論文 / 著書情報
Article / Book Information

題目(和文)	代数幾何符号の最適設計に関する研究
Title(English)	Optimum design methods for algebraic geometric codes
著者(和文)	梅原大祐
Author(English)	
出典(和文)	学位:博士(工学), 学位授与機関:東京工業大学, 報告番号:甲第4016号, 授与年月日:1999年3月26日, 学位の種別:課程博士, 審査員:
Citation(English)	Degree:Doctor (Engineering), Conferring organization: Tokyo Institute of Technology, Report number:甲第4016号, Conferred date:1999/3/26, Degree Type:Course doctor, Examiner:
学位種別(和文)	博士論文
Type(English)	Doctoral Thesis

Optimum Design Methods for Algebraic Geometric Codes

Daisuke Umehara

Advisor: Associate Professor Tomohiko Uyematsu

Department of Electrical and Electronic Engineering,
Tokyo Institute of Technology

March 1999

Acknowledgments

This work was based on research done for two years at Japan Advanced Institute of Science and Technology and three years at Tokyo Institute of Technology in Japan. I was helped by many people during my research period.

First of all, I wish to express my sincere gratitude and special thanks to my advisor, Associate Professor Tomohiko Uyematsu of Tokyo Institute of Technology for his constant encouragement and kind guidance during my research.

I also wish to express my deep gratitude to Professor Kohichi Sakaniwa of Tokyo Institute of Technology and Professor Eiji Okamoto of Japan Advanced Institute of Technology, for their suggestions and encouragements.

I also wish to express my gratitude to Professor Masaaki Homma of Kanagawa University and Dr. Shinji Miura of Sony Corporation, for their helpful suggestions and discussions.

I am very grateful to Associate Professor Isao Yamada, Research Assistant Tomoharu Shibuya and Researcher Ryutaroh Matsumoto of Tokyo Institute of Technology for their suggestions and discussions.

I am grateful to Professor Kiyomichi Araki and Professor Kaoru Kurosawa of Tokyo Institute of Technology for their suggestions and discussions.

Contents

List of Figures

Chapter 1

Introduction

1.1 Backgrounds

As data in numerous working communication systems across noisy channels increases, the demand for its reliability grows tremendously. On such a problem for reliable data transmission, C. E. Shannon observed that reliable communication systems across noisy channels could be represented by the block diagram shown in Figure 1.1 and showed an epoch-making and farseeing work so called the channel coding theorem [55]. This theorem states that appropriate codeword set with rate below channel capacity and sufficiently large length enables to achieve an arbitrary small error probability of transmitting data. Although the deterministic design of such codes has not been presented yet, their establishment has been the ultimate goal of data communication. On the other hand, from the combinatorial and constructive viewpoint, R. W. Hamming firstly presented single error-correcting codes called Hamming codes [24], and coding theory originated in their works.

A fundamental problem of coding theory is to find and design constructive good codes with reasonable encoding and decoding complexity. In this dissertation, good codes mean that their length, information rate and relative minimum distance are generally large.

Linear codes form an important class among all codes. In particular, they

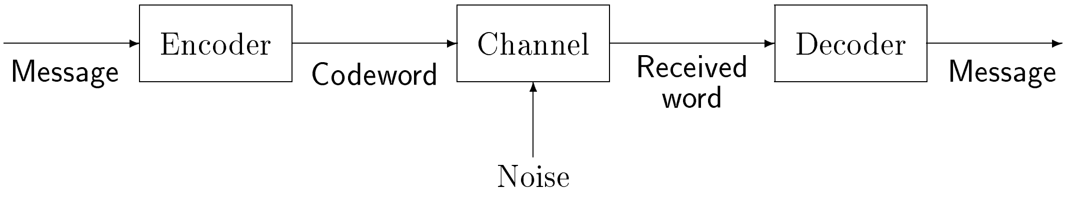


Figure 1.1: Block diagram of a reliable communication system.

provide the reasonable encoding complexity because their encoding is established by a matrix multiplication, and also infinitely many sequences of linear codes asymptotically attain the Gilbert-Varshamov bound [37, 68] which is known as a criterion of good linear codes. So far many good linear codes with reasonable decoding complexity have been designed, for example BCH codes [25, 5], Reed-Solomon codes [49], Goppa codes [16] and so on.

Reed-Solomon codes are known as maximum distance separable codes, that is, they have theoretical largest relative minimum distance for any possible information rate. However, the length of Reed-Solomon codes are restricted to at most finite field size plus one. On the other hand, the design of length and information rate of BCH codes is considerably flexible, and also BCH codes include many good codes. However, their relative minimum distance at positive information rate becomes arbitrary small for sufficiently large length [2]. Goppa codes overcome the shortcoming of BCH codes mentioned above, as an appropriate sequence of Goppa codes asymptotically achieves the Gilbert-Varshamov bound [17]. Unfortunately, the design of good Goppa codes with sufficiently large length has not been established. Thus, for a long time, the design of constructive good linear codes with sufficiently large length was an open problem for linear codes.

In 1981, V. D. Goppa presented a new class of linear codes by using algebraic curves over finite fields and a lower bound of their minimum distance [19, 20, 21], in his deep sight that the Goppa codes could be regarded as linear codes on algebraic lines [18]. Nowadays, these codes are called algebraic geometric codes or geometric Goppa codes, and the lower bound of their minimum distance is called the Goppa designed distance or Goppa bound. Because of the connection between the genus and Goppa designed distance, good algebraic geometric codes are composed of any algebraic curve with many rational points as compared with its genus, where genus is an invariant of the algebraic curve. Thus, a fundamental problem of algebraic geometric codes is to find such an algebraic curve and design codes on this one explicitly. In particular, Miura [39] presented two extensive families of plane curves which were denoted by $\boldsymbol{C}_a^b$ and ${}_r\boldsymbol{C}_a^b$ and provided their parity check matrices. Also, these families $\boldsymbol{C}_a^b$ and ${}_r\boldsymbol{C}_a^b$ include the well-known elliptic, hyper-elliptic and Hermitian curves, and besides many maximal curves which mean that their rational points are maximal as compared with their genus. Therefore, the class of codes on algebraic curves in $\boldsymbol{C}_a^b$ and ${}_r\boldsymbol{C}_a^b$ include many constructive good codes. In fact, the codes on many algebraic curves in $\boldsymbol{C}_a^b$ and ${}_r\boldsymbol{C}_a^b$ have better parameters than the conventional algebraic codes [42, 70, 71].

Ihara [26] and Tsfasman et al. [62, 60] showed the existence of algebraic curves which attained the Drinfeld-Vlăduţ bound by studying the number of rational points and genera on modular curves over finite fields. This means that there exists a sequence of codes satisfying the Tsfasman-Vlăduţ-Zink bound which is better than the Gilbert-Varshamov bound in a certain range when finite field size is a square and at least 49. Furthermore, Katsman et al. [29, 67, 68] showed that the construction of the modular curves and the corresponding codes could be done with polynomial complexity of degree 20 for classical modular curves and degree 30 for Drinfeld modular curves. The degree for the latter was reduced to 17 by Lopéz [35]. These remarkable works provided a solution for the polynomial-time design of good codes with sufficiently large length, and hence attracted many coding theoreticians to algebraic geometric codes. However, the construction of codes on modular curves still has too high complexity for practical applications. On the other hand, Garcia and Stichtenoth [14, 15] recently presented two distinct towers of Artin-Schreier extensions of algebraic function fields over finite fields, which attained the Drinfeld-Vlăduţ bound. These towers have an advantage over sequences of modular curves in that they have the explicit descriptions. At the present time, many coding theoreticians have attempted to give explicit descriptions of codes from any algebraic function field on these towers, for example [69, 23, 64, 46, 47]. Unfortunately, this objective is not quite finished yet.

In another aspect of algebraic geometric codes, their class was extremely extensive among all linear codes, for example this class included Reed-Solomon codes as algebraic geometric codes on algebraic lines. Goppa claimed that every linear code could be represented by algebraic geometric codes on appropriate algebraic curves [20], and unfortunately his proof was not sufficient. In 1991, Pellikaan et al. [48] eventually, completely solved this problem. Therefore, all linear codes can be classified in compliance with their algebraic geometric representation.

In 1989, Justesen et al. [28] first developed a decoding algorithm for algebraic geometric codes on plane curves. Further, Skorobogatov and Vlăduţ [56] extended this algorithm to arbitrary algebraic curves. These algorithms can be decoded up to half the Goppa designed distance minus the genus. These remarkable works caused an active period of research on decoding algorithms for algebraic geometric codes. In 1993, Feng and Rao [9] eventually completed this decoding problem by using the majority voting among unknown syndromes. The decoding algorithm proposed by Feng and Rao can correct up to half the Goppa designed distance with polynomial complexity of at most degree three. Furthermore, the majority voting among unknown syndromes supplied a new lower bound of the minimum distance beyond the Goppa bound. Now, this lower bound of the minimum distance is called the Feng-Rao designed distance or Feng-Rao bound.

Summarizing the results above for algebraic geometric codes, Goppa's construction provides many constructive good codes with reasonable decoding complexity. However, as the theory of algebraic geometric codes depended heavily on methods and results from algebraic curves, many beginners required much time and effort on the comprehension of this theory. So this fact yielded the movement to give an elementary treatment for algebraic geometric codes. The earlier works concerned with this movement were given by Lint et al. [34] and Justesen et al. [28]. From the viewpoint of majority voting among unknown syndromes, Feng et al. [9, 11, 13] simplified the construction, decoding and parameter determination for algebraic geometric codes without directly using the theory of algebraic curves. Besides, Feng and Rao [12] proposed a new construction of linear codes on arbitrary algebraic varieties and gave several examples such that the proposed codes had better parameters than the ordinary algebraic geometric codes when their information rate was sufficiently large. Based on these works for algebraic geometric codes, Miura [42, 43] formulated the decoding by majority voting among unknown syndromes and the Feng-Rao designed distance for arbitrary linear codes by introducing the notion of ordered bases. Consecutively, Miura [42, 43, 44] presented an explicit construction of linear codes on algebraic varieties and curves by using the monomial orders and Gröbner bases.

1.2 Objects and Outline of the Dissertation

The generalization of construction and decoding from the codes on algebraic curves to arbitrary linear codes yields optimization problems for the Feng-Rao designed distance. This dissertation deals with the design and optimization of linear codes with Feng-Rao designed distance in compliance with their construction methods.

The dissertation consists of six chapters. After the introduction, Chapter 2 is devoted to show the fundamental concepts of error-correcting codes. We first show the basic concept of block codes and their encoding and decoding problems. Next, we introduce linear codes for the purpose of simplifying the encoding and decoding. Lastly, we briefly survey algebraic geometric codes by Goppa's formulation and their basic properties.

In Chapter 3, we provide a criterion for linear codes with Feng-Rao designed distance. We first investigate the equivalent relation for ordered bases to have the identical Feng-Rao designed distance. As a result, we obtain a representative of ordered bases which provide the identical Feng-Rao designed distance. This representative is called standard normal form. Furthermore, we present a translation of any ordered basis to ordered basis whose Feng-Rao designed distance is not less than the former.

In Chapter 4, we show an optimization problem of monomial orders for the Feng-Rao designed distance of the codes on the Hermitian curve. We present explicit descriptions of the Hermitian codes for any monomial order. Then, we investigate the relationship between the monomial orders and well-behaving pairs. As a result, we obtain various conditions for monomial orders to have the large Feng-Rao designed distance, and then present a class of monomial orders which provide the largest Feng-Rao designed distance for any redundancy.

In Chapter 5, we consider the third function field on a Garcia-Stichtenoth's tower of function fields. This function field has many rational places as compared with its genus, and therefore generates many good algebraic geometric codes. We present an explicit and complete description of one-point codes from the third function field. Also, we optimize the decoding complexity of the proposed codes in the viewpoint of the number of generators of nongaps. Especially, a proposed code has the parameter [4047,1047,2504] whereas the corresponding BCH code has the parameter [4047,1047,1980]. This code can be decoded up to more 261 errors than the corresponding BCH codes.

Chapter 6 summarize results of the dissertation.

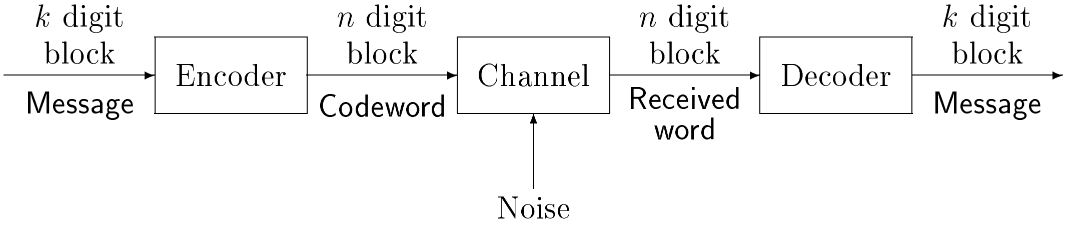
Notation: Let $\mathbb{K}$ denote a field and $\overline{\mathbb{K}}$ its algebraic closure. Let $\mathbb{F}_q = \mathrm{GF}(q)$ denote the finite field with q elements. Let $\mathbb{R}$ denote the field of real numbers and $\mathbb{Q}$ the field of rational numbers. Let $\mathbb{Z}$ denote the set of integers, $\mathbb{N}$ the set of positive integers, and $\mathbb{N}_0$ the set of nonnegative integers. Let $[m, n]$ denote the set of integers which are at least m and at most n. The cardinality of a finite set S is denoted by $\#S$. Let $\mathbf{0}$ and $\mathbf{1}$ denote $(0, 0, \cdots, 0)$ and $(1, 1, \cdots, 1)$, respectively. The transpose of any matrix $\mathbf{M}$ is denoted by $\mathbf{M}^T$.

Chapter 2

Fundamental Concepts of Error-Correcting Codes

In this chapter, we give a brief survey of the concepts of error-correcting codes. Suppose that we wish to transmit a sequence of finite alphabet across a noisy channel. If we transmit any symbol, then the transmitted symbol will probably be received. Occasionally, however, the channel noise will cause a transmitted symbol to be mistakenly interpreted as another symbol. Although we are unable to prevent the channel from causing such errors, we can reduce their undesirable effects with the use of coding. The basic idea of error-correcting codes is simple. We take a set of k massage symbols which we wish to transmit, annex to them r check symbols, and transmit the entire block of $n = k + r$ symbols. Assuming that the channel noise changes sufficiently few of these n transmitted symbols, the r check symbols may provide the receiver with sufficient information to enable him to detect and correct the channel errors. This is shown in Figure 2.1.

According to the method of coding, error-correcting codes can be divided broadly into block codes and tree codes. In this dissertation, we consider the



Message:	k digits
Codeword:	n digits
Information rate:	k/n

Figure 2.1: Error-correcting codes across a noisy channel.

block codes as the object of our research. This chapter is organized as follows. In Section 2.1, we show the basic concept of the block codes and their encoding and decoding problems. In Section 2.2, we introduce linear codes which are block codes with some algebraic structure. Their algebraic structure simplify their encoding and decoding problems. In Section 2.3, we provide the definition of algebraic geometric codes by Goppa's formulation and develop their main properties.

2.1 Block Codes

We briefly formalize the error-correcting principle based on block codes. As for the deep and general analysis for the block codes, we refer to [3, 4, 27, 36, 31].

Let $\mathbb{F}$ be a finite alphabet with q symbols, say $\mathbb{F} = \{0, 1, 2, \cdots, q-1\}$. Let $\mathbb{F}^m$ denote the set of m-tuples of $\mathbb{F}$ for any positive integer m. An element of $\mathbb{F}^m$ means a sequence of length m. An encoder is formulated by an injective map

$$\mathcal{E} : \mathbb{F}^k \to \mathbb{F}^n, \tag{2.1}$$

and the image of this map $\mathcal{E}$ forms an $[n, k]$ block code C. The number n, k and $r = n - k$ are called *length, number of information symbols* and *redundancy*, respectively. Also, the number k/n means an efficiency of transmission and is called *information rate*. A decoder for the block code C is formulated by a map

$$\mathcal{D} : \ \mathbb{F}^n \to C \cup \{?\} \tag{2.2}$$

such as $\mathcal{D}(\boldsymbol{c}) = \boldsymbol{c}$ for any codeword $\boldsymbol{c}$, where outcome "?" means a *decoding failure* which occurs when the decoder will not decode the received word into any of the possible transmitted codeword. A *decoding error* of the decoder occurs when the decoded word is different from the transmitted codeword. For any two n-tuples $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$ and $\boldsymbol{y} = (y_1, y_2, \cdots, y_n)$, the *Hamming distance* or simply *distance* $d(\boldsymbol{x}, \boldsymbol{y})$ of $\boldsymbol{x}$ and $\boldsymbol{y}$ is defined by

$$d(\boldsymbol{x}, \boldsymbol{y}) := \#\{i \in [1, n] \,|\, x_i \neq y_i\}. \tag{2.3}$$

The Hamming distance is a *metric* on $\mathbb{F}^n$. That is, for any n-tuples $\boldsymbol{x}$, $\boldsymbol{y}$ and $\boldsymbol{z}$, $d(\boldsymbol{x}, \boldsymbol{y}) \geq 0$ if equality holds only if $\boldsymbol{x} = \boldsymbol{y}$, $d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{y}, \boldsymbol{x})$, and $d(\boldsymbol{x}, \boldsymbol{y}) \leq d(\boldsymbol{x}, \boldsymbol{y}) + d(\boldsymbol{y}, \boldsymbol{z})$. If $\boldsymbol{c}$ is a transmitted codeword and $\boldsymbol{y}$ is the corresponding received word, then the Hamming distance $d(\boldsymbol{c}, \boldsymbol{y})$ is nothing else but the number of errors caused by the channel noise.

Definition 2.1.1. A *minimum distance decoder* for a block code C is a decoder $\mathcal{D}$ such that $\mathcal{D}(\boldsymbol{y})$ assigns one of the codewords which are closest in all the codewords with respect to Hamming distance for any n-tuple $\boldsymbol{y}$ of $\mathbb{F}$. □

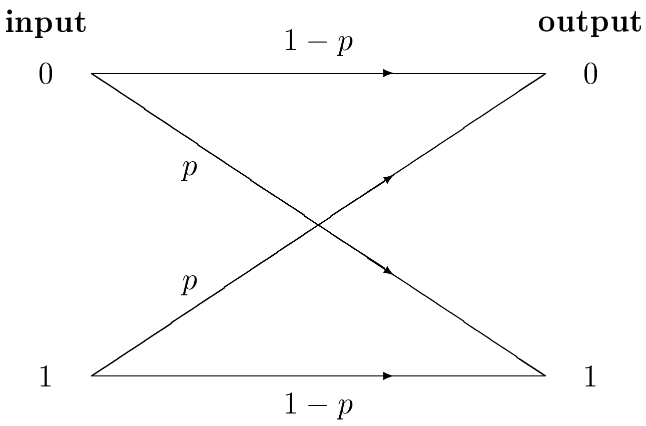


Figure 2.2: Binary symmetric channel.

If we are using a channel with the property that an error in position i does not influence other positions and a symbol in error can be each of the remaining $q-1$ symbols with equal probability, then the Hamming distance is a good way to measure the error content of the received message. Such a channel is called a *q-ary symmetric channel*, and is formulated by

$$P(b|a) = \begin{cases} 1-p & \text{if } a = b, \\ p/(q-1) & \text{if } a \neq b, \end{cases}$$

where $P(b|a)$ is the conditional probability of a symbol b given a symbol a and p is a real number such that $0 \leq p < (q-1)/q$. The q-ary symmetric channel in binary case, that is, the binary symmetric channel is illustrated in Figure 2.2. In fact, when we are using a q-ary symmetric channel, the minimum distance decoding is equivalent to the *maximum likelihood decoding*, which minimizes the probability of a decoding error [42, p. 17, Lemma 2.1].

The *minimum distance* $d = d(C)$ of the block code C is the Hamming distance of the pair of codewords with smallest Hamming distance. That is,

$$d = d(C) = \min\{d(\boldsymbol{x}, \boldsymbol{y}) \,|\, \boldsymbol{x}, \boldsymbol{y} \in C \text{ and } \boldsymbol{x} \neq \boldsymbol{y}\}. \tag{2.4}$$

The $[n, k]$ block code with minimum distance d is also denoted by the $[n, k, d]$ block code. If t errors occur such as

$$d \geq 2t + 1, \tag{2.5}$$

then the decoder will properly correct the errors if it presumes that the closest codeword to the received word was actually transmitted. It may be possible sometimes to correct certain error patterns with t errors even when the inequality (2.5) is not satisfied. However, t-error correction can not be guaranteed if $d < 2t + 1$, because it then depends on which codeword is transmitted and on the actual pattern of the t errors within the block.

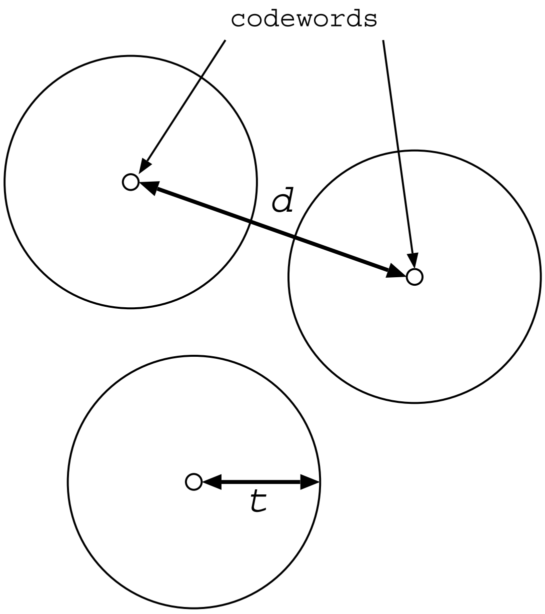


Figure 2.3: Decoding spheres.

Definition 2.1.2. Let t be any nonnegative integer satisfying (2.5). A decoder $\mathcal{D}$ for a block code C is called a *bounded distance decoder* which *corrects t errors* if

$$\mathcal{D}(\boldsymbol{y}) = \begin{cases} \boldsymbol{c} & \text{if } \boldsymbol{c} \in C \text{ and } d(\boldsymbol{c},\boldsymbol{y}) \le t, \\ ? & \text{otherwise,} \end{cases} \tag{2.6}$$

for any n-tuple $\boldsymbol{y}$ of $\mathbb{F}$. In particular, if $d = 2t+1$ or $d = 2t+2$, then the decoder $\mathcal{D}$ is said to *decode up to half the minimum distance.* □

As the minimum distance d becomes large as compared with n, more errors may be corrected by using appropriate bounded distance decoders. Therefore, the number d/n means an error-correction capability for the $[n,k,d]$ block code and is called *relative minimum distance.*

The bounded distance decoder which corrects t errors is geometrically illustrated with Figure 2.3. Note that arbitrary codewords are centered in the sphere of radius t. Figure 2.3 tells us that the spheres of radius t around the codewords are disjoint. The rule (2.6) means that any received word in a sphere is decoded as the codeword at the center of that sphere. If t or fewer errors occur, then the received word is always in the proper sphere and the decoding is correct. If the received word has more than t errors and does not lie in any decoding sphere, then the decoder yields a decoding failure. On the other hand, if the received word has more than t errors and lies in a certain sphere, then the decoder yields a decoding error.

Summarizing the arguments above, we would like to find a block code whose information rate and relative minimum distance are both large. However, there is a limit to the number of spheres of radius t which put into whole space of n-tuples of $\mathbb{F}$. This means that the number of information symbols k is limited when the length n and minimum distance d are given. Conversely, the minimum distance d is limited when the length n and number of information symbols k are given. From the heuristic arguments, we have a trade-off between the information rate k/n and the relative minimum distance d/n. Further, the following is a fundamental result of the theory of block codes: as the length n is large for given k/n and d/n, the error probability becomes small. Therefore, a fundamental problem of block codes is to find one which has generally large length, information rate and relative minimum distance, if we take no thought of its encoding and decoding methods.

2.2 Linear Codes

We now turn to the problem of constructing block codes which have some algebraic structure. Their algebraic structure will provide guidance in the search for good block codes and also help to make the encoders and decoders practical. The first idea is to take the finite field $\mathbb{F}_q$ with q elements as alphabet, and to take a linear subspace C of the n-dimensional linear space $\mathbb{F}_q^n$ as block code.

Definition 2.2.1. A *linear code* C is a linear subspace of the n-dimensional linear space $\mathbb{F}_q^n$ over $\mathbb{F}_q$. If C has *dimension* k, then C is called an $[n, k]$ linear code. □

The *Hamming weight* or simply *weight* $w(\boldsymbol{x})$ of an n-tuple $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$ of $\mathbb{F}_q$ is defined by

$$w(\boldsymbol{x}) := d(\boldsymbol{x}, \mathbf{0}) = \#\{i \in [1, n] \,|\, x_i \neq 0\}. \tag{2.7}$$

Since the Hamming distance $d(\boldsymbol{x}, \boldsymbol{y})$ between two n-tuples $\boldsymbol{x}$ and $\boldsymbol{y}$ is the number of positions in which they differ, $d(\boldsymbol{x}, \boldsymbol{y})$ is equal to $w(\boldsymbol{x} - \boldsymbol{y})$. If $\boldsymbol{x}$ and $\boldsymbol{y}$ are both codewords of a linear code, then $\boldsymbol{x} - \boldsymbol{y}$ must also be a codeword. Therefore, the Hamming distance between any two codewords equals the Hamming weight of some other codeword, and the minimum distance $d(C)$ of a linear code C is equal to the *minimum weight* of its nonzero n-tuples, that is,

$$d(C) = \min\{w(\boldsymbol{c}) \,|\, \boldsymbol{c} \in C \text{ and } \boldsymbol{c} \neq \mathbf{0}\}. \tag{2.8}$$

This property is extremely helpful in analyzing the distance structure of linear codes.

Next, we introduce a matrix representation for linear codes. A *generator matrix* $\mathbf{G}$ for an $[n, k]$ linear code C is defined by a $k \times n$ matrix $\mathbf{G}$ whose rows form a basis of the subspace C. At this time, an encoder $\mathcal{E}$ of any $[n,k]$ linear code C can be realized efficiently by using a generator matrix $\mathbf{G}$ as follows:

$$\mathcal{E}(\boldsymbol{x}) = \boldsymbol{x} \cdot \mathbf{G}, \tag{2.9}$$

for any k-tuple $\boldsymbol{x}$ of $\mathbb{F}_q$. With this expression defining the encoder, the correspondence between messages and codewords depends on the choice of generator matrix for the linear code C, and however the total set of codewords is unaffected. The generator matrix is a concise way to describe a linear code. For example, a binary $[100, 80]$ linear code is described by $100 \times 80 = 8000$ bits, and however needs more than 10^{26} bits if we list all codewords.

The *standard inner product* on $\mathbb{F}_q^n$ is defined by

$$\boldsymbol{x} \cdot \boldsymbol{y}^T := x_1y_1 + x_2y_2 + \cdots + x_ny_n \tag{2.10}$$

for any n-tuples $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$ and $\boldsymbol{y} = (y_1, y_2, \cdots, y_n)$. The *dual code* $C^\perp$ of a linear code C is defined by

$$C^\perp := \{\boldsymbol{x} \in \mathbb{F}^n \mid \boldsymbol{x} \cdot \boldsymbol{c}^T = 0 \text{ for all } \boldsymbol{c} \in C\}. \tag{2.11}$$

From [4, p. 41, Theorem 2.6.9], the dual code of an $[n,k]$ linear code is an $[n, n-k]$ linear code.

Now, we present an alternative matrix representation of linear codes. Let C be any $[n,k]$ linear code. A generator matrix $\mathbf{H}$ of the dual code $C^\perp$ is called a *parity check matrix* for C. Since $C^\perp$ is the $[n, n-k]$ linear code, any parity check matrix $\mathbf{H}$ for C is an $(n-k) \times n$ matrix with rank $n-k$, and therefore we obtain

$$C = \{\boldsymbol{x} \in \mathbb{F}_q^n \mid \boldsymbol{x} \cdot \mathbf{H}^T = \mathbf{0}\}. \tag{2.12}$$

This means that a received word $\boldsymbol{y}$ is a codeword if and only if $\boldsymbol{y} \cdot \mathbf{H}^T$ is all zero $(n-k)$-tuple. Thus, a parity check matrix checks whether a received word $\boldsymbol{y}$ is a codeword or not.

Let $\boldsymbol{c}$ be a codeword of a linear code C with weight w, and $\mathbf{H}$ a parity check matrix for C. Since $\boldsymbol{c} \cdot \mathbf{H}^T = \mathbf{0}$ and $w(\boldsymbol{c}) = w$, some w columns of $\mathbf{H}$ are linearly dependent. Conversely, if some w columns of $\mathbf{H}$ are linearly dependent, then there exists a codeword with weight w. As a result, the following proposition is obtained.

Proposition 2.2.1. [36, p. 33, Theorem 10] Let C be any linear code and $\mathbf{H}$ any parity check matrix for C. Then, the linear code C has minimum distance d if and only if every $d-1$ columns of $\mathbf{H}$ are linearly independent and some d columns are linearly dependent. □

Any parity check matrix $\mathbf{H}$ for an $[n,k]$ linear code C has rank $n-k$, and hence linearly independent columns of $\mathbf{H}$ is at most $n-k$. Therefore, we obtain the following bound.

Proposition 2.2.2. (Singleton Bound). [36, p. 33, Theorem 11] Let C be any $[n, k, d]$ linear code. Then,

$$k + d \leq n + 1. \tag{2.13}$$

□

Linear codes with $k + d = n + 1$ are called *maximum distance separable* (MDS) codes. Reed-Solomon codes are celebrated as MDS codes. The Singleton bound does not take into consideration the alphabet volume. Therefore, several other known upper bounds (for example, Hamming bound, Plotkin bound and so on) are stronger than the Singleton bound if n is large as compared with q. As for the upper bounds above, we refer to [3, 4, 27, 36, 31].

Next, we consider the general decoding problem for linear codes. Let C be any $[n, k]$ linear code and $\mathbf{H}$ any parity check matrix of C. If $\boldsymbol{y}$ is any received word, the $(n-k)$-tuple $\boldsymbol{y} \cdot \mathbf{H}^T$ is called the *syndrome.* The syndrome has much information of channel errors. The set of all words with the same syndrome as $\boldsymbol{y}$ is the *coset* $\boldsymbol{y} + C$. An element of the coset $\boldsymbol{y} + C$ of minimal weight is called a *coset leader.* A simple minimum distance decoder consists of an exhaustive search for a coset leader. An alternative would be to make a list of all coset leaders. Unfortunately, both the previous decoding methods have exponential complexity as a function of the length. Especially, the problem of computing the minimum distance of a linear code is NP-hard, and the corresponding decision problem is NP-complete [66].

2.3 Algebraic Geometric Codes

In this section, we give a brief survey of the notions of algebraic geometric codes by Goppa's formulation [19, 20, 21, 22] and their properties. As for the deep and general properties of algebraic geometric codes, we refer to several text books [22, 33, 45, 58, 61].

Let $\overline{\mathbb{F}}_q$ denote the algebraic closure of the finite field $\mathbb{F}_q$. Let $\mathbb{P}^t = \mathbb{P}^t(\overline{\mathbb{F}}_q)$ denote the t-dimensional *projective space* over $\overline{\mathbb{F}}_q$. An $\mathbb{F}_q$*-rational point* or *rational place* in $\mathbb{P}^t$ is a point whose coordinates are in $\mathbb{F}_q$.

Let $\mathcal{X}$ denote a *projective, nonsingular, absolutely irreducible curve defined over* $\mathbb{F}_q$ in $\mathbb{P}^t$, and $\mathcal{X}(\mathbb{F}_q)$ the finite set of all $\mathbb{F}_q$-rational points on the curve $\mathcal{X}$. Assume that $\mathcal{X}(\mathbb{F}_q)$ is not empty. The *function field* on $\mathcal{X}$ over $\mathbb{F}_q$ is denoted by $\mathbb{F}_q(\mathcal{X})$. Then, there exists a rational function $f \in \mathbb{F}_q(\mathcal{X})$ such that $\mathbb{F}_q(\mathcal{X})$ is a finite algebraic extension of $\mathbb{F}_q(f)$ and $\mathbb{F}_q$ is algebraically closed in $\mathbb{F}_q(\mathcal{X})$ by the assumption that $\mathcal{X}(\mathbb{F}_q)$ is not empty. That is, $\mathbb{F}_q(\mathcal{X})$ is an *algebraic function field of one variable over* $\mathbb{F}_q$. Let $\Omega_{\mathcal{X}}$ denote the linear space of rational differential forms on $\mathcal{X}$. Let $Aut(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ denote the group of automorphisms of $\overline{\mathbb{F}}_q$ over $\mathbb{F}_q$.

An $\mathbb{F}_q$-rational divisor G of $\mathbb{F}_q(\mathcal{X})$ is defined by a formal finite sum

$$G = \sum_{P \in \mathcal{X}} n_P \cdot P$$

with coefficients n_P in $\mathbb{Z}$ such that

$$\sum_{P \in \mathcal{X}} n_P \cdot P = \sum_{P \in \mathcal{X}} n_P \cdot \sigma(P),$$

where $\sigma(P) := (\sigma(a_0) : \sigma(a_1) : \cdots : \sigma(a_t))$ for any point $P = (a_0 : a_1 : \cdots : a_t) \in \mathcal{X}$. Note that $\sigma(P) \in \mathcal{X}$ for any $P \in \mathcal{X}$. The *degree* of an $\mathbb{F}_q$-rational divisor $G = \sum n_P \cdot P$ is defined by $\deg(G) := \sum n_P$. The support of an $\mathbb{F}_q$-rational divisor G, which is the set of points with nonzero coefficient in G, is denoted by *supp*(G). A partial order on $\mathbb{F}_q$-rational divisors of $\mathcal{X}$ is defined by $\sum n_P \cdot P \geq \sum m_P \cdot P$ if $n_P \geq m_P$ for any point $P \in \mathcal{X}$. The *discrete valuation* at $P \in \mathcal{X}$ is denoted by v_P. For any rational function $f \in \mathbb{F}_q(\mathcal{X}) \setminus \{0\}$, the *principal divisor* of a rational function f is defined by

$$(f) := \sum_{P \in \mathcal{X}} v_P(f) \cdot P,$$

and then the divisor (f) is an $\mathbb{F}_q$-rational divisor. The principal divisor of f is uniquely represented by the difference $(f) = (f)_0 - (f)_\infty$ with $(f)_0 \geq 0$ and $(f)_\infty \geq 0$, where $(f)_0$ is the *divisor of zeros* and $(f)_\infty$ is the *divisor of poles* of f. For any $\mathbb{F}_q$-rational divisor G on $\mathcal{X}$, a subset of $\mathbb{F}_q(\mathcal{X})$ is defined by

$$L(G) := \{f \in \mathbb{F}_q(\mathcal{X}) \mid f = 0 \text{ or } (f) \geq -G\}. \tag{2.14}$$

This subset $L(G)$ forms a finite-dimensional linear space over $\mathbb{F}_q$, and its dimension is denoted by $l(G)$. The genus of $\mathcal{X}$ is defined by the finite nonnegative integer

$$g(\mathcal{X}) := \max\{\deg(G) - l(G) + 1 \mid G \text{ is any } \mathbb{F}_q\text{-rational divisor of } \mathcal{X}\}, \tag{2.15}$$

simply denoted by g if it is clear which curve is meant. At any point P on $\mathcal{X}$ there exists a *local parameter* $u \in \mathbb{F}_q(\mathcal{X})$ such that $v_P(u) = 1$, and then for any nonzero rational differential form ω there exists a rational function f such that $\omega = f\,du$. At this time, the valuation $v_P(\omega)$ of ω at P is defined by $v_P(f)$, and then the divisor of ω is defined by

$$(\omega) := \sum_{P \in \mathcal{X}} v_P(\omega) \cdot P,$$

which is called the *canonical divisor*. The divisor (ω) is also an $\mathbb{F}_q$-rational divisor, and has the properties that $\deg((\omega)) = 2g-2$ and $l((\omega)) = g$. For any $\mathbb{F}_q$-rational divisor G, a subset of $\Omega_{\mathcal{X}}$ is defined by

$$\Omega(G) := \{\omega \in \Omega_{\mathcal{X}} \mid \omega = 0 \text{ or } (\omega) \geq G\}, \tag{2.16}$$

which is a finite-dimensional linear space over $\mathbb{F}_q$. The dimension of $\Omega(G)$ is denoted by $i(G)$. The Riemann-Roch theorem provides the relation between $l(G)$ and $i(G)$ for any $\mathbb{F}_q$-rational divisor G.

Proposition 2.3.1. (Riemann-Roch Theorem). [58, p. 28, Theorem I.5.15] Let G be any $\mathbb{F}_q$-rational divisor on $\mathcal{X}$. Then,

$$l(G) = \deg(G) - g + 1 + i(G). \tag{2.17}$$

□

Let $P_1, P_2, \cdots, P_n \in \mathcal{X}(\mathbb{F}_q)$ be n distinct $\mathbb{F}_q$-rational points on $\mathcal{X}$. The divisor $P_1 + P_2 + \cdots + P_n$ is denoted by D. Let G be an $\mathbb{F}_q$-rational divisor on $\mathcal{X}$ of degree m with support disjoint from the support of D. The *evaluation map* ev_D from $L(G)$ into $\mathbb{F}_q^n$ is defined by

$$\mathrm{ev}_D(f) := (f(P_1), f(P_2), \cdots, f(P_n)) \tag{2.18}$$

for any rational function $f \in L(G)$. Further, the *residue map* res_D from $\Omega(G-D)$ into $\mathbb{F}_q^n$ is defined by

$$\mathrm{res}_D(\omega) := (\mathrm{res}_{P_1}(\omega), \mathrm{res}_{P_2}(\omega), \cdots, \mathrm{res}_{P_n}(\omega)). \tag{2.19}$$

for any rational differential form $\omega \in \Omega(G - D)$, where $\mathrm{res}_P(\omega)$ is the *residue* of ω at P.

Definition 2.3.1. The linear code $C_L(\mathcal{X}, D, G)$ is defined by

$$C_L(\mathcal{X}, D, G) = \{\mathrm{ev}_D(f) \mid f \in L(G)\}. \tag{2.20}$$

The code $C_L(\mathcal{X}, D, G)$ is called the *functional Goppa* code associated with D and G. The linear code $C_\Omega(\mathcal{X}, D, G)$ is defined by

$$C_\Omega(\mathcal{X}, D, G) = \{\mathrm{res}_D(\omega) \mid \omega \in \Omega_{\mathcal{X}}\}. \tag{2.21}$$

The codes $C_\Omega(\mathcal{X}, D, G)$ is called the *residue Goppa* code associated with D and G. Both the codes $C_L(\mathcal{X}, D, G)$ and $C_\Omega(\mathcal{X}, D, G)$ is called the *algebraic geometric* or *geometric Goppa* codes. The codes $C_L(\mathcal{X}, D, G)$ and $C_\Omega(\mathcal{X}, D, G)$ are abbreviated to $C_L(D, G)$ and $C_\Omega(D, G)$ respectively, if it is clear which curve is meant. □

In particular, if the $\mathbb{F}_q$-rational divisor G is of form mQ for some integer m and $\mathbb{F}_q$-rational point Q, then both the codes $C_L(D, mQ)$ and $C_\Omega(D, mQ)$ is called the *one-point algebraic geometric* or simply *one-point* codes. The algebraic structure of one-point codes is extremely helpful in analyzing the dimension, minimum distance and decoding complexity.

The length, the dimension, and the minimum distance of the algebraic geometric codes $C_L(D, G)$ and $C_\Omega(D, G)$ are related as follows:

Proposition 2.3.2. [58, p. 43, Theorem II.2.2 and p. 45, Theorem II.2.7]

(a) The code $C_L(D,G)$ is an $[n,k,d]$ linear code with

$$k \geq l(G) - l(G-D) \qquad \text{and} \qquad d \geq n - m. \tag{2.22}$$

The integer $d_G := n - m$ is called the *Goppa designed distance* or *Goppa bound* of $C_L(D,G)$. In particular, if $m < n$, then $k = l(G) \geq m - g + 1$, and furthermore if $2g - 2 < m < n$, then $k = m - g + 1$.

(b) The code $C_\Omega(D,G)$ is a linear $[n,k,d]$ code with

$$k = i(G-D) - i(G) \qquad \text{and} \qquad d \geq m - 2g + 2. \tag{2.23}$$

The integer $d_G := m - 2g - 2$ is called the *Goppa designed distance* or *Goppa bound* of $C_\Omega(D,G)$. In particular, if $2g - 2 < m$, then $k = i(G-D) \geq n - m + g - 1$, and furthermore if $2g - 2 < m < n$, then $k = n - m + g - 1$.

□

From (2.22) and (2.23), both the codes $C_L(D,G)$ and $C_\Omega(D,G)$ have

$$k + d \geq n - g + 1, \tag{2.24}$$

and hence

$$R + \delta \geq 1 - \frac{g}{n}, \tag{2.25}$$

where R and δ denote the information rate and relative minimum distance, respectively. Equation (2.25) means that good algebraic geometric codes have many $\mathbb{F}_q$-rational points as compared with its genus. Therefore, a fundamental problem of algebraic geometric codes is to find such an algebraic curve. As a measure of parameters of algebraic geometric codes, the Hasse-Weil upper bound is celebrated.

Proposition 2.3.3. (Hasse-Weil upper bound). Let N denote the number of $\mathbb{F}_q$-rational points on a curve $\mathcal{X}$ with genus g. Then,

$$N \leq q + 1 + 2g\sqrt{q}. \tag{2.26}$$

□

The relation between the functional Goppa codes and the residue Goppa codes is provided by the following two proposition.

Proposition 2.3.4. [58, p. 46, Theorem II.2.8] The algebraic geometric codes $C_L(D,G)$ and $C_\Omega(D,G)$ are dual to each other, that is,

$$C_\Omega(D,G) = C_L(D,G)^\perp. \tag{2.27}$$

□

Proposition 2.3.5. [58, p. 47, Lemma II.2.9 and p. 48, Proposition II.2.10] There exists a differential form η such that a simple pole at P_i and $\mathrm{res}_{P_i}(\eta) = 1$ for any $i \in [1, n]$. Then,

$$C_\Omega(D, G) = C_L(D, D - G + (\eta)). \tag{2.28}$$

□

The linear code C is called *algebraic geometric* if there exists a projective, nonsingular, absolutely irreducible curve $\mathcal{X}$ defined over $\mathbb{F}_q$ with genus g, n distinct $\mathbb{F}_q$-rational points $P_1, P_2, \cdots, P_n$ on $\mathcal{X}$ and a $\mathbb{F}_q$-rational divisor G with support disjoint from the support of D, where $D = P_1 + P_2 + \cdots + P_n$, such that $C = C_L(\mathcal{X}, D, G)$. At this time, the triple $(\mathcal{X}, D, G)$ is called the *algebraic geometric representation* of C. From Proposition 2.3.5, C is algebraic geometric if and only if $C = C_\Omega(\mathcal{X}, D, G)$ for some curve $\mathcal{X}$ and divisors D and G. Pellikaan et al. has shown the following remarkable result in their paper [48].

Proposition 2.3.6. [48, p. 591, Theorem 2] Let C be any linear code over $\mathbb{F}_q$. Then, C has an algebraic geometric representation $(\mathcal{X}, D, G)$. □

This theorem enables to classify in compliance with their algebraic geometric representation.

Chapter 3

A Criterion for Linear Codes with Feng-Rao Designed Distance

Feng and Rao [9] developed an elegant decoding algorithm for any one-point codes $C_\Omega(D, mQ)$, which can be corrected up to half the Goppa designed distance with complexity at most $O(n^3)$ by using the *majority voting* among *unknown syndromes*. Duursma [8] extended this decoding algorithm to codes on arbitrary algebraic curves. Further, as a result of the majority voting, it was noticed that one can even correct beyond half the Goppa designed distance when their redundancy is small as compared with their length [11]. This was formalized by Kirfel and Pellikaan [30] who introduced the *Feng-Rao designed distance* or the *Feng-Rao bound* for algebraic geometric codes. Via the decoding by majority voting among unknown syndromes, Feng et al. presented simple approaches for the construction and the determination of parameters of algebraic geometric codes without directly using the theory of algebraic curves [9, 11, 13]. Furthermore, Feng and Rao [12] proposed a new construction of linear codes on arbitrary algebraic varieties by using the notion of *well-behaving sequence*. These codes are called *improved geometric Goppa codes* which can correct up to equal or more errors by majority voting as compared with ordinary algebraic geometric codes at the same redundancy. Grounding on the these achievements for algebraic geometric codes, Miura formulated the decoding by majority voting among unknown syndromes and the Feng-Rao designed distance for arbitrary linear codes by introducing the notion of *ordered bases* [42, 43].

In this chapter, we investigate the Feng-Rao designed distance of linear codes over the finite field $\mathbb{F}_q$. The Feng-Rao designed distance of linear codes is dominated by the ordered bases, which are defined in Section 3.1. A fundamental problem of linear codes with Feng-Rao designed distance is to specify a class of order bases which provide the largest Feng-Rao designed distance for any redundancy. The brute method to specify such a class of ordered bases is to calculate and compare their Feng-Rao designed distances for all possible ordered bases. However, now that the number of all distinct ordered based has $O(q^{n^2})$, such a method is intractable. Therefore, it plays an important role in engineering to reduce ordered bases that one should search.

In this chapter, we firstly clarify that the Feng-Rao designed distance of linear codes depends on the *subspace sequence* which is introduced in Sections 3.1 and 3.2. This means that all the ordered bases having the same subspace sequence provide the same Feng-Rao designed distance for any redundancy. Also, we clarify that under any column permutation of an ordered basis the Feng-Rao designed distance is invariant for any redundancy. At this time, the ordered bases that one should search can be restricted to in *standard normal form* which is introduced in Section 3.2. In particular, any ordered basis is put in standard normal form as the Feng-Rao designed distance is kept by using the Gaussian elimination only with the elementary row operation and column permutation. Further, we present the following algorithm: The input to the algorithm is any ordered basis. The output to the algorithm is the ordered basis in standard normal form whose first vector entries are all one in $\mathbb{F}_q$. Then, the Feng-Rao designed distance for the output ordered basis is larger than or equal to that for the input ordered basis. As a consequence of these, ordered bases that one should search can be restricted to in standard normal form whose first vector entries are all one in $\mathbb{F}_q$, and then their number exactly has $q^{\frac{1}{2}(n^2-3n+2)}$. The results in this chapter is based in part on a study presented at IEICE Information Theory Workshop [65].

3.1 Linear Codes with Feng-Rao Designed Distance

In this section, we introduce the Miura's formulation for linear codes with Feng-Rao designed distance [42, 43].

A positive integer n is designed as the length of linear codes. Let $\mathbb{F}_q^n$ denote the set of n-tuples of $\mathbb{F}_q$. It is well-known that $\mathbb{F}_q^n$ is the linear space over $\mathbb{F}_q$ with dimension n under ordinary summation and scalar multiplication. Further, the product of $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$ and $\boldsymbol{y} = (y_1, y_2, \cdots, y_n)$ in $\mathbb{F}_q^n$ is defined by

$$\boldsymbol{x} \cdot \boldsymbol{y} := (x_1y_1, x_2y_2, \cdots, x_ny_n),$$

and then $\mathbb{F}_q^n$ has a structure of $\mathbb{F}_q$-algebra. The zero element and identity element of $\mathbb{F}_q^n$ are denoted by $\mathbf{0} := (0, 0, \cdots, 0)$ and $\mathbf{1} := (1, 1, \cdots, 1)$, respectively. An *ordered basis* of $\mathbb{F}_q^n$ is defined as an n-tuple

$$\mathcal{B}_n := (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$$

of $\mathbb{F}_q^n$ such that $B_n := \{\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n\}$ is a basis of $\mathbb{F}_q^n$. The set of ordered bases of $\mathbb{F}_q^n$ is denoted by $\boldsymbol{O}_n$. Any ordered basis $\mathcal{B}_n = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ has the one-to-one correspondence to the following $n \times n$ nonsingular matrix with entries in $\mathbb{F}_q$

$$\mathbf{B}_n := \begin{bmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \\ \vdots \\ \boldsymbol{b}_n \end{bmatrix}.$$

The order of the sequence $\mathcal{B}_n$ play a crucial role to provide a lower bound for the minimum distance of codes constructed in this section. The total number of ordered bases of $\mathbb{F}_q^n$, which corresponds to the total number of nonsingular matrices with entries in $\mathbb{F}_q$, is

$$\#\boldsymbol{O}_n = \prod_{\ell=0}^{n-1}(q^n - q^\ell) = q^{\frac{1}{2}(n^2-n)} \prod_{\ell=0}^{n-1}(q^{\ell+1} - 1). \tag{3.1}$$

Therefore, the total number of ordered bases has the order $O(q^{n^2})$.

Hereafter, we define linear codes from the ordered basis $\mathcal{B}_n$. Designing $r \in [0, n-1]$ as the redundancy, let $H = \{\boldsymbol{h}_1, \boldsymbol{h}_2, \cdots, \boldsymbol{h}_r\}$ be any subset of B_n with cardinality r and define the corresponding $r \times n$ matrix

$$\mathbf{H} := \begin{bmatrix} \boldsymbol{h}_1 \\ \boldsymbol{h}_2 \\ \vdots \\ \boldsymbol{h}_r \end{bmatrix}. \tag{3.2}$$

Definition 3.1.1. The linear code $C(\mathcal{B}_n, H)$ over $\mathbb{F}_q$ is defined as the null space of the matrix $\mathbf{H}$ given by (3.2), that is,

$$C(\mathcal{B}_n, H) := \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \mathbf{H}^T = \mathbf{0}\},$$

where $\mathbf{H}^T$ is the transposed matrix of $\mathbf{H}$. The code $C(\mathcal{B}_n, H)$ is called by the *linear code associated with $\mathcal{B}_n$ and H*. If it is clear which ordered basis is meant, $C(\mathcal{B}_n, H)$ is abbreviated to $C(H)$. □

The linear code $C(H)$ have the length n and the dimension $k = n - r$. Hereafter, we introduce the Feng-Rao designed distance for the linear code $C(H)$ at Miura's formulation [42, 43].

Define the set $B_0 := \{\mathbf{0}\}$ and $B_s := \{\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_s\}$ for any $s \in [1, n]$. Further, the s-dimensional linear subspace spanned by B_s is denoted by $V_s := \mathrm{Span}\{B_s\}$ for any $s \in [0, n]$. The sequence of subspaces, denoted by $\mathcal{V}_n := (V_1, V_2, \cdots, V_n)$, has the following properties:

$$\begin{cases} \{\mathbf{0}\} = V_0 \underset{\neq}{\subset} V_1 \underset{\neq}{\subset} V_2 \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} V_n = \mathbb{F}_q^n, \\ \dim V_s = s \qquad \text{for all } s \in [0, n]. \end{cases} \tag{3.3}$$

This sequence of subspaces $\mathcal{V}_n$ is called the *subspace sequence* of $\mathbb{F}_q^n$ generated by $\mathcal{B}_n$. Any ordered basis generates a unique subspace sequence. The map $\mathrm{ord}_{\mathcal{B}_n}$ from $\mathbb{F}_q^n$ onto $[0, n]$ is defined by

$$\mathrm{ord}_{\mathcal{B}_n}(\boldsymbol{x}) := \min\{s \,|\, \boldsymbol{x} \in V_s\}. \tag{3.4}$$

for $\boldsymbol{x} \in \mathbb{F}_q^n$. This map $\mathrm{ord}_{\mathcal{B}_n}$ is called the *order map* of $\mathbb{F}_q^n$ corresponding to $\mathcal{B}_n$, and abbreviated to ord if it is clear which ordered basis is meant. A fundamental property of the order map is presented as follows:

Proposition 3.1.1. [43, p. 1396, Lemma 3.2.1] For any $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$ and $\alpha, \beta \in \mathbb{F}_q$,

$$\mathrm{ord}(\alpha\boldsymbol{x} + \beta\boldsymbol{y}) \leq \max\{\mathrm{ord}(\boldsymbol{x}), \mathrm{ord}(\boldsymbol{y})\}. \tag{3.5}$$

In particular, if $\alpha \neq 0$, $\beta \neq 0$ and $\mathrm{ord}(\boldsymbol{x}) \neq \mathrm{ord}(\boldsymbol{y})$, then

$$\mathrm{ord}(\alpha\boldsymbol{x} + \beta\boldsymbol{y}) = \max\{\mathrm{ord}(\boldsymbol{x}), \mathrm{ord}(\boldsymbol{y})\}. \tag{3.6}$$

□

Next, we introduce the notion of well-behaving which plays a crucial role to determine a lower bound for the minimum distance of the linear code $C(H)$.

Definition 3.1.2. A pair (i, j) in $\mathcal{B}_n$ is said to be *well-behaving* if $\mathrm{ord}(\boldsymbol{b}_u\boldsymbol{b}_v) < \mathrm{ord}(\boldsymbol{b}_i\boldsymbol{b}_j)$ for any pair $(u, v) \in [1, n]^2$ with $(u, v) <_P (i, j)$, where the relation $\geq_P$ on $[1, n]^2$ is a partial order defined by $(u, v) \leq_P (i, j)$ if $u \leq i$ and $v \leq j$. □

A nonnegative integer N_s is defined by

$$N_s := \#\{(i, j) \in [1, n]^2 \,|\, \mathrm{ord}(\boldsymbol{b}_i\boldsymbol{b}_j) = s \text{ and } (i, j) \text{ is well-behaving}\} \tag{3.7}$$

for any $s \in [1, n]$. The sequence of n nonnegative integers

$$N(\mathcal{B}_n) := (N_1, N_2, \cdots, N_n) \tag{3.8}$$

is called the *evaluation sequence* for the ordered basis $\mathcal{B}_n$. This sequence $N(\mathcal{B}_n)$ has the following properties:

Proposition 3.1.2. [43, p. 1389, Lemmas 3.1 and 3.2] Let $N(\mathcal{B}_n)$ be the evaluation sequence for any ordered basis $\mathcal{B}_n$. Then, $0 \leq N_s \leq s$ for any $s \in [1, n]$, that is,

$$N(\mathcal{B}_n) \in [0, 1] \times [0, 2] \times \cdots \times [0, n].$$

Furthermore, $N(\mathcal{B}_n)$ can be calculated with complexity $O(n^4)$. □

Definition 3.1.3. The *Feng-Rao designed distance* or *Feng-Rao bound* of the linear code $C(H)$ is defined by

$$d_{FR}(C(H)) := \min\{N_s \,|\, \boldsymbol{b}_s \notin H\}. \tag{3.9}$$

□

By Definition 3.1.3, we can see that the Feng-Rao designed distance $d_{FR}(C(H))$ of the linear code $C(H)$ is dependent only on the ordered basis $\mathcal{B}_n$ and the subset B of B_n. The linear code $C(H)$ associated with $\mathcal{B}_n$ and H has the following properties:

Proposition 3.1.3. [43, p. 1389, Theorem 3.4 and 3.5] The linear code $C(H)$ given by Definition 3.1.1 has the length n, the dimension $k = n - r$, and the minimum distance $d_{\min}(C(H))$ satisfying

$$d_{\min}(C(H)) \geq d_{FR}(C(H)). \tag{3.10}$$

The *Feng-Rao decoding algorithm* [9, 13] can be decoded up to half the Feng-Rao designed distance $d_{FR}(C(H))$ with complexity at most $O(n^3)$ for the linear code $C(H)$. □

Remark 3.1.1. Let $\boldsymbol{w} := (w_1, w_2, \cdots, w_n)$ be an n-tuple of $\mathbb{F}_q \backslash \{0\}$. The diagonal matrix of $\boldsymbol{w}$ is defined by

$$\mathbf{D}(\boldsymbol{w}) := \begin{bmatrix} w_1 & & & \text{\Large 0} \\ & w_2 & & \\ & & \ddots & \\ \text{\Large 0} & & & w_n \end{bmatrix}.$$

For the linear code with a parity check matrix $\mathbf{H} \cdot \mathbf{D}(\boldsymbol{w})$, using the Feng-Rao decoding algorithm, one can be also decoded up to $\lfloor (d_{FR}(C(H)) - 1)/2 \rfloor$ errors with complexity at most $O(n^3)$. This is the reason that $\boldsymbol{c} \cdot \boldsymbol{w}$ is a codeword of the linear code $C(H)$ with the parity check matrix $\mathbf{H}$ if $\boldsymbol{c}$ is a transmission word. This technique is equal to the decoding technique of alternant codes used a decoding algorithm of BCH codes. In this chapter, we do not consider such a modification of decoding since the matrix $\mathbf{H}$ is essentially used in the decoding. □

Next, according to the formulation above, we consider a class of the linear codes with largest Feng-Rao designed distance for given the ordered basis $\mathcal{B}_n$ and the redundancy r. Let $N(\mathcal{B}_n) = (N_1, N_2, \cdots, N_n)$ be the evaluation sequence for $\mathcal{B}_n$. Let π be a permutation of $[1, n]$ such that $N_{\pi(i)} \leq N_{\pi(j)}$ if $i < j$. In general, the permutation π is not always uniquely determined. The subset H_π of B_n is defined by $H_\pi := \{\boldsymbol{b}_{\pi(1)}, \boldsymbol{b}_{\pi(2)}, \cdots, \boldsymbol{b}_{\pi(r)}\}$. By the definition of the Feng-Rao designed distance, we obtain

$$d_{FR}(C_(H_\pi)) = N_{\pi(r+1)} \geq d_{FR}(C(H)),$$

for any subset H of B_n with cardinality r. Therefore, the linear code $C(H_\pi)$ is a linear code with largest Feng-Rao designed distance for given the ordered basis $\mathcal{B}_n$ and the redundancy r. Therefore, a class of linear codes with largest Feng-Rao designed distance is uniquely determined with respect to the ordered basis $\mathcal{B}_n$ and the redundancy r. In this dissertation, one linear code in such a class is represented by $C_r(\mathcal{B}_n)$ or simply by C_r if it is clear which ordered basis is meant. The linear codes $C_r(\mathcal{B}_n)$ is called the *linear codes associated with $\mathcal{B}_n$ and r*. Hereafter, when the ordered basis $\mathcal{B}_n$ is given, we consider only the linear code $C_r(\mathcal{B}_n)$ in this dissertation. The sequence of n nonnegative integers

$$\mathcal{N}(\mathcal{B}_n) := (N_{\pi(1)}, N_{\pi(2)}, \cdots, N_{\pi(n)}) \tag{3.11}$$

is called the *designed distance sequence* for any ordered basis $\mathcal{B}_n$. This sequence displays the Feng-Rao designed distance $d_{FR}(C_r) = N_{\pi(r+1)}$ of the linear code C_r for any redundancy r.

The choice of the ordered basis $\mathcal{B}_n$ affects the Feng-Rao designed distance for any redundancy. For given the length n and redundancy r, we would like to find the ordered basis $\mathcal{B}_n$ which provides the linear code C_r with largest Feng-Rao designed distance $d_{FR}(C_r)$. The brute method to find such an ordered basis is to calculate and compare the Feng-Rao designed distances for all possible ordered bases. However, the total number of ordered bases is too numerous to calculate the designed distance sequences for all possible ordered bases. In the next sections, we show the various relations with respect to ordered bases in order to reduce ordered bases that one should search.

3.2 Criteria for Linear Codes to Have Identical Feng-Rao Designed Distance

In this section, we provide two sufficient conditions for the linear code $C_r(\mathcal{B}_n)$ to have the identical Feng-Rao designed distance $d_{FR}(C_r(\mathcal{B}_n))$. The ordered basis $\mathcal{B}_n$ and $\mathcal{B}'_n$ are called *evaluated equivalent* if both the evaluation sequences of $\mathcal{B}_n$ and $\mathcal{B}'_n$ are identical, that is,

$$N(\mathcal{B}_n) = N(\mathcal{B}'_n).$$

If the ordered bases $\mathcal{B}_n$ and $\mathcal{B}'_n$ are evaluated equivalent, both the Feng-Rao designed distance $d_{FR}(C_r(\mathcal{B}_n))$ and $d_{FR}(C_r(\mathcal{B}'_n))$ are identical for any redundancy r.

3.2.1 Subspace Sequence

In this subsection, we firstly provide a sequence of subspaces $\mathcal{V}_n = (V_1, V_2, \cdots, V_n)$ satisfying the conditions (3.3). This sequence is called the *subspace sequence* of $\mathbb{F}_q^n$. Let $\boldsymbol{b}_s$ and $\boldsymbol{b}'_s$ be two n-tuples in $V_s \setminus V_{s-1}$ for any $s \in [1, n]$. Then, both the sequences $\mathcal{B}_n := (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ and $\mathcal{B}'_n := (\boldsymbol{b}'_1, \boldsymbol{b}'_2, \cdots, \boldsymbol{b}'_n)$ are the ordered bases having the same subspace sequence $\mathcal{V}_n$, and hence said to be generated by the subspace sequence $\mathcal{V}_n$. Then, both the order maps of $\mathcal{B}_n$ and $\mathcal{B}'_n$ are identical by the definition (3.4). These maps $\mathrm{ord}_{\mathcal{B}_n}$ and $\mathrm{ord}_{\mathcal{B}'_n}$ are called the *order map corresponding to* the subspace sequence $\mathcal{V}_n$ and denoted by $\mathrm{ord}_{\mathcal{V}_n}$ in suitable case.

Lemma 3.2.1. Let $\mathcal{B}_n = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ and $\mathcal{B}'_n = (\boldsymbol{b}'_1, \boldsymbol{b}'_2, \cdots, \boldsymbol{b}'_n)$ be two ordered bases having the same subspace sequence. If a pair (i, j) in either $\mathcal{B}_n$ or $\mathcal{B}'_n$ is well-behaving, then

$$\mathrm{ord}(\boldsymbol{b}_i\boldsymbol{b}_j) = \mathrm{ord}(\boldsymbol{b}'_i\boldsymbol{b}'_j).$$

□

Proof. Without loss of generality, we can assume that a pair (i, j) in $\mathcal{B}_n$ is well-behaving. The n-tuples $\boldsymbol{b}'_i$ and $\boldsymbol{b}'_j$ can be represented by

$$\boldsymbol{b}'_i = \sum_{\ell=1}^{i} \alpha_{i\ell}\boldsymbol{b}_\ell \qquad \text{and} \qquad \boldsymbol{b}'_j = \sum_{m=1}^{j} \alpha_{jm}\boldsymbol{b}_m$$

for some $\alpha_{i\ell}, \alpha_{jm} \in \mathbb{F}_q$ where $\alpha_{ii} \neq 0$ and $\alpha_{jj} \neq 0$. Then, the product $\boldsymbol{b}'_i\boldsymbol{b}'_j$ is represented as follows:

$$\boldsymbol{b}'_i\boldsymbol{b}'_j = \sum_{\ell=1}^{i}\sum_{m=1}^{j} \alpha_{i\ell}\alpha_{jm}\boldsymbol{b}_\ell\boldsymbol{b}_m.$$

By the assumption that the pair (i, j) in $\mathcal{B}_n$ is well-behaving and (3.5), we obtain

$$\mathrm{ord}(\boldsymbol{b}'_i\boldsymbol{b}'_j) = \mathrm{ord}\left(\sum_{\ell=1}^{i}\sum_{m=1}^{j} \alpha_{i\ell}\alpha_{jm}\boldsymbol{b}_\ell\boldsymbol{b}_m\right) = \mathrm{ord}(\boldsymbol{b}_i\boldsymbol{b}_j).$$

(Q.E.D.)

The contraposition of Lemma 3.2.1 is that if $\mathrm{ord}(\boldsymbol{b}_i\boldsymbol{b}_j) \neq \mathrm{ord}(\boldsymbol{b}'_i\boldsymbol{b}'_j)$, then both the pairs (i, j) in $\mathcal{B}_n$ and $\mathcal{B}'_n$ are not well-behaving. Using this result, the following theorem can be provided.

Lemma 3.2.2. Let $\mathcal{B}_n = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ and $\mathcal{B}'_n = (\boldsymbol{b}'_1, \boldsymbol{b}'_2, \cdots, \boldsymbol{b}'_n)$ be two ordered bases having the same subspace sequence. A pair (i, j) in $\mathcal{B}_n$ is well-behaving if and only if a pair (i, j) in $\mathcal{B}'_n$ is well-behaving. □

Proof. Assume that the pair (i, j) in $\mathcal{B}_n$ is well-behaving and the pair (i, j) in $\mathcal{B}'_n$ is not well-behaving. Since the pair (i, j) in $\mathcal{B}_n$ is well-behaving, we obtain $\mathrm{ord}(\boldsymbol{b}_i\boldsymbol{b}_j) = \mathrm{ord}(\boldsymbol{b}'_i\boldsymbol{b}'_j)$ by using Lemma 3.2.1. Define the nonnegative integer

$$s := \max\{\mathrm{ord}(\boldsymbol{b}'_u\boldsymbol{b}'_v) \mid (u, v) <_P (i, j)\}.$$

By the assumption that the pair (i, j) in $\mathcal{B}'_n$ is not well-behaving, we obtain $s \geq \mathrm{ord}(\boldsymbol{b}'_i\boldsymbol{b}'_j)$. Then, there exists a pair $(\ell, m) <_P (i, j)$ such that $\mathrm{ord}(\boldsymbol{b}'_\ell\boldsymbol{b}'_m) = s$ and the pair (ℓ, m) in $\mathcal{B}'_n$ is well-behaving. With respect to this pair (ℓ, m),

$$\mathrm{ord}(\boldsymbol{b}_\ell\boldsymbol{b}_m) < \mathrm{ord}(\boldsymbol{b}_i\boldsymbol{b}_j) = \mathrm{ord}(\boldsymbol{b}'_i\boldsymbol{b}'_j) \leq \mathrm{ord}(\boldsymbol{b}'_\ell\boldsymbol{b}'_m)$$

holds. Since $\mathrm{ord}(\boldsymbol{b}_\ell \boldsymbol{b}_m) < \mathrm{ord}(\boldsymbol{b}'_\ell \boldsymbol{b}'_m)$, both the pairs (ℓ, m) in $\mathcal{B}_n$ and $\mathcal{B}'_n$ are not well-behaving by using Lemma 3.2.1. This is a contradiction since the pair (ℓ, m) in $\mathcal{B}'_n$ is well-behaving. Therefore, the pair (i, j) in $\mathcal{B}_n$ is well-behaving if and only if the pair (i, j) in $\mathcal{B}'_n$ is well-behaving. (Q.E.D.)

From Lemmas 3.2.1 and 3.2.2, the following theorem can be obtained.

Theorem 3.2.3. Let $\mathcal{B}_n$ and $\mathcal{B}'_n$ be two ordered bases having the same subspace sequence. Then, $\mathcal{B}_n$ and $\mathcal{B}'_n$ are evaluated equivalent, that is,

$$N(\mathcal{B}_n) = N(\mathcal{B}'_n).$$

□

Proof. This follows Lemmas 3.2.1 and 3.2.2 and the definition (3.7). (Q.E.D.)

Theorem 3.2.3 means that the evaluation sequence is essentially dominated by the subspace sequence $\mathcal{V}_n$.

Let $\mathcal{B}_n = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ and $\mathcal{B}'_n = (\boldsymbol{b}'_1, \boldsymbol{b}'_2, \cdots, \boldsymbol{b}'_n)$ be ordered bases. The ordered bases $\mathcal{B}_n$ and $\mathcal{B}'_n$ are called *ordered equivalent* if $\mathcal{B}_n$ and $\mathcal{B}'_n$ have the same subspace sequence. This relation forms an equivalence relation on ordered bases. The ordered bases $\mathcal{B}_n$ and $\mathcal{B}'_n$ are ordered equivalent if and only if there exists a unique nonsingular lower triangular matrix $\mathbf{A}$ such that

$$\begin{bmatrix} \boldsymbol{b}'_1 \\ \boldsymbol{b}'_2 \\ \vdots \\ \boldsymbol{b}'_n \end{bmatrix} = \mathbf{A} \begin{bmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \\ \vdots \\ \boldsymbol{b}_n \end{bmatrix}. \tag{3.12}$$

Next, we provide a representative for all ordered bases generated by some subspace sequence.

Let $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$ be a nonzero n-tuple of $\mathbb{F}_q$. The first nonzero component of $\boldsymbol{x}$ is called the *leading* of $\boldsymbol{x}$. An ordered basis $\mathcal{B}_n = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ is said to be in *standard form* if the following two conditions hold:

1. For each $i \in [1, n]$, the leading of row vector $\boldsymbol{b}_i$ is one.
2. If $h_{ij} = 1$ is the leading of row vector $\boldsymbol{b}_i$, then $h_{\ell j} = 0$ for any $\ell \in [i+1, n]$.

Any ordered basis $\mathcal{B}_n = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ can be uniquely put in standard form $\overline{\mathcal{B}}_n = (\overline{\boldsymbol{b}}_1, \overline{\boldsymbol{b}}_2, \cdots, \overline{\boldsymbol{b}}_n)$ such that $\mathcal{B}_n$ and $\overline{\mathcal{B}}_n$ are ordered equivalent by using Gaussian elimination only with elementary row operation. Hence, any subspace sequence has a unique ordered basis in standard form. Consequently, ordered bases that one should search can be restricted to all ordered bases in standard form. The set of ordered bases in standard form is denoted by $\boldsymbol{S}_n$. By using (3.12), we estimate the total number of ordered bases in standard form. Since the total number of $n \times n$ nonsingular lower triangular matrices with entries in $\mathbb{F}_q$ is $(q-1)^n q^{\frac{1}{2}(n^2-n)}$, the total number of ordered bases in standard form is

$$\#\boldsymbol{S}_n = \prod_{\ell=0}^{n-1} \frac{q^{\ell+1}-1}{q-1} = \prod_{\ell=0}^{n-1} \sum_{m=0}^{\ell} q^m, \tag{3.13}$$

which is the quotient dividing the number (3.1) by $(q-1)^n q^{\frac{1}{2}(n^2-n)}$. Hence, the number of ordered bases that one should search can be reduced from $O(q^{n^2})$ to $O(q^{\frac{1}{2}(n^2-n)})$.

3.2.2 Column Permutation

Let σ be an arbitrary permutation of $[1, n]$ and $\mathcal{B}_n = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ an ordered basis of $\mathbb{F}_q^n$. For any n-tuple $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$ of $\mathbb{F}_q$, define the n-tuple of $\mathbb{F}_q$

$$\sigma(\boldsymbol{x}) := (x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(n)}).$$

Besides, define the

$$\sigma(\mathcal{B}_n) := (\sigma(\boldsymbol{b}_1), \sigma(\boldsymbol{b}_2), \cdots, \sigma(\boldsymbol{b}_n)).$$

Then, this sequence $\sigma(\mathcal{B}_n)$ forms an ordered basis of $\mathbb{F}_q^n$, since any column permutation preserves the linear independency of $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n$.

Theorem 3.2.4. Let $\mathcal{B}_n = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ be any ordered basis and σ any permutation of $[1, n]$. Then, the ordered bases $\mathcal{B}_n$ and $\sigma(\mathcal{B}_n)$ are evaluated equivalent, that is,

$$N(\mathcal{B}_n) = N(\sigma(\mathcal{B}_n)).$$

□

Proof. Any n-tuple $\boldsymbol{x}$ of $\mathbb{F}_q$ can be represented by

$$\boldsymbol{x} = \alpha_1 \cdot \boldsymbol{b}_1 + \alpha_2 \cdot \boldsymbol{b}_2 + \cdots + \alpha_n \cdot \boldsymbol{b}_n$$

for some $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{F}_q$. Let s denote $\mathrm{ord}_{\mathcal{B}_n}(\boldsymbol{x})$, and then $\alpha_s \neq 0$ and $\alpha_\ell = 0$ for any $\ell \in [s+1, n]$. Since

$$\sigma(\boldsymbol{x}) = \alpha_1 \cdot \sigma(\boldsymbol{b}_1) + \alpha_2 \cdot \sigma(\boldsymbol{b}_2) + \cdots + \alpha_n \cdot \sigma(\boldsymbol{b}_n),$$

we obtain $\mathrm{ord}_{\sigma(\mathcal{B}_n)}(\sigma(\boldsymbol{x})) = s$. Hence, for any pair $(i, j) \in [1, n]^2$,

$$\mathrm{ord}_{\mathcal{B}_n}(\boldsymbol{b}_i\boldsymbol{b}_j) = \mathrm{ord}_{\sigma(\mathcal{B}_n)}(\sigma(\boldsymbol{b}_i\boldsymbol{b}_j)) = \mathrm{ord}_{\sigma(\mathcal{B}_n)}(\sigma(\boldsymbol{b}_i)\sigma(\boldsymbol{b}_j)).$$

This means $N(\mathcal{B}_n) = N(\sigma(\mathcal{B}_n))$. (Q.E.D.)

Let $\overline{\mathcal{B}}_n = (\overline{\boldsymbol{b}}_1, \overline{\boldsymbol{b}}_2, \cdots, \overline{\boldsymbol{b}}_n)$ be the ordered basis in standard form which is ordered equivalent to $\mathcal{B}_n$. For each $i \in [1, n]$, let $h_{i,\sigma(i)}$ denote the leading of the n-tuple $\overline{\boldsymbol{b}}_i$ where σ is a permutation of $[1, n]$. If $\hat{\boldsymbol{b}}_i$ is $\sigma^{-1}(\overline{\boldsymbol{b}}_i)$ for any $i \in [1, n]$, then the ordered basis $\hat{\mathcal{B}}_n := (\hat{\boldsymbol{b}}_1, \hat{\boldsymbol{b}}_2, \cdots, \hat{\boldsymbol{b}}_n)$ corresponds to an $n \times n$ nonsingular upper triangular matrix with diagonal entries one. By Theorems 3.2.3 and 3.2.4, we obtain

$$N(\mathcal{B}_n) = N(\hat{\mathcal{B}}_n),$$

and hence

$$d_{FR}(C_r(\mathcal{B}_n)) = d_{FR}(C_r(\hat{\mathcal{B}}_n))$$

for any redundancy r.

Any ordered basis corresponding to an $n \times n$ nonsingular matrix with diagonal entries one is said to be in *standard normal form*. From the argument in previous paragraph, any ordered basis $\mathcal{B}_n = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ is put in standard normal form $\hat{\mathcal{B}}_n = (\hat{\boldsymbol{b}}_1, \hat{\boldsymbol{b}}_2, \cdots, \hat{\boldsymbol{b}}_n)$ such that $\mathcal{B}_n$ and $\hat{\mathcal{B}}_n$ are evaluated equivalent by using Gaussian elimination only with elementary row operation and column permutation. Therefore, ordered bases that one should search can be restricted to all ordered bases in standard normal form. The set of ordered bases in reduced standard form is denoted by $\boldsymbol{R}_n$. The total number of all ordered bases in standard normal form is

$$\#\boldsymbol{S}_n = \prod_{\ell=1}^{n-1} q^{\ell} = q^{\frac{1}{2}(n^2-n)}. \tag{3.14}$$

Hence, the number of ordered bases that one should search can be reduced from $O(q^{n^2})$ to $q^{\frac{1}{2}(n^2-n)}$.

3.3 A Criterion for Linear Codes to Have Large Feng-Rao Designed Distance

In this section, for any given ordered basis $\mathcal{B}_n$ we provide an ordered basis $\mathcal{B}'_n$ such that the Feng-Rao designed distance $d_{FR}(C_r(\mathcal{B}'_n))$ is larger than or equal to $d_{FR}(C_r(\mathcal{B}_n))$ for any redundancy r.

The set of all ordered bases in standard normal form whose first components are identity element $\mathbf{1} = (1, 1, \cdots, 1)$ of $\mathbb{F}_q^n$ is denoted by $\boldsymbol{U}_n$. We consider the map ι from $\boldsymbol{R}_n$ onto $\boldsymbol{U}_n$ defined by

$$\iota(\mathcal{B}_n) := (\mathbf{1}, \boldsymbol{b}_2, \boldsymbol{b}_3, \cdots, \boldsymbol{b}_n) \tag{3.15}$$

for any ordered basis $\mathcal{B}_n = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ in standard normal form.

In order to prove the main result in this section, we introduce the following proposition.

Proposition 3.3.1. [43, p. 1396, Lemma 3.2.2] Let $\mathcal{B}_n = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ be any ordered basis and $\boldsymbol{x}$ any n-tuple of $\mathbb{F}_q$. If $\mathrm{ord}(\boldsymbol{b}_i\boldsymbol{x})$ is smaller than i, then there exists $j \in [1, i-1]$ such that $\mathrm{ord}(\boldsymbol{b}_i\boldsymbol{x}) \leq \mathrm{ord}(\boldsymbol{b}_j\boldsymbol{x})$. □

By Proposition 3.3.1, for any ordered basis $\mathcal{B}_n = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$, if $\mathrm{ord}(\boldsymbol{b}_i\boldsymbol{b}_j) < i$ or $\mathrm{ord}(\boldsymbol{b}_i\boldsymbol{b}_j) < j$, then the pair (i, j) in $\mathcal{B}_n$ is not well-behaving. Therefore, the N_s can be redefined by

$$N_s := \#\{(i,j) \in [1,s]^2 \,|\, \mathrm{ord}(\boldsymbol{b}_i\boldsymbol{b}_j) = s \text{ and } (i,j) \text{ is well-behaving}\} \tag{3.16}$$

for any $s \in [1, n]$. Note that the first part of Proposition 3.1.2 in Section 3.1 follows (3.16).

The following lemma is the main result in this section.

Lemma 3.3.2. Let $\mathcal{B}_n = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ be any ordered basis in standard normal form and ι the map defined by (3.15). Let $N(\mathcal{B}_n) = (N_1, N_2, \cdots, N_n)$ be the evaluation sequence for $\mathcal{B}_n$, and $N(\iota(\mathcal{B}_n)) = (\tilde{N}_1, \tilde{N}_2, \cdots, \tilde{N}_n)$ the evaluation sequence for $\iota(\mathcal{B}_n)$. Then, $\tilde{N}_s \geq N_s$ for any $s \in [1, n]$, that is,

$$N(\iota(\mathcal{B}_n)) \geq_P N(\mathcal{B}_n)$$

where $\geq_P$ is the ordinary partial order on $[0, n]^n$. □

Proof. The proof of this lemma is divided into several steps.

Step 1. $\mathrm{ord}_{\mathcal{B}_n}(\boldsymbol{b}_i\boldsymbol{b}_j) = \mathrm{ord}_{\iota(\mathcal{B}_n)}(\boldsymbol{b}_i\boldsymbol{b}_j)$ for any pair $(i, j) \in [2, n]^2$.

Let (i, j) be any pair in $[2, n]^2$. Without loss of generality, we may assume that $i \geq j$. If $\boldsymbol{b}_i\boldsymbol{b}_j$ is equal to $\mathbf{0}$, then

$$\mathrm{ord}_{\mathcal{B}_n}(\boldsymbol{b}_i\boldsymbol{b}_j) = \mathrm{ord}_{\iota(\mathcal{B}_n)}(\boldsymbol{b}_i\boldsymbol{b}_j) = 0.$$

Assume that $\boldsymbol{b}_i\boldsymbol{b}_j$ is unequal to $\mathbf{0}$. From the definition of standard normal form, we obtain

$$\boldsymbol{b}_i\boldsymbol{b}_j \in \mathrm{Span}\{\boldsymbol{b}_i, \boldsymbol{b}_{i+1}, \cdots, \boldsymbol{b}_n\} \setminus \{\mathbf{0}\}.$$

Hence, from the definition (3.4) of the order map, we obtain

$$\mathrm{ord}_{\mathcal{B}_n}(\boldsymbol{b}_i\boldsymbol{b}_j) = \mathrm{ord}_{\iota(\mathcal{B}_n)}(\boldsymbol{b}_i\boldsymbol{b}_j).$$

Step 2. The pairs $(i, 1)$ and $(1, i)$ in $\iota(\mathcal{B}_n)$ is well-behaving for any $i \in [1, n]$.

For any $i \in [1, n]$,

$$\mathrm{ord}_{\iota(\mathcal{B}_n)}(\mathbf{1} \cdot \boldsymbol{b}_i) = \mathrm{ord}_{\iota(\mathcal{B}_n)}(\boldsymbol{b}_i \cdot \mathbf{1}) = \mathrm{ord}_{\iota(\mathcal{B}_n)}(\boldsymbol{b}_i) = i. \tag{3.17}$$

Hence the pairs $(i, 1)$ and $(1, i)$ in $\iota(\mathcal{B}_n)$ is well-behaving for any $i \in [1, n]$. In particular, $\tilde{N}_1 = 1$, $\tilde{N}_2 = 2$ and $\tilde{N}_s \geq 2$ for any $s \in [3, n]$.

Step 3. For any $s \in [3, n]$, let any pair $(i, j) \in [2, s-1]^2$ such that $\mathrm{ord}_{\mathcal{B}_n}(\boldsymbol{b}_i\boldsymbol{b}_j) = s$. If (i, j) in $\mathcal{B}_n$ is well-behaving, then (i, j) in $\iota(\mathcal{B}_n)$ is well-behaving.

Without loss of generality, we may assume that $i \geq j$. Assume that (i, j) in $\mathcal{B}_n$ is well-behaving. Note that $\mathrm{ord}_{\iota(\mathcal{B}_n)}(\boldsymbol{b}_i\boldsymbol{b}_j) = s$ from Step 1. We obtain

$$\mathrm{ord}_{\iota(\mathcal{B}_n)}(\boldsymbol{b}_u\boldsymbol{b}_v) = \mathrm{ord}_{\mathcal{B}_n}(\boldsymbol{b}_u\boldsymbol{b}_v) < s$$

for any pair $(u, v) <_P (i, j)$ with $u \neq 1$ and $v \neq 1$, and further

$$\mathrm{ord}_{\iota(\mathcal{B}_n)}(\boldsymbol{b}_u \cdot \mathbf{1}) = \mathrm{ord}_{\iota(\mathcal{B}_n)}(\boldsymbol{b}_u) = u < s$$

for any $u \in [1, i]$. Therefore, (i, j) in $\iota(\mathcal{B}_n)$ is well-behaving.

Now, we are in a position to finish the proof of Lemma 3.3.2. We obtain $N_1 \leq \tilde{N}_1$ and $N_2 \leq \tilde{N}_2$ by Proposition 3.1.2 and Step 2. For any $s \in [3, n]$,

$$\begin{align*}
N_s &= \# \left\{ (i,j) \in [1,s]^2 \;\middle|\; \begin{array}{l} \mathrm{ord}_{\mathcal{B}_n}(\boldsymbol{b}_i\boldsymbol{b}_j) = s \text{ and} \\ (i,j) \text{ in } \mathcal{B}_n \text{ is well-behaving} \end{array} \right\} \\
&\leq \# \left\{ (i,j) \in [1,s-1]^2 \;\middle|\; \begin{array}{l} \mathrm{ord}_{\mathcal{B}_n}(\boldsymbol{b}_i\boldsymbol{b}_j) = s \text{ and} \\ (i,j) \text{ in } \mathcal{B}_n \text{ is well-behaving} \end{array} \right\} + 2 \tag{3.18} \\
&\leq \# \left\{ (i,j) \in [1,s-1]^2 \;\middle|\; \begin{array}{l} \mathrm{ord}_{\iota(\mathcal{B}_n)}(\boldsymbol{b}_i\boldsymbol{b}_j) = s \text{ and} \\ (i,j) \text{ in } \iota(\mathcal{B}_n) \text{ is well-behaving} \end{array} \right\} + 2 \tag{3.19} \\
&= \# \left\{ (i,j) \in [1,s]^2 \;\middle|\; x \begin{array}{l} \mathrm{ord}_{\iota(\mathcal{B}_n)}(\boldsymbol{b}_i\boldsymbol{b}_j) = s \text{ and} \\ (i,j) \text{ in } \iota(\mathcal{B}_n) \text{ is well-behaving} \end{array} \right\} \tag{3.20} \\
&= \tilde{N}_u
\end{align*}$$

where (3.18) follows the fact that there exists at most one pair (i, s) (resp. (s, j)) which is well-behaving, (3.19) follows Step 3, and (3.20) follows Step 2.

Consequently, $\tilde{N}_s \geq N_s$ for any $s \in [1, n]$. (Q.E.D.)

As a consequence of these, the following theorem is obtained.

Theorem 3.3.3. Let $\mathcal{B}_n = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ be any ordered basis. Then, there exists an ordered basis $\mathcal{B}'_n = (\mathbf{1}, \boldsymbol{b}'_2, \boldsymbol{b}'_3, \cdots, \boldsymbol{b}'_n)$ such that $N(\mathcal{B}'_n) \geq_P N(\mathcal{B}_n)$. □

Proof. An ordered basis $\mathcal{B}'_n = (\mathbf{1}, \boldsymbol{b}'_2, \boldsymbol{b}'_3, \cdots, \boldsymbol{b}'_n)$ such that $N(\mathcal{B}'_n) \geq_P N(\mathcal{B}_n)$ can be systematically constructed by using Gaussian elimination only with elementary row operation and column permutation, and then the map ι defined by (3.15). (Q.E.D.)

From the argument in Section 3.2 and Lemma 3.3.2, in order to find ordered bases which provides the largest Feng-Rao designed distance for any redundancy, it is sufficient to investigate only ordered bases in standard normal form whose first component is identity element **1**. These ordered bases have the matrix representation

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ \text{0} & & & & 1 \end{bmatrix}. \tag{3.21}$$

The total number of ordered bases in standard normal form with first component **1** is

$$\#\boldsymbol{U}_n = q^{\frac{1}{2}(n-1)(n-2)}. \tag{3.22}$$

Therefore, the number of ordered bases that one should search can be reduced from $O(q^{n^2})$ to $q^{\frac{1}{2}(n-1)(n-2)}$.

3.4 Conclusion

In this chapter, we firstly have shown that the Feng-Rao designed distance of linear codes has depended on subspace sequence, that is, all the ordered bases having the same subspace sequence have provided the same Feng-Rao designed distance for any redundancy. Also, we have provided a representative for all ordered bases generated by any subspace sequence. This representative, which is called in standard form, can be constructed for any ordered basis by using the Gaussian elimination only with elementary row operation. Secondly, we have shown that under the column permutation of any ordered basis, the Feng-Rao designed distance has been invariant for any redundancy. At this time, the ordered bases to search can be restricted to the ordered bases in standard normal form. In particular, any ordered basis can be put in standard normal form as its Feng-Rao designed distance is kept by using the Gaussian elimination only with elementary row operation and column permutation. Finally, we have presented the following algorithm: The input to the algorithm has been any ordered basis. The output to the algorithm has been the ordered basis in standard normal form with first component **1**. Then, the Feng-Rao designed distance for the output ordered basis has been larger than or equal to that for the input ordered basis. As a consequence of these, ordered bases that one should search can be restricted to the ordered bases in standard normal form with first component **1**, that is, the number of ordered bases to search can be reduced from $O(q^{n^2})$ to exactly $q^{\frac{1}{2}(n^2-3n+2)}$.

Chapter 4

Optimum Design of Monomial Orders for Hermitian Codes

Linear codes on the *Hermitian curve* over $\mathbb{F}_{q^2}$, so called *Hermitian codes*, firstly were appeared as an interesting example for algebraic geometric codes in Goppa's original papers [19, 20]. From their emergence, the Hermitian codes have been paid attention by many coding theoreticians. This is the reason why the Hermitian curve has the following two special features:

(1) The Hermitian curve attains *Hasse-Weil upper bound* (Proposition 2.3.3), that is, this curve have maximal $\mathbb{F}_{q^2}$-rational points as compared with its genus. This means that the Hermitian codes are optimal in Goppa's construction.

(2) The Hermitian curve has a considerably simple structure in algebraic curves. Hence, the Hermitian codes can be expected to furnish the simple and efficient construction, encoding and decoding.

From the observation above, the Hermitian codes possessed both of the theoretical and practical meaning.

In an earlier work [34], Lint and Springer calculated the parameters of some Hermitian codes and showed an example that these codes were better than the corresponding Reed-Solomon codes with the same information rate. Tiersma [59] provided a theoretical approach to the Hermitian codes, and consequently found explicit descriptions of their dual codes and automorphism groups. Successively, Stichtenoth [57] presented explicit descriptions of generator and parity check matrices for the Hermitian codes by working with an isomorphic curve having only one point at infinity, and especially determined the exact minimum distance of these codes for almost all dimension. Yang and Kumar [72] entirely clarified the exact minimum distance of the Hermitian codes. In a practical viewpoint, Yamanishi [71] precisely compared the subfield subcodes and concatenated codes for Hermitian codes with the conventional algebraic codes. As a result, he found many good linear codes which were obtained from the Hermitian curve. Recently, Röck and Stichtenoth [52] showed that the Hermitian curve was the unique maximal curve over $\mathbb{F}_{q^2}$ with genus $g = (q-1)q/2$. Thus, the Hermitian curve increasingly take on importance in all algebraic curves.

The Hermitian curve contributes not only the discover of many new good codes, but also the development of construction and decoding for algebraic geometric codes. Miura [39] characterized the families $\boldsymbol{C}_a^b$ and ${}_r\boldsymbol{C}_a^b$ of plane curves which described explicitly such as the Hermitian curve. Also, the Hermitian curve has been employed as an example for the decoding of algebraic geometric codes in many papers, for example [28, 9, 13]. Thus, the explication of the Hermitian curve have related to those of algebraic geometric codes, and hence their research has been sill attractive.

As shown in Chapter 3, Miura [42, 43] presented the decoding by majority voting among unknown syndromes and the Feng-Rao designed distance for arbitrary linear codes by using the notion of ordered basis. Further, Miura proposed an explicit construction method of linear codes on arbitrary affine algebraic varieties by using *monomial orders* and *Gröbner bases*. This construction method generates an ordered basis which provides the large Feng-Rao designed distance for given affine algebraic variety and monomial order. When an affine algebraic variety is given, the monomial order plays a crucial role to determine the ordered basis. This means that the choice of monomial orders affect the Feng-Rao designed distance in this construction method. Unfortunately, if is not clear which monomial order provides the largest Feng-Rao designed distance for given redundancy. Now, an optimization problem of the Feng-Rao designed distance in compliance with monomial orders is established.

In this chapter, we take up the Hermitian curve as an object of the optimization problem above, and present a class of monomial orders which provides the largest Feng-Rao designed distance. This chapter is organized as follows. Section 4.1 is devoted to present an explicit construction method of algebraic geometric codes on affine algebraic varieties, which proposed by Miura [42, 43]. The monomial orders and Gröbner bases play a crucial role in this construction method. We formalize an optimization problem for the Feng-Rao designed distance by using monomial orders. In Section 4.2, we provide the Hermitian codes by Goppa's and Miura's construction and compare both the codes. Especially, we observe that Goppa's construction is Miura's construction by using the weight order which generates the structure sequence as for the Hermitian curve. Section 4.3 is the main part of this chapter. We provide sufficient conditions not to have well-behaving pairs by using the extended delta sets. Next, necessary conditions and sufficient conditions to have well-behaving pairs by using the weight order. Then, by using their relation, we clarify a class of optimal monomial orders for Hermitian codes. Also, we illustrate an example the case that finite field volume is 16. The results in this chapter is based in part on a study published at IEICE Transactions A [63].

4.1 Algebraic Geometric Codes on Affine Algebraic Varieties

In this section, we review Miura's construction method for linear codes on affine algebraic varieties [42, 43]. This construction method provides a good lower bound for the Feng-Rao designed distance of linear codes. We firstly introduce the notion of monomial orders and Gröbner bases which play a crucial role in Miura's construction method for linear codes on affine algebraic varieties.

4.1.1 Monomial Orders and Gröbner Bases

In this subsection, we show the basic concepts of monomial orders and Gröbner bases. As for the detailed properties of monomial orders and Gröbner bases, we refer to [1, 6, 7].

Let $\mathbb{K}$ be an arbitrary field, and $\mathbb{K}[\underline{X}] := \mathbb{K}[X_1, X_2, \cdots, X_t]$ the polynomial ring in the indeterminates $X_1, X_2, \cdots, X_t$ with coefficients in K.

A *monomial* in $X_1, X_2, \cdots, X_t$ is a product of the form $X^{\boldsymbol{a}} := X_1^{a_1} X_2^{a_2} \cdots X_t^{a_t}$ for any t-tuple of nonnegative integers $\boldsymbol{a} = (a_1, a_2, \cdots, a_t)$. The set of all monomials in these indeterminates is denoted by $\mathcal{M}(X_1, X_2, \cdots, X_t)$, or simply by $\mathcal{M}$. The set $\mathcal{M}$ is a multiplicative monoid with identity 1, and has the natural one-to-one correspondence to the additive monoid $\mathbb{N}_0^t$. The *divisiblity relation* $|$ on $\mathcal{M}$ is defined by $X^{\boldsymbol{b}} | X^{\boldsymbol{a}}$ if $\boldsymbol{a} - \boldsymbol{b} \in \mathbb{N}_0^t$. Further, a partial order $\geq_P$ on $\mathbb{N}_0^t$ is defined by $\boldsymbol{a} \geq_P \boldsymbol{b}$ if $\boldsymbol{a} - \boldsymbol{b} \in \mathbb{N}_0^t$. Then, $X^{\boldsymbol{b}} | X^{\boldsymbol{a}}$ if and only if $\boldsymbol{a} \geq_P \boldsymbol{b}$. In particular, we denote $X^{\boldsymbol{a}} >_P X^{\boldsymbol{b}}$ if $X^{\boldsymbol{b}} | X^{\boldsymbol{a}}$ and $X^{\boldsymbol{a}} \neq X^{\boldsymbol{b}}$.

Definition 4.1.1. A *monomial order* on $\mathcal{M}$ is defined by a total order $\geq$ on $\mathcal{M}$ satisfying the following two conditions:

1. $X^{\boldsymbol{a}} \geq 1$ for any monomial $X^{\boldsymbol{a}} \in \mathcal{M}$.

2. For any monomials $X^{\boldsymbol{a}}, X^{\boldsymbol{b}}, X^{\boldsymbol{c}} \in \mathcal{M}$, if $X^{\boldsymbol{a}} \geq X^{\boldsymbol{b}}$, then $X^{\boldsymbol{a}+\boldsymbol{c}} \geq X^{\boldsymbol{b}+\boldsymbol{c}}$.

Further, $X^{\boldsymbol{a}} \geq X^{\boldsymbol{b}}$ is also denoted by $\boldsymbol{a} \geq \boldsymbol{b}$. □

Hereafter, assume that any relation $\geq$ on $\mathcal{M}$ is a monomial order. The relation between any monomial order $\geq$ and the divisiblity relation on $\mathcal{M}$ is provided the following proposition.

Proposition 4.1.1. [1, p. 190, Theorem 5.5 (i)] Let $\geq$ be a monomial order on $\mathcal{M}$. If two monomials $X^{\boldsymbol{a}}$ and $X^{\boldsymbol{b}}$ satisfy $X^{\boldsymbol{b}} | X^{\boldsymbol{a}}$, then $X^{\boldsymbol{a}} \geq X^{\boldsymbol{b}}$. □

Next, we introduce one important class of monomial orders.

Definition 4.1.2. Assume that an $e \times t$ matrix $\mathbf{M}$ with entries in $\mathbb{R}$ satisfies the following two conditions:

1. All the row vectors of $\mathbf{M}$ are linearly independent over $\mathbb{R}$,
2. All the column vectors of $\mathbf{M}$ are linearly independent over $\mathbb{N}_0$,
3. The leading of $\boldsymbol{v} \cdot \mathbf{M}^T$ is positive for any $\boldsymbol{v} \in \mathbb{N}_0^t \setminus \{\mathbf{0}\}$,

where the leading of a vector is the first nonzero component. Such the matrix $\mathbf{M}$ is called a *independent matrix*. A total order on $\mathcal{M}$ is defined by $X^{\boldsymbol{a}} \geq_{\mathbf{M}} X^{\boldsymbol{b}}$ if the leading of $(\boldsymbol{a} - \boldsymbol{b}) \cdot \mathbf{M}^T \in \mathbb{R}^e$ is positive. This order $\geq_{\mathbf{M}}$ is called the *matrix order* associated with by $\mathbf{M}$. □

Any matrix order on $\mathcal{M}$ is a monomial order on $\mathcal{M}$. In Robbiano's papers [50] and [51, Chapter 2], he has shown that the matrix order on $\mathcal{M}$ has the following special feature:

Proposition 4.1.2. [50, p. 516, Theorem 5] Let $\geq$ be any monomial order on $\mathcal{M}$. Then, there exists an independent matrix $\mathbf{M}$ such that $X^{\boldsymbol{a}} \geq X^{\boldsymbol{b}}$ if and only if $X^{\boldsymbol{a}} \geq_{\mathbf{M}} X^{\boldsymbol{b}}$ for any monomials $X^{\boldsymbol{a}}$ and $X^{\boldsymbol{b}}$. □

Proposition 4.1.2 means that any monomial order on $\mathcal{M}$ can be represented by a matrix order defined by some independent matrix. For any t-tuples $\boldsymbol{a} = (a_1, a_2, \cdots, a_t)$ and $\boldsymbol{b} = (b_1, b_2, \cdots, b_t)$ of $\mathbb{N}_0$, let $\boldsymbol{c} = (c_1, c_2, \cdots, c_t)$ where $c_i = \max\{a_i, b_i\}$ for each $i \in [1, t]$. Then, the monomial $X^{\boldsymbol{c}}$ is called the *least common multiple* of $X^{\boldsymbol{a}}$ and $X^{\boldsymbol{b}}$, denoted by $X^{\boldsymbol{c}} = \mathrm{LCM}\{X^{\boldsymbol{a}}, X^{\boldsymbol{b}}\}$.

A *polynomial* F in the indeterminates $X_1, X_2, \cdots, X_t$ with coefficients in $\mathbb{K}$ can be uniquely represented as the following finite sum of monomials:

$$F := \sum_{\boldsymbol{a} \in \mathbb{N}_0^t} \alpha_{\boldsymbol{a}} X^{\boldsymbol{a}},$$

where $\alpha_{\boldsymbol{a}} \in K \setminus \{0\}$. Also, using a monomial order $\geq$ on $\mathcal{M}$, we can represent the nonzero polynomial F as $\sum_{i=1}^m \alpha_{\boldsymbol{a}_i} X^{\boldsymbol{a}_i}$ with $\alpha_{\boldsymbol{a}_i} \neq 0$ such that $\boldsymbol{a}_j > \boldsymbol{a}_k$ if $j > k$. Then, the *multidegree*, the *leading coefficient*, the *leading monomial* and the *leading term* of F is defined by $\mathrm{Deg}(F) := \boldsymbol{a}_m$, $\mathrm{LC}(F) := \alpha_{\boldsymbol{a}_m}$, $\mathrm{LM}(F) := X^{\boldsymbol{a}_m}$ and $\mathrm{LT}(F) := \mathrm{LC}(F) \cdot \mathrm{LM}(F)$, respectively. The ideal generated by a subset $\mathcal{F}$ of $\mathbb{K}[\underline{X}]$ is denoted by $\langle \mathcal{F} \rangle$. For any polynomial F and polynomial ideal I, Gröbner bases and the division algorithm provided by [7, p. 37, Proposition 2] are powerful tools to decide a unique polynomial R such that $F - R \in I$ and $R \notin I$. Firstly, Gröbner bases is defined as follows:

Definition 4.1.3. Let $\geq$ be a monomial order on $\mathcal{M}$. A finite subset $\mathcal{G} = \{G_1, G_2, \cdots, G_m\}$ of a polynomial ideal I is called a *Gröbner basis* if

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(G_1), \mathrm{LT}(G_2), \cdots, \mathrm{LT}(G_m) \rangle, \tag{4.1}$$

where $\mathrm{LT}(\mathcal{F}) := \{\mathrm{LT}(F) \,|\, F \in \mathcal{F}\}$ for any subset $\mathcal{F}$ of $\mathbb{K}[\underline{X}]$.

Moreover, a Gröbner basis $\mathcal{G}$ is called *reduced* if it is satisfied following two conditions:

1. $\mathrm{LC}(G_i) = 1$ for any $i \in [1, m]$.

2. $\mathrm{LT}(G_i) \notin \langle \mathrm{LT}(\mathcal{G} \setminus \{G_i\}) \rangle$ for any $i \in [1, m]$.

□

Hereafter, assume that $\mathcal{G} = \{G_1, G_2, \cdots, G_m\}$ is a Gröbner basis of I. From [7, p. 75, Corollary 6], every polynomial ideal I except $\{0\}$ has a Gröbner basis and further any Gröbner basis of I is a basis of I, that is, $I = \langle \mathcal{G} \rangle$. Also, every polynomial ideal I except $\{0\}$ has a unique reduced Gröbner basis from [7, p. 90, Proposition 6]. For a polynomial F and a Gröbner basis $\mathcal{G}$, the division algorithm of F by a Gröbner basis $\mathcal{G} = \{G_1, G_2, \cdots, G_m\}$ is formulated as follows: The inputs in this algorithm are a polynomial F and a Gröbner basis $\mathcal{G} = \{G_1, G_2, \cdots, G_m\}$. The outputs in this algorithm are polynomials $Q_1, Q_2, \cdots, Q_m$ and R with

$$F = Q_1 \cdot G_1 + Q_2 \cdot G_2 + \cdots + Q_m \cdot G_m + R \tag{4.2}$$

such that no term of R is divisible by $\mathrm{LT}(G_i)$ if $R \neq 0$ and $\mathrm{Deg}(F) \geq \mathrm{Deg}(Q_i \cdot G_i)$ if $Q_i \cdot G_i \neq 0$ for any $i \in [1, m]$. At this time, by [7, p. 79, Proposition 1], the polynomial R is uniquely determined. This polynomial R is called the *remainder* on division of F by $\mathcal{G}$ and denoted by $\overline{F}^{\mathcal{G}}$, or simply $\overline{F}$ if it is clear which Gröbner basis is meant. The notion of S-polynomials defined by the following definition plays a important role to test whether a finite polynomial subset $\mathcal{G}$ is a Gröbner basis of $\langle \mathcal{G} \rangle$.

Definition 4.1.4. The *S-polynomial* of two nonzero polynomials F and G is defined by the polynomial

$$S(F, G) = \frac{X^{\boldsymbol{c}}}{\mathrm{LT}(F)} \cdot F - \frac{X^{\boldsymbol{c}}}{\mathrm{LT}(G)} \cdot G, \tag{4.3}$$

where the monomial $X^{\boldsymbol{c}} := \mathrm{LCM}\{\mathrm{LM}(F), \mathrm{LM}(G)\}$. □

Using S-polynomials, the following criterion for deciding whether a basis of an ideal is a Gröbner basis can be provided.

Proposition 4.1.3. [7, p. 82, Theorem 6] Let I be a polynomial ideal. Then a basis $\mathcal{G} = \{G_1, G_2, \cdots, G_m\}$ of I is a Gröbner basis if and only if the remainder on division of $S(G_i, G_j)$ by $\mathcal{G}$ for any pairs $(i, j) \in [1, m]^2$ with $i \neq j$. □

Furthermore, S-polynomials also play an important role in Buchberger's algorithm [7, p. 87, Theorem 2] which is capable of constructing a Gröbner basis $\mathcal{G}$ from a finite basis $\mathcal{F}$ of I in a finite number of steps. Buchberger's algorithm is formulated as follows: The input in this algorithm is a finite basis $\mathcal{F} = \{F_1, F_2, \cdots, F_\ell\}$ of I. The output in this algorithm is a Gröbner basis $\mathcal{G} = \{G_1, G_2, \cdots, G_m\}$ of $I = \langle \mathcal{F} \rangle$ with $\mathcal{F} \subseteq \mathcal{G}$. Note that any polynomial ideal has a finite basis of an arbitrary ideals by the Hilbert basis theorem [7, p. 74, Theorem 4].

Next, we consider the ring of residue classes of polynomials $\mathcal{R} := K[\underline{X}]/I$ modulo a polynomial ideal I. The coset of X_i in $\mathcal{R}$ is denoted by x_i for any $i \in [1, t]$. The element $x_1^{a_1} x_2^{a_2} \cdots x_t^{a_t}$ for any t-tuple of nonnegative integers $\boldsymbol{a} = (a_1, a_2, \cdots, a_t)$ and the residue class ring $\mathcal{R} = K[x_1, x_2, \cdots, x_t]$ are abbreviated to $x^{\boldsymbol{a}}$ and $\mathbb{K}[\underline{x}]$, respectively. The delta set $\Delta(I)$ of the polynomial ideal I, which is defined by the following definition, plays an important role to represent the coset of any polynomial F in $\mathcal{R}$.

Definition 4.1.5. Let $\mathcal{F}$ be any subset of $\mathbb{K}[\underline{X}]$. The *delta set* of $\mathcal{F}$ is defined by

$$\Delta(\mathcal{F}) := \mathbb{N}_0^t \setminus \bigcup_{F \in \mathcal{F} \setminus \{0\}} \{\mathrm{Deg}(F) + \mathbb{N}_0^t\} \tag{4.4}$$

where $\mathrm{Deg}(F) + \mathbb{N}_0^t := \{\mathrm{Deg}(F) + \boldsymbol{a} \mid \boldsymbol{a} \in \mathbb{N}_0^t\}$. In particular, $\Delta(\{0\}) = \mathbb{N}_0^t$ and $\Delta(K[\underline{X}]) = \emptyset$. □

Hereafter, $\Delta(I)$ abbreviates to Δ. In particular,

$$\Delta = \mathbb{N}_0^t \setminus \{\mathrm{Deg}(F) \mid F \in I \setminus \{0\}\}, \tag{4.5}$$

since I is a polynomial ideal. From the definition and property of Gröbner bases, $\overline{X^{\boldsymbol{a}}} = X^{\boldsymbol{a}}$ for any $\boldsymbol{a} \in \Delta$ and $\overline{F}$ can be uniquely represented as the linear combination of $\{X^{\boldsymbol{a}} \mid \boldsymbol{a} \in \Delta\}$ over $\mathbb{K}$ for any polynomial F. Further, the following lemma and propositions can be obtained.

Lemma 4.1.4. Let Δ be the delta set of any polynomial ideal I. If $\boldsymbol{a} \in \Delta$ and $X^{\boldsymbol{b}} | X^{\boldsymbol{a}}$, then $\boldsymbol{b} \in \Delta$. In particular, $\boldsymbol{0} \in \Delta$. □

Proof. Assume that $\boldsymbol{a} \in \Delta$, $X^{\boldsymbol{b}} | X^{\boldsymbol{a}}$, and $\boldsymbol{b} \notin \Delta$. From the definition of delta sets, there exists a polynomial $F \in I$ such that $\mathrm{LM}(F) | X^{\boldsymbol{b}}$. Hence, we obtain $\mathrm{LM}(F) | X^{\boldsymbol{a}}$. This contradicts that $\boldsymbol{a} \in \Delta$. In particular, $\boldsymbol{0} \in \Delta$ since $X^{\boldsymbol{0}} (= 1) | X^{\boldsymbol{a}}$ for any $\boldsymbol{a} \in \mathbb{N}_0^t$. (Q.E.D.)

Proposition 4.1.5. [1, p. 207, Proposition 5.38 (iv)] Let Δ be and the delta set of any polynomial ideal I. Assume that a finite set $\mathcal{F} = \{F_1, F_2, \cdots, F_\ell\}$ is a subset of I. Then, $\mathcal{F}$ is a Gröbner basis of I if and only if

$$\Delta = \Delta(\mathcal{F}) = \mathbb{N}_0^t \setminus \bigcup_{i=1}^{\ell} \{\mathrm{Deg}(F_i) + \mathbb{N}_0^t\}. \tag{4.6}$$

□

Proposition 4.1.6. [43, p. 1392, Lemma 4.6 (4)] Let I be a polynomial ideal, and Δ the delta set of I. Then, the set $\{x^{\boldsymbol{a}} \mid \boldsymbol{a} \in \Delta\}$ consists of a basis of the linear space $\mathcal{R} = K[\underline{x}]$ over $\mathbb{K}$. □

The coset f of any polynomial F in $\mathcal{R}$ is represented by $\overline{F}(x_1, x_2, \cdots, x_t)$. Thus, the division algorithm by a Gröbner basis $\mathcal{G}$ is a powerful tool to represent the coset f of a polynomial F in $\mathcal{R}$ as the linear combination of $\{x^{\boldsymbol{a}} \mid \boldsymbol{a} \in \Delta\}$. Also, the linear combination of a product fg of two elements $f = F + I$ and $g = G + I$ in $\mathcal{R}$ with $F, G \in K[\underline{X}]$ can be calculated by dividing FG by $\mathcal{G}$.

4.1.2 Miura's Construction Method

Let $\mathbb{F}_q := \mathrm{GF}(q)$ denote the finite field with q elements, and $\mathbb{F}_q[\underline{X}] = \mathbb{F}_q[X_1, X_2, \cdots, X_t]$ the polynomial ring in the indeterminates $X_1, X_2, \cdots, X_t$ with coefficients in $\mathbb{F}_q$. The t-dimensional *affine space* $\mathbb{F}_q^t$ over $\mathbb{F}_q$ is defined by the set of all t-tuples of $\mathbb{F}_q$.

For any subset $\mathcal{F}$ of $\mathbb{F}_q[\underline{X}]$, a subset $V(\mathcal{F})$ of $\mathbb{F}_q^t$ is defined by

$$V(\mathcal{F}) := \{P \in \mathbb{F}_q^t \mid F(P) = 0 \text{ for all } F \in \mathcal{F}\}, \tag{4.7}$$

which is called the *affine algebraic variety*, or simply *algebraic variety* defined by $\mathcal{F}$. In particular, $V(\mathcal{F}) = V(\langle \mathcal{F} \rangle)$ for any polynomial subset $\mathcal{F}$, where $\langle \mathcal{F} \rangle$ is the ideal generated by $\mathcal{F}$. For any subset V of $\mathbb{F}_q^t$, a subset $I(V)$ of $\mathbb{F}_q[\underline{X}]$ is defined by

$$I(V) := \{F \in \mathbb{F}_q[\underline{X}] \mid F(P) = 0 \text{ for all } P \in V\}, \tag{4.8}$$

which is called the *ideal of* V. In particular, $I(V)$ is an ideal of $\mathbb{F}_q[\underline{X}]$. Now, we have a function V which maps subsets of $\mathbb{F}_q[\underline{X}]$ to algebraic varieties, and a function I which maps subsets of $\mathbb{F}_q^t$ to ideals. Their properties are summarized in the following proposition:

Proposition 4.1.7. [43, p. 1390, Nullstellensatz over $\mathbb{F}_q$] Let I be any polynomial ideal and V any subset of $\mathbb{F}_q$. Then,

1. $V(I(V)) = V$, that is, V is the affine algebraic variety defined by $I(V)$. This means that any subset of $\mathbb{F}_q^t$ is an affine algebraic variety.
2. $I(V(I)) = I + \langle X_1^q - X_1, X_2^q - X_2, \cdots, X_t^q - X_t \rangle$.

□

The ring of residue classes of polynomials $\Gamma(V) := K[\underline{X}]/I(V)$ modulo the ideal $I(V)$ is called the *coordinate ring* of V. The coset of X_i in $\Gamma(V)$ is denoted by x_i for any $i \in [1, t]$, and then $\Gamma(V) = \mathbb{F}_q[x_1, x_2, \cdots, x_t]$, simply denoted by $\mathbb{F}_q[\underline{x}]$. Any $f \in \Gamma(V)$ has a representation $f = F + I(V)$ for some $F \in \mathbb{F}_q[\underline{X}]$, and then $f(P)$ is defined by $F(\alpha_1, \alpha_2, \cdots, \alpha_t)$ for any $P = (\alpha_1, \alpha_2, \cdots, \alpha_t) \in \mathbb{F}_q^t$. Then, $f(P)$ is well-defined.

Let $V = \{P_1, P_2, \cdots, P_n\}$ be the nonempty affine algebraic variety defined by any finite polynomial set $\mathcal{F} = \{F_1, F_2, \cdots, F_\ell\}$. Note that n is at most $\#\mathbb{F}_q^t = q^t$. The *evaluation map* ev_V from $\Gamma(V)$ onto $\mathbb{F}_q^t$ is defined by

$$\mathrm{ev}_V(f) := (f(P_1), f(P_2), \cdots, f(P_n)) \tag{4.9}$$

for any $f \in \Gamma(V)$. This map ev_V has the following property:

Proposition 4.1.8. [43, p. 1390, Lemma 4.4] Let V be any algebraic variety of $\mathbb{F}_q^t$ and ev_V the evaluation map of V. Then, the map ev_V is an isomorphism from $\Gamma(V)$ onto $\mathbb{F}_q^n$ as $\mathbb{F}_q$-algebra. □

From Proposition 4.1.8, the coordinate ring $\Gamma(V)$ is the n-dimensional linear space over $\mathbb{F}_q$. An *ordered basis* of $\Gamma(V)$ is defined by an ordered n-tuple $\mathcal{F}_n := (f_1, f_2, \cdots, f_n)$ of $\Gamma(V)$ such that $F_n := \{f_1, f_2, \cdots, f_n\}$ is a basis of $\Gamma(V)$. Besides, define

$$\mathrm{ev}_V(\mathcal{F}_n) := (\mathrm{ev}_V(f_1), \mathrm{ev}_V(f_2), \cdots, \mathrm{ev}_V(f_n)), \tag{4.10}$$

and then $\mathrm{ev}_V(\mathcal{F}_n)$ is an ordered basis of $\mathbb{F}_q^n$ introduced in Section 3.1. Therefore, the argument in Chapter 3 can be applied via the isomorphism ev_V. Here, all the notions for ordered bases of $\mathbb{F}_q^t$ in Chapter 3 is diverted to those for ordered bases of $\Gamma(V)$ via the isomorphism ev_V.

In [42, 43], Miura presented a construction method which provides an ordered basis by using monomial orders and Gröbner bases introduced in Subsection 4.1.1. This ordered basis of $\Gamma(V)$ provides linear codes with the large Feng-Rao designed distance for any redundancy. Hereafter, we briefly explain Miura's construction method.

Let $\geq$ denote any monomial order on $\mathcal{M} = \mathcal{M}(X_1, X_2, \cdots, X_t)$. Let $\mathcal{G}$ and Δ be a Gröbner basis and the delta set of $I(V)$, respectively. From Propositions 4.1.6 and 4.1.8, the set $\{x^{\boldsymbol{a}} \mid \boldsymbol{a} \in \Delta\}$ is a basis of the n-dimensional linear space $\Gamma(V)$, and hence the cardinality of Δ is $n = \#V$. The following lemma is useful in later section.

Lemma 4.1.9. Let V be any nonempty affine algebraic variety with cardinality n and $\mathcal{F}$ any finite subset of $I(V)$. Then, $\mathcal{F}$ is a Gröbner basis of $I(V)$ if and only if the cardinality of $\Delta(\mathcal{F})$ is equal to n. □

Proof. Let Δ be the delta set of $I(V)$. From Proposition 4.1.5, $\mathcal{F}$ is a Gröbner basis of $I(V)$ if and only if $\Delta = \Delta(\mathcal{F})$. Also, the cardinality of Δ is n. The proof of this lemma is complete. (Q.E.D.)

Definition 4.1.6. The ordered basis $\mathcal{M}_n(V, \geq)$ of $\Gamma(V)$ is defined by

$$\mathcal{M}_n(V, \geq) := (x^{\boldsymbol{a}_1}, x^{\boldsymbol{a}_2}, \cdots, x^{\boldsymbol{a}_n})$$

such that $\boldsymbol{a}_s \in \Delta$ for any $s \in [1, n]$ and $\boldsymbol{a}_i > \boldsymbol{a}_j$ if $i > j$, which is simply denoted by $\mathcal{M}_n(V)$, $\mathcal{M}_n(\geq)$, or more simply $\mathcal{M}_n$. This ordered basis $\mathcal{M}_n$ is called the *monomial basis associated with V and $\geq$*. In particular, from Lemma 4.1.4, $\boldsymbol{a}_1 = \mathbf{0} = (0, 0, \cdots, 0)$, that is, $x^{\boldsymbol{a}_1} = 1$. □

Since $x^{\boldsymbol{a}_1} = 1$, that is, $\mathrm{ev}_V(1) = \mathbf{1} = (1, 1, \cdots, 1)$, the monomial basis $\mathcal{M}_n$ satisfies the criterion for linear codes to have the large Feng-Rao designed distance in Theorem 3.3.3. The monomial basis $\mathcal{M}_n$ has following property:

Lemma 4.1.10. Let Δ and $\mathcal{M}_n = (x^{\boldsymbol{a}_1}, x^{\boldsymbol{a}_2}, \cdots, x^{\boldsymbol{a}_n})$ be the delta set of $I(V)$ and the monomial basis of $\Gamma(V)$. Then, for any t-tuple $\boldsymbol{a} \in \Delta$ and any $s \in [1, n]$, If $X^{\boldsymbol{a}} | X^{\boldsymbol{a}_s}$, then $\boldsymbol{a} = \boldsymbol{a}_u$ for some $u \in [1, s]$. □

Proof. This follows Proposition 4.1.1 and Lemma 4.1.4. (Q.E.D.)

Here, the Miura's construction algorithm of the monomial basis $\mathcal{M}_n(V, \geq)$ of $\Gamma(V)$ is provided as follows:

Algorithm 4.1.1. [43, p. 1392]

Input: a basis $\mathcal{F} := \{F_1, F_2, \cdots, F_\ell\}$ of I and a monomial order $\geq$.

Output: the monomial basis $\mathcal{M}_n = (x^{\boldsymbol{a}_1}, x^{\boldsymbol{a}_2}, \cdots, x^{\boldsymbol{a}_n})$ associated with $V = V(I)$ and $\geq$.

[Step 1] Search all points $P \in \mathbb{F}_q^t$ such that $F_1(P) = F_2(P) = \cdots = F_n(P) = 0$.

[Step 2] Calculate a Gröbner basis $\mathcal{G} := \{G_1, G_2, \cdots, G_m\}$ of $I(V)$ by using Buchberger's algorithm. Note that $\mathcal{F} \cup \{X_s^q - X_s \,|\, s \in [1, t]\}$ is a basis of $I(V)$ from Proposition 4.1.7.

[Step 3] Calculate the delta set $\Delta = \{\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_n\}$ of I by using the Gröbner basis $\mathcal{G}$, where $\boldsymbol{a}_i > \boldsymbol{a}_j$ if $i > j$.

□

Remark 4.1.1. In Miura's papers [42, 43], the output in this algorithm was the ordered basis $\mathrm{ev}_V(\mathcal{M}_n)$ of $\mathbb{F}_q^n$. In our dissertation, however, this algorithm was finished by the derivation of the monomial basis $\mathcal{M}_n$. Because, both of the behavior of two ordered bases are the same from Proposition 4.1.8, and the monomial basis $\mathcal{M}_n$ is more convenient than the ordered basis $\mathrm{ev}_V(\mathcal{M}_n)$ for the argument in later sections.

Also, Miura suggested that one may select an ordered basis $\mathcal{F}_n := (f_1, f_2, \cdots, f_n)$ of $\Gamma(V)$ such that $f_1 \in \mathrm{Span}\{x^{\boldsymbol{a}_1}\} \backslash \{0\}$ and $f_s \in \mathrm{Span}\{x^{\boldsymbol{a}_1}, x^{\boldsymbol{a}_2}, \cdots, x^{\boldsymbol{a}_s}\} \backslash \mathrm{Span}\{x^{\boldsymbol{a}_1}, x^{\boldsymbol{a}_2}, \cdots, x^{\boldsymbol{a}_{s-1}}\}$ for any $s \in [2, n]$. Unfortunately, from Theorem 3.2.3, the evaluation sequences for such ordered bases are the same, that is, the Feng-Rao designed distance is not varied by the choice of such ordered bases. Hence, in this dissertation, we consider only the monomial basis $\mathcal{M}_n$ for simplicity. □

The monomial basis derived by Algorithm 4.1.1 has the following special feature:

Proposition 4.1.11. [43, p. 1393, Lemma 4.10] Let $\mathcal{M}_n = (x^{\boldsymbol{a}_1}, x^{\boldsymbol{a}_2}, \cdots, x^{\boldsymbol{a}_n})$ be the monomial basis associated with any affine algebraic variety V of $\mathbb{F}_q^t$. For any pair $(i, j) \in [1, n]^2$, if $\boldsymbol{a}_i + \boldsymbol{a}_j \in \Delta$, then the pair (i, j) in $\mathcal{M}_n$ is well-behaving.

□

From Proposition 4.1.11, each s-th component N_s in the evaluation sequence $N(\mathcal{M}_n)$ has the following lower bound.

Proposition 4.1.12. [43, p. 1393, Theorem 4.12] Let $\mathcal{M}_n = (x^{\boldsymbol{a}_1}, x^{\boldsymbol{a}_2}, \cdots, x^{\boldsymbol{a}_n})$ be the monomial basis associated with any affine algebraic variety V of $\mathbb{F}_q^t$, where $\boldsymbol{a}_s := (a_{s1},\ a_{s2}, \cdots, a_{sn})$ for any $s \in [1, n]$. Then,

$$N_s \geq \prod_{i=1}^{t} (a_{si} + 1) \tag{4.11}$$

□

In our experience, the lower bound provided by Proposition 4.1.12 is considerably better than the evaluation sequence for an arbitrary specified ordered basis of $\mathbb{F}_q^n$.

Let $\mathcal{M}_n$ be the monomial basis associated with any algebraic variety V of $\mathbb{F}_q^t$ and monomial order $\geq$ on $\mathcal{M}$. Recall that the Feng-Rao designed distance of linear codes depend only on the choice of the ordered basis, and moreover the monomial basis depend only on the choice of the monomial order. Therefore, the observation above leads to the following question:

Problem 4.1.1. Let V be any affine algebraic variety of $\mathbb{F}_q^t$. Find a monomial order $\geq$ on $\mathcal{M}$ such that the linear code $C_r(\mathcal{M}_n)$ associated with the monomial basis $\mathcal{M}_n$ has the largest Feng-Rao designed distance $d_{FR}(C_r(\mathcal{M}_n))$ for the given redundancy r. □

In order to formulate Problem 4.1.1, we provide some definitions as follows:

Definition 4.1.7. Let V be any affine algebraic variety of $\mathbb{F}_q^t$. A monomial order $\geq$ on $\mathcal{M}$ is called *r-optimal* if the monomial basis $\mathcal{M}_n$ provides the linear code $C_r(\mathcal{M}_n)$ with the largest Feng-Rao designed distance $d_{FR}(C_r(\mathcal{M}_n))$ in all possible monomial bases for the given redundancy r. Especially, a monomial order $\geq$ on $\mathcal{M}$ is called *optimal* if the monomial order $\geq$ is r-optimal for all $r \in [0, n-1]$.

□

Problem 4.1.1 can be restated as follows: Find a monomial order $\geq$ on $\mathcal{M}$ which is r-optimal for the given redundancy r.

In Section 4.2, we consider the set of rational points on the Hermitian curve as V, and in Section 4.3, we investigate a class of optimal monomial orders for this affine algebraic variety V.

4.2 Linear Codes on Hermitian Curves

In this section, we present linear codes based on the Hermitian curve. The Hermitian curve has the maximal number of rational points as compared with its genus, that is, it is maximal curve. Besides, the Hermitian curve has a considerably simple structure in algebraic curves. Therefore, the codes on the Hermitian curve investigated by many researchers [59, 57, 71, 72], and in the present they have been good examples for algebraic geometric codes. Now that all these results for the linear codes on the Hermitian curve were based on Goppa's construction introduced in Section 2.3, we hereafter investigate the codes on the Hermitian curve based on Miura's construction introduced in Section 4.1. Firstly, we review both the codes on the Hermitian code by Goppa's and Miura's constructions and show their relation.

4.2.1 Hermitian Codes by Goppa's Construction

Let $\mathbb{F}_{q^2} := \mathrm{GF}(q^2)$ be the finite field with q^2 elements, and $\overline{\mathbb{F}}_{q^2}$ its algebraic closure. Let $\mathbb{F}_{q^2}[X, Y]$ be the polynomial ring in two indeterminates X and Y.

Definition 4.2.1. The *Hermitian curve* $\mathcal{X}$ over $\mathbb{F}_{q^2}$ is defined by

$$Y^q Z + Y Z^q = X^{q+1}, \tag{4.12}$$

that is, $\mathcal{X} := \{(\alpha : \beta : 1) \,|\, \alpha, \beta \in \overline{\mathbb{F}}_{q^2} \text{ and } \beta^q + \beta = \alpha^{q+1}\} \cup \{(0 : 1 : 0)\}$. The Hermitian curve $\mathcal{X}$ is a projective, nonsingular, absolutely irreducible curve. □

Let $P_{\alpha,\beta}$ and Q denote the points $(\alpha : \beta : 1)$ and $(0 : 1 : 0)$, respectively. The set of $\mathbb{F}_{q^2}$-rational points is provided by

$$\mathcal{X}(\mathbb{F}_{q^2}) = \{P_{\alpha,\beta} \,|\, \alpha, \beta \in \mathbb{F}_{q^2} \text{ and } \beta^q + \beta = \alpha^{q+1}\} \cup \{Q\}. \tag{4.13}$$

For any $\alpha \in \mathbb{F}_{q^2}$, the equation $\beta^q + \beta = \alpha^{q+1}$ has q distinct roots $\beta \in \mathbb{F}_{q^2}$. Hence, the number of $\mathbb{F}_{q^2}$-rational points of on $\mathcal{X}$ is $q^3 + 1$. On the other hand, the genus of $\mathcal{X}$ is provided by

$$g = \frac{1}{2} q(q-1). \tag{4.14}$$

Therefore, the curve $\mathcal{X}$ attains the Hasse-Weil upper bound.

The polynomial $F = F(X, Y) = Y^q + Y - X^{q+1}$ in $\mathbb{F}_{q^2}[X, Y]$ is called the *Hermitian polynomial.* The cosets of X and Y in $\mathbb{F}_{q^2}[X, Y]/\langle F \rangle$ is denoted by x and y, respectively. Then, $x(P_{\alpha,\beta}) = \alpha$ and $y(P_{\alpha,\beta}) = \beta$ for any point $P_{\alpha,\beta}$ on $\mathcal{X}$ except Q. The function field $\mathbb{F}_{q^2}(\mathcal{X}) = \mathbb{F}_{q^2}(x, y)$ is called the *Hermitian function field.* For any $\alpha, \beta \in \mathbb{F}_{q^2}$, the rational functions $x - \alpha$ and $y - \beta$ have the following principal divisors:

$$(x - \alpha) = \sum_{\beta^q + \beta = \alpha} P_{0,\beta} - q \cdot Q, \tag{4.15}$$

$$(y - \beta) = \begin{cases} (q+1) \cdot P_{0,\beta} - (q+1) \cdot Q & \text{if } \beta^q + \beta = 0, \\ \displaystyle\sum_{\alpha^{q+1} = \beta^q + \beta} P_{\alpha,\beta} - (q+1) \cdot Q & \text{if } \beta^q + \beta \neq 0. \end{cases} \tag{4.16}$$

From [57, p. 1346, Proposition 1], a basis of $L(mQ)$ is provided by

$$\{x^i y^j \mid i \in \mathbb{N}_0,\, j \in [0, q-1] \text{ and } q \cdot i + (q+1) \cdot j \le m\}, \tag{4.17}$$

for any nonnegative integer m.

Let $P_1, P_2, \cdots, P_n$ be all $\mathbb{F}_{q^2}$-rational points on $\mathcal{X}$ except Q, and then n is equal to q^3. Let D be the $\mathbb{F}_{q^2}$-rational divisor $P_1 + P_2 + \cdots + P_n$. For any nonnegative integer m, the algebraic geometric code

$$C_\Omega(D, mQ) = \{\mathrm{ev}_D(x^i y^j) \mid i \in \mathbb{N}_0,\, j \in [0, q-1] \text{ and } q \cdot i + (q+1) \cdot j \le m\}^\perp \tag{4.18}$$

associated with D and mQ is called the *Hermitian codes* by Goppa's construction. Hereafter, let the code $C_\Omega(D, mQ)$ abbreviate to $C_\Omega(mQ)$.

The subset S_Q of $\mathbb{N}_0$ is defined by

$$S_Q := \{m \in \mathbb{N}_0 \mid \dim C_\Omega(mQ) + 1 = \dim C_\Omega((m-1)Q)\}. \tag{4.19}$$

By [41, p. 428, Lemma], the cardinality of S_Q is n, 0 is included in S_Q, and $m \in S_Q$ if and only if $l(mQ) = l((m-1)Q) + 1$ and $l(-D + mQ) = l(-D + (m-1)Q)$. Let $\mathcal{S}_Q = (\rho_i \mid i \in [1, n])$ denote the sequence of all elements of S_Q in increasing order, so $\rho_1 = 0$. This sequence $\mathcal{S}_Q$ is called the *structure sequence* at Q. At this time, the redundancy for $C_\Omega(\rho_r Q)$ is r. The nonnegative integer n_s is defined by

$$n_s := \#\{(i, j) \in [1, n]^2 \mid \rho_i + \rho_j = \rho_s\}.$$

The *Feng-Rao designed distance* of $C_\Omega(\rho_r Q)$ is defined by

$$d_{FR}(C_\Omega(\rho_r Q)) := \min\{n_s \mid r \in [s+1, n]\},$$

and then the Feng-Rao decoding algorithm [9, 13] can be decoded up to half the Feng-Rao designed distance $d_{FR}(C_\Omega(\rho_r Q))$. In particular, from [30, p. 1725, Theorem 3.8] and [41, p. 429, Theorem]

$$d_{FR}(C_\Omega(\rho_r Q)) \ge r - g + 1,$$

and equality holds if $3g - 1 \le r \le n - g - 1$. Furthermore, for any redundancy r, the minimum distance of $C_\Omega(\rho_r Q)$ is equal to the Feng-Rao designed distance of $C_\Omega(\rho_r Q)$, that is,

$$d(C_\Omega(\rho_r Q)) = d_{FR}(C_\Omega(\rho_r Q))$$

from [72, p. 100, Theorem 1], [40, p. 80, Main Theorem 2] and [41, p. 429, Theorem].

Remark 4.2.1. Miura proposed the family of nonsingular plane curves $\boldsymbol{C}_a^b$ over $\mathbb{F}_q$ in his paper [39]. He clarified one-point codes on any plane curves in $\boldsymbol{C}_a^b$ and provided many examples of curves which are maximal. The Hermitian curve over $\mathbb{F}_{q^2}$ is included in the family $\boldsymbol{C}_q^{q+1}$. Also, Miura extended the notion of the curve family $\boldsymbol{C}_a^b$ to a higher-dimensional affine space [42, 44] □

4.2.2 Hermitian Codes by Miura's Construction

In this subsection, we investigate the linear codes on the set of $\mathbb{F}_{q^2}$-rational points on the affine Hermitian curve by using Miura's construction method in Section 4.1.

Let V be the set of all $\mathbb{F}_{q^2}$-rational points on the affine Hermitian curve, that is,

$$V := \{(\alpha, \beta) \mid \alpha, \beta \in \mathbb{F}_{q^2} \text{ and } \beta^q + \beta = \alpha^{q+1}\}. \tag{4.20}$$

Then, the cardinality of V is $n = q^3$. The affine algebraic variety V is denoted by $\{P_1, P_2, \cdots, P_n\}$ where the order of $\mathbb{F}_{q^2}$-rational points is the same as in previous subsection. The polynomial ideal $I(V)$ is represented by $\langle X^{q^2} - X, Y^{q^2} - Y, F(X, Y)\rangle$ from Proposition 4.1.7. Let $\Gamma(V) := \mathbb{F}_{q^2}[X, Y]/I(V)$ be the coordinate ring of V. The coset of X and Y in $\Gamma(V)$ are denoted by x and y, respectively. Note that x and y in this subsection differ from those in previous subsection.

The reduced Gröbner basis and the delta set of $I(V)$ is explicitly provided by the following lemma for any monomial order $\geq$ on $\mathcal{M}(X, Y)$.

Lemma 4.2.1. Let $\geq$ be a monomial order on $\mathcal{M}(X, Y)$. The reduced Gröbner bases $\mathcal{G}$ and the delta set Δ of $I(V)$ are provided as follows:

(a) In the case of $Y^q > X^{q+1}$.

$$\mathcal{G} = \{X^{q^2} - X, F(X, Y)\}, \tag{4.21}$$
$$\Delta = [0, q^2 - 1] \times [0, q - 1]. \tag{4.22}$$

(b) In the case of $X^{q+1} > Y^q$.

$$\mathcal{G} = \left\{ Y^{q^2} - Y, X \cdot \sum_{\ell=0}^{q} (-1)^{\ell+1} Y^{\ell(q-1)}, -F(X, Y) \right\}, \tag{4.23}$$
$$\Delta = \{0\} \times [0, q^2 - 1] \cup [1, q] \times [0, q^2 - q - 1]. \tag{4.24}$$

□

Proof. The proof of this lemma parts into the following two cases.

(a) In the case of $Y^q > X^{q+1}$.

Let $\mathcal{F} := \{F_1, F_2\}$ where $F_1 := X^{q^2} - X$ and $F_2 := F(X, Y)$. Then,

$$\Delta(\mathcal{F}) = [0, q^2 - 1] \times [0, q - 1],$$

and the cardinality of $\Delta(\mathcal{F})$ is $n = q^3$. Therefore, $\mathcal{F}$ is the reduced Gröbner basis from Definition 4.1.3 and Lemma 4.1.9.

(b) In the case of $X^{q+1} > Y^q$.

Since the equation $\beta^q + \beta = 0$ has q distinct roots in $\mathbb{F}_{q^2}$, $(Y^{q^2} - Y)/(Y^q + Y)$ is a polynomial with coefficients in $\mathbb{F}_{q^2}$. If $(\alpha, \beta) \in V$ and $\alpha \neq 0$, then $\beta^{q^2} - \beta = 0$

and $\beta^q + \beta = \alpha^{q+1} \neq 0$, and hence $X \cdot (Y^{q^2} - Y)/(Y^q + Y) \in I(V)$. We obtain

$$X \cdot \frac{Y^{q^2} - Y}{Y^q + Y} = X \cdot \frac{Y^{q^2-1} - 1}{Y^{q-1} + 1} = X \cdot \sum_{\ell=0}^{q} (-1)^{\ell+1} Y^{\ell(q-1)},$$

since

$$\begin{aligned}(Y^{q-1} + 1) \cdot \sum_{\ell=0}^{q} (-1)^{\ell+1} Y^{\ell(q-1)} &= \sum_{\ell=1}^{q+1} (-1)^{\ell} Y^{\ell(q-1)} + \sum_{\ell=0}^{q} (-1)^{\ell+1} Y^{\ell(q-1)}, \\ &= (-1)^{q+1} Y^{q^2-1} - 1.\end{aligned}$$

Note that if q is even then $(-1)^{q+1} = -1 = 1$. Now, let

$$\mathcal{F} := \{F_1, F_2, F_3\},$$

where

$$F_1 := Y^{q^2} - Y, \quad F_2 := X \cdot \sum_{\ell=0}^{q} (-1)^{\ell+1} Y^{\ell(q-1)} \quad \text{and} \quad F_3 := -F(X, Y).$$

Then,

$$\Delta(\mathcal{F}) = \{0\} \times [0, q^2 - 1] \cup [1, q] \times [0, q^2 - q - 1],$$

and the cardinality of $\Delta(\mathcal{F})$ is $n = q^3$. Therefore, $\mathcal{F}$ is the reduced Gröbner basis from Definition 4.1.3 and Lemma 4.1.9.

The proof of this lemma is complete. (Q.E.D.)

By Lemma 4.2.1, the monomial basis $\mathcal{M}_n$ associated with V for any monomial order $\geq$ is explicitly determined, and hence Algorithm 4.1.1 can be omitted with respect to the set of $\mathbb{F}_{q^2}$-rational points on the Hermitian curve. Let $((a_i, b_i) \mid i \in [1, n])$ denote the sequence of all elements of Δ in increasing order with respect to the monomial order $\geq$. By Proposition 4.1.12, the evaluation sequence $N(\mathcal{M}_n)$ for the monomial basis $\mathcal{M}_n$ has a lower bound

$$N_s \geq (a_s + 1)(b_s + 1) \tag{4.25}$$

for any $s \in [1, n]$.

Next, we investigate the relation between both the codes on Hermitian curves by Goppa's and Miura's constructions. For that reason, we introduce weight order on $\mathcal{M}(X, Y)$ provided by the following definition.

Definition 4.2.2. Let μ and ν be any relatively prime positive integers. A total order on $\mathcal{M}(X, Y)$ is defined by $X^a Y^b >_{(\mu,\nu,X)} X^c Y^d$ (resp. $X^a Y^b >_{(\mu,\nu,Y)} X^c Y^d$) if $X^a Y^b$ and $X^c Y^d$ satisfy one of the following conditions

1. $a \cdot \mu + b \cdot \nu > c \cdot \mu + d \cdot \nu$,

2. $a \cdot \mu + b \cdot \nu = c \cdot \mu + d \cdot \nu$ and $a > c$ (resp. $a < c$).

This order $\geq_{(\mu,\nu,X)}$ (resp. $\geq_{(\mu,\nu,Y)}$) is called the *weight order* associated with the *weight* (μ, ν, X) (resp. (μ, ν, Y)). The set of all weights is denoted by $\mathcal{W}$. □

The weight order $\geq_{\boldsymbol{w}}$ associated with any weight $\boldsymbol{w} \in \mathcal{W}$ is a monomial order on $\mathcal{M}(X,Y)$. Also, if the weight $\boldsymbol{w}$ is (μ, ν, X) (resp. (μ, ν, Y)), then the weight order $\geq_{(\mu,\nu,X)}$ (resp. $\geq_{(\mu,\nu,Y)}$) can be represented by the matrix order $\geq_{\mathbf{M}}$ with

$$\mathbf{M} = \begin{bmatrix} \mu & \nu \\ 1 & 0 \end{bmatrix} \quad \left(\text{resp. } \begin{bmatrix} \mu & \nu \\ 0 & 1 \end{bmatrix}\right). \tag{4.26}$$

Further, since the delta set of $I(V)$ for any monomial order $\geq$ is finite, we obtain following lemma.

Lemma 4.2.2. Let $\mathcal{M}_n(\geq)$ be any monomial basis associated with V. Then, there exists a weight order $\geq_{\boldsymbol{w}}$ such that

$$\mathcal{M}_n(\geq) = \mathcal{M}_n(\geq_{\boldsymbol{w}}). \tag{4.27}$$

□

Proof. By Definition 4.1.2 and Proposition 4.1.2, all the monomial orders except the matrix order given by (4.26) can be represented by

$$\mathbf{M}_1 := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \mathbf{M}_2 := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

or

$$\mathbf{M}_\alpha := \begin{bmatrix} \alpha & 1 \end{bmatrix}$$

for any positive real number α which is not rational number. The monomial basis $\mathcal{M}_n(\geq_{\mathbf{M}_1})$ is identical with $\mathcal{M}_n(\geq_{(q^2,1,X)})$ associated with the weight order $\geq_{(q^2,1,X)}$. Similarly, the monomial basis $\mathcal{M}_n(\geq_{\mathbf{M}_2})$ is identical with $\mathcal{M}_n(\geq_{(1,q^2,Y)})$ associated with the weight order $\geq_{(1,q^2,Y)}$.

Next, we consider about the case of $Y^q >_{\mathbf{M}_\alpha} X^{q+1}$, that is, α is smaller than $q/(q+1)$. Let Δ denote the delta set for the monomial order $\mathbf{M}_\alpha$. Let A denote the set

$$\{(a-c, b-d) \mid (a,b),\ (c,d) \in \Delta,\ a-b > 0, \text{ and } X^aY^b >_{\mathbf{M}_\alpha} X^cY^d\}.$$

Since A is finite, there exist relatively prime positive integers μ and μ such that

$$\alpha \cdot (a-c) + (b-d) > \frac{\mu}{\nu} \cdot (a-c) + (b-d) > 0$$

for any $(a-c, b-d) \in A$. Here, we consider the weight order $\geq_{(\mu,\nu,\cdot)}$ on $\mathcal{M}(X,Y)$. Since $Y^q >_{(\mu,\nu,\cdot)} X^{q+1}$, the set Δ is also the delta set for the weight order $\geq_{(\mu,\nu,\cdot)}$

by Lemma 4.2.1. At this time, we will show that $X^aY^b >_{\mathbf{M}_\alpha} X^cY^d$ if and only if $X^aY^b >_{(\mu,\nu,\cdot)} X^cY^d$ for any pairs $(a,b),(c,d) \in \Delta$. Assume that $X^aY^b >_{\mathbf{M}_\alpha} X^cY^d$. If $a > c$, then $(a-c, b-d) \in A$ and hence

$$\alpha \cdot (a-c) + (b-d) > \frac{\mu}{\nu} \cdot (a-c) + (b-d) > 0.$$

If $a \leq c$, then

$$\frac{\mu}{\nu} \cdot (a-c) + (b-d) \geq \alpha \cdot (a-c) + (b-d) > 0.$$

Therefore, $X^aY^b >_{(\mu,\nu,\cdot)} X^cY^d$. Conversely, assume that $X^aY^b >_{(\mu,\nu,\cdot)} X^cY^d$. If $a \geq c$, then

$$\alpha \cdot (a-c) + (b-d) \geq \frac{\mu}{\nu} \cdot (a-c) + (b-d) > 0.$$

If $a < c$ and $X^aY^b <_{\mathbf{M}_\alpha} X^cY^d$, then $(c-a, d-b) \in A$ and hence

$$\alpha \cdot (c-a) + (d-b) > \frac{\mu}{\nu} \cdot (c-a) + (d-b) > 0.$$

that is, $X^aY^b <_{(\mu,\nu,\cdot)} X^cY^d$. Therefore, $X^aY^b >_{\mathbf{M}_\alpha} X^cY^d$. As a consequence of these,

$$\mathcal{M}_n(\geq_{\mathbf{M}_\alpha}) = \mathcal{M}_n(\geq_{(\mu,\nu,\cdot)}).$$

In the case of $X^{q+1} >_{\mathbf{M}_\alpha} Y^q$, the proof can be done in a similar way. The proof of this lemma is complete. (Q.E.D.)

Remark 4.2.2. The proof of Lemma 4.2.2 is hardly used the assumption that V is the set of $\mathbb{F}_{q^2}$-rational points on the affine Hermitian curve. Hence, with respect to any affine algebraic variety of $\mathbb{F}_q^2$, the following similar statement can be proved. Let V be an arbitrary affine algebraic variety of $\mathbb{F}_q^2$. Then, for any monomial order $\geq$ on $\mathcal{M}(X,Y)$, there exists a weight order $\geq_{\boldsymbol{w}}$ on $\mathcal{M}(X,Y)$ such that the monomial basis $\mathcal{M}_n(V,\geq)$ is identical with the monomial basis $\mathcal{M}_n(V,\geq_{\boldsymbol{w}})$. □

Let $\boldsymbol{w}$ be the weight $(q, q+1, Y)$. Since $Y^q >_{\boldsymbol{w}} X^{q+1}$, the reduced Gröbner basis $\mathcal{G}$ and the delta set Δ of $I(V)$ can be provided by (4.21) and (4.22), respectively. Let $\mathcal{M}_n$ denote the monomial basis associated with V and $\geq_{\boldsymbol{w}}$. The set

$$\{q \cdot a + (q+1) \cdot b \,|\, (a,b) \in \Delta\}$$

is identical with S_Q defined by (4.19). From [38, Lemma 3.8], if $r < 3g-1$, then

$$d_{FR}(C_r(\mathcal{M}_n)) \geq d_{FR}(C_\Omega(\rho_r Q)), \tag{4.28}$$

and if $r \geq 3g-1$, then

$$C_r(\mathcal{M}_n) = C_\Omega(\rho_r Q).$$

The inequality (4.28) follows the technique of improved geometric Goppa codes proposed by Feng and Rao [12]. Consequently, Miura's construction extends Goppa's construction to arbitrary monomial orders with respect to Hermitian codes. Hereafter, Hermitian codes indicate those by Miura's construction.

4.3 Optimal Monomial Orders for Linear Codes on Hermitian Curves

In this section, we investigate only linear codes on the Hermitian curve by Miura's construction in Subsection 4.2.2. We show which monomial order provides the largest Feng-Rao designed distance of Hermitian codes. Firstly, we provide sufficient conditions not to have well-behaving pairs by using the extended delta sets. Next, we show necessary conditions and sufficient conditions to have well-behaving pairs by using the weight order. Finally, we clarify a class of optimal monomial orders for Hermitian codes. This class includes the weight order which generates the structure sequence. All notations in previous section is also used in this section.

4.3.1 Sufficient Conditions Not to Be Well-Behaving

Let Δ and $\mathcal{M}_n$ be the delta set of $I(V)$ and the monomial basis associated with V for any monomial basis $\geq$ on $\mathcal{M}(X,Y)$. Recall that the evaluation sequence $N(\mathcal{M}_n)$ for the monomial basis $\mathcal{M}_n$ defined by the number of well-behaving pairs (i,j) in $\mathcal{M}_n$ which are mapped the same number by order map. Let $((a_i,b_i)\,|\,i \in [1,n])$ denote the sequence of all elements of Δ in increasing order with respect to the monomial order $\geq$ on $\mathcal{M}(X,Y)$. The *extended delta set* 2Δ is defined by

$$2\Delta := \{(a+c, b+d)\,|\,(a,b),\,(c,d) \in \Delta\}.$$

For convenience sake, the sum $(a_i,b_i)+(a_j,b_j)$ is denoted by (a_{ij},b_{ij}) in 2Δ. Here, we illustrate the range of the pair (a_{ij},b_{ij}) which always provide not well-behaving pair (i,j). We obtain Lemma 4.3.1 in the case of $Y^q > X^{q+1}$ and Lemma 4.3.2 in the case of $X^{q+1} > Y^q$.

Lemma 4.3.1. Let $\geq$ be any monomial order with $Y^q > X^{q+1}$. Assume that a pair (a_{ij},b_{ij}) satisfies one of the following conditions

1. $a_{ij} \in [q^2, 2q^2-2]$,
2. $a_{ij} \in [q^2-q-1, q^2-1]$ and $b_{ij} \in [q, 2q-2]$.

Then, the pair (i,j) is not well-behaving. □

Proof. From Lemma 4.1.10, for any monomials X^aY^b with $X^aY^b <_P X^{a_{ij}}Y^{b_{ij}}$, there exists a pair $(u,v) \in [1,n]^2$ with $(u,v) <_P (i,j)$ such that $X^aY^b = X^{a_{uv}}Y^{b_{uv}}$. We will show that there exists a monomial X^aY^b with $(a,b) \in 2\Delta$ and

$$X^aY^b <_P X^{a_{ij}}Y^{b_{ij}} \tag{4.29}$$

such that

$$\mathrm{LM}(\overline{X^aY^b}) \geq_P \mathrm{LM}(\overline{X^{a_{ij}}Y^{b_{ij}}}) \tag{4.30}$$

for any pair (i,j) satisfying the assumption of this lemma. To find the pair (a,b) which satisfies (4.29) and (4.30) means that the pair (i,j) in $\mathcal{M}_n$ is not well-behaving. The proof of this lemma can be done in three cases.
[Case 1] $a_{ij} \in [q^2-q-1, q^2-1]$ and $b_{ij} \in [q, 2q-2]$.

The remainder of $X^{a_{ij}}Y^{b_{ij}}$ by $\mathcal{G}$ is provided by

$$\overline{X^{a_{ij}}Y^{b_{ij}}} = X^{a_{ij}-q^2+q+2}Y^{b_{ij}-q} - X^{a_{ij}}Y^{b_{ij}-q+1}.$$

For a monomial $X^{a_{ij}}Y^{q-1}$ which satisfies (4.29), we obtain

$$X^{a_{ij}}Y^{q-1} \geq_P X^{a_{ij}-q^2+q+2}Y^{b_{ij}-q} \quad \text{and} \quad X^{a_{ij}}Y^{q-1} \geq_P X^{a_{ij}}Y^{b_{ij}-q+1}$$

since $a_{ij} - q^2 + q + 2 \in [1, q+1]$. Therefore, the pair (i,j) in $\mathcal{M}_n$ is not well-behaving.
[Case 2] $a_{ij} \in [q^2, 2q^2-2]$ and $b_{ij} \in [0, q-1]$.

$$\overline{X^{a_{ij}}Y^{b_{ij}}} = X^{a_{ij}-q^2+1}Y^{b_{ij}} \leq_P X^{q^2-1}Y^{b_{ij}} <_P X^{a_{ij}}Y^{b_{ij}}.$$

[Case 3] $a_{ij} \in [q^2, q^2-2]$ and $b_{ij} \in [q, 2q-2]$.

$$\mathrm{LM}(\overline{X^{a_{ij}}Y^{b_{ij}}}) \leq_P X^{q^2-1}Y^{q-1} <_P X^{a_{ij}}Y^{b_{ij}}.$$

The proof of this lemma is complete. (Q.E.D.)

Lemma 4.3.2. Let $\geq$ be any monomial order with $X^{q+1} > Y^q$. If a pair (a_{ij}, b_{ij}) satisfy one of the following conditions

1. $a_{ij} = 0$ and $b_{ij} \in [q^2, 2q^2-2]$,
2. $a_{ij} \in [1, q]$ and $b_{ij} \in [q^2-q, 2q^2-q-2]$,
3. $a_{ij} = q+1$ and $b_{ij} \in [q^2-q, 2q^2-2q-2]$,
4. $a_{ij} \in [q+2, 2q]$ and $b_{ij} \in [q^2-2q, 2q^2-2q-2]$,

then the pair (i,j) is not well-behaving. □

Proof. This lemma can be also proved such as Lemma 4.3.1. The proof of this lemma can be done in several cases.
[Case 1] $a_{ij} = 0$ and $b_{ij} \in [q^2, 2q^2-2]$.

$$\mathrm{LM}(\overline{X^{a_{ij}}Y^{b_{ij}}}) = Y^{b_{ij}-q^2+1} \leq_P Y^{q^2-1} <_P X^{a_{ij}}Y^{b_{ij}}.$$

[Case 2] $a_{ij} \in [1, q]$ and $b_{ij} \in [q^2-q, q^2-2]$.

$$\mathrm{LM}(\overline{X^{a_{ij}}Y^{b_{ij}}}) = X^{a_{ij}}Y^{b_{ij}-q+1} \leq_P X^{a_{ij}}Y^{q^2-q-1} <_P X^{a_{ij}}Y^{b_{ij}}.$$

[Case 3] $a_{ij} \in [1, q]$ and $b_{ij} = q^2 - 1$.

$$\mathrm{LM}(\overline{X^{a_{ij}}Y^{b_{ij}}}) = X^{a_{ij}} \leq_P X^{a_{ij}}Y^{q^2-q-1} <_P X^{a_{ij}}Y^{b_{ij}}.$$

[Case 4] $a_{ij} \in [1, q]$ and $b_{ij} \in [q^2, 2q^2 - q - 2]$.

$$\mathrm{LM}(\overline{X^{a_{ij}}Y^{b_{ij}}}) = X^{a_{ij}}Y^{b_{ij}-q^2+1} \leq_P X^{a_{ij}}Y^{q^2-q-1} <_P X^{a_{ij}}Y^{b_{ij}}.$$

[Case 5] $a_{ij} = q + 1$ and $b_{ij} \in [q^2 - q, q^2 - 2]$.

$$X^{q+1}Y^{q^2-q-1} <_P X^{a_{ij}}Y^{b_{ij}}$$

and

$$\mathrm{LM}(\overline{X^{q+1}Y^{q^2-q-1}}) = Y^{q^2-1} \geq_P \mathrm{LM}(\overline{X^{a_{ij}}Y^{b_{ij}}}) = Y^{b_{ij}+1}.$$

[Case 6] $a_{ij} = q + 1$ and $b_{ij} \in [q^2 - 1, 2q^2 - 2q - 2]$.

$$\mathrm{LM}(\overline{X^{a_{ij}}Y^{b_{ij}}}) = Y^{b_{ij}-q^2+q+1} \leq_P X^{q}Y^{q^2-q-1} <_P X^{a_{ij}}Y^{b_{ij}}.$$

[Case 7] $a_{ij} \in [q + 2, 2q]$ and $b_{ij} \in [q^2 - 2q, q^2 - q - 2]$.

If q is even, then

$$X^{a_{ij}}Y^{q^2-2q-1} <_P X^{a_{ij}}Y^{b_{ij}}$$

and

$$\mathrm{LM}(\overline{X^{a_{ij}}Y^{q^2-2q-1}}) = X^{a_{ij}-q-1}Y^{q^2-q-1} \geq_P \mathrm{LM}(\overline{X^{a_{ij}}Y^{b_{ij}}}) = X^{a_{ij}-q-1}Y^{b_{ij}-q+2}.$$

If q is odd, then

$$X^{a_{ij}}Y^{q^2-2q-1} <_P X^{a_{ij}}Y^{b_{ij}}$$

and

$$\mathrm{LM}(\overline{X^{a_{ij}}Y^{q^2-2q-1}}) = X^{a_{ij}-q-1}Y^{q^2-q-1} \geq_P \mathrm{LM}(\overline{X^{a_{ij}}Y^{b_{ij}}}) = X^{a_{ij}-q-1}Y^{b_{ij}+1}.$$

[Case 8] $a_{ij} \in [q + 2, 2q]$ and $b_{ij} \in [q^2 - q - 1, q^2 - 3]$.

$$\mathrm{LM}(\overline{X^{a_{ij}}Y^{b_{ij}}}) = X^{a_{ij}-q-1}Y^{b_{ij}-q+2} \leq_P X^{q}Y^{q^2-q-1} <_P X^{a_{ij}}Y^{b_{ij}}.$$

[Case 9] $a_{ij} \in [q + 2, 2q]$ and $b_{ij} \in [q^2 - 2, 2q^2 - 2q - 2]$

$$\mathrm{LM}(\overline{X^{a_{ij}}Y^{b_{ij}}}) = X^{a_{ij}-q-1}Y^{b_{ij}-q^2+q+1} \leq_P X^{q}Y^{q^2-q-1} <_P X^{a_{ij}}Y^{b_{ij}}.$$

The proof of this lemma is complete. (Q.E.D.)

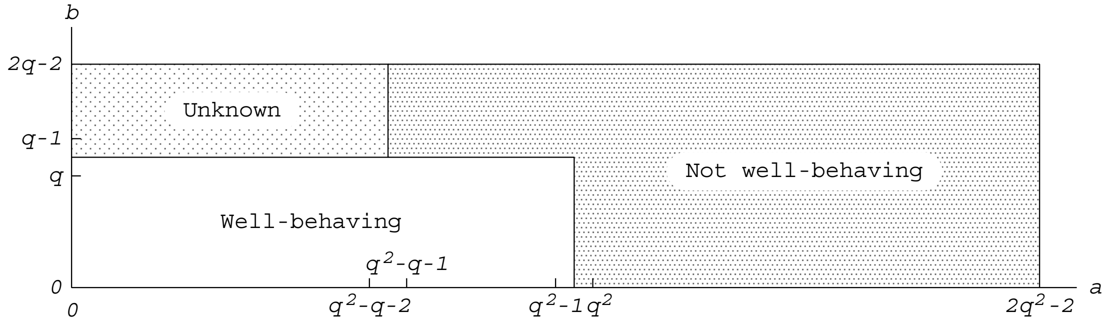


Figure 4.1: The extended delta set in the case of $Y^q > X^{q+1}$.

Hereafter, we consider only the case of $Y^q > X^{q+1}$. From Proposition 4.1.11, if

$$(a_{ij}, b_{ij}) \in \Delta = [0, q^2 - 1] \times [0, q - 1],$$

then the pair (i, j) is well-behaving. Also, if a pair (a_{ij}, b_{ij}) satisfies the assumption of Lemma 4.3.1, then the pair (i, j) is not well-behaving. These are shown in Figure 4.1. Now, as shown in Figure 4.1, it is unknown whether the pairs (i, j) which corresponds to

$$(a_{ij}, b_{ij}) \in [0, q^2 - q - 2] \times [q, 2q] \tag{4.31}$$

is well-behaving or not. Therefore, if all the pairs (i, j) which corresponds to (4.31) would be well-behaving, then Hermitian codes could have the largest Feng-Rao designed distance for any redundancy in the case of $Y^q > X^{q+1}$. In the following subsection, we investigate a class of monomial orders such that all the pairs (i, j) which corresponds to (4.31) are well-behaving. Also, in the case of $X^{q+1} > Y^q$, we can give a similar consideration from the consequence of Proposition 4.1.11 and Lemma 4.3.2.

4.3.2 Necessary Conditions and Sufficient Conditions to Be Well-Behaving

In this subsection, we provide necessary conditions and sufficient conditions to have well-behaving pairs by classifying the weight order. For convenience sake, we introduce the following total order on $\mathcal{W}$.

Definition 4.3.1. Let $(\mu_1, \nu_1, \cdot)$ and $(\mu_2, \nu_2, \circ)$ be any distinct weights in $\mathcal{W}$. A total order on $\mathcal{W}$ is defined by $(\mu_1, \nu_1, \cdot) \succ (\mu_2, \nu_2, \circ)$ if $(\mu_1, \nu_1, \cdot)$ and $(\mu_2, \nu_2, \circ)$ satisfy one of the following conditions

1. $\mu_1/\nu_1 > \mu_2/\nu_2$,

2. $\mu_1/\nu_1 = \mu_2/\nu_2$ and the dot $\cdot$ in $(\mu_1, \nu_1, \cdot)$ is X.

□

Let $(\mu_1, \nu_1, \cdot)$ and $(\mu_2, \nu_2, \circ)$ be any weights in $\mathcal{W}$ such that $(\mu_1, \nu_1, \cdot) \succ (\mu_2, \nu_2, \circ)$. If $X^aY^b \geq_{(\mu_2,\nu_2,\circ)} X^cY^d$ and $a \geq c$, then $X^aY^b \geq_{(\mu_1,\nu_1,\cdot)} X^cY^d$. Conversely, $X^aY^b \geq_{(\mu_1,\nu_1,\cdot)} X^cY^d$ and $a \leq c$, then $X^aY^b \geq_{(\mu_2,\nu_2,\circ)} X^cY^d$. From these observations, as the weight is large with respect to the total order $\succeq$ on $\mathcal{W}$, the exponent of X is given the higher priority than the exponent of Y. Next, we show some relations between weight orders and well-behaving pairs. We part into the two cases (a) and (b) in Lemma 4.2.1.

(a) In the Case of $Y^q >_{(\mu,\nu,\cdot)} X^{q+1}$.

The relation $Y^q >_{(\mu,\nu,\cdot)} X^{q+1}$ means

$$(\mu, \nu, \cdot) \preceq (q, q+1, Y). \tag{4.32}$$

Let Δ denote the delta set of $I(V)$ for the weight order $\geq_{(\mu,\nu,\cdot)}$ on $\mathcal{M}(X,Y)$. From the observation in Subsection 4.3.1, any pair (i,j) such that

$$(a_{ij}, b_{ij}) \in [0, q^2 - q - 2] \times [q, 2q - 2]. \tag{4.33}$$

is not yet decided whether well-behaving or not. We provide a necessary condition for the pair (i,j) with (4.33) to be well-behaving.

Lemma 4.3.3. Let $\mathcal{M}_n$ be the monomial basis associated with the weight order $\geq_{(\mu,\nu,\cdot)}$. If a pair (i,j) with (4.33) is well-behaving, then the weight $(\mu,\nu,\cdot)$ satisfies

$$(\mu, \nu, \cdot) \succeq (2q - b_{ij} - 1, q+1, X). \tag{4.34}$$

□

Proof. Assume that a pair (i,j) with (4.33) is well-behaving. We obtain

$$\overline{X^{a_{ij}}Y^{b_{ij}}} = X^{a_{ij}+q+1}Y^{b_{ij}-q} - X^{a_{ij}}Y^{b_{ij}-q+1}.$$

If $\mathrm{LM}(\overline{X^{a_{ij}}Y^{b_{ij}}}) = X^{a_{ij}}Y^{b_{ij}-q+1}$, then

$$X^{a_{ij}}Y^{b_{ij}-q+1} \leq_P X^{a_{ij}}Y^{q-1} <_P X^{a_{ij}}Y^{b_{ij}},$$

and hence the pair (i,j) is not well-behaving. Therefore, we obtain

$$X^{a_{ij}+q+1}Y^{b_{ij}-q} >_{(\mu,\nu,\cdot)} X^{a_{ij}}Y^{b_{ij}-q+1},$$

and hence

$$(\mu, \nu, \cdot) \succeq (1, q+1, X).$$

Since the pair (i,j) is well-behaving, we obtain

$$\mathrm{LM}(\overline{X^aY^b}) <_{(\mu,\nu,\cdot)} X^{a_{ij}+q+1}Y^{b_{ij}-q}$$

for any pair $(a, b) \in 2\Delta$ with $X^a Y^b <_P X^{a_{ij}} Y^{b_{ij}}$. For any pair $(a, b) \in [0, a_{ij}] \times [q, b_{ij}] \setminus \{(a_{ij}, b_{ij})\}$, we obtain

$$\mathrm{LM}(\overline{X^a Y^b}) = X^{a+q+1} Y^{b-q} <_P X^{a_{ij}+q+1} Y^{b_{ij}-q}.$$

For any pair $(a, b) \in [0, a_{ij}] \times [0, q-1]$, we obtain the inequality

$$\mu \cdot a + \nu \cdot b \leq \mu \cdot (a_{ij} + q + 1) + \nu \cdot (b_{ij} - q),$$

if equality holds only if the dot $\cdot$ in the weight $(\mu, \nu, \cdot)$ is X since $a < a_{ij} + q + 1$. At this time, since the maximum value of $\mu \cdot a + \nu \cdot b$ is $\mu \cdot a_{ij} + \nu \cdot (q-1)$, we obtain

$$\mu \cdot a + \nu \cdot (q-1) \leq \mu \cdot (a_{ij} + q + 1) + \nu \cdot (b_{ij} - q),$$

if equality holds only if the dot $\cdot$ in $(\mu, \nu, \cdot)$ is X. Therefore, we obtain

$$(\mu, \nu, \cdot) \succeq (2q - b_{ij} - 1, q + 1, X).$$

The proof of this lemma is complete. (Q.E.D.)

Furthermore, we provide a sufficient condition that all the pairs (i, j) with (4.33) are well-behaving by the following theorem.

Theorem 4.3.4. Let $\mathcal{M}_n$ be the monomial basis associated with the weight order $\geq_{(\mu,\nu,\cdot)}$. If the weight $(\mu, \nu, \cdot)$ satisfies

$$(q-1, q, X) \preceq (\mu, \nu, \cdot) \preceq (q, q+1, Y), \tag{4.35}$$

then all the pairs (i, j) with (4.33) are well-behaving. □

Proof. Assume that the weight $(\mu, \nu, \cdot)$ satisfies (4.35). Assume that any pair (i, j) satisfies (4.33) and any pair (u, v) satisfies $(u, v) <_P (i, j)$. From the property of monomial orders, we obtain

$$X^{a_{uv}} Y^{b_{uv}} <_{(\mu,\nu,\cdot)} X^{a_{ij}} Y^{b_{ij}}. \tag{4.36}$$

For any two pairs $(a, b), (c, d) \in \Delta$, since $0 \leq |b - d| \leq q - 1$ and μ and ν are relatively prime, if $\mu \geq q$ and $\mu \cdot a + \nu b = \mu \cdot c + \nu \cdot d$, then $(a, b) = (c, d)$. From this consequence, when $\mu \geq q$, the relation (4.36) can be rewritten as

$$\mu \cdot a_{uv} + \nu \cdot b_{uv} < \mu \cdot a_{ij} + \nu \cdot b_{ij}. \tag{4.37}$$

Hereafter, we assume that $\mu \geq q$. Assume that

$$\mu \cdot a_{ij} + \nu \cdot b_{ij} = \mu \cdot (a_{ij} + q + 1) + \nu \cdot (b_{ij} - q),$$

that is,

$$\frac{\mu}{\nu} = \frac{q}{q+1}.$$

By (4.37), we obtain

$$\mu \cdot a_{uv} + \nu \cdot b_{uv} < \mu \cdot (a_{ij} + q + 1) + \nu \cdot (b_{ij} - q).$$

This means

$$\mathrm{LM}(\overline{X^{a_{uv}} Y^{b_{uv}}}) <_{(\mu,\nu,\cdot)} \mathrm{LM}(\overline{X^{a_{ij}} Y^{b_{ij}}}),$$

and hence the pair (i, j) is well-behaving. Therefore, if $(\mu, \nu, \cdot) = (q, q + 1, Y)$, then all the pairs (i, j) with (4.33) are well-behaving.

Furthermore, the monomial basis $\mathcal{M}_n(\geq_{(\mu,\nu,\cdot)})$ associated with any weight order satisfying (4.35) is identical. The proof of this theorem is complete. (Q.E.D.)

From Theorem 4.3.4, if the weight satisfies (4.35), then all the pairs (i, j) with (4.33) are well-behaving, that is, all the pairs (a_{ij}, b_{ij}) of the unknown area in Figure 4.1 are well-behaving. This means that any monomial basis $\mathcal{M}_n = \mathcal{M}_n(\geq_{\boldsymbol{w}})$ such that the weight $\boldsymbol{w}$ satisfies (4.35) provides the linear code $C_r(\mathcal{M}_n)$ such that

$$d_{FR}(C_r(\mathcal{M}_n)) \geq d_{FR}(C_r(\mathcal{M}_n(\geq)))$$

for any redundancy r, where $\geq$ is any monomial order with $Y^q > X^{q+1}$. Note that all the weight orders satisfying (4.35) generate a unique monomial basis. For the monomial basis associated with any weight order satisfying (4.35), the corresponding N_s for any $s \in [1, n]$ is provided by the following theorem.

Theorem 4.3.5. Let $\mathcal{M}_n$ be the monomial basis associated with any weight order satisfying (4.35). Then, the evaluation sequence for the monomial basis $\mathcal{M}_n$ is provided by

$$N_s = \begin{cases} (a_s + 1) \cdot (b_s + 1) \\ \qquad\qquad \text{if } (a_s, b_s) \in [0, q] \times [0, q - 1], \\ q \cdot (a_s - q) + (q + 1) \cdot (b_s + 1) \\ \qquad\qquad \text{if } (a_s, b_s) \in [q + 1, q^2 - 1] \times [0, q - 1]. \end{cases} \tag{4.38}$$

□

Proof. For any pair (i, j) with (4.33), we obtain

$$\mathrm{LM}(\overline{X^{a_{ij}} Y^{b_{ij}}}) = X^{a_{ij}+q+1} Y^{b_{ij}-q} = X^{a_s} Y^{b_s}$$

for some pair $(a_s, b_s) \in \Delta$. From Theorem 4.3.4, the N_s with

$$(a_s, b_s) \in [q + 1, q^2 - 1] \times [0, q - 2] \tag{4.39}$$

is larger than the lower bound $(a_s + 1) \cdot (b_s + 1)$ provided by (4.25). Conversely, the N_s without (4.39) is identical with the lower bound $(a_s + 1) \cdot (b_s + 1)$. By the definition of the N_s, the N_s with (4.39) is given by adding the lower bound

$(a_s+1)(b_s+1)$ to the number of all the pairs (i,j) such that $(a_{ij}, b_{ij}) = (a_s - q - 1, b_s + q)$. Hence, the N_s with (4.39) is provided by

$$\begin{aligned} N_s &= (a_s+1)\cdot(b_s+1) + \#\{(i,j) \,|\, (a_{ij}, b_{ij}) = (a_s - q - 1, b_s + q)\} \\ &= (a_s+1)\cdot(b_s+1) + \#\{(i,j) \,|\, (a_i, b_i) = (a_s - q - 1 - a_j, b_s + q - b_j)\} \\ &= (a_s+1)\cdot(b_s+1) + \#[0, a_s - q - 1] \times [b_s + 1, q-1] \\ &= (a_s+1)\cdot(b_s+1) + (a_s - q)\cdot(q - 1 - b_s) \\ &= q\cdot(a_s - q) + (q+1)\cdot(b_s+1) \end{aligned}$$

In particular, for any $(a_s, b_s) \in [q+1, q^2-1] \times \{q-1\}$, we obtain

$$(a_s+1)\cdot(b_s+1) = (a_s+1)\cdot(b_s+1) + (a_s-q)\cdot(q-1-b_s).$$

(Q.E.D.)

(b) In the case of $X^{q+1} >_{(\mu,\nu,\cdot)} Y^q$.

The relation $X^{q+1} >_{(\mu,\nu,\cdot)} Y^q$ means

$$(\mu,\nu,\cdot) \succeq (q, q+1, X). \tag{4.40}$$

Let Δ denote the delta set of $I(V)$ for the weight order $\geq_{(\mu,\nu,\cdot)}$ on $\mathcal{M}(X,Y)$. Any pair (i,j) such that

$$(a_{ij}, b_{ij}) \in \{q+1\} \times [0, q^2 - q - 1] \cup [q+2, 2q] \times [0, q^2 - 2q - 1]. \tag{4.41}$$

is not yet decided whether well-behaving or not. We provide a necessary condition for the pair (i,j) with (4.41) to be well-behaving.

Lemma 4.3.6. Let $\mathcal{M}_n$ be the monomial basis associated with the weight order $\geq_{(\mu,\nu,\cdot)}$. If a pair (i,j) with (4.41) is well-behaving, then the weight $(\mu,\nu,\cdot)$ satisfies

$$(\mu,\nu,\cdot) \preceq (q, 2q - a_{ij} + 1, Y). \tag{4.42}$$

□

Proof. Assume that a pair (i,j) with (4.41) is well-behaving. We obtain

$$\overline{X^{a_{ij}} Y^{b_{ij}}} = X^{a_{ij}-q-1} Y^{b_{ij}+q} - X^{a_{ij}-q-1} Y^{b_{ij}+1}.$$

Since the pair (i,j) is well-behaving, we obtain

$$\mathrm{LM}(\overline{X^a Y^b}) <_{(\mu,\nu,\cdot)} X^{a_{ij}-q-1} Y^{b_{ij}+q}$$

for any pair $(a,b) \in 2\Delta$ with

$$X^a Y^b <_P X^{a_{ij}} Y^{b_{ij}}. \tag{4.43}$$

For any pair $(a, b) \in [q+1, a_{ij}] \times [q, b_{ij}] \setminus \{(a_{ij}, b_{ij})\}$, we obtain

$$\mathrm{LM}(\overline{X^a Y^b}) = X^{a-q-1} Y^{b+q} <_P X^{a_{ij}-q-1} Y^{b_{ij}+q}.$$

For any pair $(a, b) \in [0, q] \times [0, b_{ij}]$, we obtain the inequality

$$\mu \cdot a + \nu \cdot b \leq \mu \cdot (a_{ij} - q - 1) + \nu \cdot (b_{ij} + q),$$

if equality holds only if the dot $\cdot$ in the weight $(\mu, \nu, \cdot)$ is Y since $b < b_{ij} + q$. At this time, since the maximum value of $\mu \cdot a + \nu \cdot b$ is $\mu \cdot q + \nu \cdot b_{ij}$, we obtain

$$\mu \cdot q + \nu \cdot b_{ij} \leq \mu \cdot (a_{ij} - q - 1) + \nu \cdot (b_{ij} + q),$$

if equality holds only if the dot $\cdot$ in $(\mu, \nu, \cdot)$ is Y. Therefore, we obtain

$$(\mu, \nu, \cdot) \succeq (q, 2q - a_{ij} + 1, Y).$$

The proof of this lemma is complete. (Q.E.D.)

Furthermore, we provide a sufficient condition that all the pairs (i, j) with (4.41) are well-behaving by the following theorem.

Theorem 4.3.7. Let $\mathcal{M}_n$ be the monomial basis associated with the weight order $\geq_{(\mu,\nu,\cdot)}$. If the weight $(\mu, \nu, \cdot)$ satisfies

$$(q, q+1, X) \preceq (\mu, \nu, \cdot) \preceq (1, 1, Y), \tag{4.44}$$

then all the pairs (i, j) with (4.41) are well-behaving. □

Proof. Assume that the weight $(\mu, \nu, \cdot)$ satisfies (4.44). Assume that any pair (i, j) satisfies (4.41) and any pair (u, v) satisfies $(u, v) <_P (i, j)$. From the property of monomial orders, we obtain

$$X^{a_{uv}} Y^{b_{uv}} <_{(\mu,\nu,\cdot)} X^{a_{ij}} Y^{b_{ij}}. \tag{4.45}$$

For any two pairs $(a, b), (c, d) \in \Delta$, since $0 \leq |a - c| \leq q$ and μ and ν are relatively prime, if $\nu \geq q + 1$ and $\mu \cdot a + \nu b = \mu \cdot c + \nu \cdot d$, then $(a, b) = (c, d)$. From this consequence, when $\nu \geq q + 1$, the relation (4.45) can be rewritten as

$$\mu \cdot a_{uv} + \nu \cdot b_{uv} < \mu \cdot a_{ij} + \nu \cdot b_{ij}. \tag{4.46}$$

Hereafter, we assume that $\nu \geq q + 1$. Assume that

$$\mu \cdot a_{ij} + \nu \cdot b_{ij} = \mu \cdot (a_{ij} - q - 1) + \nu \cdot (b_{ij} + q),$$

that is,

$$\frac{\mu}{\nu} = \frac{q}{q+1}.$$

By (4.46), we obtain

$$\mu \cdot a_{uv} + \nu \cdot b_{uv} < \mu \cdot (a_{ij} - q - 1) + \nu \cdot (b_{ij} + q).$$

This means

$$\mathrm{LM}(\overline{X^{a_{uv}} Y^{b_{uv}}}) <_{(\mu,\nu,\cdot)} \mathrm{LM}(\overline{X^{a_{ij}} Y^{b_{ij}}}),$$

and hence the pair (i, j) is well-behaving. Therefore, if $(\mu, \nu, \cdot) = (q, q+1, X)$, then all the pairs (i, j) with (4.41) are well-behaving.

Furthermore, the monomial basis $\mathcal{M}_n(\geq_{(\mu,\nu,\cdot)})$ associated with any weight order satisfying (4.44) is identical. The proof of this theorem is complete. (Q.E.D.)

From Theorem 4.3.7, if the weight order satisfies (4.44), then all the pairs (i, j) with (4.33) are well-behaving. This means that any monomial basis $\mathcal{M}_n = \mathcal{M}_n(\geq_{\boldsymbol{w}})$ such that the weight $\boldsymbol{w}$ satisfies (4.44) provides the linear code $C_r(\mathcal{M}_n)$ such that

$$d_{FR}(C_r(\mathcal{M}_n)) \geq d_{FR}(C_r(\mathcal{M}_n(\geq)))$$

for any redundancy r, where $\geq$ is any monomial order with $X^{q+1} > Y^q$. Note that all the weight orders satisfying (4.35) generate a unique monomial basis. For the monomial basis associated with any weight order satisfying (4.44), the corresponding N_s for any $s \in [1, n]$ is provided by the following theorem.

Theorem 4.3.8. Let $\mathcal{M}_n$ be any monomial basis associated with the weight order satisfying (4.44). Then, the evaluation sequence for the monomial basis $\mathcal{M}_n$ is provided by

$$N_s = \begin{cases} (a_s + 1) \cdot (b_s + 1) \\ \qquad \text{if } (a_s, b_s) \in [0, q] \times [0, q-1], \\ q \cdot (a_s - q) + (q+1) \cdot (b_s + 1) \\ \qquad \text{if } (a_s, b_s) \in \{0\} \times [q, q^2 - 1] \cup [1, q] \times [q, q^2 - q - 1]. \end{cases} \tag{4.47}$$

□

Proof. For any pair (i, j) with (4.41), we obtain

$$\mathrm{LM}(\overline{X^{a_{ij}} Y^{b_{ij}}}) = X^{a_{ij} - q - 1} Y^{b_{ij} + q} = X^{a_s} Y^{b_s}$$

for some pair $(a_s, b_s) \in \Delta$. From Theorem 4.3.7, the N_s with

$$(a_s, b_s) \in \{0\} \times [q, q^2 - 1] \cup [1, q-1] \times [q, q^2 - q - 1] \tag{4.48}$$

is larger than the lower bound $(a_s + 1) \cdot (b_s + 1)$ provided by (4.25). Conversely, the N_s without (4.48) is identical with the lower bound $(a_s + 1) \cdot (b_s + 1)$. By the definition of the N_s, the N_s with (4.48) is given by adding the lower bound

$(a_s+1)(b_s+1)$ to the number of all the pairs (i,j) such that $(a_{ij},b_{ij}) = (a_s + q+1, b_s-q)$. Hence, the N_s with (4.48) is provided by

$$\begin{aligned} N_s &= (a_s+1)\cdot(b_s+1) + \#\{(i,j)\,|\,(a_{ij},b_{ij}) = (a_s+q+1, b_s-q)\} \\ &= (a_s+1)\cdot(b_s+1) + \#\{(i,j)\,|\,(a_i,b_i) = (a_s+q+1-a_j, b_s-q-b_j)\} \\ &= (a_s+1)\cdot(b_s+1) + \#[a_s+1,q]\times[0,b_s-q] \\ &= (a_s+1)\cdot(b_s+1) + (q-a_s)\cdot(b_s-q+1) \\ &= q\cdot(a_s-q) + (q+1)\cdot(b_s+1). \end{aligned}$$

The proof of this theorem is complete. (Q.E.D.)

4.3.3 Optimal Monomial Orders for Hermitian Codes

In this subsection, we provide a class of monomial orders which have the largest Feng-Rao designed distance for Hermitian codes by Miura's construction. From the proofs in the previous subsection, the monomial basis $\mathcal{M}_n(\geq_{(q,q+1,Y)})$ provides the largest Feng-Rao designed distance in the monomial bases associated with all monomial order $\geq$ such that $Y^q > X^{q+1}$. On the other hand, the monomial basis $\mathcal{M}_n(\geq_{(q,q+1,X)})$ provides the largest Feng-Rao designed distance in the monomial bases associated with all monomial order $\geq$ such that $X^{q+1} > Y^q$. It remains to compare the monomial basis $\mathcal{M}_n(\geq_{(q,q+1,Y)})$ with the monomial basis $\mathcal{M}_n(\geq_{(q,q+1,X)})$. As a matter of fact, both the evaluation sequences for $\mathcal{M}_n(\geq_{(q,q+1,Y)})$ and $\mathcal{M}_n(\geq_{(q,q+1,X)})$ are identical. As a consequence in this chapter, we provide the following theorem.

Theorem 4.3.9. The weight order $\geq_{(\mu,\nu,\cdot)}$ such that

$$(q-1,q,X) \preceq (\mu,\nu,\cdot) \preceq (1,1,Y) \tag{4.49}$$

is an optimal monomial order on $\mathcal{M}(X,Y)$ associated with V. In particular, both the evaluation sequences given in Theorems 4.3.5 and 4.3.8 are identical. □

Proof. It is sufficient to consider two monomial bases associated with $\mathcal{M}_n^{(1)} := \mathcal{M}_n(\geq_{(q,q+1,Y)})$ and $\mathcal{M}_n^{(2)} := \mathcal{M}_n(\geq_{(q,q+1,X)})$. Let $\mathcal{G}^{(1)}$ and $\Delta^{(1)}$ denote the reduced Gröbner basis and the delta set with the weight order $\geq_{(q,q+1,Y)}$, respectively. Similarly, let $\mathcal{G}^{(2)}$ and $\Delta^{(2)}$ denote the reduced Gröbner basis and the delta set with the weight order $\geq_{(q,q+1,X)}$, respectively. Let $((a_i^{(1)}, b_i^{(1)})\,|\,i\in[1,n])$ and denote the sequence of all elements of $\Delta^{(1)}$ in increasing order with respect to the monomial order $\geq_{(}\ q,q+1,Y)$ on $\mathcal{M}(X,Y)$. Let $((a_i^{(2)}, b_i^{(2)})\,|\,i\in[1,n])$ and denote the sequence of all elements of $\Delta^{(1)}$ in increasing order with respect to the monomial order $\geq_{(}\ q,q+1,X)$ on $\mathcal{M}(X,Y)$.

For any pair $(a,b)\in\Delta^{(1)}$, the nonnegative integer $Q(a)$ and $R(a)$ are defined by the following division:

$$a = Q(a)\cdot(q+1) + R(a) \quad \text{and} \quad 0 \leq R(a) < q+1.$$

The map Θ from $\Delta^{(1)}$ into $\mathbb{N}_0^2$ is defined by

$$\Theta(a,b) := (R(a), Q(a) \cdot q + b)$$

for any pair $(a,b) \in \Delta^{(1)}$. Since $0 \leq a < q^2$, we obtain $0 \leq Q(a) < q$, and then $0 \leq Q(a) \cdot q + b < q^2$. In particular, if $a = q^2 - 1$, then $q - 1 \leq q^2 - q + b < q^2$ and $b = 0$. If $a \neq q^2 - 1$, then $0 \leq Q(a) < q - 1$ and $0 \leq Q(a) \cdot q + b < q^2 - q$. Therefore, the map Θ is a map from $\Delta^{(1)}$ into $\Delta^{(2)}$. Further, for any pairs (a,b) and (c,d) in $\Delta^{(1)}$, if $\Theta(a,b) = \Theta(c,d)$, that is, $b - d = (Q(a) - Q(c)) \cdot q$ and $R(a) = R(c)$, then $(a,b) = (c,d)$ since $0 \leq |b - d| < q$. As a result, the map Θ is a bijective map from $\Delta^{(1)}$ to $\Delta^{(2)}$. Here, for any $(a,b) \in \Delta^{(1)}$, if we are using the weight order $\geq_{(q,q+1,X)}$, then

$$\overline{X^a Y^b}^{\mathcal{G}_2} = X^{R(a)} Y^{Q(a) \cdot q + b} + X^{R(a)} Y^{Q(a) + b},$$

and hence

$$\mathrm{LM}(\overline{X^a Y^b}^{\mathcal{G}_2}) = X^{R(a)} Y^{Q(a) \cdot q + b}.$$

This means that

$$x^{a_i^{(1)}} y^{b_i^{(1)}} \in \mathrm{Span}\{x^{a_j^{(2)}} y^{b_j^{(2)}} \mid j \in [1, i]\}$$

for any number $i \in [1, n]$. Therefore, both the monomial bases $\mathcal{M}_n^{(1)}$ and $\mathcal{M}_n^{(2)}$ have the same subspace subspace. Therefore, from Theorem 3.2.3, we obtain

$$N(\mathcal{M}_n^{(1)}) = N(\mathcal{M}_n^{(2)})$$

As a consequence of these, any weight order with (4.49) is an optimal monomial order for V. (Q.E.D.)

This theorem provides a class of optimal monomial orders for Hermitian curves. Especially, the weight order associated with $(q, q+1, Y)$ generates the structure sequence for the Hermitian codes by Goppa's construction. Therefore, improved geometric codes of Goppa's construction are optimal as for the Hermitian curve.

In Figure 4.2, we illustrate the Feng-Rao designed distance as for several weight orders when $q = 4$. The horizontal and vertical axes represents the redundancy and distance, respectively. The weight order associated with $(4, 5, Y)$ is an optimal monomial order, since the weight $(4, 5, Y)$ satisfies (4.49) in Theorem 4.3.9. On the other hand, the weight order associated with $(1, 16, Y)$ is not optimal. Note that both the delta sets are same, and but both the monomial bases are different. In fact, as shown in Figure 4.2, the Feng-Rao designed distance associated with the weight $(4, 5, Y)$ is equal to or larger than that associated with the weight $(1, 16, Y)$. Especially, the Feng-Rao designed distance associated with the weight $(4, 5, Y)$ exactly plot between Goppa bound and Singleton bound. The Feng-Rao designed distance associated with the weight $(1, 16, Y)$ is exactly equal to the lower bound provided in (4.25). This means that the Feng-Rao designed distance associated with any monomial order satisfying $Y^4 > X^5$ is always equal to or larger than that associated with the weight $(1, 16, Y)$.

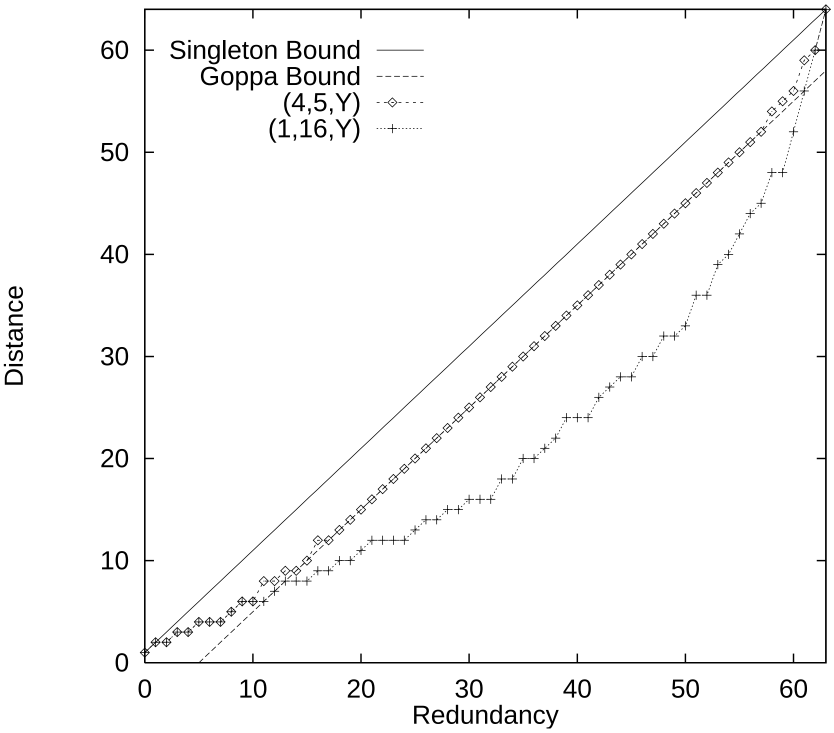


Figure 4.2: The Feng-Rao Designed Distance for Hermitian Codes over $\mathbb{F}_{16}$.

4.4 Conclusion

Miura's construction method for algebraic geometric codes on affine algebraic varieties has provided an optimization problem for Feng-Rao designed distance with respect to the monomial orders. In this chapter, we have taked up the Hermitian curve as an object of the optimization problem above, because the Hermitian curve have been optimal in the sense of Goppa's construction.

Firstly, we have provided the reduced Gröbner basis and the delta set associated with any monomial order. This means an explicit description of Hermitian codes by Miura's construction. Also, we have shown that any the monomial basis can be represented by a monomial basis associated with some weight order. Based on these results, we have shown the relation between both the linear codes on the Hermitian curve by Goppa's and Miura's construction. As for the Hermitian curve, Goppa's construction has included in Miura's construction method. Next, we have shown sufficient conditions not to have well-behaving pairs by using the exponents of monomials. Further, we have shown necessary conditions and sufficient conditions to have well-behaving pairs by using the weight order. Then, by using their relation, we have clarified a class of optimal monomial orders for linear codes on the Hermitian curve. Also, we have illustrated an example the case that finite field volume is 16.

Chapter 5

One-Point Codes from Artin-Schreier Extensions of Hermitian Function Fields

In 1982, Tsfasman et al. [62, 60] discovered a sequence of algebraic geometric codes over $\mathbb{F}_q$ which asymptotically exceeds the Gilbert-Varshamov bound when q is a square and $q \geq 49$ by studying the number of rational points and genera on modular curves over finite fields. Furthermore, Katsman et al. [29, 67, 68] showed that the construction of the codes on modular curves can be done with polynomial complexity of degree at most 30. Unfortunately, the construction of codes on modular curves has too high complexity for practical applications.

Garcia and Stichtenoth [14] discovered a tower of Artin-Schreier extensions of algebraic function fields attaining the Drinfeld-Vlăduţ bound. This means that a sequence of codes from these towers asymptotically exceed the Gilbert-Varshamov bound. This tower has an advantage over sequences of modular curves in that they have the explicit descriptions. Therefore, one may give the explicit descriptions of the codes on this tower. Further, this tower has the following properties: algebraic geometric codes from the first and second algebraic function fields on this tower are known as Reed-Solomon codes and Hermitian codes, respectively. Both the codes are optimal in Goppa's construction, since these algebraic function fields have maximal rational places as compared with their genera. Therefore, one expects that the codes from third function field are good algebraic geometric codes. In 1997, Voss and Høholdt [69] showed an explicit description of generator matrices of algebraic geometric codes from the third algebraic function field. However, the class of their codes did not entirely include all one-point codes from the third function field. Also, it requires some efforts to understand their description since bases for the linear spaces involved in the description are monomials with negative exponents.

On the other hand, Miura [42, 44] presented powerful tools to transfer from any algebraic function field into an affine nonsingular absolutely irreducible curve by using the theory of Gröbner bases. This curve is useful to construct one-point codes from the given algebraic function field.

In this chapter, we provide an explicit description of one-point codes from the third algebraic function field. This chapter is organized as follows. Section 5.1 is the part of preliminaries. We introduce the basic properties of one-point codes and the third algebraic function field on Garcia-Stichtenoth's tower. Also, we present an explicit description of all rational places of the third algebraic function field. Section 5.2 is the main part in this chapter. At first, we clarify rational functions of the third algebraic function field which correspond to generators of semigroup of nongaps at a specific rational place and further the number of generators is minimal. These rational functions and rational places of the third algebraic function field enable us to provide a explicit description of one-point codes from the third algebraic function field. Further, we illustrate the comparison between the Feng-Rao designed distance of our codes and the BCH designed distance of some BCH codes. As a result, the proposed codes are better than the BCH codes for almost all redundancy when the finite field volume is large. Especially, we obtain an one-point codes with parameters $[4047, 1047, 2504]$ which can correct more 261 errors than the corresponding BCH code.

We summarize several advantages of the proposed codes as follows:

(1) The fast implementation [54] of the decoding algorithm up to the Feng-Rao designed distance can be applied to the proposed codes.

(2) The decoding complexity of the proposed codes from the viewpoint of the number of generators is optimal.

(3) The length of the proposed codes is longer than that of codes suggested by Voss and Høholdt, as we preserve the redundancy and the Feng-Rao designed distance.

The results in this chapter is based in part on a study published at IEICE Transactions on Fundamentals [64].

5.1 Preliminaries

This section corresponds to the part of preliminaries of our work. Firstly, we investigate the basic properties of one-point codes from algebraic function fields. Next, we present the basic properties of numerical semigroup. This part play a crucial role in the analysis of the nongap sequence at a place. Lastly, we introduce a tower of Artin-Schreier extensions of algebraic function fields which is proposed by Garcia and Stichtenoth [14].

5.1.1 Fundamental Properties of One-Point Codes

In this subsection, we introduce one-point codes based on algebraic function fields. As for main properties of algebraic function fields and algebraic geometric codes, we refer to [58].

Let $\mathbb{F}_q := \mathrm{GF}(q)$ denote the finite field with q elements, and $F/\mathbb{F}_q$ an algebraic function field with the constant field $\mathbb{F}_q$. Note that Section 2.3 starts with algebraic curves whereas this section starts with algebraic function fields since Garcia-Stichtenoth's tower founds on the theory of algebraic function fields.

Let $\mathbb{P}_F$ be the set of places of $F/\mathbb{F}_q$, and $\mathbb{P}_F^1$ the set of rational places of $F/\mathbb{F}_q$. The genus of $F/\mathbb{F}_q$ denoted by $g(F)$ or simply by g which algebraic function field is meant. The number of rational places of $F/\mathbb{F}_q$ is denoted by $N(F)$ or simply by N.

Let $P_1, P_2, \cdots, P_n$, and P be n distinct rational places of $F/\mathbb{F}_q$. Then, the number n is properly less than the number of rational places N. The divisor $P_1 + P_2 + \cdots + P_n$ is denoted by D. For any integer m, the *evaluation map* ev_D from the linear space $L(mP)$ onto $\mathbb{F}_q^n$ is defined by

$$\mathrm{ev}_D(f) := (f(P_1), f(P_2), \cdots, f(P_n)),$$

such as Section 2.3. This mapping is $\mathbb{F}_q$-linear, and injective when $m < n$. An one-point code associated with divisors D and mP is defined by

$$C_L(D, mP) := \{\mathrm{ev}_D(f) \mid f \in L(mP)\}, \tag{5.1}$$

$$C_\Omega(D, mP) := C_L(D, G)^\perp, \tag{5.2}$$

where $S^\perp$ is the dual space of a subset S in $\mathbb{F}_q^n$. The kernel of the mapping ev_D is $L(mP - D)$, and hence

$$\dim C_L(D, mP) = l(mP) - l(mP - D). \tag{5.3}$$

The parameters of algebraic geometric codes satisfy

$$k + d \geq n - g + 1,$$

where k and d are their dimension and minimum distance, respectively. As special features of one-point codes $C_\Omega(D, mP)$, one can easily estimate the Feng-Rao designed distance d_{FR} [30], and apply the fast implementation [54] of the decoding algorithm up to $\lfloor (d_{FR} - 1)/2 \rfloor$ errors.

Now, we introduce the ring $K_\infty(P)$ and the numerical semigroup of nongaps at P, since they play an important role to provide an explicit description of one-point codes in later section. $K_\infty(P)$ is defined by a subring of $F/\mathbb{F}_{q^2}$ whose elements have no pole at any places except P, that is,

$$K_\infty(P) := \bigcup_{m=0}^{\infty} L(mP). \tag{5.4}$$

An integer m is called *nongap* at P if $l(mP) = l((m-1)P) + 1$. Otherwise, m is called *gap* at P. An integer m is a nongap at P if and only if there exists a rational function which has a pole of order m at P and no other poles. The number of gaps of P is equal to the genus g of algebraic function field since

$$l(mP) = m - g + 1$$

if m is greater than $2g-2$ by Riemann-Roch theorem (Proposition 2.3.1). Especially, we obtain

$$1 = l(0) \le l(P) \le \cdots \le l((2g-1)P) = g.$$

If m_1 and m_2 are nongaps at P, then $m_1 + m_2$ is also a nongap at P, since $(f_1)_\infty = m_1 P$ and $(f_2)_\infty = m_2 P$ mean $(f_1 f_2)_\infty = (m_1 + m_2)P$. Thus, the nongaps at any place form a *semigroup* in $\mathbb{N}_0$. Let $(o_i \,|\, i \in \mathbb{N})$ be an enumeration of all the nongaps at P in increasing order, so $o_0 = 0$. The semigroup of nongaps at P is given by

$$\{-v_P(f) \in \mathbb{N}_0 \,|\, f \in K_\infty(P) \setminus \{0\}\},$$

where v_P is the discrete valuation of $F/\mathbb{F}_q$ corresponding to P.

5.1.2 Semigroups

In order to analyze the semigroup of nongaps in previous section, we show the general properties of semigroups. As for the formulation of semigroups in this section, we refer to [42, 44].

Let $A := (a_1, a_2, \cdots, a_t)$ be a sequence of t distinct positive integers, and define the set $S_A := \{a_1, a_2, \cdots, a_t\}$. We assume that $\gcd S_A = 1$, where $\gcd S$ is the greatest common divisor of S. The semigroup generated by S_A in $\mathbb{N}_0$ is denoted by $\langle S_A \rangle$, that is

$$\langle S_A \rangle := \{ \sum_{i=1}^{t} u_i a_i \,|\, u_i \in \mathbb{N}_0 \text{ for all } i \in [1, t]\}\,.$$

By the assumption that the greatest common divisor of S_A is equal to 1, the cardinality of the set $\mathbb{N}_0 \setminus \langle S_A \rangle$ is finite An element in $\langle S_A \rangle$ is called a *nongap* of $\langle S_A \rangle$ and an element of $\mathbb{N}_0 \setminus \langle S_A \rangle$ is called a *gaps* of $\langle S_A \rangle$. The number of gaps is denoted by $g(A)$. From [42, 44], we obtain $g(A) = \sum_{i=1}^{a_1 - 1} \lfloor b_i / a_1 \rfloor$ where

$$b_i := \min\{b \in \langle S_A \rangle \,|\, b \equiv i \bmod a_1\}. \tag{5.5}$$

The set S_A is called *minimal set* of generators of $\langle S_A \rangle$ if $a_i \notin \langle S_A \setminus \{a_i\} \rangle$ for any $i \in [1, t]$. Note that every semigroup has a finite set of generators and that every set of generators contains a unique minimal set of generators.

Next, we introduce total ordering on $\mathbb{N}_0^t$. Consider the surjective mapping Ψ_A from $\mathbb{N}_0^t$ to $\langle S_A \rangle$ given by

$$\Psi_A((m_1, m_2, \cdots, m_t)) := \sum_{i=1}^{t} a_i m_i.$$

Then, define a total ordering $>_A$ on $\mathbb{N}_0^t$ as follows: for $M = (m_1, m_2, \cdots, m_t)$, $N = (n_1, n_2, \cdots, n_t) \in \mathbb{N}_0^t$, $M >_A N$ if and only if $\Psi_A(M) > \Psi_A(N)$, or $\Psi_A(M) = \Psi_A(N)$ and $m_1 = n_1, m_2 = n_2, \cdots, m_i < n_i$. We call $>_A$ by *A-weight order*. For $a \in \langle S_A \rangle$, let

$$M_A(a) := \min_{>_A} \{ M \in \mathbb{N}_0^t \mid \Psi_A(M) = a \} \tag{5.6}$$

where $\min_{>_A}$ is the minimum element in $\mathbb{N}_0^t$ with respect to A-weight order. $M_A(a)$ is uniquely determined for each $a \in \langle S_A \rangle$.

5.1.3 A Tower of Artin-Schreier Extensions of Algebraic Function Fields

In this subsection, we introduce a tower of Artin-Schreier extensions of algebraic function fields which was presented by Garcia and Stichtenoth [14]. As for main properties of this tower, we refer to [14, 69]. Hereafter, we apply the notations in Section 5.1.1 to the finite field $\mathbb{F}_{q^2}$.

Definition 5.1.1. Let $F_1 := \mathbb{F}_{q^2}(x_1)$ be the rational function field over $\mathbb{F}_{q^2}$. For $n \geq 1$, let

$$F_{n+1} := F_n(z_{n+1}) \tag{5.7}$$

such that z_{n+1} satisfies $z_{n+1}^q + z_{n+1} = x_n^{q+1}$, where $x_n := z_n / x_{n-1}$ for $n \geq 2$. In particular, $F_2/\mathbb{F}_{q^2}$ is the Hermitian function field. □

For the sequence $(F_i \mid i \in \mathbb{N})$,

$$\lim_{i \to \infty} \frac{N(F_i)}{g(F_i)} = q - 1, \tag{5.8}$$

that is, $(F_i \mid i \in \mathbb{N})$ attains the Drinfeld-Vlăduţ bound. For $i \in \mathbb{N}$, we obtain $[F_{i+1} : F_i] = q$.

Next, we consider rational places of the function field $F_3/\mathbb{F}_{q^2}$. Let $P_\infty^{(1)}$ be the pole of x_1 in F_1. Since $P_\infty^{(1)}$ is totally ramified in F_3/F_1, $P_\infty^{(1)}$ has a unique extension P_∞ in F_3. P_∞ is the common pole of x_1, z_2, and z_3 in F_3. To describe all rational places of $F_3/\mathbb{F}_{q^2}$ except P_∞, we prepare two sets

$$\mathcal{A} := \{ (\alpha, \beta, \gamma) \in \mathbb{F}_{q^2}^3 \mid \alpha \neq 0,\ \beta^q + \beta = \alpha^{q+1},\ \text{and}\ \gamma^q + \gamma = (\beta\alpha^{-1})^{q+1} \},$$
$$\mathcal{A}_0 := \{ \epsilon \in \mathbb{F}_{q^2} \mid \epsilon^q + \epsilon = 0 \}.$$

Then, all places $P \in \mathbb{P}_{F_3}^1 \setminus \{P_\infty\}$ are uniquely classified by three values $x_1(P)$, $z_2(P)$ and $z_3(P)$ as follows:

Type 1. $P_{00\gamma}$ for $\gamma \in \mathcal{A}_0$.

For each $\gamma \in \mathcal{A}_0$, there is a unique place $P \in \mathbb{P}^1_{F_3}$ such that $x_1(P) = 0$, $z_2(P) = 0$, and $z_3(P) = \gamma$. We denote this place P by $P_{00\gamma}$.

Type 2. $P_{0\beta*}$ for $\beta \in \mathcal{A}_0 \setminus \{0\}$.

For each $\beta \in \mathcal{A}_0 \setminus \{0\}$, there is a unique place $P \in \mathbb{P}^1_{F_3}$ such that $x_1(P) = 0$, $z_2(P) = \beta$, and $z_3(P) = \infty$. We denote this place P by $P_{0\beta*}$.

Type 3. $P_{\alpha\beta\gamma}$ for $(\alpha, \beta, \gamma) \in \mathcal{A}$.

For each $(\alpha, \beta, \gamma) \in \mathcal{A}$, there is a unique place $P \in \mathbb{P}^1_{F_3}$ such that $x_1(P) = \alpha$, $z_2(P) = \beta$, and $z_3(P) = \gamma$. We denote this place P by $P_{\alpha\beta\gamma}$.

The number of rational places of $F_3/\mathbb{F}_{q^2}$ for Type 1, Type 2 and Type 3 are q, $q - 1$ and $q^4 - q^2$, respectively. As a result, the number of rational places of $F_3/\mathbb{F}_{q^2}$ is $N(F_3) = q^4 - q^2 + 2q$ by counting P_∞. On the other hand, the genus of $F_3/\mathbb{F}_{q^2}$ is $g(F_3) = q^3 - 2q + 1$.

From now on, we consider only algebraic function field $F_3/\mathbb{F}_{q^2}$, and we abbreviate $g(F_3)$ and $N(F_3)$ by g and N, respectively.

5.2 An Explicit Description of One-Point Codes from the Third Algebraic Function Field

In this section, we provide an explicit description of one-point codes from the third function field $F_3/\mathbb{F}_{q^2}$ on the Garcia-Stichtenoth's tower $(F_i \,|\, i \in \mathbb{N})$. Firstly, we consider a basis of the linear space $L(mP)$ over $\mathbb{F}_{q^2}$. Especially, we explicitly describe a basis of the linear space $L(mP)$ by using $2q$ rational functions. The nongaps of these rational functions forms the minimal generators of nongaps at P_∞. These results are related with an explicit description of one-point codes from the third algebraic function field $F_3/\mathbb{F}_{q^2}$. Finally, we compare the Feng-Rao designed distance of these codes with the BCH designed distance of some BCH codes.

5.2.1 An Explicit Description of Basis for $L(mP_\infty)$

Voss and Høholdt clarified a basis for linear space $L(mP_\infty)$ over $\mathbb{F}_{q^2}$ by using monomials in x_1, z_2 and z_3 with negative exponents, and nongaps at P_∞ [69, Theorem 4.3 and Corollary 4.10]. Also, they provided generators of semigroup of nongaps at P_∞ in case of $q = 2$, 3 and 4 [69, Example 4.11]. In this chapter, for any prime power q, we provide generators of semigroup of nongaps at P_∞ and corresponding rational functions of F_3 by using polynomials in x_1, z_2 and z_3. As a result, we obtain a $\mathbb{F}_{q^2}$-basis of monomial type for $L(mP_\infty)$.

To express the principal divisors of x_1, z_2 and z_3, consider two divisors

$$D_0 := \sum_{\gamma \in \mathcal{A}_0 \backslash \{0\}} P_{00\gamma} \text{ and } E_0 := \sum_{\beta \in \mathcal{A}_0 \backslash \{0\}} P_{0\beta *}.$$

Then, the principal divisors of x_1, z_2, and z_3 are given by

$$\begin{aligned} (x_1) &= P_{000} + D_0 + qE_0 - q^2 P_\infty, \\ (z_2) &= (q+1)P_{000} + (q+1)D_0 - q(q+1)P_\infty, \\ (z_3) &= q(q+1)P_{000} - (q+1)E_0 - (q+1)P_\infty, \end{aligned}$$

respectively [69]. From above equations, for $i, j, k \in \mathbb{Z}$, $x_1^i z_2^j z_3^k \in K_\infty(P_\infty)$ if and only if

$$\left. \begin{array}{l} i + (q+1)j + q(q+1)k \geq 0, \\ i + (q+1)j \geq 0, \\ qi - (q+1)k \geq 0, \end{array} \right\} \tag{5.9}$$

holds. Next theorem is our main result.

Theorem 5.2.1. Let $y_1 := x_1$, $y_2 := z_2$,

$$\begin{aligned} y_{3+j} &:= x_1^{2+j} z_3^{1+j}, \\ y_{q+2+j} &:= x_1^{q+1} z_2^{-1} z_3^{1+j} = (z_2^{q-1} + 1) z_3^{1+j}, \end{aligned}$$

for $j \in [0, q-2]$. Then,

$$K_\infty(P_\infty) = \mathbb{F}_{q^2}[y_1, y_2, \cdots, y_{2q}],$$

and the semigroup of nongaps at P_∞ is generated by S_{A_3} for $A_3 := (a_1, a_2, \cdots, a_{2q})$ where $a_i := -v_{P_\infty}(y_i)$ for $i \in [1, 2q]$. Moreover, S_{A_3} is the minimal set of generators of semigroup of nongaps at P_∞. □

Proof. Proof of the theorem can be done in two parts.

(Part 1) $K_\infty(P_\infty) = \mathbb{F}_{q^2}[y_1, y_2, \cdots, y_{2q}]$.

For any $i \in [1, 2q]$, y_i satisfies (5.9). Hence, $\mathbb{F}_{q^2}[y_1, y_2, \cdots, y_{2q}]$ is included in $K_\infty(P_\infty)$. Thus, we obtain $g \leq g(A_3)$.

To show that $K_\infty(P_\infty) = \mathbb{F}_{q^2}[y_1, y_2, \cdots, y_{2q}]$ and the semigroup of nongaps at P_∞ is generated by S_{A_3}, it is enough to prove $g = g(A_3)$. Since $a_i = -v_{P_\infty}(y_i)$ for $i \in [1, 2q]$, we obtain

$$\begin{aligned} a_1 &= q^2, \\ a_2 &= q^2 + q, \\ a_{3+j} &= (j+2)q^2 + (j+1)q + j + 1, \\ a_{q+2+j} &= q^3 + jq + j + 1, \end{aligned}$$

for $j \in [0, q-2]$. Then,

$$a_1 < a_2 < \cdots < a_q < a_{q+2} < \cdots < a_{2q} < a_{q+1}. \tag{5.10}$$

Consider the following nonnegative integers

$$\begin{aligned}
c_{2,l} &:= a_2(l+1) \\
&= (l+1)q^2 + (l+1)q, \\
c_{3+j,l} &:= a_{3+j} + a_2 l \\
&= (j+l+2)q^2 + (j+l+1)q + j + l + 1, \\
c_{q+2+j,0} &:= a_{q+2+j} \\
&= q^3 + jq + j + 1,
\end{aligned}$$

for $j, l \in [0, q-2]$. Let $\bar{c}_{j,l}$ be the remainder when $c_{j,l}$ is divided by $a_1 = q^2$. Then, for $j, l \in [0, q-2]$,

$$\begin{aligned}
\bar{c}_{2,l} &= (l+1)q, \\
\bar{c}_{3+j,l} &= \begin{cases} (j+l+1)q + j + 1 & \text{if } j + l \in [0, q-2], \\ (j+l+1-q)q + j + 1 & \text{if } j + l \in [q, 2q-4], \end{cases} \\
\bar{c}_{q+2+j,0} &= jq + j + 1,
\end{aligned}$$

$\bar{c}_{j,l}$'s are distinct each other, and their number is $q^2 - 1$. Hence, for any $i \in [1, a_1 - 1]$ there is a unique $\bar{c}_{j,l}$ such that $i = \bar{c}_{j,l}$. Therefore, there is a unique $c_{j,l}$ such that $b_i \le c_{j,l}$ and $c_{j,l} \equiv i \bmod a_1$ by the definition of b_i (5.5). Since $g(A_3) = \sum_{i=1}^{a_1-1} \lfloor b_i / a_1 \rfloor$,

$$\begin{aligned}
g &= q^3 - 2q + 1 \\
&\le \sum_{i=1}^{a_1-1} \left\lfloor \frac{b_i}{a_1} \right\rfloor \\
&\le \sum_{l=0}^{q-2} \left\lfloor \frac{c_{2,l}}{a_1} \right\rfloor + \sum_{l=0}^{q-2} \sum_{j=0}^{q-2} \left\lfloor \frac{c_{3+j,l}}{a_1} \right\rfloor + \sum_{j=0}^{q-2} \left\lfloor \frac{c_{q+2+j,0}}{a_1} \right\rfloor \\
&= \sum_{l=0}^{q-2} (l+1) + \sum_{j+l \le q-2} (j+l+2) + \sum_{j+l \ge q-1} (j+l+3) + \sum_{j=0}^{q-2} q \\
&= \sum_{l=0}^{q-2} l + \sum_{l=0}^{q-2} \sum_{j=0}^{q-2} (j+l+2) + \sum_{j+l \ge q-1} 1 + q^2 - 1 \\
&= \sum_{l=0}^{q-2} l + \frac{1}{2}(q-1) \sum_{l=0}^{q-2} (2l+q+2) + \sum_{l=0}^{q-2} l + q^2 - 1 \\
&= \frac{1}{2}(q+1)(q-1)(q-2) + \frac{1}{2}(q-1)^2(q+2) + q^2 - 1 \\
&= q^3 - 2q + 1.
\end{aligned}$$

Hence, $g = g(A_3)$. Consequently, $K_\infty(P_\infty) = \mathbb{F}_q[y_1,\ y_2,\ \cdots,\ y_{2q}]$ and the semigroup of nongaps at P_∞ is generated by S_{A_3}.

(Part 2) S_{A_3} is minimal.

We show that S_{A_3} satisfies the definition of minimal set given in Section 5.1.2.

Since $a_1 = \min S_{A_3}$, $a_2 = \min\{S_{A_3} \setminus \{a_1\}\}$, and a_2 is not multiple of a_1, a_1 and a_2 are included in the minimal set of generators of $\langle S_{A_3} \rangle$.

Now, we show that $a_{3+j} \notin \langle S_{A_3} \setminus \{a_{3+j}\} \rangle$ for any $j \in [0, q-2]$. Since (5.10) and $a_{q+1} < a_1 + a_{q+2+l}$ for any $l \in [0, q-2]$, it is enough to show $a_{3+j} \notin \langle a_1, a_2, \cdots, a_{2+j} \rangle$. Assume that for any $j \in [0, q-2]$ there are nonnegative integers $u_1, u_2, \cdots, u_{2+j}$ such that $a_{3+j} = \sum_{i=1}^{2+j} u_i a_i$. We can expand above equation as

$$\left.\begin{aligned} \text{(left-hand)} &= (j+2)q^2 + (j+1)q + j + 1, \\ \text{(right-hand)} &= v_2 q^2 + v_1 q + v_0 \\ &= w_2 q^2 + w_1 q + w_0, \end{aligned}\right\} \tag{5.11}$$

where $v_2 := u_1 + u_2 + \sum_{i=3}^{2+j}(i-1)u_i$, $v_1 := u_2 + \sum_{i=3}^{2+j}(i-2)u_i$ and $v_0 := \sum_{i=3}^{2+j}(i-2)u_i$, and choose w_2, w_1 and w_0 such that $w_0, w_1 \in [0, q-1]$. We separate into the following two cases.

- Case 1. $v_1 \geq q$.

  Then, w_2 is greater than q since $v_2 \geq v_1$. Since $j+2$ is at most q, this is a contradiction.

- Case 2. $v_1 < q$.

  Then, w_2, w_1 and w_0 are equal to v_2, v_1 and v_0, respectively since $v_1 \geq v_0$. By assumption (5.11), $w_2 - w_0$ is equal to 1, i.e. $u_1 + u_2 + \cdots + u_{2+j} = 1$. This is a contradiction.

Hence, $a_{3+j} \notin \langle a_1, a_2, \cdots, a_{2+j} \rangle$ for any $j \in [0, q-2]$.

Finally, we show that $a_{q+2+j} \notin \langle S_{A_3} \setminus \{a_{q+2+j}\} \rangle$ for any $j \in [0, q-2]$. Since (5.10) and $a_{q+2+l} < a_1 + a_{q+2}$ for any $l \in [0, q-2]$, it is enough to show $a_{q+2+j} \notin \langle a_1, a_2, \cdots, a_q \rangle$. This can be shown in a similar manner as the proof of $a_{3+j} \notin \langle S_{A_3} \setminus \{a_{3+j}\} \rangle$ for $j \in [0, q-2]$.

As a consequence of these results, S_{A_3} is the minimal set of generators of $\langle S_{A_3} \rangle$. (Q.E.D.)

For $M = (m_1, m_2, \cdots, m_{2q}) \in \mathbb{N}_0^{2q}$, we denote $y_1^{m_1} y_2^{m_2} \cdots y_{2q}^{m_{2q}}$ by y^M. From Theorem 5.2.1, we have $l(mP_\infty) = |\langle S_{A_3} \rangle \cap [0, m]|$, and a $\mathbb{F}_{q^2}$-basis of monomial type for $L(mP_\infty)$ can be given by

$$\{y^{M_{A_3}(a)} \in F_3 \,|\, a \in \langle S_{A_3} \rangle \cap [0, m]\}, \tag{5.12}$$

where M_{A_3} is defined by (5.6).

Remark 5.2.1. The $\mathbb{F}_{q^2}$-basis given by (5.12) depends on the order of $a_1, a_2, \cdots, a_{2q}$. On the other hand, the codes constructed in Section 5.2.2 do not depend on the order $a_1, a_2, \cdots, a_{2q}$. Therefore, we only consider the order indicated in Theorem 5.2.1 for convenience. However, in case of practical use, the order of $a_1, a_2, \cdots, a_{2q}$ should be considered. □

5.2.2 A Generator Matrix of $C_L(D, mP_\infty)$

For the divisor

$$D := \sum_{P \in \mathbb{P}^1_{F_3} \setminus \{P_\infty\}} P,$$

Voss and Høholdt [69] considered algebraic geometric codes of type $C_L(D - E_0, lE_0 + mP_\infty)$ for appropriate $l, m \in \mathbb{N}_0$. In this chapter, we consider one-point codes of type $C_L(D, mP_\infty)$ for any $m \in \mathbb{Z}$. Obviously, the length of our codes is longer than that of codes considered by Voss and Høholdt. Let us denote the length and the dimension of $C_L(D, mP_\infty)$ by $n := |supp(D)| = N - 1$ and $k := \dim C_L(D, mP_\infty)$, respectively.

First, we show how to evaluate $f(P) \in \mathbb{F}_{q^2}$ for any $f \in K_\infty(P_\infty)$ and $P \in \mathbb{P}^1_{F_3} \setminus \{P_\infty\}$. For this purpose, we change the viewpoint from algebraic function fields to algebraic geometry by using Theorem 5.2.1. As for main properties of this change of viewpoint, please refer to [44].

Let $\overline{\mathbb{F}}_{q^2}$ be the algebraic closure of $\mathbb{F}_{q^2}$. Let $\mathbb{A}^{2q}(\mathbb{F}_{q^2})$ and $\mathbb{A}^{2q}(\overline{\mathbb{F}}_{q^2})$ be $2q$-dimensional affine space over $\mathbb{F}_{q^2}$ and $\overline{\mathbb{F}}_{q^2}$ respectively, and $\mathbb{F}_{q^2}[Y_1, Y_2, \cdots, Y_{2q}]$ the polynomial ring in $2q$ variables over $\mathbb{F}_{q^2}$. Consider the homomorphism

$$\mathbb{F}_{q^2}[Y_1, Y_2, \cdots, Y_{2q}] \to \mathbb{F}_{q^2}[y_1, y_2, \cdots, y_{2q}]$$

given by putting y_i into Y_i for every $i \in [1, 2q]$, and denote the kernel of this homomorphism by I. Define the algebraic set

$$V := \{Q \in \mathbb{A}^{2q}(\overline{\mathbb{F}}_{q^2}) \mid F(Q) = 0 \text{ for all } F \in I\}$$

where Q is a point in $\mathbb{A}^{2q}(\overline{\mathbb{F}}_{q^2})$, and denote the set of $\mathbb{F}_{q^2}$-rational points of V by $V(\mathbb{F}_{q^2}) := V \cap \mathbb{A}^{2q}(\mathbb{F}_{q^2})$. Consider the mapping

$$\Phi : \mathbb{P}^1_{F_3} \setminus \{P_\infty\} \to \mathbb{A}^{2q}(\mathbb{F}_{q^2})$$

given by $\Phi(P) := (y_1(P), y_2(P), \cdots, y_{2q}(P))$. Then, $\Phi(P) \in V(\mathbb{F}_{q^2})$ for all $P \in \mathbb{P}^1_{F_3} \setminus \{P_\infty\}$, since

$$F(\Phi(P)) = F(y_1, y_2, \cdots, y_{2q})(P) = 0$$

for any $F \in I$ [44]. Furthermore, since $K_\infty(P_\infty) = \mathbb{F}_{q^2}[y_1, y_2, \cdots, y_{2q}]$, V is an affine, nonsingular, absolutely irreducible curve over $\mathbb{F}_{q^2}$ which has only a point in the hyperplane at infinity, and the mapping Φ from $\mathbb{P}^1_{F_3}$ to $V(\mathbb{F}_{q^2})$ is bijective [44]. If $P_{\alpha\beta\gamma} \in \mathbb{P}^1_{F_3}$ is of Type 1 and Type 3 in Section 5.1.3, we can evaluate $\Phi(P_{\alpha\beta\gamma})$ by replacing x_1, z_2, and z_3 with α, β, and γ respectively. As for $P_{0\beta*}$ of Type 2, since $(y_i) \geq E_0$ for any $i \in [3, 2q]$, we obtain $\Phi(P_{0\beta*}) = (0, \beta, 0, \cdots, 0)$. Hence, we explicitly have all points of $V(\mathbb{F}_{q^2})$.

Let P be a rational place of $F_3/\mathbb{F}_{q^2}$ except P_∞, and let $\Phi(P) = Q = (\alpha_1, \alpha_2, \cdots, \alpha_{2q})$. For any $f = f(y_1, y_2, \cdots, y_{2q}) \in K_\infty(P_\infty)$, we can evaluate $f(P) \in \mathbb{F}_{q^2}$ by replacing y_i with α_i for every $i \in [1, 2q]$, i.e. $f(P) = f(\alpha_1, \alpha_2, \cdots, \alpha_{2q})$. Thus we can calculate $f(P)$ for any $f \in K_\infty(P_\infty)$ and $P \in \mathbb{P}^1_{F_3} \setminus \{P_\infty\}$. Hereafter, we describe $f(P)$ by $f(\Phi(P))$.

When $m < n$, we can show generator matrices of $C_L(D, mP_\infty)$ since the mapping ev_D is injective. In order to obtain a generator matrix of $C_L(D, mP_\infty)$ for any $m \in \mathbb{Z}$, the set S_{P_∞} is defined by

$$S_{P_\infty} := \{m \in \mathbb{Z} \,|\, \dim C_L(D, mP_\infty) = \dim C_L(D, (m-1)P_\infty) + 1\}. \tag{5.13}$$

Then, by using Theorem 5.2.1, we obtain the following theorem.

Theorem 5.2.2. *S_{P_∞} can be described by using the semigroup $\langle S_{A_3}\rangle$ as follows:*

$$S_{P_\infty} = \langle S_{A_3}\rangle \setminus \bigcup_{i=0}^{q-1} \{q^4 + i(q^2+q+1) + \langle S_{A_3}\rangle\} \subset [0, n+2g-1]. \tag{5.14}$$

□

Proof. First, we prepare some new definitions. An integer m is called $(-D)$-nongap at P_∞ if $l(mP_\infty - D) = l((m-1)P_\infty - D) + 1$. Otherwise, m is called $(-D)$-gap at P_∞. Let S be the set of $(-D)$-nongaps at P_∞. Since the kernel of the mapping ev_D from $L(mP_\infty)$ to $\mathbb{F}^n_{q^2}$ is $L(mP_\infty - D)$, we obtain $S_{P_\infty} = \langle S_{A_3}\rangle \setminus S$. Hence, it is enough to show $S = \bigcup_{i=0}^{q-1}\{q^4 + i(q^2+q+1) + \langle S_{A_3}\rangle\}$.

Consider an element $x := x_1^{q^2} - x_1$. Since $(x) = D + (q-1)E_0 - q^4 P_\infty$, $(xx_1^i z_3^i)_0 \geq D$ and $(xx_1^i z_3^i)_\infty = (q^4 + i(q^2+q+1))P_\infty$ hold for any $i \in [0, q-1]$, where $(f)_0$ and $(f)_\infty$ are the zero and pole divisor of f respectively. That is, $q^4 + i(q^2+q+1) \in S$ for any $i \in [0, q-1]$. Moreover, if $f \in L(mP_\infty)$, then $fxx_1^i z_3^i \in L((m + q^4 + i(q^2+q+1))P_\infty - D)$ for any $i \in [0, q-1]$. Consequently, $S \supseteq \bigcup_{i=0}^{q-1}\{q^4 + i(q^2+q+1) + \langle S_{A_3}\rangle\}$ holds.

Lastly, since S has g $(-D)$-nongaps in $n + \mathbb{N}_0$, we can show $|\mathbb{N}_0 \setminus \bigcup_{i=0}^{q-1}\{i(q^2 + q+1) + \langle S_{A_3}\rangle\}| = q^3 - q^2 (= g - (n - q^4))$ in a similar manner as the proof of Theorem 5.2.1. (Q.E.D.)

Let $Q_1, Q_2, \cdots, Q_n$ be n distinct points in $V(\mathbb{F}_{q^2})$, and $(\rho_i \,|\, i \in [1, n])$ a sequence in order of increasing in S_{P_∞}. The dimension k of $C_L(D, mP_\infty)$ is $\max\{i \in [1, n] \,|\, \rho_i \in [0, m]\}$, and a generator matrix of $C_L(D, mP_\infty)$ is obtained as

$$\begin{bmatrix} y^{M_1}(Q_1) & y^{M_1}(Q_2) & \cdots & y^{M_1}(Q_n) \\ y^{M_2}(Q_1) & y^{M_2}(Q_2) & \cdots & y^{M_2}(Q_n) \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots \\ y^{M_k}(Q_1) & y^{M_k}(Q_2) & \cdots & y^{M_k}(Q_n) \end{bmatrix}, \tag{5.15}$$

where $M_i := M_{A_3}(\rho_i)$ for every $i \in [0, n]$. The Matrix (5.15) is also a parity check matrix of $C_\Omega(D, mP_\infty)$ with redundancy k.

The decoding complexity of one-point codes $C_\Omega(D, mP_\infty)$ increases as the number of generators of semigroup of nongaps increases. Since we minimize the number of generators in Theorem 5.2.1, we optimize the decoding complexity from the viewpoint of the number of generators.

Remark 5.2.2. In [69], Voss and Høholdt have shown that a code $C_L(D - E_0, lE_0 + mP_\infty)$ is identical with $C_\Omega(D - E_0, l'E_0 + m'P_\infty)$ for appropriate $l', m' \in \mathbb{N}_0$. Hence, both generator and parity check matrix can be obtained explicitly. Similarly, we can pose a problem if there exist $m, m' \in \mathbb{Z}$ such that

$$C_L(D, mP_\infty) = C_\Omega(D, m'P_\infty).$$

Unfortunately, there do not exist such integers m, m' in general. Hence, the parity check matrix of $C_L(D, mP_\infty)$ can not be obtained by using Matrix (5.15). □

Example 5.2.1. The number of rational places of $F_3/\mathbb{F}_4$ is 16 and the genus of $F_3/\mathbb{F}_4$ is 5. By using Theorem 5.2.1, we obtain $A_3 = (4, 6, 11, 9)$ and $K_\infty(P_\infty) = \mathbb{F}_{q^2}[y_1, y_2, y_3, y_4]$ where $y_1 = x_1$, $y_2 = z_2$, $y_3 = x_1^2 z_3$ and $y_4 = (z_2 + 1)z_3$. Hence, y^{M_i}'s are given by

$$\begin{array}{lllll} y^{M_1} = 1, & y^{M_2} = y_1, & y^{M_3} = y_2, & y^{M_4} = y_1^2, & y^{M_5} = y_4, \\ y^{M_6} = y_1y_2, & y^{M_7} = y_3, & y^{M_8} = y_1^3, & y^{M_9} = y_1y_4, & y^{M_{10}} = y_1^2y_2, \\ y^{M_{11}} = y_1y_3, & y^{M_{12}} = y_1^2y_4, & y^{M_{13}} = y_1^3y_2, & y^{M_{14}} = y_1^2y_3, & y^{M_{15}} = y_1^3y_4. \end{array}$$

On the other hand, all points in $V(\mathbb{F}_{q^2})$ are given by

$$\begin{array}{lll} Q_1 = (0,0,0,0), & Q_2 = (0,0,0,1), & Q_3 = (0,1,0,0), \\ Q_4 = (1,\alpha,\alpha,1), & Q_5 = (1,\alpha,\alpha^2,\alpha), & Q_6 = (1,\alpha^2,\alpha,\alpha^2), \\ Q_7 = (1,\alpha^2,\alpha^2,1), & Q_8 = (\alpha,\alpha,1,1), & Q_9 = (\alpha,\alpha,\alpha,\alpha), \\ Q_{10} = (\alpha,\alpha^2,1,\alpha^2), & Q_{11} = (\alpha,\alpha^2,\alpha,1), & Q_{12} = (\alpha^2,\alpha,\alpha^2,1), \\ Q_{13} = (\alpha^2,\alpha,1,\alpha), & Q_{14} = (\alpha^2,\alpha^2,\alpha^2,\alpha^2), & Q_{15} = (\alpha^2,\alpha^2,1,1). \end{array}$$

where α is a primitive element of $\mathbb{F}_4$. From these descriptions of monomials and $\mathbb{F}_4$-rational points, a generator matrix of $C_L(D, mP_\infty)$ (or a parity check matrix of $C_\Omega(D, mP_\infty)$) can be completely described for any $m \in \mathbb{Z}$.

In Table 5.1, for the redundancy r, we evaluate the Goppa designed distance $d_G(= m - 2g + 2)$ and the Feng-Rao designed distance d_{FR} of $C_\Omega(D, mP_\infty)$ obtained by our construction. For comparison, Table 5.1 also includes the Feng-Rao

Table 5.1: The Feng-Rao designed distance over $\mathbb{F}_4$.

r	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
d_G	-	-	-	-	0	1	2	3	4	5	6	8	9	10	12	-
d_{FR}	1	2	2	2	2	2	2	4	4	6	6	8	9	10	12	-
d^*_{FR}	1	2	2	2	2	3	4	4	5	6	6	8	9	10	12	-

designed distance d^*_{FR} of improved geometric Goppa codes [12] for $C_\Omega(D, mP_\infty)$. Obviously, improved geometric Goppa codes for $C_\Omega(D, mP_\infty)$ are superior to original codes $C_\Omega(D, mP_\infty)$ for some redundancy r with respect to the Feng-Rao designed distance. However, the Feng-Rao designed distance d^*_{FR} is not superior to the designed distance of some BCH codes with length 15 for any dimension.

□

5.2.3 A Comparison with BCH Codes

In this subsection, we compare one-point codes from $F_3/\mathbb{F}_{q^2}$ with BCH codes over $\mathbb{F}_{q^2}$. Let α be a primitive element of $\mathbb{F}_{q^4}$. A BCH code C_d over $\mathbb{F}_{q^2}$ is defined by a code with parity check matrix

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha & \cdots & \alpha^{q^4-2} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha^{d-2} & \cdots & \alpha^{(q^4-2)(d-2)} \end{bmatrix}. \tag{5.16}$$

Then, the length and the minimum distance of C_d are $q^4 - 1$ and at most d, respectively. Here, this lower bound for minimum distance is called the BCH designed distance or the BCH bound for C_d.

We take up the case of $q = 8$, that is, the finite field volume is 64. The number of rational places of the third function fields $F_3/\mathbb{F}_{64}$ is 4048. The genus of $F_3/\mathbb{F}_{64}$ is 497. At this time, the length of an one-point code $C_\Omega(D, mP_\infty)$ is 4047. On the other hand, the length of a BCH code C_d is 4095. The difference between both the length is 48.

In Figure 5.1, we compare the Feng-Rao bound of one point codes with the BCH bound of BCH codes for any redundancy in the region [2650,3350]. As shown in Figure 5.1, one-point codes are better than BCH codes in this region. For example, an one-point code have the parameter $[4047, 1047, 2504]$ whereas the corresponding shorten BCH code have the parameter $[4047, 1047, 1980]$. The difference between both the designed distance is 524. At this time, this one-point code can be decoded up to more 261 errors than the corresponding shorten BCH code.

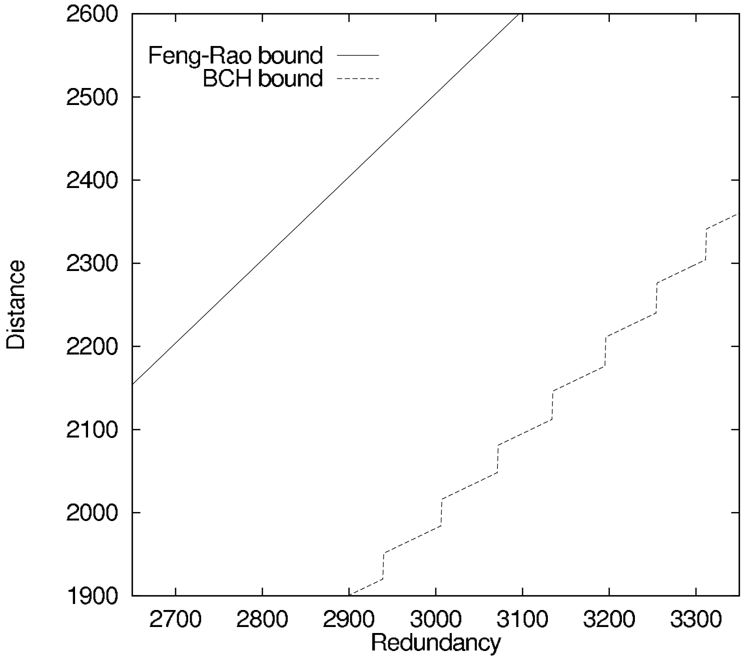


Figure 5.1: The comparison between Feng-Rao and BCH bounds over $\mathbb{F}_{64}$.

5.3 Conclusion

In this chapter, we have presented an explicit description of one-point codes from the third function field $F_3/\mathbb{F}_{q^2}$ on Garcia-Stichtenoth's tower by using Miura's method. In order to obtain such a description, we have firstly clarified a basis of $L(mP_\infty)$ over $\mathbb{F}_{q^2}$ whose elements can be represented by monomials in $2q$ rational functions. Further, we have shown that this number $2q$ is minimal. This fact is connected with an optimization of decoding complexity for one-point codes. Also, we have given an explicit description of all rational places of the third function field $F_3/\mathbb{F}_{q^2}$, and hence determined all $\mathbb{F}_{q^2}$-rational points in the curve corresponding the third function field $F_3/\mathbb{F}_{q^2}$. These have led us an explicit description of one-point codes from the third function field $F_3/\mathbb{F}_{q^2}$. Furthermore, we have compared the designed distance of the proposed codes with that of the BCH codes in the case of the finite field $\mathbb{F}_{64}$, and have provided many new better codes than the conventional algebraic codes. For example, an one-point code has had the parameter $[4047, 1047, 2504]$ whereas the corresponding BCH code has had the parameter $[4047, 1047, 1980]$. At this time, this one-point code can be decoded up to more 261 errors than the corresponding BCH codes. We have summarized several advantages of the proposed codes as follows:

(1) The fast implementation of the decoding algorithm up to half the Feng-Rao designed distance can be applied to the proposed codes.

(2) The decoding complexity of the proposed codes from the viewpoint of the number of generators has been optimal.

(3) The length of the proposed codes has been longer than that of codes suggested by Voss and Høholdt, as we have preserved the redundancy and the Feng-Rao designed distance.

As future researches, we have considered the following:

(a) Construct a sequence of one-point codes from the tower of algebraic function fields $(F_i \,|\, i \geq 4)$.

(b) Estimate the Feng-Rao designed distance of its code sequence asymptotically.

Chapter 6

Concluding Remarks

The generalization of construction and decoding from the codes on algebraic curves to arbitrary linear codes has yielded an optimization problem for the Feng-Rao designed distance. This dissertation has dealt with the design and optimization of linear codes with Feng-Rao designed distance in compliance with their construction methods.

In Chapter 3, we have shown that the Feng-Rao designed distance of linear codes depends on subspace sequence. Also, we have provided a representative for all ordered bases generated by any subspace sequence. This representative can be constructed for any ordered basis by using the Gaussian elimination only with elementary row operation. Next, we have shown that under the column permutation of any ordered basis, the Feng-Rao designed distance is invariant for any redundancy. Then, the ordered bases can be restricted to the ordered bases in standard normal form. In particular, any ordered basis can be put in standard normal form as its Feng-Rao designed distance was kept by using the Gaussian elimination only with elementary row operation and column permutation. Finally, we have presented the following algorithm: The input to the algorithm is any ordered basis. The output to the algorithm is the ordered basis in standard normal form whose first vector entries are all one. Then, the Feng-Rao designed distance for the input ordered basis has been larger than or equal to that for the output ordered basis for any redundancy. As a consequence of these, ordered bases can be restricted to the ordered bases in standard normal form whose first vector entries are all one.

In Chapter 4, we have shown an optimization problem of monomial orders for the Feng-Rao designed distance of the codes on the Hermitian curve. Firstly, we have presented explicit descriptions of the Hermitian codes for any monomial order. Also, we have shown that any the monomial basis can be represented by a monomial basis associated with some weight order. Based on these results, we have shown the relation between both the linear codes on the Hermitian curve by Goppa's and Miura's construction. As for the Hermitian curve, Goppa's construction has included in Miura's construction method. Next, we have shown sufficient conditions not to have well-behaving pairs by using the exponents of monomials. Furthermore, we have shown necessary conditions and sufficient conditions to have well-behaving pairs by using the weight order. Then, by using their relation, we have clarified a class of optimal monomial orders for linear codes on the Hermitian curve. Also, we have illustrated an example the case that finite field volume is 16.

In Chapter 5, we have presented an explicit and complete description of one-point codes from the third function field on Garcia-Stichtenoth's tower by using Miura's method. In order to obtain such a description, we have first clarified a basis whose elements can be represented by monomials in several rational functions. Furthermore, we have shown that the number of generators of nongaps is minimal. This fact is connected with an optimization of decoding complexity for one-point codes. Also, we have given an explicit description of all rational places of the third function field, and hence determined all rational points in the curve corresponding the third function field. These results have led us an explicit description of one-point codes from the third function field. Furthermore, we have compared the designed distance of the proposed codes with that of the BCH codes in the case that finite field size is 64 and have provided many new better codes than the conventional algebraic codes. For example, an one-point code has the parameter $[4047, 1047, 2504]$ whereas the corresponding BCH code has the parameter $[4047, 1047, 1980]$. At this time, this one-point code can be decoded up to more 261 errors than the corresponding BCH codes. Finally, we have summarized several advantages of the proposed codes as follows: (1) The fast implementation of the decoding algorithm up to half the Feng-Rao designed distance can be applied to the proposed codes. (2) The decoding complexity of the proposed codes from the viewpoint of the number of generators is optimal. (3) The length of the proposed codes is longer than that of codes suggested by Voss and Høholdt, preserving the redundancy and the Feng-Rao designed distance. As future researches, we shall consider providing explicit descriptions of one-point codes from other algebraic function fields on the Garcia-Stichtenoth's tower and estimating their Feng-Rao designed distance.

Bibliography

[1] T. Becker and V. Weispfenning, *Gröbner bases: a computational approach to commutative algebra* (Graduate Texts in Mathematics, vol. 141). Springer-Verlag, 1993.

[2] E. R. Berlekamp, "Long primitive binary BCH codes have distance $d \sim \ln R^{-1}/\log n \cdots$," *IEEE Transactions on Information Theory*, vol. IT-18, no. 3, May 1972.

[3] E. R. Berlekamp, *Algebraic coding theory.* Revised 1984 Edition, Aegean Park Press, 1984.

[4] R. E. Blahut, *Theory and practice of error control codes*, Addison-Wesley, 1983.

[5] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Information and Control*, vol. 3, pp. 68–79, March 1960.

[6] B. Buchberger, "Gröbner bases: An algorithmic method in polynomial ideal theory," in *Multidimensional Systems Theory: Progress, Directions and Open Problems in Multidimensional Systems*, (N. K. Bose, ed.), Reidel, 1985.

[7] D. Cox, J. Little and D. O'Shea, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra* (Undergraduate Texts in Mathematics). Second Edition, UTM, Springer, 1996.

[8] I. M. Duursma, "Majority coset decoding," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 1067–1070, May 1993.

[9] G. L. Fend and T. R. N. Rao, "Decoding algebraic-geometric codes up to the designed minimum distance," *IEEE Transactions on Information Theory*, vol. 39, no. 1, pp. 37–45, January 1993.

[10] G. L. Feng and T. R. N. Rao, "A class of algebraic geometric codes from curves in high-dimensional projective spaces," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, (G. Cohen, T. Mora, and O. Moreno, Eds.), Lecture Notes in Computer Science, vol. 673, Puerto Rico, Springer-Verlag, pp. 132–146, March 1993.

[11] G. L. Fend and T. R. N. Rao, "A simple approach for construction of algebraic-geometric codes from affine plane curves," *IEEE Transactions on Information Theory*, vol. 40, no. 4, pp. 1003–1012, July 1994.

[12] G. L. Feng and T. R. N. Rao, "Improved geometric Goppa codes - Part I: Basic theory," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1678-1693, November 1995.

[13] G. L. Feng, V. K. Wei, T. R. N. Rao and K. K. Tzeng, "Simplified understanding and efficient decoding of a class of algebraic-geometric codes," *IEEE Transactions on Information Theory*, vol. 40, no. 4, July 1994.

[14] A. Garcia and H. Stichtenoth, "A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound," *Inventiones Mathematicae*, vol. 121, pp. 211-222, 1995.

[15] A. Garcia and H. Stichtenoth, "On the asymptotic behaviour of some towers of function fields over finite fields," *Journal of Number Theory*, vol. 61, no. 2, 1996.

[16] V. D. Goppa, "A new class of linear error-correcting codes," *Problemy Peredachi Informatsii*, vol. 6, no. 3, pp. 24–30, July–September 1970. Translation: *Problems of Information Transmission*, vol. 6, no. 3, pp. 223–229, January 1971.

[17] V. D. Goppa, "A rational representation of codes and (L, g)-codes," *Problemy Peredachi Informatsii*, vol. 7, no. 3, pp. 41–49, July–September, 1971. Translation: *Problems of Information Transmission*, vol. 7, no. 3, pp. 223–229, January 1972.

[18] V. D. Goppa, "Codes associated with divisors," *Problemy Peredachi Informatsii*, vol. 13, no. 1, pp. 33–39, January–March 1977. Translation: *Problems of Information Transmission*, vol. 13, no. 1, pp. 22–26, July 1977.

[19] V. D. Goppa, "Codes on algebraic curves," *Doklady Akademii nauk SSSR*, vol. 46, pp. 1289–1290, 1981. Translation: *Soviet Mathematics Doklady*, vol. 24, pp. 170-172, 1981.

[20] V. D. Goppa, "Algebraico-geometric codes," *Izvestiia Akademii nauk SSSR*, vol. 46, 1982. Translation: *Mathematics of the USSR izvestiya*, vol. 21, pp. 75–91, 1983.

[21] V. D. Goppa, "Codes and information," *Russian Mathematical Surveys*, vol. 39, pp. 87–141, 1984.

[22] V. D. Goppa, *Geometry and codes* (Mathematics and its applications, vol. 24). Kluwer, 1991.

[23] G. Haché, "Construction effective des codes géométriques," Ph.D. dissertation, Institut National de Recherche en Informatique et en Automatique (INRIA), Paris, France, September 1996. (in French)

[24] R. W. Hamming, "Error detecting and error correcting codes," *Bell System Technical Journal*, vol. 29, pp. 147–160, April 1950.

[25] A. Hocquenghem, "Codes correcteurs d'erreurs," *Chiffres*, vol. 2, pp. 147–156, 1959. (in French)

[26] Y. Ihara, "Some remarks on the number of rational points of algebraic curves over finite fields," *Journal of the Faculty of Science*, the University of Tokyo, Sect. 1A, vol. 28, pp. 721–724, 1981.

[27] H. Imai, *Coding theory*, IEICE, 1990. (in Japanese)

[28] J. Justsen, K. J. Larsen, H. E. Jensen, A. Havemose and T. Høholdt, "Construction and decoding of a class of algebraic geometric codes," *IEEE Transactions on Information Theory*, vol. 35, no. 4, pp. 811–821.

[29] G. L. Katsman, M. A. Tsfasman and S. G. Vlăduţ, "Modular curves and codes with a polynomial construction," *IEEE Transactions on Information Theory*, vol. IT-30, no. 2, pp. 353–355, March 1984.

[30] C. Kirfel and R. Pellikaan, "The minimum distance of codes in an array coming from telescopic semigroups," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1720-1732, November 1995.

[31] W. W. Peterson and E. J. Weldon, Jr. *Error-correcting codes.* Second Edition, MIT Press, 1972.

[32] J. H. van Lint, *Introduction to coding theory* (Graduate Texts in Mathematics, vol. 86). Second Edition, Springer-Verlag, 1992.

[33] J. H. van Lint and G. van der Geer, *Introduction to coding theory and algebraic geometry* (DMV Seminar, vol. 12). Basel, Birkhäuser-Varlag, 1988.

[34] J. H. van Lint and T. A. Springer, "Generalized Reed-Solomon codes from algebraic geometry," *IEEE Transactions on Information Theory*, vol. IT-33, no. 3, pp. 305–309, May 1987.

[35] B. Lopéz, "Plane models of Drinfeld modular curves," Ph.D. dissertation, Complutense University, Madrid, Spain, March 1996.

[36] F. J. McWilliams and N. J. A. Sloane, *The theory of error-correcting codes* (North-Holland Mathematical Library, vol. 16). North-Holland, 1977.

[37] Yu. I. Manin, "What is the maximum number of points on a curve over $\mathbb{F}_2$?," *Journal of the Faculty of Science*, the University of Tokyo, Sect. 1A, vol. 28, pp. 715–720, 1981.

[38] R. Matsumoto, "Linear codes on nonsingular curves are better than those on singular curves," to appear in *IEICE Transactions on Fundamentals.*

[39] S. Miura, "Algebraic geometric codes on certain plane curves," *IEICE Transactions A*, vol. J75-A, no. 11, pp. 1735–1745, November 1992. (in Japanese)

[40] S. Miura, "On the minimum distance of codes from some maximal curves," *IEICE Technical Report*, IT92-147, March 1993.

[41] S. Miura, "On Feng-Rao designed minimum distance of geometric Goppa codes," in *Proceedings of the 16th Symposium on Information and Its Applications*, pp. 427–430, November 1993. (in Japanese)

[42] S. Miura, "Studies on error-correcting codes based on algebraic geometry," Ph.D. dissertation, University of Tokyo, Tokyo, Japan, 1997. (in Japanese)

[43] S. Miura, "Linear codes on affine algebraic varieties," *IEICE Transactions A*, vol. J81–A, no. 10, pp. 1386–1397, October 1998. (in Japanese)

[44] S. Miura, "Linear codes on affine algebraic curves," *IEICE Transactions A*, vol. J81–A, no. 10, pp. 1398–1421, October 1998. (in Japanese)

[45] C. J. Moreno, *Algebraic curves over finite fields* (Cambridge Tracts in Mathematics, vol. 97). Cambridge University Press, 1991.

[46] R. Pellikaan, "Asymptotically good sequences of curves and codes," in *Proceedings 34th Annual Allerton Conference on Communication, Control, and Computing*, Urbana-Champaign, pp. 276–285, October 1996.

[47] R. Pellikaan, "On the missing functions of a pyramid of curves," to appear in *Proceedings 35th Allerton Conference on Communication, Control, and Computing*, Urbana-Champaign, September 1997.

[48] R. Pellikaan, B. -Z. Shen and G. J. M. van Wee, "Which linear codes are algebraic-geometric?," *IEEE Transactions on Information Theory*, vol. 37, pp. 583–602, 1991.

[49] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, pp. 300–304, June 1960.

[50] L. Robbiano, "Term orderings on the polynomial ring," in European Conference on Computer Algebra, Linz, 1985, (B. F. Cabiness, ed.), Lecture Notes in Computer Science, vol. 204, Springer-Verlag, 1985.

[51] L. Robbiano, "On the theory of graded structures," *Journal of Symbolic Computation*, vol. 2, pp. 139–170, 1986.

[52] H. G. Rück and H. Stichtenoth, "A characterization of Hermitian function fields over finite fields," Journal fuer die Reine und Angewandte Mathematik, vol. 457, pp. 185–188, 1994.

[53] K. Saints and C. Heegard, "Algebraic-geometric codes and multidimensional cyclic codes: A unified theory and algorithms for decoding using Gröbner bases," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1733-1751, November 1995.

[54] S. Sakata, H. E. Jensen, and T. Høholdt, "Generalized Berlekamp-Massy decoding of algebraic-geometric codes up to half the Feng-Rao bound," *IEEE Transactions on Information Theory*, vol. 41, no. 6, November 1995.

[55] C. E. Shannon, "A mathematical theory of communications," *Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, July–October 1948.

[56] A. N. Skorobogatov and S. G. Vlăduţ, "On the decoding of algebraic-geometric codes," *IEEE Transactions on Information Theory*, vol. 36, no. 5, pp. 1051–1060, September 1990.

[57] H. Stichtenoth, "A note on Hermitian codes over GF(q^2)", *IEEE Transactions on Information Theory*, vol. 34, pp. 1345-1348, September 1988.

[58] H. Stichtenoth, *Algebraic function fields and codes*. Springer-Verlag, 1993.

[59] H. J. Tiersma, "Remarks on codes from Hermitian curves," *IEEE Transactions on Information Theory*, vol. IT-33, pp. 605-609, July 1987.

[60] M. A. Tsfasman, "Goppa codes that are better than the Varshamov-Gilbert bound," *Problemy Peredachi Informatsii*, vol. 18, no. 3, pp. 3–6, July–September 1982. Translation: *Problems of Information Transmission*, vol. 18, no. 3, pp. 163–166, January 1983.

[61] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-geometric codes*. Kluwer, 1991.

[62] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, "Modular curves, Shimura curves and Goppa codes, better than the Varshamov-Gilbert bound," *Mathematische Nachrichten*, vol. 109, pp. 21-28, 1982.

[63] D. Umehara, S. Miura, T. Uyematsu and E. Okamoto, "On optimality of Feng-Rao designed minimum distance for Hermitian codes constructed by weight order based on pole order," *IEICE Transactions A*, vol. J81-A, no. 4, pp. 733–742, January 1998. (in Japanese)

[64] D. Umehara and T. Uyematsu, “One-point algebraic geometric codes from Artin-Schreier extensions of Hermitian function fields,” *IEICE Transactions on Fundamentals*, vol. E81-A, no. 10, pp. 2025-2031, October 1998.

[65] D. Umehara, T. Uyematsu and K. Sakaniwa, “On the relation between the sequence of subspaces and the Feng-Rao designed minimum distance for geometric Goppa codes,” *IEICE Technical Report*, IT96-37, October 1996. (in Japanese)

[66] A. Vardy, “The intractability of computing the minimum distance of a code,” *IEEE Transactions on Information Theory*, vol. 43, no. 6, pp. 1757–1766, November, 1997.

[67] S. G. Vlăduţ, G. L. Katsman, and M. A. Tsfasman, “Modular curves and codes with polynomial complexity of construction,” *Problemy Peredachi Informatsii*, vol. 20, no. 1, pp. 47–55, January–March 1984. Translation: *Problems of Information Transmission*, vol. 20, no. 1, pp. 35–42, July 1984.

[68] S. G. Vlăduţ and Yu. I. Manin, “Linear codes and modular curves,” *Itogi Nauki i Tekhniki, Seriya Sovremennye Problemy Matematiki, Noveishie Dostizheniya*, vol. 25, pp. 209–257, 1984. Translation: *Journal of Soviet Mathematics*, vol. 30, pp. 2611–2643, 1985.

[69] C. Voss and T. Høholdt, “An explicit construction of a sequence of codes attaining the Tsfasman-Vlăduţ-Zink bound,” *IEEE Transactions on Information Theory*, vol. 43, no. 1, pp. 128-135, January 1997.

[70] K. Yamanishi, “On derivation of good codes based on elliptic codes and hyper-elliptic codes,” *IEICE Transactions A*, vol. J71-A, no. 10, pp. 1936–1946, October 1988. (in Japanese)

[71] K. Yamanishi, “On construction and performance evaluation of Fermat codes,” *IEICE Transactions A*, vol. J72-A, no. 3, pp. 597-607, March 1989. (in Japanese)

[72] K. Yang and P. V. Kumer, “On the true minimum distance of Hermitian codes,” in *Coding Theory and Algebraic Geometry*, Luminy, 1991, (H. Stichtenoth, M. A. Tsfasman eds.), Lecture Notes in Mathematics, vol. 1518, Springer-Verlag, pp. 99-107, 1992.

Author's Publications Related to the Dissertation

Regular papers

1. D. Umehara, S. Miura, T. Uyematsu and E. Okamoto, "On optimality of Feng-Rao designed minimum distance for Hermitian codes constructed by weight order based on pole order," *IEICE Transactions A*, vol. J81-A, no. 4, pp. 733–742, January 1998. (in Japanese)

2. D. Umehara and T. Uyematsu, "One-point algebraic geometric codes from Artin-Schreier extensions of Hermitian function fields," *IEICE Transactions on Fundamentals*, vol. E81-A, no. 10, pp. 2025-2031, October 1998.

International conferences

1. D. Umehara and T. Uyematsu, "One-point algebraic geometric codes from Artin-Schreier extensions of Hermitian function fields," in *Proceedings of International Symposium on Information Theory and Its Applications*, Mexico City, pp. 196-199, October 1998.

Domestic conferences and workshops

1. D. Umehara, S. Miura, T. Uyematsu and E. Okamoto, "On the optimum designed minimum distance of Hermitian codes based on monomial ordering," *IEICE Technical Report*, IT95-47, January 1996. (in Japanese)

2. D. Umehara, T. Uyematsu and K. Sakaniwa, "On the sequence of designed minimum distance for geometric Goppa codes," in *Proceedings of the 1996 IEICE general conference*, A-154, September 1996. (in Japanese)

3. D. Umehara, T. Uyematsu and K. Sakaniwa, "On the relation between the sequence of subspaces and the Feng-Rao designed minimum distance for

geometric Goppa codes," *IEICE Technical Report*, IT96-37, October 1996. (in Japanese)

4. D. Umehara and T. Uyematsu, "On codes from Artin-Schreier extensions of Hermitian function fields," in *Proceedings of the 20th Symposium on Information Theory and Its Applications*, vol. 1, pp. 153-156, December 1997.