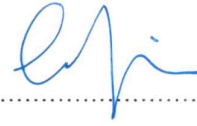


ON ADDITIVE CYCLIC CODES

APPROVED BY:

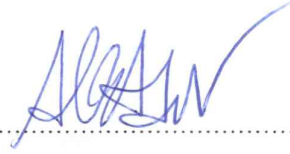
Assoc. Prof. Dr. Cem Güneri
(Thesis Supervisor)



Prof. Dr. Alev Topuzoğlu



Prof. Dr. Albert Levi



Asst. Prof. Dr. Burcu Gülmez Temür



Asst. Prof. Dr. Seher Tutdere



DATE OF APPROVAL: 04.08.2016

ON ADDITIVE CYCLIC CODES

by
FUNDA ÖZDEMİR

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy

Sabancı University

August 2016

ON ADDITIVE CYCLIC CODES

APPROVED BY:

Assoc. Prof. Dr. Cem Güneri
(Thesis Supervisor)

Prof. Dr. Alev Topuzoğlu

Prof. Dr. Albert Levi

Asst. Prof. Dr. Burcu Gülmez Temür

Asst. Prof. Dr. Seher Tutdere

DATE OF APPROVAL: 04.08.2016

©Funda Özdemir 2016

All Rights Reserved



ON ADDITIVE CYCLIC CODES

Funda Özdemir

Mathematics, PhD Dissertation, 2016

Thesis Supervisor: Assoc. Prof. Dr. Cem Güneri

Thesis Co-Supervisor: Prof. Dr. Ferruh Özbudak

Keywords: Additive cyclic code, algebraic curve over a finite field, Hasse-Weil bound, BCH bound, complementary dual code.

Abstract

In this thesis we consider two problems related to additive cyclic codes. In the first part, we obtain a lower bound on the minimum distance of additive cyclic codes via the number of rational points on certain algebraic curves over finite fields. This is an extension of the analogous bound for classical cyclic codes. Our result is the only general bound on such codes aside from Bierbrauer's BCH bound. We compare our bound's performance against the BCH bound for additive cyclic codes in a special case and provide examples where it yields better results. In the second part, we study complementary dual additive cyclic codes. We give a sufficient condition for a special class of additive cyclic codes to be complementary dual.

TOPLAMSAL DEVİRSEL KODLAR ÜZERİNE

Funda Özdemir

Matematik, Doktora Tezi, 2016

Tez Danışmanı: Doç. Dr. Cem Güneri

Tez Eş Danışmanı: Prof. Dr. Ferruh Özbudak

Anahtar Kelimeler: Toplamsal devirsel kod, sonlu bir cisim üzerinde cebirsel eğri, Hasse-Weil sınırı, BCH sınırı, bütünleyici dual kod.

Özet

Bu tez çalışmasında, toplamsal devirsel kodlara ilişkin iki ayrı problem ele alınmıştır. İlk bölümde, sonlu cisimler üzerinde tanımlı bazı cebirsel eğrilerin rasyonel nokta sayısı üzerinden toplamsal devirsel kodların minimum uzaklığına bir alt sınır elde edilmiştir. Bu sınır, klasik devirsel kodlar için yazılmış benzer bir sınırın genellemesidir. Bu sonuç, Bierbrauer'in BCH sınırı dışında bu kodlar üzerine yazılmış tek genel sınırdır. Özel bir durumda, toplamsal devirsel kodlar üzerindeki bu sınırın BCH sınırına karşı performans kıyaslaması yapılmıştır ve daha iyi sonuç verdiği örnekler sunulmuştur. İkinci bölümde, bütünleyici dual toplamsal devirsel kodlar çalışılmıştır. Toplamsal devirsel kodların özel bir alt sınıfının bütünleyici dual olabilmesi için yeter şart verilmiştir.

to my beloved baby and my love



ACKNOWLEDGMENTS

First of all, I would like to express my sincere and deepest gratitude to my thesis advisor Cem Güneri for his valuable guidance, support and encouragement throughout my PhD study. I have been inspired by his insight, and I have learned a lot from him. I would also like to extend my sincerest thanks to my co-advisor, Ferruh Özbudak, for his guidance and suggestions. He certainly helped to improve the quality of this work. I am really honored and consider myself very lucky to have them as my advisors.

I would also like to thank my thesis committee members: Alev Topuzoğlu, Albert Levi, Burcu Gülmez Temür and Seher Tutdere. I learned a lot from his classes during my PhD study so I also thank Henning Stichtenoth. My special thanks also go to Patrick Solé for his guidance and hospitality during a period of research that I spent in Paris.

I was fortunate to be a member of Sabancı University and to know some good friends here who always supported me. Their friendship is a valuable experience for me. I also thank my friend Kamil Otal in METU for his help with Magma computations.

Last but not least, I would like to express my indebtedness to my parents who have motivated and supported me unconditionally throughout my life. My most special thanks goes to my husband Ahmet Emre Özdemir for his endless love and support. To my beloved baby, it was great to defend this thesis with you. Cannot wait the change you will bring in our life!

I was supported fully by The Scientific and Technological Research Council of Turkey (TÜBİTAK) BİDEB 2211 National PhD Scholarship Programme during my PhD study and 2214-A International Doctoral Research Fellowship Programme for 5 months during my last year; thereby I would like to thank TÜBİTAK for their continued support.

Contents

Abstract	iv
Özet	v
Acknowledgments	vii
Introduction	1
1 Background on Coding Theory	3
1.1 Linear Codes	3
1.2 Cyclic Codes	4
1.2.1 Basic Definitions and the BCH Bound	4
1.2.2 Algebraic Geometric Bound	7
1.3 Linear Complementary Dual Codes	9
2 Additive Cyclic Codes	10
2.1 Notation and Definition	10
2.2 Algebraic Geometric Bound on the Minimum Distance	12
2.3 The Dual and the BCH Bound on the Minimum Distance	16
2.4 Comparison of the Bounds	24
3 Complementary Dual Additive Cyclic Codes	29
3.1 A Condition for Complementary Dual Codes	29
3.2 Examples	31
Bibliography	33

Introduction

Coding theory is concerned with improving reliability of communication over noisy channels. This is done by adding redundancy to information messages so that the transmission errors can be detected or even corrected. Linear codes are the most important classes of codes and widely studied because of their algebraic structure, which provides easier implementation. Cyclic codes form a fundamental subclass of linear codes. They are closed under all cyclic shifts. This extra combinatorial structure yields a richer algebraic structure for cyclic codes as they can be represented as ideals of certain rings. The most important parameter of a cyclic code is its minimum distance which is difficult to find in general. Therefore it is important to find general bounds for the minimum distance of a cyclic code. We will be interested in two such bounds in this dissertation. The first one is the BCH bound (Bose- Ray-Chaudhuri- Hocquenghem), which depends on the information given by the zero set of the code. The second bound is due to Wolfmann who used algebraic curves over finite fields and the Hasse-Weil bound on their number of rational points [17]. Main tools in relating the weights in cyclic codes and the number of rational points on certain algebraic curves are the trace representation of the codes and the additive version of Hilberts Theorem 90.

In this thesis, we focus on additive cyclic codes, introduced by Bierbrauer [2], which are nonlinear generalizations of cyclic codes. The alphabet of these codes is not a finite field but a vector space E over a ground field \mathbb{F}_q . Bierbrauer computed the dimension and proved a BCH type bound for the minimum distance of additive cyclic codes. In the first part of this dissertation, we obtain a Hasse-Weil type bound on additive cyclic codes, hence extend the analogous result from cyclic codes. Our bound is much easier to compute compared to the BCH bound. Moreover, we compare our bound's performance against the BCH bound in a special case and present examples where it yields better results.

Linear complementary dual (LCD) codes are linear codes that meet their dual trivially. These codes were introduced by Massey in [14]. In the same paper, Massey also showed that asymptotically good LCD codes exist and they provide an optimum linear coding solution for the two-user binary adder channel. He left open the question of whether these codes achieve the Gilbert-Varshamov bound, which is proved later by Sendrier ([15]). LCD codes were rediscovered recently for their applications to cryptography in the context of side channel attacks ([5]). So far, cyclic LCD codes were characterized completely by Yang and Massey in [18], and quasi-cyclic LCD codes were partially studied in [6] and characterized by using their concatenated structure in [11]. The second part of this dissertation is devoted to the study of complementary dual subclass of additive cyclic codes. We give a sufficient condition for a special class of additive cyclic codes to be complementary dual.

Chapter 1

Background on Coding Theory

1.1 Linear Codes

Let \mathbb{F}_q be the finite field with q elements, where q is a prime power. A q -ary linear code of length n and dimension k is a k -dimensional vector subspace of \mathbb{F}_q^n . The elements of the code are called *codewords*. The *minimum distance* of the code is minimum *weight* of its nonzero codewords, where the weight of a codeword is the number of coordinates that are not zero. A linear code of length n , dimension k and minimum distance d is referred to as $[n, k, d]$ code. The *dual* of the code C , denoted as C^\perp , is the orthogonal complement of C in \mathbb{F}_q^n , where the dual is usually taken with respect to Euclidean inner product on \mathbb{F}_q^n . One can also consider the dual with respect to other inner products.

Since a linear code is a vector space, it admits a basis. Any codeword can be expressed as the linear combination of these basis vectors. A *generator matrix* G of an $[n, k, d]$ code C is a $k \times n$ matrix whose rows form a basis for C . If G has the form $[I_k | A]$, where I_k is the $k \times k$ identity matrix, then G is said to be in *standard form*. There are many generator matrices for a linear code, but there is a unique one in standard form.

Consider the extension $F = \mathbb{F}_{q^r}$ of degree r over \mathbb{F}_q . One can construct linear codes over \mathbb{F}_q by starting with a linear code over F . Let

$$\text{Tr} : F \longrightarrow \mathbb{F}_q$$

denote the *trace* mapping, which is defined by

$$\text{Tr}(a) = a + a^q + \cdots + a^{q^{r-1}}, \text{ for } a \in F.$$

Definition 1.1.1. Let C be an F -linear code of length n . Then

- $C|_{\mathbb{F}_q} := C \cap \mathbb{F}_q^n$ is called the *subfield subcode* of C .
- $\text{Tr}(C) := \{(\text{Tr}(c_1), \dots, \text{Tr}(c_n)) : (c_1, \dots, c_n) \in C\}$ is called the *trace code* of C .

It is obvious that $C|_{\mathbb{F}_q}$ and $\text{Tr}(C)$ are q -ary linear codes of length n . The following famous theorem due to Delsarte is important to see the relation between trace code and subfield subcode.

Theorem 1.1.2. (Delsarte) [3, Theorem 12.14] For any F -linear code C of length n , the following holds:

$$(\text{Tr}(C))^\perp = (C^\perp)|_{\mathbb{F}_q}.$$

Definition 1.1.3. An F -linear code C is called *Galois closed* with respect to \mathbb{F}_q if it is invariant under the Frobenius automorphism $x \mapsto x^q$ of F over \mathbb{F}_q , i.e. if $C = C^q$. The *Galois closure* of C is the smallest Galois closed code containing C and it is denoted by \bar{C} .

Theorem 1.1.4. Let C be an F -linear code of length n .

- i. $\text{Tr}(\bar{C}) = \text{Tr}(C)$
- ii. If C is Galois closed, then
 - a. $\text{Tr}(C) = C|_{\mathbb{F}_q}$
 - b. $\dim_{\mathbb{F}_q}(\text{Tr}(C)) = \dim_F(C)$

Proof. See Theorems 12.16 and 12.17 in [3]. □

1.2 Cyclic Codes

1.2.1 Basic Definitions and the BCH Bound

Cyclic codes form an important subclass of linear codes and they have been widely studied in the literature. Cyclic codes have been generalized in various ways

and the topic of this thesis is one of these generalizations in nonlinear setting.

Definition 1.2.1. A linear code C is called *cyclic* if $(c_{n-1}, c_0, \dots, c_{n-2})$ is in C whenever $(c_0, c_1, \dots, c_{n-1})$ is in C .

In other words a linear code that is closed under cyclic shift is called a cyclic code. It is easy to verify that the dual code of a cyclic code is also cyclic.

A cyclic code can be viewed as an ideal in a polynomial ring. Hence, they have richer algebraic structure than ordinary linear codes. Consider the following \mathbb{F}_q -vector space isomorphism:

$$\begin{aligned} \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q[x]/\langle x^n - 1 \rangle \\ (a_0, a_1, \dots, a_{n-1}) &\rightarrow a_0 + a_1x + \dots + a_{n-1}x^{n-1}. \end{aligned}$$

Due to this correspondence, any codeword $c = (c_0, c_1, \dots, c_{n-1}) \in C$ can be identified with the polynomial $c(x) = \sum_{i=0}^{n-1} c_i x^i$. Since multiplication by x in the ring $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ corresponds to a cyclic shift, if $c(x)$ is in C then $xc(x) \bmod x^n - 1$ is also in C . This observation makes the following characterization obvious.

Proposition 1.2.2. [13, Theorem 6.1.3] *A linear code C in \mathbb{F}_q^n is cyclic if and only if C is an ideal in $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$.*

Since $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ is a principal ideal ring, an ideal C is generated by a nonzero unique monic polynomial $g(x)$ of the least degree, which is called the *generator polynomial* of C . We write $C = \langle g(x) \rangle$. Note that $g(x)$ divides $x^n - 1$. If the dimension of C is k , then the degree of $g(x)$ is $n - k$ and $\{g(x), xg(x), \dots, x^{k-1}g(x)\}$ forms a basis for C . Vice versa, each monic divisor $g(x) \in \mathbb{F}_q[x]$ of $x^n - 1$ is the generator polynomial of some cyclic code of dimension $k = n - \deg(g)$ in $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$.

For a polynomial $f(x) \in \mathbb{F}_q[x]$, its monic *reciprocal polynomial* is defined as

$$f^*(x) = f_0^{-1} x^{\deg(f)} f(x^{-1})$$

where f_0 is the nonzero constant term of $f(x)$. If $f(x) = f^*(x)$, then $f(x)$ is said to be *self-reciprocal*. Note that if $f(x)$ divides $x^n - 1$, then so does $f^*(x)$.

Proposition 1.2.3. [13, Section 6.2] *Let $C = \langle g(x) \rangle$ be a cyclic code of length n*

and dimension k . Then the dual code C^\perp is cyclic of dimension $n - k$ with the generator polynomial $h^*(x)$, where $h(x) = (x^n - 1)/g(x)$.

Definition 1.2.4. The q -cyclotomic coset mod n containing i is the subset of $\mathbb{Z}/n\mathbb{Z}$ defined by

$$C_i = \{i, qi, \dots, q^{b-1}i\},$$

where b is the smallest nonnegative integer such that $q^b i \equiv i \pmod{n}$.

It is easy to see that two cyclotomic cosets are either equal or disjoint, so the cyclotomic cosets partition $\mathbb{Z}/n\mathbb{Z}$.

In the rest of this chapter, assume that $\gcd(n, q) = 1$ by which we guarantee that $x^n - 1$ has distinct roots in its splitting field over \mathbb{F}_q . Let r be the multiplicative order of $q \pmod{n}$. Then $F = \mathbb{F}_{q^r}$ is the splitting field of $x^n - 1$. Let α be a primitive n^{th} root of unity in F over \mathbb{F}_q . We have

$$x^n - 1 = \prod_{j=1}^t f_j(x) = \prod_{i=0}^{n-1} (x - \alpha^i),$$

where f_j 's are distinct irreducible polynomials over \mathbb{F}_q . If α^i is a root of $f_j(x)$, then α^{qi} is also its root. So there is a one-to-one correspondence between irreducible factors of $x^n - 1$ and q -cyclotomic cosets mod n .

Definition 1.2.5. Let C be a q -ary cyclic code of length n with the generator polynomial $g(x) = \prod_{j=1}^s f_{i_j}(x)$ and $\{i_1, \dots, i_s\}$ be a set of representatives of the cyclotomic cosets corresponding to $\{f_{i_j}\}_{j=1}^s$. Then

- the set $\{i_1, \dots, i_s\}$ is called a *basic zero set* of C .
- the collection of q -cyclotomic cosets $\bigcup_{j=1}^s C_{i_j}$ is called the *zero set* of C .

Theorem 1.2.6. (BCH bound) [13, Theorem 6.6.2] *If the zero set of a cyclic code C of length n contains t consecutive integers mod n , then the minimum distance $d(C)$ of C is at least $t + 1$.*

This well-known result can be generalized. The underlying reason is that if α is a primitive n^{th} root of unity then α^j , for any j with $\gcd(j, n) = 1$, is also a primitive n^{th} root of unity. Before stating the generalized BCH bound, we need the following definition.

Definition 1.2.7. $A \subseteq \mathbb{Z}/n\mathbb{Z}$ is called an *interval* of length u if there is an integer j , which is relatively prime to n , such that $A = \{jl, j(l+1), \dots, j(l+u-1)\} \pmod{n}$ for some integer $l \in \mathbb{Z}/n\mathbb{Z}$.

Theorem 1.2.8. [2, Theorem 8] *If the zero set of a cyclic code C contains an interval of size t , then $d(C) \geq t + 1$.*

1.2.2 Algebraic Geometric Bound

Besides the BCH bound, there exists another lower bound on the minimum distance of cyclic codes which is obtained by relating the weights of codewords and the number of rational points on certain algebraic curves (see [17]). For this relation we need the trace description of cyclic codes via the basic zero sets of their duals, and the additive form of Hilbert's Theorem 90.

Proposition 1.2.9. [17, Proposition 2.1] *Let C be a q -ary cyclic code of length $n = q^r - 1$ and $\{j_1, \dots, j_\nu\} \subseteq \mathbb{Z}/n\mathbb{Z}$ be a basic zero set of C^\perp . For a primitive element α of \mathbb{F}_{q^r} , we have the following trace representation for C :*

$$C = \left\{ (\text{Tr}(f(\alpha^0)), \dots, \text{Tr}(f(\alpha^{n-1}))) : f(x) = \sum_{k=1}^{\nu} a_k x^{j_k} \in \mathbb{F}_{q^r}[x] \right\}.$$

Theorem 1.2.10. (Hilbert's Theorem 90) *For $x \in F = \mathbb{F}_{q^r}$, $\text{Tr}(x) = 0$ if and only if $y^q - y = x$ for some $y \in F$.*

Note that if $y^q - y = x$, then for any $y_0 \in \mathbb{F}_q$, the element $y + y_0$ also satisfies the same equation. Now let C be a q -ary cyclic code of length $n = q^r - 1$ (primitive case) with dual's basic zero set $\{j_i\}_{i=1}^{\nu} \subseteq \mathbb{Z}/n\mathbb{Z}$ where $j_i \geq 1$ for all i . Then the weight of the codeword $c_f \in C$ is determined by $f \in F[x]$ as follows (by Hilbert's Theorem 90):

$$\begin{aligned} wt(c_f) &= n - |\{x \in F : \text{Tr}(f(x)) = 0\}| + 1 \\ &= q^r - \frac{|\mathcal{X}_f^{af}(F)|}{q}. \end{aligned}$$

Here, $|\mathcal{X}_f^{af}(F)|$ denotes the number of affine F -rational points of the Artin-Schreier type curve

$$\mathcal{X}_f : y^q - y = f(x).$$

To write a lower bound on the minimum distance of C , we need an upper bound on the number of affine F -rational points of each curve in the family

$$\mathcal{F} = \{y^q - y = f(x) : f(x) = \sum_{k=1}^{\nu} a_k x^{j_k} \in F[x]\}.$$

If $\deg f$ is relatively prime to q , then the corresponding curve in \mathcal{F} is irreducible. For the number $|\mathcal{X}_f(F)|$ of F -rational points of any curve \mathcal{X}_f in \mathcal{F} with genus $g(\mathcal{X}_f)$ and $\gcd(\deg(f), q) = 1$, Serre's improvement on the celebrated Hasse-Weil bound ([16, Theorem 5.3.1]) states that

$$|\mathcal{X}_f(F)| \leq q^r + 1 + g(\mathcal{X}_f)[2\sqrt{q^r}]. \quad (1.2.1)$$

Since each curve in \mathcal{F} has only one F -rational point at infinity, we have

$$|\mathcal{X}_f^{af}(F)| \leq q^r + g(\mathcal{X}_f)[2\sqrt{q^r}].$$

Proposition 1.2.11. [16, Proposition 6.4.1] *The genus of the curve $\mathcal{X}_f \in \mathcal{F}$ with $\gcd(\deg(f), q) = 1$ is*

$$g(\mathcal{X}_f) = \frac{1}{2}(q-1)(\deg(f)-1).$$

Following the observations above, we are ready to state the following algebraic geometric bound on the minimum distance of cyclic codes.

Theorem 1.2.12. [17, Theorem 4.3] *Let C be a cyclic code of length $n = q^r - 1$ over \mathbb{F}_q such that $\{j_1, \dots, j_\nu\} \subseteq \mathbb{Z}/n\mathbb{Z}$ is a basic zero set of its dual, where $\gcd(j_i, q) = 1$ for all i . Let $j = \max\{j_i : 1 \leq i \leq \nu\}$. Then*

$$d(C) \geq q^r - q^{r-1} - \frac{(q-1)(j-1)[2\sqrt{q^r}]}{2q}.$$

Remark 1.2.13. It is possible to generalize the bound above to the imprimitive case (i.e. to the case where n properly divides $q^r - 1$). See [17] for details. Moreover, the Hasse-Weil bound on reducible curves (i.e. curves with $\gcd(\deg(f), q) \neq 1$) was obtained in [8] to extend Wolfmann's minimum distance bound on cyclic codes to a more general class of cyclic codes.

1.3 Linear Complementary Dual Codes

A *linear complementary dual* (LCD) code is a linear code C satisfying $C \cap C^\perp = \{0\}$. The next characterization is due to Massey [14].

Proposition 1.3.1. *Let C be a linear code of length n and dimension k with a generator matrix G . Then C is an LCD code if and only if the matrix GG^T is invertible, where G^T denotes the transpose of G .*

The complete characterization for LCD subclass of cyclic codes is given by Yang and Massey ([18]).

Theorem 1.3.2. *Let C be a q -ary cyclic code of length n with the generator polynomial $g(x)$. Then C is an LCD code if and only if $g(x)$ is self-reciprocal and all monic irreducible factors of $g(x)$ have the same multiplicity in $g(x)$ and in $x^n - 1$.*

Recall that if $\gcd(n, q) = 1$, then $x^n - 1$ has no repeated factors in $\mathbb{F}_q[x]$. We have thus the following corollary.

Corollary 1.3.3. *If $g(x)$ is the generator polynomial of a q -ary cyclic code C of length n with $\gcd(n, q) = 1$, then C is an LCD code if and only if $g(x)$ is self-reciprocal.*

Other than Proposition 1.3.1 and Theorem 1.3.2, there are two more general results on LCD codes. Firstly, Sendrier showed that LCD codes meet the Gilbert-Varshamov bound ([15]). Secondly, Güneri-Özkaya-Solé characterized quasi-cyclic LCD codes in [11] and studied further properties in this code class, which is another generalization of classical cyclic codes.

Chapter 2

Additive Cyclic Codes

Additive cyclic codes were introduced by Bierbrauer as nonlinear generalizations of cyclic codes ([2]). Results presented in Sections 2.2, 2.3 and 2.4 appeared in [10].

2.1 Notation and Definition

Let q be a prime power, $F = \mathbb{F}_{q^r}$ and $E = \mathbb{F}_q^m$ throughout this chapter, where $m \leq r$ are positive integers. Let $n \mid (q^r - 1)$ be a positive integer, W be the multiplicative subgroup of F^* of order n and α be a generator of W . Fix $A = \{i_1, \dots, i_s\} \subset \mathbb{Z}/n\mathbb{Z}$. Let

$$\mathcal{P}(A) := \{a_1x^{i_1} + \dots + a_sx^{i_s} : a_1, \dots, a_s \in F\},$$

which is an F -linear space of polynomials and set

$$\mathcal{B}(A) := \{(f(\alpha^0), \dots, f(\alpha^{n-1})) : f(x) \in \mathcal{P}(A)\} \subset F^n.$$

Let $\Gamma = \{\gamma_1, \dots, \gamma_m\} \subset F$ be a linearly independent set over \mathbb{F}_q . Define an F -linear code of length mn

$$\begin{aligned} (\mathcal{B}(A), \Gamma) := \{ & (\gamma_1 f(\alpha^0), \dots, \gamma_m f(\alpha^0); \dots \\ & \dots ; \gamma_1 f(\alpha^{n-1}), \dots, \gamma_m f(\alpha^{n-1})) : f(x) \in \mathcal{P}(A)\}. \end{aligned}$$

Consider the \mathbb{F}_q -linear mapping

$$\begin{aligned}\phi_\Gamma : F &\longrightarrow E \\ x &\longmapsto (\text{Tr}(\gamma_1 x), \dots, \text{Tr}(\gamma_m x)),\end{aligned}$$

where Tr denotes the trace map from F to \mathbb{F}_q . Note that ϕ_Γ is surjective since Γ is linearly independent. Extend ϕ_Γ naturally as follows:

$$\begin{aligned}\phi_\Gamma : F^n &\longrightarrow E^n \\ (x_1, \dots, x_n) &\longmapsto (\phi_\Gamma(x_1), \dots, \phi_\Gamma(x_n)).\end{aligned}$$

Definition 2.1.1. An *additive cyclic code* of length n over E is defined as

$$\phi_\Gamma(\mathcal{B}(A)) = \left\{ \phi_\Gamma\left((f(\alpha^0), \dots, f(\alpha^{n-1}))\right) : f(x) \in \mathcal{P}(A) \right\}.$$

The set A is called the *defining set* of the code.

Remark 2.1.2. The code $\phi_\Gamma(\mathcal{B}(A))$ is an additive subgroup of E^n and it is closed under cyclic shift. Consider the codeword

$$c_f = (\phi_\Gamma(f(\alpha^0)), \dots, \phi_\Gamma(f(\alpha^{n-1})))$$

in $\phi_\Gamma(\mathcal{B}(A))$ determined by $f(x) = \sum_{j=1}^s \lambda_j x^{i_j} \in \mathcal{P}(A)$. For $g(x) = \sum_{j=1}^s \lambda_j \alpha^{-i_j} x^{i_j} \in \mathcal{P}(A)$, we have

$$(\phi_\Gamma(f(\alpha^{n-1})), \phi_\Gamma(f(\alpha^0)), \dots, \phi_\Gamma(f(\alpha^{n-2}))) = (\phi_\Gamma(g(\alpha^0)), \phi_\Gamma(g(\alpha^1)), \dots, \phi_\Gamma(g(\alpha^{n-1}))),$$

which is also a codeword in $\phi_\Gamma(\mathcal{B}(A))$. Hence, the name additive cyclic is justified. If we view the code in \mathbb{F}_q^{mn} as

$$\begin{aligned}\phi_\Gamma(\mathcal{B}(A)) = \{ &(\text{Tr}(\gamma_1 f(\alpha^0)), \dots, \text{Tr}(\gamma_m f(\alpha^0)); \dots \\ &\dots; \text{Tr}(\gamma_1 f(\alpha^{n-1})), \dots, \text{Tr}(\gamma_m f(\alpha^{n-1}))) : f(x) \in \mathcal{P}(A) \},\end{aligned}$$

then it is an \mathbb{F}_q -linear code of length mn over \mathbb{F}_q , which is equal to $\text{Tr}((\mathcal{B}(A), \Gamma))$. Moreover, as a length mn code over \mathbb{F}_q , it is closed under shift by m coordinates. Hence, over \mathbb{F}_q , $\phi_\Gamma(\mathcal{B}(A))$ is a quasi-cyclic code of length mn and index m .

Remark 2.1.3. Classical cyclic codes correspond to the special case $m = 1$. In this case $\phi_\Gamma(\mathcal{B}(A))$ is the cyclic code of length n over \mathbb{F}_q whose dual's basic zero set is contained in $\{i_1, \dots, i_s\}$ (cf. Proposition 1.2.9).

2.2 Algebraic Geometric Bound on the Minimum Distance

In this section, we obtain a Hasse-Weil type bound on the minimum distance of additive cyclic codes.

Let $n = q^r - 1$ and assume that $i_j > 0$ for all j in this section. Then we have $f(0) = 0$ for any $f(x) \in \mathcal{P}(A)$. Hence, the weight of the codeword $c_f = (\phi_\Gamma(f(\alpha^0)), \dots, \phi_\Gamma(f(\alpha^{n-1})))$ in $\phi_\Gamma(\mathcal{B}(A))$ is

$$\begin{aligned} wt(c_f) &= n - |\{x \in F : \phi_\Gamma(f(x)) = 0\}| + 1 \\ &= q^r - |\{x \in F : \text{Tr}(\gamma_i f(x)) = 0 \text{ for all } 1 \leq i \leq m\}|. \end{aligned} \quad (2.2.1)$$

Let us define the following \mathbb{F}_q -linear subspace in F :

$$V := \{x \in F : \text{Tr}(\gamma_1 x) = \dots = \text{Tr}(\gamma_m x) = 0\}. \quad (2.2.2)$$

Since $\{\gamma_1, \dots, \gamma_m\}$ is linearly independent over \mathbb{F}_q , V is an \mathbb{F}_q -subspace of codimension m in F ([7, Proposition 2.1]).

A polynomial $A(T) \in F[T]$ is called *q-additive*, if it is of the form

$$A(T) = a_m T^{q^m} + a_{m-1} T^{q^{m-1}} + \dots + a_0 T.$$

We will use the following result.

Lemma 2.2.1. [7, Corollary 2.5] *For every \mathbb{F}_q -linear subspace U in F of codimension m , there exists a uniquely determined monic q -additive polynomial $A(T) \in F[T]$ of degree q^m , which splits in F and satisfies*

$$U = \text{Im}(A) = \{A(y) : y \in F\}.$$

The following is now easy to observe.

Proposition 2.2.2. *Let U be an \mathbb{F}_q -subspace of codimension m in F and let $A(T) \in F[T]$ be the monic q -additive polynomial attached to U as in Lemma 2.2.1. Define*

$$B(T) := \prod_{u \in U} (T - u) \in F[T],$$

which is another q -additive polynomial. Then

$$U = \text{Im}(A) = \text{Ker}(B) \quad \text{and} \quad B(A(T)) = T^{q^r} - T.$$

Proof. $B(T)$ is q -additive by Theorem 3.52 in [12]. From the definition of $B(T)$, it is clear that $\text{Ker}(B) = U$. Since $U = \text{Im}(A)$ by Lemma 2.2.1, we have

$$B(T) = \prod_{u \in \text{Im}(A)} (T - u) = \prod_{y \in F} (T - A(y)).$$

Then we have the following composition

$$B(A(T)) = \prod_{y \in F} (A(T) - A(y)) = \prod_{y \in F} A(T - y),$$

where the last equality is due to $A(T)$ being q -additive. Since $B(A(x)) = 0$ for all x in F , $T^{q^r} - T$ divides $B(A(T))$. We also have $\deg B(A(T)) = q^{r-m}q^m = q^r$. Therefore, $B(A(T)) = T^{q^r} - T$. □

Remark 2.2.3. Let $U = \{x \in F : \text{Tr}(x) = 0\}$ be a codimension 1 \mathbb{F}_q -subspace of F . Then it is easily seen that $B(T) = \text{Tr}(T)$ and $A(T) = T^q - T$ so that $\text{Im}(A) = U = \text{Ker}(B)$. This, in fact, is the well-known Hilbert's Theorem 90 (cf. Theorem 1.2.10). So, Proposition 2.2.2 can be viewed as a generalization of Hilbert's Theorem 90.

By (2.2.1) and (2.2.2), computing the weight of the codeword $c_f \in \phi_\Gamma(\mathcal{B}(A))$ requires the determination of the number of $x \in F$ such that $f(x) \in V$. Let $A(T)$ and $B(T)$ be the q -additive polynomials of degree q^m and q^{r-m} , respectively, that are attached to V as in Proposition 2.2.2. By the same proposition, we have

$$f(x) \in V \text{ for } x \in F \text{ if and only if } A(y) = f(x) \text{ for some } y \in F.$$

Moreover, if $A(y) = f(x)$ then $A(y + y_0) = A(y) = f(x)$ for all $y_0 \in \text{Ker}(A)$. Note that there are $\deg A = q^m$ such y_0 's and all lie in F since A splits in F (cf. Lemma 2.2.1). Hence,

$$wt(c_f) = q^r - \frac{|\mathcal{X}_f^{af}(F)|}{q^m}, \quad (2.2.3)$$

where $|\mathcal{X}_f^{af}(F)|$ denotes the number of affine F -rational points on the curve \mathcal{X}_f defined by

$$A(Y) = f(X). \quad (2.2.4)$$

These observations lead to the following, which is an extension of the algebraic geometric bound on the distance of classical cyclic codes to additive cyclic codes.

Theorem 2.2.4. *Consider the additive cyclic code $\phi_\Gamma(\mathcal{B}(A))$ of length $n = q^r - 1$ over E , where $A = \{i_1, \dots, i_s\} \subset \mathbb{Z}/n\mathbb{Z}$. Assume that $\gcd(i_j, q) = 1$ for all j and let $i = \max\{i_j : 1 \leq j \leq s\}$. Then,*

$$d(\phi_\Gamma(\mathcal{B}(A))) \geq q^r - q^{r-m} - \frac{(q^m - 1)(i - 1)\lfloor 2\sqrt{q^r} \rfloor}{2q^m}.$$

Proof. Since the weights of all codewords are related to F -rational affine points on the family $\mathcal{F} = \{A(Y) = f(X) : f(X) \in \mathcal{P}(A)\}$, writing an upper bound on the number of affine F -rational points that applies to all members of \mathcal{F} will yield a lower bound on the minimum distance of $\phi_\Gamma(\mathcal{B}(A))$. The assumption on i_j 's guarantee that any curve in \mathcal{F} (except for the one with $f(X) = 0$, which corresponds to the zero codeword) is irreducible. Moreover, any such curve has one F -rational point at infinity. The number $(q^m - 1)(i - 1)/2$ is an upper bound on the genera of the curves in \mathcal{F} (see the proof of Corollary 2.11 in [8]). Therefore, Serre's improvement on the Hasse-Weil bound (1.2.1) yields

$$|\mathcal{X}^{af}(F)| \leq q^r + \frac{(q^m - 1)(i - 1)}{2} \lfloor 2\sqrt{q^r} \rfloor,$$

for any $\mathcal{X} \in \mathcal{F}$. The result follows by (2.2.3). \square

Remark 2.2.5. Wolfmann's bound for classical cyclic codes corresponds to $m = 1$ in the above result (cf. Remark 2.1.3). In that case, curves (2.2.4) related to codewords are Artin-Schreier type curves, i.e. $A(T) = T^q - T$ in (2.2.4) (cf. Remark 2.2.3).

Remark 2.2.6. We can generalize our bound in Theorem 2.2.4 to the imprimitive case. For a proper divisor n of $q^r - 1$, the weight of the codeword $c_f = (\phi_\Gamma(f(\alpha^0)), \dots, \phi_\Gamma(f(\alpha^{n-1}))) \in \phi_\Gamma(\mathcal{B}(A))$ where α is a generator of the multiplicative subgroup W of F^* of order n is

$$\begin{aligned} wt(c_f) &= n - |\{x \in W : \phi_\Gamma(f(x)) = 0\}| \\ &= n - |\{x^{\frac{q^r-1}{n}} \in F : \phi_\Gamma(f(x^{\frac{q^r-1}{n}})) = 0\}| + 1 \\ &= n + 1 - |\{x^{\frac{q^r-1}{n}} \in F : \text{Tr}(\gamma_i f(x^{\frac{q^r-1}{n}})) = 0 \text{ for all } 1 \leq i \leq m\}|. \end{aligned}$$

By (2.2.2) and the argument following Remark 2.2.3, we get

$$\begin{aligned} wt(c_f) &= n + 1 - |\{x^{\frac{q^r-1}{n}} \in F : f(x^{\frac{q^r-1}{n}}) \in V\}| \\ &= \frac{n}{q^r - 1} \left(q^r - \frac{|\mathcal{X}_f^{af}(F)|}{q^m} \right) \end{aligned}$$

where $|\mathcal{X}_f^{af}(F)|$ denotes the number of affine F -rational points on the curve \mathcal{X}_f defined by

$$A(Y) = f(X^{\frac{q^r-1}{n}}).$$

Hence, we obtain the following minimum distance bound

$$d(\phi_\Gamma(\mathcal{B}(A))) \geq \frac{n}{q^r - 1} (q^r - q^{r-m} - \frac{(q^m - 1)(i - 1)\lfloor 2\sqrt{q^r} \rfloor}{2q^m})$$

where $i = \max\{\frac{q^r-1}{n}i_j \bmod q^r - 1 : 1 \leq j \leq s\}$.

A Hasse-Weil type bound for additive cyclic codes in Theorem 2.2.4 can be optimized in the following way.

Corollary 2.2.7. *Let S be the set of positive integers ν which are relatively prime to $n = q^r - 1$ and $(\nu i_j \bmod n)$ is relatively prime to q for all $1 \leq j \leq s$. Let $i_\nu = \max\{\nu i_j \bmod n : 1 \leq j \leq s\}$ and $\iota = \min\{i_\nu : \nu \in S\}$. The following bound holds for the code $\phi_\Gamma(\mathcal{B}(A))$ in Theorem 2.2.4:*

$$d(\phi_\Gamma(\mathcal{B}(A))) \geq q^r - q^{r-m} - \frac{(q^m - 1)(\iota - 1)\lfloor 2\sqrt{q^r} \rfloor}{2q^m}.$$

Proof. Since $\gcd(\nu, n) = 1$, the mapping $x \rightarrow x^\nu$ is a permutation of F^* . Hence, the number of affine F -rational points of the curve defined by $A(Y) = f(X^{\nu \bmod n})$

is the same as that of the curve defined by $A(Y) = f(X)$. Note that on the code's side, this change amounts to considering an additive cyclic code which is equivalent to $\phi_\Gamma(\mathcal{B}(A))$. Therefore, one can estimate the weights in $\phi_\Gamma(\mathcal{B}(A))$ by all such curves (i.e. any $\nu \in S$). Moreover, the assumption that $\gcd(q, \nu i_j \bmod n) = 1$ (for all j) guarantees that $A(Y) = f(X^{\nu \bmod n})$ defines an irreducible curve again. Hence, the bound of Theorem 2.2.4 holds for any $\nu \in S$, replacing i by i_ν . The best lower bound is obtained by ι . \square

Remark 2.2.8. Note that the assumption $\gcd(i_j, q) = 1$ (for all j) in Theorem 2.2.4 is made to guarantee that the equation

$$A(Y) = \lambda_1 X^{i_1} + \cdots + \lambda_s X^{i_s} \quad (2.2.5)$$

defines an irreducible curve over F whose genus and hence the Hasse-Weil bound on the number of its F -rational points are known. The Hasse-Weil bound on reducible curves was obtained in [8] to extend Wolfmann's minimum distance bound on cyclic codes (cf. Remark 1.2.13). The same result can also be used for extending Theorem 2.2.4. This involves determining degrees of the so-called left greatest common divisors for corresponding additive polynomials. For the purpose of determining such possible degrees, the notion of LGCD trees are used (see [8] for details).

2.3 The Dual and the BCH Bound on the Minimum Distance

Our purpose in this section is to introduce the BCH bound due to Bierbrauer which is a generalization of the BCH bound for cyclic codes and compute it for $\phi_\Gamma(\mathcal{B}(A))$. We will continue to use the notation introduced above. Bierbrauer proved the following BCH type bound for additive cyclic codes.

Theorem 2.3.1. [2, Theorem 8] *If A contains an interval of length $t \bmod n$, then $d(\phi_\Gamma(\mathcal{B}(A))^\perp) \geq t + 1$.*

Our goal is to compare the bound in Theorem 2.2.4 for $\phi_\Gamma(\mathcal{B}(A))$ with the bound above. For this, we need to find $B \subset \mathbb{Z}/n\mathbb{Z}$ and a set Γ' such that $\phi_\Gamma(\mathcal{B}(A)) = \phi_{\Gamma'}(\mathcal{B}(B))^\perp$. Here the dual is taken with respect to the Euclidean dot product on

E^n : $(u_1, \dots, u_n) \cdot (v_1, \dots, v_n) = \sum_{i=1}^n u_i \cdot v_i$, for $u_i, v_i \in E = \mathbb{F}_q^m$, where $u_i \cdot v_i$ is the Euclidean product.

Lemma 2.3.2. *Let A, B be subsets of $\mathbb{Z}/n\mathbb{Z}$ and Γ, Γ' be \mathbb{F}_q -linearly independent subsets of F . If $\overline{(\mathcal{B}(A), \Gamma)}^\perp = \overline{(\mathcal{B}(B), \Gamma')}$, then $\text{Tr}(\mathcal{B}(A), \Gamma) = (\text{Tr}(\mathcal{B}(B), \Gamma'))^\perp$.*

Proof. By Theorem 1.1.4 i and the assumption, we have

$$\text{Tr}(\mathcal{B}(A), \Gamma) = \text{Tr}(\overline{(\mathcal{B}(A), \Gamma)}) = \text{Tr}(\overline{(\mathcal{B}(B), \Gamma')^\perp}).$$

Theorem 1.1.2 and 1.1.4 ii imply that

$$\text{Tr}(\overline{(\mathcal{B}(B), \Gamma')^\perp}) = (\overline{(\mathcal{B}(B), \Gamma')|_{\mathbb{F}_q}})^\perp = (\text{Tr}(\overline{(\mathcal{B}(B), \Gamma')}))^\perp.$$

The result follows from Theorem 1.1.4 i. □

From the above Lemma, our problem reduces to finding $B \subset \mathbb{Z}/n\mathbb{Z}$ and an \mathbb{F}_q -independent set $\Gamma' = \{\gamma'_1, \dots, \gamma'_m\} \subset F$ such that

$$\overline{(\mathcal{B}(A), \Gamma)}^\perp = \overline{(\mathcal{B}(B), \Gamma')}.$$

In other words, we can work with codes over the extension F . The following useful fact will be needed.

Lemma 2.3.3. *If k is not a multiple of n , then*

$$\sum_{t=0}^{n-1} (\alpha^t)^k = 0.$$

Proof. Since k is not a multiple of n , $\alpha^k \neq 1$. Then we have

$$\sum_{t=0}^{n-1} (\alpha^t)^k = \frac{1 - (\alpha^k)^n}{1 - \alpha^k} = \frac{1 - (\alpha^n)^k}{1 - \alpha^k} = \frac{1 - 1}{1 - \alpha^k} = 0.$$

□

Definition 2.3.4. Let $Z \subset \mathbb{Z}/n\mathbb{Z}$ be a q -cyclotomic coset mod n . Define

$$V_F(Z) := \{(p_1(\alpha^0), \dots, p_m(\alpha^0); \dots \\ \dots ; p_1(\alpha^{n-1}), \dots, p_m(\alpha^{n-1})) : p_i(x) \in \mathcal{P}(Z)\}.$$

To simplify notation, we will denote the codeword in $V_F(Z)$ determined by $p_i(x) \in \mathcal{P}(Z)$ as $(p_1(x), \dots, p_m(x))$. Using this notation, we state the following fact on the Euclidean inner product of two vectors which will be referred to several times in the rest of this chapter.

Lemma 2.3.5. *If a and b are integers such that $a + b \not\equiv 0 \pmod{n}$, and c_1, \dots, c_m are elements of F , then*

$$(c_1 x^a, c_2 x^a, \dots, c_m x^a) \cdot (c_1 x^b, c_2 x^b, \dots, c_m x^b) = 0.$$

Proof. With our notation, the inner product above is the Euclidean product of the following vectors in F^{mn} :

$$\begin{pmatrix} c_1 \alpha^{0a} & \dots & c_m \alpha^{0a} \\ c_1 \alpha^a & \dots & c_m \alpha^a \\ c_1 \alpha^{2a} & \dots & c_m \alpha^{2a} \\ \vdots & \vdots & \vdots \\ c_1 \alpha^{(n-1)a} & \dots & c_m \alpha^{(n-1)a} \end{pmatrix} \cdot \begin{pmatrix} c_1 \alpha^{0b} & \dots & c_m \alpha^{0b} \\ c_1 \alpha^b & \dots & c_m \alpha^b \\ c_1 \alpha^{2b} & \dots & c_m \alpha^{2b} \\ \vdots & \vdots & \vdots \\ c_1 \alpha^{(n-1)b} & \dots & c_m \alpha^{(n-1)b} \end{pmatrix}.$$

For every $i \in \{1, \dots, m\}$, the i^{th} column contributes the following to the product:

$$c_i^2 \sum_{t=0}^{n-1} \alpha^{t(a+b)}.$$

By Lemma 2.3.3, this sum is 0 since $a + b \not\equiv 0 \pmod{n}$. □

In the following, by a Galois closure of a codeword $(p_1(x), \dots, p_m(x)) \in V_F(Z)$, we mean the F -space spanned by the vectors

$$(p_1(x), \dots, p_m(x)), (p_1(x)^q, \dots, p_m(x)^q), \dots, (p_1(x)^{q^{r-1}}, \dots, p_m(x)^{q^{r-1}}).$$

This space will be denoted by $\overline{(p_1(x), \dots, p_m(x))}$. The Galois closure of a set of codewords is similarly defined and denoted.

Lemma 2.3.6. *Let Z be a q -cyclotomic coset mod n . Then*

$$i. \dim V_F(Z) = m|Z|.$$

- ii. $\bigoplus_Z V_F(Z) = \bigoplus_Z V_F(-Z) = F^{mn}$, where Z runs through all q -cyclotomic cosets mod n .
- iii. $V_F(Z)^\perp = \bigoplus_{Z' \neq -Z} V_F(Z')$, where Z' runs through all q -cyclotomic cosets mod n .
- iv. If $p(x) \in \mathcal{P}(Z)$, then the Galois closure of $(\gamma_1 p(x), \dots, \gamma_m p(x))$ is contained in $V_F(Z)$. Therefore $\overline{(\mathcal{B}(Z), \Gamma)} \subseteq V_F(Z)$.

Proof. i. Consider the F -linear evaluation map

$$\begin{aligned} Ev : \mathcal{P}(Z) &\longrightarrow F^n \\ p(x) &\longmapsto (p(\alpha^0), \dots, p(\alpha^{n-1})), \end{aligned}$$

whose kernel is $\{0\}$, since any polynomial $p(x) \in \mathcal{P}(Z)$ has degree $< n$. Extend this map as

$$\begin{aligned} Ev : \mathcal{P}(Z)^m &\longrightarrow F^{mn} \\ (p_1(x), \dots, p_m(x)) &\longmapsto (Ev(p_1(x)), \dots, Ev(p_m(x))). \end{aligned}$$

Note that the image of this map is $V_F(Z)$. Hence the F -dimension of $V_F(Z)$ is $m \dim \mathcal{P}(Z) = m|Z|$.

ii. Note that the sum is indeed direct since $(p_1(x), \dots, p_m(x)) \in V_F(Z)$ is the same as $(q_1(x), \dots, q_m(x)) \in V_F(Z')$ if and only if $p_i(x) = q_i(x)$ for all $1 \leq i \leq m$ (by a degree argument). This is impossible since Z and Z' are distinct cosets. By part i, dimension of the direct sum is $m \sum_Z |Z| = mn$. Since each $V_F(Z)$ is contained in F^{mn} , the result follows.

iii. By Lemma 2.3.5, for a q -cyclotomic coset $Z' \neq -Z$, $V_F(Z') \subset V_F(Z)^\perp$. Hence the direct sum is contained in $V_F(Z)^\perp$. These two spaces have the same dimension by part i.

iv. This is clear since $\overline{(\gamma_1 p(x), \dots, \gamma_m p(x))}$ is an F -space and $p(x)^{q^i} \in \mathcal{P}(Z)$ for any i . The last assertion follows from the definition of $(\mathcal{B}(Z), \Gamma)$. \square

Corollary 2.3.7. i. $\overline{(\mathcal{B}(A), \Gamma)} = \bigoplus_Z [(\overline{(\mathcal{B}(A), \Gamma)} \cap V_F(Z))] = \bigoplus_Z \overline{(\mathcal{B}(A \cap Z), \Gamma)}$.

ii. $\overline{(\mathcal{B}(A), \Gamma)}^\perp = \bigoplus_Z [(\overline{(\mathcal{B}(A \cap Z), \Gamma)}^\perp \cap V_F(-Z))]$.

Proof.

i. Immediate from Lemma 2.3.6.

ii. Since $\overline{(\mathcal{B}(A), \Gamma)}^\perp \subseteq F^{mn}$ and $F^{mn} = \bigoplus_Z V_F(-Z)$ by Lemma 2.3.6 ii, we have the following decomposition

$$\begin{aligned} \overline{(\mathcal{B}(A), \Gamma)}^\perp &= \bigoplus_Z [\overline{(\mathcal{B}(A), \Gamma)}^\perp \cap V_F(-Z)] \\ &= \bigoplus_Z \left[\left[\bigoplus_{Z'} \overline{(\mathcal{B}(A \cap Z'), \Gamma)}^\perp \right] \cap V_F(-Z) \right] \\ &= \bigoplus_Z \left[\left[\bigcap_{Z'} \overline{(\mathcal{B}(A \cap Z'), \Gamma)}^\perp \right] \cap V_F(-Z) \right] \end{aligned}$$

where the second equality follows from part i and the third equality follows from the fact that $(U \oplus V)^\perp = U^\perp \cap V^\perp$ for any two subspaces U and V of the same space.

Fix a cyclotomic coset $Z = Z_0$. Then the corresponding summand of $\overline{(\mathcal{B}(A), \Gamma)}^\perp$ is

$$\begin{aligned} \left[\bigcap_{Z'} \overline{(\mathcal{B}(A \cap Z'), \Gamma)}^\perp \right] \cap V_F(-Z_0) &= \bigcap_{Z'} [\overline{(\mathcal{B}(A \cap Z'), \Gamma)}^\perp \cap V_F(-Z_0)] \\ &= \overline{(\mathcal{B}(A \cap Z_0), \Gamma)}^\perp \cap V_F(-Z_0) \end{aligned}$$

where the last equality follows from the fact that $\overline{(\mathcal{B}(A \cap Z'), \Gamma)}^\perp \cap V_F(-Z_0) = V_F(-Z_0)$ when $Z' \neq Z_0$, since $\bigoplus_{Z' \neq Z_0} V_F(-Z) \subseteq \overline{(\mathcal{B}(A \cap Z'), \Gamma)}^\perp$ by Lemma 2.3.6. Hence the result follows. \square

Recalling our goal, decomposition of the dual code in Corollary 2.3.7 reduces our task to finding $\Gamma' \subset F$ and $B_Z \subset \mathbb{Z}/n\mathbb{Z}$ for each summand such that

$$\overline{(\mathcal{B}(A \cap Z), \Gamma)}^\perp \cap V_F(-Z) = \overline{(\mathcal{B}(B_Z), \Gamma')}.$$

It then follows that $B = \bigcup_Z B_Z$.

The following result will yield the set B , hence the dual code, explicitly in the case $m = 2$. In fact, Theorem 2.3.8 provides an algorithm for determining the set B , which will be used for Magma computations in Section 2.4. We will denote the dimension of $\overline{(\mathcal{B}(B_Z), \Gamma')}$ by k_Z below. Note that this implies $\dim \phi_\Gamma(\mathcal{B}(A)) = mn - \sum_Z k_Z$ (cf. Theorem 1.1.4 ii).

Theorem 2.3.8. Let $m = 2$, $\Gamma = (1, \gamma)$ and $b = [\mathbb{F}_q(\gamma) : \mathbb{F}_q] > 1$. Let $Z = \{i, iq, \dots, iq^{s-1}\}$ be a q -cyclotomic coset mod n of length s . For $\Gamma' = (-\gamma, 1)$, we have the following:

- i. If $A \cap Z = \emptyset$, then $B_Z = -Z$ and $k_Z = 2s$.
- ii. If $A \cap Z = \{iq^{u_1}, iq^{u_2}, \dots, iq^{u_t}\}$ for some $0 \leq u_1 < u_2 < \dots < u_t \leq s-1$ and b does not divide s , then $B_Z = \emptyset$ and $k_Z = 0$.
- iii. If $A \cap Z = \{iq^{u_1}, iq^{u_2}, \dots, iq^{u_t}\}$ for some $0 \leq u_1 < u_2 < \dots < u_t \leq s-1$ and b divides s , set $\hat{A}_Z = \{iq^{u_a + \ell b} \bmod n : 0 \leq \ell \leq r-1\}$ for some $a \in \{1, \dots, t\}$. Then

- $B_Z = \emptyset$ and $k_Z = 0$ if $A \cap Z \not\subseteq \hat{A}_Z$.
- $B_Z = -\hat{A}_Z$ and $k_Z = s$ if $A \cap Z \subseteq \hat{A}_Z$.

Proof. i. If $A \cap Z = \emptyset$, then $\overline{(\mathcal{B}(A \cap Z), \Gamma)} = \{0\}$ which yields

$$\overline{(\mathcal{B}(A \cap Z), \Gamma)}^\perp \cap V_F(-Z) = V_F(-Z).$$

Note that $\dim V_F(-Z) = 2s$ and $\overline{(\mathcal{B}(-Z), \Gamma')} \subseteq V_F(-Z)$. By definition,

$$\overline{(\mathcal{B}(-Z), \Gamma')} = \overline{\text{Span}\{(-\gamma x^{-i}, x^{-i}), (-\gamma x^{-iq}, x^{-iq}), \dots, (-\gamma x^{-iq^{s-1}}, x^{-iq^{s-1}})\}}.$$

Codewords above, spanning $(\mathcal{B}(-Z), \Gamma')$, are F -linearly independent by Lemma 2.3.5, since orthogonality implies linear independence. Moreover, for every $a = 0, 1, \dots, s-1$, both $(-\gamma x^{-iq^a}, x^{-iq^a})$ and $(-\gamma^q x^{-iq^a}, x^{-iq^a})$ are in the Galois closure. These two codewords are linearly independent since $\gamma^q \neq \gamma$ (this would contradict $b > 1$). Hence, $\dim \overline{(\mathcal{B}(-Z), \Gamma')} = 2s$ and $\overline{(\mathcal{B}(-Z), \Gamma')} = V_F(-Z)$. Therefore $B_Z = -Z$.

ii. We have

$$\overline{(\mathcal{B}(A \cap Z), \Gamma)} = \overline{\text{Span}\{(x^{iq^{u_1}}, \gamma x^{iq^{u_1}}), (x^{iq^{u_2}}, \gamma x^{iq^{u_2}}), \dots, (x^{iq^{u_t}}, \gamma x^{iq^{u_t}})\}}.$$

Note that for any $1 \leq a \leq t$,

$$((x^{iq^{u_a}})^{q^s}, (\gamma x^{iq^{u_a}})^{q^s}) = (x^{iq^{u_a}}, \gamma^{q^s} x^{iq^{u_a}})$$

since $|Z| = s$. Hence, $(x^{iq^{u_a}}, \gamma^{q^s} x^{iq^{u_a}})$ is also an element of the Galois closure. Moreover, $(x^{iq^{u_a}}, \gamma x^{iq^{u_a}})$ and $(x^{iq^{u_a}}, \gamma^{q^s} x^{iq^{u_a}})$ are linearly independent since $\gamma^{q^s} \neq \gamma$ by the assumption that $b \nmid s$.

Suppose $u \in \{0, 1, \dots, s-1\} \setminus \{u_1, \dots, u_t\}$. Then,

$$\left((x^{iq^{u_1}})^{q^{u-u_1}}, (\gamma x^{iq^{u_1}})^{q^{u-u_1}} \right) = \left(x^{iq^u}, \gamma^{q^{u-u_1}} x^{iq^u} \right) \in \overline{(\mathcal{B}(A \cap Z), \Gamma)}.$$

Moreover, due to the length of Z again, we have

$$\left((x^{iq^u})^{q^s}, (\gamma^{q^{u-u_1}} x^{iq^u})^{q^s} \right) = \left(x^{iq^u}, \gamma^{q^{u+s-u_1}} x^{iq^u} \right) \in \overline{(\mathcal{B}(A \cap Z), \Gamma)}.$$

If $\gamma^{q^{u+s-u_1}} = \gamma^{q^{u-u_1}}$, then $\gamma^{q^{u-u_1}(q^s-1)} = 1$. The order of γ is a divisor of $q^b - 1$, hence it cannot divide a power of q . This means the order divides $q^s - 1$, which yields $\gamma^{q^s-1} = 1$. This contradicts the fact that $b \nmid s$. Hence, $(x^{iq^u}, \gamma^{q^{u-u_1}} x^{iq^u})$ and $(x^{iq^u}, \gamma^{q^{u+s-u_1}} x^{iq^u})$ are linearly independent.

Arguing as in part i, we have $\dim \overline{(\mathcal{B}(A \cap Z), \Gamma)} = 2s$ and $\overline{(\mathcal{B}(A \cap Z), \Gamma)} = V_F(Z)$. Note that $V_F(Z)^\perp \cap V_F(-Z) = \{0\}$ by Lemma 2.3.6 (iii). Therefore $B_Z = \emptyset$ and $k_z = 0$.

iii. Assume that $A \cap Z \not\subseteq \hat{A}_Z$. Let $j \in \{1, \dots, t\}$ be such that $iq^{u_j} \notin \hat{A}_Z$. Then

$$\left((x^{iq^{u_a}})^{q^{u_j-u_a}}, (\gamma x^{iq^{u_a}})^{q^{u_j-u_a}} \right) = \left(x^{iq^{u_j}}, \gamma^{q^{u_j-u_a}} x^{iq^{u_j}} \right) \in \overline{(\mathcal{B}(A \cap Z), \Gamma)}.$$

Note that $(x^{iq^{u_j}}, \gamma x^{iq^{u_j}})$ and $(x^{iq^{u_j}}, \gamma^{q^{u_j-u_a}} x^{iq^{u_j}})$ are linearly independent elements of $\overline{(\mathcal{B}(A \cap Z), \Gamma)}$, since otherwise $\gamma^{q^{u_j-u_a}} = \gamma$. This would yield $b|(u_j - u_a)$, which would contradict the assumption that $iq^{u_j} \notin \hat{A}_Z$.

Let $v \in \{1, \dots, t\}$ be such that $iq^{u_v} \in \hat{A}_Z$. Then $iq^v = iq^{u_a+\ell b}$ for some ℓ . For $j \in \{1, \dots, t\}$ with $iq^{u_j} \notin \hat{A}_Z$, we have

$$\left((x^{iq^{u_j}})^{q^{u_v-u_j}}, (\gamma x^{iq^{u_j}})^{q^{u_v-u_j}} \right) = \left(x^{iq^{u_v}}, \gamma^{q^{u_v-u_j}} x^{iq^{u_v}} \right) \in \overline{(\mathcal{B}(A \cap Z), \Gamma)}.$$

If $\gamma^{q^{u_v-u_j}} = \gamma$, then $b|(u_a - u_j)$ which contradicts $iq^{u_j} \notin \hat{A}_Z$. Hence, $(x^{iq^{u_v}}, \gamma x^{iq^{u_v}})$ and $(x^{iq^{u_v}}, \gamma^{q^{u_v-u_j}} x^{iq^{u_v}})$ are two independent elements of $\overline{(\mathcal{B}(A \cap Z), \Gamma)}$.

Finally, let $u \in \{0, 1, \dots, s-1\} \setminus \{u_1, \dots, u_t\}$. Then, for j as above and a as

in the definition of \hat{A}_Z , we have

$$\begin{aligned} \left((x^{iq^{u_j}})^{q^{u-u_j}}, (\gamma x^{iq^{u_j}})^{q^{u-u_j}} \right) &= \left(x^{iq^u}, \gamma^{q^{u-u_j}} x^{iq^u} \right) \in \overline{(\mathcal{B}(A \cap Z), \Gamma)}, \\ \left((x^{iq^{u_a}})^{q^{u-u_a}}, (\gamma x^{iq^{u_a}})^{q^{u-u_a}} \right) &= \left(x^{iq^u}, \gamma^{q^{u-u_a}} x^{iq^u} \right) \in \overline{(\mathcal{B}(A \cap Z), \Gamma)}. \end{aligned}$$

If $\gamma^{q^{u-u_j}} = \gamma^{q^{u-u_a}}$, then $\gamma^{q^{u-u_j}(1-q^{u_j-u_a})} = 1$. Multiplicative order of γ divides $q^b - 1$, hence it cannot divide q^{u-u_j} . Therefore $\gamma^{q^{u_j-u_a}-1} = 1$, which yields $\gamma \in \mathbb{F}_{q^{u_j-u_a}}$. This implies $b|(u_j - u_a)$ which yields a contradiction as above. Hence $\left(x^{iq^u}, \gamma^{q^{u-u_j}} x^{iq^u} \right)$ and $\left(x^{iq^u}, \gamma^{q^{u-u_a}} x^{iq^u} \right)$ are two independent elements of $\overline{(\mathcal{B}(A \cap Z), \Gamma)}$. Now the claim follows as in part ii.

If $A \cap Z \subseteq \hat{A}_Z$, let $u_\nu = u_a + \ell_\nu b$ for $1 \leq \nu \leq t$. It is clear that $\overline{(\mathcal{B}(A \cap Z), \Gamma)} \subseteq \overline{(\mathcal{B}(\hat{A}_Z), \Gamma)}$. Let ℓ be such that $iq^{u_a+\ell b} \in \hat{A}_Z \setminus A \cap Z$. Then, for any $\nu \in \{1, \dots, t\}$, we have

$$\begin{aligned} \left((x^{iq^{u_a+\ell_\nu b}})^{q^{(\ell-\ell_\nu)b}}, (\gamma x^{iq^{u_\nu}})^{q^{(\ell-\ell_\nu)b}} \right) &= \left(x^{iq^{u_a+\ell b}}, \gamma^{q^{(\ell-\ell_\nu)b}} x^{iq^{u_a+\ell b}} \right) \\ &= \left(x^{iq^{u_a+\ell b}}, \gamma x^{iq^{u_a+\ell b}} \right) \in \overline{(\mathcal{B}(A \cap Z), \Gamma)}, \end{aligned}$$

where the last equality holds since $\gamma \in \mathbb{F}_{q^b}$. Hence, $\overline{(\mathcal{B}(A \cap Z), \Gamma)} = \overline{(\mathcal{B}(\hat{A}_Z), \Gamma)}$.

Above discussion yields

$$\begin{aligned} \overline{(\mathcal{B}(\hat{A}_Z), \Gamma)} &= \overline{\text{Span}\{(x^{iq^{u_a}}, \gamma x^{iq^{u_a}}), (x^{iq^{u_a+b}}, \gamma x^{iq^{u_a+b}}), (x^{iq^{u_a+2b}}, \gamma x^{iq^{u_a+2b}}), \dots\}} \\ &= \overline{\text{Span}\{(x^{iq^{u_a}}, \gamma x^{iq^{u_a}})\}} \\ &= \text{Span}\{(x^{iq^{u_a+c}}, \gamma^{q^c} x^{iq^{u_a+c}}) : 0 \leq c \leq s-1\}, \end{aligned}$$

where the last equality follows from $|Z| = s$. Hence, $\dim \overline{(\mathcal{B}(\hat{A}_Z), \Gamma)} = s$. Moreover,

$$\begin{aligned} \dim \left(\overline{(\mathcal{B}(\hat{A}_Z), \Gamma)}^\perp \cap V_F(-Z) \right) &= \dim \left(\overline{(\mathcal{B}(\hat{A}_Z), \Gamma)} \oplus V_F(-Z)^\perp \right)^\perp \\ &= 2n - (\dim \overline{(\mathcal{B}(\hat{A}_Z), \Gamma)} + (2n - \dim V_F(-Z))) \\ &= 2n - (s + 2n - 2s) \\ &= s. \end{aligned}$$

Observe that the codewords

$$\begin{aligned} &(-\gamma x^{-iq^{u_a}}, x^{-iq^{u_a}}), (-\gamma^q x^{-iq^{u_a+1}}, x^{iq^{u_a+1}}), \dots \\ &\dots, (-\gamma^{q^{s-1}} x^{-iq^{u_a+(s-1)}}, x^{-iq^{u_a+(s-1)}}) \in V_F(-Z) \end{aligned}$$

are all orthogonal to the generators of $\overline{(\mathcal{B}(\hat{A}_Z), \Gamma)}$. Arguing as above, we have

$$\begin{aligned} \overline{(\mathcal{B}(\hat{A}_Z), \Gamma)}^\perp \cap V_F(-Z) &= \text{Span}\{(-\gamma^{q^c} x^{-iq^{u_a+c}}, x^{-iq^{u_a+c}}) : 0 \leq c \leq s-1\} \\ &= \overline{\text{Span}\{(-\gamma x^{-iq^{u_a}}, x^{-iq^{u_a}})\}} \\ &= \overline{\text{Span}\{(-\gamma x^{-iq^{u_a+cb}}, x^{-iq^{u_a+cb}}) : c = 0, 1, 2, \dots\}} \\ &= \overline{(\mathcal{B}(-\hat{A}_Z), \Gamma')} \end{aligned}$$

Therefore $B_Z = -\hat{A}_Z$. □

2.4 Comparison of the Bounds

In this section we will present some examples to illustrate instances where our Hasse-Weil type bound performs better than the BCH bound. To optimize the bound in Theorem 2.2.4 for $\phi_\Gamma(\mathcal{B}(A))$, we choose the set $j_0 A$ whose maximum element is the smallest among the maximum elements of jA for every j relatively prime to n (cf. Corollary 2.2.7). In this respect, we always start with the optimum defining set A for the code $\phi_\Gamma(\mathcal{B}(A))$ in the examples below.

Furthermore, to obtain the best BCH bound for the code, we will take the longest interval in the defining set B of dual code. Say this interval is $\{j_0 l, j_0(l+1), \dots, j_0(l+u-1)\}$ for some j_0 relatively prime to n and for some integer $l \in \mathbb{Z}/n\mathbb{Z}$. The length of this longest interval in B is the same as the length of the longest consecutive integer sequence in jB . In other words, to optimize the BCH bound for $\phi_\Gamma(\mathcal{B}(A))$, we collect the lengths of longest consecutive integer sequence in jB for every j relatively prime to n , and take the maximum one.

Let $m = 2$, $\Gamma = (1, \gamma)$ and $b = [\mathbb{F}_q(\gamma) : \mathbb{F}_q] > 1$. In Tables 2.1 and 2.2, we present examples of codes where the Hasse-Weil type bound performs better than the BCH bound. Our bound is easy to compute but the BCH bound requires long computations in Magma [1] to determine the set B (cf. Theorem 2.3.8) and the longest interval for this bound.

In the next example, we give details for one of the codes in Table 2.1 to describe the computations involved in the results presented in this table.

Example 2.4.1. Consider the codes corresponding to the rows with $q = 2$, $r = 8$ and $A = \{5, 7, 9\} \subset \mathbb{Z}/255\mathbb{Z}$ in Table 2.1. From Theorem 2.2.4, we have the following:

$$d(\phi_{\Gamma}(\mathcal{B}(A))) \geq 2^8 - 2^6 - \frac{(4-1)(9-1)\lfloor 2\sqrt{2^8} \rfloor}{2^3} = 96.$$

- i. First consider the code with $b = 2$. We can find B using the algorithm in Theorem 2.3.8. The cyclotomic cosets containing 5, 7 and 9 are

$$Z(5) = \{5, 10, 20, 40, 65, 80, 130, 160\}$$

$$Z(7) = \{7, 14, 28, 56, 112, 131, 193, 224\}$$

$$Z(9) = \{9, 18, 33, 36, 66, 72, 132, 144\}$$

Since b divides the cardinalities of these cyclotomic cosets, we fall in the case (iii) of Theorem 2.3.8. We have $\hat{A}_{Z(5)} = \{5, 20, 80\}$, $\hat{A}_{Z(7)} = \{7, 28, 112\}$ and $\hat{A}_{Z(9)} = \{9, 36, 144\}$. They give a contribution of $-\hat{A}_{Z(5)} \cup -\hat{A}_{Z(7)} \cup -\hat{A}_{Z(9)} = \{111, 143, 175, 219, 227, 235, 246, 248, 250\}$ to B . The cyclotomic cosets not intersecting A yield a contribution of $\bigcup_{i \neq 5, 7, 9} -Z(i)$ to B (Theorem 2.3.8 i).

We optimize the BCH bound for $\phi_\Gamma(\mathcal{B}(A))$ when $j = 133$ and obtain

$$jB = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, \\ 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 36, 37, 38, 40, 41, 42, 44, 45, 46, \\ 47, 48, 49, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, \\ 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, \\ 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, \\ 108, 109, 110, 111, 112, 113, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, \\ 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 141, \\ 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 157, 158, \\ 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 173, 174, 175, \\ 176, 177, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, \\ 193, 194, 195, 196, 197, 198, 199, \underline{203, 204, 205, 206, 207, 208, 209, 210, 211,} \\ \underline{212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227,} \\ \underline{228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243,} \\ \underline{244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254}\},$$

which contains maximum 87 consecutive integers (the underlined sequence in the set). Hence by Theorem 2.3.1 the BCH bound is 88, which is worse than the Hasse-Weil type bound.

- ii. Consider the codes with $b = 4$ and $b = 8$. By applying the same procedure as in part i, we obtain that BCH bound is 78 in both cases, which is again worse than the Hasse-Weil type bound.

Again, details for one of the codes in Table 2.2 is given in the next example.

Example 2.4.2. Consider the codes corresponding to the rows with $q = 3$, $r = 4$ and $A = \{1, 2, 4, 5\} \subset \mathbb{Z}/80\mathbb{Z}$ in Table 2.2. The Hasse-Weil type bound for these codes is 40 by Theorem 2.2.4.

First consider the code with $b = 2$. We can find B using the algorithm in

q	r	A	b	HW-bound	BCH-bound
2	7	$\{1,3,5\}$	7	63	48
2	7	$\{1,3,5,7\}$	7	47	32
2	8	$\{5,7,9\}$	8	96	78
2	8	$\{5,7,9\}$	4	96	78
2	8	$\{5,7,9\}$	2	96	88
2	8	$\{3,7,9,11\}$	8	72	64
2	8	$\{3,7,9,11\}$	4	72	64
2	9	$\{5,9,11\}$	9	216	164
2	9	$\{5,9,11\}$	3	216	175
2	9	$\{1,3,5,7,9,11,13\}$	9	182	96
2	9	$\{1,3,5,7,9,11,13\}$	3	182	112
2	9	$\{3,5,11,15\}$	9	148	116
2	9	$\{3,5,11,15\}$	3	148	138
2	9	$\{3,5,11,15,17\}$	9	114	107
2	9	$\{3,5,11,15,17\}$	3	114	108
2	10	$\{3,5,11,13,19\}$	10	336	254
2	10	$\{3,5,11,13,19\}$	5	336	254
2	10	$\{1,9,15,17,19,23\}$	10	240	195
2	10	$\{1,9,15,17,19,23\}$	5	240	195
2	10	$\{1,9,15,17,19,23\}$	2	240	224
2	10	$\{3,5,7,15,17,21,25\}$	10	192	160
2	10	$\{3,5,7,15,17,21,25\}$	5	192	160
2	10	$\{3,5,7,15,17,21,25\}$	2	192	191
2	10	$\{1,7,13,15,19,23,25,27\}$	10	144	126
2	10	$\{1,7,13,15,19,23,25,27\}$	5	144	129

Table 2.1: Codes for $q = 2$

Theorem 2.3.8. The cyclotomic cosets containing 1, 2, 4 and 5 are

$$Z(1) = \{1, 3, 9, 27\}$$

$$Z(2) = \{2, 6, 18, 54\}$$

$$Z(4) = \{4, 12, 28, 36\}$$

$$Z(5) = \{5, 15, 45, 55\}$$

Since b divides the cardinalities of these cyclotomic cosets, we fall in the case (iii) of Theorem 2.3.8. We have $\hat{A}_{Z(1)} = \{1, 9\}$, $\hat{A}_{Z(2)} = \{2, 18\}$, $\hat{A}_{Z(4)} = \{4, 36\}$ and $\hat{A}_{Z(5)} = \{5, 45\}$. They give a contribution of $-\hat{A}_{Z(1)} \cup -\hat{A}_{Z(2)} \cup -\hat{A}_{Z(4)} \cup -\hat{A}_{Z(5)} = \{35, 44, 62, 71, 75, 76, 78, 79\}$ to B . The cyclotomic cosets not intersecting A yield a contribution of $\bigcup_{i \neq 1, 2, 4, 5} -Z(i)$ to B (Theorem 2.3.8 i). We optimize the BCH

bound for $\phi_\Gamma(\mathcal{B}(A))$ when $j = 3$ and obtain

$$jB = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, \\ \underline{24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34}, 36, 37, 38, 39, 40, 41, 42, 43, 45, 46, \\ 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 63, 64, 65, 66, 67, 68, \\ 69, 70, 72, 73, 74, 77\},$$

which contains maximum 35 consecutive integers (the underlined sequence in the set). Hence, by Theorem 2.3.1 the BCH bound is 36, which is worse than the Hasse-Weil type bound.

For the code with $b = 4$, the same procedure again yields 36 for the BCH bound.

q	r	A	b	HW-bound	BCH-bound
3	4	$\{1, 2, 4, 5\}$	4	40	36
3	4	$\{1, 2, 4, 5\}$	2	40	36
3	5	$\{1, 5, 8\}$	5	120	102
3	5	$\{1, 2, 5, 7, 8\}$	5	120	79
3	5	$\{2, 4, 5, 7, 10\}$	5	92	81
3	6	$\{4, 5, 8, 10, 11, 13, 14\}$	6	336	242
3	6	$\{4, 5, 8, 10, 11, 13, 14\}$	3	336	242
3	6	$\{4, 5, 8, 10, 11, 13, 14\}$	2	336	250
3	6	$\{7, 10, 11, 14, 16, 17\}$	6	264	244
3	6	$\{7, 10, 11, 14, 16, 17\}$	3	264	244
3	6	$\{7, 10, 11, 14, 16, 17\}$	2	264	258
3	6	$\{2, 4, 7, 8, 11, 13, 14, 17, 19, 20, 22\}$	6	144	136
3	6	$\{2, 4, 7, 8, 11, 13, 14, 17, 19, 20, 22\}$	3	144	136

Table 2.2: Codes for $q = 3$

Chapter 3

Complementary Dual Additive Cyclic Codes

3.1 A Condition for Complementary Dual Codes

We will continue to use the notation introduced in the previous chapter. Let $n = q^r - 1$ and $m = 2$ throughout this chapter. For $\Gamma = (1, \gamma)$, the dual of $\phi_\Gamma(\mathcal{B}(A))$ is $\phi_{\Gamma'}(\mathcal{B}(B))$, where $\Gamma' = (-\gamma, 1)$ and the set B is determined explicitly in Theorem 2.3.8. Elements of $\phi_\Gamma(\mathcal{B}(A))$ and its dual $\phi_{\Gamma'}(\mathcal{B}(B))$ are of the form $c_f = (\text{Tr}(f(x)), \text{Tr}(\gamma f(x)))$ for $f(x) \in \mathcal{P}(A)$ and $c_g = (\text{Tr}(-\gamma g(x)), \text{Tr}(g(x)))$ for $g(x) \in \mathcal{P}(B)$, respectively. Recall that $(\text{Tr}(f(x)), \text{Tr}(\gamma f(x)))$ denotes the code-word $(\text{Tr}(f(\alpha^0)), \text{Tr}(\gamma f(\alpha^0)); \dots; \text{Tr}(f(\alpha^{n-1})), \text{Tr}(\gamma f(\alpha^{n-1})))$. Then $\phi_\Gamma(\mathcal{B}(A))$ is not complementary dual if and only if there exist $f(x) \in \mathcal{P}(A)$ and $g(x) \in \mathcal{P}(B)$ such that $c_f \neq \vec{0} \neq c_g$ and $c_f = c_g$. We will use the following result.

Lemma 3.1.1. *[9, Proposition 2.3] Let $\lambda_j \in \mathbb{F}_{q^r}$ and i_j be positive integers, for $j = 1, 2, \dots, s$. Assume that the q -cyclotomic cosets containing i_j 's are distinct. Then $\text{Tr}(\lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \dots + \lambda_s x^{i_s}) = 0$ for all x in \mathbb{F}_{q^r} if and only if $\text{Tr}(\lambda_j x^{i_j}) = 0$ for all x in \mathbb{F}_{q^r} and for all $j = 1, 2, \dots, s$.*

A slight modification of Lemma 3.1.1 is needed for our purposes.

Lemma 3.1.2. *Let $\lambda_0, \lambda_j \in F$ and i_j be positive integers, for $j = 1, 2, \dots, s$. Assume that the q -cyclotomic cosets mod n containing i_j 's are distinct. Then $\text{Tr}(\lambda_0 + \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \dots + \lambda_s x^{i_s}) = 0$ for all x in F^* if and only if $\text{Tr}(\lambda_0) = 0$ and $\text{Tr}(\lambda_j x^{i_j}) = 0$ for all x in F^* and for all $j = 1, 2, \dots, s$.*

Proof. Assume $\text{Tr}(\lambda_0 + \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) = 0$ for all x in F^* . By linearity of the trace map, $\text{Tr}(\lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) = -\text{Tr}(\lambda_0) =: c$ for all x in F^* . Then

$$\begin{aligned} (q^r - 1)c &= \sum_{x \in F^*} \text{Tr}(\lambda_1 x^{i_1} + \cdots + \lambda_s x^{i_s}) \\ &= \text{Tr}\left(\sum_{x \in F^*} (\lambda_1 x^{i_1} + \cdots + \lambda_s x^{i_s})\right) \\ &= \text{Tr}\left(\lambda_1 \sum_{x \in F^*} x^{i_1} + \cdots + \lambda_s \sum_{x \in F^*} x^{i_s}\right) \\ &= 0 \end{aligned}$$

where the last equality follows from the fact that if i is not a multiple of $q^r - 1$, then $\sum_{x \in F^*} x^i = 0$ by Lemma 2.3.3. Therefore $c = 0$, i.e. $\text{Tr}(\lambda_0) = 0$ and $\text{Tr}(\lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) = 0$ for all x in F^* . By Lemma 3.1.1, $\text{Tr}(\lambda_0) = 0$ and $\text{Tr}(\lambda_j x^{i_j}) = 0$ for all x in F^* and for all $j = 1, 2, \dots, s$.

The converse is immediate from linearity of the trace map. \square

For $A \subseteq \mathbb{Z}/n\mathbb{Z}$, denote by \bar{A} the union of all q -cyclotomic cosets mod n intersecting A nontrivially.

Proposition 3.1.3. *Let A and B be defining sets for the additive cyclic code and its dual as before. If $\bar{A} \cap B = \emptyset$, then $\phi_\Gamma(\mathcal{B}(A))$ is complementary dual.*

Proof. Let $f(x) \in \mathcal{P}(A)$ and $g(x) \in \mathcal{P}(B)$, and suppose $c_f = c_g$. Then $\text{Tr}(f(x) + \gamma g(x)) = 0$ and $\text{Tr}(\gamma f(x) - g(x)) = 0$ for all $x \in F^*$. By the assumption $\bar{A} \cap B = \emptyset$, exponents of f and g cannot lie in the same cyclotomic coset. Some exponents that appear in f (or in g) may be from the same cyclotomic coset. This is no harm for concluding $\text{Tr}(f(x)) = 0 = \text{Tr}(\gamma g(x))$ and $\text{Tr}(\gamma f(x)) = 0 = \text{Tr}(g(x))$ for all x in F^* (by Lemma 3.1.2), since $\text{Tr}(ax^j + bx^{jq}) = \text{Tr}((a + b^{1/q})x^j)$. Therefore, $c_f = \vec{0} = c_g$, i.e. anything in the intersection $\phi_\Gamma(\mathcal{B}(A)) \cap \phi_{\Gamma'}(\mathcal{B}(B))$ has to be $\vec{0}$. \square

Theorem 3.1.4. *Let $b = [\mathbb{F}_q(\gamma) : \mathbb{F}_q] > 1$. Then $\phi_\Gamma(\mathcal{B}(A))$ is complementary dual if the following conditions are satisfied by every q -cyclotomic coset Z mod n :*

- i. $A \cap Z = \emptyset$ if and only if $A \cap (-Z) = \emptyset$.*

- ii. If $A \cap Z \neq \emptyset$, then $A \cap Z$ is not contained in the q^b -cyclotomic coset mod n of some element in $A \cap Z$.

Proof. If a cyclotomic coset Z does not intersect A , then we also have $\bar{A} \cap Z = \emptyset$. Therefore, such a cyclotomic coset cannot contribute to $\bar{A} \cap B$.

Now assume that a cyclotomic coset Z intersects A . By assumption i, we have $A \cap (-Z) \neq \emptyset$ too. If b does not divide $|Z| = |-Z|$, then by Theorem 2.3.8 part ii, we have $B_{-Z} = B \cap Z = \emptyset$ and such Z cannot contribute to $\bar{A} \cap B$. So assume that b divides $|Z| = |-Z|$. Note that \hat{A}_{-Z} is nothing but the q^b -cyclotomic coset mod n of some element in $A \cap (-Z)$. Hence assumption ii implies that $A \cap (-Z) \not\subseteq \hat{A}_{-Z}$ and therefore (by Theorem 2.3.8), we have $B_{-Z} = B \cap Z = \emptyset$. Therefore such a coset Z cannot contribute to $\bar{A} \cap B$ even if b divides $|Z|$. The result follows from Proposition 3.1.3. \square

Corollary 3.1.5. *Let $b = [\mathbb{F}_q(\gamma) : \mathbb{F}_q] = r$. Then $\phi_\Gamma(\mathcal{B}(A))$ is complementary dual if the following conditions are satisfied by every q -cyclotomic coset Z mod n :*

- i. $A \cap Z = \emptyset$ if and only if $A \cap (-Z) = \emptyset$.
- ii. If $A \cap Z \neq \emptyset$, then there exists at least two elements from Z in A .

Proof. Since $b = r$, q^b -cyclotomic coset mod n of any element in $A \cap Z$ consists of a single element. Hence, by ii, $A \cap Z$ satisfies condition ii in Theorem 3.1.4 and the result follows. \square

3.2 Examples

In this section, by using our results we present examples of additive cyclic complementary dual codes over $E = \mathbb{F}_2^2$. In Table 3.1, M and d stand for the size and minimum distance of the code, respectively. The computational algebra system Magma [1] is used for computations.

In the following examples, we describe the computations briefly for some of the codes presented in Table 3.1.

Example 3.2.1. Let $r = 5 = b$. Then $n = q^r - 1 = 31$ and 2-cyclotomic cosets

mod 31 are

$$\begin{aligned}
Z_0 &= \{0\} \\
Z_1 &= \{1, 2, 4, 8, 16\} \\
Z_3 &= \{3, 6, 12, 17, 24\} \\
Z_5 &= \{5, 9, 10, 18, 20\} \\
Z_7 &= \{7, 14, 19, 25, 28\} \\
Z_{11} &= \{11, 13, 21, 22, 26\} \\
Z_{15} &= \{15, 23, 27, 29, 30\}.
\end{aligned}$$

Consider the additive cyclic code of length 31 over $E = \mathbb{F}_2^2$ with defining set $A = \{1, 2, 15, 23\}$ where $\{1, 2\} \subset Z_1$ and $\{15, 23\} \subset Z_{15} = -Z_1$. Then

$$\overline{A} = Z_1 \cup Z_{15}.$$

The cyclotomic cosets not intersecting A yield a contribution of $\bigcup_{j \neq 1, 15} -Z_j$ to B (Theorem 2.3.8 i). Since $A \cap Z_1 \not\subseteq \hat{A}_{Z_1} = \{1\}$ and $A \cap Z_{15} \not\subseteq \hat{A}_{Z_{15}} = \{15\}$, there is no contribution from Z_1 and $-Z_1 = Z_{15}$ to B (Theorem 2.3.8 iii). Therefore the defining set of the dual code is

$$B = \bigcup_{j \neq 1, 15} -Z_j.$$

For this code we satisfy the condition that $\overline{A} \cap B = \emptyset$. Indeed this code is nonlinear complementary dual over \mathbb{F}_2^2 of length $n = 31$, size $M = 4^{10}$ and minimum distance $d = 10$.

Note that the best minimum distance of LCD cyclic codes over \mathbb{F}_4 with length 31 and dimension 10 is $d = 10$ as well. For instance, the one which is generated by the self-reciprocal polynomial

$$g(x) = x^{21} + x^{17} + x^{16} + x^{15} + x^{13} + x^8 + x^6 + x^5 + x^4 + 1$$

has minimum distance 10.

Example 3.2.2. Consider the code corresponding to the row with $r = 6$, $b = 6$

and

$$A = \{1, 4, 31, 47, 21, 42\},$$

where $\{1, 4\}$, $\{31, 47\}$ and $\{21, 42\}$ are contained in the 2-cyclotomic cosets mod 63 Z_1 , $Z_{31} = -Z_1$ and $Z_{21} = -Z_{21}$, respectively. Then

$$\overline{A} = Z_1 \cup Z_{31} \cup Z_{21}.$$

From the algorithm provided in Theorem 2.3.8, the defining set of the dual code is

$$B = \bigcup_{j \neq 1, 31, 21} -Z_j.$$

For this code we satisfy the condition that $\overline{A} \cap B = \emptyset$. Indeed this code is nonlinear complementary dual over \mathbb{F}_2^2 of length $n = 63$, size $M = 4^{14}$ and minimum distance $d = 22$.

Moreover, for $b = 3$ the code is still complementary dual with the same parameters as in the case $b = 6$. On the other hand, if $b = 2$, then the code is not complementary dual since $A \cap Z_1$ is contained in the q^b -cyclotomic coset of 1 (Theorem 3.1.4 ii).

r	b	A	M	d
4	4, 2	$\{1, 2, 7, 11\}$	4^8	4
4	4	$\{1, 4, 7, 11\}$	4^8	4
4	4, 2	$\{3, 6, 5, 10\}$	4^6	6
5	5	$\{1, 2, 15, 23\}$	4^{10}	10
6	6, 3	$\{1, 4, 31, 47\}$	4^{12}	24
6	6, 3, 2	$\{1, 2, 31, 47\}$	4^{12}	24
6	6, 3	$\{1, 4, 31, 47, 21, 42\}$	4^{14}	22
7	7	$\{1, 2, 63, 126\}$	4^{14}	54
8	8, 4, 2	$\{4, 8, 127, 191\}$	4^{16}	112
8	8, 2	$\{1, 16, 127, 191\}$	4^{16}	112

Table 3.1: Codes over \mathbb{F}_2^2

Bibliography

- [1] W. Bosma, J. Cannon and C. Playoust, “The Magma algebra system I. The user language”, *J. Symbolic Comput.*, vol. 24, 235-265, 1997.
- [2] J. Bierbrauer, “The theory of cyclic codes and a generalization to additive codes”, *Des. Codes Cryptogr.*, vol. 25, 189-206, 2002.
- [3] J. Bierbrauer, *Introduction to Coding Theory*, Chapman and Hall/CRC Press, 2005.
- [4] J. Bierbrauer and Y. Edel, “Quantum twisted codes”, *J. Combin. Des.*, vol. 8, 174-188, 2000.
- [5] C. Carlet and S. Guilley, “Complementary dual codes for counter-measures to side-channel attacks”, *Adv. Math. Commun.*, vol. 10, 131-150, 2016.
- [6] M. Esmaeili and S. Yari, “On complementary-dual quasi-cyclic code”, *Finite Fields Appl.*, vol. 15, 375-386, 2009.
- [7] A. Garcia and F. Özbudak, “Some maximal function fields and additive polynomials”, *Comm. Algebra*, vol. 35, 1553-1566, 2007.
- [8] C. Güneri and F. Özbudak, “Weil-Serre type bounds for cyclic codes”, *IEEE Trans. Inform. Theory*, vol. 54, 5381-5395, 2008.
- [9] C. Güneri, “Artin-Schreier curves and weights of two-dimensional cyclic codes”, *Finite Fields Appl.*, vol. 10, 481-505, 2004.
- [10] C. Güneri, F. Özbudak and F. Özdemir, “Hasse-Weil bound for additive cyclic codes”, *Des. Codes Cryptogr.*, DOI 10.1007/s10623-016-0198-3.
- [11] C. Güneri, B. Özkaya and P. Solé, “Quasi-cyclic complementary dual codes”, *Finite Fields Appl.*, vol. 42, 67-80, 2016.

- [12] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, 1997.
- [13] J.H. van Lint, *Introduction to Coding Theory*, Graduate Texts in Mathematics, Springer-Verlag, Berlin, 1999.
- [14] J.L. Massey, “Linear codes with complementary duals”, *Discrete Math.*, vol. 106-107, 337-342, 1992.
- [15] N. Sendrier, “Linear codes with complementary duals meet the Gilbert-Varshamov bound”, *Discrete Math.*, vol. 285, 345-347, 2004.
- [16] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer GTM, vol. 254, 2009.
- [17] J. Wolfmann, “New bounds on cyclic codes from algebraic curves”, *Coding theory and applications (Toulon, 1988)*, *Lecture Notes in Comput. Sci.*, vol. 388, 47-62, 1989.
- [18] X. Yang and J.L. Massey, “The condition for a cyclic code to have a complementary dual”, *Discrete Math.*, vol. 126, 391-393, 1994.