Abidin Kaya

M.S. Thesis In Mathematics

June 2011

EXTENDING REED MULLER CODES TO $F_2 + uF_2$

by

ABİDİN KAYA

June 2011

EXTENDING REED MULLER CODES TO $F_2 + uF_2$

by

ABİDİN KAYA

A thesis submitted to

the Graduate Institute of Science and Engineering

of

Fatih University

in partial fulfillment of the requirements for the degree of

Master of Science

in

Mathematics

June 2011
Istanbul, Turkey

APPROVAL PAGE

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

_____
Assist. Prof. Dr. Bahattin YILDIZ
Head of Department

This is to certify that I have read this thesis and that in my opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____	_____
Assist. Prof. Bahattin YILDIZ	Prof. İrfan ŞİAP
Advisor	Co-advisor

Examining Committee Members

Assist. Prof. Bahattin YILDIZ _____

Prof. İrfan ŞİAP _____

Assist. Prof. Tevfik BİLGİN _____

Prof. Feyzi BAŞAR _____

Assoc. Prof. Gürsel YEŞİLOT _____

It is approved that this thesis has been written in compliance with the formatting rules laid down by the Graduate Institute of Sciences and Engineering.

_____
Assoc. Prof. Nurullah ARSLAN
Director

June 2011

EXTENDING REED MULLER CODES TO $F_2 + uF_2$

Abidin Kaya

M. S. Thesis - Mathematics
June 2011

Supervisors: Assist. Prof. Bahattin Yıldız, Prof. İrfan Şiap

ABSTRACT

In this study, the main aim is to extend some well known binary and quaternary codes to the ring $F_2 + uF_2$. Reed-Muller, Goethals, Delsarte-Goethals Codes are extended, their properties and relations to binary and quaternary versions are studied. Polar codes of some specific dimensions are expressed algebraically. Linear codes obtained as the Gray images of codes over $F_2 + uF_2$ are compared with binary codes. We present a new algebraic method of obtaining Polar codes from codes over $F_2 + uF_2$.

.

Keywords: Reed Muller Codes, Polar Codes, Gray map, Codes over rings.

$F_2 + uF_2$ HALKASI ÜZERİNE REED MULLER KODLARI

Abidin Kaya

Yüksek Lisans Tezi - Matematik
June 2011

Tez yöneticileri: Yrd. Doç. Dr. Bahattin Yıldız, Prof.Dr. İrfan Şiap

ÖZ

Bu çalışmada temel amaç bilinen bazı ikili ve dörtlü kod ailelerini $F_2 + uF_2$ halkasına genişletmektir. Çalışmada Reed-Muller, Goethals, Delsarte-Goethals Codes kodları dolayısıyla Kerdock ve Preparata kodları da $F_2 + uF_2$ halkasına genişletilmiştir. Elde edilen kodların ve duallerinin özellikleri incelenmiş. Çalışmamızda iki hata doğrulayan ikili kod aileleri elde edilmiştir. Bunun yanında son zamanlarda önemli yer tutan bazı Polar kod ailelerini de yeni bir cebirsel yolla elde etme yöntemi sunuyoruz.

Anahtar Kelimeler: Reed-Muller kodları, Polar kodlar, gray, halkalar üzerine kodlar

DEDICATION

To my parents

ACKNOWLEDGEMENT

I am glad to take the opportunity to thank my supervisors Assist. Prof. Bahattin Yıldız, Prof. İrfan Şiap for their genuine help and encouragement throughout the research.

I would like to express my great appreciation to my colleagues and friends for their valuable guidance and comments on my academic problems.

Finally, I would like to thank my parents for their understanding, motivation and patience.

TABLE OF CONTENTS

LIST OF TABLES

TABLE

CHAPTER 1

Introduction

The main aim of coding theory is to correct errors on noisy communication channels. The history of error correcting codes started with the introduction of the Hamming codes in late 1940's, at about the same time as Shannon published his seminal paper "A mathematical theory of communication". Golay codes were invented in 1949.

In the early periods of Coding Theory, codes were usually taken over finite fields, especially over the field with two elements, such codes are called binary codes. Linear codes have been the most commonly studied types of codes since they are easy to construct, encode and decode. In 1970's, nonlinear codes like Nordstrom-Robinson, Preparata and Kerdock codes were constructed which have twice as many codewords as any linear code with the same parameters. In 1967, Nordstorm and Robinson constructed an optimum nonlinear binary code as in [26]. Preparata codes were introduced by [27] in 1968 and Kerdock codes were introduced by [17] in 1972. These codes also give 3-designs as noted in [19]. These codes gave rise to interest in nonlinear binary codes. In 1994, Hammons et al. published a paper [13] in which they showed well known non-linear binary Kerdock, Preparata and Delsarte-Goethals Codes can be obtained as Gray images of linear codes over $\mathbb{Z}_4$. This construction clarified a mystery about the relation between Kerdock and Preparata codes. This paper increased the interest in codes over rings especially the codes over

$\mathbb{Z}_4$ which are called quaternary codes.

1.1. Basic definitions

Let $\mathbb{F}_q^n$ be a vector space of dimension n over the Galois Field $\mathbb{F}_q$, where q is a prime power. A subset C of $\mathbb{F}_q^n$ is called a code of length n, C is also said to be an (n, M) code over $\mathbb{F}_q$ where M is the size of C. The elements of C are called codewords. The **Hamming distance** $d_H(v, w)$ between two words v and w is the number of coordinates in which $v = (v_{1,}v_2, \ldots, v_n)$ and $w = (w_1, w_2, \ldots, w_n)$ differ

$$d_H(v, w) = |\{i : 1 \leq i \leq n, v_i \neq w_i\}|.$$

The most common weight used in coding theory is the **Hamming weight** which is the number of non-zero coordinates of v denoted by $w_H(v)$, i.e.

$$w_H(v) = |\{i : 1 \leq i \leq n, v_i \neq 0\}|.$$

The **minimum distance of a code** is the smallest distance between two distinct words. i.e. the minimum distance of C is

$$d(C) = \min\{d(x, y) \mid x, y \in C,\ x \neq y\}$$

and the **minimum weight of a code** C is

$$w(C) = \min\{w(x) \mid x \in C,\ x \neq 0\}.$$

A code C with minimum distance d can detect up to $d - 1$ errors and can correct up to $e = \left\lfloor \frac{d-1}{2} \right\rfloor$ errors.

The main part of our study is about Reed Muller codes over $\mathbb{F}_2 + u\mathbb{F}_2$ which

is a ring of characteristic 2 with 4 elements;

$$\mathbb{F}_2 + u\mathbb{F}_2 = \left\{a + bu \mid a,\ b \in \mathbb{F}_2,\ u^2 = 0\right\}$$

and it is easily seen that $\mathbb{F}_2 + u\mathbb{F}_2 \simeq \mathbb{F}_2[x]/(x^2)$. It is a local ring with unique maximal ideal (u). It has the following addition and multiplication table

$+$	0	1	u	$1+u$
0	0	1	u	$1+u$
1	1	0	$1+u$	u
u	u	$1+u$	0	1
$1+u$	$1+u$	u	1	0

Table 1 Addition table for $\mathbb{F}_2 + u\mathbb{F}_2$

$\times$	0	1	u	$1+u$
0	0	0	0	0
1	0	1	u	$1+u$
u	0	u	0	u
$1+u$	0	$1+u$	u	1

Table 2 Multiplication table for $\mathbb{F}_2 + u\mathbb{F}_2$

Cyclic and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ are studied extensively in [8], [9] and [1].

1.2. Linear codes

A **linear code over a field** $\mathbb{F}_q$ of length n is a k-dimensional subspace of $\mathbb{F}_q^n$ which is called an $[n, k]$ code. A **generator matrix** G for a linear code C is a k by n matrix for which the rows are a basis of C.

An advantage of working with linear codes is that the minimum distance and the minimum weight of a linear code are equal since $d(v, w) = w(v - w)$, $d(C) = w(C)$ for linear codes. This reduces the complexity of finding the minimum distance.

Two linear codes C and C' are said to be permutationally equivalent if one can be obtained from the other by a permutation of the coordinates. A generator matrix G is a $k \times n$ matrix whose row space is G.

$$C = \left\{xG : x \in \mathbb{F}_q^k\right\}$$

and a **parity check matrix** H is a $n-k \times n$ matrix whose null space is C. i.e.

$$C = \left\{ v \in \mathbb{F}_q^n : Hv^T = 0 \right\}$$

The code generated by the parity check matrix H is called the dual of C and is denoted by $C^\perp$, which is an $[n, n-k]$ code.

$$C^\perp = \left\{ v \in \mathbb{F}_q^n : \langle u, v \rangle = 0, \forall u \in C \right\}$$

A code C is **self-orthogonal** provided $C \subseteq C^\perp$ and **self-dual** provided $C = C^\perp$. Binary codes for which all codewords have even weight are called even. It is called doubly even if all codewords have weight divisible by 4. A self-orthogonal code is even and a doubly even code is self-orthogonal. A self orthogonal code that is not doubly even is called singly even.

Let C be a linear code of length n and let A_i be the number of codewords of weight i. Then

$$A(z) := \sum_{i=0}^{n} A_i z^i$$

is called the weight enumerator of C. If C is an $[n, k]$ code with weight enumerator $A(z)$ then

$$B(z) := \frac{1}{|C|} (1+z)^n A\left(\frac{1-z}{1+z}\right)$$

is the weight enumerator of $C^\perp$. This identity is called Macwilliams identity.

A **linear code over a ring** R of length n is an R-submodule of R^n. A Gray map is a weight preserving map which takes a code over a ring to a code over a field.

A linear code over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \cdots + u^s\mathbb{F}_2$ is permutation equivalent to

a code with generator matrix

$$G = \begin{bmatrix} I_{k_1} & A_1 & A_2 & A_3 & \cdots & A_{s+1} \\ 0 & uI_{k_2} & uB_1 & uB_2 & \cdots & B_s \\ 0 & 0 & u^2 I_{k_3} & u^2 C_1 & \cdots & C_{s-1} \\ 0 & 0 & 0 & \ddots & & \vdots \\ 0 & 0 & 0 & 0 & u^s I_{k_s} & u^s D \end{bmatrix}$$

where I_{k_i} is the identity matrix of size k_i, B_j, C_r, .. are binary matrices and A_t are matrices over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 \cdots + u^s\mathbb{F}_2$.

For linear codes over rings the concept of dimension does not work but we can define its **type**. A linear code which has the above matrix G as its generating matrix is said to be of type

$$(2^s)^{k_1}(2^{(s-1)})^{k_2} \cdots (2)^{k_s}.$$

In this case we will have

$$|C| = 2^{sk_1+(s-1)k_2+\cdots+k_s}.$$

CHAPTER 2

Binary and Quaternary Reed Muller Codes

Binary Reed Muller codes are an important class of codes which includes the extended Hamming code. In 1954, I.S. Reed introduced this family of binary linear codes in [28] and in the same year in [23] D.E. Muller introduced an efficient decoding algorithm for these codes. They have interesting properties; Reed Muller codes are linked to design theory and as Forney showed in [11] they can be considered as codes on graphs. In addition, codes in this family have relatively simple and highly structured trellises.

2.1. Boolean functions

The first definition of Reed-Muller codes was given in terms of Boolean functions. Consider the polynomial ring of m variables over $\mathbb{F}_2$ $R_m = \mathbb{F}_2[x_0, x_1, \ldots, x_{m-1}]$.

Definition 2.1. [22] A Boolean monomial is an element $p \in R_m$ of the following form $p = x_0^{r_0} x_1^{r_1} \ldots x_{m-1}^{r_{m-1}}$ where $r_i \in \mathbb{N}$. A Boolean polynomial is an $\mathbb{F}_2$-linear combination of boolean monomials. A Boolean polynomial is simply an $\mathbb{F}_2$-linear combination of Boolean monomials; any element of R_m may be thought of as a Boolean polynomial.

Definition 2.2. [22] Given a Boolean monomial $p \in R_m$, we say that p is in reduced form if it is square-free. For any Boolean monomial $q \in R_m$, it is trivial to find the reduced form of q by applying:

$$x_i x_j = x_j x_i \text{ and } x_i^2 = x_i.$$

A Boolean polynomial in reduced form is an $\mathbb{F}_2$-linear combination of reduced form

Boolean monomials.

Consider mapping $\psi : R_m \to \mathbb{F}_2^{2^m}$ defined as follows:

$$\begin{aligned}
\psi(0) &= 0^{2^m} \\
\psi(1) &= 1^{2^m} \\
\psi(x_0) &= 1^{2^{m-1}} 0^{2^{m-1}} \\
\psi(x_1) &= 1^{2^{m-2}} 0^{2^{m-2}} 1^{2^{m-2}} 0^{2^{m-2}} \\
&\vdots \\
\psi(x_i) &= 1^{2^{m-i-1}} 0^{2^{m-i-1}} 1^{2^{m--1}} 0^{2^{m-i-1}} \dots 1^{2^{m--1}} 0^{2^{m-i-1}}
\end{aligned}$$

and the vector multiplication; $x*y = (x_1y_1, x_2y_2, \dots, x_ny_n)$ where $x = (x_1, x_2, \dots, x_n)$ and $y = (y_1, y_2, \dots, y_n)$.

For any monomial $p \in R_m$, $\psi(p) = \psi(x_1)*\psi(x_2)*\cdots*\psi(x_k)$ where $x_1x_2 \dots x_k$ is the reduced form of p.

Any polynomial $q \in R_m$ can be written as a sum of monomials $q = m_1 + m_2 + \cdots + m_l$. Then $\psi(q) = \psi(m_1) + \psi(m_2) + \cdots + \psi(m_l)$.

Proposition 2.1.1. [22] *ψ is a ring isomorphism from $(R_m, +, *)$ to $\left(\mathbb{F}_2^{2^m}, +, *\right)$.*

Definition 2.3. [22] The r-th order Reed-Muller code, denoted by $RM(r, m)$, is the set of all polynomials of degree at most r in the ring R_m. Alternatively through the isomorphism ψ, it may be thought of as a subspace of $\mathbb{F}_2^{2^m}$, i.e. a linear binary code of length 2^m.

2.2. Binary Reed Muller Codes

Alternatively a recursive definition may be given for binary Reed Muller codes as follows;

Definition 2.4. [16] The first order Reed Muller codes $RM\left(1,m\right)$ are binary codes defined, for all integers $m \geq 1$, recursively as follows:

$$RM\left(1,1\right) = \mathbb{F}_2^2$$

for $m \geq 1,\ RM\left(1,m+1\right) = \left\{(u,u) : u \in RM\left(1,m\right)\right\} \cup \left\{(u,u+\mathbf{1}) : u \in RM\left(1,m\right)\right\}.$

Definition 2.5. [16] The 0-th order Reed-Muller code $RM(0,m)$ is defined to be the repetition code $\{0,1\}$ of length $2m$. The *r-th* order Reed Muller code of length $2^m;\ RM\left(r,m\right), 2 \leq r \leq m$ is defined recursively by;

$$RM(r,m) = \{(u,u+v) : u \in RM(r,m-1), v \in RM(r-1,m-1)\} \text{ if } \ m > r$$
$$\text{and } \mathbb{F}_2^{2r} \text{ if } m = r.$$

Theorem 2.2.1. [16] *(The $(u,u+v)$-construction): Let C_i be an $[n,k,d]$- linear q-ary code for $i = 1,2$. Then the code C defined by, $C = \{(u,u+v) : u \in C, v \in C\}$ is a $[2n, k+k, min(2d,d)]$ linear q-ary code.*

Proposition 2.2.2. [16] *For $m > 0$, the Reed-Muller code $RM(1,m)$ is a binary $[2m, m+1, 2m-1]$ linear code, in which every codeword except 0 and 1 has weight 2^{m-1}.*

Proposition 2.2.3. [16] *If G_m is a generator matrix for $RM(1,m)$, then a generator matrix for $RM(1,m+1)$ is*

$$G_{m+1} = \begin{bmatrix} G_m & G_m \\ \mathbf{0} & \mathbf{1} \end{bmatrix}.$$

Theorem 2.2.4. [16] *If $G_{r,m}$ is a generator matrix of $RM(r,m)$ then a generator matrix for $RM(r+1,m+1)$ is given by*

$$G_{r+1,m+1} = \begin{bmatrix} G_{r+1,m} & G_{r+1,m} \\ \mathbf{0} & G_{r,m} \end{bmatrix}.$$

The dimension of $RM(r,m)$ is $1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$ which will be denoted as

$K_{r,m}$. *The minimum weight of* $RM(r,m)$ *is* 2^{m-r}.

We summarize the properties of binary Reed-Muller codes in the following lemma.

Lemma 2.1. [16] Let r, m be integers such that $0 \leq r \leq m$. Let $RM(r,m)$ be the r-th order Reed-Muller code then we have;

1. $RM(r-1,m) \subset RM(r,m)$, $\forall r \leq m$.
2. $RM(r,m)^{\perp} = RM(m-r-1,m)$, $\forall r < m$.
3. $RM(k,2k+1)$ is a self-dual binary $\left[2^{2k+1}, K_{k,2k+1}, 2^{k+1}\right]$ code.
4. $d(RM(r,m)) = 2^{m-r}$ and its dimension is $K_{r,m} = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$.
5. $RM(m-1,m)$ consists of all binary words of length 2^m that have even weight. Therefore, if $r < m$, $RM(r,m)$ contains code words of even weight only.
6. $RM(0,m)$ is a repetition code. $RM(1,m)$ is the dual of the extended Hamming code, $(H')^{\perp}$.
7. $RM(1,m) \subset K_m \subset RM(2,m)$, where K_m is the Kerdock code, m is even and $m \geq 4$.
8. $RM(m-3,m) \subset P_m \subset RM(m-2,m)$, where P_m is the Preparata code, m is even and $m \geq 4$.
9. $RM(m-2,m)$ is the extended Hamming code H'.
10. $RM(m,m) = F_2^{2^m}$.

2.3. Quaternary Codes

The interest in quaternary codes has grown tremendously since the prize winning paper [13], and they have been extensively studied in [32]. They are interesting since nonlinear binary classes of codes, such as; Kerdock and Preparata-like codes, are the Gray images of linear quaternary codes. Also optimum Nordstorm Robinson nonlinear code appears as the first member of these classes. Nordstorm Robinson code is also the Gray image of octacode as Forney et al. proved in [10].

A linear quaternary code $\mathcal{C}$ of block length n is a submodule of $\mathbb{Z}_4^n$, and it is

permutation equivalent to a quaternary code with generator matrix of the from

$$\begin{bmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2C \end{bmatrix}$$

where A and C are binary matrices and B is a matrix over $\mathbb{Z}_4$. $\mathcal{C}$ is of type $4^{k_1}2^{k_2}$ and obviously $|\mathcal{C}| = 2^{2k_1+k_2}$.

Definition 2.6. [13] The Gray map ϕ from ($\mathbb{Z}_4^n$, Lee weight) to ($\mathbb{Z}_2^{2n}$, Hamming weight) is defined as;

$$\begin{array}{rccc} \phi: & \mathbb{Z}_4 & \longrightarrow & \mathbb{Z}_2^2 \\ & 0 & \longmapsto & 00 \\ & 1 & \longmapsto & 01 \\ & 2 & \longmapsto & 11 \\ & 3 & \longmapsto & 10 \end{array} .$$

The following three maps α, β, γ from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ defined as follows;

$\mathbb{Z}_4$	α	β	γ
0	0	0	0
1	1	0	1
2	0	1	1
3	1	1	0

.

The Gray map can also be expressed in terms of β and γ as follows:

$$\phi(x) = (\beta(x), \gamma(x)) \text{ for all } x \in \mathbb{Z}_4.$$

Theorem 2.3.1. [13] *ϕ is a weight preserving map from ($\mathbb{Z}_4^n$, Lee weight) to ($\mathbb{Z}_2^{2n}$, Hamming weight), i.e.*

$$w_L(x) = w_H(\phi(x)) \text{ for all } x \in \mathbb{Z}_4$$

and ϕ is also distance preserving map from ($\mathbb{Z}_4^n$, Lee distance) to ($\mathbb{Z}_2^{2n}$, Hamming distance), i.e.

$$d_L(x,y) = d_H(\phi(x), \phi(y)) \text{ for all } x, y \in \mathbb{Z}_4.$$

Proposition 2.3.2. [13] *The binary image $C = \phi(\mathcal{C})$ of a $\mathbb{Z}_4$-linear code $\mathcal{C}$ is linear if and only if*

$$x, y \in \mathcal{C} \implies 2\alpha(x) * \alpha(y) \in \mathcal{C}.$$

Corollary 2.3.3. [32] *Let $\mathcal{C}$ be a $\mathbb{Z}_4$-linear code, $x_1, x_2, ..., x_m$ be a set of generators of $\mathcal{C}$, and $C = \phi(\mathcal{C})$. Then C is linear if and only if $2\alpha(x_i) * \alpha(x_j) \in \mathcal{C}$ for all i, j satisfying $1 \leq i \leq j \leq m$.*

2.3.1. Quaternary Kerdock Codes

In 1972, Kerdock introduced a class of nonlinear binary codes by [17]. Later it turned out that this family of codes is the Gray image of quaternary Kerdock codes.

Let $f(x)$ be a monic polynomial of degree $m \geq 1$ in $\mathbb{Z}_4[x]$. If $\overline{f}(x)$ is irreducible over $\mathbb{Z}_2$, then $f(x)$ is called a *basic irreducible polynomial* of degree m in $\mathbb{Z}_4[x]$. If $\overline{f}(x)$ is primitive of degree m over $\mathbb{Z}_2$, then $f(x)$ is called a *basic primitive polynomial* of degree m in $\mathbb{Z}_4[x]$.

Let m be any integer ≥ 2 and $h(x)$ be a basic irreducible primitive polynomial of degree m over $\mathbb{Z}_4$ such that $h(x) \mid \left(x^{2^m-1} - 1\right)$. Clearly $h(x)$ is the Hensel lift of the binary primitive polynomial $\overline{h}(x)$. Let $n = 2^m - 1$ and $g(x)$ be the reciprocal polynomial of the polynomial $(x^n - 1)/(x - 1)h(x)$.

Definition 2.7. [32] The shortened quaternary Kerdock code $\mathcal{K}(m)^-$ is the quaternary cyclic code of length $2^m - 1$ with generator polynomial $g(x)$. The positions of the coordinates of codewords of $\mathcal{K}(m)^-$ are numbered as $0, 1, 2, .., 2^m - 2$. The quaternary Kerdock code $\mathcal{K}(m)$ is the code obtained from $\mathcal{K}(m)^-$ by adding a zero-

sum check symbol to each codeword of $\mathcal{K}(m)^{-}$ at position ∞, which is situated in front of the position 0.

Proposition 2.3.4. [32] *Let* $\deg g(x) = \delta$, *then* $\delta = 2^m - m - 2$.*Let*

$$g(x) = g_0 + g_1 x + \cdots + g_\delta x^\delta,$$

where $g_i \in \mathbb{Z}_4$, *and let* $g_\infty = -(g_0 + g_1 + \cdots + g_\delta)$, *then the following* $(m+1) \times 2^m$ *matrix*

$$\begin{bmatrix} g_\infty & g_0 & g_1 & \cdots & \cdots & g_\delta & 0 & 0 & 0 \\ g_\infty & 0 & g_0 & g_1 & \cdots & \cdots & g_\delta & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & & & & \ddots & 0 \\ g_\infty & 0 & 0 & 0 & g_0 & g_1 & \cdots & \cdots & g_\delta \end{bmatrix}$$

is a generator matrix of $\mathcal{K}(m)$.

Proposition 2.3.5. [32] *Let* ξ *be a root of* $h(x)$ *in some extension ring of* $\mathbb{Z}_4$, *for instance, in* $GR(4^m)$. *Then the* $(m+1) \times 2^m$ *matrix*

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \cdots & \xi^{n-1} \end{bmatrix}$$

is also a generator matrix of $\mathcal{K}(m)$, *where the entries* $\xi^j \, (0 \le j \le n-1)$ *in the second row are to be replaced by the corresponding* m *tuples* $[a_{1j}, a_{2j}, \ldots, a_{mj}]^T$ *if* $\xi^j = a_{1j} + a_{2j}\xi + \cdots + a_{mj}\xi^{m-1}$.

Let m be an integer ≥ 2. Denote the binary image of the quaternary Kerdock code $\mathcal{K}(m)$ by $K(m)$, i.e. $K(m) = \phi(\mathcal{K}(m))$. Then we have

Theorem 2.3.6. [32] *Let* m *be an integer* ≥ 2. *Then* $K(m)$ *is a nonlinear binary code of length* 2^{m+1} *and with* 4^{m+1} *codewords. This code is distance invariant and all its codewords are of even weight.*

Proposition 2.3.7. [32] *Let* m *be an integer* ≥ 2. *Then the binary image of the*

linear subcode of $\mathcal{K}(m)$ *with generator matrix*

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 2 & 2\xi & 2\xi^2 & \dots & 2\xi^{n-1} \end{bmatrix}$$

is the first-order Reed-Muller code $RM(1, m+1)$ *contained in* $K(m)$.

Theorem 2.3.8. [32] *Let* m *be odd and* ≥ 3. *Then* $K(m) = K_{m+1}$, *binary Kerdock code.*

2.3.2. Quaternary Preparata Codes

In 1968, Preparata introduced in [27] Preparata codes which is an optimum double error correcting family of nonlinear binary codes. They were studied in [4], [27] and [30]. Quaternary Preparata codes as given below have Gray image Preparata-like codes.

Definition 2.8. [32] The $\mathbb{Z}_4$-cyclic code of length n with generator polynomial $h(x)$ is called the shortened quaternary Preparata code and denoted by $\mathcal{P}(m)^-$. The $\mathbb{Z}_4$-linear code obtained from $\mathcal{P}(m)^-$ by adding a zero-sum check symbol to each codeword of $\mathcal{P}(m)^-$ is called the quaternary Preparata code and denoted by $\mathcal{P}(m)$.

Proposition 2.3.9. [32] $\mathcal{P}(m)^-$ *has parity check matrix*

$$\begin{bmatrix} 1 & \xi & \xi^2 & \dots & \xi^{n-1} \end{bmatrix}.$$

$\mathcal{P}(m)$ *is the dual of* $\mathcal{K}(m)$ *and has parity check matrix*

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \xi & \xi^2 & \dots & \xi^{n-1} \end{bmatrix}.$$

Proposition 2.3.10. [32] *Let* m *be an integer* ≥ 2, *then all codewords of* $\mathcal{P}(m)$ *are of even Lee weight. Moreover, when* m *is even and* $\geq 2, \mathcal{P}(m)$ *has minimum Lee distance* 4 *and when* m *is odd and* $\geq 3, \mathcal{P}(m)$ *has minimum Lee distance* 6.

Denote the binary image of the quaternary Preparata code $\mathcal{P}(m)$ by $P(m)$, i.e. $P(m) = \phi(\mathcal{P}(m))$. Then we have

Theorem 2.3.11. [32] *Let m be an integer ≥ 2. $P(m)$ is a binary code of length 2^{m+1} and has $2^{2^{m+1}-2m-2}$ codewords. It is distance invariant, and all its codewords have even weight and is the formal dual of $K(m)$. Its weight enumerator is*

$$W_{P(m)}(X,Y) = \frac{1}{4^{m+1}} W_{K(m)}(X+Y, X-Y).$$

When $m \geq 3$, $P(m)$ is nonlinear. When m is even and ≥ 2, the minimum distance of $P(m)$ is 4 and when m is odd and ≥ 3, the minimum distance of $P(m)$ is 6.

Proposition 2.3.12. [32] *For odd $m \geq 5$, $P(m)$ is contained in a nonlinear code with the same weight distribution as the extended binary Hamming code of the same length, and the linear code spanned by the codewords of $P(m)$ has minimum weight 2.*

Proposition 2.3.13. [32] *The Preparata code P_{m+1} and the "Preparata" code $P(m)$ have the same length, the same number of codewords, the same minimum distance and the same weight enumerator.*

$P(m)$ is also called Preparata-like code.

For $m = 3$, Kerdock and Preparata-like codes coincide, i.e. $K(3) = P(3)$ and it is the Nordstorm-Robinson code which is an optimum binary code.

2.3.3. Quaternary Reed Muller codes

The quaternary Reed Muller codes were studied in detail in [13] and [7]. Kerdock and Preparata codes belong to this family of codes.

Definition 2.9. [13] QRM codes are defined over $\mathbb{Z}_4$ as follows, let m be an integer greater than 1 and $n = 2^m - 1$. Let $h(x)$ be a basic primitive polynomial over $\mathbb{Z}_4$ of order m dividing $x^n - 1$ and ξ be one of its roots ($h(x)$ is obtained by Hensel

lift). Then the m distinct roots of $h(x)$ are $\xi, \xi^2, \ldots, \xi^{2^{m-1}}$, and ξ is of order $2^m - 1$. Consider the $(m+1) \times 2^m$ matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & \xi & \xi^2 & \ldots & \xi^{n-1} \end{bmatrix}.$$

Here ξ^i corresponds to the column $[a_{1i}, a_{2i}, \ldots, a_{mi}]^T$ where

$$\xi^i = a_{1i} + a_{2i}\xi + \cdots + a_{mi}\xi^{m-1}.$$

Denote the ith row of the matrix by v_i $(i = 0, 1, 2, \ldots, m)$ are 2^m-tuples over Z_4 and v_0 is the all 1 2^m-tuple 1^{2^m}.The quaternary r-th order Reed-Muller code $QRM(r, m)$ is the code generated by all 2^m-tuples of the form

$$v_{i_1} v_{i_2} v_{i_3} \ldots v_{i_s},\ 1 \leq i_1 \leq i_2 \leq \ldots \leq i_s \leq m,\ 0 \leq s \leq r.$$

We agree that $v_{i_1} v_{i_2} \ldots v_{i_s} = 1^{2^m}$, when $s = 0$.

Proposition 2.3.14. [13] *$QRM(1, m) = \mathcal{K}(m)$ where $\mathcal{K}(m)$ is the quaternary Kerdock code.*

Example 2.3.1. *Let $m = 3$ and $h(x) = x^3 + 2x^2 + x - 1$ be a basic primitive polynomial of degree 3 over $\mathbb{Z}_4$ which is the Hensel lift of the binary polynomial $x^3 + x + 1$. Then we have*

$$\xi^3 = 2\xi^2 + 3\xi + 1$$
$$\xi^4 = 3\xi^2 + 3\xi + 2$$
$$\xi^5 = \xi^2 + 3\xi + 3$$
$$\xi^6 = \xi^2 + 2\xi + 1$$

where ξ is a root of $h(x)$. Then $QRM(1,3)$ is the $\mathbb{Z}_4$-code generated by

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

which can also be viewed as the extended cyclic code that is generated by $g(x) = x^3 + 2x^2 + x - 1$ i.e. the $\mathbb{Z}_4$-code generated by

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

For these parameters Kerdock and Preparata codes coincide $QRM(1,3) = \mathcal{K}(3) = \mathcal{P}(3)$ moreover it is the quaternary code octacode. Its gray image is the optimum non-linear binary $(16, 2^8, 6)$ Nordstorm-Robinson code as Forney showed in [10].

Proposition 2.3.15. [13] *$\alpha(QRM(r,m)) = RM(r,m)$ where α is modulo 2 map.*

Lemma 2.2. [13] The following 2^m-tuples over Z_4

$$v_{i_1} v_{i_2} v_{i_3} \dots v_{i_s},\ 1 \le i_1 \le i_2 \le \dots \le i_s \le m,\ 0 \le s \le m,$$

form a basis of the free $\mathbb{Z}_4$-module $\mathbb{Z}_4^{2^m}$.

Corollary 2.3.16. [32] *For $0 \le r \le m, QRM(r,m)$ is of type $4^{K_{r,m}}$, where*

$$K_{r,m} = 1 + \binom{m}{1} + \binom{m}{2} + \dots + \binom{m}{r}.$$

Proposition 2.3.17. [32] *Let m be an integer ≥ 2 and $0 \le r \le m-1$. Then*

$$QRM(r,m)^{\perp} = QRM(m-r-1, m).$$

In conclusion, properties of QRM codes are;

1. Under modulo 2 map (α) they are binary Reed-Muller codes;
   $\alpha\left(QRM\left(r,m\right)\right)=RM\left(r,m\right).$
2. First order QRM code is the quaternary Kerdock code; $QRM\left(1,m\right)=\kappa\left(m\right).$
3. $QRM\left(m-2,m\right)=\mathcal{P}\left(m\right)$, quaternary Preparata code.
4. $QRM\left(r,m\right)^{\perp}=QRM\left(m-r-1,m\right)$
5. Obviously, it is of type

   $4^{K_{r,m}}$, where $K_{r,m}=1+\binom{m}{1}+\binom{m}{2}+\cdots+\binom{m}{r}$.

2.3.4. Quaternary Goethals Codes

In 1972, Goethals introduced Goethals codes in [12] which is a family of three error correcting codes. They are also studied in [4].

Definition 2.10. [13] Let m be an odd integer ≥ 3 and ξ be an element of order 2^m-1 in the Galois ring $GR\left(4^m\right)$. The quaternary Goethals code $\mathcal{G}\left(m\right)$ of length 2^m is defined to be the $\mathbb{Z}_4-$linear code with parity check matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & \xi & \xi^2 & \ldots & \xi^{n-1} \\ 0 & 2 & 2\xi^3 & 2\xi^6 & \ldots & 2\xi^{3(n-1)} \end{bmatrix}$$

where $n=2^m-1$ and each $\xi^i\,(i\geq 0)$ is replaced by $[a_{1i},a_{2i},...,a_{mi}]^T$ where $\xi^i=a_{1i}+a_{2i}\xi+.....+a_{mi}\xi^{m-1}$. The columns of the matrix are numbered by $\infty,0,1,2,...,n-1$. If we delete the $\infty-$components of the codewords of $\mathcal{G}\left(m\right)$, the code thus obtained is called the shortened quaternary Goethals code and denoted by $\mathcal{G}\left(m\right)^{-}$.

Corollary 2.3.18. [13] *The quaternary Goethals code $\mathcal{G}\left(m\right)$ of length $2^m, m$ odd $\geq 3, m$ is of type $4^{2^m-2m-1}2^m$ and of minimal Lee distance 8.*

Corollary 2.3.19. [13] *The shortened quaternary Goethals code $\mathcal{G}\left(m\right)^{-}$ has parity*

check matrix

$$\begin{bmatrix} 1 & \xi & \xi^2 & \dots & \xi^{n-1} \\ 2 & 2\xi^3 & 2\xi^6 & \dots & 2\xi^{3(n-1)} \end{bmatrix}$$

and is a $\mathbb{Z}_4$-cyclic code of length $2^m - 1$, of type $4^{2^m-2m-1}2^m$ and of minimal Lee distance 7.

Proposition 2.3.20. [13] *Let m be an odd integer ≥ 3. The "Goethals" code $\phi(\mathcal{G}(m))$ is a binary code of length 2^{m+1}. It is distance invariant, and has $2^{2^{m+1}-3m-2}$ codewords and minimal Hamming distance 8. If $m \geq 5$, it is nonlinear; but $\phi(\mathcal{G}(3))$ is linear.*

2.3.5. Quaternary Delsarte-Goethals and Goethals-Delsarte Codes

Delsarte-Goethals codes were studied in [15]. The quaternary Goethals codes and its $\mathbb{Z}_4$-duals can be further generalized as follows,

Definition 2.11. [13] Let m be an odd integer $\geq 3, m = 2t+1, 1 \leq r \leq t$ and ξ be an element of order $n = 2^m - 1$ in Galois ring $GR(4^m)$. The quaternary Delsarte-Goethals code $\mathcal{DG}(m, \delta)$, where $\delta = \frac{m+1}{2} - r$, is the Z_4-linear code with generator matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \xi & \xi^2 & \dots & \xi^{n-1} \\ 0 & 2 & 2\xi^3 & 2\xi^6 & \dots & 2\xi^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 2 & 2\xi^{1+2^j} & 2\xi^{(1+2^j)2} & \dots & 2\xi^{(1+2^j)(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 2 & 2\xi^{1+2^r} & 2\xi^{(1+2^r)2} & \dots & 2\xi^{(1+2^r)(n-1)} \end{bmatrix}.$$

It is easily seen that this is a generalization of QRM.

The quaternary Goethals-Delsarte code $\mathcal{GD}(m,\delta)$ is the $\mathbb{Z}_4$-linear code with the matrix as its parity check matrix.

Denote the binary images of $\mathcal{DG}(m,\delta)$ and $\mathcal{GD}(m,\delta)$ by $\phi(\mathcal{DG}(m,\delta))$ and $\phi(\mathcal{GD}(m,\delta))$, respectively. Then we have

Proposition 2.3.21. [13] *Let m be an odd integer $\geq 3, m = 2t+1, 1 \leq r \leq t$ and $\delta = \frac{m+1}{2} - r$. Then the quaternary Delsarte-Goethals code $\mathcal{DG}(m,\delta)$ is of length 2^m and has type $4^{m+1}2^{rm}$ and minimum Lee weight $2^m - 2^{m-\delta}$. Its binary image $\phi(\mathcal{DG}(m,\delta))$ is the Delsarte-Goethals code $DG(m+1,\delta)$, which is a binary code of length 2^{m+1}, is distance invariant, and has $2^{2(m+1)+rm}$ codewords nad minimum Hamming distance $2^m - 2^{m-\delta}$. When $m \geq 5$, $DG(m+1,\delta)$ is nonlinear.*

Proposition 2.3.22. [13] *Let m be an odd integer $\geq 3, m = 2t+1, 1 \leq r \leq t$ and $\delta = \frac{m+1}{2} - r$. Then the Goethals-Delsarte $\mathbb{Z}_4$-code $\mathcal{GD}(m,\delta)$ is of length 2^m and has type $4^{2^m-(r+1)m-1}2^{rm}$ and minimum Lee weight 8. Its binary image $\phi(\mathcal{GD}(m,\delta))$ is a binary code of length 2^{m+1}, it has $2^{2^{m+1}-(r+2)m-2}$ codewords, and is distance invariant. It has the same weight distribution as the binary Goethals-Delsarte code $GD(m+1,\delta)$. When $m \geq 5, \phi(\mathcal{GD}(m,\delta))$ is nonlinear.*

Theorem 2.3.23. [22] *$DG(m,\delta)$, where $m = 2t+2 \geq 4$, is a code of length 2^m containing $2^{(2t+1)(t-\delta+2)+2t+3}$ codewords and having minimum distance $2^{2t+1} - 2^{2t+1-\delta}$. If $\delta = 1$, $DG(m,1) = RM(1,m)$, while for $2 \leq \delta \leq \frac{m}{2}$, $DG(m,\delta)$ is a nonlinear subcode of $RM(2,m)$.*

2.4. Polar codes

The idea of channel polarization is introduced by Prof. Arıkan in [2]. Polar codes are the first family of capacity achieving codes and they have many applications. Polar coding is a code construction method that can be used to construct capacity achieving codes on memoryless channels. As Arıkan showed in [3] with respect to some decoding algorithms they have lower decoding complexity compared to the Reed Muller codes. Polar coding may be considered as a generalization of Reed Muller coding. Non-binary version of polar codes are studied by Arıkan, Şaşoğlu, Telatar in [29].

Arıkan gives a heuristic construction for polar codes as follows:

Definition 2.12. [23] Let

$$F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

For any $N = 2^n, n \geq 1$ and $1 \leq K \leq N$ an (N, K) polar code is a linear code whose generator matrix $G_P(N, K)$ is a $K \times N$ submatrix of $F^{\otimes n}, n$th tensor power of F. It is not easy to understand Polar code construction, we use the following recursion and choose some rows of Kronecker product of the matrix; first we compute the vector $z_N = (z_{N,1}, z_{N,2}, .., z_{N,N})$ by recursion

$$z_{2k,j} = \begin{bmatrix} 2z_{k,j} - z_{k,j}^2 & \text{for } 1 \leq j \leq k \\ z_{k,j-k}^2 & \text{for } k+1 \leq j \leq 2k \end{bmatrix}$$

for $k = 1, 2, 2^2, ., 2^{n-1}$, with $z_{1,1} = 1/2$. Then we form a permutation $\pi_N = (i_1, i_2, \ldots, i_N)$ of $(1, 2, \ldots, N)$ so that for any $1 \leq j < k \leq N$, the inequality $z_{N,i_j} \leq z_{N,i_k}$ is satisfied. The generator matrix $G_P(N, K)$ for an (N, K) polar code is defined as the submatrix of $F^{\otimes n}$ consisting of the rows with indices $i_1, i_2, \ldots, i_K$.

Example 2.4.1. *For example, for $n = 3$ we get*

$$z_8 = (0.996, 0.684, 0.809, 0.121, 0.879, 0.191, 0.316, 0.004)$$

which gives $\pi_8 = (8, 4, 6, 7, 2, 3, 5, 1)$. Polar code picks the rows of $F^{\otimes 3}$ by the order given in π_8. So for $G_P(8, 5)$ we choose the $8, 4, 6, 7$ and 2nd rows of $F^{\otimes 3}$

$$G_P(8, 5) = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Polar codes prefer the rows with shorter span of 1s. For instance $G_P(8,5)$ prefers 2nd row of $F^{\otimes 3}$.

Efficient **construction for polar codes is given by Mori and Tanaka** recursively as follows:

Definition 2.13. [25] $G_N = B_N F^{\otimes n}$ for any $N = 2^n, n \geq 0$, B_N is a permutation matrix known as bit-reversal and can be computed recursively as: $B_N = R_N \left(I_2 \otimes B_{\frac{N}{2}} \right)$ where $B_2 = I_2$ and R_N is permutation matrix for reverse shuffle $(v_1, v_2, \ldots, v_N) R_N = (v_1, v_3, \ldots, v_{N-1}, v_2, v_4, \ldots, v_N)$.

Example 2.4.2. *By using the last recursive definition G_8 is obtained as follows;*

$$G_8 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Korada, Şaşoğlu and Urbanke defined the rate of polarization; *exponent* as follows:

Definition 2.14. [18] Given an $l \times l$ matrix $G = \left[g_1^T, g_2^T, ..., g_l^T \right]^T$. Partial distances $D_i,\ i = 1, 2, ..l$ are defined as

$$D_i = d\left(g_i, \langle g_{i+1}, g_{i+2}, \ldots, g_l \rangle\right), \text{ for } i = 1, 2, \ldots, l-1$$
$$D_l = d\left(g_l, 0\right)$$

and the rate of polarization, exponent of G is given by

$$E(G) = \frac{1}{l}\sum_{i=1}^{l} \log_l D_i \ .$$

Example 2.4.3. *The partial distances of the matrix*

$$G = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

are $d_1 = 1, d_2 = 2, d_3 = 2$. *Hence,* $E(G) = \frac{1}{3}(\log_3 1 + \log_3 2 + \log_3 2) = 0.42062$.

Korada, Şaşoğlu, Urbanke showed in [18] that the rate of polarization for binary matrices exceeds 0.5 at $l = 16$ i.e.

$$E_l = \max_{G \in \{0,1\}^{l \times l}} E(G)\,, \ E_l \leq \frac{1}{2}, \text{ for } l \leq 15 \text{ and } E_{16} = 0.51828.$$

2.5. Galois Ring Extension of $F_2 + uF_2$, $GR(R, m)$

This chapter introduces the main machinery, Galois rings, for the study of codes over $R = \mathbb{F}_2 + u\mathbb{F}_2$. Krull developed the theory of Galois rings. Galois rings are studied in detail in [31] and [32].

A polynomial $h(x)$ of degree m over $F_2 + uF_2$ is called a *basic irreducible polynomial* if it is a monic irreducible polynomial over $\mathbb{F}_2 + u\mathbb{F}_2$ such that $\overline{h}(x)$ is irreducible over $\mathbb{F}_2$ and that if $\overline{h}(x)$ is primitive, then $h(x)$ is called *basic primitive polynomial* over $F_2 + uF_2$.

There is a basic primitive polynomial of degree m over $F_2 + uF_2$ for any positive integer m. Let $h(x)$ be a basic irreducible polynomial of degree m over $\mathbb{F}_2 + u\mathbb{F}_2$.

Consider the residue class ring

$$R[x]/(h(x))$$

The residue classes

$$a_0 + a_1x + \cdots + a_{m-1}x^{m-1} + (h(x)),$$

where $a_0, a_1, .., a_{m-1} \in \mathbb{F}_2 + u\mathbb{F}_2$, are all distinct elements. Therefore $|\mathbb{F}_2 + u\mathbb{F}_2[x]/(h(x))| = 4^m$. The ring $\mathbb{F}_2 + u\mathbb{F}_2[x]/(h(x))$ is called the Galois ring over R and is denoted by $GR(R, m)$ which is unique for a given m.

Write $\xi = x + (h(x))$, then $h(\xi) = 0$, ξ is a root of $h(x)$, and the elements

$$a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1},$$

where $a_0, a_1, .., a_{m-1}$ runs through $\mathbb{F}_2 + u\mathbb{F}_2$ independently, are all distinct elements of $GR(R, m)$. Hence $GR(R, m) = \mathbb{F}_2 + u\mathbb{F}_2[\xi]$.

The group of units of $GR(R, m)$ denoted by

$$GR^*(R, m) = G_C \times G_A$$

where G_C is a cyclic group of order $2^m - 1$ and G_A is an Abelian group of order 2^m.

$$G_A = \{(1 + u\alpha) \mid \alpha \in \mathbb{F}_{2^m}\}.$$

Lemma 2.3. [31] The set $G_C \times \{0\}$ is isomorphic to the field $\mathbb{F}_{2^m}$.

Lemma 2.4. [31] The only ideals of $GR(R, m)$ are (0), (1) and (u).

Theorem 2.5.1. [31] *Let $h(x)$ be a basic irreducible polynomial of degree m over $\mathbb{F}_2 + u\mathbb{F}_2$. Then the residue class ring $GR(R, m) = \mathbb{F}_2 + u\mathbb{F}_2[x]/(h(x))$ is a finite ring of characteristic 2 with 4^m elements. Write $\xi = x + (h(x))$, then $h(\xi) = 0$,*

every element of $GR(R,m)$ *can be written uniquely in the following form*

$$a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1},\ a_i \in F_2 + uF_2,\ 0 \le i \le m-1\ ,$$

and $GR(R,m) = \mathbb{F}_2 + u\mathbb{F}_2[\xi]$. *Moreover, the ideal* (u) *of* $\mathbb{F}_2 + u\mathbb{F}_2[\xi]$ *is the unique maximal ideal which consists of all the zero divisors together with the zero element. Write* $\overline{\xi} = x + \left(\overline{h}(x)\right)$, *then* $\overline{h}(\xi) = 0$ *and* $\mathbb{F}_2 + u\mathbb{F}_2[\xi]/(u) \simeq \mathbb{F}_2[\xi]$ *is the Galois field* $\mathbb{F}_{2^m}$.

In general, a Galois ring is defined to be a finite commutative ring R with identity such that the set of zero divisors of R with 0 added is a principal ideal (p) for some prime number p.

Proposition 2.5.2. [31] *Let* R *be a Galois ring whose zero divisors together with* 0 *form a principal ideal* (u) *for some prime* u. *Then* (u) *is the only maximal ideal of* R, $R/(u)$ *is a Galois field* $\mathbb{F}_{p^m}$ *for some positive integer* m, *and the characteristic of* R *is a power of* p.

Corollary 2.5.3. [31] *Any two Galois rings both of characteristic* 2 *and having the same number of elements are isomorphic.*

Theorem 2.5.4. [31] *In the Galois ring* $GR(R,m)$ *there exists a nonzero element* ξ *of order* $2^m - 1$, *which is a root of a basic primitive polynomial* $h(x)$ *of degree* m *over* $\mathbb{F}_2 + u\mathbb{F}_2$ *and* $GR(R,m) = \mathbb{F}_2 + u\mathbb{F}_2[\xi]$. *Moreover,* $h(x)$ *is the unique polynomial of degree* $\le m$ *over* $\mathbb{F}_2 + u\mathbb{F}_2$ *having* ξ *as a root. Let* $\tau = \left\{0, 1, \xi, \xi^2, \ldots, \xi^{2^m-2}\right\}$, *then any element* $c \in GR(R,m)$ *can be written uniquely as*

$$c = a + ub,\ a, b \in \tau.$$

The representation is called u*-adic representation of the element* $c \in GR(R,m)$, *which is a generalization of the multiplicative representation of the elements of* $\mathbb{F}_{2^m}$.

Corollary 2.5.5. [31] *Express any element* $c \in GR(R,m)$ *in the form*

$$c = a + ub,\ \textit{where } a, b \in \tau.$$

Then

1. all the elements c with $a \neq 0$ are invertible and form a multiplicative group of order $(2^m - 1)\, 2^m$, which is a direct product $\langle \xi \rangle \times \varepsilon$ where $\langle \xi \rangle$ is a cyclic group of order $2^m - 1$ generated by ξ and $\varepsilon = \{1 + ub \mid b \in \tau\}$ has the structure of an abelian group of type 2^m and is isomorphic to the additive group of $\mathbb{F}_{2^m}$.
2. All the elements with $a = 0$ are nilpotent, and they form the ideal (u) of $GR(R, m)$.
3. The order of c is a divisor of $2^m - 1$ if and only if $a \neq 0$ and $b = 0$.
4. Any element $\eta \in GR(R, m)$ of order $2^m - 1$ is of the form ξ^i, where $(i, 2^m - 1) = 1$ and is a root of a basic primitive polynomial of degree m over $\mathbb{F}_2 + u\mathbb{F}_2$ and $\tau = \left\{0, 1, \eta, \eta^2, \ldots, \eta^{2^m - 2}\right\}$.

Example 2.5.1. *Let* $m = 3$, $h(x) = x^3 + x + 1$, *and* $\xi = x + (h(x))$. *Then* $\mathbb{F}_2 + u\mathbb{F}_2[\xi] = GR(R, 3)$ *and* ξ *is an element of order* $2^3 - 1 = 7$. *We have*

$$\begin{aligned}
&\xi^0 = 1,\ \xi^1 = \xi,\ \xi^2 = \xi^2 \\
&\xi^3 = \xi + 1, \\
&\xi^4 = \xi^2 + \xi, \\
&\xi^5 = \xi^2 + \xi + 1, \\
&\xi^6 = \xi^2 + 1.
\end{aligned}$$

Therefore

$$\tau = \left\{0, 1, \xi, \xi^2, \xi + 1, \xi^2 + \xi, \xi^2 + \xi + 1, \xi^2 + 1\right\}.$$

$GR(R, 3) = \{a + ub \mid a, b \in \tau,\ u^2 = 0\}$ *is a ring with* 64 *elements.*

Corollary 2.5.6. [31] *Let* $c_1, c_2 \in \tau$, *and express*

$$c_1 + c_2 = a + ub, \quad a, b \in \tau,$$

Then

$$a = c_1 + c_2 + u\left(c_1 c_2\right)^{1/2},$$
$$b = \left(c_1 c_2\right)^{1/2},$$

where $\left(c_1 c_2\right)^{1/2}$ *denotes the unique element in* τ *such that* $\left(\left(c_1 c_2\right)^{1/2}\right)^2 = c_1 c_2$.

Corollary 2.5.7. [31] *Let* $c_1, c_2, .., c_k \in \tau$, *and express*

$$\sum_{i=1}^{k} c_i = a + ub, \quad a, b \in \tau,$$

then

$$a = \sum_{i=1}^{k} c_i + u \sum_{1 \le i < j \le k} \left(c_i c_j\right)^{1/2}$$
$$b = \sum_{1 \le i < j \le k} \left(c_i c_j\right)^{1/2}$$

Automorphisms of $GR\left(R, m\right)$;

The Frobenius map of the Galois field $\mathbb{F}_{2^m}$

$$f_2 : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_{2^m}$$
$$a \mapsto a^2$$

can be generalized to $GR\left(R, m\right)$ as follows:

$$f : GR\left(R, m\right) \rightarrow GR\left(R, m\right)$$
$$c = a + ub \mapsto c^f = a^2 + ub^2$$

will be called the generalized Frobenius map of $GR\left(R, m\right)$.

Theorem 2.5.8. [31] *The generalized Frobenius map* f *of* $GR\left(R, m\right)$ *is a ring au-*

tomorphism of $GR(R,m)$, *the fixed elements of* f *are the elements of* $\mathbb{F}_2+u\mathbb{F}_2$, *and* f *is of order* m.

Theorem 2.5.9. [31] *Let* σ *be a ring of automorphism of* $GR(R,m)$, *then* $\sigma=f^i$ *for some* $i, 0\leq i\leq m-1$.

The cyclic group $\langle f\rangle$ generated by f is called the Galois group of $GR(R,m)$ over F_2+uF_2.

Recall that the trace map Tr from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ is defined by

$$Tr(a)=a+a^{f_2}+a^{f_2^2}+\cdots+a^{f_2^{m-1}} \text{ for all } a\in\mathbb{F}_{2^m}.$$

Define the generalized trace map T from $GR(R,m)$ to $\mathbb{F}_2+u\mathbb{F}_2$ by

$$Tr(c)=c+c^f+c^{f^2}+\cdots+c^{f^{m-1}} \text{ for all } c\in GR(R,m).$$

Proposition 2.5.10. [31] *We have*

1. $T(c+c')=T(c)+T(c')$ for all $c,c'\in GR(R,m)$,
2. $T(ac)=aT(c)$ for all $a\in F_2+uF_2$ and $c\in GR(R,m)$,
3. $\circ f=f_2\circ, i.e., \overline{c^f}=\overline{c}^{f_2}$for all $c\in GR(R,m)$,
4. $\circ T=Tr\circ, i.e., \overline{T(c)}=Tr(\overline{c})$ for all $c\in GR(R,m)$.

Moreover, T is a surjective map from $GR(R,m)$ to $\mathbb{F}_2+u\mathbb{F}_2$.

Proposition 2.5.11. [31] *Let* $h(x)$ *be a basic irreducible polynomial of degree* m *over* F_2+uF_2 *and* η *be a root of* $h(x)$ *in* $GR(R,m)$. *Then* $\eta,\eta^f,\eta^{f^2},...,\eta^{f^{m-1}}$ *are all distinct roots of* $h(x)$ *in* $GR(R,m)$ *and* $h(x)$ *has the following unique factorization into linear factors in* $GR(R,m)[x]$:

$$h(x)=(x-\eta)\left(x-\eta^f\right)\ldots\left(x-\eta^{f^{m-1}}\right).$$

In particular, if $h(x)$ *is a basic primitive polynomial of degree* m, $h(x)\mid\left(x^{2^m-1}-1\right)$

in $\mathbb{F}_2 + u\mathbb{F}_2 [x]$, *and* ξ *is a root of* $h(x)$ *in* $GR(R, m)$, *then* $\xi, \xi^2, \xi^{2^2}, .., \xi^{2^{m-1}}$ *are all distinct roots of* $h(x)$ *in* $GR(R, m)$ *and* $h(x)$ *has the unique factorization:*

$$h(x) = (x - \xi)\left(x - \xi^2\right) \ldots \left(x - \xi^{2^{m-1}}\right).$$

Proposition 2.5.12. [31] *Let* $\xi \in GR(R, m)$ *be such that both* ξ *and* $\bar{\xi}$ *are of order* $2^m - 1$. *Then*

1. $\xi^i + \xi^j$ is invertible for $0 \leq j < k < 2^m - 1$, where $m \geq 2$.
2. $\xi^i + \xi^j \neq \xi^k$ for distinct $i,\ j,\ k$ in $[0, 2^m - 2]$, where $m \geq 2$.
3. Assume that $m \geq 3$ and $i,\ j,\ k,\ l$ are in the range $[0, 2^m - 2]$ and $i \neq j, k \neq l$. Then

$$\xi^i + \xi^j = \xi^k + \xi^l \Leftrightarrow i = k \text{ and } j = l.$$

4. For odd $m \geq 3$,

$$\xi^i + \xi^j = 0 \Rightarrow i = j.$$

CHAPTER 3

Extending Reed-Muller codes to $\mathbb{F}_2 + u\mathbb{F}_2$

In this chapter, we extend the Reed-Muller codes to the ring $\mathbb{F}_2 + u\mathbb{F}_2$. In 1994, they were extended to $\mathbb{Z}_4$ as in [13], this quaternary version were also studied in detail in [7] and later they are extended to $\mathbb{Z}_q$ as in [33]. Type II, type IV and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ have been studied extensively in [8],[9]and[1] respectively. The ring $\mathbb{F}_2 + u\mathbb{F}_2$ is defined as the ring of characteristic 2 with 4 elements with the restriction $u^2 = 0$.

$$\mathbb{F}_2 + u\mathbb{F}_2 = \left\{ a + bu \mid a,\ b \in \mathbb{F}_2,\ u^2 = 0 \right\}$$

and it is easily seen that $\mathbb{F}_2 + u\mathbb{F}_2 \simeq \mathbb{F}_2 [x] / (x^2)$. Any code over $\mathbb{F}_2 + u\mathbb{F}_2$ is permutation equivalent to a code C with generator matrix

$$G = \begin{bmatrix} I_{k_1} & A & B_1 + uB_2 \\ 0 & uI_{k_2} & uD \end{bmatrix}$$

where $A,\ B_1,\ B_2$ and D are binary matrices.

3.1. Reed-Muller codes over $\mathbb{F}_2 + u\mathbb{F}_2$

Definition 3.1. A linear code C of length n over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ is an $\mathbb{F}_2 + u\mathbb{F}_2$-submodule of $(\mathbb{F}_2 + u\mathbb{F}_2)^n$.

Definition 3.2. Reed-Muller codes over $\mathbb{F}_2 + u\mathbb{F}_2$, denoted them by FRM are defined as follows, let m be an integer greater than 1 and $n = 2^m - 1$. Let $h(x)$ be a basic primitive polynomial over $\mathbb{F}_2 + u\mathbb{F}_2$ of order m dividing $x^n - 1$ and ξ be one of its roots.Then the m distinct roots of $h(x)$ are $\xi, \xi^2, ..., \xi^{2^{m-1}}$, and ξ is of order

$2^m - 1$. Consider the $(m+1) \times 2^m$ matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \xi & \xi^2 & \dots & \xi^{n-1} \end{bmatrix}.$$

Here ξ^i corresponds to the column $[a_{1i}, a_{2i}, ..., a_{mi}]^T$ where

$$\xi^i = a_{1i} + a_{2i}\xi + \cdots + a_{mi}\xi^{m-1}.$$

Denote the ith row of the matrix by v_i $(i = 0, 1, 2, ..., m)$ are 2^m-tuples over F_2+uF_2 and v_0 is the all 1 2^m-tuple 1^{2^m}.The r-th order Reed-Muller code $FRM\,(r, m)$ over $\mathbb{F}_2 + u\mathbb{F}_2$ is the code generated by all 2^m-tuples of the form

$$v_{i_1} v_{i_2} v_{i_3}, \dots, v_{i_s},\ 1 \le i_1 \le i_2 \le \dots \le i_s \le m,\ 0 \le s \le r$$

where $v_{i_1} v_{i_2}, \dots, v_{i_s} = 1^{2^m}$, when $s = 0$.

Obviously $FRM\,(r, m)$ is of type $4^{K_{r,m}}$, where $K_{r,m} = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$. We consider these codes with Lee weight

$$w\,(1) = w\,(1+u) = 1,\ w\,(u) = 2,\ w\,(0) = 0$$

and linear Gray map

$$\begin{aligned} \phi: \quad & \mathbb{F}_2 + u\mathbb{F}_2 \longrightarrow \mathbb{F}_2^2 \\ & a + bu \longmapsto (b, a+b)\ . \end{aligned}$$

Also a recursive definition maybe given as follows:

Definition 3.3. The 0-th order Reed-Muller code is defined to be the repetition code $\{0, 1\}$ of length $2m$. For any $0 \le r \le m$, the r-th order Reed-Muller code

$FRM(r,m)$ is defined recursively by;

$$FRM(r,m) = \{(u, u+v) : u \in FRM(r, m-1), v \in FRM(r-1, m-1)\} \text{ if } m > r$$
$$(\mathbb{F}_2 + u\mathbb{F}_2)^{2m} \text{ if } m = r.$$

Proposition 3.1.1. *If G_m is a generator matrix for $FRM(1,m)$, then a generator matrix for $FRM(1,m+1)$ is*

$$G_{m+1} = \begin{bmatrix} G_m & G_m \\ \mathbf{0} & \mathbf{1} \end{bmatrix}.$$

Proof. Follows from the construction as in the case of binary Reed Muller codes.

Theorem 3.1.2. *If $G_{r,m}$ is a generator matrix of $FRM(r,m)$ then a generator matrix for $FRM(r+1,m+1)$ is given by*

$$G_{r+1,m+1} = \begin{bmatrix} G_{r+1,m} & G_{r+1,m} \\ \mathbf{0} & G_{r,m} \end{bmatrix}.$$

The dimension of $FRM(r,m)$ is $K_{r,m} = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$.

Proof. Follows from the construction as in the case of binary Reed Muller codes.

3.2. Properties of FRM codes and their duals

Proposition 3.2.1. *FRM codes have the following properties;*

1. $FRM\,(r-1,m) \subset FRM\,(r,m)$
2. $FRM\,(r,m)^{\perp} = FRM\,(m-r-1,m)$
3. $FRM\,(k,2k+1)$ is self-dual with Gray image a $\left[2^{2k+2}, 2^{2k+1}, 2^{k+1}\right]$ binary

code.

4. $d\left(FRM\left(r,m\right)\right)=2^{m-r}$
5. The weight enumerator polynomial is symmetric.

Proof (1) Follows from the definition.

(2) Easily follows from the type of codes. Consider $r\leq m-r-1$

$FRM\left(r,m\right)\subseteq FRM\left(m-r-1,m\right)$ result follows from the generators,

$K_{r,m}+K_{m-r-1,m}=2^{m}$ implies $\left|FRM\left(r,m\right)\right|\left|FRM\left(m-r-1,m\right)\right|=4^{2^{m}}$ gives the result. Similarly for the case $r>m-r-1$.

(3) $\phi\left(FRM\left(r,m\right)\right)\subseteq RM\left(r+1,m+1\right)$ implies

$d\left(\phi\left(FRM\left(r,m\right)\right)\right)\geq d\left(RM\left(r+1,m+1\right)\right)=2^{m-r}$.

(4) Follows from all 1 binary codeword contained in $\phi(FRM\left(r,m\right))$.

(5) All 1 vector is in $FRM\left(r,m\right)$ follows from all 1 binary codeword contained in $\phi(FRM\left(r,m\right))$.

Proposition 3.2.2. *$FRM\left(1,m\right)$ has weight distribution*

weight	*# of codewords*
0	1
2^{m-1}	$4\left(2^{m}-1\right)$
2^{m}	$2^{2(m+1)}-2^{m+3}+6$
$2^{m+1}-2^{m-1}$	$4\left(2^{m}-1\right)$
2^{m+1}	1 .

Proof. Generator matrix of $FRM\left(1,m\right)$ has m minimum weight rows and their possible combinations also have minimum weight and there are $\binom{m}{1}+\binom{m}{2}+$

$\binom{m}{3}+....+\binom{m}{m} = 2^m-1$ such codewords. $(1+u)$ times these codewords, all 1 codeword + these codewords and $(1+u)$ times the previous one all have same weight. So there are at least $4\left(2^m-1\right)$ codewords of weight 2^{m-1}. $\phi\left(FRM\left(1,m\right)\right)$ has all 1 codeword and when we add it to the Gray images of the codewords above we get codewords of weight $2^{m+1}-2^{m-1}$. So $\#\left(c : w_H(c) = 2^{m-1}\right) = \#\left(c : w_H(c) = 2^{m+1}-2^{m-1}\right)$.

Example 3.2.1. *Let* $m = 3,\ h\left(x\right) = x^3+x+1$ *then* $FRM\left(1,3\right)$ *is the code over* $\mathbb{F}_2 + u\mathbb{F}_2$ *generated by*

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

is a $[2^3, 4^{1+3}, 2^{3-1}]$ *code over* $\mathbb{F}_2 + u\mathbb{F}_2$ *with weight enumerator* $1+28z^4+198z^8+28z^{12}+z^{16}$ *and it is self dual. Consider it's subcode generated by* $RM\left(0,3\right)$, $uRM\left(1,3\right)$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & u & 0 & 0 & u & 0 & u & u \\ 0 & 0 & u & 0 & u & u & u & 0 \\ 0 & 0 & 0 & u & 0 & u & u & u \end{bmatrix}$$

which has Gray image $RM\left(1,4\right)$. $FRM\left(2,3\right)$ *has generator matrix*

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

and similarly its Gray image has $RM\left(2,4\right)$ *as a subcode, consider the subcode gen-*

erated by $RM(1,3)$, $uRM(2,3)$ *i.e. with generator matrix*

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & u & 0 & u & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & u & u \\ 0 & 0 & 0 & 0 & 0 & u & u & 0 \end{bmatrix}$$

$$RM(1,4) \subset \phi(FRM(1,3)) \subset RM(2,4) \subset \phi(FRM(2,3)).$$

Let us consider the code $F_1RM(r,m) = \langle RM(r-1,m), uRM(r,m)\rangle$.

Theorem 3.2.3. *For any* $1 \leq r \leq m-1$, *we have*

$$\phi(F_1RM(r,m)) = RM(r,m+1).$$

Proof.

$$\begin{aligned} F_1RM(r,m) &= \langle RM(r-1,m), uRM(r,m)\rangle \\ &= \{a+bu \mid a \in RM(r-1,m),\ b \in RM(r,m)\}. \end{aligned}$$

$|F_1RM(r,m)| = 2^f$, where

$$\begin{aligned} f &= 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r-1} + 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r} \\ &= 1 + \left[\binom{m}{0} + \binom{m}{1}\right] + \cdots + \left[\binom{m}{r-1} + \binom{m}{r}\right] \\ &= 1 + \binom{m+1}{1} + \binom{m+1}{2} + \cdots + \binom{m+1}{r} = K_{r,m+1}. \end{aligned}$$

So, f is the dimension of $RM\left(r, m+1\right)$.

$$\begin{aligned}\phi\left(F_1RM\left(r,m\right)\right) &= \left\{\left(b, a+b\right) \mid b \in RM\left(r,m\right),\ a \in RM\left(r-1,m\right)\right\} \\ &= RM\left(r, m+1\right)\end{aligned}$$

by recursive definition.

Corollary 3.2.4. *The binary Reed-Muller codes $RM\left(r,m\right)$ are all $\mathbb{F}_2 + u\mathbb{F}_2$-linear for $0 \leq r \leq m$.*

$$RM\left(r, m+1\right) = \phi\left(F_1RM(r,m)\right) \subset \phi\left(FRM(r,m)\right) \subset RM\left(r+1, m+1\right).$$

Corollary 3.2.5. $F_1RM\left(r,m\right)^{\perp} = F_1RM\left(m-r,m\right)$, *for* $0 \leq r \leq m$.

Proof Follows immediately from

$$\phi\left(F_1RM\left(r,m\right)^{\perp}\right) = RM\left(r,m+1\right)^{\perp} = RM\left(m-r,m+1\right) = \phi\left(F_1RM\left(m-r,m\right)\right).$$

The binary $\phi\left(FRM(r,m)\right)$ codes can be considered as codes on graphs since it is a subcode of $RM\left(r+1,m+1\right)$.

3.3. Polar codes obtained from $\mathbb{F}_2 + u\mathbb{F}_2$

Obviously, in $F_1RM\left(r,m\right)$ weight 2^{m+1-r} rows of $RM\left(r,m+1\right)$ are expressed in two groups. We claim that a family of polar codes can be expressed as the gray image of the subcode $F_2RM\left(r,m\right) = \left\langle RM\left(r-2,m\right), uRM\left(r,m\right)\right\rangle$ of $F_1RM\left(r,m\right)$ therefore $FRM\left(r,m\right)$.

Example 3.3.1. $F_2RM\left(2,2\right) = \left\langle RM\left(0,2\right), uRM\left(2,2\right)\right\rangle$ *in other words the code*

generated by

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & u & 0 & u \\ 0 & 0 & u & u \\ 0 & 0 & 0 & u \end{bmatrix}$$

has gray image the Polar code $G_P(8,5)$.

Example 3.3.2. *The subcode of* $F_1RM(2,3)$ *therefore* $FRM(2,3)$ *that is generated by;*

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & u & 0 & 0 & u & 0 & u & u \\ 0 & 0 & u & 0 & u & u & u & 0 \\ 0 & 0 & 0 & u & 0 & u & u & u \\ 0 & 0 & 0 & 0 & u & 0 & u & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & u & u \\ 0 & 0 & 0 & 0 & 0 & u & u & 0 \end{bmatrix}$$

has gray image the Polar code $G_P(16,8)$.

$F_1RM(r,m) = \langle RM(r-1,m), uRM(r,m)\rangle$ has gray image $RM(r,m+1)$

$F_2RM(r,m) = \langle RM(r-2,m), uRM(r,m)\rangle$ has gray image the Polar code $G_P\left(2^{m+1}, K_{r,m} - \binom{m}{r-1}\right)$.

Conjecture. The gray image of $F_2RM(r,m) = \langle RM(r-2,m), uRM(r,m)\rangle$ is a polar code.

In $\phi(F_1RM(r,m)) = RM(r,m+1)$ weight 2^{m+1-r} generators are expressed in two different forms, weight 2^{m+1-r} rows of $F^{\otimes m+1}$, $G_P\left(2^{m+1}, K_{r,m+1} - \binom{m}{r-1}\right)$

$F_2RM(r,m)$ picks the even indexed rows of $F^{\otimes m+1}$, we expect proof may

follow from reverse shuffle permutation R_N ;

$$(v_1, v_2, \ldots, v_N)\, R_N = (v_1, v_3, \ldots, v_{N-1}, v_2, v_4, \ldots, v_N)\,.$$

3.4. Some specific codes over $\mathbb{F}_2 + u\mathbb{F}_2$

$\mathbb{F}_2 + u\mathbb{F}_2$ version of C_{10} is a $4^2 2^6$ type code generated by

$$\begin{bmatrix}
1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & u & 0 & 0 & 0 & 0 & 0 & 0 & u \\
0 & 0 & 0 & u & 0 & 0 & 0 & 0 & 0 & u \\
0 & 0 & 0 & 0 & u & 0 & 0 & 0 & 0 & u \\
0 & 0 & 0 & 0 & 0 & u & 0 & 0 & 0 & u \\
0 & 0 & 0 & 0 & 0 & 0 & u & 0 & u & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & u & u & u
\end{bmatrix}$$

has Gray image a binary $[20, 10, 4]$ (ub6) self-dual code with weight enumerator;

$$1 + 21x^4 + 48x^6 + 234x^8 + 416x^{10} + 234x^{12} + 48x^{14} + 21x^{16} + x^{20}.$$

The quaternary **octacode** O_8 is a special code with gray image Nordstorm-Robinson code, $\mathbb{F}_2 + u\mathbb{F}_2$ version of it is generated by

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 1 & u & 1 \\
0 & 1 & 0 & 0 & 1 & u & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & u \\
0 & 0 & 0 & 1 & u & 1 & 1 & 1
\end{bmatrix}$$

and has Gray image a $[16, 8, 4]$ (ub5) self-dual binary code with weight enumerator;

$$1 + 12x^4 + 64x^6 + 102x^8 + 64x^{10} + 12x^{12} + x^{16}.$$

Q_8

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & u & 0 & u & 0 & u & 0 & u \\ 0 & 0 & 0 & 0 & 0 & 0 & u & u \end{bmatrix}$$

gives a binary self dual $[16, 8, 4]$ (ub5) code which has the same weight enumerator with $FRM\,(1, 3)$;

$$1 + 28x^4 + 198x^8 + 28x^{12} + x^{16}.$$

$\mathbb{F}_2 + u\mathbb{F}_2$ version K_{4m} codes have self-dual binary codes as Gray images, for instance K_8 is the code generated by

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & u & 0 & 0 & 0 & 0 & 0 & u \\ 0 & 0 & u & 0 & 0 & 0 & 0 & u \\ 0 & 0 & 0 & u & 0 & 0 & 0 & u \\ 0 & 0 & 0 & 0 & u & 0 & 0 & u \\ 0 & 0 & 0 & 0 & 0 & u & 0 & u \\ 0 & 0 & 0 & 0 & 0 & 0 & u & u \end{bmatrix}$$

its Gray image is a $[16, 8, 4]$ self-dual binary linear code which has same weight enumerator with $FRM\,(1, 3)$.

K_{12} has Gray image a self-dual binary linear $[24, 12, 4]$ code with weight enu-

merator;

$$1 + 66x^4 + 495x^8 + 2972x^{12} + 495x^{16} + 66x^{20} + x^{24}.$$

In fact, the quaternary code K_{4m} satisfies the linearity criteria so $\mathbb{Z}_4$-code and $\mathbb{F}_2 + u\mathbb{F}_2$-code have the same binary image.

$\mathbb{F}_2 + u\mathbb{F}_2$ version of **hexacode** generated by

$$\begin{bmatrix} 1 & 0 & 0 & 1 & u & u \\ 0 & 1 & 0 & u & 1 & u \\ 0 & 0 & 1 & u & u & 1 \end{bmatrix}$$

is a self dual code with Gray image binary $[12, 6, 4]$ (ub4) self dual code with weight enumerator

$$1 + 15x^4 + 32x^6 + 15x^8 + x^{12}.$$

CHAPTER 4

Generalizations of Reed Muller codes over $\mathbb{F}_2 + u\mathbb{F}_2$

Quaternary Reed Muller codes are generalized to Goethals [12], [4] Delsarte-Goethals [15] and Goethals-Delsarte codes. In this chapter, we generalize the Reed Muller codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and define Goethals, Delsarte-Goethals and Goethals-Delsarte codes over $\mathbb{F}_2 + u\mathbb{F}_2$. We have seen that Goethals and shortened Goethals codes over $\mathbb{F}_2 + u\mathbb{F}_2$ are classes of double error correcting codes. Therefore we obtained double error correcting families of binary codes as the gray images of Goethals and shortened Goethals codes. Delsarte-Goethals and Goethals-Delsarte codes over $\mathbb{F}_2 + u\mathbb{F}_2$ did not give us interesting results. But a class of codes obtained from Delsarte-Goethals was interesting.

4.1. Goethals Codes over $\mathbb{F}_2 + u\mathbb{F}_2$

Definition 4.1. Let m be an odd integer ≥ 3 and ξ be an element of order $2^m - 1$ in the Galois ring $GR(R, m)$. The Goethals code $FG(m)$ of length 2^m is defined to be the $\mathbb{F}_2 + u\mathbb{F}_2$-linear code with parity check matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \xi & \xi^2 & \dots & \xi^{n-1} \\ 0 & u & u\xi^3 & u\xi^6 & \dots & u\xi^{3(n-1)} \end{bmatrix}$$

where $n = 2^m - 1$ and each ξ^i $(i \geq 0)$ is replaced by $[a_{1i}, a_{2i}, ..., a_{mi}]^T$ where $\xi^i = a_{1i} + a_{2i}\xi + \cdots + a_{mi}\xi^{m-1}$. The columns of the matrix are numbered by $\infty, 0, 1, 2, \dots, n-1$. If we delete the $\infty-$components of the codewords of $FG(m)$, the code thus obtained is called the shortened Goethals code over $\mathbb{F}_2 + u\mathbb{F}_2$ and denoted by $FG(m)^-$.

Proposition 4.1.1. *The Goethals code* $FG(m)$ *of length* $2^m, m \geq 5$ *is of type* $4^{2^m-2m-1}2^m$ *and of minimal Lee distance* 6, $d(FG(3)) = 8$.

Proof. $FG(m) \subseteq FRM(1,m)^{\perp} = FRM(m-2,m)$ which gives us $d(FG(m)) \geq d(FRM(m-2,m)) = 4$. Since all codewords of $FG(m)$ have even weight it is enough to show that it has no codeword of weight 4 and has a codeword of weight 6.

Corollary 4.1.2. *The shortened Goethals code* $FG(m)^{-}$ *has parity check matrix*

$$\begin{bmatrix} 1 & \xi & \xi^2 & \dots & \xi^{n-1} \\ u & u\xi^3 & u\xi^6 & \dots & u\xi^{3(n-1)} \end{bmatrix}$$

and is a $\mathbb{F}_2 + u\mathbb{F}_2$*-cyclic code of length* $2^m - 1$*, of type* $4^{2^m-2m-1}2^m$ *and of minimal Lee distance* 5 *for* $m \geq 5$.

4.2. Delsarte-Goethals and Goethals-Delsarte Codes over $\mathbb{F}_2 + u\mathbb{F}_2$

For any parameter quaternary Delsarte-Goethals codes are contained in the first order Reed-Muller subcode of Kerdock code and by Theorem 2.3.23 $\mathcal{DG}(m,1)$ has gray image the second order Reed Muller code. In other words, the corresponding quaternary codes has binary images which are nonlinear subcodes of the second order Reed Muller code which contain the first order Reed Muller code. But in our case the binary image is linear so we obtaine linear codes between the corresponding RM codes.

Definition 4.2. Let m be an odd integer $\geq 3, m = 2t+1, 1 \leq r \leq t$ and ξ be an element of order $n = 2^m - 1$ in Galois ring $GR(R,m)$ .The Delsarte-Goethals code over $\mathbb{F}_2 + u\mathbb{F}_2$, $FDG(m,\delta)$, where $\delta = \frac{m+1}{2} - r$, is the $\mathbb{F}_2 + u\mathbb{F}_2$-linear code with

generator matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \xi & \xi^2 & \dots & \xi^{n-1} \\ 0 & u & u\xi^3 & u\xi^6 & \dots & u\xi^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & u & u\xi^{1+2^j} & u\xi^{\left(1+2^j\right)2} & \dots & u\xi^{\left(1+2^j\right)(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & u & u\xi^{1+2^r} & u\xi^{(1+2^r)2} & \dots & u\xi^{(1+2^r)(n-1)} \end{bmatrix}$$

The Goethals-Delsarte code $FGD\left(m,\delta\right)$ is the $\mathbb{F}_2+u\mathbb{F}_2$-linear code with the matrix as its parity check matrix. Denote the binary images of $FDG\left(m,\delta\right)$ and $FGD\left(m,\delta\right)$ by $\phi\left(FDG\left(m,\delta\right)\right)$ and $\phi\left(FGD\left(m,\delta\right)\right)$, respectively. Then we have:

Proposition 4.2.1. *Let m be an odd integer $\geq 3, m = 2t+1, 1 \leq r \leq t$ and $\delta = \frac{m+1}{2} - r$. Then the Delsarte-Goethals code $FDG\left(m,\delta\right)$ is of length 2^m and has type $4^{m+1}2^{rm}$ and minimum Lee weight 2^{m-1}. For $r = \frac{m-1}{2}$ its gray image is the same as $RM(2, m+1)$.*

Proposition 4.2.2. *Let m be an odd integer $\geq 3, m = 2t+1, 1 \leq r \leq t$ and $\delta = \frac{m+1}{2} - r$. Then the Goethals-Delsarte code $FGD\left(m,\delta\right)$ is of length 2^m and has type $4^{2^m-(r+1)m-1}2^{rm}$ and minimum Lee weight 4.*

Example 4.2.1. *Let $m = 3,\ h\left(x\right) = x^3 + x + 1$ then $FDG\left(3,1\right)$ is the code over $\mathbb{F}_2 + u\mathbb{F}_2$ generated by*

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & u & u & u & 0 & u & 0 & 0 \\ 0 & 0 & u & 0 & 0 & u & u & u \\ 0 & 0 & 0 & u & u & u & 0 & u \end{bmatrix}$$

is a $[2^3, 4^4 2^3, 4]$ *code over* $\mathbb{F}_2 + u\mathbb{F}_2$ *with weight enumerator*

$$1 + 140z^4 + 448z^6 + 870z^8 + 448z^{10} + 140z^{12} + z^{16}.$$

The Gray image of this code is a binary $[16, 11, 4]$ *code which has the best known distance.*

Definition 4.3. Let m be an odd integer ≥ 3, $\delta = \frac{m+1}{2} - r$. Let $IFDG(m, \delta)$ be the code generated by

$$\begin{bmatrix}
1 & 1 & 1 & 1 & \dots & 1 \\
0 & u & u\xi & u\xi^2 & \dots & u\xi^{n-1} \\
0 & u & u\xi^3 & u\xi^6 & \dots & u\xi^{3(n-1)} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & u & u\xi^{1+2^j} & u\xi^{\left(1+2^j\right)2} & \dots & u\xi^{\left(1+2^j\right)(n-1)} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & u & u\xi^{1+2^r} & u\xi^{(1+2^r)2} & \dots & u\xi^{(1+2^r)(n-1)}
\end{bmatrix}$$

Example 4.2.2. *Let* $m = 5, h(x) = x^5 + x^4 + x^3 + x^2 + 1$ *which gives* $FDG(5, 2)$ *that is a* $[2^5, 4^6 2^5, 16]$ *code over* $F_2 + uF_2$. $IFDG(5, 2)$ *is a* $[2^5, 4 \times 2^{10}, 24]$ *code over* $\mathbb{F}_2 + u\mathbb{F}_2$ *, its Gray image is a* $[64, 12, 24]$ *binary code for these parameters best known code has distance* 25 *and upper bound on distance is* 26.

Proposition 4.2.3. *All codewords of* $IFDG(m, \delta)$ *have weight divisible by* 4 *and*

$$d(IFDG(m, \delta)) = d(\mathcal{DG}(m, \delta)) = 2^m - 2^{m-\delta}.$$

Proof. The subcode of $\mathcal{DG}(m,\delta)$ that is generated by

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 2 & 2\xi & 2\xi^2 & \dots & 2\xi^{n-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 2 & 2\xi^{1+2^j} & 2\xi^{\left(1+2^j\right)2} & \dots & 2\xi^{\left(1+2^j\right)(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 2 & 2\xi^{1+2^r} & 2\xi^{(1+2^r)2} & \dots & 2\xi^{(1+2^r)(n-1)} \end{bmatrix}$$

satisfies the lineartiy criteria(Corollary 2.3.3) and obviously its gray image is the same as $\phi\left(IFDG\left(m,\delta\right)\right)$. In other words, $\phi\left(IFDG\left(m,\delta\right)\right)$ is a linear code contained in nonlinear binary code $DG\left(m,\delta\right)$. So it is enough to find a codeword of weight $2^m - 2^{m-\delta}$.

$DG(3,1)$ has same weight enumerator with $FDG\left(3,1\right)$.

$\phi\left(FDG\left(3,1\right)\right)$ is $RM(2,4)$ so its dual is $RM(1,4)$.

$\phi\left(FDG\left(5,2\right)\right)^{\perp}$ is a $[64,47,6]$ code.

Proposition 4.2.4. *$IFDG(m,\frac{m-1}{2})$ has weight distribution*

weight	*# of codewords*
0	1
$2^m - 2^{\frac{m+1}{2}}$	$2^{m-1}\left(2^m-1\right)$
2^m	$3\times 2^{2m} - 2^m - 2$
$2^m + 2^{\frac{m+1}{2}}$	$2^{m-1}\left(2^m-1\right)$
2^{m+1}	1

Proposition 4.2.5. $d\left(IFDG(m,\frac{m-1}{2})^{\perp}\right) = 4$.

Proof. $IFDG(m, \frac{m-1}{2})^{\perp}$ is the code with parity check matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & u & u\xi & u\xi^2 & \dots & u\xi^{n-1} \\ 0 & u & u\xi^3 & u\xi^6 & \dots & u\xi^{3(n-1)} \end{bmatrix}$$

So, it is contained in the code with parity check matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & u & u\xi & u\xi^2 & \dots & u\xi^{n-1} \end{bmatrix}$$

Which is $(F_1 RM(1,m))^{\perp} = F_1 RM(m-1,m)$ that has gray image $RM(m-1,m+1)$. So $d\left(IFDG(m, \frac{m-1}{2})^{\perp}\right) \geq d(RM(m-1,m+1)) = 4$. It is enough to find a codeword of weight 4 to reach the conclusion.

CHAPTER 5

Reed Muller Codes over S_k

In this chapter, we extended Reed Muller codes to the ring $S_k = \mathbb{F}_2[x] / \left(x^{2^k}\right)$. Obviously, $S_1 = \mathbb{F}_2 + u\mathbb{F}_2$. In chapter 3, we studied Reed Muller codes over S_1 in detail. We observed that for $k = 2$ we obtain polar codes as subcodes of Reed Muller codes.

5.1. Reed Muller Codes over S_2

Reed Muller Codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$

Definition 5.1. Let $S_2 = \mathbb{F}_2[x] / \left(x^{2^2}\right)$, i.e. $S_2 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$. Similarly we define Reed Muller codes over S_2. Let $h(x)$ be a basic primitive polynomial over S_2 of order m dividing $x^n - 1$ and ξ be one of its roots.

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \xi & \xi^2 & \dots & \xi^{n-1} \end{bmatrix}$$

Denote the i-th row of the matrix by $v_i\,(i = 1, 2, ..., m+1)$ The r-th order Reed-Muller code over S_2 which will be denoted by $S_2RM(r, m)$ is the code generated by all 2^m-tuples of the form

$$v_{i_1} v_{i_2} v_{i_3}, \dots, v_{i_s},\ 1 \le i_1 \le i_2 \le \dots \le i_s \le m+1,\ 0 \le s \le r.$$

We consider these codes with Lee weight

$$w(1) = 1,\ w(u) = w\left(u^2\right) = 2,\ w\left(u^3\right) = 4,\ w(0) = 0.$$

and linear Gray map

$$\begin{aligned}\phi: \quad & \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 \longrightarrow \mathbb{F}_2^4 \\ & a + bu \ + cu^2 + du^3 \longmapsto (a+b+c+d, c+d, b+d, d)\end{aligned}$$

We claim that;

1. $S_2RM\left(r-1,m\right) \subset S_2RM\left(r,m\right)$
2. $S_2RM\left(r,m\right)^{\perp} = S_2RM\left(m-r-1,m\right)$
3. $S_2RM\left(k,2k+1\right)$ is self-dual with Gray image a $\left[2^{2k+3}, 2^{2k+2}, 2^{k+1}\right]$ binary code.
4. $d\left(S_2RM\left(r,m\right)\right) = 2^{m-r}$ moreover it's Gray image $\phi\left(S_2RM\left(r,m\right)\right)$ lies between the corresponding binary Reed Muller Codes.
   $RM\left(r,m+2\right) \subseteq \phi\left(S_2RM\left(r,m\right)\right) \subseteq RM\left(r+1,m+2\right).$
5. The weight enumerator polynomial is symmetric.

Let us consider the subcode

$$S_2^1RM\left(r,m\right) = \left\langle RM\left(r-2,m\right), uRM\left(r-1,m\right), u^3RM\left(r,m\right)\right\rangle.$$

Theorem 5.1.1. *For any* $1 \leq r \leq m-2$, *we have* $\phi\left(S_2^1RM\left(r,m\right)\right) = RM\left(r,m+2\right)$

Proof.

$$\begin{aligned}S_2^1RM\left(r,m\right) &= \left\langle RM\left(r-2,m\right), uRM\left(r-1,m\right), u^3RM\left(r,m\right)\right\rangle \\ &= \left\{ \begin{array}{c} a+bu+cu^2+du^3 \mid a \in RM\left(r-2,m\right),\ b \in RM\left(r-1,m\right), \\ c \in b \in RM\left(r-1,m\right),\ d \in RM\left(r,m\right) \end{array} \right\}\end{aligned}$$

$|S_2^1 RM\,(r,m)| = 2^k$, where

$$
\begin{aligned}
k &= 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r-2} + 2\left(1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r-1}\right) \\
&\quad + 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r} \\
&= 1 + \left[\binom{m}{0} + \binom{m}{1}\right] + \cdots + \left[\binom{m}{r-2} + \binom{m}{r-1}\right] \\
&\quad + 1 + \left[\binom{m}{0} + \binom{m}{1}\right] + \cdots + \left[\binom{m}{r-1} + \binom{m}{1}\right] \\
&= 1 + \binom{m+1}{1} + \binom{m+1}{2} + \cdots + \binom{m+1}{r-1} \\
&\quad + 1 + \binom{m+1}{1} + \binom{m+1}{2} + \cdots + \binom{m+1}{r} \\
&= 1 + \left[\binom{m+1}{0} + \binom{m+1}{1}\right] + \cdots + \left[\binom{m+1}{r-1} + \binom{m+1}{r}\right] \\
&= 1 + \binom{m+2}{1} + \binom{m+2}{2} + \cdots + \binom{m+2}{r} \\
&= K_{r,m+2}.
\end{aligned}
$$

So, k is the dimension of $RM\,(r, m+2)$.

$$
\phi\left(S_2^1 RM\,(r,m)\right) = \left\{ \begin{array}{c} (a+b+c+d, c+d, b+d, d) \mid \\ a \in RM\,(r-2,m)\,,\ b,c \in RM\,(r-1,m)\,,\ d \in RM\,(r,m) \end{array} \right\}
$$

Let $(a+b+c+d, c+d, b+d, d) = (x, x+y)$ where $x = (a+b+c+d, c+d)$ and $y = (a+c, c)$

Now we can write $x = (a+b+c+d, (a+b+c+d)+a+b)$ As a runs through $RM\,(r-2,m)$; b, c runs through $RM\,(r-1,m)$; d runs through $RM\,(r,m)$, we see that a+b+c+d runs through $RM\,(r,m+2)$ and a+b runs through $RM\,(r-1,m+2)$ because of the inclusion $RM\,(r-2,m) \subseteq RM\,(r-1,m) \subseteq RM\,(r,m)$. We see that x runs through $RM\,(r,m+1)$. Similarly, by wirting $y = (a+c, (a+c)+a)$, we see that y runs through $RM\,(r-1,m+1)$. But this means

$$
\phi\left(S_2^1 RM\,(r,m)\right) = \{(x, x+y)\ |, x \in RM\,(r,m+1)\,,\ y \in RM\,(r-1,m+1)\}
$$

which is exactly $RM\,(r,m+2)$.

Corollary 5.1.2. *The binary Reed-Muller codes* $RM\left(r,m\right)$ *are all* $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2+u^3\mathbb{F}_2$*-linear for* $0\leq r\leq m$.

$$RM\left(r,m+2\right)=\phi\left(S_2^1RM(r,m)\right)\subset\phi\left(S_2RM(r,m)\right)\subset RM\left(r+1,m+2\right)$$

Corollary 5.1.3. $S_2^1RM\left(r,m\right)^{\perp}=S_2^1RM\left(m-r+1,m\right)$, *for* $0\leq r\leq m$.

Proof. Follows immediately from

$$\phi\left(S_2^1RM\left(r,m\right)^{\perp}\right)=RM\left(r,m+2\right)^{\perp}=\phi\left(S_2^1RM\left(m-r+1,m\right)\right).$$

$$\begin{aligned}
S_2RM\left(r,m\right)&=\langle RM\left(r,m\right)\rangle\\
S_2^1RM\left(r,m\right)&=\left\langle RM\left(r-2,m\right),uRM\left(r-1,m\right),u^3RM\left(r,m\right)\right\rangle,\\
\phi\left(S_2^1RM\left(r,m\right)\right)&=RM\left(r,m+2\right)\\
S_2^2RM\left(r,m\right)&=\left\langle RM\left(r-3,m\right),uRM\left(r-1,m\right),u^3RM\left(r,m\right)\right\rangle,\\
\phi\left(S_2^2RM\left(r,m\right)\right)&=G_P\left(2^{m+1},A\right)\\
S_2^3RM\left(r,m\right)&=\left\langle RM\left(r-3,m\right),uRM\left(r-2,m\right),u^3RM\left(r,m\right)\right\rangle,\\
\phi\left(S_2^2RM\left(r,m\right)\right)&=G_P\left(2^{m+1},B\right)\\
\text{where } A=K_{r,m+2}-\binom{m}{r-2},\ B&=K_{r,m+2}-\binom{m}{r-2}-2\binom{m}{r-1}
\end{aligned}$$

Example 5.1.1. *$S_2RM\,(3,3)$ is the code generated by*

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

which has subcode $S_2^1RM\,(3,3)$ with gray image $RM\,(3,5)$ that is generated by

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ u & u & 0 & 0 & 0 & 0 & 0 & 0 \\ u & 0 & u & 0 & 0 & 0 & 0 & 0 \\ u & 0 & 0 & 0 & u & 0 & 0 & 0 \\ u^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

and weight 4 rows of $F^{\otimes 5}$ are splitted into 3 groups, and the code $S_2^2RM\,(3,3)$ generated by the following matrix has gray image the polar code $G_P\,(32,23)$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ u & u & u & u & 0 & 0 & 0 & 0 \\ u & u & 0 & 0 & u & u & 0 & 0 \\ u & 0 & u & 0 & u & 0 & u & 0 \\ u & u & 0 & 0 & 0 & 0 & 0 & 0 \\ u & 0 & u & 0 & 0 & 0 & 0 & 0 \\ u & 0 & 0 & 0 & u & 0 & 0 & 0 \\ u^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

similarly the subcode $S_2^3RM\,(3,3)$ *generated by the following matrix has gray image* $G_P\,(32,17)$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ u & u & u & u & 0 & 0 & 0 & 0 \\ u & u & 0 & 0 & u & u & 0 & 0 \\ u & 0 & u & 0 & u & 0 & u & 0 \\ u^3 & u^3 & 0 & 0 & 0 & 0 & 0 & 0 \\ u^3 & 0 & u^3 & 0 & 0 & 0 & 0 & 0 \\ u^3 & 0 & 0 & 0 & u^3 & 0 & 0 & 0 \\ u^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Conjecture. $S_2^2RM\,(r,m)$ and $S_2^3RM\,(r,m)$ have gray images the Polar codes $G_P\left(2^{m+2}, K_{r,m+2} - \binom{m}{r-2}\right)$ and $G_P\left(2^{m+2}, K_{r,m+2} - \binom{m}{r-2} - 2\binom{m}{r-1}\right)$ respectively.

$S_2RM\,(r,m)$ has a subcode with Gray image equivalent to $RM\,(r,m+2)$ and $\binom{m}{r-2}$ less wanted weight 2^{m+2-r} rows appears as $\phi\left(v_{i_1}v_{i_2}\dots v_{i_{r-1}}\right)$ and we remove them by expanding corresponding rows by u and obtain $G_P\left(2^{m+2}, K_{r,m+2} - \binom{m}{r-1}\right)$ and further we can remove the next group of rows by expanding $v_{i_1}v_{i_2}\dots v_{i_{r-1}}$ by u^3 and obtain $G_P\left(2^{m+2}, K_{r,m+2} - \binom{m}{r-2} - 2\binom{m}{r-1}\right)$.

5.2. Complexity comparison Polar and RM codes

Arıkan defined in [23] Reed Muller code $RM\,(N,K)$ of dimension K for length $N = 2^m$ as it picks the K heaviest rows of $F^{\otimes m}$, $F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and compared these codes with polar codes with the same parameters i.e. $G_P\,(N,K)$. In that case, one possible choice for Reed Muller coincides with polar code for most of the values for K.

Definition 5.2. We add an additional condition as Reed Muller code $RM\,(N,K)$ be generated by the heaviest K rows of $F^{\otimes m}$ and the order is determined by the

length of span of 1's, i.e. we pick the row with the shortest span of 1's among the possible choices.

At length 8 Polar codes are not different from Reed Muller code.

At length 16 they differ at dimension 8 the Polar code $G_P(16,8)$ differs from $RM(16,8)$ by one row

Example 5.2.1.

$$\pi_{16} = (16, 8, 12, 14, 15, 4, 6, 10, 7, 11, 13, 2, 3, 5, 9, 1)$$
$$RM_{16} = (16, 8, 12, 14, 15, 4, 6, 7, 10, 11, 13, 2, 3, 5, 9, 1)\,.$$

So $G_P(16,8)$ *and* $RM(16,8)$ *are as the following*

$$G_P(16,8) = \begin{bmatrix} 1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0 \\ 1&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0 \\ 1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0 \\ 1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0 \\ 1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0 \\ 1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \end{bmatrix}$$

$$RM(16,8) = \begin{bmatrix} 1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0 \\ 1&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0 \\ 1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0 \\ 1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0 \\ 1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0 \\ 1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \end{bmatrix}$$

Trellis oriented generator matrix is a matrix where the rows have different starting and ending points. They have the following Trellis oriented generators respectively;

$$G_P(16,8) = \begin{bmatrix} 0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0 \\ 1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0 \\ 0&1&0&1&1&0&1&0&1&0&1&0&1&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1 \end{bmatrix}$$

brach complexity $2^1+2^2+2^2+2^3+\cdots+2^3+2^2+2^1=108$ *similarly state sequence is* $0,1,2,3,2,3,2,3,2,3,2,3,2,3,2,1,0$ *(i.e. the number of active generators at each instant), state complexity* $2^0+2^1+2^2+2^3+2^2+\cdots+2^2+2^1+2^0=82$

$$RM(16,8) = \begin{bmatrix} 0&1&0&1&1&0&1&0&0&0&0&0&0&0&0&0 \\ 1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&1&1&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1 \end{bmatrix}$$

$RM(16,8)$ *with branch complexity* 88 *state complexity* 67*.*

At length 32 they differ at dimensions $9,10,11,12,13,16,19,21,22,23,26$ we

compared them and obtained the following table:

		Polar bit level		RM bit level		Polar parallelized		RM parallelized	
N	K	E	V	E	V	E	V	E	V
16	8	108	82	88	67	56	44	88	67
32	9	428	374	348	328	112	100	176	139
32	10	396	338	344	299	200	167	344	299
32	11	556	454	388	320	280	230	388	320
32	12	1004	798	540	402	280	230	540	402
32	13	972	726	876	614	540	434	540	402
32	16	1628	1222	6396	4798	292	232	540	434
32	19	1212	758	956	646	308	224	184	125
32	26	1180	638	1180	638	700	390	700	390

Table 3. Trellis complexity comparison

where E and V stands for branch and state complexities respectively.

$G_P(32,16)$ has distance 4 on the other hand $RM(32,16)$ has distance 8.

$d(G_P(32,16)) = 4$, $d(RM(32,16)) = 8$.

An advantage of a code over S_k may be that the trellis oriented generator matrix of the Gray image can be obtained easily from trellis oriented generator matrix over S_k.

5.3. Reed Muller Codes over S_k

Definition 5.3. Let $S_k = \mathbb{F}_2[x] / \left(x^{2^k}\right)$, Let $h(x)$ be a basic primitive polynomial over S_k of order m dividing $x^n - 1$ and ξ be one of its roots:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \xi & \xi^2 & \dots & \xi^{n-1} \end{bmatrix}.$$

Denote the i-th row of the matrix by $v_i\,(i = 1, 2, \dots, m+1)$ The r-th order Reed-Muller code over $S_k RM(r, m)$ is the code generated by all 2^m-tuples of the form

$$v_{i_1} v_{i_2} v_{i_3} \dots v_{i_s},\ 1 \le i_1 \le i_2 \le \dots \le i_s \le m+1,\ 0 \le s \le r.$$

We consider these codes with new weight defined as

$$w\left(u^l\right) = \begin{cases} 2^k & l = 2^k - K_{0,m} \\ 2^{k-1} & 2^k - K_{1,m} \le l \le 2^k - K_{0,m} - 1 \\ 2^{k-2} & 2^k - K_{2,m} \le l \le 2^k - K_{1,m} - 1 \\ 2^{k-r} & 2^k - K_{r,m} \le l \le 2^k - K_{r-1,m} - 1 \\ 2 & 1 \le l \le 2^k - K_{m-1,m} \\ 1 & l = 0 \end{cases}$$

Gray map as u^l is sent to $2^k - l$ th row of the generator matrix $RM(k, k)$.

Example 5.3.1. *Consider Reed-Muller codes over*

$$S_3 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2 + u^4\mathbb{F}_2 + u^5\mathbb{F}_2 + u^6\mathbb{F}_2 + u^7\mathbb{F}_2$$

with weight defined as

$$w(1) = 1,\ w(u) = w\left(u^2\right) = w\left(u^3\right) = 2,\ w\left(u^4\right) = w\left(u^5\right) = w\left(u^6\right) = 4,\ w\left(u^7\right) = 8$$

and linear Gray map

$$
\begin{array}{ccccccccc}
u^7 & \rightarrow & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
u^6 & \rightarrow & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
u^5 & \rightarrow & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
u^4 & \rightarrow & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
u^3 & \rightarrow & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
u^2 & \rightarrow & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
u^1 & \rightarrow & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & \rightarrow & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}
$$

$S_3RM\,(3,3)$ is the code generated by

$$
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
$$

which has subcode with gray image $RM\,(3,6)$ which is generated by

$$
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
u & u & u & u & 0 & 0 & 0 & 0 \\
u & u & 0 & 0 & u & u & 0 & 0 \\
u & 0 & u & 0 & u & 0 & u & 0 \\
u^4 & u^4 & 0 & 0 & 0 & 0 & 0 & 0 \\
u^4 & 0 & u^4 & 0 & 0 & 0 & 0 & 0 \\
u^4 & 0 & 0 & 0 & u^4 & 0 & 0 & 0 \\
u^7 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
$$

weight 8 rows of $F^{\otimes 6}$ are splitted into 4 groups with respect to RM_{2^6} introduced in the previous section. So we obtain Reed Muller codes defined in the previous section as

Gray images of subcodes of $S_3RM\,(3,3)$. *So* $RM\,(64,41)$, $RM\,(64,32)$, $RM\,(64,23)$ *are obtained as subcodes of* $S_3RM\,(3,3)$.

CHAPTER 6

Conclusion

6.1. Results of the dissertation

In chapter 3, we extended Reed Muller codes to $\mathbb{F}_2 + u\mathbb{F}_2$ and studied the properties of FRM codes. We conjectured that we obtain families of polar codes from FRM. In other words, we claim that families of polar codes are expressed algebraically.

In chapter 4, we generalized the Reed Muller codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and define Goethals, Delsarte-Goethals and Goethals-Delsarte codes over $\mathbb{F}_2 + u\mathbb{F}_2$. We have seen that Goethals and shortened Goethals codes over $\mathbb{F}_2 + u\mathbb{F}_2$ are classes of double error correcting codes which gives us two error correcting families of binary linear codes. Therefore we obtained double error correcting families of binary codes as the Gray images of Goethals and shortened Goethals codes. Delsarte-Goethals and Goethals-Delsarte codes over $\mathbb{F}_2 + u\mathbb{F}_2$ did not give us interesting results. A class of codes; $IFDG$, obtained from Delsarte-Goethals was interesting. They have distance quite close to upper bound for some parameters. We obtained binary linear codes with the same correcting capability of quaternary Delsarte Goethals codes as Gray images of $IFDG$ codes.

In the last chapter, we extended Reed Muller codes to S_k. For S_2 we claim that S_2RM codes have subcodes with gray image polar codes. S_3RM gave us RM codes as subcodes. This chapter is mostly related with our future research.

6.2. Future research

We wish to study Reed Muller codes over S_k in detail and see whether their gray images have families of polar codes or not. We hope that it may be an algebraic way to express some polar codes. In [29] Şaşoğlu, Telatar and Arıkan extended the polar codes to non-binary cases. They also gave examples over $\mathbb{F}_3$ and $\mathbb{F}_4$. We want to search for matrices with large rate of polarization over rings, especially over $\mathbb{Z}_4$. In other words, we would like to study polar codes over rings.

We wish to compare in detail RM codes introduced in last chapter with polar codes. We observed that RM codes have lower trellis complexity than the polar ones. Is it true for large blocklength?

In [14] and [19] designs were obtained from supports of codewords in extremal quaternary codes like Goethals, Kerdock and Preparata. We would like to study the relation between design theory and codes over $\mathbb{F}_2 + u\mathbb{F}_2$ like Goethals and $IFDG$. We will try to answer the question "Is it possible to obtain designs from codes over $\mathbb{F}_2 + u\mathbb{F}_2$?".

REFERENCES

[1] Abulraub T, Siap I, *Cyclic Codes over the Rings* $\mathbb{Z}_2 + u\mathbb{Z}_2$ *and* $\mathbb{Z}_2 + u\mathbb{Z}_2 + u_2^2\mathbb{Z}$, Designs, Codes and Cryptography, Vol 42, N. 3, 273-287, 2007.

[2] Arıkan E, *Channel polarization: A method for constructing capacity achieving codes for symmetric binary-input memoryless channels*, IEEE Transactions on Information Theory 55 no 7:3051-3073, 2009.

[3] Arıkan E, *A performance comparison of polar codes and Reed-Muller codes*, IEEE Commun. Lett., vol. 12, no 6, 447-449, 2008.

[4] Baker RD, Van Lint JH, Wilson RM, *On the Preparata and Goethals codes*, IEEE Transactions on Information Theory 29:342-345, 1983.

[5] Bonnecaze A, Udaya P, *Cyclic Codes and self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Transactions on Information Theory 45:1250-1255, 1999.

[6] Bonnecaze A, Udaya P, *Decoding of cyclic codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Transactions on Information Theory 45:2148-2157, 1999.

[7] Borges J, Fernandez C, Phelps KT, *Quaternary Reed-Muller Codes*, IEEE Transactions on Information Theory 51, 2005.

[8] Dougherty ST, Gaborit P, Harada M, Sole P, *Type II codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Transactions on Information Theory 45:32-45, 1999.

[9] Dougherty ST, Gaborit P, Harada M, Munemasa A, Sole P, *Type IV self-dual codes over rings*, IEEE Transactions on Information Theory 45:2345-2360, 1999.

[10] Forney GD, Sloane NJA, Trott MD, *The Nordstorm Robinson code is the binary image of the octacode*, Proceedings DIMACS/IEEE Workshop on Coding and Quantization, Amer. Math. Soc., 1993.

[11] Forney GD, *Codes on graphs: normal realizations*, IEEE Transactions on Information Theory 47:520-548, 2001.

[12] Goethals JM, *Two dual families of nonlinear binary codes*, Electronic Letters, 10:471-472, 1974.

[13] Hammons AR, Kumar V, Calderbank AR, Sloane NJA, Sole P, *The* $\mathbb{Z}_4$-

Linearity of Kerdock, Preparata, Goethals and Related Codes, IEEE Transactions on Information Theory 40:301-319, 1994.

[14] Helleseth T, Rong C, Yang K, *On t-designs from codes over $\mathbb{Z}_4$*, Discrete Mathematics, 238:67-80, 2001.

[15] Hergert FB, *On the Delsarte-Goethals codes and their formal duals*, Discrete Math, 83:249-263, 1990.

[16] Huffman W, Pless V, *Fundamentals of Error Correcting Codes*, Cambridge University Press, 2003.

[17] Kerdock AM, *A class of low-rate non-linear binary codes*, Inform. and Control 20:182-187, 1972.

[18] Korada S, Şaşoğlu E, Urbanke R, *Polar codes: characterization of exponent, bounds and constructions*, [Online] Available: http://arxiv.org/abs/0901.0536v2, 2009.

[19] Lahtonen J, Ranto K, Vehkalahti R, 3-*Designs from all $\mathbb{Z}_4$-Goethals-like codes with block size* 7 *and* 8, Finite Fileds and Their Applications,13:815-827, 2007.

[20] Lin S, Costello DJ, *Error Control Coding*, 2nd ed., Pearson, 2004.

[21] Ling S, Sole P, *Duadic codes over $\mathbb{F}_2 + u\mathbb{F}_2$*, AAECC Applicable Algebra in Engineering, Communication and Computing 12:365-379, 2001.

[22] MacWilliams FJ, Sloane NJA, *The Theory of Error Correcting Codes*, North Holland Publishing Company, 1977.

[23] Muller DE, *Application of boolean algebra to switching circuit design and to error detection*, IEEE Transactions on Computers, 3:6–12, 1954.

[24] Mori R, Tanaka, *Non-Binary Polar Codes using Reed-Solomon Codes and Algebraic Geometry Codes*, 2010 IEEE Information Theory Workshop - ITW 2010 Dublin.

[25] Mori R, Tanaka, *Performance and construction of polar codeson symmetric binary-input memoryless channels*, Proceedings 2009 IEEE Int. Symposium on Inform. Theory, Seoul, South Korea, pp. 1496-1500, 2009.

[26] Nordstorm AW, Robinson JP, *An optimum nonlinear code*, Inform and Control 11:613-616, 1967.

[27] Preparata FP, *A class of optimum nonlinear double error correcting codes*, Inform and Control 13:378-400, 1968.

[28] Reed IS, *A class of multiple-error-correcting codes and the decoding scheme*, IEEE Transactions on Information Theory, 4:38–49, 1954.

[29] Şaşoğlu E, Telatar E, Arıkan E, *Polarization for arbitrary discrete memoryless channels*, [Online] Available: http://arxiv.org/abs/0908.0302v1, 2009.

[30] Van Lint JH, *Kerdock and Preparata codes*, Congress Numerantium, 39:25-41, 1983.

[31] Wan ZX, *Lectures on Finite Fields and Galois Rings*, World Scientific, 2003.

[32] Wan ZX, *Quaternary Codes*, World Scientific, 1997.

[33] Wasan SK, Bhaintwal M, *Generalized Reed-Muller codes over* $\mathbb{Z}_q$, Des. Codes Cryptogr., 54:149-166, 2010.

[34] Yıldız B, Karadeniz S, *Linear codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes Crypt. 54:61-81, 2010.