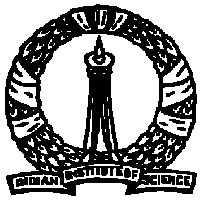
Elias Upper Bound for Euclidean Space Codes and Codes Close to the Singleton Bound

A Thesis submitted
for the degree of

Doctor of Philosophy

in the Faculty of Engineering
by

G Viswanath



Department of Electrical Communication Engineering
Indian Institute of Science
Bangalore 560 012 (India)

April 2004

Acknowledgments

I would like to express my gratitude to research supervisor Prof. B. Sundar Rajan for his guidance and support during the course of this work. I would also like to thank him for valuable inputs through several courses he taught in the area of error correcting codes and information theory.

I would like to thank Prof. U. R. Prasad, Prof. C. E. Veni Madhavan, Dr. Venkatachala and Prof. Mythili Ramaswamy for valuable inputs during the course work.

I would like to thank Prof. Anurag Kumar, Prof. A. Selvarajan and Prof. G. V. Anand for their support and encouragement. I was fortunate to have interacted with Prof. K. S. Jagadish and Prof. Raghunandan during the course of my stay in campus. Prof. T. V. Sreenivas, Dr. S. V. Narasimhan and Dr. G. Narayanan were always a source of inspiration. I also thank Mr. Srinivasamurthy and all other staff in the ECE office for their kind help and assistance.

A lot of good will showered by my friends made the stay in IISc. a pleasant experience. Alok, Shesha, Shobit and Santosh were always willing to do anything to help me sustain my work. Joby, Dev, Akash, Toby, Bhavtosh, Raghu, Sandeep, Imthias, Sesha and Santosh for taking care of me when I was in the hospital. Dr. Nagabushan, Dr. Alex Thomas and Prof. Balakrishnan ensured that I got all possible medical support. I am grateful them for their concern. I am also grateful to all the staff of Health Center, IISc. for their support.

Baburaj, GVSK and Joby for broadening the vistas of knowledge. The members of Green-Gang opened up another dimension to life. I am grateful to Anil, Subbu, Konda, Akash and Prof. Rohini Balakrishnan for the same.

I am grateful to Sunil Chandran and Manoj for the several problem solving sessions on “beautiful results” in mathematics. I also thank Bikas, Kiran, Nandakishore, Shashidhar, Sripathi and Zafar for all help.

I am fondly acknowledge Appa, Amma and Indu for all the affection they shower on me. I am grateful to my brother and sisters for being supportive and inspiring. I am also grateful to Chittappa, Chithi and Anand for all those kind words of encouragement.

I am grateful to the Indian Institute of Science for financial assistance.

Abstract

A typical communication system consists of a channel code to transmit signals reliably over a noisy channel. In general the channel code is a set of codewords which are used to carry information over the channel. This thesis deals with Elias upper bound on the normalized rate for Euclidean space codes and on codes which are close to the generalized Singleton bound, like Maximum-Distance Separable (MDS) codes, Almost-MDS codes, Near-MDS codes and certain generalizations of these.

The Elias bound for codes designed for Hamming distance, over an alphabet of size q is well known. Piret has obtained a similar Elias upper bound for codes over symmetric PSK signal sets with Euclidean distance under consideration instead of Hamming distance. A signal set is referred to as uniform if the distance distribution is identical from any point of the signal set. In this thesis we obtain the Elias upper bound for codes over uniform signal sets. This extension includes the PSK signal sets which Piret has considered as a subclass. This extended Elias bound is used to study signal sets over two, three and four dimensions which are matched to groups. We show that codes which are matched to dicyclic groups lead to tighter upper bounds than signal sets matched to comparable PSK signal sets, signals matched to binary tetrahedral, binary octahedral and binary icosahedral groups.

The maximum achievable minimum Hamming distance of a code over a finite alphabet set of given length and cardinality is given by the Singleton bound. The codes which meet the Singleton bound are called maximum distance separable codes (MDS). The problem of constructing of MDS codes over given length, cardinality and cardinality of the finite alphabet set is an unsolved problem. There are results which show the non existence of MDS codes for particular lengths of the code, the cardinality of the code and the alphabet size. Therefore we look at codes which are close to Singleton bound. Almost-MDS codes and Near-MDS codes are a family of such codes. We obtain systematic matrix characterization of these codes over finite fields. Further we charac-

terize these code over Z_m, R-modules and finite abelian groups. Based on the systematic matrix characterization of the codes over cyclic groups we obtain non-existence results for Almost-MDS codes and Near-MDS codes over cyclic groups.

The generalized Singleton bound of the code gives the upper bound on the generalized Hamming weights of the code. Generalized Hamming weights of the code are defined based on the minimum cardinality of the support of the subcodes of the code. MDS code achieves the generalized Singleton bound with equality. We obtain systematic matrix characterization of codes over finite fields with a given Hamming weight hierarchy. Further based on the systematic matrix characterization we characterize codes which are close to the generalized Singleton bound. We also characterize codes and their dual based on their distance from the generalized Singleton bound. We study the properties of codes whose duals are also at the same distance from the generalized Singleton bound. The systematic matrix characterization of codes which meet the generalized Greismer bound is also given.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

A typical communication system consists of a channel code to transmit signals reliably over a noisy channel. In general codewords are restricted to sequences of fixed length over finite alphabets. A code is by the following parameters: the length n of the code, number of information symbols k, the minimum distance between any two code words d and the cardinality of the alphabet, q, over which the code is constructed. Here the d denotes the minimum possible Hamming distance between two distinct codewords. The basic questions in coding theory include the following:

- given n, k, q find a (n, k) code C with $d_{min} \geq d$ that maximizes k
- given n, k, q find a (n, k) code C that maximizes the minimum distance d_{min}

Here the first condition looks at maximizing the rate of the code. Classical bounds on codes gives the lower and upper bound on the k for given d_{min}. The lower and upper bounds are obtained in terms of the normalized rate $\frac{k}{n}$ and the normalized distance $\frac{d}{n}$. The lower bound has been studied using different approaches. These include the classical Gilbert-Varshamov bound. The upper bounds on the rate of the code is given by Plotkin bound, Elias bound, linear programming bound etc. For an (n, k) code the maximum possible minimum distance between any two code words is given by the Singleton bound.
Hamming distance is the appropriate performance index for a given error correcting when the code is used on a binary symmetric channel. For other channels Hamming distance may not be an appropriate performance index. For instance, when used in Additive White

Gaussian noise $(AWGN)$ channel the minimum squared Euclidean distance $(MSED)$ of the resulting signal space code is the appropriate performance index [3] [71] [75]. Piret, [46], studied the Gilbert Varshamov lower bound and Elias upper bound for codes over PSK signal sets with squared Euclidean distance as the metric. In [56] the Pirets' lower bound for Euclidean space codes over PSK signal sets have been extended to codes over distance uniform signal sets. In this thesis we obtain an Elias type upper bound for codes over distance uniform signal sets.

The Singleton bound gives the maximum possible minimum Hamming distance of an (n, k) code. Maximum distance separable (MDS) codes are a class of codes which achieve the Singleton bound with equality. A general solution for construction of maximal length MDS codes over finite alphabet sets is still an open problem. There exists classes of codes having minimum distance close to the Singleton bound. These include the Almost MDS and Near MDS codes. In this thesis we study codes close to the Singleton bound over finite fields and obtain a systematic matrix characterizations.

The study of codes over groups is motivated by the observation in [37] [38] that when more that two signals are used for transmission, a group structure, instead of the finite field structure traditionally assumed, for the alphabet is matched to the relevant distance measure. The minimum squared Euclidean distance is the appropriate distance measure for signal sets matched to groups [37] [24]. The Hamming distance gives a simple lower bound on the minimum squared Euclidean distance for signal sets matched to groups. Hence it is interesting to study codes over signal sets which are matched to groups. It is well known that binary linear codes are matched to binary signaling over an Additive White Gaussian Noise (AWGN) channel in the sense that the squared Euclidean distance between two signal points in the signal space corresponding to two codewords is proportional to the Hamming distance between codewords. Similarly, linear codes over Z_m are matched to M-PSK modulation systems for an AWGN channel [40] [41]. The general problem of matching signal sets to linear codes over general algebraic structure of groups has been studied in [37] [38]. Also, group codes constitute an important ingredient for the construction of Geometrically Uniform codes [23]. This motivates the study of codes over groups both abelian and nonabelian. In [6] construction of group codes over abelian groups that mimics the construction of algebraic codes over finite fields is considered and it is shown that

the construction can be on the basis of a parity check matrix which provides the relevant information about the minimum Hamming distance of the code. The parity check symbols are seen as images of certain homomorphisms from G^k to G. The bound on the minimum Hamming distance of codes over groups is given by Singleton Bound. The codes over groups which meet the Singleton bound are the class of MDS group codes. MDS codes over groups have been studied in [76] [78]. Here again we study codes, $AMDS$ codes and $NMDS$ codes over groups, which are close to the Singleton bound and characterize them. Generalized Hamming weight hierarchy of linear codes over finite fields is discussed in [72]. The generalized Hamming weight hierarchy of a linear code is defined in terms of the minimum support of the subcodes of the code. The bound on the maximum possible minimum support of any subcode is given by the generalized Singleton bound. MDS code achieves the generalized Singleton bound with equality for all the subcodes. The codes which are close to the generalized Singleton bound are form an important class of codes. We obtain matrix characterization of these codes over finite fields in terms of the systematic generator matrix.

1.1 Preliminaries and Background

In this section we introduce basic set of concepts and symbols which we use in this thesis. Further in each chapter we will discuss results which are relevant to it. Consider an n dimensional space over a finite field F_q. Any subset of the all possible n tuples over F_q is a code. If the subset forms a linear subspace it is a linear code.

Definition 1.1 *The minimum Hamming distance of a n-length code C is defined as $d_{min} = min\{d(x,y) \mid \forall x, y \in C$ and $x \neq y\}$ where $d(x,y)$ denotes minimum Hamming distance between the codewords x and y*

A code C over a F_q is defined in terms of n, k and d_{min}. Codes can be defined over any finite sets. In thesis we study codes over finite fields, finite module over a commutative ring and finite abelian group. We also study codes over finite distance uniform signal sets.
The normalized rate of an $[n,\ k]$ code is defined as $\frac{k}{n}$. Similarly the normalized distance of $[n\ \ k\ \ d]$ code is defined as $\frac{d}{n}$. The normalized rate and normalized distance are important parameters of the code.

An $[n,\ k]$ linear code C over F_q is generated by k independent code words, i.e, the code is generated by k rank matrix over F_q. This is called the generator matrix of the code (this is a $(k \times n)$ matrix over F_q). Every generator matrix of a linear code can be written as a $[I_{k\times k}\ P_{k\times(n-k)}]$ matrix (upto column permutations). Throughout this thesis we refer to this matrix as the systematic generator matrix of the code with the understanding that it is the generator matrix of the equivalent code obtained by appropriate column permutations.
The dual of an $[n\ k]$ code C denoted as $C^{\perp}$ is the set of all $\{x \in F_q^n \mid \langle x, y\rangle = 0\ \forall\ y \in C\}$. The dual code, $C^{\perp}$, is an $[n\ \ (n-k)]$ code. The systematic generator matrix of the dual code is called as the systematic parity check matrix of the code. The systematic parity check matrix of the code is given by the matrix $[-P^T_{(n-k)\times k}\ \ I_{(n-k)\times(n-k)}]$.

1.1.1 Bounds on Codes

Consider a code over a finite alphabet set of cardinality q with length n and minimum Hamming distance d. An important question which comes up here is what is the maximum value of M for which such a code exists.

Definition 1.2 *[60]* $A(n,d) := max\{M \mid an(n,M,d)$*code exists*$\}$ *where* d *is the minimum Hamming distance of the code,* M *the cardinality of the code and* n *is the length of the code* C*. A code* C *such that* $\mid C \mid = A(n,d)$ *is called optimal.*

Obtaining lower and upper bounds on $A(n,d)$ is considered as an important problem in coding theory. In this section we collect results on the bounds on $A(n,d)$ based on Hamming distance. In the case of long length code (asymptotic case) the normalized distance is denoted as δ and

Definition 1.3 *[60]* $\alpha(\delta) := \lim_{n\to\infty} sup\{n^{-1} log_q A(n,\delta)\}$

The asymptotic lower and upper bounds on $\alpha(\delta)$ is given in terms of the generalized entropy function. The generalized entropy function is defined as follows:

$$H_q(x) \ = \ -x\log_q\left[\frac{x}{q-1}\right] - (1-x)\log_q(1-x), \quad if \quad 0 \ \leq \ x \ \leq \ \left[\frac{q-1}{q}\right]. \quad (1.1)$$

The asymptotic Gilbert-Varshamov bound (a lower bound) is given by

Theorem 1.1 *[39] [60] If* $0 \leq \delta \leq \frac{q-1}{q}$ *then* $\alpha(\delta) \geq 1 - H_q(\delta)$

The upper bounds on the rate of the code for a given distance include the Singleton bound, Hamming bound, Plotkin bound, Greismer bound, Elias bound, and the linear programming bound. Among these the linear programing bound gives the tightest upper bound on the rate of the code for any given distance. The Elias bound is tighter than the Singleton bound, Hamming bound, Plotkin bound and the Greismer bound. Moreover for small distances the Elias bound and the linear programing bound are comparable.
The Singleton bound is given by the following theorem

Theorem 1.2 *For q,n,$d \in N$, $q \geq 2$ we have $A(n,d) \leq q^{n-d+1}$*

For an $[n,\ k]$ linear code C we have $d \leq (n-k+1)$. A code meeting this bound is called the maximum distance separable code. The Greismer bound is defined for linear codes. The following theorem states the Greismer bound.

Theorem 1.3 *For an $[n,\ k,\ d]$ code over F_q we have $n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil$*

The Elias bound for the finite case and the asymptotic case are given by the following results.

Theorem 1.4 *Let q,n, d, $r \in N$, $q \geq 2$, $\theta = 1 - q^{-1}$ and assume that $r \leq \theta n$ and $r^2 - 2\theta nr + \theta nd > 0$. Then*

$$A(n,d) \leq \frac{\theta nd}{r^2 - 2\theta nr + \theta nd} \frac{q^n}{V_q(n,r)}.$$

Theorem 1.5 *We have*

$$\begin{aligned} &\alpha(\delta) \leq 1 - H_q(\theta - \sqrt{\theta(\theta-\delta)}) && \text{if } 0 \leq \delta \leq theta, \\ &\alpha(\delta) = 0, && \text{if} \theta \leq \delta < 1. \end{aligned} \tag{1.2}$$

1.1.2 Generalized Hamming Weight Hierarchy

The minimum distance of the of the code C over F_q is defined as $d(C) \stackrel{def}{=} \min_{\substack{a,b \in C \\ a \neq b}} \{w(a-b)\}$, where $w(a)$ denotes the number of non-zero locations of a. If C is a linear code then $d(C) \stackrel{def}{=} \min_{\substack{a \in C \\ a \neq b}} \{w(a)\}$. Next possible generalization is to consider the distance between triples of codewords [61]. This is defined as

$$d_2(C) \stackrel{def}{=} \min_{\substack{a,b,c \in C \\ a \neq b \neq c}} \{w((a-c) \vee (b-c))\}. \tag{1.3}$$

Here $\vee$ denotes the logical OR operation. For a linear code this reduces to

$$d_2(C) \stackrel{def}{=} \min_{\substack{a,b \in C \\ a \neq b}} \{w(a \vee b)\}. \tag{1.4}$$

Further generalization to the distance between i codewords leads to the generalized Hamming weight hierarchy of the code.

Definition 1.4 *Let C be an $[\ n\ k\ ]$ linear code. Let $\chi(C)$ be the support of C, namely, $\chi(C) = \{i \mid x_i \neq 0 for some (x_1, x_2, \ldots, x_n) \in C\}$. The r-th generalized Hamming weight of C is then defined as $d_r(C) = min\{\mid \chi(D) \mid :\ D is an r-dimensional subcode of C\}$.*

The Hamming weight hierarchy of C is then the set of generalized Hamming weights $\{d_r(C) \mid 1 \leq r \leq k\}$. There are several equivalent definitions of generalized Hamming weight. They include:

- $d_r(C)$ of an $[\ n\ k\ ]$ code C is the minimum size of union of supports of r linearly independent codewords in C.
- [28] Consider $[\ n\ k\ ]$ code C. Let G be a generator matrix of the code. For any $\underline{x} \in GF(q)^k$ the multiplicity of $\underline{x}$ will denote the number of of occurrences of $\underline{x}$ as column of G. Then the support of the code, $\chi(C) = n - m(\underline{0})$. Let GF_{kl} denote the set of l dimensional subspaces of the k dimensional space $GF(q)^k$. Then $d_r(C)$ is $n - \max\{m(U) \mid U \in GF_{k,k-r}(q)\}$

We also collect the following known results on Hamming weight hierarchy for codes over finite fields. The sequence of Hamming weight hierarchy is strictly increasing, i.e.,

$$d_1(C) < d_2(C) < \ldots < d_k(C) = n \tag{1.5}$$

The following result [72] which relates the Hamming weight hierarchy of a code to that of its dual will be useful. If $C^{\perp}$ denotes the dual of the code C, then

$$\{d_r(C) \mid r = 1, 2, ..., k\} \bigcup \{n + 1 - d_r(C^{\perp}) \mid r = 1, 2.., n - k\} = \{1, 2, ..., n\}.$$

The generalized Singleton bound of $[\ n\ k\ ]$ code C states that $d_r(C) \leq (n - k + i)$.

Definition 1.5 MDS Codes: *MDS codes are characterized in terms Hamming weight hierarchy as codes with the property that $d_i(C)$ is $(n - k + i)$ for $i = 1, 2, 3, 4, \ldots, k$.*

Definition 1.6 Almost MDS Codes: *Almost MDS codes are a class of $[\, n\, k\,]$ codes such that $d_1(C) = (n-k)$ and $d_i(C) \leq (n-k+i)$ for all $1 < i \leq k$.*

Definition 1.7 Near-MDS Codes: *Near MDS ($NMDS$) codes are a class of $[\, n\, k\,]$ codes with the following generalized Hamming weight hierarchy $d_1(C) = (n-k)$ and $d_i(C) = (n-k+i)$ for $i = 2, 3, 4, \ldots, k$.*

Definition 1.8 *An equivalent definition of $NMDS$ code is as follows: An $[\, n\, k\,]$ code is $NMDS$ if and only if the $d_1(C) = n-k$ and $d_1(C^{\perp}) = k$.*

Proposition 1.5.1 *An $[\, n\, k\,]$ code is a $NMDS$ if and only if $d_1 + d_1^{\perp} = n$, were d_1 is the minimum Hamming distance of the code and $d_1^{\perp}$ is the minimum Hamming distance of the dual code.*

The above result is proved in [15]. If an $[\, n\, k\,]$ is $NMDS$ we know that $d_1 = (n-k)$. The above proposition implies that the $d_1^{\perp} = k$. That is code as well as it dual are Almost-MDS codes. NMDS codes can be characterized in terms of their generator matrices and parity check matrices as follows [15]:
A linear $[n, k]$ code is NMDS iff a parity check matrix **H** of it satisfies the following conditions:

- every $n-k-1$ columns of **H** are linear independent
- there exists a set of $n-k$ linearly dependent columns in **H**
- every $n-k+1$ columns of **H** are of rank $n-k$

A linear $[n, k]$ code is NMDS iff a generator matrix **G** of it satisfies the following conditions:

- every $k-1$ columns of **G** are linear independent
- there exists a set of k linearly dependent columns in **G**
- every $k+1$ columns of **G** are of rank k

N^2MDS **Codes:** N^2MDS codes are a class of $[\,n\,k\,]$ codes where $d_1(C) = (n-k-1)$, $d_2(C) = (n-k+1)$ and $d_i(C) = (n-k+i)$ for $i = 3, 4, \ldots, k$. $A^\mu MDS$ **Codes:** $A^\mu MDS$ codes are a class of $[\,n\,k\,]$ codes where $d_1(C) = (n-k+1-\mu)$ and $d_i(C) \leq (n-k+i)$ for $i = 2, 3, \ldots, k$.

1.2 Contribution in this Thesis

A typical communication system consists of a channel code to transmit signals reliably over a noisy channel. In general the channel code is a set of codewords which are used to carry information over the channel. This thesis deals with Elias upper bound on the normalized rate for Euclidean space codes and on codes which are close to the generalized Singleton bound, like Maximum-Distance Separable (MDS) codes, Almost-MDS codes, Near-MDS codes and certain generalizations of these. The results presented in the second and third chapters are not directly related to the results presented in the subsequent chapters.

The Elias bound for codes designed for Hamming distance, over an alphabet of size q is well known. The Hamming distance is the appropriate performance index for codes over binary symmetric channel. For other channels Hamming distance may not be an appropriate performance index. For instance, when used in Additive White Gaussian noise $(AWGN)$ channel the minimum squared Euclidean distance $(MSED)$ of the resulting signal space code is the appropriate performance index[3; 71; 75]. Piret has obtained a similar Elias upper bound for codes over symmetric PSK signal sets with Euclidean distance under consideration instead of Hamming distance. A signal set is referred to as uniform if the distance distribution is identical from any point of the signal set. In Chapter 2 we obtain the Elias upper bound for codes over uniform signal sets called by us as Extended Elias Upper Bound ($EEUB$). Moreover this extension includes the PSK signal sets which Piret has considered as a subclass. The Elias bound for all values of q is shown to be obtainable by specializing the extended Elias bound obtained here to the class of simplex signal sets.The extended Elias upper bound depends on the choice of a probability distribution. In Chapter 2 we obtain the distribution that achieves the best bounds for codes over Simplex signal sets and biorthogonal signal sets. We also verify Pirets' conjecture for codes over PSK signal sets with cardinality five. (The results of Chapter 2 has been published in [58]

and [57].)

In Chapter 3, [68], we use the $EEUB$ to study signal sets over two, three and four dimensions which form distance uniform signal sets. We obtain a probability distribution that achieves the tightest $EEUB$ for codes over several signal sets in multidimensions and compare the bounds based on the normalized rate per two dimensions. A method to obtain a probability distribution that achieves the tightest bound is discussed. We also show that all distance uniform signal sets are equal energy signal sets. The codes which are matched to dicyclic groups is shown to have tighter upper bounds than signal sets matched to comparable PSK signal sets, signals matched to binary tetrahedral, binary octahedral and binary icosahedral groups. Further the upper bound for codes over finite unitary groups, Slepian signal set in six dimensions and Slepian signal set in six dimensions is also discussed. (A part of these results in Chapter 3 is available in [68].)

The maximum achievable minimum Hamming distance of a code over a finite alphabet set of given length and cardinality is given by the Singleton bound. The codes which meet the Singleton bound are called maximum distance separable codes (MDS). The problem of construction of MDS codes of given length, cardinality and cardinality of the finite alphabet set is an unsolved problem. There are results which show the non existence of MDS codes for particular lengths of the code, the cardinality of the code and the alphabet size. In Chapter 4 we study codes whose minimum Hamming distance is close to the Singleton bound. Almost-MDS codes and Near-MDS codes are a family of such codes. We obtain systematic matrix characterization of these codes over finite fields. The systematic matrix characterization of $NMDS$ codes and $AMDS$ codes is useful in erasure channels. Using the systematic matrix characterization that for an $[n,\ k]$ $NMDS$ code given any $(k+1)$ locations of the n length codeword we can obtain the transmitted message. (The results of Chapter 4 appear in [65] and [66].)

In Chapter 5 we characterize the class of $AMDS$ and $NMDS$ codes over finite abelian groups and finite R modules. The class of group linear codes over finite abelian groups are in general described in terms of the defining homomorphism. We report conditions on the defining homomorphism to characterize $AMDS$ and $NMDS$ codes. Specializing to cyclic groups we obtain characteristics of the defining homomorphisms for $AMDS$ codes and $NMDS$ codes. The defining homomorphisms for $AMDS$ and $NMDS$ codes over

cyclic groups lead to codes over Z_m. Based on the systematic matrix characterization of these codes over cyclic groups we obtain non-existence results for $AMDS$ codes and $NMDS$ codes over cyclic groups. (A part of these results appear in [69].)

The generalized Singleton bound of the code gives the upper bound on the generalized Hamming weights of the code. Generalized Hamming weights of the code are defined based on the minimum cardinality of the support of the subcodes of the code. MDS code achieves the generalized Singleton bound with equality. In Chapter 6 we obtain systematic generator/check matrix characterization of codes over finite fields with a given Hamming weight hierarchy. Further based on the systematic matrix characterization we characterize classes of codes which are close to the generalized Singleton bound. These include $NMDS$, N^2MDS, $AMDS$, $A^\mu MDS$ and $N^\mu MDS$ codes. The MDS-rank of C is the smallest integer η such that $d_{\eta+1} = n - k + \eta + 1$ and the defect vector of C with MDS-rank η is defined as the ordered set $\{\mu_1(C), \mu_2(C), \mu_3(C), \ldots, \mu_\eta(C), \mu_{\eta+1}(C)\}$, where $\mu_i(C) = n-k+i-d_i(C)$. We call C a dually defective code if the defect vector of its dual is the same as that of C. The systematic matrix characterization of dually defective codes is also obtained. Codes meeting the generalized Greismer bound are characterized in terms of their generator matrices. The HWH of dually defective codes meeting the generalized Greismer bound are also reported. We also characterize codes and their dual based on the defect vector. A code is dually defective if the defect vector is same for the code as well as its dual. (Results of Chapter 6 has been partly reported in [67] and [70].)

In Chapter 7 we conclude the thesis with a summary of results and a listing of several directions for further work.

Chapter 2

Asymptotic Elias Bound for Euclidean Space Codes over Distance-Uniform Signal Sets

[1]

2.1 Introduction

Hamming distance of a binary code is the appropriate performance index when the code is used on a binary symmetric channel. For other channels Hamming distance may not be an appropriate performance index. For instance, when used in Additive White Gaussian noise $(AWGN)$ channel the minimum squared Euclidean distance $(MSED)$ of the resulting signal space code is the appropriate performance index[3; 71; 75]. For codes designed for the Hamming distance, Elias bound gives an asymptotic upper bound on the normalized rate of the code for a specified normalized Hamming distance. To be precise, let C be a length n code over a q-ary alphabet with minimum Hamming distance $d_H(C)$. The asymptotic Elias bound, [60; 39; 45], is given by

$$R(\delta_H) \leq 1 - H_q(\theta - \sqrt{\theta(\theta - \delta_H)}), \;\; if \;\; 0 \leq \delta < \theta;$$
$$R(\delta_H) = 0 \;\; if \;\; \theta \leq \delta < 1. \tag{2.1}$$

[1] The results of this chapter are available also in [57] and [58].

where $\theta = (q-1)/q$, $R(\delta_H) = \lim_{n\to\infty} \frac{1}{n}\log_q \mid C \mid$ is the normalized rate, $\delta_H = \lim_{n\to\infty} \frac{1}{n} d_H(C)$ is the normalized Hamming distance and $H_q(x)$ is the generalized entropy function given by

$$H_q(x) = -x\log_q\left[\frac{x}{q-1}\right] - (1-x)\log_q(1-x), \quad if \quad 0 \leq x \leq \left[\frac{q-1}{q}\right]. \quad (2.2)$$

Piret [46] has extended this bound for codes over symmetric PSK signal sets for Euclidean distance and Ericsson [20] for codes over any signal set that forms a group for the general distance function. These bounds and their tightness depend on the choice of a probability distribution. In this chapter we point out that these bounds hold for the wider class of signal sets, namely the distance-uniform signal sets. The existence of distance-uniform signal sets that are not matched to any group was shown in [53]. We also show that the tightest bound (optimum distribution) is obtainable for simplex, Hamming spaces and biorthogonal signal sets. Also, we verify the conjecture of Piret regarding the optimum distribution for codes over symmetric 5-PSK signal set.

A signal set is said to be distance-uniform if the Euclidean distance distribution of all the points in the signal set from a particular point in the signal set is same from any point, *i.e*, if the signal set is $S = \{s_0, s_1, \ldots, s_{M-1}\}$ and $D_i = \{d_{ij}, j = 0, 1, \ldots, M-1\}$ is the Euclidean distance distribution from the signal point s_i, then D_i is the same for all $i = 0, 1, ..., M-1$. Examples of uniform signal sets are all binary signal sets, symmetric PSK Signal sets, orthogonal signal sets, simplex signal sets [3], [71], [75] and hypercubes in any dimension. The class of signal sets matched to groups [38], [37] form an important class of distance-uniform signal sets. A signal set S is said to be matched to a group G, if there exists a mapping μ from G onto S such that for all g and g' in G,

$$d_E(\mu(g), \mu(g')) = d_E(\mu(g^{-1}g'), \mu(e)) \quad (2.3)$$

where $d_E(x, y)$ denotes the squared Euclidean distance between $x, y \in S$ and e is the identity element of G. Signal sets matched to groups constitute an important ingredient in the construction of geometrically uniform codes [23] which include important classes of codes as special cases. Moreover, it has been shown that signal sets matched to non-commutative groups have the capacity of exceeding the PSK limit [8], whereas the capacity of signal sets matched to commutative groups are upper-bounded by the PSK limit [38], [37].

In this chapter we discuss the asymptotic upper bound on the normalized rate of Euclidean space codes ([38], [23]) over distance-uniform signal sets, for given normalized squared Euclidean distance. However, the arguments are valid for any distance function. We show that

- The Piret's and Ericsson's bound are valid for codes over any uniform-signal set.
- The distribution that gives the tightest bound (optimum distribution) for codes over simplex signal sets, Hamming spaces and biorthogonal signal sets are easily obtained.
- The bound for codes over simplex signal sets with optimum distribution is essentially the classical Elias bound. We also verify Piret's conjecture regarding the optimum distribution for codes over 5-PSK signal sets.

The content of this chapter is organized as follows: The validity of Piret's and Ericsson's bound for codes over the wider class of distance-uniform signal sets is given in Section(2.2). Also, the optimum distribution for codes over simplex, Hamming spaces and biorthogonal signal sets are obtained. The relation between classical asymptotic Elias bound and the extended bound is established by specializing to the codes over simplex signal sets. Further we verify Piret's conjecture on the optimum distribution for codes over 5-PSK signal sets. Section(2.3) contains directions concluding remarks.

2.2 Extended Elias Upper Bound ($EEUB$)

Following the arguments in the spirit of Elias bound [60], Piret, [46], has obtained an asymptotic upper bound in the parametric form on the rate of Euclidean space codes over symmetric PSK signal sets from which the Elias bound for $q = 2$ is obtainable and not for $q \geq 4$. Ericsson [20] has shown that this bound is valid for codes over any signal set that forms a group and for any general distance function. We point out in the following that the validity of this bound extends to codes over the wider class of distance-uniform signal sets. theorem(2.1) gives the extended upper bound, the proof of which uses similar arguments as that of Piret [46].

Theorem 2.1 *Let A be a distance-uniform signal set with M signal points $\{s_0, s_1, \ldots, s_{M-1}\}$ and S be a $M \times M$ matrix with $(i,j)^{th}$ entry s_{ij} equal to $d^2_{i,j}$, the squared Euclidean distance between a_i and a_j. For C, a length n code over A, let*

$$\delta(C) = \frac{1}{n} d^2(C), \quad R(C) = \frac{1}{n} \ln \mid C \mid \quad and$$
$$R(M, \delta) = \lim_{n \to \infty} sup_{\substack{|C| \geq n \\ \delta(C) \geq \delta}} R(C) \tag{2.4}$$

$d^2(C)$ is the minimum squared Euclidean distance $(MSED)$ of the code. The asymptotic upper bound $R_U(M, \delta)$ on $R(C)$ is given in terms of a probability distribution $\underline{\beta} = (\beta_0, \beta_1, \cdots, \beta_{M-1})$, by

$$R_U(M, \delta) = \ln(M) - H(\underline{\beta}) \ \ and \ \ \delta = \underline{\beta} S \underline{\beta}^T \tag{2.5}$$

where $H(\underline{\beta}) = -\Sigma_{i=0}^{M-1} \beta_i \, ln(\beta_i)$

Proof: The proof is essentially same as that of Piret, [46]. We give below the minor adjustments that are needed in the initial part of Piret's proof to make it valid for codes over distance-uniform signal sets:

Let $\{s_0, s_1, ..., s_{M-1}\}$ be the signal set S, and let the ordered vector $d = (d(0), d(1), ..., d(M-1))$ denote the Euclidean distance profile of S from s_0. Let Φ_r, $r = 0, 1, ..., M-1$, be a permutation on S such that $\Phi_r(s_r) = s_0$ and $\Phi_r(s_u) = s_v$, $u, v = 1, 2, ..., M-1$, where the squared Euclidean distance between s_r and s_u is $d^2(v)$. Such a permutation exists since S is distance-uniform. For any $\underline{x} = (x_1, x_2, ..., x_n)$ and $\underline{y} = (y_1, ..., y_n) \in S^n$, define $\Phi_{\underline{y}}(\underline{x}) = (\Phi_{y_1}(x_1), ..., \Phi_{y_n}(x_n))$ and call $b(\underline{x}) = (b_0(\underline{x}), b_1(\underline{x}), ..., b_{M-1}(\underline{x}))$, where $b_r(\underline{x})$ denotes the number of coordinates in $\underline{x}$ that are equal to s_r, as in [46], the composition of $\underline{x}$. For an arbitrary $\underline{u} \in S^n$ and a specified composition $\underline{b} = (b_0, b_1, ..., b_{M-1})$ denote by $B - \underline{b}(\underline{u})$ the set of all $\underline{x} \in S^n$ for which composition of $\Phi_{\underline{u}}(\underline{x}) = \underline{b}$.

These points replace the arguments used in [46] for PSK with cyclic group structure. Also, lemmas (4.1) and (4.2) in [46], which are specifically for PSK signal sets can be replaced by the following two lemmas to make the proof valid for codes over any distance-uniform signal set. □

Lemma 2.1.1 *$\beta_i^t = \beta_i \ \forall i = 0, 1, 2, \cdots, M-1, \quad t = 1, 2, \cdots, n$, where β_i^t is the normalized number of occurrences of the i-th symbol in the t-th co-ordinate as n tends to ∞.*

Proof: The normalized number of occurrences of i - th symbol from among M possible symbols is

$$b_i = \frac{N_i}{\sum_{j=0}^{M-1} N_j} \tag{2.6}$$

where N_i indicates the number of times the i-th symbol occurs. The normalized number of occurrences of the i-th symbol in the t-th co-ordinate b_i^t is obtained as

$$b_i^t = \frac{\left((\sum_{j=0}^{M-1} N_j - 1)!\right) / \left(\prod_{j=0, j\neq i}^{M-1} N_j!\right)}{\left(\sum_{j=0}^{M-1} N_j\right)! / \left(\prod_{k=0, k\neq i}^{M-1} N_k!\right)} \tag{2.7}$$

The above equation can be simplified to obtain the following result

$$b_i^t = \frac{N_i}{\sum_{j=0}^{Q-1} N_j} = b_i \tag{2.8}$$

Therefore the number of occurrences of any symbol at any co-ordinate is same. As $n \to \infty$, we have b_r tends to β_r and b_r^t tends to β_r^t. Hence we have $\beta_r^t = \beta_r$. □

Lemma 2.1.2 *For $n \to \infty$ the Q-tuples β^j satisfy*

$$\sum_{t=1}^{n} \beta^{(t)} S \beta^{(t)T} = n(\underline{\beta} S \underline{\beta^T}) \tag{2.9}$$

Proof: Follows from lemma(2.1.1). □

In the following three theorems we obtain the optimum distribution that gives the tightest bound for simplex, Hamming spaces and biorthogonal signal sets respectively.

Theorem 2.2 (Simplex signal sets)*: The distribution $\underline{\beta} = (\beta_0, \beta_1, \beta_2, \cdots, \beta_{M-1})$ that gives the best bound for codes over M-ary simplex signal set is given by*

$$\beta_r = \frac{1}{M}\left[1 - \sqrt{1 - M\frac{\delta}{K(M-1)}}\right],\ r = 1, \ldots, M-1 \tag{2.10}$$

where K is the squared Euclidean distance between any two signal points. Moreover for all values of q the asymptotic Elias bound given in equation(2.1), can be obtained from this bound.

Proof: For simplex signal sets, the squared Euclidean distance between any two signal points is the same. Let K denote this squared Euclidean distance, *i.e.*,

$$\begin{aligned} d^2(i,j) &= 0 \;\; if \;\; i=j \\ &= K \; (a \;\; constant), \;\; if \;\; i \neq j, \\ & \quad i,j = 0,1,2,\cdots,M-1 \end{aligned} \tag{2.11}$$

then

$$S = \begin{bmatrix} 0 & K & K & \dots & K & K \\ K & 0 & K & \dots & K & K \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ K & K & K & \dots & 0 & K \\ K & K & K & \dots & K & 0 \end{bmatrix} \tag{2.12}$$

Let $\underline{\beta} = (\beta_0, \beta_1, \dots, \beta_{M-1})$ be any probability distribution. We find the best distribution by using Lagrange multipliers. Let

$$\begin{aligned} \Phi(\underline{\beta}, \lambda) &= H(\underline{\beta}) - \lambda \left[\delta - \underline{\beta} S \underline{\beta}^T\right] \\ &= H(\underline{\beta}) - \lambda \left[\delta - K \sum_{i=0}^{M-1} \sum_{j=0, j\neq i}^{M-1} \beta_i \beta_j\right] \end{aligned} \tag{2.13}$$

Here note that $H(\underline{\beta})$ is concave function. Also note that we can show that the quadratic form $\underline{\beta} S \underline{\beta}^T$ is also concave. Therefore the extremal point of the Lagrangian gives the optimal distribution, [4]. Using $\sum_{i=0}^{M-1} \beta_i = 1$ in the inner summation, the above becomes

$$\Phi(\underline{\beta}, \lambda) = H(\underline{\beta}) - \lambda \left[\delta - K \left\{\sum_{i=0}^{M-1} \beta_i (1-\beta_i)\right\}\right] \tag{2.14}$$

Now for $r = 1, 2, \dots, M-1$, we have

$$\begin{aligned} \frac{\partial \Phi(\underline{\beta}, \lambda)}{\partial \beta_r} &= 1 - \log(\beta_r) - 1 \\ &\quad + \log(\beta_0) + K\lambda \left[1 - 2\beta_r - 1 + 2\beta_0\right] \\ &= \log \beta_0 - \log \beta_r + 2K\lambda(\beta_0 - \beta_r). \end{aligned} \tag{2.15}$$

Now the solution of the equation

$$\frac{\partial \Phi(\underline{\beta}, \lambda)}{\partial \beta_r} = 0 \tag{2.16}$$

for β_r will be the same for all $r = 1, 2, \ldots, M-1$, since the form of the equation(2.15) is same for all $r = 1, 2, \ldots, M-1$. Let p be the solution of equation(2.16), *i.e.*, $\beta_r = p$, for all $r = 1, 2, \ldots, M-1$. Now substituting $\beta_r = p$ in equation(2.14) and taking partial derivative w.r.t λ we get

$$\begin{aligned} \delta &= K\left[2\beta_0(1-\beta_0) + \sum_{i=1}^{M-1}\sum_{\substack{j=1 \\ j\neq i}}^{M-1} p^2\right] \\ &= 2K\left[\{1-(M-1)p\}(M-1)p\right] + \\ &\quad + K(M-1)(M-2)p^2 \end{aligned} \tag{2.17}$$

which is the same as the quadratic equation

$$KM(M-1)p^2 - 2K(M-1)p + \delta = 0 \tag{2.18}$$

The solutions of the quadratic equation after simplification are

$$\frac{1}{M}\left[1 \overset{+}{-} \sqrt{1-\frac{\delta}{K\theta}}\right] \tag{2.19}$$

where $\theta = \frac{(M-1)}{M}$. It can be checked that, $H(\underline{\beta})$ is minimum for

$$\begin{aligned} \underline{\beta} = \{&1-\left[\theta - \sqrt{\theta^2 - \frac{\delta\theta}{K}}\right], \frac{1}{M}\left[1-\sqrt{1-\frac{\delta}{K\theta}}\right], \\ &\ldots, \frac{1}{M}\left[1-\sqrt{1-\frac{\delta}{K\theta}}\right]\} \end{aligned} \tag{2.20}$$

For the above distribution

$$\ln M - H(\underline{\beta}) = \ln M + \beta_0 \ln \beta_0 + (M-1)\beta_r \ln \beta_r \tag{2.21}$$

Changing the base of the logarithm to M, the above expression becomes,

$$1 - H_M\left(\theta - \sqrt{\theta^2 - \frac{\theta\delta}{K}}\right) \tag{2.22}$$

Substituting $\delta_H = \delta/K$ in equation(2.22) we get

$$1 - H_M\left(\theta - \sqrt{\theta(\theta-\delta_H)}\right) \tag{2.23}$$

which is the same as the classical asymptotic Elias bound. It remains to show that the range for δ_H on the Elias bound is $0 \leq \delta_H < (M-1)/M$. With the substitution $\delta_H = \delta/K$, the range for δ becomes $0 \leq \delta < K\theta$. Choosing $K = 2/\theta$ and hence the range for δ is $0 \leq \delta < 2$ consistent with Theorem 2.1.

The substitution given by $K = 2M/M - 1$ and $\delta = \delta/K$, can be combined to obtain the relation between normalized squared Euclidean distance in the extended bound and the normalized Hamming distance in Elias bound as

$$\delta \left[\frac{(M-1)}{2M} \right] = \delta_H \tag{2.24}$$

The term $\frac{M-1}{2M}$ is the factor by which the plot of Elias bound can be obtained from the plot of the bound of Theorem 2.2. □

Example 2.1 *Figure(2.1) shows binary, ternary and quaternary simplex signal sets on a unit radius sphere. Figure(2.2) shows the classical $Elias$ bound (with natural logarithm) for simplex signal set of size $2, 3$ and 4 and the corresponding bounds for Euclidean distance.*

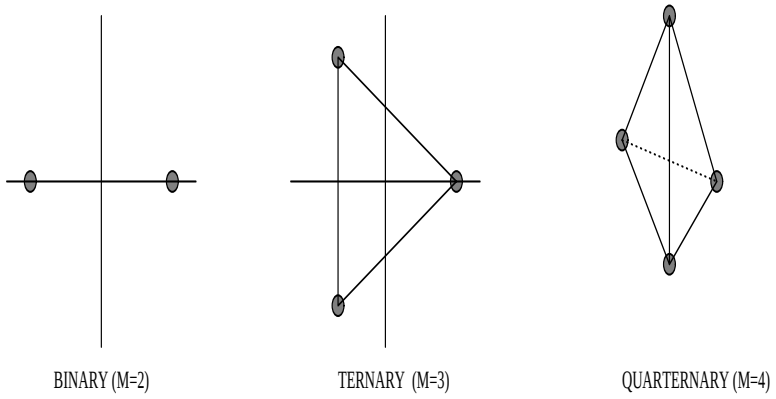


Figure 2.1: Binary, ternary and quaternary simplex signal sets.

Theorem 2.3 (Hamming spaces): *Let A be a signal set which is an m-th order q-ary Hamming space. Then*

$$R_U(q^m, \delta) = m \left(1 - H_q \left(\theta - \sqrt{\theta^2 - \frac{\theta\delta}{K}} \right) \right) \tag{2.25}$$

where $\theta = \frac{(q-1)}{q}$ and K is the squared Euclidean distance between any two points differing in only one position in the label.

Proof: Since A is an m-th order q-ary Hamming space A has q^m points. Let A' be a subset such that the elements of A' differ only in one fixed coordinate. A' is a simplex signal set consisting of q signal points. Codes of length n over A can be considered as codes of length mn over A'. Hence we have

$$R_U(q^m, \delta) = mR_U(q, \delta) \tag{2.26}$$

Note that A' is a simplex signal set consisting of q points. Hence $R_U(q, \delta)$ is given by Theorem 2.2. □

Observe that a simplex signal set with M points is a first order M-ary Hamming space. In this sense Theorem 2.3 is a generalization of Theorem 2.2.

Corollary 2.3.1 *For N-dimensional cube, the extended Piret's bound is given by*

$$R_U(2^N, \delta) = N\left(1 - H_2\left(\frac{1}{2} - \frac{1}{2}\sqrt{1 - \frac{\delta}{2}}\right)\right) \tag{2.27}$$

Proof: Straightforward application of Theorem 2.3. □

Example 2.2 *The 3-dimensional cube shown in Figure 2.3 is a third order binary Hamming space with labeling as shown. The bound for this cube is given by*

$$R_U(8, \delta) = 3\left(1 - H_2\left(\frac{1}{2} - \frac{1}{2}\sqrt{1 - \frac{\delta}{2}}\right)\right) \tag{2.28}$$

Theorem 2.4 (Biorthogonal signal sets): *The optimum distribution $\underline{\beta} = (\beta_0, \beta_1, \beta_2, \cdots, \beta_{M-1})$ giving the tightest bound for codes over biorthogonal signal set is given in terms of a parameter $\mu > 0$, as*

$$\beta_r(\mu) = \frac{e^{-\mu d^2(r)}}{\sum_{s=0}^{M-1} e^{-\mu d^2(s)}} \quad r = 0, 1, 2, \cdots, M-1, \tag{2.29}$$

where $d^2(r)$ is the squared Euclidean distance between 0 th point and the rth point of the M point biorthogonal signal set.

Proof: The squared Euclidean distance profile of a M point biorthogonal signal set is as follows

$$\begin{aligned} d^2(r) &= 0 \;\; if \;\; r = 0 \\ &= K \;\; (a\ constant), \; if \;\; r \neq 0 \; and \; r \neq \frac{M}{2} \\ &= 2K \;\; if \;\; r = \frac{M}{2} \end{aligned} \tag{2.30}$$

$$S = \begin{bmatrix} 0 & K & K & \dots & K & 2K & K & \dots & K \\ K & 0 & K & \dots & K & K & 2K & \dots & K \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 2K & K & K & \dots & K & 0 & K & \dots & K \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ K & K & K & \dots & 2K & K & K & \dots & 0 \end{bmatrix} \tag{2.31}$$

Here S is a circulant matrix.Therefore the second row of the S matrix is obtained by circularly shifting the first row to the right once. All the M rows of the S matrix can be obtained similarly.

Let $\underline{\beta} = (\beta_0, \beta_1, \dots, \beta_{M-1})$ be any probability distribution. We find the best bound using Lagrange multipliers. Consider the Lagrangian

$$\begin{aligned} \Phi(\underline{\beta}, \lambda) &= H(\underline{\beta}) - \lambda \left[\delta - \underline{\beta} S \underline{\beta}^T\right] \\ &= H(\underline{\beta}) - \lambda \left[\delta - \sum_{i=0}^{M-1} \sum_{j=0, j\neq i}^{M-1} \beta_i s_{ij} \beta_j\right] \end{aligned} \tag{2.32}$$

Here β_r will be the same for $\{r = 1, 2, \dots, \frac{M}{2} - 1, \frac{M}{2} + 1, \dots, M-1\}$. Hence we have to find the optimum values for β_1 and $\beta_{\frac{M}{2}}$. These correspond to

$$\frac{\partial \Phi(\underline{\beta}, \lambda)}{\partial \beta_1} = \log(\beta_0) - \log(\beta_1) + 2K\lambda\beta_0 - 2K\lambda\beta_{\frac{M}{2}} \tag{2.33}$$

and

$$\frac{\partial \Phi(\underline{\beta}, \lambda)}{\partial \beta_{\frac{M}{2}}} = \log(\beta_0) - \log(\beta_{\frac{M}{2}}) + 4K\lambda\beta_0 - 4K\lambda\beta_{\frac{M}{2}} \tag{2.34}$$

Equating (2.33) and (2.34) to zero and simplifying we get

$$\beta_0 \beta_{\frac{M}{2}} = \beta_1^2 \tag{2.35}$$

It is easily verified that

$$\beta_r(\mu) = \frac{e^{-\mu d^2(r)}}{\sum_{s=0}^{M-1} e^{-\mu d^2(s)}} \;\; r \;=\; 0, 1, 2, \cdots, M-1 \tag{2.36}$$

constitute a solution of the equation(2.35) with parameter μ.

Also note that $H(\underline{\beta})$ is a concave function in $\underline{\beta}$. For biorthogonal signal sets the S matrix is circulant as given above. We verify whether the quadratic form $\underline{\beta}S\underline{\beta}$ is concave. From [4] we know that the quadratic form is concave if all the eigenvalues except the largest eigenvalues of S are non-positive. This we verify as follows: The m-th eigenvalue η_m of the circulant matrix S can be expressed as, [13], $\eta_m = \sum_{i=0}^{M-1} s_i e^{(j\frac{2\pi mi}{M})}$, where $(s_0 = 0, s_1 = K, s_2 = K, \ldots, s_{\frac{M}{2}} = 2K, \ldots, s_{M-1} = K)$ forms the first row of the S matrix. When $m = 0$ we see that η_0 is the sum of the first row of S.

1. In the first row of S matrix there are equal number of K on either side of the $\frac{M}{2}$- *th* location and $s_{\frac{M}{2}} = 2K$.

2. Consider the eigenvalue η_m when m is odd. Obtain η_m using discrete Fourier transform of the first row of S matrix, i.e, $\eta_m = \sum_{i=0}^{M-1} s_i e^{(j\frac{2\pi mi}{M})}$. The expression $e^{(j\frac{2\pi m}{M}\frac{M}{2})}$ can be simplified to $e^{(j\pi m)} = -1$. Therefore the $\frac{M}{2}$-th term in the discrete Fourier transform sum for η_m is $-1s_{\frac{M}{2}} = -2K$. The first term of the first row of S, i.e., s_0 is zero. Therefore it does not contribute to the discrete Fourier transform sum. The terms s_i and $s_{i+\frac{M}{2}}$, where $i < \frac{M}{2}$, sum to zero for every such i. This can be seen as follows: $s_{i+\frac{M}{2}}$ is $e^{(j\frac{2\pi m}{M}(i+\frac{M}{2}))}$. Simplifying we get $s_{i+\frac{M}{2}}$ equals to $-1e^{(j\frac{2\pi mi}{M})}$. Therefore $s_{i+\frac{M}{2}}$ is equal to $-1s_i$.

   Hence in the discrete Fourier transform sum of all terms except except the term associated with $s_{\frac{M}{2}}$ is equal to zero. Therefore for m odd the sum is $-2K$ and hence the eigenvalues are non positive for m odd.

3. Consider the eigenvalue η_m for m even. The expression $e^{(j\frac{2\pi m}{M}\frac{M}{2})}$ simplifies to $e^{(j\pi m)} = 1$. The $\frac{M}{2}$-*th* term in the discrete Fourier transform sum is $s_{\frac{M}{2}}$ which is equal to $2K$. The term s_0 of the first row of S is zero. Therefore it does not contribute to the discrete Fourier transform sum. The terms s_i and $s_{i+\frac{M}{2}}$ for $i < \frac{M}{2}$ can be shown to sum to zero. For $i < \frac{M}{2}$ $s_i = s_{i+\frac{M}{2}}$ and $s_{i+\frac{M}{2}} = e^{(j\frac{2\pi m}{M}(i+\frac{M}{2}))}$ is equal to $e^{(j\frac{2\pi mi}{M})}$. Therefore η_m for m even is equal to $2K\sum_{i=0}^{\frac{M}{2}} e^{(j\frac{2\pi mi}{M})} - 2K + 2k$. But $\sum_{i=0}^{\frac{M}{2}} e^{(j\frac{2\pi mi}{M})}$ is the sum of $\frac{M}{2}$ terms of a geometric series whose common ratio is $e^{(j\frac{2\pi m}{M})}$. The sum of these $\frac{M}{2}$ terms is zero. Therefore for m even the discrete Fourier

transform coefficients are zero. Hence the eigenvalues are zero for even m.

Therefore all the secondary eigenvalues are non positive and the primary eigenvalue equals the sum of the elements of the first row. This shows that the quadratic form $\underline{\beta}S\underline{\beta}^T$ is a concave function. Therefore the the Lagrangian is a concave function and the extremal point given by equation(2.36) gives an optimal distribution. □

Example 2.3 *Consider the biorthogonal signal set for $M = 4$. Biorthogonal signal with $M = 4$ is same as $4 - PSK$ signal set (Figure 2.4). The optimum distribution achieving the tightest bound is given by following equations*

$$\begin{aligned} \beta_1(\mu) = \frac{e^{-2\mu}}{\sum_{s=0}^{3} e^{-\mu d^2(s)}},\ \beta_2(\mu) = \frac{e^{-4\mu}}{\sum_{s=0}^{3} e^{-\mu d^2(s)}} \\ \beta_3(\mu) = \beta_1(\mu),\ \beta_0(\mu) = 1 - 2\beta_1(\mu) - \beta_2(\mu) \end{aligned} \tag{2.37}$$

The above distribution for 4-PSK signal set is same as optimal distribution conjectured by Piret for PSK signal sets. The $EEUB$ for 4-point biorthogonal signal set is shown in Figure 2.5. In Figure 2.5 RUB for biorthogonal signal sets is plotted for different values of M. First curve from the bottom is for $M = 4$ and the top curve is for $M = 128$

2.2.1 Piret's Conjecture for codes over 5-PSK signal sets

Piret has obtained both asymptotic lower and upper bounds for codes over symmetric PSK signal sets. Both the bounds are obtained in terms of a probability distribution. However, for lower bound the distribution giving the best lower bound is obtained whereas, as mentioned in the previous section, the distribution giving the best upper bound is not given but it is conjectured that the distribution which gives the optimum lower bound also gives the best upper bound. For 5-PSK we check the conjecture.

Piret's Lower Bound:

Let A be a M point uniform signal set with Euclidean distance distribution $\{d(r), r = 0, 1, \ldots, M-1\}$. For C, a length n code over S, let

$$\delta(C) = \frac{1}{n} d^2(C)$$

$$R(C) = \frac{1}{n} \ln \mid C \mid$$
$$R(M, \delta) = \lim_{n \to \infty} sup_{\substack{|C| \geq n \\ \delta(C) \geq \delta}} R(C) \tag{2.38}$$

where $d^2(C)$ is the $MSED$ of C and $R(C)$ is the rate of the code. Then a lower bound $R_L(M, \delta)$ on $R(C)$ is given in terms of a parameter μ by

$$R_L(M, \delta) = \ln M - H(\underline{\beta}(\mu)) \qquad 0 \leq \delta \leq 2 \tag{2.39}$$

where $\underline{\beta}(\mu)$ is the distribution $\{\beta_r, r = 0, 1, \ldots, M-1\}$ is given by

$$\beta_r(\mu) = \frac{e^{-\mu d^2(r)}}{\sum_{s=0}^{M-1} e^{-\mu d^2(s)}} \tag{2.40}$$
$$\delta = \sum_{s=0}^{M-1} \beta_s(\mu) d^2(s) \tag{2.41}$$

Note that bound is not given in terms of an arbitrary distribution-instead the distribution given above is optimum for the lower bound. The Equation 2.39 is counterpart of the equation for the upper bound (Equation 2.5). Piret conjectures that the distribution given in equation(2.40) is the optimum distribution for the upper bound also.

If Piret's conjecture was true then the distribution given in equation(2.40) should satisfy the set of equations to get the optimal distribution for $5 - PSK$ signal set (Lagrange multiplier method is used to get optimum distribution). The distance distribution matrix S is given by

$$S = \begin{bmatrix} 0 & a & b & b & a \\ a & 0 & a & b & b \\ b & a & 0 & a & b \\ b & b & a & 0 & a \\ a & b & b & a & 0 \end{bmatrix} \tag{2.42}$$

Here note that S matrix is circulant. Therefore using the same approach as in Berlekamp[4] we can show that the quadratic $\underline{\beta} S \underline{\beta}^T$ is a function (we use the result in [13] to obtain the eigenvalues). $H(\underline{\beta})$ is a concave function. Therefore the extremal point of the Lagrangian is an optimal solution.

$$\Phi(\underline{\beta}, \lambda) = H(\underline{\beta}) - \lambda \left[\delta - \underline{\beta} S \underline{\beta^T}\right]$$

$$= \quad H(\underline{\beta}) - \lambda \left[\delta - \sum_{i=0}^{4} \sum_{j=0, j\neq i}^{4} \beta_i s_{ij} \beta_j \right] \tag{2.43}$$

where s_{ij} is of the form $4sin^2\left[(i-j)\pi/M\right]$. Now for $r = 1, 2$ we obtain the partial derivatives,

$$\frac{\partial \Phi(\underline{\beta}, \lambda)}{\partial \beta_r} = \log(\beta_0) - \log(\beta_r) - 2\lambda \sum_{j=1}^{4} s_{0,j}\beta_j + 2\lambda \sum_{j=0, j\neq r}^{4} s_{r,j}\beta_j \tag{2.44}$$

Since the above expression is identical for $r = 1, 4$ and $r = 2, 3$ we have $\beta_1 = \beta_4$ and $\beta_2 = \beta_3$. Taking $r = 1$ we solve for λ in terms of β_1 and β_2.

$$\lambda = \frac{\log \beta_1 - \log \beta_0}{2(a + (b-4a)\beta_1 - (a+b)\beta_2)} \tag{2.45}$$

where $a = 4sin^2(\pi/5)$ and $b = 4sin^2(2\pi/5)$. From the optimal distribution for lower bound ([46]) we have $\beta_1 = \beta_0 e^{-\mu a}$ and $\beta_2 = \beta_0 e^{-\mu b}$. Substituting for β_1 and β_2 in the equation(2.45) we get

$$\lambda = \frac{-\mu a}{2(a + (b-4a)\beta_0 e^{\mu a} - (a+b)\beta_0 e^{-\mu b})} \tag{2.46}$$

The partial derivative of the Lagrangian for $r = 2$ is

$$\log \beta_0 - \log \beta_2 + 2\lambda \left[b - (a+b)\beta_1 + (a-4b)\beta_2 \right] \tag{2.47}$$

Substituting for λ, β_1 and β_2 in equation(2.47) we get the following

$$b - a\frac{\left[b - (a+b)\beta_0 e^{-(\mu a)} + (a-4b)\beta_0 e^{-(\mu b)}\right]}{\left[a + (b-4a)\beta_0 e^{-(\mu a)} - (a+b)\beta_0 e^{-(\mu b)}\right]} = 0 \tag{2.48}$$

Simplifying these equations we get

$$\frac{b}{a} = \frac{\left[-(a+b)\beta_0 e^{-(\mu a)} + (a-4b)\beta_0 e^{-(\mu b)}\right]}{\left[(b-4a)\beta_0 e^{-(\mu a)} - (a+b)\beta_0 e^{-(\mu b)}\right]} \tag{2.49}$$

The right hand side of the above equation was computed by varying μ (here μ is any non-negative real number). The right hand side was equal to 2.6180 for every value of μ. This is same as $\frac{b}{a}$. Therefore we conclude that Piret's conjecture for 5-PSK is correct.

2.3 Discussions

The known upper bounds [46] and [20], respectively, on the normalized rate of a code over symmetric PSK signal set for a specified $NSED$ and of a code over any signal set constituting a group for a general distance function are shown to be valid for codes over any distance-uniform signal set. In general, the tightness of these bounds depends on a choice of a probability distribution. The optimum distribution for the cases (i) simplex (ii) Hamming spaces and (iii) biorthogonal signal sets leading to tightest bounds are obtained. The classical asymptotic Elias bound is shown to be same as the bound of this chapter for codes over simplex signal sets with the optimum distribution obtained. In chapter(3) we attempt to get best bounds for codes over several signal sets which include signal sets matched to specific groups, like dihedral, quaternion, dicyclic groups etc.

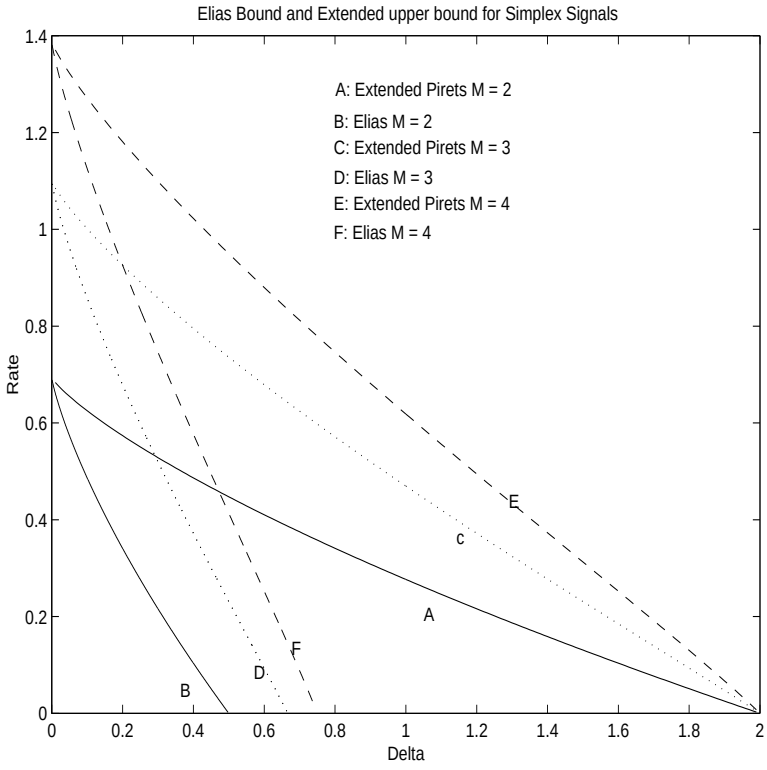


Figure 2.2: The Elias and extended upper bounds for binary, ternary and quaternary simplex signal sets.

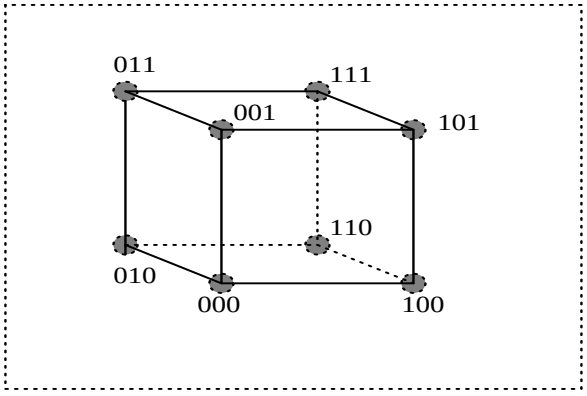


Figure 2.3: 3-dimensional cube.

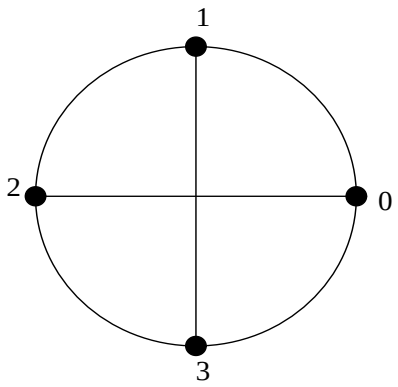


Figure 2.4: Biorthogonal Signal Set with $M = 4$. This is same as 4-PSK with points uniformly distributed on the unit circle

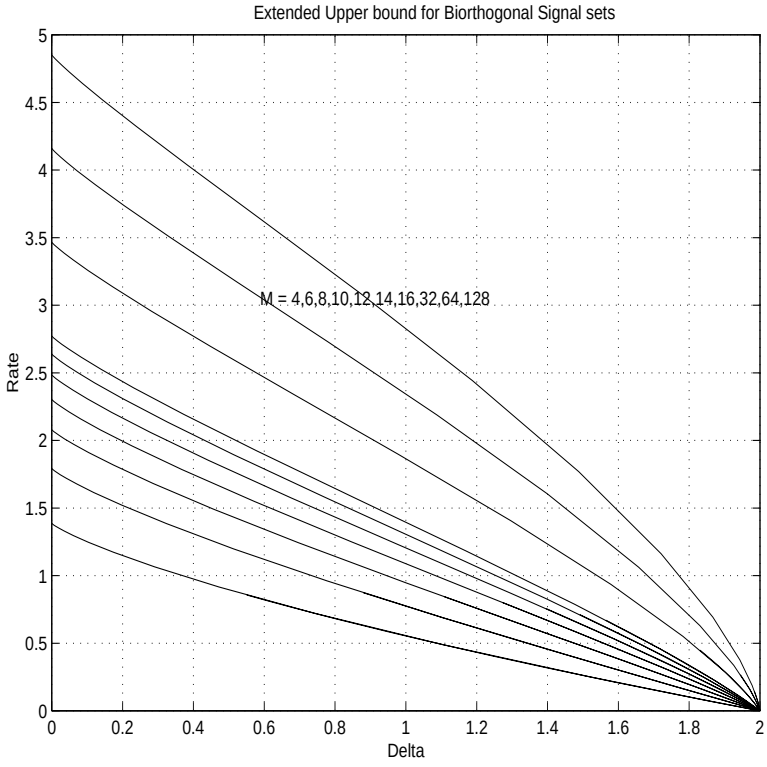


Figure 2.5: The extended upper bounds for M-point biorthogonal signal set.

Chapter 3

Extended Elias Upper Bound (EEUB) for Euclidean Space Codes over Certain 2-, 3-, 4-Dimensional Signal Sets

[1]

3.1 Introduction

The extended Elias upper of distance uniform signal sets obtained in theorem(2.1) depends on a probability distribution function. For codes over simplex (theorem(2.2)and biorthogonal signal sets (theorem(2.4) we found probability distribution function that achieves the best $EEUB$. In this chapter we study the $EEUB$ of codes over signal sets in two dimensional spaces, three dimensional spaces, four dimensional spaces and n-dimensional spaces. We obtain a probability distribution that achieves the tightest $EEUB$ for codes over several signal sets in multidimensions and compare the bounds based on the normalized rate per two dimensions.

We call a distribution that obtains the best bound as an optimal distribution. In the following section we obtain optimum distributions for Euclidean space codes over signal sets matched to the binary tetrahedral group, the binary octahedral group, the binary icosahedral group, n-dimensional cube and biorthogonal signal set. Also an optimum distribution

[1] A part of the results of this chapter is available in [68]

was obtained for specific cardinalities of Euclidean space codes matched to dihedral group, dicyclic group, double prism group and finite unitary groups. We also obtain an optimum distribution for codes over Slepian signal sets, [53], in five and six dimensions.
The remaining part of this chapter is organized as follows:

- In section(2) we discuss the method to arrive at an optimum distribution for Euclidean space codes over distance uniform signal sets. We also show that the quadratic form $\underline{\beta}S\underline{\beta}^T$ is concave for all signal sets having elements of equal energy. Further we also prove that distance uniform signal sets are signal sets having all elements with equal energy.

- In section(3) we compute an optimum distribution for Euclidean space codes over several distance uniform signal sets. We also compare the signal sets based on the normalized spectral rate.

- In section(4) we conclude the chapter.

3.2 Optimum Distribution for Euclidean Space Codes over Distance Uniform Signal Sets

Let $\underline{\beta} = (\beta_0, \beta_1, \ldots, \beta_{M-1})$ be any probability distribution. We find the best distribution by using Lagrange multipliers. Let (using equation(2.1))

$$\begin{aligned} \Phi(\underline{\beta}, \lambda) &= H(\underline{\beta}) - \lambda \left[\delta - \underline{\beta}S\underline{\beta}^T\right] \\ &= H(\underline{\beta}) - \lambda \left[\delta - \sum_{i=0}^{M-1} \sum_{j=0, j\neq i}^{M-1} \beta_i s_{i,j} \beta_j\right] \end{aligned} \tag{3.1}$$

where $s_{i,j}$ is the squared Euclidean distance between the i-th element and j-th element of the signal set.
In the above equation $H(\underline{\beta})$ is a concave function of $\underline{\beta}$ i.e., an inverted cup shaped function and $\underline{\beta}S\underline{\beta}^T$ is a quadratic form in $\underline{\beta}$. If $\underline{\beta}S\underline{\beta}^T$ is also a concave function of $\underline{\beta}$ then

$$H(\underline{\beta}) + \lambda\underline{\beta}S\underline{\beta}^T \tag{3.2}$$

is a concave function for $\lambda \geq 0$ [22]. Affine combinations of concave functions is also concave if the coefficients are positive, i.e. in this case we want $\lambda \geq 0$.

Now we have to look for conditions for $\underline{\beta}S\underline{\beta}^T$ to be concave. The structure of S matrix can be used to obtain these conditions. In general S is a symmetric matrix with positive entries and the rows of S are obtained by some permutation of the first row.

- The S matrix is a symmetric matrix with positive entries such that each row of S is some permutation of the first row. In this case, we don't have a closed form expression for the eigenvalues of S in general. The eigenvectors of S are orthonormal [49] (since S is a symmetric matrix). Therefore we compute the eigenvalues and eigenvector of the S matrix. For the quadratic form to be concave we need all the eigenvalues except the largest to be non-positive and the sum of each eigenvector except the one associated with the largest eigenvalue be zero. Note that for any $(M \times M)$ symmetric matrix we can get a set of M eigenvectors such that they orthonormal [49].

- For Euclidean space codes over certain signal sets the S matrix will be circulant matrix. Examples of such signal sets include simplex and biorthogonal signal sets. The S matrix is a symmetric circulant matrix with the first row $(s_0, s_1, \ldots, s_{M-1})$. Then the eigenvector matrix of S is the discrete Fourier transform matrix [13], [49]. Then from [2], [4] (page number 320) $\underline{\beta}S\underline{\beta}^T$ is a concave function if all the eigenvalues except the largest eigenvalue are non-positive. In the case of symmetric circulant S matrix then the eigenvalues, η_m, of S are given by [13], $\eta_m = \sum_{i=0}^{M-1} s_i e^{(j\frac{2\pi mi}{M})}$.

Taking partial derivatives of the Lagrange multiplier equation w.r.t $\beta_0, \beta_1, \beta_2, \ldots, \beta_{M-1}$ we can obtain the extremal points.

$$\frac{\partial \Phi(\underline{\beta}, \lambda)}{\partial \beta_r} = \frac{\partial}{\partial \beta_r} H(\beta) + \lambda \frac{\partial}{\partial \beta_r} \left(\sum_{i=0}^{M-1} \sum_{j=0, j\neq i}^{M-1} \beta_i s_{i,j} \beta_j \right) \tag{3.3}$$

The extremal points correspond to the maximum of $\Phi(\underline{\beta}, \lambda)$ if $\Phi(\underline{\beta}, \lambda)$ is a concave function.

Simplifying the equation(3.3) and using the condition that $\beta_0 = 1 - \sum_{i=1}^{M-1} \beta_i$ we get

$$\frac{\partial \Phi(\underline{\beta}, \lambda)}{\partial \beta_r} = \log(\beta_0) - \log(\beta_r) - 2\lambda \sum_{j=1}^{M-1} s_{0,j}\beta_j + 2\lambda \sum_{j=0, j\neq r}^{M-1} s_{r,j}\beta_j \tag{3.4}$$

As these are a set of nonlinear equations they are not amenable for direct solution. Therefore we assume a solution and verify whether it satisfies the set of equations represented by

equation(3.3). In other words we check whether the assumed solution is an extremal point of the Lagrangian. Further based on the structure of S matrix we can conclude whether the Lagrangian is a concave function in $\underline{\beta}$. If the Lagrangian is a concave function then a $\underline{\beta}$ which is an extremal point turns out to be an optimal solution.

We verify whether the following distribution is an extremal point of the Lagrangian

$$\beta_r(\mu) = \frac{e^{-\mu d^2(r)}}{\sum_{s=0}^{M-1} e^{-\mu d^2(s)}} \quad r \; = \; 0, 1, 2, \cdots, M-1 \tag{3.5}$$

where $d^2(r)$ is the squared Euclidean distance between 0th point and the rth point of the M point signal set. It turns out that the above is an optimal distribution for several Euclidean space codes over distance uniform signal sets. These include Euclidean space codes that are matched to

- the binary tetrahedral group, the binary octahedral group, the binary icosahedral group, n-dimensional cube and biorthogonal signal set.
- specific cardinalities of Euclidean space codes over finite unitary groups, cyclic group, dihedral group and dicyclic group.
- Slepian signal sets in five and six dimensions[53].

Also optimum distribution depends only on the distance distribution of the signal set and parameter μ.

In short to conclude whether equation(3.5) is an optimum distribution we check for the following:

- check whether $\underline{\beta} S \underline{\beta}^T$ is a concave function in $\underline{\beta}$.
- check whether equation(3.5) is an extremal point of the Lagrangian, .i.e. a solution of the equation(3.3).

In the next section we describe several distance uniform signal sets and check whether equation(3.5) gives an optimum distribution for Euclidean space codes over these signal sets. Further we compare their performance based on the normalized rate per two dimensions.

To illustrate we obtain an optimum $\underline{\beta}$ for codes over biorthogonal signal sets.

3.2.1 Euclidean Space Codes over Biorthogonal Signal Sets

Consider codes over biorthogonal signal set The squared Euclidean distance profile of a M point biorthogonal signal set is as follows

$$\begin{aligned} d^2(r) &= 0 \ \ if \ \ r = 0 \\ &= K \ \ (a\ constant), \ if \ \ r \neq 0 \ and \ r \neq \frac{M}{2} \\ &= 2K \ \ if \ \ r = \frac{M}{2} \end{aligned} \tag{3.6}$$

$$S = \begin{bmatrix} 0 & K & K & \dots & K & 2K & K & \dots & K \\ K & 0 & K & \dots & K & K & 2K & \dots & K \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 2K & K & K & \dots & K & 0 & K & \dots & K \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ K & K & K & \dots & 2K & K & K & \dots & 0 \end{bmatrix} \tag{3.7}$$

Here S is a positive symmetric circulant matrix.Therefore the second row of the S matrix is obtained by circularly shifting the first row to the right once. All the M rows of the S matrix can be obtained similarly. The eigenvector matrix is the discrete Fourier transform matrix. The quadratic form $\underline{\beta} S \underline{\beta}^T$ represents a concave function if all the eigenvalues except the largest eigenvalue is non-positive [4]. The largest eigenvalue is given by sum of the first row of the S matrix ([13]) and therefore positive. All we need to do now is to verify whether the other eigenvalues S are non-positive. This can be seen as follows ([13]):
The m-th eigenvalue η_m of the circulant matrix S can be expressed as $\eta_m = \sum_{i=0}^{M-1} s_i e^{(j\frac{2\pi mi}{M})}$, where $(s_0 = 0, s_1 = K, s_2 = K, \dots, s_{\frac{M}{2}} = 2K, \dots, s_{M-1} = K)$ forms the first row of the S matrix. When $m = 0$ we see that η_0 is the sum of the first row of S.

1. In the first row of S matrix there are equal number of K on either side of the $\frac{M}{2}$- *th* location and $s_{\frac{M}{2}} = 2K$.

2. Consider the eigenvalue η_m when m is odd. Obtain η_m using discrete Fourier transform of the first row of S matrix, i.e, $\eta_m = \sum_{i=0}^{M-1} s_i e^{(j\frac{2\pi mi}{M})}$. The expression $e^{(j\frac{2\pi m}{M}\frac{M}{2})}$ can be simplified to $e^{(j\pi m)} = -1$. Therefore the $\frac{M}{2}$-th term in the discrete Fourier transform sum for η_m is $-1 s_{\frac{M}{2}} = -2K$. The first term of the first row of S, i.e., s_0 is zero. Therefore it does not contribute to the discrete Fourier transform sum. The terms s_i and $s_{i+\frac{M}{2}}$, where $i < \frac{M}{2}$, sum to zero for every such i. This can be

seen as follows: $s_{i+\frac{M}{2}}$ is $e^{(j\frac{2\pi m}{M}(i+\frac{M}{2}))}$. Simplifying we get $s_{i+\frac{M}{2}}$ equals to $-1e^{(j\frac{2\pi mi}{M})}$. Therefore $s_{i+\frac{M}{2}}$ is equal to $-1s_i$.

Hence in the discrete Fourier transform sum of all terms except except the term associated with $s_{\frac{M}{2}}$ is equal to zero. Therefore for m odd the sum is $-2K$ and hence the eigenvalues are non positive for m odd.

3. Consider the eigenvalue η_m for m even. The expression $e^{(j\frac{2\pi m}{M}\frac{M}{2})}$ simplifies to $e^{(j\pi m)} = 1$. The $\frac{M}{2}$-*th* term in the discrete Fourier transform sum is $s_{\frac{M}{2}}$ which is equal to $2K$. The term s_0 of the first row of S is zero. Therefore it does not contribute to the discrete Fourier transform sum. The terms s_i and $s_{i+\frac{M}{2}}$ for $i < \frac{M}{2}$ can be shown to sum to zero. For $i < \frac{M}{2}$ $s_i = s_{i+\frac{M}{2}}$ and $s_{i+\frac{M}{2}} = e^{(j\frac{2\pi m}{M}(i+\frac{M}{2}))}$ is equal to $e^{(j\frac{2\pi mi}{M})}$. Therefore η_m for m even is equal to $2K\sum_{i=0}^{\frac{M}{2}} e^{(j\frac{2\pi mi}{M})} - 2K + 2k$. But $\sum_{i=0}^{\frac{M}{2}} e^{(j\frac{2\pi mi}{M})}$ is the sum of $\frac{M}{2}$ terms of a geometric series whose common ratio is $e^{(j\frac{2\pi m}{M})}$. The sum of these $\frac{M}{2}$ terms is zero. Therefore for m even the discrete Fourier transform coefficients are zero. Hence the eigenvalues are zero for even m.

Therefore all the secondary eigenvalues are non positive and the primary eigenvalue equals the sum of the elements of the first row. This shows that the quadratic form $\underline{\beta}S\underline{\beta}^T$ is a concave function.

Next is to find a $\underline{\beta} = (\beta_0, \beta_1, \ldots, \beta_{M-1})$ which is an extremal point of the Lagrangian. We find the extremal point by solving the first derivative of the Lagrangian. Let

$$\begin{aligned}\Phi(\underline{\beta}, \lambda) &= H(\underline{\beta}) - \lambda\left[\delta - \underline{\beta}S\underline{\beta}^T\right] \\ &= H(\underline{\beta}) - \lambda\left[\delta - \sum_{i=0}^{M-1}\sum_{j=0, j\neq i}^{M-1}\beta_i s_{ij}\beta_j\right] \end{aligned} \tag{3.8}$$

Here β_r will be the same for $\{r = 1, 2, \ldots, \frac{M}{2} - 1, \frac{M}{2} + 1, \ldots, M-1\}$. Hence we have to find the optimum values for β_1 and $\beta_{\frac{M}{2}}$. These correspond to

$$\frac{\partial\Phi(\underline{\beta}, \lambda)}{\partial\beta_1} = \log(\beta_0) - \log(\beta_1) + 2K\lambda\beta_0 - 2K\lambda\beta_{\frac{M}{2}} \tag{3.9}$$

and

$$\frac{\partial\Phi(\underline{\beta}, \lambda)}{\partial\beta_{\frac{M}{2}}} = \log(\beta_0) - \log(\beta_{\frac{M}{2}}) + 4K\lambda\beta_0 - 4K\lambda\beta_{\frac{M}{2}} \tag{3.10}$$

Equating (3.9) and (3.10) to zero and simplifying we get

$$\beta_0 \beta_{\frac{M}{2}} = \beta_1^2 \tag{3.11}$$

It can be easily verified that

$$\beta_r(\mu) = \frac{e^{-\mu d^2(r)}}{\sum_{s=0}^{M-1} e^{-\mu d^2(s)}} \quad r = 0, 1, 2, \cdots, M-1 \tag{3.12}$$

constitute a solution of the equation(3.11) with parameter μ. Thus we have obtained an optimal distribution for Euclidean space codes over biorthogonal signal sets. □

3.2.2 Signal Sets of Equal Energy

In section(3.2.1) we showed that if the S matrix is circulant we can obtain closed form expressions for conditions under which $\underline{\beta} S \underline{\beta}^T$ is concave. When the S matrix is symmetric with positive entries it is hard to obtain general conditions on concavity of the quadratic form $\underline{\beta} S \underline{\beta}^T$. In general S matrix is Therefore we study signal sets where all elements of the signal set have equal energy. For signal sets with equal energy we verify whether the quadratic form is concave. We also show that the class of distance uniform signal sets are equal energy signal sets.

Proposition 3.0.1 *The quadratic $\underline{\beta} S \underline{\beta}^T$ is concave if S is the distance distribution matrix of a signal set with all elements having equal energy.*

Proof: Consider a signal set of cardinality M with equal energy. Let us assume that the energy has been normalized and is equal to one. Here the distance between i-th element and the j-th element of the signal set (*(i,j)-th* entry of S matrix) is equal to $(2 - 2\langle s_i, s_j \rangle)$, where $\langle s_i, s_j \rangle$ is the correlation between the *i-th* element and the *j-th* element of the signal set. Therefore the distance distribution matrix can be written as

$$S = \begin{bmatrix} 2 & 2 & \dots & 2 \\ 2 & 2 & \dots & 2 \\ \vdots & \vdots & \ddots & \vdots \\ 2 & 2 & \dots & 2 \end{bmatrix} - 2 \begin{bmatrix} 1 & \rho_{12} & \dots & \rho_{1M} \\ \rho_{21} & 1 & \dots & \rho_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{M1} & \rho_{M2} & \dots & 1 \end{bmatrix} \tag{3.13}$$

Here the first matrix on the right side of the above equation with all entries as 2 is a circulant matrix. It can be easily verified that the only non zero eigenvalue is positive. The eigenvectors of the matrix with all entries as 2 are orthonormal. The sum of components of the eigenvector associated with the largest eigenvalue alone is nonzero. All the other secondary eigenvalues are zero and the sum of the components of each eigenvector associated with the secondary eigenvalues is zero. These follow the properties of circulant matrices [13]. The second matrix on the right side of the above equation is the correlation matrix. The correlation matrix is a symmetric positive semi definite [52]. Therefore the eigenvalues are greater than or equal to zero. Also, the eigenvectors of correlation matrix are orthonormal [49].

Let $\underline{e}$ be an eigenvector of S matrix. Then

$$S\underline{e} = \begin{bmatrix} 2 & 2 & \dots & 2 \\ 2 & 2 & \dots & 2 \\ \vdots & \vdots & \ddots & \vdots \\ 2 & 2 & \dots & 2 \end{bmatrix} \underline{e} - 2 \begin{bmatrix} 1 & \rho_{12} & \dots & \rho_{1M} \\ \rho_{21} & 1 & \dots & \rho_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{M1} & \rho_{M2} & \dots & 1 \end{bmatrix} \underline{e} \tag{3.14}$$

$$S\underline{e} = \eta_S \underline{e} = (\eta_2 - \eta_{Corr})\underline{e} \tag{3.15}$$

where $\underline{e}$ is an eigenvector of S, η_S is an eigenvalue of S, η_2 is an eigenvector of the matrix with all entries as 2 and η_{Corr} is an eigenvalue of the correlation matrix. All the secondary eigenvalues of the matrix with all entries as 2 are zero. Therefore the secondary eigenvalues of S are non positive as all the eigenvalues of correlation matrix are positive or zero.

Hence the quadratic $\underline{\beta} S \underline{\beta^T}$ is concave for signal sets having all elements are at the same distance from origin (signal sets with all elements of the set having the same energy). □

This class where all the elements of signal set are at the same distance from the origin include the signal sets matched to dihedral group (both symmetric and asymmetric PSK), Massey Signal set, dicyclic group, binary tetrahedral group, binary octahedral group, binary icosahedral group, the n dimensional cube and the double prism. Slepian signal sets also have signal points which are at the same distance from the origin. We also consider examples of signal sets matched to finite unitary groups of Type(I), Type(II), Type(III), Type(IV), Type(V), Type(VI) and Type(VII). In all these cases elements of the signal set have same energy [79]. Therefore for all these signal sets $\beta S \beta^T$ is concave.

Proposition 3.0.2 *If the signal set is distance uniform then all elements of the signal set have equal energy.*

Proof: Consider a distance uniform signal set $S = \{s_0, s_1, s_2, \ldots, s_{M-1}\}$, with M points in a finite p dimensional space. Consider the situation where $\sum_{i=0}^{i=M-1} s_i$ is equal to zero. If the $\sum_{i=0}^{i=M-1} s_i$ is not equal to zero it is always possible to translate the signal set by a x in the p dimensional space such that the sum of the elements of the translated signal set is zero. The translated signal set is also constitutes a distance uniform signal set. Let the squared Euclidean distance profile as seen form m and n-th point of the signal set be denoted as d_{mi}^2 and d_{ni}^2 respectively, where $0 \leq i \leq M-1$.

$$\sum_{i=0}^{M-1} d_{mi}^2 = \sum_{i=0}^{M-1} \left(\sum_{j=0}^{p-1} (s_{mj}^2 + s_{ij}^2) - 2\langle s_{mj}, s_{ij} \rangle \right) \tag{3.16}$$

$$= \sum_{i=0}^{M-1} \left(\sum_{j=0}^{p-1} (s_{mj}^2 + s_{ij}^2) \right) - \left(2\langle (\sum_{i=0}^{M-1} s_i), s_m \rangle \right) \tag{3.17}$$

Since $(\sum_{i=0}^{M-1} s_i) = 0$ we can write the above equation as

$$\sum_{i=0}^{M-1} d_{mi}^2 = M \sum_{j=0}^{p-1} s_{mj}^2 + \sum_{i=0}^{M-1} \sum_{j=0}^{p-1} (s_{ij}^2) \tag{3.18}$$

Similarly for d_{ni}^2

$$\sum_{i=0}^{M-1} d_{ni}^2 = M \sum_{j=0}^{p-1} s_{nj}^2 + \sum_{i=0}^{M-1} \sum_{j=0}^{p-1} s_{ij}^2 \tag{3.19}$$

For distance uniform signal sets we know that

$$\sum_{i=0}^{M-1} d_{mi}^2 = \sum_{i=0}^{M-1} d_{ni}^2 \tag{3.20}$$

Therefore by equating the equation(3.18) and equation(3.19) we get

$$M \sum_{j=0}^{p-1} s_{mj}^2 + \sum_{i=0}^{M-1} \sum_{l=0}^{p-1} s_{il}^2 = M \sum_{j=0}^{p-1} s_{nj}^2 + \sum_{i=0}^{M-1} \sum_{j=0}^{p-1} s_{ij}^2 \tag{3.21}$$

$$M \sum_{j=0}^{p-1} s_{mj}^2 = M \sum_{j=0}^{p-1} s_{nj}^2 \tag{3.22}$$

Therefore the n-*th* and m-*th* element of the signal set are at the same distance from the origin. This is true for any element of the signal set. Hence, from the above equations it follows that all the signal points are at the same distance from the origin for distance uniform signal sets. In other words distance uniform signal sets have signal points of equal energy. □

3.3 $EEUB$ of Distance Uniform Signal sets

In this section we compute the $EEUB$ for a class of distance uniform signal sets based on the optimum distribution which achieves the best bound for each signal set.

3.3.1 Two Dimensional Signal Sets Matched to Group

Two classes of signal sets in two dimensions matched to groups are those matched to cyclic groups (symmetric PSK (SPSK)) and those matched to dihedral groups (asymmetric PSK (APSK)). Several authors have studied codes over APSK signal sets [5], [12] and [25]. The dihedral group D_{2M} with $2M$ elements generated by two of its elements r and s with identity element e is

$$D_{2M} = \{r^i s^j \mid r^M = s^2 = e, r^i s = s r^{-i}, 0 \leq i < M, j = 0, 1\} \tag{3.23}$$

and the group operation can be expressed as

$$(r^{i_1} s^{j_1})(r^{i_2} s^{j_2}) = r^{i_1 + i_2(1-2j_1)} s^{j_1 + j_2} \tag{3.24}$$

In general, such signal sets are matched to D_{2M} under the mapping

$$\mu(r^i s^j) = e^{\sqrt{-1}(j\pi/M + \theta + 2\pi i/M)} \tag{3.25}$$

where θ is the angle of symmetry. Figure(3.1) shows the general $2M-$ APSK signal set matched to D_{2M}. Figure(3.2) shows the $EEUB$ bound for codes over 8-SPSK signal sets for seven different angles of asymmetry.

In the case of both symmetric and asymmetric PSK all points of the signal set are on the unit circle and therefore have equal energy. Therefore from section(3.2.2) we see that the Lagrangian is a concave function. We check whether equation(3.5) satisfies equation(3.3)

for signal sets of different M. Here we can only verify only the result computationally for signal sets of different cardinality. For codes symmetric PSK signal set with cardinality four we have shown in example(2.3)we have shown that equation(3.5) satisfies equation(3.3).

Example 3.1 *Consider a* 8 *PSK signal set. The* S *matrix of symmetric* 8 *PSK is*

$$\begin{bmatrix} 0 & 0.5858 & 2.0000 & 3.4142 & 4.0000 & 3.4142 & 2.0000 & 0.5858 \\ 0.5858 & 0 & 0.5858 & 2.0000 & 3.4142 & 4.0000 & 3.4142 & 2.0000 \\ 2.0000 & 0.5858 & 0 & 0.5858 & 2.0000 & 3.4142 & 4.0000 & 3.4142 \\ 3.4142 & 2.0000 & 0.5858 & 0 & 0.5858 & 2.0000 & 3.4142 & 4.0000 \\ 4.0000 & 3.4142 & 2.0000 & 0.5858 & 0 & 0.5858 & 2.0000 & 3.4142 \\ 3.4142 & 4.0000 & 3.4142 & 2.0000 & 0.5858 & 0 & 0.5858 & 2.0000 \\ 2.0000 & 3.4142 & 4.0000 & 3.4142 & 2.0000 & 0.5858 & 0 & 0.5858 \\ 0.5858 & 2.0000 & 3.4142 & 4.0000 & 3.4142 & 2.0000 & 0.5858 & 0 \end{bmatrix} \tag{3.26}$$

This is a real symmetric circulant matrix. Therefore the eigenvector matrix is a discrete Fourier transform matrix. The largest eigenvalue is positive. We have to check whether the other eigenvalues are non-positive. The eigenvalues are $[-8\,-8\,0\,0\,0\,16]$. *Moreover sum of any eigenvector except the one associated with the eigenvalue* 16 *is equal to zero. Therefore the Lagrangian is a concave function of* $\underline{\beta}$. *We need to check whether the distribution given in equation(3.5) is an extremal point. Computationally we see that it is an extremal point. Thus we get an optimal distribution.* □

The uppermost curve in the set of curves in figure(3.2) corresponds to 8-SPSK and the bottom most to 8-APSK with angle of asymmetry 10^o. The intermediate curves correspond to values of angle of asymmetry as listed in the figure. We see that equation(3.5) satisfies equation(3.3) for 8 PSK for all these angles of asymmetry. As the angle of asymmetry is increased the curve moves up toward the 8-SPSK curve. As the angle of asymmetry is increased from 0^o degrees to 40^o the curve tends from 8-SPSK to 4-PSK. This is similar to behavior seen in [56] for EGV bound. We conjecture that the behavior of $EEUB$ must be similar for M-PSK in general.

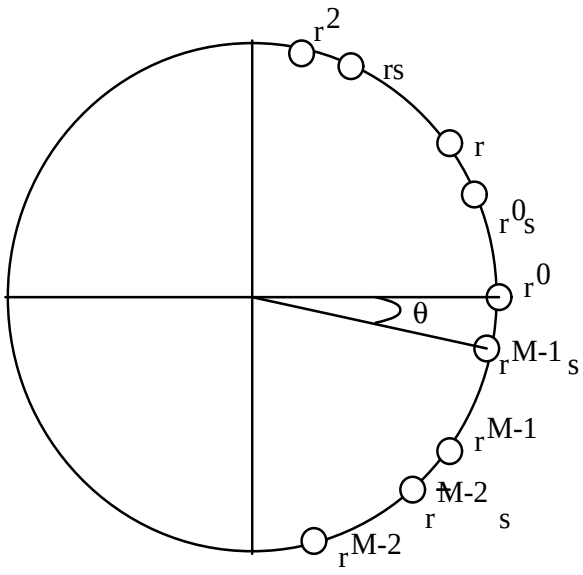


Figure 3.1: $2M$-point Asymmetric PSK signal set matched to dihedral group.

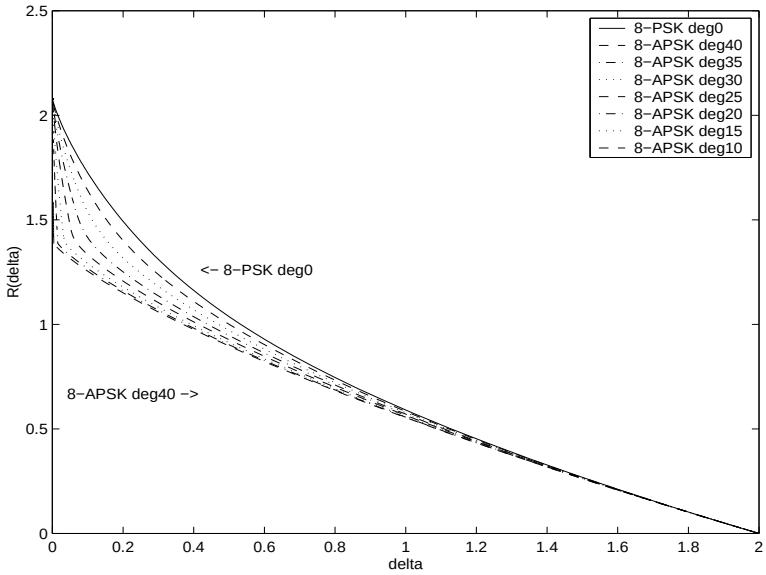


Figure 3.2: $EEUB$ for codes over 8-APSK for different angles. The top most curve represents 8 PSK. The bottommost curve represents the asymmetric PSK with angle of asymmetry 40 degrees.

3.3.2 Three-Dimensional Signal Sets Matched to Groups

Loeliger [37] has discussed a class of three-dimensional signal sets observed by Massey with points on a unit sphere matched to cyclic groups with even number of elements which we refer as Massey signal sets. Figure(3.3) shows a Massey signal set, with parameter r, matched to a cyclic group with eight elements. In general a Massey signal set with $2M$ points has its points on two circles parallel to the $x-y$ plane separated by a distance $2r$ along the $z-$axis, with M points on each circle. The points on each circle constitute an M-SPSK signal set with one M-SPSK signal set when projected onto the other circle forming another M-SPSK signal set which is a rotated version of the other by π/M. The points on each circle are indexed by $0, 2, ..., M-2$ and $1, 3, ..., 2M-1$ in the anticlockwise direction. This signal set is matched to the cyclic group of integers modulo $2M$ under the canonical map. All the elements of the Massey signal are at the same distance from the origin and hence have the same norm.

In the section(3.3.5) we compare the Massey signal set with eight points with 16 point dicyclic signal set and three-dimensional cube.

Example 3.2 *Consider an* 4 *point Massey signal set. The* S *matrix is as follows*

$$\begin{bmatrix} 0 & 1.8149 & 1.2800 & 3.6251 & 2.5600 & 3.6251 & 1.2800 & 1.8149 \\ 1.8149 & 0 & 1.8149 & 1.2800 & 3.6251 & 2.5600 & 3.6251 & 1.2800 \\ 1.2800 & 1.8149 & 0 & 1.8149 & 1.2800 & 3.6251 & 2.5600 & 3.6251 \\ 3.6251 & 1.2800 & 1.8149 & 0 & 1.8149 & 1.2800 & 3.6251 & 2.5600 \\ 2.5600 & 3.6251 & 1.2800 & 1.8149 & 0 & 1.8149 & 1.2800 & 3.6251 \\ 3.6251 & 2.5600 & 3.6251 & 1.2800 & 1.8149 & 0 & 1.8149 & 1.2800 \\ 1.2800 & 3.6251 & 2.5600 & 3.6251 & 1.2800 & 1.8149 & 0 & 1.8149 \\ 1.8149 & 1.2800 & 3.6251 & 2.5600 & 3.6251 & 1.2800 & 1.8149 & 0 \end{bmatrix} \tag{3.27}$$

The eigenvalues of S *are* $[-5.76 -5.12 -5.12000016]$. *Here all the secondary eigenvalues are non-positive. Also the sum of the each eigenvector is zero for all eigenvectors other than the one associated with the largest eigenvalue. Therefore the quadratic form is concave. We check whether the distribution represented by equation(3.5) is an extremal point of the Lagrangian (check whether it satisfies equation(3.3)). Here we see that it does satisfy the equation(3.3).* □

Consider For $M = 64$, Figure(3.4) shows the $EEUB$ bound for several values of r. From Figure(3.4), it is seen that the best bound depends on the normalized distance. Curves are plotted for $r = 0.6, 0.5, 0.4, 0.3, 0.2, 0.1$. All these curves intersect showing that for different values of normalized distances different r gives the best bound on rate.

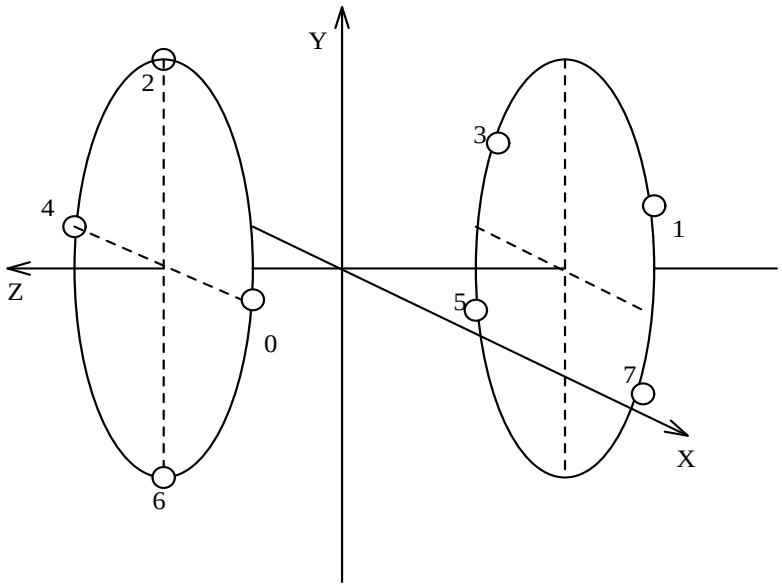


Figure 3.3: M-point Massey signal set ($M = 8$).

3.3.3 Bounds for Four-Dimensional Signal Sets Matched to Groups

Modulation schemes with four-dimensional signal sets have been studied by several authors [37], [79], [11], [50]. [26], [48], [64] and [73]. Gresho and Lawrence, [26], describe the basic theory and implementation for a particular lattice type, four-dimensional signal set, which readily lends itself to simple encoding with around $1.2dB$ gain in noise margin over the conventional two-dimensional 16 point QAM signaling. Moreover, a four dimensional signal set matched to a non-commutative group with 7200 signal points has been observed to have higher capacity than the PSK limit [37]. In this subsection, we apply the $EEUB$ bound for four-dimensional signal sets matched to dicyclic, binary tetrahedral, binary octahedral and binary icosahedral groups. The class of signal sets matched to dicyclic groups include those matched to the quaternion group and generalized quaternion groups since

these two are special cases of dicyclic groups. The groups are simply described in terms of the quaternions as follows. The elements of the set

$$H = \{\sigma = a\underline{e} + b\underline{j} + c\underline{k} + d\underline{l} \mid a, b, c, d \in R, a^2 + b^2 + c^2 + d^2 = 1\} \tag{3.28}$$

where R denotes the field of real numbers and $\underline{e}$, $\underline{j}$, $\underline{j}$, $\underline{k}$ and $\underline{l}$ are the vectors satisfying $\underline{i}^2 = \underline{j}^2 = \underline{k}^2 = -e$, $\underline{jk} = -\underline{kj} = i\underline{l}$, $\underline{kl} = -\underline{lk} = \underline{j}$, $\underline{lj} = -\underline{jl} = \underline{k}$, $\forall \sigma \in H$
In the infinite commutative group H, multiplication of two elements $(a_1\underline{e} + b_1\underline{j} + c_1\underline{k} + d_1\underline{l})$ and $(a_2\underline{e} + b_2\underline{j} + c_2\underline{k} + d_2\underline{l})$ results in $(a_3\underline{e} + b_3\underline{j} + c_3\underline{k} + d_3\underline{l})$ where

$$[a_3\ b_3\ c_3\ d_3] = [a_1\ b_1\ c_1\ d_1] \begin{bmatrix} a_2 & b_2 & c_2 & d_2 \\ -b_2 & a_2 & -d_2 & c_2 \\ -c_2 & d_2 & -a_2 & b_2 \\ -d_2 & -c_2 & -b_2 & -a_2 \end{bmatrix} \tag{3.29}$$

We look at following finite subgroups of H.

Dicyclic Groups DC_{4M}

The subgroup of H with $4M$ elements, (M arbitrary positive integer)

$$\sigma_\nu = (\ cos(\pi\nu/M),\ sin(\pi\nu/M),\ 0,\ 0), \tag{3.30}$$

$$v = 0, 1, \ldots, 2M - 1 \tag{3.31}$$

and

$$\tau_\nu = (\ 0,\ 0,\ cos(\pi\nu/M),\ sin(\pi\nu/M)), \tag{3.32}$$

$$v = 2M, 2M + 1, \ldots, 4M - 1 \tag{3.33}$$

The special case $M = 2$ gives the quaternion group $Q_8 = \{\bar{+}\ \underline{e}, \bar{+}\ \underline{j}, \bar{+}\ \underline{k}, \bar{+}\ \underline{l}\}$ with eight elements.
The signal points are all have the same energy. Therefore the conditions discussed in section(3.2.2) are valid. Thus the quadratic form $\beta S \beta^T$ is a concave function. For codes over dicyclic signal sets of different cardinality we verify whether the distribution given by equation(3.5) satisfies the Lagrangian (i.e. equation(3.3)). For dicyclic groups of different

cardinality which we have considered equation(3.5) satisfies the Lagrangian (for different cardinalities of dicyclic groups we have considered we computationally verified whether the distribution given by equation(3.3) satisfies the Lagrangian)

The Binary Tetrahedral Group G_{24}

This group with 24 elements consist of Q_8 and the two cosets ωQ_8 and $\omega^2 Q_8$ of Q_8, where

$$\omega = \frac{1}{2}(\underline{e} + \underline{j} + \underline{k} + \underline{l}) \tag{3.34}$$

Note $\omega^3 = (-\underline{e}) \in Q_8$. Explicitly, we have $G_{24} = Q_8 \cup \omega^2 Q_8 \cup \omega^2 Q_8$.
The signal points are in the binary tetrahedral group have the same energy. Therefore the conditions discussed in section(3.2.2) are valid. For tetrahedral group we compute the distance distribution matrix S and check the eigenvalues and the associated eigenvectors. S is a positive symmetric circulant matrix. We see that only one eigenvalue is positive and all other eigenvalues are non-positive. Moreover the eigenvectors are orthogonal and the sum of each eigenvector is zero except for the eigenvector associated with the largest eigenvalue. The largest eigenvalue is 48 and all others are zero or negative. Therefore the Lagrangian is concave for positive λ. λ is greater than or equal zero. The distribution given in equation(3.5) is an optimal distribution.

The Binary Octahedral Group G_{48}

This group with 48 elements is obtained by adding G_{24} and its coset $\omega_1 G_{24}$ where

$$\omega_1 = \frac{1}{\sqrt{2}}(\underline{e} + \underline{j}) \tag{3.35}$$

i.e., $G_{48} = G_{24} \cup \omega_1 G_{24}$.
In the case of binary octahedral group also the S matrix is positive symmetric matrix. The analysis of S matrix is carried out as in the case of the binary tetrahedral group. Therefore as in the case of tetrahedral group the distribution given in equation(3.5) is optimal.

The Binary Icosahedral Group G_{120}

This group consists of 120 elements and is obtainable as elements generated by the following three generators: $\sigma_1 = \frac{1}{2}(\gamma\underline{e} + \gamma^{-1}\underline{j} + \underline{l})$, $\sigma_2 = \frac{1}{2}(\underline{e} + \gamma^{-1}\underline{k} + \gamma\underline{k})$ and $\sigma_3 = l$, where

$\gamma = \frac{1}{2}(1+\sqrt{5})$.

As in the case of binary tetrahedral group and octahedral group the S matrix for icosahedral group is also positive, symmetric and circulant. Also except the primary eigenvalue all other eigenvalues are non-positive. The eigenvectors are orthogonal and the sum of each eigenvector except the one associated with the largest eigenvalue is also zero. We verify whether the distribution given in equation(3.5) is optimal. This we do by checking whether equation(3.5) is a solution of the equation(3.3).

Tetrahedral	Octahedral	Icosahedral
48	96	240
-12	-24	-60
-12	-24	-60
-12	-24	-60
-12	-24	-60

Table 3.1: The table shows the non-zero eigenvalues of squared Euclidean distance distribution matrix S. Here we consider codes over tetrahedral, octahedral and icosahedral groups.

Figure(3.5) shows four-dimensional signal sets matched to DC_{24}. Figures for four-dimensional signal sets matched to binary tetrahedral group with 24 elements, binary octahedral group with 48 elements, binary icosahedral group with 120 elements, and other numerous groups can be seen in [11]. Note that a signal point is specified by four coordinates with the first two co-ordinates in the $x_1 - x_2$ plane and the other two in the $x_3 - x_4$ plane. The mapping that matches these signal sets to the respective groups is the natural mapping $\mu(a\underline{e} + b\underline{j} + c\underline{k} + d\underline{l}) = (a, b, c, d)$.

Based on the $EEUB$ for signal sets matched to dicyclic groups of different order, it was obtained that for larger values of the normalized distance the number of points in the signal set does not matter and when a smaller normalized distance is the requirement, a larger number of points in the signal set are desirable; an observation which is true for symmetric PSK $(SPSK)$ signal sets as pointed on in [46]. The existence of DC_{24}, DC_{48} and DC_{120} makes these directly comparable with G_{24}, G_{48} and G_{120}, respectively, in terms of their bounds in figure(3.6). The bounds for codes over DC_{48} and DC_{120} appear indistinguish-

able. As seen from this set of bounds, signal sets matched to dicyclic groups with the same number of signal points give better bounds than signal sets matched to binary tetrahedral group, binary octahedral group and binary icosahedral group.

3.3.4 Extended Upper Bounds for Codes over Finite Unitary Groups

In this section we look at codes over different classes of finite unitary groups in four dimensions. We construct specific examples of finite unitary groups by enumerating the generator for each type of finite unitary group [11]. We look at specific examples of groups in each class and compute the $EEUB$ for codes over each class.

Type - I finite unitary group

The elements of one such group with ns elements are generated by

$$\frac{1}{2^{0.5}}(\epsilon_1^{q\nu'+\mu}\epsilon_2^{-(q\nu'+d\mu)}, \epsilon_1^{q\nu'+\mu}\epsilon_2^{q\nu'+d\mu})$$

where $\epsilon_1 = exp(j\pi/n)$ and $\epsilon_2 = exp(j\pi/r)$ and $\nu = 0, 1, \ldots, p-1$, $\nu' = 0, 1, \ldots, (s-1)$ and $\mu = 0, 1, \ldots, (q-1)$. The integers p, s, q satisfy the following relation: $2n = qp$ and $2r = qs$. The integer d must be relatively prime to q. Here we have freedom to choose the phase values freely.

Type - II finite unitary group

The elements of one such Type-II finite unitary group with $4nr$ elements is generated as follows

$$(\epsilon^{\nu}\omega^{-\mu}, 0)\text{and}(0, -\epsilon^{\nu}\omega^{\mu})$$

where $\epsilon = exp(j\pi/n)$ and $\omega = exp(j\pi/r)$ and $\nu = 0, 1, \ldots, (n-1)$ and $\mu = 0, 1, \ldots, (2r-1)$. These codes have the same structure as dicyclic groups but the phase can be chosen independently.

Type - III finite unitary group

Consider the group with 24 elements in the unitary plane is generated by

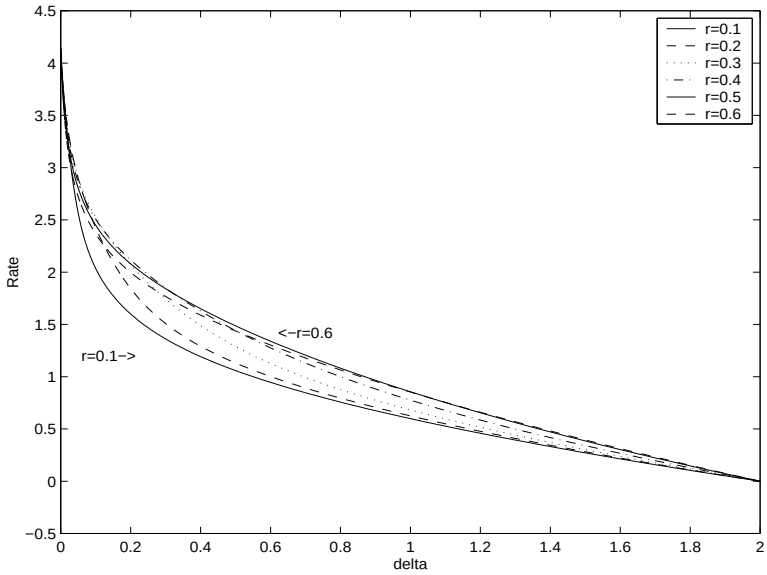


Figure 3.4: $EEUB$ for 64-point Massey signal set for different r.

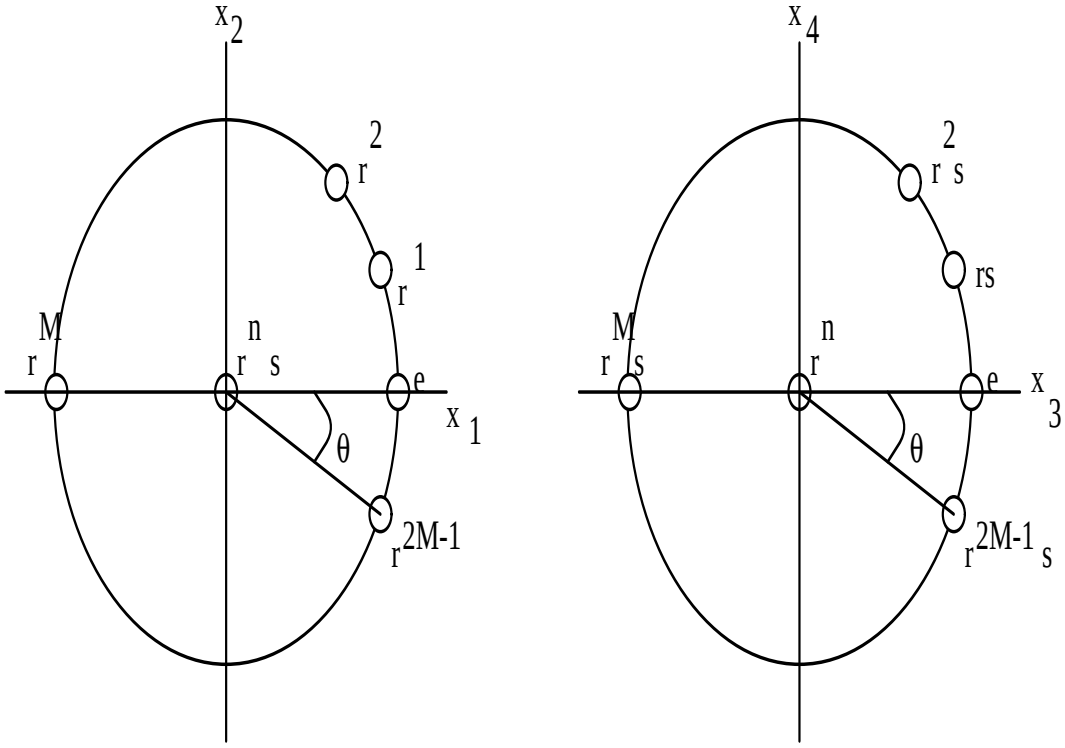


Figure 3.5: Signal set matched to dicyclic group.

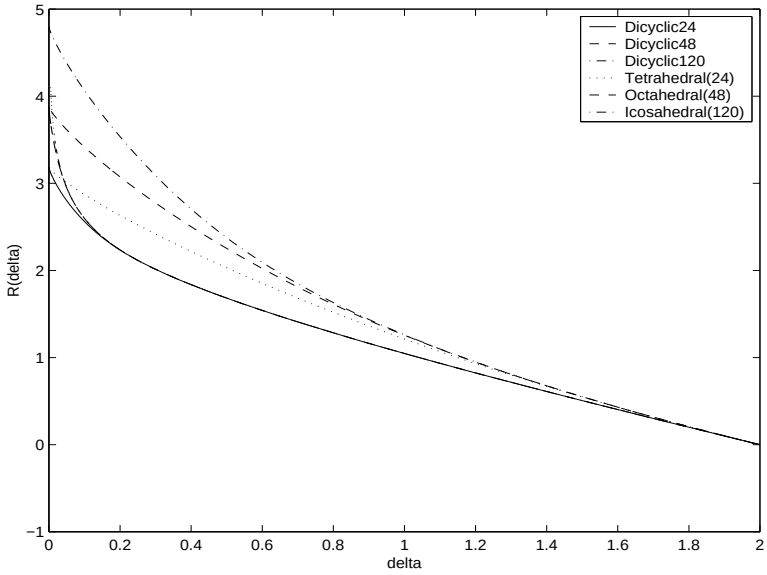


Figure 3.6: $EEUB$ for signal sets matched to $DC_{24}, DC_{48}, DC_{120}$, Binary tetrahedral, octahedral and icosahedral groups.

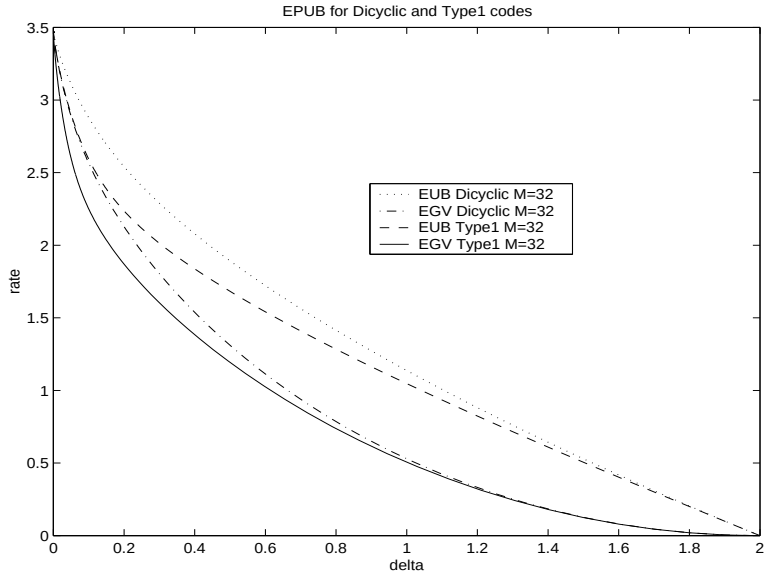


Figure 3.7: The figure shows the $EEUB$ and EGV for codes over 32-point Type(1) signal set and 32 point Dicyclic signal set.

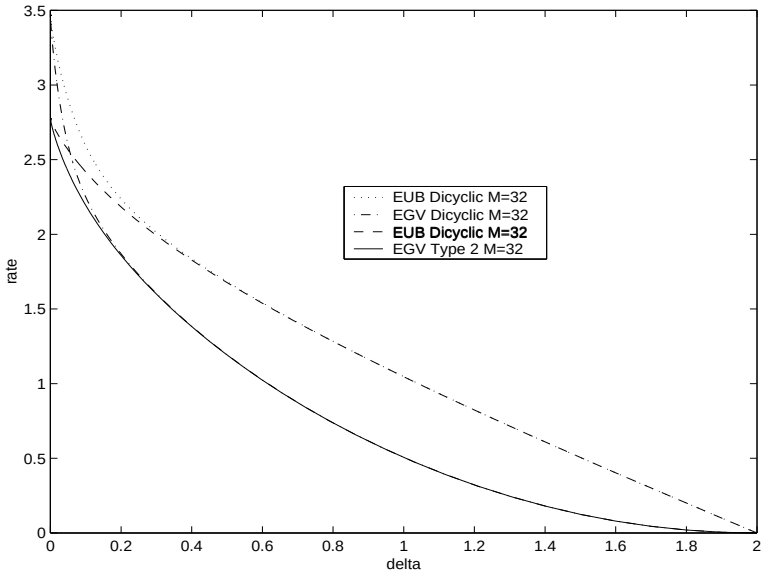


Figure 3.8: The figure shows the $EEUB$ and EGV for codes over 32-point Type(2) signal set and 32 point Dicyclic signal set.

- $(jcos(\alpha)\epsilon^{2\nu}, sin(\alpha)\epsilon^{2\nu})$,
- $(-cos(\alpha)\epsilon^{2\nu}, -jsin(\alpha)\epsilon^{2\nu})$,
- $(-sin(\alpha)\epsilon^{2\nu+1}, jcos(\alpha)\epsilon^{2\nu+1})$
- and $(jsin(\alpha)\epsilon^{2\nu+1}, -cos(\alpha)\epsilon^{2\nu+1})$

where α is any chosen angle, $\epsilon = e^{j(\frac{\pi}{6})}$ and $\nu = 0, 1, \ldots, 5$.

Type - IV finite unitary group

An example of Type-IV finite unitary group with 16 elements is as follows. The eight elements of the the group are σG_0, where G_0 is the eight element quaternion group and $\sigma = jcos(\alpha) + ksin(\alpha)$. The other eight elements of the group are $j\sigma G_0 e^{(j\frac{\pi}{4})}$. This form a 16 element Type-II finite unitary group.

Type(I)	Type(II)	Type(III)
64	64	48
-16	-16	-12
-16	-16	-12
-16	-16	-12
-16	-16	-12

Table 3.2: The table shows the non-zero eigenvalues of squared Euclidean distance distribution matrix S for Type(I), Type(II) and Type(III) finite unitary groups. Here we consider codes over Type(I) group of cardinality 32, Type(II) code with cardinality 32 and Type(III) group with cardinality 24.

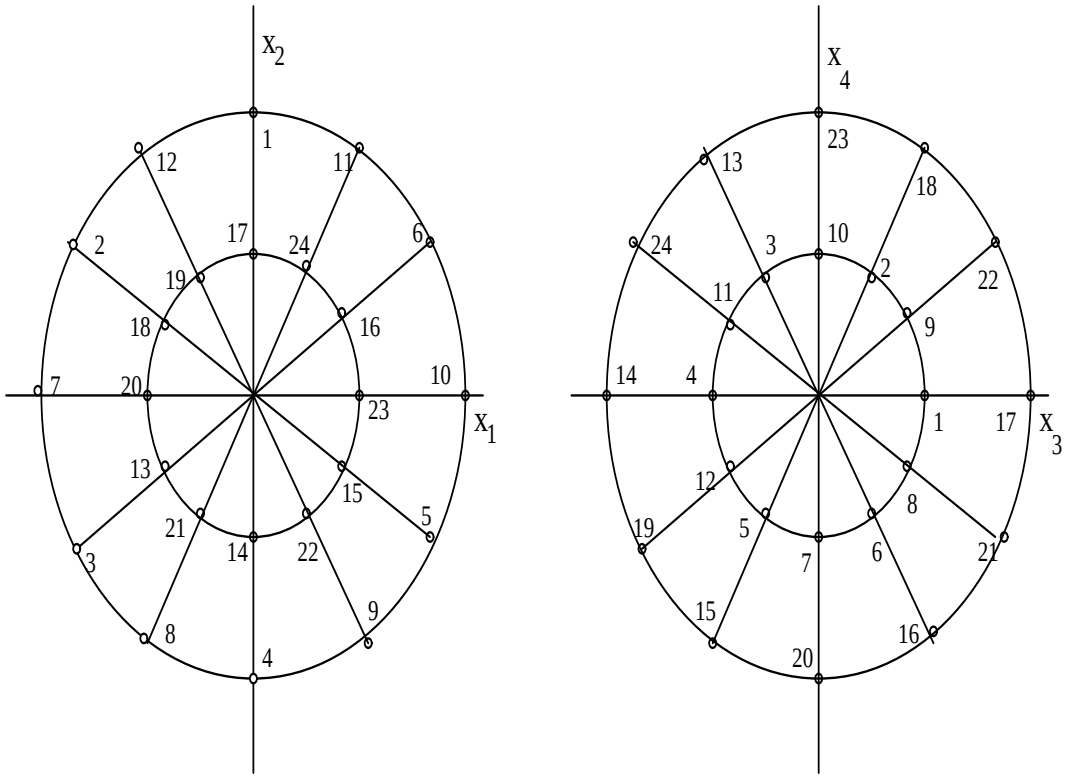


Figure 3.9: The figure shows an example of Type-(III) finite unitary group with 24 points in four dimensional space.

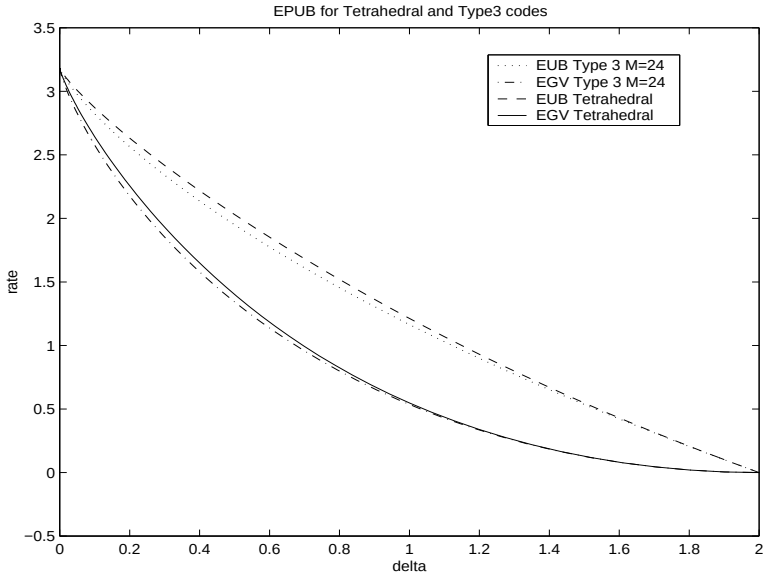


Figure 3.10: The figure shows the $EEUB$ and EGV for codes over 24-point Type(3) signal set and tetrahedral signal set.

Type - V finite unitary group

Consider the binary octahedral group with 48 elements. Choose a σ in the four dimensional unit sphere. The corresponding elements are $\sigma\chi^{-1}$ and $j\sigma\chi^{-1}$ where χ is one of the first 24 elements of the binary octahedral group. The order of this Type-IV group is also 48.

Type - VI finite unitary group

We consider an Type(VI) group with 24 elements. Let σ be an element of the unit sphere in four dimensions. The elements are $\sigma\chi^{-1}$, $\epsilon\sigma\lambda^{-1}$ and $\epsilon^2\sigma\mu^{-1}$, where $\epsilon = e^{j(\frac{\pi}{3})}$, χ is an element of the quaternion group, $\lambda \in \omega G_o$ and $\mu \in \omega^2 G_o$ with $\omega = \frac{1}{2}(e + j + k + l)$.

Type - VII finite unitary group

Consider an example of finite unitary group with 96 elements. Let σ be an element of the unit sphere in four dimensions. The elements are $\sigma\chi^{-1}$ and $j\sigma\chi^{-1}$, where χ is an arbitrary element of the binary octahedral group. Thus the 96 element group is completely

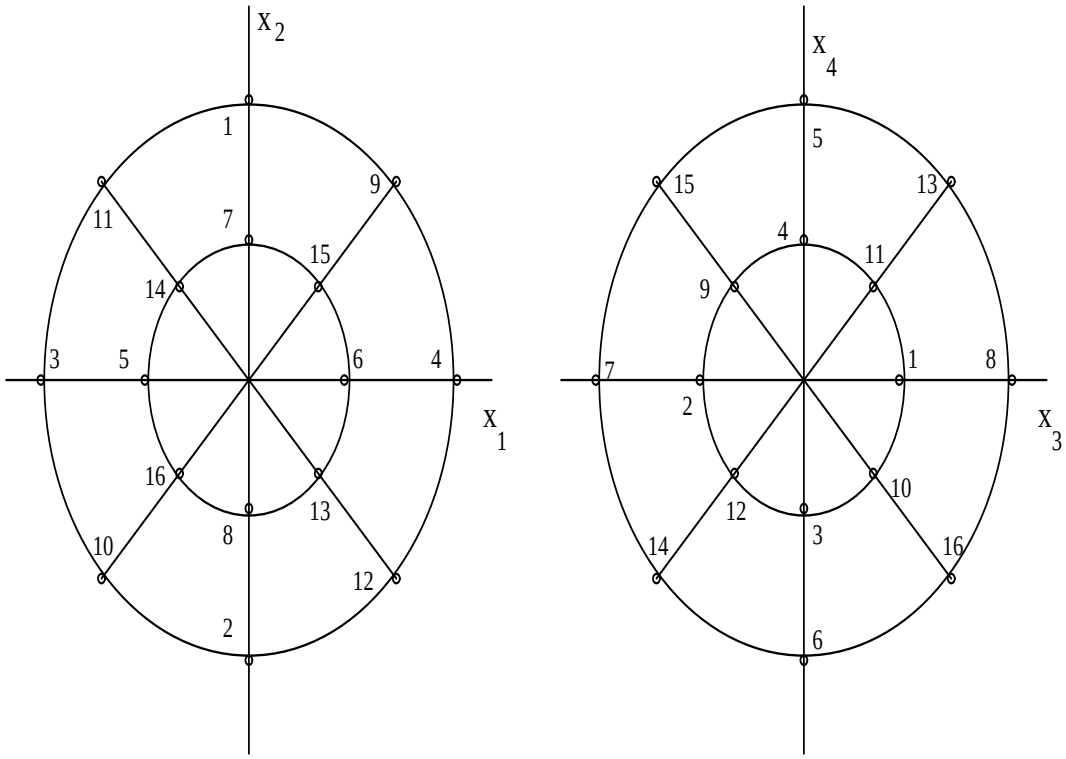


Figure 3.11: The figure shows an example of Type-(IV) finite unitary group with 16 points in four dimensional space.

Type(IV)	Type(V)	Type(VI)	Type(VII)
32	96	48	192
-8	-24	-12	-48
-8	-24	-12	-48
-8	-24	-12	-48
-8	-24	-12	-48

Table 3.3: The table shows the non-zero eigenvalues of squared Euclidean distance distribution matrix S for Type(IV), Type(V), Type(VI) and Type(VII) finite unitary groups. Here we consider codes over Type(IV) group of cardinality 16, Type(V) code with cardinality 48, Type(VI) group with cardinality 24 and Type(VII) group with cardinality 96.

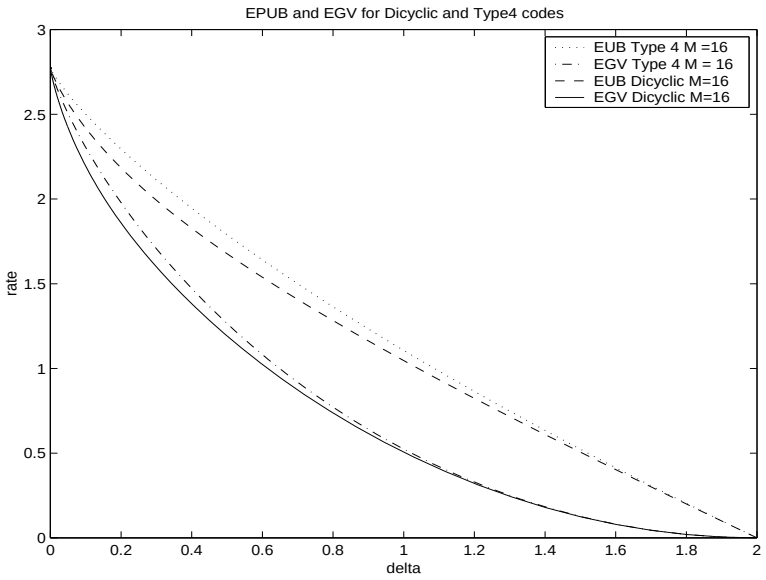


Figure 3.12: The figure shows the $EEUB$ and EGV for codes over 16-point Type(4) signal set and 16 point Dicyclic signal set.

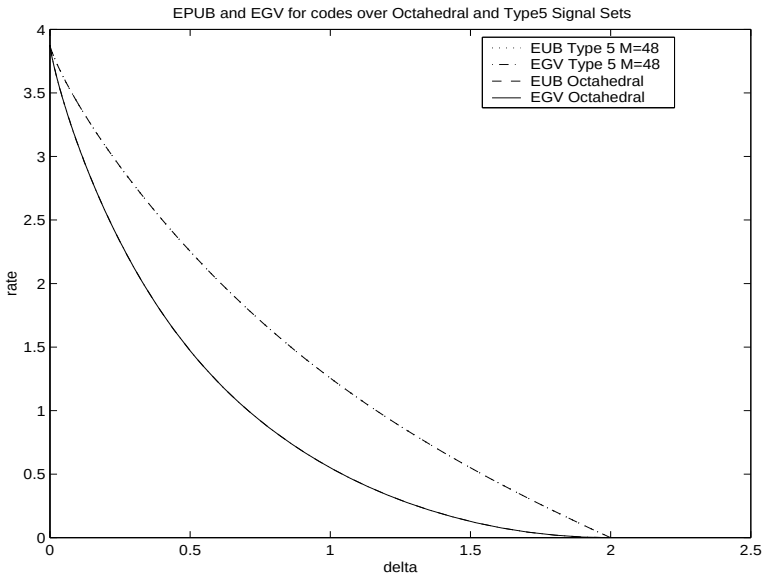


Figure 3.13: The figure shows the $EEUB$ and EGV for codes over 48-point Type(5) signal set and octahedral signal set.

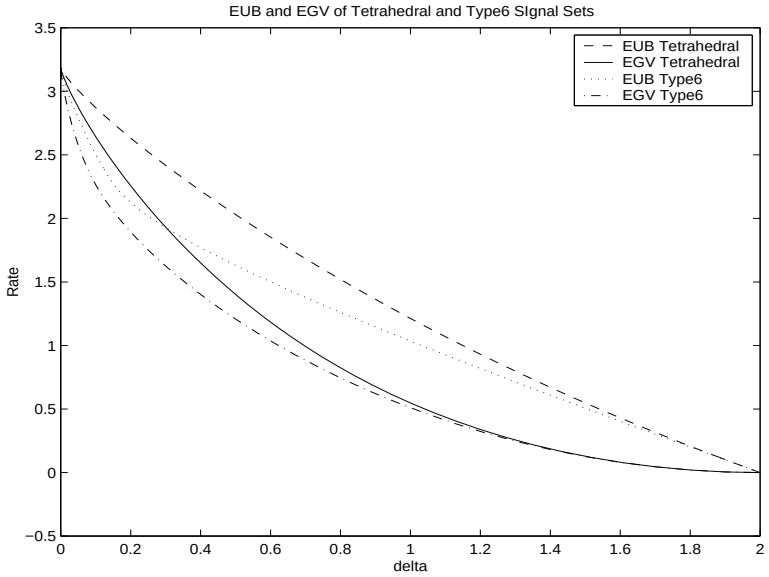


Figure 3.14: The figure shows the $EEUB$ and EGV for codes over 24-point Type(6) signal set and tetrahedral signal set.

characterized.

3.3.5 Comparison of the Bounds for codes over Finite Unitary Groups

The generators of finite unitary groups offer possibilities for independently varying the phase. Therefore it is interesting to compare the $EEUB$ and extended Gilbert Varshamov bound (EGV) of codes over finite unitary group with codes over mutlidimensional signal sets.

Codes over Type(I) signal sets have tighter lower bound when compared to codes over dicyclic signal set. The Upper bound of codes over dicyclic group is tighter than that of codes over Type(1) signal sets. This is shown in figure(3.7).

We compare the bounds for codes over Type(II) signal sets and dicyclic signal sets in figure(3.8). In double prism group, Type(I) and Type(II) groups we can see that there is greater independence to choose the phase values when compared to dicyclic groups. Here again we get a tighter lower bound for codes over Type(II) signal sets. The upper bound is tighter for codes over dicyclic groups. In the figure(3.10) we compare the bounds for codes

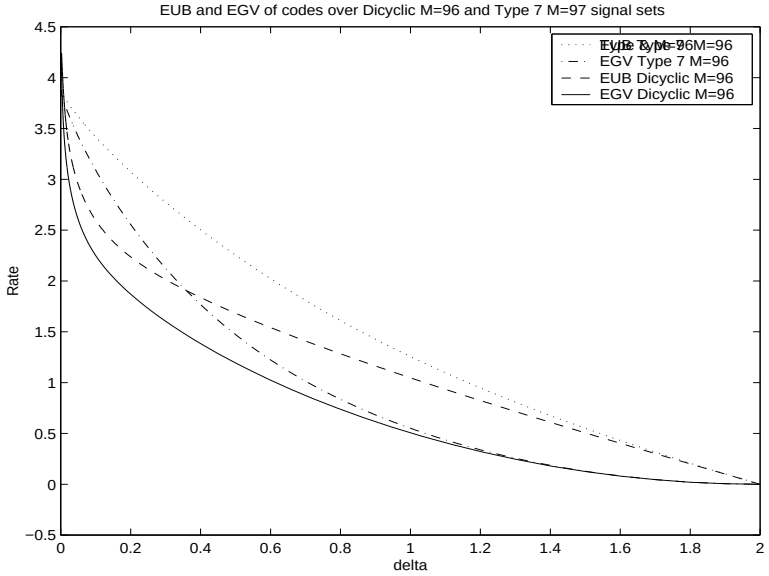


Figure 3.15: The figure shows the $EEUB$ and EGV for codes over 96-point Type(7) signal set and 96 point Dicyclic signal set.

over Type(III) signal sets and codes over tetrahedral group. Here codes over tetrahedral group have a tighter lower bound and looser upper bound.

In figure(3.12) a comparison of bounds of codes over Type(IV) and dicyclic signal sets is shown. Here codes over dicyclic signal sets have a tighter upper bound and a looser lower bound. Figure(3.13) shows the lower and upper bounds for codes over Type(V) groups and octahedral groups. The codes over both the groups have a comparable bounds.

Figure(3.14) show the bounds for codes over Type(VI) groups and tetrahedral group. The codes over Type(VI) groups have a tighter upper bound and a looser lower bound. Figure(3.15) compares the bounds for codes over Type(VII) signal sets and codes over dicyclic signal sets.

We also see that the codes over double prism have tighter lower bound when compared with codes over dicyclic group. The upper bound of codes over dicyclic group is tighter than that of codes over double prism group. This is shown in figure(3.24).

3.3.6 Slepian Signal Sets

In [53] Slepian gives two signal sets. One of them has the property that the distance distribution remains same from all elements of the signal set and that it is not a group code. An example of a signal set which is distance uniform but not matched to a group. We compute the extended lower bound, [56] and the $EEUB$ for codes over this signal set. Figure(3.16) gives the upper and lower bound.

Slepian also gives an example of a signal set with cardinality M but does not posses a transitive symmetry group of order M. In [37] it is shown that this signal set is matched to a group. The signal points in the case of both Slepian signal set have the same energy. Therefore the conditions discussed in section(3.2.2) are valid. We check whether the equation(3.5) satisfies equation(3.3).

Slepian (I)	Slepian(II)
-2.4493	-4
-2.721	-4
-1.463	-4
-0.323	-4
-0.144	-4
6.6520	20

Table 3.4: The table shows the non-zero eigenvalues of squared Euclidean distance distribution matrix S for Slepian(I) - a signal set in six dimensions with six points and Slepian(II)- a signal set in five dimensions with ten points.

From table(3.3.6) we see that all eigenvalues of S matrix other than the primary eigenvalue are non-positive. Therefore maximizing the constrained optimization problem reduces to finding a solution of equation(3.3). We verify that the distribution function given in equation(3.5) satisfies the equation(3.3).

For these two signal sets we compute the extended lower [56] and the extended upper bounds. Figure(3.17) shows the upper and lower bounds for the 5 dimensional signal set with cardinality 10.

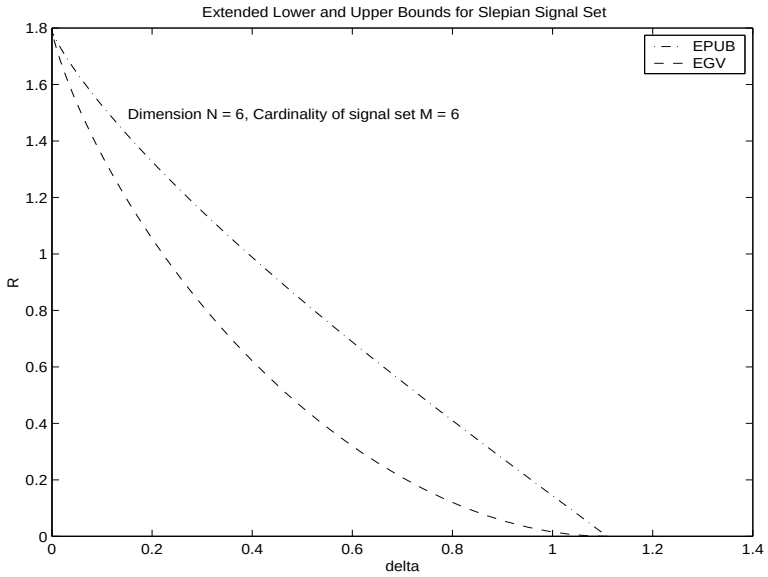


Figure 3.16: Extended upper and lower bounds for Slepian signal set in 6 dimensions with $M = 6$

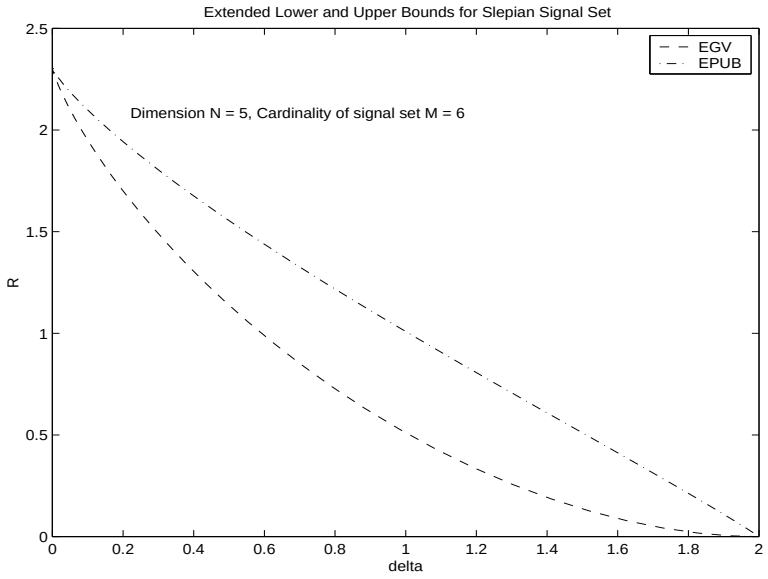


Figure 3.17: Extended upper and lower bounds for Slepian signal set in 5 dimensions with $M = 10$

3.3.7 Codes over n Dimensional Cube

The set of points which constitute an n-dimensional cube can be represented as the set of n-tuples $x = (\pm 1, \pm 1, \ldots, \pm 1)$. In 2 dimensions these are set of corners of a square. In three dimensions the set of vertices of the cube. We order the vertices (represented as n-tuples) in such a way that the Hamming distance of any two successive n-tuples is one(we consider gray encoding).

Example 3.3 *In the two dimensional case the vertices (2-tuples) are ordered as follows (gray encoding)*

$$[(0,0),(0,1),(1,1),(1,0)]$$

The distance distribution matrix is (d_{ij} is the squared Euclidean distance between the i-th element of the signal set and j-th element of the signal set)

$$\begin{bmatrix} 0 & 1 & 2 & 1 \\ 1 & 0 & 1 & 2 \\ 2 & 1 & 0 & 1 \\ 1 & 2 & 1 & 0 \end{bmatrix} \tag{3.36}$$

Note that this is a circulant matrix. □

Example 3.4 *In the case of 3 dimensional cube the vertices (3-tuples) are ordered as follows:*

$$[(0,0,0),(0,0,1),(0,1,1),(0,1,0),(1,1,0),(1,1,1),(1,0,1),(1,0,0)]$$

The distance distribution matrix is

$$\begin{bmatrix} 0 & 1 & 2 & 1 & 2 & 3 & 2 & 1 \\ 1 & 0 & 1 & 2 & 3 & 2 & 1 & 2 \\ 2 & 1 & 0 & 1 & 2 & 1 & 2 & 3 \\ 1 & 2 & 1 & 0 & 1 & 2 & 3 & 2 \\ 2 & 3 & 2 & 1 & 0 & 1 & 2 & 1 \\ 3 & 2 & 1 & 2 & 1 & 0 & 1 & 2 \\ 2 & 1 & 2 & 3 & 2 & 1 & 0 & 1 \\ 1 & 2 & 3 & 2 & 1 & 2 & 1 & 0 \end{bmatrix} \tag{3.37}$$

The above matrix can be obtained from the following two matrices

$$A = \begin{bmatrix} 0 & 1 & 2 & 1 \\ 1 & 0 & 1 & 2 \\ 2 & 1 & 0 & 1 \\ 1 & 2 & 1 & 0 \end{bmatrix} \tag{3.38}$$

As noted in the earlier example A is a circulant matrix.

$$B = \begin{bmatrix} 2 & 3 & 2 & 1 \\ 3 & 2 & 1 & 2 \\ 2 & 1 & 2 & 3 \\ 1 & 2 & 3 & 2 \end{bmatrix} \tag{3.39}$$

Note that B is anti circulant matrix. Therefore the distance distribution matrix S can be written as a block circulant matrix with blocks A and B.

$$\begin{bmatrix} A & B \\ B & A \end{bmatrix} \tag{3.40}$$

The distance distribution matrix S is a block circulant matrix with component circulant and anti circulant matrices. Also note that $B_{ij} = A_{i(4-j+1)} + 1$ where $1 \leq j \leq 4$. Therefore the A matrix completely describes the distance distribution matrix. This follows from the iterative construction of gray codes, i.e., construct a 3 bit code from a 2 bit code and so on construct the n-bit code. □

An n-bit gray encoding can be summarized as follows: Consider the $(n-1)$ bit gray code. Let the $(n-1)$ bit gray code be the ordered sequence of $(n-1)$ tuples $(\underline{a_0}, \underline{a_1}, \ldots, \underline{a_{2^{(n-1)}-1}})$. Then the n-bit gray code is the ordered sequence of n-tuples obtained as follows

$$\Big[(0, \underline{a_0}), (0, \underline{a_1}), \ldots, (0, \underline{a_{2^{(n-1)}-1}}), (1, \underline{a_{2^{(n-1)}-1}}), (1, \underline{a_{2^{(n-1)}-2}}), \ldots, (1, \underline{a_1}), (1, \underline{a_0})\Big]$$

The distances $[d_{0,1}, d_{0,2}, \ldots, d_{0,2^{n-1}-1}]$ are common for the $(n-1)$-tuple gray code and n-tuple gray code. The remaining distances in the cases of an n-tuple gray code are

$$[d_{0,2^{n-1}} = d_{0,2^{n-1}-1} + 1, d_{0,2^{n-1}+1} = d_{0,2^{n-1}-2} + 1, \ldots, d_{0,2^n-1} = d_{0,0} + 1]$$

In general distance distribution matrix S of an n-dimensional cube can written as a block circulant matrix as follows:

$$\begin{pmatrix} A_1 & A_2 & A_3 & A_4 & \dots & A_{2^{n-2}} \\ A_{2^{n-2}} & A_1 & A_2 & A_3 & \dots & A_{2^{n-2}-1} \\ A_{2^{n-2}-1} & A_{2^{n-2}} & A_1 & A_2 & \dots & A_{2^{n-2}-2} \\ \vdots & \vdots & \vdots & \ddots & \dots & \vdots \\ A_{2^{n-3}} & A_{2^{n-3}+1} & A_{2^{n-3}+2} & A_{2^{n-3}+3} & \dots & A_1 \end{pmatrix} \tag{3.41}$$

where each A_i is (4×4) block circulant matrix. Here we see that the i-th column of each (4×4) matrix is related to the other blocks as follows $A_{2_{ij}} = A_{1_{i(4-j+1)}} + 1$ where $1 \leq j \leq 4$. Similarly $A_{3_{ij}} = A_{2_{i(4-j+1)}} + 1$ where $1 \leq j \leq 4$ and $A_{4_{ij}} = A_{1_{i(4-j+1)}} + 1$ where $1 \leq j \leq 4$. Therefore in general $A_{(2^l+k)_{ij}} = A_{(2^l-k+1)_{i(4-j+1)}} + 1$ where $1 \leq j \leq 4$. Each A_i for i even is a anti circulant matrix and for i odd A_i is a circulant matrix.

Example 3.5 *Consider the the* 4 *dimensional cube the distance distribution matrix is*

$$\begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_4 & A_1 & A_2 & A_3 \\ A_3 & A_4 & A_1 & A_2 \\ A_2 & A_3 & A_4 & A_1 \end{pmatrix} \tag{3.42}$$

where each A_i *is a* (4×4) *matrix.*

$$A_1 = \begin{pmatrix} 0 & 1 & 2 & 1 \\ 1 & 0 & 1 & 2 \\ 2 & 1 & 0 & 1 \\ 1 & 2 & 1 & 0 \end{pmatrix} \tag{3.43}$$

$$A_2 = \begin{pmatrix} 2 & 3 & 2 & 1 \\ 3 & 2 & 1 & 2 \\ 2 & 1 & 2 & 3 \\ 1 & 2 & 3 & 2 \end{pmatrix} \tag{3.44}$$

$$A_3 = \begin{pmatrix} 2 & 3 & 4 & 3 \\ 3 & 2 & 3 & 4 \\ 4 & 3 & 2 & 3 \\ 3 & 4 & 3 & 2 \end{pmatrix} \tag{3.45}$$

$$A_4 = \begin{pmatrix} 2 & 3 & 2 & 1 \\ 3 & 2 & 1 & 2 \\ 2 & 1 & 2 & 3 \\ 1 & 2 & 3 & 1 \end{pmatrix} \tag{3.46}$$

□

The distance achieving distribution for codes over n dimensional cubes can be derived starting from the equation(3.3). For n-dimensional cube the number of distinct distances between the elements of the signal set is n. The number signal points at a Hamming distance of i is given by

$$\binom{n}{i} \tag{3.47}$$

The squared Euclidean distance is a constant multiple of the Hamming distance between the elements of the signal set.

Lemma 3.0.1 *For Euclidean space codes over three dimensional cube the distribution given by* $\{\beta_0(\mu), \beta_1(\mu), \ldots, \beta_{M-1}(\mu)\}$*, where* $\beta_r(\mu) = \frac{e^{-\mu d^2(r)}}{\sigma_{s=0}^{M-1} e^{-\mu d^2(r)}}$ *(equation(3.5)) is optimal.*

Proof: Consider the case of three dimensional cube. The structure of the distance distribution matrix can be used for finding a solution to equation(3.3). From the distance distribution matrix given in example(3.4) for 3 dimensional cube it follows that $\underline{\beta} = \{\beta_0, \beta_1 = \beta_3 = \beta_7, \beta_2 = \beta_4 = \beta_6, \beta_5\}$. Therefore we need to solve equation(3.3) for only $r = 1, 2, 5$. For $r = 1$. Therefore equation(3.3) can be written as

$$\frac{\partial \Phi(\underline{\beta}, \lambda)}{\partial \beta_1} = \log(\beta_0) - \log(\beta_1) + 2\lambda(\beta_0 + \beta_1 - \beta_2 - \beta_5) \tag{3.48}$$

$$\frac{\partial\Phi(\underline{\beta},\lambda)}{\partial\beta_2} = \log(\beta_0) - \log(\beta_2) + 4\lambda(\beta_0+\beta_1-\beta_2-\beta_5) \tag{3.49}$$

$$\frac{\partial\Phi(\underline{\beta},\lambda)}{\partial\beta_3} = \log(\beta_0) - \log(\beta_3) + 3\lambda(\beta_0+\beta_1-\beta_2-\beta_5) \tag{3.50}$$

Equating equation(3.48), equation(3.49) and equation(3.50) to zero and simplifying we get the following relationships

$$\beta_1^2 = \beta_2\beta_0 \tag{3.51}$$

$$\beta_1^3 = \beta_5\beta_0^2 \tag{3.52}$$

We can easily verify that

$$\beta_r(\mu) = \frac{e^{-\mu d^2(r)}}{\sum_{s=0}^{M-1} e^{-\mu d^2(s)}} \quad r = 0,1,2,\cdots,M-1 \tag{3.53}$$

satisfy the above relationship among β_0, β_1, β_2 and β_5. Thus we have an optimal distribution for three dimensional cube. □

Lemma 3.0.2 *For Euclidean space codes over four dimensional cube the distribution given by* $\{\beta_0(\mu),\beta_1(\mu),\ldots,\beta_{M-1}(\mu)\}$, *where* $\beta_r(\mu) = \frac{e^{-\mu d^2(r)}}{\sigma_{s=0}^{M-1} e^{-\mu d^2(r)}}$ *(equation(3.5)) is optimal.*

Proof: Consider the case four dimensional cube. The distance distribution matrix is given in example(3.5). Here $\underline{\beta} = \{\beta_0,\beta_1=\beta_3=\beta_7=\beta_{15},\beta_2=\beta_4=\beta_6=\beta_8=\beta_{12}=\beta_{14},\beta_5=\beta_9=\beta_{11}=\beta_{13}\}$. Therefore we need to solve the equation(3.3) for only $r = 1,2,5,10$. As in the case of 3 dimensional cube the analysis leads to the following relationships

$$\beta_1^2 = \beta_2\beta_0 \tag{3.54}$$

$$\beta_1^3 = \beta_5\beta_0^2 \tag{3.55}$$

$$\beta_1^4 = \beta_{10}\beta_0^3 \tag{3.56}$$

We can easily verify that

$$\beta_r(\mu) = \frac{e^{-\mu d^2(r)}}{\sum_{s=0}^{M-1} e^{-\mu d^2(s)}} \quad r = 0,1,2,\cdots,M-1 \tag{3.57}$$

satisfy the above relationship among β_0, β_1, β_2, β_5 and β_{10}. Thus we have an optimal distribution Euclidean space codes over four dimensional cube. □

In general for an n dimensional cube we can carry out the analysis similar to that of 3 and 4 dimensional cubes. Also the structure of the distance distribution matrix remains same for any n-dimensional cube. In the case of n-dimensional cube there are n distances between the elements of the signal set. It can be easily verified that following relation holds for n-dimensional cube, for any chosen value of n

$$\beta_1^{\frac{d_{0i}}{d_{01}}} = \beta_i \beta_0^{\frac{d_{0i}}{d_{01}}-1} \tag{3.58}$$

$$\tag{3.59}$$

Therefore for n-dimensional cube an optimal distribution is given by equation(3.5).

3.3.8 Comparison of Signal Sets Based on the Spectral Rate

For band-limited applications, the rate of the code per dimension is the appropriate parameter based on which signal sets are to be compared. To facilitate this we measure the rate of the code per two dimensions, i.e.

$$\frac{2}{N} R(C) = \frac{2}{Nn} ln \mid C \mid \tag{3.60}$$

and call it the spectral rate (rate in bits per symbol per two dimensions) of the code. In this subsection, we compare the signal sets based on the spectral rate.

Figure(3.18) shows the normalized $EEUB$ bound for the Massey signal set with eight elements, N-dimensional cube, and the signal set matched to DC_{16}. Notice that the comparison is made among signal sets of different sizes in different dimensions but having the same number of signal points per dimension. For the Massey signal set, the parameter r is chosen to be 0.6. It is seen from the figure(3.18), that the DC_{16} gives a better normalized bound compared to the other two.

In particular, 4-SPSK has a better bound than the Massey signal set with eight points. However, this superiority of the SPSK signal set over the corresponding Massey signal set is not true in general. For instance, the Massey signal set with 64 points is superior in comparison to the 16-SPSK signal set. This is demonstrated in figure(3.19). However, the supremacy of dicyclic groups over the corresponding signal sets matched to the Massey signal set and the SPSK signal set holds in this case as well. Note that the value of r that

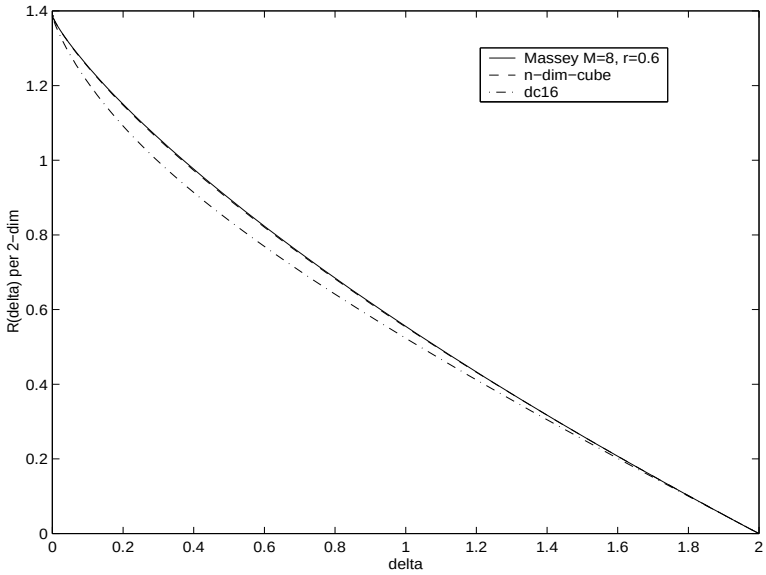


Figure 3.18: $EEUB$ for Massey signal set M=8, r=0.6, n-dimensional cube and dicyclic signal set with 16 elements

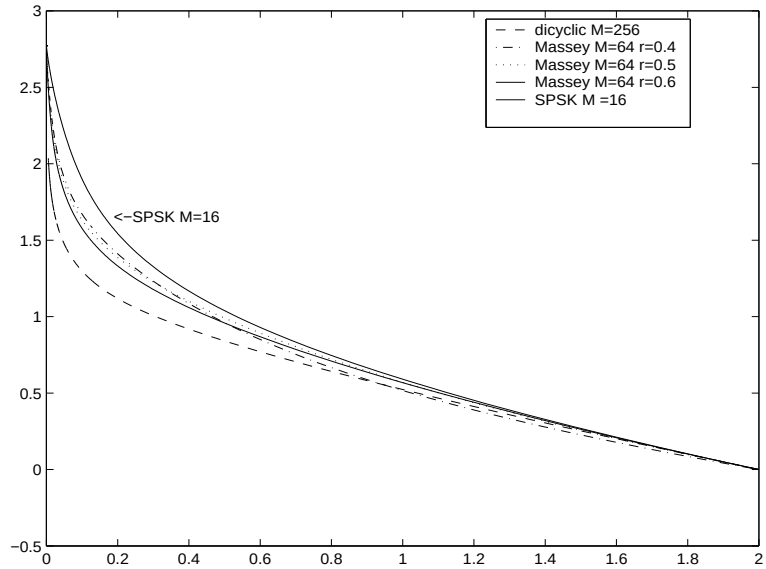


Figure 3.19: The figure shows $EEUB$ for 16-SPSK, 64 point Massey signal set for r = 0.6, 0.5, 0.4 and dicyclic signal set with 256 elements. In these two figures we have the rate per 2 dimensions along y-axis and delta along x-axis.

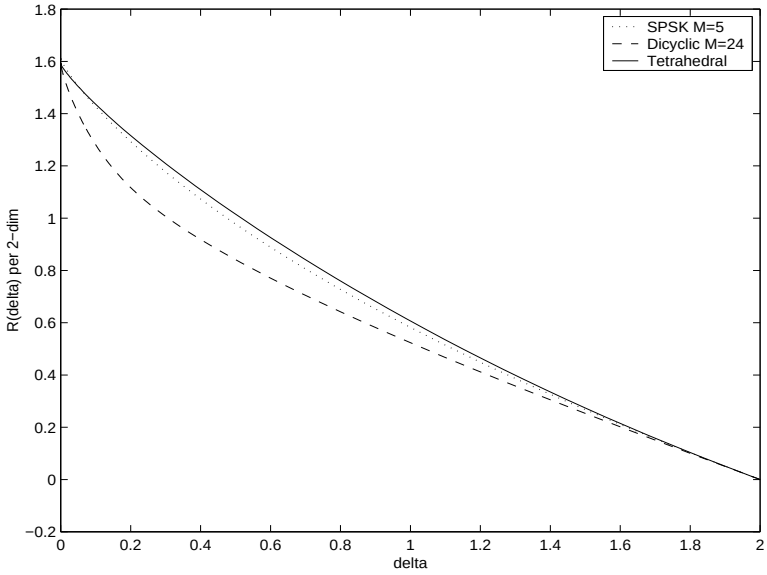


Figure 3.20: The figure shows $EEUB$ of 5 PSK, tetrahedral signal set and dicyclic signal set with 24 points.

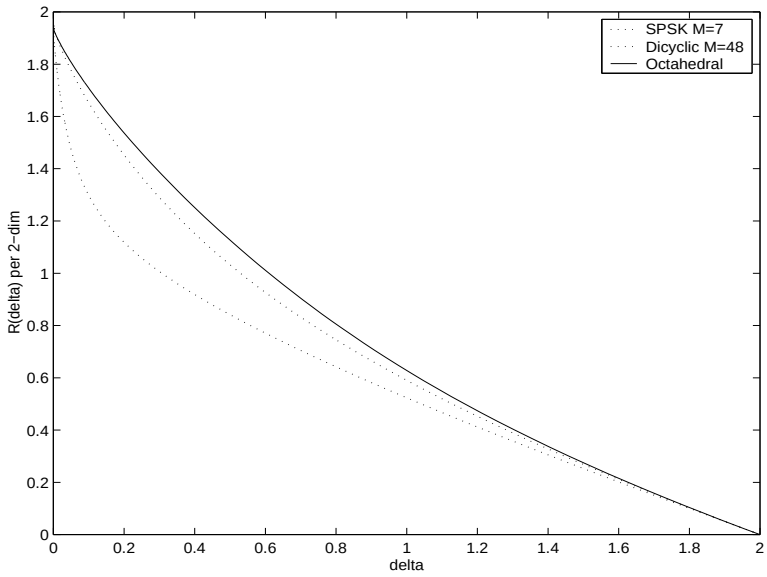


Figure 3.21: $EEUB$ for 7 PSK, octahedral signal set and dicyclic signal set with 48 points. In these two figures we have the rate per 2 dimensions along y-axis and delta along x-axis.

gives the best bound for the 64-point Massey signal set is not unique; depending on the value of δ it varies. The 16-SPSK gives a larger value for spectral rate for all values of δ. Figure(3.20) shows the $EEUB$ bound for a spectral rate of signal sets matched to G_{24} and DC_{24}. The bound corresponding to 5-SPSK is also shown. Note that the 5-SPSK signal set has a slightly lower rate. It has 25 points in four dimensions compared to 24 for the other two signal sets considered. The signal set matched to G_{24} gives a looser bound than the 5-SPSK signal set. Clearly, G_{24} gives larger values compared to signal sets matched to DC_{24}. Similar bounds for comparison between signal sets matched to G_{48}, DC_{48}, and the closest SPSK signal set, 7-SPSK, are shown in figure(3.21), leading to a similar conclusion. The closest SPSK signal set that can be compared with signal sets matched to G_{120} and DC_{120} is the 11-SPSK signal set. Figure(3.22) shows the bounds for these signal sets with an identical conclusion.

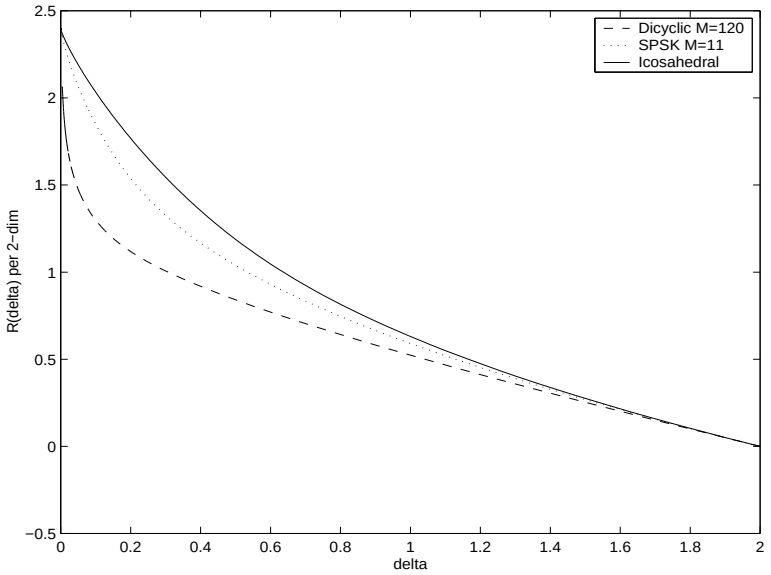


Figure 3.22: (a). The figure shows $EEUB$ of 11 PSK, icosahedral signal set and dicyclic signal set with 120 points.

3.4 Conclusion

In this chapter we have obtained an optimum distribution for a set distance uniform signal sets. We have also shown that the quadratic form $\underline{\beta} S \underline{\beta}^T$ is concave for all distance

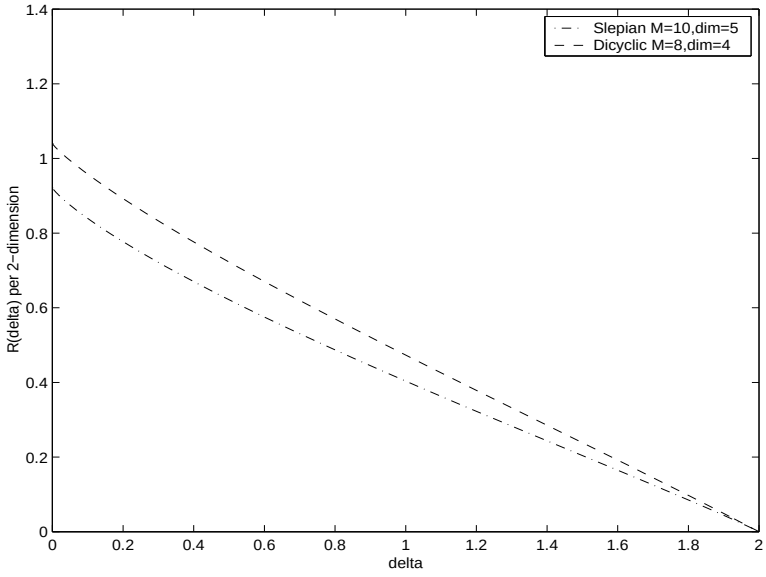


Figure 3.23: The figure shows $EEUB$ of 11 PSK, icosahedral signal set and dicyclic signal set with 120 points.

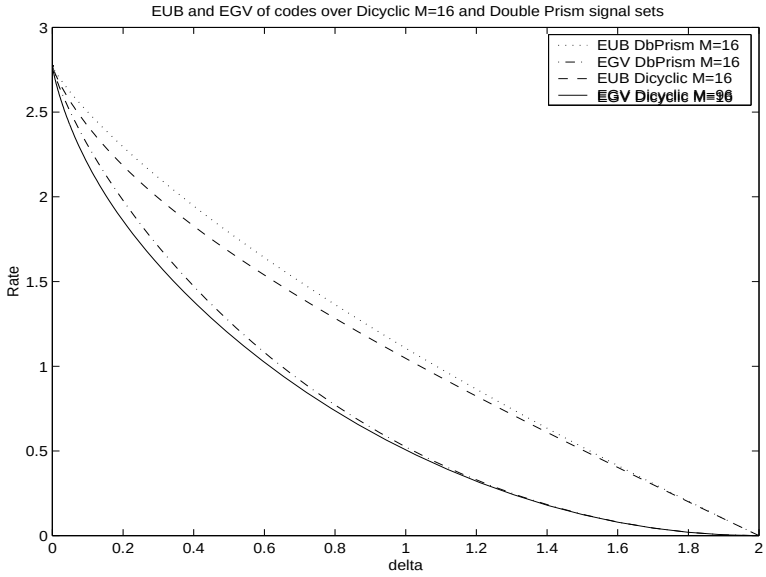


Figure 3.24: The figure shows the $EEUB$ and EGV for codes over 32-point double prism signal set and 16 point Dicyclic signal set.

uniform signal sets. Optimum distribution remains similar for all these signal sets. In the case PSK, Massey, dicyclic and signal sets over finite unitary groups we verified that the probability distribution given by equation(3.5) is optimum. Further, we conjecture that the optimum distribution for all distance uniform signal sets is similar to the optimum distribution obtained in this chapter.

Chapter 4

Matrix Characterization of Near-MDS codes

[1]

4.1 Introduction

The class of Near-MDS (NMDS)codes [15], [16], [17], [10] is obtained by weakening the restrictions in the definition of classical MDS codes. The support of a code C is the set of coordinate positions, where not all codewords of C are zero. The r-th generalized Hamming weight $d_r(C)$ of a code C is defined to be the cardinality of the minimal support of an (n, r) subcode of C, $1 \leq r \leq k$ [28], [29], [72]. Near-MDS ($NMDS$) codes are a class of codes where for an (n, k) code the i-th generalized Hamming weight $d_i(C)$ is $(n - k + i)$ for $i = 2, 3, \ldots, k$ and $d_1(C)$ is $(n - k)$. This class contains remarkable representatives as the ternary Golay code and the quaternary (11,6,5) and (12,6,6) codes as well as a large class of Algebraic Geometric codes. The importance of NMDS codes is that there exist NMDS codes which are considerably longer than the longest possible MDS codes for a given size of the code and the alphabet. Also, these codes have good error detecting capabilities [17].

It is well known that a linear MDS code can be described in terms of its systematic generator matrix as follows: If $[I \mid P]$ is the generator matrix then every square submatrix of P is

[1] The results of this chapter also appear in [65] and [66]

nonsingular. In this chapter, we obtain a similar characterization for the class of NMDS codes. Also, using a general property of generalized Hamming weights, we point out that an algebraic geometric code over an elliptic curve, if not MDS is necessarily NMDS.

4.2 Preliminaries

In this section we present the known results concerning NMDS codes and generalized Hamming weight hierarchy that will be used in the following sections.
A Near-MDS code can be characterized in terms of either an arbitrary generator matrix or a parity check matrix of the code as follows [15]:
A linear $[n, k]$ code is NMDS iff a parity check matrix **H** of it satisfies the following conditions:

- any $n - k - 1$ columns of **H** are linearly independent
- there exists a set of $n - k$ linearly dependent columns in **H**
- any $n - k + 1$ columns of **H** are of rank $n - k$

A linear $[n, k]$ code is NMDS iff a generator matrix **G** of it satisfies the following conditions:

- any $k - 1$ columns of **G** are linearly independent
- there exists a set of k linearly dependent columns in **G**
- any $k + 1$ columns of **G** are of rank k

Several interesting properties of Hamming weight hierarchy are discussed in [72] and [29]. A basic property is that the sequence of Hamming weight hierarchy is strictly increasing, i.e.,

$$d_1(C) < d_2(C) < \ldots < d_k(C) = n. \tag{4.1}$$

The following result [72] relates the Hamming weight hierarchy of a code to that of its dual. If $C^{\perp}$ denotes the dual of the code C, then

$$\{d_r(C) \mid r = 1, 2, ..., k\} \bigcup \{n + 1 - d_r(C^{\perp}) \mid r = 1, 2.., n - k\}$$
$$= \{1, 2, ..., n\}.$$

4.3 Systematic Generator Matrix Characterization of NMDS Codes

Theorem Let $G = [I|P]$ be the systematic generator matrix of a linear non-MDS code C over a finite field. Then C is NMDS iff every $(g, g+1)$ and $(g+1, g)$ submatrix of P has at least one (g, g) nonsingular submatrix.

Proof: First we prove the 'if part'. We have to show that $d_1(C) = n - k$ and $d_2(C) = n-k+2$. Consider any one dimensional subcode generated by a minimum weight codeword $\underline{c}$ of C. In terms of linear combination of rows of G, let

$$\underline{c} = \sum_{j=1}^{g} \alpha_j \underline{r}_{i_j} \tag{4.2}$$

where $i_j \in \{1, 2, \ldots, k\}, j = 1, 2, \ldots, g$ and $\underline{r}_{i_j}$ is the i_j-th row of G.

The weight of $\underline{c}$ within the first k positions is g. We need to show that the weight in the last $n - k$ positions is $(n - k - g)$ or the number of zeros in the last $n - k$ positions is g. Let the number of zeros in the last $n - k$ positions of $\underline{c}$ be $\lambda > g$. Choose any $g + 1$ of these λ positions and let these positions be $j_1, j_2, \ldots, , j_{g+1}$. Then

$$\begin{bmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_g \end{bmatrix} \begin{bmatrix} r_{i_1 j_1} & r_{i_1 j_2} & \ldots & r_{i_1 j_{g+1}} \\ r_{i_2 j_1} & r_{i_2 j_2} & \ldots & r_{i_2 j_{g+1}} \\ \vdots & \vdots & \ldots & \vdots \\ r_{i_g j_1} & r_{i_g j_2} & \ldots & r_{i_g j_{g+1}} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \ldots & 0 \end{bmatrix}$$

Since there is a (g, g) nonsingular submatrix $\alpha_1 = \alpha_2 = \ldots \alpha_g = 0$, which is a contradiction. Hence $\lambda \leq g$ and $d_1 = n - k$. Notice that this means there can be at most one zero in each row of P.

To prove that $d_2(C) = n - k + 2$ consider a two dimensional subcode generated by two codewords $\underline{c}$ and $\underline{d}$. If the size of the union of supports of $\underline{c}$ and $\underline{d}$ is at least $n - k + 2$ then we are through. So, we need to consider the case where the support of both $\underline{c}$ and $\underline{d}$ is

within an identical set of $n-k+1$ locations. Let g of these locations be within the first k positions and let

$$\underline{c} = \sum_{j=1}^{g} \alpha_j \underline{r}_{i_j} \text{ and } \underline{d} = \sum_{j=1}^{g} \beta_j \underline{r}_{i_j}. \tag{4.3}$$

Consider an arbitrary linear combination of $\underline{c}$ and $\underline{d}$, i.e.,

$$\underline{e} = a\underline{c} + b\underline{d} = \sum_{j=1}^{g} (a\alpha_j + b\beta_j)\underline{r}_{i_j} \tag{4.4}$$

There are $g-1$ zeros in the last $n-k$ positions of e. Let these be $j_1, j_2, \ldots j_{g-1}$. Then we have

$$\begin{bmatrix} a\alpha_1 + b\beta_1 & \ldots & a\alpha_g + b\beta_g \end{bmatrix} \begin{bmatrix} r_{i_1 j_1} & r_{i_1 j_2} & \ldots & r_{i_1 j_{g-1}} \\ r_{i_2 j_1} & r_{i_2 j_2} & \ldots & r_{i_2 j_{g-1}} \\ \vdots & \vdots & \ldots & \vdots \\ r_{i_g j_1} & r_{i_g j_2} & \ldots & r_{i_g j_{g-1}} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \ldots & 0 \end{bmatrix}$$

Since every $(g, g-1)$ submatrix of P has a $(g-1, g-1)$ nonsingular submatrix, without loss of generality we assume the first $g-1$ rows to constitute this nonsingular submatrix and choose a and b such that $a\alpha_g + b\beta_g = 0$. Then it follows that $a\alpha_t + b\beta_t = 0$ for all $t = 1, 2, \ldots g-1$.

Now, if both α_g and β_g are non zeros, then $\underline{c}$ and $\underline{d}$ are scalar multiple of one another which means the code is one dimensional. Hence $d_2(C) = n-k+2$. (Note that from (4.1), $d_2(C) = n-k$ is not possible since $d_1(C) = n-k$.) If one of them is zero, say $\beta_g = 0$, then $a = 0$ and $b\beta_t = 0$ for all $t = 1, 2, \ldots g-1$ which is not true. This completes the proof for the if part.

To prove the 'only if' part: For $NMDS$ codes every $(k-1)$ columns of the generator matrix are linearly independent. This follows from the fact that for an $[n\ k]$ $NMDS$ code the dual code is also $NMDS$ and that the minimum distance of the dual code is k. Consider a set of $(k-1)$ columns of the generator matrix. If all the columns are from the P part of

the generator matrix, then since every $(k-1)$ columns are linearly independent we have a $(k-1, k-1)$ nonsingular submatrix.

If $k-g$ columns (say $j_1, j_2, \ldots j_{k-g}$) are from I and the rest $g-1$ columns from P, then let A denote the $(k, k-1)$ submatrix consisting of these columns. By suitable row exchanges and appropriate elementary column operations A can be brought to the form

$$\begin{bmatrix} \mathbf{0}_{g\times(k-g)} & \mathbf{A^*}_{g\times(g-1)} \\ \mathbf{I}_{(k-g)\times(k-g)} & \mathbf{0}_{(k-g)\times(g-1)} \end{bmatrix}.$$

Note that the column rank has not changed by these operations and the submatrix A^* is indeed a submatrix of A. Moreover, since the above matrix has column rank $k-1$ the submatrix A^* has column rank $g-1$ and hence contains a $(g-1, g-1)$ nonsingular submatrix. Therefore every $(g+1, g)$ submatrix of P has atleast one (g, g) nonsingular submatrix.

To show that every $(g, g+1)$ submatrix has atleast one (g, g) submatrix we make use of the fact that the minimum distance of the $NMDS$ code is $(n-k)$. Therefore for $NMDS$ codes every $(n-k-1)$ columns of the parity check matrix are linearly independent. The parity check matrix of the code can be written as $[-P^{\perp}\ \ I]$. Following the arguments for the systematic generator matrix we can see that every $(g+1, g)$ submatrix of $-P^{\perp}$ has atleast one (g, g) submatrix which is nonsingular. Therefore every $(g, g+1)$ submatrix of P submatrix has atleast one nonsingular (g, g) submatrix. This completes the proof. □

4.4 Discussion

In this chapter we have extended the well known $[I|P]$ matrix characterization of MDS codes to the class of Near-MDS codes. This characterization of NMDS codes will be helpful to obtain NMDS over finite fields. The matrix characterization of MDS codes finds application in constructing MDS codes for erasure channels [35], [35]. Based on the systematic matrix characterization of $NMDS$ codes we can see that if any $(k+1)$ locations of the n length codeword are known we can obtain all the k transmitted symbols. In a $[n,\ k]$ code, to add redundancy, for every k symbols transmitted additional $(n-k)$ parity symbols are transmitted. Based on the systematic matrix characterization we can see

that an $NMDS$ erasure code can recover the k transmitted packets from any of the $(k+1)$ of the n transmitted packets. This is useful in computer communications.

Chapter 5

Matrix Characterization of Near-MDS codes over Finite Abelian Groups

[1]

5.1 Introduction

In this chapter we study $AMDS$ and $NMDS$ codes over Z_m and finite abelian groups. The study of codes over groups is motivated by the observation in [37; 38] that when more that two signals are used for transmission, a group structure, instead of the finite field structure traditionally assumed, for the alphabet is matched to the relevant distance measure. The Hamming distance properties of codes over groups have been studied in [24] and in [6; 7] construction of group codes over abelian groups is given in terms of a 'parity check' matrix. Given the length of the code n and the number of information symbols K, the maximum possible minimum distance is $(n-k+1)$ for codes over any alphabet. (n,k) codes that achieve a minimum distance $d=(n-k+1)$ are called maximum distance separable codes (MDS). In [24] MDS group codes is discussed and nonexistence results for group codes over nonabelian groups have been discussed. MDS codes over Z_m have been studied in in [9; 62; 63]. In [63] several applications of codes over the ring of integers modulo m is discussed. These codes find applications in peak-shift correction in magnetic recording systems. MDS group codes over cyclic groups are characterized in [76]. For MDS group

[1] A part of the results of this chapter also appears in [69]

codes over abelian groups a quasi determinant characterization is obtained in [78]. In [18] matrix characterization of MDS codes over modules is discussed.

It is well known that binary linear codes are matched to binary signaling over an Additive White Gaussian Noise (AWGN) channel, in the sense that the squared Euclidean distance between two signal points in the signal space corresponding to two codewords is proportional to the Hamming distance between codewords. Similarly, linear codes over Z_m are matched to M–PSK modulation systems for an AWGN channel [40; 41]. The general problem of matching signal sets to linear codes over general algebraic structure of groups has been studied in [37; 38]. Also, group codes constitute an important ingredient for the construction of Geometrically Uniform codes [23]. This motivates the study of codes over groups both abelian and nonabelian. In [6] construction of group codes over abelian groups that mimics the construction of algebraic codes over finite fields is considered and it is shown that the construction can be on the basis of a parity check matrix which provides the relevant information about the minimum Hamming distance of the code. The parity check symbols are seen as images of certain homomorphisms from G^k to G.

In this chapter we obtain systematic matrix characterization of Almost MDS ($AMDS$) and Near MDS ($NMDS$) codes over Z_m and finite abelian groups. In chapter(4) we have obtained matrix characterization of $AMDS$ and $NMDS$ over finite fields. The rest of the chapter is organized as follows:

- In section(5.2) we introduce the basic results which are used in the chapter
- In section(5.3) we characterize $AMDS$ codes and $NMDS$ codes over Z_m based on the systematic generator matrix
- In section(5.4) $AMDS$ and $NMDS$ codes over abelian groups are characterized based on the defining homomorphisms. For $AMDS$ codes and $NMDS$ codes abelian groups we also obtain an associated matrix characterization based on the component homomorphisms. In the case of $AMDS$ codes over cyclic groups we show that the associated matrix characterization is same as the systematic matrix characterization of $AMDS$ codes over Z_m. Further also obtain the a set of results concerning the length of $[\, n\, k\,]$ $AMDS$ codes over cyclic groups of cardinality m.

- We conclude the chapter in section(5.5).

5.2 Hamming Weight Hierarchy of Codes over Z_m

Definition 5.1 *(Support) Let C be any code over Z_m and let B be any subset of C. Then the support of B denoted as $supp(B)$ equals $\{i \mid \exists a, b \in B$ such that $a_i \neq b_i\}$. If the size of B is one we define the $supp(B) = 1$*

Definition 5.2 *Let C be a code over Z_m of length n. Then we define the following function $S_C(p) = min_{B \subseteq C \, |B|=p \geq 2} Supp(B)$*

Definition 5.3 *Let the sequence $d_1, d_2, \ldots, d_l$ of generalized Hamming weights be defined such that $d_1 < d_2 < \ldots < d_l$, and $d_1, d_2, \ldots, d_l$ are distinct values of $S_C(p)$ for $p = 2, 3, \ldots, \#C$. Further $M_i = max\{p \in \{2, 3, \ldots, \#C\} \mid S_C(p) = d_i\}$ for $i = 1, 2, \ldots l$, where $\#C$ denotes the cardinality of the code C.*

Definition 5.4 *The generalized Hamming Weight hierarchy of a code C over Z_m is the set $\{(d_1, M_1), (d_2, M_2), \ldots, (d_l, \#C)\}$, where $\#C$ denotes the cardinality of the code.*

Definition 5.5 *Consider Z_m (whose cardinality is m). We denote the cardinality of a the code C over Z_m as $\#C$. If an code $[n,\ k = log_m(\#C)]$ code C over Z_m is an MDS code then the Hamming weight hierarchy of C is $\{(d_1 = n - k + 1, M_1 = m), (d_2 = n - k + 2, M_2 = m^2), \ldots, (d_k = n, M_k = \#C)\}$*

Definition 5.6 *Consider a code C over Z_m. An $[n,\ k = log_m(\#C)]$ code C over Z_m is defined as an $AMDS$ code if the $d_{min} = d_1$ of C is $(n - k)$.*

Definition 5.7 *An $[n\ ,\ k]$ code C over Z_m is defined to be $NMDS$ code if the code C as well as its dual code $C^{\perp}$ are $AMDS$.*

5.3 Almost MDS codes over Z_m

We consider linear $AMDS$ codes over Z_m, where $m = p_1^{r_1} p_2^{r_2} \ldots p_s^{r_s}$ and each p_i is a prime number. An $[\, n\, k\,]$ code is defined as an $AMDS$ if $d_1 = n - k$. First we consider $AMDS$ codes over Z_m where $m = p_1^{r_1}$.

5.3.1 Almost MDS codes of size m^2 over $Z_{p^{r_1}}$

AMDS codes over $Z_{p^{r_1}}$ with k=2

This the simplest non-trivial situation, with $k = 2$ and $d = n - 2$. In what follows, we will concentrate on linear $AMDS$ codes only, thus exploiting the additive structure of $Z_{p_1^{r_1}}$, where p_1 is a prime number. Consider the following generator matrix of a code C

$$G = \begin{bmatrix} 1 & 0 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \dots & \alpha_n \\ 0 & 1 & \beta_3 & \beta_4 & \beta_5 & \beta_6 & \dots & \beta_n \end{bmatrix} \tag{5.1}$$

where $\alpha_3, \alpha_4, \alpha_5 \dots, \alpha_n$ are elements in $Z_{p_1^{r_1}}$. Similarly $\beta_3, \beta_4, \beta_5, \dots, \beta_n$ are also elements in $Z_{p_1^{r_1}}$. Some of the α_i's and β_i's can be units or zero divisors in $Z_{p_1^{r_1}}$.
All the codewords of the code are of the form $C_{a,b} = a \cdot (1, 0, \alpha_3, 0, \alpha_5, \alpha_6, \dots, \alpha_n) - b \cdot (0, 1, 0, \beta_4, \beta_5, \beta_6, \dots, \beta_n)$ with $a, b \in Z_{p_1^{r_1}}$. If the code C generated by G is $AMDS$ then $d_{min} = d_1 = n - 2$. Also note that if C is an $AMDS$ code then there are maximum two zeros on any code word. Therefore the linear combination of the rows of the generator matrix also should have code words with maximum two zeros. This leads to the following condition

- Let $\alpha_i, \alpha_j, \alpha_k, \beta_i, \beta_j, \beta_k$ be units in $Z_{p_1^{r_1}}$. There exists utmost two locations i, j such that

$$\begin{aligned} a\alpha_i + b\beta_i &= 0 \\ a\alpha_j + b\beta_j &= 0 \end{aligned} \tag{5.2}$$

  for $4 < i, j < n$ and $i \neq j$. Therefore $\frac{a}{b} = -\frac{\beta_i}{\alpha_i} = -\frac{\beta_j}{\alpha_j}$, i.e., the ratios belong to the same coset modulo p_1. Here b has to be a unit for $\frac{a}{b}$ to be well defined. There do not exist three columns i, j and k such that

$$\begin{aligned} a\alpha_i + b\beta_i &= 0 \\ a\alpha_j + b\beta_j &= 0 \\ a\alpha_k + b\beta_k &= 0 \end{aligned} \tag{5.3}$$

i.e.the ratios $\frac{a}{b} = -\frac{\beta_i}{\alpha_i} = -\frac{\beta_j}{\alpha_j} = -\frac{\beta_k}{\alpha_k}$ do not belong to the same coset modulo p_1 (if not we will have $d_1 = (n-3)$ and not $(n-2)$). This ensures that $d_{min} = n-k = n-2$. In matrix language, every $(g, g+1)$ submatrix of P (where P is the sub matrix of the systematic generator matrix of the form $[I, \ P]$) has a (g, g) submatrix whose determinant is a unit in $Z_{p^{r_1}}$.

- Consider any $(2, 3)$ submatrix of the P submatrix, where the generator matrix is of the form $[I \ \ P]$. Consider the case where $\alpha_i, \alpha_j, \alpha_k, \beta_i, \beta_j, \beta_k$ can be units or zero divisors in $Z_{p^{r_1}}$. The linear combination of the two row of the generator matrix can have utmost two zeros. Consider the $(2, 2)$ submatrices of the $(2, 3)$ submatrix and their determinants. If one of the $(2, 2)$ submatrix has determinant which is a unit then there are utmost two zeros in these three locations of the code word. Suppose all the $(2, 2)$ submatrices have determinants which are zero divisors. In $Z_{p_1^{r_1}}$ the zero divisors are multiples of p_1. Then the rows of the $(2, 3)$ submatrix are linearly dependent and hence $d_1 \leq (n-3)$. Therefore we can have only utmost one $(2, 2)$ submatrix of the $(2, 3)$ submatrix whose determinant is a zero divisor in $Z_{p_1^{r_1}}$. If not all these three locations in the codeword will be identically zero and code will not be $AMDS$.

- In general consider every $(g, g+1)$ submatrix of the P submatrix. There exists atleast one (g, g) submatrix whose determinant is an unit in $Z_{p_1^{r_1}}$.

If the $AMDS$ code C is generated by minimum weight vectors the generator matrix can be written as

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & \gamma_5 & \gamma_6 & \dots & \gamma_n \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & \dots & 1 \end{bmatrix} \tag{5.4}$$

where each γ_i for $i > 5$ is a unit. Here we can see that every $(1, 2)$ submatrix of P has a $(1, 1)$ submatrix which is an unit in $Z_{p_1^{r_1}}$. Also every $(2, 3)$ should have atleast one $(2, 2)$ submatrix which is an unit in $Z_{p_1^{r_1}}$.

Example 5.1 *The generator matrix of a* $[n, \ 2]$ $NMDS$ *code over* $Z_{p_1^{r_1}}$ *is (here we take* $p_1 = 2$ *and* $r_1 = 1$*).*

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \tag{5.5}$$

Here the length of the code is 6. *It is easy to see that* $d_1 = 4$

Example 5.2 *The generator matrix of a* $[n,\ 2]$ $AMDS$ *code over* Z_2 *is*

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} \tag{5.6}$$

Here the length of the code is 5 *and* $d_1 = 3$. *The code word generated by a minimum weight code word and a code word of weight* $(d_{min} + 1)$.

AMDS codes over $Z_{p^{r_1}}$ *with k=3*

Consider the following generator matrix for a $[n,\ 3]$ code over $Z_{p^{r_1}}$.

$$G = \begin{bmatrix} 1 & 0 & 0 & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 & \dots & \alpha_n \\ 0 & 1 & 0 & \beta_4 & \beta_5 & \beta_6 & \beta_7 & \beta_8 & \dots & \beta_n \\ 0 & 0 & 1 & \gamma_4 & \gamma_5 & \gamma_6 & \gamma_7 & \gamma_8 & \dots & \gamma_n \end{bmatrix} \tag{5.7}$$

where $\alpha_i, \beta_i, \gamma_i \ \ 4 \leq i \leq n$ be elements in $Z_{p^{r_1}}$.

Codewords are of the form $c_{a,b,c} = [\ a\ b\ c\ ]G$, with $a, b, c \in Z_m$. If G generates an $AMDS$ code then $d_1 = n-3$, i.e., any codeword can have utmost three zero co-ordinates. Therefore each row of the of P sub matrix of $G = [I\ P]$ can have utmost one element which is a zero divisor in $Z_{p^{r_1}}$.

Suppose $b = 0$. Then the codeword $c_{a,b,c}$ can have utmost two zeros in the codeword from the fourth location to the n-th location. This leads to the condition that if we consider any $(2, 3)$ submatrix of P submatrix there exists atleast one $(2, 2)$ submatrix whose determinant is an unit in $Z_{p_1^{r_1}}$. If the determinants of all the $(2, 2)$ submatrices of the $(2, 3)$ submatrix of P are zero divisors both the rows of the $(2, 3)$ submatrix are linearly dependent. Then $d_{min} \leq (n - 4)$. Therefore atleast one of $(2, 2)$ submatrices of $(2, 3)$ must have a determinant which is an unit in $Z_{p^{r_1}}$.

Suppose all $a,\ b,\ c$ are not equal to zero. In the codeword $c_{a,b,c}$ utmost three locations, i, j, k are zero. All other co-ordinates must be non-zero. In other words for every any $(3, 4)$ submatrix of P, where $G = [I\ \ P]$, there is atleast one $(3, 3)$ submatrix such that the determinant is an unit in $Z_{p_1^{r_1}}$. In $Z_{p_1^{r_1}}$ the zero divisors are all multiples of p_1. Therefore

atleast one of (g, g) submatrices must have a determinant which is an unit in $Z_{p_1^{r_1}}$. This condition ensures that there are utmost three zeros in any codeword, i.e., $d_1 = n - 3$.

5.3.2 AMDS Codes over Z_m

Here we consider the case where $m = p_1^{r_1} p_2^{r_2} p_3^{r_3} \dots p_s^{r_s}$ where p_i $1 \leq i \leq s$ are prime numbers. Let p_1 be the smallest prime number which divides m.

AMDS codes over Z_m with k=2

Consider the simplest non-trivial situation, with $k = 2$ and $d = n - 2$. In what follows, we will concentrate on linear $AMDS$ codes only, thus exploiting the additive structure of Z_m, where $m = p_1^{r_1} p_2^{r_2} p_3^{r_3} \dots p_s^{r_s}$, p_i $1 \leq i \leq s$ are prime numbers and p_1 is the smallest prime number. Consider the following generator matrix of a code C

$$G = \begin{bmatrix} 1 & 0 & \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 & \dots & \alpha_n \\ 0 & 1 & \beta_3 & \beta_4 & \beta_5 & \beta_6 & \dots & \beta_n \end{bmatrix} \tag{5.8}$$

where $\alpha_{s+3}, \alpha_{s+4}, \dots, \alpha_n$ are units in Z_m. Similarly $\beta_{s+3}, \beta_{s+4}, \dots, \beta_n$ are units in Z_m. $\alpha_3, \alpha_4, \dots, \alpha_{s+2}$ are zero divisors in Z_m such that they are pairwise relatively prime. Similarly $\beta_3, \beta_4, \dots, \beta_{s+2}$ are zero divisors in Z_m such that they are pairwise relatively prime. All the codewords of the code are of the form $C_{a,b} = a \cdot (1, 0, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \dots, \alpha_n) - b \cdot (0, 1, \beta_3, \beta_4, \beta_5, \beta_6, \dots, \beta_n)$ with $a, b \in Z_m$. If the code C generated by G is $AMDS$ then $d_{min} = d_1 = n - 2$. Therefore if C is $AMDS$ there are maximum two zeros on any code word. Therefore the linear combination of the rows of the generator matrix also should have code words with maximum two zeros. This leads to the following condition

- There exists utmost two locations, $s + 3 \leq i, j \leq n$ such that (note that in these locations α_i and β_i are units)

$$\begin{aligned} a\alpha_i + b\beta_i &= 0 \\ a\alpha_j + b\beta_j &= 0 \end{aligned} \tag{5.9}$$

for $s+3 < i, j < n$ and $i \neq j$. If $\alpha_i, \alpha_j, \alpha_k, \beta_i, \beta_jand\beta_k$ are units then $\frac{a}{b} = -\frac{\beta_i}{\alpha_i} = -\frac{\beta_j}{\alpha_j}$, i.e., the ratios belong to the same coset modulo p_1. There do not exist three columns i, j and k such that

$$\begin{aligned} a\alpha_i + b\beta_i &= 0 \\ a\alpha_j + b\beta_j &= 0 \\ a\alpha_k + b\beta_k &= 0 \end{aligned} \tag{5.10}$$

i.e.the ratios $\frac{a}{b} = -\frac{\beta_i}{\alpha_i} = -\frac{\beta_j}{\alpha_j} = -\frac{\beta_k}{\alpha_k}$ do not belong to the same coset modulo p_1 (if not then $d_1 = (n-3)$ and not $(n-2)$). This ensures that $d_{min} = n - k = n - 2$. In matrix language, every $(g, g+1)$ submatrix of P (where P is the sub matrix of the systematic generator matrix of the form $[I, \ P]$) has a (g, g) submatrix whose determinant is a unit.

- In general if choose any three locations i, j, k of any codeword. All these three locations cannot be zero identically. This implies that in the associated $(2, 3)$ submatrix the rows are dependent. This leads to the condition that atleast one of the $(2, 2)$ submatrix has to be a unit in Z_m or the greatest common divisor of the determinants of $(2, 2)$ submatrices has to be an unit in Z_m. In Z_m it is possible to have $(2, 3)$ matrix whose $(2, 2)$ submatrices have zero divisors as determinants such that greatest common divisor of these determinants is an unit in Z_m.

- Consider any $(g, g+1)$ submatrix of P. If the determinants of all (g, g) submatrices are zero divisors then the greatest common divisor of the determinants must be an unit. Otherwise we will have a code word in C whose $d_1 \leq n-3$. In both the rows of the generator matrix zero divisors are chosen such that they are relatively prime , i.e., the greatest common divisor of all $(1, 1)$ submatrices of any $(1, 2)$ submatrix is an unit. Now consider $(2, 2)$ submatrices of any $(2, 3)$ submatrix. Here the greatest common divisor of the determinants of all $(2, 2)$ submatrices has to be an unit. Therefore in each row we have maximum s zero divisors corresponding different prime powers in the prime factorization of m.

The generator matrix G can be rewritten as (if the code is not generated by minimum weight code words)

$$G = \begin{bmatrix} 1 & 0 & \alpha_3 & \alpha_4 & \ldots \alpha_{s+2} & \gamma_{s+3} & \ldots & \gamma_n \\ 0 & 1 & \beta_3 & \beta_4 & \ldots & \beta_{s+2} & 1 & \ldots & 1 \end{bmatrix} \tag{5.11}$$

Let α_i, β_i for $i > (s+2)$ be units in Z_m. Then $\gamma_i = \frac{\alpha_i}{\beta_i}$ for $i > s+2$ are units in Z_m. α_i, β_i for $3 \leq i \leq s+2$ are zero divisors. The zero divisors are chosen such that pairwise they relatively prime on each row.

Example 5.3 *The generator matrix of a* $[n,\ 2]$ $NMDS$ *code over* Z_6 *is (Here we have* $p_1 = 2$ *and* $r_1 = 1$*. Also* $p_2 = 3$ *and* $r_2 = 1$*).*

$$G = \begin{bmatrix} 1 & 0 & 2 & 3 & 1 & 1 \\ 0 & 1 & 3 & 2 & 1 & 1 \end{bmatrix} \tag{5.12}$$

Here the length of the code is 6*. It is easy to see that* $d_1 = 4$

We can similarly analyze the generator matrix for $AMDS$ codes with $k = 3$ over Z_m. Now we obtain the general systematic generator matrix characterization of $AMDS$ codes over Z_m.

Theorem 5.1 *An* $[\ n\ k\ ]$ *linear code over* Z_m*, where* $m = p_1^{r_1} p_2^{r_2} p_3^{r_3} \ldots p_s^{r_s}$ *(where* $p_i\ 1 \leq i \leq s$ *are prime numbers,* p_1 *the smallest prime number) with systematic generator matrix* $G = [I_{k,k}\ \ P_{k,(n-k)}]$ *is an* $AMDS$ *code if and only if every* $(g, g+1)$ *submatrix has* (g, g) *submatrices with the following properties:*

- *there exists atleast one* (g, g) *submatrix whose determinant is a unit in* Z_m *or*
- *if the determinants of all the* (g, g) *submatrices are zero divisors the greatest common divisor of these determinants is an unit in* Z_m*. equal to one.*

Proof: Let us assume that the $[\ n\ k\ ]$ code is $AMDS$. Therefore $d_1 = n - k$. Consider any code word which is a the linear combination of g rows of the the generator matrix. From the I part of systematic G matrix the codeword has g non-zero elements. Therefore in any codeword $c = (c_1, c_2, \ldots, c_n)$ there are utmost g locations such that $c_i = 0$ for $k+1 \leq i \leq n$. Consider any $(g, g+1)$ submatrix of P matrix. The linear combination

of g rows of a $(g, g+1)$ submatrix of P there can be utmost g zeros. This implies that the greatest common divisor of the determinants of the (g, g) submatrices is an unit or one of the (g, g) submatrix has a determinant which is an unit. This proves the theorem in one direction. To prove that code is $AMDS$ if the condition stated in the theorem we proceed as follows: From the condition of theorem we know that there are utmost g zeros in the linear combination of g rows of the generator matrix. Therefore $d_1 = n - k$. □

5.3.3 Dual Code of an $[\, n\, k\,]$ Code over Z_m

Consider an $[\ n\ k\ ]$ code C over Z_m, $m = p_1^{r_1} p_2^{r_2} p_3^{r_3} \ldots p_s^{r_s}$, $p_i\ 1 \leq i \leq s$ are prime numbers and let p_1 be the smallest prime number. Let C be generated by a systematic generator matrix with $G = [I_{k,k}\ \ P_{k,(n-k)}]$ where $I_{k,k}$ is the identity matrix and $P_{k,(n-k)}$ is a matrix over Z_m. The dual of the code C with parameters $[n\ \ (n-k)]$ is generated by the $[-P^T_{k,(n-k)}\ \ I_{n-k,n-k}]$ matrix.

From theorem(5.1) it can be seen that the dual code is $AMDS$ if and only if the every $(g, g+1)$ matrix of $-P^T_{k,(n-k)}$ has either atleast on (g, g) submatrix whose determinant is a unit or has (g, g) submatrices such that the greatest common divisor of the determinants is an unit (if the determinants of all (g, g) submatrices are zero divisors in Z_m).

Corollary 5.1.1 *The $[\ n\ \ (n-k)\ ]$ dual code $C^{\perp}$ of code C generated by the matrix $\left[-P^T_{k,(n-k)} I_{(n-k),(n-k)}\right]$ is $AMDS$ if and only if for every $(g, g+1)$ submatrix of $-P^T_{k,(n-k)}$ satisfies the following condition*

- *the determinant of one of the (g, g) submatrices is an unit in Z_m or*
- *if the determinants of every (g, g) submatrix of $(g, g+1)$ submatrix is a zero divisor then the greatest common divisor of the determinants of these (g, g) matrices must be an unit in Z_m.*

Proof: The proof follows along the same lines as in the case of theorem(5.1). □

If the a code C and its dual are $AMDS$ we know that it is $NMDS$. In the following section we characterize $NMDS$ codes over Z_m.

5.3.4 Near MDS codes over Z_m

Consider an $[\, n\ k\,]$ code over Z_m. Let the code be generated by a generator matrix $G = \left[I_{(k,k)}\ P_{(k,n-k)}\right]$. The dual code is generated by $H = \left[-P^T_{(k,n-k)}\ I_{(n-k,n-k)}\right]$. If an (j,j) submatrix of $P_{(k,n-k)}$ is nonsingular we can easily see that the corresponding (j,j) submatrix in $-P^T_{(k,n-k)}$ is also nonsingular. Also note that λ_{ij} is an unit in Z_m then $-\lambda_{ij}$ is also an unit in Z_m.

An $[n\,k]$ code C is defined as $NMDS$ if code C as well as its dual, $C^{\perp}$, are $AMDS$ codes. In terms of the generalized Hamming weight hierarchy an $[\, n\, k\,]$ code C over Z_m is defined as $NMDS$ if $d_1 = n-k$ and $d_i = (n-k+i)$ for $2 \leq i \leq k$.

In the following theorem we characterize $NMDS$ based on the systematic generator matrix.

Theorem 5.2 *Let $G = [I_{k,k}\ \ P_{k,n-k}]$ be the systematic generator matrix of a linear Near-MDS code C over Z_m. Then C is NMDS iff every $(g, g+1)$ and $(g+1, g)$ submatrix of P satisfies the following condition:*

- *the determinant of atleast one (g,g) submatrix is an unit in Z_m or*
- *if the determinants of every (g,g) submatrix of $(g, g+1)$ submatrix be a zero divisor in Z_m then the greatest common divisor of the determinants of these (g,g) matrices must be an unit in Z_m. Similarly for $(g+1, g)$ submatrix if the determinants of every (g,g) submatrix is a zero divisor in Z_m then the greatest common divisor of these determinant must be an unit in Z_m.*

We prove this result in two different ways.

First Proof: Here we characterize $NMDS$ code using the definition which states for a $NMDS$ code the code as well as its dual are $AMDS$.

Initially assuming that the code is $NMDS$ we arrive the characterization of the systematic generator matrix. The generator matrix of the code C over Z_m is given by $[I_{k,k}\ \ P_{k,n-k}]$. Here the code is $AMDS$ if and only if satisfies the condition given in theorem(5.1). The dual code generated by $\left[-P^T_{k,n-k}\ \ I_{n-k,n-k}\right]$ is also $AMDS$ if and only if it satisfies the condition of theorem(5.1). Combining these results we get the following condition on every $(g, g+1)$ and $(g+1, g)$ submatrices of the P matrix:

- the greatest common divisor of the determinants of every (g, g) submatrix of every $(g, g+1)$ matrix of P is one or atleast one (g, g) submatrix has a determinant which is an unit Z_m
- the greatest common divisor of the determinants of every (g, g) submatrix of every $(g+1, g)$ matrix of P is one or atleast one (g, g) submatrix has a determinant which is an unit in Z_m.

Now assuming the conditions of the theorem we can easily show that the code and its dual are $AMDS$. Therefore the code is $NMDS$. This completes the first proof. □

Second Proof: The proof is along the same lines as in the case of $NMDS$ codes over finite fields. Here we explicitly prove that $d_1 = n - k$ and the minimum support of any two dimensional subcode of C is $d_2 = n - k + 2$.

First we prove the 'if part'. We have to show that $d_1(C) = n - k$ and $d_2(C) = n - k + 2$. Consider any one dimensional subcode generated by a minimum weight codeword of C. In terms of linear combination of rows of G, let

$$\underline{c} = (c_1, c_2, \ldots, c_n) = \sum_{j=1}^{g} \alpha_j \underline{r}_{i_j} \tag{5.13}$$

where $i_j \in \{1, 2, \ldots, k\}, j = 1, 2, \ldots, g$ and $\underline{r}_{i_j}$ is the i_j-th row of G.

The weight of $\underline{c}$ within the first k positions is g. We need to show that the weight in the last $n - k$ positions is $(n - k - g)$ or the number of zeros in the last $n - k$ positions is g. Let the number of zeros in the last $n - k$ positions of $\underline{c}$ be $\lambda > g$. Choose any $g + 1$ of these λ positions and let these positions be $j_1, j_2, \ldots, , j_{g+1}$. Then

$$\begin{bmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_g \end{bmatrix} \begin{bmatrix} r_{i_1 j_1} & r_{i_1 j_2} & \ldots & r_{i_1 j_{g+1}} \\ r_{i_2 j_1} & r_{i_2 j_2} & \ldots & r_{i_2 j_{g+1}} \\ \vdots & \vdots & \ldots & \vdots \\ r_{i_g j_1} & r_{i_g j_2} & \ldots & r_{i_g j_{g+1}} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \ldots & 0 \end{bmatrix}$$

Since the greatest common divisor of determinants (g, g) submatrices is an unit in Z_m or one of the (g, g) submatrix has a determinant which is an unit in Z_m only $\alpha_1 = \alpha_2 =$

$\ldots \alpha_g = 0$ is the solution of the above set of equation, which is a contradiction. Hence $\lambda \leq g$ and $d_1 = n - k$. Also it follows that if there are more than one zero divisor on a row of the P submatrix then they are pairwise relatively prime.

To prove that $d_2(C) = n - k + 2$ consider a two dimensional subcode generated by two codewords $\underline{c}$ and $\underline{d}$. If the size of the union of supports of $\underline{c}$ and $\underline{d}$ is at least $n - k + 2$ then we are through. So, we need to consider the case where the support of both $\underline{c}$ and $\underline{d}$ is within an identical set of $n - k + 1$ locations. Let g of these locations be within the first k positions and let

$$\underline{c} = (c_1, c_2, \ldots, c_n) = \sum_{j=1}^{g} \alpha_j \underline{r}_{i_j}$$
$$\underline{d} = (d_1, d_2, \ldots, d_n) = \sum_{j=1}^{g} \beta_j \underline{r}_{i_j} \tag{5.14}$$

Consider an arbitrary linear combination of $\underline{c}$ and $\underline{d}$, i.e.,

$$\underline{e} = a\underline{c} + b\underline{d} = \sum_{j=1}^{g} (a\alpha_j + b\beta_j)\underline{r}_{i_j} \tag{5.15}$$

There are $g - 1$ zeros in the last $n - k$ positions of e. Let these be $j_1, j_2, \ldots j_{g-1}$. Then we have

$$\begin{bmatrix} a\alpha_1 + b\beta_1 & a\alpha_2 + b\beta_2 & \ldots & a\alpha_g + b\beta_g \end{bmatrix} \begin{bmatrix} r_{i_1 j_1} & r_{i_1 j_2} & \ldots & r_{i_1 j_{g-1}} \\ r_{i_2 j_1} & r_{i_2 j_2} & \ldots & r_{i_2 j_{g-1}} \\ \vdots & \vdots & \ldots & \vdots \\ r_{i_g j_1} & r_{i_g j_2} & \ldots & r_{i_g j_{g-1}} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \ldots & 0 \end{bmatrix}$$

Since every $(g, g-1)$ submatrix of P has one $(g-1, g-1)$ submatrices whose determinant is an unit or the greatest common divisor of the determinants of all $(g-1, g-1)$ submatrices is an unit in Z_m.

There are two cases to consider

- In the first case the determinants of all $(g-1, g-1)$ submatrices are not units and the greatest common divisor of the determinants is an unit. Therefore we can choose a pair a and b such that the linear combination of the first $(g-1)$ rows is zero. For this pair a and b the linear combination cannot be an all zero vector. Therefore d_2 is not equal to $(n-k+1)$. It is therefore equal to $(n-k+2)$.

- The second case is when the determinants of one of the $(g-1, g-1)$ sub matrix is a unit. Without loss of generality we assume the first $g-1$ rows to constitute the submatrix whose determinant is unit and choose a and b such that $a\alpha_g + b\beta_g = 0$. Then it follows that $a\alpha_t + b\beta_t = 0$ for all $t = 1, 2, \ldots g-1$. Now, if both α_g and β_g are non zeros, then $\underline{c}$ and $\underline{d}$ are scalar multiple of one another which means the code is one dimensional. Hence $d_2(C) = n-k+2$. (Note that from (1), $d_2(C) = n-k$ is not possible since $d_1(C) = n-k$.) If one of them is zero, say $\beta_g = 0$, then $a = 0$ and $b\beta_t = 0$ for all $t = 1, 2, \ldots g-1$ which is not true.

This completes the proof for the if part.

To prove the only if part: For $NMDS$ codes $d_1 = n-k$. Consider a the linear combination of any g rows of the generator matrix. The first k columns of the generator matrix will have g non zero locations. For the code to have $d_1 = n-k$, the last $n-k$ columns of P submatrix must have $(n-k-g)$ non zero locations. Consider any $(g, g+1)$ submatrix of these g rows from P submatrix. The linear combination of these g rows cannot lead to a all zero vector in these $(g+1)$ locations. If so d_1 will be $(n-k-1)$ or less. Therefore the determinants of the (g, g) submatrices must be relatively prime or one of the (g, g) submatrices has a determinant which is an unit in Z_m. This leads to the condition $(g, g+1)$ submatrices of P matrix.

Also for $NMDS$ codes $d_2 = n-k+2$. This we can easily prove by contradiction. If the all the determinants of (g, g) submatrices of $(g+1, g)$ submatrices of P are not relatively prime we can see that $d_2 < n-k+2$. This leads to condition on every $(g+1, g)$ submatrix of P. This completes the proof. □

Example 5.4 *The generator matrix of a* $[n, 2]$ $NMDS$ *code over* Z_m *is (let the the smallest*

prime divisor of m *be* 2*.*

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \tag{5.16}$$

Here the length of the code is 6*. The maximum length possible by the previous theorem. It is easy to see that* $d_1 = 4$ *and* $d_2 = 6$*. Also note that the code is generated by minimum weight vectors.*

Example 5.5 *The generator matrix of a* $[n, 2]$ $NMDS$ *code over* Z_m *is (let the the smallest prime divisor of* m *be* 2*)*

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} \tag{5.17}$$

Here the length of the code is 5*. The code word generated by a minimum weight code word and a code word of weight* $(d_{min} + 1)$*. We see that the code achieves the maximum length possible if and only if it is generated by minimum weight vectors.*

5.4 AMDS Codes over Abelian Groups

5.4.1 Preliminaries

Let G be a finite group with a multiplicative operation and identity e. Codes over groups are discussed in [6] and [31]. MDS codes over cyclic groups are discussed in [76]. MDS codes over abelian groups are characterized in [78].

Definition 5.8 *Let* G *and* H *be any groups. The function* $\phi : G \to H$ *is said to be a homomorphism of* G *into* H *if* $\phi(xy) = \phi(x)\phi(y)$ *for all* $x,\ y$ *in* G*.*

Definition 5.9 *Two groups* G *and* H *are said to be isomorphic if there is a bijection* ϕ *of* G *onto* H *such that if* $\phi(xy) = \phi(x)\phi(y)$ *for all* $x,\ y$ *in* G*.*

Definition 5.10 *An endomorphism of a group* G *is a homomorphism of* G *into itself, and an automorphism of* G *is an isomorphism of* G *onto itself.*

Proposition 5.2.1 *([31]) Let G be any group. Then every homomorphism $\phi : G \times G \times \ldots \times G \to G$ of G^k into G admits canonical decomposition*

$$\phi(x_1, \ldots, x_k) = \prod_{j=1}^{k} \phi_j(e, \ldots, e, x_j, e, \ldots, e)$$

The direct product of G forms a group. Note that $\phi_j(e, \ldots, e, x_j, e, \ldots, e)$ is essentially an endomorphism of G. $\phi_j(e, \ldots, e, x_j, e, \ldots, e) = \phi_{1j}(e)\phi_{2j}(e) \ldots \phi_{jj}(x_j) \ldots \phi_{kj}(e)$, where ϕ_{ij} for $j = 1, 2, 3, \ldots, k$ are k endomorphisms of G. We say that ϕ_i decomposes as these k endomorphisms.

A block code of length n over G is any non-empty subset of the n-fold direct product G^n, i.e., of the set of all the n-tuples of group elements. We assume that the group order $\mid G \mid$ to be finite. The dimension of a code C is $k = log_{|G|} \mid C \mid$ symbols per block, where $\mid C \mid$ is the code size, bounded above by $\mid G \mid^n$. The code rate is $r = \frac{k}{n}$. The Hamming distance between two code words is the number of positions in which they differ. Let I denote the index set of n-tuples of C. An information set of C is any index subset $J \subseteq I$ of size $\mid J \mid = k$ such that every k-tuple of elements of G occurs in J precisely once as the code words run through C. Every C has an information set. A linear block code over G is a subset of $\mid G \mid^n$ that forms a group, i.e., is a subgroup of $\mid G \mid^n$.

Definition 5.11 *An $[\, n\, k\,]$ code C over a group G^n is defined to be generalized linear code if $(x_1, x_2, x_3, \ldots x_n)$ and $(y_1, y_2, \ldots, y_n)$ are in the code then $(x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n)$ is also an element of the code. Here $\oplus$ denotes the binary group operation.*

Definition 5.12 *An $[\, n\, k\,]$ systematic block code C with block length n and dimension k over a group G is a subgroup of G^n with order $\mid G \mid^k$ formed by n-tuples*

$$(x_1, x_2, \ldots, x_k, y_1, \ldots, y_{n-k})$$

with $y_i = \phi_i(x_1, x_2, \ldots, x_k)$ where ϕ_i are $(n - k)$ homomorphisms from G^k into G.

In general ϕ_i is a map from G^k into G. For linearity these maps must be homomorphisms [31].

The notion of support and Hamming weight hierarchy follows can be generalized to codes over group G as follows.

Definition 5.13 *(Support) Let C be any code over a group G and let B be any subset of C. The the support of B is $supp(B) = \{i \mid \exists a, b \in B$such that $a_i \neq b_i\}$. If the size of B is one we define the $supp(B) = 1$*

Definition 5.14 *Let C be a code over a group of length n. The we define the following function $S_C(m) = min_{B \subseteq C\, |B|=m \geq 2} Supp(B)$*

Definition 5.15 *Let the sequence $d_1, d_2, \ldots, d_l$ of generalized Hamming weights be defined such that $d_1 < d_2 < \ldots < d_l$, and $d_1, d_2, \ldots, d_l$ are distinct values of $S_C(m)$ for $m = 2, 3, \ldots, \#C$ $\#C$ denotes the cardinality of C. Further $M_i = max\{m \in \{2, 3, \ldots, \#C\} \mid S_C(m) = d_i\}$ for $i = 1, 2, \ldots l$.*

Definition 5.16 *The generalized Hamming Weight hierarchy of a code C over a group G is the set $\{(d_1, M_1), (d_2, M_2), \ldots, (d_l, \#C)\}$*

Definition 5.17 *Consider a finite group G with cardinality m. If an code $[n, k = log_m(\#C)]$ code C over a group G is an MDS code then the Hamming weight hierarchy of C is $\{(d_1 = n - k + 1, M_1 = m), (d_2 = n - k + 2, M_2 = m^2), \ldots, (d_k = n, \#C)\}$*

Definition 5.18 *Consider a finite group G with cardinality m. If an code $[n, k = log_m(\#C)]$ code C over a group G is an $AMDS$ code then $d_1 = n - k$*

The group of characters of an abelian group G can be used to define the dual code of a group code over G. The group of characters is isomorphic to the group G, and hence the characters can be indexed by the elements of G in accordance with the isomorphism.

Definition 5.19 *Let C be an (n, k) group code over g. The dual code denoted by $C^{\perp}$ is defined as*

$$C^{\perp} = \{(y_1, y_2, \ldots, y_n) \in G^n | \prod_{i=1}^{n} \eta_{x_i}(y_i) = 1, \forall (x_1, x_2, \ldots x_n) \in C\} \tag{5.18}$$

where η_g denotes the character of g corresponding to $g \in G$, and 1 is the identity element of the group of nth roots of unity in the complex field. The dual codes of group codes over abelian groups have been characterized in [76], [77].

Definition 5.20 *Consider a finite group G with cardinality m. An $[n,\ k = log_m(\#C)]$ code C over a group G defines an $NMDS$ code if the code C and its dual $C^{\perp}$ are $AMDS$ codes.*

We use this definition to characterize $NMDS$ over groups from $AMDS$ code and its dual code over groups.

5.4.2 Matrix Characterization of $AMDS$ Codes over Abelian Groups

Definition 5.21 *A systematic $[nk]$ linear group code over an abelian group G is a subgroup of G^n with order $\mid G \mid^k$ described by $(n-k)$ homomorphisms ϕ_l for $l = 1, 2, \ldots, (n-k)$, of G^k onto G. Its codewords are of the form $(x_1, \ldots, x_k, x_{k+1}, \ldots, x_n)$ where*

$$x_{k+l} = \phi_l(x_1, \ldots, x_k) = \oplus_{j=1}^{k} \phi_l(e, \ldots, e, x_j, e, \ldots, e),\ l = 1, 2, \ldots, (n-k) \tag{5.19}$$

where e is the identity element of the group G. $\oplus$ denotes binary operation of the group.

Every codeword of a $(k+s, k)$ group code is of the form

$$\begin{aligned}(x_1, x_2, \ldots, x_k, x_{k+1}, x_{k+2}, \ldots, x_{k+s}) &= (x_1, x_2, \ldots, x_k, \phi_1(x_1, \ldots, x_k), \\ &\quad \phi_2(x_1, x_2, \ldots, x_k), \ldots, \phi_s(x_1, x_2, \ldots, x_k)) \\ &= (x_1, x_2, \ldots, x_k, \psi_{11}(x_1) \oplus \ldots \oplus \psi_{k1}(x_k), \\ &\quad , \ldots, \psi_{1s}(x_1) \oplus \ldots \oplus \psi_{ks}(x_k))\end{aligned} \tag{5.20}$$

where $x_i \in G$, $i = 1, 2, \ldots, k$, $\phi_{jl} \in End(G)$, $j = 1, 2, \ldots, k$, $1 \leq l \leq s$. The homomorphism ϕ_l is said to decompose in terms of the elements of $End(G)$ and is written as $\phi_l = \psi_{11}\psi_{21} \ldots \psi_{k1}$ for $1 \leq l \leq s$.

Definition 5.22 *For a $(k+s, k)$ group code C over G, defined by the homomorphisms $\{\phi_1, \phi_2, \ldots, \phi_s\}$, the $k \times s$ matrix over $End(G)$, denoted by Ψ,*

$$\Psi = \begin{bmatrix} \psi_{11} & \psi_{12} & \ldots & \psi_{1s} \\ \psi_{21} & \psi_{22} & \ldots & \psi_{2s} \\ \vdots & \vdots & \ldots & \vdots \\ \psi_{k1} & \psi_{k2} & \ldots & \psi_{ks} \end{bmatrix} \tag{5.21}$$

where $\phi_l = \psi_{1l}\psi_{2l} \ldots \psi_{kl}$, for $l = 1, 2, \ldots, s$, is called the associated matrix of the code

Every matrix of the form (5.21) defines a $(k+s,k)$ group code over G. Moreover, when this matrix operates on an element $(x_1, x_2, \ldots, x_k) \in G^k$ (information vector) gives the check vector $(x_{k+1}, x_{k+2}, \ldots, x_{k+s}$ as given below:

$$[x_{k+1}\ x_{k+2}\ \ldots\ x_{k+s}] = [x_1\ x_2\ \ldots x_k]\Psi$$

or

$$[x_{k+1}\ x_{k+2}\ \ldots\ x_{k+s}]^{tr} = \Psi^{tr}[x_1\ x_2\ \ldots x_k]^{tr}$$

where $x_{k+l} = \psi_{1l}(x_1) \oplus \psi_{2l}(x_2) \oplus \ldots \psi_{kl}(x_k)$ for $l = 1, 2, \ldots s$. The generator matrix which operates on an information vector gives the corresponding codeword is given by

$$\left[\begin{array}{cccc|cccc} \psi_I & \psi_e & \ldots & \psi_e & \psi_{11} & \psi_{12} & \ldots & \psi_{1s} \\ \psi_e & \psi_I & \ldots & \psi_e & \psi_{21} & \psi_{22} & \ldots & \psi_{2s} \\ \vdots & \vdots & \ldots & \vdots & \vdots & \vdots & \ldots & \vdots \\ \psi_e & \psi_e & \ldots & \psi_I & \psi_{k1} & \psi_{k2} & \ldots & \psi_{ks} \end{array}\right] \tag{5.22}$$

The associated matrix Ψ in (5.21) is over $End(G)$ which is in general a non-commutative ring. In the case of linear codes over $GF(p^m)$ the associative matrix is Ψ is over $GF(p^m)$. In the case of codes over cyclic group of cardinality m, C_m, the associated matrix is over Z_m, a commutative ring. For codes over G the associated matrix in general is over a non-commutative ring and the conventional notions of determinant and singularity of matrices do not carry over directly.

Theorem 5.3 *A $(k+s,k)$ group code over G, defined by homomorphisms $\{\phi_1, \phi_2, \ldots, \phi_s\}$ is $AMDS$ if and only if every $(g, g+1)$ submatrix of the associated matrix of the form*

$$\Psi_{g,g+1} = \left[\begin{array}{cccc} \psi_{i_1 j_1} & \psi_{i_1 j_2} & \ldots & \psi_{i_1 j_{g+1}} \\ \psi_{i_2 j_1} & \psi_{i_2 j_2} & \ldots & \psi_{i_2 j_{g+1}} \\ \vdots & \vdots & \ldots & \vdots \\ \psi_{i_g j_1} & \psi_{i_g j_2} & \ldots & \psi_{i_g j_{g+1}} \end{array}\right] \tag{5.23}$$

for $1 \le i_k \le g$, $1 \le j_k \le (g+1)$, $g = 1, 2, \ldots, min\{s, k\}$, has

- *atleast one (g, g) submatrix which represents an automorphism of G^g or*

- *if every (g, g) submatrix represents an endomorphism of G^g then the intersection of the kernels of the endomorphisms is only the identity element of G^k.*

Proof: Consider the associated matrix given by equation(5.21). Suppose all the $(g, g+1)$ submatrices satisfy the conditions given in this theorem we have to show that the code is $AMDS$. Consider a codeword $\underline{c} = (c_1, c_2, \ldots, c_k, c_{k+1}, c_{k+2}, \ldots, c_{k+s})$. We have $c_{k+i} = \psi_{1i}(c_1) \oplus \psi_{2i}(c_2) \oplus \ldots \oplus \psi_{ki}(c_k)$ for $1 \leq i \leq s$. Suppose only in $(c_1, c_2, \ldots, c_k)$ only g elements are non identity elements. Then we have the following relation $c_{k+i} = \psi_{j_1 i}(c_{j_1}) \oplus \psi_{j_2 i}(c_{j_2}) \oplus \ldots \oplus \psi_{j_g i}(c_{j_g})$ for $1 \leq i \leq (g+1)$. Since every $(g, g+1)$ submatrix has atleast on (g, g) submatrix which is an automorphism or the kernel of endomorphisms represented by the (g, g) submatrices are non intersecting atleast one of the elements c_{k+i} is an non identity element. Since this is true for every $(g, g+1)$ submatrix of the associated matrix the code is $AMDS$.
Now assuming that the code is $AMDS$ show that the condition of the theorem is satisfied. Choose a codeword $\underline{c}$ of minimum weight. Let $c_{1_1}, c_{i_2}, \ldots, c_{i_g}$ be nonzero elements in $\underline{c}$. Consider a set of homomorphisms $\psi_{i_1}, \psi_{i_2}, \ldots, \psi_{i_g}$. If these homomorphisms are such that they do not satisfy the conditions given in the theorem we have a codeword of weight $\leq g+s-(g+1) = (s-1)$. Then the code is not an $AMDS$. This is contrary to the assumption that the code is $AMDS$. Thus the defining homomorphisms satisfy the conditions given above. □

5.4.3 AMDS Codes over Cyclic Group C_m

We specialize to the case where the group G is a cyclic group C_m, i.e., a cyclic group of order m. The set of homomorphisms which describe a $AMDS$ code are described in the following paragraphs.

Definition 5.23 *An homomorphism $\phi : C_m^k \rightarrow C_m$ is called a distance non decreasing homomorphism $(DNDH)$ if either $K_\phi = \{\vec{e}\}$ or $d_{min}(K_\phi) = 1$, where $\vec{e}$ is the identity element of C_M^k, K_ϕ denotes the kernel of ϕ and d_{min} stands for minimum Hamming distance.*

Lemma 5.3.1 *An homomorphism ϕ_1 from C_m^k to C_m where $\phi_1 = \phi_{11}\phi_{21} \ldots \phi_{k1}$ is $DNDH$ iff atleast one of ϕ_{i1} for $1 \leq i \leq k$ is an endomorphism of C_m.*

Proof: Assume that ϕ is a $DNDH$. Therefore we know that $d_{min}(K_\phi) = 1$. This implies that atleast one of $\phi_{i1}(x_i)$ is an endomorphism since $\phi_{i1}(x_i) = e$ for $x_i \neq e$. Similarly assuming that one of ϕ_{i1} is an endomorphism we can conclude that ϕ_1 is an $DNDH$. □

Lemma 5.3.2 *A $(k+1, k)$ group code is $AMDS$ if and only if the defining homomorphism is $DNDH$*

Proof: Assuming that the defining homomorphism is $DNDH$ we can prove that the $(k+1, k)$ code is an $AMDS$ as follows. Essentially have to show that $d_1 = 1$. This follows from the definition of $DNDH$, i.e., $d_{min}(K_{\phi_1}) = 1$.
Assuming that the code is $AMDS$, we have $d_{min} = 1$. Therefore there exists a k-tuple $\underline{x}$ in G^k with weight one such that $\phi(\underline{x}) = e$. Therefore it follows that $d_{min}(K_{\phi_1}) = 1$. □
The definition of $DNDH$ can be extended to a set of homomorphisms from the C_m^k to C_m, where C_m is a cyclic group, C_m^k is a direct product of the cyclic group, as follows:

Definition 5.24 *Let $\{\phi\}_{i=1}^{i=s}$ denoted as Φ_s be a set of homomorphisms from $C_m^k \rightarrow C_m$ denoted as $\Phi_{(s)}$. Let $K_{\phi_1\phi_2\ldots\phi_s}$ denote $K_{\phi_1} \cap K_{\phi_2} \cap \ldots K_{\phi_s}$ where K_{ϕ_i} is the kernel of ϕ_i. Φ_s is said to be a distance non decreasing set of homomorphisms, $(DNDSH)$, if the following conditions are satisfied:*

- *the homomorphisms do not constitute a set of $DISH$*
- *for all $1 \leq r \leq s$ $d_{min}(K_{\phi_{i_1}\phi_{i_2}\ldots\phi_{i_r}}) \geq r$ or*
- *$K_{\phi_{i_1}\phi_{i_2}\ldots\phi_{i_r}} = \{\vec{e}\}$*

Lemma 5.3.3 *A $(k+2, k)$ group code is an $AMDS$ code if and only if the defining homomorphism, $\Phi = \phi_1\phi_2$, constitute a $DNDSH$.*

Proof: We can prove this lemma along the lines of the characterization of $(k+1, k)$ $AMDS$ codes. Initially assuming that homomorphisms are $DNDSH$ we prove that the code is $AMDS$, i.e., we show that $d_{min} = 2$.

- To prove that $d_1 = 2$. Since the Φ is set of $DNDSH$. Either $d_{min}(K_{\phi_i}) = 1$ or $d_{min}(K_{\phi_i}) = 2$ for $i \in \{1, 2\}$. If $d_{min}(K_{\phi_i}) = 1$ for $i = 1$ or $i = 2$ then the

corresponding ϕ_i is an endomorphism. Without loss of generality we can take $i = 1$. For an $\underline{x} \in G$ which in the kernel of ϕ_1 the weight of the codeword is 2. Therefore $d_{min} = 2$. Hence the code is $AMDS$.

- If $d_{min}(K_{\phi_i}) = 2$ for $i = 1$ and $i = 2$ then both ϕ_1 and ϕ_2 are automorphisms. In this case if $d_{min}(K_{\phi_1\phi_2})$ is also 3 the code is MDS. Then it follows that the homomorphisms are not $DNDSH$. Therefore $d_{min}(K_{\phi_1\phi_2}) = 2$. Hence there exists $\underline{x} \in G^k$ such that $\underline{x} \in K_\Phi$. Therefore the d_{min}, i.e, $d_1 = 2$. The code is $AMDS$.

To prove in the reverse direction we assume that the code is $AMDS$ and show that the defining homomorphisms constitute a $DNDSH$. The $(k + 2, k)$ code over the group C_m is $AMDS$ implies that $d_1 = 2$. We will show that the defining homomorphism $\Phi = \phi_1\phi_2$ is a $DNDSH$.

- $d_{min} = 2$ this implies that either $d_{min}(K_{\phi_1\phi_2})$ is 2 or $d_{min}(K_{\phi_i}) = 1$ for $i \in \{1, 2\}$. $d_{min}(K_{\phi_i})$, for $i = 1$ or 2 equals to 1 implies that atleast one of the component homomorphisms of ϕ_i is an endomorphism. In general we can say that $d_{min}(K_{\phi_1\phi_2}) \geq 2$. or $d_{min}(K_{\phi_i}) \geq 1$. Moreover also note that inequality for $d_{min}(K_\Phi)$ is not a strict inequality as in the of DISH [76]. Therefore the defining homomorphisms constitute a set of $DNDSH$.

□

Theorem 5.4 *A $(k+s, k)$ group code is $AMDS$ if and only if the defining homomorphisms Φ_s constitute a set of $DNDSH$.*

Proof: The proof is along the lines of the proof for $(k + 2, k)$ $AMDS$ group code.
Assuming that the set of homomorphisms $\{\phi_1, \phi_2, \ldots, \phi_s\}$ constitute a set of $DNDSH$ we will show that the $(k + s, k)$ code is $AMDS$. Since $\Phi = \phi_1\phi_2 \ldots \phi_s$ constitute a set of $DNDSH$ there exits $\phi_{i_1}\phi_{i_2} \ldots \phi_{i_r}$ where $1 \leq r \leq s$ such that $d_{min}(K_{\phi_{i_1}\phi_{i_2}\ldots\phi_{i_r}}) = r$. Therefore there exists $\underline{x} \in G^k$ such that $\underline{x} \in K_{\phi_{i_1}\phi_{i_2}\ldots\phi_{i_r}}$ with Hamming weight r. Therefore the Hamming weight of the associated code word is $r + (s - r) = s$. Therefore d_{min} of the $(k + s, k)$ code is s. Hence the code is $AMDS$.

Now assuming that the code is $AMDS$ to show that the set of defining homomorphisms constitute a $DNDSH$. Since the code is $AMDS$ we know that the d_{min} of the $(k+s,k)$ code is s. Choose a code word with minimum weight. Let the number of non identity elements in the chosen minimum weight codeword in the locations $(k+1, k+2, \ldots, k+s)$ be r (i.e. the number locations where identity element occurs is $(s-r)$). Therefore there exist a set of homomorphisms $\phi_{i1}\phi_{i2}\ldots\phi_{i_{s-r}}$ such that $d_{min}(K_{\phi_{i_1}\phi_{i_2}\ldots\phi_{i_{s-r}}}) = (s-r)$. In general $d_{min}K_{\phi_{1_1}\phi_{i_2}\ldots\phi_{i_r}} \geq r$ for every r, where $1 \leq r \leq s$. Hence the set of homomorphisms constitute a $DNDSH$. This completes the proof. □

Let C be an (n,k) systematic group code over G, defined by homomorphisms ϕ_i for $1 \leq i \leq (n-k)$. Then it is shown in [77] that the dual of the code C denoted as $C^{\perp}$ is an $(n, n-k)$ code defined by $\hat{\phi}_1, \hat{\phi}_2, \ldots, \hat{\phi}_k$ where $\hat{\phi}_{i,j} = \phi^d_{j,i}$. In terms of generator matrices if $[I \mid \Phi]$ generates the code C then it dual has the generator matrix $[(\Phi^d)^{tr} \mid I]$, where $[\Phi^d]$ is the matrix obtained by replacing each entry of $[\Phi]$ by its dual.

Proposition 5.4.1 *An $(k+s,k)$ code over a cyclic group is $NMDS$ if and only if*

- *the defining set of homomorphisms, Φ, constitute a set of $DNDSH$*
- *the dual of the defining set of homomorphisms, $\hat{\Phi}$, also constitute a $DNDSH$.*

Proof: The proof follows from the fact that if the code as well as its dual are $AMDS$ then the code is $NMDS$. From the characterization of $AMDS$ code we know that the code is $AMDS$ if and only if the defining homomorphism is DNDSH. Therefore if the defining homomorphism and its dual are $DNDSH$ the code is $NMDS$. □

5.4.4 Matrix Characterization of $AMDS$ Codes over Cyclic Groups

Every endomorphism of C_m is uniquely defined by the image of the generator of C_m under the endomorphism. Moreover, the ring of endomorphisms of C_m is isomorphic to Z_m, the ring of integers modulo m. An endomorphism $\phi(g) = g^{\lambda}$, where g is the generator of C_m is an automorphism iff λ is relatively prime to m, or equivalently, λ is a multiplicative unit in the ring Z_m.

Definition 5.25 *For a $(k+s,k)$ group code L over C_m, given by*

$$L = \{(x_1, \ldots, x_k, \phi_1(x_1, \ldots, x_k), \ldots, \phi_s(x_1, \ldots, x_k)) / x_i \in C_M, i = 1, 2, \ldots, k\} \quad (5.24)$$

the $k \times s$ matrix over Z_m, denoted by Λ, $\Lambda = [\lambda_{ij}]_{k\times s}$ where $\phi_j = \psi_{1j}\psi_{2j}\ldots\psi_{kj}$, for $j = 1, 2, \ldots, s$ and $\psi_{ij}(g) = g^{\lambda_{ij}}$ where $i = 1, 2, \ldots, k$, is called the associated matrix of the code L.

The generator matrix G of L can then be written as $G = [I_{k\times k} \mid \Lambda]$, where $I_{k\times k}$ denote the $(k \times k)$ identity matrix, and the codeword corresponding to the information vector $(x_i, x_2, \ldots, x_k)$ is given by $[x_1 x_2 \ldots x_k]\ \ G$. The dual codes of group codes over abelian groups have been characterized in [76], [77]. Specializing the characterization to codes over cyclic groups leads to the following.

Theorem 5.5 *[77] If the generator matrix of group code over a cyclic group is $[I \mid \Lambda]$, where Λ is the associated matrix. Then the generator matrix of the dual code is $[-\Lambda^T \mid I]$.*

It is easy to see that the for every $(g + 1, g)$ submatrix of $-\Lambda^T$ has atleast one (g, g) submatrix whose determinant is a unit of Z_M if the associated $(g, g + 1)$ submatrix of Λ has atleast one (g, g) submatrix whose determinant is a unit of Z_M.
The parity check equations are $x_{\kappa+u} = \Sigma_{i=1}^{k} x_i\lambda_{iu},\ \ u = 1, 2 \ldots, s$ which when put in the matrix form, become

$$[-\Lambda^T \mid -I_{s\times s}][x_1, x_2, \ldots, x_{k+s}]^T = [O_{s\times 1}] \tag{5.25}$$

The parity check matrix, denoted by H, is given by $H = [-\Lambda^T | I_{s\times s}]$.This parity check matrix H can be obtained from the parity check matrix given in [6], [7] for group codes over abelian groups by specializing to cyclic groups. The associated matrix of a group code uniquely defines the code. Therefore follows that a necessary condition for a group code over C_m to be $AMDS$ is that all the entries of its associated matrix represent $DNDSH$. The complete characterization is given in the following theorem.

Theorem 5.6 *A $(k+s, k)$ group code $L = (x_1, \ldots, x_k, \phi_{(x_i,\ldots,x_k)}, \ldots, \phi_s(x_1, \ldots, x_k))$ over C_m is $AMDS$ iff*

- *Consider every $(h, h+1)$ submatrix $h = 1, 2, \ldots,$ min$\{s, k\}$, of the associated matrix. Then the determinants of (h, h) sub matrices of each $(h, h + 1)$ submatrix satisfy the following condition: atleast one of them has a determinant which is a unit in Z_m or the greatest common divisor of the determinants is a unit in Z_m.*

Proof: This is same as the characterization of the $AMDS$ code over Z_m (theorem(5.1)). □
Give the associated matrix of an $(k+s,k)$ code over the cyclic group we know the associated matrix of the dual code. If the code is generated by $[I \mid \Lambda]$ the dual code is generated by $[-\Lambda^T \mid I]$. Also if the sub matrices of $[-\Lambda^T \mid I]$ satisfy the conditions needed for the code to be $AMDS$ then the $(k+s,k)$ code is $NMDS$. This is stated as the following theorem.

Theorem 5.7 *A $(k+s,k)$ group code $L = (x_1,\ldots,x_k,\phi_{(x_i,\ldots,x_k)},\ldots,\phi_s(x_1,\ldots,x_k))$ over C_m is $NMDS$ iff*

- *Consider every $(h,h+1)$ submatrix $h = 1,2,\ldots,min\{s,k\}$, of the associated matrix. Then the determinants of (h,h) sub matrices of each $(h,h+1)$ submatrix satisfy the following condition: atleast one of the (h,h) submatrix has a determinant which is an unit in Z_m or the greatest common divisor of the determinants of (h,h) submatrices is a unit in Z_m. are pairwise relatively prime.*

- *Consider every $(h+1,h)$ submatrix, $h = 1,2,\ldots,min\{s,k\}$, of the associated matrix. Then the determinants of (h,h) sub matrices of each $(h+1,h)$ submatrix satisfy the following condition: atleast one of them has a determinant which is an unit in Z_m or the greatest common divisor of the determinants of (h,h) submatrices is a unit in Z_m.*

Proof: Follows is same as characterization of $NMDS$ codes over Z_m (theorem(5.1)). □

5.4.5 Nonexistence Results of $AMDS$ codes over Cyclic Group C_m

m is a Power of a Prime

In this section we restrict our discussion to the case where m is a power of a prime say $m = p^d$.
First we consider the cases $(k+1,k)$ and $(k+1,1)$ codes over C_{p^d}.
For $(k+1,k)$ codes the associated matrix is of the form $[\lambda_{11}\ \lambda_{21}\ \ldots\ \lambda_{k1}\ ]^T$ where each entry is an element of Z_{p^d}. If atleast one λ_{i1} is a zero divisor then the code is an $AMDS$ code. Each entry can occur any number of times.

Lemma 5.7.1 *Over C_{p^d}, $(k+1,k)$ $AMDS$ groups codes exist for all values of k, p and d if all there exits at least one entry in the associated matrix which is a zero divisor.*

For $(k+1,1)$ codes, dual of a the $(k=1,k)$ code, the associated matrix is of the form $[-\lambda_{11} \ -\lambda_{21} \ \ldots \ -\lambda_{k1}]$ where each entry is an element of Z_{p^d}. If the greatest common divisor of every pair $(-\lambda_{i1}, -\lambda_{j1})$ is is an unit in Z_{p^d} then the code is an $AMDS$ code. Therefore for $m = p^d$ any multiple of p occurs once and all the other $-\lambda_{i1}$'s are unit in Z_m. This can be stated as an lemma as follows:

Lemma 5.7.2 *Over C_{p^d}, $(1+k,1)$ $NMDS$ groups codes exist for all values of p and d if the following conditions are met Let $[-\lambda_{11} \ -\lambda_{21} \ \ldots \ -\lambda_{k1}]$ be the associated matrix.*

- *greatest common divisor of every pair $(-\lambda_{i1}, -\lambda_{j1})$ is an unit in Z_{p^d} or one of the elements of the pair is an unit in Z_{p^d}.*
- *one of the $(-\lambda_{i1})$ is a zero divisor.*

Proof: Follows from the condition on every $(1,2)$ submatrix of the associated matrix (theorem(5.1)). □

Consider $(k+2,k)$ codes over C_{p^d}. The associated matrix is of the form

$$\begin{bmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \\ \vdots & \vdots \\ \lambda_{k1} & \lambda_{k2} \end{bmatrix} \tag{5.26}$$

where $\lambda_{ij} \in Z_{p^d}, \forall i = 1,2; j = 1,2,\ldots,k$. Taking all the entries to be units, for the code to be $AMDS$, we require that for any (1×2) sub matrix the greatest common divisor of the elements be an unit in Z_m or one of the $(1,1)$ submatrices is an unit in Z_m.

Lemma 5.7.3 *Over C_{p^d}, $(k+2,k)$ $AMDS$ groups codes exists for all values of k, p and d*

Consider the dual of $(k+2,k)$ code, i.e. the $(k+2,2)$ code. The associated matrix is

$$\begin{bmatrix} -\lambda_{11} & -\lambda_{21} & \ldots & -\lambda_{k1} \\ -\lambda_{12} & -\lambda_{22} & \ldots & -\lambda_{k2} \end{bmatrix} \tag{5.27}$$

For the dual code to be $AMDS$ every $(2,3)$ sub matrix of the associated matrix has $(2,2)$ submatrices whose determinants are pair wise relatively prime or has atleast one (g,g) submatrix which is an unit. Therefore the maximum possible length is $2+2+2(p-1)$. Since there are $(p-1)$ units, two information symbols and one zero divisor.

Lemma 5.7.4 *Over C_{p^d}, $(k+2,2)$ $AMDS$ groups codes exists for values of $k \leq 2+2(p-1)$.*

We can generalize the above result as follows:

Theorem 5.8 *Over C_{p^d}, for all values of d and for $s \geq 2, k \geq 2, (k+s,s)$ $AMDS$ groups codes exist for $k \leq 2+2(p-1)$.*

General m

Let the prime factorization of the integer m be $p_1^{d_1}p_2^{d_2}p_3^{d_3}\ldots p_r^{d_r}$, where $p_1, p_2, \ldots, p_r$ are distinct primes.

Lemma 5.8.1 *Over C_m, where $m = p_1^{d_1}p_2^{d_2}p_3^{d_3}\ldots p_r^{d_r}$, with all primes distinct, $(k+s,s)$ $AMDS$ group codes, for all $s,k \geq 2$, do not exist if $k \geq r+2(p-1)$, where $p = min\{p_1,p_2,\ldots,p_r\}$ and r is the number of distinct primes in the prime factorization of m*

Proof: Let the associated matrix of a $(k+s,k)$ group code over C_m be Λ. Consider every $(1,2)$ sub matrix of Λ. Either one of the entries is an unit in Z_m or the greatest common of divisor is one. This holds for every $(1,2)$ submatrix. Therefore each row can have utmost r zero divisors corresponding to some power of the distinct primes. Also every $(2,3)$ submatrix has a $(2,2)$ submatrix whose determinant is an unit or the greatest common divisor of the determinant of $(2,2)$ submatrices is one. Therefore each row can have utmost two units which lie in the same coset modulo the smallest prime divisor of m. Putting both the conditions together we get the result. □

For the dual code the result can be stated as follows:

Lemma 5.8.2 *Over C_m, where $m = p_1^{d_1}p_2^{d_2}p_3^{d_3}\ldots p_r^{d_r}$, with all primes distinct, Consider the dual of $(k+s,s)$ $AMDS$ group codes, for all $s,k \geq 2$. Such codes do not exist if $s \geq r+2(p-1)$, where $p = min\{p_1,p_2,\ldots,p_r\}$ and r is the number of distinct primes in the prime factorization of m*

Combining the two lemmas we can state the following result for $NMDS$ codes as follows:

Lemma 5.8.3 *Over C_m, where $m = p_1^{d_1} p_2^{d_2} p_3^{d_3} \dots p_r^{d_r}$, with all primes distinct, $(k+s, s)$ $NMDS$ group codes, for all $s, k \geq 2$, do not exist if max$\{s, k\} \geq r + 2(p-1)$, where $p =$ min$\{p_1, p_2, \dots, p_r\}$ and r is the number of distinct primes in the prime factorization of m*

Note that for the code to be $NMDS$ the code as well as its dual must be $AMDS$.

5.5 Conclusion

In this chapter we have obtained the systematic generator matrix characterization of $AMDS$ and $NMDS$ codes over Z_m. Further we have characterized $AMDS$ and $NMDS$ codes over abelian groups. Specializing to cyclic groups we have obtained systematic generator matrix characterization for $AMDS$ and $NMDS$ codes. We have also obtained non-existence results for these codes over cyclic groups. It is interesting to see if it is possible to obtain a quasi-determinant type of characterization for $AMDS$ codes over abelian groups. This is a interesting direction for further work.

Chapter 6

Matrix Characterization of Linear Codes with Arbitrary Hamming Weight Hierarchy

[1]

6.1 Introduction and Preliminaries

Let C be an $[n, k]$ linear code over F_q. Let $\chi(C)$ be the support of C, defined by, $\chi(C) = \{i \mid x_i \neq 0$ for some $(x_1, x_2, \ldots, x_n) \in C\}$. The r-th generalized Hamming weight of C is then defined as $d_r(C) = min\{\mid \chi(D) \mid$: D is an $r-$dimensional subcode of C$\}$ [28], [29], [72]. The sequence $(d_1(C), d_2(C), \cdots, d_k(C))$ is called the Hamming Weight Hierarchy (HWH) of C. The notion of HWH has been found to be useful in several applications. The HWH characterizes the performance of C on the Type-II wire-tap channels [44]. The HWH also finds application in the following areas: state complexity of trellis diagrams of codes [32], t-resilient functions [72] and designing codes for the switching multiple access channel [61].

A linear $[n, k, d]$ code satisfying the Singleton bound $d \leq n-k+1$ with equality is called a Maximum Distance Separable (MDS) code [51]. All Reed-Solomon (RS) codes are MDS.

[1] Part of the results of this chapter has appeared in [67] and have been communicated as [70]

The lengths of RS codes are at most the size of the alphabet and hence are short. Moreover, all known MDS codes are such that there is an RS code (with slight modifications) with identical parameters [74]. The problem of obtaining the maximal length of MDS codes, in general, is still open. Algebraic Geometric (AG) codes [54] are a generalization of RS codes with minimum distances deviating from the Singleton bound by a small quantity known as the genus of the curve over which the code is defined and the length of the code is determined by the number of rational points on the curve. It was shown in [59] that the class of AG codes contains codes that exceed the Varshamov-Gilbert bound [39]. Hence, to find long codes, codes with minimum distance not reaching the Singleton bound, but deviating from it only slightly need to be studied in general. An explicit approach to this problem was developed by Dodunekov and Landgev [15; 16] by considering Near-MDS (NMDS) codes. The class of NMDS codes contains remarkable representatives as the ternary Golay code and the quaternary [11,6,5] and [12,6,6] codes as well as a large class of Algebraic Geometric codes [19]. The importance of NMDS codes is that there exist NMDS codes which are considerably longer than the longest possible MDS codes for a given size of the code and the alphabet. Also, these codes have good error detecting capabilities [17]. Generalizations of NMDS codes like Almost-MDS codes [10] and several classes classes of codes with distances close to Singleton bound have been studied [43]. One such class of codes is the Near-Near-MDS codes, which we denote by N^2-MDS codes [42]. Other classes of codes with generalized Hamming weights close to the generalized Singleton bound include A^μ-MDS codes, dually A^μ-MDS codes [43]. The generalized Singleton bound for an $[n, k]$ code C is given by

$$d_r(C) \leq (n - k + r); \quad 1 \leq r \leq k \tag{6.1}$$

and it is well known fact that the sequence of generalized Hamming weights is strictly increasing [72], i.e.,

$$d_1(C) < d_2(C) < \ldots < d_k(C) = n \tag{6.2}$$

and the HWH of a code is related to that of its dual code $C^\perp$ as follows:

$$\{d_r(C) \mid r = 1, 2, ..., k\} \cup \{n + 1 - d_r(C^\perp) \mid r = 1, 2.., n - k\} = \{1, 2, ..., n\}. \tag{6.3}$$

AMDS (Almost-MDS), NMDS (Near-MDS), N^2-MDS (Near-Near-MDS) and A^μ-MDS Codes : Linear $[n, k, d]$ codes meeting the generalized Singleton bound 6.1 with equality

for every $r;\ \ 1 \leq r \leq k$ are MDS codes. Almost-MDS (AMDS) codes are the class of codes with $d_1(C) = n-k$ and $d_i(C) \leq (n-k+i)$ for all $2 < i \leq k$. Near-MDS (NMDS) codes are those with the following HWH: $d_1(C) = (n-k)$ and $d_i(C) = (n-k+i)$ for $i = 2, 3, 4, \ldots, k$. Equivalently a code is NMDS iff the $d_1(C) = n-k$ and $d_1(C^{\perp}) = k$. Near-Near-MDS Codes (N^2-MDS) are codes with the property that $d_1(C) = (n-k-1)$, $d_2(C) = (n-k+1)$ and $d_i(C) = (n-k+i)$ for $i = 3, 4, \ldots, k$ [43], [42]. A^{μ}-MDS codes are those with the property that $d_1(C) = (n-k+1-\mu)$ and $d_i(C) \leq (n-k+i)$ for $i = 2, 3, \ldots, k$ [43].

An $[n, k]$ code is a NMDS iff $d_1(C)+d_1(C^{\perp}) = n$, where $d_1(C)$ is the minimum Hamming distance of the code and $d_1(C^{\perp})$ is that of the dual code [15]. This implies that an $[n, k]$ NMDS as well as its dual code are AMDS. NMDS codes can be characterized in terms of their check matrices and generator matrices as follows [15]: A linear $[n, k]$ code is NMDS iff its check matrix satisfies (i) any $n-k-1$ columns of the parity check matrix are linear independent, (ii) there exists a set of $n-k$ linearly dependent columns in the parity check matrix and (iii) any $n-k+1$ columns of the parity check matrix are of rank $n-k$. A linear $[n, k]$ code is NMDS iff its generator matrix satisfies (i) any $k-1$ columns of the generator matrix are linear independent (ii) there exists a set of k linearly dependent columns in the generator matrix and (iii) any $k+1$ columns of the generator matrix are of rank k.

Definition 6.1 (Defect, MDS-rank and Dually A^{μ}-MDS codes) *The defect $\mu_i(C)$ of the i-th generalized Hamming weight of a code C is defined as $\mu_i(C) = n-k+i-d_i(C)$ ($\mu_i(C)$ is zero for MDS codes for every i, $1 \leq i \leq k$) and the MDS-rank of an $[n, k]$ code C is defined as the smallest η such that $d_{\eta+1} = n-k+\eta+1$. A^{μ}-MDS codes are a class of codes where $\mu_1(C) = \mu$, i.e., $d_1(C) = n-k+1-\mu$. Dually A^{μ}-MDS codes are a class of codes consisting codes C such that $\mu_1(C) = \mu_1(C^{\perp}) = \mu$.*

It is well known that a linear MDS code can be described in terms of its systematic generator matrix as follows: a linear code with systematic generator matrix $[I \mid P]$ is MDS iff every square submatrix of P is nonsingular. Since MDS codes are characterized by the HWH $d_r(C) = n-k+r$ for $1 \leq r \leq k$, the systematic generator matrix characterization of MDS codes can be viewed as the systematic generator matrix characterization of linear codes with specific generalized HWH: $d_r = n-k+r;\ \ 1 \leq r \leq k$. In this chapter, we generalize this

characterization to all linear codes in terms of their HWH. We also generalize the classes of NMDS and N^2-MDS codes to what we call N^μ-MDS codes and characterize these codes in terms of their systematic generator matrices using their respective HWH. Codes meeting the generalized Greismer bound are also characterized in terms of their systematic generator matrices and the systematic check matrix characterization and the HWH of dually defective codes meeting the generalized Greismer bound are also reported.

The contents of this chapter is organized as follows: In Section 6.2 we discuss the systematic check matrix characterization of an arbitrary linear code with a specified HWH. We apply this systematic matrix characterization to A^μ-MDS codes, NMDS codes and N^2-MDS codes. Section 6.3 describes a class of codes which are close to Singleton bound called the N^μ-MDS codes and presents their systematic matrix characterization. This class of codes include A^μ-MDS codes, NMDS codes and N^2-MDS codes. In Section 6.4 we define a class of codes which we call dually defective codes. The matrix characterization of dually defective codes as well as of codes meeting the Greismer bound are obtained. We also arrive at the conditions for dually defective codes to meet the generalized Greismer bound.

6.2 Systematic check matrix characterization in terms of HWH

The following result from [21] gives a check matrix characterization of the HWH for a linear code which we will make use of to prove our main result presented in Theorem 6.1.

Proposition 6.0.1 *An $[n, k]$ code C with MDS-rank μ and a check matrix H has the HWH $\{d_i(C) \mid 1 \leq i \leq k\}$ iff*

1. *For every i, every $(d_i(C) - 1)$ columns of H has rank greater than or equal to $(d_i(C) - i)$.*
2. *There exists $d_i(C)$ columns of H for every i, with rank equal to $(d_i(C) - i)$.*
3. *Every $(n - k + \mu)$ columns of H are of full rank.*

For $[n, k]$ linear MDS codes or equivalently for linear codes with the HWH $d_i(C) = n-k+i$ for all $i = 1, 2, \cdots, k$ the systematic check matrix characterization assumes that the check matrix is in the form $[I \mid P]$ where I is the $(n-k) \times (n-k)$ identity matrix. Since for MDS codes any k coordinate positions can be taken as information symbols and the remaining as check symbols there always exists such a systematic check matrix. However, this need not be possible for arbitrary linear codes in general. But with suitable column permutations on the check matrix one can obtain a check matrix in the systematic form $[I \mid P]$ which in the strict sense is a check matrix for an equivalent code obtained by the coordinate permutation corresponding to the column permutations that led to the systematic form. In the sequel, we will always assume that the code under consideration has a check matrix in the systematic form $[I \mid P]$ with the understanding that we are dealing with the corresponding equivalent code. Then the conditions on P should be taken as conditions on the submatrix of the original code that correspond to check positions. With this understanding we present our main result in the following theorem.

Theorem 6.1 *An $[n, k]$ code with parity check matrix $H = [I \mid P]$ and MDS-rank η has the HWH, $\{d_i(C) = n - k + i - \mu_i(C)\}$ where $\mu_i(C) \geq 0$ for $1 \leq i \leq k$ iff the following conditions are satisfied:*

1. *For $i < g \leq min\{d_i(C) - 1,\ k\}$, every $(g + \mu_i(C) + 1 - i) \times g$ submatrix of P has rank $\geq (g - i + 1)$.*

2. *There exists a g, $i < g \leq min\{d_i(C), k\}$, such that the rank of a $(g + \mu_i(C) - i) \times g$ submatrix of P is $(g - i)$.*

3. *For $1 < g \leq min\{(n - k), (k - \eta)\}$ every $g \times (g + \eta)$ submatrix of P has rank g.*

Proof: We establish equivalence between the conditions of Proposition 6.0.1 and Theorem 6.1. In the Part (i) of the proof we prove that the conditions of Proposition 6.0.1 imply those of Theorem 6.1 and in Part (ii) we prove the converse.
Part (i): Let $d_i(C) = n - k + i - \mu_i(C)$. From the condition 1 of Proposition 6.0.1, we know that every $(n - k + i - 1 - \mu_i(C))$ columns of H has rank greater than or equal to $(n - k - \mu_i(C))$. Choose a set of $(n - k + i - 1 - \mu_i(C))$ columns of H. If all these

columns are from the P submatrix then the $(n-k) \times (n-k+i-1-\mu_i(C))$ submatrix of P has rank greater than or equal to $(n-k-\mu_i(C))$ which indeed is the condition 1 of Theorem 6.1. Consider the case where g columns are from the P submatrix. Then $(n-k+i-1-\mu_i(C)-g)$ columns are from the I submatrix of H. The rank of these $(n-k+i-1-\mu_i(C)-g)$ columns is $(n-k+i-1-\mu_i(C)-g)$. Hence the g columns from the P submatrix of H have rank greater than or equal to $(g-i+1)$. Therefore every $(g+\mu_i(C)-i+1) \times g$ submatrix has rank greater than or equal to $(g-i+1)$, where $i \leq g \leq \min\{d_i(C)-1, k\}$. The range of g follows from $g \leq k$, $(g+\mu_i(C)-i+1) \leq (n-k)$ and $(g-i+1) \geq 0$.

Using the second condition of Proposition 6.0.1 we prove the second condition of our theorem as follows: Choose a set of $(n-k+i-\mu_i(C))$ columns of H with rank $(n-k-\mu_i(C))$. If all these columns are from P, then we have a $(n-k) \times (n-k+i-\mu_i(C))$ submatrix of P with rank $n-k-\mu_i(C)$. Let g' of the $(n-k+i-\mu_i(C))$ columns be from the P submatrix. Then $(n-k+i-\mu_i(C)-g')$ columns are from I. These $(n-k+i-\mu_i(C)-g')$ columns of the I submatrix have rank equal to $(n-k+i-\mu_i(C)-g')$. Therefore in the set of g' columns from the P submatrix we have a $(g'-i+\mu_i(C)) \times g'$ submatrix of P with rank $(g'-i)$.

Now from the third condition Proposition 6.0.1 we establish the third condition of our theorem as follows: Consider a set of $(n-k+\eta)$ columns of H. Let g of these columns be from the P submatrix and the remaining $(n-k+\eta-g)$ columns be from the I submatrix. The rank of the columns from the I submatrix is $(n-k+\eta-g)$. The g columns of the P submatrix has a $g \times (g+\eta)$ submatrix of rank g. If all the $n-k+\eta$ columns of H matrix are from P we have an $(n-k) \times (n-k+\eta)$ submatrix of rank $(n-k)$. This completes Part (i) of the proof.

Part (ii): To prove the first condition of Proposition 6.0.1, pick any $(g+\mu_i(C)-i+1) \times g$ submatrix from P. Take a set of $(n-k+i-1-\mu_i(C)-g)$ columns from the I submatrix such that these columns have zeros in the $(g+\mu_i(C)-i+1)$ rows associated with the $(g+\mu_i(C)-i+1) \times g$ submatrix of P. The $(g+\mu_i(C)-i+1) \times g$ submatrix has rank $\geq (n-k-\mu_i(C))$. Since we have chosen an appropriate set of columns from the I submatrix of H, the $(n-k+i-\mu_i(C))$ columns of H has rank $\geq (n-k-\mu_i(C))$ = sum of the ranks of the columns from the I submatrix and the P submatrix of H.

The second condition of Proposition 6.0.1 is obtained from the second condition of our theorem as follows: From our second condition, it follows that there exists a $(g' + \mu_i(C) - i) \times g'$ submatrix of P with rank equal to $(g' - i + 1)$. Choose $(n - k + i - \mu_i(C) - g')$ columns from the I submatrix of H such that these columns have zeros in the $(g'+\mu_i(C)-i)$ rows associated with the $(g' + \mu_i(C) - i) \times g'$ submatrix of P. These columns have rank $(n - k + i - \mu_i(C) - g')$. Thus we have $(n - k + i - \mu_i(C))$ columns of H with rank $(n - k - \mu_i(C))$ which is equal to the sum of the ranks of columns from the I submatrix and the P submatrix.

The third condition of Proposition 6.0.1 follows from our third condition i.e., every $g \times (g + \eta)$ submatrix of P has rank g as follows: Consider $(n - k - g)$ columns from the I submatrix. Choose these columns from I submatrix such that they have zeros in all the g rows associated with the $g \times (g + \eta)$ submatrix of P. Then we have $(n - k + \eta)$ columns with rank $(n - k)$. This completes the proof. □

The well known systematic check or generator matrix characterization of MDS codes is obtained from Theorem 6.1 by putting $\mu_1(C) = 0$. From the second condition of the theorem we see that every $g \times g$ submatrix of the P submatrix has rank g. This systematic generator matrix characterization is used for constructing MDS codes in [47].

Now we apply our systematic parity matrix characterization of Theorem 6.1 to other well known codes which are close to meeting the generalized Singleton bound in the following sections.

6.3 N^{μ}-MDS Codes

We generalize the classes of NMDS and N^2-MDS codes to μ-Near MDS codes as follows:

Definition 6.2 *An $[n, k]$ linear code C is a μ-Near-MDS code (N^{μ}-MDS), where $1 \leq \mu < (n - k + 1)$, if it has the following HWH:*

$$\begin{aligned} d_r(C) &= (n - k + r) - (\mu - r + 1) \qquad if \;\; 1 \leq r < (\mu + 1) \\ &= (n - k + r) \qquad\qquad\qquad\qquad if \;\; (\mu + 1) \leq r \leq k. \end{aligned} \tag{6.4}$$

Clearly, $\mu = 1$ and $\mu = 2$ give the classes of Near-MDS and Near-Near-MDS codes respectively. Note that the MDS-rank of an N^{μ}-MDS code is $(\mu + 1)$ and it follows from

(6.3) that the dual of an N^{μ}-MDS is also N^{μ}-MDS.

Lemma 6.1.1 *[29] Let C be an $[n,k]$ code with weight hierarchy $[d_i(C) : 1 \leq i \leq k]$. Then $(q^r-1)d_l(C) \leq (q^r - q^{r-l})d_r(C), \quad 1 \leq l \leq r \leq k$. Specializing this to $l=1$ and $r=2$ gives $(q+1)d_1 \leq qd_2$.*

Lemma 6.1.2 *For an $[n,k]$ N^{μ}-MDS code over F_q we have $n \leq 2q+k+(\mu-1)$.*

Proof: From Lemma 6.1.1 we have

$$(q^r-1)d_{r-1}(C) \leq (q^r-q)d_r(C)$$

and for $r=2$

$$(q^2-1)(n-k-\mu+1) \leq (q^2-q)(n-k-\mu+3)$$

The above inequality leads to

$$n \leq 2q+k+\mu-1. \quad \square$$

The following result from [14] is useful in proving Theorem 6.2: For any linear q-ary code C of length $n = 1 + g_q(k,d)$, we can select a generator matrix with codewords of weights not exceeding $t+d$, where

$$g_q(k,d) = \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \tag{6.5}$$

with $\lceil x \rceil$ denoting the smallest integer not less than x.

Theorem 6.2 *For $\mu > 1$, an $[n,k]$ N^{μ}-MDS code over F_q is generated by codewords of weights $(n-k-\mu+1)$, $(n-k-\mu)$ and $(n-k-\mu-1)$. If $n > q+k+\mu-1$ then the code is generated by codewords of weight $(n-k-\mu+1)$ and $(n-k-\mu)$.*

Proof: From the Greismer bound we have

$$n \geq g_q(k, n-k-\mu+1) = \sum_{i=0}^{k-1} \left\lceil \frac{n-k-\mu+1}{q^i} \right\rceil. \tag{6.6}$$

The above equation leads to

$$n \geq g_q(k, n-k-\mu+1) \geq (n-k-\mu+1) + \left\lceil \frac{n-k-\mu+1}{q} \right\rceil + (k-2)$$

(6.7)

which gives

$$n \geq (n-\mu-1) + \left\lceil \frac{n-k-\mu+1}{q} \right\rceil \tag{6.8}$$

where $\lceil \frac{n-k-\mu+1}{q} \rceil$ can take any value from $1, 2, \ldots, (\mu-1)$. But from Lemma 6.1.2 $n \leq 2q + k + (\mu-1)$. Therefore $\lceil \frac{n-k-\mu+1}{q} \rceil$ can take the value 1 or 2 which leads to

$$1 + g_q(k, n-k-\mu+1) \leq n \leq 2 + g_q(k, n-k-\mu+1). \tag{6.9}$$

Now using the result of [14] stated before the theorem statement on the structure of the generator matrices of linear codes, the N^{μ}-MDS code is generated by code words of weights $n-k-\mu+1, n-k-\mu$ or $n-k-\mu+1$. If $n > q+k-\mu+1$ then $n = 1+g(k, n-k-\mu+1)$. Therefore the code is generated by codewords of weights $(n-k-\mu+1)$ and $(n-k-\mu)$. □

Corollary 6.2.1 *An $[n, k]$ code with parity check matrix $[I \mid P]$ is N^{μ}-MDS iff the following conditions are satisfied:*

1. *For $i = 1, 2, \ldots, \mu$*
   - *(a) For $i < g \leq min\{d_i(C) - 1, k\}$, every $(g - 2i + 1 + \mu) \times g$ submatrix of P has rank $\geq (g - i + 1)$.*
   - *(b) There exist a g, $i < g \leq min\{d_i(C), k\}$, such that $(g - 2i + \mu) \times g$ submatrix of P has rank equal to $(g - i)$.*
2. *For $1 < g \leq min\{(n-k), (k-\mu)\}$ every $g \times (g+\mu)$ submatrix of P has rank g.*

Proof: This is a special case of Theorem 6.1. We know that the HWH of N^{μ}-MDS codes is

$$\begin{aligned} d_r(C) &= (n-k+r) - (\mu-r+1) \;\; if \;\; 1 \leq r < (\mu+1) \\ &= (n-k+r) \;\; if \;\; (\mu+1) \leq r \leq k \end{aligned} \tag{6.10}$$

Now $\mu_i(C) = \mu - i + 1$ and substituting $\mu_i(C) = (\mu - i + 1)$ for $1 \leq i \leq \mu$ in Theorem 6.1 the result follows. □

Example 6.1 *The binary code with the following generator matrix is a* $[10, 4, 4]$ N^3*-MDS code:*

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

and the binary code with the following generator matrix is a $[8, 4, 4]$ N^3*-MDS code:*

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

It is easy to check that all the conditions of systematic matrix characterization are satisfied for the two codes of the above example.

Corollary 6.2.2 *: An* $[n, k]$ *code* C *with parity check matrix* $[I \mid P]$ *is* N^2*-MDS iff the following conditions are satisfied:*

1. *For* $1 < g \leq min\{(n-k-2), k\}$ *every* $(g+2) \times g$ *submatrix of* P *has rank* $\geq g$*.*
2. *For* $2 < g \leq min\{(n-k), k\}$ *every* $g \times g$ *submatrix of* P *has rank* $\geq (g-1)$*.*
3. *For* $1 < g \leq min\{(n-k-1), k\}$ *there exits a* $(g+1) \times g$ *submatrix of* P *with rank* $(g-1)$*.*
4. *For* $2 < g \leq min\{(n-k+1), k\}$ *there exits a* $(g-1) \times g$ *submatrix of* P *with rank* $(g-2)$*.*
5. *For* $1 < g \leq min\{(n-k), (k-2)\}$ *every* $g \times (g+2)$ *submatrix of* P *has rank* g*.*

Corollary 6.2.3 *An* $[n, k]$ *code with parity check matrix* $[I \mid P]$ *is NMDS iff the following conditions are satisfied:*

- *For* $1 < g \leq min\{(n-k-1), k\}$ *every* $(g+1) \times g$ *submatrix of* P *has rank* $\geq g$*.*

- *For* $1 < g \leq min\{(n-k), k\}$ *there exists a* $g \times g$ *submatrix of* P *with rank equal to* $(g-1)$.
- *For* $1 < g \leq min\{(n-k), (k-1)\}$ *every* $g \times (g+1)$ *submatrix of* P *has rank* g.

Corollary 6.2.3 has been reported in [65] as an independent result with different proof.

Lemma 6.2.1 *[42] If* $k > q > 3$ *and* $n < 2q - 1 + k$ *then every* $[n, k, (n-k-1)]$ *code* C *is an* N^2*-MDS code.*

Corollary 6.2.4 *For* $k > q > 3$ *and* $n > 2q - 1 + k$*, a code with the systematic parity check matrix* $[I \mid P]$ *is* N^2*-MDS iff every* $(g+2) \times g$ *submatrix of* P *has rank* $\geq g$*.*

Proof: This corollary is obtained by combining following two results: (i) for the given range of n and k any code with $d_1(C) = n - k - 1$ is a N^2-MDS code (follows from Lemma 6.2.1 and (ii) the systematic matrix characterization given in Theorem 6.1. We substitute $\eta_1 = 2$ in Theorem 6.1 to get this characterization of N^2-MDS code. □

Corollary 6.2.5 *If* $n > (k+q)$ *the* $[n, k]$ *code with systematic parity check matrix* $H = [I \mid P]$ *is NMDS iff every* $(g+1) \times g$ *submatrix of* P *has rank* g*.*

Proof: This corollary is obtained by using the fact for the given range of k and n any $(n-k)$ code is a NMDS code. Therefore all we need to show is that $d_1(C) = n - k$. We know that $d_1(C) = (n-k)$ iff every $(n-k-1)$ columns of H are linearly independent and there exist $(n-k)$ linearly dependent columns. Therefore if follows that every $(g+1) \times g$ submatrix of the P submatrix has rank g. Therefore the result follows. □.
The above result is useful in decoding codes for the erasure channel [39], [35], [36].

Example 6.2 *The binary code with the following generator matrix is a* $[8, 3, 4]$ N^2*-MDS code*

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

and the code with the following generator matrix is a N^2-MDS code over F_8

$$\begin{bmatrix} 1 & 0 & 0 & \alpha^3 & \alpha & 1 & \alpha^3 \\ 0 & 1 & 0 & \alpha^6 & 0 & 1 & \alpha^2 \\ 0 & 0 & 1 & 0 & 0 & 1 & \alpha^4 \end{bmatrix}.$$

Proposition 6.2.1 *A code C is dually A^{μ}-MDS iff it's MDS-rank is μ.*

Proof: The MDS-rank is μ implies that $d_{\mu+1}(C) = n - k + \mu + 1$ and $\mu + 1$ is the first i such that $d_i(C) = n - k + i$ for $1 \leq i \leq k$. Therefore $d_{\mu+1}(C) - d_{\mu}(C) \geq 2$. It follows that $d_1(C^{\perp}) = k + 1 - \mu$. Therefore the code is dually A^{μ}-MDS. □

Proposition 6.2.2 *For an A^{μ}-MDS code C with parity check matrix H the following conditions hold*

1. *Every $(n - k - \mu)$ columns of H are linearly independent.*
2. *There exists $(n - k + 1 - \mu)$ linearly dependent columns of H.*

Proof: We have $d_1(C) = n - k + 1 - \mu$. Therefore there exits $(n - k + 1 - \mu)$ linearly dependent columns H and every $(n - k - \mu)$ columns of H are linearly independent. □
The following corollary characterizes dually A^{μ}-MDS codes.

Corollary 6.2.6 *A systematic generator matrix $[I \mid P]$ is of a dually A^{μ}-MDS code (C) iff every $(g + \mu, g)$ and $g \times (g + \mu)$ submatrix of the P submatrix has rank greater than or equal to g.*

Proof: For A^{μ}-MDS code to be dually defective we know that the MDS-rank has to be μ. The proof follows from Theorem 6.1 by taking $\eta_1 = \mu$. For A^{μ}-MDS codes we specify only $d_1(C)$ and other Hamming weights are arbitrary. Therefore we need to ensure only $d_1(C)$. Hence the result essentially follows from Theorem 6.1. □

Example 6.3 *Consider an A^6-MDS code. For the code to be dually A^6-MDS the MDS-rank of the code must be 7. Therefore $d_1 = n - k + 1 - 6$ and $d_7 = n - k + 7$ (7 is the smallest value for which the code meets the generalized Singleton bound). Therefore the difference between μ_6 and μ_7 of the code is at least 1. Applying the relation 6.3 we see that*

$(n+1)-(n-k+7)$ *which is* $(k-6)$ *and* $(n+1)-(n-k+5)=(k-4)$ *are not elements of the weight hierarchy of the dual. Therefore* $d_1(C)$ *of the dual code is* $(k-5)$*, i.e.,* μ_1 *of the dual code is also* 6*.*

Example 6.4 *Consider an* $[n,k]$ *code of MDS-rank 2 and let its HWH be* $\{(n-k),(n-k+1),(n-k+3),\ldots,n\}$*. For this code the HWH of the dual is* $(k-1),(k+2),(k+3),\ldots,n$*. Then, if* $H=[I\mid P]$ *is a parity check matrix of the code then the following conditions characterize the code*

- *Every* $(g+1)\times g$ *submatrix has rank* g*.*
- *Every* $g\times g$ *submatrix has rank* $\geq (g-1)$*.*
- *Every* $g\times(g+1)$ *submatrix has rank* $\geq (g-1)$*.*
- *Every* $g\times(g+2)$ *submatrix has rank* g*.*

If $G=[I\mid P]$ *is a generator matrix of the code then the following conditions characterize the code*

- *Every* $(g+2)\times g$ *submatrix has rank* g*.*
- *Every* $(g+1)\times g$ *submatrix has rank* $\geq (g-1)$*.*
- *Every* $g\times(g+1)$ *submatrix has rank* g*.*

6.4 Matrix Characterization of Dually Defective Codes and Codes meeting Generalized Greismer Bound

We define

Definition 6.3 *The defect vector of an* $[n,k]$ *code* C *with MDS-rank* $(\eta+1)$ *is defined as ordered the set* $\{\mu_1(C),\mu_2(C),\ldots,\mu_\eta(C),\mu_{\eta+1}(C)\}$*, where* $\mu_i(C)=n-k+i-d_i(C)$*. (Note that* $\mu_{\eta+1}(C)$ *is equal to zero.) A code is called dually defective if the defect vector is same for the code and its dual. The difference set of the defect vector of an* $[n,k]$ *code* C *with MDS-rank* η *is the ordered set* $\{(\mu_1(C)-\mu_2(C)),(\mu_2(C)-\mu_3(C)),\ldots,(\mu_{\eta-1}(C)-\mu_\eta(C)),(\mu_\eta(C)-\mu_{\eta+1}(C))\}$*.*

Example 6.5 *Consider an N^2-MDS code. The defect vector is $\{2,1,0\}$ and the difference set is the ordered set $\{(2-1)=1,(1-0)=1\}$. Therefore between the first three Hamming weights of the code there is a gap. From Theorem 6.3 we see that the HWH of the dual code is $\{d_1(C^\perp)=k-1, d_2(C^\perp)=n-k+1, d_3(C^\perp)=n-k+3,\ldots,d_{n-k}(C^\perp)=n\}$. Therefore the defect vector of the dual code $C^\perp$ is $\{2,1,0\}$ and hence C is dually defective. This is shown in figure(6.1).*

Example 6.6 *Consider a code C with $\mu_1(C)=8$. For C to be dually defective it's MDS-rank should be 9 and $(\mu_8(C)-\mu_9(C))>1$. Let the code have a defect vector as $\{8,7,7,7,6,5,4,1,0\}$. The difference set is $\{1,0,0,1,1,1,3,1\}$. Since $\mu_2(C)=\mu_3(C)=\mu_4(C)=7$ and $\mu_5(C)=6$ for the code to be dually defective $(\mu_8(C)-\mu_9(C))=1$ and $(\mu_7(C)-\mu_8(C))=3$. Similarly since $\mu_5(C)=6$ and $\mu_6(C)=5$ we have $(\mu_6(C)-\mu_5(C))=1$.*

In figure(6.2) we have shown the defect vector of the code on the left and that of the dual on the right. The defect vector of the code is read from the top and the defect vector of the dual it is read from bottom. The code is dually defective if there is a symmetry in the difference vector of the code read from the top and the defect vector of the dual code read from the bottom. In terms of the symmetry of the figure we can see that there is an axis of symmetry. About the axis of symmetry for every line with arrow above the axis there is a dotted line below the axis at the same relative distance. Therefore for dually defective code we can see an axis of symmetry.

Now we proceed to study the properties of the defect vector.

Lemma 6.2.2 *For an $[n,k]$ code C with MDS-rank η, we have $\mu_1(C)\geq\mu_2(C)\geq\ldots\mu_\eta(C)\geq\mu_{\eta+1}(C)$.*

Proof: This result can be proved from the monotonicity of the HWH We know that $d_{i+1}(C)>d_i(C)$, i.e., $(n-k+i+1-\mu_{i+1}(C))>(n-k+i-\mu_i(C))$. Simplifying the inequality we get the result $\mu_i(C)+1>\mu_{i+1}(C)$. □

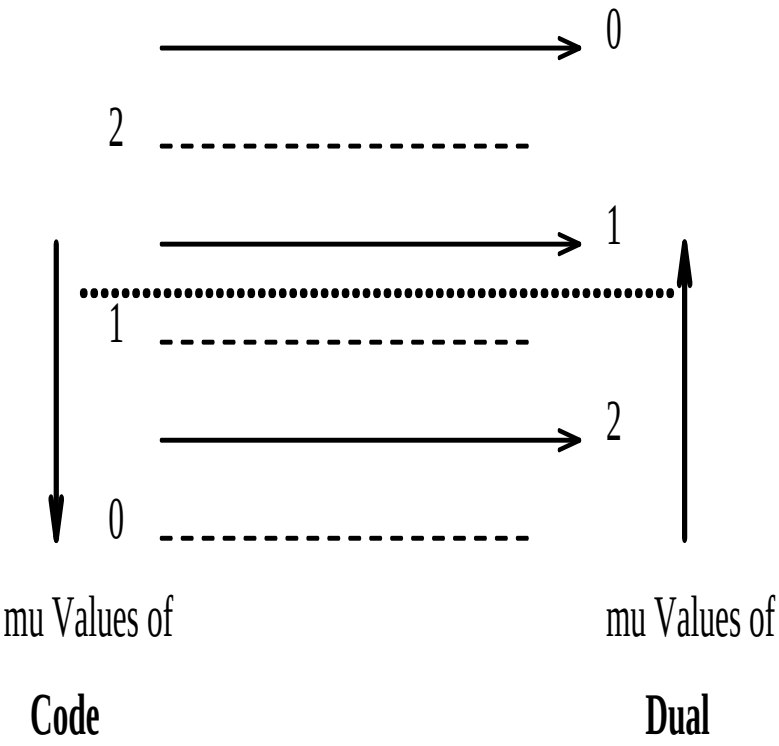


Figure 6.1: The figure shows the defect vector for the Near Near MDS code on the left side. The defect vector for the dual is shown on the right hand side. The bold dotted line shows the axis of symmetry. For every line with arrow above the symmetry axis there is a dashed line without arrow below the axis at the same relative position

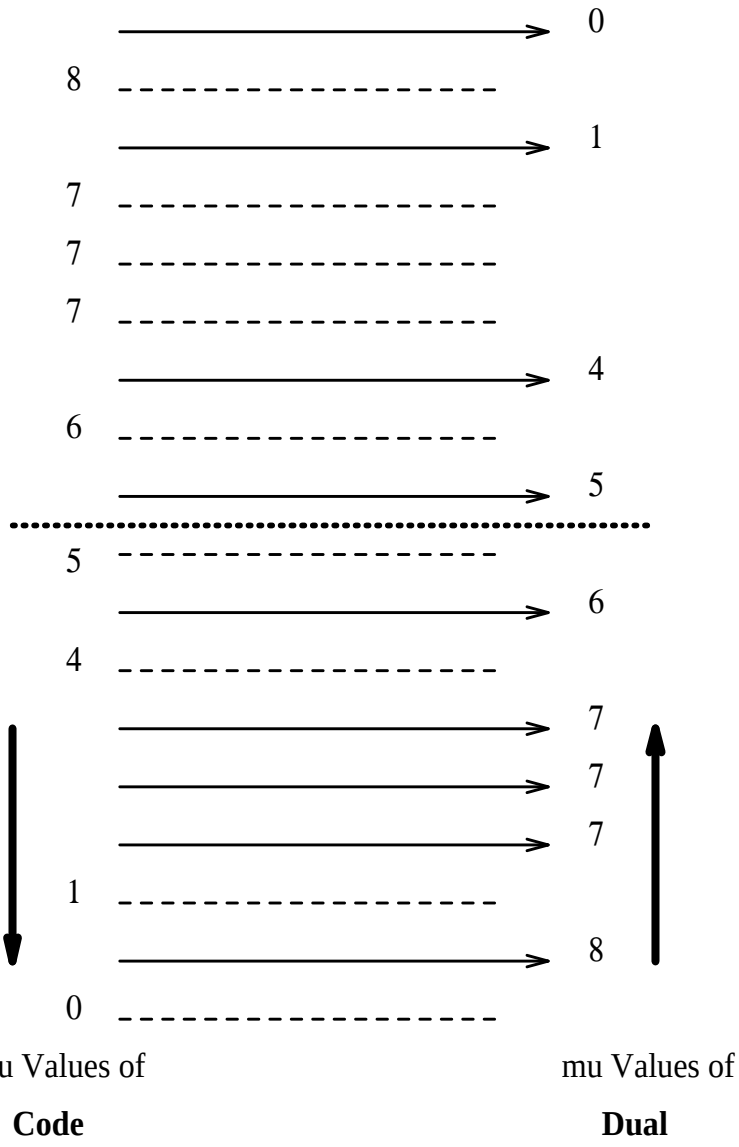


Figure 6.2: The figure shows the defect vector for the code on the left side. The defect vector for the dual is shown on the right hand side. The dotted line shows the axis of symmetry. For every line with arrow above the symmetry axis there is a dashed line without arrow below the axis at the same relative position

Lemma 6.2.3 *Consider an $[n, k]$ code C with MDS-rank η. Then $\sum_{i=1}^{\eta}(\mu_i(C)-\mu_{i+1}(C)) = \mu_1(C)$.*

Proof Since the MDS-rank of C is η we have $\mu_{\eta+1}(C) = 0$. In the sum all terms except $\mu_1(C)$ and $\mu_{\eta+1}(C)$ cancel out. Therefore the sum is equal to μ_1. □

The class of dually defective codes include the well known classes of MDS codes, N^{μ}-MDS codes and self dual codes. The following lemma gives the conditions for a dually A^{μ}-MDS code to be dually defective the proof of which follows from that of Theorem 5.27 of [43] in a straight forward manner,

Lemma 6.2.4 *Let C be an $[n, k, d]$ dually A^{μ}-MDS code over F_q with $s \geq 2$. If $n \leq s(q+1)-1+k$ and $2 \leq s \leq q$. Then C is a dually defective code with $d_1(C) = n-k+1-s$ and $d_i(C) = n - k + i - 1$ for $2 \leq i \leq s$.*

The following proposition gives the matrix characterization of dually defective codes.

Theorem 6.3 *An $[n, k]$ code C with MDS-rank η and systematic generator matrix $[I \mid P]$ is dually defective iff the following conditions are satisfied:*

1. *For $i < g \leq min\{d_i(C)-1, k\}$, every $(g+\mu_i(C)+1-i)\times g$ and $g\times(g+\mu_i(C)+1-i)$ submatrix of P has rank $\geq (g - i + 1)$.*
2. *There exists a g, $i < g \leq min\{d_i(C), k\}$, such that the rank of every $(g-i+\mu_i(C))\times g$ and $g \times (g - i + \mu_i(C))$ submatrix of P is $(g - i)$.*
3. *For $1 < g \leq min\{(n - k), (k - \eta)\}$ every $(g, g + \eta)$ and $(g + \eta) \times g$ submatrix of P has rank g.*

Proof: Let us assume that C is dually defective. Then $d_i(C) = n - k + i - \mu_i(C)$ and $d_i(C^{\perp}) = k + i - \mu_i(C)$. Therefore from Theorem 6.1 every submatrix of $-P^T$, where P^T denotes the transpose of P, of the type $(g + \mu_i(C) - i) \times g$ have rank $\geq (g - i + 1)$ since $d_i(C) = n - k + i - \mu_i(C)$ [65]. For dually defective code $d_i(C^{\perp}) = k + i - \mu_i(C)$. Therefore every $(g+\mu_i(C)-i)\times g$ submatrix of P matrix has rank $\geq (g-i+1)$. Therefore if follows that for every $(g + \mu_i(C) + 1 - i) \times g$ and $g \times (g + \mu_i(C) + 1 - i)$ submatrix of P has rank $\geq (g - i + 1)$.

The fact that $d_i(C) = n-k+i-\mu_i(C)$ and $d_i(C^\perp) = k+i-\mu_i(C)$ leads to the condition that there exist $(g-i+\mu_i(C)) \times g$ and $g \times (g-i+\mu_i(C))$ submatrices of P such that the rank is $(g-i)$. The third condition of the theorem follows similarly. Establishing that the code is dually defective assuming the three conditions is straight forward. □

The following theorem which states the generalized Greismer bound is discussed in detail in [28].

Proposition 6.3.1 (The generalized Greismer bound): *For an $[n,k,d]$ code over F_q we have $d_r(C) \geq \sum_{i=0}^{r-1} \lceil \frac{d}{q^i} \rceil$ for $1 \leq r \leq k$.*

Theorem 6.4 *If an $[n,k,d]$ code C over F_q meets the Greismer bound then the code will have a generator matrix whose structure is as follows:*

$$\begin{array}{ccccc} \overbrace{d_1(C)}^{} & \overbrace{d_2(C)-d_1(C)}^{} & \overbrace{d_3(C)-d_2(C)}^{} & \dots & \overbrace{d_k(C)-d_{k-1}(C)}^{} \\ * & 0 & 0 & \dots & 0 \\ \star & * & 0 & \dots & 0 \\ \star & \star & * & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ \star & \star & \star & \dots & * \end{array} \tag{6.11}$$

where $\star$ denotes an element of F_q, $*$ denotes a non-zero element of F_q and $(d_{i+1}(C)-d_i(C))$ denotes the number of columns with the structure as shown under it.

Proof: As the code meets the Greismer bound for all the values of d_r we can construct the matrix in the proposition as follows. Since the minimum distance is d we can choose a generator matrix with the first row having d consecutive non zeros followed by $n-d$ zeros. Next we know that $d_2(C) = d + \lceil \frac{d}{q} \rceil$. Therefore we can choose a second row such that first d elements can be any element from the field followed by $\lceil \frac{d}{q} \rceil$ non zero elements of the field. Thus we have constructed a two dimensional subcode with support $d_2(C)$ meeting the Greismer bound. It is possible to construct rows with a sequence of zeros and non-zeros as we can permute the columns of the generator matrix without affecting the weight distribution of the code. We can repeat the above construction for all $d_i(C)$ where $3 \leq i \leq k$. Thus we can construct the generator matrix for a code meeting the Greismer bound as given in the proposition. □

From this matrix characterization we can obtain the systematic matrix characterization of codes meeting the (generalized) Greismer bound by elementary row operations and permutations of the columns.

Theorem 6.5 *Consider an* $[n,\ k]$ *code* C *of MDS rank* η *meeting the generalized Greismer bound with defect vector* $\{\mu_1, \mu_2, \ldots, \mu_\eta, \mu_{\eta+1}\}$ *and* $\mu_{\eta+1} = 0$*.Consider the difference set between successive elements of the defect vector* $\{(\mu_1 - \mu_2), (\mu_2 - \mu_3), \ldots, (\mu_i - \mu_{i+1}), \ldots, (\mu_\eta - \mu_{\eta+1})\}$.

1. *If* $(\mu_1 - \mu_2) > 1$ *then the code is not dually defective.*
2. *If the difference set between successive elements of the defect vector is* $\{0, 1, 1, \ldots, 1, 2\}$*, then the code* C *is not dually defective.*
3. *If the difference set between successive elements of the defect vector is* $\{1, 1, 1, \ldots, 1\}$*, then the code* C *is dually defective.*

Proof:

1. Consider the case where $(\mu_1(C) - \mu_2(C)) > 1$. For the proof we make use of the equation(6.3) and the fact code meets the generalized Greismer bound.

   Assume that a dually defective code meeting the generalized Greismer bound exists with $(\mu_1(C) - \mu_2(C)) > 1$. Let $d_1(C) = n - k + 1 - \mu_1(C)$ and $d_2(C) = n - k + 2 - \mu_2(C)$. Let $\mu_1(C) - \mu_2(C) = \delta > 1$. For the code to be dually defective $d_{\eta+1}(C) = n - k + \eta + 1$, $d_\eta(C) = n - k + \eta - 1$ and $d_{\eta-i}(C) = n - k + \eta - i - 1$ for $1 \leq i \leq (\delta - 1)$. Since the code also meets the generalized Greismer bound we have $d_{\eta+1}(C) - d_\eta(C) = \lceil \frac{d_1(C)}{q^\eta} \rceil$. Since the code is assumed to be dually defective we have $\lceil \frac{d_1(C)}{q^\eta} \rceil = 2$. We also have $d_\eta(C) - d_{\eta-1}(C) = \lceil \frac{d_(C)}{q^{\eta-1}} \rceil$. This difference must be equal to 1 for the code to be dually defective. But this is not possible since $\lceil \frac{d_1(C)}{q^\eta} \rceil = 2$. Therefore the code does not meet the generalized Greismer bound. This is a contradiction.

2. Assume that a dually defective code meeting the generalized Greismer bound exists with the given defect vector. Let $d_1(C) = n - k + 1 - \mu_1(C)$ and $d_2(C) = n -$

$k+2-\mu_2(C)$. Note that here $\mu_1(C) = \mu_2(C)$. For the code to be dually defective $d_{\eta+1}(C) = n-k+\eta+1$, $d_\eta(C) = n-k+\eta-2$ and $d_{\eta-1}(C) = n-k+\eta-4$. Since the code meets the generalized Greismer bound we have $d_{\eta+1}(C) - d_\eta(C) = \lceil \frac{d_1(C)}{q^\eta} \rceil$. From that fact that the code is dually defective we have $\lceil \frac{d}{q^\eta} \rceil = 3$. Moreover $d_\eta(C) - d_{\eta-1}(C) = \lceil \frac{d_1(C)}{q^{\eta-1}} \rceil$. This difference is equal to one for the code C. But this is not possible since $\lceil \frac{d_1(C)}{q^\eta} \rceil = 3$. Therefore the code does not meet the generalized Greismer bound. This is a contradiction.

3. Assuming that the difference set between successive elements of the defect vector is an all one set we will prove that the code C is dually defective. Since $\mu_{\eta+1}(C) = 0$ we have $\mu_\eta(C) = 1$. This follows from the fact that the difference between the elements of the defect vector is one. Therefore from equation(6.3) it follows that $\mu_1(C)$ of the dual code is also same as that of the code. Since $\mu_1(C)$ of the code and the dual is same and the difference between all the elements of the defect vector is one all the successive elements of the defect vector of the dual code also differ by one (this follows from equation(6.3)). Therefore the code aswell as its dual have the same defect vector.

□

6.5 Conclusion

The systematic generator matrix of a linear code is unique and the characterization of MDS codes based on systematic generator matrix is well known. Here we have given the systematic generator matrix characterization of a general linear code with a specified Hamming weight hierarchy along with several sub classes of codes like $N^\mu MDS$. We have also discussed matrix characterization of dually defective codes and codes meeting generalized Greismer bound.

Chapter 7

Conclusions

In this thesis we have obtained results in the broad area of upper bounds on codes. Explicitly we have obtained an Elias type upper bound for codes over distance uniform signal sets and characterized codes close to the generalized Singleton bound.

We have obtained the asymptotic Elias type upper bound for a large class of Euclidean space codes over distance uniform signal sets. We also study codes over two, three, four and n-dimensional signal sets and compare them based on the rate per two dimensions.

Further we study codes which are close to the generalized Singleton bound and obtain characterization based on the systematic generator matrix. For $NMDS$ codes we obtain systematic generator matrix characterization. This result is useful to obtain nonexistence results of $AMDS$ and $NMDS$ codes over finite fields. Further the systematic matrix characterization is useful when we consider $NMDS$ or $AMDS$ codes over erasure channels.

Further $AMDS$ and $NMDS$ are characterized over Z_m, finite abelian groups and finite modules over commutative rings. We obtain nonexistence results for these codes over cyclic groups. A similar approach can be taken for non existence results for these codes over finite R-modules.

Matrix characterization of codes with a given Hamming weight hierarchy is also obtained. Based on the matrix characterization we study codes which are close to the generalized Singleton bound. These codes include $A^{\mu}MDS$ codes and $N^{\mu}MDS$ codes. We also study codes meeting the generalized Greismer bound in terms of the systematic matrix characterization. We also define dually defective codes and obtain the matrix characterization.

7.1 Directions for Further Work

1. In Chapter 2, Section 2.2 we obtain Elias type upper bound for codes over distance uniform signal sets. In general there exists several signal sets which are not distance uniform. These include the well known class of rectangular signal sets like QAM. In [27], [55] Gilbert Varshamov type lower bound is obtained for codes over non-uniform signal sets. It will be interesting to obtain an Elias type upper bound for codes over signal sets which are not distance uniform.

2. For codes over finite sets with hamming distance as the metric the linear programing bound gives the tightest upper bound [60]. The Elias upper bound is also discussed [60]. In Chapter 2 and Chapter 3 we obtain an Elias type upper bound for Euclidean space codes over distance uniform signal sets. We also compare the bound for Euclidean space codes over several signal sets based on the rate per two dimensions. But an upper bound based on an approach similar to linear programing bound is not known for Euclidean space codes. This is another interesting area for further research.

3. In Chapter 4 we obtain a systematic matrix characterization for $NMDS$ codes. The systematic matrix characterization of MDS codes is used to construct MDS codes [47]. It is known that every square submatrix of Cauchy matrices over finite fields will be non-singular [39]. In the case of Vandermonde matrices over finite fields every square sub matrix need not be non singular [39]. Construction of MDS codes using Vandermonde matrices is discussed in [35], [36]. The construction of $NMDS$ codes based on the systematic generator matrix characterization discussed in Chapter 4 needs to be explored.

4. In Chapter 5 we discuss the characterization of $AMDS$ and $NMDS$ codes over finite abelian groups. Here we characterize only information set supporting codes. The characterization of these codes over cyclic groups leads to the characterization of systematic $AMDS$ and $NMDS$ codes over Z_m. Characterization of non systematic $AMDS$ and $NMDS$ codes over Z_m is another possible area for further work. In [78] a quasi-determinant characterization is given for MDS codes over non-abelian

groups. Obtaining a quasi determinant characterization of $AMDS$ codes is non trivial since there exists component homomorphisms in the characterization of $AMDS$ codes which are not automorphisms. Therefore obtaining a quasi determinant type characterization for $AMDS$ and $NMDS$ codes is a challenging problem.

5. In Chapter 6 we consider matrix characterization of codes over finite fields with arbitrary generalized Hamming weight hierarchy. The generalized Hamming weight hierarchy of codes over finite chain rings is discussed in [30] and codes over Galois rings in [1]. Matrix characterization of codes over finite chain rings with a given Hamming weight hierarchy is an open problem.

Bibliography

[1] A. Ashikhmin, “On Generalised Hamming Weight for Galois Ring Linear Codes”, *Designs, Codes and Cryptography*, Vol.14, 1998, pp.107-128.

[2] Jaakko T. Astola, “An Elias-Type Bound for Lee Codes over Large Alphabets and its Applications to Perfect Codes”, *IEEE Trans. Information Theory*, Vol.28, No.1, 1982, pp.111-113.

[3] S. Benedetto, E. Bilglieri and Castellani, Digital Transmission Theory, Prentice-Hall, 1987.

[4] E. R. Berlekamp, Algebraic coding Theory, Mc Graw-Hill, 1968.

[5] E. Biglieri, D. Divsalar, P. J. McLane and S. K. Simon, Introduction to Trellis-Coded Modulation with Applications, New York, Macmillan, 1991.

[6] Ezio Biglieri and Michele Elia, “On Construction of Group Block Codes”, *Proc. International Symposium on Information Theory, ISIT*, San Antonio, TX, 1993, pp. 360.

[7] Ezio Biglieri and Michele Elia, “On Construction of Group Block Codes”, *Annals of Telecommunication*, Vol. 50, No. 9-10, 1995, pp. 817-823.

[8] R. E. Blahut, Principles and Practice of Information theory, Addison Wesley, 1987.

[9] Ian F. Blake, “Codes over Integer Residue Rings”, *Information and Control*, Vol. 29, 1975, pp. 295-300.

[10] M. A. deBoer, “Almost MDS Codes”, *Designs, Codes and Cryptography*, Vol.9, 1996, pp.143-155.

[11] H. Brandstorm, "Classification of Codes for Phase and Amplitude Modulated Signals in Four Dimensional Space", Technical Report No.105, Telecommunication theory, Royal Institute of Technology, Stockholm, Sweden, Jan.1995.

[12] C. Caire and E. Biglieri, "Linear Block Codes over Cyclic Groups", *IEEE Trans. Information Theory*, Vol.41, No.5, 1995, pp.1246-1256.

[13] Philip J. Davis, Circulant Matrices, John Wiley, New York, 1979.

[14] S. M. Dodunekov, "A comment on the weight structure of generator matrices of linear codes", *Problems of Information Transmission*,Vol.26, No.2, Apr-June, 1990, pp.173-176.

[15] S. M. Dodunekov and I. N. Landgev, "On Near-MDS Codes", Technical Report, No:LiTH-ISY-R-1563, Department of Electrical Engineering, Linkoping University, February, 1994.

[16] S. M. Dodunekov and I. N. Landgev, "On Near-MDS Codes", *Proc. International Symposium on Information Theory*, Trondheim, Norway, 1994, p.427.

[17] R. Dodunekova, S. M. Dodunekov and Torleiv Klove, "Almost-MDS and Near-MDS codes for error detection", *IEEE Trans. on Information Theory*, IT-Vol.43, No.1, Jan.1997, pp.285-290.

[18] Xue-Dong Dong, Cheong Boon Soh and Erry Gunawan, "Matrix Characterisation of MDS linear codes over modules", *Linear Algebra and its Applications*, Vol.277, 1988, pp. 57-61.

[19] I. Dumer and V. A. Zinovev, "Some new maximal codes over GF(4)", *Problems of Information Transmission*, Vol.14, No.3, Sept.1978, pp.24-34.

[20] T. Ericsson, "Generalizations of the Johnson and the Bassalygo-Elias bounds", *Fourth Joint Swedish-Soviet International Workshop on Information Theory*, Gotland, Sweden, Aug. 27- Sept. 1, 1989.

[21] G. L. Feng, K. K. Tzeng, V. K. Wei, "On the Generalized Hamming Weights of several classes of Cyclic codes", *IEEE Trans. on Information Theory*, IT-Vol.38, No.3, May 1992, pp.1125-1130.

[22] R. R. Fletcher, "Practical Methods of Optimization", John Wiley, New York, 1988.

[23] G. D. Forney, Jr., "Geometrically Uniform Codes", *IEEE Trans. Information Theory*, Vol.IT-37, No.5, Nov.1991, pp.1241-1260.

[24] G. D. Forney, Jr., "On the Hamming Distance Properties of Group Codes", *IEEE Trans. Information Theory*, Vol.IT-38, No.6, 1992, pp. 1797-1801.

[25] R. Garello and S. Benedetto, "Multilevel Construction of Block and Trellis Group Codes", *IEEE Trans. Information Theory*, Vol.IT-41, No.5, Sept.1995, pp.1257-1264.

[26] A. Gresho and V. B. Lawrence, "Multidimensional Signal Constellations for Voice band Data Transmission", *IEEE J. on Selected Areas in Communication*, Vol.SAC-2, No.5, Sept.1984, pp.687-702.

[27] Jian Gu and Tom Fuja, "A Generalised Gilbert-Varshamov Bound Derived via Analysis of a Code-Search Algorithm", *IEEE Trans. on Information Theory*, Vol.IT-39, No.3, May 1993, pp.1089-1093.

[28] T. Helleseth, Torleiv Klove and Oyvind Ytrehus, "Generalized Hamming Weights of Linear Codes", *IEEE Trans. on Information Theory*, IT-Vol.38, No:3, May 1992, pp.1133-1140.

[29] T. Helleseth, T. Klove, V. I. Levenshtein, O. Ytrehus, "Bounds on the Minimum Support Weights", *IEEE Trans. Information Theory*, Vol.IT-41, No.2, Nov.1995, pp.432-440.

[30] H. Horimoto and K. Shiromoto, "On Generalised Hamming Weights for Codes over Finite Chain Rings", *Lecture Notes in Computer Science*, No.2227, 1997, pp.141-150.

[31] J. Carmelo Interlando, Reginaldo Palazzo, Jr., and Michele Elia, "Group Block Codes over Non abelian groups are Asymptotically Bad", *IEEE Trans. on Information Theory*, IT-Vol.42, No.4, May 1996, pp.1277-1280.

[32] T. Kasami, T. Takata, T. Fujiwara and S. Lin, "On the Optimum Bit Order with respect to the State Complexity of Trellis Diagrams for Binary Linear Codes", *IEEE Trans. Information Theory*, Vol.IT-41, No.2, Nov.1995, pp.432-440.

[33] Torleiv Klove, "Support Weight Distribution of Linear Codes", *Discrete Mathematics*, 106/107, 1992, pp.311-316.

[34] F. R. Kschischang, P. G. deBuda and S. Pasupathy, "Block Codes for M-ary Parse Shift Keying", *IEEE J. on Selected Areas in Communications*, Vol.7, No.6, Aug. 1989. pp.900-913.

[35] J. Lacan and J. Fimes, "Construction of Matrices over Finite Fields with No Singular Square Submatrix", *Seventh International Conference on Finite Fields*, Toulouse, France, May 2003.

[36] J. Lacan and J. Fimes, "Systematic MDS Erasure Codes Based on Vandermonde Matrices", paper submitted to *IEEE Communication Letters*, Feb. 2004.

[37] H. A. Loeliger, "Signal Sets Matched to Groups", *IEEE Trans. Information Theory*, Vol.IT-37, No.6, Nov.1991, pp.1675-1682.

[38] H. A. Loeliger, "On Euclidean Space Group codes", Ph.D. Thesis, Swiss Federal Institute of Technology, Zurich, 1992.

[39] F. J. Mac Williams, Theory of Error Correcting Codes, Amsterdam, The Netherlands: North Hollands, 1977.

[40] J. L. Massey, T. Mittelholzer, "Systematicity and rotational Invariance of Convolutional Codes over Rings", *Proc. 2nd Int. Workshop on Algebraic and Combinatorial Coding Theory*, Leningrad Russia, Sept. 1990, pp.6-22.

[41] J. L. Massey, T. Mittelholzer, T. Riedel and M. Vollenweider, “Ring Convolutional codes for Phase Modulation”, *Int. Symposium on Information Theory*, ISIT-90, San Diego, CA, Jan. 1990.

[42] Jonas Olsson, “On Near-Near-MDS Codes”, *Proceedings of Algebraic and Combinatorial Coding Theory Workshop*, Bulgaria, June, 1996, pp. 231-236.

[43] Jonas Olsson, “Linear Codes with Performance Close to Singleton Bound”, Linkoping Studies in Science and Technology, Dissertation No.605, Linkoping, 1999.

[44] L. H. Ozarow and A. D. Wyner, “Wire-Tap Channel of Type-II”, *AT and T Bell Labs Technical Journal*, Vol. 63, 1984, pp. 2135-2157.

[45] W. W. Peterson, and E. J. Weldon, Error Correcting Codes, Cambridge, M.A., MIT Press, 1972

[46] P. Piret, “Bounds for Codes Over the Unit Circle”, *IEEE Trans. Information Theory*, Vol.IT-32, No.6, Nov.1986, pp.760-767.

[47] Ron M. Roth and Gadiel Seroussi, “On Generator Matrices of MDS codes”, *IEEE Trans. on Information Theory*, Vol.IT-31, No.6, Nov. 1985, pp.826-830.

[48] D. Saha and T. Birdsall, “Quadrature-Quadrature Phase-Shift Keying”, *IEEE Trans. on Communication*, Vol.37, No.5, May 1985, pp.437-448.

[49] James R. Schott, Matrix Analysis for Statistics, John Wiley and Sons, New York, 1997

[50] T. V. Selvakumaran and B. Sundar Rajan, “Block Coded Modulation using Two-Level Group Codes Over Generalized Quaternion Groups”, *IEEE Trans. Information Theory*, Vol.45, Jan. 1999, pp. 365-372.

[51] R. C. Singleton, “Maximum Distance Q-Nary Codes”, *IEEE Trans. on Information Theory*, Vol.IT-24, No.2, Apr.1964, pp.116-118.

[52] D. Slepian, “Group Codes for the Gaussian Channel”, *Bell System Technical Journal*, Apr. 1968, pp.575-602.

[53] D. Slepian, "On neighbor distances and symmetries in group codes", *IEEE Trans. Inform. Theory*, Vol.17, Sept.1971, pp.630-632.

[54] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, Berlin, 1993.

[55] Ludo M. G. M. Tolhuizen, "Generalised Gilbert-Varshamov bound is implied by Turan's Theorem", *IEEE Trans. on Information Theory*, Vol.43, Sept.1997, pp.1605-1606.

[56] B. Sundar Rajan, L. Venkata Subramanian and R. Bahl, "Gilbert-Varshamov bound for Euclidean space codes over distance uniform signal sets", *IEEE Trans. on Information Theory*, Vol. 48, No. 2, Feb.2002.

[57] B. Sundar Rajan and G. Viswanath, "Asymptotic Upper Bound for Euclidean Space Codes over Distance Uniform Signal Sets", *IEEE Information Theory Workshop-1999*, Kruger National Park, South Africa, 1999, pp.109.

[58] B. Sundar Rajan and G. Viswanath, "Asymptotic Elias Bound for Euclidean Space Codes over Distance Uniform Signal Sets", *IEICE Trans. on Fundamentals of Information, Communication and Computing*, Vol.E86-A, No.2, Feb.2003, pp.480-486.

[59] M. A. Tsfasman, S. G. Vladut and T. Zink, "Modular Curves, Shimura Curves and Goppa Codes better than Varshamov-Gilbert Bounds", *Matematische Nachrichten*, Vol.109, 1982, pp.21-28.

[60] J. H. Van Lint, Introduction to coding Theory, Heidelberg, Germany, Springer Verlag, 1982.

[61] P. Vanroose, "Code Construction for the Noiseless Binary Switching Multiple-Access Channel", *IEEE Trans. on Information Theory*, Vol. 34, No. 5, Sept. 1988, pp. 1100-1106.

[62] P. Vanroose, "In Search of Maximum Distance Separable Codes over the Ring of Integers Modulo m", Presented in 15-th *Denelux Symposium on Information Theory*, May 30-31, 1994.

[63] A. J. Han Vinck and H. Morita, "Codes over Rings of Integers Modulo m", *IEICE Trans. Fundamentals of Information, Communication and Computing*, Vol. E81-A, No. 10, Oct.1998, pp.2013-2018.

[64] M. Visintin, E. Biglieri and V. Castellani, "Four-Dimensional Signaling for Band limited Channels", *IEEE Trans. on Communications*, Vol.42, No.2/3/4, Feb.-Apr.1989, pp.403-409.

[65] G. Viswanath and B. Sundar Rajan, "Systematic Generator Matrix Characterization of Near-MDS Codes", *Proceedings of the Seventh International Workshop on Algebraic and Combinatorial Coding Theory*, Bansko, Bulgaria, June 18-24, 2000, pp.316-319.

[66] G. Viswanath and B. Sundar Rajan, "Matrix Characterisation of Near-MDS Codes over Finite Fields", accepted for publication in *ARS Combinatorica*.

[67] G. Viswanath and B. Sundar Rajan, "Matrix Characterization of Generalised Hamming Weight Hierarchy", *IEEE International Symposium on Information Theory-2001*, Washington D.C., U.S.A, 2001, pp.61.

[68] G. Viswanath and B. Sundar Rajan, "On Asymptotic Elias Bound for Euclidean Space Codes over Distance Uniform Signal Sets", *IEEE International Symposium on Information Theory-2003*, Yokohama, Japan, pp.466.

[69] G. Viswanath and B. Sundar Rajan, "Matrix Characterisation of Near-MDS Codes over Z_m and Cyclic Groups", *IEEE International Symposium on Information Theory-2004*, Chicago, U. S. A., 2004, pp.528.

[70] G. Viswanath and B. Sundar Rajan, "Matrix Characterization of Generalised Hamming Weight Hierarchy", submitted to *Linear Algebra and its Applications*.

[71] A. J. Viterbi and J. K. Omura, Digital Communication and Coding , McGraw-Hill, 1979.

[72] V. K. Wei, "Generalized Hamming Weights for linear codes", *IEEE Trans. on Information Theory*, IT-Vol.37, No:5, Sept.1991, pp.1412-1418.

[73] G. R. Welti and J. S. Lee, "Digital Transmission with Coherent Four-Dimensional modulation", *IEEE Trans. Information Theory*, Vol.20, No.4, July 1974.

[74] S. B. Wicker and V. K. Bhargava (Eds), Reed-Solomon Codes and their Applications, Chapter 13, pp.292-314, IEEE Press, 1994.

[75] J. M. Wozencraft and I. M. Jacobs, Principles of Communication Engineering, N.Y., Wiley, 1965.

[76] A. A. Zain and B. Sundar Rajan, "Algebraic Characterization of MDS Group Codes over Cyclic Groups", *IEEE Trans. Information Theory*, Vol.41, No.6, Nov.1997, pp.2052-2056.

[77] A. A. Zain and B. Sundar Rajan, "Dual Codes of Systematic Group Codes over Abelian Groups", *Applicable Algebra in Engineering, Communication and Computing*, Vol.8, 1997, pp.1412-1418.

[78] A. A. Zain and B. Sundar Rajan, "Quasi-Determinant Characterisation Dual Codes of MDS Group Codes over Abelian Groups", *Designs, Codes and Cryptography*, Vol.13, 1998, pp.313-330.

[79] L. H. Zetterberg and H. Brandstrom, "Codes for Combined Phase and Amplitude Modulated Signals in Four Dimensional Space", *IEEE Trans. on Communications*, Vol.COM-25, No.9, Sept.1977, pp.943-950.