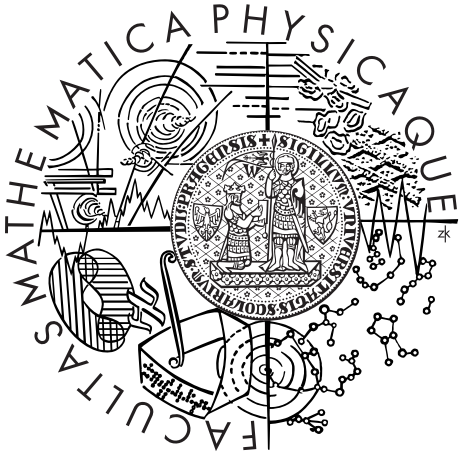
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE



Kateřina Teplá

Kerdockovy kódy a okolí

Katedra algebry

Vedoucí diplomové práce: prof. RNDr. Aleš Drápal, CSc., DSc.
Studijní program: Matematika
Studijní obor: Matematické metody informační bezpečnosti

Praha 2012

I would like to thank my supervisor prof. RNDr. Aleš Drápal CSc., DSc. for his enormous patience and support during the writing of this thesis.

I declare that I carried out this master thesis independently, and only with the cited sources, literature and other professional sources.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Coll., the Copyright Act, as amended, in particular the fact that the Charles University in Prague has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 paragraph 1 of the Copyright Act.

In Prague date 2nd August 2012

Název práce: Kerdockovy kódy a okolí

Autor: Kateřina Teplá

Katedra: Katedra algebry

Vedoucí diplomové práce: prof. RNDr. Aleš Drápal, CSc., DSc., Katedra algebry

Abstrakt: Kerdockovy kódy tvoří rodinu nelineárních kódů, které obsahují více kódových slov než libovolný známý lineární kód se stejnými parametry. Hlavním cílem této práce je propojení Kerdockových kódů s jinými oblastmi matematiky, zejména ortogonální geometrií, kombinatorikou a kryptografií. Je zde popsána teorie symplektických a kvadratických forem na vektorových prostorech charakteristiky 2 a jejich vztah ke Kerdockovým kódům. Dále je dokázáno, že kódová slova Kerdockova kódu libovolné váhy tvoří kombinatorický 3-design. Závěrem je rozebrána použitelnost Kerdockových kódů při konstrukci Booleovských bent funkcí a t-resilientních funkcí, které jsou základem mnoha kryptografických primitiv.

Klíčová slova: Kerdockův kód, Kerdockova množina, t-design, resilientní funkce

Title: Kerdock codes and around

Author: Kateřina Teplá

Department: Department of algebra

Supervisor: prof. RNDr. Aleš Drápal, CSc., DSc., Department of algebra

Abstract: Kerdock codes form a family of nonlinear codes, that contains more codewords than any known linear code with the same parameters. The main goal of this thesis is a connection of Kerdock codes with other areas of mathematics, mainly orthogonal geometry, combinatorics and cryptography. It describes theory of symplectic and quadratic forms on vector spaces of characteristic 2 and its relationship to Kerdock codes. Then it is proven, that codewords of Kerdock code of constant weight form combinatorial 3-design. Finally usage of Kerdock codes in construction of Boolean bent functions and t-resilient functions, that are basis of many cryptographic primitives, is analysed.

Keywords: Kerdock code, Kerdock set, t-design, resilient function

Contents

Introduction

Kerdock codes represent one of the well known families of nonlinear binary error correcting codes that contains more codewords than any comparable currently known linear code for fixed length n and minimum distance d.

Kerdock codes $\mathcal{K}(m)$ can be constructed for each even integer m with the following parameters

- length 2^m,
- number of codewords 2^{2m},
- minimum distance $2^{m-1} - 2^{\frac{m}{2}-1}$.

Theory of error-correcting codes was historicaly interested mainly in linear codes over the finite fields $\mathbb{F}_q$ (usually q=2), i.e. subspaces of a vector space $\mathbb{F}_q^n$, $n \in \mathbb{N}$.

In 1968 high school student A. W. Nordstrom and J. P. Robinson constructed $(15, 256, 5)$ optimal nonlinear code (now we usually denote by Nordstrom-Robinson code its extension by parity check). In the same year F. P. Preparata defined a family of practicaly useful nonlinear codes. And finally, in 1972 A.M. Kerdock in his article [21] described a construction of the family of optimal nonlinear binary codes. Due to their convenient parameters, these three discoveries renewed an interest in nonlinear codes and supported their more intensive research.

Shortly after the first definition of Kerdock codes, it was observed that they behave like dual codes of Preparata codes of the same length in the sense that the weight and distance distributions of these codes are connected via the MacWilliams identity.

This property seemed very strange until a publication of article [15]. Hammons et al. here showed that both, Kerdock and Preparata codes, are images of dual codes over the ring $\mathbb{Z}_4$ under an appropriate mapping from $\mathbb{Z}_4^n$ to $\mathbb{Z}_4^{2n}$.

The complete description of algebraic structure of Kerdock codes in both of their forms then opened the doors to their extensive study with respect to another areas of mathematics.

This master thesis describes basic constructions of both binary and quaternary Kerdock codes. Then the connection of Kerdock codes with another areas of mathematics is investigated.

The thesis is divided into four chapters. The first chapter contains two basic methods of definition of Kerdock codes. The second part connect the construction of Kerdock codes to theory of orthogonal and symplectic geometry. In the third part, Kerdock codes are used for description of infinite sets of combinatorial designs. And finally, the fourth chapter contains usage of Kerdock codes related to the basic cryptographic primitives.

Original definition of Kerdock codes, described in [21], uses the trace function from the field $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. But now Kerdock codes are commonly defined in two different ways described in Chapter 1.

The first method of construction shows the Kerdock code as a union of certain cosets of the first order Reed-Muller code $\mathcal{RM}(1,m)$ in the second order Reed-Muller code $\mathcal{RM}(2,m)$ (see Definition 1.1.2). The second method define Kerdock codes as images of $\mathbb{Z}_4$-cyclic codes under the Gray map (see Definition 1.2.14).

In Section 1.1 we expect an existence of the Kerdock set $\mathcal{K}$ of $m \times m$ skew-symmetric matrices such that

- the zero matrix is in $\mathcal{K}$,
- a difference between each two distinct matrices from $\mathcal{K}$ is regular.

The existence of Kerdock set is not obvious.

In the second chapter we will consider the vector space $\mathbb{F}_2^m$, m even, equipped with a quadratic form

$$Q(v) = x_1y_1 + \ldots + x_my_m = \sum_{i=1}^{m} x_iy_i, \tag{1}$$

where $v \in V$ and $v = (x_1, \ldots, x_m, y_1, \ldots, y_m)$. Then we will divide the set of singular vectors of quadratic form Q to $2^{m-1}+1$ sets of the same cardinality. This division defines an algebraic structure called orthogonal spread. The main result of the chapter is proof of one-to-one correspondence between orthogonal spreads and Kerdock sets.

The problem of construction of the Kerdock set is then convert to a construction of well-known structure from finite geometry.

As was written above, the third part is dedicated to combinatorial designs. The $t-(v,k,\lambda)$ design is a set of v points and k-subsets called blocks, such that any subset of t points is contained in precisely λ blocks.

Let C be a binary (n,k,d) code. Now we can imagine each coordinate of codewords from C as one of v points and the set of nonzero coordinates in given codeword as a block. Therefore, when we formulate some additional conditions the set of codewords of given weight can be regarded as a combinatorial design.

The formulation of such conditions is in Theorem 3.2.2. Since the binary Kerdock code satisfies them, we get 3 infinite sets of combinatorial 3-design.

The second part of the section then considers quaternary Kerdock codes and designs that are provided by them. In Theorem 3.3.9 we construct next two infinite sets of 3-designs.

The last chapter investigates possibilities of a connection between theory of Kerdock codes and cryptography.

Codewords of the second order Reed-Muller code are just evaluations of Boolean functions of arity m and degree ≤ 2 and we can therefore look to codewords of binary Kerdock codes in the same way.

If we use an algebraic structure of Kerdock code $\mathcal{K}(m)$, we can show that the difference between each two codewords from $\mathcal{K}(m)$ corresponds to an affine Boolean function or to a Boolean function that reaches maximal distance from the set of affine functions. These maximal functions are called bent and due to their high nonlinearity are very useful in construction of basic cryptographic schemes.

In the second part of the last chapter we will use the systematicity of Kerdock codes to construction of functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^k$, such that for each choice of values of t bits ($t \leq n$), each possible output k-tuple occurs equally likely. The function with this property is called (n, k, t)-resilient.

The reader is expected to have at least basic knowledge of theory of error-correcting codes, linear algebra and theory of finite fields.

1. Constructions and basic properties of Kerdock codes

There are many different ways how to construct binary codes with the same parametres as codes defined by A. M. Kerdock in [21]. In this chapter we will describe two of them.

The first method takes the Kerdock code of length 2^m, $m \geq 4$ even, as a union of certain cosets of the first order Reed-Muller code $\mathcal{RM}(1, m)$ in the second order Reed-Muller code $\mathcal{RM}(2, m)$. This approach allows us to study Kerdock codes from a geometrical point of view.

The second method is based on an observation that the Kerdock code of length 2^m, $m \geq 4$ even, is a binary image of an extended cyclic code over the ring $\mathbb{Z}_4$ of length 2^{m-1}.

The second part of this chapter is dedicated to a description of several basic properties of Kerdock codes, which will be used in the following chapters of this thesis.

1.1 Kerdock code as union of cosets of $\mathcal{RM}(1, m)$

Reed-Muller codes form a well-known family of binary linear codes that can be defined in terms of Boolean functions.

Let m be an integer and let elements of vector space $\mathbb{F}_2^m$ be numbered in some way. Usually we use a lexicographical ordering, i.e. we bind an index $i = \sum_{j=1}^{m} v_j 2^{m-j}$ to a vector $\mathbf{v} = (v_1, \ldots, v_m) \in \mathbb{F}_2^m$ and elements of the space $\mathbb{F}_2^m$ are then ordered by this index.

A *Boolean function* f of arity m is any function $f: \mathbb{F}_2^m \to \mathbb{F}_2$. We can assign to each Boolean function f an evaluation vector $v_f = (u_0, \ldots, u_{2^m-1})$, where $u_i = f(v_1, \ldots, v_m)$ for $i = \sum_{j=1}^{m} v_j 2^{m-j}$.

There is a one-to-one correspondence between Boolean functions of given arity m and polynomials from the ring $\mathbb{F}_2[x_1, \ldots, x_m]/(x_1 + x_1^2, \ldots, x_m + x_m^2)$. Elements of this ring are often called *Boolean polynomials* and every such polynomial $p(x_1, \ldots, x_m)$ can be expressed in the form

$$p(x_1, \ldots, x_m) = \sum a_{i_1,\ldots,i_m} x_1^{i_1} \cdot \ldots \cdot x_m^{i_m}, \tag{1.1}$$

where $i_1, \ldots, i_m \in \{0, 1\}$ and $a_{i_1,\ldots,i_m} \in \mathbb{F}_2$. The maximal value of sum $i_1 + \ldots + i_m$ over all terms with a nonzero value of $a_{i_1,\ldots,i_m}$ is called the *degree* of the polynomial $p(x_1, \ldots, x_m)$. In the following text we will mean by a *degree* of the Boolean function f a degree of the corresponding Boolean polynomial $p(x_1, \ldots, x_m)$.

Boolean functions of degree $d \leq 1$ are often called *affine*. Boolean polynomial that corresponds to an affine Boolean function of arity m is therefore in the form

$$\sum_{i=1}^{m} a_i x_i + a_0, \tag{1.2}$$

where $a_0, a_1, \ldots, a_m \in \mathbb{F}_2$.

Connections between Boolean functions and Boolean polynomials are described in more detail e.g. in Chapter 2 in [25].

Definition 1.1.1. The *first order Reed-Muller code* $\mathcal{RM}(1, m)$ of length 2^m, $m \geq 1$, is the binary code that consists of evaluation vectors v_f where f runs through all affine Boolean functions f of arity m, i.e. each codeword of $\mathcal{RM}(1, m)$ is equal to v_f for a Boolean function f of arity m and degree $d \leq 1$.

The *second order Reed-Muller code* $\mathcal{RM}(2, m)$ of length 2^m, $m \geq 2$, is a binary code consisting of evaluation vectors v_f corresponding to Boolean functions f of arity m and degree $d \leq 2$.

The first-order Reed-Muller code $\mathcal{RM}(1, m)$ is a linear code with 2^{m+1} codewords and minimum distance 2^{m-1}. The second-order Reed-Muller code $\mathcal{RM}(2, m)$ is a linear code that contains $2^{\frac{m^2+m}{2}+1}$ codewords and its minimum distance is equal to 2^{m-2}.

Denote the set of all affine Boolean functions of arity m by L_m and the set of all Boolean functions of arity m of degree $d \leq 2$ by Q_m. Both sets L_m and Q_m then form vector spaces, since the sum of two Boolean functions of degree $d \leq 1$ or $d \leq 2$, is the Boolean function of degree $d \leq 1$ or $d \leq 2$, respectively. It is easy to see that L_m is a vector subspace of Q_m.

Due to correspondence between Boolean functions and Boolean polynomials, each Boolean function $l(x_1, \ldots, x_m) \in L_m$ can be expressed in the polynomial form

$$l(x_1, \ldots, x_m) = \sum_{k=1}^{m} a_k x_k + c, \tag{1.3}$$

and each element Boolean function $q(x_1, \ldots, x_m) \in Q_m$ has the polynomial form

$$q(x_1, \ldots, x_m) = \sum_{1 \leq i < j \leq m} q_{ij} x_i x_j + \sum_{k=1}^{m} a_k x_k + c, \tag{1.4}$$

where $q_{ij} \in \mathbb{F}_2$ for $1 \leq i < j \leq m$, $a_k \in \mathbb{F}_2$ for $1 \leq k \leq m$ and $c \in \mathbb{F}_2$.

Moreover, the set Q_m can be divided into $2^{\frac{m^2-m}{2}}$ disjoint parts with respect to the quadratic term $\sum_{1 \leq i < j \leq m} q_{ij} x_i x_j$ in the polynomial representation of elements of Q_m, i.e.

$$Q_m = \bigcup_{q \in Q'_m} \left\{ q + \sum_{k=1}^{m} a_k x_k + c; a_k \in \mathbb{F}_2, 1 \leq k \leq m, c \in \mathbb{F}_2 \right\}, \tag{1.5}$$

where $Q'_m = \left\{ \sum_{1 \leq i < j \leq m} q_{ij} x_i x_j;\ q_{ij} \in \mathbb{F}_2,\ 1 \leq i < j \leq m \right\}$.

The set Q'_m forms the complete set of representants of cosets modulo L_m. A cardinality of each coset C modulo L_m is then equal to cardinality of the set L_m ($|C| = |L_m| = 2^{m+1}$).

From Definition 1.1.1 it immediately follows that $\mathcal{RM}(1,m)$ can be identified with the vector space L_m and $\mathcal{RM}(2,m)$ corresponds precisely to the vector space Q_m. The first order Reed-Muller code $\mathcal{RM}(1,m)$ is therefore the vector subspace of $\mathcal{RM}(2,m)$ and each coset in $\mathcal{RM}(2,m)$ modulo $\mathcal{RM}(1,m)$ is uniquely identified by quadratic term $q \in Q'_m$.

The quadratic term $q = \sum_{1\leq i<j\leq m} q_{ij}x_ix_j \in Q'_m$ is fully described by its coefficients q_{ij}, $1 \leq i < j \leq m$. If we arrange the coefficients into a matrix such that indices i and j determine a corresponding row and column, we get an upper triangular matrix $Q = (q_{ij})_{1\leq i<j\leq m}$ of size $m \times m$ with zeros at diagonal. The matrix Q uniquely corresponds to given coset C of the first order Reed-Muller code.

In the following chapters we will identify the coset C of $\mathcal{RM}(1,m)$ (with a coefficient upper triangular matrix Q) also with a skew-symmetric matrix (antisymmetric matrix with zero diagonal) $B = Q + Q^T$, i.e. $B = (b_{ij})_{i,j=1}^m$, where $b_{ij} = b_{ji} = q_{ij}$).

From now, let $m \geq 4$ be an even integer. We will construct a binary Kerdock code $\mathcal{K}(m)$ of length 2^m as a union of certain cosets of $\mathcal{RM}(1,m)$. An appropriate set of cosets is identified by a Kerdock set of skew-symmetric matrices. This set is maximal in the sense that a difference between each two distinct matrices is a regular matrix and it has the biggest possible cardinality.

Definition 1.1.2. Let $m \geq 4$ be an even integer. A *Kerdock set* $\mathcal{K}$ is a set of 2^{m-1} skew-symmetric $m \times m$ matrices such that

- the zero matrix is in $\mathcal{K}$,
- a difference between each two distinct matrices in $\mathcal{K}$ is regular.

The *Kerdock code* $\mathcal{K}(m)$ of length 2^m is a union of cosets of the first order Reed-Muller code $\mathcal{RM}(1,m)$ corresponding to matrices in the Kerdock set $\mathcal{K}$.

1.2 Kerdock code as $\mathbb{Z}_4$-code

Error-correcting codes were historicaly considered as sets of n-tuples ($n \in \mathbb{N}$) over a finite field $\mathbb{F}_q$, usually $q = 2$. But in [15] it has been observed that an analogical construction of sets over the ring $\mathbb{Z}_4$ also makes sense. The next research of $\mathbb{Z}_4$-codes has led to a generalization of understanding of error-correcting codes.

One of the first findings in theory of $\mathbb{Z}_4$-codes was an observation that the binary Kerdock code of length 2^m can be viewed as an image of a linear $\mathbb{Z}_4$-code of length 2^{m-1} under the specific mapping.

This section contains a basic introduction to theory of $\mathbb{Z}_4$-codes and their connection to suitable binary codes, especially the Kerdock codes.

The main sources for the section were book [35] and article [15].

Definition 1.2.1. Let $\mathbb{Z}_4$ be a ring of integers mod 4 and let $\mathbb{Z}_4^n$, $n \in \mathbb{N}$, be a set of n-tuples over $\mathbb{Z}_4$. Any non-empty subset $\mathcal{C}$ of $\mathbb{Z}_4^n$ is called a $\mathbb{Z}_4$-*code* (or a *quaternary code*) of length n.

If a $\mathbb{Z}_4$-code $\mathcal{C}$ is an additive subgroup of the group $\mathbb{Z}_4^n$ we call it a $\mathbb{Z}_4$-*linear code*.

Similarly as for the linear codes over a finite field, each $\mathbb{Z}_4$-linear code can be described in the form of the generator matrix.

Definition 1.2.2. Let $\mathcal{C}$ be a $\mathbb{Z}_4$-linear code. A matrix G is called a *generator matrix* of $\mathcal{C}$ if the rows of G span the code $\mathcal{C}$ and none of them can be written as a linear combination of the other rows of G.

The previous definition allows us to write any codeword $\mathbf{c} \in \mathbb{Z}_4^n$ from a $\mathbb{Z}_4$-linear code $\mathcal{C} \subseteq \mathbb{Z}_4^n$ as a linear combination of rows of its generator matrix with coefficients from $\mathbb{Z}_4$.

On $\mathbb{Z}_4^n$ we can define an *inner product* of two vectors $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}_4^n$ and $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_4^n$ by

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \pmod 4. \tag{1.6}$$

It allows us to construct a dual code $\mathcal{C}^\perp$ to a quaternary code $\mathcal{C}$ in a standard way.

Definition 1.2.3. Let $\mathcal{C}$ be a $\mathbb{Z}_4$-linear code of length n. The set

$$\mathcal{C}^\perp = \{\mathbf{x} \in \mathbb{Z}_4^n; \mathbf{x} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{y} \in \mathcal{C}\} \tag{1.7}$$

forms a $\mathbb{Z}_4$-linear code called a *dual code* of $\mathcal{C}$.

For each binary code, three basic parameters can be found — the length of the code n, the number of codewords k, and the minimum distance d. The quaternary codes can be described by analogical parameters. The length and the number of the codewords have the same meaning in both cases. The only difference is in the definition of distance between two codewords (and generally between two vectors). For binary codes, the Hamming distance is considered. In the quaternary case we will define a Lee weight and consequently a Lee distance.

Definition 1.2.4. *Lee weights* $w_L(i)$ of elements $i \in \mathbb{Z}_4$ are defined by

$$w_L(0) = 0, \quad w_L(1) = w_L(3) = 1, \quad w_L(2) = 2. \tag{1.8}$$

The *Lee weight* $w_L(\mathbf{x})$ of a vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}_4^n$ is the rational sum of Lee weights of its components, i.e.

$$w_L(\mathbf{x}) = \sum_{i=1}^{n} w_L(x_i). \tag{1.9}$$

The Lee weight function determines on $\mathbb{Z}_4^n$ a distance function

$$d_L(x, y) = w_L(\mathbf{x} - \mathbf{y}), \ \mathbf{x}, \mathbf{y} \in \mathbb{Z}_4^n \tag{1.10}$$

called the *Lee distance*.

Now we connect quaternary and binary codes using an appropriate mapping. A suitable encoding that assigns two bits to each value from $\mathbb{Z}_4$ is called the *Gray map*. Its definition reflects physical properties of a transmission channel.

In the following text, when we speak about a *binary image* of quaternary code $\mathcal{C}$, we always mean its image $C = \phi(\mathcal{C})$ under the Gray map ϕ.

Definition 1.2.5. Define two maps β and γ from $\mathbb{Z}_4$ to $\mathbb{Z}_2$ by

$$\begin{aligned} \beta(0) = \beta(1) = 0, \qquad & \beta(2) = \beta(3) = 1, \\ \gamma(0) = \gamma(3) = 0, \qquad & \gamma(1) = \gamma(2) = 1 \end{aligned} \tag{1.11}$$

and extend them to the maps from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^n$ by

$$\begin{aligned} \beta(\mathbf{x}) &= (\beta(x_1), \ldots, \beta(x_n)), \\ \gamma(\mathbf{x}) &= (\gamma(x_1), \ldots, \gamma(x_n)), \end{aligned} \tag{1.12}$$

for all $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}_4^n$.

The *Gray map* ϕ is a mapping from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$ given by

$$\phi(\mathbf{x}) = (\beta(\mathbf{x}), \gamma(\mathbf{x})), \quad \mathbf{x} \in \mathbb{Z}_4^n. \tag{1.13}$$

A property that confirms applicability of the Gray map ϕ is its ability to preserve distances between suitable vectors in their binary and quaternary forms.

Lemma 1.2.6. *The Gray map ϕ is a weight-preserving map from*

$$(\mathbb{Z}_4^n, \textit{Lee weight}) \textit{ to } (\mathbb{Z}_2^{2n}, \textit{Hamming weight}),$$

and a distance-preserving map from

$$(\mathbb{Z}_4^n, \textit{Lee distance}) \textit{ to } (\mathbb{Z}_2^{2n}, \textit{Hamming distance}),$$

i.e.

$$\begin{aligned} w_L(\mathbf{x}) &= w(\phi(\mathbf{x})), \textit{ for all } \mathbf{x} \in \mathbb{Z}_4^n, \\ d_L(\mathbf{x}, \mathbf{y}) &= d(\phi(\mathbf{x}), \phi(\mathbf{y})), \textit{ for all } \mathbf{x}, \mathbf{y} \in \mathbb{Z}_4^n, \end{aligned} \tag{1.14}$$

where functions w and d are the Hamming weight and distance functions of binary vectors.

Proof. Due to Definition 1.2.5, equations $w_L(x_i) = w(\phi(x_i))$ hold for all $x_i \in \mathbb{Z}_4$. Moreover, for all $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}_4^n$

$$w_L(\mathbf{x}) = \sum_{i=1}^{n} w_L(x_i) \tag{1.15}$$

and

$$w(\phi(\mathbf{x})) = w(\beta(\mathbf{x}), \gamma(\mathbf{x})) = \sum_{i=1}^{n} w(\beta(x_i), \gamma(x_i)) = \sum_{i=1}^{n} w(\phi(x_i)). \tag{1.16}$$

The equation $w_L(\mathbf{x}) = w(\phi(\mathbf{x}))$ then holds.

An analogical approach can be used for distances. □

From the previous lemma it also follows that the minimum Lee weight and the minimum Lee distance of quaternary code $\mathcal{C}$ is equal to the minimum Hamming weight and the minimum Hamming distance of its binary image $C = \phi(\mathcal{C})$, i.e.

$$\begin{aligned} \min\{w_L(\mathbf{c}); \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq \mathbf{0}\} &= \min\{w(\phi(\mathbf{c})); \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq \mathbf{0}\}, \\ \min\{d_L(\mathbf{c}, \mathbf{c}'); \mathbf{c}, \mathbf{c}' \in \mathcal{C}, \mathbf{c} \neq \mathbf{c}'\} &= \min\{d(\phi(\mathbf{c}), \phi(\mathbf{c}')); \mathbf{c}, \mathbf{c}' \in \mathcal{C}, \mathbf{c} \neq \mathbf{c}'\}. \end{aligned} \tag{1.17}$$

In traditional theory of error-correcting codes, a large part of the research is dedicated to the study of cyclic codes, since they are easy to describe and encode. Theory of binary cyclic codes depends upon the structure of the ring $\mathbb{F}_2[x]/(x^n - 1)$, where n is the length of a given code. Each cyclic code is an ideal of this ring and each codeword can be represented as a polynomial from $\mathbb{F}_2[x]$ of degree less than n (sometimes called the *code polynomial*).

A similar theory can be built if we want to introduce and study quaternary cyclic codes.

Definition 1.2.7. Let $\mathcal{C}$ be a $\mathbb{Z}_4$-linear code of length n. The code $\mathcal{C}$ is called *cyclic* (or $\mathbb{Z}_4$-*cyclic*), if it is invariant under a cyclic shift, i.e. if

$$\mathbf{c} = (c_0, c_1, \ldots, c_{n-2}, c_{n-1}) \in \mathcal{C} \Rightarrow \tilde{\mathbf{c}} = (c_{n-1}, c_0, \ldots, c_{n-3}, c_{n-2}) \in \mathcal{C}. \tag{1.18}$$

A structure of $\mathbb{Z}_4$-cyclic code $\mathcal{C}$ of length n will be more understandable if we will think about the codewords from $\mathcal{C}$ as about the elements of the ring $R_n = \mathbb{Z}_4[x]/(x^n - 1)$. The ring consists of the residue classes of $\mathbb{Z}_4[x]$ modulo $x^n - 1$. Each polynomial from $\mathbb{Z}_4[x]$ of a degree less than n belongs to the different residue class and we can take these polynomials as representants of the residue classes. The ring R_n can be therefore considered as ring of polynomials from $\mathbb{Z}_4[x]$ of degree less than n with addition, subtraction and multiplication modulo $x^n - 1$. Each codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-2}, c_{n-1}) \in \mathcal{C}$ can be identified with a polynomial

$$c(x) = c_0 + c_1 x + \ldots + c_i x^i + \ldots + c_{n-1} x^{n-1} \in R_n.$$

In the following text we will use both notations, i.e. we will write both $\mathbf{c} \in \mathcal{C}$ and $c(x) \in \mathcal{C}$ to express that given codeword belongs to the code $\mathcal{C}$. If $p(x)$ is a polynomial from $\mathbb{Z}_4[x]$ whose remainder, upon division by $x^n - 1$, belongs to $\mathcal{C}$, we write $p(x) \in \mathcal{C} \pmod{x^n - 1}$.

Now we show that $\mathbb{Z}_4$-cyclic codes correspond precisely to ideals of the ring R_n. The theorem can be found in [1] (Theorem 2.1).

Theorem 1.2.8. *There is a one-to-one correspondence between $\mathbb{Z}_4$-cyclic codes of length n and ideals of the ring $R_n = \mathbb{Z}_4[x]/(x^n - 1)$.*

Proof. Let $\mathcal{C}$ be a $\mathbb{Z}_4$-linear code of length n and let $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ be a codeword of $\mathcal{C}$ identified with a polynomial $c(x)$. Shifted codeword

$$\tilde{\mathbf{c}} = (c_{n-1}, c_0, \ldots, c_{n-3}, c_{n-2}) \in \mathcal{C} \tag{1.19}$$

is then associated with a polynomial

$$\tilde{c}(x) = xc(x) \in \mathcal{C} \pmod{x^n - 1}. \tag{1.20}$$

The additional shifts of the codeword $\mathbf{c}$ don't take us out of the code $\mathcal{C}$ and we have

$$x^i c(x) \in \mathcal{C} \pmod{x^n - 1}, \text{ for all } i \in \mathbb{N}. \tag{1.21}$$

Due to the $\mathbb{Z}_4$-linearity of code $\mathcal{C}$,

$$a_i x^i c(x) \in \mathcal{C} \pmod{x^n - 1} \tag{1.22}$$

and consequently

$$\sum_{i=0}^{m} a_i x^i c(x) \in \mathcal{C} \pmod{x^n - 1} \tag{1.23}$$

for any $a_i \in \mathbb{Z}_4$, $0 \leq i \leq m$. For every polynomial $a(x) = \sum_{i=0}^{m} a_i x^i \in \mathbb{Z}_4[x]$ the product $a(x)c(x) \pmod{x^n-1}$ thus belongs to $\mathcal{C}$. Moreover, from the $\mathbb{Z}_4$-linearity it follows that code $\mathcal{C}$ is closed under polynomial addition and therefore $\mathcal{C}$ is an ideal of the ring $\mathbb{Z}_4[x]/(x^n - 1)$.

Otherwise, let I be an ideal of the ring $\mathbb{Z}_4[x]/(x^n - 1)$ and let $p(x) \in I$ be a polynomial over $\mathbb{Z}_4$ of degree less than n. Since any ideal of the ring is closed under a multiplication by any element from the ring and since the polynomial $q(x) = x$ is in $\mathbb{Z}_4[x]/(x^n - 1)$ for all $n \geq 2$, the product $q(x)p(x) \pmod{x^n - 1}$ belongs to the ideal I. We have shown that if I contains a polynomial corresponding to the vector $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ then it contains a polynomial corresponding to the shifted vector $\bar{\mathbf{c}} = (c_{n-1}, c_0, \ldots, c_{n-2})$ and the ideal I therefore forms a $\mathbb{Z}_4$-cyclic code. □

For any polynomial $f(x) \in \mathbb{Z}_4[x]$ of degree less than n define a principal ideal of the ring R_n generated by the polynomial $f(x)$ by

$$(f(x)) = \{f(x)h(x);\ h(x) \in R_n\} \tag{1.24}$$

(the multiplication of the polynomials is done modulo $x^n - 1$).

Definition 1.2.9. Let $g(x) \in \mathbb{Z}_4[x]$ be a monic polynomial dividing $x^n - 1$ (i.e. there exist a polynomial $h(x) \in \mathbb{Z}_4[x]$ such that $g(x)h(x) = x^n - 1$). Let $\mathcal{C} = (g(x))$ be a principal ideal of R_n generated by $g(x)$. Then $\mathcal{C}$ is called a $\mathbb{Z}_4$-cyclic code with the *generator polynomial* $g(x)$.

Let $\mathcal{C}$ be a $\mathbb{Z}_4$-cyclic code of length n with a generator polynomial $g(x) = \sum_{i=0}^{m} g_i x^i \in \mathbb{Z}_4[x]$ of degree $m < n$ (i.e. $g(x) \in R_n$). Each codeword $c(x) = \sum_{j=0}^{n-1} c_j x^j \in \mathcal{C}$ is element of the ring R_n and can be therefore expressed as product

$$c(x) = g(x)f(x) = \sum_{i=0}^{n-m} f_k x^k g(x), \tag{1.25}$$

where $f(x) \in R_n$ is a polynomial of degree $\leq n - m$ (the multiplication of the polynomials is done modulo $x^n - 1$).

Moreover, the codeword $c(x) \in \mathcal{C}$ can be expressed as a linear combination of polynomials $g(x)$, $xg(x)$, $\ldots$, $x^{n-m}g(x)$. Since there exists a polynomial $h(x) \in R_n$ of degree $n - m$ such that $g(x)h(x) = 0$ in R_n (i.e. $g(x)h(x) \equiv 0 \pmod{x^n - 1}$), the polynomial $x^{n-m}g(x)$ can be expressed as a linear combination

of $g(x),\ xg(x),\ \ldots,\ x^{n-m-1}g(x)$. The polynomial $h(x)$ is often called the *check polynomial* of code $\mathcal{C}$.

The generator matrix of $\mathbb{Z}_4$-cyclic code $\mathcal{C}$ with generator polynomial $g(x) = \sum_{i=0}^{m} g_i x^i$ is then $n \times (n-m)$ matrix in the form

$$G = \begin{pmatrix} g_0 & g_1 & \ldots & g_m & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & g_m & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \ldots & 0 & g_0 & g_1 & \ldots & g_m \end{pmatrix}. \tag{1.26}$$

Each codeword from $\mathcal{C}$ can be described as a linear combination of rows from the matrix G.

In Theorem 1.2.8 we have shown that $\mathbb{Z}_4$-cyclic codes correspond precisely to ideals of the ring R_n. Previous paragraphs were concerned with codes that correspond to a principal ideal of the ring R_n generated by polynomial $g(x)$ dividing $x^n - 1$.

In the binary case, each cyclic code is generated by a monic polynomial $g(x)$ dividing $x^n - 1$. In the quaternary case, we have to be more careful. If we consider the $\mathbb{Z}_4$-cyclic codes of odd length n, then every ideal in the ring R_n is principal, but its generating polynomial don't have to be a divisor of polynomial $x^n - 1$ in $\mathbb{Z}_4[x]$. The previous construction therefore doesn't cover all $\mathbb{Z}_4$-cyclic codes, but it is sufficient for an introduction to quaternary Kerdock codes.

The more detailed information about ideals in the ring $\mathbb{Z}_4[x]/(x^n - 1)$ can be found in Chapter 7.4 in [35].

When we want to study binary cyclic codes, we usually use fields $\mathbb{F}_{2^m}$ for an appropriate $m \in \mathbb{N}$. The parameter m is chosen so that the field $\mathbb{F}_{2^m}$ contains an nth root of unity. Similarly in the case of $\mathbb{Z}_4$-cyclic codes, it is convenient to introduce the Galois ring $\mathrm{GR}(4^m)$ for an appropriate $m \in \mathbb{N}$.

In the following paragraphs we introduce the basic structure of Galois ring $\mathrm{GR}(4^m)$. Then we use it in a construction of quaternary Kerdock codes.

First polynomials over $\mathbb{Z}_4$ analogous to the irreducible and primitive polynomials from $\mathbb{F}_2[x]$ will be defined.

Let $\mu : \mathbb{Z}_4[x] \to \mathbb{Z}_2[x]$ be a map that naturally extends the modulo-2 map from $\mathbb{Z}_4$ to $\mathbb{F}_2$, i.e.

$$\mu\left(\sum_{i=0}^{k} a_i x^i\right) = \sum_{i=0}^{k} (a_i \bmod 2) x^i \tag{1.27}$$

for all polynomials $\sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_4[x]$ of a degree $k \geq 0$.

It is easy to see that this extended map is a ring homomorphism from $\mathbb{Z}_4[x]$ onto $\mathbb{Z}_2[x]$ with kernel $(2) = 2\mathbb{Z}_4[x]$.

Definition 1.2.10. Let $h(x) \in \mathbb{Z}_4[x]$ be a monic polynomial of degree m that divides $x^n - 1 \pmod 4$, where $n = 2^m - 1$ (i.e. there exists a polynomial $f(x) \in \mathbb{Z}_4[x]$ such that $h(x)f(x) = x^n - 1$ in $\mathbb{Z}_4[x]$). Let $\mu(h(x)) \in \mathbb{F}_2[x]$ be the irreducible

polynomial (in $\mathbb{F}_2[x]$). Then the polynomial $h(x)$ is called a *basic irreducible polynomial* of degree m over $\mathbb{Z}_4[x]$.

If the polynomial $\mu(h(x)) \in \mathbb{F}_2[x]$ is primitive in $\mathbb{F}_2[x]$, then the polynomial $h(x)$ is called a *basic primitive polynomial*.

In theory of Galois fields, it is known that for any integer $m \geq 0$ there exists both irreducible and primitive polynomials of degree m over any finite field $\mathbb{F}_q$ ($q \in \mathbb{N}$ is a power of prime number), i.e. the existence of such polynomials is ensured also in $\mathbb{F}_2[x]$. This fact can be extended to polynomials over $\mathbb{Z}_4$. The main idea of the proof is an application of the Hensel's lemma (see Lemma 5.2 in [35]) on irreducible or primitive polynomial from $\mathbb{F}_2[x]$. For any positive integer m thus exists basic irreducible polynomial and basic primitive polynomial of degree m in $\mathbb{Z}_4[x]$.

Let $h(x) \in \mathbb{Z}_4[x]$ be a basic irreducible polynomial of degree m. The set of all polynomials over $\mathbb{Z}_4$ of degree less than m with operations modulo $h(x)$ forms a Galois ring $\mathrm{GR}(4^m)$, i.e. each element of $\mathrm{GR}(4^m)$ can be expressed as the residue class

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_{m-1} x^{m-1} + (h(x)), \tag{1.28}$$

where $a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}_4$.

Definition 1.2.11. Let $h(x)$ be a basic irreducible polynomial of degree $m \in \mathbb{N}$ over $\mathbb{Z}_4$. The residue class ring $\mathbb{Z}_4[x]/(h(x))$ is called the Galois ring and is denoted by $\mathrm{GR}(4^m)$.

Basic properties of the Galois ring $\mathrm{GR}(4^m)$ for $m \in \mathbb{N}$ are summarized in the following theorem. These results can be found in Theorem 6.1 in [35]. In finite field theory the similar basic description of $\mathbb{F}_{2^m}$ is often formulated.

Theorem 1.2.12. *Let $h(x) \in \mathbb{Z}_4[x]$ be a basic irreducible polynomial of degree $m \in \mathbb{N}$. Then the Galois ring $\mathrm{GR}(4^m) = \mathbb{Z}_4[x]/(h(x))$ is a finite ring of characteristic 4 (i.e. the order of 1 in the additive group of ring $\mathrm{GR}(4^m)$ is equal to 4) with 4^m elements. Denote $\xi = x + (h(x))$, then $h(\xi) = 0$ and every element of $\mathrm{GR}(4^m)$ can be written uniquely in the form*

$$a_0 + a_1 \xi + \ldots + a_{m-1} \xi^{m-1}, \tag{1.29}$$

where $a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}_4$, and $\mathrm{GR}(4^m) = \mathbb{Z}_4[\xi]$.

Proof. A characteristic of ring is an order of the identity 1 in its additive group and in the case of Galois ring $\mathrm{GR}(4^m)$ it is equal to 4 because $(1 + (h(x))) + (1 + (h(x))) + (1 + (h(x))) + (1 + (h(x))) = 0 + (h(x))$.

The number of elements in the Galois ring can be easily determined from expression (1.28) since there exist precisely 4^m sets of coefficients $a_0, a_1, \ldots, a_{m-1}$.

Denote $\xi = x + (h(x))$, then

$$h(\xi) = h(x) + (h(x)) = 0 + (h(x)) \tag{1.30}$$

and ξ is therefore a root of polynomial $h(x)$ and elements

$$a_0 + a_1 \xi + \ldots + a_{m-1} \xi^{m-1}, \tag{1.31}$$

where $a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}_4$, correspond precisely to all distinct elements of the ring $\mathrm{GR}(4^m)$. Therefore $\mathrm{GR}(4^m) = \mathbb{Z}_4[\xi]$.

□

The expression (1.29) gives us an *additive representation* of elements of Galois ring $\mathrm{GR}(4^m) = \mathbb{Z}_4[\xi]$.

The construction of Galois ring $\mathrm{GR}(4^m)$ based on factorization of the polynomial ring $\mathbb{Z}_4[x]$ by a basic irreducible polynomial from $\mathbb{Z}_4[x]$ of degree $m \in \mathbb{N}$ doesn't tell anything about the uniqueness of Galois ring. But it can be shown that any two Galois rings, both of characteristic 4 and having the same number of the elements, are isomorphic (see [35], Theorem 6.5 and Corollary 6.6).

Since the additive representation of element of the Galois ring $\mathrm{GR}(4^m)$ doesn't have to be appropriate in all cases, we introduce the second canonical way of representation called *multiplicative* or *2-adic*.

The proof of the following results is only sketched, the complete proofs of particular parts can be found in [35], Chapter 6.

Theorem 1.2.13. *Let m be a positive integer.*

(i) In the Galois ring $\mathrm{GR}(4^m)$ there exist a nonzero element ξ of order $2^m - 1$, which is a root of basic primitive polynomial $h(x)$ of degree m over $\mathbb{Z}_4$ and $\mathrm{GR}(4^m) = \mathbb{Z}_4[\xi]$.

(ii) Let $\mathcal{T}_m = \{0, 1, \xi, \ldots, \xi^{2^m-2}\}$, then any element $c \in \mathrm{GR}(4^m)$ can be written uniquely as

$$c = a + 2b, \tag{1.32}$$

where $a, b \in \mathcal{T}_m$.

(iii) Any element $\eta \in \mathrm{GR}(4^m)$ of order $2^m - 1$ is of the form ξ^j, where integers j and $2^m - 1$ are coprime (i.e. $\mathrm{GCD}(j, 2^m - 1) = 1$), and it is a root of basic primitive polynomial of degree m over $\mathbb{Z}_4$. Moreover, the set $\mathcal{T}_m$ is equal to $\{0, 1, \eta, \ldots, \eta^{2^m-2}\}$.

Proof. (sketch)

(i) Let ξ_2 be a primitive element of $\mathbb{F}_{2^m}$. Then order of ξ_2 is $2^m - 1$ and ξ_2 is a root of polynomial $x^{2^m-1} - 1$ over $\mathbb{F}_2$. Using Taylor series of $x^{2^m-1} - 1$, it can be shown that there exists a unique root $\xi \in \mathrm{GR}(4^m)$ of polynomial $x^{2^m-1} - 1$ over $\mathbb{Z}_4$ such that $\mu(\xi) = \xi_2$. Then $\xi^{2^m-1} = 1$ and ξ is of order $2^m - 1$ (since $\mu(\xi)$ has order $2^m - 1$).

From the structure of finite fields it follows that the polynomial $x^{2^m-1} - 1 \in \mathbb{F}_2[x]$ can be in $\mathbb{F}_2[x]$ factored into the product of distinct irreducible polynomials of degrees > 1 dividing m, i.e.

$$x^{2^m-1} - 1 = f_1(x) \ldots f_r(x), \tag{1.33}$$

where r is the number of divisors of m greater than 1. Without loss of generality we can assume that $f_1(x)$ is a primitive polynomial of degree m over $\mathbb{Z}_2$ and $\mu(\xi)$ is a root of $f_1(x)$.

Using Hensel's lemma (see Lemma 5.2 in [35]) we get the factorization of polynomial $x^{2^m-1} - 1$ in $\mathbb{Z}_4[x]$ in the form

$$x^{2^m-1} - 1 = h_1(x) \ldots h_r(x), \tag{1.34}$$

where $h_1(x), \ldots, h_r(x)$ are pairwise coprime monic polynomials and $\mu(h_i(x)) = f_i(x)$, $1 \leq i \leq r$.

Let $h(x) = h_1(x)$, then $h(x)$ is a basic primitive polynomial of degree m over $\mathbb{Z}_4$ and there exists the unique root $\eta \in \mathrm{GR}(4^m)$ of polynomial $h(x)$ such that $\mu(\eta) = \mu(\xi)$. But since η is also the root of $x^{2^m-1} - 1$, η is equal to ξ and ξ is a root of $h(x)$.

(ii) Since the Galois ring $\mathrm{GR}(4^m)$ has cardinality 4^m, it is sufficient to show that all of 4^m elements of the form $c = a + 2b$, where $a, b \in \mathcal{T}_m$, are distinct.

Assume that

$$a + 2b = a' + 2b', \tag{1.35}$$

where $a, b, a', b' \in \mathcal{T}_m$. If we apply the modulo-2 reduction μ we get $\mu(a) = \mu(a')$. Since both elements ξ and $\mu(\xi)$ are of an order $2^m - 1$, the map $\xi^i \to \mu(\xi^i)$, for $0 \leq i \leq 2^m - 2$, is bijective and $a = a'$.

It implies $2b = 2b'$. Let $b = 0$ and $b' = \xi^i$ for some $i \in \{0, \ldots, 2^m - 2\}$. From the equality $0 = 2\xi^i$ it follows that $0 = 0 \cdot \xi^{2^m-1-i} = 2\xi^i \cdot \xi^{2^m-1-i} = 2$, which contradicts $0 \neq 2$ in $\mathbb{Z}_4$. Thus $b = 0$ if and only if $b' = 0$. Now let $b = \xi^i$ and $b' = \xi^{i'}$, for $i, i' \in \{0, \ldots, 2^m - 2\}$. If $i \neq i'$ we can assume without loss of generality that $i > i'$. It implies $2\xi^{i-i'} = 2$. The element $\xi^{i-i'} - 1$ is the zero divisor or 0 and therefore it is in the ideal (2). Then $(\mu(\xi))^{i-i'} = 1$ which contradicts that $\mu(\xi)$ has order $2^m - 1$.

(iii) The assertion is corollary of the previous results.

□

The set $\mathcal{T}_m$ is often called a *Teichmuller set*.

On the finite field $\mathbb{F}_{p^n}$ ($p, n \in \mathbb{N}$, p prime) we often define a *Frobenius automorphism* $\sigma: \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ by formula $\sigma(a) = a^p$ for all $a \in \mathbb{F}_{p^n}$. The Frobenius automorphism of the field $\mathbb{F}_{p^n}$ allows us to express any authomorphism σ_i of $\mathbb{F}_{p^n}$ in the form $\sigma_i = \sigma^i$, where $i = 0, \ldots, n-1$. The automorphism group of the finite field $\mathbb{F}_q$ is therefore a cyclic group of order n.

The Frobenius map σ of the field $\mathbb{F}_{2^m}$, $m \geq 1$, thus assigns element $a^2 \in \mathbb{F}_{2^m}$ to any $a \in \mathbb{F}_{2^m}$. The map σ can be generalized to the Galois ring $\mathrm{GR}(4^m)$ as a map σ' as follows

$$\begin{aligned} \sigma': \mathrm{GR}(4^m) &\to \mathrm{GR}(4^m) \\ c = a + 2b &\mapsto c' = a^2 + 2b^2,\ a, b \in \mathcal{T}_m. \end{aligned} \tag{1.36}$$

The map σ' is called a *generalized Frobenius map* of $\mathrm{GR}(4^m)$. Since the structure of the Teichmuller set $\mathcal{T}_m$ of the Galois ring $\mathrm{GR}(4^m) = \mathbb{Z}_4[\xi]$ doesn't depend on a choice of element $\xi \in \mathrm{GR}(4^m)$ of order $2^m - 1$, the map σ' is correctly defined.

The generalized Frobenius map on $\mathrm{GR}(4^m)$ satisfies the similar conditions as the Frobenius map on finite field. The map σ' is a ring automorphism of $\mathrm{GR}(4^m)$. Moreover, any ring automorphism σ'_i of $\mathrm{GR}(4^m)$ is in the form $\sigma'_i = (\sigma')^i$ for some $0 \leq i \leq m-1$. The automorphism σ' therefore generates a cyclic group of an order m, which is usually called the *Galois group* of $\mathrm{GR}(4^m)$.

Now we define a trace map of the field $\mathbb{F}_{2^m}$ and its generalized version over the ring $\mathrm{GR}(4^m)$. The *trace map* Tr of $\mathbb{F}_{2^m}$ is a function given by

$$\begin{aligned} \mathrm{Tr}:\mathbb{F}_{2^m} &\to \mathbb{F}_2 \\ a &\mapsto a+\sigma(a)+\sigma^2(a)+\ldots+\sigma^{m-1}(a). \end{aligned} \tag{1.37}$$

The *generalized trace map* T of the ring $\mathrm{GR}(4^m)$ can be analogically defined by

$$\begin{aligned} \mathrm{T}:\mathrm{GR}(4^m) &\to \mathbb{Z}_4 \\ c &\mapsto c+\sigma'(c)+(\sigma')^2(c)+\ldots+(\sigma')^{m-1}(c). \end{aligned} \tag{1.38}$$

It can be easily verified that the generalized trace map T of $\mathrm{GR}(4^m)$ and the trace map Tr of $\mathbb{F}_{2^m}$ are connected via relationship

$$\mu \circ \mathrm{T} = \mathrm{Tr} \circ \mu, \tag{1.39}$$

where μ is the modulo-2 reduction map.

Now we have all tools needed for the construction of quaternary Kerdock codes $\mathcal{K}_4(m)$ of length $n = 2^m$.

Definition 1.2.14. Let $h(x) \in \mathbb{Z}_4[x]$ be a basic primitive polynomial of degree m for an odd integer $m \geq 3$ and let $g(x)$ be the reciprocal polynomial to the polynomial

$$\frac{x^n-1}{(x-1)h(x)}, \tag{1.40}$$

where $n = 2^m - 1$.

The $\mathbb{Z}_4$-cyclic code $\mathcal{K}_4^-(m)$ of length $n-1 = 2^m-1$ with a generator polynomial $g(x)$ is called the *shortened quaternary Kerdock code*.

The *quaternary Kerdock code* $\mathcal{K}_4(m)$ of length $n = 2^m$ is the $\mathbb{Z}_4$-code obtained from $\mathcal{K}_4^-(m)$ by adjoining the zero-sum check symbol.

Since the generator polynomial $g(x) = \sum_{i=0}^{d} g_i x^i \in \mathbb{Z}_4[x]$ of the shortened quaternary Kerdock code $\mathcal{K}_4^-(m)$ has degree

$$d = (2^m-1)-(m+1) = 2^m-m-2, \tag{1.41}$$

the generating matrix G of quaternary Kerdock code $\mathcal{K}_4(m)$ is $2^m \times (m+1)$ matrix over $\mathbb{Z}_4$ in the form

$$G = \begin{pmatrix} g_\infty & g_0 & g_1 & \cdots & g_d & & \\ g_\infty & & g_0 & g_1 & \cdots & g_d & \\ \vdots & & & \ddots & \ddots & & \\ g_\infty & & & & g_0 & g_1 & \cdots & g_d \end{pmatrix}, \tag{1.42}$$

where $g_\infty = -\sum_{i=0}^{d} g_i$ (operations are done in the ring $\mathbb{Z}_4$).

Let m be an odd integer, $m \geq 3$. Then the binary image $\mathcal{K}(m+1) = \phi(\mathcal{K}_4(m))$ of the quaternary Kerdock code $\mathcal{K}_4(m)$ is the nonlinear binary code of length

2^{m+1} with $2^{2(m+1)}$ codewords and the minimum Hamming distance $2^m - 2^{(m-1)/2}$. Therefore $\mathcal{K}(m+1)$ has the same parameters as the binary Kerdock code of length 2^{m+1} (see Definition 1.1.2).

In original article [21] A. M. Kerdock uses the trace function over the field $\mathbb{F}_2$ for construction of binary nonlinear codes. A similar approach can be provided also in the quaternary case.

Now we use the generalized trace function of the ring $\mathrm{GR}(4^m)$ to description of particular codewords of the quaternary Kerdock code $\mathcal{K}_4(m)$. The theorem can be found in [35].

Theorem 1.2.15. *Let* $\mathrm{GR}(4^m) = \mathbb{Z}_4[\xi]$ *be the Galois ring, where* ξ *is a root of basic primitive polynomial* $h(x)$ *in* $\mathrm{GR}(4^m)$*. The quaternary Kerdock code* $\mathcal{K}_4(m)$ *has the following trace description over* $\mathrm{GR}(4^m)$

$$\mathcal{K}_4(m) = \{\varepsilon\mathbf{1} + \mathbf{u}^{(\lambda)}; \varepsilon \in \mathbb{Z}_4, \lambda \in \mathbb{Z}_4[\xi]\}, \tag{1.43}$$

where

$$\mathbf{u}^{(\lambda)} = (T(\lambda\xi^{\infty}), T(\lambda\xi^0), T(\lambda\xi^1), \ldots, T(\lambda\xi^{n-1})),\ n = 2^m - 1, \tag{1.44}$$

$\mathbf{1}$ *is the all-one vector of length* $n+1$ *and with the convention that* $\xi^{\infty} = 0$*.*

Proof. First we show that the trace description of the shortened Kerdock code is

$$\mathcal{K}_4^-(m) = \{\varepsilon\mathbf{1} + \mathbf{v}^{(\lambda)}; \varepsilon \in \mathbb{Z}_4, \lambda \in \mathbb{Z}_4[\xi]\}, \tag{1.45}$$

where

$$\mathbf{v}^{(\lambda)} = (T(\lambda\xi^0), T(\lambda\xi^1), \ldots, T(\lambda\xi^{n-1})),\ n = 2^m - 1. \tag{1.46}$$

Let $\mathcal{C}$ be a code defined in (1.45). Let $\mathbf{c}$ be a codeword from $\mathcal{C}$ and $c(x)$ its polynomial expression. Then $c(x)(x-1)h(x)$ is equal to 0 because the vector $\mathbf{1}$ is annihilated by polynomial $x-1$ and the vector $\mathbf{v}^{(\lambda)}$ is annihilated by $h(x)$, since ξ is a root of $h(x)$.

The generator polynomial of code $\mathcal{K}_4^-(m)$ is a reciprocal polynomial to $(x^n - 1)/(x-1)h(x)$. It follows that check polynomial of $\mathcal{K}_4^-(m)$ is $(x-1)h(x)$. Therefore $\mathcal{C} \subseteq \mathcal{K}_4^-(m)$.

Since both codes $\mathcal{C}$ and $\mathcal{K}_4^-(m)$ contain the same number of codewords ($|\mathcal{C}| = |\mathcal{K}_4^-(m)| = 4^{m+1}$), the equality $C = \mathcal{K}_4^-(m)$ holds.

The theorem now follows from the fact that the zero-check sum for $\varepsilon\mathbf{1}$ is equal to ε and the zero-check sum for $\mathbf{v}^{(\lambda)}$ is equal to 0. □

The previous theorem showed that each codeword of quaternary Kerdock code $\mathcal{K}_4(m)$ of length 2^m can be expressed in the form

$$c = (c_{\infty}, c_0, c_1, \ldots, c_{n-1}),\ n = 2^m - 1, \tag{1.47}$$

where

$$c_i = T(\lambda\xi^i) + \varepsilon, \quad i \in \{\infty, 0, 1, \ldots, n-1\} \tag{1.48}$$

for some $\varepsilon \in \mathbb{Z}_4$ and $\lambda \in \mathrm{GR}(4^m)$.

1.3 Basic properties of Kerdock codes

Kerdock codes can be viewed as nonlinear binary codes or linear quaternary codes with parameters that are summarized in Tables 1.1 and 1.2.

They form a family of well-known codes with many interesting properties. In the following paragraphs we formulate several basic facts about the Kerdock codes, which will be consequently used in the next chapters of this thesis.

length	$n = 2^m$
number of codewords	$k = 2^{2m}$
(Hamming) minimum distance	$d = 2^{m-1} - 2^{\frac{m-2}{2}}$

Table 1.1: Parameters of the binary Kerdock code $\mathcal{K}(m)$, $m \geq 4$ even

length	$n = 2^{m-1}$
number of codewords	$k = 2^{2m}$
(Lee) minimum distance	$d = 2^{m-1} - 2^{\frac{m-2}{2}}$

Table 1.2: Parameters of the quaternary Kerdock code $\mathcal{K}_4(m-1)$, $m \geq 4$ even

The Kerdock codes are systematic.

A binary code is *systematic* if each codeword can be splitted into two disjoint parts. Bits in the first part carry an information that is present in the codeword. On the other hand, bits in the second part serve as check bits and they guarantee an ability of error-correctness.

The systematic property is always fulfilled for linear codes, but it isn't assured in the case of nonlinear codes. But although the binary Kerdock codes are nonlinear, they are systematic. This fact was shown in article [29]. It was proved that in the Kerdock code $\mathcal{K}(m)$ of length 2^m ($m \geq 4$ even) we can find a fixed set of $2m$ coordinates such that for each binary $2m$-tuple there exists exactly one codeword which take on this value in given coordinates.

The Kerdock codes are distance invariant.

A binary code C is called *distance invariant* if (Hamming) weight distributions of its translates $\mathbf{c} + C$ are the same for all codewords $\mathbf{c} \in C$.

Since a binary linear code C of length n is a linear subspace of the vector space $\mathbb{F}_2^n$, it is a distance invariant code. But similarly as for the systematicity of a code, the distance invariancy isn't guaranteed for nonlinear codes.

In the following lemma we will specify a set of binary codes (not necessarily linear) which satisfy a condition of distance invariancy. The lemma can be found in [35].

Lemma 1.3.1. *If $\mathcal{C}$ is a $\mathbb{Z}_4$-linear code, then its binary image $C = \phi(\mathcal{C})$ is distance invariant.*

Proof. Since $\mathcal{C}$ is $\mathbb{Z}_4$-linear (an additive subgroup of $\mathbb{Z}_4^n$), $\mathbf{c} + \mathcal{C} = \mathcal{C}$ for all codewords $\mathbf{c} \in \mathcal{C}$. Therefore $\mathcal{C}$ is distance invariant with respect to the Lee weight.

The result then follows from Lemma 1.2.6. □

In Section 1.2, we have defined the binary Kerdock codes $\mathcal{K}(m)$ ($m \geq 4$ even) as binary images of $\mathbb{Z}_4$-linear codes $\mathcal{K}_4(m-1)$. By applying the previous lemma, the distance invariancy of the binary Kerdock codes is confirmed.

The Kerdock codes are formally dual to Preparata codes.

The Preparata codes were first constructed in 1968 and form another important family of nonlinear binary codes. Similarly as the Kerdock codes $\mathcal{K}(m)$, the Preparata codes $\mathcal{P}(m)$ are systematic and distance invariant codes of length 2^m, where $m \geq 4$ is even. They contain 2^{2^m-2m} codewords and the minimum distance between each two codewords is equal to 6.

length	$n = 2^m$
number of codewords	$k = 2^{2^m-2m}$
(Hamming) minimum distance	$d = 6$

Table 1.3: Parameters of the binary Preparata code $\mathcal{P}(m)$, $m \geq 4$ even

Shortly after publication of Kerdock's article in 1972 ([21]), it was observed that weight and distance distributions of the Preparata code $\mathcal{P}(m)$ of length 2^m are the MacWilliams transformations of weight and distance distributions of the Kerdock code $\mathcal{K}(m)$ of the same length (i.e. these two codes behave like dual linear codes). This property was very surprising because both Kerdock and Preparata codes are nonlinear and they cannot be dual due to the standard definition.

An explanation was given in [15]. It was observed that both of these codes can be defined as binary images of $\mathbb{Z}_4$-linear codes that are dual (in the sense of Definition 1.2.3). Weight and distance distrubutions of dual quaternary codes are connected by the quaternary version of the MacWilliams identity, similarly as in the binary case.

Finally, due to Lemma 1.2.6, binary images of dual quaternary codes are connected via the binary version of MacWilliams identity. Thus the strange behaviour of the Kerdock and Preparata codes was explained.

2. Kerdock sets

One of the basic ways to define the binary Kerdock codes is based on tools of orthogonal and symplectic geometry. This chapter contains an introduction to theory of quadratic and symplectic forms and orthogonal spreads which are then used to construction of Kerdock sets and consequently the Kerdock codes.

In the whole chapter we will confine mainly to fields of characteristic 2 and vector spaces over the field of characteristic 2.

2.1 Symplectic and quadratic forms

Bilinear and quadratic forms are one of basic objects in linear algebra. In this section, we describe several properties of these forms especially over the field $\mathbb{F}_2$.

An introduction to theory of forms used in the following paragraphs can be found in Chapter 103 in [19], Chapter 2 in [7] or Chapter 1 in [28].

Definition 2.1.1. Let V be a vector space over a field F. A *quadratic* form on V is a mapping $Q\colon V \to F$ satisfying the conditions

(i) $Q(\lambda v) = \lambda^2 Q(v)$, for all $\lambda \in F, v \in V$.

(ii) The function $\beta\colon V \times V \to F$ defined by

$$Q(v+w) = Q(v) + Q(w) + \beta(v,w) \tag{2.1}$$

is a bilinear form on V.

The pair (V, Q) is an *orthogonal space*.

A relationship between bilinear form β corresponding to quadratic form Q is called a *polarisation* (i.e. quadratic form Q polarises to bilinear form β).

Let Q be a quadratic form that polarises to the bilinear form β. From point (ii) in the previous definition it follows that

$$\beta(v,w) = Q(v+w) - Q(v) - Q(w) = Q(w+v) - Q(w) - Q(v) = \beta(w,v)$$

for all $v, w \in V$ and the form β is therefore a symmetric bilinear form.

Moreover, if a characteristic of field F is equal to 2, an equation $\beta(v,v) = 0$ holds for all $v \in V$ since

$$\beta(v,v) = Q(v+v) - Q(v) - Q(v) = Q(2v) - 2Q(v) = 0$$

(i.e. the bilinear form β is alternating).

Definition 2.1.1 implies that we can assign a unique symmetric bilinear form β to any quadratic form Q on a vector space V by formula

$$\beta(v,w) = Q(v+w) - Q(v) - Q(w) \tag{2.2}$$

for all $v, w \in V$. But converse relation isn't so obvious. In the case of forms over a field F with chararacteristic different from 2, a quadratic form Q can be uniquely recovered from a symmetric bilinear form β by the formula $Q(v) = \frac{1}{2}B(v, v)$, for all $v \in V$.

If a characteristic of field F is equal to 2, the situation is different since many quadratic forms can polarise to one bilinear form. If two quadratic forms Q_1 and Q_2 both polaris to the same bilinear form β, then the quadratic form $Q = Q_1 - Q_2$ polarises to the zero form, i.e. from equations

$$\begin{aligned} Q_1(v+w) &= Q_1(v) + Q_1(w) + \beta(v, w), \\ Q_2(v+w) &= Q_2(v) + Q_2(w) + \beta(v, w), \end{aligned} \tag{2.3}$$

it follows an equation

$$Q(v+w) = Q(v) + Q(w) \tag{2.4}$$

for all $v, w \in V$. Moreover, since $\alpha^2 = \alpha$ for all $\alpha \in F$, we have

$$Q(\alpha v) = \alpha Q(v) \tag{2.5}$$

and the form Q is therefore linear. Otherwise, if two quadratic forms differ by a linear form, they polarise to the same bilinear form.

From now, we will assume that all used vector spaces are in the form $V = \mathbb{F}_2^n$, $n \in \mathbb{N}$, and all mentioned forms (bilinear or quadratic) are defined on such vector spaces.

Most bilinear forms that will be used in the following text are non-degenerate alternating bilinear forms.

Definition 2.1.2. Let β be a bilinear form on a vector space V.

If $\beta(v, v) = 0$ for all $v \in V$, the form β is called *alternating*.

The form β is said to be *non-degenerate*, if it satisfies conditions

(i) $(\beta(v, w) = 0 \text{ for all } w \in V) \Rightarrow v = 0$;

(ii) $(\beta(v, w) = 0 \text{ for all } v \in V) \Rightarrow w = 0$.

The non-degenerate alternating bilinear form is called *symplectic*. The pair (V, β) is a *symplectic space* if β is a symplectic form on V.

From remarks above it follows that any non-degenerate bilinear form β on a vector space $V = \mathbb{F}_2^m$ that corresponds to a quadratic form Q on V is symplectic.

Now we equip a vector space V with a symplectic bilinear form β. Suppose that V is even-dimensional (i.e. $\dim V = 2m$, $m \in \mathbb{N}$) and suppose that there is a basis $\{v_1, \ldots, v_m, w_1, \ldots, w_m\}$ of V such that

$$\begin{aligned} &\beta(v_i, v_j) = \beta(w_i, w_j) = 0, \text{ for all } i, j \in \{1, \ldots, m\}, \\ &\beta(v_i, w_j) = \beta(w_j, v_i) = 0, \text{ for all } i \neq j, i, j \in \{1, \ldots, m\}, \\ &\beta(v_i, w_i) = -\beta(w_i, v_i) = 1, \text{ for all } i \in \{1, \ldots, m\}. \end{aligned} \tag{2.6}$$

This basis is called *symplectic*.

By induction on the dimension of the vector space V it can be shown, that for every even-dimensional vector space, there exists a symplectic basis. This is one of basic facts for symplectic geometry and it can be found for example in Theorem 6 in [23].

In the following sections, we focus mainly on non-singular quadratic forms. Informally, a quadratic form Q on a vector space V of dimension m is non-singular, if it can't be written in fewer than m variables by any linear transformation of variables. More formal definition follows.

Definition 2.1.3. Let V be a vector space and Q be a quadratic form on V that polarises to a bilinear form β. The form Q is said to be *non-singular* if the only subspace $W \subseteq V$ with the property that Q vanishes on W and $\beta(v, w) = 0$ for all $v \in V$ and $w \in W$ is the zero subspace.

If V is a vector space over a field of an odd characteristic, then the quadratic form Q on V is non-singular if and only if the bilinear form β corresponding to Q is non-degenerate. But for the fields of a characteristic 2, the situation is again different. In this case, a quadratic form Q is non-singular if and only if the bilinear form β obtained by polarisation is non-singular.

In the next paragraphs we will need a notion of orthogonality and singularity of vectors in vector spaces equipped with a quadratic form that polarises to the symmetric bilinear form.

Definition 2.1.4. Let U be a subset of vector space V and let β be a symmetric bilinear form on V. Then the *orthogonal complement* $U^\perp$ of U is defined by

$$U^\perp = \{v \in V;\ \beta(u, v) = 0 \text{ for all } u \in U\}. \tag{2.7}$$

If $U = u$ is a singleton then $U^\perp$ is also denoted by $u^\perp$.

Definition 2.1.5. Let Q be a quadratic form on vector space V and let β be a bilinear form on V.

A vector $v \in V$ is called *isotropic* if $v \in v^\perp$, i.e. if $\beta(v, v) = 0$. A subspace $U \subseteq V$ is called *totally isotropic* if $U \leq U^\perp$, i.e. if β vanishes identically on U.

A vector $v \in V$ is called *singular* if $Q(v) = 0$. A subspace $U \subseteq V$ is said to be *totally singular*, if Q vanishes identically on U, i.e. if $Q(u) = 0$ for all $u \in U$.

Now we would like to classify quadratic forms on a vector space $V = \mathbb{F}_2^m$. First, two types of subspaces of V equipped with quadratic form Q should be defined.

Definition 2.1.6. Let Q be a quadratic form on a vector space V that polarises to a bilinear form β.

A subspace $W \subseteq V$ is called *anisotropic*, if it has no non-zero singular vectors (i.e. if $Q(w) = 0$ if and only if $w = 0$, for all $w \in W$).

A two-dimensional subspace $U = \langle v_1, v_2 \rangle$ of V is a *hyperbolic plane* if $Q(v_1) = Q(v_2) = 0$ and $\beta(v_1, v_2) = 1$.

In order to identify quadratic forms that behaves identically, we define an equivalence of quadratic forms in the following way.

Definition 2.1.7. Let Q_1, Q_2 be quadratic forms on vector spaces V_1, V_2 over a field F, respectively.

An *isometry* $\sigma\colon (V_1, Q_1) \to (V_2, Q_2)$ of orthogonal spaces (V_1, Q_1) and (V_2, Q_2) is a bijective linear mapping from V_1 to V_2 satisfying

$$Q_1(v) = Q_2(\sigma(v)), \text{ for all } v \in V_1. \tag{2.8}$$

The quadratic forms Q_1 and Q_2 are called *equivalent* if there exists an isometry σ from V_1 to V_2.

Let V be a vector space equipped with a quadratic form Q. Since a composition of two isometries of V is again an isometry and the identity function is also an isometry of V, isometries of V form a group $O(V)$ called the *orthogonal group* of V.

The orthogonal group of V of dimension m can be also viewed as a subgroup of general linear group $GL(m, 2)$ of regular $m \times m$ matrices over $\mathbb{F}_2$ that preserves the quadratic form Q (i.e. it consists of matrices $A \in GL(m, 2)$ that satisfy $Q(Ax) = Q(x)$ for all $x \in V$).

Let Q be a quadratic form on V and let f be a linear form on V, then the mapping $Q + f$ is also the quadratic form equivalent to Q since in the field of characteristic two squaring is an automorphism, i.e. there exists an isometry σ on V such that

$$Q(v) + f(v) = Q(\sigma(v)) \tag{2.9}$$

for all $v \in V$.

The classification of quadratic forms will be formulated using anisotropic spaces and hyperbolic planes. The theorem can be found in [7] (Theorem 2.1).

Theorem 2.1.8. *Let Q be a quadratic form on a vector space $V = \mathbb{F}_2^m$ that polarises to a bilinear form β.*

(i) An anisotropic space has dimension at most 2.

(ii) Let Q be a non-singular quadratic form on V. Then

$$V = W \oplus U_1 \oplus \cdots \oplus U_r, \tag{2.10}$$

where W is anisotropic, $U_1, \ldots, U_r$ are hyperbolic planes, and the summands are pairwise orthogonal.

(iii) If quadratic forms Q_1, Q_2 on vector spaces V_1, V_2, respectively, give decompositions

$$\begin{aligned} V_1 &= W_1 \oplus U_{11} \oplus \cdots \oplus U_{1r}, \\ V_2 &= W_2 \oplus U_{21} \oplus \cdots \oplus U_{2r}, \end{aligned} \tag{2.11}$$

then Q_1 and Q_2 are equivalent if and only if $r = s$ and $\dim(W_1) = \dim(W_2)$.

Proof.

(i) Let W be an anisotropic space. Then for all distinct non-zero vectors $v, w \in W$ it holds

$$\beta(v, w) = Q(v + w) + Q(v) + Q(w) = 1. \tag{2.12}$$

If $w_1, w_2, w_3 \in W$ are linearly independent, then

$$1 = \beta(w_1, w_2 + w_3) = \beta(w_1, w_2) + \beta(w_1, w_3) = 0 \tag{2.13}$$

and we have a contradiction. Therefore, in W there don't exist three linearly independent vectors and $\dim(W) \leq 2$.

(ii) The proof will be done by induction on $\dim(V)$. If $V = \{0\}$ or V is anisotropic, then $W = V$ and we have a trivial decomposition. Thus, we can suppose that there is a vector $u \in V$ such that $u \neq 0$ and $Q(u) = 0$. Since Q is nonsingular, β is also non-singular and there exists a vector $v \in V$ with $\beta(u, v) = 1$. Then

$$Q(v) + Q(u + v) = \beta(u, v) + Q(u) = 1, \tag{2.14}$$

and therefore either $Q(v) = 0$ or $Q(u + v) = 0$. If $Q(v) = 0$, then $U_1 = \langle u, v\rangle$ is a hyperbolic plane. If $Q(u + v) = 0$, then

$$\beta(u, u + v) = \beta(u, u) + \beta(u, v) = 1, \tag{2.15}$$

since β is alternating bilinear form, and $U_1 = \langle u, u + v\rangle = \langle u, v\rangle$ is again a hyperbolic plane. Moreover, $\dim(U_1^{\perp}) = \dim(v) - 2$, since

$$\dim(U) + \dim(U^{\perp}) = \dim(V) \tag{2.16}$$

for non-singular bilinear form β and for all subspaces $U \leq V$, and the restriction of Q to $U_1^{\perp}$ is nonsingular. By the induction hypothesis, $U_1^{\perp}$ can be decomposed in given form and the result is proved.

(iii) The condition on equality of number of hyperbolic planes and dimensions of anisotropic parts is sufficient since we can consider an isometry $\sigma\colon (V_1, Q_1) \to (V_2, Q_2)$ of orthogonal spaces (V_1, Q_1) and (V_2, Q_2) such that $\sigma(W_1) = W_2$ and $\sigma(U_{1i}) = U_{2i}$ for all $i = 1, \ldots, r$.

Since isometry is a bijective map on finite-dimensional vector space, it is clear that equivalent quadratic forms are defined on spaces of the same dimension. Thus, it remains to show that they have the same number r of hyperbolic planes in decomposition of V_1 and V_2. We show that the number r is for each non-singular quadratic form Q on a vector space V equal to the maximal dimension of any totally singular subspace of V, which implies the required equality.

Let Q be a non-singular quadratic form on vector space V that polarises to bilinear form β. Let

$$V = W \oplus U_1 \oplus \cdots \oplus U_r, \tag{2.17}$$

where W is anisotropic, $U_1, \ldots, U_r$ are hyperbolic planes, and the summands are pairwise orthogonal. Let $U_i = \langle u_i, v_i\rangle$, where $Q(u_i) = Q(v_i) = 0$ and $\beta(u_i, v_i) = 1$. Then $X = \langle u_1, \ldots, u_r\rangle$ is a totally singular subspace of dimension r. Now we show by induction on r that no larger totally singular subspace exists.

If $r = 0$, then V is anisotropic and the proposition is true. Let Y be a totally singular subspace of $\dim(Y) = k > 0$. Let $y \in Y$ be a nonzero vector. If we consider the vector space $V' = \langle y \rangle^{\perp} / \langle y \rangle$, then Q induces a nonsingular quadratic form Q' on V'. The decomposition of V' provides by Q' then conatins $r - 1$ hyperbolic planes. Moreover, the subspace $Y' = Y / \langle y \rangle$ of V' is a totally singular space of dimension $k - 1$. If Y is maximal totally singular subspace of V then Y' is maximal totally singular subspace of V' and from inductive hypothesis, it follows that $k - 1 = r - 1$ and thus $k = r$. □

From the previous theorem it follows that non-singular quadratic forms on a vector space $\mathbb{F}_2^m$ are determined up to equivalence by two parameters — the dimension of anisotropic part and the number of hyperbolic planes.

Definition 2.1.9. Let Q be a quadratic form on a vector space $\mathbb{F}_2^m$ and let

$$V = W \oplus U_1 \oplus \cdots \oplus U_r \tag{2.18}$$

be the decomposition given by Q. The quadratic form Q is said to be of *type* 1, 0 or -1, if $\dim(W)$ is equal to 0, 1 or 2, respectively. The number r of hyperbolic pairs, is called the *Witt index*.

In the proof of item (*iii*) we have shown that the maximal dimension of totally singular subspace of orthogonal space (V, Q) is equal to the Witt index.

Now we consider only non-singular quadratic forms on vector spaces of even dimension over the field $\mathbb{F}_2^m$, i.e. $V = \mathbb{F}_2^m$, m even. Since each hyperbolic plane U_i, $1 \leq i \leq r$, in a decomposition of V corresponding to non-singular quadratic form Q has dimension 2, the type of Q is 1 or -1 (an anisotropic part in decomposition must be of even dimension).

Moreover, if Q is the form of type 1 (i.e. vector space V can be decomposed to the direct sum of hyperbolic planes $U_1, \ldots, U_{m/2}$), it is equivalent to the form

$$Q^+(\mathbf{x}) = x_1 x_2 + \ldots + x_{m-1} x_m, \tag{2.19}$$

since we can define an isometry $\sigma : V \to V$ that identifies the basis of V with generators of hyperbolic planes $U_1, \ldots, U_{m/2}$ (in appropriate order). This case is often called *hyperbolic*.

If Q is the form of type -1 (i.e. Q decompose the vector space V to the direct sum of hyperbolic planes $U_1, \ldots, U_{m/2-1}$ and anisotropic space W of dimension 2), it is equivalent to the form

$$Q^-(\mathbf{x}) = x_1 x_2 + \ldots + x_{m-1}^2 + x_{m-1} x_m + x_m^2, \tag{2.20}$$

since we can define an isometry σ on V that identifies $m - 2$ basis vectors with generators of hyperbolic planes $U_1, \ldots, U_{m/2-1}$ and 2 vectors with generators of anisotropic space W. This case is called *elliptic*.

In the following chapters we will often need to determine the weight of evaluation vector of non-singular quadratic form on even-dimensional vector space. First we show that if we allow not only isometries between two non-singular quadratic forms, but any affine transformation, we get just one type of non-singular quadratic forms.

Lemma 2.1.10. *Let $V = \mathbb{F}_2^m$ be a vector space of even dimension m. Let Q_1 and Q_2 be non-singular quadratic forms on V. Then there exists a bijective affine mapping $\tau: V \to V$ and $t \in \mathbb{F}_2$, such that*

$$Q_1(v) = Q_2(\tau(v)) + t \tag{2.21}$$

for all $v \in V$.

Proof. If the quadratic forms Q_1 and Q_2 are of the same type, then there exist an isometry σ on V such that $Q_1(v) = Q_2(\sigma(v))$ for all $v \in V$ and we can take $\tau = \sigma$ and $t = 0$.

Let Q_1 be of type 1 and Q_2 be of type -1, then Q_1 is equivalent to Q^+ and Q_2 is equivalent to Q^-. Now it is sufficient to show, that there exist an affine mapping τ on V and $t \in \mathbf{F}_2$ such that $Q^+(v) = Q^-(\tau(v)) + t$. But if we take $t = 1$ and if τ is a mapping defined by

$$\tau(v) = (v_1, \ldots, v_{m-1} + 1, v_m + 1) \tag{2.22}$$

for all $v = (v_1, \ldots, v_{m-1}, v_m) \in V$, we get the desired equation since $x_{m-1}^2 + x_{m-1}x_m + x_m^2 = (x_{m-1} + 1)(x_m + 1) + 1$. □

From the previous lemma, it immediately follows that for all vectors $v \in V$

$$Q^+(v) = 0 \Leftrightarrow Q^-(\tau(v)) = 1 \tag{2.23}$$

where τ is defined as in (2.22). Moreover, since τ is bijective, we have that the number of singular vectors of Q^+ is equal to the number of non-singular vectors of Q^- and conversely.

Now it is easy to determine cardinalities of sets of singular and non-singular vectors of any non-singular quadratic form on $V = \mathbb{F}_2^m$, m even. The theorem can be found e.g. in [24].

Lemma 2.1.11. *Let Q be a non-singular quadratic form on vector space $V = \mathbb{F}_2^m$, where m is an even integer. If Q is of type $\varepsilon \in \{-1, 1\}$, then there exist exactly $2^{m-1} + \varepsilon 2^{m/2-1}$ singular vectors of Q.*

Proof. Let Q be of type 1. Then Q is equivalent to the quadratic form Q^+ and it is sufficient to calculate the number of singular vectors of Q^+. Let $x = (x_1, \ldots, x_m)$ be a vector from $\mathbb{F}_2^m$. If a vector $(x_1, x_3, \ldots, x_{m-1})$ is the zero vector, we have $2^{\frac{m}{2}}$ choices for $(x_2, x_4, \ldots, x_m)$ to get singular vector x. If there is at least one nonzero element at positions $x_1, x_3, \ldots, x_{m-1}$, then there are $2^{\frac{m}{2}-1}$ choices of $x_2, x_4, \ldots, x_m$ to get singular vector x. The number of singular vectors of the form Q^+ is therefore equal to $2^{\frac{m}{2}} + (2^{\frac{m}{2}} - 1)2^{\frac{m}{2}-1}$.

Let Q be of type -1. From Lemma 2.1.10, it follows that the number of singular vectors of Q is equal to the number of non-singular vectors of quadratic form of type 1, which is $2^m - (2^{m-1} + 2^{m/2-1}) = 2^{m-1} - 2^{m/2-1}$.

□

In the previous text, we have identified a quadratic form Q on a vector space V with a homogeneous polynomial of degree 2. This correspondence is formalized by the next lemma (see Proposition 1.2 in [28]).

Lemma 2.1.12. *Let V be a vector space of dimension n over field F. There is one-to-one correspondence between quadratic forms on V and homogeneous polynomials of degree 2 in n variables (i.e. homogeneous quadratic polynomials from $F[x_1, \ldots, x_n]$).*

Proof. Let $v_1, \ldots, v_n \in V$ be a fixed basis of vector space V. Let

$$p(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} \alpha_{ij} x_i x_j \tag{2.24}$$

be a homogeneous polynomial of degree 2 from $F[x_1, \ldots, x_m]$. We define a mapping $Q: V \to F$ by $Q(v) = p(\lambda_1, \ldots, \lambda_n)$, where $v = \sum_{i=1}^n \lambda_i v_i \in V$. Now we will check the conditions for Q being a quadratic form.

(i) For all $\lambda \in F$ and $v \in V$

$$Q(\lambda v) = Q(\sum_{i=1}^n \lambda \lambda_i v_i) = p(\lambda\lambda_1, \ldots, \lambda\lambda_n) = \lambda^2 p(\lambda_1, \ldots, \lambda_n) = \lambda^2 Q(v). \tag{2.25}$$

(ii) If we define a form $\beta: V \times V \to F$ by

$$\beta(v, w) = \sum_{1 \le i \le j \le n} \alpha_{ij}(\lambda_i \mu_j + \lambda_j \mu_i), \tag{2.26}$$

where $v = \sum_{i=1}^n \lambda_i v_i$ and $w = \sum_{i=1}^n \mu_i v_i$, then β is a symmetric bilinear form on V. Moreover, for all $v, w \in V$

$$\begin{aligned} Q(v+w) &= p(\lambda_1 + \mu_1, \ldots, \lambda_n + \mu_n) = \sum_{1 \le i \le j \le n} \alpha_{ij}(\lambda_i + \mu_i)(\lambda_j + \mu_j) \\ &= \sum_{1 \le i \le j \le n} \alpha_{ij}\lambda_i\lambda_j + \sum_{1 \le i \le j \le n} \alpha_{ij}\mu_i\mu_j + \sum_{1 \le i \le j \le n} \alpha_{ij}(\lambda_i\mu_j + \lambda_j\mu_i) \\ &= p(\lambda_1, \ldots, \lambda_n) + p(\mu_1, \ldots, \mu_n) + \beta(v, w) \\ &= Q(v) + Q(w) + \beta(v, w). \end{aligned} \tag{2.27}$$

The function Q is therefore a quadratic form on V.

Conversely, let $Q: V \to F$ be a quadratic form on V and $\beta: V \times V \to F$ be the corresponding bilinear form. Define a homogeneous polynomial $p(x_1 \ldots, x_n) = \sum_{1 \le i \le j \le n} \alpha_{ij} x_i x_j$ by

$$\begin{aligned} \alpha_{ii} &= Q(v_i),\ 1 \le i \le n, \\ \alpha_{ij} &= \beta(v_i, v_j),\ 1 \le i < j \le n. \end{aligned} \tag{2.28}$$

Then we have for all $v = \sum_{i=1}^n \lambda_i v_i \in V$

$$\begin{aligned} Q(v) &= Q(\sum_{i=1}^n \lambda_i v_i) = \sum_{i=1}^n Q(\lambda_i v_i) + \sum_{1 \le i < j \le n} \beta(\lambda_i v_i, \lambda_j v_j) \\ &= \sum_{i=1}^n \lambda_i^2 Q(v_i) + \sum_{1 \le i < j \le n} \lambda_i \lambda_j \beta(v_i, v_j) \\ &= \sum_{i=1}^n \alpha_{ii}\lambda_i^2 + \sum_{1 \le i < j \le n} \alpha_{ij}\lambda_i\lambda_j \\ &= \sum_{1 \le i \le j \le n} \alpha_{ij}\lambda_i\lambda_j = p(\lambda_1, \ldots, \lambda_n). \end{aligned} \tag{2.29}$$

□

2.2 Orthogonal spreads and Kerdock sets

In the previous chapter we have introduced orthogonal spaces together with their totally singular subspaces. Now we focus on totally singular subspaces of maximal dimension. These structures are in the geometric literature also called *generators*.

It is a natural question whether a set of singular points can be partitioned into generators. These partitions are called *spreads*.

In the following paragraphs we investigate spreads on orthogonal spaces and their connection to Kerdock sets. The main sources for this section were Chapter 79 in book [19] and article [4].

Let $V = \mathbb{F}_2^{2m}$ be a vector space of dimension $2m$, where m is an even integer. We equip the vector space V with a quadratic form Q that polarises to the bilinear form β defined by

$$Q(v) = x_1y_1 + \ldots + x_my_m = \sum_{i=1}^{m} x_iy_i = (x_1, \ldots, x_m) \cdot (y_1, \ldots, y_m), \tag{2.30}$$

$$\beta(v, v') = \sum_{i=1}^{m}(x_i + x'_i)(y_i + y'_i) - \sum_{j=1}^{m} x_jy_j - \sum_{k=1}^{m} x'_ky'_k = \sum_{i=1}^{m} x_iy'_i + \sum_{j=1}^{m} x'_jy_j,$$

where $v, v' \in V$ and $v = (x_1, \ldots, x_m, y_1, \ldots, y_m)$, $v' = (x'_1, \ldots, x'_m, y'_1, \ldots, y'_m)$.

The quadratic form Q is equivalent to the form Q^+ (see equation (2.19)) since we can consider an isometry σ on V that changes ordering of basis vectors of V in an appropriate way.

Note that all symplectic forms on V are equivalent to the form (2.31), i.e. if β_1 and β_2 are symplectic forms then there exist bijective linear map σ on V (*isometry*) such that $\beta_1(u, v) = \beta_2(\sigma(u), \sigma(v))$. For more information see Section 3.6 in [2].

Let $\{e_1, \ldots, e_m, f_1, \ldots, f_m\}$ be a symplectic basis of V (the symplectic basis exists since V is even-dimensional). The vector space V can be now considered as

$$V = \mathbb{F}_2^m \oplus \mathbb{F}_2^m = X \oplus Y, \tag{2.31}$$

where X and Y are the subspaces of V with bases $\{e_i\}_{i=1}^m$ and $\{f_j\}_{j=1}^m$, respectively. From now, all vectors from V will be considered with respect to the basis $\{e_1, \ldots, e_m, f_1, \ldots, f_m\}$ (i.e. for a vector $v = (x_1, \ldots, x_m, y_1, \ldots, y_m) \in V$ the element x_i is a coordinate associated with the basis vector e_i and the element y_j represents a coordinate associated with the basis vector f_j). All matrices corresponding to isometries on V will be with respect to the basis $\{e_1, \ldots, e_m, f_1, \ldots, f_m\}$.

The vector spaces X and Y are totally singular subspaces of V of dimension m (i.e. generators) since

$$Q(\mathbf{x}) = Q((x_1, \ldots, x_m, 0, \ldots, 0)) = 0, \text{ for all } x \in X \tag{2.32}$$

and

$$Q(\mathbf{y}) = Q((0, \ldots, 0, y_1, \ldots, y_m)) = 0, \text{ for all } y \in Y. \tag{2.33}$$

The vector space $V = \mathbb{F}_2^{2m}$ is therefore expressed as a direct sum of two totally singular subspaces of maximal dimension (since m is the Witt index of Q).

In Lemma 2.1.11 we have shown that the number of singular vectors of the form $Q = Q^+$ on a vector space $V = \mathbb{F}_2^m$ is equal to $2^{2m-1} + 2^{m-1}$. If we consider only nonzero singular vectors in V then the number is equal to

$$2^{2m-1} + 2^{m-1} - 1 = (2^m - 1)(2^{m-1} + 1). \tag{2.34}$$

Since each totally singular space of V of maximal dimension (i.e. dimension m) consists of $2^m - 1$ nonzero singular vectors, it suggests that in V there exists a family of totally singular spaces of dimension m that partition the set of all nonzero singular vectors, i.e. spread.

Definition 2.2.1. Let V be a vector space of dimension $2m$ and Q be a quadratic form on V of type 1. The family Σ of $2^{m-1} + 1$ totally singular subspaces of dimension m that divides the set of all nonzero singular vectors is called an *orthogonal spread*.

Now we would like to describe totally singular subspaces of a vector space $\mathbb{F}_2^{2m}$ of maximal dimension disjoint with a subspace Y.

First we formulate an auxiliary lemma that describes isometries of V fixing the subspace Y (see Lemma 3.1 in [20]).

Lemma 2.2.2. *The isometries of $V = X \oplus Y$ that fix every vector of Y are just those whose matrices are*

$$\begin{pmatrix} I & M \\ 0 & I \end{pmatrix}, \tag{2.35}$$

for some skew-symmetric $m \times m$ matrix M.

Moreover, these isometries form a group isomorphic to the additive group of all binary skew-symmetric $m \times m$ matrices.

Proof. Every linear transformation σ on the vector space V is in the form

$$S = \begin{pmatrix} L & M \\ 0 & N \end{pmatrix}, \tag{2.36}$$

for some $m \times m$ matrices L, M and N.

Since σ fix every vector y from Y, equation $yS = y$ holds for all $y \in Y$ and N is the identity matrix.

Since σ is an isometry, the equation $Q(uS) = Q(u)$ must be satisfied for all vectors $u = (v_1, \ldots, v_m, w_1, \ldots, w_m) \in V$, where $v = (v_1, \ldots, v_m) \in X$ and $w = (w_1, \ldots, w_m) \in Y$, i.e. equation $vL \cdot (vM + w) = v \cdot w$ must hold. From the expression of equation using particular coordinates it follows that L must be the identity matrix I and M is skew-symmetric matrix.

The second part of the lemma follows from the fact that

$$\begin{pmatrix} I & M \\ 0 & I \end{pmatrix} \begin{pmatrix} I & N \\ 0 & I \end{pmatrix} = \begin{pmatrix} I & M+N \\ 0 & I \end{pmatrix}. \tag{2.37}$$

□

The previous lemma will be now used for an identification of totally singular subspaces of V with maximal dimension such that their intersection with the space Y is equal to 0.

Theorem 2.2.3. *There is a one-to-one correspondence between totally singular subspaces Z of V of dimension m such that $Y \cap Z = 0$ and subspaces of V in the form*

$$X \begin{pmatrix} I & M \\ 0 & I \end{pmatrix}, \tag{2.38}$$

where M is a skew-symmetric $m \times m$ matrix.

Proof. Let Z be a totally singular subspace of V of dimension m such that $Y \cap Z = 0$. Then each vector $z \in Z$ can be written in the form $z = (x, xM)$ for $x \in X$ and the unique $m \times m$ matrix M, i.e.

$$Z = \{(x, xM); x \in X\}. \tag{2.39}$$

Since Z is totally singular it must hold

$$Q(z) = Q((x, xM)) = x \cdot xM = 0, \text{ for all } z \in Z, \tag{2.40}$$

which is exactly the condition for M to be skew-symmetric.

Otherwise, let Z be a subspace of V in the form $X \begin{pmatrix} I & M \\ 0 & I \end{pmatrix}$ for skew-symmetric $m \times m$ matrix M. Then each vector $z \in Z$ can be expressed in the form $z = (x, xM)$ for $x \in X$. This implies that dimension of Z is equal to m and $Y \cap Z = 0$. Moreover, due to a skew-symmetricity of M, it holds

$$Q(z) = Q((x, xM)) = x \cdot xM = 0 \tag{2.41}$$

for all $z = (x, xM) \in Z$ and the space Z is totally singular. □

The last auxiliary observation will connect dimension of intersection of two totally singular subspaces in the form (2.38) with the rank of their matrix representants. The lemma can be found in [6] (Lemma 2.12).

Lemma 2.2.4. *Let M_1 and M_2 be binary skew-symmetric $m \times m$ matrices for which the corresponding totally singular m-spaces $W_1 = X \begin{pmatrix} I & M_1 \\ 0 & I \end{pmatrix}$ and $W_2 = X \begin{pmatrix} I & M_2 \\ 0 & I \end{pmatrix}$ satisfy $Y \cap W_1 = Y \cap W_2 = 0$. Then $W_1 \cap W_2 = 0$ if and only if $M_1 - M_2$ is regular (i.e. $\operatorname{rank}(M_1 - M_2) = m$).*

Proof. A vector $v \in V$ is in the intersection of those two subspaces if it can be written in the form $v = (x_1, x_1M_1)$ and $v = (x_2, x_2M_2)$ for some vectors $x_1, x_2 \in X$. This means that $(x_1, x_1M_1) = (x_2, x_2M_2)$ and thus $x_1 = x_2$.

The dimension of intersection of two totally singular m-subspaces is then equal to dimension of solution of linear equations system $xM_1 = xM_2$ (i.e. system of linear equations $x(M_1 - M_2) = 0$). This dimension is equal to $m - \operatorname{rank}(M_1 - M_2)$ and we have shown that

$$\dim \left(X \begin{pmatrix} I & M_1 \\ 0 & I \end{pmatrix} \cap X \begin{pmatrix} I & M_2 \\ 0 & I \end{pmatrix} \right) = m - \operatorname{rank}(M_1 - M_2). \tag{2.42}$$

□

Now we have all information necessary for construction of Kerdock set $\mathcal{K}$ (see Definition 1.1.2) of size 2^{m-1} (and consequently Kerdock code $\mathcal{K}(m)$ of length 2^m) from an orthogonal spread Σ in vector space $\mathbb{F}_2^{2m}$.

Theorem 2.2.5. *Let $V = \mathbb{F}_2^{2m}$ be a vector space. Let X, Y be m-subspaces of V such that $V = X \oplus Y$.*

If $\mathcal{K}$ is a Kerdock set of 2^{m-1} skew-symmetric $m \times m$ matrices, then

$$\Sigma = \{Y\} \cup \left\{ X \begin{pmatrix} I & M \\ 0 & I \end{pmatrix} ; M \in \mathcal{K} \right\} \tag{2.43}$$

is an orthogonal spread of V.

Conversely, if Σ is an orthogonal spread of V that contains subspaces X and Y, then the set of $m \times m$ skew-symmetric matrices that are associated with subspaces $\Sigma - \{Y\}$ is a Kerdock set.

Proof. From Theorem 2.2.3 and properties of the space Y it follows that the set Σ consists of $2^{m-1}+1$ totally singular subspaces. For each subspace Z from $\Sigma - \{Y\}$ it holds that its intersection with the space Y is equal to 0 (i.e. $Z \cap Y = 0$).

Now it remains to show that intersection of each two elements of $\Sigma - \{Y\}$ is equal to 0. But this follows from Lemma 2.2.4, because difference between each two matrices M_1 and M_2 from $\mathcal{K}$ is regular (i.e. it has rank m).

We have shown that the set Σ is an orthogonal spread.

Otherwise, let Σ be orthogonal spread that contains X and Y and let $\mathcal{K}$ be the set of skew-symmetric matrices associated with subspaces from $\Sigma - \{Y\}$. Since X is in Σ, the set $\mathcal{K}$ contains zero matrix.

The intersection of each two spaces Z_1 and Z_2 from $\Sigma - \{Y\}$ with associated matrices M_1 and M_2 is equal to 0. Now we can use Lemma 2.2.4 which implies that $\operatorname{rank}(M_1 - M_2) = m$ and thus difference between each two matrices from $\mathcal{K}$ is regular matrix.

We have proved that $\mathcal{K}$ is a Kerdock set. □

The notation of Kerdock set $\mathcal{K}$ in the previous theorem is very ambiguous. If we consider an orthogonal spread Σ, the Kerdock set depends on the choice of a pair of totally singular spaces from Σ that will play the role of X and Y and on the choice of symplectic basis. But up to equivalence of codes, the Kerdock code $\mathcal{K}(m)$ depends only on Σ and on a subspace $Y \in \Sigma$. For more information see Chapter 3 in [6].

3. Kerdock designs

Combinatorial design theory forms an important branch of combinatorial mathematics. Its main concern is the existence and a construction of finite sets systems with various specific properties.

Theory of error-correcting codes gives us a rich source of combinatorial designs with various parameters. Let C be a code. If we form a matrix whose rows are codewords from C of the same Hamming weight, we can possibly get an incidence matrix of a design. Therefore, it may be feasible to view coordinates in codewords as elements (points) of a supporting set and codewords of the same weight then represents blocks of design.

According to Definitions 1.1.2 and 1.2.14, the Kerdock code can be seen as a nonlinear binary code of length 2^m or as a quaternary linear code of length 2^{m-1} for even m. This gives us a chance to construct combinatorial designs on a set of 2^k elements, $k \geq 3$, whose blocks corresponds to codewords of the Kerdock code with the same weight. However, the existence of such designs isn't obvious neither for the binary case nor for the quaternary case.

The chapter is divided into three sections. The first one compiles basic facts about combinatorial design theory and its connection with error-correcting codes. The main source for the section was Chapter VII.1.

In the second part a weight distribution of the binary Kerdock codes $\mathcal{K}(m)$, $m \geq 4$ even, is calculated and then it is shown that codewords of each weight form a combinatorial design. Connections between codes and designs are in more detail described in Chapter 6 in [26].

The third part determines weight enumerators of the quaternary Kerdock codes $\mathcal{K}_4(m-1)$ and describes a construction of designs derived from these codes. For more information on designs based on $\mathbb{Z}_4$-codes see [17] or [36].

3.1 Combinatorial designs from codes

Definition 3.1.1. A $t-(v,k,\lambda)$ *design* D is a set of v points with a collection of k-subsets called *blocks*, such that any subset of t points is contained in precisely λ blocks.

Parameters v, k and λ are often omitted from the previous notation and a $t-(v,k,\lambda)$ design is referred to as a *t-design*.

According to Definition 3.1.1, any $t-(v,k,\lambda)$ design D can be seen as a pair $(V,\mathcal{B})$, where V is a set of v elements (points) and $B \subset \mathcal{P}(V)$ is a set of k-subsets (blocks) of V with mentioned properties.

If we consider a $t-(v,k,\lambda)$ design $D = (V,\mathcal{B})$ based on a binary code C of length n, then points from the set V are identified with coordinates in the codewords from C and a parameter v is equal to n. Each block $B \in \mathcal{B}$ then corresponds to a set of nonzero coordinates of a codeword $\mathbf{c} \in C$ with the Hamming

weight k. Moreover, for each set of t coordinates $i_1, \ldots, i_t$ there exist exactly λ codewords $\mathbf{c_1} = (c_{11}, \ldots, c_{1n}), \ldots, \mathbf{c}_\lambda = (c_{\lambda 1}, \ldots, c_{\lambda n}) \in C$ of Hamming weight k with nonzero elements in given coordinates (i.e. $c_{ji_l} \neq 0$ for each $j \in \{1, \ldots, \lambda\}$ and $l \in \{1, \ldots, t\}$).

This construction can be formalized using the following definition (see [10], part VII.1.2).

Definition 3.1.2. Let $V = \mathbb{F}_q^n$ be a vector space of dimension n over the field $\mathbb{F}_q$. The *support* $\mathrm{supp}(\mathbf{x})$ of a vector $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in V$ is a set of indices of its nonzero coordinates, i.e.

$$\mathrm{supp}(\mathbf{x}) = \{i;\ x_i \neq 0, 1 \leq i \leq n\}. \tag{3.1}$$

Let C be a binary code of length n. Let K be a set of all codewords from C of the Hamming weight k, $1 \leq k \leq n$. If we take the n coordinate indices as the points and the supports of vectors from K as the blocks, it may be possible to construct t-design with $v = n$ for an integer t. Such design is called *support design*.

We have described the connection between binary codes and designs. But for quaternary codes, a situation is slightly different since the notion of "weight" of codeword is ambiguous.

Let $\mathbf{c} = (c_1, \ldots, c_n)$ be a codeword from a $\mathbb{Z}_4$-linear code $\mathcal{C}$ of length n. For ciphers $i = 0, 1, 2, 3$ denote by n_i a number of occurences of i in the codeword $\mathbf{c}$, i.e.

$$n_i(\mathbf{c}) = |\{j;\ c_j = i,\ 1 \leq j \leq n\}|, \text{ for } i = 0, 1, 2, 3. \tag{3.2}$$

We can associate several weight enumerators with the code $\mathcal{C}$. The *complete weight enumerator* (CWE) of $\mathcal{C}$ is a homogeneous polynomial of degree n in four indeterminates

$$CWE_{\mathcal{C}}(w, x, y, z) = \sum_{\mathbf{c} \in \mathcal{C}} w^{n_0(\mathbf{c})} x^{n_1(\mathbf{c})} y^{n_2(\mathbf{c})} z^{n_3(\mathbf{c})}. \tag{3.3}$$

In many technical applications of quaternary codes it isn't necessary to distinguish between ciphers 1 and -1 ($-1 = 3$ in $\mathbb{Z}_4$). For this purpose an appropriate weight enumerator called *symmetrized* (SWE) is defined as

$$SWE_{\mathcal{C}}(w, x, y) = \sum_{\mathbf{c} \in \mathcal{C}} w^{n_0(\mathbf{c})} x^{n_1(\mathbf{c}) + n_3(\mathbf{c})} y^{n_2(\mathbf{x})}. \tag{3.4}$$

The Hamming weight enumerator (HWE) of the code $\mathcal{C}$ is a polynomial defined by

$$HWE_{\mathcal{C}}(w, x) = \sum_{\mathbf{c} \in \mathcal{C}} w^{n_0(\mathbf{c})} x^{n_1(\mathbf{c}) + n_2(\mathbf{c}) + n_3(\mathbf{c})}. \tag{3.5}$$

There are two basic ways to proceed with research of designs based on the quaternary codes. In the first one, we choose a weight enumerator (complete, symmetrized or Hamming) of given quaternary code $\mathcal{C}$ and we check if supports of codewords from $\mathcal{C}$ with constant weight (complete, symmetrized or Hamming) form a t-design.

The second approach uses a generalization of t-designs into colored t-designs. The notion of colored t-designs was introduced in article [5]. It adds a set of colors that are assigned to each point in each block into the definition of design. An ordinary design can be viewed as 2-colored with colors "incident" and "not incident" since we distingiush if given point is incident with given block. In colored designs based on quaternary codes, colors are identified with ciphers 0,1,2 and 3 in given coordinates of a codeword.

In this chapter we focus only on the former approach to designs from quaternary codes.

3.2 Designs from binary Kerdock codes

The first step in the construction of combinatorial design from binary code C of length n lies in a calculation of its Hamming weight distribution (i.e. in the calculation of list $\{A_i\}_{i=0}^{n}$, where A_i is the number of codewords of weight i from the code C). The second step then involves a proof of existence of support design made by codewords with given weight k, $1 \leq k \leq n$ and a determination of its parameters.

This section is divided into two parts. In the first part, the Hamming weight distribution of binary Kerdock code $\mathcal{K}(m)$, $m \geq 4$ even, is calculated. For more information see [24].

The main goal of the second part is to show that codewords of the binary Kerdock code $\mathcal{K}(m)$ of each weight form a combinatorial design.

3.2.1 Hamming weight distribution of binary Kerdock code

The binary Kerdock code $\mathcal{K}(m)$ of length 2^m, $m \geq 4$ even, is usually defined as a union of certain 2^{m-1} cosets of the first order Reed-Muller code $\mathcal{RM}(1, m)$ in the second order Reed-Muller code $\mathcal{RM}(2, m)$ (see Definition 1.1.2). These cosets are determined by skew-symmetric $m \times m$ matrices from the Kerdock set $\mathcal{K}$. Since the zero matrix is always in $\mathcal{K}$, an inclusion $\mathcal{RM}(1, m) \subseteq \mathcal{K}(m)$ holds. The cosets that form the binary Kerdock code $\mathcal{K}(m)$ can be therefore divided into two groups that should be investigated independently

(i) one coset identified with the first order Reed-Muller code $\mathcal{RM}(1, m)$;

(ii) $2^{m-1} - 1$ cosets corresponding to regular skew-symmetric matrices from the Kerdock set $\mathcal{K}$.

First, we calculate a weight distribution of the first order Reed-Muller code $\mathcal{RM}(1, m)$. According to Definition 1.1.1 the codewords of $\mathcal{RM}(1, m)$ correspond to the set of Boolean functions of arity m and degree ≤ 1 (i.e. each codeword $\mathbf{c} \in \mathcal{RM}(1, m)$ is equal to evaluation vector v_f of an affine Boolean function).

Let f be an affine Boolean function of arity m, i.e.

$$f(\mathbf{x}) = \sum_{i=1}^{m} a_i x_i + a_0, \tag{3.6}$$

where $a_0, a_1, \ldots, a_m \in \mathbb{F}_2$. Let $\mathbf{c} \in RM(1,m)$ be the codeword corresponding to the function f (i.e. $\mathbf{c} = v_f$).

Let a_i be equal to zero for all $1 \leq i \leq m$. If a_0 is zero, then $f(\mathbf{x}) = 0$ for all $\mathbf{x} \in \mathbb{F}_2^m$ and the codeword $\mathbf{c}$ is the zero vector $\mathbf{0}$ of length 2^m. Conversely, if a_0 is 1, then $f(\mathbf{x}) = 1$ for all $\mathbf{x} \in \mathbb{F}_2^m$ and the codeword $\mathbf{c}$ is equal to the all-one vector $\mathbf{1}$ of length 2^m.

Now let a_i be equal to 1 for some $1 \leq i \leq m$. Let x_j be selected arbitrarily for all $1 \leq j \leq m$, $j \neq i$. Then $f(\mathbf{x}) = a_0 + \sum_{i \neq j} a_j x_j + x_i$ and we can choose the value of x_i such that $f(\mathbf{x}) = 0$. The opposite choice of x_i gives us $f(\mathbf{x}) = 1$. This means that for all codewords $\mathbf{c} \in \mathcal{RM}(1,m)$ except the zero and the all-one codeword, a Hamming weight of $\mathbf{c}$ is equal to 2^{m-1} (each of 2^{m-1} choices of values for $m-1$ variables x_j $(i \neq j)$ cause that one coordinate in the codeword $\mathbf{c}$ is equal to 1 and one coordinate in $\mathbf{c}$ is equal to 0).

The weight distribution of the first order Reed-Muller code $\mathcal{RM}(1,m)$ (and thus the corresponding coset in the Kerdock code $\mathcal{K}(m)$) is then shown in Table 3.1.

i	A_i
0	1
2^{m-1}	$2^{m+1} - 2$
2^m	1

Table 3.1: Weight distribution of the first order Reed-Muller code $\mathcal{RM}(1,m)$

A weight distribution of a coset of $\mathcal{RM}(1,m)$ corresponding to a regular skew-symmetric matrix will be now determined.

Let B be a nonzero $m \times m$ skew-symmetric matrix from the Kerdock set $\mathcal{K}$ and let C_B be a coset of $\mathcal{RM}(1,m)$ assigned to the matrix B. Then B is a matrix of a symplectic form β on a vector space $V = \mathbb{F}_2^m$ that establishes a non-singular quadratic form Q.

Each codeword from C_B can be therefore expressed as an evaluation vector of a quadratic Boolean function f in the form

$$f(\mathbf{x}) = Q(\mathbf{x}) + \sum_{k=1}^{m} a_k x_k + a_0, \tag{3.7}$$

for all $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{F}_2^m$, where $a_k \in \mathbb{F}_2^m$ for $0 \leq k \leq m$.

In Section 2.1 we have shown that each non-singular quadratic form on vector space $\mathbb{F}_2^m$ is equivalent to one of quadratic forms

$$Q^+(\mathbf{x}) = x_1 x_2 + x_3 x_4 + \ldots + x_{m-1} x_m \tag{3.8}$$

or

$$Q^-(\mathbf{x}) = x_1 x_2 + x_3 x_4 + \ldots + x_{m-1}^2 + x_{m-1} x_m + x_m^2 \tag{3.9}$$

for all $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{F}_2^m$. Moreover, from Lemma 2.1.11 we know numbers of singular vectors of forms Q^+ and Q^-.

Assume that the quadratic form Q is equivalent to the form Q^+. The function $f(\mathbf{x})$ from (3.7) is therefore equivalent to a quadratic Boolean function

$$Q^+(\mathbf{x}) + a_0, \tag{3.10}$$

since the sum of quadratic form and linear function is equivalent with the quadratic form itself (see equation (2.9)).

Since number of singular vectors of the form Q^+ is equal to $2^{m-1} + 2^{\frac{m}{2}-1}$, there is exactly $2^{m-1} - 2^{\frac{m}{2}-1}$ vectors $\mathbf{x} = (x_1, \ldots, x_m)$ such that $Q^+(\mathbf{x}) = 1$ and an evaluation vector v_f has one of weights $2^{m-1} \pm 2^{\frac{m}{2}-1}$ depending on value of a_0.

If the quadratic form Q is equivalent to Q^-, situation is very similar since the forms Q^+ and Q^- have the opposite number of singular vectors.

The whole situation is summarized in Table 3.2. [1].

Quadratic form	$\mathbf{a_0}$	**Weight of vector**	**Number of functions**
Q^+	0	$2^{m-1} - 2^{\frac{m}{2}-1}$	2^m
	1	$2^{m-1} + 2^{\frac{m}{2}-1}$	2^m
Q^-	0	$2^{m-1} + 2^{\frac{m}{2}-1}$	2^m
	1	$2^{m-1} - 2^{\frac{m}{2}-1}$	2^m

Table 3.2: Weights and numbers of vectors from the coset C_B

The previous table shows that each coset of the first order Reed-Muller code that corresponds to a regular skew-symmetric matrix from the Kerdock set $\mathcal{K}$ has the weight distribution as in Table 3.3.

i	A_i
$2^{m-1} - 2^{m/2-1}$	2^m
$2^{m-1} + 2^{m/2-1}$	2^m

Table 3.3: Weight distribution of coset of $\mathcal{RM}(1, m)$

Since the binary Kerdock code $\mathcal{K}(m)$ contains one coset of the type (i) and $2^{m-1} - 1$ cosets of the type (ii) the weight distribution of $\mathcal{K}(m)$ is summarized in Table 3.4.

[1] An interpretation of a row in Table 3.2 in terms of column names is following: "If the quadratic form Q is equivalent to quadratic form (Quadratic form), then there exist (Number of functions) codewords from the coset C_B of weight (Weight of vector) such that absolute term corresponding Boolean function is equal to (a_0)."

i	A_i
0	1
$2^{m-1} - 2^{m/2-1}$	$2^m(2^{m-1} - 1)$
2^{m-1}	$2^{m+1} - 2$
$2^{m-1} + 2^{m/2-1}$	$2^m(2^{m-1} - 1)$
2^m	1

Table 3.4: Weight distribution of the binary Kerdock code $\mathcal{K}(m)$

3.2.2 Existence of designs from binary Kerdock codes

Each binary (n, k, d) code C can be described by four fundamental paramaters — minimum distance, number of different nonzero distances between two codewords, dual distance and external distance. In the following text these parameteres will be defined and then used to specify sufficient conditions for the existence of design based on the code C. For more information see Section 6.2 in [26].

Definition 3.2.1. Let C be a binary (n, k, d) code. The *(Hamming) distance distribution* of the code C is a list $\{B_i\}_{i=0}^n$, where

$$B_i = \frac{1}{k} \sum_{\mathbf{c} \in C} |\{\mathbf{c}' \in C; d(\mathbf{c}', \mathbf{c}) = i\}|. \tag{3.11}$$

If (n, k, d) code C is a distance invariant code that contains the zero codeword, a distance distribution $\{B_i\}_{i=0}^n$ of C is equal to the Hamming weight distribution $\{A_i\}_{i=0}^n$, where A_i is the number of codewords $\mathbf{c} \in C$ of weight i.

Let $\tau_0, \tau_1, \ldots, \tau_s$ be the indices i for which $B_i \neq 0$, where

$$0 \leq \tau_0 < \tau_1 < \ldots < \tau_s \leq n. \tag{3.12}$$

Since the distance of each codeword from itself is equal to zero (i.e. $d(\mathbf{c}, \mathbf{c}) = 0$ for all $\mathbf{c} \in C$), the coefficient B_0 is equal to 1 and $\tau_0 = 0$.

A *minimum distance* of a code C is defined as the minimal Hamming distance between two different codewords $\mathbf{c_1}$ and $\mathbf{c_2}$ from code C (i.e. $d = \min d(\mathbf{c_1}, \mathbf{c_2})$, where $\mathbf{c_1}, \mathbf{c_2} \in C$ and $\mathbf{c_1} \neq \mathbf{c_2}$). From Definition 3.2.1 it follows that the minimum distance is equal to the index τ_1.

For a distance invariant code that contains the zero codeword, values of minimum weight and minimum distance are the same. Since we focus only on these codes, a letter d will denote both minimum weight and minimum distance of given code.

As was shown in Section 1.3, the binary Kerdock code $\mathcal{K}(m)$ is a distance invariant code. Since the zero codeword is in $\mathcal{K}(m)$, a distance distribution of the Kerdock code is equal to its Hamming weight distribution (see Table 3.4), i.e. the distance distribution of the Kerdock code $\mathcal{K}(m)$ is a list of values B_i, $0 \leq i \leq 2^m$,

where

$$\begin{aligned}
&B_0 = 1,\\
&B_{2^{m-1}-2^{(m-2)/2}} = 2^m(2^{m-1}-1),\\
&B_{2^{m-1}} = 2^{m+1}-2,\\
&B_{2^{m-1}+2^{(m-2)/2}} = 2^m(2^{m-1}-1),\\
&B_{2^m} = 1,\\
&B_j = 0,\ 0 \le j \le 2^m,\ j \notin \{0, 2^{m-1} \pm 2^{(m-2)/2}, 2^{m-1}, 2^m\}.
\end{aligned} \tag{3.13}$$

A minimum distance d of the binary Kerdock code $\mathcal{K}(m)$ is then equal to $2^{m-1} - 2^{(m-2)/2}$.

The second parameter of a code C related to its distance distribution is a number s which represents the number of distinct nonzero distances between any two codewords from C.

The set of equations (3.13) implies, that parameter s is for the Kerdock code $\mathcal{K}(m)$ equal to 4.

Now we determine the remaining two parameters associated with a (n, k, d) code C. Both of them relates to the MacWilliams transform of distance distribution $\{B_i\}_{i=0}^n$ of the code C. More detailed information about this transform can be found e.g. in [26].

Let $\{B'_k\}_{k=0}^n$ be the MacWilliams transform of distance distribution $\{B_i\}_{i=0}^n$ of the code C given by

$$B'_k = \frac{1}{|C|} \sum_{i=0}^{n} B_i K_k(i),\ k = 0, 1, \ldots, n, \tag{3.14}$$

where $K_k(x) \in \mathbb{Z}[x]$ are the *Krawtchouk polynomials* defined as

$$K_k(x; n) = K_k(x) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j},\ k = 0, 1, \ldots, n. \tag{3.15}$$

Let $\sigma_0, \sigma_1, \ldots, \sigma_{s'}$ be the indices k for which $B'_k \neq 0$, where

$$0 \le \sigma_0 < \sigma_1 < \ldots < \sigma_{s'} \le n. \tag{3.16}$$

Since $K_0(x)$ is equal to 1 for any x and B_0 is equal to 1 for any code C, the coefficient B'_0 is always equal to 1 and $\sigma_0 = 0$.

The index σ_1 is called a *dual distance* of the code C and is denoted by d'. If C is the linear code then its dual distance d' is equal to the minimal distance of its dual code $C^\perp$.

The number s' of nonzero indices k such that $B'_k \neq 0$ is called an *external distance* of the code C. This parameter was defined for completeness of code description and won't be used for design construction.

In Section 1.3, we have introduced the Preparata codes whose weight distribution is the MacWilliams transform of weight distribution of the binary Kerdock

codes $\mathcal{K}(m)$. Since both of these codes are distance invariant and contains the zero codeword, their distance distributions are connected via MacWilliams identity (3.14).

A dual distance d' of the Kerdock code $\mathcal{K}(m)$ is therefore equal to the minimum distance of the Preparata code of the same length, which is 6. The external distance s' of the Kerdock code $\mathcal{K}(m)$ corresponds to a number of nonzero weights in the Preparata code, which is equal to 4 (see Table 1.3).

Now we have all information required for a formulation of theorem that gives us a sufficient condition for the existence of combinatorial designs based on the binary code C. Since neither the special formulation of the theorem for the Kerdock codes nor its proof would be much simpler, we formulate it in a general form. Then we apply the result on the binary Kerdock codes $\mathcal{K}(m)$. The theorem can be found in [26] (Chapter 6, Theorem 9).

Theorem 3.2.2. *Let C be a binary distance invariant (n, k, d) code (not necessarily linear) with dual distance d'. Let $\{A_i\}_{i=0}^n = \{B_i\}_{i=0}^n$ be its weight (respectively distance) distribution and let $0, \tau_1, \ldots, \tau_s$ denote the indices i for which $A_i = B_i \neq 0$, where*

$$0 < \tau_1 < \ldots < \tau_s \leq n. \tag{3.17}$$

Let $\bar{s}$ be defined as follows

$$\bar{s} = \begin{cases} s & \text{if } A_n = 0, \\ s - 1 & \text{if } A_n = 1. \end{cases} \tag{3.18}$$

Let $S(x)$ be a polynomial defined as

$$S(x) = \prod_{j=1}^{\bar{s}} (\tau_j - x). \tag{3.19}$$

If $\bar{s} < d'$ then the codewords of weight τ_i in C form a $t - (n, \tau_i, \lambda_{\tau_i})$ design, where $t = d' - \bar{s}$ and λ_{τ_i} is given by

$$\lambda_{\tau_i} \cdot \prod_{\substack{j=1 \\ j \neq i}}^{\bar{s}} (\tau_j - \tau_i) = \frac{A_n S(n)}{n - \tau_i} + \frac{k}{2^n} \sum_{r=t}^{n} \binom{n-t}{r-t} \frac{S(r)}{\tau_i - r}. \tag{3.20}$$

Proof. We say that a vector $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ covers a vector $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{F}_2^n$ if an implication $(u_i = 1 \Rightarrow v_i = 1)$ holds for all $i \in \{1, \ldots, n\}$.

Let $\mathbf{u} \in \mathbb{F}_2^n$ be a fixed vector of weight $t = d' - \bar{s}$. For $\tau_i \geq t$, let $\lambda_{\tau_i}(\mathbf{u})$ denotes the number of codewords from C of weight τ_i that cover $\mathbf{u}$.

First, we prove that the numbers $\lambda_{\tau_i}(\mathbf{u})$ satisfy a set of $d' - t$ equations

$$\sum_{i=1}^{s} \binom{\tau_i - t}{j} \lambda_{\tau_i}(u) = \frac{k}{2^{t+j}} \binom{n-t}{j}, \tag{3.21}$$

where $0 \leq j \leq d' - 1 - t$.

For each equation, we show that both sides express a number of vectors of weight $t+j$ which cover $\mathbf{u}$ and are covered by a codeword from C.

Since we count the number of vectors of weight $t+j$ and t ones in each such vector are determined by fixed coordinates in the vector $\mathbf{u}$, we have to choose exactly j ones from each codeword $\mathbf{c} \in C$. The choice can be provided in $\binom{\tau_i - t}{j}$ ways. If we consider all possible values of τ_i we get the sum on the left side of equation (3.21).

The right side of equation (3.21) follows from the fact that if we fix the set of $r \leq d' - 1$ coordinates then each r-tuple appears exactly $k/2^r$ times in a set of codewords from C (see e.g. Theorem 5.8 in [26]).

Let take $r = t + j$ and fix r coordinates in the codewords from C. A number of codewords of C that has ones at all r coordinates is equal to $k/2^r = k/2^{t+j}$. Since the vector $\mathbf{u}$ has weight t, we can choose only j of r coordinates (remaining t coordinates correspond to ones in the vector $\mathbf{u}$). The choice can be done in $\binom{n-t}{j}$ ways and we get the right side of equation (3.21).

The all-one vector of length n covers every vector from $\mathbb{F}_2^n$. Thus we can subtract its appearence from the both sides of equation (3.21) for all $0 \leq j \leq d' - 1 - t$ and rewrite them to the form

$$\sum_{i=1}^{\bar{s}} \binom{\tau_i - t}{j} \lambda_{\tau_i}(u) = \left(\frac{k}{2^{t+j}} - A_n \right) \binom{n-t}{j}. \tag{3.22}$$

Now we have a set of $\bar{s}$ linear equations with $\bar{s}$ unknowns $\lambda_{\tau_i}(u)$. From construction of equations (3.22) it follows that the value of $\lambda_{\tau_i}(u)$ for all $0 \leq i \leq \bar{s}$ doesn't depend on a choice of vector $\mathbf{u}$ and we can denote it by λ_{τ_i} for all vectors $u \in \mathbb{F}_2^n$ of weight t.

Thus we have shown that the codewords from C of each weight τ_i forms $t - (n, \tau_i, \lambda_{\tau_i})$ design because if we choose t coordinates in vectors from $\mathbb{F}_2^n$, then there exist exactly λ_{τ_i} codewords from C of weight τ_i that have ones at prescribed t positions.

Now it remains to deduce formulas for the parameters λ_{τ_i}, $1 \leq \tau_i \leq \bar{s}$, as a solution of set of equations (3.22).

This set of equations can be expressed as

$$A\mathbf{x} = \mathbf{b}, \tag{3.23}$$

where $\mathbf{x}$ is a column vector of length $\bar{s}$ of unknowns λ_{τ_i}, A is an $\bar{s} \times \bar{s}$ matrix equals to

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \tau_1 - t & \tau_2 - t & \dots & \tau_{\bar{s}} \\ \binom{\tau_1 - t}{2} & \binom{\tau_2 - t}{2} & \dots & \binom{\tau_{\bar{s}} - t}{2} \\ \vdots & & \ddots & \vdots \\ \binom{\tau_1 - t}{\bar{s}-1} & \binom{\tau_2 - t}{\bar{s}-1} & \dots & \binom{\tau_{\bar{s}} - t}{\bar{s}-1} \end{pmatrix}, \tag{3.24}$$

and $\mathbf{b}$ is a column vector of the right sides

$$\mathbf{b}^T = \left(\left(\frac{k}{2^t} - A_n \right), \ldots, \left(\frac{k}{2^{t+\bar{s}-1}} - A_n \right) \binom{n-t}{\bar{s}-1} \right). \tag{3.25}$$

The vector $\mathbf{x}$ is then equal to the product $A^{-1}\mathbf{b}$ (since $\mathbf{x} = AA^{-1}\mathbf{x} = A^{-1}\mathbf{b}$) and therefore we need to calculate an inverse matrix A^{-1}.

Define rational polynomials f_{τ_i} by

$$f_{\tau_i}(x) = \prod_{\substack{j=1 \\ j \neq i}}^{\bar{s}} \frac{\tau_j - t - x}{\tau_j - \tau_i}. \tag{3.26}$$

Because the degree of polynomial f_{τ_i} is for all $i \in \{1, \ldots, \bar{s}\}$ at most $\bar{s} - 1$ there exist rational numbers f_{ij} ($1 \leq i \leq \bar{s}$, $0 \leq j \leq \bar{s} - 1$), such that

$$f_{\tau_i}(x) = \sum_{j=0}^{\bar{s}-1} f_{ij} \binom{x}{j}. \tag{3.27}$$

Let F be a matrix $\{f_{ij}\}$, $1 \leq i \leq \bar{s}$, $0 \leq j \leq \bar{s} - 1$. The inner product of the i-th row in the matrix F and the k-th column in the matrix A is expressed by

$$\sum_{j=0}^{\bar{s}-1} f_{ij} \binom{\tau_k - t}{j} = f_{\tau_i}(\tau_k - t) = \prod_{\substack{j=1 \\ j \neq i}}^{\bar{s}} \frac{\tau_j - \tau_k}{\tau_j - \tau_i} = \delta_{ik}, \tag{3.28}$$

where δ_{ik} is the Kronecker delta, i.e. it is equal to 1 if $i = k$ and it's equal to 0 otherwise. The matrix product FA gives the unitary matrix of size $\bar{s}$ and thus $A^{-1} = F$.

Now we can calculate the unknowns λ_{τ_i} for all $1 \leq i \leq \bar{s}$ using the inverse transform matrix A^{-1} by

$$\lambda_{\tau_i} = \sum_{j=0}^{\bar{s}-1} f_{ij} \left(\frac{k}{2^{t+j}} - A_n \right) \binom{n-t}{j}. \tag{3.29}$$

From the binomial theorem we derive the following formula that help us to express equation (3.29) in a suitable form

$$2^{n-t-j} \binom{n-t}{j} = \sum_{k=0}^{n-t-j} \binom{n-t-j}{k} \binom{n-t}{j} = \sum_{r=j}^{n-t} \binom{n-t}{r} \binom{r}{j}. \tag{3.30}$$

Now we can modify equation (3.29) as

$$\begin{aligned}
\lambda_{\tau_i} &= \sum_{j=0}^{\bar{s}-1} f_{ij}\left(k\frac{2^{n-t-j}}{2^n} - A_n\right)\binom{n-t}{j} \\
&= \frac{k}{2^n}\sum_{j=0}^{\bar{s}-1} f_{ij}2^{n-t-j}\binom{n-t}{j} - A_n\sum_{j=0}^{\bar{s}-1} f_{ij}\binom{n-t}{j} \\
&= \frac{k}{2^n}\sum_{j=0}^{\bar{s}-1} f_{ij}\sum_{r=j}^{n-t}\binom{n-t}{r}\binom{r}{j} - A_n\sum_{j=0}^{\bar{s}-1} f_{ij}\binom{n-t}{j} \\
&= \frac{k}{2^n}\sum_{r=0}^{n-t}\binom{n-t}{r}\sum_{j=0}^{\bar{s}-1} f_{ij}\binom{r}{j} - A_n\sum_{j=0}^{\bar{s}-1} f_{ij}\binom{n-t}{j} \\
&= \frac{k}{2^n}\sum_{r=0}^{n-t}\binom{n-t}{r}\prod_{\substack{j=1\\ j\neq i}}^{\bar{s}}\frac{\tau_j - t - r}{\tau_j - \tau_i} - A_n\prod_{\substack{j=1\\ j\neq i}}^{\bar{s}}\frac{\tau_j - n}{\tau_j - \tau_i}, \qquad (3.31)
\end{aligned}$$

which is exactly the desired form (3.20). □

Now we apply the previous theorem on the binary Kerdock codes.

The binary Kerdock code $\mathcal{K}(m)$, where $m \geq 4$ is even, is the distance invariant $(2^m, 2^{2m}, 2^{m-1} - 2^{m-2/2})$ code with the parameters $s = 4$ and $d' = 6$. Since $\mathcal{K}(m)$ contains the all-one vector the value of $\bar{s}$ is equal to 3 and the assumptions of Theorem 3.2.2 are satisfied.

From the code $\mathcal{K}(m)$ therefore arose following three combinatorial designs

- $3 - (2^m, 2^{m-1} - 2^{m-2/2}, \lambda_{2^{m-1}-2^{m-2/2}})$,
- $3 - (2^m, 2^{m-1}, \lambda_{2^{m-1}})$,
- $3 - (2^m, 2^{m-1} + 2^{m-2/2}, \lambda_{2^{m-1}+2^{m-2/2}})$,

where $\lambda_{2^{m-1}-2^{m-2/2}}$, $\lambda_{2^{m-1}}$ and $\lambda_{2^{m-1}+2^{m-2/2}}$ are given by expression (3.20).

3.3 Designs from quaternary Kerdock codes

Let $\mathcal{K}_4(m)$, $m \geq 3$ odd, be a quaternary Kerdock code of length 2^m. Similarly as Section 3.2 about designs based on binary Kerdock codes, this section contains two parts. In the first part we investigate a weight distribution and weight enumerators of the quaternary Kerdock code $\mathcal{K}_4(m)$. Its main source is article [36]. The second part is dedicated to a proof of existence of designs that arose from the quaternary Kerdock code.

For more information about t-designs based on quaternary codes see [17].

3.3.1 Weight enumerators of quaternary Kerdock code

Throughout this section we consider the Galois ring $\mathrm{GR}(4^m)$ as an extension ring $\mathbb{Z}_4[\xi]$ for an appropriate $\xi \in \mathrm{GR}(4^m)$ (see Theorem 1.2.12). The Teichmuller set

of $\mathrm{GR}(4^m)$ is denoted by $\mathcal{T}_m$ and $\mathcal{T}_m^* = \mathcal{T}_m - 0$ denotes a set of invertible elements of $\mathcal{T}_m$.

We use the trace description of the quaternary Kerdock codes presented in Theorem 1.2.15. Each codeword $\mathbf{c}_{\lambda,\varepsilon} \in \mathcal{K}_4(m)$, $m \geq 3$ odd, can be therefore expressed in the form

$$(\mathrm{T}(0) + \varepsilon, \mathrm{T}(\lambda) + \varepsilon, \mathrm{T}(\lambda\xi) + \varepsilon, \ldots, \mathrm{T}(\lambda\xi^{2^m-2}) + \varepsilon), \tag{3.32}$$

where $\lambda \in \mathbb{Z}_4[\xi]$, $\varepsilon \in \mathbb{Z}_4$ and T denotes the generalized trace map of the ring $\mathrm{GR}(4^m) = \mathbb{Z}_4[\xi]$. Parameters λ and ε uniquely determine the codeword $\mathbf{c}_{\lambda,\varepsilon} \in \mathcal{K}_4(m)$.

First, we formulate an auxiliary lemma that simplify the following calculations with the generalized trace function T over the Galois ring $\mathrm{GR}(4^m)$.

Lemma 3.3.1. *Let* T *be the generalized trace map* $\mathrm{T} : \mathrm{GR}(4^m) \to \mathbb{Z}_4$. *Denote the set of all invertible elements of* $\mathrm{GR}(4^m)$ *by* R^* *(i.e.* $R^* = \mathrm{GR}(4^m) - 2\mathrm{GR}(4^m)$*).*

(i) If α *runs through the Teichmuller set* $\mathcal{T}_m = \{0, 1, \xi, \ldots, \xi^{2^m-2}\}$, *then* $\mathrm{T}(2\alpha)$ *takes the values 0 and 2 equally often.*

(ii) If λ *runs through the ideal* $2\mathrm{GR}(4^m)$, *then* $\mathrm{T}(\lambda)$ *takes the values 0 and 2 equally often.*

(iii) If λ *runs through* $\mathrm{GR}(4^m)$, *then* $\mathrm{T}(\lambda)$ *takes the values 0, 1, 2 and 3 equally often.*

Proof. Let μ be the modulo-2 reduction map. Since $\mu(\xi)$ is a primitive element of the finite field $\mathbb{F}_{2^m}$, a set $\mu(\mathcal{T}_m)$ is isomorphic to $\mathbb{F}_{2^m}$ (i.e. $\mu(\mathcal{T}_m) \simeq \mathbb{F}_{2^m}$). From Section 1.2 we know that the trace function $\mathrm{Tr} : \mathbb{F}_{2^m} \to \mathbb{F}_2$ is related to the generalized trace function T by the relationship $\mu \circ \mathrm{T} = \mathrm{Tr} \circ \mu$.

Moreover, the trace map Tr is a surjective map such that $\mathrm{Tr}(x)$ is 0 or 1 equally often when x runs through $\mathbb{F}_{2^m}$. Since $2 \cdot 0 \equiv 2 \cdot 2 \equiv 0 \pmod 4$ and $2 \cdot 1 \equiv 2 \cdot 3 \equiv 1 \pmod 4$, part (i) is proved.

Since $2\mathrm{GR}(4^m) = \{2b;\ b \in \mathcal{T}_m\}$, part (ii) is equivalent to part (i).

Part (iii) then follows from the uniqueness of 2-adic representation of each element from $\mathrm{GR}(4^m)$ and the previous notes. □

Now we investigate weight enumerators of the quaternary Kerdock codes $\mathcal{K}_4(m)$. First, codewords from $\mathcal{K}_4(m)$ will be divided into groups with respect to numbers of particular ciphers from $\mathbb{Z}_4$. The following definition gives us a useful notation.

Definition 3.3.2. Let $V = \mathbb{Z}_4^n$, $n \in \mathbb{N}$, be a set of n-tuples over the ring $\mathbb{Z}_4$. A vector $\mathbf{x} \in V$ is defined to be of the *type* $1^{n_1}2^{n_2}3^{n_3}0^{n_0}$ if i occurs n_i times as a component of $\mathbf{x}$ for $i = 0, 1, 2, 3$.

A type distribution of the quaternary Kerdock code is determined in the next theorem (see Lemma 1 in [36]).

Theorem 3.3.3. *Let* $m \geq 3$ *be an odd integer and let* $\mathcal{K}_4(m)$ *be the quaternary Kerdock code of length* $n = 2^m$. *Then every codeword* $\mathbf{c}_{\lambda,\varepsilon} \in \mathcal{K}_4(m)$, *where* $\lambda \in \mathbb{Z}_4[\xi]$ *and* $\varepsilon \in \mathbb{Z}_4$ *is of one of this types*

(i) i^n, *once for each* $i \in \{0,1,2,3\}$;

(ii) $2^{\frac{n}{2}}0^{\frac{n}{2}}$, $2(2^m-1)$ *times;*

(iii) $1^{\frac{n}{2}}3^{\frac{n}{2}}$, $2(2^m-1)$ *times;*

(iv) $1^{n_1}2^{n_2}3^{n_3}0^{n-n_1-n_2-n_3}$, $2^m(2^m-1)$ *times, where* $n_1 = 2^{m-2} \pm 2^{\frac{m-3}{2}}$, $n_2 = 2^{m-2} - 2^{\frac{m-3}{2}}$ *and* $n_3 = 2^{m-2} \mp 2^{\frac{m-3}{2}}$;

(v) $1^{n_1}2^{n_2}3^{n_3}0^{n-n_1-n_2-n_3}$, $2^m(2^m-1)$ *times, where* $n_1 = 2^{m-2} \pm 2^{\frac{m-3}{2}}$, $n_2 = 2^{m-2} + 2^{\frac{m-3}{2}}$ *and* $n_3 = 2^{m-2} \mp 2^{\frac{m-3}{2}}$.

Proof. Let $\mathbf{c}_{\lambda,\varepsilon}$ ($\lambda \in \mathbb{Z}_4[\xi]$, $\varepsilon \in \mathbb{Z}_4$) be a codeword from the quaternary Kerdock code $\mathcal{K}_4(m)$. Let the parameter λ has a 2-adic representation in the form $\lambda = \alpha + 2\beta$, where $\alpha, \beta \in \mathcal{T}_m$. The type distribution of the code $\mathcal{K}_4(m)$ will be calculated with respect to parametres α, β and ε.

First, let $\alpha = \beta = 0$ and let ε be equal to $i \in \mathbb{Z}_4$. Then all values $\mathrm{T}(\lambda\xi^j)$, for $j \in \{\infty, 0, 1, \ldots, 2^m-2\}$, are equal to zero and the codeword $\mathbf{c}_{0,\varepsilon}$ is of the type i^n.

Let $\alpha = 0$, $\beta \in \mathcal{T}_m^*$ and $\varepsilon \in \mathbb{Z}_4$. From Lemma 3.3.1 we know that the value $T(2\beta)$ is equal to 0 or 2 equally often. Therefore, if $\varepsilon \in \{0,2\}$, then the codeword $\mathbf{c}_{2\beta,\varepsilon}$ is of the type $0^{n/2}2^{n/2}$ and if $\varepsilon \in \{1,3\}$, then the codeword $\mathbf{c}_{2\beta,\varepsilon}$ is of the type $1^{n/2}3^{n/2}$.

The option $\alpha \in \mathcal{T}_m^*$, $\beta \in \mathcal{T}_m$ and $\varepsilon \in \mathbb{Z}_4$ remains. Let

$$v^{(\lambda)} = (T(\lambda), T(\lambda\xi), \ldots, T(\lambda\xi^{2^m-2})), \tag{3.33}$$

where $\lambda = \alpha + 2\beta$, be a codeword of the shortened quaternary Kerdock code $\mathcal{K}_4^-(m)$. Let n_i, where $i \in \{0,1,2,3\}$, be the number of coordinates with value i in the codeword $v^{(\lambda)}$.

We claim that there exist parameters δ_1 and δ_2 both equal to 1 or -1 such that

$$\begin{aligned} n_0 &= 2^{m-2} - 1 + \delta_1 2^{(m-3)/2}, \quad n_1 = 2^{m-2} + \delta_2 2^{(m-3)/2}, \\ n_2 &= 2^{m-2} - \delta_1 2^{(m-3)/2}, \quad n_3 = 2^{m-2} - \delta_2 2^{(m-3)/2}. \end{aligned} \tag{3.34}$$

Let S be an exponential sum

$$S = \sum_{x \in \mathcal{T}_m^*} \omega^{\mathrm{T}(\lambda x)} = n_0 - n_2 + \omega n_1 - \omega n_3, \tag{3.35}$$

where $\omega = \sqrt{-1}$.

The complex conjugate $\bar{S}$ of the sum S is equal to

$$\bar{S} = \sum_{x \in \mathcal{T}_m^*} \omega^{-\mathrm{T}(\lambda x)}, \tag{3.36}$$

since $\omega^0 = \omega^{-0} = 1$, $\omega^2 = \omega^{-2} = -1$ and $\omega^1 = \omega^{-3} = \omega$, $\omega^3 = \omega^{-1} = -\omega$.

Then

$$\begin{aligned} |S|^2 &= S \cdot \bar{S} = \sum_{x \in \mathcal{T}_m^*} \omega^{\mathrm{T}(\lambda x)} \cdot \sum_{y \in \mathcal{T}_m^*} \omega^{-\mathrm{T}(\lambda y)} \\ &= \sum_{i,j=0}^{2^m-2} \omega^{\mathrm{T}(\lambda(\xi^i - \xi^j))} = (2^m - 1) + \sum_{i \neq j} \omega^{\mathrm{T}(\lambda(\xi^i - \xi^j))}. \end{aligned} \tag{3.37}$$

Elements $\pm\xi^k$ are invertible for all $0 \leq k \leq 2^m - 2$ and elements $\xi^i - \xi^j$ are invertible and different from $\pm\xi^k$ for distinct $i, j, k \in \{0, \ldots, 2^m - 2\}$ (see section III.C in [15]). A set

$$R^* = \{\pm\xi^k; 0 \leq k \leq 2^m - 2\} \cup \{\xi^i - \xi^j; i \neq j, 0 \leq i, j \leq 2^m - 2\} \tag{3.38}$$

of distinct invertible elements has therefore a cardinality $2(2^m-1)+(2^m-1)(2^m-2) = 2^{2m}-2^m$ and it is exactly the set of all invertible elements of the Galois ring $\mathrm{GR}(4^m)$ (i.e. $R^* = \mathrm{GR}(4^m) - 2\mathrm{GR}(4^m)$).

From Lemma 3.3.1 it follows that $\sum_{\nu \in R^*} \omega^{T(\nu)} = 0$ since

$$\sum_{\nu \in R^*} \omega^{T(\nu)} = \sum_{\nu \in \mathrm{GR}(4^m)} \omega^{T(\nu)} - \sum_{\nu \in 2\mathrm{GR}(4^m)} \omega^{T(\nu)} \tag{3.39}$$

and both sums are equal to 0.

The number $|S|^2$ can be therefore rewritten to the form

$$\begin{aligned} |S|^2 &= (2^m - 1) + \sum_{\nu \in R^*} \omega^{\mathrm{T}(\nu)} - \sum_{i=0}^{2^m-2} \omega^{\mathrm{T}(\lambda\xi^i)} - \sum_{j=0}^{2^m-2} \omega^{-\mathrm{T}(\lambda\xi^j)} \\ &= (2^m - 1) - S - \bar{S}. \end{aligned} \tag{3.40}$$

An equation $S\bar{S} + S + \bar{S} + 1 = 2^m$ holds and after a substitution of number S by $n_0 - n_2 + \omega n_1 - \omega n_3$ we get a diophantine equation

$$(n_0 - n_2 + 1)^2 + (n_1 - n_3)^2 = 2^m. \tag{3.41}$$

The equation has four possible solutions

$$n_0 - n_2 + 1 = \pm 2^{\frac{m-1}{2}}, \quad n_1 - n_3 = \pm 2^{\frac{m-1}{2}}. \tag{3.42}$$

Lemma 3.3.1 implies that

$$n_0 + n_2 = 2^{m-1} - 1, \quad n_1 + n_3 = 2^{m-1}. \tag{3.43}$$

By combining the previous two results we get desired equations (3.34).

Finally, by adding a parity check symbol to four codewords $\varepsilon\mathbf{1} + v^{(\lambda)}$ we get type distributions of codewords from items (iv) and (v). □

In Section 3.1 we have introduced three basic weight enumerators of $\mathbb{Z}_4$-codes. Expression of weight enumerators of the quaternary Kerdock codes $\mathcal{K}_4(m)$ is a direct corollary of the previous theorem.

Corollary 3.3.4. *Let $m \geq 3$ be an odd integer and let $\mathcal{K}_4(m)$ be the quaternary Kerdock code of length 2^m. Let m^+ denote an expression $2^{m-2} + 2^{\frac{m-3}{2}}$ and m^- denote an expression $2^{m-2} - 2^{\frac{m-3}{2}}$.*

The complete weight enumerator CWE of the code $\mathcal{K}_4(m)$ is a polynomial

$$\begin{aligned} CWE_{\mathcal{K}_4(m)}(w,x,y,z) &= w^{2^m} + x^{2^m} + y^{2^m} + z^{2^m} + \\ &\quad 2(2^m-1)w^{2^{m-1}}y^{2^{m-1}} + 2(2^m-1)x^{2^{m-1}}z^{2^{m-1}} + \\ &\quad 2^m(2^m-1)w^{m^+}x^{m^+}y^{m^-}z^{m^-} + \\ &\quad 2^m(2^m-1)w^{m^+}x^{m^-}y^{m^-}z^{m^+} + \\ &\quad 2^m(2^m-1)w^{m^-}x^{m^+}y^{m^+}z^{m^-} + \\ &\quad 2^m(2^m-1)w^{m^-}x^{m^-}y^{m^+}z^{m^+}. \end{aligned} \tag{3.44}$$

The symmetrized weight enumerator SWE of the code $\mathcal{K}_4(m)$ has the form

$$\begin{aligned} SWE_{\mathcal{K}_4(m)}(w,x,y) &= w^{2^m} + 2^{m+1}x^{2^m} + y^{2^m} + 2(2^m-1)w^{2^{m-1}}y^{2^{m-1}} + \\ &\quad 2^{m+1}(2^m-1)w^{m^+}x^{2^{m-1}}y^{m^-} + \\ &\quad 2^{m+1}(2^m-1)w^{m^-}x^{2^{m-1}}y^{m^+}. \end{aligned} \tag{3.45}$$

The Hamming weight enumerator HWE of the code $\mathcal{K}_4(m)$ is in the form

$$\begin{aligned} HWE_{\mathcal{K}_4(m)}(w,x) &= w^{2^m} + (2^{m+1}+1)x^{2^m} + 2(2^m-1)w^{2^{m-1}}x^{2^{m-1}} + \\ &\quad 2^{m+1}(2^m-1)w^{m^+}x^{3\cdot 2^{m-2}-2^{\frac{m-3}{2}}} + \\ &\quad 2^{m+1}(2^m-1)w^{m^-}x^{3\cdot 2^{m-2}+2^{\frac{m-3}{2}}}. \end{aligned} \tag{3.46}$$

Proof. Weight enumerators of the quaternary Kerdock code $\mathcal{K}_4(m)$ can be directly calculated using the type distribution of $\mathcal{K}_4(m)$ from Theorem 3.3.3. □

In Theorem 3.3.3 we have described the type distribution of the quaternary Kerdock code $\mathcal{K}_4(m)$ but we still cannot determine the type of a codeword $\mathbf{c}_{\lambda,\varepsilon} \in \mathcal{K}_4(m)$ identified by given values of parameters $\lambda \in \mathbb{Z}_4[\xi]$ and $\varepsilon \in \mathbb{Z}_4$. The following paragraphs help us to solve this problem. The main source was Chapter 2 in [36].

The Lee weight $w_L(i)$ of $i \in \mathbb{Z}_4$ is related to a real part of ω^i by

$$w_L(i) = 1 - \mathrm{Re}(\omega^i), \tag{3.47}$$

where $\omega = \sqrt{-1}$ (see Table 3.5).

The Lee weight of a codeword $\mathbf{c}_{\lambda,\varepsilon} \in \mathcal{K}_4(m)$ can be then expressed as

$$\begin{aligned} w_L(\mathbf{c}_{\lambda,\varepsilon}) &= \sum_{x\in\mathcal{T}_m} \left(1 - \mathrm{Re}(\omega^{\mathrm{T}(\lambda x)+\varepsilon})\right) = 2^m - \mathrm{Re}\left(\sum_{x\in\mathcal{T}_m} \omega^{\mathrm{T}(\lambda x)+\varepsilon}\right) \\ &= 2^m - \mathrm{Re}\left(\omega^{\varepsilon} \sum_{x\in\mathcal{T}_m} \omega^{\mathrm{T}(\lambda x)}\right). \end{aligned} \tag{3.48}$$

i	ω^i	$w_L(i)$	$1-\mathrm{Re}(\omega^i)$
0	1	0	1-1=0
1	i	1	1-0=1
2	-1	2	1-(-1)=2
3	-i	1	1-0=1

Table 3.5: Relationship between Lee weights of $i \in \mathbb{Z}_4$ and real parts of ω^i

For simplification, let $\Gamma(\lambda)$ denotes an expression $\sum_{x\in\mathcal{T}_m} \omega^{\mathrm{T}(\lambda x)}$. Then we have

$$w_L(\mathbf{c}_{\lambda,\varepsilon}) = 2^m - \mathrm{Re}\left(\omega^{\varepsilon}\Gamma(\lambda)\right). \tag{3.49}$$

Now it is sufficient to determine the value of exponential sum $\Gamma(\lambda)$ for $\lambda \in \mathbb{Z}_4[\xi]$ to find the Lee weight of given codeword $\mathbf{c}_{\lambda,\varepsilon}$.

First we formulate an auxiliary lemma (see Lemma 5 in [36]).

Lemma 3.3.5. *Let $\lambda \in \mathbb{Z}_4[\xi]$ has a 2-adic represenation $\lambda = \alpha + 2\beta$, where $\alpha \in \mathcal{T}_m^*$ and $\beta \in \mathcal{T}_m$. Then*

$$\Gamma(\alpha + 2\beta) = \omega^{-\mathrm{T}\left(\frac{\beta}{\alpha}\right)}\Gamma(1). \tag{3.50}$$

Proof. Let x and y be in $\mathcal{T}_m$. First we show that also $x + y + 2\sqrt{xy}$ is in $\mathcal{T}_m$. We use a 2-adic representation of element $x + y \in \mathbb{Z}_4[\xi]$. Let $x + y = d + 2e$ for some $d, e \in \mathcal{T}_m$. Then we calculate a value $(x + y)^{2^m}$ in two ways. First, $(x + y)^2 = d^2$ and therefore $(x + y)^{2^m} = d^{2^m} = d$. The second calculation uses an induction

$$\begin{aligned}(x+y)^{2^m} &= (x^2 + 2xy + y^2)^{2^{m-1}} = (x^{2^2} + 2x^2y^2 + y^{2^2})^{2^{m-2}} \\ &= x^{2^m} + 2x^{2^{m-1}}y^{2^{m-1}} + y^{2^m} = x + y + 2\sqrt{xy}.\end{aligned} \tag{3.51}$$

By comparison of previous two formulas we get an equation $d = x + y + 2\sqrt{xy}$ and $x + y + 2\sqrt{xy}$ is in $\mathcal{T}_m$. Moreover, when we fix y and let x run through $\mathcal{T}_m$ then $x + y + 2\sqrt{xy}$ also runs through $\mathcal{T}_m$.

Therefore we have

$$\begin{aligned}\Gamma(\lambda) &= \sum_{x\in\mathcal{T}_m} \omega^{\mathrm{T}(\lambda x)} = \sum_{x\in\mathcal{T}_m} \omega^{\mathrm{T}(\lambda(x+y+2\sqrt{xy}))} \\ &= \omega^{\mathrm{T}(\lambda y)} \sum_{x\in\mathcal{T}_m} \omega^{\mathrm{T}(\lambda(x+2\sqrt{xy}))}.\end{aligned} \tag{3.52}$$

If we set $\lambda = 1$, we get

$$\Gamma(1) = \omega^{\mathrm{T}(y)} \sum_{x\in\mathcal{T}_m} \omega^{\mathrm{T}(x+2xy))} = \omega^{\mathrm{T}(y)}\Gamma(1 + 2y) \tag{3.53}$$

since $\mathrm{T}(2\sqrt{xy}) = \mathrm{T}(2xy)$.

We have shown that for $\lambda = \alpha + 2\beta$ ($\alpha \neq 0$), the sum $\Gamma(\lambda)$ can be expressed as

$$\begin{aligned}\Gamma(\lambda) &= \Gamma(\alpha + 2\beta) = \Gamma\left(\alpha\left(1 + 2\frac{\beta}{\alpha}\right)\right) \\ &= \sum_{x\in\mathcal{T}_m} \omega^{\mathrm{T}\left(\alpha x\left(1+2\frac{\beta}{\alpha}\right)\right)} = \sum_{y\in\mathcal{T}_m} \omega^{\mathrm{T}\left(y\left(1+2\frac{\beta}{\alpha}\right)\right)} \\ &= \Gamma\left(1 + 2\frac{\beta}{\alpha}\right) = \omega^{-\mathrm{T}\left(\frac{\beta}{\alpha}\right)}\Gamma(1).\end{aligned} \tag{3.54}$$

□

When we combine equation (3.49) and Lemma 3.3.5, we get an expression of Lee weight for an arbitrary Kerdock codeword in terms of coefficients in its trace description and 2-adic representation.

For $\alpha \in \mathcal{T}_m^*$, $\beta \in \mathcal{T}_m$ and $\varepsilon \in \mathbb{Z}_4$, the Lee weight of codeword $\mathbf{c}_{\alpha+2\beta,\varepsilon} \in \mathcal{K}_4(m)$ is expressed as

$$w_L(\mathbf{c}_{\alpha+2\beta,\varepsilon}) = 2^m - \mathrm{Re}\left(\omega^{\varepsilon - T\left(\frac{\beta}{\alpha}\right)}\Gamma(1)\right). \tag{3.55}$$

For $\alpha = 0$, $\beta \in \mathcal{T}_m^*$ and $\varepsilon \in \mathbb{Z}_4$, the Lee weight of codeword $\mathbf{c}_{2\beta,\varepsilon} \in \mathcal{K}_4(m)$ can be expressed by

$$w_L(\mathbf{c}_{2\beta,\varepsilon}) = 2^m, \tag{3.56}$$

since

$$\sum_{x\in\mathcal{T}_m} \omega^{T((2\beta)x)} = \sum_{y\in\mathcal{T}_m} \omega^{T(2y)} = 2^{m-1}\omega^0 + 2^{m-1}\omega^2 = 0 \tag{3.57}$$

and the second term in expression (3.48) disappears.

For $\alpha = 0$, $\beta = 0$ and $\varepsilon \in \mathbb{Z}_4$, the Lee weight of codeword $\mathbf{c}_{0,\varepsilon} \in \mathcal{K}_4(m)$ can be expressed by modification of equation (3.48) in the form

$$w_L(\mathbf{c}_{0,\varepsilon}) = 2^m - 2^m\,\mathrm{Re}(\omega^\varepsilon). \tag{3.58}$$

The previous general formulas for the Lee weight of given codeword $\mathbf{c}_{\alpha+2\beta,\varepsilon} \in \mathcal{K}_4(m)$ help us to identify the codeword type.

Theorem 3.3.6. *Let $m \geq 3$ be an odd integer and let $\mathbf{c}_{\alpha+2\beta,\varepsilon}$ be a codeword from the quaternary Kerdock code $\mathcal{K}_4(m)$ of length $n = 2^m$, where $\alpha \in \mathcal{T}_m$, $\beta \in \mathcal{T}_m$ and $\varepsilon \in \mathbb{Z}_4$.*

(i) If $\alpha = 0$, $\beta = 0$ and $\varepsilon = i$, for $i \in \{0,1,2,3\}$ then the codeword $\mathbf{c}_{\alpha+2\beta,\varepsilon}$ is of the type i^n.

(ii) If $\alpha = 0$, $\beta \in \mathcal{T}_m^*$ and $\varepsilon \in \{0,2\}$, then the codeword $\mathbf{c}_{\alpha+2\beta,\varepsilon}$ is of the type $2^{\frac{n}{2}}0^{\frac{n}{2}}$.

(iii) If $\alpha = 0$, $\beta \in \mathcal{T}_m^*$ and $\varepsilon \in \{1,3\}$, then the codeword $\mathbf{c}_{\alpha+2\beta,\varepsilon}$ is of the type $1^{\frac{n}{2}}3^{\frac{n}{2}}$.

(iv) If $\alpha \in \mathcal{T}_m^*$, $\beta \in \mathcal{T}_m$ and $\varepsilon \in \mathbb{Z}_4$ such that $\varepsilon - \mathrm{T}(\beta/\alpha) \equiv \frac{1-m}{2} \pmod 4$, then the codeword $\mathbf{c}_{\alpha+2\beta,\varepsilon}$ is of the type $1^{n_1}2^{n_2}3^{n_3}0^{n-n_1-n_2-n_3}$ with

$$n_1 = 2^{m-2} + 2^{\frac{m-3}{2}},\ n_2 = 2^{m-2} - 2^{\frac{m-3}{2}},\ n_3 = 2^{m-2} - 2^{\frac{m-3}{2}}. \tag{3.59}$$

(v) If $\alpha \in \mathcal{T}_m^*$, $\beta \in \mathcal{T}(m)$ and $\varepsilon \in \mathbb{Z}_4$ such that $\varepsilon - \mathrm{T}(\beta/\alpha) \equiv \frac{3-m}{2} \pmod 4$, then the codeword $\mathbf{c}_{\alpha+2\beta,\varepsilon}$ is of type $1^{n_1}2^{n_2}3^{n_3}0^{n-n_1-n_2-n_3}$ with

$$n_1 = 2^{m-2} + 2^{\frac{m-3}{2}},\ n_2 = 2^{m-2} + 2^{\frac{m-3}{2}},\ n_3 = 2^{m-2} - 2^{\frac{m-3}{2}}. \tag{3.60}$$

(vi) *If* $\alpha \in \mathcal{T}_m^*$, $\beta \in \mathcal{T}(m)$ *and* $\varepsilon \in \mathbb{Z}_4$ *such that* $\varepsilon - \mathrm{T}(\beta/\alpha) \equiv \frac{3-m}{2} + 1 \pmod 4$, *then the codeword* $\mathbf{c}_{\alpha+2\beta,\varepsilon}$ *is of type* $1^{n_1}2^{n_2}3^{n_3}0^{n-n_1-n_2-n_3}$ *with*

$$n_1 = 2^{m-2} - 2^{\frac{m-3}{2}},\ n_2 = 2^{m-2} + 2^{\frac{m-3}{2}},\ n_3 = 2^{m-2} + 2^{\frac{m-3}{2}}. \tag{3.61}$$

(iv) *If* $\alpha \in \mathcal{T}_m^*$, $\beta \in \mathcal{T}_m$ *and* $\varepsilon \in \mathbb{Z}_4$ *such that* $\varepsilon - \mathrm{T}(\beta/\alpha) \equiv \frac{1-m}{2} - 1 \pmod 4$, *then the codeword* $\mathbf{c}_{\alpha+2\beta,\varepsilon}$ *is of the type* $1^{n_1}2^{n_2}3^{n_3}0^{n-n_1-n_2-n_3}$ *with*

$$n_1 = 2^{m-2} - 2^{\frac{m-3}{2}},\ n_2 = 2^{m-2} - 2^{\frac{m-3}{2}},\ n_3 = 2^{m-2} + 2^{\frac{m-3}{2}}. \tag{3.62}$$

Proof. The first three items can be shown using the same arguments as in parts (i) and (ii) of Theorem 3.3.3.

Let $\alpha \in \mathcal{T}_m^*$, $\beta \in \mathcal{T}_m$ and $\varepsilon \in \mathbb{Z}_4$. Denote an expression $\varepsilon - \mathrm{T}(\beta/\alpha)$ by x. Let m^+ denotes a number $2^{m-2}+2^{\frac{m-3}{2}}$ and let m^- denotes a number $2^{m-2}-2^{\frac{m-3}{2}}$.

The value of $\Gamma(1)$ for odd m is equal to $(1+\omega)^m$ (see Lemma 4 in [22]). The main idea of the proof lies in definition of L-function which provides an equation $\Gamma(1) = -\eta^m$ for some complex number η. When we set $m = 1$ we get $-\eta = 1+\omega$ and therefore $\Gamma(1) = -(-(1+\omega)^m)$.

Combining equation (3.48) and expression of $\Gamma(1)$ we get the Lee weight of codeword $\mathbf{c}_{\alpha+2\beta,\varepsilon}$ as

$$w_L(\mathbf{c}_{\alpha+2\beta,\varepsilon}) = 2^m - \mathrm{Re}(\omega^x(1+\omega)^m). \tag{3.63}$$

Since $(1+\omega)^2 = 2\omega$ and $(1+\omega)^3 = (2\omega)(1+\omega)$, the value of $(1+\omega)^m$ can be for odd $m \geq 3$ expressed as

$$(1+\omega)^m = (2\omega)^{\frac{m-1}{2}}(1+\omega). \tag{3.64}$$

Equation (3.63) is then in the form

$$\begin{aligned} w_L(\mathbf{c}_{\alpha+2\beta,\varepsilon}) &= 2^m - \mathrm{Re}(\omega^x(2\omega)^{\frac{m-1}{2}}(1+\omega)) \\ &= 2^m - \mathrm{Re}(2^{\frac{m-1}{2}}(\omega^{x+\frac{m-1}{2}} + \omega^{x+1+\frac{m-1}{2}})). \end{aligned} \tag{3.65}$$

Therefore the Lee weight of codeword $\mathbf{c}_{\alpha+2\beta,\varepsilon}$ depends on an expression $x+\frac{m-1}{2}$ and it is equal to $2^m - 2^{(m-1)/2}$ or $2^m + 2^{(m-1)/2}$.

Now we investigate values of the sum $x + \frac{m-1}{2}$.

- If $x + \frac{m-1}{2} \equiv 0 \pmod 4$, then the Lee weight $w_L(\mathbf{c}_{\alpha+2\beta,\varepsilon})$ is equal to $2^m - 2^{(m-1)/2}$ and $x \equiv \frac{1-m}{2} \pmod 4$.
- If $x + \frac{m-1}{2} \equiv 1 \pmod 4$, then the Lee weight $w_L(\mathbf{c}_{\alpha+2\beta,\varepsilon})$ is equal to $2^m + 2^{(m-1)/2}$ and $x \equiv \frac{3-m}{2} \pmod 4$.
- If $x + \frac{m-1}{2} \equiv 2 \pmod 4$, then the Lee weight $w_L(\mathbf{c}_{\alpha+2\beta,\varepsilon})$ is equal to $2^m + 2^{(m-1)/2}$ and $x \equiv \frac{3-m}{2} + 1 \pmod 4$.
- If $x + \frac{m-1}{2} \equiv 3 \pmod 4$, then the Lee weight $w_L(\mathbf{c}_{\alpha+2\beta,\varepsilon})$ is equal to $2^m - 2^{(m-1)/2}$ and $x \equiv \frac{1-m}{2} - 1 \pmod 4$.

Finally, we assign a type of codeword to the previous four options. The Lee weight $w_L(\mathbf{c}_{\alpha+2\beta,\varepsilon})$ indicates that the first and the last items correspond to codewords of types $1^{m^+}2^{m^-}3^{m^-}0^{m^+}$ or $1^{m^-}2^{m^-}3^{m^+}0^{m^+}$. The second and the third items then corresponds to codewords of types $1^{m^+}2^{m^+}3^{m^-}0^{m^-}$ or $1^{m^+}2^{m^+}3^{m^-}0^{m^-}$. □

3.3.2 Existence of designs from quaternary Kerdock code

In theory of codes over a finite field $\mathbb{F}_q$, a general method of a construction of t-designs as the support designs in linear codes is known. It was formulated and proven in 1969 by Assmus and Mattson. For the linear codes over the ring $\mathbb{Z}_4$, no similar theorem has been known until the beginning of the 21^{st} century.

Note that Theorem 3.2.2 is a generalization of Assmus-Mattson theorem for binary distance invariant codes.

In this section we use an Assmus-Mattson-type theorem for the $\mathbb{Z}_4$-linear codes formulated in [31] for a construction of designs based on the quaternary Kerdock codes.

Let $\mathcal{C}$ be a $\mathbb{Z}_4$-linear code of length n and let $T = \{T_1, \ldots, T_i\}$ be a set of i coordinates of $\mathcal{C}$. The *punctured code* of $\mathcal{C}$ at T (i.e. a code of length $n-i$ with deleted coordinates from the set T) will be denoted by $\mathcal{C}^T$. The *shortened code* of $\mathcal{C}$ at T is a code that contains only the codewords from $\mathcal{C}$ which have 0 in the coordinates from the set T and that are consequently punctured at T. This code is denoted by $\mathcal{C}^{0@T}$. The $\{0,2\}$-*subcode* of $\mathcal{C}$ consists of the codewords having only 0 and 2 as its elements and is denoted by $\mathcal{C}_{[0,2]}$.

A connection between Hamming weight enumerators of a code C and its dual $C^\perp$ is for the binary linear codes often expressed by the MacWilliams identity (see equation 3.14). The similar equations in terms of complete, symmetrized or Hamming weight enumerators can be formulated also for $\mathbb{Z}_4$-linear codes and their duals (see Chapter 2 in [11]). The MacWilliams identities of a $\mathbb{Z}_4$-linear code $\mathcal{C}$ have form

$$\begin{aligned} CWE_{\mathcal{C}}(w,x,y,z) &= \frac{1}{|\mathcal{C}^\perp|} CWE_{\mathcal{C}^\perp}(\bar{w},\bar{x},\bar{y},\bar{z}), \\ SWE_{\mathcal{C}}(w,x,y) &= \frac{1}{|\mathcal{C}^\perp|} SWE_{\mathcal{C}^\perp}(w+2x+y, w-y, w-2x+y), \\ HWE_{\mathcal{C}}(w,x) &= \frac{1}{|\mathcal{C}^\perp|} HWE_{\mathcal{C}^\perp}(w+3x, w-x), \end{aligned} \tag{3.66}$$

where $\bar{w} = w+x+y+z$, $\bar{x} = w+ix-y-iz$, $\bar{y} = w-x+y-z$, $\bar{z} = w-ix-y+iz$ and $i = \sqrt{-1}$.

Now we can formulate an analogy of the Assmus-Mattson theorem for $\mathbb{Z}_4$-linear codes (see Theorem 10 in [31]).

Theorem 3.3.7. *Let $\mathcal{C}$ be a $\mathbb{Z}_4$-linear code of length n such that all codewords of constant Hamming weight in the subcodes $\mathcal{C}_{[0,2]}$ and $(\mathcal{C}^\perp)_{[0,2]}$ of $\mathcal{C}$ and $\mathcal{C}^\perp$ yield*

the t-designs. Let s be the number of nonzero weights in $(\mathcal{C}^\perp - (\mathcal{C}^\perp)_{[0,2]})^{0@T}$ where $T \subset \mathcal{T}$ is of size t. Let d be the minimum Hamming weight in $(\mathcal{C} - \mathcal{C}_{[0,2]})$.

Then the codewords of the constant Hamming weight in $\mathcal{C}$ and the codewords of the constant Hamming weight $w \leq n-t$ in $\mathcal{C}^\perp$ yield the t-designs possibly with repeated blocks if $d - t \geq s$.

Proof. Let $\mathcal{C}$ be a quaternary code of length n satisfying assumptions of the theorem.

Hamming weight enumerators of $\mathcal{C}$ and $\mathcal{C}^\perp$ satisfy equations

$$HWE_{\mathcal{C}^\perp}(w,x) = \frac{1}{|\mathcal{C}|} HWE_{\mathcal{C}}(w+3x, w-x) \tag{3.67}$$

and

$$HWE_{(\mathcal{C}^\perp)^{0@T}}(w,x) = \frac{1}{|\mathcal{C}^T|} HWE_{\mathcal{C}^T}(w+3x, w-x) \tag{3.68}$$

since the dual of punctured code $\mathcal{C}^T$ at T is the shortened dual code $(\mathcal{C}^\perp)^{0@T}$ at T.

Now we express the Hamming weight enumerator of the code $(\mathcal{C}^\perp)^{0@T}$ in two ways as

$$HWE_{(\mathcal{C}^\perp)^{0@T}}(w,x) = w^{n-t} + \sum_{i=1}^{s} a_i w^{n-t-e_i} x^{e_i} + \sum_{i=1}^{n-t} b_i w^{n-t-i} x^i, \tag{3.69}$$

where the term w^{n-t} expresses the zero codeword, the sum with coefficients a_i corresponds to the codewords from $(\mathcal{C}^\perp - (\mathcal{C}^\perp)_{[0,2]})^{0@T}$ and the sum with coefficients b_i corresponds to the codewords from $(\mathcal{C}^\perp)^{0@T}_{[0,2]}$, and

$$HWE_{(\mathcal{C}^\perp)^{0@T}}(w,x) = \frac{1}{|\mathcal{C}^T|} \sum_{i=1}^{n-t} c_i (w+3x)^{n-t-i} (w-x)^i. \tag{3.70}$$

The assumptions of the theorem ensure that the coefficients b_i are known for $1 \leq i \leq n-t$. Moreover, since in $(\mathcal{C} - \mathcal{C}_{[0,2]})$ there doesn't exist a codeword of weight less than $d-t$ and the weight distribution of $\mathcal{C}_{[0,2]}$ is known, the coefficients c_i are known for $0 \leq i \leq d-1-t$.

If we combine equations (3.69) and (3.70) and put $w = 1$, we get

$$1 + \sum_{i=1}^{s} a_i x^{e_i} + \sum_{i=1}^{n-t} b_i x^i = \frac{1}{|\mathcal{C}^T|} \sum_{i=1}^{n-t} c_i (1+3x)^{n-t-i} (1-x)^i. \tag{3.71}$$

If we set $x = 1$ in equation (3.71), we have

$$\sum_{i=1}^{s} a_i = \frac{1}{|\mathcal{C}^T|} c_0 4^{n-t} - 1 - \sum_{i=1}^{n-t} b_i, \tag{3.72}$$

which is known value.

Now we diferentiate equation (3.71) j times about x for $1 \leq j \leq d-1-t$ and again set $x = 1$. We get a set of equations that can be expressed in the form

$$\sum_{i=1}^{s} a_i \binom{e_i}{j} = \lambda_j, \text{ for } 0 \leq j \leq d-1-t, \tag{3.73}$$

where λ_j is known value and with convention $\binom{e_i}{j} = 0$ if $j > e_i$.

Since $d-t \geq s$ and the previous equations are linearly independent, we obtain values $a_1, \ldots, a_s$.

The Hamming weight enumerator of the shortened dual code $(\mathcal{C}^\perp)^{0@T}$ is then independent of t coordinates from T that shortening takes place in. Thus if we consider zeros in codewords from $\mathcal{C}^\perp$ of the same Hamming weight as blocks, we get t-design. This yields the complementary t-design from codewords of constant Hamming weight $w \leq n-t$ in $\mathcal{C}^\perp$. (A t-design D' is called *complementary* to the t-design D if all blocks of D' are complements of the blocks of D.)

Codewords of constant Hamming weight in $\mathcal{C}$ also form a t-design since the Hamming weight enumerator of $\mathcal{C}^T$ is independent of the choice of T. □

Now we use the quaternary version of Assmus-Mattson theorem for the quaternary Kerdock and Preparata codes.

Corollary 3.3.8. *Let $\mathcal{K}_4(m)$, $m \geq 3$ odd, be the quaternary Kerdock code of length 2^m. Then supports of codewords of constant Hamming weight in $\mathcal{K}_4(m)$ form 3-design (not necessarily simple).*

Proof. The corollary is an application of the quaternary version of Assmus-Mattson theorem (Theorem 3.3.7) on the quaternary Kerdock and Preparata codes of the same length 2^m, $m \geq 3$ odd.

Let code $\mathcal{C}$ in Theorem 3.3.7 be the quaternary Preparata code $\mathcal{P}_4(m)$. Then the code $\mathcal{C}^\perp$ is the quaternary Kerdock code $\mathcal{K}_4(m)$.

Subcode $\mathcal{C}_{[0,2]} = \mathcal{P}(m)_{[0,2]}$ can be expressed as

$$\mathcal{P}(m)_{[0,2]} = \{2\mathbf{c};\ \mathbf{c} \in \hat{\mathcal{H}}(m)\}, \tag{3.74}$$

where $\hat{\mathcal{H}}(m)$ is the extended Hamming code of length 2^m (see Chapter 13.3 in [26]). Since the codewords of constant Hamming weight in the extended Hamming code form 3-design, $\mathcal{P}(m)_{[0,2]}$ also give 3-designs.

Subcode $\mathcal{C}^\perp_{[0,2]} = \mathcal{K}(m)_{[0,2]}$ corresponds to a union of zero codeword, all-two codeword and codewords of type $0^{2^{m-1}}2^{2^{m-1}}$, i.e.

$$\mathcal{K}(m)_{[0,2]} = \mathbf{c}_{0,0} \cup \mathbf{c}_{0,2} \cup \left\{ \bigcup_{\beta \in \mathcal{T}_m^*} \{\mathbf{c}_{2\beta,0} \cup \mathbf{c}_{2\beta,2}\} \right\}, \tag{3.75}$$

where $\mathbf{c}_{\lambda,\varepsilon} = (\mathrm{T}(0)+\varepsilon, \mathrm{T}(\lambda)+\varepsilon, \mathrm{T}(\lambda\xi)+\varepsilon, \ldots, \mathrm{T}(\lambda\xi^{2^m-2})+\varepsilon)$, for $\lambda \in \mathbb{Z}_4[\xi]$ and $\varepsilon \in \mathbb{Z}_4$ (see proof of Theorem 3.3.3).

The zero and all-two codewords both form trivial 3-design. Thus it remains to show that the codewords of type $0^{2^{m-1}}2^{2^{m-1}}$ also give 3-design.

Since the generalized trace map T is a linear map such that $\mu \circ \mathrm{T} = \mathrm{Tr} \circ \mu$, where μ is a modulo-2 reduction, each codeword $\mathbf{c}_{2\beta,\varepsilon}$, $\beta \in \mathcal{T}_m^*$, $\varepsilon \in \{0,2\}$ can be expressed as

$$\begin{aligned} \mathbf{c}_{2\beta,\varepsilon} &= (\mathrm{T}(0)+\varepsilon, \mathrm{T}(2\beta)+\varepsilon, \mathrm{T}(2\beta\xi)+\varepsilon, \ldots, \mathrm{T}(2\beta\xi^{2^m-2})+\varepsilon) \\ &= 2(\mathrm{T}(0)+e, \mathrm{T}(\beta)+e, \mathrm{T}(\beta\xi)+e, \ldots, \mathrm{T}(\beta\xi^{2^m-2})+e) \\ &= 2(\mathrm{Tr}(0)+e, \mathrm{Tr}(b)+e, \mathrm{Tr}(b\alpha)+e, \ldots, \mathrm{Tr}(b\alpha^{2^m-2})+e), \end{aligned} \tag{3.76}$$

where $e = \mu(\varepsilon) \in \mathbb{F}_2$, $b = \mu(\beta) \in \mathbb{F}_{2^m}$ (it follows from an isomorphism $\mathcal{T}_m \simeq \mathbb{F}_{2^m}$) and $\alpha = \mu(\xi)$ is a primitive element of $\mathbb{F}_2^m$. The set $\left\{\frac{\mathbf{c}_{2\beta,\varepsilon}}{2}\right\}$ therefore correspond exactly to the set of extended m-sequences of length 2^m, i.e. maximum length binary sequences generated by primitive polynomial (see Chapter II in [30]), and form a 3-design. Thus the subcode $\mathcal{K}(m)_{[0,2]}$ also forms a 3-design.

The subcode $\mathcal{K}(m)^{0@T}$ contains codewords with 5 distinct weights (see Theorem 3.3.3). Since 3 of them corresponds to the code $\mathcal{K}(m)_{[0,2]}$, the parameter s is equal to 2. Moreover, parameter d is equal to 5 and assumptions of the Assmus-Mattson theorem are satisfied for $t \leq 3$.

Codewords of the quaternary Kerdock code $\mathcal{K}(m)$ of constant Hamming weight $w \leq 2^m - 3$ therefore yield 3-design. Since supports of codewords of Hamming weight 2^m give trivial design, the corollary is proved. □

Changing the sign of codeword (i.e. multiplying by -1) doesn't change its support. Therefore, we consider only codewords from $\mathcal{K}(m)$ of types $1^{m^+}2^{m^-}3^{m^-}0^{m^+}$ and $1^{m^+}2^{m^+}3^{m^-}0^{m^-}$, where m^+ is equal to $2^{m-2} + 2^{\frac{m-3}{2}}$ and m^- is equal to $2^{m-2} - 2^{\frac{m-3}{2}}$, to construct nontrivial simple designs.

Theorem 3.3.9. *Let $m \geq 3$ be an odd integer and let $\mathcal{K}_4(m)$ be the quaternary Kerdock code of length $n = 2^m$. Let m^+ denote an expression $2^{m-2} + 2^{\frac{m-3}{2}}$ and m^- denote an expression $2^{m-2} - 2^{\frac{m-3}{2}}$.*

(i) The supports of codewords of the type $1^{m^+}2^{m^-}3^{m^-}0^{m^+}$ in $\mathcal{K}_4(m)$ form a $3-(2^m, k, \lambda)$ design, where

$$k = 2^{m-1} + 2^{m-2} - 2^{\frac{m-3}{2}},\ \lambda = \frac{k(k-1)(k-2)}{2^m - 2}. \tag{3.77}$$

(ii) The supports of codewords of the type $1^{m^+}2^{m^+}3^{m^-}0^{m^-}$ in $\mathcal{K}_4(m)$ form a $3-(2^m, k, \lambda)$ design, where

$$k = 2^{m-1} + 2^{m-2} + 2^{\frac{m-3}{2}},\ \lambda = \frac{k(k-1)(k-2)}{2^m - 2}. \tag{3.78}$$

Proof. From Corollary 3.3.8 and the remark that follows, we know that the supports of codewords of types $1^{m^+}2^{m^-}3^{m^-}0^{m^+}$ and $1^{m^+}2^{m^+}3^{m^-}0^{m^-}$ in $\mathcal{K}_4(m)$ form $t-(v, k, \lambda)$ designs, where t is 3 and v is equal to the length of $\mathcal{K}(m)$ (i.e. $v = 2^m$). Since k corresponds to number of nonzero coordinates in codewords of given type, it is equal to $2^{m-1} + 2^{m-2} - 2^{\frac{m-3}{2}}$ or $2^{m-1} + 2^{m-2} + 2^{\frac{m-3}{2}}$ respectively.

It remains to determine the parameter λ. We use a general property of t-designs (see Corollary 2.10 in [26]).

Each $t-(v, k, \lambda)$ design satisfy a property

$$\lambda\binom{v}{t} = B\binom{k}{t}, \tag{3.79}$$

where B is a number of blocks.

Since number of blocks is for mentioned designs based on the quaternary Kerdock codes equal to $2^m(2^m-1)$, we get an equation

$$\lambda\binom{2^m}{3} = 2^m(2^m-1)\binom{k}{3}, \tag{3.80}$$

and finally we have

$$\lambda = \frac{k(k-1)(k-2)}{2^m-2} \tag{3.81}$$

for an appropriate k. □

In the previous paragraphs we have constructed designs from codewords of the quaternary Kerdock code $\mathcal{K}(m)$ with constant Hamming weight. Article [12] compiles the results about colored designs based on the code $\mathcal{K}(m)$. It is shown that the codewords of given complete weight define a 4-colored 3-design (colors are identified with numbers 0,1,2,3 at given coordinates). Moreover, if we consider symmetrized weight enumerator of $\mathcal{K}(m)$, codewords of given symmetrized weight define blocks of 3-colored 3-design (numbers 1 and 3 at codeword coordinates correspond to the same color).

4. Application of Kerdock codes in Cryptography

In the previous chapter we have shown how to use Kerdock codes to derive combinatorial designs. In this chapter we shall show how they can be applied in cryptography. In particular we shall link them to bent functions and to resilient functions.

Definition 4.0.10. Let m be a non-negative integer. A *Boolean function* f of arity m is a function $f: \mathbb{F}_2^m \to \mathbb{F}_2$.

Modern cryptography is closely related to computer science (i.e. to the world of zeros and ones). Probably all conventional cryptographical systems are based on Boolean functions or, more generally, on functions from $\mathbb{F}_2^m$ to $\mathbb{F}_2^n$, where $m > n$ are the non-negative integers.

In order to assure a resistance of a system against attacks, it is necessary to choose the involved functions very carefully. Based on known attacks on cryptographical systems, several requirements on functions in use have been formulated (e.g. nonlinearity, resiliency, balancedness, propagation criterions).

4.1 Bent functions from Kerdock codes

If we want to study a cryptographic scheme that uses a Boolean function of arity m, one of the first properties that should be investigated is a Hamming distance of the examined function from a set of all affine Boolean functions (i.e. from the Boolean functions corresponding to the first order Reed-Muller code $\mathcal{RM}(1, m)$). Since affine functions can be easily attacked the distance should be as big as possible. Informally, the larger the distance, the less accurate an approximation by an affine function can be.

First we formulate few basic definitions and remarks that help us to formalize the desired property. An introduction to Boolean functions can be found in survey [8].

In the following text we will identify Boolean functions of arity m with Boolean polynomials in m indeterminates. By a degree of a Boolean function we will mean a degree of the corresponding Boolean polynomial. This notation was introduced in Section 1.1.

A distance between two Boolean functions of the same arity is a number of values where they differ.

Definition 4.1.1. Let f_1 and f_2 be Boolean functions of the same arity m. A *distance* $d(f_1, f_2)$ between them is defined by

$$d(f_1, f_2) = |\{\mathbf{x} \in \mathbb{F}_2^m; f_1(\mathbf{x}) \neq f_2(\mathbf{x})\}|. \tag{4.1}$$

As was written above, we are interested mainly in a distance of a Boolean function f from the set of all affine functions. This distance is often called a nonlinearity of f.

Definition 4.1.2. Let f be a Boolean function of arity m. A *nonlinearity* of the function f is defined as

$$N_f = \min_{a(\mathbf{x})\in A} |\{\mathbf{x} \in \mathbb{F}_2^m; f(\mathbf{x}) \neq a(\mathbf{x})\}|, \tag{4.2}$$

where A is the set of all affine Boolean functions, i.e.

$$A = \left\{ a(\mathbf{x}) = a_0 + \sum_{i=1}^{m} a_i x_i;\ \mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{F}_2^m,\ a_0, a_1, \ldots, a_m \in \mathbb{F}_2 \right\}. \tag{4.3}$$

Since each codeword of the first order Reed-Muller code $\mathcal{RM}(1, m)$ of length 2^m is equal to the evaluation of an affine Boolean function of arity m, we can identify the set A with the code $\mathcal{RM}(1, m)$. A nonlinearity of a Boolean function f of arity m thus corresponds to the minimum of Hamming distances between the codeword from $\mathcal{RM}(1, m)$ and an evaluation vector v_f of the function f, i.e.

$$N_f = \min_{\mathbf{c}\in\mathcal{RM}(1,m)} d(\mathbf{c}, v_f). \tag{4.4}$$

Now we see that the maximal nonlinearity of a Boolean function of arity m is equal to a maximal distance from an arbitrary vector $\mathbf{x} \in \mathbb{F}_2^{2^m}$ to the nearest codevord $\mathbf{c} \in \mathcal{RM}(1, m)$ (i.e. to the covering radius ρ_m of the code $\mathcal{RM}(1, m)$).

Definition 4.1.3. Let C be a binary code of length n. The *covering radius* ρ of C is

$$\rho = \max_{\mathbf{x}\in\mathbb{F}_2^n} \min_{\mathbf{c}\in C} d(\mathbf{x}, \mathbf{c}), \tag{4.5}$$

where d is a Hamming distance function.

The covering radius ρ_m of the first order Reed-Muller code $RM(1, m)$ for even m will be calculated using its upper and lower bounds that are approximated in the following lemmas. The upper bound is derived in Theorem 1.8 in article [7]. The lower bound of the covering radius ρ_m can be found in [18].

An approximation of the upper bound of the covering radius ρ_m is formulated in more general form. Assumption of the lemma uses property of error-correcting codes called strength.

Definition 4.1.4. A binary code C has a *strength* s, if all possible s-tuples from $\mathbb{F}_2^s$ occur the same number of times in any s coordinates. The *maximum strength* of a code is defined as the largest integer s for which the code has strength s.

Let C be an $[n, k, d]$ binary linear code and let $C^\perp$ be the $[n, n-k, d']$ code dual to C. Let $[C]$ be the $2^k \times n$ array of all codewords of C. Then any set of $s \leq d' - 1$ columns of $[C]$ are linearly independent, since otherwise the code $C^\perp$ would contain a vector of weight $s < d'$. In terms of strength of the code C, the previous fact implies that the maximum strength s of C is equal to $d' - 1$.

The strength of a code can be defined in the same way also for codes over an arbitrary finite field $\mathbb{F}_q$. The maximum strength of a code over $\mathbb{F}_q$ is then derived from its dual distance as in the binary case.

Lemma 4.1.5. *Let C be a linear binary code of length n containing the all-one codeword. If C has maximum strength at least 2, then its covering radius ρ is at most $(n - \sqrt{n})/2$, i.e.*

$$\rho \leq \frac{n - \sqrt{n}}{2}. \tag{4.6}$$

Proof. Suppose that the covering radius ρ is $\frac{n}{2} - k$, where $k \geq 0$. Since

$$d(\mathbf{v}, \mathbf{c} + \mathbf{1}) = n - d(\mathbf{v}, \mathbf{c}), \tag{4.7}$$

all distances from a vector $\mathbf{v}$ to the code C lie in the interval $\left[\frac{n}{2} - k, \frac{n}{2} + k\right]$ for all $\mathbf{v} \in \mathbb{F}_2^n$.

Now we calculate the variance of distances of an arbitrary vector $\mathbf{v} \in \mathbb{F}_2^n$ from codewords $\mathbf{c} \in C$.

Let $d_i(\mathbf{c}) = 0$ if $\mathbf{v}$ and $\mathbf{c}$ agree in the ith coordinate and $d_i(\mathbf{c}) = 1$ otherwise, for $1 \leq i \leq n$ and $\mathbf{c} \in C$. Then

$$d(\mathbf{v}, \mathbf{c}) = \sum_{i=1}^{n} d_i(\mathbf{c}) \tag{4.8}$$

and

$$d(\mathbf{v}, \mathbf{c})(d(\mathbf{v}, \mathbf{c}) - 1) = \sum_{i \neq j} d_i(\mathbf{c}) d_j(\mathbf{c}). \tag{4.9}$$

If C has strength 2, then

$$\sum_{\mathbf{c} \in C} d_i(\mathbf{c}) d_j(\mathbf{c}) = \frac{|C|}{4} \tag{4.10}$$

for all $1 \leq i, j \leq n$, $i \neq j$.

Thus the average value of $d(\mathbf{v}, \mathbf{c})(d(\mathbf{v}, \mathbf{c}) - 1)$ for any $\mathbf{v} \in \mathbb{F}_2^n$ is

$$\begin{aligned} \frac{1}{|C|} \sum_{\mathbf{c} \in C} d(\mathbf{v}, \mathbf{c})(d(\mathbf{v}, \mathbf{c}) - 1) &= \frac{1}{|C|} \sum_{\mathbf{c} \in C} \sum_{i \neq j} d_i(\mathbf{c}) d_j(\mathbf{c}) \\ &= \frac{1}{|C|} \sum_{i \neq j} \frac{|C|}{4} = \frac{n(n-1)}{4}. \end{aligned} \tag{4.11}$$

Moreover, the average distance of $\mathbf{v}$ from codewords of C is

$$\frac{1}{|C|} \sum_{\mathbf{c} \in C} d(\mathbf{v}, \mathbf{c}) = \frac{1}{|C|} \sum_{i=1}^{n} \sum_{\mathbf{c} \in C} d_i(\mathbf{c}) = \frac{1}{|C|} \sum_{i=1}^{n} \frac{|C|}{2} = \frac{n}{2}, \tag{4.12}$$

since C has also strength 1.

A variance σ^2 of distances $d(\mathbf{v}, \mathbf{c})$ is therefore equal to

$$\sigma^2 = \frac{1}{|C|} \sum_{\mathbf{c} \in C} d(\mathbf{v}, \mathbf{c})^2 - \left(\frac{1}{|C|} \sum_{\mathbf{c} \in C} d(\mathbf{v}, \mathbf{c}) \right)^2 = \frac{n(n-1)}{4} + \frac{n}{2} - \frac{n^2}{4} = \frac{n}{4}. \tag{4.13}$$

A standard deviation σ of distances from a vector $\mathbf{v}$ to the code C, which shows difference of distances from the average $\frac{n}{2}$, is then equal to $\frac{\sqrt{n}}{2}$ and we have $k \geq \frac{\sqrt{n}}{2}$, since the interval $\left[\frac{n}{2} - k, \frac{n}{2} + k\right]$ contains interval $\left[\frac{n}{2} - \sigma, \frac{n}{2} + \sigma\right]$ □

Lemma 4.1.6. *Let ρ_m, $m \geq 0$, be a covering radius of $RM(1,m)$. Then*

$$\rho_m \geq 2^{m-1} - 2^{\lceil m/2 \rceil - 1}. \tag{4.14}$$

Proof. Let us use a recursive definition of the first order Reed-Muller codes, i.e.

$$\begin{aligned} RM(1,0) &= \{(0),(1)\}, \\ RM(1,m+1) &= \bigcup_{\mathbf{c} \in RM(1,m)} \{(\mathbf{c},\mathbf{c}),(\mathbf{c},\bar{\mathbf{c}})\} \end{aligned} \tag{4.15}$$

where $\bar{\mathbf{c}}$ denotes a complement of the codeword $\mathbf{c}$ (i.e. $\bar{\mathbf{c}} = \mathbf{c} + \mathbf{1}$, where $\mathbf{1}$ is the all-one vector of length 2^m). The definition is correct, since each affine Boolean function f of arity $m+1$ can be expressed using an affine Boolean function g of arity m as

$$f((x_1,\ldots,x_{m+1})) = g((x_1,\ldots,x_m)) + a_{m+1}x_{m+1}, \tag{4.16}$$

for all $(x_1,\ldots,x_{m+1}) \in \mathbb{F}_2^{m+1}$, where $a_{m+1} \in \mathbb{F}_2$.

A code $RM(1,m+2)$ can be therefore expressed in terms of codewords from $RM(1,m)$ as

$$RM(1,m+2) = \bigcup_{\mathbf{c} \in RM(1,m)} \{(\mathbf{c},\mathbf{c},\mathbf{c},\mathbf{c}),(\mathbf{c},\mathbf{c},\bar{\mathbf{c}},\bar{\mathbf{c}}),(\mathbf{c},\bar{\mathbf{c}},\mathbf{c},\bar{\mathbf{c}}),(\mathbf{c},\bar{\mathbf{c}},\bar{\mathbf{c}},\mathbf{c})\}. \tag{4.17}$$

Let $\mathbf{v} \in \mathbb{F}_2^{2^m}$ be a vector such that $d(\mathbf{v},\mathbf{c}) \geq \rho_m$ for all $\mathbf{c} \in RM(1,m)$. The definition of covering radius ρ_m ensures the existence of such vector. Then

$$d(\bar{\mathbf{v}},\bar{\mathbf{c}}) = d(\mathbf{v},\mathbf{c}) \tag{4.18}$$

and

$$d(\bar{\mathbf{v}},\mathbf{c}) = d(\mathbf{v},\bar{\mathbf{c}}) = 2^m - d(\mathbf{v},\mathbf{c}). \tag{4.19}$$

If we consider vector $\mathbf{u} = (\mathbf{v},\mathbf{v},\mathbf{v},\bar{\mathbf{v}}) \in \mathbb{F}_2^{2^{m+2}}$, we have

$$\begin{aligned} d((\mathbf{v},\mathbf{v},\mathbf{v},\bar{\mathbf{v}}),(\mathbf{c},\mathbf{c},\mathbf{c},\mathbf{c})) &= 3d(\mathbf{v},\mathbf{c}) + d(\bar{\mathbf{v}},\mathbf{c}) \\ &= 2d(\mathbf{v},\mathbf{c}) + 2^m \geq 2\rho_m + 2^m. \end{aligned} \tag{4.20}$$

Similarly, using formulas (4.18) and (4.19) we show that $d(\mathbf{u},\mathbf{c}') \geq 2\rho_m + 2^m$ also for other types of codewords $\mathbf{c}' \in RM(1,m+2)$. Therefore $\rho_{m+2} \geq 2\rho_m + 2^m$.

The theorem now follows by induction, since $\rho_0 = 0$ and $\rho_1 = 0$ and if $\rho_m \geq 2^{m-1} - 2^{\lceil m/2 \rceil - 1}$, then

$$\begin{aligned} \rho_{m+2} &\geq 2\rho_m + 2^m \geq 2(2^{m-1} - 2^{\lceil m/2 \rceil - 1}) + 2^m \\ &= 2^{(m+2)-1} - 2^{\lceil (m+2)/2 \rceil - 1}. \end{aligned} \tag{4.21}$$

□

Now we get the covering radius ρ_m of the first order Reed-Muller code as a direct consequence of auxiliary lemmas 4.1.5 and 4.1.6.

Corollary 4.1.7. *Let $m \geq 0$ be an even integer. The covering radius ρ_m of the first order Reed-Muller code $\mathcal{RM}(1, m)$ is equal to*

$$\rho_m = 2^{m-1} - 2^{\frac{m}{2}-1}. \tag{4.22}$$

Proof. According to the note on the strength of a code, a maximum strength of the first order Reed-Muller code $\mathcal{RM}(1, m)$ is equal to 3, since its dual code $\mathcal{RM}(m-2, m)$ has minimum weight $2^{m-(m-2)} = 4$ (see Chapter 13 in [26]). Moreover, the length of the first order Reed-Muller code $\mathcal{RM}(1, m)$ is 2^m and Lemma 4.1.5 therefore implies that the covering radius ρ_m is at most $2^{m-1} - 2^{\frac{m}{2}-1}$.

Conversely, from Lemma 4.1.6 it follows that for even m, the covering radius ρ_m is at least $2^{m-1} - 2^{\frac{m}{2}-1}$. □

Boolean functions that reach the upper bound of the nonlinearity are often called bent or perfect nonlinear functions.

Definition 4.1.8. A Boolean function $f: \mathbb{F}_2^m \to \mathbb{F}_2$ of arity m is called *bent* if its Hamming distance to the first order Reed-Muller code $\mathcal{RM}(1, m)$ (i.e. to the set of all affine Boolean functions of arity m) is equal to $2^{m-1} - 2^{\frac{m}{2}-1}$.

From the definition it immediatly follows that no affine Boolean function is bent. A Boolean function can be therefore bent, if it has a degree at least 2. The following theorem identifies the quadratic bent functions. A recognition of bent functions of low degrees can be found in section 6.2. in [8]. A complete characterization of bent functions of degree $d \geq 3$ is an open problem.

Theorem 4.1.9. *Let $f: \mathbb{F}_2^m \to \mathbb{F}_2$ be a quadratic Boolean function of arity m. Then f is bent if and only if one of the following equivalent properties is satisfied:*

(i) the Hamming weight of its evaluation vector v_f is equal to $2^{m-1} \pm 2^{\frac{m}{2}-1}$;

(ii) the function f can be expressed as

$$f(\mathbf{x}) = Q(\mathbf{x}) + a_0, \tag{4.23}$$

where $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{F}_2^m$, Q is a non-singular quadratic form on a vector space $\mathbb{F}_2^m$ and $a_0 \in \mathbb{F}_2$.

Proof. In Section 3.2.1 we have determined a weight distribution of coset of the first order Reed Muller code corresponding to a non-singular quadratic form. The equivalence of conditions (i) and (ii) is a consequence of discussion on Table 3.2.

Let f be a quadratic bent Boolean function of arity m. Then its distance from $\mathcal{RM}(1, m)$ is equal to $2^{m-1} - 2^{\frac{m}{2}-1}$. Since $\mathcal{RM}(1, m)$ is a linear code that contains the all-one codeword, weight of evaluation vector v_f is $2^{m-1} - 2^{\frac{m}{2}-1}$ or $2^{m-1} + 2^{\frac{m}{2}-1}$.

Let f be a quadratic Boolean function that can be expressed in the form (4.23) for some non-singular quadratic form Q. Then the coset $f + \mathcal{RM}(1, m)$ of the first order Reed-Muller code in the second order Reed-Muller code is equal to the coset $Q + \mathcal{RM}(1, m)$. Distances from an evaluation vector of Q to codewords

from $\mathcal{RM}(1,m)$ are equal to weights of vectors in the coset $Q+\mathcal{RM}(1,m)$, which is $2^{m-1} \pm 2^{\frac{m}{2}-1}$ (see section 3.2.1).

Since a nonlinearity of function f is equal to its minimal distance from a codeword of $\mathcal{RM}(1,m)$ (i.e. to the minimal weight of a vector from $Q+\mathcal{RM}(1,m)$), it is equal to $2^{m-1} - 2^{\frac{m}{2}-1}$. The function f is therefore bent. □

In section 1.1 we have defined the binary Kerdock code $\mathcal{K}(m)$ ($m \geq 4$ even) as a union of certain cosets of the first order Reed-Muller code $\mathcal{RM}(1,m)$ in the second order Reed-Muller code $\mathcal{RM}(2,m)$. Since each codeword of $\mathcal{RM}(2,m)$ is an evaluation vector of given Boolean function of arity m and degree $d \leq 2$, the second order Reed-Muller code $\mathcal{RM}(2,m)$ (and consequently the Kerdock code $\mathcal{K}(m)$) can be viewed as a set of Boolean functions of arity m.

Now we classify the nonlinearity of codewords from the Kerdock code $\mathcal{K}(m)$ and their differences.

Theorem 4.1.10. *Let $\mathcal{K}(m)$ be the binary Kerdock code of length 2^m, $m \geq 4$ even. Then the difference of any two codewords $\mathbf{c_1}, \mathbf{c_2} \in \mathcal{K}(m)$ is either bent or affine Boolean function (i.e. the nonlinearity of a Boolean function corresponding to the vector $\mathbf{c_1} - \mathbf{c_2}$ is equal to $2^{m-1} - 2^{\frac{m}{2}-1}$ or 0).*

Proof. The binary Kerdock code $\mathcal{K}(m)$ can be viewed as a union of the first order Reed-Muller code together with cosets corresponding to non-singular quadratic forms determined by the Kerdock set $\mathcal{K}$ of regular skew-symmetric matrices.

Since the difference between each two matrices from the Kerdock set $\mathcal{K}$ is again a regular matrix, it gives us a coset of $\mathcal{RM}(1,m)$ (not necessarily included in the code $\mathcal{K}(m)$) corresponding to a non-singular quadratic form.

The result therefore follows from Theorem 4.1.9.

□

In the literature, an inverse approach to the relationship between Kerdock codes and bent functions is sometimes considered (see [33]). The Kerdock code of length 2^m, $m \geq 4$ even, is then defined as a union of the first order Reed-Muller code $\mathcal{RM}(1,m)$ together with $2^{m-1}-1$ cosets of $\mathcal{RM}(1,m)$ in the second order Reed-Muller code $\mathcal{RM}(2,m)$ such that the Boolean functions associated with the cosets are quadratic bent functions such that the sum of every two of them is again a bent function.

4.2 Resilient functions from Kerdock codes

Resilient functions form a family of functions defined on a vector space $\mathbb{F}_q^n$ that can be succesfully applied in a cryptography. We shall assume that $q = 2$ since this is the case that usually occurs in cryptographical applications. The basic idea was formulated independently in the eighties in articles [9] and [3].

The main usage of resilient functions lies in a construction of stream ciphers. In a stream cipher the plaintext is added (by XOR) with a pseudorandom keystream that is typically generated by combining the outputs of several linear feedback shift registers (LFSR). Security of the cipher depends significantly on a choice of the combining function. If there exist a correlation between the

keystream and the output sequence of some LFSRs, the divide and conquer algorithm can be used to decrease the complexity of a brute force attack on the cipher (the correlated registers are attacked separately). Such a type of attack is called a correlation attack. A sufficient resiliency of the combining function of a LFSR based stream cipher serves as an efficient prevention from the attack.

For more information about correlation attacks see [27], Chapter 6, or [32]. The main source for the section was [34].

Let $n \geq k \geq 1$ be integers and let f be a function

$$f: \mathbb{F}_2^n \to \mathbb{F}_2^k, \tag{4.24}$$

i.e. the input of f consists of n bits and the output of f consists of k bits. Now assume that t input bits are fixed and remaining $n - t$ input bits are chosen randomly and independently. If each possible output of k bits occurs equally likely, the function f is called t-resilient. A more formal definition follows.

Definition 4.2.1. Let $n \geq k \geq 1$ be integers and let f be a function

$$f : \mathbb{F}_2^n \to \mathbb{F}_2^k. \tag{4.25}$$

Let $t \leq n$ be an integer. The function f is called (n, k, t)-*resilient* if for every subset of indices $\{i_1, \ldots, i_t\} \subseteq \{1, \ldots, n\}$ of cardinality t, for every choice of $z_j \in \mathbb{F}_2$, $1 \leq j \leq t$, and for every k-tuple $(y_1, \ldots, y_k) \in \mathbb{F}_2^k$

$$\begin{aligned} &P(f(x_1, \ldots, x_n) = (y_1, \ldots, y_k) \mid x_{i_j} = z_j, 1 \leq j \leq t) \\ &\quad = P(f(x_1, \ldots, x_n) = (y_1, \ldots, y_k)) = \frac{1}{2^k}. \end{aligned} \tag{4.26}$$

An (n, k, t)-resilient function f that can be expressed in the form

$$f(x) = xG, \tag{4.27}$$

for a $n \times k$ binary matrix G is called *linear*. The basic construction of linear resilient functions uses a direct connection between linear (n, k, t)-resilient functions and linear $[n, k, t + 1]$ error-correcting codes.

In articles [9] and [3] it is shown that these two structures are equivalent. The main idea of proof lies in an identification of a matrix G determining the linear (n, k, t)-resilient function f with a generating matrix G^T of an $[n, k, t + 1]$ linear code.

The authors of article [3] also conjectured that if there exists an (n, k, t)-resilient function, then there exist a linear (n, k, t)-resilient function. The conjecture was disproved in article [34] by exhibiting an infinite class of counterexamples based on binary Kerdock codes.

In the next paragraphs we describe a general connection between the resilient functions and the codes (not necessarily linear) and apply it to binary Kerdock codes.

Resilient functions are closely related to a combinatorial structure called an orthogonal array. It forms a bridge between error-correcting codes and resilient functions.

Definition 4.2.2. An *orthogonal array* $\mathrm{OA}_\lambda(t, n, v)$ is a $\lambda v^t \times n$ array of v symbols, such that in any t columns of the array each of possible v^t ordered t-tuples of symbols occurs in exactly λ rows. An orthogonal array is said to be simple if no two rows are identical.

A large set of orthogonoal arrays $\mathrm{LOA}_\lambda(t, n, v)$ is a set of v^{n-t}/λ simple orthogonal arrays $\mathrm{OA}_\lambda(t, n, v)$ such that every possible n-tuple of symbols occurs in exactly one of the orthogonal arrays in the set.

The main usage of orthogonal arrays is in design of experiments. In terms of statistics, colums in an orthogonal array are often called factors since they represent the studied variables. Rows of an orthogonal array then corresponds to the particular observations or runs of an experiment.

A comprehensive source on orthogonal array theory is book [16]. In article [13], applications of orthogonal arrays in computer science and cryptography are summarized.

Now we formulate the first part of mentioned link and prove an equivalence between resilient functions and orthogonal arrays. The proof can be found in section 5 of article [14].

Theorem 4.2.3. *An (n, k, t)-resilient function is equivalent to a large set of orthogonal arrays* $\mathrm{LOA}_{2^{n-k-t}}(t, n, 2)$.

Proof. First, let $f: \mathbb{F}_2^n \to \mathbb{F}_2^k$ be an (n, k, t)-resilient function. For any k-tuple $\mathbf{y} \in \mathbb{F}_q^k$, form an array $A_\mathbf{y}$ whose rows are vectors from $f^{-1}(\mathbf{y})$. $A_\mathbf{y}$ is then a $|f^{-1}(\mathbf{y})| \times n$ array of elements from $\mathbb{F}_2$ and each vector from the vector space $\mathbb{F}_2^n$ occurs in exactly one array $A_\mathbf{y}$. It is therefore sufficient to show that each array $A_\mathbf{y}$ is an orthogonal array $\mathrm{OA}_{2^{n-k-t}}(t, n, 2)$.

Let $\{i_1, \ldots, i_t\} \subseteq \{1, \ldots, n\}$ be a t-subset, and let $z_j \in \mathbb{F}_2$, $1 \leq j \leq t$, be fixed elements. For every vector $\mathbf{y} \in \mathbb{F}_2^k$, let $\lambda_\mathbf{y}$ denotes a number of rows in the array $A_\mathbf{y}$ in which z_j occurs in the column i_j for all $1 \leq j \leq t$.

Since $\lambda_\mathbf{y}$ expresses the number of vectors $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ from $f^{-1}(\mathbf{y})$ with $x_{i_j} = z_j$ for all $1 \leq j \leq t$, and 2^{n-t} is the number of all vectors from $\mathbb{F}_2^n$ that satisfy the required equations, we can use the Bayes formula for the conditional probability and we get for all $\mathbf{y} \in \mathbb{F}_2^k$

$$P(f(x_1, \ldots, x_n) = (y_1, \ldots, y_k) \mid x_{i_j} = z_j, 1 \leq j \leq t) = \frac{\frac{\lambda_\mathbf{y}}{2^n}}{\frac{2^{n-t}}{2^n}} = \frac{\lambda_\mathbf{y}}{2^{n-t}}. \tag{4.28}$$

Moreover, since f is an (n, k, t)-resilient function we have for all $\mathbf{y} \in \mathbb{F}_2^k$

$$P(f(x_1, \ldots, x_n) = (y_1, \ldots, y_k) \mid x_{i_j} = z_j, 1 \leq j \leq t) = \frac{1}{2^k}. \tag{4.29}$$

The previous two equations imply that

$$\lambda_\mathbf{y} = \frac{2^{n-t}}{2^k} = 2^{n-t-k} \tag{4.30}$$

for all $\mathbf{y} \in \mathbb{F}_2^k$.

We have shown that the number $\lambda_\mathbf{y}$ is independent on a choice of a vector $\mathbf{y} \in \mathbb{F}_2^k$ and it is also independent on particular choices of coordinates $i_1, \ldots, i_t$

and elements z_j, $1 \leq j \leq t$. Therefore the arrays $A_{\mathbf{y}}$, $\mathbf{y} \in \mathbb{F}_2^k$ form a set of 2^k orthogonal arrays $\mathrm{OA}_{2^{n-k-t}}(t, n, 2)$ and the first implication is proved.

Conversely, suppose that we have the large set $\mathrm{LOA}_{2^{n-k-t}}(t, n, 2)$ of orthogonal arrays. The set contains $\frac{2^{n-t}}{2^{n-k-t}} = 2^k$ arrays that can be denoted by $A_{\mathbf{y}}$, $\mathbf{y} \in \mathbb{F}_2^k$. Now define a function $f: \mathbb{F}_2^n \to \mathbb{F}_2^k$ by an equivalence

$$f(x_1, \ldots, x_n) = (y_1, \ldots, y_m) \Longleftrightarrow (x_1, \ldots, x_m) \in A_{(y_1,\ldots,y_m)} \tag{4.31}$$

for all $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$.

Let $\{i_1, \ldots, i_t\} \subseteq \{1, \ldots, n\}$ be a t-subset, and let $z_j \in \mathbb{F}_2$, $1 \leq j \leq t$, be fixed elements and $\mathbf{y} \in \mathbb{F}_2^k$ be a fixed vector. Now we calculate the probability $P(f(x_1, \ldots, x_n) = (y_1, \ldots, y_k) \mid x_{i_j} = z_j, 1 \leq j \leq t)$. We again use the Bayes formula and explain the required conditional probability as a quotient of a joint probability of events and a probability of condition. From basic probability theory and the definition of orthogonal array follows that

$$\begin{aligned}
&P(f(x_1, \ldots, x_n) = (y_1, \ldots, y_k) \ \&\ x_{i_j} = z_j, 1 \leq j \leq t) \\
&\quad = P((x_1, \ldots, x_n) \in A_{(y_1,\ldots,y_k)} \ \&\ x_{i_j} = z_j, 1 \leq j \leq t) \\
&\quad = P((x_1, \ldots, x_n) \in A_{(y_1,\ldots,y_k)} \ \&\ v_{i_j} = z_j, 1 \leq j \leq t, \mathbf{v} = (v_1, \ldots, v_n)) \\
&\quad = P((x_1, \ldots, x_n) \in A_{(y_1,\ldots,y_k)}) \cdot P(v_{i_j} = z_j, 1 \leq j \leq t, \mathbf{v} = (v_1, \ldots, v_n)) \\
&\quad = \frac{2^{n-k}}{2^n} \cdot \frac{2^{n-k-t}}{2^{n-k}} = \frac{2^{n-k-t}}{2^n}
\end{aligned} \tag{4.32}$$

and

$$P(x_{i_j} = z_j, 1 \leq j \leq t, \mathbf{x} \in \mathbb{F}_2^n) = \frac{2^{n-t}}{2^n}. \tag{4.33}$$

Therefore we have

$$P(f(x_1, \ldots, x_n) = (y_1, \ldots, y_k) \mid x_{i_j} = z_j, 1 \leq j \leq t) = \frac{\frac{2^{n-k-t}}{2^n}}{\frac{2^{n-t}}{2^n}} = \frac{1}{2^k} \tag{4.34}$$

and the function f is (n, k, t)-resilient. □

Theory of resilient functions doesn't have to be restricted to the field $\mathbb{F}_2$, but we can define them in general as functions $\mathbb{F}_q^n \to \mathbb{F}_q^k$. The proof of the previous theorem can be then easily generalized and we get an equivalence between a (n, k, t)-resilient function over a field $\mathbb{F}_q$ and a large set of orthogonal arrays $\mathrm{LOA}_{q^{n-k-t}}(t, n, q)$.

Now we can formulate a necessary condition on an (n, K, d) error-correcting code C that provides an $(n, n-k, d'-1)$-resilient function, where $K = 2^k$ and d' is a dual distance of the code C defined in Section 3.2.2. The theorem was first proved in [34].

Theorem 4.2.4. *If there exists a systematic (n, K, d) code C having a dual distance d', then there is an $(n, n-k, d'-1)$-resilient function, where $K = 2^k$.*

Proof. Write codewords of C as rows of $K \times n$ array. Any set of $d'-1$ columns now contains each $d'-1$-tuple exactly $K/2^{d'-1}$ times. Therefore, we get an orthogonal array $\mathrm{OA}_\lambda(t, n, 2)$, where $t = d' - 1$ and

$$\lambda = \frac{K}{2^{d'-1}} = \frac{2^k}{2^{d'-1}} = 2^{k-d'+1}. \tag{4.35}$$

Since C is systematic, we can assume without loss of generality that information bits correspond to the first k coordinates.

For any possible $(n-k)$-tuple $\mathbf{z} = (z_1, \ldots, z_{n-k}) \in \mathbb{F}_2^{n-k}$ we denote by $C_\mathbf{z}$ a set of vectors from $\mathbb{F}_2^n$ obtained from C by adding a vector $(0, \ldots, 0, z_1, \ldots, z_{n-k})$ to each codeword. The set $C_\mathbf{z}$ is then a simple orthogonal array $\mathrm{OA}_{2^{k-d'+1}}(d'-1, n, 2)$.

Moreover, a set of arrays $\{C_\mathbf{z};\, \mathbf{z} \in \mathbb{F}_2^{n-k}\}$ is a large set of orthogonal arrays $\mathrm{LOA}_{2^{k-d'+1}}(d'-1, n, 2)$ since all rows in the arrays $C_\mathbf{z}$, $\mathbf{z} \in \mathbb{F}_2^{n-k}$, are distinct.

From Theorem 4.2.3 it follows, that an $(n, n-k, d'-1)$-resilient function exists. □

If an (n, k, d)-code C is linear, a set of orthogonal arrays from the proof correspond precisely to cosets of the code C.

Since the binary Kerdock code $\mathcal{K}(m)$ is a systematic code of length $n = 2^m$ with $K = 2^{2m}$ codewords and dual distance d' equal to 6 (see Sections 1.3 and 3.2.2), assumptions of the previous theorem are satisfied. Therefore, we can apply it to the code $\mathcal{K}(m)$ and for all even $m \geq 4$ we obtain a $(2^m, 2^m - 2m, 5)$-resilient function.

Theorem 4.2.5. *Let $m \geq 4$ be an even integer. Then there exist a nonlinear $(2^m, 2^m - 2m, 5)$-resilient function.*

Proof. An existence of desired resilient function is a direct consequence of Theorem 4.2.4 and paramaters of the binary Kerdock codes. □

By an application of Theorem 4.2.4 on the Preparata codes $\mathcal{P}(m)$, $m \geq 4$ even, we get a $(2^m, 2m, 2^{m-1} - 2^{(m-2)/2} - 1)$-resilient function.

Conclusion

The main goal of the previous chapters was to show that the Kerdock codes are not interesting only for their capability of correcting errors but that they also interfere to many other areas of mathematics that are not on the first sight related to the theory of error-correcting codes.

This thesis contains applications of Kerdock codes in orthogonal geometry, combinatorial mathematics and cryptography.

We have shown that the algebraic structure defining these codes is equivalent with a structure from orthogonal geometry called orthogonal spread. Then we confirmed that there exist five infinite sets of 3-designs based on the Kerdock codes in their binary and quaternary form. Finally, we used the algebraic structure of Kerdock codes to construction of two different types of cryptographically interesting functions.

After all, the list of applications of Kerdock codes is still not complete. Recently, the Kerdock codes were used in communication theory to coding wireless communication between multiple senders and multiple receivers. This topic is not included in the thesis since the application is related mainly to physical properties on transmission channel or implementation of coding algorithm but not to underlying algebraic structures.

Although the Kerdock codes are intensively studied for 40 years, they still aren't fully examined. There are formulated several open problems related to Kerdock codes. The first one concerns existence or nonexistence of linear code with the same parameters as the Kerdock code. Nonexistence of such linear code is proven only for the Nordstrom-Robinson code $\mathcal{NR} = \mathcal{K}(4)$. For $m > 4$ there exists a conjecture about the nonexistence of such linear code, but it is still not proven.

The second open problem is related to calculation of the covering radius of the Kerdock code $\mathcal{K}(m)$ for even $m > 4$. Similarly as the previous problem the covering radius of the Nordstrom-Robinson code $\mathcal{NR}$ is known but for $m > 4$ we have only upper and lower bounds that help us to estimate the covering radius but the exact value is in general case unknown.

I am sure that in the following years the Kerdock codes will serve as a base for many other applications mainly in computer science and communication theory.

Bibliography

[1] Andrade, A. A. de, Palazzo, R. Jr.. *Linear Codes over Finite Rings*. TEMA Tend. Mat. Apl. Comput., 6, No. 2, (2005), 207–217.

[2] Ball, Simeon, Weiner, Zsuzsa.. *An Introduction to finite geometry*. Lecture Notes, (2011). Published at http://www-ma4.upc.es/ simeon/IFG.pdf

[3] Bennet, C. H., Brassard, G., Robert, J. M.. *Privacy amplification by public discussion*. SIAM J. on Computing, 17, 210–229, (1988).

[4] Bierbrauer, Juergen. *Finite geometries*. Published at http://www.math.mtu.edu/ jbierbra/HOMEZEUGS/finitegeom04.ps.

[5] Bonnecaze, A., Rains, E., Solé, P.. *3-Colored 5-designs and Z4-codes*, J. Stat. Plann. Inference, (1998).

[6] Calderbank, A. R., Cameron, P. J., Kantor, W. M., Seidel, J. J.. *Z4-Kerdock codes, orthogonal spreads and extremal euclidean line-sets*. Proceedings of The London Mathematical Society, (1997).

[7] Cameron, Peter J.. *Finite Geometry and Coding Theory*. Socrates Lecture Notes, (1999). Published at http://dwispc8.vub.ac.be/Potenza/lectnotes.html.

[8] Carlet, C.. *Boolean Functions for Cryptography and Error Correcting Codes*. to appear as a chapter of the monography Boolean methods and models, Cambridge University Press (Ed. Peter Hammer and Yves Crama).

[9] Chor, B., et al.. *The bit extraction problem or t-resilient functions*. 26th IEEE Symposium on Foundations of Computer Science, 396–407, (1985).

[10] Colbourn, C. J., Dinitz, J. H.. *Handbook of combinatorial designs*. Taylor & Francis, (2006). ISBN 9781584885061.

[11] Conway, J. H., Sloane, N. J. A.. *Self dual codes over the integers modulo 4*. Academic Press, Inc., (1993). ISSN 0097-3165.

[12] Duursma, I., et al.. *Split Weight Enumerators for the Preparata Codes with Applications to Designs*. Designs, Codes and Cryptography, 18, 103–124, (1999).

[13] Gopalakrishnan, K., Stinson, D. R., *Applications of orthogonal arrays to computer science*. Proc. of ICDM, 149–164, (2006).

[14] Gopalakrishnan, K., Stinson, D. R.. *Three characterizations of non-binary correlation-immune and resilient functions*. Netherlands: Springer, (1995).

[15] Hammons, A. R., Kumar, P. V., Calderbank, A. R.. *The Z4-1inearity of Kerdock, Preparata, Goethals, and related codes*. IEEE Trans. on Inform. Theory, (1994).

[16] Hedayat, A. S., Sloane, N. J. A., Stufken, John. *Orthogonal Arrays: Theory and Applications*. Springer, (1999).

[17] Helleseth, T., Rong, Chunming., Yang, Kyeongcheol.. *On t-designs from codes over Z4.*. Discrete Mathematics, 238, 67–80, (2001).

[18] Helleseth, T., Klove, T., Mykkeltveit, J.. *On the Covering Radius of binary codes*. IEEE Transactions on Information Theory, 5, (1978).

[19] Johnson, N., Jha, V., Biliotti, M.. *Handbook of Finite Translation Planes*. Taylor & Francis, (2007). ISBN 9781584886051.

[20] Kantor, W. M.. *Codes, Quadratic Forms and Finite Geometries*, Proceedings of Symposia in Applied Mathematics, (1995).

[21] Kerdock, A. M.. *A class of low-rate nonlinear binary codes*. Inform. Control, (1972).

[22] Kumar, P. V., Helleseth, T., Calderbank, A. R.. *An upper bound for Weil exponential sums over Galois rings and applications*. IEEE Transactions on Information Theory, 41, 456–468, 2, (1995).

[23] Lerman, E.. *Symplectic geometry and Hamiltonian systems*. Berkeley, (1989). Published at www.math.uiuc.edu/ lerman/467/v3.pdf.

[24] Lint, J. H. van. *Kerdock and Preparata codes*. Congressus Numerantium, (1983).

[25] Logachev, O. A., Salnikov, A. A., Yashchenko, V. V.. *Boolean Functions in Coding Theory and Cryptography*. American Mathematical Society, (2012). ISBN 9780821846803.

[26] MacWilliams, F. J., Sloane, N. J. A.. *The theory of error-correcting codes*. North-Holland Pub. Co., (1978). ISBN 9780444851932.

[27] Menezes, Alfred J., Vanstone, Scott A., Oorschot, Paul C. Van. *Handbook of Applied Cryptography*, CRC Press, Inc., (1996), ISBN 0849385237.

[28] Munemasa, Akihiro. *The geometry of orthogonal groups over finite fields*. Lecture Note in Mathematics, 3, Sophia University, Tokyo, Japan, (1996).

[29] Mykkeltveit, J.. *A Note on Kerdock Codes*. Deep Space Network Progress Report, (1972).

[30] Rise, Michael, Tretter, Steven, Mathys, Peter.. *On Differentially Encoded M-Sequences*. IEEE Transactions on Communications, (2001).

[31] Shin, Dong-joon. Kumar, P. V. Helleseth, T.. *An Assmus-Mattson type approach for idetifying 3-designs from linear codes over Z4*. Kluwer Academic Publishers, (2004). ISSN 0925-1022.

[32] Siegenthaler, T.. *Decrypting a Class of Stream Ciphers Using Ciphertext Only*. Washington, DC, USA, IEEE Computer Society, (1985). ISBN 0018-9340.

[33] Solov'eva, F., Tokareva, N.. *Distance regularity of Kerdock codes*. New York: Springer, (2008).

[34] Stinson, D. R., Massey, J. L.. *An infinite class of counterexamples to a conjecture concerning nonlinear resilient function*. Journal of Cryptology, 8, 167–173, (1995).

[35] Wan, Z. Wan, C.. *Quaternary codes*. World Scientific Pub., (1997).

[36] Yang, K., Helleseth, T.. *Two New Infinite Families of 3-Designs from Kerdock Codes over Z4*. Designs, Codes and Cryptography, 15, 201–214, (1998).

List of Tables