論文 / 著書情報
Article / Book Information

題目(和文)	線形符号の限界とその代数幾何符号への応用
Title(English)	Bounds of Linear Codes and Their Applications to Algebraic Geometry Codes
著者(和文)	澁谷智治
Author(English)	TOMOHARU SHIBUYA
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:乙第3292号, 授与年月日:1999年3月31日, 学位の種別:論文博士, 審査員:
Citation(English)	Degree:Doctor of Engineering, Conferring organization: Tokyo Institute of Technology, Report number:乙第3292号, Conferred date:1999/3/31, Degree Type:Thesis doctor, Examiner:
学位種別(和文)	博士論文
Type(English)	Doctoral Thesis

Bounds of Linear Codes and Their Applications to Algebraic Geometry Codes

Tomoharu Shibuya

Department of Electrical and Electronic Engineering,
Tokyo Institute of Technology

December 1998

Acknowledgment

I think that it is too difficult to express in words my gratitude and appreciation to the many individuals who have helped and supported me.

I wish to express my deepest gratitude to professor Dr. Kohichi Sakaniwa in Tokyo Institute of Technology (TIT) for giving me an opportunity to start to study coding theory. I consider myself very fortunate to have pursued my studies under him, because my research style was established by his theoretical direction in my bachelor and master courses. I don't think I have been noticed the beauty of coding theory without his direction.

I also wish to express my gratitude to Dr. Tomohiko Uyematsu who is an associate professor in TIT. At the early days of my study, he showed me some current researches and direction of coding theory of those days. He also arranged many opportunity for me to present my researches to other researchers.

I also thank Dr. Hajime Jinushi who is an associate professor in Aoyama Gakuin university. When I started to study coding theory, we was a assistant professor of Sakaniwa lab. and taught me a lot of things about coding theory. Though I studied under him only for two years, his advice put my researches on a firm basis.

I also wish to express my gratitude towards Dr. Masaaki Homma who is a professor in Kanagawa University. In order to strengthen the mathematical basis of algebraic geometry codes, I asked him for his advice and we was willing to organize a seminar of algebraic geometry for us for these three years. I would also like to thank members of the seminar; Dr. Isao Yamada (TIT), Dr. Norihisa Shirota, Dr. Masayuki Hattori and Mr. Tatsuo Shinbashi (Sony), Mr. Seigo Arita and Mr. Norifumi Kamiya (NEC), Mr. Yoshinori Takei (TIT) and Ms. Makiko Kan and Ms. Motoko Suzuki (Ochanomizu University).

I would like to thank Dr. Shinji Miura at Sony Corporation who is also one of the member of the seminar. When I started to study algebraic geometry codes, we proposed me to start above seminar and introduced us to Dr. Homma. Moreover, many examples in

this dissertation are based on his deep research on AG codes on C_{ab}.

I would like to thank Mr. Daisuke Umehara and Mr. Ryutaroh Matsumoto who are Ph.D students in TIT. Because there are few staff who studies coding theory, they are precious colleagues whom I can discuss together. I also would like to thank Mr. Ryo Hasegawa at TIT and Mr. Jiro Mizutani at Chubu Electric Power Company who calculated some examples and gave many suggestion in my researches.

Contents

Chapter 1

General Introduction

The main goal of coding theory is to construct efficient error-correcting codes and for this purpose, a considerable number of researches has been done so far.

In 1981, Goppa introduced a new class of error-correcting codes, which originates from classical Goppa codes and is called *geometric Goppa codes* or *algebraic geometry* (AG) *codes* [7]. In 1982, Tsfasman showed a remarkable result [40] that there exist some AG codes which exceed Varshamov-Gilbert bound [17]. Subsequently, it has been shown that AG codes can be regarded as a natural generalization of Reed-Solomon codes and Reed-Muller codes, and arbitrary linear codes can be represented as AG codes [16, 30]. Since then, studies of AG codes have been much attractive.

Because of the difficult mathematical background, only a few good AG codes have been found besides ones on elliptic, hyper-elliptic and Hermitian curves. On the other hand, it is known that the problem of seeking good AG codes can be paraphrased, in some sense, into the problem of seeking algebraic curves with many rational points for given genus [19]. Thus it is a main problem to specify a class of algebraic curves which have many rational points. From an engineering point of view, it is also required to develop an explicit construction method of AG codes on a given algebraic curve. These two problems have been deeply investigated for a decade, and as a solution, Miura defined a class of algebraic curves called C_{ab} and gave explicit construction method of AG codes on C_{ab} [19]. C_{ab} is a very wide class of algebraic curves which contains not only conventional representative curves, i.e., elliptic, hyper-elliptic and Hermitian curves, but also other *maximal curves*, on which the number of rational points reaches the *Hasse-Weil-Serre* upper bound [38].

Actually a couple of good codes on C_{ab}, which have better parameters than BCH codes, have been discovered by computer search [19, 45, 46].

Though it is widely accepted that AG codes on C_{ab} yield many good linear codes, still it has not been clear that conditions under which AG codes on C_{ab} really have good parameters. This is an important problem to be solved if we intend to utilize AG codes in actual applications. So in this dissertation, we first compare the parameters of AG codes on C_{ab} with those of BCH codes, and draw a necessary condition for AG codes on C_{ab} to have better parameters than BCH codes. More precisely, we derive a boundary on the number of check symbols in terms of a, b (parameters which determine the essential part of the curve C_{ab}) and the genus of C_{ab}. Then, AG codes on C_{ab} with the number of check symbols beyond the boundary can be better than BCH codes. It is noted that this boundary on the number of check symbols is relatively small in general compared with code length. In other words, AG codes on C_{ab} which satisfy the condition include codes whose rate is high enough to be utilized in practical applications.

It is known that taking subfield subcodes is one of the most important approaches to obtain good codes. Representative examples are BCH codes (subfield subcodes of Reed-Solomon codes), classical Goppa codes and alternant codes (subfield subcodes of generalized Reed-Solomon codes). But it is also known that it is difficult in general to explicitly determine the parameters of subfield subcodes from the parameters of the original codes. Therefore, to develop methods to evaluate the parameters of subfield subcode is an important open problem. For this purpose, several authors have investigated how to estimate parameters of subfield subcodes [13, 43, 45, 46]. Stichtenoth [37] has given a general estimate for the dimension of subfield subcodes of arbitrary linear codes. By investigating Stichtenoth's approach in detail, we propose in this dissertation a tighter lower bound, denoted by k_{prop}, for the dimension of subfield subcodes of arbitrary linear codes.

Next, we restrict our discussion to subfield subcodes of AG codes on C_{ab}. The bound k_{prop} is rather good when the number of check symbols of original codes is relatively small, while unfortunately, it does not give a sufficiently good estimate when the number of check symbols is relatively large. On the other hand, we have shown in Chapter 3 of this dissertation that AG codes on C_{ab} can be good when the number of check symbols is relatively large. Thus in order to find good codes in subfield subcodes of AG codes on C_{ab}, it is considered effective to take AG codes on C_{ab} with relatively large number of

check symbols as original codes. By restricting the codes to AG codes on C_{ab}, we can improve the bound k_{prop} especially when the number of check symbols is relatively large. Moreover the improved bound for the dimension of subfield subcodes of AG codes on C_{ab} can be computed only from a, b and q (the order of the field over which subfield subcodes are defined) when the code length is given. Thus calculating the improved bound is much easier than calculating the true dimension from the parity check matrix by Gaussian elimination. We also show through a numerical example that the improved bound can exceed the true dimension of a shortened BCH code with the same code length and designed distance, while the Stichtenoth's bound cannot.

In the early 1990s, a new parameter of linear codes called *generalized Hamming weights* was introduced by Wei [42]. He clarified in his paper the relation between the generalized Hamming weights and a *wire-tap channel* problem in an area of security [44]. Subsequently, it was also shown that the generalized Hamming weights reflect a *trellis* or *state complexity* of linear codes [11, 12], which determines the complexity of maximum likelihood decoder employing trellis structures of linear codes. Moreover, the *Carlitz-Uchiyama* bound, which gives a lower bound for the minimum distance of the dual of binary BCH codes [17], was generalized to a bound for the generalized Hamming weights of trace codes [39].

For the applications of generalized Hamming weights mentioned above, it is important to evaluate the true generalized Hamming weights for given codes. However, it is not easy to evaluate the true weights except for some special codes such as Hamming codes, Reed-Muller codes and MDS (Maximum Distance Separable) codes. Thus bounds for the generalized Hamming weights have been investigated in many literatures [20, 27, 41, 47]. Recently in [8], a bound called *order bound* was introduced in a general setting of codes on algebraic varieties which includes the one-point AG codes.

In this dissertation, we introduce a new lower bound for the generalized Hamming weights of arbitrary linear codes in terms of a notion of well-behaving, which is known to act an essential role in the Feng-Rao decoding algorithm [3]. While the conventional bound requires some structures of the concerned $[n, k]$ code C, the proposed lower bound can be calculated only from a sequence of vectors, $B := \{\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_n\}$, which is a basis of F_q^n and whose first $n-k$ elements constitute the row vectors of parity check matrix of the code C. Next, we introduce a parameter $g(C)$, which is uniquely determined from the basis B, and show that the t-th generalized Hamming weight of C is equal to $n-k+t$ for

$g(C)+1 \leq t \leq k$. A code whose t-th generalized Hamming weight is equal to $n-k+t$ is said to be *t-th rank MDS* [42]. Thus we can say that any linear code is t-th rank MDS for $g(C)+1 \leq t \leq k$.

This dissertation is organized as follows. In Chapter 2, we briefly review AG codes, especially AG codes on $\boldsymbol{C}_{ab}$, and codes on affine algebraic varieties. We also give a couple of propositions needed in the following chapters. In Chapter 3, we compare the parameters of AG codes on $\boldsymbol{C}_{ab}$ with some shortened BCH codes. In Chapter 4, we propose a lower bound for the dimension of subfield subcodes which exceeds Stichtenoth's bound and improve the proposed bound for AG codes on $\boldsymbol{C}_{ab}$. In Chapter 5, we investigate a lower bound for the generalized Hamming weights of arbitrary linear codes. Finally in Chapter 6, we summarize the results obtained in this dissertation and list problems for further studies.

Chapter 2

AG Codes and Codes on Affine Algebraic Varieties

Throughout of this dissertation, we denote a finite field with q elements by F_q or simply F.

2.1 Algebraic geometry codes

We review the definition of AG codes [38].

Let $\mathbf{F}/F$ be an algebraic function field of genus g over a finite constant field F. Let $\{P_1, P_2, \ldots, P_n\}$ be a set of places of degree one in $\mathbf{F}/F$. Let G and D be divisors of $\mathbf{F}/F$ such that $D = P_1 + P_2 + \cdots + P_n$ and $Supp\,(D) \cap Supp\,(G) = \emptyset$. Define the vector space $L(G)$ as follows:

$$L(G) := \{f \in \mathbf{F} : (f) \geq -G \text{ or } f = 0\}, \tag{2.1}$$

where (f) is the principal divisor of f.

Consider the F-linear evaluation map ϕ by

$$\begin{aligned} \phi : L(G) &\to F^n \\ f &\mapsto (f(P_1), f(P_2), \ldots, f(P_n)). \end{aligned} \tag{2.2}$$

Then the algebraic geometry (AG) codes $\mathcal{C}_L(D, G)$ and $\mathcal{C}_\Omega(D, G)$ associated with two divisors D and G is defined by

$$\mathcal{C}_L(D, G) := \text{Image}(\phi) = \phi(L(G)), \;\; \mathcal{C}_\Omega(D, G) := \mathcal{C}_L(D, G)^\perp. \tag{2.3}$$

For a divisor A of $\mathbf{F}/F$, denote by $\dim A$ and $\deg A$ the dimension of $L(A)$ over F and the degree of A, respectively.

Proposition 2.1 [38] Let D and G be divisors of $\mathbf{F}/F$ defined above.

(i) $C_L(D,G)$ is an $[n,k,d]$ code with parameters

$$k = \dim G - \dim(G-D) \text{ and } d \geq n - \deg G.$$

(ii) $C_\Omega(D,G)$ is an $[n,k',d']$ code with parameters

$$k' = n - (\dim G - \dim(G-D)) \text{ and } d' \geq \deg G - (2g-2).$$

□

2.2 AG codes on C_{ab}

Definition 2.1 [10, 19] Let a and b be positive integers such that $a < b$ and $\gcd(a,b) = 1$. Then the defining polynomial of the curve C_{ab} is expressed as

$$\left.\begin{array}{c} h(x,y) = \alpha_{(b,0)}x^b + \alpha_{(0,a)}y^a + h'(x,y), \\ h'(x,y) = \sum_{\substack{0\leq i,j, \\ i+j\leq b, \\ ai+bj<ab}} \alpha_{(i,j)}x^i y^j, \\ \alpha_{(i,j)} \in F_q, \alpha_{(0,a)} \neq 0, \alpha_{(b,0)} \neq 0 \end{array}\right\} \quad (2.4)$$

where $h(x,y)$ is non-singular and absolutely irreducible. □

It is well known that the genus of C_{ab} is [19]

$$g = \frac{1}{2}(a-1)(b-1). \quad (2.5)$$

We denote by $\mathbf{F}(C_{ab})/F$ an algebraic function field $F(x,y)/F$ with $h(x,y) = 0$. Let Q be the common pole of x and y and $G := mQ$. Then a basis of $L(G)$ is given by the following proposition.

Proposition 2.2 [19] For $x^k y^\ell \in \mathbf{F}(C_{ab})/F$, let $\tau(x^k y^\ell) := ak + b\ell$. Then

$$\Gamma_{ab}(m) := \{x^k y^\ell : 0 \leq k, 0 \leq \ell \leq a-1, \tau(x^k y^\ell) \leq m\} \quad (2.6)$$

is a basis of $L(mQ)$. □

It is known that for $f = x^k y^\ell \in L(mQ)$, $\tau(f) = -v_Q(f)$ where v_Q is a *discrete valuation* [38] of $\mathbf{F}(\boldsymbol{C}_{ab})/F$ associated with the place Q.

Lemma 2.1 The code length n of $C_L(D, mQ)$ and $C_\Omega(D, mQ)$ on $\boldsymbol{C}_{ab}$ is less than q^2.

(Proof) It is known that there exists one-to-one correspondence between places of degree one in $\mathbf{F}(\boldsymbol{C}_{ab})/F$ and F-rational points of $\boldsymbol{C}_{ab}$[26]. By Eq.(2.4),

$$n = |\{(x, y) \in F^2 : h(x, y) = 0\}|.$$

Noting $\alpha^q = \alpha$ for all $\alpha \in F = GF(q)$, we can replace $h(x, y)$ by its *reduced* polynomial [15], which we denote by $\bar{h}(x, y)$. Since the degree of $\bar{h}(x, y)$ with respect to y is less than q, the number of roots of $\bar{h}(\alpha, y) = 0$ is less than q for all $\alpha \in F$, which implies $n < q^2$.

□

2.3 Codes on affine algebraic varieties

In this section, we denote by $R := F[X_1, X_2, \ldots, X_s]$ the polynomial ring R in s variables and by $\mathbf{N}_0 := \{0, 1, 2, \ldots, \}$ the set of non-negative integers.

2.3.1 Codes on affine algebraic varieties

Definition 2.2 [23, 24, 26] For a subset $V \subset F^s$, we denote by $I(V)$ the ideal of the polynomial ring R given by

$$I(V) := \{f \in R : f(P) = 0 \text{ for all } P \in V\}.$$

We also denote by $R(V)$ the *coordinate ring* of V defined by $R(V) := R/I(V)$. □

For $f \in R$ and $V = \{P_1, P_2, \ldots, P_n\}$ where $n := |V|$, let $\psi(f) := (f(P_1), f(P_2), \ldots, f(P_n))$. Then it is shown in [23, 24, 26] that the coordinate ring $R(V)$ and F^n are *isomorphic* as linear spaces over F and an isomorphism is given by the F-linear map $\overline{\psi} : R(V) \to F^n$ which is induced by ψ. For subspace L of $R(V)$, $\overline{\psi}(L)$ is called a code constructed on an affine algebraic variety V [23, 24, 26].

It is shown that in addition to the definition of codes on affine algebraic varieties, if a monomial order and a Gröbner basis are given, a non-trivial lower bound for its minimum distance can be derived as the Feng-Rao designed distance of the code. We review monomial orders and Gröbner basis in the next subsection.

2.3.2 Monomial orders and Gröbner bases

A *monomial* in R is a polynomial of the form

$$a_{(\alpha_1,\alpha_2,\ldots,\alpha_s)}X_1^{\alpha_1}X_2^{\alpha_2}\cdots X_s^{\alpha_s},\ \ a_{(\alpha_1,\alpha_2,\ldots,\alpha_s)}\neq 0.$$

For simplicity, we shall use the notation $a_{\boldsymbol{\alpha}}\boldsymbol{X}^{\boldsymbol{\alpha}}$ with $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\ldots,\alpha_s)\in \mathbf{N}_0^s$ to denote $a_{(\alpha_1,\alpha_2,\ldots,\alpha_s)}X_1^{\alpha_1}X_2^{\alpha_2}\cdots X_s^{\alpha_s}$.

Definition 2.3 [1] A *monomial order* on R is an order $\prec$ on $\mathbf{N}_0^s$, or equivalently an order on the set of monomials $\boldsymbol{X}^{\boldsymbol{\alpha}}$ $(\boldsymbol{\alpha}\in\mathbf{N}_0^s)$, satisfying:

(i) $\prec$ is a *well-order* on $\mathbf{N}_0^s$, that is, $\prec$ is a *total order* on $\mathbf{N}_0^s$ and every nonempty subset of $\mathbf{N}_0^s$ has the smallest element with respect to $\prec$.

(ii) If $\boldsymbol{\alpha}\prec\boldsymbol{\beta}$ and $\boldsymbol{\gamma}\in\mathbf{N}_0^s$, then $\boldsymbol{\alpha}+\boldsymbol{\gamma}\prec\boldsymbol{\beta}+\boldsymbol{\gamma}$ [1] .

□

We write $\boldsymbol{\alpha}\preceq\boldsymbol{\beta}$ if $\boldsymbol{\alpha}\prec\boldsymbol{\beta}$ or $\boldsymbol{\alpha}=\boldsymbol{\beta}$.

Definition 2.4 [1] Let $f=\sum_{\boldsymbol{\alpha}\in\mathbf{N}_0^s}a_{\boldsymbol{\alpha}}\boldsymbol{X}^{\boldsymbol{\alpha}}$ be a polynomial in $F[\boldsymbol{X}]$ and $\prec$ be a monomial order. Then the *multidegree* of f, denoted by $\mathrm{mdeg}(f)$, is defined by

$$\mathrm{mdeg}(f):=\begin{cases}-\boldsymbol{\infty}:=(-\infty,-\infty,\ldots,-\infty), & \text{if } f=0,\\ \max_{\prec}\{\boldsymbol{\alpha}\in\mathbf{N}_0^s : a_{\boldsymbol{\alpha}}\neq 0\}, & \text{if } f\neq 0\end{cases}$$

where the maximum is taken with respect to $\prec$. The *leading term* of f, denoted by $LT(f)$, is defined by

$$LT(f):=\begin{cases}0, & \text{if } f=0,\\ a_{\mathrm{mdeg}(f)}\boldsymbol{X}^{\mathrm{mdeg}(f)}, & \text{if } f\neq 0.\end{cases}$$

□

Proposition 2.3 [1] Let f,g be polynomials in R. Then:

(i) $\mathrm{mdeg}(fg)=\mathrm{mdeg}(f)+\mathrm{mdeg}(g)$.

(ii) $\mathrm{mdeg}(f+g)\preceq\max_{\prec}\{\mathrm{mdeg}(f),\mathrm{mdeg}(g)\}$, and equality holds if $\mathrm{mdeg}(f)\neq\mathrm{mdeg}(g)$.

---

[1] For $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\ldots,\alpha_s)$, $\boldsymbol{\beta}=(\beta_1,\beta_2,\ldots,\beta_s)\in\mathbf{N}_0^s$, $\boldsymbol{\alpha}+\boldsymbol{\beta}:=(\alpha_1+\beta_1,\alpha_2+\beta_2,\ldots,\alpha_s+\beta_s)$.

□

Definition 2.5 [1] Fix a monomial order on R. A finite subset $G = \{g_1, g_2, \ldots, g_\ell\}$ of an ideal I of R is said to be a *Gröbner basis* of I if

$$(LT(I)) = (LT(g_1), LT(g_2), \ldots, LT(g_\ell)),$$

where $(LT(I))$ and $(LT(g_1), LT(g_2), \ldots, LT(g_\ell))$ denote the ideals generated by $\{LT(f) : f \in I \setminus \{0\}\}$ and $\{LT(g_1), LT(g_2), \ldots, LT(g_\ell)\}$, respectively. □

It is known that the following propositions hold for Gröbner bases.

Proposition 2.4 [1] Let $G = \{g_1, g_2, \ldots, g_\ell\}$ be a Gröbner basis of an ideal I of R. Then for any $f \in F[\boldsymbol{X}]$, there exists a unique polynomial $\overline{f}^G \in R$ which satisfies the following two properties.

(i) $\overline{f}^G = 0$ or no term of $\overline{f}^G$ is divisible by $LT(g_i)$ $(1 \leq \forall i \leq \ell)$.

(ii) $f' := f - \overline{f}^G \in I$, i.e.,

$$f' = f - \overline{f}^G = \sum_{i=1}^{\ell} f_i g_i,\ f_i \in R,\ g_i \in G. \tag{2.7}$$

□

In Eq.(2.7), $\overline{f}^G$ is called *the remainder on division of f by G*, and denoted simply by $\overline{f}$ if there is no fear of confusion. By Proposition 2.4, we see that $\{\overline{f} : f \in R\}$ gives the representatives of all cosets of $R(V) := R/I(V)$. Thus, in what follows, we identify $R(V)$ with $\{\overline{f} : f \in R\}$ and use the F-linear map ψ for $\overline{\psi}$.

Definition 2.6 [23, 24, 26] For given $V \subset F^s$, define $\Lambda(V) \subset \mathbf{N}_0^s$ by

$$\Lambda(V) := \mathbf{N}_0^s \setminus \bigcup_{f \in I(V) \setminus \{0\}} \{\mathrm{mdeg}(f) + \mathbf{N}_0^s\} \tag{2.8}$$

where $\{\mathrm{mdeg}(f) + \mathbf{N}_0^s\} := \{\mathrm{mdeg}(f) + \boldsymbol{\alpha} : \boldsymbol{\alpha} \in \mathbf{N}_0^s\}$. □

Proposition 2.5 [23, 24, 26] Let $G = \{g_1, g_2, \ldots, g_\ell\}$ be a Gröbner basis of $I(V)$. Then:

(i) $\overline{\boldsymbol{X}^{\boldsymbol{\lambda}}}^G = \boldsymbol{X}^{\boldsymbol{\lambda}}$ for $\boldsymbol{\lambda} \in \Lambda(V)$.

(ii) $\{\boldsymbol{X}^{\boldsymbol{\lambda}} : \boldsymbol{\lambda} \in \Lambda(V)\}$ is a basis of $R(V)$.

(iii) $\Lambda(V) = \mathbf{N}_0^s \setminus \cup_{i=1}^{\ell} \{\mathrm{mdeg}(g_i) + \mathbf{N}_0^s\}$.

□

Since $|V| = n$ and $R(V)$ is an n-dimensional linear space over F, we have from Proposition 2.5-(ii) that

$$n = \dim R(V) = |\{\boldsymbol{X}^{\boldsymbol{\lambda}} : \boldsymbol{\lambda} \in \Lambda(V)\}| = |\Lambda(V)|.$$

Thus we may write $\Lambda(V)$ as

$$\Lambda(V) = \{\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \ldots, \boldsymbol{\lambda}_n\},\ \boldsymbol{\lambda}_i \prec \boldsymbol{\lambda}_{i+1}. \tag{2.9}$$

Then by Proposition 2.5-(ii) again, a basis of $R(V)$, denoted by $B(V)$ can be written as

$$B(V) := \{\boldsymbol{X}^{\boldsymbol{\lambda}_1}, \boldsymbol{X}^{\boldsymbol{\lambda}_2}, \ldots, \boldsymbol{X}^{\boldsymbol{\lambda}_n}\} =: \{f_1, f_2, \ldots, f_n\}. \tag{2.10}$$

Lemma 2.2 Notations as in Proposition 2.4 and Proposition 2.5. Let $f \in R$ be a monomial. Then:

(i) $\mathrm{mdeg}(\overline{f}) \preceq \mathrm{mdeg}(f)$.

(ii) $\mathrm{mdeg}(\overline{f}) \prec \mathrm{mdeg}(f)$ if $f' \neq 0$.

(iii) $\mathrm{mdeg}(\overline{f}) \prec \mathrm{mdeg}(f)$ if and only if $\mathrm{mdeg}(f) \notin \Lambda(V)$.

(Proof) (i) As is noted after Proposition 2.4, $\overline{f} \in R(V)$ and by using the basis $B(V)$ of $R(V)$ given in Eq.(2.10), $\overline{f}$ can be expressed as

$$\overline{f} = \sum_{\boldsymbol{\lambda}_j \in \Lambda(V)} a_{\boldsymbol{\lambda}_j} \boldsymbol{X}^{\boldsymbol{\lambda}_j},\ a_{\boldsymbol{\lambda}_j} \in F. \tag{2.11}$$

Therefore $\mathrm{mdeg}(\overline{f}) \in \Lambda(V)$.

If $f' = 0$, $f = \overline{f}$ and obviously $\mathrm{mdeg}(\overline{f}) \preceq \mathrm{mdeg}(f)$.

If $f' \neq 0$, there exists a term $f_i g_i$ in Eq.(2.7) such that $\mathrm{mdeg}(f') = \mathrm{mdeg}(f_i g_i)$ and we have from Proposition 2.3-(i) that $\mathrm{mdeg}(f') = \mathrm{mdeg}(f_i) + \mathrm{mdeg}(g_i)$, which implies $\mathrm{mdeg}(f') \notin \Lambda(V)$ by Proposition 2.5-(iii). Thus $\mathrm{mdeg}(f') \neq \mathrm{mdeg}(\overline{f})$ and we have from Proposition 2.3-(ii) that

$$\mathrm{mdeg}(f) = \max_{\prec}\{\mathrm{mdeg}(f'), \mathrm{mdeg}(\overline{f})\}. \tag{2.12}$$

Therefore $\mathrm{mdeg}(\overline{f}) \preceq \mathrm{mdeg}(f)$.

(ii) Suppose $\mathrm{mdeg}(f) = \mathrm{mdeg}(\overline{f})$. Then $\mathrm{mdeg}(f) \in \Lambda(V)$ by Eq.(2.11), and since f is a monomial, f must be expressed as $f = a_{\boldsymbol{\lambda}}\boldsymbol{X}^{\boldsymbol{\lambda}}$ for some $\boldsymbol{\lambda} \in \Lambda(V)$. This implies by Proposition 2.5-(i) that $f = \overline{f}$, i.e., $f' = 0$ and contradicts the hypothesis.

(iii) If $\mathrm{mdeg}(\overline{f}) \prec \mathrm{mdeg}(f)$, i.e., $\mathrm{mdeg}(f) \neq \mathrm{mdeg}(\overline{f})$, we immediately get

$$\mathrm{mdeg}(f) = \mathrm{mdeg}(f') \notin \Lambda(V)$$

since we have from Eq.(2.12) that either

$$\mathrm{mdeg}(f) = \mathrm{mdeg}(\overline{f}) \text{ or } \mathrm{mdeg}(f) = \mathrm{mdeg}(f')$$

must hold.

Conversely, if $\mathrm{mdeg}(f) \notin \Lambda(V)$, we have $\mathrm{mdeg}(f) \neq \mathrm{mdeg}(\overline{f})$, since $\mathrm{mdeg}(\overline{f}) \in \Lambda(V)$ by Eq.(2.11). This implies that $\mathrm{mdeg}(\overline{f}) \prec \mathrm{mdeg}(f)$ by (i) of this lemma. □

Chapter 3

The Performance of Algebraic Geometry Codes

3.1 Introduction

In this chapter, we show that the conventional BCH codes can be better than the AG codes when the number of check symbols is relatively small. More precisely, we consider an AG code on C_{ab} whose number of check symbols is less than $\min\{g+a, n-g\}$, where n and g denote the code length and the genus of the curve, respectively. It is shown that there always exists an extended BCH code, (i) which has the same designed distance as the Feng-Rao designed distance of the AG code and the code length and the rate greater than those of the AG code, or (ii) which has the same number of check symbols as that of the AG code, the designed distance not less than that of the AG code and the code length longer than that of the AG code.

3.2 Preliminaries

In this section, we review Feng-Rao designed distances of AG codes on C_{ab} in terms of the structure sequence define in [21].

Hereafter we examine the residue Goppa code $C_\Omega(D, mQ)$ on C_{ab} with genus g. In this chapter, we always take $\{P_1, \ldots, P_n\}$ as the set of all places of degree one in $\mathbf{F}(C_{ab})/F$ except Q in order to make the code length as long as possible. Thus we denote $C_\Omega(D, mQ)$ as $C_\Omega(mQ)$ for simplicity.

3.2.1 Structure sequence and gap sequence

Denote the code length, the number of information symbols and the number of check symbols of $\mathcal{C}_\Omega(mQ)$ by $n = n[\mathcal{C}_\Omega(mQ)]$ (independent of m), $k[\mathcal{C}_\Omega(mQ)]$ and $r[\mathcal{C}_\Omega(mQ)]$, respectively.

Definition 3.1 [21] The *structure sequence* associated with $\mathcal{C}_\Omega(mQ)$ $(m = 0, 1, 2, \ldots)$ is given by

$$\mathcal{S}(Q) := \{m : m \in \{0, 1, 2, \ldots\},\ k[\mathcal{C}_\Omega(mQ)] < k[\mathcal{C}_\Omega((m-1)Q)]\}.$$

□

It is known that the cardinality of $\mathcal{S}(Q)$ is n [21], and therefore we can express $\mathcal{S}(Q)$ as $\{\rho_1, \rho_2, \ldots, \rho_n\}$ $(\rho_i < \rho_{i+1})$. It is also known that any $\rho_i \in \mathcal{S}(Q)$ $(1 \leq i \leq n)$ can be expressed as [21]

$$\rho = ak + b\ell,\ 0 \leq k,\ 0 \leq \ell \leq a - 1. \tag{3.1}$$

Proposition 3.1 [21]

(i) $\rho_1 = 0$ and $\rho_n = n + 2g - 1$.

(ii) If $n \geq 2g$, then $\rho_g = 2g - 2$.

(iii) If $n \geq 2g + 1$, then $\rho_i = g + i - 1$ for $g + 1 \leq i \leq n - g$.

(iv) If $t \leq n - g$, then $\{\rho_1, \ldots, \rho_t\} = \{\tau(f) : f \in \Gamma_{ab}(\rho_t)\}$.[1]

□

Proposition 3.2 [21]

(i) For $m < \rho_1$, $\mathcal{C}_\Omega(mQ) = F^n$.

(ii) For m such that $\rho_t \leq m \leq \rho_{t+1} - 1$, $\mathcal{C}_\Omega(mQ) = \mathcal{C}_\Omega(\rho_t Q)$ and $r[\mathcal{C}_\Omega(\rho_t Q)] = t$ $(1 \leq t \leq n)$.

(iii) For $m \geq \rho_n$, $\mathcal{C}_\Omega(mQ) = \{0\}$.

[1] It is concluded from Eq.(3.1) and this proposition that all integers such that $ak + b\ell$ $(\leq \rho_{n-g})$ $(0 \leq k,\ 0 \leq \ell \leq a - 1)$ are elements of $\mathcal{S}(Q)$.

□

We see from Proposition 3.2 that it is sufficient to examine the codes $C_\Omega(\rho_t Q)$ $(t = 1, 2, \ldots, n-1)$. It is noted here that the parity check matrix of $C_\Omega(\rho_t Q)$ is given in terms of the structure sequence as follows. Let $f_1(x, y)$ and $f_j(x, y)$ $(j = 2, 3, \ldots, t)$ be nonzero elements in $L(\rho_1 Q)$ and $L(\rho_j Q) \setminus L(\rho_{j-1} Q)$ $(j = 2, 3, \ldots, t)$ which satisfy $\tau(f_j(x, y)) = \rho_j$ $(j = 1, 2, \ldots, t)$, respectively.[2] Then the matrix

$$\boldsymbol{H}_t = \begin{bmatrix} f_1(P_1) & f_1(P_2) & \cdots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \cdots & f_2(P_n) \\ \vdots & \vdots & & \vdots \\ f_t(P_1) & f_t(P_2) & \cdots & f_t(P_n) \end{bmatrix} \tag{3.2}$$

becomes a parity check matrix of $C_\Omega(\rho_t Q)$ where $\{P_1, P_2, \ldots, P_n\}$ denotes the set of all places of degree one in $\mathbf{F}(\boldsymbol{C}_{ab})/F$ except Q.

Definition 3.2 [21] Denote by $\ell(mQ)$ the dimension of the linear space $L(mQ)$ given in Eq.(2.1). Then the *gap sequence* at Q is defined by

$$\mathcal{G}(Q) := \{m : m \in \{0, 1, 2, \ldots, \}, \ \ell(mQ) = \ell((m-1)Q)\}.$$

□

It is known that the cardinality of $\mathcal{G}(Q)$ is g [21], and therefore we can express $\mathcal{G}(Q)$ as $\{\lambda_1, \lambda_2, \ldots, \lambda_g\}$ $(\lambda_i < \lambda_{i+1})$. It is also known that if $n \geq 2g$, then $\rho_g = 2g - 2$, $\lambda_g = 2g - 1$ and $\{\rho_1, \ldots, \rho_g\} \cup \{\lambda_1, \ldots, \lambda_g\} = \{0, 1, 2, \ldots, 2g-1\}$ [21].

3.2.2 Feng-Rao designed distance

The Feng-Rao designed distances of the residue Goppa codes on $\boldsymbol{C}_{ab}$ are given in terms of the structure sequence as shown in the following theorem.

[2] For example, $f_j \in \Gamma_{ab}(\rho_j)$ with $\tau(f_j) = \rho_j$ satisfies this condition.

Proposition 3.3 [14, 21] The Feng-Rao designed distance $d_{\rm FR}[\mathcal{C}_\Omega(\rho_t Q)]$ of the residue Goppa code $\mathcal{C}_\Omega(\rho_t Q)$ on $\boldsymbol{C}_{ab}$ is given by

$$d_{\rm FR}[\mathcal{C}_\Omega(\rho_t Q)] = \begin{cases} \lfloor \rho_t/b \rfloor + 2, & \text{for } 1 \le t < \min\{g, n-g\}, \\ \min\{\rho \in \mathcal{S}(Q) : \rho \ge t+1-g\}, & \text{for } \min\{g, n-g\} \le t < \\ & \qquad \min\{3g-1, n-g\}, \\ t+1-g, & \text{for } \min\{3g-1, n-g\} \le t < n-g, \end{cases} \tag{3.3}$$

where n is the code length of $\mathcal{C}_\Omega(\rho_t Q)$. □

For our later discussion, we give a modified version of Proposition 3.3.

Theorem 3.1 $d_{\rm FR}[\mathcal{C}_\Omega(\rho_t Q)]$ is given or bounded by

$$d_{\rm FR}[\mathcal{C}_\Omega(\rho_t Q)] \begin{cases} = \lfloor \rho_t/b \rfloor + 2, & \text{for } 1 \le t < \min\{g+a, n-g\}, \\ \ge \lfloor \rho_t/b \rfloor + 2, & \text{for } \min\{g+a, n-g\} \le t < n-g. \end{cases} \tag{3.4}$$

(Proof is given in Appendix 3A.1.) □

3.3 Extended BCH codes better than AG codes

3.3.1 Codes for mediator

Define

$$M(u) := \begin{cases} \{1\}, & \text{for } u = 0, \\ \{x^{u-\ell} y^\ell : 0 \le \ell \le u\}, & \text{for } u > 0 \end{cases} \tag{3.5}$$

and

$$M^*(u) := M(0) \cup M(1) \cup \cdots \cup M(u).$$

For $f_k(x, y) \in M^*(u)$ $(k = 1, 2, \ldots, \nu,\ \nu := |M^*(u)|)$, we use $f_k(P_i)$ to indicate $f_k(x_i, y_i)$ for $P_i = (x_i, y_i)$ which is a F-rational point of $\boldsymbol{C}_{ab}$ defferent from Q.

Let α be a primitive element of $GF(q^2)$, and define $\boldsymbol{H}_1(u)$, $\boldsymbol{H}_2(u)$, $\boldsymbol{H}'_2(u)$ and $\boldsymbol{H}_3(u)$ by

$$\boldsymbol{H}_1(u) := \begin{bmatrix} f_1(P_1) & f_1(P_2) & \cdots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \cdots & f_2(P_n) \\ \vdots & \vdots & & \vdots \\ f_\nu(P_1) & f_\nu(P_2) & \cdots & f_\nu(P_n) \end{bmatrix}, \tag{3.6}$$

$$\boldsymbol{H}_2(u) := \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & \alpha^0 & \alpha^1 & \cdots & \alpha^{q^2-2} \\ 0 & \alpha^0 & \alpha^2 & \cdots & \alpha^{2(q^2-2)} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & \alpha^0 & \alpha^u & \cdots & \alpha^{u(q^2-2)} \end{bmatrix}, \tag{3.7}$$

$$\boldsymbol{H}_2'(u) := \begin{bmatrix} 1 & \alpha^0 & \alpha^1 & \cdots & \alpha^{q^2-2} \\ 0 & \alpha^0 & \alpha^2 & \cdots & \alpha^{2(q^2-2)} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & \alpha^0 & \alpha^u & \cdots & \alpha^{u(q^2-2)} \end{bmatrix}, \tag{3.8}$$

$$\boldsymbol{H}_3(u) := \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{\xi_1} & \alpha^{\xi_2} & \cdots & \alpha^{\xi_n} \\ \alpha^{2\xi_1} & \alpha^{2\xi_2} & \cdots & \alpha^{2\xi_n} \\ \vdots & \vdots & & \vdots \\ \alpha^{u\xi_1} & \alpha^{u\xi_2} & \cdots & \alpha^{u\xi_n} \end{bmatrix} \tag{3.9}$$

where in Eq.(3.9) α^{ξ_i} is the representation of $x_i\alpha + y_i$ as a power of α for $P_i = (x_i, y_i)$ with the convention that for $x_i = y_i = 0$,

$$\alpha^{k\xi_i} = (x_i\alpha + y_i)^k = \begin{cases} 1, & \text{for } k = 0, \\ 0, & \text{for } k > 0. \end{cases}$$

Denote by $\mathcal{C}_1(u)$, $\mathcal{C}_2(u)$, $\mathcal{C}_2'(u)$ and $\mathcal{C}_3(u)$ the codes over $F = GF(q)$ whose parity check matrices are $\boldsymbol{H}_1(u)$, $\boldsymbol{H}_2(u)$, $\boldsymbol{H}_2'(u)$ and $\boldsymbol{H}_3(u)$, respectively. We also denote by $n[\mathcal{C}_i(u)]$, $r[\mathcal{C}_i(u)]$, $d_{\text{BCH}}[\mathcal{C}_i(u)]$ and $R[\mathcal{C}_i(u)]$, the code length, the number of check symbols, the designed distance given by the BCH bound and the rate of $\mathcal{C}_i(u)$ $(i = 1, 2, 3)$ and $\mathcal{C}_2'(u)$. Then we have the following lemmas.

Lemma 3.1

(i) $n[\mathcal{C}_1(u)] = n[\mathcal{C}_3(u)] = n < q^2$ and $n[\mathcal{C}_2(u)] = n[\mathcal{C}_2'(u)] = q^2$.

(ii) $d_{\text{BCH}}[\mathcal{C}_2(u)] = u + 2$.

(iii) $\mathcal{C}_1(u)$ is a subcode of $\mathcal{C}_3(u)$.

(Proof) (i) Obvious from the definitions of $\mathcal{C}_i(u)$ $(i = 1, 2, 3)$ and $\mathcal{C}_2'(u)$ and Lemma 2.1.

(ii) The BCH bound for $\mathcal{C}_2(u)$ (an extended BCH code over $GF(q)$ with code length q^2).

(iii) Note in Eq.(3.6) that

$$\{f_1(x,y), f_2(x,y), \ldots, f_\nu(x,y)\} = \{x^{k-\ell}y^\ell : 0 \le k \le u,\ 0 \le \ell \le k\}.$$

Then since $\boldsymbol{H}_1(u)\boldsymbol{c}^t = \boldsymbol{0}$ for $\boldsymbol{c} := (c_1, c_2, \ldots, c_n) \in \mathcal{C}_1(u)$, we have

$$\sum_{i=1}^{n} c_i x_i^{k-\ell} y_i^\ell = 0$$

for all k $(k = 0, 1, \ldots, u)$ and ℓ $(\ell = 0, 1, \ldots, k)$. Thus for $\boldsymbol{c} \in \mathcal{C}_1(u)$, we have

$$\begin{aligned}
\sum_{i=1}^{n} c_i (\alpha^{\xi_i})^k &= \sum_{i=1}^{n} c_i (x_i\alpha + y_i)^k \\
&= \sum_{i=1}^{n} c_i \sum_{\ell=0}^{k} \binom{k}{\ell} \alpha^{k-\ell} x_i^{k-\ell} y_i^\ell \\
&= \sum_{\ell=0}^{k} \binom{k}{\ell} \alpha^{k-\ell} \left(\sum_{i=1}^{n} c_i x_i^{k-\ell} y_i^\ell \right) \\
&= 0
\end{aligned}$$

for all k $(k = 0, 1, \ldots, u)$. This, by Eq.(3.9), implies $\boldsymbol{c} \in \mathcal{C}_3(u)$ and completes the proof. □

Lemma 3.2

(i) $r[\mathcal{C}_2(u)] = r[\mathcal{C}_3(u)] \le r[\mathcal{C}_1(u)]$.

(ii) $R[\mathcal{C}_1(u)] \le R[\mathcal{C}_3(u)] < R[\mathcal{C}_2(u)]$.

(Proof) (i) The equality $r[\mathcal{C}_2(u)] = r[\mathcal{C}_3(u)]$ is directly obtained from the definition of $\boldsymbol{H}_2(u)$ and $\boldsymbol{H}_3(u)$. The inequality $r[\mathcal{C}_3(u)] \le r[\mathcal{C}_1(u)]$ is an immediate consequence of Lemma 3.1-(iii).

(ii) By the definition of code rate, $R[\mathcal{C}_i(u)] = 1 - r[\mathcal{C}_i(u)]/n[\mathcal{C}_i(u)]$, $i = 1, 2, 3$. Note Lemma 3.1-(i) and (i) of this lemma. □

Lemma 3.3 For $1 \le t < \min\{g + a, n - g\}$,

$$d_{\mathrm{BCH}}[\mathcal{C}_2(\lfloor \rho_t/b \rfloor)] = d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)] = \lfloor \rho_t/b \rfloor + 2. \tag{3.10}$$

(Proof) Immediate consequence of Theorem 3.1 and Lemma 3.1-(ii). □

Lemma 3.4 The number of check symbols of $\mathcal{C}_2(u)$ $(0 \leq u \leq q^2-2)$ satisfies

$$r[\mathcal{C}_2(u+1)] - r[\mathcal{C}_2(u)] = \begin{cases} 2, \ iq+i \leq u < iq+(q-1), \ 0 \leq i \leq q-2, \\ 0, \ iq+(q-1) \leq u < (i+1)q+i, \ 0 \leq i \leq q-2, \\ 1, \ u = (i+1)q+i, \ 0 \leq i \leq q-3. \end{cases} \tag{3.11}$$

(Proof is given in Appendix 3A.2.) □

Lemma 3.5 For $0 \leq u \leq q^2-2$,

(i) $r[\mathcal{C}_2(0)] = 1$, $r[\mathcal{C}_2'(1)] = 2$.

(ii) $r[\mathcal{C}_2'(u)] + 1 = r[\mathcal{C}_2(u)]$.

(iii) $d_{\mathrm{BCH}}[\mathcal{C}_2'(u)] = d_{\mathrm{BCH}}[\mathcal{C}_2(u)] - 1 = u+1$.

(Proof) (i) As shown in the proof of Lemma 3.4,

$$\left.\begin{array}{l} r[\mathcal{C}_2(0)] = \deg G_0(x), \\ G_0(x) = \mathrm{LCM}[m_0(x)] = x-1. \end{array}\right\}$$

Therefore we have $r[\mathcal{C}_2(0)] = 1$. Then by the definitions of $\boldsymbol{H}_2(1)$ and $\boldsymbol{H}_2'(1)$ and the first expression of Lemma 3.4, we have $r[\mathcal{C}_2'(1)] = r[\mathcal{C}_2(1)] - 1 = r[\mathcal{C}_2(0)] + 1 = 2$.

(ii) is directly given by the definitions of $\boldsymbol{H}_2(u)$ and $\boldsymbol{H}_2'(u)$.

(iii) is immediately obtained from the definitions of $\boldsymbol{H}_2(u)$ and $\boldsymbol{H}_2'(u)$ and the BCH bound. □

Lemma 3.6 For any t such that $1 \leq t < \min\{g+a, n-g\}$, there exists an extended BCH code $\mathcal{C}_2(u)$ or $\mathcal{C}_2'(u)$ whose number of check symbols is t and code length is q^2. (Proof is given in Appendix 3A.3.) □

3.3.2 Relation between $\mathcal{C}_\Omega(\rho_t Q)$ and extended BCH code (I)

Here we investigate the relation between the parameters of $\mathcal{C}_\Omega(\rho_t Q)$ and those of $\mathcal{C}_2(u)$ whose designed distance is equal to $d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)]$.

Lemma 3.7 For $M(u)$ defined in Eq.(3.5),

$$M(u) \subset L(\rho_t Q) \tag{3.12}$$

holds if and only if $y^u \in L(\rho_t Q)$.

(Proof) It is obvious that if $M(u) \subset L(\rho_t Q)$, then $y^u \in L(\rho_t Q)$.

To prove the converse, suppose $y^u \in L(\rho_t Q)$. This implies that $\tau(y^u) \leq \rho_t$. Note here that since $a < b$,

$$\tau(x^{u-\ell}y^{\ell}) = a(u-\ell) + b\ell \leq bu = \tau(y^u).$$

Therefore for any $f \in M(u)$, $\tau(f) \leq \tau(y^u) \leq \rho_t$, which implies $f \in L(\rho_t Q)$. □

Lemma 3.8 Let $u_{\max}$ be the maximum value of u that satisfies Eq.(3.12) for given ρ_t. Then

$$u_{\max} = \lfloor \rho_t / b \rfloor. \tag{3.13}$$

(Proof) Since $\tau(y^{\lfloor \rho_t/b \rfloor}) = b\lfloor \rho_t/b \rfloor \leq \rho_t$ and $\tau(y^{\lfloor \rho_t/b \rfloor + 1}) = b(\lfloor \rho_t/b \rfloor + 1) > \rho_t$, we have

$$y^{\lfloor \rho_t/b \rfloor} \in L(\rho_t Q) \text{ and } y^{\lfloor \rho_t/b \rfloor + 1} \notin L(\rho_t Q).$$

Therefore $u_{\max} = \lfloor \rho_t/b \rfloor$ by Lemma 3.7. □

Lemma 3.9 $\mathcal{C}_\Omega(\rho_t Q)$ is a subcode of $\mathcal{C}_1(\lfloor \rho_t/b \rfloor)$. Therefore $r[\mathcal{C}_\Omega(\rho_t Q)] \geq r[\mathcal{C}_1(\lfloor \rho_t/b \rfloor)]$ and $R[\mathcal{C}_\Omega(\rho_t Q)] \leq R[\mathcal{C}_1(\lfloor \rho_t/b \rfloor)]$.

(Proof) Lemma 3.7 and Lemma 3.8 imply that $M^*(\lfloor \rho_t/b \rfloor) \subset L(\rho_t Q)$. Then we see that the linear space spanned by $\boldsymbol{H}_1(\lfloor \rho_t/b \rfloor)$ is a subspace of the spaces spanned by $\boldsymbol{H}_t$ given in Eq.(3.2). Since $\mathcal{C}_\Omega(\rho_t Q)$ and $\mathcal{C}_1(\lfloor \rho_t/b \rfloor)$ are the orthogonal spaces of linear spaces spanned by $\boldsymbol{H}_t$ and $\boldsymbol{H}_1(\lfloor \rho_t/b \rfloor)$, respectively, $\mathcal{C}_\Omega(\rho_t Q)$ is a subcode of $\mathcal{C}_1(\lfloor \rho_t/b \rfloor)$. □

Now, we have (a) $d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)] = d_{\mathrm{BCH}}[\mathcal{C}_2(\lfloor \rho_t/b \rfloor)]$ for $1 \leq t < \min\{g+a, n-g\}$ by Lemma 3.3, (b) $n[\mathcal{C}_\Omega(\rho_t Q)] < n[\mathcal{C}_2(\lfloor \rho_t/b \rfloor)]$ by Lemma 3.1-(i), and (c) $R[\mathcal{C}_\Omega(\rho_t Q)] \leq R[\mathcal{C}_1(\lfloor \rho_t/b \rfloor)] < R[\mathcal{C}_2(\lfloor \rho_t/b \rfloor)]$ by Lemma 3.2-(ii) and Lemma 3.9, which are summarized as:

Theorem 3.2 For a residue Goppa code $\mathcal{C}_\Omega(\rho_t Q)$ with $1 \leq t\ (= r[\mathcal{C}_\Omega(\rho_t Q)]) < \min\{g+a, n-g\}$, there exists an extended BCH code, *i.e.*, $\mathcal{C}_2(\lfloor \rho_t/b \rfloor)$, having the same designed distance as the Feng-Rao designed distance of $\mathcal{C}_\Omega(\rho_t Q)$ and the code length and the rate greater than those of $\mathcal{C}_\Omega(\rho_t Q)$. □

Example 3.1 To illustrate Theorem 3.2, we consider the residue Goppa code $\mathcal{C}_\Omega(\rho_t Q)$ on the curve $x^5 + y^4 + y = 0$ over $F = GF(2^4)$, which is known as a Hermitian curve. In

this case, $a = 4, b = 5$ and $g = 6$, and the code length is 64. For $C_\Omega(\rho_t Q)$, we can take a corresponding extended BCH code $C_2(\lfloor \rho_t/5 \rfloor)$ over $GF(2^4)$ with code length 256.

By using the Feng-Rao and the BCH bounds, Fig. 3.1 compares the minimum numbers of check symbols which are required for $C_\Omega(\rho_t Q)$ and $C_2(\lfloor \rho_t/t \rfloor)$ to attain the given designed distance. The Goppa bound for $C_\Omega(\rho_t Q)$ is also shown for comparison. As seen from Fig. 3.1, when $r[C_\Omega(\rho_t Q)]$ satisfies the condition of Theorem 3.2, *i.e.*, $1 \leq r[C_\Omega(\rho_t Q)] < \min\{g + a, n - g\} = 10$, and even in the case of $r[C_\Omega(\rho_t Q)] = 10$ or 11, the extended BCH code $C_2(\lfloor \rho_t/5 \rfloor)$ does not require a larger number of check symbols than that of the AG code while achieving the same designed distance.

For example, to attain the designed distance 5, the extended BCH code needs only 7 check symbols while the AG code needs 10 symbols, and rates of the BCH and the AG codes are $249/256 = 0.973$ and $54/64 = 0.844$, respectively. □

3.3.3 Relation between $C_\Omega(\rho_t Q)$ and extended BCH code (II)

Here we investigate the relation between the parameters of $C_\Omega(\rho_t Q)$ and those of $C_2(u)$ and $C_2'(u)$ whose numbers of check symbols are equal to that of $C_\Omega(\rho_t Q)$.

Theorem 3.3 For a residue Goppa code $C_\Omega(\rho_t Q)$ with $1 \leq t\ (= r[C_\Omega(\rho_t Q)]) < \min\{g + a, n - g\}$, there exists an extended BCH code, *i.e.*, $C_2(u_0)$ or $C_2'(u_0)$ for some u_0, having the same number of check symbols as that of the AG code, the designed distance not less than that of the AG code and the code length longer than that of the AG code. (Proof is given in Appendix 3A.4.) □

Example 3.2 We show in Fig. 3.2 an illustration of Theorem 3.3 for the same AG code as in Example 3.1. As for extended BCH codes $C_2(u)$ and $C_2'(u)$, we can take ones defined by $\boldsymbol{H}_2(u)$ and $\boldsymbol{H}_2'(u)$, respectively, with code length 256. Fig. 3.2 compares the designed distance of $C_\Omega(\rho_t Q)$ with that of $C_2(u)$ or $C_2'(u)$, which are guaranteed by the Feng-Rao and the BCH bounds for given number of check symbols. As seen from Fig. 3.2, when the $r[C_\Omega(\rho_t Q)]$ satisfies the condition of Theorem 3.3, *i.e.*, $1 \leq r[C_\Omega(\rho_t Q)] < g + a = 10$, and even in the case of $r[C_\Omega(\rho_t Q)] = 10$, the designed distance of $C_2(u)$ or $C_2'(u)$ [3] is not less than that of $C_\Omega(\rho_t Q)$.

[3] In this example, we have $C_2((t-1)/2)$ for odd t's and $C_2'(t/2)$ for even t's.

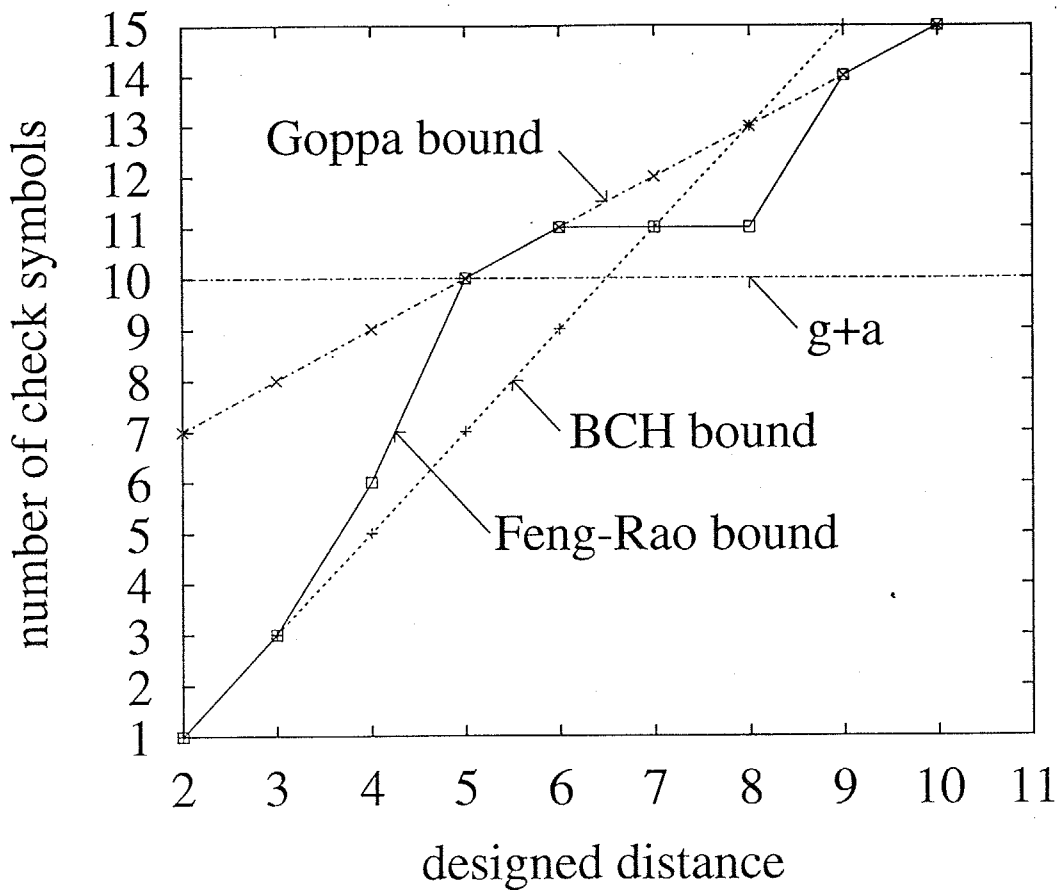

Figure 3.1: Relation between Feng-Rao bound for $C_\Omega(\rho_t Q)$ and BCH bound for $C_2(\lfloor \rho_t/b \rfloor)$.

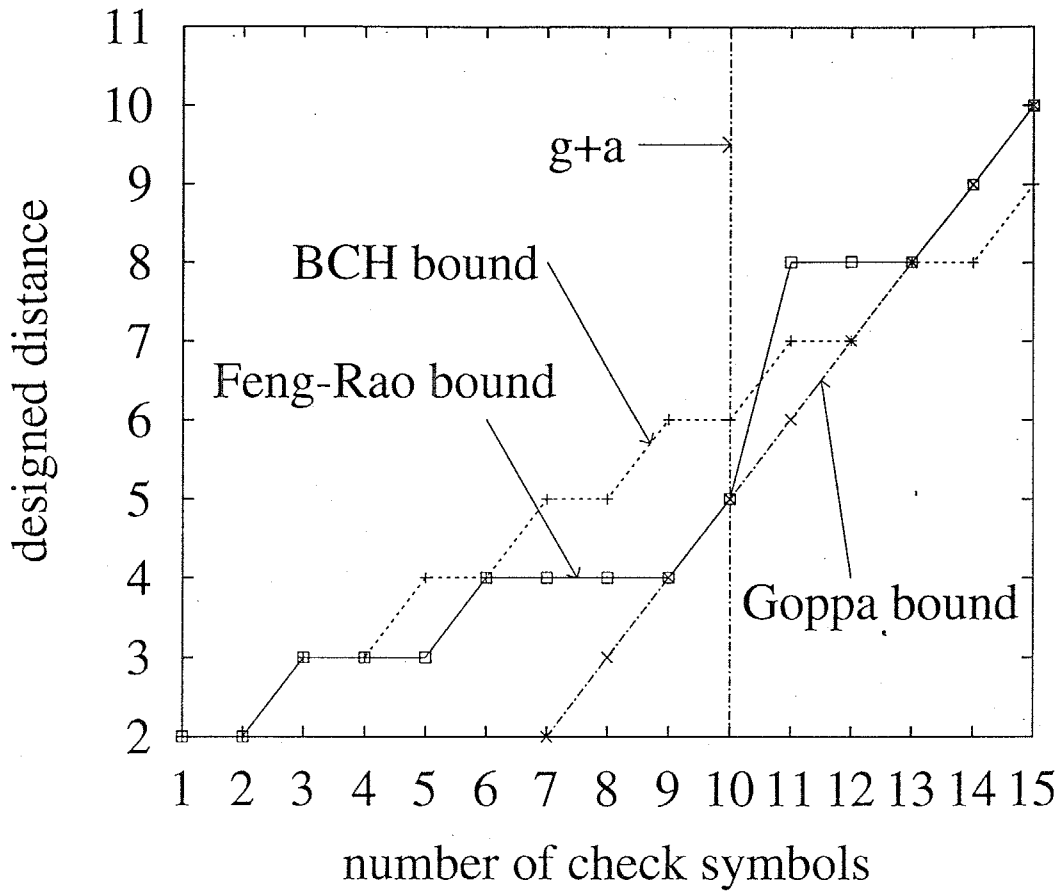

Figure 3.2: Relation between Feng-Rao bound for $C_\Omega(\rho_t Q)$ and BCH bound for $C_2(u_0)$ and $C_2'(u_0)$.

For example, when we use 9 check symbols, the designed distances of the extended BCH code $\mathcal{C}_2(4)$ and the AG code $\mathcal{C}_\Omega(\rho_9 Q)$ are 6 and 4, and the rates are $247/256 = 0.965$ and $55/64 = 0.859$, respectively. □

3.4 Conclusion

In this chapter, we have shown that for an AG code on C_{ab} whose number of check symbols is less than $\min\{g+a, n-g\}$, there always exists an extended BCH code, (i) which has the same designed distance as the Feng-Rao designed distance of $\mathcal{C}_\Omega(\rho_t Q)$ and the code length and the rate greater than those of $\mathcal{C}_\Omega(\rho_t Q)$, (ii) which has the same number of check symbols as that of $\mathcal{C}_\Omega(\rho_t Q)$, the designed distance not less than that of $\mathcal{C}_\Omega(\rho_t Q)$ and the code length longer than that of $\mathcal{C}_\Omega(\rho_t Q)$.

Appendices

3A.1 Proof of Theorem 3.1

(I) The first expression of Eq.(3.4): We separate this case into the following two cases.
(I-i) In the case $1 \le t < \min\{g, n-g\}$: Theorem 3.1 is Proposition 3.3 itself in this case.
(I-ii) In the case $\min\{g, n-g\} \le t < \min\{g+a, n-g\}$: If $g \ge n-g$ then $g+a > n-g$ and we have $n-g \le t < n-g$, *i.e.*, this case is empty. Hence it is sufficient to consider the case

$$\min\{g, n-g\} = g \le t < \min\{g+a, n-g\}. \tag{3A.1}$$

We examine Eq.(3A.1) by appending the additional conditions (a) $g+a \le 3g-1$ and (b) $g+a > 3g-1$.
(a) In the case $g+a \le 3g-1$: Since $\min\{g+a, n-g\} \le \min\{3g-1, n-g\}$, $d_{\rm FR}[\mathcal{C}_\Omega(\rho_t Q)]$ is given by the second expression of Eq.(3.3). Noting Eq.(3.1) and $0 \le t-g < \min\{g+a, n-g\} - g \le a$ by Eq.(3A.1), it is clear that the minimum $\rho \in \mathcal{S}(Q)$ which satisfies $\rho = ak + b\ell \ge t+1-g$ is a $(k=1, \ell=0)$, *i.e.*,

$$d_{\rm FR}[\mathcal{C}_\Omega(\rho_t Q)] = a.$$

On the other hand, by noting that $g < n-g$ from Eq.(3A.1), *i.e.*, $n \ge 2g+1$, we

have from Proposition 3.1-(ii) and (iii) that ρ_t is expressed as

$$\rho_t = \begin{cases} 2g-2, & \text{for } t = g, \\ g+t-1, & \text{for } g+1 \le t < \min\{g+a, n-g\}. \end{cases}$$

Hence for $g \le t < \min\{g+a, n-g\}$

$$\left\lfloor \frac{2g-2}{b} \right\rfloor \le \left\lfloor \frac{\rho_t}{b} \right\rfloor \le \left\lfloor \frac{g+t-1}{b} \right\rfloor \le \left\lfloor \frac{2g+a-2}{b} \right\rfloor.$$

But

$$\left\lfloor \frac{2g-2}{b} \right\rfloor = \left\lfloor \frac{(a-1)(b-1)-2}{b} \right\rfloor = a-2$$

and

$$\left\lfloor \frac{2g+a-2}{b} \right\rfloor = \left\lfloor \frac{(a-1)(b-1)+a-2}{b} \right\rfloor = a-2.$$

Thus we have for $g \le t < \min\{g+a, n-g\}$

$$\left\lfloor \frac{\rho_t}{b} \right\rfloor = a-2$$

and therefore, for case (a)

$$d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)] = \left\lfloor \frac{\rho_t}{b} \right\rfloor + 2.$$

(b) In the case $g+a > 3g-1$: Since $3g-1-(g+a) = (a-1)(b-2)-2 < 0$, we have only two cases; (b-1) $a=1$ ($g=0$) and (b-2) $a=2$, $b=3$ ($g=1$). But for (b-1), there is no t (≥ 1) that satisfies Eq.(3A.1). Therefore, we only need to consider the case (b-2), that is,

$$1 \le t < \min\{3, n-1\}.$$

Then it is clear that only two cases, *i.e.*, (b-2-i) $t=1$ for which we must have $n \ge 3$ and (b-2-ii) $t=2$ for which $n \ge 4$, are possible.

For the case (b-2-i), $d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)]$ is given by the second expression of Eq.(3.3) because $t = 1 < \min\{3g-1, n-g\} = \min\{2, n-1\} = 2$ ($n \ge 3$). Then it is clear that the minimum $\rho \in \mathcal{S}(Q)$ which satisfies $\rho = ak + b\ell \ge t+1-g = 1$ is $\rho = 2$ ($k=1, \ell=0$), and we have

$$d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)] = 2.$$

For the case (b-2-ii), $d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)]$ is given by the third expression of Eq.(3.3) because $t = 2 \ge \min\{3g-1, n-g\} = 2$. Then we have

$$d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)] = 2.$$

On the other hand, because $\rho_1 = 0$ by Proposition 3.1-(i) and $\rho_2 = a$ by Footnote 2, we have

$$\left\lfloor \frac{\rho_1}{b} \right\rfloor + 2 = \left\lfloor \frac{0}{3} \right\rfloor + 2 = 2,$$
$$\left\lfloor \frac{\rho_2}{b} \right\rfloor + 2 = \left\lfloor \frac{2}{3} \right\rfloor + 2 = 2.$$

Therefore for case (b),

$$d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)] = \left\lfloor \frac{\rho_t}{b} \right\rfloor + 2.$$

(II) The second expression of Eq.(3.4): We only need to consider the case where $\min\{g+a, n-g\} = g+a$, since otherwise there is no t that satisfies $\min\{g+a, n-g\} \le t < n-g$. Then by the second and third expressions of Eq.(3.3), we have

$$d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)] \ge t+1-g = a+1+t', \tag{3A.2}$$

where $t' := t-g-a$ $(0 \le t' < n-2g-a)$.

On the other hand, noting $n \ge 2g+1$ since $g+a < n-g$, we have from Proposition 3.1-(iii) and Eq.(2.5) that

$$\begin{aligned}\left\lfloor \frac{\rho_t}{b} \right\rfloor + 2 &= \left\lfloor \frac{g+t-1}{b} \right\rfloor + 2 \\ &= \left\lfloor \frac{2g+a+t'-1}{b} \right\rfloor + 2 \\ &= \left\lfloor \frac{(a-1)b+t'}{b} \right\rfloor + 2 \\ &= a+1+\left\lfloor \frac{t'}{b} \right\rfloor . \end{aligned} \tag{3A.3}$$

Therefore, noting $t' \ge \lfloor t'/b \rfloor$ for $t' \ge 0$ we have from Eqs.(3A.2) and (3A.3) that

$$d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)] \ge \left\lfloor \frac{\rho_t}{b} \right\rfloor + 2.$$

(Q.E.D.)

3A.2 Proof of Lemma 3.4

Let $C_2^*(u)$ be the BCH code with code length q^2-1 defined by the parity check matrix given by removing the first column of $\boldsymbol{H}_2(u)$. Then $r[\mathcal{C}_2(u)] = r[\mathcal{C}_2^*(u)]$ for $0 \le u \le q^2-2$.

Let α be a primitive element of $GF(q^2)$ and denote the minimal polynomial of α^ℓ $(\ell = 0, 1, \ldots, u)$ by $m_\ell(x)$. Then the generator polynomial $G_u(x)$ of $\mathcal{C}_2^*(u)$ is given by

$$G_u(x) = \mathrm{LCM}[m_0(x), m_1(x), \ldots, m_u(x)]$$

and $r[\mathcal{C}_2^*(u)] = \deg G_u(x)$.

Note that any u $(0 \le u \le q^2-2)$ is expressed as $u = iq + j$ $(0 \le i, j \le q-1)$ and thereby any $\varepsilon \in GF(q^2)\setminus\{0\}$ is expressed as $\varepsilon = \alpha^{iq+j}$ with some i and j. Therefore $\varepsilon^q = \varepsilon$, if and only if $i = j$ since $(\alpha^{iq+j})^q = \alpha^{jq+i}$. This implies that

$$\deg m_{iq+j}(x) = \begin{cases} 1, & i = j, \\ 2, & i \neq j. \end{cases} \tag{3A.4}$$

Next for given $u = iq + j(\le q^2-2)$, we divide the set $\{\alpha^s : 0 \le s \le u\}$ into the following three sets

$$\begin{aligned} A_k &:= \{\alpha^s : s = kq + k \le u\}, \\ B_k &:= \{\alpha^s : kq + (k+1) \le s \le \min\{kq + (q-1), u\}\}, \\ C_k &:= \{\alpha^s : (k+1)q \le s \le \min\{(k+1)q + k, u\}\}, \end{aligned}$$

which are all disjoint, and define

$$D_k := \left(\bigcup_{\ell=0}^{k} A_\ell\right) \bigcup \left(\bigcup_{\ell=0}^{k} B_\ell\right) \bigcup \left(\bigcup_{\ell=0}^{k-1} C_\ell\right).$$

Then it is easily verified that

$$\left.\begin{aligned} &\beta^q = \beta \in A_k, && \text{for } \forall \beta \in A_k, \\ &\gamma^q \in \bigcup_{\ell=k}^{\infty} C_\ell \not\subset D_k, && \text{for } \forall \gamma \in B_k, \\ &\delta^q \in \bigcup_{\ell=0}^{k} B_\ell, && \text{for } \forall \delta \in C_k. \end{aligned}\right\} \tag{3A.5}$$

Note that $D_\infty = \{\alpha^s : 0 \le s \le u\}$ by the definition of D_ℓ. Then it is easily seen from Eq.(3A.5) that the set of minimal polynomials which is necessary and sufficient to construct the generator polynomial of $\mathcal{C}_2^*(u)$ is given by the all minimal polynomials for the elements of $D_\infty \setminus \cup_{k=0}^{\infty} C_k$. Note from Eq.(3A.4) that the degrees of minimal polynomials for elements in A_k, B_k and C_k are 1, 2 and 2, respectively. Thus

$$\begin{aligned} \deg G_u(x) &= \left|\bigcup_{k=0}^{\infty} A_k\right| + 2\left|\bigcup_{k=0}^{\infty} B_k\right| \\ &= \sum_{k=0}^{\infty} |A_k| + 2\sum_{k=0}^{\infty} |B_k| \end{aligned}$$

where $\sum_{k=0}^{\infty}|A_k|$ and $\sum_{k=0}^{\infty}|B_k|$ are given by

$$\sum_{k=0}^{\infty}|A_k| = \begin{cases} i, & \text{for } i > j, \\ i+1, & \text{for } i \le j, \end{cases}$$

$$\sum_{k=0}^{\infty}|B_k| = \begin{cases} iq - \frac{1}{2}i(i+1), & \text{for } i > j, \\ iq - \frac{1}{2}i(i+1) + (j-i), & \text{for } i \le j, \end{cases}$$

respectively. Therefore we have for given $u = iq + j$

$$r[\mathcal{C}_2^*(u)] = \begin{cases} 2(u-j) - i^2, & \text{for } i > j, \\ 2(u-i) - i^2 + 1, & \text{for } i \le j. \end{cases} \tag{3A.6}$$

The following four cases are possible.

(i) $iq + i \le u < iq + (q-1)$ $(0 \le i \le q-2)$.

Since $u = iq + j$ with $i \le j$ and $u+1 = iq + (j+1)$ with $i < j+1$, both $r[\mathcal{C}_2^*(u)]$ and $r[\mathcal{C}_2^*(u+1)]$ are given by the second expression of Eq.(3A.6) and we have

$$r[\mathcal{C}_2(u+1)] - r[\mathcal{C}_2(u)] = 2.$$

(ii) $u = iq + (q-1)$ $(0 \le i \le q-2)$.

$r[\mathcal{C}_2^*(u)]$ is given by the second expression of Eq.(3A.6) since $i < j = q-1$ and $r[\mathcal{C}_2^*(u+1)]$ is given by the first expression of Eq.(3A.6) since $u+1 = (i+1)q$, *i.e.*, $i+1 > j = 0$. Thus we have

$$\begin{aligned} & r[\mathcal{C}_2(u+1)] - r[\mathcal{C}_2(u)] \\ &= \{2(u+1-0) - (i+1)^2\} - \{2(u-i) - i^2 + 1\} \\ &= 0. \end{aligned}$$

(iii) $(i+1)q \le u < (i+1)q + i$ $(0 \le i \le q-2)$.

Both $r[\mathcal{C}_2^*(u)]$ and $r[\mathcal{C}_2^*(u+1)]$ are given by the first expression of Eq.(3A.6) since $u = (i+1)q + j$ with $i+1 > j$ and $u+1 = (i+1)q + (j+1)$ with $i+1 > j+1$. Therefore we have

$$r[\mathcal{C}_2(u+1)] - r[\mathcal{C}_2(u)] = 0.$$

(iv) $u = (i+1)q + i$ $(0 \le i \le q-3)$.

$r[\mathcal{C}_2^*(u)]$ is given by the first expression of Eq.(3A.6) since $i+1 > j$ and $r[\mathcal{C}_2^*(u+1)]$ is given by the second expression of Eq.(3A.6) since $u+1 = (i+1)q + (i+1)$. Therefore

we have

$$\begin{aligned} & r[\mathcal{C}_2(u+1)] - r[\mathcal{C}_2(u)] \\ &= \{2(u+1-(i+1)) - (i+1)^2 + 1\} - \{2(u-i) - (i+1)^2\} \\ &= 1. \end{aligned}$$

(i) through (iv) yield Eq.(3.11). (Q.E.D.)

3A.3 Proof of Lemma 3.6

For $a = 1$, $g = 0$ by Eq.(2.5) and there is no t which satisfies $1 \leq t < \min\{g + a, n - g\}$. Hence it is sufficient to consider the case $2 \leq a < b$, in which $g \geq 1$ by Eq.(2.5).

By noting $n \leq q^2$, $g \geq 1$ and the first expression of Eq.(3A.6) with $u = (q-1)q+(q-2)$, we have

$$\begin{aligned} \min\{g + a, n - g\} &\leq q^2 - 1 \\ &= r[\mathcal{C}_2^*(q^2 - 2)] \\ &= r[\mathcal{C}_2(q^2 - 2)]. \end{aligned}$$

Since $r[\mathcal{C}_2(0)] = 1$ by Lemma 3.5-(i), on the other hand, we see that all t in $1 \leq t < \min\{g + a, n - g\}$ are included in

$$r[\mathcal{C}_2(0)] \leq t \leq r[\mathcal{C}_2(q^2 - 2)]. \tag{3A.7}$$

We prove the theorem for t given in Eq.(3A.7) by examining all $r[\mathcal{C}_2(u)]$ and $r[\mathcal{C}_2'(u)]$ for $0 \leq u \leq q^2 - 2$.

(i) $iq + i \leq u < iq + (q - 1)$ $(0 \leq i \leq q - 2)$.

Let $r[\mathcal{C}_2(u)] = t$, then $r[\mathcal{C}_2(u + 1)] = t + 2$ by the first relation of Eq.(3.11) and $r[\mathcal{C}_2'(u + 1)] = r[\mathcal{C}_2(u + 1)] - 1 = t + 1$ by Lemma 3.5-(ii). Therefore, by induction on u, for any t satisfying

$$r[\mathcal{C}_2(iq + i)] \leq t \leq r[\mathcal{C}_2(iq + (q - 1))],\ (0 \leq i \leq q - 2) \tag{3A.8}$$

there exists $\mathcal{C}_2(u)$ or $\mathcal{C}_2'(u)$ $(iq + i \leq u \leq iq + (q - 1), 0 \leq i \leq q - 2)$ such that $r[\mathcal{C}_2(u)] = t$ or $r[\mathcal{C}_2'(u)] = t$.

(ii) $(i + 1)q - 1 \leq u < (i + 1)q + i$ $(0 \leq i \leq q - 2)$.

Table 3.1: Proof of Theorem 3.3 for $1 \leq t \leq 3$.

	$t=1$	$t=2$	$t=3$
$r[\mathcal{C}_\Omega(\rho_t Q)]$	1 (by Proposition 3.2-(ii))	2 (by Proposition 3.2-(ii))	3 (by Proposition 3.2-(ii))
$d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)]$	2 (by Theorem 3.1, $\rho_1 = 0$)	2 (by Theorem 3.1, $\rho_2 = a$)	≤ 3 (by Theorem 3.1, $\rho_3 \leq b$)
$r[\mathcal{C}_2]$ or $r[\mathcal{C}_2']$	$r[\mathcal{C}_2(0)] = 1$ (by Lemma 3.5-(i))	$r[\mathcal{C}_2'(1)] = 2$ (by Lemma 3.5-(i))	$r[\mathcal{C}_2(1)] = 3$ (by Lemma 3.5-(i), (ii))
$d_{\mathrm{BCH}}[\mathcal{C}_2]$ or $d_{\mathrm{BCH}}[\mathcal{C}_2']$	$d_{\mathrm{BCH}}[\mathcal{C}_2(0)] = 2$ (by Lemma 3.1-(ii))	$d_{\mathrm{BCH}}[\mathcal{C}_2'(1)] = 2$ (by Lemma 3.5-(iii))	$d_{\mathrm{BCH}}[\mathcal{C}_2(1)] = 3$ (by Lemma 3.1-(ii))

Use the second relation of Eq.(3.11) repeatedly to get

$$\begin{aligned} r[\mathcal{C}_2(iq + (q-1))] &= r[\mathcal{C}_2((i+1)q)] \\ &= \cdots \\ &= r[\mathcal{C}_2((i+1)q + i)]. \end{aligned} \tag{3A.9}$$

(iii) $u = (i+1)q + i$ $(0 \leq i \leq q-3)$.

We have from the third relation of Eq.(3.11),

$$r[\mathcal{C}_2((i+1)q + i)] = r[\mathcal{C}_2((i+1)q + (i+1))] - 1. \tag{3A.10}$$

Note here that the range of t given in Eq.(3A.7) is fully covered by the ranges given by Eq.(3A.8), (3A.9) and (3A.10). Therefore we can conclude that for all t which satisfy Eq.(3A.7), there exists $\mathcal{C}_2(u)$ or $\mathcal{C}_2'(u)$ whose number of check symbols is t. (Q.E.D.)

3A.4 Proof of Theorem 3.3

As in the proof of Lemma 3.6, it is sufficient to consider the case $2 \leq a < b$ and $g \geq 1$. We will give a proof only for the designed distance since it is obvious for the code length by Lemma 3.1-(i).

For $1 \leq t\ (= r[\mathcal{C}_\Omega]) \leq 3 < \min\{g+a, n-g\}$, the theorem is directly verified as shown in Table 3.1.

In what follows, therefore, we only consider $\mathcal{C}_\Omega(\rho_t Q)$ for $4 \leq t\ (= r[\mathcal{C}_\Omega]) < \min\{g+a, n-g\}$.

By Lemma 3.6, there always exists $\mathcal{C}_2$ or $\mathcal{C}_2'$ whose number of check symbols equals $r[\mathcal{C}_\Omega(\rho_t Q)](= t)$ for all t $(1 \leq t < \min\{g+a, n-g\})$.

(I) In the case where there exists $\mathcal{C}_2(u_0)$ such that $r[\mathcal{C}_2(u_0)] = r[\mathcal{C}_\Omega(\rho_t Q)](= t)$:

We have from Lemma 3.9 and Lemma 3.2-(i) that

$$r[\mathcal{C}_2(u_0)] = r[\mathcal{C}_\Omega(\rho_t Q)] \geq r[\mathcal{C}_2(\lfloor \rho_t/b \rfloor)].$$

From this relation and Lemma 3.3, we obtain

$$d_{\mathrm{BCH}}[\mathcal{C}_2(u_0)] \geq d_{\mathrm{BCH}}[\mathcal{C}_2(\lfloor \rho_t/b \rfloor)] = d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)].$$

(II) In the case where there exists no $\mathcal{C}_2(u)$ such that $r[\mathcal{C}_2(u)] = r[\mathcal{C}_\Omega(\rho_t Q)](= t)$:

As seen from the proof of Lemma 3.6, this case happens only when the first relation of Eq.(3.11) holds, and by Lemma 3.6, there exists $\mathcal{C}_2'(u_0+1)$ such that $r[\mathcal{C}_2'(u_0+1)] = r[\mathcal{C}_\Omega(\rho_t Q)]$ where $iq + i \leq u_0 < iq + (q-1)$. It is noted here that we have from Eq.(3.11) and Lemma 3.5-(ii) that

$$\begin{aligned} r[\mathcal{C}_\Omega(\rho_t Q)] &= r[\mathcal{C}_2'(u_0+1)] \\ &= r[\mathcal{C}_2(u_0+1)] - 1 \\ &= r[\mathcal{C}_2(u_0)] + 1. \end{aligned} \tag{3A.11}$$

In the following, we show

$$d_{\mathrm{BCH}}[\mathcal{C}_2'(u_0+1)] \geq d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)]. \tag{3A.12}$$

Note first that since $\rho_t - \rho_{t-1} < b$ for $t < n - g$ by Proposition 3.1-(iv) (or Footnote 2), we have from the first expression of Eq.(3.4) that

$$d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)] = \begin{cases} d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_{t-1} Q)], \text{ or} \\ d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_{t-1} Q)] + 1 \end{cases} \tag{3A.13}$$

for $1 \leq t < \min\{g + a, n - g\}$.

From Eq.(3A.11) and Proposition 3.2-(ii), we have

$$\begin{aligned} r[\mathcal{C}_2(u_0)] &= r[\mathcal{C}_\Omega(\rho_t Q)] - 1 \\ &= r[\mathcal{C}_\Omega(\rho_{t-1} Q)]. \end{aligned} \tag{3A.14}$$

Hence we have from the discussion given in (I) that

$$d_{\mathrm{BCH}}[\mathcal{C}_2(u_0)] \geq d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_{t-1} Q)]. \tag{3A.15}$$

(i) If

$$d_{\mathrm{BCH}}[\mathcal{C}_2(u_0)] \geq d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_{t-1}Q)] + 1$$

in Eq.(3A.15), we have from Lemma 3.5-(iii) and Eq.(3A.13) that

$$\begin{aligned} d_{\mathrm{BCH}}[\mathcal{C}_2'(u_0+1)] &= d_{\mathrm{BCH}}[\mathcal{C}_2(u_0)] \\ &\geq d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_{t-1}Q)] + 1 \\ &\geq d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)] \end{aligned}$$

and Eq.(3A.12) holds.

(ii) Suppose

$$d_{\mathrm{BCH}}[\mathcal{C}_2(u_0)] = d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_{t-1}Q)] \tag{3A.16}$$

holds in Eq.(3A.15).

If the first expression of Eq.(3A.13) holds, by using Lemma 3.5-(iii), Eq.(3A.16) and Eq.(3A.13), we have

$$\begin{aligned} d_{\mathrm{BCH}}[\mathcal{C}_2'(u_0+1)] &= d_{\mathrm{BCH}}[\mathcal{C}_2(u_0)] \\ &= d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_{t-1}Q)] \\ &= d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_t Q)] \end{aligned}$$

and Eq.(3A.12) holds.

To complete the proof, we show that the second relation of Eq.(3A.13) does not hold in this case. Noting $iq+i \leq u_0 < iq+(q-1)$, we have from the first and third expressions of Eq.(3.11) that

$$r[\mathcal{C}_2(u_0-1)] = r[\mathcal{C}_2(u_0)] - s,$$

where $s = 1$ or 2. Apply Eq.(3A.14) and Proposition 3.2-(ii) to this expression to get

$$\begin{aligned} r[\mathcal{C}_2(u_0-1)] &= (t-1) - s \\ &= r[\mathcal{C}_\Omega(\rho_{t-1-s}Q)]. \end{aligned}$$

Thus we have from the discussion given in (I) that

$$d_{\mathrm{BCH}}[\mathcal{C}_2(u_0-1)] \geq d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_{t-1-s}Q)],\ s = 1 \text{ or } 2. \tag{3A.17}$$

On the other hand, if the second expression of Eq.(3A.13) holds, then $\rho_t = \theta b$ for some integer θ (> 0) and $\rho_t - \rho_{t-3} \leq b$.[4] Therefore we have from the first expression of Eq.(3.4) that

$$d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_{t-1}Q)] = d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_{t-1-s}Q)] \tag{3A.18}$$

with $s = 1$ or 2. Therefore

$$\begin{aligned} d_{\mathrm{BCH}}[\mathcal{C}_2(u_0 - 1)] &= d_{\mathrm{BCH}}[\mathcal{C}_2(u_0)] - 1 \quad \text{(by BCH bound)} \\ &< d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_{t-1}Q)] \quad \text{(by Eq.(3A.16))} \\ &= d_{\mathrm{FR}}[\mathcal{C}_\Omega(\rho_{t-1-s}Q)] \quad \text{(by Eq.(3A.18))} \end{aligned}$$

and this contradicts Eq.(3A.17). (Q.E.D.)

[4] As is easily seen from the first expression of Eq.(3.4), in order for the second relation of Eq.(3A.13) to hold, there must be an integer θ (> 0) such that $(\theta - 1)b \leq \rho_{t-1} < \theta b \leq \rho_t < (\theta + 1)b$. Since $t < \min\{g + a, n - g\} \leq n - g$, we have from Footnote 2 that θb ($\leq \rho_t < \rho_{n-g}$) $\in S(Q)$. Then we can conclude that $\rho_t = \theta b$ since there is no $\rho_i \in S(Q)$ between ρ_{t-1} and ρ_t.

Assume $\rho_t - \rho_{t-3} > b$ and let

$$\rho_i := \rho_{t-3} + a,\ \rho_j := \rho_{t-3} + b,$$

$$\rho_k := \begin{cases} \rho_t - b, & \text{if } \rho_t - b \neq \rho_i, \rho_j \\ \rho_{t-3} + 2a, & \text{if } \rho_t - b = \rho_i \\ \rho_{t-3} + a + b, & \text{if } \rho_t - b = \rho_j. \end{cases}$$

Then ρ_i, ρ_j, ρ_k are all different and $\rho_{t-3} < \rho_i, \rho_j, \rho_k < \rho_t$ since $a < b$ and $\gcd(a, b) = 1$. This contradicts the fact that there are only ρ_{t-2} and ρ_{t-1} between ρ_{t-3} and ρ_t. Hence $\rho_t - \rho_{t-3} \leq b$.

Chapter 4

The Dimension of Subfield Subcodes

4.1 Introduction

It is well known that some good codes such as BCH codes, Goppa codes and alternant codes are constructed as subfield subcodes of algebraic codes over a larger field. To evaluate the performance of subfield subcodes, several authors have investigated how to estimate their parameters (dimension, minimum distance, etc.). Wirtz [43] obtained estimates for the parameters of subfield subcode of certain AG codes. Katsman and Tsfasman [13] proved a special case of Wirtz's result. Both papers use concepts from algebraic geometry, and their results seem to depend substantially on the algebraic geometric construction of AG codes. Stichtenoth [37], however, showed that the result of [13, 43] are actually special cases of a general estimate for the dimension of subfield subcodes of arbitrary linear codes.

In this chapter, we improve the lower bound for the dimension of subfield subcodes obtained by Stichtenoth [37]. Moreover, we introduce the simple estimation for the dimension of subfield subcodes of AG codes on C_{ab}, which is based on the proposed bound.

4.2 Preliminaries

For a subspace W of the n-dimensional linear space $F_{q^m}^n$ over F_{q^m}, we denote by $W|_{F_q}$ the restriction of W to F_q, i.e., $W|_{F_q} := W \cap F_q^n$. Thus if W is a linear code of length n over F_{q^m}, $W|_{F_q}$ means a subfield subcode of W over F_q. $W^\perp$ stands for the dual space of W defined by

$$W^\perp := \{\boldsymbol{v} \in F_{q^m}^n : \boldsymbol{v} \cdot \boldsymbol{w}^T = 0 \text{ for } \forall \boldsymbol{w} \in W\}.$$

To study the dimension of $W|_{F_q}$, the operation of the Galois group of F_{q^m} over F_q, denoted by $Gal(F_{q^m}/F_q)$, on the vector space $F_{q^m}^n$ is introduced in [37]. $Gal(F_{q^m}/F_q)$ is a cyclic group of order m, generated by the Frobenius automorphism $\sigma : F_{q^m} \to F_{q^m}$ $(\alpha \mapsto \alpha^q)$. For $\boldsymbol{c} = (c_1, c_2, \ldots, c_n) \in F_{q^m}^n$ and $W \subset F_{q^m}^n$, $\sigma(\boldsymbol{c})$ and $\sigma(W)$ are defined by

$$\begin{cases} \sigma(\boldsymbol{c}) := (\sigma(c_1), \sigma(c_2), \ldots, \sigma(c_n)), \\ \sigma(W) := \{\sigma(\boldsymbol{c}) : \boldsymbol{c} \in W\}. \end{cases} \tag{4.1}$$

Lemma 4.1 Let W be a subspace of $F_{q^m}^n$ over F_{q^m}, and $\{\boldsymbol{w}_j\}_{j=1}^k$ be a basis of W where $k := \dim W$. Then $\{\sigma^i(\boldsymbol{w}_j)\}_{j=1}^k$ is a basis of $\sigma^i(W)$ $(i = 0, 1, \ldots, m-1)$.

(Proof) Obvious. □

Definition 4.1 [37] For a subspace $W \subset F_{q^m}^n$, we define W^0 and W^* by

$$W^0 := \bigcap_{i=0}^{m-1} \sigma^i(W), \quad W^* := \sum_{i=0}^{m-1} \sigma^i(W).$$

□

Lemma 4.2 [37] Let W be a linear code of length n over F_{q^m}. Then

$$\dim(W|_{F_q}) = n - \dim(W^\perp)^*. \tag{4.2}$$

□

This lemma implies that the dimension of subfield subcode $W|_{F_q}$ is determined if we can know the dimension of $(W^\perp)^*$. Though it is not easy in general to know $\dim W^*$ for a given subspace $W \subset F_{q^m}^n$, an upper bound for $\dim W^*$ is given as follows.

Lemma 4.3 [37] Let $V \subset W \subset F_{q^m}^n$ be subspaces such that $\sigma(V) \subset W$. Then

$$\dim W^* \leq \dim V^0 + m(\dim W - \dim V) \tag{4.3}$$

where V^0 as defined in Definition 4.1. □

4.3 A new lower bound for the dimension of subfield subcodes

In the remaining part of this chapter, we exclusively use symbols T, U, V and W to indicate subspaces of $F_{q^m}^n$ such that

$$V \subset W, \sigma(V) \subset W$$

and

$$U := V + \sigma(V),\ W = U + T. \tag{4.4}$$

Since $W^* = U^* + T^*$ by the second condition of Eq.(4.4), we have from the first relation of Eq.(4.4) and Lemma 4.3 that

$$\begin{aligned} \dim W^* &\le \dim U^* + \dim T^* \\ &\le \dim V^0 + m(\dim U - \dim V) + \dim T^*. \end{aligned} \tag{4.5}$$

By comparing two upper bounds given in Eqs.(4.3) and (4.5), we have

$$\begin{aligned} &\dim V^0 + m(\dim W - \dim V) - \{\dim V^0 + m(\dim U - \dim V) + \dim T^*\} \\ &= m(\dim W - \dim U) - \dim T^*. \end{aligned}$$

This means, if we can find a subspace $T \subset W$ and an upper bound τ for $\dim T^*$ such that

$$(\dim T^* \le)\ \tau \le m(\dim W - \dim U), \tag{4.6}$$

we can get from Eq.(4.5) a tighter upper bound for $\dim W^*$ than that of Eq.(4.3). It is obvious in Eq.(4.6) that τ should be chosen as small as possible. Next theorem gives this upper bound τ for $\dim T^*$.

Theorem 4.1 Let T and T_i's be subspaces of $F_{q^m}^n$ such that

$$\left.\begin{aligned} &T = \sum_{i=1}^{k} T_i,\ \sigma^{\ell(i)}(T_i) \subset T, \\ &1 \le \ell(1) \le \ell(2) \le \cdots \le \ell(k) \le m.^{1} \end{aligned}\right\} \tag{4.7}$$

Then

$$T^* = \sum_{i=1}^{k} \sum_{j=0}^{\ell(i)-1} \sigma^j(T_i) \tag{4.8}$$

and we have

$$\dim T^* \le \tau := \sum_{i=1}^{k} \ell(i) \dim T_i. \tag{4.9}$$

(Proof) Since Eq.(4.9) is an immediate consequence of Eq.(4.8) and Lemma 4.1, we prove Eq.(4.8).

Let $T' := \sum_{i=1}^{k} \sum_{j=0}^{\ell(i)-1} \sigma^j(T_i)$. Since $T^* \supset T'$ is obvious, it is sufficient to show $T^* \subset T'$.

---

[1] It is noted that we can always find such $\ell(i)$'s since $\sigma^m(T_i) = T_i \subset T$.

It is easily seen that T^* is the *smallest* subspace in the set of subspaces

$$\mathcal{S} := \{S \subset F_{q^m}^n : \text{(i) } S \supset T \text{ and (ii) } \sigma(S) = S\}.$$

Thus any subspace in $\mathcal{S}$ must contain T^*. Therefore the proof finishes if we can say that $T' \in \mathcal{S}$.

It is obvious that T' satisfies the condition (i) for $\mathcal{S}$. As for the condition (ii), we immediately have from the assumption given in Eq.(4.7) that

$$\begin{aligned}\sigma(T') &= \sum_{i=1}^{k} \sum_{j=1}^{\ell(i)-1} \sigma^j(T_i) + \sum_{i=1}^{k} \sigma^{\ell(i)}(T_i) \\ &\subset \sum_{i=1}^{k} \sum_{j=1}^{\ell(i)-1} \sigma^j(T_i) + T.\end{aligned}$$

Since $T = \sum_{i=1}^{k} \sigma^0(T_i)$, this implies $\sigma(T') \subset T'$. Therefore, by Lemma 4.1, we can conclude that $\sigma(T') = T'$. □

In order to make τ in Eq.(4.9) satisfy the another inequality of Eq.(4.6), we may impose additional conditions on T and T_i's in Eq.(4.4) and Eq.(4.7), that is,

$$W = U \oplus T \quad \text{and} \quad T = \bigoplus_{i=1}^{k} T_i. \tag{4.10}$$

By the second condition of Eq.(4.10), we have in Eq.(4.9) that

$$\dim T^* \le \sum_{i=1}^{k} \ell(i) \dim T_i \le m \dim T, \tag{4.11}$$

and we have

$$m \dim T = m(\dim W - \dim U)$$

by the first condition of Eq.(4.10).

We may say a little more about how to select T_i's in order to make τ smaller. Suppose T_i is decomposed as the direct sum of its subspaces, say, $T_i = \oplus_{j=1}^{r} S_j$. Then since $S_j \subset T_i$, we have $\sigma^{\ell(i)}(S_j) \subset \sigma^{\ell(i)}(T_i) \subset T$, which means for every S_j there exists a positive integer $\nu(j)$ such that

$$\sigma^{\nu(j)}(S_j) \subset T,\ \nu(j) \le \ell(i)$$

and we have

$$\sum_{j=1}^{r} \nu(j) \dim S_j \le \ell(i) \dim T_i.$$

After all, we may decompose T as the direct sum of its one-dimensional subspaces $T_i := \langle \boldsymbol{t}_i \rangle$, where $\{\boldsymbol{t}_i\}_{i=1}^{k}$ ($k := \dim T$) is a basis of T, and Eq.(4.11) reduces to

$$\dim T^* \leq \sum_{i=1}^{k} \ell(i) \leq m \dim T$$

where $\ell(i)$ is the smallest positive integer such that $\sigma^{\ell(i)}(\langle \boldsymbol{t}_i \rangle) \subset T$.[2]

In the next subsection, we give a couple of illustrative examples.

4.4 Examples

We denote by $\langle A \rangle$ the vector space over a field E spanned by a set $A \subset E^n$.

4.4.1 BCH code

We consider first a primitive BCH code over F_q with code length $n = q^m - 1$, which is the subfield subcode of the code with parity check matrix

$$H = \begin{pmatrix} \boldsymbol{h}_1 \\ \boldsymbol{h}_2 \\ \vdots \\ \boldsymbol{h}_{2t} \end{pmatrix} \tag{4.12}$$

where $\boldsymbol{h}_i := (1, \alpha^i, \alpha^{2i}, \ldots, \alpha^{(n-1)i})$ ($i = 1, 2, \ldots$) and α is the primitive element of F_{q^m}. Let $A_W := \{\boldsymbol{h}_i\}_{i=1}^{2t}$, the set of all row vectors in the parity check matrix H, and $W := \langle A_W \rangle$. Then the BCH code we consider is $W^{\perp}|_{F_q}$. It is noted that $\{\boldsymbol{h}_i\}_{i=1}^{n}$ constitutes a basis of $F_{q^m}^n$.

In the following , we consider the case in which $q = 2$, $m = 7$, $n = 127$ and $2t = 26$, i.e., designed distance $2t + 1 = 27$. It is noted that $2tq \leq n$ holds in this case. The true dimension of this code is known to be 50.

Conventional bound It is shown in [37] that in a primitive BCH code, we have $\dim V^0 = 0$ for $\forall V \subset W$ with $\sigma(V) \subset W$. Therefore, in order to get the best estimate for $\dim W^*$ by Eq.(4.3), it is needed to choose V with $\sigma(V) \subset W$ as the subspace of W having the largest dimension.

[2] As is easily seen, one can collect t_i's having the same $\ell(i)$'s to make up one subspace $\langle \{t_i : \ell(i) = \text{const.}\} \rangle$ of T with no effect on the result.

Lemma 4.4 If $2tq \leq n = q^m - 1$ holds, the best choice of V is given by $V := \langle A_V \rangle$ where $A_V := \{\boldsymbol{h}_i\}_{i=1}^{\lfloor 2t/q \rfloor}$.

(Proof) What we need to show is:

$$V', \sigma(V') \subset W \Longrightarrow V' \subset V.$$

Let $\boldsymbol{v} \in V'$, then it can be expressed as $\boldsymbol{v} = \sum_{i=1}^{2t} a_i \boldsymbol{h}_i$ for $\exists a_i \in F_{q^m}$ and we also have

$$\sigma(\boldsymbol{v}) = \sum_{i=1}^{2t} a_i^q \boldsymbol{h}_{qi} \in W$$

which implies $\sigma(\boldsymbol{v}) = \sum_{i=1}^{2t} b_i \boldsymbol{h}_i$ for $\exists b_i \in F_{q^m}$. Then we have a linear relation

$$\sum_{i=1}^{2t} a_i^q \boldsymbol{h}_{qi} - \sum_{i=1}^{2t} b_i \boldsymbol{h}_i = 0$$

which implies

$$a_i = 0 \text{ for } qi > 2t$$

since $\{\boldsymbol{h}_i\}_{i=1}^{n}$ are linearly independent and both $\{\boldsymbol{h}_{qi}\}_{i=1}^{2t}$ and $\{\boldsymbol{h}_i\}_{i=1}^{2t}$ are subsets of $\{\boldsymbol{h}_i\}_{i=1}^{n}$ by the hypothesis $2tq \leq n$.

Therefore $\boldsymbol{v} \in V'$ must be expressed as $\boldsymbol{v} = \sum_{i=1}^{\lfloor 2t/q \rfloor} a_i \boldsymbol{h}_i$ implying $\boldsymbol{v} \in V$. □

Then since $\dim W = 26$ and $\dim V = \lfloor 2t/q \rfloor = 13$, we have from Eq.(4.3) that

$$\dim W^* \leq 0 + 7(26 - 13) = 91$$

which by Eq.(4.2) states that the dimension of this BCH code is at least $127 - 91 = 36$. □

Proposed bound Let W and V be as given above. Then by Lemma 4.1, $\sigma(V) = \langle A_{\sigma(V)} \rangle$ with

$$A_{\sigma(V)} := \{\sigma(\boldsymbol{h}_i) : \boldsymbol{h}_i \in A_V\} = \{\boldsymbol{h}_{2i}\}_{i=1}^{13}.$$

Therefore $U = \langle A_V \rangle + \langle A_{\sigma(V)} \rangle$ by definition and we have $\dim U = |A_V \cup A_{\sigma(V)}| = 20$.

Let $A_T := A_W \setminus (A_V \cup A_{\sigma(V)})$ and $T := \langle A_T \rangle$ so that $W = U \oplus T$. By finding the smallest positive integer $\ell(i)$ for each $\boldsymbol{h}_i \in A_T$ such that $\sigma^{\ell(i)}(\boldsymbol{h}_i) \in A_T$ and collecting $\boldsymbol{h}_i$'s having the same value of $\ell(i)$, we easily see that T is decomposed as the direct sum of

$$\begin{cases} T_1 := \langle \{\boldsymbol{h}_{19}\} \rangle, \ T_2 := \langle \{\boldsymbol{h}_{25}\} \rangle, \\ T_3 := \langle \{\boldsymbol{h}_{15}, \boldsymbol{h}_{17}, \boldsymbol{h}_{21}, \boldsymbol{h}_{23}\} \rangle, \end{cases}$$

and $\ell(i)$'s for which $\sigma^{\ell(i)}(T_i) \subset T$ $(i = 1, 2, 3)$ are given by $\ell(1) = 3$, $\ell(2) = 4$ and $\ell(3) = 7$.

Then by Theorem 4.1, we have

$$\dim T^* \leq \sum_{i=1}^{3} \ell(i) \dim T_i = 3 + 4 + 7 \cdot 4 = 35,$$

and Eq.(4.5) yields

$$\dim W^* \leq 0 + 7(20 - 13) + 35 = 84.$$

By Eq.(4.2), therefore, the dimension of this BCH code is at least $127 - 84 = 43$. □

Thus Theorem 4.1 gives a tighter estimate for the dimension of this BCH code than that given by Stichtenoth.

4.4.2 AG code on a hyperelliptic curve

Here we consider a subfield subcode over F_4 of residue Goppa code on a hyperelliptic curve defined by

$$x^{17} + y^2 + y = 0, \text{ over } F_{4^4}. \tag{4.13}$$

It is known that the number of F_{4^4}-rational points on this curve is 513 and reaches the Hasse-Weil upper bound [19].

The parity check matrix of this residue Goppa code is given as follows [19]. Let

$$\begin{aligned} \Gamma(\rho) &:= \{x^k y^\ell : 0 \leq k,\ 0 \leq \ell \leq 1,\ 2k + 17\ell \leq \rho\} \\ &= \{f_1, f_2, \ldots, f_r\} \end{aligned} \tag{4.14}$$

where $r := |\Gamma(\rho)|$. The ordering of f_i's is such that for $f_i = x^{k_i} y^{\ell_i}$ and $f_j = x^{k_j} y^{\ell_j}$, $i < j$ if and only if $2k_i + 17\ell_i < 2k_j + 17\ell_j$.

For $f \in \Gamma(\rho)$, define $\boldsymbol{c}(f) := (f(P_1), \ldots, f(P_n))$ where P_i $(i = 1, \ldots, n\ (= 512))$ denotes all F_{4^4}-rational points on Eq.(4.13) except P_∞ (the rational point at infinity) and $f(P_i) := x_i^k y_i^\ell$ for $f = x^k y^\ell$ and $P_i = (x_i, y_i)$. Then it is known that $\boldsymbol{c}(f_1), \boldsymbol{c}(f_2), \ldots, \boldsymbol{c}(f_r)$ are linearly independent and the parity check matrix is given by

$$H = \begin{pmatrix} \boldsymbol{c}(f_1) \\ \vdots \\ \boldsymbol{c}(f_r) \end{pmatrix}.$$

Let $A_W := \{\boldsymbol{c}(f_i)\}_{i=1}^r$, the set of all row vectors in the parity check matrix H, and $W := \langle A_W \rangle$. Then the subfield subcode we consider is given by $W^\perp|_{F_4}$. In the following,

we consider the case in which $\rho = 66$ in Eq.(4.14), which yields $r = 59$. Note that in this case, $q = 4$ and $m = 4$.

Conventional bound It is shown in [37] that in this residue Goppa code, we have $\dim V^0 = 1$ for $\{\mathbf{0}\} \neq \forall V \subset W$ with $\sigma(V) \subset W$. It is also shown in [37] that the largest subspace V of W such that $\sigma(V) \subset W$, by which we can get the best estimate for $\dim W^*$ by Eq.(4.3), is given by $V := \langle A_V \rangle$ where

$$A_V := \{\boldsymbol{c}(f) : f \in \Gamma(16)\} = \{\boldsymbol{c}(x^k)\}_{k=0}^{8}.$$

Then since $\dim W = |\Gamma(66)| = 59$ and $\dim V = |\Gamma(16)| = 9$, we have from Eq.(4.3) that

$$\dim W^* \leq 1 + 4(59 - 9) = 201$$

and by Eq.(4.2), therefore, $\dim(W^{\perp}|_{F_4}) \geq 512 - 201 = 311$. □

Proposed bound Let W and V be as given above. Then by Lemma 4.1, $\sigma(V) = \langle A_{\sigma(V)} \rangle$ with

$$A_{\sigma(V)} := \{\boldsymbol{c}(x^{4i})\}_{i=0}^{8}.$$

Therefore $U = \langle A_V \rangle + \langle A_{\sigma(V)} \rangle$ by definition and we have $\dim U = |A_V \cup A_{\sigma(V)}| = 15$.

Let $A_T := A_W \setminus (A_V \cup A_{\sigma(V)})$ and $T := \langle A_T \rangle$ so that $W = U \oplus T$. By finding the smallest positive integer $\ell(i)$ for each $\boldsymbol{c}(f_i) \in A_T$ such that $\sigma^{\ell(i)}(\boldsymbol{c}(f_i)) \in A_T$ and collecting $\boldsymbol{c}(f_i)$'s having the same value of $\ell(i)$, we see that T is decomposed as the direct sum of

$$\begin{cases} T_1 := \langle \{\boldsymbol{c}(x^{18}),\ \boldsymbol{c}(x^{33}),\ \boldsymbol{c}(x^{17})\} \rangle, \\ T_2 := \langle A_T \setminus \{\boldsymbol{c}(x^{18}),\ \boldsymbol{c}(x^{33}),\ \boldsymbol{c}(x^{17})\} \rangle, \end{cases}$$

and $\ell(i)$'s for which $\sigma^{\ell(i)}(T_i) \subset T$ $(i = 1, 2)$ are given by $\ell(1) = 2$ and $\ell(2) = 4$.

Then by Theorem 4.1, we have

$$\dim T^* \leq \sum_{i=1}^{2} \ell(i) \dim T_i = 2 \cdot 3 + 4 \cdot 41 = 170$$

and Eq.(4.9) yields

$$\dim W^* \leq 1 + 4(15 - 9) + 170 = 195.$$

By Eq.(4.2), therefore, $\dim(W^{\perp}|_{F_4}) \geq 512 - 195 = 317$.

□

Thus Theorem 4.1 gives a tighter estimate for the dimension of $W^{\perp}|_{F_4}$ than that given by Stichtenoth.

4.5 Simple estimation for the dimension of subfield subcodes of AG codes

4.5.1 Overview

In what follows, we fix a and b, and abbreviate $\Gamma_{ab}(\rho)$ in Eq.(2.6) as $\Gamma(\rho)$ for simplicity. In order to specify each element of $\Gamma(\rho)$, we let

$$\Gamma(\rho) = \{f_1, f_2, \ldots, f_r\},\ \tau(f_i) < \tau(f_{i+1}).^3 \tag{4.15}$$

We also denote by $\{P_1, P_2, \ldots, P_n\}$ the set of all F_{q^m}-rational points on $\boldsymbol{C}_{ab}$ different from Q and use the notation $f(P_i)$ to indicate $f(x_i, y_i)$ for $f(x, y) \in L(\rho Q)$ and $P_i = (x_i, y_i)$.

In the remaining part of this section, for the code length n of $\mathcal{C}_\Omega(\rho Q)$ we assume $\rho < n$ for simplicity. Since $\mathcal{C}_\Omega(\rho Q)^\perp$ is the image of the linear map ϕ in Eq.(2.2), we have $\dim L(\rho Q) = \dim \mathcal{C}_\Omega(\rho Q)^\perp + \dim \mathrm{Ker}(\phi)$, and if $\rho < n$ it is known that $\dim \mathrm{Ker}(\phi) = 0$ [38]. Therefore for $\rho < n$, we have

$$\dim \mathcal{C}_\Omega(\rho Q)^\perp = \dim L(\rho Q) = |\Gamma(\rho)|.$$

In [37], based on Eq.(4.3), a general lower bound for the dimension of subfield subcode of a residue Goppa code on an arbitrary curve is derived. We can apply the result to the residue Goppa codes on $\boldsymbol{C}_{ab}$ as follows. Letting $W := \mathcal{C}_\Omega(\rho Q)^\perp$ and $V := \mathcal{C}_\Omega(\rho' Q)^\perp$ where $\rho' \leq \lfloor \rho/q \rfloor$ so that $V \subset W$ and $\sigma(V) \subset W$, we get $\dim V^0 = 1$[4] , $\dim W = \dim L(\rho Q) = |\Gamma(\rho)|$ and $\dim V = \dim L(\rho' Q) = |\Gamma(\rho')|$, and Eq.(4.3) yields

$$\dim(\mathcal{C}_\Omega(\rho Q)^\perp)^* \leq 1 + m\{|\Gamma(\rho)| - |\Gamma(\rho')|\}. \tag{4.16}$$

By noting that $L(\rho_1 Q) \subset L(\rho_2 Q)$ for $\rho_1 < \rho_2$, we have the smallest upper bound for $\dim(\mathcal{C}_\Omega(\rho Q)^\perp)^*$ of this form by taking $\rho' = \lfloor \rho/q \rfloor$ in Eq.(4.16).

In this section, we improve the bound for $\dim(\mathcal{C}_\Omega(\rho Q)^\perp)^*$ for subfield subcodes of AG codes on $\boldsymbol{C}_{ab}$. Let

$$A := \{\boldsymbol{c}(f) = \phi(f) : f \in \Gamma(\rho)\}.$$

---

[3] If $f_i = x^{k_i} y^{\ell_i} \neq f_j = x^{k_j} y^{\ell_j}$ then it is easily shown from $0 \leq \ell_i, \ell_j \leq a - 1$ that $\tau(f_i) \neq \tau(f_j)$.

[4] It is shown in [37] that $\dim V^0 \leq 1$ for this case. Since $1 = x^0 y^0 \in \Gamma(\rho' Q)$ for $\rho \geq 0$ and $\sigma(1) = 1$, we have $\sigma(\phi(1)) = \phi(1) \in V^0$. Thus $V^0 \neq \{\mathbf{0}\}$ which implies that $\dim V^0 = 1$.

Then by Proposition 2.2 and Eq.(2.2),

$$\langle A \rangle = \phi(L(\rho Q)) = \mathcal{C}_\Omega(\rho Q)^\perp \tag{4.17}$$

and therefore $\dim(\mathcal{C}_\Omega(\rho Q)^\perp)^* = \dim \langle A \rangle^*$.

4.5.2 Upper bound for $\dim \langle A \rangle^*$

In the following, we let $\rho' := \lfloor \rho/q \rfloor$ for given positive integer ρ.

Definition 4.2 Define Γ_1, Γ_2 by

$$\Gamma_1 := \Gamma(\rho'),\ \Gamma_2 := \Gamma(\rho) \setminus \Gamma(\rho'),$$

and let

$$A_i := \{\boldsymbol{c}(f) : f \in \Gamma_i\},\ (i = 1, 2).$$

□

Then by noting that $\Gamma(\rho) = \Gamma_1 \cup \Gamma_2$, we have

$$\langle A \rangle = \langle A_1 \rangle + \langle A_2 \rangle. \tag{4.18}$$

We further divide Γ_1 into the following three sets which are mutually disjoint.

Definition 4.3 Define Δ_i $(i = 1, 2, 3)$ by

$$\begin{aligned}
\Delta_1 &:= \{f \in \Gamma_1 : f^{q^{\xi_f}} \notin \Gamma_2, f = y^j\ (j \geq 0)\},\\
\Delta_2 &:= \{f \in \Gamma_1 : f^{q^{\xi_f}} \notin \Gamma_2, f \neq y^j\ (j \geq 0)\},\\
\Delta_3 &:= \{f \in \Gamma_1 : f^{q^{\xi_f}} \in \Gamma_2\},
\end{aligned}$$

where ξ_f $(f \in \Gamma(\rho))$ is

$$\xi_f := \begin{cases} 0, & \text{for } f = 1,\\ \max\{\xi : \tau(f^{q^\xi}) \leq \rho\}, & \text{for } f \neq 1, \end{cases}$$

and let

$$B_i := \{\boldsymbol{c}(f) : f \in \Delta_i\},\ (i = 1, 2, 3).$$

□

Then we have the following theorem.

Theorem 4.2 $\langle A\rangle^* = \langle B_1\rangle + \langle A_2\rangle^*$. □

In order to show this theorem, we need the following lemma.

Lemma 4.5

(i) $\langle A\rangle^* = \langle A_1\rangle + \langle A_2\rangle^*$.

(ii) $\langle B_3\rangle \subset \langle A_2\rangle^*$.

(iii) $\langle B_2\rangle \subset \langle A_2\rangle^*$.

(Proofs are given in Appendices 4A.1, 4A.2 and 4A.3.) □

(Proof of Theorem 4.2)

By Definition 4.3 and (ii) and (iii) of Lemma 4.5, we have

$$\langle A_1\rangle = \sum_{i=1}^{3} \langle B_i\rangle \subset \langle B_1\rangle + \langle A_2\rangle^*.$$

Hence by (i) of Lemma 4.5, we have

$$\langle A\rangle^* \subset \langle B_1\rangle + \langle A_2\rangle^* \ (\subset \langle A\rangle^*).$$

□

Denote $A_2 = \{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\mu\}$. Then $\langle A_2\rangle = \oplus_{i=1}^{\mu} T_i$, where $T_i := \langle\{\boldsymbol{c}_i\}\rangle$ and $\oplus$ denotes direct sum. For each $\boldsymbol{c}_i \in A_2$, we denote by $\nu(i)$ the smallest integer ν which satisfies

$$1 \le \nu \le m,\ \sigma^\nu(\boldsymbol{c}_i) \in \langle A_2\rangle.^5 \tag{4.19}$$

Then we have from Theorem 4.1 that

$$\langle A_2\rangle^* = \sum_{i=1}^{\mu} \sum_{j=0}^{\nu(i)-1} \sigma^j(T_i)$$

and

$$\dim \langle A_2\rangle^* \le \sum_{i=1}^{\mu} \nu(i) \le m|A_2|. \tag{4.20}$$

It is noted that the second equality in Eq.(4.20) holds *iff* $\nu(i) = m$ for $i = 1, 2, \ldots, \mu$.

For any $\boldsymbol{c}_i \in A_2$, we also denote by $\nu'(i)$ the smallest integer ν' which satisfies

$$1 \le \nu' \le m,\ \sigma^{\nu'}(\boldsymbol{c}_i) \in A_2.^5 \tag{4.21}$$

Then it is obvious that for all $\boldsymbol{c}_i \in A_2$, $\nu(i) \le \nu'(i)$ and we have from Eq.(4.20) that

$$\dim \langle A_2\rangle^* \le \sum_{i=1}^{\mu} \nu(i) \le \sum_{i=1}^{\mu} \nu'(i) \le m|A_2|,$$

which together with Theorem 4.2 yields:

[5] Since $\sigma^m(\boldsymbol{c}_i) = \boldsymbol{c}_i \in A_2 \subset \langle A_2\rangle$, we can always find ν and ν' that satisfy these conditions.

Theorem 4.3 For $\boldsymbol{c}_i \in A_2$, let $\nu'(i)$ be as defined above. Then

$$\dim(\mathcal{C}_\Omega(\rho Q)^\perp)^* = \dim \langle A \rangle^* \leq |B_1| + \sum_{i=1}^{\mu} \nu'(i), \tag{4.22}$$

where $\mu := |\Gamma_2|$. □

By noting that $|\Gamma(\rho)| - |\Gamma(\rho')| = |\Gamma_2| = |A_2|$ in Eq.(4.16), we have that the difference between two upper bounds given by Eqs.(4.16) and (4.22) is

$$\begin{aligned} & 1 + m\{|\Gamma(\rho)| - |\Gamma(\rho')|\} - \left\{ |B_1| + \sum_{i=1}^{\mu} \nu'(i) \right\} \\ & = \left(m|A_2| - \sum_{i=1}^{\mu} \nu'(i) \right) + 1 - |B_1|. \end{aligned} \tag{4.23}$$

As shown in Subsection 4.5.4, since $|B_1|$ ($\leq a$) is relatively small, we can make Eq.(4.23) positive in many cases and can get a tighter bound for $\dim((\mathcal{C}_\Omega(\rho Q)^\perp)^*)$ by Eq.(4.22) than that given by Eq.(4.16).

4.5.3 Computational complexity

Here we briefly evaluate the computational complexity, on the basis of arithmetic operations (additions/subtractions, multiplications/divisions and comparisons) in integers, required to calculate the proposed bound Eq.(4.22) by assuming that we are given $\Gamma(\rho)$. Eq.(4.22) would be calculated from $\Gamma(\rho)$ by:

(i) Dividing $\Gamma(\rho)$ into the disjoint union of Γ_1 and Γ_2. This, by the definition of $\Gamma(\rho)$ (Eq.(4.14)), requires arithmetic operations proportional to $|\Gamma(\rho)|$ at most.

(ii) Deciding $\Delta_1 \subset \Gamma_1$ in Definition 4.3 to get $|B_1| = |\Delta_1|$ in Eq.(4.22). This requires arithmetic operations proportional to $|\Gamma_1|$ at most (See Appendices 4A.4 for the detail).

(iii) Calculating $\nu'(i)$ for $\boldsymbol{c}_i \in A_2$, the smallest integer ν' which satisfies Eq.(4.21). As shown in Appendices 4A.4, $\nu'(i)$ is obtained directly from $f_i \in \Gamma_2$, and requires arithmetic operations proportional to $|\Gamma_2|m$.

(iv) Finally summing up $|\Delta_1| + \sum_{i=1}^{\mu} \nu'(i)$ to get Eq.(4.22). This requires arithmetic operations proportional to $\mu = |\Gamma_2|$.

Totally, the computational complexity for calculating Eq.(4.22) is evaluated as

$$\max\{\mathcal{O}(|\Gamma(\rho)|), \mathcal{O}(|\Gamma_2|m)\}. \tag{4.24}$$

On the other hand, if one try to find the true dimension of the same residue Goppa code by using Lemma 4.2, it may be the easiest way

(i) to obtain the set of vectors,

$$\{\sigma^j(\boldsymbol{c}(f_i)) : f_i \in \Gamma(\rho), j = 1, \ldots, m-1\}, \tag{4.25}$$

which spans $\langle A \rangle^*$ and

(ii) to calculate dim $\langle A \rangle^*$ as the rank of $m|\Gamma(\rho)| \times n$ matrix whose row vectors are $\sigma^j(\boldsymbol{c}(f_i))$ by Gaussian elimination.

It is obvious that the computational complexity for obtaining $\{\sigma^j(\boldsymbol{c}(f_i))\}$ from $\Gamma(\rho)$ is far small compared to the calculation of dim $\langle A \rangle^*$ by Gaussian elimination which requires

$$\min\{\mathcal{O}(|\Gamma(\rho)|^2 m^2 n), \mathcal{O}(|\Gamma(\rho)| m n^2)\} \tag{4.26}$$

arithmetic operations in F_{q^m} [9].

Roughly speaking, the computational complexity for calculating Eq.(4.22), which is given by Eq.(4.24), is much less ($\leq 1/n^2$ times) than that for calculating the true dimension by Gaussian elimination, which is given by Eq.(4.26).

Moreover, it is noted that only $\Gamma(\rho)$, or equivalently a, b and ρ, is required to calculate Eq.(4.22) while the whole parity check matrix, i.e., the vectors given in Eq.(4.25), is needed to calculate the true dimension by Gaussian elimination.

4.5.4 Numerical example

We consider a residue Goppa code $C_\Omega(\rho Q)$, which is constructed on the curve $x^{33}+y^2+y=0$ over $F_{2^{10}}$, and its subfield subcode over F_{2^2}. This curve is a hyper elliptic curve whose number of rational points reaches Hasse-Weil upper bound [19], 2049 in this case, and the code length is $n = 2048$.

In Fig.4.1, we compare two lower bounds, derived from Eq.(4.16) and Eq.(4.22) respectively, for the dimension of subfield subcode $C_\Omega(\rho Q)|_{F_{2^2}}$. The horizontal axis denotes the Feng-Rao designed distance $d_{\rm FR}$ of $C_\Omega(\rho Q)$ [21]. The lower bound for the dimension of subfield subcode of $C_\Omega(\rho Q)$ is improved for $d_{FR} \geq 4$.

In Fig.4.2, we magnifies the area in Fig.4.1 surrounded with dotted line and show for comparison the true dimension of the shortened BCH code over F_{2^2} with code length

2048 which is obtained by shortening the primitive BCH code over F_{2^2} with code length 4095. The horizontal axis in this case denotes the designed distance given by the BCH bound. We can see from Fig.4.2 that the proposed bound can exceed the true dimension of a shortened BCH code while the conventional one cannot.

4.6 Conclusion

In this chapter, we have introduced a lower bound for the dimension of subfield subcodes of linear codes which improves Stichtenoth's bound. We also presented a lower bound for the dimension of subfield subcodes of residue Goppa codes on C_{ab}, which exceeds the conventional lower bound given by Stichtenoth when the number of check symbols is not small.

We have also given a numerical example in which the proposed bound can exceed the true dimension of a shortened BCH code with the same code length and designed distance, while the conventional bound cannot.

Appendices

4A.1 Proof of Lemma 4.5-(i)

Since we have from Eq.(4.18) that $\langle A\rangle^* = \langle A_1\rangle^* + \langle A_2\rangle^*$, it is sufficient to show that

$$\sigma^\ell(\langle A_1\rangle) \subset \langle A_1\rangle + \langle A_2\rangle^* \quad \text{for } \ell = 1, \ldots, m-1,$$

which is proved by induction on ℓ.

(i) In the case $\ell = 1$: Since $\tau(f^q) = q\tau(f) \leq \rho$ for all $f \in L(\rho' Q)$ where $\rho' = \lfloor \rho/q \rfloor$, $f^q \in L(\rho Q)$. Then by noting that $\langle A_1\rangle = \phi(L(\rho' Q))$, we have from Eqs.(4.1), (4.17) and (4.18) that

$$\begin{aligned}\sigma(\langle A_1\rangle) &= \{\boldsymbol{c}(f^q) : f \in L(\rho' Q)\} \\ &\subset \phi(L(\rho Q)) = \langle A_1\rangle + \langle A_2\rangle \subset \langle A_1\rangle + \langle A_2\rangle^*.\end{aligned}$$

(ii) Assume $\sigma^\ell(\langle A_1\rangle) \subset \langle A_1\rangle + \langle A_2\rangle^*$ $(\ell \geq 1)$. Then by noting that $\sigma(\langle A_2\rangle^*) \subset \langle A_2\rangle^*$ we immediately have

$$\sigma^{\ell+1}(\langle A_1\rangle) \subset \sigma(\langle A_1\rangle) + \sigma(\langle A_2\rangle^*) \subset \langle A_1\rangle + \langle A_2\rangle^*.$$

(Q.E.D.)

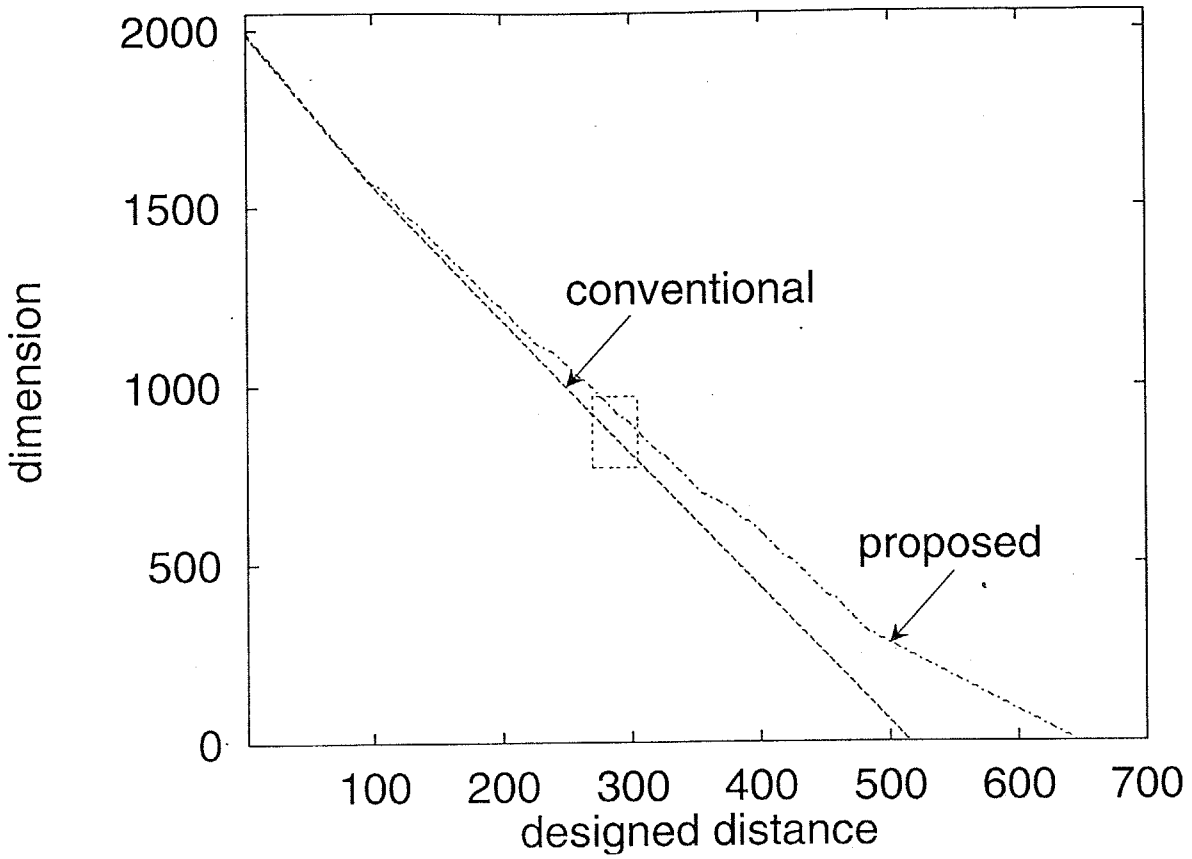

Figure 4.1: Comparison of the proposed and conventional lower bounds for the dimension of subfield subcodes.

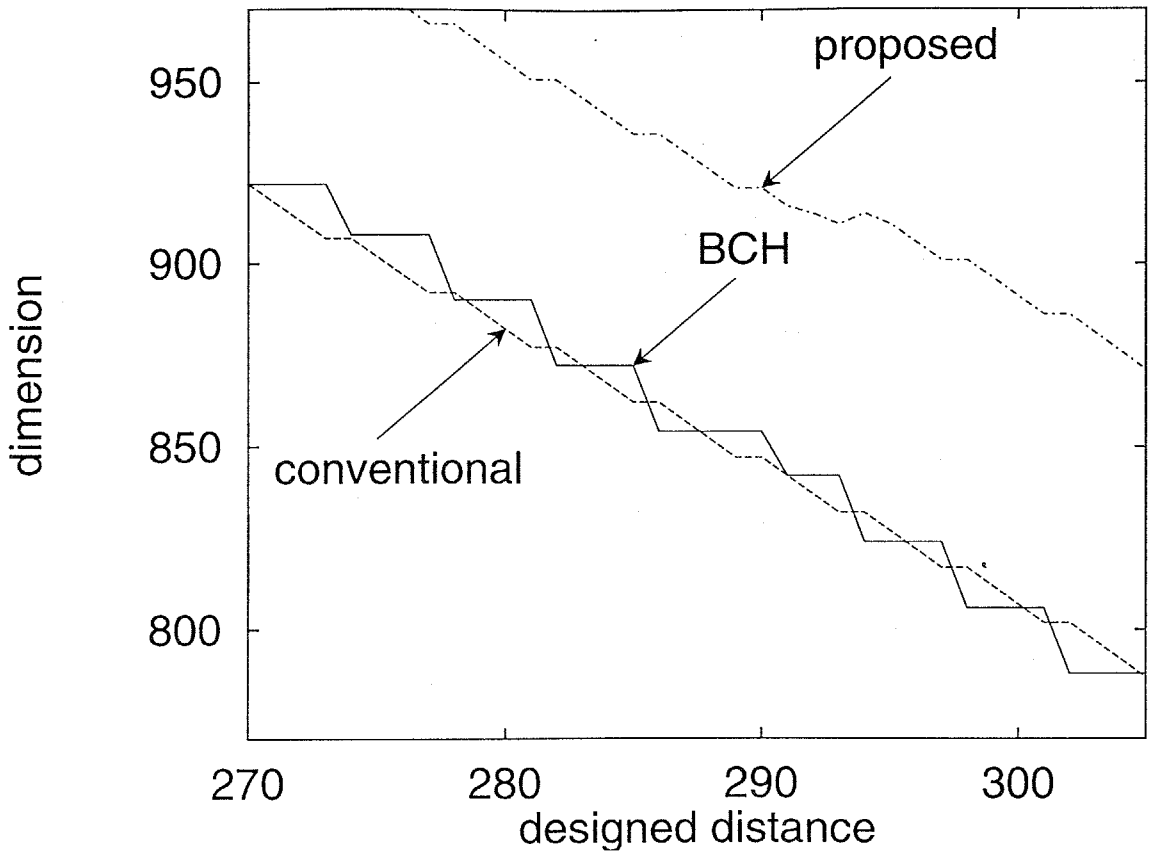

Figure 4.2: Magnification of Fig.4.1.

4A.2 Proof of Lemma 4.5-(ii)

For $f \in \Delta_3$, let $g := f^{q^{\xi_f}} \in \Gamma_2$. Then $\boldsymbol{c}(g) \in \langle A_2 \rangle$ and $\sigma^{m-\xi_f}(\boldsymbol{c}(g)) \in \langle A_2 \rangle^*$. On the other hand, we have

$$\sigma^{m-\xi_f}(\boldsymbol{c}(g)) = \boldsymbol{c}(g^{q^{m-\xi_f}}) = \boldsymbol{c}(f^{q^m}) = \boldsymbol{c}(f).$$

Thus $\boldsymbol{c}(f) \in \langle A_2 \rangle^*$ for all $f \in \Delta_3$. Since any element in $\langle B_3 \rangle$ is expressed as a linear combination of $\{\boldsymbol{c}(f) : f \in \Delta_3\}$, we have $\langle B_3 \rangle \subset \langle A_2 \rangle^*$. (Q.E.D.)

4A.3 Proof of Lemma 4.5-(iii)

To prove Lemma 4.5-(iii), we first show a couple of lemmas.

Lemma 4A.1 Any $f \in \Delta_2$ is written as $f = x^s y^t$ with $s, t \geq 1$.

(Proof) Note first that we have $\lfloor \rho/q \rfloor < \tau(f^{q^{\xi_f}}) \leq \rho$, for all $f \in \Gamma(\rho) \setminus \{1\}$ from the definition of ξ_f.[6]

It is obvious from the definition of Δ_2 that $f \in \Delta_2$ is written as $f = x^s y^t$ with $s \geq 1$ and $t \geq 0$. Assume $t = 0$ then $f^{q^{\xi_f}} = x^{sq^{\xi_f}}$. Since $\deg f^{q^{\xi_f}}$ with respect to y is 0 $(< a)$ and $\tau(x^{sq^{\xi_f}}) \leq \rho$, we have $x^{sq^{\xi_f}} \in \Gamma(\rho)$ by the definition of $\Gamma(\rho)$ (Eq.(2.6)). Moreover, since $\lfloor \rho/q \rfloor < \tau(x^{sq^{\xi_f}})$, we have $x^{sq^{\xi_f}} \in \Gamma_2$ by Definition 4.2. This contradicts with the fact that $f \in \Delta_2$ and therefore $t \geq 1$. □

Lemma 4A.2 For $f \in \Delta_2$, f^{q^ℓ} $(\ell = 1, 2, \ldots)$ can be expressed as

$$\left.\begin{aligned} f^{q^\ell} &= \sum_{\gamma=1}^{\ell} \left(\sum_i a_{\gamma,i} g_{\gamma,i} \right)^{q^{\ell-\gamma}} + \sum_i b_{\ell,i} h_{\ell,i}, \\ & g_{\gamma,i} \in \Gamma_2 \cup \Delta_3, \ h_{\ell,i} \in \Delta_2 \end{aligned}\right\} \tag{4A.1}$$

where $a_{\gamma,i}, b_{\ell,i} \in F_{q^m}$ [7] and $h_{\ell,i} \neq f$.

(Proof) By induction on ℓ.

---

[6] $\tau(f^{q^{\xi_f}}) \leq \rho$ is obvious by the definition of ξ_f. Assume $\tau(f^{q^{\xi_f}}) \leq \lfloor \rho/q \rfloor$, then we have

$$\tau(f^{q^{\xi_f+1}}) = q\tau(f^{q^{\xi_f}}) \leq q\lfloor \rho/q \rfloor \leq \rho,$$

which contradicts the definition of ξ_f.

[7] All coefficients which appear in Appendices 4A.3 belong to F_{q^m}. So hereafter we do not mention it every time.

(1) In the case $\ell = 1$. By Lemma 4A.1, $f \in \Delta_2$ is written as $f = x^s y^t$ $(s, t \geq 1)$. For this $f = x^s y^t$, let $\tau_y := \tau(y^{tq})$. Then we have $y^{tq} \in L(\tau_y Q)$ and $y^{tq} \notin L((\tau_y - 1)Q)$. Therefore y^{tq} is expressed as

$$y^{tq} = \sum_{i=1}^{k} a_i f_i,\ f_i \in \Gamma(\tau_y),\ a_k \neq 0,$$

where $\tau(f_k) = \tau_y$ and $f_1, \ldots, f_k$ are the first k elements of $\{f_1, f_2, \ldots, f_r\}$ in Eq.(4.15). Thus f^q is expressed as

$$\left.\begin{aligned} f^q = x^{sq} y^{tq} = \sum_{i=1}^{k} a_i x^{sq} f_i, \\ f_i \in \Gamma(\tau_y),\ a_k \neq 0. \end{aligned}\right\} \tag{4A.2}$$

Since $\deg f_i$ $(i = 1, 2, \ldots, k)$ with respect to y is less than a by Proposition 2.2, so is $\deg x^{sq} f_i$ $(i = 1, 2, \ldots, k)$. Moreover, since

$$\tau(x^{sq} f_i) \leq \tau(x^{sq} f_k) = asq + \tau(f_k) = \tau(f^q) \leq \rho,$$

we have $x^{sq} f_i \in \Gamma(\rho)$ for $i = 1, 2, \ldots, k$ by Proposition 2.2. Therefore by classifying each $x^{sq} f_i \in \Gamma(\rho)$ into $\Gamma_2 \cup \Delta_3$ and $\Delta_1 \cup \Delta_2$, we can rewrite Eq.(4A.2) as

$$\left.\begin{aligned} f^q = \sum_i a_{1,i} g_{1,i} + \sum_i b_{1,i} h_{1,i}, \\ g_{1,i} \in \Gamma_2 \cup \Delta_3,\ h_{1,i} \in \Delta_1 \cup \Delta_2. \end{aligned}\right\} \tag{4A.3}$$

Since $h_{1,i}$ equals $x^{sq} f_j$ $(s \geq 1)$ for some j, we have from Definition 4.3 that $h_{1,i} \notin \Delta_1$ i.e. $h_{1,i} \in \Delta_2$.

Finally assume that $f = x^s y^t$ $(s, t \geq 1)$ equals $h_{1,i} = x^{sq} f_j = x^{sq} x^{s_j} y^{t_j}$ $(s_j, t_j \geq 0)$, then we must have $s = sq + s_j$. But this is possible only when $s = s_j = 0$ which contradicts with $s \geq 1$. Thus $f \neq h_{1,i}$ for all i.

(2) Assume that this lemma holds for ℓ (≥ 1). Then we have from Eq.(4A.1) that

$$\begin{aligned} f^{q^{\ell+1}} &= \sum_{\gamma=1}^{\ell} \left(\sum_i a_{\gamma,i} g_{\gamma,i} \right)^{q^{\ell+1-\gamma}} + \left(\sum_i b_{\ell,i} h_{\ell,i} \right)^q \\ &= \sum_{\gamma=1}^{\ell} \left(\sum_i a_{\gamma,i} g_{\gamma,i} \right)^{q^{\ell+1-\gamma}} + \sum_i b_{\ell,i}^q h_{\ell,i}^q. \end{aligned}$$

Therefore in order to show that Eq.(4A.1) holds for $\ell + 1$, it is sufficient to show that $h_{\ell,i}^q$ can be expressed as

$$\left.\begin{aligned} h_{\ell,i}^q = \sum_j a_{\ell+1,j} g_{\ell+1,j} + \sum_j b_{\ell+1,j} h_{\ell+1,j} \\ g_{\ell+1,j} \in \Gamma_2 \cup \Delta_3,\ h_{\ell+1,j} \in \Delta_2 \end{aligned}\right\} \tag{4A.4}$$

where $h_{\ell+1,j} \neq f$.

Since $h_{\ell,i} \in \Delta_2$ by assumption, we can substitute $h_{\ell,i}$ for f of Eq.(4A.1) with $\ell = 1$, which proves Eq.(4A.4).

To show $h_{\ell+1,j} \neq f$, we give the following claim.

(Claim) In Eq.(4A.1), $h_{\ell,i}$ $(\ell \geq 1)$ is expressed as

$$h_{\ell,i} = x^{sq^\ell} x^{s_{\ell,i}} y^{t_{\ell,i}}, \ \ s \geq 1, \ s_{\ell,i}, t_{\ell,i} \geq 0. \tag{4A.5}$$

Suppose in Eq.(4A.4) that $f = x^s y^t$ $(s, t \geq 1)$ equals $h_{\ell+1,j}$. Then since $h_{\ell+1,j} = x^{sq^{\ell+1}} x^{s_{\ell+1,j}} y^{t_{\ell+1,j}}$ by Eq.(4A.5), $f = h_{\ell+1,j}$ implies $s = sq^{\ell+1} + s_{\ell+1,j}$. But this is possible only when $s = s_{\ell+1,j} = 0$ which contradicts with $s \geq 1$. Thus $h_{\ell+1,j} \neq f$.

To conclude the proof of Lemma 4A.2, we give the proof of the claim.

(Proof of Claim) We have already shown just after Eq.(4A.3) that Eq.(4A.5) hold for $\ell = 1$.

Assume that Eq.(4A.5) holds for ℓ (≥ 1). Then since $h_{\ell,i} \in \Delta_2$, we have by the same argument which derives Eq.(4A.2) that

$$\left.\begin{aligned} h_{\ell,i}^q = (x^{sq^\ell} x^{s_{\ell,i}} y^{t_{\ell,i}})^q = \sum_{j=1}^{k'} a_j x^{(sq^\ell + s_{\ell,i})q} f_j, \\ f_j \in \Gamma(\tau'_y), \ a_{k'} \neq 0, \end{aligned}\right\} \tag{4A.6}$$

where $\tau'_y := \tau(y^{qt_{\ell,i}})$ and $f_1, \ldots, f_{k'}$ with $\tau(f_{k'}) = \tau'_y$ are the first k' elements of $\{f_1, \ldots, f_r\}$ in Eq.(4.15). Since Eq.(4A.6) is equal to Eq.(4A.4), we have $h_{\ell+1,i} = x^{(sq^\ell + s_{\ell,i})q} f_j$ for some $f_j = x^{k_j} y^{\ell_j}$, which means $s_{\ell+1,i} = s_{\ell,i} q + k_j$ and $t_{\ell+1,i} = \ell_j$ and Eq.(4A.5) holds for $\ell + 1$.

□

It was shown in Lemma 4A.2 that f^{q^ℓ} is expressed as the sum of two major terms: the first term is the sum of $g^{\ell-\gamma}$-th power of a linear combination of elements in $\Gamma_2 \cup \Delta_3$ and the second is the linear combination of elements in $\Delta_2 \setminus \{f\}$. Moreover, as is shown below, the second term in the expression of f^{q^ℓ} vanishes for sufficiently large ℓ.

Lemma 4A.3 Let $E_\ell := \{h_{\ell,i}\}_i \subset \Delta_2$ in Eq.(4A.1). Then $E_\ell = \emptyset$ for all $\ell > |\Delta_2|$. In other words, there exists an integer $k \leq |\Delta_2| + 1$ such that

$$f^{q^\ell} = \sum_{\gamma=1}^{k} \left(\sum_i a_{\gamma,i} g_{\gamma,i} \right)^{q^{\ell-\gamma}}, \ g_{\gamma,i} \in \Gamma_2 \cup \Delta_3 \tag{4A.7}$$

for all $\ell \geq k$.

(Proof) It is sufficient to show that Eq.(4A.7) holds for $\ell = k$ with some $k \leq |\Delta_2| + 1$.

We consider the tree of functions in Δ_2 generated as follows. Put given $f \in \Delta_2$ on the first level vertex or the root of the tree. Take f^q to get $E_1 = \{h_{1,i}\}_i \subset \Delta_2$ by Eq.(4A.1) and put these $h_{1,i}$ on the second level vertices of the tree. Next, for each h_{1,i_2} ($\in \Delta_2$) attached to the second level vertices, take h_{1,i_2}^q. Then by Eq.(4A.1), h_{1,i_2}^q is expressed as a linear sum of functions in $\Gamma_2 \cup \Delta_3$ and in Δ_2. Denote the functions in Δ_2 by $h_{(1,i_2),i}$ and put these $h_{(1,i_2),i}$ (for all i_2 and i) on the third level vertices of the tree. Note here that if we define $E_{(1,i_2)} := \{h_{(1,i_2),i}\}_i$, we obviously have

$$\bigcup_{i_2} E_{(1,i_2)} \supset E_2 = \{h_{2,i}\}_i.$$

In general, for each function attached to the $(j-1)$-th level vertices of the tree, which we denote by $h_{((1,i_2),i_3,\ldots,i_{j-1}),i_j}$, take its q-th power as above. Then by Eq.(4A.1) again, $h^q_{((1,i_2),i_3,\ldots,i_{j-1}),i_j}$ is expressed as a linear sum of functions in $\Gamma_2 \cup \Delta_3$ and in Δ_2, the latter we denote by $h_{((1,i_2),i_3,\ldots,i_j),i}$. Let $E_{((1,i_2),i_3\ldots,i_j)} := \{h_{((1,i_2)i_3,\ldots,i_j),i}\}_i$, then we have

$$\bigcup_{i_2,i_3,\ldots,i_j} E_{((1,i_2),i_3,\ldots,i_j)} \supset E_j = \{h_{j,i}\}_i.$$

Thus in order to show $E_\ell = \emptyset$ for $\ell > |\Delta_2|$, it is sufficient to show that

$$E_{((1,i_2),i_3,\ldots,i_\ell)} = \emptyset \text{ for all } i_2, i_3, \ldots, i_\ell,\ \ell > |\Delta_2|.$$

Let

$$f \to h_{1,i_2} \to h_{(1,i_2),i_3} \to \cdots \to h_{((1,i_2),i_3,\ldots,i_{\ell-1}),i_\ell}$$

represent a path from the root to a vertex in the ℓ-th level of the tree. Then by Lemma 4A.2, we have

$$\left.\begin{aligned}
&f \neq h_{1,i_2}, h_{(1,i_2),i_3}, \ldots, h_{((1,i_2),i_3,\ldots,i_{\ell-1}),i_\ell},\\
&h_{1,i_2} \neq h_{(1,i_2),i_3}, h_{((1,i_2),i_3),i_4}, \ldots,\\
&\qquad\qquad h_{((1,i_2),i_3,\ldots,i_{\ell-1}),i_\ell},\\
&h_{(1,i_2),i_3} \neq h_{((1,i_2),i_3),i_4}, \ldots, h_{((1,i_2),i_3,\ldots,i_{\ell-1}),i_\ell},\\
&\qquad\vdots\\
&h_{((1,i_2),i_3,\ldots,i_{\ell-2}),i_{\ell-1}} \neq h_{((1,i_1),i_2,\ldots,i_{\ell-1}),i_\ell}.
\end{aligned}\right\}$$

This implies that all functions

$$f, h_{1,i_2}, h_{(1,i_2)i_3}, \ldots, h_{((1,i_2),i_3,\ldots,i_{\ell-1}),i_\ell} \in \Delta_2$$

on the path differ each other. Since $|\Delta_2|$ is finite, this means any path must terminate at a vertex with level not greater than $|\Delta_2|$. This proves

$$E_{((1,i_2),i_3,\ldots,i_k)} = \{h_{((1,i_2),i_3,\ldots,i_k),i}\}_i = \emptyset \text{ for some } k \leq |\Delta_2| + 1.$$

Hence $E_\ell = \emptyset$ for all $\ell > |\Delta_2|$ and Eq.(4A.7) holds. □

(Proof of Lemma 4.5-(iii))

We have from Eq.(4A.7) that for all $f \in \Delta_2$,

$$\left.\begin{aligned} \boldsymbol{c}(f^{q^k}) = \boldsymbol{c}\left(\sum_{\gamma=1}^{k}\left(\sum_i a'_{\gamma,i}g'_{\gamma,i} + \sum_i a''_{\gamma,i}g''_{\gamma,i}\right)^{q^{k-\gamma}}\right) \\ g'_{\gamma,i} \in \Gamma_2,\ g''_{\gamma,i} \in \Delta_3 \text{ for some } k \leq |\Delta_2| + 1. \end{aligned}\right\}$$

Applying to this expression the relationship

$$\boldsymbol{c}(f^{q^k}) = \sigma^k(\boldsymbol{c}(f)) \text{ for all } f \in L(\rho Q),\ k = 0, 1, 2, \ldots, \tag{4A.8}$$

which is an immediate consequence of the definition of Frobenius automorphism σ, and the trivial relation $\boldsymbol{c}(f_1 + f_2) = \boldsymbol{c}(f_1) + \boldsymbol{c}(f_2)$ for all $f_1, f_2 \in L(\rho Q)$, we have

$$\begin{aligned} \boldsymbol{c}(f^{q^k}) &= \sum_{\gamma=1}^{k} \sigma^{k-\gamma}\left(\boldsymbol{c}\left(\sum_i a'_{\gamma,i}g'_{\gamma,i} + \sum_i a''_{\gamma,i}g''_{\gamma,i}\right)\right) \\ &= \sum_{\gamma=1}^{k} \sigma^{k-\gamma}\left(\sum_i a'_{\gamma,i}\boldsymbol{c}(g'_{\gamma,i}) + \sum_i a''_{\gamma,i}\boldsymbol{c}(g''_{\gamma,i})\right) \\ &\in \sum_{\gamma=1}^{k} \sigma^{k-\gamma}(\langle A_2\rangle + \langle B_3\rangle). \end{aligned}$$

This, by Lemma 4.5-(ii), implies

$$\boldsymbol{c}(f^{q^k}) \in \sum_{\gamma=1}^{k} \sigma^{k-\gamma}(\langle A_2\rangle^*) \subset \langle A_2\rangle^*$$

and therefore by using Eq.(4A.8) we have

$$\begin{aligned} \boldsymbol{c}(f) &= \sigma^{-k}(\boldsymbol{c}(f^{q^k})) \\ &\in \sigma^{-k}(\langle A_2\rangle^*) \subset \langle A_2\rangle^* \text{ for all } f \in \Delta_2. \end{aligned}$$

Finally, since $B_2 = \{\boldsymbol{c}(f) : f \in \Delta_2\}$, we immediately have $\langle B_2\rangle \subset \langle A_2\rangle^*$. (Q.E.D.)

4A.4 Computational complexity

Let c_a, c_s, c_m, c_d and c_c represent the unit complexities of addition, subtraction, multiplication, division and comparison in integers, respectively.

In (ii), we need to examine whether $y^i \in \Delta_1$ or not for $y^i \in \Gamma_1 \setminus \{1\}$ [8] which is tested if $iq^\ell \geq a$ holds or not for ℓ such that $\rho' < \tau(y^{iq^\ell}) = biq^\ell \leq \rho$. This test is realized by:

Step.1 Let $\tau := \tau(y^i) = ib$.

Step.2 $\tau := \tau q$.

Step.3 If $\tau \leq \rho'$ then go to Step.2.

Step.4 If $\tau/b \geq a$ then $y^i \in \Delta_1$, else $y^i \notin \Delta_1$.

By noting that Step.2 and 3 are repeated at most $\lfloor \log_q(\rho/ib) \rfloor$ times, the total arithmetic operations required for (ii) is at most

$$|\Gamma_1 - 1|\Big\{c_m + \lfloor \log_q(\rho/ib) \rfloor (c_m + c_c) + c_d + c_c\Big\}.$$

In (iii), we need to decide $\nu'(i)$ given in Eq.(4.21) for each $\boldsymbol{c}_i \in A_2$, i.e., $\boldsymbol{c}_i = \boldsymbol{c}(g_i)$, $g_i = x^{k_i} y^{\ell_i} \in \Gamma_2$, which is done by:

Step.1 Let $\nu := 1$, $M := q^m - 1$ and for $g_i = x^{k_i} y^{\ell_i}$, let $k := k_i$, $\ell := \ell_i$.

Step.2 Let $k := [kq]_M$ and $\ell := [\ell q]_M$ where $[x]_y$ $(0 \leq [x]_y < y)$ denotes the remainder of x divided by y.

Step.3 If $\rho' < ak + b\ell \leq \rho$ and $\ell < a$, then $\nu'(i) := \nu$, else let $\nu := \nu + 1$ and go to Step.2.

Each step requires $mc_m + c_s$, $2(c_s + 2c_m + c_d)$ [9] and $c_a + 2c_m + 3c_c$ arithmetic operations, respectively. Thus by noting that Step.2 and 3 are repeated at most m times, calculating $\nu'(i)$ for all $g_i \in \Gamma_2$ requires

$$\begin{aligned} &|\Gamma_2|\Big[mc_m + c_s + m\{2(c_s + 2c_m + c_d) + c_a + 2c_m + 3c_c\}\Big] \\ &= |\Gamma_2|\{mc_a + (2m+1)c_s + 7mc_m + 2mc_d + 3mc_c\} \end{aligned}$$

arithmetic operations.

---

[8] Since $1 \in \Delta_1$ is obvious, it is sufficient to consider $y^i \in \Gamma_1 \setminus \{1\}$.

[9] $[kq]_M$ is calculated by $kq - \lfloor kq/M \rfloor M$.

Chapter 5

A Lower Bound for Generalized Hamming Weights

5.1 Introduction

In this chapter, we first introduce a lower bound for the generalized Hamming weights of arbitrary linear code in terms of the notion of well-behaving. We only assume that we are given a sequence of vectors, $B := \{\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_n\}$, which is a basis of F_q^n and whose first $n-k$ elements constitute the row vectors of a parity check matrix of the $[n,k]$ code C. Next, we introduce a parameter $g_B(C)$, which is uniquely determined from the basis B, and show that any linear code C is the t-th rank MDS for $g_B(C)+1 \leq t \leq k$ which, compared to the conventional sufficient conditions [41], gives a new type of sufficient condition for the t-th rank MDS codes.

Finally, we apply our result to some well-known codes, i.e., Reed-Solomon (RS) codes, Reed-Muller (RM) codes and AG codes on the curve $\boldsymbol{C}_{ab}$. Then we show that $g_B(C)$ for RS and RM codes can be determined explicitly and the range of t for which these codes are the t-th rank MDS is the same as the conventional result. As for AG codes on $\boldsymbol{C}_{ab}$, we show that $g_B(C)$ is upper bounded by the genus of the curve $\boldsymbol{C}_{ab}$ and the range of t for which the code is the t-th rank MDS is wider than the conventional result.

5.2 Preliminaries

For a subset A of F^n, we denote by $Supp\,(A)$ the support of A, i.e.,

$$Supp\,(A) := \{i : 1 \leq i \leq n,\ c_i \neq 0 \text{ for some } \boldsymbol{c} = (c_1, c_2, \ldots, c_n) \in A\}.$$

Definition 5.1 [42] Let C be an $[n, k]$ linear code over F. We denote by $\mathcal{D}_t$ the set of all t-dimensional subcodes of C for $1 \leq t \leq k$. Then the t-th generalized Hamming weight of C is defined by

$$d_t(C) := \min\{|Supp\,(D)| : D \in \mathcal{D}_t\}, \tag{5.1}$$

where $|S|$ denotes the cardinality of a set S. □

The following results for the generalized Hamming weights are well known.

Proposition 5.1 [42, 47] For any linear $[n, k]$ code C over F, we have:

(i) Monotonicity:

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n.$$

(ii) Generalized Singleton bound:

$$d_t(C) \leq n - k + t \text{ for all } t, 1 \leq t \leq k.$$

(iii) Duality: Let $C^\perp$ be the dual code of C. Then

$$\{d_t(C)\}_{t=1}^{k} \cup \{n + 1 - d_t(C^\perp)\}_{t=1}^{n-k} = \{1, 2, \ldots, n\}.$$

□

Hereafter, let $B := \{\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_n\}$ denote a basis of F^n. It is noted that when we say that B is a basis of F^n, we include the order of $\boldsymbol{h}_i$'s in B.

We denote by $L_i := \langle \boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_i \rangle$ $(1 \leq i \leq n)$ the linear space over F spanned by $\{\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_i\}$, the first i elements of B, and let $L_0 := \{\boldsymbol{0}\}$.

For $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ and $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ in F^n, $\boldsymbol{u} \cdot \boldsymbol{v}$ denotes inner product of $\boldsymbol{u}$ and $\boldsymbol{v}$, that is, $\boldsymbol{u} \cdot \boldsymbol{v} := \sum_{i=1}^{n} u_i v_i$.

Definition 5.2 For $\{\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_r\} \subset B$ $(1 \leq r \leq n)$, we define $[n, n-r]$ code C_r by

$$\begin{aligned} C_r &:= L_r^{\perp} = \langle \boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_r \rangle^{\perp} \\ &= \{\boldsymbol{c} \in F^n : \boldsymbol{c} \cdot \boldsymbol{h}_i = 0 \text{ for all } i = 1, 2, \ldots, r\}. \end{aligned}$$

□

Definition 5.2 means that $\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_r$ are the row vectors of a parity check matrix of C_r.

Definition 5.3 For given $D \in \mathcal{D}_t$, we define an F-linear map $\theta_D : F^n \to F^n$, $\boldsymbol{v} = (v_1, v_2, \ldots, v_n) \mapsto \boldsymbol{v}^D = (v_1^D, v_2^D, \ldots, v_n^D)$ by

$$v_i^D := \begin{cases} v_i, & \text{if } i \in Supp\,(D), \\ 0, & \text{if } i \notin Supp\,(D). \end{cases}$$

□

For $D \in \mathcal{D}_t$, we denote by $S_i^D := \langle \boldsymbol{h}_1^D, \boldsymbol{h}_2^D, \ldots, \boldsymbol{h}_i^D \rangle$ $(1 \leq i \leq n)$ the linear space over F spanned by $\{\boldsymbol{h}_1^D, \boldsymbol{h}_2^D, \ldots, \boldsymbol{h}_i^D\}$ and let $S_0^D := \{\boldsymbol{0}\}$. In general, vectors $\boldsymbol{h}_1^D, \boldsymbol{h}_2^D, \ldots, \boldsymbol{h}_n^D$ are not necessarily linearly independent and $\dim S_i^D \leq i$.

Proposition 5.2 For any $D \in \mathcal{D}_t$, $|Supp\,(D)| = \dim S_n^D$.

(Proof) It is obvious that

$$\mathrm{Ker}(\theta_D) = \{\boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in F^n : v_i = 0 \text{ for all } i \in Supp\,(D)\}.$$

This implies that $\dim(\mathrm{Ker}(\theta_D)) = n - |Supp\,(D)|$. Since $\{\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_n\}$ is a basis of F^n, we see $S_n^D = \mathrm{Im}(\theta_D)$. Thus we have

$$\dim S_n^D = \dim(\mathrm{Im}(\theta_D)) = \dim(F^n) - \dim(\mathrm{Ker}(\theta_D)) = |Supp\,(D)|.$$

□

For $\boldsymbol{u} = (u_1, u_2, \ldots, u_n), \boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in F^n$, we denote $\boldsymbol{u} * \boldsymbol{v} := (u_1 v_1, u_2 v_2, \ldots, u_n v_n) \in F^n$.

Definition 5.4 [5, 23] We define the map $\rho : F^n \to \{0, 1, 2, \ldots, n\}$ by

$$\rho(\boldsymbol{v}) := \begin{cases} 0, \text{ if } \boldsymbol{v} = \boldsymbol{0}, \\ k, \text{ if } \boldsymbol{v}(\neq \boldsymbol{0}) \in L_k \setminus L_{k-1}. \end{cases}$$

A pair $(\boldsymbol{h}_i, \boldsymbol{h}_j)$ $(\boldsymbol{h}_i, \boldsymbol{h}_j \in B,\ 1 \leq i, j \leq n)$ is said to be *well-behaving* if $\rho(\boldsymbol{h}_u * \boldsymbol{h}_v) < \rho(\boldsymbol{h}_i * \boldsymbol{h}_j)$ for all $\boldsymbol{h}_u, \boldsymbol{h}_v \in B$ with $1 \leq u \leq i, 1 \leq v \leq j$ and $u + v < i + j$. □

For each $\boldsymbol{h}_i \in B$, we define

$$\begin{aligned}\Lambda_i := \{k : k \in \{0,1,2,\ldots,n\} \text{ such that } k = \rho(\boldsymbol{h}_i * \boldsymbol{h}_j) \\ \text{where } \boldsymbol{h}_j \in B \text{ and } (\boldsymbol{h}_i, \boldsymbol{h}_j) \text{ is well-behaving}\}.\end{aligned} \tag{5.2}$$

For a subset T of $\{1,2,\ldots,r\}$, we also define

$$\left.\begin{aligned}\Lambda_T &:= \bigcup_{i\in T} \Lambda_i, \\ \Lambda_T^* &:= \{r+1, r+2, \ldots, n\} \setminus \Lambda_T.\end{aligned}\right\} \tag{5.3}$$

For given $D \in \mathcal{D}_t$, let

$$T_D := \{i : 1 \le i \le r, \boldsymbol{h}_i^D \in S_{i-1}^D\}.$$

Remark 5.1 It can be seen from Definition 5.4 that ρ depends on B and the order of $\boldsymbol{h}_i$'s in B. Thus so do Λ_i, Λ_T and Λ_T^*. □

5.3 A lower bound for generalized Hamming weights and condition for t-th rank MDS

5.3.1 A lower bound for generalized Hamming weights

Let $\mathcal{D}_t$ be the set of all t-dimensional subcodes of C_r with $1 \le t \le n-r$. For $D \in \mathcal{D}_t$ and a linear subspace $W \subset F^n$, we define $W^{\perp_D}$ by

$$W^{\perp_D} := \{\boldsymbol{v} \in F^n : Supp(\boldsymbol{v}) \subset Supp(D) \qquad \text{and } \boldsymbol{v}\cdot\boldsymbol{u} = 0 \text{ for all } \boldsymbol{u} \in W\}.$$

Since $D \subset C_r$, for all $\boldsymbol{c} = (c_1, c_2, \ldots, c_n) \in D$ and $\boldsymbol{h}_i = (h_{i1}, h_{i2}, \ldots, h_{in})$ $(1 \le i \le r)$, we have

$$0 = \boldsymbol{c}\cdot\boldsymbol{h}_i = \sum_{j=1}^{n} c_j h_{ij} = \sum_{j\in Supp(D)} c_j h_{ij} = \boldsymbol{c}\cdot\boldsymbol{h}_i^D,$$

which means

$$D \subset \langle \boldsymbol{h}_1^D, \boldsymbol{h}_2^D, \ldots, \boldsymbol{h}_r^D\rangle^{\perp_D} = (S_r^D)^{\perp_D}. \tag{5.4}$$

In order to derive a lower bound of generalized Hamming weights, we need a couple of lemmas.

Lemma 5.1 For any $D \in \mathcal{D}_t$, there exist at least t elements $\boldsymbol{h}_i^D$'s in $\{\boldsymbol{h}_{r+1}^D, \boldsymbol{h}_{r+2}^D, \ldots, \boldsymbol{h}_n^D\}$ such that $\boldsymbol{h}_i^D \notin S_{i-1}^D$, $r+1 \le i \le n$.

(Proof) Assume that there exist only μ ($\leq t-1$) elements, denoted by $\boldsymbol{h}_{i_1}^D, \boldsymbol{h}_{i_2}^D, \ldots, \boldsymbol{h}_{i_\mu}^D$, in $\{\boldsymbol{h}_{r+1}^D, \boldsymbol{h}_{r+2}^D, \ldots, \boldsymbol{h}_n^D\}$ which satisfy $\boldsymbol{h}_{i_j}^D \notin S_{i_j-1}^D$. Then we can write

$$S_n^D = S_r^D + \langle \boldsymbol{h}_{r+1}^D, \boldsymbol{h}_{r+2}^D, \ldots, \boldsymbol{h}_n^D \rangle = S_r^D \oplus \langle \boldsymbol{h}_{i_1}^D, \ldots, \boldsymbol{h}_{i_\mu}^D \rangle \tag{5.5}$$

where $\oplus$ denotes *direct sum*. Hence, by noting that $\dim S_n^D = \dim S_r^D + \dim (S_r^D)^{\perp_D}$, we have from Eqs.(5.4) and (5.5) that

$$\begin{aligned} \dim D &\leq \dim (S_r^D)^{\perp_D} = \dim S_n^D - \dim S_r^D \\ &= \dim \langle \boldsymbol{h}_{i_1}^D, \ldots, \boldsymbol{h}_{i_\mu}^D \rangle = \mu \leq t-1 \end{aligned}$$

which contradicts with $\dim D = t$. □

Lemma 5.2 Let $(\boldsymbol{h}_i, \boldsymbol{h}_j)$ $(\boldsymbol{h}_i, \boldsymbol{h}_j \in B)$ be well-behaving and $k := \rho(\boldsymbol{h}_i * \boldsymbol{h}_j)$. For given $D \in \mathcal{D}_t$, if $\boldsymbol{h}_i^D \in S_{i-1}^D$ or $\boldsymbol{h}_j^D \in S_{j-1}^D$, then $\boldsymbol{h}_k^D \in S_{k-1}^D$.

(Proof) Since $k = \rho(\boldsymbol{h}_i * \boldsymbol{h}_j)$, $\boldsymbol{h}_i * \boldsymbol{h}_j$ can be expressed as $\boldsymbol{h}_i * \boldsymbol{h}_j = \sum_{\nu=1}^k \alpha_\nu \boldsymbol{h}_\nu$ with $\boldsymbol{h}_\nu \in B$, $\alpha_\nu \in F$ and $\alpha_k \neq 0$. Thus by noting that $\boldsymbol{h}_i^D * \boldsymbol{h}_j^D = \theta_D(\boldsymbol{h}_i * \boldsymbol{h}_j)$, $\boldsymbol{h}_i^D * \boldsymbol{h}_j^D$ is expressed as

$$\boldsymbol{h}_i^D * \boldsymbol{h}_j^D = \sum_{\nu=1}^{k} \alpha_\nu \boldsymbol{h}_\nu^D, \quad \boldsymbol{h}_\nu \in B, \alpha_\nu \in F, \alpha_k \neq 0. \tag{5.6}$$

Without loss of generality, we assume that $\boldsymbol{h}_i^D \in S_{i-1}^D$. Since $\boldsymbol{h}_j^D \in S_j^D$, $\boldsymbol{h}_i^D * \boldsymbol{h}_j^D$ can be also expressed as

$$\begin{aligned} \boldsymbol{h}_i^D * \boldsymbol{h}_j^D &= \left(\sum_{u=1}^{i-1} a_u \boldsymbol{h}_u^D \right) * \left(\sum_{v=1}^{j} b_v \boldsymbol{h}_v^D \right) = \sum_{\substack{1 \leq u \leq i-1, \\ 1 \leq v \leq j}} \beta_{u,v} \boldsymbol{h}_u^D * \boldsymbol{h}_v^D \\ &= \sum_{\substack{1 \leq u \leq i-1, \\ 1 \leq v \leq j}} \beta_{u,v} \theta_D(\boldsymbol{h}_u * \boldsymbol{h}_v), \quad \boldsymbol{h}_u, \boldsymbol{h}_v \in B, a_u, b_v, \beta_{u,v} \in F. \end{aligned}$$

Since $(\boldsymbol{h}_i, \boldsymbol{h}_j)$ is well-behaving, $\rho(\boldsymbol{h}_u * \boldsymbol{h}_v) < k$ for every $0 \leq u \leq i-1$ and $0 \leq v \leq j$. Hence

$$\boldsymbol{h}_i^D * \boldsymbol{h}_j^D = \sum_{\nu=1}^{k-1} \beta_\nu \boldsymbol{h}_\nu^D, \quad \boldsymbol{h}_\nu \in B, \beta_\nu \in F. \tag{5.7}$$

Therefore, we have from Eqs.(5.6) and (5.7) that

$$\boldsymbol{h}_k^D = \frac{1}{\alpha_k} \sum_{\nu=1}^{k-1} (\beta_\nu - \alpha_\nu) \boldsymbol{h}_\nu$$

which implies that $\boldsymbol{h}_k^D \in S_{k-1}^D$. □

Lemma 5.3 For any $\boldsymbol{h}_k \in B$ $(r+1 \leq k \leq n)$ and given $D \in \mathcal{D}_t$, if $\boldsymbol{h}_k^D \notin S_{k-1}^D$, then $k \notin \Lambda_{T_D}$.

(Proof) We show the contraposition. For any $k \in \Lambda_{T_D} = \cup_{i \in T_D} \Lambda_i$, there exists some $i \in T_D$ such that $k \in \Lambda_i$. Therefore, by the definition of Λ_i, there exists some $\boldsymbol{h}_j \in B$ such that $k = \rho(\boldsymbol{h}_i * \boldsymbol{h}_j)$ and $(\boldsymbol{h}_i, \boldsymbol{h}_j)$ is well behaving.

On the other hand, by the definition of T_D, $\boldsymbol{h}_i^D \in S_{i-1}^D$ for any $i \in T_D$. Thus by Lemma 5.2 we have $\boldsymbol{h}_k^D \in S_{k-1}^D$. □

Theorem 5.1 For $[n, n-r]$ code C_r given in Definition 5.2, let

$$\eta_t := r - \max\{|T| : T \subset \{1, 2, \ldots, r\} \text{ such that } |\Lambda_T^*| \geq t\}. \tag{5.8}$$

Then $d_t(C_r) \geq \eta_t + t$ for any t, $1 \leq t \leq n-r$.

(Proof) Note that for $D \in \mathcal{D}_t$, we have defined $T_D := \{i : 1 \leq i \leq r,\ \boldsymbol{h}_i^D \in S_{i-1}^D\}$, which yields

$$|\{i : 1 \leq i \leq r, \boldsymbol{h}_i^D \notin S_{i-1}^D\}| = r - |T_D|. \tag{5.9}$$

On the other hand, we have from Lemma 5.1 that

$$|\{i : r+1 \leq i \leq n, \boldsymbol{h}_i^D \notin S_{i-1}^D\}| \geq t \ \text{ for any } D \in \mathcal{D}_t. \tag{5.10}$$

Thus if $r - |T_D| \geq \eta_t$ for any $D \in \mathcal{D}_t$, we have from Proposition 5.2, Eqs.(5.9) and (5.10) that

$$\begin{aligned} |Supp\,(D)| &= \dim \langle \boldsymbol{h}_1^D, \ldots, \boldsymbol{h}_n^D \rangle \\ &= |\{i : 1 \leq i \leq n, \boldsymbol{h}_i^D \notin S_{i-1}^D\}| \\ &= |\{i : 1 \leq i \leq r, \boldsymbol{h}_i^D \notin S_{i-1}^D\}| + |\{i : r+1 \leq i \leq n, \boldsymbol{h}_i^D \notin S_{i-1}^D\}| \\ &\geq \eta_t + t. \end{aligned}$$

Therefore it is sufficient to show that $r - |T_D| \geq \eta_t$ for any $D \in \mathcal{D}_t$.

For each i $(r+1 \leq i \leq n)$, if $\boldsymbol{h}_i^D \notin S_{i-1}^D$ then $i \notin \Lambda_{T_D}$ by Lemma 5.3, which means

$$\{i : r+1 \leq i \leq n, \boldsymbol{h}_i^D \notin S_{i-1}^D\} \subset \{r+1, r+2, \ldots, n\} \setminus \Lambda_{T_D} = \Lambda_{T_D}^*. \tag{5.11}$$

Thus we see from Eqs.(5.10) and (5.11) that $|\Lambda_{T_D}^*| \geq t$ for any $D \in \mathcal{D}_t$. Moreover, by noting that $T_D \subset \{1, 2, \ldots, r\}$, we have

$$\{T_D : D \in \mathcal{D}_t\} \subset \{T \subset \{1, 2, \ldots, r\} : |\Lambda_T^*| \geq t\}.$$

Therefore for any $D \in \mathcal{D}_t$

$$\begin{aligned} r - |T_D| &\geq r - \max\{|T_{D'}| : D' \in \mathcal{D}_t\} \\ &\geq r - \max\{|T| : T \subset \{1, 2, \ldots, r\}, |\Lambda_T^*| \geq t\} =: \eta_t, \end{aligned}$$

which completes the proof. □

By applying Proposition 5.1-(i) to this theorem, we immediately obtain a slightly improved bound.

Corollary 5.1 For C_r and η_t, let $\overline{\eta}_1 := \eta_1 + 1$ and

$$\overline{\eta}_t := \max\{\eta_t + t, \overline{\eta}_{t-1} + 1\},\ t = 2, 3, \ldots, n - r.$$

Then $d_t(C_r) \geq \overline{\eta}_t$ for $1 \leq t \leq n - r$. □

Theorem Theorem 5.1 may look like a paraphrase of the original problem into an equally difficult question because we have to take all subsets T's in $\{1, 2, \ldots, r\}$ to calculate Eq.(5.8). However, as shown in the next theorem, we can obtain a further information on the generalized Hamming weights of C_r via Theorem Theorem 5.1.

Theorem 5.2 For C_r, let $\mathcal{A}_i := \{r + 1, r + 2, \ldots, n\} \setminus \Lambda_i$ $(i = 1, 2, \ldots, r)$ and $g_B(C_r) := \max\{|\mathcal{A}_i| : 1 \leq i \leq r\}$. Then $d_t(C_r) = r + t$ for all t, $g_B(C_r) + 1 \leq t \leq n - r$.

(Proof) Let T be a subset of $\{1, 2, \ldots, r\}$. Since $\Lambda_T^* \subset \mathcal{A}_i$ for all $i \in T$, $|\Lambda_T^*| \leq g_B(C_r)$ for any T. So there is no $T(\neq \emptyset) \subset \{1, 2, \ldots, r\}$ such that $|\Lambda_T^*| \geq g_B(C_r) + 1$. Thus, for $t \geq g_B(C_r) + 1$, $\eta_t = r$ in Eq.(5.8) and we have $d_t(C_r) \geq r + t$.

On the other hand, $d_t(C_r) \leq r + t$ by Proposition 5.1-(ii). □

Remark 5.2 For given B and r, it is easy to calculate Λ_i $(1 \leq i \leq r)$ by using, for example, Gaussian elimination. Thus it is relatively easy to obtain $g_B(C_r)$ in Theorem 5.2. By the same reason as mentioned in Remark 5.1, $g_B(C_r)$ also depends on B and the order of $\boldsymbol{h}_i$'s in B. □

An $[n, n-r]$ code C is called the t-th rank MDS if an equality holds in the generalized Singleton bound, that is, $d_t(C) = r + t$ [42], and some sufficient conditions for the t-th rank MDS are discussed in [41]. Since any $[n, n - r]$ linear code C_r can be expressed as in Definition 5.2, we see from Theorem 5.2 that C_r is the t-th rank MDS for $g_B(C_r) + 1 \leq t \leq n - r$, which gives a new type of sufficient condition for the t-th rank MDS codes.

5.3.2 A lower bound for generalized Hamming weights of dual codes

Here we investigate generalized Hamming weights of $C_r^{\perp}$.

Theorem 5.3 Define $\{\delta_1, \delta_2, \ldots, \delta_r\}$ $(\delta_i < \delta_{i+1})$ by

$$\{\delta_1, \delta_2, \ldots, \delta_r\} := \{1, 2, \ldots, n\} \setminus \{n+1-\overline{\eta}_\nu\}_{\nu=1}^{n-r}.$$

Then $d_t(C_r^{\perp}) \geq \delta_t$ for $1 \leq t \leq r$.

(Proof) We have from Corollary 5.1 that

$$n+1-d_\nu(C_r) \leq n+1-\overline{\eta}_\nu \tag{5.12}$$

for $1 \leq \nu \leq n-r$ and in particular with equality for $g_B(C_r)+1 \leq \nu \leq n-r$ by Theorem 5.2. By Proposition 5.1-(i) and (iii), $d_t(C_r^{\perp})$ is the t-th smallest element in

$$\{1, 2, \ldots, n\} \setminus \{n+1-d_\nu(C_r)\}_{\nu=1}^{n-r}$$

and δ_t is the t-th smallest element in $\{\delta_1, \delta_2, \ldots, \delta_r\}$. Therefore we have from Eq.(5.12) that $d_t(C_r^{\perp}) \geq \delta_t$ $(1 \leq t \leq r)$. □

Corollary 5.2 Let

$$\overline{\delta}_t := \begin{cases} n-r-g_B(C_r)+1, & \text{for } t=1, \\ \delta_t, & \text{for } 2 \leq t \leq r-\overline{\eta}_1+1, \\ n-r+t, & \text{for } r-\overline{\eta}_1+2 \leq t \leq r. \end{cases}$$

Then $d_t(C_r^{\perp}) \geq \overline{\delta}_t$ with equality for $r-\overline{\eta}_1+2 \leq t \leq r$.

(Proof) (i) In the case $t=1$: By Corollary 5.1 and Theorem 5.2, we can write

$$\begin{aligned} &\{n+1-d_\nu(C_r)\}_{\nu=1}^{n-r} \\ &= \{1, 2, \ldots, n-r-g_B(C_r), n+1-d_{g_B(C_r)}(C_r), \ldots, n+1-d_1(C_r)\}. \end{aligned}$$

Hence by Proposition 5.1-(iii) $d_1(C_r^{\perp})$ is not less than $n-r-g_B(C_r)+1$.

(ii) In the case $2 \leq t \leq r-\overline{\eta}_1+1$: Trivial from Theorem 5.3.

(iii) In the case $r-\overline{\eta}_1+2 \leq t \leq r$: We have $\max\{n+1-d_\nu(C_r)\}_{\nu=1}^{n-r} = n+1-d_1(C_r)$ by Proposition 5.1-(i) and $n+1-d_1(C_r) \leq n-\overline{\eta}_1+1$ by Corollary 5.1. Thus we have

from Proposition 5.1-(iii) that all integers i such that $n - \overline{\eta}_1 + 2 \leq i \leq n$ are not included in $\{n+1-d_\nu(C_r)\}_{\nu=1}^{n-r}$, that is, $\{n - \overline{\eta}_1 + 2, \ldots, n\}$ are included in $\{d_t(C_r^\perp)\}_{t=1}^{r}$ and are the largest $\overline{\eta}_1 - 1$ elements in $\{1, 2, \ldots, n\}$. Therefore, by Proposition 5.1-(i), we have

$$\{n - \overline{\eta}_1 + 2, \ldots, n\} = \{d_t(C_r^\perp)\}_{t=r-\overline{\eta}_1+2}^{r}$$

and $d_t(C_r^\perp) = n - r + t$. □

5.3.3 Comparison of the proposed bound with the order bound

In this subsection, we compare the proposed bound with the order bound [8] from some technical points of view.

(a) A major advantage of the proposed bound would be an introduction of $g_B(C_r)$ which, as shown in the next section, gives a rather fine range of t for which RS, RM and AG codes are t-th rank MDS.

(b) It is seen that the class of codes to which the proposed bound can be applied is wider than that for the order bound.

We can see that the order bound can not be applied to all linear codes since it requires an order function which must satisfy some specific conditions and therefore can not always produce a basis of F_q^n which includes the vectors of a parity check matrix of a given linear code as its first r elements. It is also noted that no concrete procedure to construct an order function for a given code is presented in [8].

On the other hand, the proposed bound can be computed for any linear code because a basis $B = \{\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_n\}$ of F_q^n can be obtained by simply adding independent vectors to the vectors of a parity check matrix of a given linear code.

(c) As for the tightness of the bounds, as we show some numerical examples in the next section, the proposed bound has given no worse value so far than the conventional ones including the order bound.

However, it seems difficult to make a general comparison between the two bounds and we must leave it for further study to clarify the tightness of the bounds.

(d) Finally, we shall roughly compare the computational complexity to calculate these two bounds.

As is seen from Eq.(5.8), the proposed bound needs to verify whether $|\Lambda_T^*| \geq t$ for all subsets T's of $\{1, 2, \ldots, r\}$ and find the maximum value of $|T|$ with $|\Lambda_T^*| \geq t$. The

complexity to verify if $|\Lambda_T^*| \geq t$ for T is proportional to $|T|$. Since the number of subsets T's of $\{1, 2, \ldots, r\}$ with $|T| = i$ is $\binom{r}{i}$, the complexity is proportional to $\sum_{i=1}^{r} i\binom{r}{i}$ which increases as r increases and does not depend on t. It is noted that for $t \geq g_B(C_r) + 1$, the proposed bound requires no calculation as Theorem Theorem 5.2 gives the exact value $d_t(C_r) = r + t$ for the generalized Hamming weight.

On the other hand, the order bound needs to evaluate a function, denoted by $a(\ell_1, \ell_2, \ldots, \ell_t)$ in [8], for all t-tuples $(\ell_1, \ell_2, \ldots, \ell_t)$ such that $\ell_i \in \{r+1, r+2, \ldots, n\}$ and $\ell_1 < \ell_2 < \cdots < \ell_t$, and to find the minimum value of $a(\ell_1, \ell_2, \ldots, \ell_t)$. Provided that an order function is given, the complexity to calculate $a(\ell_1, \ell_2, \ldots, \ell_t)$ for a t-tuple $(\ell_1, \ell_2, \ldots, \ell_t)$ is proportional to t. Since there are $\binom{n-r}{t}$ such t-tuples, the complexity is proportional to $t\binom{n-r}{t}$, which increases as r decreases, and increases with t for $1 \leq t \leq (n-r+1)/2$ and decreases with t for $(n-r+1)/2 \leq t \leq n-r$.

As an example, $\sum_{i=1}^{r} i\binom{r}{i}$ and $t\binom{n-r}{t}$ are compared for $n = 64$ in Figs. 5.1 and 5.2. We can see from Fig. 5.1 that the computational complexity for the proposed bound is smaller than or comparable to that for the order bound when the rate of a code is relatively large (i.e., for a smaller r), and the complexities for the two bounds are complementary with respect to r.

In Fig. 5.2, we compare the complexities of the two bounds for $r = 8$ and 16. Fig. 5.2 shows that the complexity for the proposed bound is much less than that for the order bound in most of t.

It is noted again that while the complexity for the proposed bound is drawn for whole range of r and t in Figs. 5.1 and 5.2, respectively, no computation is required for $t \geq g_B(C_r) + 1$.

5.4 Applications

In this section, we apply Theorem 5.1 and Theorem 5.2 to a couple of representative codes, i.e., Reed-Solomon codes and Reed-Muller codes.

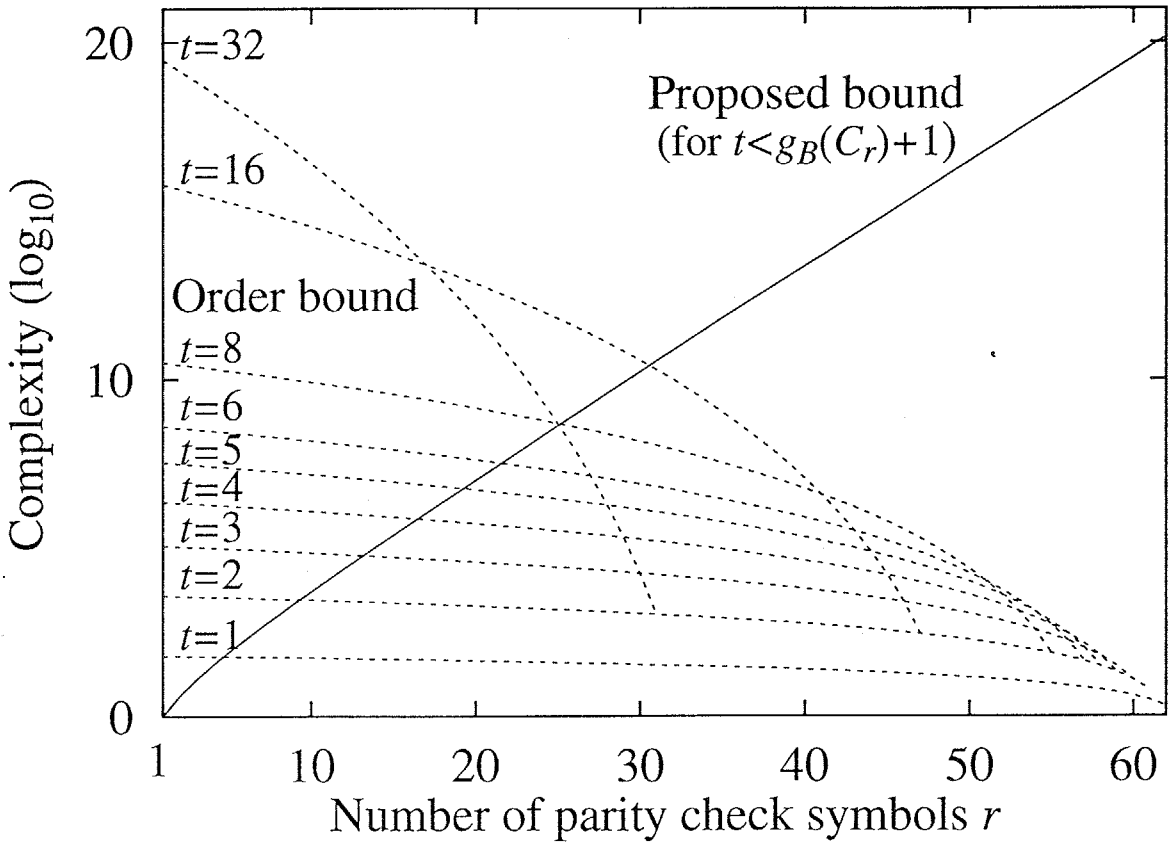

Figure 5.1: Comparison of complexity (1)

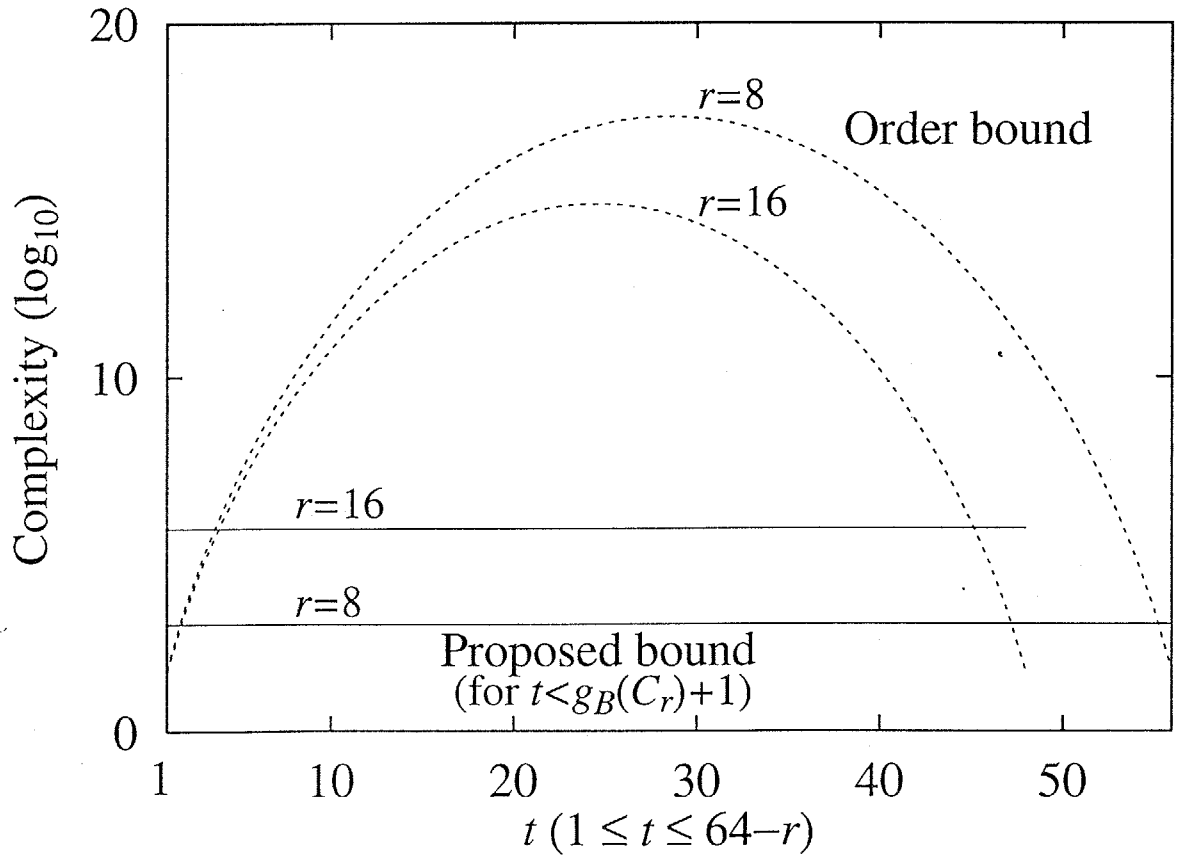

Figure 5.2: Comparison of complexity (2)

5.4.1 Reed-Solomon codes

Let α be a primitive element of $F := GF(q)$ and $n := q - 1$. We set the basis of F^n as $B = \{\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_n\}$ where

$$\boldsymbol{h}_i := (1, \alpha^{i-1}, \alpha^{2(i-1)}, \ldots, \alpha^{(n-1)(i-1)}) \in F^n.$$

Then C_r becomes the $[n, n-r, r+1]$ Reed-Solomon (RS) code.

For each $\boldsymbol{h}_i$ $(1 \leq i \leq r)$,

$$\begin{aligned} \boldsymbol{h}_i * \boldsymbol{h}_j &= (1, \alpha^{i+j-2}, \alpha^{2(i+j-2)}, \ldots, \alpha^{(n-1)(i+j-2)}) \\ &= \boldsymbol{h}_{i+j-1}, \quad j = 1, 2, \ldots, n-i+1, \end{aligned}$$

which implies that $\rho(\boldsymbol{h}_i * \boldsymbol{h}_j) = i + j - 1$. Moreover, it can be easily verified that for each $\boldsymbol{h}_i$ $(1 \leq i \leq r)$, $(\boldsymbol{h}_i, \boldsymbol{h}_j)$ are all well-behaving for $j = 1, 2, \ldots, n-i+1$. Thus we have

$$\Lambda_i = \{i, i+1, \ldots, n\}$$

and

$$\mathcal{A}_i = \{r+1, r+2, \ldots, n\} \setminus \Lambda_i = \emptyset$$

for all $i = 1, 2, \ldots, r$. Therefore, by the definition, we have $g_B(C_r) = 0$.

By Theorem 5.2, it holds that $d_t(C_r) = r + t$ for all t $(1 \leq t \leq n - r)$, which implies that RS codes are the first rank MDS codes. This is a well known fact [41, 42].

5.4.2 Reed-Muller codes

Let R be the polynomial ring over $F := GF(q)$ with m variables, i.e., $R := F[X_1, X_2, \ldots, X_m]$. We also let $\mathcal{P}$ be the set of all distinct points of F^m, that is, $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ where $n = q^m$. For $f \in R$ and $\mathcal{P}$, let $\psi(f) := (f(P_1), f(P_2), \ldots, f(P_n))$. The map $\psi : R \to F^n$ is a surjective homomorphism of F-algebra [8].

We define $\deg(f) := \sum_{\ell=1}^{m} i_\ell$ for a monomial $f = X_1^{i_1} X_2^{i_2} \cdots X_m^{i_m} \in R$ and $\deg(f) := \max\{\deg(f_i)\}$ for $f = \sum_i f_i$, where f_i's $\in R$ denote monomials.

Definition 5.5 [8] The q-ary Reed-Muller code of order u and in m variables is defined by

$$\mathrm{RM}_q(u, m) := \{\psi(f) : f \in R, \deg(f) \leq u\}.$$

□

A monomial $\prod_{\ell=1}^{m} X_\ell^{i_\ell} \in R$ is said to be *reduced* if $0 \le i_\ell \le q-1$ for all ℓ $(1 \le \ell \le m)$. There are q^m $(= n)$ reduced monomials in R, and it is shown in [8] that

$$\mathrm{RM}_q(u,m) = \mathrm{span}\{\psi(f) : f \in R \text{ is a reduced monomial with } \deg(f) \le u\}. \tag{5.13}$$

In [8], *graded lexicographic order*, which is one of the *monomial orders* on R [1], is employed to construct from $\{\psi(f) : f \in R$ is a reduced monomial$\}$ a basis of Reed-Muller code.

Definition 5.6 (Graded lexicographic order $\prec_{\mathrm{GL}}$) [1] For $f_i = \prod_{\ell=1}^{m} X_\ell^{i_\ell}$ and $f_j = \prod_{\ell=1}^{m} X_\ell^{j_\ell}$ in R, we say $f_i \prec_{\mathrm{GL}} f_j$ if (i) $\deg(f_i) < \deg(f_j)$, or (ii) $\deg(f_i) = \deg(f_j)$ and $f_i \prec_{\mathrm{L}} f_j$, where $\prec_{\mathrm{L}}$ denotes a lexicographic order [1], i.e., $f_i \prec_{\mathrm{L}} f_j$ if, in the vector $(j_1 - i_1, j_2 - i_2, \ldots, j_m - i_m)$, there exists nonzero entry and the left-most nonzero entry is positive. □

Write

$$\{f \in R : f \text{ is a reduced monomial}\} = \{f_1, f_2, \ldots, f_n\} =: \Gamma_q$$

with $f_i \prec_{\mathrm{GL}} f_{i+1}$ and $n = q^m$, and define

$$B := \{\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_n\}, \quad \boldsymbol{h}_i := \psi(f_i).$$

We also let $\Gamma_q(u) := \{f \in \Gamma_q : \deg(f) \le u\}$. Then it is obvious from Eq.(5.13) that

$$\mathrm{RM}_q(u,m) = \mathrm{span}\{\psi(f) : f \in \Gamma_q(u)\} = \langle \boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_k \rangle$$

where $k := |\Gamma_q(u)|$, and have our final result as follows.

Proposition 5.3 [8] The dual code of $\mathrm{RM}_q(u,m)$ is $\mathrm{RM}_q(m(q-1)-u-1, m)$. □

By this proposition, we see that

$$\mathrm{RM}_q(u,m) = \langle \boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_r \rangle^{\perp} = C_r$$

where $r := |\Gamma_q(m(q-1)-u-1)|$.

Theorem 5.4 Consider $C_r = \mathrm{RM}_q(u,m)$ where $r = |\Gamma_q(m(q-1)-u-1)|$. Let Q and R be integers such that

$$m(q-1) - u - 1 = Q(q-1) + R, \quad 0 \le Q, 0 \le R \le q-2. \tag{5.14}$$

Then $g_B(C_r) = q^m - r - (q-R)q^{m-(Q+1)} + 1$. (Proof is given in the Appendix 5A.1.) □

A method to compute t-th generalized Hamming weights for $\mathrm{RM}_q(u,m)$ has been shown in [42] for $q = 2$ and in [8] for arbitrary q. But no explicit condition on t for $\mathrm{RM}_q(u,m)$ to be t-th rank MDS has been given yet in terms of parameters of RM codes such as q, u and m. On the other hand, we can get from Theorem Theorem 5.2 and Theorem 5.4 an explicit condition: $\mathrm{RM}_q(u,m)$ is t-th rank MDS for t satisfying

$$q^m - r - (q-R)q^{m-(Q+1)} + 2 \leq t \leq n - r$$

where $r = |\Gamma_q(m(q-1)-u-1)|$ and Q and R are as given in Eq.(5.14).

Numerical Examples Here we consider $\mathrm{RM}_3(2,3)$ and $\mathrm{RM}_3(3,3)$. As described above, we have $n = 3^3 = 27$, $\mathrm{RM}_3(2,3) = C_{17}$ and $\mathrm{RM}_3(3,3) = C_{10}$.

For C_{17}, Q and R in Eq.(5.14) are $Q = R = 1$ and $g_B(C_{17}) = 5$. Hence $d_t(C_{17}) = 17+t$ for $6 \leq t \leq 10$ by Theorem 5.2.

For C_{10}, Q and R in Eq.(5.14) are $Q = 1$ and $R = 0$ and therefore $g_B(C_{10}) = 9$. Thus $d_t(C_{10}) = 10 + t$ for $10 \leq t \leq 17$ by Theorem 5.2.

For these two codes, we see from Examples 5.13 and 5.14 in [8] that $g_B(C_{17})$ and $g_B(C_{10})$ give the maximum range of t for which $d_t(C_r) = r + t$ holds.

5.5 Generalized Hamming weights of codes on affine algebraic varieties

In the preceding sections, we only assumed that we are given a sequence of vectors B, which is a basis of F^n and whose first $n-$k elements constitute the row vectors of a parity check matrix of the $[n,k]$ code C. In this section, we add some structure of codes, say, a monomial order and Gröbner basis, by restricting C_r to codes on affine algebraic varieties given in Section 2.3. Then we can define an upper bound of $g_B(C_r)$ for the given monomial order. Especially, by taking a monomial order such as C_r agrees with the AG code on C_{ab}, then we show that $g_B(C_r)$ is upper bounded by the genus of the curve C_{ab}.

5.5.1 Bound for generalized Hamming weights of codes on affine algebraic varieties

We consider the code C_r on a given affine algebraic variety $V = \{P_1, P_2, \ldots, P_n\} \subset F^n$ for fixed monomial order $\prec$ on $\mathbf{N}_0^s$. Let $R := F[X_1, X_2, \ldots, X_s]$ be the polynomial ring in s variables. For a basis $\{f_1, f_2, \ldots, f_n\}$ $(f_i \prec f_{i+1})$ of $R(V) := R/I(V)$ over F, let $B = \{\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_n\}$, $\boldsymbol{h}_i := \overline{\psi}(f_i)$. Then B becomes a basis of F^n over F and code C_r can be defined as in Definition 5.2.

In the following, we show that η_t in Eq.(5.8) and $g_B(C_r)$ in Theorem 5.2 depend only on a given monomial order $\prec$ and any choice of a basis of $R(V)$ including the order in it does not effect to η_t and $g_B(C_r)$.

By Proposition 2.4-(ii) and Proposition 2.5-(iii), $\mathrm{mdeg}(f_i) \in \Lambda(V)$, $(i = 1, 2, \ldots, n)$, which implies $\{\mathrm{mdeg}(f_i)\}_{i=1}^n \subset \Lambda(V)$. And since $\mathrm{mdeg}(f_i) \neq \mathrm{mdeg}(f_j)$ $(i \neq j)$, we have $|\{\mathrm{mdeg}(f_i)\}_{i=1}^n| = n = |\Lambda(V)|$. Thus

$$\{\mathrm{mdeg}(f_i)\}_{i=1}^n = \lambda(V) = \{\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \ldots, \boldsymbol{\lambda}_n\}$$

where $\boldsymbol{\lambda}_i$'s are given in Eq.(2.9).

Set

$$B_V := \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\},\ \boldsymbol{b}_i := \overline{\phi}(\boldsymbol{X}^{\boldsymbol{\lambda}_i})$$

and consider Λ_i given in Eq.(5.2) for B and B_V.

Lemma 5.4 $(\boldsymbol{h}_i, \boldsymbol{h}_j)$ $(\boldsymbol{h}_i, \boldsymbol{h}_j \in B)$ is well-behaving if and only if $(\boldsymbol{b}_i, \boldsymbol{b}_j)$ $(\boldsymbol{b}_i, \boldsymbol{b}_j \in B_V)$ is well-behaving.

(Proof) Assume that $(\boldsymbol{h}_i, \boldsymbol{h}_j)$ $(\boldsymbol{h}_i, \boldsymbol{h}_j \in B)$ is well-behaving. Since $\mathrm{mdeg}(f_i) = \boldsymbol{\lambda}_i$ $(i = 1, 2, \ldots, n)$, $\rho(\boldsymbol{h}_i) = \rho(\boldsymbol{b}_i) = i$ $(i = 1, 2, \ldots, n)$. Thus

$$\begin{aligned} \boldsymbol{b}_i * \boldsymbol{b}_j &= \left(\sum_{u=1}^{i} a_u \boldsymbol{h}_u\right) * \left(\sum_{v=1}^{i} b_v \boldsymbol{h}_v\right) \\ &= \sum_{\substack{1 \le u \le i-1, \\ 1 \le v \le j}} \alpha_{u,v} \boldsymbol{h}_u * \boldsymbol{h}_v, \quad a_u, b_v, \alpha_{u,v} \in F, a_i \neq 0, b_j \neq 0. \end{aligned} \tag{5.15}$$

Since $(\boldsymbol{h}_i, \boldsymbol{h}_j)$ is well-behaving, Eq.(5.15) implies that $\rho(\boldsymbol{b}_i * \boldsymbol{b}_j) = \rho(\boldsymbol{h}_i * \boldsymbol{h}_j)$ for all i and j such that $1 \le i, j \le n$. Thus

$$\rho(\boldsymbol{b}_u * \boldsymbol{b}_v) = \rho(\boldsymbol{h}_u * \boldsymbol{h}_v) < \rho(\boldsymbol{h}_i * \boldsymbol{h}_j) = \rho(\boldsymbol{b}_i * \boldsymbol{b}_j)$$

for all u and v with $1 \leq u \leq i$, $1 \leq v \leq j$ and $u+v < i+j$. Thus $(\boldsymbol{b}_i, \boldsymbol{b}_j)$ is well-behaving.

The proof for the converse assertion is exactly same. □

We see from Lemma 5.4 that Λ_i, and therefore, Λ_T, Λ_T^* and $\mathcal{A}_i$ depend not on the choice of B but only on a monomial order $\prec$. Thus η_t in Eq.(5.8) and $g_B(C_r)$ in Theorem 5.2 also depend only on $\prec$. We write η_{to} and $g_o(C_r)$ for given $\prec$ instead of η_t and $g_B(C_r)$, respectively, and call a lower bound of generalized Hamming weight

$$d_t(C_r) \geq \eta_{to} + t$$

bound for generalized Hamming weights of codes on affine algebraic variety for given monomial order $\prec$.

5.5.2 Upper bound of $g_B(C_r)$ for codes on C_{ab}

We consider the case in which V is the set of all rational points on the curve $\boldsymbol{C}_{ab}$ except Q. Let $R := F[x, y]$ and

$$V := \{(x, y) \in F^2 : h(x, y) = 0\} \tag{5.16}$$

where $h(x, y)$ is the defining polynomial of $\boldsymbol{C}_{ab}$ given in Eq.(2.4)

Definition 5.7 For positive integers a and b and monomials $x^{i_1}y^{j_1}, x^{i_2}y^{j_2} \in R$, we say that $x^{i_1}y^{j_1} \prec_{ab} x^{i_2}y^{j_2}$ if (i) $ai_1 + bj_1 < ai_2 + bj_2$, or (ii) $ai_1 + bj_1 = ai_2 + bj_2$ and $i_1 > i_2$. □

It is shown in [23, 24, 26] that $\prec_{ab}$ is a monomial order on R and we can take n monomials $\{f_1, f_2, \ldots, f_n\}$ in R as a basis of $R(V)$, where $f_i \prec_{ab} f_{i+1}$ $(i = 1, 2, \ldots, n-1)$. Now, for these f_i's, let $\boldsymbol{h}_i := \overline{\psi}(f_i)$, $B := \{\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_n\}$, and construct C_r as in Definition 5.2.

We define a semigroup S_{ab} associated with $\boldsymbol{C}_{ab}$ by

$$S_{ab} := \{ai + bj : i, j \in \mathbf{N}_0\}.$$

It is known that $|\mathbf{N}_0 \setminus S_{ab}| = (a-1)(b-1)/2 = g$.

Lemma 5.5 For $f_i, f_k \in B(V)$, if $\tau(f_k) - \tau(f_i) \in S_{ab}$, then there exists $f_j \in B(V)$ s.t. $\rho(\overline{f_i f_j}) = k$. (Proof is given in Appendix 5A.2.) □

Lemma 5.6 For $f_i, f_k \in B(V)$, if there exists some $f_j \in B(V)$ such that $\rho(\overline{f_i f_j}) = k$ and (f_i, f_j) is not well-behaving, then $\tau(f_k) - \tau(f_i) \in \mathbf{N}_0 \backslash S_{ab}$. (Proof is given in Appendix 5A.3.) □

By Lemma 5.5 and Lemma 5.6, we obtain the following theorem on the relation between $g_B(C_r)$ and g.

Theorem 5.5 Let g be the genus of the curve $\boldsymbol{C}_{ab}$. Then $g_B(C_r) \leq g$ $(1 \leq r \leq n)$.

(Proof) By the definitions of $\mathcal{A}_i$ (Theorem 5.2) and Λ_i (Eq.(5.2)), if $k \in \mathcal{A}_i$, then $r+1 \leq k \leq n$ and (i) $k \neq \rho(\overline{f_i f_j})$ for all $j = 1, 2, \ldots, n$, or (ii) for f_j such that $k = \rho(\overline{f_i f_j})$, (f_i, f_j) is not well-behaving. We have from the contraposition of Lemma 5.5 for the case (i) and from Lemma 5.6 for the case (ii) that

$$\mathcal{A}_i \subset \{\lambda_k : r+1 \leq k \leq n, \tau(f_k) - \tau(f_i) \in N \setminus S_{ab}\}.$$

This implies that

$$|\mathcal{A}_i| \leq |N \setminus S_{ab}| = g \quad \text{for all } i = 1, 2, \ldots, r$$

and therefore $g_B(C_r) \leq g$. □

Consider AG code on $\boldsymbol{C}_{ab}$, denoted by $\mathcal{C}_L(D, G)$. Then it is shown that $C_r = \mathcal{C}_L(D, G)^\perp$ where r is the dimension of $\mathcal{C}_L(D, G)$ [26]. For the generalized Hamming weights of AG code $\mathcal{C}_L(D, G)$, the following proposition is known.

Proposition 5.4 [27, 41, 47] If $\deg G > 2g - 2$, the AG code $\mathcal{C}_L(D, G)$ has $d_t(\mathcal{C}_L(D, G)) = n - k + t$ for all t such that $g + 1 \leq t \leq k$, where k is the dimension of $\mathcal{C}_L(D, G)$. □

It is also known that $\mathcal{C}_L(D, G)^\perp = \mathcal{C}_L(D, H)$ for some divisor H (see [38] for the detail). Thus we have the translation of Proposition 5.4 for the dual code of $\mathcal{C}_L(D, G)$.

Corollary 5.3 Notations are as above. If $\deg H > 2g - 2$, the dual of the AG code $\mathcal{C}_L(D, G)^\perp$ $(= \mathcal{C}_L(D, H))$ has $d_t(\mathcal{C}_L(D, G)^\perp) = k + t$ for all t such that $g + 1 \leq t \leq n - k$, where k is the dimension of $\mathcal{C}_L(D, G)$. □

By Corollary 5.3, we have $d_t(C_r) = r + t$ for $g + 1 \leq t \leq n - r$ where g is the genus of $\boldsymbol{C}_{ab}$. On the other hand, we see from Theorem 5.2 and Theorem 5.5 that $d_t(C_r) = r + t$ for $g_B(C_r) + 1 \leq t \leq n - r$ with $g_B(C_r) \leq g$. Thus we can conclude that $g_B(C_r)$ gives the range of t not narrower than that given in [27, 41, 47], for which the generalized Singleton bound holds with equality.

Table 5.1: The values for $g_B(C_r)$ of Hermitian code on $x^5 + y^4 + y = 0$ over $GF(2^4)$ with order $\prec_{ab}$ in B

r	1	2, 3	4, 5, 6	7, ..., 47	48	49, 50, 51	52	53	54, 55	56	57	58, 59	60	61, 62	63
$g_B(C_r)$	0	3	5	6	5	6	5	4	6	5	4	3	2	1	0

Numerical Example 1 Let $a = 4, b = 5$ and consider the curve defined by $h(x, y) = x^5 + y^4 + y$ over $GF(2^4)$. This curve is known as a Hermitian curve and its genus is $g = 6$.

The values of $g_B(C_r)$ obtained from its definition given in Theorem 5.2 are listed in Table 5.1. We can see from Table 5.1 that $g_B(C_r) < g$ for $r = 1, \ldots, 6, 48, 52, 53, 56, \ldots, 63$. For these r, the range of t for which $d_t(C_r) = r + t$ holds is wider than that given in [27, 41, 47].

□

The following example shows that the order of elements of B led by a monomial order does not always give the best value of $g_B(C_r)$.

Numerical Example 2 Let α be a primitive element of $F_q := GF(2^3)$ and consider a code on affine algebraic variety

$$\begin{aligned} V &:= \{(0,0), (0,1), (1,\alpha), (1,\alpha^2), (1,\alpha^4), (\alpha,\alpha^5), (\alpha^2,\alpha^3), (\alpha^4,\alpha^6)\} \\ &=: \{P_1, P_2, \ldots, P_8\}. \end{aligned}$$

We employ a monomial order on R defined by Definition Definition 5.7 with $a = 3$ and $b = 4$. Then a basis of $R(V)$ is given by[1]

$$\{1, x, y, x^2, xy, y^2, x^3, x^2y\} =: \{f_1, f_2, \ldots, f_8\}$$

and we have

$$\begin{aligned} &B = \{\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_8\}, \\ &\boldsymbol{h}_i := \overline{\psi}(f_i) = (f_i(P_1), f_i(P_2), \ldots, f_i(P_8)). \end{aligned}$$

The values of $g_B(C_r)$ obtained from the definition given in Theorem Theorem 5.2 are

$$\begin{aligned} &g_B(C_1) = 0, g_B(C_2) = \cdots = g_B(C_6) = 2, \\ &g_B(C_7) = 1. \end{aligned}$$

[1] A basis of $R(V)$ obtained in [36] always consists of monomials of the form $\overline{f}^G = f$, where $\overline{f}^G$ denotes *the remainder on division of f by Gröbner basis G of $I(V)$.*

For any basis $B' = \{\boldsymbol{h}'_1, \boldsymbol{h}'_2, \ldots, \boldsymbol{h}'_8\}$ of F^8, which is obtained by changing the order of elements of B, such that

$$\langle \boldsymbol{h}'_1, \boldsymbol{h}'_2, \ldots, \boldsymbol{h}'_r \rangle^{\perp} = \langle \boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_r \rangle^{\perp} = C_r,$$

we can verify by computer search that $g_B(C_r) \leq g_{B'}(C_r)$ for $r = 1, 2, \ldots, 5$ and 7, while for $r = 6$, we can find that B''s given by

$$\{\boldsymbol{h}_1, \boldsymbol{h}_3, \boldsymbol{h}_2, \boldsymbol{h}_6, \boldsymbol{h}_5, \boldsymbol{h}_4, \boldsymbol{h}_7, \boldsymbol{h}_8\},$$
$$\{\boldsymbol{h}_1, \boldsymbol{h}_3, \boldsymbol{h}_5, \boldsymbol{h}_2, \boldsymbol{h}_6, \boldsymbol{h}_4, \boldsymbol{h}_7, \boldsymbol{h}_8\},$$
$$\{\boldsymbol{h}_1, \boldsymbol{h}_6, \boldsymbol{h}_3, \boldsymbol{h}_4, \boldsymbol{h}_2, \boldsymbol{h}_5, \boldsymbol{h}_7, \boldsymbol{h}_8\},$$
$$\{\boldsymbol{h}_1, \boldsymbol{h}_2, \boldsymbol{h}_3, \boldsymbol{h}_6, \boldsymbol{h}_4, \boldsymbol{h}_5, \boldsymbol{h}_7, \boldsymbol{h}_8\}$$

yield $g_{B'}(C_6) = 1 < g_B(C_6)$. Moreover, we can show that these four B''s are not obtained from a monomial order considered in [36].

(a) We first show that $\{f_1, f_2, \ldots, f_8\}$ is the only set of monomial in R with $\psi(f_i) = \boldsymbol{h}_i$ and $f_i = \overline{f_i}^G$ $(i = 1, 2, \ldots, 8)$.

Let $F_i := \{f_i + h : h \in I(V)\}$. Then since $I(V)$ is the kernel of $\psi : R \to F^8$, it is obvious that $\psi(f) = \boldsymbol{h}_i$ if and only if $f \in F_i$.

Choose next an arbitrary monomial $f'_i \in F_i$ $(i = 1, 2, \ldots, 8)$ such that $\{f'_1, f'_2, \ldots, f'_8\} \neq \{f_1, f_2, \ldots, f_8\}$. Then $\{f'_1, f'_2, \ldots, f'_8\}$ is also a set of monomials in R with $\psi(f'_i) = \boldsymbol{h}_i$. We show that $f'_i = \overline{f'_i}^G$ $(i = 1, 2, \ldots, 8)$ cannot hold for this $\{f'_1, f'_2, \ldots, f'_8\}$.

Let $f_j \neq f'_j$. Then since $\overline{f'_j}^G = \overline{f_j}^G$ by Proposition 5 in [36] and $\overline{f_j}^G = f_j$ by the footnote on p.73, we have $\overline{f'_j}^G = f_j \neq f'_j$. Thus we can conclude that $\{f_1, f_2, \ldots, f_8\}$ is the only set of monomials in R such that $\psi(f_i) = \boldsymbol{h}_i$ and $f_i = \overline{f_i}^G$ $(i = 1, 2, \ldots, 8)$.

(b) In order to verify if there exists a monomial order which leads any of the above four bases, it is sufficient by (a) above to examine whether the set $\{f_1, f_2, \ldots, f_8\}$ with its order so changed as it gives each of the above four bases satisfies the condition of a monomial order.

Note that for $f, g \in R$ and $h \in R \setminus \{0\}$, any monomial order $\prec_{\mathrm{M}}$ must satisfy that $fh \prec_{\mathrm{M}} gh$ if $f \prec_{\mathrm{M}} g$. It is easy to see that none of the above four bases satisfy this condition. In fact, for the first basis, for example, we must have $y \prec x$ and $x^2 y \succ x^3$ at the same time, which contradicts the condition for a monomial order. Thus we can conclude that the above four bases are not obtained from a monomial order treated in [36]. □

5.6 Conclusion

In this chapter, we have introduced a lower bound for the generalized Hamming weights of arbitrary linear code and its dual in terms of the notion of well-behaving. The proposed bound can be obtained only from the basis B of F_q^n whose first r elements constitute the parity check matrix of the code and requires no other structure of the code. We have also shown that any $[n, k]$ linear code C is the t-th rank MDS for $g_B(C) + 1 \leq t \leq k$ where $g_B(C)$ is uniquely determined from B. Finally, we have applied our results to RS codes, RM codes and codes on affine algebraic varieties. Then we have given explicit formulae of $g_B(C)$ for RS and RM codes and shown that η_t and $g_B(C)$ depend not on the choice of B but on the monomial order. Especially we have shown that $g_B(C) \leq g$ holds for AG codes on C_{ab} where g is the genus of C_{ab}.

Appendices

5A.1 Proof of Theorem 5.4

Γ_q, $\Gamma_q(u)$ and B with graded lexicographic order are as defined in Subsection 5.4.2.

Lemma 5A.1 A pair $(\boldsymbol{h}_i, \boldsymbol{h}_j)$ $(\boldsymbol{h}_i, \boldsymbol{h}_j \in B)$ is well-behaving if and only if $\overline{f_i f_j} = f_i f_j$, where $\overline{f}$ is a reduced polynomial[2] of f.

(Proof) Assume $\overline{f_i f_j} = f_i f_j$ and note that since

$$\boldsymbol{h}_u * \boldsymbol{h}_v = \psi(f_u)\psi(f_v) = \psi(f_u f_v) = \psi(\overline{f_u f_v})$$

and $\overline{f_u f_v} \in \Gamma_q$, we have $\rho(\boldsymbol{h}_u * \boldsymbol{h}_v) < \rho(\boldsymbol{h}_i * \boldsymbol{h}_j)$ for any $\boldsymbol{h}_u, \boldsymbol{h}_v \in B$ if and only if $\overline{f_u f_v} \prec_{\mathrm{GL}} \overline{f_i f_j}$ and $\overline{f_u f_v} \neq \overline{f_i f_j}$. Thus we show that $\overline{f_u f_v} \prec_{\mathrm{GL}} f_i f_j$ and $\overline{f_u f_v} \neq f_i f_j$ for every u, v such that $1 \leq u \leq i$, $1 \leq v \leq j$ and $u + v < i + j$.

By the definition of Γ_q, $f_u \prec_{\mathrm{GL}} f_i$ (resp. $f_v \prec_{\mathrm{GL}} f_j$) for $1 \leq u \leq i$ (resp. $1 \leq v \leq j$) and the equality with respect to $\prec_{\mathrm{GL}}$ holds only when $u = i$ (resp. $v = j$). Since $\prec_{\mathrm{GL}}$ is a monomial order, if $f_u \prec_{\mathrm{GL}} f_i$ (resp. $f_v \prec_{\mathrm{GL}} f_j$) then $f_u f_j \prec_{\mathrm{GL}} f_i f_j$ (resp. $f_u f_v \prec_{\mathrm{GL}} f_u f_j$) [1], which implies that

$$f_u f_v \prec_{\mathrm{GL}} f_u f_j \prec_{\mathrm{GL}} f_i f_j \tag{5A.1}$$

[2] A polynomial in R is called *reduced* if it is a linear combination of reduced monomials. For every polynomial $f \in R$, there exists a unique reduced polynomial $\overline{f}$ such that $\psi(f) = \psi(\overline{f})$.

for $1 \le u \le i$ and $1 \le v \le j$. In Eq.(5A.1), $f_u f_v =_{\mathrm{GL}} f_i f_j$ holds only when $u = i$ and $v = j$, but which is impossible for u and v with $u + v < i + j$.

Finally, as $\overline{f} \prec_{\mathrm{GL}} f$ for any monomial in R, we have $\overline{f_u f_v} \prec_{\mathrm{GL}} f_i f_j$ for u and v which satisfy $1 \le u \le i$, $1 \le u \le j$ and $u + v < i + j$. For such u and v, $\overline{f_u f_v} \neq f_i f_j$ is trivial. Therefore it is concluded that $(\boldsymbol{h}_i, \boldsymbol{h}_j)$ is well-behaving.

Conversely, let $f_i := X_1^{i_1} X_2^{i_2} \cdots X_m^{i_m}$ and $f_j := X_1^{j_1} X_2^{j_2} \cdots X_m^{j_m}$, and assume that $\overline{f_i f_j} \neq f_i f_j$. Then there exists a nonempty set

$$\mathcal{R} := \{\ell : 1 \le \ell \le m, i_\ell + j_\ell \ge q\}.$$

For each $\ell \in \mathcal{R}$, let i'_ℓ and j'_ℓ be integers such that

$$i'_\ell + j'_\ell = i_\ell + j_\ell - (q-1), \quad 0 \le i'_\ell \le i_\ell, 0 \le j'_\ell \le j_\ell.$$

For these i'_ℓ and j'_ℓ, define

$$f_u := \prod_{\ell=1}^{m} X_\ell^{u_\ell}, \quad u_\ell := \begin{cases} i_\ell & \text{for } \ell \notin \mathcal{R}, \\ i'_\ell & \text{for } \ell \in \mathcal{R}, \end{cases}$$
$$f_v := \prod_{\ell=1}^{m} X_\ell^{v_\ell}, \quad v_\ell := \begin{cases} j_\ell & \text{for } \ell \notin \mathcal{R}, \\ j'_\ell & \text{for } \ell \in \mathcal{R}. \end{cases}$$

Since $f_u \neq f_i$, $f_v \neq f_j$ and $f_u \prec_{\mathrm{GL}} f_i$, $f_v \prec_{\mathrm{GL}} f_j$, we have $1 \le u \le i$, $1 \le v \le j$ and $u + v < i + j$. For these f_u and f_v, we also have $\overline{f_u f_v} = \overline{f_i f_j}$, which implies that $(\boldsymbol{h}_i, \boldsymbol{h}_j)$ is not well-behaving. □

Since $f \in \Gamma_q$ is a reduced monomial, $0 \le \deg(f) \le m(q-1)$ for all $f \in \Gamma_q$.

Definition 5.8 For each Λ_i defined in Eq.(5.2), we define

$$\Lambda_i^\delta := \{\ell \in \Lambda_i : \deg(f_\ell) = \delta\}, \quad 0 \le \delta \le m(q-1).$$

□

It is obvious that $\Lambda_i = \cup_{\delta=0}^{m(q-1)} \Lambda_i^\delta$ and Λ_i^δ $(\delta = 0, 1, \ldots, m(q-1))$ are mutually disjoint.

Definition 5.9 For given $f_i \in \Gamma_q$, define $i_{\max}$ as the integer such that

$$f_{i_{\max}} = \max_{\prec_{\mathrm{GL}}} \{f \in \Gamma_q : \deg(f) = \deg(f_i)\},$$

where maximum is taken with respect to $\prec_{\mathrm{GL}}$. □

For given $f_i \in \Gamma_q$, let Q and R be integers such that $\deg(f_i) = Q(q-1)+R$, $0 \le Q$, $0 \le R \le q-2$. Then by the definition of graded lexicographic order, $f_{i_{\max}}$ is expressed as

$$f_{i_{\max}} = X_1^{q-1} \cdots X_Q^{q-1} X_{Q+1}^R. \tag{5A.2}$$

By the definition of Λ_i (Eq.(5.2)) and Lemma 5A.1, Λ_i is rewritten as

$$\Lambda_i = \{k : k \in \{0,1,2,\ldots,n\} \text{ such that } f_k = f_i f_j \text{ where } f_j \in \Gamma_q \text{ and } \overline{f_i f_j} = f_i f_j\}.$$

Moreover, for $f_i = \prod_{\ell=1}^m X_\ell^{i_\ell}$, we can write

$$\Lambda_i = \{k : k \in \{0,1,2,\ldots,n\} \text{ such that } f_k = f_i f_j \text{ where } f_j = \prod_{\ell=1}^m X_\ell^{j_\ell}, 0 \le j_\ell \le q-1-i_\ell, \ell = 1,2,\ldots,m\}. \tag{5A.3}$$

Hereafter, we determine the number i^* $(1 \le i^* \le r)$ for $C_r = \mathrm{RM}_q(u,m)$ $(r = |\Gamma_q(u(q-1)-u-1)|)$ which satisfies

$$|\mathcal{A}_{i^*}| \ge |\mathcal{A}_i|, \text{ for all } i, 1 \le i \le r.$$

Then $g_B(C_r) = |\mathcal{A}_{i^*}|$ by the definition.

Lemma 5A.2 For all $i \in \{1,2,\ldots,n\}$,

$$|\Lambda_i^\delta| \ge |\Lambda_{i_{\max}}^\delta|, \quad \delta = 0,1,\ldots,m(q-1).$$

(Proof) *Step 1.* At first, we fix i and δ. Let $f_i = \prod_{\ell=1}^m X_\ell^{i_\ell}$ and define the subset J_i^δ of $\{0,1,\ldots,q-1\}^m$ by

$$J_i^\delta := \{(j_1,j_2,\ldots,j_m) : 0 \le j_\ell \le q-1-i_\ell, \ell = 1,2,\ldots,m, \textstyle\sum_{\ell=1}^m j_\ell = \delta - \deg(f_i)\}.$$

By Definition 5.8 and Eq.(5A.3), we see that $|\Lambda_i^\delta| = |J_i^\delta|$. Thus we show that $|J_i^\delta| \ge |J_{i_{\max}}^\delta|$.

Fix ℓ_1 and ℓ_2 $(1 \le \ell_1 < \ell_2 \le m)$ and define the subsets $J_i^\delta(\omega)$ and $J_i^\delta(\omega, j)$ of J_i^δ by

$$\begin{cases} J_i^\delta(\omega) := \{(j_1,j_2,\ldots,j_m) \in J_i^\delta : j_{\ell_1} + j_{\ell_2} = \omega\}, \\ J_i^\delta(\omega,j) := \{(j_1,j_2,\ldots,j_m) \in J_i^\delta(\omega) : j_{\ell_1} = j\}. \end{cases}$$

Since $0 \le j_{\ell_\nu} \le q-1-i_{\ell_\nu}$ $(\nu = 1,2)$, we have $0 \le \omega \le 2(q-1)-(i_{\ell_1}+i_{\ell_2})$ and

$$J_i^\delta = \bigcup_{\omega=0}^{2(q-1)-(i_{\ell_1}+i_{\ell_2})} J_i^\delta(\omega).$$

Moreover, $J_i^\delta(\omega)$'s are mutually disjoint for $\omega = 0, 1, \ldots, 2(q-1) - (i_{\ell_1} + i_{\ell_2})$. Thus

$$|J_i^\delta| = \sum_{\omega=0}^{2(q-1)-(i_{\ell_1}+i_{\ell_2})} |J_i^\delta(\omega)|. \tag{5A.4}$$

On the other hand, for fixed ω, $J_i^\delta(\omega, j)$ is defined for j such that

$$0 \le j \le q-1-i_{\ell_1} \text{ and } 0 \le \omega - j \le q-1-i_{\ell_2}. \tag{5A.5}$$

Thus

$$J_i^\delta(\omega) = \bigcup_{\substack{0 \le j \le q-1-i_{\ell_1}, \\ 0 \le \omega - j \le q-1-i_{\ell_2}}} J_i^\delta(\omega, j).$$

It is obvious that, for fixed ω, $J_i^\delta(\omega, j) \cap J_i^\delta(\omega, j') = \emptyset$ for $j \neq j'$, and $|J_i^\delta(\omega, j)|$'s are constant for all j satisfying Eq.(5A.5). Therefore, $|J_i^\delta(\omega)|$ can be expressed as

$$|J_i^\delta(\omega)| = N(\omega)|J_i^\delta(\omega, j_\omega)| \tag{5A.6}$$

where j_ω is an arbitrary integer satisfying Eq.(5A.5) and $N(\omega)$ is the number of j's satisfying Eq.(5A.5) for given ω.

Let $\sigma_{\min} := \min\{q-1-i_{\ell_1}, q-1-i_{\ell_2}\}$ and $\sigma_{\max} := \max\{q-1-i_{\ell_1}, q-1-i_{\ell_2}\}$. Then it is easily verified that $N(\omega)$ is expressed by using i_{ℓ_1}, i_{ℓ_2} and w as

$$N(\omega) = \begin{cases} \omega + 1 & \text{for } 0 \le \omega \le \sigma_{\min}, \\ \sigma_{\min} + 1 & \text{for } \sigma_{\min} + 1 \le \omega \le \sigma_{\max} - 1, \\ 2(q-1) - (i_{\ell_1} + i_{\ell_2}) - \omega + 1 & \text{for } \sigma_{\max} \le \omega \le 2(q-1) - (i_{\ell_1} + i_{\ell_2}). \end{cases}$$

By these expressions and Eqs.(5A.4) and (5A.6), we have

$$\begin{aligned} |J_i^\delta| = {} & \sum_{\omega=0}^{\sigma_{\min}} (\omega+1)|J_i^\delta(\omega, j_\omega)| + \sum_{\omega=\sigma_{\min}+1}^{\sigma_{\max}-1} (\sigma_{\min}+1)|J_i^\delta(\omega, j_\omega)| \\ & + \sum_{\omega=\sigma_{\max}}^{2(q-1)-(i_{\ell_1}+i_{\ell_2})} (2(q-1) - (i_{\ell_1} + i_{\ell_2}) - \omega + 1)|J_i^\delta(\omega, j_\omega)|. \end{aligned} \tag{5A.7}$$

Step 2. In this step, we also fix i and δ. Since Eq.(5A.7) does not depend on the order of i_ℓ in $(i_1, i_2, \ldots, i_m)$, we assume that $i_\ell \ge i_{\ell+1}$ $(\ell = 1, 2, \ldots, m-1)$ when we consider $|J_i^\delta|$.

Let ℓ_1 $(1 \le \ell_1 \le m)$ be the smallest integer such that $i_{\ell_1} \le q-2$ and ℓ_2 $(1 \le \ell_2 \le m)$ be the largest integer such that $i_{\ell_2} \ge 1$. Since we assume that $i_\ell \ge i_{\ell+1}$, we have the following three cases.

(i) The case $\ell_1 > \ell_2$. This corresponds to $(i_1, i_2, \ldots, i_m) = (q-1, \ldots, q-1, 0, \ldots, 0)$ where the number of $q-1$ is Q and $Q(q-1) = \deg(f_i)$.

(ii) The case $\ell_1 = \ell_2$. This corresponds to $(i_1, i_2, \ldots, i_m) = (q-1, \ldots, q-1, R, 0, \ldots, 0)$ where the number of $q-1$ is Q, $1 \le R \le q-2$ and $Q(q-1) + R = \deg(f_i)$.

(iii) The case $\ell_1 < \ell_2$. All $(i_1, i_2, \ldots, i_m)$ other than the cases (i) and (ii) fall into this case.

We show that if $\ell_1 < \ell_2$, there exists i' $(\neq i)$ $(1 \le i' \le n)$ such that $\deg(f_i) = \deg(f_{i'})$ and $|J_i^\delta| \ge |J_{i'}^\delta|$.

Let

$$i'_\ell := \begin{cases} i_\ell & \text{for } \ell = 1, 2, \ldots, m, \ell \neq \ell_1, \ell_2, \\ i_\ell + 1 & \text{for } \ell = \ell_1, \\ i_\ell - 1 & \text{for } \ell = \ell_2, \end{cases}$$

and $f_{i'} := \prod_{\ell=1}^m X_\ell^{i'_\ell}$. Since it holds that $0 \le i'_\ell \le q-1$, $f_{i'} \in \Gamma_q$. Moreover,

$$\deg(f_{i'}) = \sum_{\ell=1}^m i'_\ell = \sum_{\substack{\ell=1, \\ \ell \neq \ell_1, \ell_2}}^m i_\ell + (i_{\ell_1} + 1) + (i_{\ell_2} - 1) = \sum_{\ell=1}^m i_\ell = \deg(f_i).$$

For this $f_{i'}$, we define $J_{i'}^\delta$, $J_{i'}^\delta(\omega)$ and $J_{i'}^\delta(\omega, j_\omega)$ similarly to J_i^δ, $J_i^\delta(\omega)$ and $J_i^\delta(\omega, j_\omega)$ above. It is noted here that for fixed ω, there exists j_ω and j'_ω for i'_{ℓ_1} and i'_{ℓ_2} which satisfy Eq.(5A.5) and $|J_i^\delta(\omega, j_\omega)| = |J_{i'}^\delta(\omega, j'_\omega)|$. Hence by Eq.(5A.7), we have

$$\begin{aligned}
&|J_i^\delta| - |J_{i'}^\delta| \\
&= \sum_{\omega=0}^{q-1-i_{\ell_1}} (\omega+1)|J_i^\delta(\omega, j_\omega)| + \sum_{\omega=q-i_{\ell_1}}^{q-2-i_{\ell_2}} (q - i_{\ell_1})|J_i^\delta(\omega, j_\omega)| \\
&\qquad + \sum_{\omega=q-1-i_{\ell_2}}^{2(q-1)-(i_{\ell_1}+i_{\ell_2})} (2(q-1) - (i_{\ell_1} + i_{\ell_2}) - \omega + 1)|J_i^\delta(\omega, j_\omega)| \\
&\quad - \left(\sum_{\omega=0}^{q-1-i'_{\ell_1}} (\omega+1)|J_{i'}^\delta(\omega, j'_\omega)| + \sum_{\omega=q-i'_{\ell_1}}^{q-2-i'_{\ell_2}} (q - i'_{\ell_1})|J_{i'}^\delta(\omega, j'_\omega)| \right. \\
&\qquad \left. + \sum_{\omega=q-1-i'_{\ell_2}}^{2(q-1)-(i_{\ell_1}+i_{\ell_2})} (2(q-1) - (i'_{\ell_1} + i'_{\ell_2}) - \omega + 1)|J_{i'}^\delta(\omega, j'_\omega)| \right) \\
&= ((q - 1 - i_{\ell_1}) + 1)|J_i^\delta(q - 1 - i_{\ell_1}, j_\omega)| - (q - (i_{\ell_1} + 1))|J_{i'}^\delta(q - (i_{\ell_1} + 1), j'_\omega)| \\
&\qquad - (q - (i_{\ell_1} + 1))|J_{i'}^\delta(q - 2 - (i_{\ell_2} - 1), j'_\omega)|
\end{aligned}$$

$$+ (2(q-1) - (i_{\ell_1} + i_{\ell_2}) - (q-1-i_{\ell_2}) + 1)|J_i^\delta(q-1-i_{\ell_2}, j_\omega)|$$
$$+ \sum_{\omega=q-i_{\ell_1}}^{q-i_{\ell_2}-2} |J_i^\delta(\omega, j_\omega)|$$
$$= |J_i^\delta(q-1-i_{\ell_1}, j_\omega)| + |J_i^\delta(q-1-i_{\ell_2}, j_\omega)| + \sum_{\omega=q-i_{\ell_1}}^{q-i_{\ell_2}-2} |J_i^\delta(\omega, j_\omega)|$$
$$\geq 0.$$

Step 3. Let ℓ_1 and ℓ_2 be integers defined in Step 2. For given $f_i = \prod_{\ell=1}^m X_\ell^{i_\ell}$, if there exists no i' $(\neq i)$ such that $\deg(f_i) = \deg(f_{i'})$ and $|J_i^\delta| \geq |J_{i'}^\delta|$, then by Step 2, we can conclude that $\ell_1 \geq \ell_2$. This means $(i_1, i_2, \ldots, i_m) = (q-1, \ldots, q-1, R, 0, \ldots, 0)$ where the number of $q-1$ is Q, $0 \leq R \leq q-2$ and $\deg(f_i) = Q(q-1)+R$. Therefore by Eq.(5A.2), $f_i = f_{i_{\max}}$.

Finally, by noting that the above discussion holds for any i and δ, we have the lemma. □

Lemma 5A.3 For $i, j \in \{1, 2, \ldots, n\}$ such that $\deg(f_i) < \deg(f_j)$, we have $\Lambda_{i_{\max}} \supset \Lambda_{j_{\max}}$.

(Proof) It is sufficient to prove it for the case when $\deg(f_i) + 1 = \deg(f_j)$. By Eqs.(5A.2) and (5A.3), $\Lambda_{i_{\max}}$ is rewritten as

$$\Lambda_{i_{\max}} = \{k : k \in \{0, 1, 2, \ldots, n\} \text{ such that } f_k = f_{i_{\max}} f_u \text{ where}$$
$$f_u = X_{Q+1}^{u_{Q+1}} X_{Q+2}^{u_{Q+2}} \cdots X_m^{u_m}, 0 \leq u_{Q+1} \leq q-1-R$$
$$0 \leq u_\ell \leq q-1 \text{ for } \ell = Q+2, Q+3, \ldots, m\}.$$

Note that by changing the condition on u_{Q+1} as $0 \leq u_{Q+1} \leq q-2-R$, we obtain the exactly similar expression for $\Lambda_{j_{\max}}$ and these expressions for $\Lambda_{i_{\max}}$ and $\Lambda_{j_{\max}}$ immediately imply $\Lambda_{i_{\max}} \supset \Lambda_{j_{\max}}$. □

(Proof of Theorem 5.4)

By noting that $\deg(f_{r+1}) = \deg(f_r) + 1$, we can write

$$\Lambda_i = \left(\bigcup_{\delta=0}^{\deg(f_r)} \Lambda_i^\delta \right) \bigcup \left(\bigcup_{\delta=\deg(f_{r+1})}^{m(q-1)} \Lambda_i^\delta \right).$$

Since $\deg(f_\ell) < \deg(f_{r+1})$ for $\ell = 1, 2, \ldots, r$, we have

$$\left(\bigcup_{\delta=0}^{\deg(f_r)} \Lambda_i^\delta \right) \bigcap \{r+1, r+2, \ldots, n\} = \emptyset.$$

On the other hand,

$$\overline{\Lambda}_i := \left(\bigcup_{\ell=\deg(f_{r+1})}^{m(q-1)} \Lambda_i^{\delta} \right) \subset \{r+1, r+2, \ldots, n\}.$$

Thus

$$\mathcal{A}_i = \{r+1, r+2, \ldots, n\} \setminus \Lambda_i = \{r+1, r+2, \ldots, n\} \setminus \overline{\Lambda}_i.$$

and $|\mathcal{A}_i| = n - r - |\overline{\Lambda}_i|$.

For $i \leq r$, we have from Lemma 5A.2 that

$$|\overline{\Lambda}_i| = \sum_{\delta=\deg(f_{r+1})}^{m(q-1)} |\Lambda_i^{\delta}| \geq \sum_{\delta=\deg(f_{r+1})}^{m(q-1)} |\Lambda_{i_{\max}}^{\delta}| = |\overline{\Lambda}_{i_{\max}}|.$$

Moreover, for $i \leq r$,

$$|\overline{\Lambda}_{i_{\max}}| \geq |\overline{\Lambda}_{r_{\max}}| = |\overline{\Lambda}_r|$$

by Lemma 5A.3. Thus $|\overline{\Lambda}_i| \geq |\overline{\Lambda}_r|$ for all $1 \leq i \leq r$.

Finally, $|\overline{\Lambda}_r|$ is equal to the number of $(j_1, j_2, \ldots, j_m) \neq (0, 0, \ldots, 0)$ satisfying

$$\begin{cases} j_\ell = 0 \text{ for } \ell = 1, 2, \ldots, Q, \\ 0 \leq j_{Q+1} \leq q - 1 - R, \\ 0 \leq j_\ell \leq q - 1 \text{ for } \ell = Q+2, Q+3, \ldots, m. \end{cases}$$

Thus $|\overline{\Lambda}_r| = (q-R)q^{m-(Q+1)} - 1$ and we have

$$\begin{aligned} g_B(C_r) &= n - r - |\overline{\Lambda}_r| \\ &= n - r - (q-R)q^{m-(Q+1)} + 1. \end{aligned}$$

□

5A.2 Proof of Lemma 5.5

It immediately follows from Eqs.(2.9) and (2.10) that for any element $f \in R(V)$,

$$f \in \langle \boldsymbol{X}^{\boldsymbol{\lambda}_1}, \boldsymbol{X}^{\boldsymbol{\lambda}_2}, \ldots, \boldsymbol{X}^{\boldsymbol{\lambda}_i} \rangle \Leftrightarrow \mathrm{mdeg}(f) \preceq \boldsymbol{\lambda}_i = \mathrm{mdeg}(\boldsymbol{X}^{\boldsymbol{\lambda}_i})$$

and

$$f \in \langle \boldsymbol{X}^{\boldsymbol{\lambda}_1}, \boldsymbol{X}^{\boldsymbol{\lambda}_2}, \ldots, \boldsymbol{X}^{\boldsymbol{\lambda}_{i-1}} \rangle \Leftrightarrow \mathrm{mdeg}(f) \prec \boldsymbol{\lambda}_i, \tag{5A.8}$$

where $\langle f_1, f_2, \ldots, f_i \rangle$ indicates a linear space spanned by $f_1, f_2, \ldots, f_i$.

Lemma 5A.4 For V given in Eq.(5.16), let $B(V)$ be the basis of $R(V)$ given in Eq.(2.10) with a monomial order defined in Definition 5.7. Denote $f_i \in B(V)$ as $f_i = x^{\ell_i} y^{m_i}$ $(i = 1, 2, \ldots, n)$. Then $m_i < a$ for all $i = 1, 2, \ldots, n$.

(Proof) Since $f_i = x^{\ell_i} y^{m_i} \in B(V)$, $(\ell_i, m_i) \in \Lambda(V)$ by the definition of $B(V)$. Let $f := h(x, y)$ where $h(x, y)$ is given in Eq.(2.4). Then $f \in I(V)$ and $\mathrm{mdeg}(f) = (0, a)$. Assume $m_i \geq a$, then

$$\mathrm{mdeg}(f_i) = (\ell_i, m_i) = \mathrm{mdeg}(f) + (\ell_i, m_i - a).$$

This implies $\mathrm{mdeg}(f_i) \notin \Lambda(V)$ by Eq.(2.8), a contradiction. □

Lemma 5A.5 Let $f \in F[\boldsymbol{X}]$ be a nonzero monomial such that $\tau(f) < \tau(f_i)$ for some $f_i \in B(V)$. Then $\rho(\overline{f}) < i$.

(Proof) By Definition 5.7 and $\psi(f) < \psi(f_i)$, we have $\mathrm{mdeg}(f) \prec_{ab} \mathrm{mdeg}(f_i)$. Furthermore, by noting that $\mathrm{mdeg}(f_i) = \mathrm{mdeg}(\overline{f}_i)$ by Proposition 2.5-(i), we have from Lemma 2.2-(i) that

$$\mathrm{mdeg}(\overline{f}) \preceq_{ab} \mathrm{mdeg}(f) \prec_{ab} \mathrm{mdeg}(f_i) = \mathrm{mdeg}(\overline{f}_i),$$

which implies $\rho(\overline{f}) < \rho(\overline{f}_i) = i$ by Eq.(5A.8). □

Lemma 5A.6 Let $f \in F[\boldsymbol{X}]$ be a nonzero monomial such that $\tau(f) = \tau(f_i)$ for some $f_i \in B(V)$. Then $\rho(\overline{f}) = i$.

(Proof) If $f = f_i$, then $\rho(\overline{f}) = i$. Thus in the following, we assume that $f \neq f_i$.

Denote $f := x^{\ell} y^{m}$ and $f_i := x^{\ell_i} y^{m_i}$ $(\ell, \ell_i, m, m_i \geq 0)$. Since $\psi(f) = \psi(f_i)$, we have

$$a(\ell - \ell_i) + b(m - m_i) = 0. \tag{5A.9}$$

If $\ell = \ell_i$, then $m = m_i$ and $f = f_i$. Therefore, $\ell \neq \ell_i$ and $m \neq m_i$.

In Eq.(5A.9), since a and b are relatively prime, we have $a | m - m_i$ and $b | \ell - \ell_i$. In addition, since $f_i \in B(V)$, we have $m_i < a$ by Lemma 5A.4. Thus, noting $m, m_i \geq 0$, there exists a non-negative integer s such that

$$m - m_i = as, \ \ell - \ell_i = -bs. \tag{5A.10}$$

For $1 \leq k \leq s = (m - m_i)/a$, let

$$\left.\begin{aligned} \ell[k] &:= \ell_i - bk, \\ m[k] &:= m_i + ak. \end{aligned}\right\} \tag{5A.11}$$

Then it holds that $\tau(x^{\ell[k]}y^{m[k]}) = \tau(f_i)$ for $k = 1, 2, \ldots, s$. In what follows, in order to show that $\rho(\overline{x^{\ell}y^{m}}) = \rho(\overline{x^{\ell[s]}y^{m[s]}}) = i$, we show that $\rho(\overline{x^{\ell[k]}y^{m[k]}}) = i$ for $k = 1, 2, \ldots, s$ by the induction on k.

(i) For $k = 1$: Since $y^a = \alpha_{(0,a)}^{-1}(h(x,y) - \alpha_{(b,0)}x^b - h'(x,y))$ by Eq.(2.4), we can write

$$\begin{aligned} x^{\ell[1]}y^{m[1]} &= x^{\ell[1]}y^{m[1]-a}y^a \\ &= \alpha_{(0,a)}^{-1}x^{\ell[1]}y^{m[1]-a}h(x,y) - \alpha_{(0,a)}^{-1}\alpha_{(b,0)}x^{\ell[1]+b}y^{m[1]-a} \\ &\quad -\alpha_{(0,a)}^{-1}\sum_{\substack{0\le\mu,\nu,\\ \mu+\nu\le b,\\ a\mu+b\nu<ab}} \alpha_{(\mu,\nu)}x^{\ell[1]+\mu}y^{m[1]-a+\nu}. \end{aligned} \tag{5A.12}$$

For the first term of the right hand side of Eq.(5A.12), we see $x^{\ell[1]}y^{m[1]-a}h(x,y) \in I(V)$. For the second term, we have from Eq.(5A.11) that $x^{\ell[1]+b}y^{m[1]-a} = x^{\ell_i}y^{m_i} = f_i$. And finally, for each terms in summation of the third term in Eq.(5A.12), by noting that $a\mu + b\nu < ab$, we have

$$\begin{aligned} \tau(x^{\ell[1]+\mu}y^{m[1]-a+\nu}) &= a\ell[1] + bm[1] + a\mu + b\nu - ab \\ &< a\ell[1] + bm[1] = \tau(f_i). \end{aligned}$$

Thus by Lemma 5A.5, $\rho(\overline{x^{\ell[1]+\mu}y^{m[1]-a+\nu}}) < i$ for all μ and ν. From the above discussion, we conclude that $\rho(\overline{x^{\ell[1]}y^{m[1]}}) = i$.

(ii) Assume that $\rho(\overline{x^{\ell[k]}y^{m[k]}}) = i$ for $k < s$. As seen in Eq.(5A.12), we can also write

$$\begin{aligned} x^{\ell[k+1]}y^{m[k+1]} &= \alpha_{(0,a)}^{-1}x^{\ell[k+1]}y^{m[k+1]-a}h(x,y) - \alpha_{(0,a)}^{-1}\alpha_{(b,0)}x^{\ell[k+1]+b}y^{m[k+1]-a} \\ &\quad -\alpha_{(0,a)}^{-1}\sum_{\substack{0\le\mu,\nu,\\ \mu+\nu\le b,\\ a\mu+b\nu<ab}} \alpha_{(\mu,\nu)}y^{\ell[k+1]+\mu}y^{m[k+1]-a+\nu}. \end{aligned} \tag{5A.13}$$

From the similar discussion to the case $k = 1$, we have $x^{\ell[k+1]}y^{m[k+1]-a}h(x,y) \in h(x,y)$ and $\rho(\overline{x^{\ell[k+1]+\mu}y^{m[k+1]-a+\nu}}) < i$ for all μ and ν.

Moreover, we have from Eq.(5A.11) that

$$\begin{aligned} \ell[k+1] + b &= \ell_i - b(k+1) + b = \ell[k], \\ m[k+1] - a &= m_i + a(k+1) - a = m[k]. \end{aligned}$$

Thus $\rho(\overline{x^{\ell[k+1]+b}y^{m[k+1]-b}}) = \rho(\overline{x^{\ell[k]}y^{m[k]}}) = i$ by the hypothesis of the induction. Then we conclude $\rho(\overline{x^{\ell[k+1]}y^{m[k+1]}}) = i$ and complete the proof. □

(Proof of Lemma 5.5)

Since $\tau(f_k)-\tau(f_i) \in S_{ab}$, there exists a monomial $f \in F[\boldsymbol{X}]$ with $\tau(f)=\tau(f_k)-\tau(f_i)$, and we have $\tau(f_i f)=\tau(f_k)$. Thus it follows from Lemma 5A.6 that

$$\rho(\overline{f_i f}) = k. \tag{5A.14}$$

Let $j := \rho(\overline{f})$ and note that $f_j \in B(V)$. Then the following three cases may be possible.

(i) $\tau(f)=\tau(f_j)$, then $f_j = f \in B(V)$.

(ii) $\tau(f) < \tau(f_j)$, then $\rho(\overline{f}) < j$ by Lemma 5A.5 contradicting with the assumption $j := \rho(\overline{f})$.

(iii) $\tau(f) > \tau(f_j)$, then by the definition of j, $\overline{f}$ can be expressed as $\overline{f} = \sum_{\nu=1}^{j} \alpha_\nu f_\nu$ ($\alpha_\nu \in F$). Since $\tau(f_\nu) \le \tau(f_j)$ for $\nu = 1, 2, \ldots, j$ and $\tau(f_j) < \tau(f)$, we have

$$\tau(f_i f_\nu) \le \tau(f_i f_j) < \tau(f_i f) = \tau(f_k),\ \nu = 1, 2, \ldots, j.$$

Thus $\rho(\overline{f_i f_\nu}) < k$ for $\nu = 1, 2, \ldots, j$ by Lemma 5A.5. Therefore

$$\rho(\overline{f_i f}) = \rho(\overline{f_i \overline{f}}) = \max\{\rho(\overline{f_i f_\nu}) : \nu = 1, 2, \ldots, j\} < k,$$

which contradicts with Eq.(5A.14).

5A.3 Proof of Lemma 5.6

We prove the contraposition. If $\tau(f_k) - \tau(f_i) \in S_{ab}$, by Lemma 5.5, there exists $f_j \in B(V)$ such that $\rho(\overline{f_i f_j}) = k$. Thus it suffices to show that (f_i, f_j) is well behaving.

For u, v with $1 \le u \le i$, $1 \le v \le j$ and $u+v < i+j$, it is obvious from the definition of τ that

$$\tau(f_u f_v) \le \tau(f_i) + \tau(f_j)$$

and equality holds only when $u = i$ and $v = j$. Thus $\tau(f_u f_v) < \tau(f_i f_j) = \tau(f_k)$ and $\rho(\overline{f_u f_v}) < \rho(\overline{f_i f_j}) = k$. □

Chapter 6

General Conclusion

In this dissertation, we have discussed various bounds of linear codes and their applications to algebraic geometry codes.

In Chapter 3, we have compared the parameters of AG codes on C_{ab} with those of BCH codes. From this comparison, we have drawn a necessary condition under which AG codes can be better than BCH codes. More precisely, in order for AG codes on C_{ab} to have better parameters than those of BCH codes, it is necessary that the number of check symbols of AG codes on C_{ab} is not less than $\min\{g+a, n-g\}$ where n and g denote the code length and the genus of C_{ab}, respectively.

In Chapter 4, we have discussed the dimension of subfield subcodes of arbitrary linear codes. First, we have proposed a lower bound for the dimension of subfield subcodes which exceeds the bound given by Stichtenoth. Next, we have improved the proposed bound by restricting the codes to AG codes on C_{ab}. It has been also shown that calculating this improved bound is much easier than calculating the true dimension from the parity check matrix by Gaussian elimination. Finally, we have shown through an example that the improved bound for the dimension of subfield subcodes of AG codes on C_{ab} can exceed the true dimension of a shortened BCH code with the same code length and designed distance, while the conventional bound cannot. This implies that by using the improved bound, some codes which were regarded as inefficient by conventional estimates are rediscovered to be good codes.

In Chapter 5, we have investigated a lower bound for the generalized Hamming weights of linear codes. Conventional lower bounds are only applicable to some special classes of codes or require some structures of codes, while the proposed bound can be applied to

arbitrary linear codes and requires only a basis of F_q^n whose first $n-k$ elements constitute the row vectors of parity check matrix of the $[n,k]$ code. We have also derived a sufficient condition for a linear code to be t-th rank MDS.

The newly obtained results in this dissertation have shown some directions of deriving linear codes with good parameters. However, there is still room for further studies. To conclude the dissertation, we list some problems not yet solved.

(i) In order to design AG codes on C_{ab} with desired parameters, not only the necessary condition derived in Chapter 3 but also a sufficient condition which can be easily verified is required.

(ii) The lower bound for the dimension of subfield subcodes of AG codes on C_{ab} given in Chapter 4 is easily calculated from a, b, q (the order of the field over which subfield subcodes are defined) and n (code length). In order to determine n, however, we need to fix a defining polynomial of C_{ab} and calculate rational points on it, which requires not a small amount of computation. Therefore a lower bound which is expressed without the code length n as its parameter and can be calculated with less computational complexity is desired.

(iii) The bound for the generalized Hamming weights proposed in Chapter 5 depends on the order of elements in B. It has not been clarified which order makes the proposed bound tighter. A bound which does not depend on the order of elements in B is also desired.

Bibliography

[1] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms: An introduction to computational algebraic geometry and commutative algebra*, Second edition, Springer-Verlag, 1996.

[2] O. Endler, *Valuation Theory* (Universitext), Berlin, Germany, Springer-Verlag, 1972.

[3] G. L. Feng and T. R. N. Rao, "Decoding Algebraic-Geometric Codes up to the Designed Minimum Distance," *IEEE Trans. Inform. Theory*, vol.IT-39, No.1, pp.37–45, 1993.

[4] G. L. Feng and T. R. N. Rao, "A Simple Approach for Construction of Algebraic-Geometric Codes from Affine Plane Curves," *IEEE Trans. Inform. Theory*, vol.IT-40, No.4, pp.1003–1012, 1994.

[5] G. L. Feng and T. R. N. Rao, "Improved Geometric Goppa Codes," *IEEE Trans. Inform. Theory*, vol.IT-41, No.6, pp.1678–1693, 1995.

[6] G. L. Feng, T. R. N. Rao, G. A. Berg, and J. Zhu, "Generalized Bezout's Theorem and Its Applications in Coding Theory," *IEEE Trans. Inform. Theory*, vol.IT-43, No.6, pp.1799–1819, 1997.

[7] V. D. Goppa, "Codes on Algebraic Curves," *Soviet Math. Dokl.* vol.24, No.1, pp.170–172, 1981.

[8] P. Heijnen and R. Pellikaan, "Generalized Hamming weights of q-ary Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol.IT-44, No.1, pp. 181–196, 1998.

[9] A. Jennings, *Matrix Computation for Engineers and Scientists*, John Wiley & Sons. 1977.

[10] N. Kamiya and S. Miura, "On a Recursive Decoding Algorithm for Codes Defined on Algebraic Curves with at Most One Higher Order Cusp," *IEICE Trans. Fundamentals*, vol.J76-A, No.3, pp.480–492, 1993. (in Japanese)

[11] T. Kasami, T. Takata, T. Fujiwara and S. Lin, "On the Optimum Bit Orders with Respect to the State Complexity of Trellis Diagrams for Binary Linear Codes," *IEEE Trans. Inform. Theory*, vol. 39, No.1, pp. 242–245, 1993.

[12] T. Kasami, T. Tanaka, T. Fujiwara and S. Lin, "On Complexity of Trellis Structure of Linear Block Codes," *IEEE Trans. Inform. Theory*, vol. 39, No.3, pp. 1057–1064, 1993.

[13] G. L. Katsman and M. A. Tsfasman, "A Remark on Algebraic Geometric Codes," *Contemp. Math.*, vol.93, pp.197–199, 1989.

[14] C. Kirfel and R. Pellikaan, "The Minimum Distance of Codes in an Array Coming from Telescopic Semigroups," *IEEE Trans. Inform. Theory*, vol.IT-41, No.6, pp.1720–1732, 1995.

[15] S. Lang, *Algebra*, 3rd Ed., Addison-Wesley Publishing Company, 1993.

[16] J. H. van Lint and T. A. Springer, "Generalized Reed-Solomon Codes from Algebraic Geometry," *IEEE Trans. Inform. Theory*, vol.IT-33, No.3, pp.305–309, 1987.

[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[18] Mathematical Society of Japan, ed., *Encyclopedic Dictionary of Mathematics*, 3rd edition, Iwanami Shoten, Tokyo, 1985.

[19] S. Miura, "Algebraic Geometric Codes on Certain Plane Curves," *IEICE Trans. Fundamentals*, vol.J75-A, No.11, pp.1735–1745, Nov. 1992. (in Japanese)

[20] S. Miura, "On the Generalized Hamming Weights of Geometric Goppa Codes," *Proc. of the 1993 IEICE Fall Conference*, vol.1, pp.316–317, 1993. (in Japanese)

[21] S. Miura, "On Feng-Rao Designed Minimum Distance of Geometric Goppa Codes," *Proceedings of 16th SITA*, pp.427–430, Nov., 1993. (in Japanese)

[22] S. Miura, "Constructive Theory of Algebraic Curves," *Proceedings of 17th SITA*, pp.461–464, Nov., 1994. (in Japanese)

[23] S. Miura, "Geometric Goppa Codes on Affine Algebraic Variety," *Proceedings of 18th SITA*, pp.243–246, 1995. (in Japanese)

[24] S. Miura, "Linear Codes on Affine Algebraic Varieties," *IEICE Trans. Fundamentals*, vol.J81-A, No.10, pp.1386–1397, 1998. (in Japanese)

[25] S. Miura, "Linear Codes on Affine Algebraic Curves," *IEICE Trans. Fundamentals*, vol.J81-A, No.10, pp.1398–1421, 1998. (in Japanese)

[26] S. Miura, Ph.D dissertation, Univ. of Tokyo, 1997.

[27] C. Munuera, "On the Generalized Hamming Weights of Geometric Goppa Codes," *IEEE Trans. Inform. Theory*, vol.IT-40, No.6, pp.2092–2099, 1994.

[28] R. Pellikaan, "The Shift Bound for Cyclic, Reed-Muller and Geometric Goppa Code," *Arithmetic, Geometry and Coding Theory*, R. Pellikaan, M. Perret, and S. G. Vlăduţ, Eds., Berlin, Germany: Walter de Gruyter, pp. 155–175, 1996.

[29] R. Pellikaan, "On the Existence of Order Functions," to be published in *J. Statist. Planning and Inference.*

[30] R. Pellikaan, B.-Z. Shen, and G. J. M. van Wee, "Which linear codes are algebraic-geometric?," *IEEE Trans. Inform. Theory*, vol.37, No.3, pp.583–602, 1991.

[31] T. Shibuya, H. Jinushi, S. Miura and K. Sakaniwa, "On Designed Distance of Algebraic Geometric Codes," *Proceedings of ISITA '94*, pp.47–52, Nov., 1994.

[32] T. Shibuya, H. Jinushi, S. Miura and K. Sakaniwa, "On the Performance of Algebraic Geometric Codes," *IEICE Trans. Fundamentals*, vol.E79-A, no.6, pp.928–937, 1996.

[33] T. Shibuya, R. Matsumoto and K. Sakaniwa "An Improved Bound for the Dimension of Subfield Subcodes," *IEICE Trans. Fundamentals*, vol.E80-A, no.5, pp876–880, 1997.

[34] T. Shibuya, J. Mizutani and K. Sakaniwa, "On Generalized Hamming Weights of Codes Constructed on Affine Algebraic Sets," *Proceedings of AAECC-12, Lecture Notes in Computer Science*, vol.1255, Springer-Verlag, pp.311–320, 1997.

[35] T. Shibuya, J. Mizutani and K. Sakaniwa, "On Lower Bound of Generalized Hamming Weights for Codes on C_{ab}," *Proceedings of 20th SITA*, vol.2, pp. 853–856, 1997.

[36] T. Shibuya, J. Mizutani and K. Sakaniwa, "On Generalized Hamming Weights of Codes Constructed on Affine Algebraic Varieties," *IEICE Trans. Fundamentals*, vol.E81–A, No.10, pp.1979–1989, 1998.

[37] H. Stichtenoth, "On the Dimension of Subfield Subcodes," *IEEE Trans. Inform. Theory*, vol.36, pp.90–93, 1990.

[38] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, 1993.

[39] H. Stichtenoth and C. Voß, "Generalized Hamming Weights of Trace Codes," *IEEE Trans. Inform. Theory*, vol.40, No.2, pp.554-558, 1994.

[40] M. A. Tsfasman, "Goppa Codes That Are Better Than the Varshamov–Gilbert Bound," *Problemy Peredachi Informatsii*, vol.18, No.3, pp.3–6, 1982.

[41] M. A. Tsfasman and S. G. Vlăduţ, "Geometric Approach to Higher Weights," *IEEE Trans. Inform. Theory*, vol.IT-41, No.6, pp.1564–1588, 1995.

[42] V. K. Wei, "Generalized Hamming Weights for Linear Codes," *IEEE Trans. Inform. Theory*, vol.IT-37, No.5, pp.1412–1418, 1991.

[43] M. Wirtz, "On the Parameters of Goppa Codes," *IEEE Trans. Inform. Theory*, vol.34, pp.1341–1343, 1988.

[44] L. H. Ozarow and A. D. Wyner, "The Wire-Tap Channel II," *AT&T Bell Laboratories Technical Journal*, Vol.63, No.10, pp.2135–2157, 1984.

[45] K. Yamanishi, "On Derivation of Good Codes Based on Elliptic Codes and Hyper Elliptic Codes," *IEICE Trans. Fundamentals*, vol.J71-A, no.10, pp.1936-1946, 1988. (in Japanese)

[46] K. Yamanishi, "On Construction and Performance Evaluation of Fermat Codes," *IEICE Trans. Fundamentals*, vol.J72-A, no.3, pp.597-607, 1989. (in Japanese)

[47] K. Y. Yang, P. V. Kumar and H. Stichtenoth, "On the Weight Hierarchy of Geometric Goppa Codes," *IEEE Trans. Inform. Theory*, vol.IT-40, No.3, pp.913–920, 1994.

Publications Related to the Dissertation

Regular papers

1. T. Shibuya, H. Jinushi, S. Miura, K. Sakaniwa, "On the Performance of Algebraic Geometric Codes," *IEICE Trans. Fundamentals*, vol.E79–A, no.6, pp.928–937, 1996.

2. T. Shibuya, R. Matsumoto and K. Sakaniwa, "An Improved Bound for the Dimension of Subfield Subcodes," *IEICE Trans. Fundamentals*, vol.E80–A, no.5, pp876–880, 1997.

3. T. Shibuya, J. Mizutani and K. Sakaniwa, "On Generalized Hamming Weights of Codes Constructed on Affine Algebraic Sets," Springer LNCS 1255, AAECC-12, pp.311-320, 1997.

4. T. Shibuya, R. Matsumoto and K. Sakaniwa, "Simple Estimation for the dimension of subfield subcodes of AG codes," *IEICE Trans. Fundamentals*, vol.E80–A, no.11, pp.2058-2065, 1997.

5. T. Shibuya, J. Mizutani and K. Sakaniwa, "On Generalized Hamming Weights of Codes Constructed on Affine Algebraic Varieties," *IEICE Trans. Fundamentals*, vol.E81–A, no.10, pp.1979–1989, 1998.

6. T. Shibuya, R. Hasegawa and K. Sakaniwa, "A Lower Bound for Generalized Hamming Weights and Condition for t-th Rank MDS," conditionally accepted in *IEICE Trans. Fundamentals*.

International conferences

1. T. Shibuya, H. Jinushi, K. Sakaniwa, "On Minimum Lee Distance of Generalized Reed-Muller Code," *Proceedings of Singapore ICCS/ISITA '92*, pp.603-607, 1992.

2. T. Shibuya, H. Jinushi, K. Sakaniwa, "On Minimum Lee Distance of Generalized Reed-Muller Code," *Proceedings of International Symposium on Information Theory* (ISIT'93), p.36, 1993.

3. T. Shibuya, H. Jinushi, S. Miura, K. Sakaniwa, "On Designed Distance of Algebraic Geometric Codes," *Proceedings of International Symposium on Information Theory and its Applications* (ISITA'94), vol.1, pp.47–52, 1994.

4. T. Shibuya, R. Matsumoto and K. Sakaniwa, "On the Simple Estimation for the Dimension of Subfield Subcodes of AG Codes," *Proceedings of International Symposium on Information Theory and its Applications* (ISITA'96), vol.1, pp.24–30, 1996.

5. T. Shibuya, R. Matsumoto and K. Sakaniwa, "An Improved Lower Bound for the Dimension of Subfield Subcodes of AG Codes," *Proceedings of Second Shanghai Conference on Designs, Codes and Finite Geometries*, pp.28–29, 1996

6. T. Shibuya, J. Mizutani and K. Sakaniwa, "On the Comparison of Lower Bounds for Generalized Hamming Weights," *Proc. of Taiwan-Japan Joint Workshop on the Latest Development of Telecommunication Research*, (TJCOM '98), vol.1, pp.23-28, 1998.

7. T. Shibuya and K. Sakaniwa, "Lower Bound on Generalized Hamming Weights in Terms of a Notion of Well-behaving," *Proceedings of International Symposium on Information Theory* (ISIT'98), p.96, 1998.

8. T. Shibuya, R. Hasegawa and K. Sakaniwa, "On Generalized Hamming Weight of Linear Codes and a Sufficient Condition of tth-rank MDS Codes," *Proceedings of International Symposium on Information Theory and its Applications* (ISITA'98), vol.1, pp.323-326, 1998.

Domestic conferences and workshops

1. T. Shibuya, H. Jinushi and K. Sakaniwa, "On Minimum Lee Distances of Generalized Reed-Muller Codes," *IEICE Technical Report*, vol.IT92-28, pp.37–40, 1992. (in Japanese)

2. T. Shibuya, H. Jinushi and K. Sakaniwa, "On Designed Distance of Algebraic Geometric Codes," *IEICE Technical Report*, vol.IT93-112, pp.37–42, 1994. (in Japanese)

3. T. Kobayashi, T. Shibuya, H. Jinushi and K. Sakaniwa, "On Minimum Lee Distance of Extended Generalized Reed-Muller Codes," *The Proceedings of The 17 th Symposium on Information Theory and Its Applications* (SITA'94), vol.2, pp.643–646, 1994. (in Japanese)

4. T. Shibuya, H. Jinushi, S. Miura and K. Sakaniwa, "On the Performance of Algebraic Geometric Codes," *The Proceedings of The 17 th Symposium on Information Theory and Its Applications* (SITA'94), vol.2, pp.647–650, 1994. (in Japanese)

5. T. Shibuya and K. Sakaniwa, "On the Dimensions of Subfield Subcodes of AG codes," *The Proceedings of The 18 th Symposium on Information Theory and Its Applications* (SITA'95), vol.1, pp.247–250, 1995. (in Japanese)

6. T. Kaneko, K. Genko, T. Shibuya, I. Yamada and K. Sakaniwa, "Error Control Based on Structure of Sentences," *Proceedings of the 1996 IEICE general conference*, A-248, 1996. (in Japanese)

7. T. Shibuya and K. Sakaniwa, "On the Dimension of Subfield Subcodes of AG Codes," *Proceedings of the 1996 IEICE general conference*, A-243, 1996. (in Japanese)

8. T. Shibuya, J. Mizutani and K. Sakaniwa, "Lower Bounds for Generalized Hamming Weights of Linear Codes on Affine Algebraic Varieties," *IEICE Technical Report*, IT96-57, pp.61–66, 1997.

9. T. Shibuya, J. Mizutani and K. Sakaniwa, "Lower Bounds for Generalized Hamming Weights of Linear Codes on Affine Algebraic Varieties," *Proceedings of the 1997 IEICE general conference*, A-6-2.

10. S. Ochi, T. Shibuya and K. Sakaniwa, "On Iterative Decoding Using Parallel-form Decodes," *The Proceedings of The 20 th Symposium on Information Theory and Its Applications* (SITA'97), vol.2, pp.849–852, 1997.

11. T. Shibuya, J. Mizutani, and K. Sakaniwa, "On Lower Bound of Generalize Hamming Weights for Codes on Cab," *The Proceedings of The 20 th Symposium on Information Theory and Its Applications* (SITA'97), vol.2, pp.853–856, 1997.

12. S. Ochi, T. Shibuya and K. Sakaniwa, I. Yamada, "Fast Decoding of Turbo-Codes by Processing MAP Algorithm in Parallel," *IEICE Technical Report*, IT97-57, pp.1–6, 1998. (in Japanese)