ON SOME LINEAR CODES OVER $\mathbb{Z}_{2^s}$

A Thesis Submitted

in Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

by

MANISH K. GUPTA

to the

DEPARTMENT OF MATHEMATICS

INDIAN INSTITUTE OF TECHNOLOGY, KANPUR

December, 1999

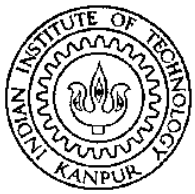
To

My Parents, Brother and Sister

यथा शिखा मयुराणां नागानां मणयो यथा
तद्वेदांगशास्त्राणां गणितं मूर्धनि स्थितम्।

As are the crests on the heads of Peacocks,
As are the gems on the hoods of the Cobras,
So is Mathematics, at the top of all Sciences.

The Yajurveda, circa 600 B.C.



CERTIFICATE

It is certified that the work contained in the thesis entitled *On Some Linear Codes over* $\mathbb{Z}_{2^s}$ by *Manish K. Gupta* has been carried out under our supervision and that this work has not been submitted elsewhere for a degree.

Professor M. C. Bhandari Professor A. K. Lal
Department of Mathematics
Indian Institute of Technology
December, 1999 Kanpur

Nomenclature

S	:	A Commutative ring with unity
$\|S\|$	:	Cardinality of the set S
S^n	:	Set of all n-tuples over S
$\mathbb{F}_q$	:	Set of q Alphabets
$\mathbb{F}_q^n$	:	Set of all n-tuples over $\mathbb{F}_q$
$\mathcal{M}$	:	A left S-module
$GF(q)$	:	Galois field with q elements
$\mathbb{Z}_q$	:	Ring of integers modulo m
$\mathbb{Z}_{p^s}$	:	Ring of integers modulo p^s
U	:	Set of all units of $\mathbb{Z}_{p^s}$
Z	:	Set of all zero divisors of $\mathbb{Z}_{p^s}$
$\lfloor x \rfloor$	:	*Greatest integer less* than or equal to x
$\lceil x \rceil$	:	*Smallest integer greater* than or equal to x
$\mathbf{x}$	:	Element of $\mathbb{F}_q^n$
$w_H(\mathbf{x})$	:	Hamming weight of $\mathbf{x}$
$w_L(\mathbf{x})$	:	Lee weight of $\mathbf{x}$
$w_E(\mathbf{x})$	:	Euclidean weight of $\mathbf{x}$
$d_H(\mathbf{x}, \mathbf{y})$	:	Hamming distance between $\mathbf{x}$ and $\mathbf{y}$
$d_L(\mathbf{x}, \mathbf{y})$	:	Lee distance between $\mathbf{x}$ and $\mathbf{y}$
$d_{GL}(\mathbf{x}, \mathbf{y})$	:	Generalized Lee distance between $\mathbf{x}$ and $\mathbf{y}$
d_H	:	Minimum Hamming distance of $\mathcal{C}$
d_L	:	Minimum Lee distance of $\mathcal{C}$
d_{GL}	:	Minimum generalized Lee distance of $\mathcal{C}$

$d(\mathbf{x}, D)$	:	Smallest distance of $\mathbf{x}$ from a word in D
$\mathcal{C}$	:	A code of length n
$\mathbf{c}$	:	A codeword of $\mathcal{C}$
(n, M, d_H, d_L, d_E)	:	A code of length n, number of codewords M and minimum Hamming, Lee and Euclidean distances respectively d_H, d_L and d_E
$[n, k, d_H, d_L, d_E]$	:	A Linear code of length n, 2-dimension k and minimum distances d_H, d_L and d_E respectively
$[n, k, d_H, d_L, d_{GL}]$	:	A Linear code of length n, 2-dimension k and minimum distances d_H, d_L and d_{GL} respectively
$[n, k]$	:	A Linear Code
$A_H(i)(A_L(i))$	:	Number of codewords of Hamming (Lee) weight i
$d_r(\mathcal{C})$	:	r^{th} Generalized Hamming weight (GHW) of $\mathcal{C}$
$w_S(\mathcal{D})$	:	Support size of $\mathcal{C}$
$\mathcal{C}^{\perp}$	:	Dual code of $\mathcal{C}$
$Aut(\mathcal{C})$	:	Automorphism group of $\mathcal{C}$
$Ham_{\mathcal{C}}(x, y)$ or $W_{\mathcal{C}}(x, y)$	:	Hamming weight enumerator (hwe) of $\mathcal{C}$
$\omega_j(\mathbf{c})$	:	$\lvert\{k : c_k = j\}\rvert$
$cwe_{\mathcal{C}}(x_0, \ldots, x_m)$	:	Complete weight enumerator (cwe) of $\mathcal{C}$
$swe_{\mathcal{C}}(x, y, z)$	:	Symmetrized weight enumerator (swe) of $\mathcal{C}$
$Lee_{\mathcal{C}}(x, y)$	:	Lee weight enumerator of $\mathcal{C}$
$S_k(q)$	:	q-ary Simplex Code
$G_k(q)$	:	Generator matrix of $S_k(q)$
$\mathcal{M}_{k,u}(q)$	:	q-ary MacDonald Code
$G_{k,u}(q)$	:	Generator matrix of $\mathcal{M}_{k,u}(q)$
S_k	:	Binary Simplex Code
$\hat{S}_k$	:	Extended binary Simplex Code
$G(S_k)$	:	Generator matrix of S_k

$G(\hat{S}_k)$	:	Generator matrix of $\hat{S}_k$
$RM(r,m)$	:	r^{th}-order Reed Müller Code
$P(m)$	:	Binary nonlinear Preparata Code
$K(m)$	:	Binary nonlinear Kerdock Code
$A(n,d_H)$	:	$\max\{M\vert$ there exists a binary (n,M,d_H) code $\}$
ϕ	:	Gray map
$\phi(\mathcal{C})$	:	$\{\phi(\mathbf{c}) : \mathbf{c} \in \mathcal{C}\}$: Gray image of $\mathcal{C}$
$h_2(x)$	:	Irreducible polynomial over $\mathbb{Z}_2$ such that it divides x^n-1 over $\mathbb{Z}_2$
$h(x)$	:	Hensel uplift of $h_2(x)$ over $\mathbb{Z}_4$
$\mathcal{B}$	:	p-basis of $\mathcal{C}$
$p-\dim(\mathcal{C})$	:	p-dimension of $\mathcal{C}$
ϕ_G	:	Generalized gray map
$\phi_G(\mathcal{C})$	:	Generalized gray image of $\mathcal{C}$
$\mathcal{C}_\phi$	:	Generalized gray image of $\mathcal{C}$ in 2-basis form
$\mathcal{C}^{(1)}$	:	Binary residue code of $\mathcal{C}$
$\mathcal{C}^{(2)}$	:	Binary torsion code of $\mathcal{C}$
$\theta(\mathbf{c})$	:	Correlation of $\mathbf{c} \in \mathcal{C}$
S_k^α	:	Simplex Code of type α
S_k^β	:	Simplex Code of type β
G_k	:	Generator matrix of S_k^α
G_k^β	:	Generator matrix of S_k^β
$\bar{S_k^\alpha}$	:	Punctured code of S_k^α obtained by deleting the zero coordinate
R_i	:	Rows of a generator matrix
$\mathcal{K}_{4m}$	:	Klemm code
$\mathcal{O}_8$	:	Octacode code
QR_n	:	Uplifted extended quadratic residue code over $\mathbb{Z}_4$
$\mathcal{R}^{1,m-s+1}$	:	First order Reed Müller code over $\mathbb{Z}_{2^s}$
$\mathcal{C}_p$	:	Norm quadratic residue (NQR) code

H_p	:	Finite version of Poincáre upper half-plane
δ	:	Arbitrary chosen quadratic non residue modulo p
γ	:	First row of a circulant matrix C
$P_\gamma(z)$	:	Polynomial corresponding to γ
$PSL_2(p)$	:	Projective special linear group on GF(p)
$SL_2(p)$	:	Special linear group on GF(p)
$R(\mathcal{C})$	:	Covering radius of $\mathcal{C}$
$N^{(i)}$	:	Norm of $\mathcal{C}$ with respect to i^{th}-coordinate
$N(\mathcal{C})$	:	Norm of $\mathcal{C}$
∎	:	End of the proof

Synopsis

Name of the student: **Manish Kumar Gupta** Roll No.: **9310863**

Degree for which submitted: **Ph.D.** Department: **Mathematics**

Thesis Title: **On Some Linear Codes over** $\mathbb{Z}_{2^s}$

Name of the Thesis Supervisors: **Prof. M. C. Bhandari** & **Prof. A. K. Lal**

Month and Year of Thesis Submission: **December, 1999**

Let q be a positive integer and let $\mathbb{F}_q$ be a set of q-alphabets. A code $\mathcal{C}$ of length n and size M is a subset of $\mathbb{F}_q^n$ having M elements. The elements of $\mathcal{C}$ are called *codewords*. In order to be able to correct errors we associate some algebraic structure with $\mathbb{F}_q$. If q is a prime power one usually take $\mathbb{F}_q = GF(q)$ otherwise $\mathbb{F}_q = \mathbb{Z}_q$. Let $\mathbb{F}_q = GF(q)(\mathbb{Z}_q)$. A linear code of length n over $GF(q)(\mathbb{Z}_q)$ is a subspace (submodule) of $\mathbb{F}_q^n$. Two codes over $\mathbb{Z}_{p^s}$ are said to be equivalent if one can be obtained from the other by a permutation of coordinates and or by multiplying one or more coordinates by a unit in $\mathbb{Z}_{p^s}$. Let $\mathcal{C}$ be a linear code of length n over $\mathbb{Z}_{p^s}$. In 1995, Calderbank and Sloane have shown that $\mathcal{C}$ is equivalent to a code generated by the rows of the matrix (see[15])

$$G = \begin{bmatrix} I_{k_0} & A_{01} & A_{02} & \cdots & A_{0s-1} & A_{0s} \\ \mathbf{0} & pI_{k_1} & pA_{12} & \cdots & pA_{1s-1} & pA_{1s} \\ \mathbf{0} & \mathbf{0} & p^2I_{k_2} & \cdots & p^2A_{2s-1} & p^2A_{2s} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & p^{s-1}I_{k_{s-1}} & p^{s-1}A_{s-1s} \end{bmatrix}, \tag{1}$$

where A_{ij} are matrices over $\mathbb{Z}_{p^s}$ and the columns are grouped into blocks of size $k_0, k_1, \cdots, k_{s-1}, k_s$. Let $k = \sum_{i=0}^{s-1}(s-i)k_i$. Then $|\mathcal{C}| = p^k$. Note that $\mathcal{C}$ is a free module if and only if $k_i = 0$ for all $i = 1, 2, \ldots, s-1$. Notion of dual code of $\mathcal{C}$ is defined via inner product $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i \pmod{p^s}$.

Two notorious binary nonlinear codes–the Kerdock code and the Preparata code--have in the past been something of an enigma in coding theory since they possess many linear-like properties. Until recently, their mysterious formal duality (with respect to the MacWilliams transform) had been dismissed as a "mere coincidence" since an appropriate algebraic notion of duality was lacking for nonlinear codes. In[52], Hammons et al have shown that both Kerdock and Preparata codes are gray images of some linear codes over $\mathbb{Z}_4$ which are dual to each other over $\mathbb{Z}_4$. Description of these codes become simpler using the properties of corresponding linear codes over $\mathbb{Z}_4$. In addition, the customary notions of generator matrices, parity-check matrices, syndromes etc., become meaningful. Since then many linear codes over $\mathbb{Z}_4$ and in general over $\mathbb{Z}_{p^s}$ have been investigated by several researchers. They have also studied the Gray images of different codes.

Let $\mathcal{C}$ be a linear code over $\mathbb{Z}_4$. Then $\mathcal{C}$ has a generator matrix of the form

$$G = \begin{bmatrix} I_{k_0} & A & B_1 + 2B_2 \\ 0 & 2I_{k_1} & 2C \end{bmatrix}, \tag{2}$$

where A, B_1, B_2, C have entries 0 and 1 and I_k is the identity matrix of order k.

Let $d_H(d_L)$ be the minimum Hamming (Lee) distance of $\mathcal{C}$. In[93], E. M. Rains has shown that $d_H \geq \lceil \frac{d_L}{2} \rceil$. $\mathcal{C}$ is said to be of *type* α (β) if $d_H = \lceil \frac{d_L}{2} \rceil$ ($d_H > \lceil \frac{d_L}{2} \rceil$). The *Gray map* $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ is the coordinate wise extension of the function from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ defined by $0 \to (0,0), 1 \to (0,1), 2 \to (1,1)$ and $3 \to (1,0)$. The image $\phi(\mathcal{C}) = \{\phi(\mathbf{c}) : \mathbf{c} \in \mathcal{C}\}$ of $\mathcal{C}$ under the Gray map ϕ is a binary code of length $2n$.

However it may not be linear. If $\phi(\mathcal{C})$ is linear then $\mathcal{C}$ is called $\mathbb{Z}_2$-*linear*. A binary code of even length is called $\mathbb{Z}_4$-*linear* if it is equivalent to $\phi(\mathcal{C})$ for some linear code over $\mathbb{Z}_4$. In[53], Hammons et al have shown that many known binary nonlinear codes are $\mathbb{Z}_4$-linear.

In the present dissertation we have constructed Simplex codes of type α and β over $\mathbb{Z}_4$ and over $\mathbb{Z}_{2^s}$, and first order Reed Müller code over $\mathbb{Z}_{2^s}$. Some fundamental properties like 2-dimension, weight hierarchy etc. are obtained. We have also considered their gray images in two ways and obtained some interesting binary codes. It is shown that Simplex code of type α and β and many known self dual codes satisfy the chain condition. A brief survey of known results is given in Chapter 2.

A vector v is a *p-linear combination* of the vectors $v_1, v_2, \ldots, v_k$ if $v = l_1v_1 + \ldots + l_kv_k$ with $l_i \in \mathbb{Z}_p$ for $1 \leq i \leq k$. A subset $S = \{v_1, v_2, ..., v_k\}$ of $\mathcal{C}$ is called a *p-basis* for $\mathcal{C}$ if for each $i = 1, 2, ..., k-1$, pv_i is a $p-$linear combination of $v_{i+1}, ..., v_k$, $pv_k = 0$, $\mathcal{C}$ is the p-linear span of S and S is p-linearly independent[112]. The number of elements in a p-basis for $\mathcal{C}$ is called the *p-dimension* of $\mathcal{C}$. It is easy to verify that the rows of the matrix

$$\mathcal{B} = \begin{bmatrix} I_{k_0} & A & B_1 + 2B_2 \\ 2I_{k_0} & 2A & 2B_1 \\ 0 & 2I_{k_1} & 2C \end{bmatrix} \tag{3}$$

form a 2-basis for the code $\mathcal{C}$ generated by the matrix G given in (1).

A linear code $\mathcal{C}$ over $\mathbb{Z}_{2^s}$ ($\mathbb{Z}_2$) of length n, 2-dimension k, minimum Hamming distance d_H and minimum Lee distance d_L is called an $[n, k, d_H, d_L]$ ($[n, k, d_H]$) or simply an $[n, k]$ code.

Let $\phi(\mathcal{B})$ be the matrix obtained from $\mathcal{B}$ (given in (3)) by applying the gray map ϕ to each row of $\mathcal{B}$. The code $\mathcal{C}_\phi$ generated by $\phi(\mathcal{B})$ is a $[2n, k, \geq \lceil \frac{d_L}{2} \rceil]$ binary linear code.

Let $\mathcal{C}$ be an $[n,k]$ linear code over $\mathbb{Z}_{2^s}$. For $1 \leq r \leq k$, *the r-th generalized Hamming weight* of $\mathcal{C}$ is defined by

$$d_r(\mathcal{C}) = \min\{w_S(D_r) : D_r \text{ is an } [n,r] \text{ subcode of } \mathcal{C}\},$$

where $w_S(D)$, called *support size* of D, is the number of coordinates in which some codeword of D has a nonzero entry. The set $\{d_1(\mathcal{C}), d_2(\mathcal{C}), \ldots, d_k(\mathcal{C})\}$ is called the *weight hierarchy* of $\mathcal{C}$. $\mathcal{C}$ is said to satisfy the *chain condition* if there exists a chain

$$D_1 \subseteq D_2 \subseteq \cdots \subseteq D_k,$$

of subcodes of $\mathcal{C}$ satisfying $w_S(D_r) = d_r(\mathcal{C})$, $1 \leq r \leq k$.

Let G_k and G_k^β be defined inductively by

$$G_1 = [0123], \quad G_k = \left[\begin{array}{c|c|c|c} 00\cdots0 & 11\cdots1 & 22\cdots2 & 33\cdots3 \\ \hline G_{k-1} & G_{k-1} & G_{k-1} & G_{k-1} \end{array}\right],$$

$$G_2^\beta = \left[\begin{array}{c|c|c} 1111 & 0 & 2 \\ \hline 0123 & 1 & 1 \end{array}\right], \quad G_k^\beta = \left[\begin{array}{c|c|c} 11\cdots1 & 00\cdots0 & 22\cdots2 \\ \hline G_{k-1} & G_{k-1}^\beta & G_{k-1}^\beta \end{array}\right].$$

Note that columns of G_k consist of all elements of $\mathbb{Z}_4^k$ and no two columns of G_k^β are multiples of each other. The code S_k^α (S_k^β) generated by G_k (G_k^β) over $\mathbb{Z}_4$ is of type α (β) and is called *Simplex code of type α (β).* In[97], Satyanarayana has shown that the Lee weight of every nonzero codeword of S_k^α is 2^{2k} and in[20] Carlet has classified all constant Lee weight codes over $\mathbb{Z}_4$.

For each $a \in \mathbb{Z}_4$, let $\bar{a}$ be the reduction of a modulo 2 then the code $\mathcal{C}^{(1)} = \{(\bar{c_1}, \bar{c_2}, \ldots, \bar{c_n}) : (c_1, c_2, \ldots, c_n) \in \mathcal{C}\}$ is a binary linear code called the *residue code* of $\mathcal{C}$. It is shown that the residue code of S_k^α $\left(S_k^\beta\right)$ is equivalent to 2^k copies of the extended binary simplex code (2^{k-1} copies of the binary simplex code).

The following theorems that give properties of S_k^α and S_k^β are proved in Chapter 3.

Theorem 0.1 *The Hamming and Lee weight distribution of S_k^α are:*

1. $A_H(0) = 1, A_H(2^{2k-1}) = 2^k - 1, A_H(3 \cdot 2^{2k-2}) = 2^k(2^k - 1)$ *and*

2. $A_L(0) = 1, A_L(2^{2k}) = 2^{2k} - 1$.

   where $A_H(i)(A_L(i))$ *denotes the number of codewords of Hamming (Lee) weight* i *in* S_k^α.

Theorem 0.2 *The Hamming and Lee weight distributions of* S_k^β *are:*

1. $A_H(0) = 1, A_H(2^{2k-2}) = 2^k - 1, A_H(2^{k-3}[3(2^k - 1) + 1]) = 2^k(2^k - 1)$ *and*

2. $A_L(0) = 1, A_L(2^{2k-1}) = 2^k - 1, A_L(2^{k-1}(2^k - 1)) = 2^k(2^k - 1)$.

Thus S_k^α is a $[2^{2k}, 2k, 2^{2k-1}, 2^{2k}]$ and S_k^β is a $[2^{k-1}(2^k - 1), 2k, 2^{2k-2}, 2^{k-1}(2^k - 1)]$ linear code over $\mathbb{Z}_4$. It is further shown that both S_k^α and S_k^β are not $\mathbb{Z}_2$-linear.

Following theorems have been obtained for S_k^α and S_k^β.

Theorem 0.3 S_k^α *satisfies the chain condition and its weight hierarchy is given by*

$$d_r(S_k^\alpha) = \sum_{i=1}^{r} 2^{2k-i} = 2^{2k} - 2^{2k-r}, \quad 1 \leq r \leq 2k.$$

Theorem 0.4 S_k^β *satisfies the chain condition and its weight hierarchy is given by*

$$d_r(S_k^\beta) = n(k) - 2^{k-r-1}(2^k - 2^{\lceil \frac{r}{2} \rceil}), \quad 1 \leq r \leq 2k,$$

where $n(k) = 2^{k-1}(2^k - 1)$.

The description of the code $\mathcal{C}_\phi$ for the simplex codes of type α and β are given by the following theorems.

Theorem 0.5 *Let* $\mathcal{C} = \bar{S_k^\alpha}$, *be the punctured code of* S_k^α. *Then* $\mathcal{C}_\phi$ *is an* $[2^{2k+1} - 2, 2k, 2^{2k}]$ *binary linear code consisting of two copies of binary simplex code* S_{2k} *with Hamming weight distribution same as the Lee weight distribution of* $\bar{S_k^\alpha}$.

Theorem 0.6 *Let $\mathcal{C} = S_k^\beta$. Then $\mathcal{C}_\phi$ is the binary MacDonald code*

$$M_{2k,k} : [2^{2k} - 2^k, 2k, 2^{2k-1} - 2^{k-1}]$$

with Hamming weight distribution same as the Lee weight distribution of S_k^β.

The gray image $\phi(\mathcal{C})$ of a linear code $\mathcal{C}$ over $\mathbb{Z}_4$ is a binary code of even length and the minimum Hamming distance as the minimum Lee distance of $\mathcal{C}$. A natural Question arises : Does there exist a generalized gray map which maps a linear code over $\mathbb{Z}_{p^s}$ to a code over $\mathbb{Z}_p$ having similar properties? Recently Ana *Sălăgean − Mandache* has shown that it is not possible to construct a weight function on $\mathbb{Z}_{p^s}$ for which $\mathbb{Z}_{p^s}$ is isometric to $\mathbb{Z}_p^s$ with the Hamming metric unless $p = s = 2$[98].

In[19], Carlet has introduced the generalized gray map ϕ_G from $\mathbb{Z}_{2^s}$ to $\mathbb{Z}_2^{2^{s-1}}$ and has obtained the $\mathbb{Z}_{2^s}$ version of Kerdock code. ϕ_G is a mapping from $\mathbb{Z}_{2^s}$ onto the Reed Müller code of order 1 and length 2^{s-1}. ϕ_G is defined as a Boolean function $\phi_G(u)$ evaluated on $GF(2^{s-1})$ by :

$$\phi_G(u) : (y_1, y_2, \cdots, y_{s-1}) \mapsto u_s + \sum_{i=1}^{s-1} u_i y_i.$$

Note that ϕ_G is distance preserving[19]. We have used ϕ_G to obtain generalization of theorems 0.5 to 0.6 for codes over $\mathbb{Z}_{2^s}$ in Chapter 4.

The concept of chain condition is extended to the codes over $\mathbb{Z}_{p^s}$ in Chapter 2. In Chapter 5, we have shown that various known self dual codes over $\mathbb{Z}_4$ satisfy the chain condition. The construction of the first order Reed Müller code $\mathcal{R}^{1,m-s+1}$ of length 2^{m-s+1} is also given in Chapter 5. The following theorems are proved in Chapter 5.

Theorem 0.7 *$\mathcal{D}_{2m}, \mathcal{E}_7, \mathcal{E}_7^+$ and $\mathcal{E}_8$ satisfy the chain conditions.*

Theorem 0.8 *Klemm Code $\mathcal{K}_{4m} (m \geq 1)$ and the code $\mathcal{K}_8^{'}$ satisfy the chain condition and the weight hierarchy of $\mathcal{K}_{4m}$ is given by*

$$d_r(\mathcal{K}_{4m}) = \begin{cases} r+1, & 1 \leq r \leq 4m-2 \\ 4m, & r = 4m-1 \ \& \ 4m. \end{cases}$$

Theorem 0.9 *Extended quadratic residue codes QR_8 and QR_{24} over $\mathbb{Z}_4$ satisfy the chain condition.*

Theorem 0.10 *$\mathcal{R}^{1,m-s+1}$ satisfies the chain condition and its weight hierarchy is given by*

$$d_t(\mathcal{R}^{1,m-s+1}) = \begin{cases} \sum_{i=0}^{t-1} 2^{m-s-i}, & 1 \le t \le m-s+1 \\ 2^{m-s+1}, & m-s+1 < t \le m+1. \end{cases}$$

Theorem 0.11 *$\mathcal{R}^{1,m-s+1}$ is $\mathbb{Z}_2$-linear.*

Let p be an odd prime. The Poincaré finite upper half plane is the set

$$H_p := \left\{ x + \sqrt{\delta} y \,\middle|\, x, y \in GF(p), y \neq 0,\ \delta \text{ is a quadratic non residue (q.n.r.)} \pmod p \right\}.$$

In[110], Tiu and Wallace have used it to construct a new class of binary linear code $\mathcal{C}_p$ called *norm quadratic residue (NQR) codes*. The length of each codeword in $\mathcal{C}_p$ is $p(p-1)$, the number of points in H_p. The points in H_p are ordered lexicographically; i.e, $(x, y) < (u, v)$ if $x < u$ or $x = u$ and $y < v$. For each $a \in GF(p)$, the set $B_a = \{(a, 1), (a, 2), \ldots, (a, p-1)\}$ is called a *block*. Let G be the $(p+1) \times p(p-1)$ matrix

$$G = \begin{bmatrix} R_0 \\ R_1 \\ \vdots \\ R_p \end{bmatrix},$$

where each $R_i \in I\!F_2^{p(p-1)}$ is defined as follows.

R_0 has an 1 in position (x, y) if $x^2 - \delta y^2$, the norm of (x, y) in H_p, is a quadratic residue (q.r.) mod p and 0, otherwise. $R_1, R_2, \ldots, R_{p-1}$ are block wise cyclic shifts of R_0 corresponding to blocks $B_0, B_1, \ldots, B_{p-1}$ and R_p is the all one vector.

The code $\mathcal{C}_p$ generated by the matrix G is called the NQR Code[110]. If p is of the form $4m+1$ then Tiu and Wallace[110] have shown that $\dim \mathcal{C}_p \le p$, $d_H \ge p-1$, $\mathcal{C}_p$ is

weakly self dual and that the weight of each codeword is divisible by 4. They conjectured that $dim\ \mathcal{C}_p = p$. In Chapter 6, we show that if p is a prime of the form $4m-1$ then also $\mathcal{C}_p$ satisfies similar properties. The following results are proved for $\mathcal{C}_p$.

Theorem 0.12 $\dim \mathcal{C}_p = p, (p \neq 2)$.

Theorem 0.13 *$PSL_2(p)$ fixes $\mathcal{C}_p$ and acts transitively on the coordinate positions.*

Theorem 0.14 *$\mathcal{C}_p$ is $\mathbb{Z}_4$-linear.*

The *Covering Radius* $R(\mathcal{C})$ of a linear code $\mathcal{C}$ is the least integer R such that spheres of radius R around the codewords cover the whole space. It is known that $R(\mathcal{C})$ is the maximum weight of the coset leader.

The following theorem gives the covering radius of $\mathcal{C}_p$.

Theorem 0.15 *Covering radius of $\mathcal{C}_p$ is $\frac{p(p-1)}{2}$. Moreover $\mathcal{C}_p$ is a normal code with every coordinate acceptable.*

The last chapter concludes with some general remarks.

Acknowledgments

It is better to do the right problem the wrong way than to do the wrong problem the right way. ... Richard W. Hamming (1915-1998)

The best way to learn a craft is to work under the guidance of a skilled professional. I am very grateful to my "guruji" Prof. M. C. Bhandari who has not only made me aware about the beautiful subject of "Algebraic Coding Theory" but also constantly supported me with his many ideas and healthy discussions. It has been a privilege to work with him. Learning how to do research and how to write technical papers from him has been a life time experiences in itself.

I am also grateful to Prof. A. K. Lal for having accepted to be my co-guide. His critical comments and constructive suggestions have helped me to substantially improve the presentation of this thesis.

I am highly indebted to both of my gurus for the patience they have shown in guiding and going through my work.

This is also a unique occasion to express my sincere thanks to many people who have shared time to cooperate with and to help me. First of all I wish to thank Prof. R.K.S. Rathore for continuously inspiring me throughout my stay at IIT K. I also thank with pleasure Prof. U.B. Tewari, Prof. Shobha Madan, Prof. Prabha Sharma, Prof. A. K. Maloo and to all other members of the Mathematics Department, IIT K.

I also thank to Prof. H.L. Janwa and Brajesh Kumar for helping me during my

visits at MRI, Allahabad. I am also thankful to C. Carlet, C. Charnes, C. Ding, M. Harada, Z. Quian, E.M. Rains, J. Wolfmann and J.A. Wood for sending the re/pre prints of their manuscripts.

I wish to thank all my friends who has contributed to make my stay at IIT K as one of the most beautiful periods in my life. Let me express my sincere thanks to my colleagues and batch mates: Chanduka, Durairajan, K. Balaji, S.B. Rao, Mahesh, V.S.N. Kaliprasad and Nemade.

It would be really immodest if i do not appreciate the various facilities provided by IIT Kanpur.

Last but not least, it were the blessings of my parents and family members who have always shadowed me. Its really beyond words to express my feelings regarding them.

Manish K. Gupta

Contents

Chapter 1

Introduction

Men are from Mars, women are from Venus and computers are from hell thats what we say once they makes an error . . . , IEEE Computer Magazine

Information Theory is a field in which profound theoretical investigation often has immediate and far-reaching impact on Technology and practice. Last year it was an exciting time for Information Theory distinguished to celebrate 50^{th} year anniversary of Shannon's seminal paper *A Mathematical Theory of Communication*[101]. Soon after Shannon's paper Richard W. Hamming in 1950 published the paper[51] which together with Golay's paper[41] forms the foundation of the constructive counterpart to Shannon's theory, namely, *Algebraic Coding Theory.* Applications of Coding Theory ranges from deep space communications to consumer electronics. Infact, *" Algebraic Coding Theory is a branch of Engineering with roots in Mathematics and applications to Computer Science."*

The origins of the Binary Code can be traced as far back as the *17th century*, when the *secretary of nature* and the great philosopher of the world *Sir Francis Bacon* devised a binary scheme called *Biliterarie Cipher or omnia per omnia* a five letter binary code first mentioned in *The Advancement of Learning (1605)* and later published in detail in

De Augmentis Scientarum (1623) for encoding his diplomatic secret messages (see web site[4]). After this three men approached the subject from different directions. Early in the 19th century in France *Joseph Marie Jacquard* designed the first binary coded punched cards for operating Looms. The other two men were *George Boole* the English Mathematician whose algebra of propositional calculus forms the basis of the modern design of computer logic and *Emile Baudot* a french engineer whose cyclic-permuted code (now often called *Gray code* as it was patented by *Frank Gray* on 17.03.1953[46]) represented a major advance in telegraphy. There are various other applications of this code like solving puzzles such as Tower of Hanoi and the Brain. It is very recent when it was used in solving a 30 year old coding theory puzzle[53].

The key idea of this puzzle can be described in few sentences. For many years it was observed that binary nonlinear Preparata and Kerdock codes satisfy the duality relations and they appeared to be duals to each other. Many researchers viz MacWilliams, Sloane etc. worked hard to explain this mystery. The answer turns out to be astonishingly simple. In 1994, Hammons et al have shown that both Kerdock and Preparata codes are gray images of linear codes over $\mathbb{Z}_4$, which are dual to each other. This has motivated a great deal of research in Codes over $\mathbb{Z}_4$ and in general Codes over $\mathbb{Z}_{p^s}$[113], [15]*etc.* Though there were few papers on codes over the ring of integers modulo q in early seventies, it was forgotten by the researchers partly because of the presence of the zero divisors. These codes also found various other applications like orthogonal frequency division multiplexing (OFDM), phase modulated channels etc. to diverse areas such as bent functions and various lattice constructions.

There are various binary linear codes studied so far by several researchers[79]. Some important class of binary codes are Hamming code, the first order Reed Müller code and Simplex code. Any nonzero codeword of the simplex code has many of the properties that we would expect from a sequence obtained by tossing a fair coin $2^m - 1$ times.

This randomness makes these codewords very useful in a number of applications such as range-finding, synchronizing, modulation, scrambling etc. Similar properties holds for the binary first order Reed Müller code. This family of code is one of the few for which maximum likelihood decoding is practical. Hamming code is the dual of the simplex code. All these codes have been generalized to codes over $GF(q)$. A binary code of even length is said to be $\mathbb{Z}_4$-linear if upto suitable permutation of coordinates it is the image of some linear code over $\mathbb{Z}_4$. In[53], Hammons et al have shown that the first order Reed Müller code, Kerdock code and Preparata code are $\mathbb{Z}_4$-linear. Since then many researchers have constructed various linear codes over $\mathbb{Z}_4$ and over $\mathbb{Z}_{p^s}$ and studied their gray images (see[113],[15],[53],[21] etc.).

In the present dissertation, we have constructed Simplex code of type α and β over $\mathbb{Z}_4$ and over $\mathbb{Z}_{2^s}$. Some fundamental properties like 2-dimension, Hamming, Lee and Generalized Lee weight distributions, weight hierarchy etc. are determined for these codes. It is shown that binary images of these codes give rise to some interesting binary codes. The concept of chain condition defined for $GF(q)$ is extended to codes over $\mathbb{Z}_{2^s}$.

In[110], Tiu and Wallace constructed a binary linear family of self orthogonal codes C_p based on the concept of quadratic residue and conjectured that $\dim(\mathrm{C}_p) = p$. We have proved the conjecture and extended the construction to any odd prime p. It is shown that C_p is $\mathbb{Z}_4$-linear.

This dissertation is divided into seven chapters. Chapter 2 contains preliminary definitions and a brief survey of known results on codes over $GF(q)$, and codes over integer modulo p^s. Some new results are also included.

Chapter 3 introduces Simplex codes of type α and type β, denoted S_k^α and S_k^β over $\mathbb{Z}_4$. Basic properties like 2- dimension, weight hierarchy, and Symmetrized weight enumerator etc. are obtained in section 1. The gray images of these codes are constructed in two ways and some interesting linear and nonlinear binary families are obtained. It

is also shown that both S_k^{α} and S_k^{β} satisfy the chain condition.

Chapter 4 deals with simplex codes of type α and β over $\mathbb{Z}_{2^s}$. Using the generalized gray map introduced by Carlet, the result obtained in Chapter 3 over $\mathbb{Z}_4$ are extended for Simplex codes of type α and β over $\mathbb{Z}_{2^s}$.

The concept of chain condition for various self-dual and self-orthogonal codes over $\mathbb{Z}_4$ is studied in chapter 5. Section 1 deals with self dual codes of length at most 9 or of length $2m$ and $4m$. A construction and some of the fundamental properties of the first order Reed Müller code over $\mathbb{Z}_{2^s}$ is given in section 2.

In Chapter 6, we study binary linear Norm Quadratic Residue (NQR) codes C_p for any odd prime p. It is shown that C_p is $\mathbb{Z}_4$ linear, $\dim(\mathrm{C}_p) = p$ and its covering radius is $\frac{p(p-1)}{2}$.

The thesis concludes with some general remarks in the last chapter.

Chapter 2

Preliminaries and Survey

If you are faced by a difficulty or a controversy in science, an ounce of algebra is worth a ton of verbal argument. ... J.B.S. Haldane (1892-1964)

2.1 Introduction

A nonempty set S with two binary operations '+' and '.' (called addition and multiplication) is a *ring* if (i) $< S, + >$ is an abelian group, (ii) '.' is associative , and (iii) distributive laws hold. If in addition, $a.b = b.a$ for all $a, b \in S$, S is called a *commutative* ring. If S contains a multiplicative identity, denoted 1, then S is called a *ring with unity*. A nonzero element 'a' in a ring S with 1 is called a *unit* if there exists $b \in S$ such that $a.b = b.a = 1$. A commutative ring with 1 in which every nonzero element is a unit is called a *field*. It is known that a finite field with q elements exists if and only if q is a prime power. A finite field having q elements is unique up to isomorphism, called the *Galois field*, denoted $GF(q)$.

Let q be a positive integer. The set $\mathbb{Z}_q$ of all equivalent classes of integers modulo q, with respect to addition and multiplication modulo q, forms a commutative ring with unity. If p is a prime and s is a positive integer then the set of all units in $\mathbb{Z}_{p^s}$ is

the set $U = \{ap + b | 0 \leq a \leq p^{(s-1)} - 1, 1 \leq b \leq p - 1\}$. The set of zero divisors in $\mathbb{Z}_{p^s}$ is given by $Z = \{ap | 0 \leq a \leq p^{s-1} - 1\}$.

Let S be a commutative ring with unity. An abelian group $< \mathcal{M}, + >$ is called a left S-module if there exists a function $\mu : S \times \mathcal{M} \rightarrow \mathcal{M}$ denoted by $\mu(\alpha, a)$ satisfying (i) $\mu(\alpha, a + b) = \mu(\alpha, a) + \mu(\alpha, b)$, (ii) $\mu(\alpha\beta, a) = \mu(\alpha, \mu(\beta, a))$, (iii) $\mu(\alpha + \beta, a) = \mu(\alpha, a) + \mu(\beta, a)$, (iv) $\mu(1, a) = a$. $\forall \alpha, \beta \in S$ and $a, b \in \mathcal{M}$. The set $S^n = \{x = (x_1, x_2, \ldots, x_n) | x_i \in S\}$ is a left S-module.

A subset $\mathcal{B}$ of $\mathcal{M}$ is a generating set for $\mathcal{M}$ if every element of $\mathcal{M}$ is a finite linear combination of elements in $\mathcal{B}$ over S. $\mathcal{B}$ is called a basis for $\mathcal{M}$ if the above representation is unique for each element of $\mathcal{M}$. A module which admits a basis is called a *free* module. If S is a field then a left S-module $\mathcal{V}$ is called a vector space. It is well known that every vector space has a basis. Moreover, if $\mathcal{V}$ has a finite basis then any two bases for $\mathcal{V}$ have the same number of elements. In such a case, if $|\mathcal{B}| = n$, then $\mathcal{V}$ is called an n-dimensional vector space and we write, dim $\mathcal{V} = n$. If S is a field then S^n is an n-dimensional vector space over the field S.

Let $\mathbb{F}_q$ be a set of q-alphabets. A code $\mathcal{C}$ of length n and size M is a subset of $\mathbb{F}_q^n$ having M elements. The elements of $\mathcal{C}$ are called *codewords*. In order to be able to correct errors, if any, arising out of noise one would like to have some algebraic structure attached to the set $\mathbb{F}_q$ of alphabets. If q is a prime power one usually takes $\mathbb{F}_q$ to be $GF(q)$ and otherwise $\mathbb{F}_q = \mathbb{Z}_q$. Let $\mathbb{F}_q = GF(q)(\mathbb{Z}_q)$ and let $\mathcal{C} \subseteq \mathbb{F}_q^n$. If $\mathcal{C}$ is a subspace (submodule) of $\mathbb{F}_q^n$ then $\mathcal{C}$ is called a *linear code* over $\mathbb{F}_q$. In case $\mathbb{F}_q = GF(2)(GF(3))$ then $\mathcal{C}$ is called a *binary (ternary)* code.

Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$. The number of nonzero components in $\mathbf{x}$ is called the *Hamming weight* of $\mathbf{x}$, denoted $w_H(\mathbf{x})$. *Hamming distance* $d_H(\mathbf{x}, \mathbf{y})$ between $\mathbf{x}$ and $\mathbf{y}$ is the number of coordinates in which they differ. Note that for $\mathbf{x}, \mathbf{y} \in \mathcal{C}$, $d_H(\mathbf{x}, \mathbf{y}) = w_H(\mathbf{x} - \mathbf{y})$. Let $d_H = min\{d_H(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\}$. d_H is called the *minimum Hamming distance*

of $\mathcal{C}$. A code $\mathcal{C}$ with minimum Hamming distance d_H can correct up to $\lfloor \frac{(d_H-1)}{2} \rfloor$ errors using nearest neighborhood decoding. Almost all codes in classical coding theory are defined for the Hamming distance. Hamming distance codes are ideal for the balanced channel in which error probability of each symbol is same. In 1958, C. Y. Lee, defined Lee distance which is suitable for memory less, discrete and symmetric channels[75]. Another useful distance is the Euclidean distance. The Lee (Euclidean) weight of an element $a \in \mathbb{Z}_q$ is given by $w_L(a) = min\{a, q-a\}$ $(w_E(a) = (w_L(a))^2)$. The *Lee (Euclidean) weight* of a vector $\mathbf{x} \in \mathbb{Z}_q^n$ is the sum of the Lee (Euclidean) weights of its components. For $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_q^n$, $d_L(\mathbf{x}, \mathbf{y}) = w_L(\mathbf{x}-\mathbf{y})(d_E(\mathbf{x}, \mathbf{y}) = w_E(\mathbf{x}-\mathbf{y}))$ is called the *Lee (Euclidean) distance* between $\mathbf{x}$ and $\mathbf{y}$. For binary codes the concept of Hamming, Lee and Euclidean distance coincide while for ternary codes the Hamming and Lee weight coincide. The minimum Lee (Euclidean) distance $d_L(d_E)$ of a code $\mathcal{C}$ is defined analogously. The choice of distance for any code depends on the decoding procedure and the channel under consideration.

Let $\mathbb{F}_q = GF(q)(\ \mathbb{Z}_q)$ and let $\mathcal{C} \subseteq \mathbb{F}_q^n$. If $\mathcal{C}$ has M codewords and minimum Hamming, Lee and Euclidean distances as d_H, d_L and d_E respectively then $\mathcal{C}$ is called an (n, M, d_H, d_L, d_E) code. If in addition, for $\mathbb{F}_q = GF(q)$, $\mathcal{C}$ is linear and dim $\mathcal{C}$ = k then $\mathcal{C}$ is called an $[n, k, d_H, d_L, d_E]$ or simply an $[n, k]$ code if we do not wish to specify distances. Any $[n, k]$ linear code $\mathcal{C}$, being a subspace can be specified either by a $k \times n$ generator matrix G (rows of G form a basis for $\mathcal{C}$) or by an $(n-k) \times n$ full rank matrix H (called *parity-check matrix*) whose solution space is $\mathcal{C}$. Therefore, $\mathcal{C}$ must contain a codeword of Hamming weight $n-k+1$ and hence

$$d_H \leq n - k + 1. \tag{2.1}$$

This bound is called the *Singleton bound* for Hamming distance. For given k and d_H the minimum value of n for which there exists an $[n, k, d_H]$ code is denoted by $n_q(k, d_H)$. In 1965 Solomon and Stiffler[105] have shown that $n_q(k, d_H) \geq \sum_{i=0}^{k-1} \left\lceil \frac{d_H}{q^i} \right\rceil \equiv g_q(k, d_H)$.

The binary version of this was first proved by Griesmer in 1960[49]. A code meeting this bound is called a *Griesmer code*. An $[n_q(k, d_H), k, d_H]$ code is called an *optimum code*.

In 1991, V. K. Wei introduced the notion of Generalized Hamming weights for binary linear codes[115]. This was later extended to linear codes over $GF(q)$ by Klove et al[72] and to linear codes over $\mathbb{Z}_4$ by Ashikhmin[1]. It has been further studied by many researchers[60],[72],[59],[61],[22],[73]. Let $\mathcal{C}$ be an $[n, k]$ linear code over $GF(q)$ and let $1 \leq r \leq k$. The *r-th Generalized Hamming weight(GHW)* , $d_r(\mathcal{C})$, of $\mathcal{C}$ is defined by

$$d_r(\mathcal{C}) = \min\{w_S(D) \mid D \text{ is an } [n, r] \text{ subcode of } \mathcal{C}\},$$

where $w_S(D)$, called the *support size* of D, is the number of coordinates in which some codeword of D has a nonzero entry. The set $\{d_1(\mathcal{C}), d_2(\mathcal{C}), \ldots, d_k(\mathcal{C})\}$ is called the *weight hierarchy* of $\mathcal{C}$. The following theorem summarizes some of the basic properties of the weight hierarchy of $\mathcal{C}$.

Theorem 2.1 *Let $\mathcal{C}$ be an $[n, k]$ linear code over $GF(q)$. Then*

1. *(Monotonicity):* $1 \leq d_1(\mathcal{C}) < d_2(\mathcal{C}) < \cdots < d_k(\mathcal{C}) \leq n$
2. *(Generalized Singleton Bound):*
   $d_r(\mathcal{C}) \leq n - k + r$; *for* $1 \leq r \leq k$ *(r=1 yields (2.1)).*
3. *(Duality):* $\{d_r(\mathcal{C}) : 1 \leq r \leq k\} = \{1, 2, \ldots, n\} \backslash \{n + 1 - d_r(\mathcal{C}^{\perp}) : 1 \leq r \leq n - k\}$

In[60], Helleseth, Klove, Levenshtein and Ytrehus have proved the following lemma connecting the Hamming weight distribution and support size of any linear code $\mathcal{C}$.

Lemma 2.2 *If $\mathcal{D}$ is an $[n, r]$ linear code over $GF(q)$ then*

$$\sum_{\mathbf{c} \in \mathcal{D}} w_H(\mathbf{c}) = q^{r-1}(q-1)w_S(\mathcal{D}).$$

Thus, an alternative definition of $d_r(\mathcal{C})$ is given by

$$d_r(\mathcal{C}) = \frac{1}{q^{r-1}(q-1)} min \left\{ \sum_{\mathbf{d} \in D_r} w_H(\mathbf{d}) : D_r \text{ is an } [n,r] \text{ subcode of } \mathcal{C} \right\}.$$

In another paper[116], Wei and Yang have introduced the concept of chain condition for studying the weight hierarchies of linear codes. A linear code $\mathcal{C}$ is said to satisfy the *chain condition* if there exists a chain

$$D_1 \subseteq D_2 \subseteq \cdots \subseteq D_k,$$

of subcodes of $\mathcal{C}$ satisfying $w_S(D_r) = d_r(\mathcal{C})$, $1 \leq r \leq k$. It is known that almost all good codes over $GF(q)$ satisfy the chain condition[31],[23],[32],[24]. The weight hierarchies of linear codes over finite fields play an important role in Cryptography, for example, Wire-Tap Channel-II (WTC-II)[84]. For various other applications see[67],[56],[115] etc. In[2], Ashikhmin has shown that Octacode code over $\mathbb{Z}_4$ is better (from the point of view of GHW) than any optimal linear code over $GF(4)$ of the same length and cardinality.

Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$. The standard inner product of $\mathbf{x}$ and $\mathbf{y}$ is the scalar $< \mathbf{x}, \mathbf{y} >= \sum_{i=1}^{n} x_i y_i$ in $\mathbb{F}_q$. The subset $\mathcal{C}^{\perp} = \{\mathbf{x} \in \mathbb{F}_q^n | < \mathbf{x}, \mathbf{c} >= 0, \forall \mathbf{c} \in \mathcal{C}\}$ is called the *dual code* of $\mathcal{C}$. It is easy to verify that $|\mathcal{C}||\mathcal{C}^{\perp}| = |\mathbb{F}_q^n|$ and $\mathcal{C}^{\perp\perp} = \mathcal{C}$. If $\mathcal{C}$ is an $[n,k]$ linear code over a field then $\mathcal{C}^{\perp}$ is an $[n, n-k]$ linear code. Moreover, G is a generator matrix of $\mathcal{C}$ if and only if, G is a parity-check matrix of $\mathcal{C}^{\perp}$. If $\mathcal{C} = \mathcal{C}^{\perp} (\mathcal{C} \subset \mathcal{C}^{\perp})$ then $\mathcal{C}$ is called a *self-dual (self orthogonal or weakly self dual)* code. A self dual linear code $\mathcal{C}$ over a field must have even length. However this need not be true for codes over $\mathbb{Z}_4$. In[87] Pless et al have constructed self dual codes of odd lengths over $\mathbb{Z}_4$. A self dual code over $\mathbb{Z}_q$, q even, is called a code of *type II(I)* if all the Euclidean weights are divisible by $2q(q)$. For details on self dual codes, see the excellent survey written by Rains and Sloane[92].

Two codes are said to be *equivalent* if one can be obtained from the other by applying finitely many operations of the type (i) permutation of coordinates, (ii) multiplying one or more coordinates by a unit. A mapping $\theta : \mathcal{C} \to \mathcal{C}$ is called an *automorphism* of $\mathcal{C}$ if θ is $1-1$, onto and a homomorphism. The collection of all automorphisms of $\mathcal{C}$ is a group called the *automorphism group* of $\mathcal{C}$, denoted $Aut(\mathcal{C})$.

For each $1 \leq i \leq n$, let $A_H(i)(A_L(i))$ be the number of codewords of Hamming (Lee) weight i in $\mathcal{C}$. Then $\{A_H(0), A_H(1), \ldots, A_H(n)\}$ $(\{A_L(0), A_L(1), \ldots, A_L(n)\})$ is called the *Hamming (Lee) weight distribution* of $\mathcal{C}$. The *Hamming weight enumerator (hwe)* of $\mathcal{C}$ is a polynomial defined by

$$W_{\mathcal{C}}(x,y) \text{ or } Ham_{\mathcal{C}}(x,y) = \sum_{\mathbf{c}\in\mathcal{C}} x^{n-w_H(\mathbf{c})} y^{w_H(\mathbf{c})} = \sum_{i=0}^{n} A_H(i) x^{n-i} y^i.$$

There is an analogous definition for nonlinear codes. *Complete weight enumerator(cwe)* for a code $\mathcal{C}$ over $\mathbb{Z}_{p^s}$ is defined as follows. Let $m = p^s - 1$, and let $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$. For each $j \in \mathbb{Z}_{p^s}$, let $\omega_j(\mathbf{c}) = |\{k : c_k = j\}|$. Then the *cwe* is the polynomial $cwe_{\mathcal{C}}(x_0, \ldots, x_m) = \sum_{\mathbf{c}\in\mathcal{C}} {x_0}^{\omega_0(\mathbf{c})} {x_1}^{\omega_1(\mathbf{c})} \cdots {x_m}^{\omega_m(\mathbf{c})}$. Note that permutation equivalent codes have the same cwe but in general two equivalent codes may have different cwe's. The appropriate weight enumerator for an equivalent class of codes is called a *Symmetrized weight enumerator(swe)*. For example, the swe of a code over $\mathbb{Z}_4$ is the polynomial: $swe(x,y,z) = cwe(x,y,z,y)$. The *Lee weight enumerator* of $\mathcal{C}$ is the homogeneous polynomial of degree $2n$ given by $Lee_{\mathcal{C}}(x,y) = \sum_{\mathbf{c}\in\mathcal{C}} x^{2n-w_L(\mathbf{c})} y^{w_L(\mathbf{c})}$. The Hamming weight enumerators of code $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are connected by the identity

$$Ham_{\mathcal{C}^{\perp}} = \frac{1}{|\mathcal{C}|} Ham_{\mathcal{C}}(x+y, x-y) \tag{2.2}$$

called the *MacWilliams identities*. Similar identities have been obtained for codes over rings[92]. The following analogue of (2.2) holds for codes over $\mathbb{Z}_4$.

$swe_{\mathcal{C}^{\perp}}(x,y,z) = \frac{1}{|\mathcal{C}|} swe_{\mathcal{C}}(x+2y+z, x-z, x-2y+z)$.

$Lee_{\mathcal{C}^{\perp}}(x,y) = \frac{1}{|\mathcal{C}|} Lee_{\mathcal{C}}(x+y, x-y)$.

$Ham_{\mathcal{C}^{\perp}}(x,y) = \frac{1}{|\mathcal{C}|} Ham_{\mathcal{C}}(x+3y, x-y)$.

2.2 Classical Codes over $GF(q)$

Let $\mathbb{F}_q = GF(q) = \{0, 1, \alpha_3, \ldots, \alpha_q\}$. For a given k and q, let $G_k(q)$ be a $k \times (q^k - 1)/(q-1)$ matrix over $\mathbb{F}_q$ in which any two columns are linearly independent. The code $S_k(q)$ generated by the matrix $G_k(q)$ is called the *Simplex code*. Note that $S_k(q)$ is a $\left[(q^k-1)/(q-1), k, q^{k-1}\right]$ code. It is known that any linear code with the above parameters is equivalent to $S_k(q)$[40]. $G_k(q)$ can be defined inductively by

$$G_2(q) = \begin{bmatrix} 0 & 1 & 1 & \alpha_3 & \cdots & \alpha_{q-1} & \alpha_q \\ 1 & 0 & 1 & 1 & \cdots & 1 & 1 \end{bmatrix},$$

and

$$G_k(q) = \left[\begin{array}{c|c|c|c|c|c} 00\cdots0 & 1 & 11\cdots1 & \alpha_3\cdots\alpha_3 & \cdots & \alpha_q\cdots\alpha_q \\ \hline G_{k-1}(q) & \mathbf{0} & G_{k-1}(q) & G_{k-1}(q) & \cdots & G_{k-1}(q) \end{array}\right].$$

Every nonzero codeword of $S_k(q)$ has weight q^{k-1}. The binary simplex code (usually denoted S_k) was first discovered by Ronald A. Fisher[35] in 1942 in connection with statistical designs. In 1945, it was further generalized to arbitrary prime powers[36]. The dual of the Simplex code is the well known $\left[\frac{q^k-1}{q-1}, \frac{q^k-1}{q-1} - k, 3\right]$ *Hamming Code*.

A nice way to construct new codes is by puncturing or appending one or more coordinates of a known code. Let $1 \leq u \leq k-1$ and let $G_{k,u}(q)$ be the matrix obtained from $G_k(q)$ by deleting columns corresponding to the columns of the matrix $G_u(q)$, i.e,

$$G_{k,u}(q) = \left[\begin{array}{c} G_k(q) \end{array} \setminus \begin{array}{c} \mathbf{0} \\ \hline \mathbf{G_u(q)} \end{array}\right],$$

where $\mathbf{0}$ is a $(k-u) \times \frac{q^u-1}{q-1}$ zero matrix and $[A \backslash B]$ denotes the matrix obtained from the matrix A by deleting the columns of the matrix B. The code $\mathcal{M}_{k,u}(q)$ generated by the matrix $G_{k,u}(q)$ is the punctured code of $S_k(q)$ and is called a *MacDonald code*. $\mathcal{M}_{k,u}(q)$ is a $\left[\frac{q^k-q^u}{q-1}, k, q^{k-1} - q^{u-1}\right]$ code in which every nonzero codeword has weight either q^{k-1} or $q^{k-1} - q^{u-1}$[77].

In 1954, I. S. Reed and R. Müller constructed a $\left[2^m, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r}\right]$ binary linear code, denoted $RM(r,m)$, called the r^{th}-*order Reed Müller code* for all $m \geq 0$, $0 \leq r \leq m$. If $G(r,m)$ is a generator matrix for $RM(r,m)$ then

$$G(r+1,m+1) = \begin{bmatrix} G(r+1,m) & G(r+1,m) \\ \mathbf{0} & G(r,m) \end{bmatrix}$$

is a generator matrix for $RM(r+1,m+1)$. Further $RM(r,m)^{\perp} = RM(m-r-1,m)$.

Let $A(n,d_H) = \max\{M|$ there exists a binary (n,M,d_H) code$\}$. It is known that $A(16,6) \leq 2^8 = 256$. Hence a question arose whether there exists a $(16,256,6)$ code or not? In[83], Nordstrom constructed a $(16,256,6)$ nonlinear code popularly known as *Nordstrom Robinson code*. In 1968, Preparata generalized this by constructing a $(2^m, 2^{(2^m-2m)}, 6)$ binary nonlinear code, $P(m)$, called *Preparata code* for m even and $m \geq 4$ [89]. Another construction of a $\left(2^m, 2^{2m}, 2^{m-1} - 2^{(m-2)/2}\right)$ binary nonlinear code $K(m)$, called *Kerdock code* for m even and $m \geq 4$ was given by Kerdock in 1972 [70]. For $m = 4$, $P(4) = K(4)$. Further nonlinear generalizations were later found by Goethals, Delsarte and Hergert[28],[42],[43],[62].

2.3 Codes over Integer Residue Rings

Codes over $\mathbb{Z}_q$ have various applications including phase modulated channels[6],[81], multifrequency phase telegraphy[82], multilevel quantized pulse amplitude modulated channels[6], multilevel transmission system[80], multiplexing in multiaccess communication system[109], multichannel communication[109]etc. By Chinese Remainder theorem, the study of codes over $\mathbb{Z}_q$ can be reduced to the study of codes over $\mathbb{Z}_{p^s}$. Many different kind of codes over $\mathbb{Z}_q$ have been constructed in seventies by Blake[7],[8], Spigel(1977)[106], Priti Shankar (1979)[100] etc. In early eighties not much attention was paid to such codes[114]. This is partly due to the difficulties arising due to the presence of zero divisors in $\mathbb{Z}_{p^s}$. In 1989, P. Solé[104] discovered a family of nearly optimal

four-phase sequences of period $2^{2r+1}-1$ with alphabet $1, i, -1, -i$, where $i = \sqrt{-1}$. This was also found independently by Boztas, Hammons and Kumar in 1990 [13]. The above family may be viewed as a linear code over $\mathbb{Z}_4$ by identifying the alphabet i^a by its exponent a. When studying these four-phase sequences, Hammons and Kumar and later independently Calderbank, Sloane and Solé noticed the resemblance between the 2-base expansion of the quaternary codewords and the standard construction of the Kerdock codes. Thus they realized that the Kerdock code is simply the image of a linear code over $\mathbb{Z}_4$ under a suitable map. In October 1992, in a DIMACS/IEEE workshop M. D. Trott, acting on a suggestion by Forney proved that the Nordstrom-Robinson (NR) code is the binary image of a linear code over $\mathbb{Z}_4$, called *Octacode*[38]. However, this was already known to Hammons and Kumar in June 1992 [13]. After realizing that they are working on the same problem they formed a group. Combined efforts of the group lead to an award winning paper[53] in which they could map various good nonlinear binary families of codes to some linear codes over $\mathbb{Z}_4$. They have shown that Kerdock and Preparata codes are actually dual to each other when viewed as a linear code over $\mathbb{Z}_4$. They observed that ($\mathbb{Z}_4^n$, Lee distance) and ($\mathbb{Z}_2^{2n}$, Hamming distance) are isometric to each other and hence obtained the explanation for the mysterious connection $|P(m)||K(m)| = 2^{2^m}$.

The mapping $\phi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2^2$ defined by $\phi(0) = 00, \phi(1) = 01, \phi(2) = 11$ and $\phi(3) = 10$ is called the *Gray map*. It is extended from $\mathbb{Z}_4^n \rightarrow \mathbb{Z}_2^{2n}$ by applying ϕ to each coordinate and is popularly known as *Gray map*. It was used by F. Gray to avoid large errors in transmitting signals by pulse code modulation (PCM) in 1940's. Clearly, Gray map is distance preserving[53].

If $\mathcal{C}$ is a linear code over $\mathbb{Z}_4$ then $\phi(\mathcal{C})$ will denote the image of $\mathcal{C}$ under the Gray map. $\mathcal{C}$ is called $\mathbb{Z}_2$-*Linear* if $\phi(\mathcal{C})$ is a binary linear code. A binary code is said to be $\mathbb{Z}_4$-*linear* if it is equivalent to $\phi(\mathcal{C})$ for some linear code $\mathcal{C}$ over $\mathbb{Z}_4$. A necessary and

sufficient conditions for $\mathbb{Z}_4$-linearity ($\mathbb{Z}_2$-linearity) is given by the following Theorem.

Theorem 2.3 Hammons et al*[53]*

1. *A binary linear code C of even length is $\mathbb{Z}_4$-linear if and only if its coordinates can be permuted so that*

$$\mathbf{u}, \mathbf{v} \in C \Rightarrow (\mathbf{u} + \sigma(\mathbf{u})) \star (\mathbf{v} + \sigma(\mathbf{v})) \in C \tag{2.3}$$

   where σ is the swap map that interchanges the left and the right halfs of a vector and $\star$ denotes the componentwise product of two vectors.

2. *For each $a \in \mathbb{Z}_4$, let $\bar{a}$ be the reduction of a modulo 2 and let $\mathcal{C}$ be a linear code over $\mathbb{Z}_4$, then $\mathcal{C}$ is $\mathbb{Z}_2$-linear if and only if $\mathbf{c} = (c_1, \ldots, c_n)$ and $\mathbf{c}' = (c_1', \ldots, c_n') \in \mathcal{C}$ implies $2\bar{\mathbf{c}} \star \bar{\mathbf{c}}' = (2\bar{c_1}\bar{c_1}', \ldots, 2\bar{c_n}\bar{c_n}') \in \mathcal{C}$.*

It is known that the r^{th} order binary Reed Müller code $R(r, m)$ is $\mathbb{Z}_4$-linear for $r = 0, 1, 2, m-1$ and m[53] and is not $\mathbb{Z}_4$- linear for other values of r[63]. The Golay code and the extended Hamming code of length $n = 2^m (m \geq 5)$ are not $\mathbb{Z}_4$-linear[53].

Let $h_2(x) \in \mathbb{Z}_2[x]$ be an irreducible polynomial over $\mathbb{Z}_2$ such that $h_2(x)|(x^n - 1)$ over $\mathbb{Z}_2$. Then *Hensel lemma* (see[78]) guarantees the existence of a polynomial $h(x) \in \mathbb{Z}_4[x]$ such that (i) $h(x) \equiv h_2(x) \pmod 2$, (ii) $h(x)|(x^n - 1)$ over $\mathbb{Z}_4$. This polynomial $h(x)$ can be obtained, for example, by *Graffe's method*, called the *Hensel uplift* of $h_2(x)$[11]. In[53], Hammons et al have shown that the gray image of the Hensel uplift of the first order Reed Müller code $R(1, m)$ is the Kerdock code and the Gray image of the Hensel uplift of the extended Hamming code is Preparata code (differ slightly from classical Preparata code but shares the same distance structure). Thus these nonlinear codes are extended cyclic codes over $\mathbb{Z}_4$. This process of Hensel uplifts can be continued till $\mathbb{Z}_{2^s}$ or in general up to the ring of 2-adic integers.

The classical Theory of cyclic codes over finite fields was extended to cyclic codes over $\mathbb{Z}_4$ by Pless and Quian[88] and over $\mathbb{Z}_{p^s}$ by Pramod Kanwar and Permouth[68].

Some basic theorems giving the structure of cyclic codes of length n over $\mathbb{Z}_{p^s}$ and over the p-adic numbers was considered by Calderbank and Sloane[15]. A generalization of McEliece theorem that characterizes the possible Hamming weights of a binary cyclic code was given by Calderbank, Li and Poonen[17].

2.4 Codes over $\mathbb{Z}_{p^s}$

Let $\mathcal{C}$ be a linear code of length n over $\mathbb{Z}_{p^s}$. Then $\mathcal{C}$ is a finite abelian group of type $p^{sk_0}p^{(s-1)k_1}\cdots p^{k_{s-1}}$ with $\sum_{i=0}^{s} k_i = n$ and k_i $(0 \le i \le s)$ are nonnegative integers[15]. Using this Calderbank and Sloane[15] have shown that $\mathcal{C}$ has a generator matrix G (rows of G generate $\mathcal{C}$) of the form

$$G = \begin{bmatrix} I_{k_0} & A_{01} & A_{02} & \cdots & A_{0s-1} & A_{0s} \\ \mathbf{0} & pI_{k_1} & pA_{12} & \cdots & pA_{1s-1} & pA_{1s} \\ \mathbf{0} & \mathbf{0} & p^2I_{k_2} & \cdots & p^2A_{2s-1} & p^2A_{2s} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & p^{s-1}I_{k_{s-1}} & p^{s-1}A_{s-1s} \end{bmatrix}, \tag{2.4}$$

where A_{ij} are matrices over $\mathbb{Z}_{p^s}$ and the columns are grouped into blocks of size k_0, k_1, $\cdots$, k_{s-1}, k_s. Let $k = \sum_{i=0}^{s-1}(s-i)k_i$. Then $|\mathcal{C}| = (p^s)^{\sum_{i=0}^{s-1} k_i} / \left(1^{k_0}p^{k_1}(p^2)^{k_2}\cdots(p^{s-1})^{k_{s-1}}\right)$ which is equal to p^k. Note that $\mathcal{C}$ is a free module if and only if $k_i = 0$ for all $i = 1, 2, \cdots, s-1$. It is easy to see that a generator matrix for $\mathcal{C}^{\perp}$ is of the form

$$H = \begin{bmatrix} B_{0s} & B_{0s-1} & \cdots & B_{01} & I_{k_s} \\ pB_{1s} & pB_{1s-1} & \cdots & pI_{k_{s-1}} & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ p^{s-1}B_{s-1s} & p^{s-1}I_{k_1} & \cdots & \mathbf{0} & \mathbf{0} \end{bmatrix},$$

where B_{ij} are matrices over $\mathbb{Z}_{p^s}$ and the columns are grouped into blocks of size $k_s, k_{s-1}, \cdots, k_1$. Therefore $|\mathcal{C}^{\perp}| = (p^s)^{\sum_{i=0}^{s-1} k_i} / \left(1^{k_s}p^{k_{s-1}}(p^2)^{k_{s-2}}\cdots(p^{s-1})^{k_1}\right) = p^{sn-k}$.

Note that $sn - k = \sum_{i=1}^{s} ik_i$.

2.4.1 p-dimension of Linear Codes over $\mathbb{Z}_{p^s}$

The presence of zero divisors in $\mathbb{Z}_{p^s}$ creates problem in defining linear dependence of vectors in $\mathbb{Z}_{p^s}^n$. For example, the following two statements are equivalent for a subset D of a vector space over a field.

1. A nontrivial linear combination of vectors in D is zero.

2. One of the vector in D is a linear combination of some other vectors of D.

However, these are not equivalent for modules over $\mathbb{Z}_{p^s}$. For example, the subset $D = \{(1,2),(1,0)\}$ of $\mathbb{Z}_4^2$ satisfies 1 but not 2. Also, note that the module generated by (2,0) and (0,2) over $\mathbb{Z}_4$ are properly contained in the module generated by (1,0) and (0,1). Consequently, defining the dimension of a module as a cardinality of its basis is not meaningful. Recently, while studying Trellis description of linear codes over $\mathbb{Z}_{p^s}$ Vazirani, Saran and Sundar Rajan[112] have introduced the following notion of p-dimension for finitely generated modules over $\mathbb{Z}_{p^s}$.

A vector $\mathbf{v} \in \mathbb{Z}_{p^s}^n$ is a *p-linear combination* of the vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k$ if $\mathbf{v} = \sum_{i=1}^{k} \lambda_i \mathbf{v}_i$ with $\lambda_i \in \mathbb{Z}_p$; $1 \leq i \leq k$. Let $D = \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k\}$ be an ordered subset of $\mathbb{Z}_{p^s}^n$. Then p-span of D is the set $\left\{\sum_{i=1}^{k} a_i \mathbf{v}_i : a_i \in \mathbb{Z}_p\right\}$. D is called a *p-generating sequence* if for each $i = 1, 2, \cdots, k-1$, $p\mathbf{v}_i$ is a p-linear combination of $\mathbf{v}_{i+1}, ..., \mathbf{v}_k$ and $p\mathbf{v}_k = 0$. If in addition, $\mathbf{0}$ is a nontrivial p-linear combination of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k$ then D is called *p-linearly dependent*. A subset $\mathcal{B}$ of $\mathcal{C}$ is a *p-basis* for the linear code $\mathcal{C}$ over $\mathbb{Z}_{p^s}$ if $\mathcal{B}$ is p-linearly independent and $\mathcal{C}$ is the p-span of $\mathcal{B}$. The number of vectors in any two p-bases for $\mathcal{C}$ is same and is called *p-dimension* of $\mathcal{C}$, denoted $p-\dim(\mathcal{C})$. The following theorem summarizes results for a p-basis.

Theorem 2.4 *[112]*

1. *Every module over* $\mathbb{Z}_{p^s}$ *admits a p-basis.*

2. $p-\dim\left(\mathbb{Z}_{p^s}^{n}\right) = sn.$

3. $\mathcal{B}$ *is a p-basis for* $\mathcal{C}$ *if and only if every vector in* $\mathcal{C}$ *is a unique p-linear combination of vectors in* $\mathcal{B}$.

Let $\mathcal{C}$ be the linear code generated by the matrix B given in (2.4) and $\mathcal{B}$ be the matrix

$$\mathcal{B} = \left[\begin{array}{cccccc}
I_{k_0} & A_{01} & A_{02} & \cdots & A_{0s-1} & A_{0s} \\
pI_{k_0} & pA_{01} & pA_{02} & \cdots & pA_{0s-1} & pA_{0s} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
p^{s-1}I_{k_0} & p^{s-1}A_{01} & p^{s-1}A_{02} & \cdots & p^{s-1}A_{0s-1} & p^{s-1}A_{0s} \\
\hline
\mathbf{0} & pI_{k_1} & pA_{12} & \cdots & pA_{1s-1} & pA_{1s} \\
\mathbf{0} & p^2I_{k_1} & p^2A_{12} & \cdots & p^2A_{1s-1} & p^2A_{1s} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\mathbf{0} & p^{s-1}I_{k_1} & p^{s-1}A_{12} & \cdots & p^{s-1}A_{1s-1} & p^{s-1}A_{1s} \\
\hline
\mathbf{0} & \mathbf{0} & p^2I_{k_2} & \cdots & \cdots & p^2A_{2s} \\
\mathbf{0} & \mathbf{0} & p^3I_{k_2} & \cdots & \cdots & p^3A_{2s} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\mathbf{0} & \mathbf{0} & p^{s-1}I_{k_2} & \cdots & \cdots & p^{s-1}A_{2s} \\
\hline
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\hline
\mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & p^{s-1}I_{k_{s-1}} & p^{s-1}A_{s-1s}
\end{array}\right]. \tag{2.5}$$

Then for an appropriate permutation matrix P it is easy to see that rows of $P\mathcal{B}$ form a p-basis for the code generated by $\mathcal{B}$. Hence $p-\dim(\mathcal{C}) = k = \sum_{i=0}^{s-1}(s-i)k_i$. Note that, for an $[n,k]$ linear code $\mathcal{C}$ over $\mathbb{Z}_{p^s}$, the dual code $\mathcal{C}^{\perp}$ is an $[n, sn-k]$ linear code. The p-span of the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k$ will be denoted by $< \mathbf{v}_1, \ldots, \mathbf{v}_k >$.

2.4.2 Generalized Gray Map

It was observed in section 2.3 that the image of the linear code over $\mathbb{Z}_4$ under the Gray map is a binary code of twice the length and whose minimum Hamming distance is same as the minimum Lee distance of $\mathcal{C}$. Thus, it is natural to ask: Does there exist a generalized gray map which maps a linear code over $\mathbb{Z}_{p^s}$ to a code over $\mathbb{Z}_p$ having similar properties? Unfortunately, no such generalization is known. Infact, recently, Ana *Sălăgean*- Mandache[98] has shown that except for the well-known case $p = s = 2$, it is not possible to construct a weight function on $\mathbb{Z}_{p^s}$ for which $\mathbb{Z}_{p^s}$ is isometric to $\mathbb{Z}_p^s$ with the Hamming metric. In[19], C. Carlet has defined a generalized gray map ϕ_G from $\mathbb{Z}_{2^s}$ to $\mathbb{Z}_2^{2^{s-1}}$ and has obtained the $\mathbb{Z}_{2^s}$ version of Kerdock and Delsarte-Goethals codes.

Let s be a positive integer and let E_s be the $s \times 2^s$ matrix whose columns consist of binary representation of numbers $0, 1, 2, \cdots, 2^s - 1$ (elements of $\mathbb{Z}_{2^s}$). Thus E_s can be inductively defined by

$$E_s = \left[\begin{array}{c|c} E_{s-1} & E_{s-1} \\ \hline 00\ldots0 & 11\ldots1 \end{array}\right], \text{ with } E_1 = [01]. \tag{2.6}$$

Let $s > 1$ and let $u \in \mathbb{Z}_{2^s}, 0 \leq u < 2^s$. Let $u = \sum_{i=1}^{s} u_i 2^{i-1} (u_i = 0 \text{ or } 1)$ and let $E_{s-1} = [y_{ij}]; 1 \leq i \leq s-1, 0 \leq j \leq 2^{s-1} - 1$. Define a map $\phi_G : \mathbb{Z}_{2^s} \mapsto \mathbb{Z}_2^{2^{s-1}}$ by $\phi_G(u) = (x_0, x_1, \ldots, x_{2^{s-1}-1})$; where

$$x_j = u_s + \sum_{i=1}^{s-1} u_i y_{ij} \in \mathbb{Z}_2. \tag{2.7}$$

Note that ϕ_G is a mapping from $\mathbb{Z}_{2^s}$ onto the Reed Müller code of order 1 and length 2^{s-1}. ϕ_G can also be defined as a Boolean function $\phi_G(u)$ evaluated on $GF(2^{s-1})$ by :

$$\phi_G(u) : (y_1, y_2, \cdots, y_{s-1}) \mapsto u_s + \sum_{i=1}^{s-1} u_i y_i.$$

ϕ_G is a mapping from $\mathbb{Z}_{2^s}$ onto the Reed Müller code of order 1 and length 2^{s-1}.

Note that this map is distance preserving[19]. For $s = 3$ this is a well understood generalization of the gray map but for $s > 3$ still several things need to be investigated.

Note that E_{s-1} is the generator matrix of the extended binary simplex code of dimension $s-1$. Thus weight of any row will be 2^{s-2}. Hence corresponding to entries $1, 2, 2^2, \cdots, 2^{s-2}$ of $\mathbb{Z}_{2^s}$, $\phi_G(u)$ will have weight 2^{s-2} and the weight of $\phi_G(2^{s-1})$ will be 2^{s-1} (see (2.6) and (2.7)). Now all other nonzero elements of $\mathbb{Z}_{2^s}$ will also give the weight 2^{s-2} since the weight of other entries corresponds to some linear combination of rows of E_{s-1}. Thus, for $u \neq 0$, we have

$$wt(\phi_G(u)) = \begin{cases} 2^{s-2}, & u \neq 2^{s-1} \\ 2^{s-1}, & u = 2^{s-1}. \end{cases} \tag{2.8}$$

We call this weight the *Generalized Lee weight* of u and is denoted by $w_{GL}(u)$. Also, we have the matrix

$$G_s(say) = \begin{bmatrix} \phi_G(1) \\ \phi_G(2) \\ \phi_G(2^2) \\ \vdots \\ \phi_G(2^{s-2}) \\ \phi_G(2^{s-1}) \end{bmatrix} = \begin{bmatrix} 0101 & 0101 & 0101 & 0101 & \cdots & 0101 & 0101 & 0101 \\ 0011 & 0011 & 0011 & 0011 & \cdots & 0011 & 0011 & 0011 \\ 0000 & 1111 & 0000 & 1111 & \cdots & 1111 & 0000 & 1111 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0000 & \cdots & 0000 & \cdots & \cdots & 1111 & \cdots & 1111 \\ 1111 & 1111 & 1111 & 1111 & \cdots & 1111 & 1111 & 1111 \end{bmatrix}. \tag{2.9}$$

Also, let G_{s-i} denote the matrix obtained from G_s by dropping first i rows. Note that ϕ_G can be naturally extended to $\mathbb{Z}_{2^s}^n$ by applying ϕ_G to its components.

Definition 2.1 *A binary code is called* $\mathbb{Z}_{2^s}$-linear *if it is equivalent to* $\phi_G(\mathcal{C})$ *for some linear code* $\mathcal{C}$ *over* $\mathbb{Z}_{2^s}$.

A necessary and sufficient condition for the $\mathbb{Z}_{2^3}$-linearity is given in[19]. It is also shown that any $\mathbb{Z}_{2^s}$-linear code is distance invariant and $d_H(\phi_G(u), \phi_G(v)) = w_{GL}(u-v)$[19]. The minimum generalized Lee weight, d_{GL}, of $\mathcal{C}$ can be defined in the usual sense. Note also that for $s = 2$, $d_{GL} = d_L$. The following Lemma is useful in Sections 3.3 and 4.2.1.

Lemma 2.5 *For $p = 2$, the images of the rows of the matrix $\mathcal{B}$ given by (2.5) under the generalized gray map ϕ_G are linearly independent over $\mathbb{Z}_2$.*

Proof: Applying the generalized gray map ϕ_G to the rows of $\mathcal{B}$ with a suitable arrangements of rows yields a binary matrix of the type

$$\begin{bmatrix}
G_s & & & & & & & & & & & \\
\mathbf{0} & \ddots & & & & & & & & & & \\
\mathbf{0} & \mathbf{0} & G_s & & & & & & & & & \\
\mathbf{0} & \mathbf{0} & \mathbf{0} & G_{s-1} & & & & & & & & \\
\mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \ddots & & & & & & & \\
\mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & G_{s-1} & & & & & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & & & & & \\
\mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & G_2 & & & & \\
\mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \ddots & & & \\
\mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & G_2 & & \\
\mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & G_1 & * \\
\end{bmatrix},$$

where G_s and G_{s-i} are as defined in (2.9) and $*$ is some block. It is easy to see that the rows of the above matrix are linearly independent. ∎

Remark 2.1 *Lemma 2.5 implies that the transform of a 2-basis of $\mathcal{C}$ under the generalized gray map gives rise to linearly independent over $\mathbb{Z}_2$. The converse of this need not be true, in general, For example, If $s = 2$, then $\{101100,011100\}$ are $\mathbb{Z}_2$-independent but $\{320,120\}$ are not.*

A linear code $\mathcal{C}$ over $\mathbb{Z}_{2^s}$ of length n, 2-dimension k, minimum Hamming distance d_H, minimum Lee distance d_L and minimum Generalized Lee distance d_{GL} is called an $[n, k, d_H, d_L, d_{GL}]$ code or simply an $[n, k]$ code. $\mathcal{C}$ is called $\mathbb{Z}_2$-*linear* if $\phi_G(\mathcal{C})$ is a

binary linear code. Thus, if $\mathcal{C}$ is an $[n, k, d_H, d_L, d_{GL}]$ $\mathbb{Z}_2$-linear code then $\phi_G(\mathcal{C})$ is a binary linear code of length $2^{s-1}n$, dimension k and minimum Hamming distance d_{GL}. Hence, by the Griesmer bound for binary linear codes[79], we have

$$n \geq \left\lceil \frac{1}{2^{s-1}} \sum_{i=0}^{k-1} \left\lceil \frac{d_{GL}}{2^i} \right\rceil \right\rceil. \tag{2.10}$$

2.4.3 Generalized Hamming weights of Linear codes over $\mathbb{Z}_{p^s}$

Let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{Z}_{p^s}$. The definitions of Generalized Hamming weight (GHW), weight hierarchies and chain condition given in section 2.1 for linear codes over $GF(q)$ can be extended in a similar fashion for linear codes over $\mathbb{Z}_{p^s}$. The only difference is that we replace dimension by p-dimension everywhere. Thus for $1 \leq r \leq k$, the r^{th} generalized hamming weight of $\mathcal{C}$ is defined as $d_r(\mathcal{C}) = min\{w_S(\mathcal{D}_r) : \mathcal{D}_r$ is an $[n, r]$ subcode of $\mathcal{C}\}$, where $w_S(\mathcal{D}_r)$ is the support size of a subcode $\mathcal{D}_r$ of $\mathcal{C}$ with $p-\dim(\mathcal{D}_r) = r$.

The following theorem summarizes basic properties of GHW[2].

Theorem 2.6 *Let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{Z}_{p^s}$. Then*

1. *(Monotonicity): $1 \leq d_1(\mathcal{C}) \leq d_2(\mathcal{C}) \leq \cdots \leq d_k(\mathcal{C}) \leq n$ and if, $d_r(\mathcal{C}) = d_{r+1}(\mathcal{C}) = \cdots = d_{r+s-1}(\mathcal{C})$, then $d_{r+s-1}(\mathcal{C}) < d_{r+s}(\mathcal{C})$.*

2. *(Duality): $\{d_r(\mathcal{C}) : 1 \leq r \leq k\} = \{\underbrace{1, \cdots, 1}_{s}, \underbrace{2, \cdots, 2}_{s}, \ldots, \underbrace{n, \cdots, n}_{s}\} \backslash \{n + 1 - d_r(\mathcal{C}^\perp) : 1 \leq r \leq sn - k\}$*

For $p = 2$, the following Lemma is a generalization of Lemma 2.2.

Lemma 2.7 *If $\mathcal{D}$ is an $[n, r]$ linear code over $\mathbb{Z}_{2^s}$ then*

1. *$\sum_{\mathbf{c} \in \mathcal{D}} w_L(\mathbf{c}) = 2^{r+s-2} w_S(\mathcal{D})$,*

2. *$\sum_{\mathbf{c} \in \mathcal{D}} w_{GL}(\mathbf{c}) = 2^{r+s-2} w_S(\mathcal{D})$.*

Proof: Consider the $(2^r \times n)$ array of all codewords in $\mathcal{D}$. Let $0 \leq m \leq s$ and let n_{m-1} be the number of columns that contain the entries $0, 1 \cdot 2^{s-m}, 2 \cdot 2^{s-m}$, $3 \cdot 2^{s-m}, \cdots, (2^m - 1) \cdot 2^{s-m}$ equally often. Then $\sum_{m=1}^{s} n_{m-1} = w_S(\mathcal{D})$ and hence

$$\sum_{\mathbf{c} \in \mathcal{D}} w_L(\mathbf{c}) = \sum_{m=1}^{s} \left(n_{m-1} \frac{2^r}{2^m} \left(\sum_{t=0}^{(2^m-1)} w_L(t \cdot 2^{s-m}) \right) \right) \tag{2.11}$$

$$= \sum_{m=1}^{s} \left(n_{m-1} 2^{r-m} (2^{s+m-2}) \right) = 2^{r+s-2} \cdot w_S(\mathcal{D})$$

as

$$w_L(t \cdot 2^{s-m}) = \begin{cases} t \cdot 2^{s-m}, & t \neq 2^{m-1} \\ 2^{s-1}, & otherwise. \end{cases}$$

This proves 1. Proof of 2 follows using (2.8) and an equation similar to the equation (2.11). ∎

Remark 2.2 *For $s = 2$, above Lemma was first proved by K. Yang et al (cf.[117]).*

Corollary 2.8 *(Plotkin-type Bound) Let $\mathcal{C}$ be an $[n, k, d_L, d_{GL}]$ linear code over $\mathbb{Z}_{2^s}$. Then $d_L \leq n \cdot 2^{s-1}$ and $d_{GL} \leq n \cdot 2^{s-1}$.*

Proof: By Lemma 2.7, the average Lee weight of the codewords will be $n \cdot \frac{2^{k+s-2}}{(2^k-1)} \geq d_L$. ∎

The proof of the following Corollary follows immediately by Lemma 2.7.

Corollary 2.9 *If $1 \leq r \leq k$, then r^{th} GHW of $\mathcal{C}$ satisfies*

$$d_r(\mathcal{C}) \geq \left\lceil \frac{(2^r - 1) d_L}{2^{r+s-2}} \right\rceil, \text{ and } d_r(\mathcal{C}) \geq \left\lceil \frac{(2^r - 1) d_{GL}}{2^{r+s-2}} \right\rceil.$$

Remark 2.3 *In view of Lemma 2.7, GHW can be defined alternately as*

$$d_r(\mathcal{C}) = \frac{1}{2^{r+s-2}} \, min \left\{ \sum_{d \in D_r} w_L(d) : D_r \text{ is an [n,r] subcode of } \mathcal{C} \right\} \text{ for } 1 \leq r \leq k.$$

Similar definition hold for w_{GL}. If $r = 1$, we get the following corollary from Lemma 2.7. In[93](see also[25]), Rains has proved that for a linear code over $\mathbb{Z}_4, d_H \geq \lceil \frac{d_L}{2} \rceil$. The following corollary generalizes it.

Corollary 2.10 *Let $\mathcal{C}$ be a Linear code over $\mathbb{Z}_{2^s}$, then*

$$d_H \geq \left\lceil \frac{d_L}{2^{s-1}} \right\rceil, \quad \textit{and} \quad d_H \geq \left\lceil \frac{d_{GL}}{2^{s-1}} \right\rceil.$$

A linear code over $\mathcal{C}$ over $\mathbb{Z}_{2^s}$ is said to be of *type* α (β) if

$$d_H = \left\lceil \frac{d_{GL}}{2^{s-1}} \right\rceil \left(d_H > \left\lceil \frac{d_{GL}}{2^{s-1}} \right\rceil \right).$$

2.4.4 Codes over $\mathbb{Z}_4$

Codes over $\mathbb{Z}_4$ have been studied extensively (cf.[103],[113] etc.). In this section we collect some basic definitions specific to these codes and some further results.

A linear code $\mathcal{C}$ over $\mathbb{Z}_4$ has a generator matrix G of the form

$$G = \begin{bmatrix} I_{k_0} & A & B_1 + 2B_2 \\ \mathbf{0} & 2I_{k_1} & 2C \end{bmatrix},$$

where A, B_1, B_2 and C are matrices with entries 0 and 1 and I_k is the identity matrix of order k. One can associate two binary linear codes with $\mathcal{C}$ as follows. The *residue code* , $\mathcal{C}^{(1)}$ of $\mathcal{C}$ is given by $\mathcal{C}^{(1)} = \{(\bar{c_1}, \bar{c_2}, \ldots, \bar{c_n}) : (c_1, c_2, \ldots, c_n) \in \mathcal{C}\}$ where $\bar{c_i}$ denotes the reduction of c_i modulo 2. Another binary linear code $\mathcal{C}^{(2)}$, called the *torsion code* of $\mathcal{C}$ is given by

$$\mathcal{C}^{(2)} = \left\{ \frac{\mathbf{c}}{2} : \mathbf{c} = (c_1, \ldots, c_n) \in \mathcal{C} \textit{ and } c_i \equiv 0 \pmod 2 \textit{ for } 1 \leq i \leq n \right\}.$$

If $k_1 = 0$ then $\mathcal{C}^{(1)} = \mathcal{C}^{(2)}$. The generator matrices of these codes are given by $G^{(1)}$ and $G^{(2)}$, respectively, where

$$G^{(1)} = \begin{bmatrix} I_{k_0} & A & B_1 \end{bmatrix} \text{ and } G^{(2)} = \begin{bmatrix} I_{k_0} & A & B_1 \\ \mathbf{0} & I_{k_1} & C \end{bmatrix}.$$

If $\mathcal{C}$ is self orthogonal then $\mathcal{C}^{(1)}$ is doubly even and $\mathcal{C}^{(1)} \subset \mathcal{C}^{(2)} \subset \mathcal{C}^{(1)^\perp}$ and if $\mathcal{C}$ is self dual then $\mathcal{C}^{(2)} = \mathcal{C}^{(1)^\perp}$[26].

Let $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$. The *Correlation* of $\mathbf{c}$ is defined by $\theta(\mathbf{c}) = (\omega_0(\mathbf{c}) - \omega_2(\mathbf{c})) + i(\omega_1(\mathbf{c}) - \omega_3(\mathbf{c}))$; where $i = \sqrt{-1}$ and $\omega_j(\mathbf{c}) = |\{k : c_k = j\}|$ [104].

If $d_1, d_2, \ldots, d_k$ is the weight hierarchy of an $[n, k, d_H, d_L]$ linear code $\mathcal{C}$ over $\mathbb{Z}_4$ then for $s = 2,$ and $p = 2$ by Theorem 2.6 and Corollary 2.10, $\frac{d_L}{2} \leq d_1 < d_3 < \cdots < d_k \leq n$. Hence $n - \frac{d_L}{2} \geq \frac{k-1}{2}$. Thus we get the following corollary.

Corollary 2.11 *For any $[n, k, d_H, d_L]$ linear code over $\mathbb{Z}_4$, $n \geq \left\lceil \frac{d_L+k-1}{2} \right\rceil$.*

If $\mathcal{C}$ is $\mathbb{Z}_2$-linear then the following proposition gives another lower bound, though not tight for type β code of $\mathcal{C}$.

Proposition 2.1 *Let $\mathcal{C}$ be a $\mathbb{Z}_2$-linear code over $\mathbb{Z}_4$. Then*

$$d_r(\mathcal{C}) \geq \left\lceil \frac{1}{2} \sum_{i=0}^{r-1} \left\lceil \frac{d_L}{2^i} \right\rceil \right\rceil.$$

Proof: Follows easily using inequality (2.10). ∎

The following upper bound on the weight hierarchy of a linear code $\mathcal{C}$ follows from Theorem 2.6 for $s = 2$.

Proposition 2.2 *1.* $d_r(\mathcal{C}) \geq n - \frac{(k-r)}{2}$; $(k, r$ *even* $)$.

2. $d_r(\mathcal{C}) \geq n - \frac{(k-r-1)}{2}$; $(k$ *even* $, r$ *odd or* k *odd,* r *even* $)$.

3. $d_r(\mathcal{C}) \geq n - \frac{(k-r-2)}{2}$; $(k, r$ *odd* $)$.

Chapter 3

$\mathbb{Z}_4$-Simplex Codes and their Gray Images

The binary Gray code is fun,
For in it strange things can be done,
Fifteen, as you know,
Is one,oh,oh,oh,
And ten is one,one,one, and one. ... Anon

3.1 Introduction

In this chapter, we introduce simplex codes of types α and β over $\mathbb{Z}_4$. These are generalizations of binary simplex codes in many ways. The torsion/reduction codes of these families are equivalent to several copies of binary simplex codes. Basic properties of these codes are determined in section 1. The gray images of these codes are constructed in two ways in section 2. It is shown that these families satisfy the chain condition. Generalization of these codes to codes over $\mathbb{Z}_{2^s}$ is done in the next chapter.

3.2 $\mathbb{Z}_4$-Simplex Codes of Type α and β

Let G_k be a $k \times 2^{2k}$ matrix over $\mathbb{Z}_4$ defined inductively by

$$G_k = \left[\begin{array}{c|c|c|c} 00\cdots0 & 11\cdots1 & 22\cdots2 & 33\cdots3 \\ \hline G_{k-1} & G_{k-1} & G_{k-1} & G_{k-1} \end{array}\right] \tag{3.1}$$

with G_1 =[0123]. Note that columns of G_k consist of all distinct k-tuples over $\mathbb{Z}_4$. Clearly, the code S_k^α generated by G_k has length 2^{2k} and 2-dimension $2k$. The following observations are useful in determining Hamming and Lee weights of S_k^α.

Remark 3.1 *If A_{k-1} denotes an array of codewords in S_{k-1}^α and if $\mathbf{i} = (iii...i)$ then an array of all codewords of S_k^α is given by*

$$\left[\begin{array}{cccc} A_{k-1} & A_{k-1} & A_{k-1} & A_{k-1} \\ A_{k-1} & \mathbf{1}+A_{k-1} & \mathbf{2}+A_{k-1} & \mathbf{3}+A_{k-1} \\ A_{k-1} & \mathbf{2}+A_{k-1} & A_{k-1} & \mathbf{2}+A_{k-1} \\ A_{k-1} & \mathbf{3}+A_{k-1} & \mathbf{2}+A_{k-1} & \mathbf{1}+A_{k-1} \end{array}\right].$$

Remark 3.2 *If $R_1, R_2, ..., R_k$ denote the rows of the matrix G_k then $w_H(R_i) = 3 \cdot 2^{2k-2}, w_H(2R_i) = 2^{2k-1}$ and $w_L(R_i) = 2^{2k} = w_L(2R_i)$.*

It may be observed that each element of $\mathbb{Z}_4$ occurs equally often in every row of G_k. In fact we have the following lemma.

Lemma 3.1 *Let $\mathbf{c}(\neq 0) \in S_k^\alpha$. If one of the coordinates of $\mathbf{c}$ is a unit then every element of $\mathbb{Z}_4$ occurs 4^{k-1} times as a coordinate of $\mathbf{c}$. Otherwise $w_H(\mathbf{c}) = 2^{2k-1}$.*

Proof: By Remark 3.1, any x $\in S_{k-1}^\alpha$ gives rise to following four codewords of S_k^α

$$y_1 = \left(\begin{array}{c|c|c|c} x & x & x & x \end{array} \right), \qquad y_2 = \left(\begin{array}{c|c|c|c} x & \mathbf{1}+x & \mathbf{2}+x & \mathbf{3}+x \end{array} \right),$$

$y_3 = \left(\begin{array}{c|c|c|c} x & \mathbf{2}+x & x & \mathbf{2}+x \end{array} \right)$ and $y_4 = \left(\begin{array}{c|c|c|c} x & \mathbf{3}+x & \mathbf{2}+x & \mathbf{1}+x \end{array} \right)$.
Hence by induction, the assertion follows. ∎

Let $G(S_k)$ (columns consist of all nonzero binary k-tuples) be a generator matrix for an $[n, k]$ binary simplex code S_k. Then the extended binary simplex code $\hat{S}_k$ is generated by the matrix

$$G(\hat{S}_k) = \left[\begin{array}{c|c} \mathbf{0} & G(S_k) \end{array} \right].$$

Inductively,

$$G(\hat{S}_k) = \left[\begin{array}{c|c} 00\ldots0 & 11\ldots1 \\ \hline G(\hat{S_{k-1}}) & G(\hat{S_{k-1}}) \end{array} \right] \text{ with } G(\hat{S}_1) = [0\ 1]. \tag{3.2}$$

Lemma 3.2 *Torsion code of S_k^α is equivalent to the 2^k copies of $\hat{S}_k$.*

Proof: Recall that torsion code of S_k^α is the set of codewords obtained by replacing 2 by 1 in all 2-linear combination of the rows of the matrix $2G_k$ where G_k is defined in (3.1). The proof is by induction on k. It is easy to see that the result holds for $k = 2$. If $2G_{k-1}$ is permutation equivalent to the 2^{k-1} copies of $2G(\hat{S_{k-1}})$ then the matrix $2G_k$ takes the form

$$\left[\begin{array}{c|c|c|c} 00\cdots0 & 22\cdots2 & 00\cdots0 & 22\cdots2 \\ \hline 2G(\hat{S_{k-1}})|\cdots|2G(\hat{S_{k-1}}) & 2G(\hat{S_{k-1}})|\cdots|2G(\hat{S_{k-1}}) & 2G(\hat{S_{k-1}})|\cdots|2G(\hat{S_{k-1}}) & 2G(\hat{S_{k-1}})|\cdots|2G(\hat{S_{k-1}}) \end{array} \right].$$

Regrouping the columns according to (3.2) (Infact, $2G(\hat{S}_k)$) gives us the desired result.

∎

As a consequence of Lemmas 3.1 and 3.2 we determine Hamming and Lee weight distributions of S_k^α.

Theorem 3.3 *Hamming and Lee weight distribution of S_k^α are:*

1. $A_H(0) = 1, A_H(2^{2k-1}) = 2^k - 1,$ *and* $A_H(3 \cdot 2^{2k-2}) = 2^k(2^k - 1)$

2. $A_L(0) = 1, A_L(2^{2k}) = 2^{2k} - 1,$

Proof: By Lemma 3.1, each nonzero codeword of S_k^α has Hamming weight either $3 \cdot 4^{k-1}$ or 2^{2k-1} and Lee weight 2^{2k}. By Lemma 3.2, the dimension of the torsion code of S_k^α is k, Thus there will be $2^k - 1$ codewords of Hamming weight 2^{2k-1}. Hence the number of codewords having Hamming weight , $3 \cdot 4^{k-1}$, is $4^k - 2^k$. ∎

Remark 3.3 *1.* S_k^α *is an equidistant code with respect to Lee distance whereas* S_k *is an equidistant binary code with respect to Hamming distance.*

2. S_k^α *is of type* α.

3. S_k^α *is a* 4*-ary balanced code (see[111]).*

4. The minimum Euclidean weight d_E *of* S_k^α *is* $3 \cdot 2^{2k-1}$.

Let $\bar{S_k^\alpha}$ be the punctured code of S_k^α obtained by deleting the zero coordinate. Then the swe (see section 2.4.4) of $\bar{S_k^\alpha}$ is

$$swe(x, y, z) = x^{n(k)} + (2^k - 1)(xz)^{n(k-1)} z[(xz)^{n(k-1)+1} + 2^k y^{2^{2k-1}}],$$

where $n(k) = 4^k - 1$ and correlation of any $\mathbf{c} \in \bar{S_k^\alpha}$ is given by

$$\theta(\mathbf{c}) = -1. \tag{3.3}$$

The length of S_k^α is large compared to its 2-dimension and increases fast with increment in 2-dimension. But one can always puncture some columns from G_k to yield good codes over $\mathbb{Z}_4$ in the sense of having maximum possible Lee weights for a given length and 2-dimension.

Let G_k^β be the $k \times 2^{k-1}(2^k - 1)$ matrix defined inductively by

$$G_2^\beta = \left[\begin{array}{c|c|c} 1111 & 0 & 2 \\ \hline 0123 & 1 & 1 \end{array}\right], \tag{3.4}$$

and for $k > 2$

$$G_k^\beta = \left[\begin{array}{c|c|c} 11\cdots1 & 00\cdots0 & 22\cdots2 \\ \hline G_{k-1} & G_{k-1}^\beta & G_{k-1}^\beta \end{array}\right], \tag{3.5}$$

where G_{k-1} is the generator matrix of S_{k-1}^α. Note that G_k^β is obtained from G_k by deleting $2^{k-1}(2^k+1)$ columns. By induction it is easy to verify that no two columns of G_k^β are multiple of each other. Let S_k^β be the code generated by G_k^β. Note that S_k^β is a $[2^{k-1}(2^k-1), 2k]$ code. To determine Hamming (Lee) weight distributions of S_k^β we first make few observations.

Remark 3.4 *If A_{k-1} (B_{k-1}) denotes an array of codewords in S_{k-1}^α(S_{k-1}^β) and if $\mathbf{i} = (i, i, \ldots, i)$ then an array of all codewords of S_k^β is given by*

$$\left[\begin{array}{ccc} A_{k-1} & B_{k-1} & B_{k-1} \\ \mathbf{1}+A_{k-1} & B_{k-1} & \mathbf{2}+B_{k-1} \\ \mathbf{2}+A_{k-1} & B_{k-1} & B_{k-1} \\ \mathbf{3}+A_{k-1} & B_{k-1} & \mathbf{2}+B_{k-1} \end{array}\right].$$

Remark 3.5 *Each row of G_k^β has Hamming weight $2^{k-3}[3(2^k-1)+1]$ and Lee weight $2^{k-1}(2^k-1)$.*

Proposition 3.1 *Each row of G_k^β contains $2^{2(k-1)}$ units and $\omega_0 = \omega_2 = 2^{k-2}(2^{k-1}-1)$.*

Proof: The result can be easily verified for the $k = 2$. Assume that the result holds for each row of G_{k-1}^β. Then the number of units in each row of G_{k-1}^β is $2^{2(k-2)}$. By Lemma 3.1, the number of units in any row of G_{k-1} is 2^{2k-3}. Hence the total number of units in any row of G_k^β will be $2^{2k-3} + 2 \cdot 2^{2(k-2)} = 2^{2(k-1)}$. A similar argument holds for the number of 0's and 2's. ∎

Infact, similar to S_k^α, we have the following lemma

Lemma 3.4 *Let* $\mathbf{c} \in S_k^\beta, \mathbf{c} \neq 0$. *If one of the coordinates of* $\mathbf{c}$ *is a unit then* $\omega_1(\mathbf{c}) + \omega_3(\mathbf{c}) = 2^{2(k-1)}$ *and* $\omega_0(\mathbf{c}) = \omega_2(\mathbf{c}) = 2^{k-2}(2^{k-1}-1)$. *Otherwise* $\omega_1(\mathbf{c}) = \omega_3(\mathbf{c}) = 0$, *and* $\omega_0(\mathbf{c}) = 2^{k-1}(2^{k-1}-1), \omega_2(\mathbf{c}) = 2^{2(k-1)}$.

Proof: By Remark 3.4, there exist $y_1 \in S_{k-1}^\alpha$ and $y_2 \in S_{k-1}^\beta$ such that $\mathbf{c}$ can have any of the following four forms:

$$\mathbf{c} = \left(\begin{array}{c|c|c} y_1 & y_2 & y_2 \end{array} \right), \quad \ldots(i) \qquad \mathbf{c} = \left(\begin{array}{c|c|c} \mathbf{1}+y_1 & y_2 & \mathbf{2}+y_2 \end{array} \right), \quad \ldots(ii)$$

$$\mathbf{c} = \left(\begin{array}{c|c|c} \mathbf{2}+y_1 & y_2 & y_2 \end{array} \right) \quad \ldots(iii) \quad \text{and} \quad \mathbf{c} = \left(\begin{array}{c|c|c} \mathbf{3}+y_1 & y_2 & \mathbf{2}+y_2 \end{array} \right) \quad \ldots(iv).$$

We prove the result by induction on k. Clearly result holds for $k = 2$. So assume that it holds for S_{k-1}^β. Let $y_2 \in S_{k-1}^\beta$ such that y_2 is neither all zero nor all 2 codeword. If all the components of $\mathbf{c}(\neq 0)$ are zero divisors (Note that this can happen only in the first or the third form of $\mathbf{c}$). In either of these forms of $\mathbf{c}$, if $y_2 \in S_{k-1}^\beta$ then by induction hypothesis $\omega_0(y_2) = 2^{k-2}(2^{k-2}-1)$ and $\omega_2(y_2) = 2^{2(k-2)}$. Since $y_1 \in S_{k-1}^\alpha$, by Lemma 3.1, $\omega_0(y_1) = 2^{2k-3} = \omega_2(y_1)$. Thus if $\mathbf{c}$ is of the form (i) and then $\omega_0(\mathbf{c}) = 2\{2^{k-2}(2^{k-2}-1)\} + 2^{2k-3} = 2^{k-1}(2^{k-1}-1)$ and $\omega_2(\mathbf{c}) = 2\{2^{2(k-2)}\} + 2^{2k-3} = 2^{2(k-1)}$ so the result holds. Similar arguments hold if $\mathbf{c}$ is of the form (iii). If one of the coordinate of $\mathbf{c}$ is a unit then $\mathbf{c}$ can be of any form (i)-(iv) above. In any of these forms by Lemma 3.1 each entry in $(\mathbf{i} + y_1)$; will occur equally often $(= 4^{k-2}$ times). Therefore total number of units in $\mathbf{c}$ will be $2 \times 4^{k-2} + 2^{2(k-2)} + 2^{2(k-2)} = 2^{2(k-1)}$ Similarly, the number of zero divisors occurs equally often $2^{k-2}(2^{k-1}-1)$ times. The case when $y_2 = \mathbf{0}$ or $\mathbf{2}$ is trivial as codewords will be the multiple of the first row of G_k^β only. ∎

Lemma 3.5 *The torsion code of* S_k^β *is equivalent to the* 2^{k-1} *copies of the binary simplex code* S_k.

Proof: The proof is by induction on k and is similar to that of Lemma 3.2. If $2G_{k-1}^\beta$ is permutation equivalent to the 2^{k-2} copies of $2G(S_{k-1})$ then $2G_k^\beta$, where G_k^β is given

by (3.5), takes the form

$$2G_k^\beta = \left[\begin{array}{c|ccc|ccc} 22\cdots2 & \multicolumn{3}{c|}{22\cdots2} & \multicolumn{3}{c}{00\cdots0} \\ \hline \mathbf{0} & 2G(S_{k-1}) & \cdots & 2G(S_{k-1}) & 2G(S_{k-1}) & \cdots & 2G(S_{k-1}) \end{array}\right].$$

Now grouping one column from first block together with one block of $2G(S_{k-1})$ from each of second and third block yields the desired result. ∎

Again, as a consequence of Lemmas 3.4 & 3.5 one obtains Hamming and Lee weight distributions of S_k^β.

Theorem 3.6 *The Hamming and Lee weight distributions of S_k^β are:*

1. $A_H(0) = 1, A_H(2^{2k-2}) = 2^k - 1, A_H(2^{k-3}[3(2^k-1)+1]) = 2^k(2^k-1)$ *and*
2. $A_L(0) = 1, A_L(2^{2k-1}) = 2^k - 1, A_L(2^{k-1}(2^k-1)) = 2^k(2^k-1)$.

Proof: Similar to the proof of Theorem 3.3. ∎

Remark 3.6 *(i) S_k^β is of type β.*
(ii) The correlation of each nonzero codeword of S_k^β with components 0's or 2's only is -2^{k-1}.
(iii) The swe of S_k^β is given as

$$swe(x,y,z) = x^{n(k)} + (2^k-1)x^{2\cdot n(k-1)}z^{4^{k-1}} + 2\cdot n(k)x^{n(k-1)}y^{4^{k-1}}z^{n(k-1)},$$

where $n(k) = 2^{k-1}(2^k-1)$.
(iv) The minimum Euclidean weight of S_k^β is $2^k(3\cdot 2^{k-2}-1)$.

3.3 Gray Image Families

Let $\mathcal{C}$ be an $[n,k,d_H,d_L]$ linear code over $\mathbb{Z}_4$. Then $\phi(\mathcal{C})$, the image of $\mathcal{C}$ under the Gray map ϕ, is a binary code having 2^k codewords of length $2n$, and minimum Hamming

distance d_L. However $\phi(\mathcal{C})$ need not be linear. Let $\mathcal{B}$ be the matrix (given in (2.5) for $p = 2, s = 2$) whose rows form a 2-basis for $\mathcal{C}$ and let $\phi(\mathcal{B})$ be the matrix obtained from $\mathcal{B}$ by applying gray map to each entry of $\mathcal{B}$. The code $\mathcal{C}_\phi$ generated by $\phi(\mathcal{B})$ is a $[2n, k, \geq \lceil \frac{d_L}{2} \rceil]$ binary linear code. Note that $\phi(\mathcal{C})$ and $\mathcal{C}_\phi$ have same number of codewords but in general they are not equal. The following proposition shows that both $\phi(\bar{S}_k^\alpha)$ and $\phi(S_k^\beta)$ are not linear.

Proposition 3.2 *$\phi(\bar{S}_k^\alpha)$ and $\phi(S_k^\beta)$ are nonlinear for all k.*

Proof: Let $R_1, R_2, \ldots R_k$ be the rows of the generator matrix G_k (G_k^β). Let $\mathbf{c} = R_k$ (R_1) and let $\mathbf{c}' = R_{k-1}$ (R_k) then by (3.3) (Remark 3.6(ii)), $2\bar{\mathbf{c}} \star \bar{\mathbf{c}}' \notin \bar{S}_k^\alpha$ (S_k^β). Hence, by Theorem 2.3, the result follows. ∎

Remark 3.7 *(i) $\phi(\bar{S}_k^\alpha)$ is a binary nonlinear code of length $2^{2k+1} - 2$ and minimum Hamming distance 2^{2k}. It meets the Plotkin bound[79] and $n < 2d_H$.*
(ii) $\phi(S_k^\beta)$ is a binary nonlinear code of length $2^k(2^k - 1)$ and minimum Hamming distance $2^{k-1}(2^k - 1)$. This is an example of a code having $n = 2d_H$[79].
(iii) Even though, both $\bar{S}_k^\alpha$ and S_k^β are not $\mathbb{Z}_2-$linear they meet the bound given by (2.10) which is true for $\mathbb{Z}_2$-linear codes.

Next two results are about the binary linear codes obtained from $\bar{S}_k^\alpha$ and S_k^β.

Theorem 3.7 *Let $\mathcal{C} = \bar{S}_k^\alpha$. Then $\mathcal{C}_\phi$ is an $[2^{2k+1} - 2, 2k, 2^{2k}]$ binary linear code consisting of two copies of binary simplex code S_{2k} with Hamming weight distribution same as the Lee weight distribution of $\bar{S}_k^\alpha$.*

Proof: By Lemma 2.5, $\mathcal{C}_\phi$ is a binary linear code of length $2^{2k+1}-2$ and dimension $2k$. Let $\mathcal{G}_k$ be a generator matrix of S_k^α in 2-basis form. Then

$$\mathcal{G}_k = \left[\begin{array}{c|c|c|c} 0\ldots0 & 1\ldots1 & 2\ldots2 & 3\ldots3 \\ 0\ldots0 & 2\ldots2 & 0\ldots0 & 2\ldots2 \\ G_{k-1} & G_{k-1} & G_{k-1} & G_{k-1} \\ 2G_{k-1} & 2G_{k-1} & 2G_{k-1} & 2G_{k-1} \end{array}\right].$$

Upto the suitable rearrangement of rows, $\phi(\mathcal{G}_k)$ is given by

$$\phi(\mathcal{G}_k) = \left[\begin{array}{c|c|c|c} 0000\ldots00 & 0101\ldots01 & 1111\ldots11 & 1010\ldots10 \\ 0000\ldots00 & 1111\ldots11 & 0000\ldots00 & 1111\ldots11 \\ \hline \phi(\mathcal{G}_{k-1}) & \phi(\mathcal{G}_{k-1}) & \phi(\mathcal{G}_{k-1}) & \phi(\mathcal{G}_{k-1}) \end{array}\right].$$

The proof now follows by induction on k. Statement trivially holds for $k=2$. Assume that $\phi(\mathcal{G}_{k-1})$ yields a $\left[2^{2k-1}, 2(k-1), 2^{2k-2}\right]$ binary code in which every nonzero codeword is of weight 2^{2k-2}. Then the possible nonzero weight from the lower portion of the above matrix $\phi(\mathcal{G}_k)$ will be $4\cdot 2^{2k-2} = 2^{2k}$. From the structure of the first two rows of $\phi(\mathcal{G}_k)$ it is easy to verify that any linear combination of these rows with other rows has weight 2^{2k}. Puncturing the first two columns and rearranging the columns yields the code having two copies of S_{2k}. ∎

Theorem 3.8 *Let $\mathcal{C} = S_k^\beta$. Then $\mathcal{C}_\phi$ is the binary MacDonald code*

$$M_{2k,k} : [2^{2k} - 2^k, 2k, 2^{2k-1} - 2^{k-1}]$$

with Hamming weight distribution same as the Lee weight distribution of S_k^β.

Proof: We again use induction on k. For $k=2$ the result can be easily verified. If $\mathcal{G}_k^\beta$ is a generator matrix of S_k^β in 2-basis form then upto rearrangement of rows

$$\phi(\mathcal{G}_k^\beta) = \left[\begin{array}{c|c|c} 0101\cdots01 & 0000\cdots00 & 1111\cdots11 \\ 1111\cdots11 & 0000\cdots00 & 0000\cdots00 \\ \hline \phi(\mathcal{G}_{k-1}) & \phi(\mathcal{G}_{k-1}^\beta) & \phi(\mathcal{G}_{k-1}^\beta) \end{array}\right],$$

where $\mathcal{G}_{k-1}$ is the generator matrix of S^{α}_{k-1} in 2-basis form. Assume that the result holds for S^{β}_{k-1} i.e., $\phi(\mathcal{G}^{\beta}_{k-1})$ yields a $\left[2^{2k-2}-2^{k-1}, 2k-2, 2^{2k-3}-2^{k-2}\right]$ binary code with possible nonzero weights either 2^{2k-3} or $2^{k-2}(2^{k-1}-1)$. By Theorem 3.7, $\phi(\mathcal{G}_{k-1})$ is a $\left[2^{2k-1}, 2(k-1), 2^{2k-2}\right]$ binary code in which every nonzero codeword is of weight 2^{2k-2}. Thus possible nonzero weights from lower portion of the above matrix will be either $2(2^{2k-3})+2^{2(k-1)}$ or $2\left(2^{2k-3}-2^{k-2}\right)+2^{2k-2}$, i.e., either 2^{2k-1} or $2^{k-1}(2^k-1)$. Now the proof easily follows (due to structure of first two rows of the above matrix) by showing that the resulting weight of any linear combination of first two rows with lower portion of the matrix, does not changes. ∎

The weight hierarchy of S^{α}_{k} and S^{β}_{k} are given by the following two theorems.

Theorem 3.9 *S^{α}_{k} satisfies the chain condition and its weight hierarchy is given by*

$$d_r(S^{\alpha}_{k}) = \sum_{i=1}^{r} 2^{2k-i} = 2^{2k} - 2^{2k-r} \quad ; 1 \le r \le 2k.$$

Proof: By Remark 3.3(1), Any r-dimensional subcode of S^{α}_{k} is of constant Lee weight. Hence by Remark 2.3 (for $s=2$),

$$d_r(S^{\alpha}_{k}) = \frac{1}{2^r}(2^r-1)2^{2k} = 2^{2k} - 2^{2k-r}.$$

Let $D_1 =< 2R_1 >$, $D_2 =< 2R_1, 2R_2 >$, $D_3 =< R_1, 2R_1, 2R_2 >$,
$D_4 =< R_1, 2R_1, R_2, 2R_2 >$, $\ldots$, $D_{2k} =< R_1, 2R_1, \ldots, R_k, 2R_k >$. It is easy to verify that

$$D_1 \subseteq D_2 \subseteq \cdots \subseteq D_{2k},$$

and $w_S(D_r) = d_r(S^{\alpha}_{k})$ for $1 \le r \le 2k$. ∎

Theorem 3.10 *S^{β}_{k} satisfies the chain condition and its weight hierarchy is given by*

$$d_r(S^{\beta}_{k}) = n(k) - 2^{k-r-1}(2^k - 2^{\lceil \frac{r}{2} \rceil}) \quad 1 \le r \le 2k,$$

where $n(k) = 2^{k-1}(2^k-1)$.

Proof: The proof follows by induction on k. Clearly result holds for $k = 2$. Assume that the result holds for S^{β}_{k-1}. Hence if $1 \leq r \leq 2k-2$, then there exists an r-dimensional subcode of S^{β}_{k-1} with minimum support size as $n(k-1) - 2^{k-r-2}(2^{k-1} - 2^{\lceil \frac{r}{2} \rceil})$. By Remark 3.4,

$$d_r(S^{\beta}_k) = 2d_r(S^{\beta}_{k-1}) + d_r(S^{\alpha}_{k-1}). \tag{3.6}$$

But all r-dimensional subcodes of S^{α}_{k-1} have constant support size $(2^{2k-2} - 2^{2k-2-r})$. Thus simplifying (3.6) yields the result. The case $r = 2k-1$ & $2k$ are trivial. Let $D_1 =< 2R_1 >$, $D_2 =< R_1, 2R_1 >$, $D_3 =< R_1, 2R_1, 2R_2 >$, $D_4 =< R_1, 2R_1, R_2, 2R_2 >$, $\ldots$, $D_{2k} =< R_1, 2R_1, \ldots, R_k, 2R_k >$. It is easy to see that

$$D_1 \subseteq D_2 \subseteq \cdots \subseteq D_{2k},$$

is the required chain of subcodes. ∎

The dual code of S^{α}_k is a code of length 2^{2k} and 2-dimension $2^{2k+1} - 2k$, whereas the dual code of S^{β}_k is a code of length $2^{k-1}(2^k - 1)$ and 2-dimension $2^{2k} - 2^k - 2k$. The Hamming and Lee weight distributions of these dual codes can be obtained with the help of Theorems 3.3 and 3.6 and the MacWilliams Identities[92]. Similarly, the weight hierarchies of duals can be obtained from Theorems 2.6, 3.9 & 3.10. For example, we have

Proposition 3.3 *If* $1 \leq r \leq 2^{2k+1} - 2k - 2$. *Then*

$$\{d_r(S^{\alpha\perp}_k)\} = \{1, 1, 2, 2, \ldots, n, n\} \backslash \{2^i : 0 \leq i < 2k\}.$$

In[108], Sun and Leib have considered the dual of S^{β}_k $(k \geq 3)$ in a different context. They have used combinatorial arguments to obtain a code of length $n = 2^{r-1}(2^r - 1)$, redundancy r and minimum squared noncoherent weight $N+1-\sqrt{(N-2)^2+9}$, where $N = n - 1$. They have further punctured these codes to get some good codes in the sense of having larger coding gains over noncoherent detection.

Chapter 4

$\mathbb{Z}_{2^s}$-Simplex Codes and their Generalized Gray Images

The purpose of computing is insight, not numbers.
... Richard W. Hamming (1915-1998)

4.1 Introduction

In section 2.4.2 we have studied some basic properties of generalized gray map ϕ_G introduced by Carlet. In[19] he has given two other generalizations of gray map ϕ. There may be several other generalizations. Thus the study of gray map on linear codes over $\mathbb{Z}_4$, as seen in section 3.3 of the last chapter can be extended to codes over $\mathbb{Z}_{2^s}$ in several ways. In this chapter we restrict ourselves to the map ϕ_G. Simplex codes of type α and β over $\mathbb{Z}_{2^s}$ are studied in section 4.2. Section 4.2.1 deals with the properties of generalized gray images of S_k^α and S_k^β.

4.2 $\mathbb{Z}_{2^s}$-Simplex Codes of Type α and β

Let G_k be a $k \times 2^{sk}$ matrix over $\mathbb{Z}_{2^s}$ defined inductively by

$$G_1 = [0123 \cdots 2^s - 1],$$

$$G_k = \left[\begin{array}{c|c|c|c|c} 00\cdots0 & 11\cdots1 & 22\cdots2 & \cdots & (2^s-1)(2^s-1)\cdots(2^s-1) \\ \hline G_{k-1} & G_{k-1} & G_{k-1} & \cdots & G_{k-1} \end{array}\right]; k \geq 2.$$

Clearly, the code S_k^α generated by G_k over $\mathbb{Z}_{2^s}$ has length 2^{sk} and 2-dimension sk. The following observations are straightforward generalizations of Remarks 3.1 and 3.2 of the previous chapter.

Remark 4.1 *If A_{k-1} denotes an array of codewords in S_{k-1}^α and if $\mathbf{i} = (iii...i)$ then an array of all codewords of S_k^α is given by*

$$\begin{bmatrix} A_{k-1} & A_{k-1} & A_{k-1} & \cdots & A_{k-1} \\ A_{k-1} & \mathbf{1} + A_{k-1} & \mathbf{2} + A_{k-1} & \cdots & (\mathbf{2^s - 1}) + A_{k-1} \\ A_{k-1} & \mathbf{2} + A_{k-1} & \mathbf{2^2} + A_{k-1} & \cdots & (\mathbf{2^s - 2}) + A_{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{k-1} & (\mathbf{2^s - 1}) + A_{k-1} & (\mathbf{2^s - 2}) + A_{k-1} & \cdots & \mathbf{1} + A_{k-1} \end{bmatrix}.$$

Remark 4.2 *If $R_1, R_2, ..., R_k$ denote the rows of the matrix G_k then $w_H(R_i) = 2^{sk} - 2^{s(k-1)}, w_H(2^{s-1}R_i) = 2^{sk-1}, w_L(R_i) = 2^{s(k+1)-2}$, and $w_{GL}(R_i) = 2^{s(k+1)-2}$.*

For each m, $0 \leq m \leq s$, let $S_m = \{0, 1 \cdot 2^{s-m}, 2 \cdot 2^{s-m}, \cdots, (2^m - 1) \cdot 2^{s-m}\}$. Note that $S_{s-1} = Z$, the set of all zero divisors of $\mathbb{Z}_{2^s}$ and $S_s = \mathbb{Z}_{2^s}$. A codeword $\mathbf{c} = (c_1, \ldots, c_n) \in S_k^\alpha$ is said to be of *type m* if all of its components belong to the set S_m. It may be observed that each element of $\mathbb{Z}_{2^s}$ occurs equally often in every row of G_k. In fact we have the following Lemma.

Lemma 4.1 *Let $\mathbf{c} \in S_k^\alpha$ be a type m codeword. Then all the components of $\mathbf{c}$ will occur equally often 2^{sk-m} times.*

Proof: Any x $\in S_{k-1}^{\alpha}$ gives rise to following 2^s codewords of S_k^{α}

$$y_1 = \left(\; x \;\middle|\; x \;\middle|\; x \;\middle|\; \cdots \;\middle|\; x \; \right), \qquad y_2 = \left(\; x \;\middle|\; \mathbf{1}+x \;\middle|\; \mathbf{2}+x \;\middle|\; \cdots \;\middle|\; (\mathbf{2^s}-\mathbf{1})+x \; \right),$$

$$y_3 = \left(\; x \;\middle|\; \mathbf{2}+x \;\middle|\; \mathbf{2^2}+x \;\middle|\; \cdots \;\middle|\; (\mathbf{2^s}-\mathbf{2})+x \; \right), \ldots, \text{ and}$$

$$y_{2^s} = \left(\; x \;\middle|\; (\mathbf{2^s}-\mathbf{1})+x \;\middle|\; (\mathbf{2^s}-\mathbf{2})+x \;\middle|\; \cdots \;\middle|\; \mathbf{1}+x \; \right).$$

Hence the proof follows easily by induction on k and the Remark 4.1. ∎

To determine weight distribution of S_k^{α} one needs to determine the number of codewords of type m in S_k^{α} for $1 \leq m \leq s$. Let C_m be the matrix defined by

$$C_m = \begin{bmatrix} 2^{s-m}R_1 \\ \vdots \\ 2^{s-1}R_1 \\ 2^{s-m}R_2 \\ \vdots \\ 2^{s-1}R_2 \\ \vdots \\ 2^{s-m}R_k \\ \vdots \\ 2^{s-1}R_k \end{bmatrix},$$

where R_i is the i^{th} row of the matrix G_k. The subcodes $\mathcal{D}^{(m)}$ of $\mathcal{C}$ generated by the 2-linear combinations of the rows of C_m will have 2^{mk} codewords. Note that the codewords generated by the matrix C_1 have components either 0 or 2^{s-1} and C_s yields the whole code S_k^{α}. Thus, for all m, $1 \leq m \leq s$, a codeword of type m will occur $2^{mk} - 2^{(m-1)k}$ times in S_k^{α}. This proves the following Lemma.

Lemma 4.2 *Let $0 < m \leq s$. Then the number of codewords of type m in S_k^{α} is $2^{(m-1)k}(2^k - 1)$.*

Theorem 4.3 *The Hamming, Lee and the generalized Lee weight distributions of* S_k^α *are:*

1. $A_H(0) = 1, A_H(2^{sk-m}(2^m-1)) = 2^{(m-1)k}(2^k-1)$ *for* $1 \le m \le s$,
2. $A_L(0) = 1, A_L(2^{s(k+1)-2}) = 2^{sk}-1$ *and*
3. $A_{GL}(0) = 1, A_{GL}(2^{s(k+1)-2}) = 2^{sk}-1$.

Proof: Let $\mathbf{c} \in S_k^\alpha$ be a codeword of type $m(\neq 0)$. Then by Lemma 4.1, $w_H(\mathbf{c}) = 2^{sk} - 2^{sk-m}$ and hence by Lemma 4.2, $A_H(2^{sk-m}(2^m-1)) = 2^{(m-1)k}(2^k-1)$. For $m = 0$, $A_H(0) = 1$. Also, by Lemma 4.1 $w_L(\mathbf{c}) = 2^{sk-m}\left(\sum_{t=0}^{(2^m-1)} w_L(t \cdot 2^{s-m})\right) = 2^{s(k+1)-2}$ which is independent of m. Thus all type $m(\neq 0)$ codewords will have same Lee weight. Similar argument holds for generalized Lee weight. ∎

Remark 4.3 *(i)* S_k^α *is an equidistant code with respect to Lee and generalized Lee distances.*
(ii) S_k^α *is of type* α.
(iii) For $s = 1, S_k^\alpha$ *reduces to extended binary simplex code* $\hat{S}_k$.
(iv) In[97], Satyanarayna also visited the codes S_k^α *and obtained the second part of the above theorem.*

Let G_k^β be the $k \times 2^{(s-1)(k-1)}(2^k-1)$ matrix defined inductively by

$$G_2^\beta = \left[\begin{array}{c|c|c|c|c|c|c} 111\cdots1 & 0 & 2 & 4 & 6 & \cdots & (2^s-2) \\ \hline 0123\cdots(2^s-1) & 1 & 1 & 1 & 1 & \cdots & 1 \end{array}\right],$$

and for $k > 2$,

$$G_k^\beta = \left[\begin{array}{c|c|c|c|c|c} 11\cdots1 & 00\cdots0 & 22\cdots2 & 44\cdots4 & \cdots & (2^s-2)\cdots(2^s-2) \\ \hline G_{k-1} & G_{k-1}^\beta & G_{k-1}^\beta & G_{k-1}^\beta & \cdots & G_{k-1}^\beta \end{array}\right],$$

where G_{k-1} is the generator matrix of S^{α}_{k-1}. By induction, it is easy to verify that no two columns of G^{β}_{k} are multiple of each other. Let S^{β}_{k} be the linear code over $\mathbb{Z}_{2^s}$ generated by G^{β}_{k}. Note that S^{β}_{k} is a $[2^{(s-1)(k-1)}(2^k-1), sk]$ code. Now the Remarks 3.4 & 3.5 of previous chapter generalize to the following.

Remark 4.4 *If A_{k-1} (B_{k-1}) denotes an array of codewords in $S^{\alpha}_{k-1}(S^{\beta}_{k-1})$ and if $\mathbf{i} = (i, i, \ldots, i)$ then an array of all codewords of S^{β}_{k} is given by*

$$\begin{bmatrix} A_{k-1} & B_{k-1} & B_{k-1} & B_{k-1} & \cdots & B_{k-1} \\ \mathbf{1}+A_{k-1} & B_{k-1} & \mathbf{2}+B_{k-1} & \mathbf{2^2}+B_{k-1} & \cdots & (\mathbf{2^s}-\mathbf{2})+B_{k-1} \\ \mathbf{2}+A_{k-1} & B_{k-1} & \mathbf{2^2}+B_{k-1} & \mathbf{2^3}+B_{k-1} & \cdots & (\mathbf{2^s}-\mathbf{2^2})+B_{k-1} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ (\mathbf{2^s}-\mathbf{1})+A_{k-1} & B_{k-1} & (\mathbf{2^s}-\mathbf{2})+B_{k-1} & (\mathbf{2^s}-\mathbf{2^2})+B_{k-1} & \cdots & \mathbf{2}+B_{k-1} \end{bmatrix}.$$

Remark 4.5 *Each row of G^{β}_{k} has Hamming weight $2^{(s-1)(k-1)-s}[(2^k-1)(2^s-1)+1]$, and Generalized Lee weight $2^{sk-k-1}(2^k-1)$. The Lee weight of the first row will be $2^{s(k-1)} + 2^{sk-2} - 2^{sk-k-1}$.*

Let U, Z be the set of units and zero divisors of $\mathbb{Z}_{2^s}$, respectively. Proposition 3.1 generalizes to the following.

Proposition 4.1 *Let $1 \leq j \leq k$ and let R_j be the j^{th} row of G^{β}_{k}. Then $\sum_{i\in U}\omega_i = 2^{s(k-1)}$, and each zero divisor in $\mathbb{Z}_{2^s}$ occurs $2^{(s-1)(k-2)}(2^{k-1}-1)$ times in R_j.*

Proof: It follows by induction and is similar to the proof of proposition 3.1 ∎

The next Proposition is similar to Lemma 4.2 of S^{α}_{k}.

Proposition 4.2 *Let $\mathbf{c} \in S^{\beta}_{k}$. If one of the coordinates of $\mathbf{c}$ is a unit then $\sum_{i\in U}\omega_i = 2^{s(k-1)}$, and each zero divisor in $\mathbb{Z}_{2^s}$ occurs $2^{(s-1)(k-2)}(2^{k-1}-1)$ times in $\mathbf{c}$.*

Proof: By Remark 4.4, there exist $y_1 \in S_{k-1}^{\alpha}$ and $y_2 \in S_{k-1}^{\beta}$ such that $\mathbf{c}$ can have any of the following 2^s forms:

$$\mathbf{c} = \left(\; y_1 \; \middle| \; y_2 \; \middle| \; y_2 \; \middle| \cdots \middle| \; y_2 \; \right), \qquad \mathbf{c} = \left(\; \mathbf{1} + y_1 \; \middle| \; y_2 \; \middle| \; \mathbf{2} + y_2 \; \middle| \cdots \middle| \; (\mathbf{2^s - 2}) + y_2 \; \right),$$

$$\mathbf{c} = \left(\; \mathbf{2} + y_1 \; \middle| \; y_2 \; \middle| \; \mathbf{2^2} + y_2 \; \middle| \cdots \middle| \; (\mathbf{2^s - 2^2}) + y_2 \; \right), \ldots, \text{ or}$$

$$\mathbf{c} = \left(\; (\mathbf{2^s - 1}) + y_1 \; \middle| \; y_2 \; \middle| \; (\mathbf{2^s - 2}) + y_2 \; \middle| \cdots \middle| \; \mathbf{2} + y_2 \; \right).$$

The proof now follows on the lines of the proof of Lemma 3.4. ∎

Let $\mathcal{C}$ be a linear code over $\mathbb{Z}_{2^s}$. We can define the reduction code $\mathcal{C}^{(1)}$ and the torsion code $\mathcal{C}^{(2)}$ of $\mathcal{C}$ as follows. Let $D = \{\mathbf{c} \in \mathcal{C} | c_i = 0 \text{ or } 2^{s-1} \text{ for all } i\}$. Then $\mathcal{C}^{(2)} = \{\frac{1}{2^{s-1}}\mathbf{c} | \mathbf{c} \in D\}$ is the torsion code of $\mathcal{C}$. The binary code $\mathcal{C}^{(1)} = \mathcal{C} \pmod 2$ is called the reduction code of $\mathcal{C}$. If $\mathcal{C}$ is a free module then $\mathcal{C}^{(2)} = \mathcal{C}^{(1)}$. Hence the reduction and torsion codes of S_k^{α} $\left(S_k^{\beta}\right)$ are equal. Next proposition determines these binary codes.

Proposition 4.3 *The torsion code of* S_k^{α} $\left(S_k^{\beta}\right)$ *is equivalent to* $2^{(s-1)k}$ *copies of the extended binary simplex code* $\left(2^{(s-1)(k-1)}\right.$ *copies of the binary simplex code* $\left.\right)$.

Proof: The proof is by induction on k and follows on the lines of the proof of Lemmas 3.2 and 3.5. ∎

Theorem 4.4 *The Hamming and Generalized Lee weight distributions of* S_k^{β} *are*

1. $A_H(0) = 1, A_H(2^{(s-1)(k-1)}[2^{k-m}\{2^m - 1\} + \{2^{1-m} - 1\}]) = 2^{(m-1)k}(2^k - 1)$, *for each* $m; 1 \leq m \leq s$, *and*

2. $A_{GL}(0) = 1, A_{GL}(2^{sk-1}) = 2^k - 1, A_{GL}(2^{sk-k-1}(2^k - 1)) = 2^k(2^{(s-1)k} - 1)$.

Proof: By induction on k. By Theorem 4.3 and Remark 4.4 it is easy to see that the possible nonzero Hamming (Generalized Lee) weights of S_k^{β} are

$$\left\{2^{(s-1)(k-1)}\left(2^{k-m}(2^m - 1) + (2^{1-m} - 1)\right) : 1 \leq m \leq s\right\} \left(\left\{2^{sk-1}, 2^{sk-k-1}(2^k - 1)\right\}\right).$$

By Lemma 4.2, Hamming weight of type m will occur $2^{(m-1)k}(2^k-1)$ times. Moreover generalized lee weight 2^{sk-1} will occur 2^k-1 times. Thus the other weight will occur $2^{sk}-2^k$ times. ∎

Corollary 4.5 *(i) S_k^β is of type β.*
(ii) For $s=1$, S_k^β reduces to binary Simplex Code S_k.

4.2.1 Gray Image Families

Let $\mathcal{C}$ be an $[n,k,d_H,d_{GL}]$ linear code over $\mathbb{Z}_{2^s}$ and let ϕ_G be the Generalized Gray map defined in section 2.4.2. Then $\phi_G(\mathcal{C})$ is a binary code having 2^k codewords of length $2^{s-1}n$, and minimum Hamming distance d_{GL}. However $\phi_G(\mathcal{C})$ need not be linear. Let $\mathcal{B}$ be the matrix given in (2.5) for $p=2$. The rows of $\mathcal{B}$ form a 2-basis for $\mathcal{C}$ and let $\phi_G(\mathcal{B})$ be the matrix obtained from $\mathcal{B}$ by applying the generalized gray map ϕ_G to each entry of $\mathcal{B}$. The code $\mathcal{C}_\phi$ generated by $\phi_G(\mathcal{B})$ is a $[2^{s-1}n,k,\geq\lceil\frac{d_{GL}}{2^{s-1}}\rceil]$ binary linear code. Note that $\phi_G(\mathcal{C})$ and $\mathcal{C}_\phi$ have the same number of codewords but they are not equal in general.

Recall that $\bar{S_k^\alpha}$ is the punctured code S_k^α.

Remark 4.6 *(i) $\phi_G(\bar{S_k^\alpha})$ is a binary code of length $2^{s-1}(2^{sk}-1)$ and minimum Hamming distance $2^{s(k+1)-2}$. It meets the Plotkin bound (cf.[79]) and $n<2d_H$.*
(ii) $\phi_G(S_k^\beta)$ is a binary code of length $2^{k(s-1)}(2^k-1)$ and minimum Hamming distance $2^{sk-k-1}(2^k-1)$. This is an example of a code having $n=2d_H$ (cf.[79]).

The next two results are about the binary linear codes obtained from $\bar{S_k^\alpha}$ and S_k^β.

Theorem 4.6 *Let $\mathcal{C}=\bar{S_k^\alpha}$. Then $\mathcal{C}_\phi$ is a $[2^{s-1}\cdot(2^{sk}-1),sk,2^{s(k+1)-2}]$ binary linear code consisting of 2^{s-1} copies of the binary simplex code S_{sk} with Hamming weight dis-*

tribution same as the Generalized Lee weight distribution of $\bar{S_k^\alpha}$.

Proof: By Lemma 2.5, $\mathcal{C}_\phi$ is a binary linear code of length $2^{s-1} \cdot (2^{sk} - 1)$ and dimension sk. Let $\mathcal{G}_k$ be a generator matrix of S_k^α in 2-basis form. Then

$$\mathcal{G}_k = \left[\begin{array}{c|c|c|c|c|c} 0\ldots0 & 1\ldots1 & 2\ldots2 & 3\ldots3 & \ldots & (2^s-1)\ldots(2^s-1) \\ 0\ldots0 & 2\ldots2 & 4\ldots4 & 3\cdot2\ldots3\cdot2 & \ldots & (2^s-2)\ldots(2^s-2) \\ 0\ldots0 & 4\ldots4 & 8\ldots8 & 3\cdot2^2\ldots3\cdot2^2 & \ldots & (2^s-2^2)\ldots(2^s-2^2) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0\ldots0 & 2^{s-1}\ldots2^{s-1} & 0\ldots0 & 2^{s-1}\ldots2^{s-1} & \ldots & 2^{s-1}\ldots2^{s-1} \\ G_{k-1} & G_{k-1} & G_{k-1} & G_{k-1} & \ldots & G_{k-1} \\ 2G_{k-1} & 2G_{k-1} & 2G_{k-1} & 2G_{k-1} & \ldots & 2G_{k-1} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 2^{s-1}G_{k-1} & 2^{s-1}G_{k-1} & 2^{s-1}G_{k-1} & 2^{s-1}G_{k-1} & \ldots & 2^{s-1}G_{k-1} \end{array}\right]$$

and

$$\phi_G(\mathcal{G}_k) = \left[\begin{array}{c|c|c|c|c|c} 0000\ldots00 & 0101\ldots01 & 0011\ldots11 & 0110\ldots10 & \ldots & \phi_G(2^s-1)\ldots\phi_G(2^s-1) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0000\ldots00 & 1111\ldots11 & 0000\ldots00 & 1111\ldots11 & \ldots & 1111\ldots11 \\ \hline \phi_G(\mathcal{G}_{k-1}) & \phi_G(\mathcal{G}_{k-1}) & \phi_G(\mathcal{G}_{k-1}) & \phi_G(\mathcal{G}_{k-1}) & \ldots & \phi_G(\mathcal{G}_{k-1}) \end{array}\right].$$

The proof is by induction on k and proceeds on the lines of the proof of Theorem 3.7. For $k = 2$, result follows trivially. Assume that result holds for $k-1$, i.e, $\phi_G(\mathcal{G}_{k-1})$ yields a binary code in which every nonzero codeword is of weight 2^{sk-2}. Then by induction hypothesis the possible nonzero weight from the lower portion of the matrix $\phi_G(\mathcal{G}_k)$ will be $2^s \cdot 2^{sk-2} = 2^{s(k+1)-2}$. From the structure of the first s rows of $\phi(\mathcal{G}_k)$ it is easy to verify that any linear combination of these rows with other rows coming from the lower portion has weight 2^{sk+s-2}. Puncturing the first 2^{s-1} columns corresponding to the first column of $\mathcal{G}_k$ and rearranging the rest of the columns yields the code having 2^{s-1} copies of S_{sk}. ∎

Theorem 4.7 *Let $\mathcal{C} = S_k^\beta$. Then $\mathcal{C}_\phi$ is the binary MacDonald code*

$$M_{sk,(s-1)k} : [2^{sk} - 2^{(s-1)k}, sk, 2^{sk-1} - 2^{(s-1)k-1}]$$

with Hamming weight distribution same as the Generalized Lee weight distribution of S_k^β.

Proof: By induction on k and is similar to the proof of Theorem 3.8. Let $\mathcal{G}_k^\beta$ be a generator matrix of S_k^β in 2-basis form then

$$\phi_G(\mathcal{G}_k^\beta) = \left[\begin{array}{c|c|c|c|c|c} 0101\cdots01 & 0000\cdots00 & 0011\cdots11 & 0000\cdots1111 & \cdots & \phi_G(2^s-2)\cdots\phi_G(2^s-2) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1111\cdots11 & 0000\cdots00 & 0000\cdots00 & 0000\cdots0000 & \cdots & 0000\cdots0000 \\ \hline \phi_G(\mathcal{G}_{k-1}) & \phi_G(\mathcal{G}_{k-1}^\beta) & \phi_G(\mathcal{G}_{k-1}^\beta) & \phi_G(\mathcal{G}_{k-1}^\beta) & \cdots & \phi_G(\mathcal{G}_{k-1}^\beta) \end{array}\right],$$

where $\mathcal{G}_{k-1}$ is the generator matrix of S_{k-1}^α in 2-basis form. It is easy to verify that result holds for $k = 2$. Assume that result holds for S_{k-1}^β. Then $\phi_G(\mathcal{G}_{k-1}^\beta)$ yields a binary code with possible nonzero weights either 2^{sk-s-1} or $2^{sk-s-k}(2^{k-1} - 1)$. By Theorem 4.6, $\phi_G(\mathcal{G}_{k-1})$ is a binary code in which every nonzero codeword is of weight 2^{sk-2}. Thus possible nonzero weights from lower portion of the above matrix will be either $2^{s-1}(2^{sk-s-1}) + 2^{sk-2}$ or $2^{s-1}\left(2^{sk-s-1} - 2^{sk-s-k}\right) + 2^{sk-2}$. Now the proof follows (easily from the structure of first s rows of the above matrix) by showing that the resulting weight, of any linear combination of first s rows with lower portion of the matrix, does not changes. ∎

The weight hierarchy of S_k^α and S_k^β are given by the following two theorems.

Theorem 4.8 *S_k^α satisfies the chain condition and its weight hierarchy is given by*

$$d_r(S_k^\alpha) = \sum_{i=1}^{r} 2^{sk-i} = 2^{sk} - 2^{sk-r} \quad ; 1 \le r \le sk.$$

Proof: By Remark 4.3, any r-dimensional subcode of S_k^α is of constant Generalized Lee weight. Hence by definition (see Remark 2.3)

$$d_r(S_k^\alpha) = \frac{1}{2^{r+s-2}} \sum_{\mathbf{c}(\neq 0)\in\mathcal{D}_r} w_{GL(\mathbf{c})} = 2^{-r-s+2} \cdot 2^{sk+s-2} \cdot \sum_{\mathbf{c}(\neq 0)\in\mathcal{D}_r} 1 = 2^{sk-r}(2^r - 1).$$

Let $D_1 =< 2^{s-1}R_1 >, D_2 =< 2^{s-1}R_1, 2^{s-1}R_2 >, \ldots, D_k =< 2^{s-1}R_1, \ldots, 2^{s-1}R_k >$, $D_{k+1} =< 2^{s-2}R_1, 2^{s-1}R_1, 2^{s-1}R_2, \ldots, 2^{s-1}R_k >, \ \ldots,$

$D_{sk} =< R_1, 2R_1, \ldots, 2^{s-1}R_1, \ldots, R_k, 2R_k, \ldots, 2^{s-1}R_k >$. It is easy to verify that

$$D_1 \subseteq D_2 \subseteq \cdots \subseteq D_{sk},$$

and $w_S(D_r) = d_r(S_k^\alpha)$ for $1 \leq r \leq sk$. ∎

Theorem 4.9 *Weight hierarchy of S_k^β is given by $d_r(S_k^\beta) = n(k) - 2^{(s-1)(k-1)}(2^{k-r} - 2^{i-r})$, where $1 \leq i \leq k$, $(i-1)s < r \leq is$ and $n(k) = 2^{(s-1)(k-1)}(2^k - 1)$. Moreover S_k^β satisfies the chain condition.*

Proof: The proof follows by induction on k. Clearly the result holds for $k = 2$. Assume that the result holds for S_{k-1}^β. Hence, if $1 \leq i \leq k-1$, then there exists an r-dimensional subcode of S_{k-1}^β with minimum support size as $n(k-1) - 2^{(s-1)(k-2)}(2^{k-1-r} - 2^{i-r})$. By Remark 4.4,

$$d_r(S_k^\beta) = 2^{s-1}d_r(S_{k-1}^\beta) + d_r(S_{k-1}^\alpha). \tag{4.1}$$

But all r-dimensional subcodes of S_{k-1}^α have constant support size $(2^{sk-s} - 2^{sk-s-r})$. Thus simplifying (4.1) yields the result. The case $i = k$ is trivial. Let $D_1 =< 2^{s-1}R_1 >$, $D_2 =< 2^{s-2}R_1, 2^{s-1}R_1 >, \ldots, D_s =< R_1, 2R_1, 2^2R_2, \ldots, 2^{s-1}R_1 >,$

$D_{s+1} =< R_1, 2R_1, 2^2R_2, \ldots, 2^{s-1}R_1, 2^{s-1}R_2 >, \ldots,$

$D_{s+s} =< R_1, 2R_1, 2^2R_2, \ldots, 2^{s-1}R_1, R_2, 2R_2, \ldots, 2^{s-1}R_2 >, \ldots,$

$D_{sk} =< R_1, 2R_1, 2^2R_2, \ldots, 2^{s-1}R_1, R_2, 2R_2, \ldots, 2^{s-1}R_2, \ldots, R_k, 2R_k, 2^2R_k, \ldots, 2^{s-1}R_k >$.

It is easy to see that

$$D_1 \subseteq D_2 \subseteq \cdots \subseteq D_{sk}$$

is the required chain of subcodes. ∎

The dual code of S_k^α is a code of length 2^{sk} and 2-dimension $s(2^{sk}-k)$, whereas the dual code of S_k^β is a code of length $2^{(s-1)(k-1)}(2^k-1)$ and 2-dimension $s\left(2^{(s-1)(k-1)}(2^k-1)-k\right)$. The weight hierarchies of duals can be obtained from Theorem 2.6, 4.8 & 4.9.

Chapter 5

Codes Satisfying the Chain Condition

As the births of living creatures, at first, are ill-shapen: so are all Innovations, which are the births of time. ... Francis Bacon (1561-1626)

The concept of chain condition for linear codes over $GF(q)$ was found useful in expressing weight hierarchies of a product code in terms of the weight hierarchies of its component codes. In Chapter 2, we extended the concept of chain condition to codes over $\mathbb{Z}_{p^s}$. In this chapter, it is shown that various known self-dual codes over $\mathbb{Z}_4$ satisfy the chain condition. Construction and properties of first order Reed Müller code over $\mathbb{Z}_{2^s}$ are given in section 2.

5.1 Self-Dual and Self Orthogonal Codes over $\mathbb{Z}_4$

Self dual and self orthogonal codes over $\mathbb{Z}_4$ were recently studied by several researchers like Bonnecaze, Conway, Harada, Pless, Quian, Rains and Sloane etc. (see[26],[11],[12], [33],[50],[39],[54],[86],[64],[87],[93],[92],[88] etc.). The binary image under the gray map ϕ of a self dual code over $\mathbb{Z}_4$ is formally self-dual and distance-invariant[53]. Let $\mathcal{C}$ be

a linear code over $\mathbb{Z}_4$. A codeword $\mathbf{c} \in \mathcal{C}$ is said to be a *tetrad* if it has exactly four coordinates congruent to 1 *or* 3 (mod 4) and the rest congruent to 0 (mod 4).

Let $m \geq 2$ be a positive integer. Let $\mathcal{D}_{2m}$ be the $[2m, 2m-2, 4, 4]$ type β code generated by $(m-1) \times 2m$ matrix

$$\begin{bmatrix} 1 & 1 & 1 & 3 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 3 & \cdots & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 & 1 & 3 \end{bmatrix}, \tag{5.1}$$

and let $\mathcal{D}_{2m}^0$ be the $[2m, 2m-1]$ code generated by $\mathcal{D}_{2m}$ and the tetrads $1300\ldots0011$. Equivalently $\mathcal{D}_{2m}^0$ is generated by the matrix (see[26])

$$\begin{bmatrix} 1 & 1 & 1 & 3 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 3 & \cdots & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 & 1 & 3 \\ 2 & 0 & 2 & 0 & 2 & 0 & \cdots & 0 & 2 & 0 & 2 & 0 \end{bmatrix}. \tag{5.2}$$

Let $\mathcal{D}_{2m}^+$ be the $[2m, 2m-1]$ code generated by $\mathcal{D}_{2m}$ and $00\ldots0022$ and let $\mathcal{D}_{2m}^{\oplus}$ be the code generated by $\mathcal{D}_{2m}^0$ and $\mathcal{D}_{2m}^+$. Note that $\mathcal{D}_{2m}^{\oplus}$ is a $[2m, 2m]$ self-dual code([26]).

Let $\mathcal{E}_7$ be the $[7, 6, 4, 4]$ type β code generated by the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 3 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 3 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 3 \end{bmatrix} \tag{5.3}$$

and let $\mathcal{E}_7^+$ be the $[7, 7, 4, 4]$ type β code generated by $\mathcal{E}_7$ and 2222222. It was observed in[26] that $\mathcal{E}_7^+$ is a self-dual code and the reduction code of both $\mathcal{E}_7$ & $\mathcal{E}_7^+$ is the

Hamming code of length 7. They also show that the code $\mathcal{E}_8$ generated by the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 3 & 0 & 1 & 3 \\ 0 & 0 & 1 & 0 & 3 & 3 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 & 1 & 3 & 0 \end{bmatrix} \tag{5.4}$$

is a $[8, 8, 4, 4]$ self dual code. Note that it is a type β code.

In[26] Conway and Sloane has shown that any self orthogonal code over $\mathbb{Z}_4$ generated by *'tetrads'* is equivalent to a direct sum of codes $\mathcal{D}_{2m}, \mathcal{D}_{2m}^0, \mathcal{D}_{2m}^+, \mathcal{D}_{2m}^{\oplus}(m = 1, 2, \dots), \mathcal{E}_7, \mathcal{E}_7^+, \mathcal{E}_8$. The following Theorem shows that $\mathcal{D}_{2m}, \mathcal{E}_7, \mathcal{E}_7^+$ and $\mathcal{E}_8$ satisfy the chain condition. Note that the smallest self-dual code $\mathcal{A}_1 = \{0, 2\}$ trivially satisfies the chain condition.

Theorem 5.1 *$\mathcal{D}_{2m}, \mathcal{E}_7, \mathcal{E}_7^+$ and $\mathcal{E}_8$ satisfies chain conditions.*

Proof: It is easy to verify that the weight hierarchy of $\mathcal{E}_7$ is $\{4, 4, 6, 6, 7, 7\}$. Consider the codewords $\mathbf{x}_1 = (1101003), \mathbf{x}_2 = (2111030)$ and $\mathbf{x}_3 = (3023132)$ of $\mathcal{E}_7$. Let $D_1 =< 2\mathbf{x}_1 >$, $D_2 =< \mathbf{x}_1, 2\mathbf{x}_1 >$, $D_3 =< \mathbf{x}_1, 2\mathbf{x}_1, 2\mathbf{x}_2 >$, $D_4 =< \mathbf{x}_1, 2\mathbf{x}_1, \mathbf{x}_2, 2\mathbf{x}_2 >$, $D_5 =< \mathbf{x}_1, 2\mathbf{x}_1, \mathbf{x}_2, 2\mathbf{x}_2, 2\mathbf{x}_3 >$, and $D_6 =< \mathbf{x}_1, 2\mathbf{x}_1, \mathbf{x}_2, 2\mathbf{x}_2, \mathbf{x}_3, 2\mathbf{x}_3 >$. It is easy to verify that $D_1 \subseteq D_2 \dots \subseteq D_6$ is the required chain of subcodes.

Therefore for $\mathcal{E}_7^+$ the required chain of subcodes can be taken as $D_1 \subseteq D_2 \dots \subseteq D_6 \subseteq D_7$ where D_i for $1 \leq i \leq 6$ are the subcodes defined for $\mathcal{E}_7$ and
$D_7 =< \mathbf{x}_1, 2\mathbf{x}_1, \mathbf{x}_2, 2\mathbf{x}_2, \mathbf{x}_3, 2\mathbf{x}_3, 2222222 >$. Hence $\mathcal{E}_7^+$ satisfies the chain condition and its weight hierarchy is $\{4, 4, 6, 6, 7, 7, 8\}$.

Clearly, the weight hierarchy of $\mathcal{E}_8$ is $\{4, 4, 6, 6, 7, 7, 8, 8\}$. If $R_i (1 \leq i \leq 4)$ denote the first four rows of the matrix given in (5.4) and if $D_1 =< 2R_4 >$, $D_2 =< R_4, 2R_4 >$, $D_3 =< 2R_3, R_4, 2R_4 >$, $D_4 =< R_3, 2R_3, R_4, 2R_4 >, \dots$,
$D_8 =< R_1, 2R_1, \dots, R_3, 2R_3, R_4, 2R_4 >$ then $D_1 \subseteq D_2 \dots \subseteq D_8$ and $w_s(D_r) = d_r(\mathcal{E}_8)$.

It is easy to see that the code $\mathcal{D}_{2m}$ has weight hierarchy $\{4, 4, 6, 6, 8, 8, \ldots, 2m-2, 2m-2, 2m, 2m\}$. Let $R_1, \ldots R_{m-1}$ be the first $m-1$ rows of the matrix given in (5.1) and let $D_1 =< 2R_1 >$, $D_2 =< R_1, 2R_1 >, \ldots$, $D_{2m-3} =< R_1, 2R_1, \ldots, R_{m-2}, 2R_{m-2}, 2R_{m-1} >$,
$D_{2m-2} =< R_1, 2R_1, \ldots, R_{m-2}, 2R_{m-2}, R_{m-1}, 2R_{m-1} >$. Then $D_1 \subseteq D_2 \ldots \subseteq D_{2m-2}$ and $w_s(D_r) = d_r(\mathcal{D}_{2m}), 1 \leq r \leq 2m-2$. ∎

There is another self-dual code $\mathcal{L}_8$ of length 8 defined in[26]. $\mathcal{L}_8$ is $[8, 8, 2, 4]$ type α code generated by the matrix

$$\begin{bmatrix} 00 & 11 & 02 & 13 \\ 00 & 02 & 13 & 11 \\ 11 & 02 & 00 & 13 \\ 02 & 02 & 02 & 02 \\ 00 & 00 & 00 & 22 \end{bmatrix}. \tag{5.5}$$

Proposition 5.1 *$\mathcal{L}_8$ satisfies the chain condition.*

Proof: It is easy to see that the weight hierarchy of $\mathcal{L}_8$ is $\{2, 4, 5, 6, 7, 7, 8, 8\}$. Let $\mathbf{x}_1 = (00000022), \mathbf{x}_2 = (11020013), \mathbf{x}_3 = (13000211), \mathbf{x}_4 = (02001131)$ and $\mathbf{x}_5 = (13021122)$ be the five codewords of $\mathcal{L}_8$. Let $\mathcal{D}_1 =< \mathbf{x}_1 >$, $\mathcal{D}_2 =< 2x_2, \mathbf{x}_1 >$, $\mathcal{D}_3 =< \mathbf{x}_2, 2\mathbf{x}_2, \mathbf{x}_1 >$, $\mathcal{D}_4 =< \mathbf{x}_3, \mathbf{x}_2, 2\mathbf{x}_2, \mathbf{x}_1 >$, $\mathcal{D}_5 =< 2\mathbf{x}_4, \mathbf{x}_3, \mathbf{x}_2, 2\mathbf{x}_2, \mathbf{x}_1 >$, $\mathcal{D}_6 =< \mathbf{x}_4, 2\mathbf{x}_4, \mathbf{x}_3, \mathbf{x}_2, 2\mathbf{x}_2, \mathbf{x}_1 >$, $\mathcal{D}_7 =< 2\mathbf{x}_5, \mathbf{x}_4, 2\mathbf{x}_4, \mathbf{x}_3, \mathbf{x}_2, 2\mathbf{x}_2, \mathbf{x}_1 >$, and $\mathcal{D}_8 =< \mathbf{x}_5, 2\mathbf{x}_5, \mathbf{x}_4, 2\mathbf{x}_4, \mathbf{x}_3, \mathbf{x}_2, 2\mathbf{x}_2, \mathbf{x}_1 >$. Then $D_1 \subseteq D_2 \ldots \subseteq D_8$ and $w_s(D_r) = d_r(\mathcal{L}_8),\ 1 \leq r \leq 8$. ∎

Let $m \geq 1$. Let $\mathcal{K}_{4m}$ be the $[4m, 4m, 2, 4]$ type α code generated by the $(4m-1) \times 4m$

matrix

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 2 & 0 & \cdots & 0 & 2 \\ 0 & 0 & 2 & \cdots & 0 & 2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 2 & 2 \end{bmatrix} \tag{5.6}$$

and let $\mathcal{K}_8^{'}$ be the $[8, 8, 2, 4]$ type α code generated by the matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 2 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \end{bmatrix}. \tag{5.7}$$

Both of these self dual codes can also be obtained from a labeled graph[26]. The code $\mathcal{K}_{4m}$ was first constructed by Klemm[71].

Theorem 5.2 *Klemm Code $\mathcal{K}_{4m}(m \geq 1)$ and the code $\mathcal{K}_8^{'}$ satisfy the chain condition and weight hierarchy of $\mathcal{K}_{4m}$ is given by*

$$d_r(\mathcal{K}_{4m}) = \begin{cases} r+1, & 1 \leq r \leq 4m-2, \\ 4m, & r = 4m-1 \ \& \ 4m. \end{cases} \tag{5.8}$$

Proof: It is easy to see that the weight hierarchy of the Klemm code is given by (5.8). Let $R_i (1 \leq i \leq 4m-1)$ be the first $4m-1$ rows of (5.6). For $1 \leq r \leq 4m-2$, let $D_r =< R_{4m-i} : 1 \leq i \leq r >$ also let $\mathcal{D}_{4m-1} =< 2R_1, R_2, R_3, \cdots, R_{4m-2}, R_{4m-1} >$, $\mathcal{D}_{4m} =< R_1, 2R_1, R_2, R_3, \cdots, R_{4m-2}, R_{4m-1} >$. Then $D_1 \subseteq D_2 \ldots \subseteq D_{4m}$ and $w_s(D_r) = d_r(\mathcal{K}_{4m}), 1 \leq r \leq 4m$.

For the code $\mathcal{K}_8^{'}$ it can be easily checked that its weight hierarchy is $\{2, 3, 4, 5, 6, 7, 8, 8\}$. Let $\mathbf{x}_1 = (00000022), \mathbf{x}_2 = (00000202), \mathbf{x}_3 = (00021111), \mathbf{x}_4 = (00201111)$,

$\mathbf{x}_5 = (02001111), \mathbf{x}_6 = (20001111)$ and $\mathbf{x}_7 = (20001133)$ be the seven codewords of $\mathcal{K}_8'$. Then $D_1 =< \mathbf{x}_1 >$, $D_2 =< \mathbf{x}_2, \mathbf{x}_1 >$, $D_3 =< 2\mathbf{x}_3, \mathbf{x}_2, \mathbf{x}_1 >$, $D_4 =< \mathbf{x}_3, 2\mathbf{x}_3, \mathbf{x}_2, \mathbf{x}_1 >$, $D_5 =< \mathbf{x}_4, \mathbf{x}_3, 2\mathbf{x}_3, \mathbf{x}_2, \mathbf{x}_1 >$, $D_6 =< \mathbf{x}_5, \mathbf{x}_4, \mathbf{x}_3, 2\mathbf{x}_3, \mathbf{x}_2, \mathbf{x}_1 >$,
$D_7 =< \mathbf{x}_6, \mathbf{x}_5, \mathbf{x}_4, \mathbf{x}_3, 2\mathbf{x}_3, \mathbf{x}_2, \mathbf{x}_1 >$ and $D_8 =< \mathbf{x}_7, \mathbf{x}_6, \mathbf{x}_5, \mathbf{x}_4, \mathbf{x}_3, 2\mathbf{x}_3, \mathbf{x}_2, \mathbf{x}_1 >$ form the required chain of subcodes. ∎

Some of the self-dual $\mathbb{Z}_4$-codes have the property that all Euclidean weights are multiple of 8 and they contain the all-one vector. These codes are called *Type-II* codes over $\mathbb{Z}_4$ (see[54],[26]). The key motivation to study these codes is that one can associate a Type-II even unimodular lattice via the construction $A \pmod 4$[92],[16]. Several such Type-II lattices have been obtained in such a fashion.

Quadratic residue codes over $\mathbb{Z}_4$ is a well known family of Type-II codes. These codes are obtained by Hensel uplifting of the binary quadratic residue codes[88],[54]. If $n = q + 1$ and $q \equiv -1 \pmod 8$ is a prime power then Pless and Quian have shown that an extended quadratic residue code QR_n of length n is a Type II code[88]. These have been widely studied by Pless et al for $n = 8, 24, 32, 48$ etc.[88],[87]. QR_8 is the well known *Octacode* generated by the matrix

$$\begin{bmatrix} 3 & 3 & 2 & 3 & 1 & 0 & 0 & 0 \\ 3 & 0 & 3 & 2 & 3 & 1 & 0 & 0 \\ 3 & 0 & 0 & 3 & 2 & 3 & 1 & 0 \\ 3 & 0 & 0 & 0 & 3 & 2 & 3 & 1 \end{bmatrix}. \tag{5.9}$$

It is an $[8, 8, 4, 6]$ code of type β. The code QR_{24} is the well known *lifted Golay Code*. It is a $[24, 24, 8, 12]$ code of type β generated by the matrix

$$\begin{bmatrix}
3&3&1&0&0&2&3&3&3&0&3&2&1&0&0&0&0&0&0&0&0&0&0&0\\
3&0&3&1&0&0&2&3&3&3&0&3&2&1&0&0&0&0&0&0&0&0&0&0\\
3&0&0&3&1&0&0&2&3&3&3&0&3&2&1&0&0&0&0&0&0&0&0&0\\
3&0&0&0&3&1&0&0&2&3&3&3&0&3&2&1&0&0&0&0&0&0&0&0\\
3&0&0&0&0&3&1&0&0&2&3&3&3&0&3&2&1&0&0&0&0&0&0&0\\
3&0&0&0&0&0&3&1&0&0&2&3&3&3&0&3&2&1&0&0&0&0&0&0\\
3&0&0&0&0&0&0&3&1&0&0&2&3&3&3&0&3&2&1&0&0&0&0&0\\
3&0&0&0&0&0&0&0&3&1&0&0&2&3&3&3&0&3&2&1&0&0&0&0\\
3&0&0&0&0&0&0&0&0&3&1&0&0&2&3&3&3&0&3&2&1&0&0&0\\
3&0&0&0&0&0&0&0&0&0&3&1&0&0&2&3&3&3&0&3&2&1&0&0\\
3&0&0&0&0&0&0&0&0&0&0&3&1&0&0&2&3&3&3&0&3&2&1&0\\
3&0&0&0&0&0&0&0&0&0&0&0&3&1&0&0&2&3&3&3&0&3&2&1
\end{bmatrix}. \tag{5.10}$$

The following theorem shows that these codes satisfy the chain condition.

Theorem 5.3 *Extended quadratic residue codes QR_8 and QR_{24} over $\mathbb{Z}_4$ satisfy the chain condition.*

Proof: It is easy to see that the weight hierarchy of the Octacode is $\{4,5,6,6,7,7,8,8\}$ (see also[1]). Let $R_i, 1 \leq i \leq 4$, be the last four rows of the matrix (5.9). Let $\mathcal{D}_1 =< 2R_1 >$, $\mathcal{D}_2 =< R_1, 2R_1 >$, $\mathcal{D}_3 =< 2R_2, R_1, 2R_1 >$, $\mathcal{D}_4 =< R_2, 2R_2, R_1, 2R_1 >$, $\mathcal{D}_5 =< 2R_3, R_2, 2R_2, R_1, 2R_1 >$, $\mathcal{D}_6 =< R_3, 2R_3, R_2, 2R_2, R_1, 2R_1 >$, $\mathcal{D}_7 =< 2R_4, R_3, 2R_3, R_2, 2R_2, R_1, 2R_1 >$, and $\mathcal{D}_8 =< R_4, 2R_4, R_3, 2R_3, R_2, 2R_2, R_1, 2R_1 >$. Then it is easy to verify that $D_1 \subseteq D_2 \ldots \subseteq D_8$ and $w_s(D_r) = d_r(QR_8), 1 \leq r \leq 8$.

It can be seen easily that $\{8,10,12,13,14,15,16,16,17,17,18,18,19,19,20,20,21,21,22,22,23,23,24,24\}$ is the weight hierarchy of QR_{24}. Let $R_i; 1 \leq i \leq 12$ be the first 12 rows of (5.10). Let $\mathcal{D}_1 =< 2R_{12} >$, $\mathcal{D}_2 =< R_{12}, 2R_{12} >$, $\mathcal{D}_3 =< R_{12}, 2R_{12}, 2R_{11} >, \ldots,$ $\mathcal{D}_{24} =< R_1, 2R_1, \ldots, R_{12}, 2R_{12} >$. Then $D_1 \subseteq D_2 \ldots \subseteq D_{24}$ and $w_s(D_r) = d_r(QR_{24})$, $1 \leq r \leq 24$. ∎

5.2 First order Reed Müller Code over $\mathbb{Z}_{2^s}$

In[53], Hammons et al have constructed a linear code over $\mathbb{Z}_4$ (called Quaternary first order Reed Müller code) whose gray image is the binary first order Reed Müller code. In this section we construct a linear code over $\mathbb{Z}_{2^s}$ whose image under the generalized gray map ϕ_G is the binary first order Reed Müller code. Some basic properties of these are also obtained.

Let $1 \leq i \leq m-s+1$. Let $\mathbf{v}_i$ be a vector of length 2^{m-s+1} consisting of successive blocks of $0's$ and $1's$ each of size $2^{(m-s+1)-i}$ and let $\mathbf{1} = (111\ldots11) \in \mathbb{Z}_2^{2^{m-s+1}}$. Let G be a $(m-s+2) \times 2^{m-s+1}$ matrix given by (consisting of the rows as $\mathbf{1}$ and $2^{s-1}\mathbf{v}_i$ $(1 \leq i \leq m-s+1)$)

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 0 & \cdots & 0 & 0 & 2^{s-1} & 2^{s-1} & \cdots & 2^{s-1} & 2^{s-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 2^{s-1} & \cdots & 0 & 2^{s-1} & 0 & 2^{s-1} & \cdots & 0 & 2^{s-1} \end{bmatrix} \tag{5.11}$$

The code generated by G is called the *first order Reed Müller code over* $\mathbb{Z}_{2^s}$, denoted $\mathcal{R}^{1,m-s+1}$. It is a $[2^{m-s+1}, m+1, 2^{m-s}, 2^{m-s+1}, 2^{m-1}]$ linear code over $\mathbb{Z}_{2^s}$. It's generator matrix in 2-basis form is given by

$$\mathcal{G} = \begin{bmatrix} 1 & 1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 2 & 2 & \cdots & 2 & 2 & 2 & 2 & \cdots & 2 & 2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 2^{s-1} & 2^{s-1} & \cdots & 2^{s-1} & 2^{s-1} & 2^{s-1} & 2^{s-1} & \cdots & 2^{s-1} & 2^{s-1} \\ 0 & 0 & \cdots & 0 & 0 & 2^{s-1} & 2^{s-1} & \cdots & 2^{s-1} & 2^{s-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 2^{s-1} & \cdots & 0 & 2^{s-1} & 0 & 2^{s-1} & \cdots & 0 & 2^{s-1} \end{bmatrix} \tag{5.12}$$

Remark 5.1 *For $s = 2$, $\mathcal{R}^{1,m-s+1}$ reduces to Quaternary first order Reed Müller Code $ZRM(1, m)$ defined in[53].*

Proposition 5.2 *Hamming and Generalized Lee weight distributions of $\mathcal{R}^{1,m-s+1}$ are:*

1. $A_H(0) = 1, A_H(2^{m-s}) = 2^{m-s+2} - 2$ & $A_H(2^{m-s+1}) = 2^{m+1} - 2^{m-s+2} + 1$,

2. $A_{GL}(0) = 1, A_{GL}(2^m) = 1$ & $A_{GL}(2^{m-1}) = 2^{m+1} - 2$.

Proof: Note that first s rows of the matrix $\mathcal{G}$ given by (5.12) have Hamming weight 2^{m-s+1} and remaning $m - s + 1$ rows are of Hamming weight 2^{m-s}. It is easy to see that any 2-linear combination of last $m - s + 1$ rows also has Hamming weight 2^{m-s}. Hence $A_H(2^{m-s}) = 2^{m-s+2} - 2$. Since $-2^{s-1} = 2^{s-1}$ in $\mathbb{Z}_{2^s}$, every other nontrivial 2-linear combination has weight 2^{m-s+1}. Thus $A_H(2^{m-s+1}) = 2^{m+1} - 2^{m-s+2} + 1$. Similar arguments holds for generalized Lee weight. ∎

Theorem 5.4 *Weight hierarchy of $\mathcal{R}^{1,m-s+1}$ is given by*

$$d_t(\mathcal{R}^{1,m-s+1}) = \begin{cases} \sum_{i=0}^{t-1} 2^{m-s-i}, & 1 \le t \le m-s+1 \\ 2^{m-s+1}, & m-s+1 < t \le m+1. \end{cases}$$

Moreover, $\mathcal{R}^{1,m-s+1}$ satisfies the chain condition.

Proof: By Corollary 2.9,

$$d_t(\mathcal{R}^{1,m-s+1}) \ge \left\lceil \frac{(2^t-1)2^{m-1}}{2^{t+s-2}} \right\rceil = \begin{cases} \sum_{i=0}^{t-1} 2^{m-s-i}, & 1 \le t \le m-s+1 \\ 2^{m-s+1}, & m-s+1 < t \le m+1. \end{cases} \quad (5.13)$$

Let $1 \le t \le m - s + 1$. Let D be a t-dimensional subcode of $\mathcal{R}^{1,m-s+1}$ generated by any t rows chosen from last $m - s + 1$ rows of (5.12). Thus chosen t rows shares $2^{m-s+1-t}$ common zero bit positions. Hence the support size of D is $\sum_{i=0}^{t-1} 2^{m-s-i}$. If $t > m - s + 1$ then trivially equality holds in (5.13).

Let $\mathcal{D}_1 =< 2^{s-1}\mathbf{v}_{m-s+1} >$, $\mathcal{D}_2 =< 2^{s-1}\mathbf{v}_{m-s}, 2^{s-1}\mathbf{v}_{m-s+1} >, \ldots ,$

$\mathcal{D}_{m-s+1} =< 2^{s-1}\mathbf{v}_1, \ldots , 2^{s-1}\mathbf{v}_{m-s}, 2^{s-1}\mathbf{v}_{m-s+1} >,$

$\mathcal{D}_{m-s+2} =< \mathbf{2^{s-1}}, 2^{s-1}\mathbf{v}_1, \ldots , 2^{s-1}\mathbf{v}_{m-s}, 2^{s-1}\mathbf{v}_{m-s+1} >, \ldots ,$ and

$\mathcal{D}_{m-1} =< \mathbf{1}, \mathbf{2}, \mathbf{2^2}, \ldots , \mathbf{2^{s-1}}, 2^{s-1}\mathbf{v}_1, \ldots , 2^{s-1}\mathbf{v}_{m-s}, 2^{s-1}\mathbf{v}_{m-s+1} > .$

Then $D_1 \subseteq D_2 \ldots \subseteq D_{m+1}$ and $w_s(D_r) = d_r(\mathcal{R}^{1,m-s+1}); 1 \leq r \leq m+1.$ ∎

The map ϕ_G is nonlinear over $\mathbb{Z}_{2^s}$ as $\phi_G(2+3) \neq \phi_G(2) + \phi_G(3)$. However we have the following Lemma.

Lemma 5.5 *Let* $T = \{2^i : 0 \leq i \leq s-1\} \cup \{0\}$. *Then*

$$\phi_G(a+b) = \phi_G(a) + \phi_G(b), \quad \textit{for all} \quad a, b \in T.$$

Proof: The verification follows easily using the structure of E_s given by (2.6) and the definition of ϕ_G in (2.7). ∎

Theorem 5.6 $\mathcal{R}^{1,m-s+1}$ *is* $\mathbb{Z}_2$*-linear.*

Proof: Let $\mathbf{c} \in \mathcal{R}^{1,m-s+1}$. Then $\mathbf{c}$ can be written as a 2-linear combination of the rows of the matrix $\mathcal{G}$ given by (5.12). Since ϕ_G maps $\mathcal{G}$ to a generator matrix of a binary first order Reed Müller code (with some permutation of the rows, see (2.9, 5.12 and the Lemma 5.5). Thus $\phi_G(\mathbf{c})$ belongs to the binary linear first order Reed Müller code. Hence $\mathcal{R}^{1,m-s+1}$ is $\mathbb{Z}_2$-linear. ∎

Chapter 6

Norm Quadratic Residue Codes

Often you have to rely on intuition. ... Bill Gates (1955-till date)

In this chapter we investigate a weakly self dual family of binary linear codes, called, *NQR Codes* based on the concept of quadratic residues and obtain its basic properties over binary field. It is shown that NQR Codes are $\mathbb{Z}_4$-linear.

6.1 Definitions and Basic Results

Let p be an odd prime. The Poincáre finite upper half plane is the set

$$H_p := \{x + \sqrt{\delta}y \quad \Big| \quad x, y \in GF(p), y \neq 0, \\ \delta \text{ is a quadratic non residue (q.n.r.)} \pmod p\}. \tag{6.1}$$

In[110] Tiu and Wallace have used it to construct a new class of binary linear codes $\mathcal{C}_p$ called *norm quadratic residue (NQR) codes*. The length of each codeword in $\mathcal{C}_p$ is $p(p-1)$, the number of points in H_p. The points in H_p are ordered lexicographically; i.e, $(x, y) < (u, v)$ if $x < u$ or $x = u$ and $y < v$. For each $a \in GF(p)$, the set $B_a = \{(a, 1), (a, 2), \ldots, (a, p-1)\}$ is called a *block*. Let G be the $(p+1) \times p(p-1)$

matrix

$$G = \begin{bmatrix} R_0 \\ R_1 \\ \vdots \\ R_p \end{bmatrix}$$

where each $R_i \in I\!F_2^{p(p-1)}$ is defined as follows. R_0 has an 1 in position (x, y) if $x^2 - \delta y^2$, the norm of (x, y) in H_p, is a quadratic residue (q.r.) mod p and 0, otherwise. $R_1, R_2, \ldots, R_{p-1}$ are block wise cyclic shifts of R_0 corresponding to blocks $B_0, B_1, \ldots, B_{p-1}$, and R_p is the all one vector. The set of entries in R_0 corresponding to the block B_a will be denoted by b_a. For example, for $p = 7$, the columns of G are grouped corresponding to blocks $B_0, B_1, \cdots, B_6$, and the corresponding generator matrix of the NQR code $\mathcal{C}_7$ with $\delta = 6$ is

$$G = \begin{bmatrix} b_0 & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 \\ b_6 & b_0 & b_1 & b_2 & b_3 & b_4 & b_5 \\ b_5 & b_6 & b_0 & b_1 & b_2 & b_3 & b_4 \\ b_4 & b_5 & b_6 & b_0 & b_1 & b_2 & b_3 \\ b_3 & b_4 & b_5 & b_6 & b_0 & b_1 & b_2 \\ b_2 & b_3 & b_4 & b_5 & b_6 & b_0 & b_1 \\ b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_0 \\ \mathbf{e} & \mathbf{e} & \mathbf{e} & \mathbf{e} & \mathbf{e} & \mathbf{e} & \mathbf{e} \end{bmatrix};$$

where $b_0 = 111111$, $b_1 = 100001$, $b_2 = 010010$, $b_3 = 001100$, $b_4 = 001100$, $b_5 = 010010$, $b_6 = 100001$, and $\mathbf{e} = 111111$.

The code $\mathcal{C}_p$ generated by the matrix G is called the NQR Code[110]. If p is of the form $4m+1$ then Tiu and Wallace[110] have shown that $\dim \mathcal{C}_p \leq p$, $d_H \geq p-1$, $\mathcal{C}_p$ is weakly self dual and that the weight of each codeword is divisible by 4. In the present chapter we show that if p is a prime of the form $4m-1$ then also $\mathcal{C}_p$ satisfies similar

properties. It is shown that $\dim \mathcal{C}_p = p$, $\mathcal{C}_p$ is normal and its covering radius is $\frac{p(p-1)}{2}$. It is also shown that $\mathcal{C}_p$ is $\mathbb{Z}_4$-linear.

The following observations about the matrix G are useful for further discussion.

Remark 6.1 *In R_0, the entries corresponding to the block B_0 has all 0's (all 1's) if p is of the form $4m+1$ $(4m-1)$.*

Remark 6.2 *For $a > 0$, $b_a = b_{p-a}$.*

Remark 6.3 *In any row of G, the entries corresponding to any block B_a, have mirror symmetry with respect to its center. Thus, in R_i, the entry corresponding to point (a, j) is same as the entry corresponding to the point $(a, p-j)$ for every $0 \leq a \leq p-1$ and $1 \leq j \leq \frac{(p-1)}{2}$.*

The following result of Perrön [85] (also see [79]) about the q.r. is useful in determining properties of NQR codes.

Theorem 6.1 *(i) Let $p = 4m+1$ and let $r_1, r_2, \ldots, r_{2m+1}$ be the $(2m+1)$ quadratic residues mod p (together with 0). If k is a q.n.r. mod p then among $(2m+1)$ numbers $r_i + k$ there are m quadratic residues (not including 0) and $m+1$ quadratic non residues.*
(ii) Let $p = 4m+1$ and let $n_1, n_2, \ldots, n_{2m}$ be the $2m$ quadratic non residues mod p. If k is a q.r. mod p then among the $2m$ numbers $n_i + k$ there are exactly m quadratic residues (not including 0) and m quadratic non residues.
(iii) Let $p = 4m-1$ be a prime and let $r_1, r_2, \ldots, r_{2m}$ be the $2m$ quadratic residues mod p (together with 0). If a is relatively prime to p then among the $2m$ numbers $r_i + a$ there are m quadratic residues and m quadratic non residues.
(iv) Let $p = 4m-1$. Suppose $n_1, n_2, \ldots, n_{2m-1}$ are the $(2m-1)$ quadratic non residues and let a be relatively prime to p. Then among the $(2m-1)$ numbers $n_i + a$ there are m quadratic residues (possibly including 0) and $m-1$ quadratic non residues.

Lemma 6.2 *Every row of G except the last row has weight* $\frac{(p-1)^2}{2}$.

Proof: Since each row except the last row of G is a block wise cyclic shift of $R_0, wt(R_i) = wt(R_0)$ for all $i = 1, 2, \ldots, p-1$. By Remark 6.2,

$$wt(R_0) = wt(b_0) + 2\{wt(b_1) + \ldots + wt(b_{\frac{p-1}{2}})\} \tag{6.2}$$

and by Remark 6.1, $wt(b_0) = \begin{cases} 0 & \text{if } p = 4m+1 \\ p-1 & \text{if } p = 4m-1. \end{cases}$

To determine $wt(b_a)$ for $a \neq 0$, let $B'_a = \{(a,1), \ldots, (a, \frac{(p-1)}{2})\}$, and let $N(B'_a) = \{a^2 - \delta.1^2, a^2 - \delta.2^2, \ldots, a^2 - \delta.\frac{(p-1)}{4}^2\}$. If $p = 4m+1$ by (ii) of Theorem 6.1, $N(B'_a)$ contains m quadratic residues and m quadratic non residues. Therefore by equation (6.2), $wt(R_0) = 0 + 2.\{2m + \ldots + 2m\} = 8m^2 = \frac{(p-1)^2}{2}$. If $p = 4m-1$, by (iii) of Theorem 6.1 there will be $(m-1)$ quadratic residues and m quadratic non residues in $N(B'_a)$. Hence by Equation (6.2) $wt(R_0) = \frac{(p-1)^2}{2}$. ∎

As an immediate Corollary we have

Corollary 6.3 *The minimum distance of* $\mathcal{C}_p$ *is at most* $\frac{(p-1)^2}{2}$.

Lemma 6.4 *Weight of each column of G is* $\frac{(p+1)}{2}$.

Proof: It is sufficient to show that the result is true for the coordinate position $(0, a) \in H_p$, for some $a \in GF(p)$. The first p entries in this column will be entries from R_0 corresponding to coordinate positions $M_a = \{(0,a), (1,a), \ldots, (p-1, a)\}$. Let $N(M_a) = \{0^2 - \delta a^2, \ldots, (p-1)^2 - \delta a^2\}$. If $p = 4m+1$, then $(-\delta a^2)$ is a q.n.r. and hence by (i) of Theorem 6.1, $N(M_a)$ contains $2m$ quadratic residues and $(2m+1)$ quadratic non residues. Hence total number of 1's in the a^{th} column is $(2m+1)$.

If $p = 4m-1$, then $(-\delta a^2)$ is a q.r. and $(p, -\delta a^2) = 1$. Hence by (iii) of Theorem 6.1, $N(M_a)$ contains $(2m-1)$ quadratic residues and $2m$ quadratic non residues. Thus the

number of 1's in the a^{th} column is $2m$. ∎

The following relation among the rows of G follows immediately from the above Lemma.

Corollary 6.5 *(i) If $p = 4m + 1$ then $R_0 = R_1 + R_2 + \ldots + R_{p-1}$;*

(ii) If $p = 4m - 1$ then $R_p = R_0 + R_1 + \ldots + R_{p-1}$.

Before stating our next theorem we recall some basic facts needed about the circulant matrices over binary fields as they play an important role in the proof.

A binary square matrix C of order p is said to be *circulant* if $C = (c_{ij}) = (c_{j-i+1}) := cir(\gamma)$; where $\gamma = (c_0, c_1, \ldots, c_{p-1})$ is the first row of C and subscripts are mod p. We state some of its basic properties in the following Lemma. These are given as an exercise in[79].

Lemma 6.6 *(i) The algebra of $p \times p$ circulant matrices over a field $\mathbb{F}$ is isomorphic to the algebra of polynomials in the ring $\mathbb{F}[z]/(z^p - 1)$, if the circulant matrix $C = cir(\gamma)$ is mapped onto the polynomial $P_\gamma(z) = c_0 + c_1 z + \ldots + c_{p-1} z^{p-1}$.*

(ii) Let $\alpha_0(= 1), \alpha_1, \ldots, \alpha_{p-1}$ be the pth roots of unity in some extension field, say, $GF(2^r)$ and let $A = (a_{ij}) = (\alpha_i^j), 0 \leq i, j \leq p - 1$, be the van der Monde matrix over $GF(2^r)$. Then A diagonalizes C with diagonal entries as the eigen values of C. More precisely we have,

$$A^{-1}CA = \ diag(P_\gamma(\alpha_0), P_\gamma(\alpha_1), \ldots, P_\gamma(\alpha_{p-1})).$$

Theorem 6.7 $\dim \mathcal{C}_p = p, (p \neq 2)$.

Proof: Let C be the $p \times p$ sub matrix of G obtained by deleting the last row and by considering columns corresponding to coordinate positions $(0, 1), (1, 1)$ $(2, 1), \ldots, (p - 1, 1)$. In view of Corollary 6.5 it is sufficient to show that rank(C) is

$p-1$ or p according to the form $4m+1$ or $4m-1$ of p. We observe that C is a binary circulant matrix, say , $C = \mathrm{cir}(\gamma) = \mathrm{cir}(c_0, c_1, \ldots, c_{p-1}); c_i \in GF(2)$. Hence, by Lemma 6.6,

$$A^{-1}CA = \ \mathrm{diag}(P_\gamma(\alpha_0), P_\gamma(\alpha_1), \ldots, P_\gamma(\alpha_{p-1}));$$

where the matrix A, the polynomial $P_\gamma(z) = c_0 + c_1 z + \ldots + c_{p-1}z^{p-1}$, and the α_i's for $0 \leq i \leq p-1$ are as in Lemma 6.6. If $1 \leq i \leq p-1, P_\gamma(\alpha_i) \neq 0$ and $P_\gamma(\alpha_0) = \frac{p-1}{2} \equiv 0(\mathrm{mod}2)$ if and only if p is of the form $4m+1$. ∎

Recall that $\mathrm{PSL}_2(p)$, the projective special linear group, is the factor group $SL_2(p)/\zeta$, where $SL_2(p)$ is the special linear group on $GF(p)$ and $\zeta = \{I, -I\}$ with I the 2×2 identity matrix. Moreover, $\mathrm{PSL}_2(p)$ is generated by the coset of matrices

$$S = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } \quad T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

On choosing a coset representative $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ for each member we can define the group action on a point in H_p by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} (x + \sqrt{\delta}y) = \frac{a(x+\sqrt{\delta}y)+b}{c(x+\sqrt{\delta}y)+d} = x' + \sqrt{\delta}y'.$$

If $p = 4m+1$ then Tiu and Wallace have shown that $\mathrm{PSL}_2(p)$ fixes $\mathcal{C}_p$ and acts as a group of automorphism for $\mathcal{C}_p$. The following theorem shows that the result is also true for primes of the form $4m-1$.

Theorem 6.8 *$PSL_2(p)$ fixes $\mathcal{C}_p$ and acts transitively on the coordinate positions.*

Proof: Proof of the fact that $PSL_2(p)$ fixes $\mathcal{C}_p$ for $p = 4m-1$ is similar to the case $p = 4m+1$ (see[110]). To prove the next part, for given $x + \sqrt{\delta}\ y$ and $u + \sqrt{\delta}\ v$ in H_p we have to show that there exist $P \in \mathrm{PSL}_2(p)$ such that $P(x + \sqrt{\delta}\ y) = u + \sqrt{\delta}$ v. If

$P_1 = \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix}$ and $P_2 = \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix}$ then $P_1(x+\sqrt{\delta}y) = \sqrt{\delta}y$ and $P_2(\sqrt{\delta}v) = u+\sqrt{\delta}v$. Thus we need to find $Q \in \mathrm{PSL}_2(p)$ such that $Q(\sqrt{\delta}\ y) = \sqrt{\delta}$ v. Two cases arise:

Case 1: Both v and y are either quadratic residues or quadratic non residues mod p. Then $v = a^2y$ for some $a \in GF(p)$. Let $Q = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}$, then $Q(\sqrt{\delta}y) = v\sqrt{\delta}$.

Case 2: Either v is a q.r. and y is a q.n.r. or v is a q.n.r. and y is a q.r. mod p. In either case $v \cdot y \cdot \delta$ is a q.r. mod p and hence $v \cdot y \cdot \delta = a^2$ for some $a \in GF(p)$. Let $Q = \begin{bmatrix} 0 & a \\ a^{-1} & 0 \end{bmatrix}$ then $Q(\sqrt{\delta}y) = v \cdot \sqrt{\delta}$. ∎

Theorem 6.9 *$\mathcal{C}_p$ is $\mathbb{Z}_4$-linear.*

Proof: It follows from Theorem 2.3 and Remark 6.3. ∎

The *Covering Radius* $R(\mathcal{C})$ of a linear code $\mathcal{C}$ is the least integer R such that spheres of radius R around the codewords cover the whole space. It is known that $R(\mathcal{C})$ is the maximum weight of the coset leader. For $i = 1, 2, \ldots, n$ and for $\alpha \in I\!F_2$ let

$$C_\alpha^{(i)} = \{(c_1, c_2, \ldots, c_n) \in \mathcal{C} | c_i = \alpha\}$$

and let $N^{(i)} = \max_{\mathbf{x} \in I\!F_2^n}\{\sum_{\mathbf{x} \in I\!F_2^n} d(\mathbf{x}, C_\alpha^{(i)})\}$ with the convention that $d(\mathbf{x}, \Phi) = n$; where Φ is the empty set. The number $N^{(i)}$ is called the *Norm of $\mathcal{C}$ with respect to the i^{th} coordinate* and $N(\mathcal{C}) = \min_i N^{(i)}$ is called the *Norm* of the code $\mathcal{C}$. If for some $i, N^{(i)} \leq 2R+1$, then $\mathcal{C}$ is said to be *normal* and the coordinate i is called *acceptable*. The following theorem determines the covering radius of $\mathcal{C}_p$ and shows that $\mathcal{C}_p$ is normal.

Theorem 6.10 *Covering radius of $\mathcal{C}_p$ is $\frac{p(p-1)}{2}$. Moreover $\mathcal{C}_p$ is a normal code with every coordinate acceptable.*

Proof: Observe that $N(\mathcal{C}_p) \leq p(p-1)$. Since $\mathcal{C}_p$ has no coordinate identically zero,

$$R(\mathcal{C}_p) \leq \left\lfloor \frac{N(\mathcal{C}_p)}{2} \right\rfloor \leq \frac{p(p-1)}{2}. \tag{6.3}$$

Let $\mathbf{x} \in I\!F_2^{p(p-1)}$ such that its coordinates when divided in p blocks each of length $(p-1)$ have a 1 in the first $\frac{p-1}{2}$ coordinate positions of each block and zero at other positions. Then by Remark 6.2 $d(\mathbf{x}, \mathbf{c}) = \frac{p(p-1)}{2}$ for all $\mathbf{c} \in \mathcal{C}_p$. Thus using Equation (6.3) we get $R(\mathcal{C}_p) = \frac{p(p-1)}{2}$. Since $N(\mathcal{C}_p) \leq p(p-1) < 2R(\mathcal{C}_p) + 1, \mathcal{C}_p$ is normal. Moreover Since $\mathcal{C}_p$ is an even code, $N(\mathcal{C}_p) = 2R(\mathcal{C}_p) = p(p-1)$[45]. Hence its every coordinate is acceptable. ∎

In[66], Janwa has shown that the length n, the minimum distance d_H, the dimension k and the covering radius R of a linear code are related by $\sum_{i=1}^{k} \left\lceil \frac{d_H}{2^i} \right\rceil \leq n - R$. Applying this to the code $\mathcal{C}_p$ we get the following corollary.

Corollary 6.11 *The minimum distance d of an NQR code $\mathcal{C}_p$ satisfies the inequality*

$$\sum_{i=1}^{p} \left\lceil \frac{d}{2^i} \right\rceil \leq \frac{p(p-1)}{2}$$

The bound given by Corollary 6.11 although poor but is better than the bound given by Corollary 6.3.

Chapter 7

Conclusions

Anything that won't sell, I don't want to invent. Its sale is proof of utility, and utility is success. ... Thomas A. Edison (1847-1931)

In the present dissertation, we have studied Simplex Codes of type α and β, first order Reed Müller code, over $\mathbb{Z}_{2^s}$. The concept of 2-dimension has been used extensively to derive the fundamental properties of these codes. It seems to be an appropriate tool for studying linear codes over $\mathbb{Z}_{2^s}$. The concept of 'chain condition' has been extended in this sense. The method used can be easily extended to study linear codes over $\mathbb{Z}_{p^s}$. One will need to suitably extend the definition of ϕ_G. Determining the Automorphism group of these codes and giving a valuable decoding algorithms for these codes can be an interesting future task. In chapter 5, we have shown that various self-dual codes over $\mathbb{Z}_4$ satisfy the chain condition. This study can be further carried to higher lengths code over $\mathbb{Z}_{2^s}$.

The bound given in Equation (2.10) for $\mathbb{Z}_2$-linear codes seems to be true, in general, for any linear code over $\mathbb{Z}_{2^s}$. But we are neither able to prove it nor provide a counter example for it, even for the particular case $s = 2$.

Hensel uplift of NQR codes, studied in Chapter 6, needs further investigation.

Bibliography

[1] A. E. Ashikhmin. Generalized hamming weights for $\mathbb{Z}_4$-linear codes. In *Proc. of the 1994 IEEE Int. Symp. Inform. Theory*, page 306, 1994.

[2] A. E. Ashikhmin. On generalized hamming weights for galois ring linear codes. *Designs, Codes and Cryptography*, **14**:107–126, 1998.

[3] A. I. Barbero and J. G. Tena. Weight hierarchy of a product code. *IEEE Trans. Inform. Theory*, **41**(5):1475–1480, 1995.

[4] http://www.sirbacon.org/toc.html.

[5] L. A. Bassalygo. Supports of a code. *Springer Lecture Notes in Computer Science*, **948**:1–3, 1995.

[6] E. R. Berlekamp. *Algebraic Coding Theory*. McGraw-Hill, New York, 1968.

[7] I. F. Blake. Codes over certain rings. *Inform. Control*, **20**:396–404, 1972.

[8] I. F. Blake. Codes over integer residue rings. *Inform. Control*, **29**:295–300, 1975.

[9] A. Bonnecaze, E. M. Rains, and P. Solé. 3-colored 5-designs and $\mathbb{Z}_4$-codes.

[10] A. Bonneeaze and I. M. Duursma. Translates of linear codes over $\mathbb{Z}_4$. *IEEE Trans. Inform. Theory*, **43**(4):1218–1230, 1997.

[11] A. Bonnecaze, P. Solé, and A. R. Calderbank. Quaternary quadratic residue codes and unimodular lattices. *IEEE Trans. Inform. Theory*, **41**:366–377, 1995.

[12] A. Bonnecaze, P. Solè, C. Bachoc, and B. Mourrain. Type ii codes over $\mathbb{Z}_4$. *IEEE Trans. Inform. Theory*, **43**(3):969–976, 1997.

[13] S. Boztas, A. R. Hammons, and P. V. Kumar. 4-phase sequences with near-optitum correlation properties. *IEEE Trans. Inform. Theory*, **38**(3):1101–1113, 1992.

[14] A. R. Calderbank and G. Mcguire. Construction of a $(64, 2^{37}, 12)$ code via galois rings. *Designs, Codes and Cryptography*, **10**:157–165, 1997.

[15] A. R. Calderbank and N. J. A. Sloane. Modular and p-adic cyclic codes. *Designs, Codes and Cryptography*, **6**:21–35, 1995.

[16] A. R. Calderbank and N. J. A. Sloane. Double circulant codes over $\mathbb{Z}_4$ and even unimodular lattices. *J. Alg. Combin.*, **6**:119–131, 1997.

[17] A. R. Calderbank, W.-C. W. Li, and B. Poonen. A 2-adic approach to the analysis of cyclic codes. *IEEE Trans. Inform. Theory*, **43**(3):977–986, 1997.

[18] C. Carlet. On $\mathbb{Z}_4$-duality. *IEEE Trans. Inform. Theory*, **41**(5):1487–1494, 1995.

[19] C. Carlet. $\mathbb{Z}_{2^k}$-linear codes. *IEEE Trans. Info. Theory*, **44**(4):1543–1547, 1998.

[20] C. Carlet. One weight $\mathbb{Z}_4$-linear code. In *Lecture Notes in Computer Science*, 1998. (To Appear).

[21] C. Charnes. Hadamard matrices, self-dual codes over the integers modulo 4 and their gray images. In *Lecture Notes in Computer Science*, 1998. (To Appear).

[22] W. Chen and T. Klove. The weight hierarchies of q-ary codes of dimension 4. *IEEE Trans. Inform. Theory*, **42**(6):2265–2272, 1996.

[23] W. Chen and T. Klove. Weight hierarchies of linear codes satisfying the chain condition. *Designs, Codes and Cryptography*, **11**:47–66, 1998.

[24] W. Chen and T. Klove. Weight hierarchies of extremal non chain binary codes of dimension 4. *IEEE Trans. Inform. Theory*, **45**(1):276–281, 1999.

[25] J. C. Chiang and J. K. Wolf. On channels and codes for the lee metric. *Inform. Control*, **19**:159–173, 1971.

[26] J. H. Conway and N. J. A. Sloane. Self-dual codes over the integers modulo 4. *Jr. of Comb. Theory*, **Series A 62**:30–45, 1993.

[27] H. Chung. The 2nd generalized hamming weight of double-error-correcting binary bch codes and their dual. *Lecture Notes in Computer Science*, **539**:118–129, 1991.

[28] P. Delsarte and J. M. Goethals. Alternating bilinear forms over $gf(q)$. *J. Comb. Theory*, **19**:26–50, 1975.

[29] S. T. Dougherty, P. Gaborit, M. Harada, and P. Solé. Type ii codes over $\mathbb{F}_q + u\mathbb{F}_q$. *IEEE Trans. Inform. Theory*, **45**(1):32–45, 1999.

[30] S. B. Encheva and H. E. Jensen. Optimal binary linear codes and $\mathbb{Z}_4$-linearity. *IEEE Trans. Inform. Theory*, **42**(4):1216–1222, 1996.

[31] S. Encheva and T. Klove. Codes satisfying chain condition. *IEEE Trans. Inform. Theory*, **40**(1):175–180, 1994.

[32] S. Encheva. On binary linear codes which satisfy the two-way chain condition. *IEEE Trans. Inform. Theory*, **42**(3):1038–, 1996.

[33] J. Fields, P. Gaborit, J. S. Leon, and V. Pless. All self-dual codes of length 15 or less are known. *IEEE Trans. Inform. Theory*, **44**(1):311–322, 1998.

[34] J. Fields and P. Gaborit. On the non $\mathbb{Z}_4$-linearity of certain good binary codes. *IEEE Trans. Inform. Theory*, **45**(5):1674–1677, 1999.

[35] R. A. Fisher. The theory of confounding in factorial experiments in relation to the theory of groups. *Ann. Eugenics*, **11**:341–353, 1942.

[36] R. A. Fisher. A system of confounding for factors with more than two alternatives, giving completely orthogonal cubes and higher powers. *Ann. Eugenics*, **12**:2283–2290, 1945.

[37] G. D. Forney. Dimension/length profiles and trellis complexity of linear block codes. *IEEE Trans. Inform. Theory*, **40**(6):1741–1752, 1994.

[38] G. D. Forney, N. J. A. Sloane, and M. D. Trott. The nordstrom-robinson code is the binary image of the octacode. In *Coding and Quantization:DIMACS/IEEE Workshop, Amer. Math. Soc.*, pages 19–26, October 19-21, 1992.

[39] P. Gaborit. Mass formulas for self-dual codes over $\mathbb{Z}_4$ and $\mathbb{F}_q + u\mathbb{F}_q$ rings. *IEEE Trans. Inform. Theory*, **42**(4):1222–1227, 1996.

[40] M. S. Garg. *On Optimum Codes and their Covering Radii*. PhD thesis, IIT Kanpur, India, 1990.

[41] M. J. E. Golay. Notes on digital coding. *Proc. IEEE*, **37**:657, 1949.

[42] J. M. Goethals. Two dual families of nonlinear binary codes. *Electronics Letters*, **10**:471–472, 1974.

[43] J. M. Goethals. Nonlinear codes defined by quadratic forms over $gf(2)$. *Inform. Control*, **31**:43–74, 1976.

[44] S. W. Golomb and L. R. Welch. Algebraic coding and the lee metric. In *Error Correcting Codes, H.B. Mann Ed.* New York Wiley, 1968.

[45] R. L. Graham and N. J. A. Sloane. On the covering radius of codes. *IEEE Trans. Inform. Theory*, **31**(3):385–401, 1985.

[46] F. Gray.

March 17, 1953. Pulse Code Communication, US Patent 2632058.

[47] M. Greferath and U. Vellbinger. Efficient decoding of $\mathbb{Z}_{p^k}$-linear codes. *IEEE Trans. Inform. Theory*, **44**(3):1288–1291, 1998.

[48] M. Greferath and U. Vellbinger. On the extended error-correcting capabilities of the quaternary preparta codes. *IEEE Trans. Inform. Theory*, **44**(5):2018–2019, 1998.

[49] J. H. Griesmer. A bound for error-correcting codes. pages 532–542, 1960.

[50] T. A. Gulliver and M. Harada. Double circulant self-dual codes over $\mathbb{Z}_{2k}$. *IEEE Trans. Inform. Theory*, **44**(7), 1998.

[51] R. W. Hamming. Error detecting and error correcting codes. *The Bell System Tech. Journal*, **XXIX**(2):147–160, 1950.

[52] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Slonae, and P. Solé. On the apparent duality of the kerdock and preparata codes. *Lecture Notes in Computer Science*, **673**, 1993.

[53] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé. The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals, and related codes. *IEEE Trans. Inform. Theory*, **40**(2):301–319, 1994.

[54] M. Harada. New extremal type ii codes over $\mathbb{Z}_4$. *Designs, Codes and Cryptography*, **13**:271–284, 1998.

[55] P. Heijnen and R. Pellikaan. Generalized hamming weights of q-ary reed müller codes. *IEEE Trans. Inform. Theory*, **44**(1):181–196, 1998.

[56] G. A. Helfrich. Weight hierarchy of cyclic codes and their applications, 1991. MS Thesis, Deptt. of Electrial Engineering, Lehigh University.

[57] T. Helleseth, B. Hove, and K. Yang. Further results on generalized hamming weights for goethals and preparata codes over $\mathbb{Z}_4$. *IEEE Trans. Inform. Theory*, **45**(4):1255–1258, 1999.

[58] T. Helleseth and P. V. Kumar. The algebraic decoding of the $\mathbb{Z}_4$- linear goethals code. *IEEE Trans. Inform. Theory*, **41**(6):2040–2048, 1995.

[59] T. Helleseth, T. Klove, and ϕ. Ytrehus. Generalized hamming weights of linear codes. *IEEE Trans. Inform. Theory*, **38**(3):1133–1140, 1992.

[60] T. Helleseth, T. Klove, V. I. Levenshtein, and ϕ. Ytrehus. Bounds on the minimum support weights. *IEEE Trans. Inform. Theory*, **41**(2):432–439, 1995.

[61] T. Helleseth and T. Klove. The weight hierarchies of some product codes. *IEEE trans. Inform. Theory*, **42**(3):1029–1034, 1996.

[62] F. B. Hergert. On the delsarte-goethals codes and their formal duals. *Disc. Math.*, **83**:249–263, 1990.

[63] X.-D. Hou, J. T. Lahtonen, and S. Koponen. The reed-müller code $r(r, m)$ is not $\mathbb{Z}_4$-linear for $3 \leq r \leq m-2$. *IEEE Trans. Inform. Theory*, **44**(2):798–799, 1998.

[64] W. C. Huffman. Decomposition and extremal type ii codes over $\mathbb{Z}_4$. *IEEE Trans. Inform. Theory*, **44**(2):800–809, 1998.

[65] J. C. Interlando, R. P. Jr., and M. Elia. On the decoding of reed-solomon and bch codes over integer residue rings. *IEEE Trans. Inform. Theory*, **43**(3):1013–1020, 1997.

[66] H. Janwa. On the optimality and covering radius of some algebraic geometric codes. In *Workshop on Coding Theory, at Institute for Mathematics and Its Applications (IMA), University of Minnesota*, July 13-24, 1988.

[67] G. Kabatianski. Generalized hamming weight and a problem in cryptography. In *All-Union winter Schools on Information Theory and Applications, Mtsensk, Russia*, 1992.

[68] P. Kanwar and S. R. Lopez-Permouth. Cyclic codes over integers modulo p^m. *Finite Fields and their Applications*, **3**(4):334–352, 1997.

[69] T. Kasami, T. Tanaka, T. Fujiwara, and S. Lin. On the optimum bit orders with respect to the state complexity of trellis diagrams for binary linear codes. *IEEE Trans. Inform. Theory*, **39**:242–245, 1993.

[70] A. M. Kerdock. A class of low-rate nonlinear codes. *Inform. Control*, **20**:182–187, 1972.

[71] M. Klemm. Selbstduale codes über dem ring der ganzen zahlen modulo 4. *Arch. Math.*, **53**:201–207, 1989.

[72] T. Klove. Support weight distribution of linear codes. *Disc. Math.*, **106/107**:311–316, 1992.

[73] T. Klove. Minimum support weights of binary codes. *IEEE Trans. Inform. Theory*, **39**(2):648–654, 1993.

[74] P. V. Kumar, T. Helleseth, A. R. Calderbank, and A. R. Hammons. Large family of quaternary sequence with low correlation. *IEEE Trans. Inform. Theory*, **42**:579–592, 1996.

[75] C. Y. Lee. Some properties of nonbinary error-correcting codes. *IEEE Trans. Inform. Theory*, **4**:77–82, 1958.

[76] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and their Applications*. Cambridge Univ. Press, 1994.

[77] J. E. MacDonald. Design methods for maximum minimum-distance error-correcting codes. pages 43–57, 1960.

[78] B. R. Macdonald. *Finite Rings with Identity*. Marcel-Decker, New York, 1974.

[79] F. J. MacWillams and N. J. A. Sloane. *Theory of Error-Correcting Codes*. North Holland, Amsterdam, 1977.

[80] F. J. MacWilliams. Error correcting codes for multi-level transmission. pages 281–308, 1961.

[81] J. L. Massey and T. M. Mittelholzer. Convolutions codes over rings. In *Proceedings of the Fourth Joint Swedish-USSR Int. Workshop in Inform. Theory, Sweden*, 1989.

[82] E. E. Nemirovskiy. Codes on residue class rings with multi-frequency phase telegraphy. *Radiotechnika I electronika*, **9**:1745–1753, 1984.

[83] A. W. Nordstrom and J. P. Robinson. An optitum nonlinear code. *Inform. Control*, **11**:613–616, 1967.

[84] L. H. Ozarow and A. D. Wyner. Wire-tap channel ii. *AT & T Bell Labs Tech. J.*, **63**:2135–2157, 1984.

[85] O. Perrön. Bemerkungen über die verteilung der quadratischen reste. *Math. Zeit*, **56**:122–130, 1952.

[86] V. Pless, J. S. Leon, and J. Fields. All $\mathbb{Z}_4$ codes of type ii and length 16 are known. *Jr. Comb. Theory*, **Series A 78**:32–50, 1997.

[87] V. Pless, P. Solé, and Z. Qian. Cyclic self-dual $\mathbb{Z}_4$-codes. *Finite Fields and Their Applications*, **3**:48–69, 1997.

[88] V. Pless and Z. Qian. Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. *IEEE Trans. Inform. Theory*, **42**(5):1594–1600, 1996.

[89] F. P. Preparata. A class of optimum nonlinear double-error-correcting codes. *Inform. Control*, **13**:378–400, 1968.

[90] E. M. Rains. Bounds for self-dual codes over $\mathbb{Z}_4$. submitted to Fin. Fields Appl.

[91] E. M. Rains and N. J. A. Sloane. The shadow theory of modular and unimodular lattices. *J. Number Theory*, **73**:359–389, 1998.

[92] E. M. Rains and N. J. A. Sloane. *Self-Dual Codes : The Handbook of Coding Theory*. North-Holland, New York, 1998.

[93] E. M. Rains. Optimal self-dual codes over $\mathbb{Z}_4$. *Discrete Math.*, **203**:215–228, 1999.

[94] I. Reuven and Y. Be'ery. Generalized hamming weights of nonlinear codes and the relation to the $\mathbb{Z}_4$-linear representation. *IEEE Trans. Inform. Theory*, **45**(2):713–720, 1999.

[95] J. Rosenthal and E. V. York. On the generalized hamming weights of convolutional codes. *IEEE Trans. Inform. Theory*, **43**(1):331–335, 1997.

[96] R. M. Roth and P. H. Siegel. Lee-metric bch codes and their application to constrained and partial-response channels. *IEEE Trans. Inform. Theory*, **40**(4):1083–1096, 1994.

[97] C. Satyanarayana. Lee metric codes over integer residue rings. *IEEE Trans. Inform. Theory*, **25**(2):250–254, 1979.

[98] A. *Sălăgean*-Mandache. On the isometries between $\mathbb{Z}_{p^k}$ and $\mathbb{Z}_p^k$. *IEEE Trans. Inform. Theory*, **45**(6):2146–2148, 1999.

[99] A. G. Shanbhag, P. V. Kumar, and T. Helleseth. Improved binary codes and sequence families from $\mathbb{Z}_4$-linear codes. *IEEE Trans. Inform. Theory*, **42**(5):1582–1587, 1996.

[100] P. Shankar. On bch codes over arbitary integer rings. *IEEE Trans. Inform. Theory*, **25**(4):480–483, 1979.

[101] C. E. Shannon. A mathematical theory of communication. *Bell Sys. Tech. J.*, **27**:379–423 and 623–656, 1948.

[102] V. Sidorenko, I. Martin, and B. Honary. On the rectangularity of nonlinear block codes. *IEEE Trans. Inform. Theory*, **45**(2):720–725, 1999.

[103] N. J. A. Sloane. Algebraic coding theory: Recent developments related to the integers mod 4. In *Study of Algebraic Combinatorics (Proceedings Conference on Algebraic Combinatorics, Kyoto 1993)*, pages 38–52, 1995.

[104] P. Solè. A quaternary cyclic code, and a family of quadriphase sequence with low correlation properties. *Springer Lecture Notes in Computer Science*, **388**:193–201, 1989.

[105] G. Soloman and J. J. Stiffler. Algebraically punctured cyclic codes. *Inform. Control*, **8**:170–179, 1965.

[106] E. Spiegel. Codes over $\mathbb{Z}_m$. *Inform. Control*, **35**:48–51, 1977.

[107] E. Spiegel. Codes over $\mathbb{Z}_m$, revisited. *Inform. control*, **37**:100–104, 1978.

[108] F. W. Sun and H. Leib. Multiple-phase codes for detection without carrier phase reference. *IEEE Trans. Inform. Theory*, **44**(4):1477–1491, 1998.

[109] B. S. Rajan. *Transform Domain Study of Cyclic and Abelian Codes over Residue Class Integer Rings*. PhD thesis, Deptt. of Elec. Engg., IIT Kanpur, Kanpur, India, 1989.

[110] P. D. Tiu and D. Wallace. Norm quadratic residue codes. *IEEE Trans. Inform. Theory*, **40**(3):946–949, 1994.

[111] L. G. Tallini and U. Vaccaro. Efficient m-ary balanced codes. *Disc. Applied Math.*, **92**:17–56, 1999.

[112] V. V. Vazirani, H. Saran, and B. S. Rajan. An efficient algorithm for constructing minimal trellises for codes over finite abelian groups. *IEEE Trans. Inform. Theory*, **42**(6):1839–1854, 1996.

[113] Z. Wan. *Quaternary Codes*. World Scientific, Singapore, 1997.

[114] S. K. Wasan. On codes over $\mathbb{Z}_m$. *IEEE Trans. Inform. Theory*, **28**(1):117–120, 1982.

[115] V. K. Wei. Generalized hamming weights for linear codes. *IEEE Trans. Inform. Theory*, **37**(5):1412–1418, 1991.

[116] V. K. Wei and K. Yang. On the generalized hamming weights of product codes. *IEEE Trans. Inform. Theory*, **39**(5):1709–1713, 1991.

[117] K. Yang, T. Helleseth, P. V. Kumar, and A. G. Shangbhag. On the weight hierarchy of kerdock codes over $\mathbb{Z}_4$. *IEEE Trans. Inform. Theory*, **42**(5):1587–1593, 1996.

[118] K. Yang and T. Helleseth. Two new infinite families of 3-designs from kerdock codes over $\mathbb{Z}_4$. *Designs, Codes and Cryptography*, **15**:201–214, 1998.

[119] K. Yang and T. Helleseth. On the weight hierarchy of goethals codes over $\mathbb{Z}_4$. *IEEE Trans. Inform. Theory*, **44**(1):304–307, 1998.