^5 = z^5 + z^4y_1 + zy_1^4 + y_1^5$. So finally we get a familiar form

$$\begin{aligned} |U(a,b,c)|^2 =& \sum_{z\in\mathcal{T}} e\big((a_1z, a_2z + b_2z^3 + c_2z^5)\big) \\ & \sum_{y_1\in\mathbb{F}} e_{\mathbb{F}}(b_2z^2y_1 + b_2zy_1^2 + c_2z^4y_1 + c_2zy_1^4 + a_1^2y_1z) \\ =& \sum_{z\in\mathcal{T}} e\big((a_1z, a_2z + b_2z^3 + c_2z^5)\big) \\ & \sum_{y_1\in\mathbb{F}} e_{\mathbb{F}}\big(y_1^4(\underbrace{b_2^4z^8 + b_2^2z^2 + c_2^4z^{16} + c_2z + a_1^8z^4}_{=L(z)})\big) \\ =& 2^m \sum_{\substack{z\in\mathcal{T} \\ L(z)=0}} e\big((a_1z, a_2z + b_2z^3 + c_2z^5)\big) =: 2^mV(a,b,c). \end{aligned}$$

The following final trick is due to Hannu Tarnanen.

We have as a factor of y_1^4 linearized polynomial $L(z)$ which zeros form a group, say X_0, under addition. The set X_0 is also a subspace of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ but it is not the whole space because $f(x)$ was not the zero polynomial. Hence

$$|X_0| \in \{0, 1, 2, 4, 8, 16\}.$$

We know that $V(a,b,c)$ is real and non–negative, but in order to use the same method as in the previous theorems we should know that the value of $V(a,b,c)$ is a power of 2. It could happen that in $V(a,b,c)$ we have 14 ones, i and $-i$ as summands and then we have 14 as a sum. For this end we consider the values of $|V(a,b,c)|^2$.

The summands of $V(a,b,c)$ have exactly the same form as summands in $U(a,b,c)$ but we have just restricted the range of the variable. We do exactly the same tricks for $|V(a,b,c)|^2$ as for $|U(a,b,c)|$ and get similar expression where only thing that differs is the range of variables. Substituting $z = s+t$ for variables ranging over X_0 is valid since X_0 is a group under addition. So

$$\begin{aligned}
|V(a,b,c)|^2 &= V(a,b,c)^2 \\
&= \sum_{s\in X_0} e\big((a_1 s, a_2 s + b_2 s^3 + c_2 s^5)\big) \sum_{t\in X_0} e_{\mathbb{F}}\big(s^4 L(t)\big) \\
&= |X_0| V(a,b,c)
\end{aligned}$$

This implies that

$$V(a,b,c) = 0 \quad \text{or} \quad V(a,b,c) = |X_0|$$

and we can complete the proof as before with the argument

$$|U(a,b,c)|^2 = u^2 + v^2 = 2^{m+i} \quad 0 \le i \le 4, \quad u, v \in \mathbb{Z}.$$

□

Corollary 4.14. *Values of* $\sum_{x\in\mathcal{T}} e(d+ax+2bx^3+2cx^5)$ *satisfy the conditions of Theorem 4.13.*

The above techniques can be generalized for polynomials of a certain type. We state the next theorem without proof.

Theorem 4.15. *Let m be odd, $1 \le r \le \frac{m-1}{2}$ and $f(x) = a_0 x + 2\sum_{i=1}^{r} a_i x^{1+2^i} \in R[x]$. Then*

$$\Re\left(\sum_{x\in\mathcal{T}} e\big(f(x)\big)\right) \le 2^{r-\frac{1}{2}} 2^{\frac{m}{2}}$$

and moreover this bound is thight.

The bound $r \leq \frac{m-1}{2}$ comes from the observation that if we have $r = \frac{m+1}{2}$ then the previous theorem gives the trivial upper bound 2^m.

One special case of the polynomials covered by the previous theorem is a binomial with terms of degree 1 and $\frac{m-1}{2}$. In this special case we can tighten the bound as the theorem below shows.

Theorem 4.16. *Let $m = 2j+1$ and $f(x) = ax + 2bx^{2^j+1} \in R[x]$. Then*

$$|Y(a,b)| = \sum_{x \in \mathcal{T}} e\big(f(x)\big) \leq 2 \cdot 2^{\frac{m}{2}}.$$

Proof. Let $a = (a_1, a_2)$ and $2b = (0, b_2)$. As in the case $f(x) = ax$ we get

$$|Y(a,b)|^2 = \sum_{x,y \in \mathcal{T}} e\big(f(x) - f(y)\big).$$

Likewise

$$\begin{aligned} f(x) - f(y) &= (a_1, a_2)(x_1, 0) + (0, b_2)(x_1, 0)^{2^j+1} - (a_1, a_2)(y_1, 0) - (0, b_2)(y_1, 0)^{2^j+1} \\ &= (a_1 x_1, a_2 x_1^2) + (0, b_2 x_1^{2^{j+1}+2}) - (a_1 y_1, a_2 y_1^2) - (0, b_2 y_1^{2^{j+1}+2}) \\ &= (a_1 x_1, a_2 x_1^2 + b_2 x_1^{2^{j+1}+2}) + (a_1 y_1, a_2 y_1^2 + b_2 y_1^{2^{j+1}+2} + a_1^2 y_1^2) \\ &= \big(a_1(x_1 + y_1), a_2(x_1^2 + y_1^2) + b_2(x_1^{2^{j+1}+2} + y_1^{2^{j+1}+2}) + a_1^2(y_1^2 + x_1 y_1)\big) \\ &= \big(a_1 z, a_2 z^2 + b_2(z^{2^{j+1}+2} + x_1^{2^{j+1}} z^2 + x_1^2 z^{2^{j+1}}) + a_1^2(z^2 + x_1 z)\big) \end{aligned}$$

by substituting $z = x_1 + y_1$ and noticing that $x_1^2 + y_1^2 = (x_1 + y_1)^2$ and $x_1^{2^{j+1}+2} + y_1^{2^{j+1}+2} = [x_1^{2^j+1} + (x_1 + z)(x_1^{2^j} + z^{2^j})]^2$.

Now we can separate terms including x_1 and have

$$\begin{aligned} |Y(a,b)| = \sum_{z \in \mathbb{F}} & e\big((a_1 z, a_1^2 z^2 + a_2 z^2 + b_2 z^{2^{j+1}+2})\big) \cdot \\ & \sum_{x_1 \in \mathbb{F}} e_{\mathbb{F}}(a_1^2 x_1 z + b_2 x_1^{2^{j+1}} z^2 + b_2 x_1^2 z^{2^{j+1}}) \end{aligned} \tag{2}$$

We can use the relation $e_{\mathbb{F}}(x^{2^i} + y^{2^j}) = e_{\mathbb{F}}(x^{2^i}) e_{\mathbb{F}}(y^{2^j}) = e_{\mathbb{F}}(x) e_{\mathbb{F}}(y) = e_{\mathbb{F}}(x + y)$ for the additive characters of the field $\mathbb{F}$ to get the polynomial of the latter sum to form

$$a_1^2 x_1 z + (b_2 x_1^{2^{j+1}} z^2)^{2^j} + (b_2 x_1^2 z^{2^{j+1}})^{2^{2j}} = x_1(a_1^2 z + b_2^{2^j} z^{2^{j+1}} + b_2^{2^{2j}} z^{2^j} = x_1 p(z)$$

where exponents are reduced according to the relation $x^{2^m} = x$.

A zero $\alpha \in \mathbb{F}$ of $p(z)$ is also a zero of a polynomial

$$q(z) = a_1^{2^{j+2}} z^{2^{j+1}} + b_2 z^2 + b_2^{2^j} z \equiv p(z)^{2^{j+1}} \pmod{z^{2^m} + z, b_2^{2^m} + b_2}$$

and also a zero of a polynomial

$$r(z) = a_1^{2^{j+2}} p(z) + b_2^{2^j} q(z) = a_1^{2^{j+2}+2} z + a_1^{2^{j+2}} b_2^{2^{2j}} z^{2^j} + b_2^{2^j+1} z^2 + b_2^{2^{j+1}} z.$$

In the previous trick we get terms with factor $z^{2^{j+1}}$ cancelled. In the same manner we can construct $\mathbb{F}$-linear combination $s(z)$ of $r(z)^2$ and $q(z)$ to get term with factor z^{2^j} cancelled from $r(z)$. Hence $s(z)$ will be of the form $a_1^{2^{j+2}} b_2 q(z) + r(z)^2$ and the coefficient for the term with the highest degree 4 is

$$b_2^{2^{j+1}+2}$$

which is clearly non–zero iff b_2 is non–zero. If b_2 is zero, then claim follows directly from Theorem 4.7.

If b_2 is non–zero, then $p(z)$ has at most 4 zeros because every zero of $p(z)$ is also a zero of $s(z)$ which has at most 4 zeros. When z is a non–zero of $p(z)$ the latter sum in (2) vanishes and when z is a zero of $p(z)$ the latter sum equals to 2^m. Therefore $|Y(a,b)|^2 \leq 4 \cdot 2^m$ and this concludes the proof. □

4.4 An upper bound for certain character sums

Now we shall present an upper bound for the moduli of certain character sums over R analogous to the Carlitz–Uchiyama bound presented in Theorem 2.6. The original result [6] concerns all Galois rings.

Definition 4.17. We call a polynomial $f(x) = \sum_{i=0}^{k} f_i x^i \in R[x]$ *non–degenerate* if $f_i = 0$ for all even i.

Definition 4.18. Let $f(x) = \sum_{i=0}^{n} f_i x^i \in R[x]$ be a non–degenerate polynomial where $f_i = (a_i, b_i)$. The *weighted degree* of a term $f_i x^i$ is $2i$ if f_i is a unit, i.e. $a_i \neq 0$, and i if f_i is a non–zero non–unit, i.e. $a_i = 0$ and $b_i \neq 0$.

The *weighted degree* N_f of the polynomial $f(x)$ is then the maximum of the weighted degrees of the terms in $f(x)$.

Theorem 4.19 (Kumar–Helleseth–Calderbank). *Let* $f(x) = \sum_{i=0}^{n} a^{(i)} x^i \in R[x] \setminus \{0\}$ *be a non–degenerate polynomial with a weighted degree* N_f*. Then*

$$\left| \sum_{x \in \mathcal{T}} e\big(f(x)\big) \right| \leq (N_f - 1) 2^{\frac{m}{2}}.$$

Part II
$\mathbb{Z}_4$-linear codes and sequences

5 $\mathbb{Z}_4$-linear codes

Galois rings discussed in earlier chapters are now used in the construction of linear codes over alphabet $\mathbb{Z}_4$. This is analogous to the use of finite fields in the construction of binary linear codes.

Those codes over $\mathbb{Z}_4$ are further mapped to binary codes which are usually non–linear. Ideas presented in this section were introduced in the article [2] by Hammons et al. in 1994.

Definition 5.1. Set $C \subseteq \mathbb{Z}_4^n$ is called $\mathbb{Z}_4$-*code* of length n. If C is also a submodule of $\mathbb{Z}_4^n$ then C is *linear*.

5.1 Gray map

In order to get binary codes from $\mathbb{Z}_4$-codes we define the Gray map.

Definition 5.2. The *Gray map* is the mapping $\mathcal{G} : \mathbb{Z}_4 \to \mathbb{F}_2 \times \mathbb{F}_2$

$$0 \mapsto 00,\ 1 \mapsto 01,\ 2 \mapsto 11,\ 3 \mapsto 10.$$

This can be viewed as consisting of two component maps π and $\nu : \mathbb{Z}_4 \to \mathbb{F}_2$

$$\mathcal{G}(x) = \big(\pi(x), \nu(x)\big) \quad x \in \mathbb{Z}_4.$$

The map $\mathcal{G}$ can be naturally extended to a mapping $\mathcal{G} : \mathbb{Z}_4^n \to \mathbb{F}_2^{2n}$

$$\mathcal{G}(\mathbf{a}) = \big(\pi(\mathbf{a}), \nu(\mathbf{a})\big) \quad \mathbf{a} \in \mathbb{Z}_4^n,$$

where maps π and ν are taken componentwise.

Definition 5.3. The *Lee weights* of $0, 1, 2, 3 \in \mathbb{Z}_4$ are $0, 1, 2, 1$, respectively, and the Lee weight of a vector $\mathbf{a} \in \mathbb{Z}_4^n$ is the sum of Lee weights of its components. This weight is denoted by $w_L(\mathbf{a})$.

The Lee weight induces *Lee metric* $d_L(\mathbf{a}, \mathbf{b}) = w_L(\mathbf{a} - \mathbf{b})$ in $\mathbb{Z}_4^n$. One can easily see that d_L really is a metric.

We can see from the Hamming weights of the Gray map images that the following lemma holds.

Lemma 5.4. *The Gray map* $\mathcal{G} : (\mathbb{Z}_4^n, d_L) \to (\mathbb{F}_2^{2n}, d_H)$ *is an isometry of metric spaces.*

In above d_H stands for the usual Hamming distance of binary vectors.

In addition we can connect the Lee metric to an inner product.

Definition 5.5. The *inner product* of two vectors $\mathbf{a} = (a_0, \ldots, a_{n-1})$ and $\mathbf{b} = (b_0, \ldots, b_{n-1})$ in $\mathbb{Z}_4^n$ is

$$\rho(\mathbf{a}, \mathbf{b}) = \Re \left(\sum_{k=0}^{n-1} i^{a_k - b_k} \right).$$

The Lee weight of an element $x \in \mathbb{Z}_4$ can be expressed as

$$w_L(x) = 1 - \Re(i^x).$$

Hence we have the following relation between the Lee metric and the inner product

$$d_L(\mathbf{a}, \mathbf{b}) = n - \rho(\mathbf{a}, \mathbf{b}).$$

Definition 5.6. Binary code $C \subseteq \mathbb{F}_2^{2n}$ is called $\mathbb{Z}_4$-*linear*, if it is the image of a linear $\mathbb{Z}_4$-code C_4 of length n under the Gray map, i.e. $\mathcal{G}(C_4) = C$.

From the discussion above and lemma 5.4 we get the following theorem.

Theorem 5.7. *Let* C_4 *be* $\mathbb{Z}_4$*-code of length* n *and* $C = \mathcal{G}(C_4)$ *be its image under the Gray map. Then the minimum distance* $d_{\min}$ *of the binary code* C *is given by*

$$d_{\min} = n - \max\{\rho(\mathbf{a}, \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in C_4, \mathbf{a} \neq \mathbf{b}\} =: n - \rho_{\max}.$$

5.2 The Kerdock code $\mathcal{K}$

One of the best binary codes is the so–called Kerdock code which is non–linear. This code has much more codewords than the best known binary linear codes. In order to handle non–linear codes they should have some algebraic structure. One such a structure was found in [2] where the $\mathbb{Z}_4$-codes described below were represented by generator matrices over R. We use the trace form which is in our investigations much easier. These trace forms can be found for example in [11] and [3].

Definition 5.8. Let x_i, $0 \le i \le 2^m - 1$, be some enumeration of the elements of $\mathcal{T} \subset R$. For example $x_0 = 0$ and $x_i = (\gamma^i, 0)$, $1 \le i \le 2^m - 1$, for some primitive element γ of $\mathbb{F}$.

The $\mathbb{Z}_4$-*Kerdock code* $\mathcal{K}_4 \subset \mathbb{Z}_4^{2^m}$ is the set of vectors

$$\mathbf{k}(a,b) = \big(\operatorname{Tr}(ax_i) + b\big)_{i=0}^{2^m-1}, \quad a \in R,\ b \in \mathbb{Z}_4.$$

The *Kerdock code* $\mathcal{K} \subset \mathbb{F}_2^{2^{m+1}}$ is the Gray image of $\mathcal{K}_4$, i.e. $\mathcal{K} = \mathcal{G}(\mathcal{K}_4)$.

We can easily see that $\mathcal{K}_4$ is linear and hence $\mathcal{K}$ is $\mathbb{Z}_4$-linear: $\big(\mathbf{k}(a,b) + \mathbf{k}(c,d)\big)_i = \operatorname{Tr}(ax_i) + b + \operatorname{Tr}(cx_i) + d = \operatorname{Tr}\big((a+c)x_i\big) + (b+d)$ and $\big(f\mathbf{k}(a,b)\big)_i = f\big(\operatorname{Tr}(ax_i) + b\big) = \operatorname{Tr}\big((fa)x_i\big) + fb$ for $f \in \mathbb{Z}_4$.

With our knowledge of the character sums we can easily prove the following theorem.

Theorem 5.9. *The Kerdock code $\mathcal{K}$ has parameters*

$$\textit{length} = 2^{m+1}, \quad \textit{size} = 4^{m+1}, \quad \textit{and} \quad d_{\min} = \begin{cases} 2^m - 2^{\frac{m}{2}} & \textit{if } 2 \mid m \\ 2^m - 2^{\frac{m-1}{2}} & \textit{if } 2 \nmid m \end{cases}.$$

Proof. The Gray map doubles the length of a code so it is clear from the construction that $\mathcal{K}$ has length $2 \cdot 2^m$.

We can choose parameter a in $|R| = 4^m$ different ways and b in 4 different ways. So the size of $\mathcal{K}$ is $4 \cdot 4^m$. The fact that all codewords really are different follows from the discussion below.

We calculate next the inner product of two distinct codewords

$$\begin{aligned} \rho\big(\mathbf{k}(a,c), \mathbf{k}(b,d)\big) &= \Re\left(\sum_{j=0}^{2^m-1} i^{\operatorname{Tr}(ax_j)+c-\operatorname{Tr}(bx_j)-d}\right) \\ &= \Re\left(i^{c-d} \sum_{x \in \mathcal{T}} e\big((a-b)x\big)\right) \\ &= \Re\big(i^{c-d} S(a-b)\big). \end{aligned}$$

The inner product is equal to 2^m only if $a = b$ and $c = d$. Therefore codewords must be different from each other.

We know from Theorems 4.7 and 4.9 that

$$\rho_{\max} = \begin{cases} 2^{\frac{m}{2}} & \text{if } 2 \mid m \\ 2^{\frac{m-1}{2}} & \text{if } 2 \nmid m \end{cases},$$

so the claim follows from Theorem 5.7. $\square$

5.3 The Delsarte–Goethals codes $DG(m, r)$

The so–called Delsarte–Goethals codes are generalizations of the Kerdock code.

Definition 5.10. Let $m \geq 3$ be odd, $1 \leq r \leq \frac{m-1}{2}$ and x_i, $0 \leq i \leq 2^m - 1$, some enumeration of $\mathcal{T}$. The $\mathbb{Z}_4$-*Delsarte–Goethals code* is the code

$$DG_4(m, r) = \{\mathbf{d}(\mathbf{a}, b) \mid \mathbf{a} \in R \times \mathcal{T}^r, b \in \mathbb{Z}_4\}$$

where the codewords are defined as

$$\mathbf{d}(\mathbf{a}, b) = \left(\operatorname{Tr}\left(a_0 x_i + 2\sum_{j=1}^{r} a_j x_i^{1+2^j}\right) + b\right)_{i=0}^{2^m-1}. \tag{3}$$

The *binary Delsarte–Goethals code* $DG(m, r)$ is the Gray image of $DG_4(m, r)$, i.e. $DG(m, r) = \mathcal{G}\big(DG(m, r)\big)$.

Obviously $DG(m, r)$ is $\mathbb{Z}_4$-linear and we have the following result.

Theorem 5.11. *$DG(m, r)$ has parameters*

$$\textit{length} = 2^{m+1}, \quad \textit{size} = 4^{m+1}2^{rm} \quad \textit{and} \quad d_{\min} = 2^m - 2^{r-\frac{1}{2}}2^{\frac{m}{2}}.$$

Proof. Length is clearly $2 \cdot 2^m$. We can choose a_0 in 4^m, a_j in 2^m and b in 4 different ways, so we have a total of $4 \cdot 4^m \cdot (2^m)^r$ different codewords.

By Theorem 4.15 we can calculate the inner product

$$\begin{aligned}
&\rho\big(\mathbf{d}(\mathbf{a}, c), \mathbf{d}(\mathbf{b}, d)\big) \\
&\quad = \Re\left(\sum_{j=0}^{2^m-1} i^{\operatorname{Tr}\left(a_0 x_j + 2\sum_{k=1}^{r} a_k x_j^{1+2^k}\right) + c - \operatorname{Tr}\left(b_0 x_j + 2\sum_{k=1}^{r} b_k x_j^{1+2^k}\right) - d}\right) \\
&\quad = \Re\left(i^{c-d}\sum_{x \in \mathcal{T}} e\Big((a_0 - b_0)x + 2\sum_{k=1}^{r}(a_k - b_k)x^{1+2^k}\Big)\right)
\end{aligned}$$

and this inner product can be zero only if $c = d$ and $\mathbf{a} = \mathbf{b}$. Moreover we know that

$$\rho_{\max} = 2^{r-\frac{1}{2}}2^{\frac{m}{2}}$$

which completes the proof when using Theorem 5.7. $\square$

If we choose the parameter r to be zero, then we get the Kerdock code with odd m. For values $r = 1$ and $r = 2$ we can use Theorems 4.11 and 4.13, respectively, which we have proved. These are the most important codes in the family $DG(m, r)$ as we shall see in the next section.

We notice that every code $DG(m, r)$ is contained in the code $DG(m, r+1)$ so we have a nested chain of codes.

5.4 The codes $C(m, D)$

If we consider the bound for character sums given in Theorem 4.19, we see that for r greater than for example 5 the polynomials (3) defining $DG(m,r)$ codes have large weighted degree. With respect to the weighted degree the set of these polynomials is quite small.

With these observations we can construct a different nested chain of codes with an equal length and size but a larger minimum distance. These codes were introduced by Shanbhag, Kumar and Helleseth in [11] and also the comparison of the next section is due to them.

Definition 5.12. S_D is the set of all non–degenerate polynomials in $R[x]$ with weighted degree at most D.

Definition 5.13. Let $1 \leq D \leq 2^{\frac{m}{2}}$ and x_i, $0 \leq i \leq 2^m - 1$, some enumeration of $\mathcal{T}$. We set

$$C_4(m, D) = \{\mathbf{c}(f, b) \mid f \in S_D, b \in \mathbb{Z}_4\}$$

where

$$\mathbf{c}(f, b) = \Big(\operatorname{Tr}\big(f(x_i)\big) + b\Big)_{i=0}^{2^m-1}.$$

The binary code $C(m, D)$ is the Gray image of $C_4(m, D)$, i.e. $C(m, D) = \mathcal{G}\big(C(m, D)\big)$.

The restriction $D \leq 2^{\frac{m}{2}}$ is used, since with $N_f = 2^{\frac{m}{2}} + 1$ Theorem 4.19 gives the trivial bound 2^m.

The code $C(m, D)$ is $\mathbb{Z}_4$-linear, because any $\mathbb{Z}_4$-linear combination of two polynomials with weighted degree less than k has weighted degree less than k.

To derive parameters of the code $C(m, D)$ we need one lemma.

Lemma 5.14. *Let $D \geq 1$ be an integer. Then* $|S_D| = 2^{m(D - \lfloor \frac{D}{4} \rfloor)}$.

Proof. We know that every element $x \in R$ can be expressed uniquely as $x = a + 2b$ where $a, b \in \mathcal{T}$. Hence we can express every coefficient of a polynomial $f(x) \in R[x]$ in the form $a + 2b$. This implies that we can express the whole polynomial uniquely as $a(x) + 2b(x)$ where $a(x), b(x) \in \mathcal{T}[x]$.

Let us now consider a polynomial $f(x) = a(x) + 2b(x) \in S_D$. For every even exponent i the coefficient is zero and there are $D - \lfloor \frac{D}{2} \rfloor$ odd exponents which are at most D. So we have

$$|\{b(x) \in \mathcal{T}[x] \mid 2b(x) \in S_D\}| = 2^{m(D - \lfloor \frac{D}{2} \rfloor)}.$$

On the other hand for coefficients belonging to $\mathcal{T}$ exponents cannot exceed $\lfloor \frac{D}{2} \rfloor$ and we have $\lfloor \frac{D}{2} \rfloor - \lfloor \frac{\lfloor \frac{D}{2} \rfloor}{2} \rfloor = \lfloor \frac{D}{2} \rfloor - \lfloor \frac{D}{4} \rfloor$ such exponents and therefore

$$|\{a(x) \in \mathcal{T}[x] \mid a(x) \in S_D\}| = 2^{m(\lfloor \frac{D}{2} \rfloor - \lfloor \frac{D}{4} \rfloor)}.$$

Combining these two results we can conclude the claim. □

Theorem 5.15. *The binary code $C(m, D)$ has parameters*

$$\textit{length} = 2^{m+1}, \quad \textit{size} = 2^{m(D - \lfloor \frac{D}{4} \rfloor) + 2} \quad \textit{and} \quad d_{\min} \geq 2^m - (D-1)2^{\frac{m}{2}}.$$

Proof. The length of the code $C(m, D)$ is clearly 2^{m+1}. The cardinality follows from Lemma 5.14. Observe that the restriction $D \leq 2^{\frac{m}{2}}$ guarantees that the codewords $\mathbf{c}(f, b)$ are distinct.

The minimum distance can now be deduced from Theorems 4.19 and 5.7. □

5.5 A comparison between $C(m, D)$ and $DG(m, r)$

In order to compare these codes we should have some equal parameters. The lengths of these codes are equal when we have the same parameter m. Sizes of these codes equal when

$$\begin{aligned} 4^{m+1} 2^{rm} = 2^{m(D - \lfloor \frac{D}{4} \rfloor) + 2} &\Leftrightarrow 2m + 2 + rm = m(D - \left\lfloor \frac{D}{4} \right\rfloor) + 2 \\ &\Leftrightarrow r = D - \left\lfloor \frac{D}{4} \right\rfloor - 2. \end{aligned} \tag{4}$$

If we consider the last formula as a function of D, we see that whenever $4 \mid D$ the value of r is the same as for an argument $D - 1$. This can be seen immediately by considering the sets S_D. If $4 \mid D$, then $S_{D-1} = S_D$ and we can choose $D - 1$ instead of D for a given r.

We can transform the condition (4) for D by substituting $D = 4s + t$ where $1 \leq t \leq 3$. Then we have

$$r = 4s + t - s - 2 = 3s + t - 2, \quad \left\lfloor \frac{r+1}{3} \right\rfloor = s \quad \text{and} \quad D = \left\lfloor \frac{r+1}{3} \right\rfloor + r + 2.$$

We present these observations in the next theorem.

Theorem 5.16. *Let $m \geq 3$ be odd. For a given integer r, $1 \leq r \leq \frac{m-1}{2}$, let the integer D_r be given by $D_r = \lfloor \frac{r+1}{3} \rfloor + r + 2$. Then the binary codes $DG(m, r)$ and $C(m, D_r)$ have the same size $4^{m+1} 2^{rm}$, but different minimum distances $d_{\min}$ given by $2^m - 2^{r - \frac{1}{2}} 2^{\frac{m}{2}}$ and $\geq 2^m - (D_r - 1) 2^{\frac{m}{2}}$, respectively.*

Remark 5.17. For values of $D_r = 2, 3, 5$ the codes $C(m, D_r)$ coincide with the Kerdock code and the first two members of the DG chain, respectively.

r	D_r	Common Code Size	$d_{\min}$ $DG(m,r)$	$d_{\min} \geq$ $C(m,D_r)$
3	6	2^{5m+2}	$2^m - (4\sqrt{2})2^{\frac{m}{2}}$	$2^m - (5)2^{\frac{m}{2}}$
4	7	2^{6m+2}	$2^m - (8\sqrt{2})2^{\frac{m}{2}}$	$2^m - (6)2^{\frac{m}{2}}$
5	9	2^{7m+2}	$2^m - (16\sqrt{2})2^{\frac{m}{2}}$	$2^m - (8)2^{\frac{m}{2}}$
6	10	2^{8m+2}	$2^m - (32\sqrt{2})2^{\frac{m}{2}}$	$2^m - (9)2^{\frac{m}{2}}$

Table 1: A comparison of $C(m, D_r)$ with $DG(m, r)$ ($m \geq 13$)

5.6 Nechaev permutation

Nechaev [10] found that by permutating the coordinates of a punctured Kerdock code one gets a cyclic code. This idea was generalized in [11] by Shanbhag et al.

The basic idea comes from two observations:

A primitive element γ of $\mathbb{F}_{2^m}$ has order $L = 2^m - 1$, $\beta = (\gamma, 0)$ generates the set $\mathcal{T}^*$, $-\beta = (\gamma, \gamma^2)$ generates the set $\mathcal{T}^* \cup -\mathcal{T}^*$ and has therefore order $n = 2(2^m - 1)$.

The Gray map $\mathcal{G} = (\pi, \nu)$ satisfies the relation $\mathcal{G}(x) = \pi(x)\pi(-x)$ where π is the most significant bit map given by Definition 5.2.

Definition 5.18. We now define the binary code

$$P(m, D) = \{\mathbf{p}(f, b) \mid f \in S_D, b \in \mathbb{Z}_4\},$$

where

$$\mathbf{p}(f, b) = \Big(\pi\big((-1)^i \big[\operatorname{Tr}\big(f(\beta^i)\big) + b\big]\big)\Big)_{i=0}^{n-1}$$

in which β is as above, i.e. generator of $\mathcal{T}^*$.

Let us now denote $s_i = \operatorname{Tr}\big(f(\beta^i)\big) + b$ for a fixed codeword $\mathbf{p}(f, b)$. $(s_i)_{i=0}^{L-1}$ is now a $\mathbb{Z}_4$-codeword which satisfies conditions

$$\mathbf{p}(f, b) = \big(\pi(s_0), \pi(-s_1), \dots, \pi(s_{L-1}), \pi(-s_0), \pi(s_1), \dots, \pi(-s_{L-1})\big)$$

and

$$\mathcal{G}\big((s_i)_{i=0}^{L-1}\big) = \big(\pi(s_0), \pi(s_1), \dots, \pi(s_{L-1}), \pi(-s_0), \pi(-s_1), \dots, \pi(-s_{L-1})\big).$$

Definition 5.19. The *Nechaev permutation* η is a permutation acting on the set $\{0, 1, \dots, 2L - 1\}$ by transitions

$$(1, L + 1)(3, L + 3)(5, L + 5) \dots (L - 2, 2L - 2).$$

This permutation acts on the coordinates of codewords, so $\eta\big((t_i)_{i=0}^{2L-1}\big) = (t_{\eta(i)})_{i=0}^{2L-1}$.

The discussion before the previous definition shows that

$$\eta \circ \mathcal{G}\big((s_i)_{i=0}^{L-1}\big) = \mathbf{p}(f, b).$$

5.7 Cyclic $\mathbb{Z}_4$-linear codes

The code $P(m, D) \subset \mathbb{F}_2^{2(2^m-1)}$ defined in the previous section is a permutated version of Gray image of punctured code $C_4^*(m, D)$ where puncturing is done in the coordinate $x = 0$.

The code $P(m, D)$ is clearly $\mathbb{Z}_4$-linear and it can be seen to be cyclic:

$$\mathbf{p}\big(f(x), b\big)_{i+1} = \mathbf{p}\big(-f(\beta x), -b\big)_i.$$

In addition $-f(\beta x) \in S_D$ if $f(x) \in S_D$.

So we have result:

Theorem 5.20. *Let $1 \leq D \leq 2^{\frac{m}{2}}$. Then the cyclic binary code $P(m, D)$ has the following parameters*

$$\textit{length} = 2^{m+1} - 2, \quad \textit{size} = 2^{m(D-\lfloor\frac{D}{4}\rfloor)+2} \quad \textit{and} \quad d_{\min} \geq 2^m - (D-1)2^{\frac{m}{2}} - 2.$$

Proof. Clearly by puncturing the code $C_4^*(m, D)$ we get a code with length $2^m - 1$ and Gray map doubles this length. Size remains the same as in $C(m, D)$.

To derive the lower bound for the minimum distance we have to observe that

$$\left|\sum_{x\in\mathcal{T}^*} e\big(f(x)\big)\right| = \left|\sum_{x\in\mathcal{T}} e\big(f(x)\big) - 1\right| \leq \left|\sum_{x\in\mathcal{T}} e\big(f(x)\big)\right| + 1.$$

Now we get the result as before. □

Remark 5.21. Research Problem 2.6 in the book by MacWilliams and Sloane [8] asks for constructions of efficient nonlinear cyclic codes. The discussion above describes one family of such codes.

6 $\mathbb{Z}_4$-linear sequences

Binary sequences are used in many applications of communication, for example in Code–Division–Multiple–Access used in mobile phone networks. In this chapter we introduce the best known binary sequence family with respect to low correlation. In the next chapter this family is compared to other sequence families.

6.1 Correlations

In communication applications sequences should have low correlations. We now define the most important ones.

Definition 6.1. Let S be a family of sequences of period n and $s_1(t), s_2(t) \in S$. Then the *even correlation* $\theta_{1,2}(\tau)$ is defined by the formula

$$\theta_{1,2}(\tau) = \sum_{t=0}^{n-1} (-1)^{s_1(t+\tau)-s_2(t)}, \qquad 0 \leq \tau < n.$$

The *maximum non–trivial even correlation* is the quantity

$$\theta_{\max} = \theta_{\max}(S) = \max\{|\theta_{i,j}(\tau)| \mid s_i, s_j \in S,\ i \neq j \text{ or } \tau \neq 0\}.$$

The *odd correlation* $\theta^-_{1,2}(\tau)$ is the sum

$$\theta^-_{1,2}(\tau) = \sum_{t=0}^{n-\tau-1} (-1)^{s_1(t+\tau)-s_2(t)} - \sum_{t=n-\tau}^{n-1} (-1)^{s_1(t+\tau)-s_2(t)}, \qquad 0 \leq \tau < n,$$

and the *maximum non–trivial odd correlation* is

$$\theta^-_{\max} = \theta^-_{\max}(S) = \max\{\left|\theta^-_{i,j}(\tau)\right| \mid s_i, s_j \in S,\ i \neq j \text{ or } \tau \neq 0\}.$$

The *aperiodic correlation* $\theta^a_{1,2}(\tau)$ is

$$\theta^a_{1,2} = \sum_{t=\max\{0,-\tau\}}^{\min\{n-1,n-1-\tau\}} (-1)^{s_1(t+\tau)-s_2(t)}, \qquad -n < \tau < n,$$

and the *maximum non–trivial aperiodic correlation* is

$$\theta^a_{\max} = \theta^a_{\max}(S) = \max\{\left|\theta^a_{i,j}(\tau)\right| \mid s_i, s_j \in S,\ i \neq j \text{ or } \tau \neq 0\}.$$

The maximum non–trivial correlations defined above should be low for a sequence family used for example in CDMA. Known good sequence families have maximum non–trivial correlations of the form $a\sqrt{n}$. However good estimates for odd and aperiodic correlations are not known. Normally the even correlations are calculated somehow first and if these are good enough one can continue to derive some estimates for the other correlations.

6.2 The sequence family $P(m, D)$

As above the ideas of the following sections are from [11] but the representation is mostly from [3].

We can view the codewords of the cyclic code $P(m, D)$ defined in Section 5.6 as sequences. We will follow the usual notation of sequences and write an element $\mathbf{p}(f, b)$ from $P(m, D)$ in the form

$$p_{f,b}(t) = \pi\big((-1)^t\big[\operatorname{Tr}\big(f(\beta^t)\big) + b\big]\big), \qquad \forall t \in \mathbb{N}_0.$$

Let us now consider even correlations of sequences in $P(m, D)$. We do not know exact periods of these sequences but these periods must divide $n = 2L = 2(2^m - 1)$. So let p_{f_1,b_1} and p_{f_2,b_2} be sequences from $P(m, D)$. Then we have

$$\theta_{1,2}(\tau) = \sum_{t=0}^{n-1}(-1)^{p_{f_1,b_1}(t+\tau)-p_{f_2,b_2}(t)}, \quad 0 \le \tau < n,$$

which can be rephrased in terms of Hamming distance as

$$\begin{aligned}\theta_{1,2}(\tau) =& 1 \cdot \Big[n - d_H\Big(\big(p_{f_1,b_1}(t+\tau)\big)_{t=0}^{n-1}, \big(p_{f_2,b_2}(t)\big)_{t=0}^{n-1}\Big)\Big] \\ &+ (-1) \cdot d_H\Big(\big(p_{f_1,b_1}(t+\tau)\big)_{t=0}^{n-1}, \big(p_{f_2,b_2}(t)\big)_{t=0}^{n-1}\Big) \\ =& n - 2d_H\Big(\big(p_{f_1,b_1}(t+\tau)\big)_{t=0}^{n-1}, \big(p_{f_2,b_2}(t)\big)_{t=0}^{n-1}\Big).\end{aligned}$$

Let $s_{f,b}(t) = \operatorname{Tr}\big(f(\beta^t)\big) + b$ be a $\mathbb{Z}_4$-sequence. Then we know that

$$p_{f,b}(t) = \pi\big((-1)^t s_{f,b}(t)\big) = \eta \circ \mathcal{G}(s_{f,b})(t).$$

The Nechaev permutation η described in Section 5.6 does not affect the Hamming distance and the Gray map is an isometry from $(\mathbb{Z}_4^L, d_L)$ to $(\mathbb{F}_2^n, d_H)$. In addition we have the relation between the Lee metric and the inner product, so we get

$$\begin{aligned}
\theta_{1,2}(\tau) &= n - 2d_H\Big(\big(\pi\left[(-1)^t[(-1)^\tau s_{f_1,b_1}(t+\tau)]\right]\big)_{t=0}^{n-1}, \big(\pi\left[(-1)^t[s_{f_2,b_2}(t)]\right]\big)_{t=0}^{n-1}\Big)\\
&= n - 2d_L\Big(\big((-1)^\tau s_{f_1,b_1}(t+\tau)\big)_{t=0}^{L-1}, \big(s_{f_2,b_2}(t)\big)_{t=0}^{L-1}\Big)\\
&= n - 2\Big(L - \rho\Big(\big((-1)^\tau s_{f_1,b_1}(t+\tau)\big)_{t=0}^{L-1}, \big(s_{f_2,b_2}(t)\big)_{t=0}^{L-1}\Big)\\
&= 2\Re\left(\sum_{t=0}^{L-1} i^{(-1)^\tau\left[\operatorname{Tr}\left(f_1(\beta^{t+\tau})\right)+b_1\right]-\left[\operatorname{Tr}\left(f_2(\beta^t)\right)+b_2\right]}\right)\\
&= 2\Re\left(i^{(-1)^\tau b_1 - b_2}\sum_{t=0}^{L-1} i^{\operatorname{Tr}\left((-1)^\tau f_1(\beta^{t+\tau})-f_2(\beta^t)\right)}\right) \qquad (5)
\end{aligned}$$

A sequence $p_{f_1,b_1}(t)$ has period less than n, iff $\theta_{1,1}(\tau)=n$ for some τ such that $0<\tau<n$.

We see from the formula above that $\theta_{1,1}(\tau)=n$, $0<\tau<n$, is possible iff

$$(-1)^\tau f_1(\beta^{t+\tau}) = f_1(\beta^t), \quad \forall t \qquad \text{and} \qquad (-1)^\tau b_1 = b_1.$$

Because f_1 is non–degenerate and hence have only terms with odd exponent, we have

$$(-1)^\tau f_1(\beta^{t+\tau}) = f_1\big((-\beta)^\tau\beta^t\big) = f_1(\beta^t)\ \forall t \quad \text{and} \quad (-1)^\tau b_1 = b_1. \qquad (6)$$

If two non–degenerate polynomials f and g in $R[x]$ with weighted degree at most $D \le \frac{m}{2}$ coincide in the Teichmüller set $\mathcal{T}$, i.e. $f(x)=g(x)\ \forall x\in\mathcal{T}$, then these polynomials are equal. This is a consequence of Theorem 4.19 and can be seen as follows:

$$\sum_{x\in\mathcal{T}} e\big(f(x)-g(x)\big) = 2^m > (D-1)2^{\frac{m}{2}} \quad \Longrightarrow \quad f(x)-g(x)=0.$$

Definition 6.2. Let $f\in R[x]$ be a non–degenerate polynomial with weighted degree at most D. The set E_f consists of the exponents of the non–zero terms of f.

Let us now write $f_1 = \sum_{i\in E_{f_1}} a_i x^i$. We can deduce from (6) that $\theta_{1,1}(\tau) = n$, $0<\tau<n$, iff $(-1)^\tau b_1 = b_1$ and

$$\sum_{i\in E_{f_1}} a_i(-\beta)^{\tau i}x^i = \sum_{i\in E_{f_1}} a_i x^i$$

or when expressed only with the coefficients

$$a_i(-\beta)^{\tau i} = a_i \quad \forall i\in E_{f_1}.$$

If $a_i \in R^*$, we can divide it from both sides and the condition can be formulated: $2L \mid \tau i$ for all $i \in E_{f_1}$.

If $a_i \in 2R \setminus \{0\}$, we have in Witt vector form

$$(-1)^{\tau i}(0, a)(\beta_1^{\tau i}, 0) = (-1)^{\tau i}(0, a\beta_1^{2\tau i}) = (0, a\beta_1^{2\tau i}) = (0, a).$$

So in this case the condition becomes to form: $L \mid \tau i$ for all $i \in E_{f_1}$.

Lemma 6.3. *Let*

$$T_D = \{f \in S_D \mid \gcd(E_f, L) = 1\}$$

where $\gcd(E_f, L)$ *denotes the greatest common divisor of all the exponents in* E_f *and* L. *Then the subset*

$$\{p_{f,b}(t) \mid f \in T_D \text{ and } 2[f(x) + b] \neq 0\} \subset P(m, D)$$

contains exactly those sequences which have the full period n.

Proof. We should now show that the condition stated by this lemma is equivalent to the conditions discussed just before the lemma.

Let us consider a sequence $p_{f,b}(t) \in P(m, D)$. If some coefficient of f is unit, i.e. $f(x) \in R[x] \setminus 2R[x]$, the sequence $p_{f,b}(t)$ has period less than n iff $2L \mid \tau i \ \forall i \in E_f$ and $(-1)^\tau b = b$. This is possible only if $2 \mid \tau$, because every $i \in E_f$ is odd. Then the latter requirement for b holds trivially. Now

$$2L \mid \tau i \quad \forall i \in E_f,\ 0 < \tau < n \quad \Leftrightarrow \quad \gcd(E_f, L) > 1.$$

If $f(x) \in 2R[x]$, then for period less than n we have to require only that $L \mid \tau i \ \forall i \in E_f$ and $(-1)^\tau b = b$. When compared to the previous case there is just one difference: τ can be L. To eliminate sequences with period L we require that $2b \neq 0$. Because L is odd, we get $(-1)^L b = -b \neq b$. Now the gcd–condition implies as in the first case that the sequence has full period. $\square$

To eliminate high correlation $\theta_{1,1}(\tau) = -n$ we have to exclude all the polynomials in $2R[x]$ from this construction. Since for every $b \in \mathbb{Z}_4$ we have $(-1)^\tau b - b \in \{0, 2\} \subset \mathbb{Z}_4$ the condition for b affects only on the sign of $\theta_{1,1}(\tau)$ in the formula (5). Hence for every $f_1 \in 2R[x]$ and $b_1 \in \mathbb{Z}_4$ we have $\theta_{1,1}(L) = -n$.

Lemma 6.4. *For sequences* $p_{f_1,b_1}(t)$, *where* $f_1 \in T_D \setminus 2R[x]$, *and* $b_1 \in \mathbb{Z}_4$ *we have*

$$|\theta_{1,1}(\tau)| \leq 2 + 2(D-1)2^{\frac{m}{2}}, \qquad 0 < \tau < n.$$

Proof. From (5) and Theorem 4.19 we get

$$\begin{aligned}|\theta_{1,1}(\tau)| &\le 2\left|\sum_{x\in\mathcal{T}} e\big((-1)^\tau f_1(\beta^\tau x) - f_2(x)\big) - 1\right| \\ &\le 2\big((D-1)2^{\frac{m}{2}} + 1\big),\end{aligned}$$

because when taking polynomials f_1 and f_2 from $T_D \setminus 2R[x]$ the polynomial inside the character sum is in S_D and cannot be the zero–polynomial. □

6.3 The sequence family $Q(m, D)$

To get low correlations $\theta_{1,2}(\tau)$ for different sequences we should not include to the family sequences which are cyclical shifts of each other. Nor should we allow a sequence to be a bitwise negation of a cyclic shift of another sequence. So for two sequnces p_{f,b_1} and p_{f,b_2} in our family we should require that $b_1 - b_2 \not\equiv 0 \pmod 2$. If this condition is satisfied, then the sum in (5) will be purely imaginary which gives then zero correlation. These facts are captured in the next definition.

Definition 6.5. We define two sequences

$$\pi\Big((-1)^{t+\tau}\big[\operatorname{Tr}\big(f(\beta^{t+\tau})\big) + b\big]\Big) \quad \text{and} \quad \pi\Big((-1)^{t}\big[\operatorname{Tr}\big(f(\beta^{t})\big) + b + c\big]\Big)$$

to be equivalent where $0 \le \tau < n$ and $c \in \{0, 2\} \subset \mathbb{Z}_4$.

This equivalence divides the subset of sequences in $P(m, D)$ described in Lemma 6.4 to equivalence classes of size $2n$. The *sequence set* $Q(m, D)$ is now obtained by taking one sequence from each equivalence class.

The definition of $Q(m, D)$ is not very constructive and the formula for the size of $Q(m, D)$ is quite complicated, but in the next section we give one subset of $Q(m, D)$ which has a more constructive representation.

Definition 6.6. The *Mobius function* μ is given by the formula

$$\mu(d) = \begin{cases} 1 & \text{if } d = 1, \\ (-1)^r & \text{if } d \text{ is the product of } r \text{ distinct primes}, \\ 0 & \text{otherwise.}\end{cases}$$

Theorem 6.7. *Let $L = 2^m - 1$ and $n = 2L$. Then the sequence family $Q(m, D)$ has the following parameters*

$$\textit{period} = 2(2^m - 1), \qquad \theta_{\max} \le 2(D-1)2^{\frac{m}{2}} + 2 \quad \textit{and}$$
$$\textit{size} = \frac{1}{L}\sum_{d|L} \mu(d)\big(2^{m(\lfloor\frac{D}{d}\rfloor - \lfloor\frac{D}{4d}\rfloor)} - 2^{m(\lfloor\frac{D}{d}\rfloor - \lfloor\frac{D}{2d}\rfloor)}\big)$$

Proof. We have chosen sequences so that the polynomial in the character sum (5) can not be the zero–polynomial. Then we derive the upper bound for $\theta_{\max}$ as in Lemma 6.4.

We do not actually refer to this family later and therefore we omit the proof for the size, but it can be found in [3]. $\square$

Here we present without proof a result for the maximal non–trivial odd and aperiodic correlations of the sequence family $Q(m, D)$.

Theorem 6.8 (Koponen–Lahtonen [5]). *For the sequence family $Q(m, D)$ we have following upper bounds for maximum non–trivial odd and aperiodic correlations:*

$$\theta^{-}_{\max} < \frac{8}{\pi} D \frac{m}{2} \left(\ln \frac{4n}{\pi} + \frac{\pi}{4} \right) - 2\frac{m}{2} + 2$$

and

$$\theta^{a}_{\max} < \frac{4}{\pi} D \frac{m}{2} \left(\ln \frac{4n}{\pi} + \frac{\pi}{2} \right) - 2\frac{m}{2} + 2.$$

The results of the previous theorem are derived with so–called Vinogradov method for partial–period correlations.

6.4 The sequence family $Q_1(m, D)$

Now we describe one subset of $Q(m, D)$ for which the size is a little easier to formulate.

Let us now restrict the polynomials used in the sequences of $Q(m, D)$ so that there always exists a non–zero coefficient in the term of degree one and moreover this coefficient is of the form $1 + 2\beta^i$ where β is a generator of $\mathcal{T}^*$. Let f be such a polynomial and $p_{f,b}(t)$ corresponding sequence. We consider now the cyclic shifts of $p_{f,b}(t)$. With $0 < \tau < n$ we have

$$p_{f,b}(t + \tau) = \pi\Big((-1)^t \Big[\operatorname{Tr}\Big(f\big((-\beta)^\tau \beta^t\big)\Big) + (-1)^\tau b \Big]\Big)$$

and in the polynomial $f\big((-\beta)^\tau x\big)$ the coefficient of the term of degree one is

$$\begin{aligned}
(1 + 2\beta^i)(-1)^\tau \beta^\tau &= \big((1, 0) + 2(\beta_1^i, 0)\big)(-1)^\tau (\beta_1^\tau, 0) \\
&= (1, \beta_1^{2i}) \cdot \begin{cases} (\beta_1^\tau, 0) & \text{if } 2 \mid \tau \\ (\beta_1^\tau, \beta_1^{2\tau}) & \text{if } 2 \nmid \tau \end{cases} = \begin{cases} (\beta_1^\tau, \beta_1^{2i+2\tau}) & \text{if } 2 \mid \tau \\ \big(\beta_1^\tau, \beta_1^{2\tau}(1 + \beta_1^{2i})\big) & \text{if } 2 \nmid \tau. \end{cases}
\end{aligned}$$

This coefficient can be equal to $1 + 2\beta^j = (1, \beta_1^{2j})$ only if $L \mid \tau$ iff $L = \tau$. Because $2 \nmid L$, we should have $1 + \beta_1^{2i} = \beta_1^{2j}$ or equivalently $1 + \beta_1^i = \beta_1^j$.

Definition 6.9. Let $\beta = (\beta_1, 0)$ be a generator of $\mathcal{T}^*$. Two elements $a = (\beta_1^i, 0)$ and $b = (\beta_1^j, 0)$ of $\mathcal{T}$ are equivalent, if $a = b$ or $\beta_1^j = \beta_1^i + 1$ in $\mathbb{F}$. Let now $\hat{\mathcal{T}} \subset \mathcal{T}$ be such that there is exactly one element from each equivalence class.

Definition 6.10. Let $D \geq 2$ be an integer. The sequence family $Q_1(m, D)$ consists of sequences

$$q_{f,b} = \pi\Big((-1)^t \big[\operatorname{Tr}\big(f(\beta^t)\big) + b\big]\Big), \quad f \in S_D, f_1 = 1 + 2a, a \in \hat{\mathcal{T}}, b \in \{0, 1\}$$

where f_1 denotes the coefficient of the term of degree one.

The restriction $D \geq 2$ comes naturally from the requirement $f_1 = 1+2a \in R^*$. Therefore the weighted degree of f is at least 2.

Theorem 6.11. *Let $L = 2^m - 1$ and $n = 2L$. The sequence family $Q_1(m, D) \subset Q(m, D)$ has parameters*

$$\textit{period} = 2(2^m - 1), \quad \theta_{\max} \leq 2(D-1)2^{\frac{m}{2}} + 2 \quad \textit{and} \quad \textit{size} = 2^{m(D - \lfloor \frac{D}{4} \rfloor - 1)}.$$

Proof. We have required that in polynomials used in the construction there exists a term of first degree and moreover its coefficient is a unit of R. This implies that $\gcd(E_f, L) = 1$ and $f \in R[x] \setminus 2R[x]$. So we have sequences with full period n.

The requirement $f_1 = 1 + 2a$, $a \in \hat{\mathcal{T}}$, guarantees that the resulting sequences are cyclically distinct and condition $b \in \{0, 1\}$ guarantees that $(-1)^\tau b \not\equiv b \pmod 2$. Therefore $Q_1(m, D)$ really is a subset of $Q(m, D)$ and certainly θ_{max} can not be greater than in Theorem 6.7.

The size can be seen by Lemma 5.14. We have $|S_D|$ polynomials in S_D, $\frac{|S_D|}{|R|}$ of them have $f_1 = 0$ and $|\hat{\mathcal{T}}|\frac{|S_D|}{|R|}$ of them have $f_1 = 1 + 2a$ for some $a \in \hat{\mathcal{T}}$. Moreover we can choose b in two ways. Clearly $|\hat{\mathcal{T}}| = 2^{m-1}$ and hence we have $2\frac{2^{m-1}}{4^m} 2^{m(D - \lfloor \frac{D}{4} \rfloor)} = 2^{m(D - \lfloor \frac{D}{4} \rfloor - 1)}$ such polynomials. $\square$

We give now a couple of examples.

Example 6.12 (The Kerdock sequences). Let m be odd and $D = 2$. We have the sequence family

$$Q_1(m, 2) = \Big\{\pi\Big((-1)^t \big[\operatorname{Tr}\big((1 + 2a)\beta^t\big) + b\big]\Big) \;\Big|\; a \in \hat{\mathcal{T}}, b \in \{0, 1\}\Big\}$$

of size 2^m and length $2(2^m - 1)$. We require m to be odd to get a little better upper bound for $\theta_{\max}$. Theorem 4.9 can now be applied instead of the Kumar–Helleseth–Calderbank bound. Hence we can replace $(2-1)2^{\frac{m}{2}}$ by $2^{\frac{m-1}{2}}$ in the upper bound and we get

$$\theta_{\max} \leq 2^{\frac{m+1}{2}} + 2.$$

Example 6.13 (The Delsarte–Goethals sequences). Let m be odd and $D = 3$. In this case we derive the family

$$Q_1(m,3) = \left\{\pi\Big((-1)^t\big[\operatorname{Tr}\left((1+2a)\beta^t + 2c\beta^{3t}\right) + b\big]\Big) \mid a \in \hat{\mathcal{T}}, b \in \{0,1\}, c \in \mathcal{T}\right\}$$

of size 2^{2m}, length $2(2^m - 1)$ and with maximal non–trivial even correlation satisfying

$$\theta_{\max} \leq 2^{\frac{m+3}{2}} + 2$$

by Theorem 4.11.

Also the next element in the chain of sets $Q(m,D)$ is formed with polynomials which are of the same form as those used in the Delsarte–Goethals codes.

Let m be odd and $D = 5$. Then we get the family

$$Q_1(m,5) = \left\{\pi\Big((-1)^t\big[\operatorname{Tr}\left((1+2a)\beta^t + 2c\beta^{3t} + 2d\beta^{5t}\right) + b\big]\Big) \mid \right.$$
$$\left. a \in \hat{\mathcal{T}}, b \in \{0,1\}, c, d \in \mathcal{T}\right\}$$

of size 2^{3m}, length $2(2^m - 1)$ and with maximal non–trivial even correlation satisfying

$$\theta_{\max} \leq 2^{\frac{m+5}{2}} + 2$$

by Theorem 4.13.

Remark 6.14. For $D > 5$ the polynomials used in these constractions are not any more necessarily of the Delsarte–Goethals form. Therefore we no longer require m to be odd. On the other hand we have to use the upper bound from Theorem 6.11 for $\theta_{\max}$ instead of the bound used in the previous examples. The general bound is larger approximately by a factor $\sqrt{2}$.

7 A comparison of known good sequence families

In this chapter we present some well–known good sequence families and compare them to the families presented in the previous chapter. Proofs are mostly omitted and they can be found in [4].

7.1 Sequence family constructions in finite fields

In this section the sequence constructions use the theory of finite fields instead of Galois rings used in the previous chapters. So let $\mathbb{F}$ be the finite field with 2^m elements as before and γ a primitive element of this field.

Definition 7.1. The binary cyclic code $C(P)$ is the set

$$C(P) = \{\mathbf{c} = c(f) \mid f \in P\}$$

where P is some additive subgroup of $\mathbb{F}[x]$ and

$$\mathbf{c} = c(f) = \Big(\mathrm{Tr}_{\mathbb{F}}\left(f(1)\right), \mathrm{Tr}_{\mathbb{F}}\left(f(\gamma)\right), \ldots, \mathrm{Tr}_{\mathbb{F}}\left(f(\gamma^{2^m-2})\right)\Big).$$

We think this cyclic code as a sequence family and present below a relation between the even correlations and the character sums.

For $f, g \in P$, $\left(s_1(t+\tau)\right)_{t=0}^{2^m-2} = c(f)$, $\left(s_2(t)\right)_{t=0}^{2^m-2} = c(g)$ and $h = f-g \in P$ we see that

$$\begin{aligned}
\theta_{1,2}(\tau) &= \sum_{i=0}^{2^m-2} (-1)^{\mathrm{Tr}_{\mathbb{F}}\left(f(\gamma^i)\right) - \mathrm{Tr}_{\mathbb{F}}\left(g(\gamma^i)\right)} \\
&= \sum_{i=0}^{2^m-2} (-1)^{\mathrm{Tr}_{\mathbb{F}}\left(h(\gamma^i)\right)} \\
&= \sum_{i=0}^{2^m-2} e_{\mathbb{F}}\big(h(\gamma^i)\big).
\end{aligned}$$

Let $S = \{s_1(t), \ldots, s_k(t)\} \subset C(P)$ be a set of cyclically distinct sequences with period $2^m - 1$. Because P is an additive subgroup of $\mathbb{F}[x]$, we have

$$\forall i, j \in \{1, \ldots, k\}, i \neq j \text{ or } \tau \neq 0 : \quad 0 \neq \left(s_i(t+\tau) + s_j(t)\right)_{t=0}^{2^m-2} \in C(P)$$

and therefore

$$\theta_{\max}(S) \leq \max_{f \in P \setminus \{0\}} \left| \sum_{i=0}^{2^m-2} e_{\mathbb{F}}\big(f(\gamma^i)\big) \right|.$$

Example 7.2 (Dual BCH sequences). Let $1 \leq t \leq 2^{\frac{m}{2}-1}$. It is well known that the dual code of the primitive narrow sense t-error correcting BCH code can be represented as $C(P)$ where

$$P = \left\{ \sum_{i=1}^{t} a_j x^{2i-1} \;\middle|\; a_i \in \mathbb{F} \right\}.$$

The conditions of the Carlitz–Uchiyama bound from Theorem 2.6 are now satisfied by the polynomials in P and we can conclude that

$$\theta_{\max} \leq \max_{f \in P \setminus \{0\}} \left| \sum_{x \in \mathbb{F}} e_{\mathbb{F}}\big(f(x)\big) - 1 \right| \leq (2t-2)2^{\frac{m}{2}} + 1$$

where correlations are taken over cyclically distinct codewords. Also the upper bound for the parameter t becomes reasonable, since for t greater than $2^{\frac{m}{2}-1}$ we get an upper bound which is greater than 2^m.

We restrict a_1 to be non–zero to get sequences of full period (analogue: with Kerdock sequences we required $f_1 = 1 + 2a$). Hence we get $(2^m - 1)2^{m(t-1)}$ sequences of full period and there exist $2^m - 1$ cyclical shifts of any sequence. Therefore there are $\frac{(2^m-1)2^{m(t-1)}}{2^m-1} = 2^{m(t-1)}$ cyclically distinct sequences with full period.

Example 7.3 (Kasami sequences). Let $m = 2k$ be even and $\epsilon \in \mathbb{F} \setminus \mathbb{F}_{2^k}$. Then we derive the so–called Kasami sequences as cyclically distinct sequences in $C(P)$ when choosing

$$P = \{ax + \beta_0 x^{2^k+1} + \beta_1 x^{2^{k-1}+1} + \cdots + \beta_t x^{2^{k-t}+1} \mid \beta_0 \in \epsilon\mathbb{F}_{2^k}, a, \beta_1, \ldots, \beta_t \in \mathbb{F}\}.$$

For $t = 0, 1, 2$ we get the small Kasami set, the large Kasami set and the very large Kasami set, respectively. For larger values of t we do not get very good sequence families.

Again we restrict a to be non–zero to get full period sequences. We have $\frac{(2^m-1)2^k 2^{mt}}{2^m-1} = 2^{m(t+\frac{1}{2})}$ cyclically distinct sequences with full period in $C(P)$. We state without proof that this sequence family satisfies the condition

$$\theta_{\max} \leq 2^t 2^{\frac{m}{2}} + 1.$$

We refer the interested reader to [4].

There are also analogues of the Kasami families for odd m. Let $m = 2k+1$ and P as above except that β_0 can be any element of $\mathbb{F}$. Then we get $2^{m(t+1)}$ sequences with

$$\theta_{\max} \leq 2^{t+\frac{1}{2}} 2^{\frac{m}{2}} + 1.$$

7.2 A comparison of $Q_1(m, D)$ with other sequence families

We have in Table 7.2 on page 37 compared the first three $Q_1(m, D)$ sequence families with the Kasami sequence families of approximately same period and $\theta_{\max}$.

We can see that compared to Kasami families $Q_1(m, D)$ families have much more sequences.

Usually the asymptotic comparison of sequence families where the period tends to infinity is more appropriate. Next we shall compare parameters of presented families as a functions of the period n. The values in Table 7.2 on page 37 are taken from Examples 6.12, 6.13, 7.2 and 7.3.

We use these parameters to get Figure 1 on page 38. In this figure $m\big(n, a\sqrt{n}\big)$ denotes the maximum size of a family containing sequences of period n and with correlations satisfying $\theta_{\max} \leq a\sqrt{n}$.

The lower bounds presented in the figure show that one can not construct a sequence family with correlations below the bound. We observe that there is a huge cap between the known constructions and the lower bounds. Much more detailed analysis of these bounds can be found in [4].

The Kasami sequence families are quite good when the size of the family is small compared to the period of sequences. In these coordinates the plots for Kasami families lie on the parabola $a = 2^{u-\frac{1}{2}}$ and it can be seen that these families are not so good when the size is large compared to the period.

The dual BCH families were former the best known families when u is large. They are better than Kasami families when we have $u \geq 4$, i.e. the family size is greater than or equal to the period to power 4. The plots for these families lies on a line of slope 2.

The $Q_1(m, D)$ families investigated in Chapter 6 are the best known at the moment with respect to low correlations. The first three plots are lower by the factor $\sqrt{2}$ than the other plots. When $u \geq 4$ the plots lies on line segments with three plots in each. If we consider a line going via every third plot, we see by the values given in Table 7.2 that this line is of slope

$$\frac{\sqrt{2}\big((D-1)+4\big) - \sqrt{2}(D-1)}{3} = \frac{4}{3}\sqrt{2} < 2.$$

Therefore $Q_1(m, D)$ families are even better outside the figure when compared to the dual BCH families.

Family	Period n	Size of Family	$\theta_{\max}$
Kasami (Small set)	$2^m - 1$, m even	$2^{\frac{m}{2}} \approx n^{\frac{1}{2}}$	$2^{\frac{m}{2}} + 1 \approx n^{\frac{1}{2}}$
$Q_1(m, 2)$	$2(2^m - 1)$, m odd	$2^m \approx \frac{n}{2}$	$2^{\frac{m+1}{2}} + 2 \approx n^{\frac{1}{2}}$
Kasami (Large set)	$2^m - 1$, m even	$2^{\frac{3}{2}m} \approx n^{\frac{3}{2}}$	$2 \cdot 2^{\frac{m}{2}} + 1 \approx 2n^{\frac{1}{2}}$
$Q_1(m, 3)$	$2(2^m - 1)$, m odd	$2^{2m} \approx \frac{n^2}{4}$	$2^{\frac{m+3}{2}} + 2 \approx 2n^{\frac{1}{2}}$
Kasami (Very large set)	$2^m - 1$, m even	$2^{\frac{5}{2}m} \approx n^{\frac{5}{2}}$	$4 \cdot 2^{\frac{m}{2}} + 1 \approx 4n^{\frac{1}{2}}$
$Q_1(m, 5)$	$2(2^m - 1)$, m odd	$2^{3m} \approx \frac{n^3}{8}$	$2^{\frac{m+5}{2}} + 2 \approx 4n^{\frac{1}{2}}$

Table 2: Comparison of $Q_1(m, D)$, $D = 2, 3, 5$, with Kasami sequence families

Family	Parameter	Size of Family	$\theta_{\max}$
dual BCH	$1 \leq t \leq \frac{\sqrt{n}}{2}$	n^{t-1}	$2(t-1)\sqrt{n}$
Kasami, m even	$0 \leq t \leq \frac{m}{2}$	$n^{t+\frac{1}{2}}$	$2^t\sqrt{n}$
Kasami, m odd	$0 \leq t \leq \frac{m-1}{2}$	n^{t+1}	$2^{t+\frac{1}{2}}\sqrt{n}$
$Q_1(m, D)$	$D \in \{2, 3, 5\}$	$\left(\frac{n}{2}\right)^{D-\lfloor\frac{D}{4}\rfloor-1}$	$(D-1)\sqrt{n}$
$Q_1(m, D)$	$D > 5$	$\left(\frac{n}{2}\right)^{D-\lfloor\frac{D}{4}\rfloor-1}$	$\sqrt{2}(D-1)\sqrt{n}$

Table 3: Parameters of some sequence families as functions of the period n

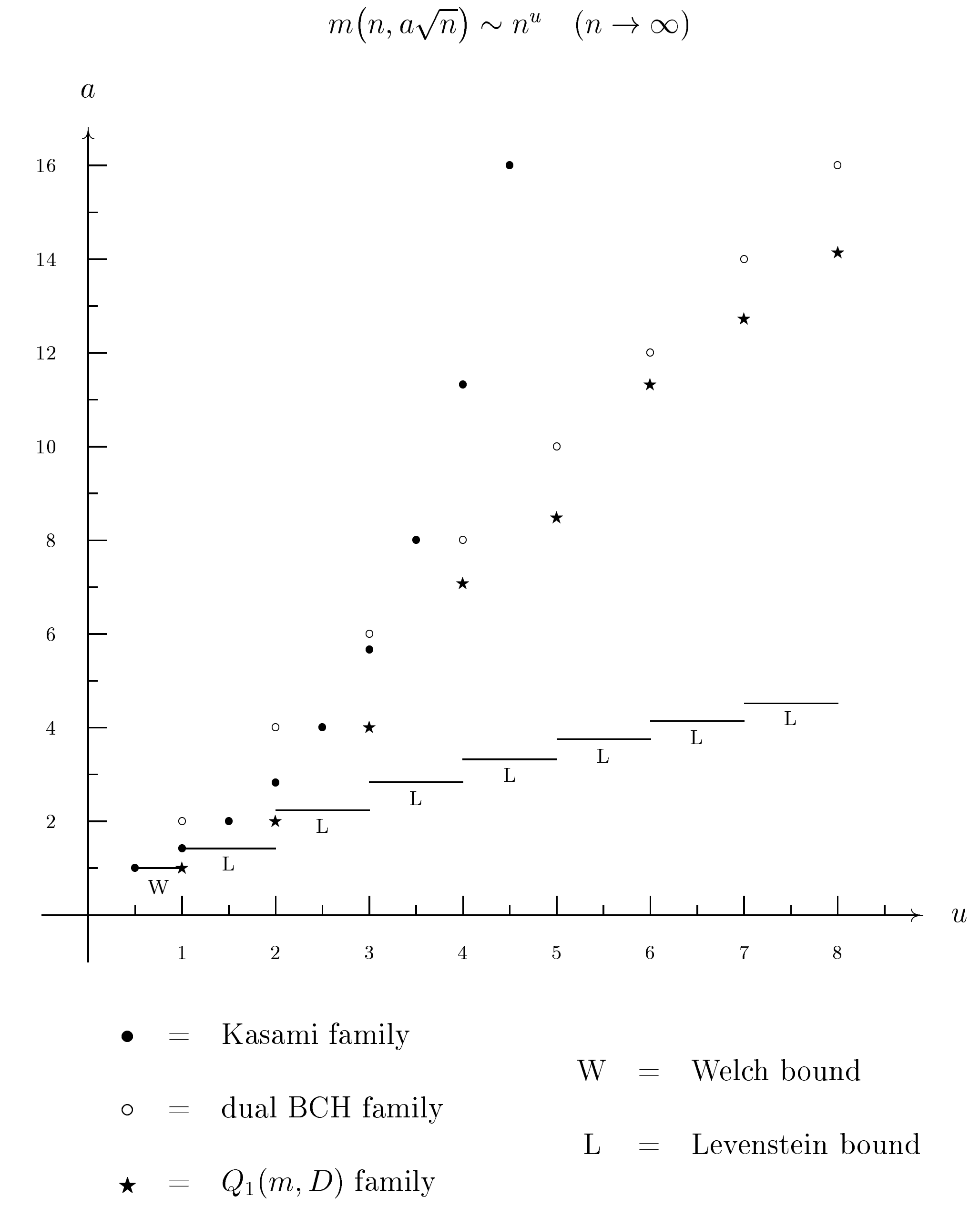

Figure 1: An asymptotic comparison of some sequence families and bounds

References

[1] L. Carlitz and S. Uchiyama, *Bounds for Exponential Sums*, Duke Math. J. **24** (1957), 37–41.

[2] A. Roger Hammons Jr., P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane, and Patrick Solè, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and Related Codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

[3] Tor Helleseth and P. Vijay Kumar, *Sequences with Low Correlation*, Handbook of Coding Theory (R. Brualdi, C. Huffman, and A. G. Shanbhag, eds.), preprint.

[4] Sami Koponen, *On the Correlation of Sequences*, Ph.Lic. dissertation, University of Turku, 1995.

[5] Sami Koponen and Jyrki Lahtonen, *On the Aperiodic and Odd Correlations of the Binary Shanbhag–Kumar–Helleseth Sequences*, IEEE Trans. Inform. Theory **43** (1997), no. 5, 1593–1596.

[6] P. Vijay Kumar, Tor Helleseth, and A. R. Calderbank, *An Upper Bound for Weil Exponential Sums over Galois Rings and Applications*, IEEE Trans. Inform. Theory **41** (1995), no. 2, 456–468.

[7] Rudolf Lidl and Harald Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison–Wesley, Reading, 1983.

[8] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error–Correcting Codes*, North–Holland, Amsterdam, 1977.

[9] Bernard R. McDonald, *Finite Rings with Identity*, Marcel Dekker Inc., New York, 1974.

[10] A. A. Nechaev, *Kerdock code in a cyclic form*, Discr. Math. Appl. **39** (1991), no. 2, 365–384.

[11] Abhijit G. Shanbhag, P. Vijay Kumar, and Tor Helleseth, *Improved Binary Codes and Sequence Families from $\mathbb{Z}_4$-Linear Codes*, IEEE Trans. Inform. Theory **42** (1996), no. 5, 1582–1587.

[12] Aimo Tietäväinen, *Äärellisen kunnan karakterit ja yhtälöt*, Lecture notes, University of Turku, 1996.

Turku Centre for Computer Science
Lemminkäisenkatu 14
FIN-20520 Turku
Finland

http://www.tucs.abo.fi

University of Turku
- **Department of Mathematical Sciences**

Åbo Akademi University
- **Department of Computer Science**
- **Institute for Advanced Management Systems Research**

Turku School of Economics and Business Administration
- **Institute of Information Systems Science**