8-2001

Artin-Schreier Families and 2-D Cyclic Codes

Cem Guneri
Louisiana State University and Agricultural and Mechanical College

ARTIN-SCHREIER FAMILIES AND 2-D CYCLIC CODES

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
Cem Guneri
B.S., Middle East Technical University, Turkey, 1995
M.S., Louisiana State University, 1998
August 2001

MANUSCRIPT THESES

Unpublished theses submitted for the Master's and Doctor's Degrees and deposited in the Louisiana State University Libraries are available for inspection. Use of any thesis is limited by the rights of the author. Bibliographical references may be noted, but passages may not be copied unless the author has given permission. Credit must be given in subsequent written and published work.

A library which borrows this thesis for use by its clientele is expected to make sure that the borrower is aware of the above restrictions.

LOUISIANA STATE UNIVERSITY LIBRARIES

Acknowledgments

I was very lucky to have Robert F. Lax as my advisor. He suggested a dissertation topic which has been quite pleasant and interesting to work on. He has been a great source of guidance and support for my work, and I thank him for that.

I should also acknowledge the fine research environment at the Mathematics Department of Louisiana State University. Helpful comments provided by Arnaldo Garcia on parts of my work are also appreciated.

I must especially thank my wife, Ceren, who has been very patient and supportive during my studies. She has been a great companion. Finally, we both would like to thank our families for all the things that they did for our happiness and the support that they provided from very far away.

Table of Contents

Abstract

We start with the study of certain Artin-Schreier families. Using coding theory techniques, we determine a necessary and sufficient condition for such families to have a nontrivial curve with the maximum possible number of rational points over the finite field in consideration. This result produces several nice corollaries, including the existence of certain maximal curves; i.e., curves meeting the Hasse-Weil bound. We then present a way to represent two-dimensional (2-D) cyclic codes as trace codes starting from a basic zero set of its dual code. This representation enables us to relate the weight of a codeword to the number of rational points on certain Artin-Schreier curves via the additive form of Hilbert's Theorem 90. We use our results on Artin-Schreier families to give a minimum distance bound for a large class of 2-D cyclic codes. Then, we look at some specific classes of 2-D cyclic codes that are not covered by our general result. In one case, we obtain the complete weight enumerator and show that these types of codes have two nonzero weights. In the other cases, we again give minimum distance bounds. We present examples, in some of which our estimates are fairly efficient.

Introduction

The use of algebraic geometry in coding theory was initiated in the late 70's by the Russian engineer/mathematician V. D. Goppa ([11]) who showed that one can create powerful codes using linear systems on algebraic curves over finite fields. It turns out that the codes constructed this way, which are now called Algebraic Geometry Codes, have very good parameters when the curves used in their construction have "a lot of" rational points over their field of definition.

Goppa's discovery inspired two trends among interested mathematicians and engineers. The first is the renewed interest in the study of curves over finite fields and the second is the search for other applications of algebraic geometry to coding theory. This dissertation gives results in both directions. We give some results on Artin-Schreier families and then apply these to the weight computations of the so called 2-D cyclic codes. Here is a detailed description of the chapters:

We start Chapter 1 with basic definitions in coding theory. We then recall the method that enables us to compute the weights of binary double-error-correcting BCH codes via families of certain elliptic curves. This method is the main source of our results throughout and it has also helped researchers in the weight computations of other classes of cyclic codes via other families of algebraic curves (see [9] and [25] for examples of such results). Then we give some background on Artin-Schreier curves and in the last section, we answer the following question:
Question: Let $q = p^l$ for some prime p and let $\mathbb{F}_{q^m}$ be the finite field with q^m elements. For which Artin-Schreier families of the form

$$\mathcal{F} = \{y^q - y = \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s};\ \lambda_j \in \mathbb{F}_{q^m},\ i_j > 0\}$$

can we find a "nontrivial" member with q^{m+1} affine $\mathbb{F}_{q^m}$-rational points?

It is easy to see that q^{m+1} is the maximum possible number of affine $\mathbb{F}_{q^m}$-rational points that can be attained by the members of $\mathcal{F}$. The trivial member of $\mathcal{F}$ is the one obtained by taking all the coefficients λ_γ to be zero, which obviously has q^{m+1} solutions over $\mathbb{F}_{q^m}$. We obtain certain corollaries from this result, one of which guarantees the existence of certain maximal curves, i.e.; curves that meet the Hasse-Weil bound.

In Chapter 2, we explain properties of 2-D cyclic codes. These are generalizations of cyclic codes. The birth of interest in these codes goes back to the 70's and the first two papers that attempt to lay out a general theory of such codes are the works of Ikai, et al ([13]) and Imai ([15]). The properties of 2-D cyclic codes are essentially the same as those of cyclic codes, but they require a little more work to prove.

In Chapter 3, we give a trace representation for any "square" 2-D cyclic code via the basic zero set of its dual 2-D cyclic code. We then use this representation and the method described in Chapter 1 to relate the weight of a codeword to certain Artin-Schreier curves. This leads to a minimum distance bound which applies to a large class of 2-D cyclic codes. The final section deals with classes of 2-D cyclic codes that are not covered by our general minimum distance bound. In one case, we get the complete weight enumerator and show that for such a class there are two nonzero weights. For other classes, we again give minimum distance bounds. For each case considered, we present examples and sometimes give specific arguments to improve the bounds from our results.

Chapter 1. Cyclic Codes and Algebraic Curves

1.1 Definition of BCH Codes

Let $\mathbb{F}_q$ be a characteristic p finite field. A q-ary linear code of length n and dimension k is a k-dimensional vector subspace of $\mathbb{F}_q^n$. An element of a linear code is called a codeword. The minimum distance of a code is defined as the minimum codeword weight, where the weight of a codeword is the number of nonzero coordinates in it. A linear code with length n, dimension k, and minimum distance d is called an $[n, k, d]$ code. If A_i denotes the number of codewords with weight i, then $\sum_{i=0}^{n} A_i x^i$ is called the weight enumerator of a linear code of length n. Finally the set of n-tuples that are orthogonal to the members of the code C, with respect to the usual inner product on $\mathbb{F}_q^n$, is called the dual of C and is denoted $C^{\perp}$.

We now define an important class of linear codes, which are called cyclic codes.

Definition 1.1. A linear code C is called *cyclic* if for every $c = (c_0, c_1, \ldots, c_{n-1})$ in C, $(c_{n-1}, c_0, \ldots, c_{n-2})$ is also in C.

In other words a linear code that is closed under cyclic shift is called a cyclic code. Observe that the dual of a cyclic code is also cyclic. We will assume $(n, p) = 1$.

One of the most important features of cyclic codes is that they can be represented as ideals in certain rings. For this, observe the $\mathbb{F}_q$-vector space isomorphism between $\mathbb{F}_q^n$ and $\mathbb{F}_q[t]/(t^n - 1)$:

$$(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n \longleftrightarrow a(t) = \sum_{i=0}^{n-1} a_i t^i \in \mathbb{F}_q[t]/(t^n - 1)$$

Under this identification a codeword $c \in C$ can now be viewed as a polynomial $c(t)$ and this way we can think of a cyclic code as a subset of $\mathbb{F}_q[t]/(t^n - 1)$.

Proposition 1.2. *A linear code C in $\mathbb{F}_q^n$ is cyclic if and only if C is an ideal in $\mathbb{F}_q[t]/(t^n-1)$.*

Proof. Being closed under cyclic shift in $\mathbb{F}_q^n$ is the same as being closed under multiplication by t in $\mathbb{F}_q[t]/(t^n-1)$. □

Since a cyclic code is an ideal in the principal ideal ring $\mathbb{F}_q[t]/(t^n-1)$ it is generated by a unique monic polynomial of lowest degree, which is called the generator polynomial of the cyclic code. The generator polynomial gives us a simple way to compute the dimension of a cyclic code.

Proposition 1.3. *Let $g(t)$ be the generator polynomial of a cyclic code C of length n over $\mathbb{F}_q$ and suppose that the degree of $g(t)$ is k. Then the dimension of C is $n-k$.*

Proof. Since C is cyclic and generated by $g(t)$ it is of the form $C = \big(g(t)\big) \subset \mathbb{F}_q[t]/(t^n-1)$. Note that $\{g(t), tg(t), \ldots, t^{n-k-1}g(t)\}$ forms a basis for C. □

Remark 1.4. (i) The roots of $g(t)$ in extensions of $\mathbb{F}_q$ are called zeros of the cyclic code C. Obviously the zeros of a cyclic code are common roots of all the codewords and their number is equal to the degree of $g(t)$. Hence the dimension of a cyclic code C of length n is $n-k$ where k is the number of zeros of C.

(ii) The dual cyclic code $C^{\perp}$ is of dimension $n-(n-k)=k$. Therefore we can also say that the dimension of the dual cyclic code $C^{\perp}$ is equal to the number of zeros of C.

We are now ready to define the BCH codes, which are important types of cyclic codes.

Definition 1.5. Let C be a cyclic code of length n over $\mathbb{F}_q$ where $(n,q)=1$. Let m be the order of q mod n, and let α be a primitive n^{th} root of unity in

$\mathbb{F}_{q^m}$. C is a *BCH code of designed distance* δ if the generator polynomial of C is the product of the distinct minimal polynomials of the $\delta - 1$ consecutive elements $\alpha^l, \alpha^{l+1}, \ldots, \alpha^{l+\delta-2}$ over $\mathbb{F}_q$.

When $l = 1$, we call such a code a narrow-sense BCH code and if $n = q^m - 1$, i.e., α is a primitive element of $\mathbb{F}_{q^m}$, then the BCH code is called primitive.

Proposition 1.6. (BCH Bound) *The minimum distance of a BCH code with designed distance δ is at least δ.*

Proof. See [20] or [22]. □

Example 1.7. Let $q = 2^m > 4$ for some positive integer m and let α be a primitive element in $\mathbb{F}_q$. Consider the ideal generated by the product of the distinct minimal polynomials of $\alpha, \alpha^2, \alpha^3$ and α^4 in $\mathbb{F}_2[t]/(t^{q-1} - 1)$. Since α, α^2 and α^4 have the same minimal polynomial over $\mathbb{F}_2$, this ideal is

$$\mathbf{B}_m = \left(f_\alpha(t) f_{\alpha^3}(t)\right) \subset \mathbb{F}_2[t]/(t^{q-1} - 1),$$

where $f_\alpha(t)$ (resp., $f_{\alpha^3}(t)$) is the minimal polynomial of α (resp., α^3) over $\mathbb{F}_2$. $\mathbf{B}_m$ is called the binary double-error-correcting BCH code, and is denoted BCH(2). It is a primitive, narrow sense BCH code of length $q - 1 = 2^m - 1$ with designed distance 5.

1.2 Weights of Binary BCH(2) from a Family of Elliptic Curves

Our purpose in this section is to compute the weight enumerator of the binary BCH(2) code via a family of certain elliptic curves. Our main reference will be Schoof [25], even though similar method was also used by others, including van der Geer, van der Vlugt, Wolfmann, etc.

Recall that $\mathbb{F}_q = \mathbb{F}_{2^m}$, where $m > 2$. Since α and α^3 are not $\mathbb{F}_2$-conjugate, we have

$$\mathbf{B}_m = J \cap \mathbb{F}_2[t]/(t^{q-1} - 1),$$

where $J = \big((t-\alpha)(t-\alpha^3)\big) \subset \mathbb{F}_q[t]/(t^{q-1}-1)$ is a cyclic code over $\mathbb{F}_q$. In this case we call $\mathbf{B}_m$ the restriction of J to $\mathbb{F}_2$ and denote it by $J|_{\mathbb{F}_2}$.

Observe that for any codeword $a(t) = \sum_{i=0}^{q-2} a_i t^i$ in J, $a(\alpha) = a(\alpha^3) = 0$. These equalities can also be written as

$$(a_0, a_1, \ldots, a_{q-2}) \cdot (1, \alpha^1, \ldots, \alpha^{q-2}) = 0$$

$$(a_0, a_1, \ldots, a_{q-2}) \cdot (1, (\alpha^3)^1, \ldots, (\alpha^3)^{q-2}) = 0$$

for any $a(t) \in J$. Remembering the vector representation of cyclic codes, the above equalities mean that $v_1 = (1, \alpha^1, \ldots, \alpha^{q-2})$ and $v_2 = (1, (\alpha^3)^1, \ldots, (\alpha^3)^{q-2})$ are both codewords in $J^\perp$.

The generator polynomial of J reveals that the $\mathbb{F}_q$-dimension of $J^\perp$ is two (cf. Remark 1.4). Also, we have found two elements, v_1 and v_2, in $J^\perp$. Using the fact that α is a primitive element in $\mathbb{F}_q$, we can easily observe that all the elements in $\mathbb{F}_q^*$ are listed in v_1 and for each coordinate in v_1, the corresponding coordinate in v_2 is the cube of it. Suppose there exists d_1 and d_2 in $\mathbb{F}_q$ such that $d_1 v_1 + d_2 v_2 = \vec{0}$. Then, by the above observation, we have $d_1 x + d_2 x^3 = 0$ for any x in $\mathbb{F}_q^*$. But a polynomial of degree three has at most three roots in $\mathbb{F}_q$, and we chose $\mathbb{F}_q = \mathbb{F}_{2^m}$ with $m > 2$. Therefore $d_1 = d_2 = 0$ and this shows that the vectors (codewords) v_1 and v_2 in $J^\perp$ are $\mathbb{F}_q$-linearly independent. This makes the set $\{v_1, v_2\}$ an $\mathbb{F}_q$-basis for $J^\perp$, which gives us

$$\begin{aligned} J^\perp &= \{\lambda v_1 + \mu v_2; \lambda, \mu \in \mathbb{F}_q\} \\ &= \{(\lambda x + \mu x^3)_{x \in \mathbb{F}_q^*}; \lambda, \mu \in \mathbb{F}_q\}. \end{aligned}$$

Note that $(\lambda x + \mu x^3)_{x \in \mathbb{F}_q^*}$ denotes a vector of length $q-1$ in which the components are obtained by letting x take every value in $\mathbb{F}_q^*$, following the order $\{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$.

The following theorem will clarify why we have been interested in these new codes J and $J^\perp$ over $\mathbb{F}_q$ even though our main code is the BCH code, $\mathbf{B}_m$, over $\mathbb{F}_2$.

Theorem 1.8. (Delsarte) *For any code C over $\mathbb{F}_{q^m}$, we have*

$$(C|_{\mathbb{F}_q})^\perp = \mathbf{tr}(C^\perp)$$

where $\mathbf{tr}$ *is defined by applying the trace mapping* tr *from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ componentwise on the codewords of $C^\perp$.*

Proof. See [5] or [29]. □

This theorem implies that $\mathbf{B}_m^\perp = \mathbf{tr}(J^\perp)$. Our attention will be switched from the weight enumerator of $\mathbf{B}_m$ to that of $\mathbf{B}_m^\perp$, which will still serve our purpose due to the MacWilliams Identity.

Theorem 1.9. (MacWilliams) *Let C be an $[n,k]$ code over $\mathbb{F}_q$ with weight enumerator $W_C(x)$ and let $W_{C^\perp}(x)$ be the weight enumerator of $C^\perp$. Then*

$$W_{C^\perp}(x) = q^{-k}(1+(q-1)x)^n W_C\Big(\frac{1-x}{1+(q-1)x}\Big).$$

Proof. See [20] or [21]. □

Since we showed by Theorem 1.8 that $\mathbf{B}_m^\perp = \mathbf{tr}(J^\perp)$, we have the following representation:

$$\mathbf{B}_m^\perp = \{\big(\mathrm{tr}(\lambda x + \mu x^3)\big)_{x \in \mathbb{F}_q^*}; \lambda, \mu \in \mathbb{F}_q\}.$$

Example 1.10. In this example we will go over what we've described so far for the code $\mathbf{B}_3$, which is the the binary double-error-correcting BCH code of length $q-1 = 2^3 - 1 = 7$. By definition, we have

$$\mathbf{B}_3 = \big(f_\alpha(t) f_{\alpha^3}(t)\big) \subset \mathbb{F}_2[t]/(t^7-1),$$

where α is the primitive element of $\mathbb{F}_8$ which satisfies $\alpha^3+\alpha+1=0$. Note that $f_\alpha(t)=t^3+t+1$ and $f_{\alpha^3}(t)=t^3+t^2+1$ are the corresponding minimal polynomials over $\mathbb{F}_2$. Also note that $\dim(\mathbf{B}_3^\perp)=\deg\big(f_\alpha(t)f_{\alpha^3}(t)\big)=6$ over $\mathbb{F}_2$ and $\mathbf{B}_3^\perp=\mathbf{tr}(J^\perp)$ where $J=\big((t-\alpha)(t-\alpha^3)\big)\subset\mathbb{F}_8[t]/(t^7-1)$.

Another representation we had for the dual was $\mathbf{B}_3^\perp=\{\big(\mathrm{tr}(\lambda x+\mu x^3)\big)_{x\in\mathbb{F}_8^*};\lambda,\mu\in\mathbb{F}_8\}$. To illustrate this representation more clearly, let's write the codeword $v_{1,1}$ in $\mathbf{B}_3^\perp$ which is obtained by choosing $\lambda=\mu=1\in\mathbb{F}_8$.

$$\begin{aligned} v_{1,1} &= \big(\mathrm{tr}(x+x^3)\big)_{x\in\mathbb{F}_8^*} \\ &= \big(\mathrm{tr}(1+1^3),\mathrm{tr}(\alpha+\alpha^3),\mathrm{tr}(\alpha+(\alpha^2)^3),\ldots,\mathrm{tr}(\alpha^6+(\alpha^6)^3)\big) \\ &= \big(\mathrm{tr}(0),\mathrm{tr}(1),\mathrm{tr}(1),\mathrm{tr}(\alpha^5),\mathrm{tr}(1),\mathrm{tr}(\alpha^6),\mathrm{tr}(\alpha^3)\big) \end{aligned}$$

The trace mapping from $\mathbb{F}_8$ to $\mathbb{F}_2$ takes $\{0,\alpha,\alpha^2,\alpha^4\}$ to 0 and it takes the remaining four elements of $\mathbb{F}_8$ to 1. Therefore we obtain $v_{1,1}=(0,1,1,1,1,1,1)$. Similarly one can easily show that $v_{\alpha,\alpha}=\big(\mathrm{tr}(\alpha x+\alpha x^3)\big)_{x\in\mathbb{F}_8^*}=(0,0,0,1,0,1,0)$.

In general, if we take an arbitrary nonzero codeword $v_{\lambda,\mu}=\big(\mathrm{tr}(\lambda x+\mu x^3)\big)_{x\in\mathbb{F}_q^*}$ in $\mathbf{B}_m^\perp$, then we can find how many times the trace takes the value zero by the additive form of Hilbert's Theorem 90.

Theorem 1.11. (Hilbert's Theorem 90) *For $a\in\mathbb{F}_{q^m}$, one has $\mathrm{tr}(a)=0$ if and only if $a=b^q-b$ for some $b\in\mathbb{F}_{q^m}$.*

Proof. See [18] □

Theorem 1.11 and our preceding arguments lead us to the following result.

Proposition 1.12. *(i)* $\mathbf{B}_m^\perp=\{\big(\mathrm{tr}(\lambda x+\mu x^3)\big)_{x\in\mathbb{F}_q^*};\lambda,\mu\in\mathbb{F}_q\}$.

(ii) If $v_{\lambda,\mu}=\big(\mathrm{tr}(\lambda x+\mu x^3)\big)_{x\in\mathbb{F}_q^*}$ is an arbitrary codeword in $\mathbf{B}_m^\perp$, then its weight is given by

$$|v_{\lambda,\mu}|=q-1-\frac{1}{2}\big(\#_{\mathbb{F}_q}(y^2+y=\lambda x+\mu x^3)-2\big),$$

where $\#_{\mathbb{F}_q}(y^2+y=\lambda x+\mu x^3)$ *denotes the number of* $\mathbb{F}_q$*-rational points on the affine plane curve* $y^2+y=\lambda x+\mu x^3$.

Proof. (i) This was already proved in the arguments before Example 1.10.

(ii) We need to find how many components of the vector $\left(\mathrm{tr}(\lambda x+\mu x^3)\right)_{x\in\mathbb{F}_q^*}$ are zero. By Hilbert's Theorem 90, for each $x_0\in\mathbb{F}_q$ with $\mathrm{tr}(\lambda x_0+\mu x_0^3)=0$ there exists $y_0\in\mathbb{F}_q$ such that $y_0^2+y_0=\lambda x_0+\mu x_0^3$. Observe that $\tilde{y_0}=y_0+1$, also satisfies the same equality with x_0, meaning that (x_0,y_0) and $(x_0,\tilde{y_0})$ are $\mathbb{F}_q$-rational points on the curve $y^2+y=\lambda x+\mu x^3$. In other words, for every zero trace component in $v_{\lambda,\mu}$, there exists two $\mathbb{F}_q$-rational points on this affine curve. First subtract two from $\#_{\mathbb{F}_q}(y^2+y=\lambda x+\mu x^3)$ to exclude two points corresponding to $x=0$, which is not in the representation of $v_{\lambda,\mu}$, and then divide the result by two to actually count the number of $x\in\mathbb{F}_q^*$ for which $\mathrm{tr}(\lambda x+\mu x^3)=0$. □

Relating the weights of codewords in $\mathbf{B}_m^{\perp}$ to algebraic curves as above makes it clear that we should understand the number of $\mathbb{F}_q$-rational points on the family $\mathcal{F}=\{y^2+y=\lambda x+\mu x^3;\lambda,\mu\in\mathbb{F}_q\}$. When $\mu=0$ and $\lambda\neq 0$ these curves are rational curves and they have q affine points over $\mathbb{F}_q$. Otherwise these are elliptic curves of special type. We will briefly look at the properties of these elliptic curves that we need and refer to the literature for some important results.

Definition 1.13. An elliptic curve E over $\mathbb{F}_q$ is called *supersingular* if $\mathrm{End}_{\overline{\mathbb{F}}_q}(E)$ is non-commutative, where $\overline{\mathbb{F}}_q$ denotes the algebraic closure of $\mathbb{F}_q$.

By definition, supersingularity depends on the curve over $\overline{\mathbb{F}}_q$ and elliptic curves over $\overline{\mathbb{F}}_q$ are determined, up to isomorphism, by their j-invariant (For the usual formulaire on elliptic curves, including the j-invariant, see [28]). In general, if j is not 0 or 1728, then $\#\mathrm{Aut}_{\overline{\mathbb{F}}_q}(E)$ equals 2 and in characteristic 2, if j is 0=1728, then $\#\mathrm{Aut}_{\overline{\mathbb{F}}_2}(E)$ equals 24 (see the end of Section 2 in [30]). On the other hand,

we have the following mass formula of Eichler and Deuring (see [28] or [30]):

$$\sum_{E/\bar{\mathbb{F}}_p:\text{supsing.}} \frac{1}{\#\text{Aut}_{\bar{\mathbb{F}}_p}(E)} = \frac{p-1}{24}.$$

For $p = 2$, this implies that the sum is $\frac{1}{24}$ and hence the only supersingular elliptic curves in characteristic 2 are the ones with j-invariant 0. Note that elliptic curves in our family $\mathcal{F}$ have $j = 0$ and hence they are supersingular.

Definition 1.14. Two elliptic curves E_1 and E_2 over $\mathbb{F}_q$ are called *isogenous* if there is a homomorphism, i.e., a map that respects the group structure of $\mathbb{F}_q$-rational points, between them. This notion is equivalent to having $\#_{\mathbb{F}_q}(E_1) = \#_{\mathbb{F}_q}(E_2)$ (see [32], in particular Tate's Theorem in Chapter 2 and Theorem 4.1 of this paper).

Proposition 1.12 indicates that not only do we need to figure out the number of $\mathbb{F}_q$-rational points in $\mathcal{F}$ (i.e., isogeny classes appearing in $\mathcal{F}$), but also we need to understand the distribution of such numbers in the family.

Proposition 1.15. *Let $\mathbb{F}_q = \mathbb{F}_{2^m}$ be a finite field. If m is odd (resp., m is even), there are, up to isomorphism, three (resp., seven) supersingular elliptic curves over $\mathbb{F}_q$. The table below shows some properties of these supersingular curves.*

Table 1. Supersingular Elliptic Curves in characteristic 2

m odd

$\#_{\mathbb{F}_q}(E)$	freq.	$\#\text{Aut}_{\mathbb{F}_q}(E)$
$q+1-\sqrt{2q}$	1	4
$q+1$	1	2
$q+1+\sqrt{2q}$	1	4

m even

$\#_{\mathbb{F}_q}(E)$	freq.	$\#\text{Aut}_{\mathbb{F}_q}(E)$
$q+1-2\sqrt{q}$	1	24
$q+1-\sqrt{q}$	2	6
$q+1$	1	4
$q+1+\sqrt{q}$	2	6
$q+1+2\sqrt{q}$	1	24

Proof. Basically [26] gives this result but to make it more understandable we will give detail and references. We know that the number of $\mathbb{F}_q$-rational points on an elliptic curve is $q+1-t$ for some integer t, which is in fact the trace of the so-called Frobenious endomorphism of the curve (See [26], [28] or [30]). Theorem 4.1 in [32] gives the possible t values for supersingular elliptic curves and Theorem 4.6 of [26] gives the number of isomorphism classes which share the same t value, i.e., which are in the same isogeny class. □

Note that one point at infinity is also counted in Table 1. In the weight computations we disregard that point since our formulas involve the number of points on the affine part of the curves. We now need to count how often an isomorphism class of a supersingular elliptic curve occurs in our family $\mathcal{F}$.

Proposition 1.16. *Let E be a supersingular elliptic curve over $\mathbb{F}_q$. The number of curves with $\mu \neq 0$ in the family $\mathcal{F}$ that are isomorphic over $\mathbb{F}_q$ to E is equal to*

$$\frac{(q-1)(\#_{\mathbb{F}_q}(E)-1)}{\#Aut_{\mathbb{F}_q}(E)}.$$

Proof. See [25] □

It is now easy to get the weights in $\mathbf{B}_m^{\perp}$ from Propositions 1.12, 1.15 and 1.16.

Table 2. Weights of $\mathbf{B}_m^{\perp}$

m odd

weight	frequency
0	1
$\frac{q+\sqrt{2q}}{2}$	$\frac{q-1}{4}(q-\sqrt{2q})$
$\frac{q}{2}$	$\frac{q-1}{2}q+(q-1)$
$\frac{q-\sqrt{2q}}{2}$	$\frac{q-1}{4}(q+\sqrt{2q})$

m even

weight	frequency
0	1
$\frac{q+2\sqrt{q}}{2}$	$\frac{q-1}{24}(q-2\sqrt{q})$
$\frac{q+\sqrt{q}}{2}$	$\frac{q-1}{3}(q-\sqrt{q})$
$\frac{q}{2}$	$\frac{q-1}{4}q+(q-1)$
$\frac{q-\sqrt{q}}{2}$	$\frac{q-1}{3}(q+\sqrt{q})$
$\frac{q-2\sqrt{q}}{2}$	$\frac{q-1}{24}(q+2\sqrt{q})$

Finally, by using The MacWilliams Identity one can obtain the weight enumerator for the binary BCH(2) code.

1.3 Artin-Schreier Curves

Our purpose in this section is to introduce a class of well-known algebraic curves, called Artin-Schreier curves.

Let $\mathbb{F}_q = \mathbb{F}_{p^l}$ with $l \geq 1$ and consider $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$ with $m > 1$. Let $f(x)$ be a polynomial in $\mathbb{F}_q[x]$. A curve of the form

$$y^p - y = f(x) \tag{1.1}$$

is an Artin-Schreier (A-S) cover of the projective line over $\mathbf{F}_q$ (i.e., A-S extension of the rational function field $\mathbf{F}_q(x)/\mathbf{F}_q$) if $f(x)$ can't be written as $w^p - w$ for any w in $\mathbf{F}_q(x)$. For these curves, one can use Lemma III.7.7 and Proposition III.7.8 in [29] to compute the genus and obtain other necessary information. However, we want to look at a bit more general curves, namely curves of the form

$$y^q - y = f(x), \tag{1.2}$$

where $f(x)$ is a polynomial in $\mathbf{F}_{q^m}[x]$. If the polynomail $t^q - t - f(x)$ in $\mathbf{F}_{q^m}(x)[t]$ is irreducible over $\mathbf{F}_{q^m}(x)$, then such a curve is an elementary abelian p-extension of the rational function field $\mathbf{F}_{q^m}(x)/\mathbf{F}_{q^m}$, but we will also refer to the curve (1.2) as an A-S curve. The following fact is taken from [8] and it states when the above polynomial is irreducible.

Proposition 1.17. *The following conditions are equivalent:*

(i) $t^q - t - f(x)$ *is irreducible over* $\mathbf{F}_{q^m}(x)$.

(ii) $t^p - t - \mu f(x)$ *is irreducible over* $\mathbf{F}_{q^m}(x)$ *for every* μ *in* $\mathbf{F}_q^*$.

(iii) $\mu f(x) \notin \psi(\mathbf{F}_{q^m}(x))$ *for any* μ *in* $\mathbf{F}_q^*$, *where* $\psi : z \mapsto z^p$ *is the Artin-Schreier operator.*

We would like to remark that for our arguments on function fields in this section, [29] is a good reference. We first start with the following observation.

Lemma 1.18. *Let $f(x) \in \mathbb{F}_{q^m}[x]$ be a polynomial function in the rational function field $\mathbb{F}_{q^m}(x)$ of degree relatively prime to $p = char(\mathbb{F}_{q^m})$. Then we have:*

(i) If P is an affine place of $\mathbb{F}_{q^m}(x)$ and v_P is the corresponding valuation, then there exists $z \in \mathbb{F}_{q^m}(x)$ such that $v_P(f - (z^q - z)) \geq 0$ and there is no $z \in \mathbb{F}_{q^m}(x)$ such that $v_P(f - (z^q - z))$ is a negative integer which is not 0 mod p.

(ii) If P_∞ is the place at infinity of $\mathbb{F}_{q^m}(x)$ and v_∞ is the corresponding valuation, then there exists $z \in \mathbb{F}_{q^m}(x)$ such that $v_\infty(f - (z^q - z)) = -m < 0$ for some integer m which is not divisible by p and $v_\infty(f - (z^q - z))$ is not positive for any $z \in \mathbb{F}_{q^m}(x)$. The number m is uniquely determined and, actually, equal to $deg(f)$.

Proof. For notational convenience, we will have $K = \mathbb{F}_{q^m}$ and $F = K(x) = \mathbb{F}_{q^m}(x)$. Places of the rational function field F can be considered in two parts. The affine places, which correspond to irreducible polynomials in $K[x]$ and the place at infinity which corresponds to the element $\frac{1}{x} \in F$.

Let $P \in \mathbb{P}_F$ be an affine place corresponding to the irreducible polynomial $p(x) \in K[x]$. Obviously, one has

$$v_P(f - (0^q - 0)) \geq 0.$$

Let $z \in F$ be an arbitrary function. Our claim is to show that z can't satisfy

$$v_P(f - (z^q - z)) = -m < 0 \tag{1.3}$$

for any $m > 0$ relatively prime to p.

Since $v_P(f) \geq 0$, one must have $v_P(z^q - z) = -m$ for some $m > 0$ and $m \not\equiv 0 \bmod p$ in order for (1.3) to hold. (This is due to the triangle and strict triangle inequalities for valuations.) On the other hand, $v_P(z^q) = q \cdot v_P(z)$ and therefore if

$v_P(z) \geq 0$, then $v_P(z^q - z) \geq 0$ as well. Hence, we also need $v_P(z) < 0$ for (1.3) to hold. So, $z \in F$ must be chosen as

$$z = \frac{a(x)}{p(x)^i b(x)},$$

where $a(x)$ and $b(x)$ are in $K[x]$, $p(x)$ doesn't divide $a(x)$ and $b(x)$, and $i \geq 1$. Then we have

$$\left.\begin{array}{l} v_P(z) = -i \\ v_P(z^q) = -iq \end{array}\right\} \implies v_P(z^q - z) = -iq \equiv 0 \ mod\ p.$$

Therefore (1.3) can't hold for any $z \in F$ at any affine place P.

Now let P_∞ be the place at infinity of the rational function field F and let v_∞ denote the corresponding valuation. This time we have

$$v_\infty(f - (0^q - 0)) = -deg(f) < 0$$

and this is not equivalent to 0 mod p by the hypothesis on the degree of f. We want to show that the following can't hold for any $z \in F$:

$$v_\infty(f - (z^q - z)) \geq 0. \tag{1.4}$$

Note that since $v_\infty(f) < 0$, one must have $v_\infty(z^q - z) = v_\infty(f) = -deg(f)$ for (1.4) to have a chance to hold. This implies that $v_\infty(z)$ is negative and one needs $-deg(f) = v_\infty(z^q - z) = q \cdot v_\infty(z)$. However, the last equality is impossible since $deg(f)$ is relatively prime to p. Therefore (1.4) can't hold for any $z \in F$ at P_∞.

Finally, we will show the uniqueness of the number m for the place at infinity. The following equation holds for any $z \in F$ and is easy to see from the triangle inequality, strict triangle inequality and some of our observations in the proof up to this point.

$$v_\infty(f - (z^q - z)) = \begin{cases} -deg(f), & \text{if } v_\infty(z^q - z) > -deg(f) \\ < -deg(f) \ \& \ \equiv_p 0, & \text{if } v_\infty(z^q - z) < -deg(f) \end{cases} \tag{1.5}$$

Note that the case $v_\infty(z^q - z) = -deg(f)$ has already been ruled out by our observations along the proof. By (1.5), $-m$ is the maximal value of $v_\infty(f-(z^q-z))$ which is not divisible by p. In fact $m = deg(f)$. □

Definition 1.19. A polynomial of the form

$$a(t) = a_n t^{p^n} + a_{n-1} t^{p^{n-1}} + \cdots + a_0 t \in K[t],$$

where K is a characteristic p field, is called an *additive polynomial.*

Note that an additive polynomial satisfies

$$a(u+v) = a(u) + a(v)$$

for any u and v in some extension field of K.

The following is taken from [29].

Theorem 1.20. *Consider an algebraic function field F/K with constant field K of characteristic $p > 0$ and an additive separable polynomial $a(t) \in K[t]$ of degree p^n which has all its roots in K. Let $u \in F$ and suppose that for any place $P \in \mathbb{P}_F$, there is an element $z \in F$ such that*

$$v_P(u - a(z)) \geq 0$$

or

$$v_P(u - a(z)) = -m < 0$$

with $m \not\equiv 0 \mod p$. Define $m_P = -1$ in the first case and $m_P = m$ in the second case. Then m_P is a well-defined integer. Consider the extension $F' = F(y)$ where y satisfies the equation

$$a(y) = u.$$

If there exists at least one place $Q \in \mathbb{P}_F$ with $m_Q > 0$, then the following holds.

(i) F'/F is a Galois extension of degree $[F' : F] = p^n$

(ii) K is algebraically closed in F'.

(iii) Any place $P \in \mathbb{P}_F$ is unramified in F'/F if $m_P = -1$ and totally ramified if $m_P > 0$.

(iv) Let g' (resp., g) be the genus of F' (resp., F). Then

$$g' = p^n g + \frac{p^n - 1}{2}\left(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) deg P\right).$$

Recall that we are interested in curves of the form $y^q - y = f(x)$ over $\mathbb{F}_{q^m}$, where $\deg(f)$ is relatively prime to p. Note that our additive separable polynomial is $a(t) = t^q - t \in \mathbb{F}_{q^m}[t]$, which obviously has all its roots in $\mathbb{F}_q \subset \mathbb{F}_{q^m}$. Also, our curves are extensions of the rational function field $\mathbb{F}_{q^m}(x)/\mathbb{F}_{q^m}$ and they satisfy the hypothesis of Theorem 1.20 by Lemma 1.18. Therefore, these curves have all the properties that are listed in Theorem 1.20. We use this fact to compute the genus in the next lemma.

Proposition 1.21. *Let $X : y^q - y = f(x)$ be an A-S curve over $\mathbb{F}_{q^m}$, where $f(x) \in \mathbb{F}_{q^m}[x]$ and $(\deg(f), p) = 1$. Then the genus of X is*

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

Proof. By Lemma 1.18 and Theorem 1.20(iii), the only ramification occurs at the place at infinity, P_∞, of $\mathbb{F}_{q^m}(x)$ and $m_{P_\infty} = \deg(f)$. Then using Theorem 1.20(iv), we get the genus of X. □

If $\deg(f)$ is not relatively prime to p, then one can still compute the genus assuming that the curve is A-S. For this, let's assume that $t^q - t - f(x) \in \mathbb{F}_{q^m}(x)[t]$ is irreducible over $\mathbb{F}_{q^m}(x)$, which may be true even if the degree of $f(x)$ is divisible by p. Theorem 2.1 in [8] gives a formula for the genus of X, i.e., the function field extension $\mathbb{F}_{q^m}(x, y)/\mathbb{F}_{q^m}(x)$ given with the equation $y^q - y = f(x)$, in terms of the

genera of degree p intermediate fields of the extension $\mathbb{F}_{q^m}(x,y)/\mathbb{F}_{q^m}(x)$. There are $\frac{q-1}{p-1} = \frac{p^l-1}{p-1}$ such subfields and they are of the form

$$y_\mu^p - y_\mu = \mu f(x), \quad \mu \in \mathbb{F}_q^*, \tag{1.6}$$

where

$$y_\mu = (\mu y)^{p^{l-1}} + (\mu y)^{p^{l-2}} + \cdots (\mu y)^p + \mu y.$$

If these degree p intermediate fields are denoted as E_i for $i \in \mathcal{J}$, then

$$g(X) = \sum_{i \in \mathcal{J}} g(E_i).$$

Note that since the degree of $\mu f(x)$ is not relatively prime to p, we can't compute the genus of E_i using Proposition 1.21. We show what could be done in such a situation in the following proposition in which we will show that a certain curve is A-S and we will compute its genus even though its degree on the right hand side is not relatively prime to p.

Proposition 1.22. *Consider the extension $F = \mathbb{F}_{q^m}(x,y)$ of the rational function field $\mathbb{F}_{q^m}(x)$ which is defined by the equation*

$$y^q - y = \sum_{j=0}^{d} \lambda_j x^{r_j p^{i_j}},$$

where $\lambda_j \in \mathbb{F}_{q^m}$, $p \nmid r_j$ for any j, and the r_j's are distinct. Then F is A-S and its genus is

$$\frac{(q-1)(r-1)}{2},$$

where r is the maximum of $\{r_1, r_2, \ldots, r_d\}$.

Proof. We will denote $\sum_j \lambda_j x^{r_j p^{i_j}}$ by $f(x)$ for simplicity. Assume, without loss, that $r_d p^{i_d}$ is the degree of $f(x)$. Note that this is relatively prime to p if and only if $i_d = 0$. In this case r_d is the maximum of all r_i's and the result follows from Proposition 1.21. Therefore we assume that $i_d > 0$. We will first show that the extension

F is A-S and for this, showing that the polynomial $t^q - t - f(x)$ is irreducible over $\mathbb{F}_{q^m}(x)$ is enough. Suppose this is not the case. Then, by Proposition 1.17, there exists β in $\mathbb{F}_q^*$ such that $\beta f(x) = \sum_j \beta\lambda_j x^{r_j p^{i_j}}$ is in $\psi(\mathbb{F}_{q^m}(x))$. In other words, there exits $u \in \mathbb{F}_{q^m}(x)$ such that $\beta f(x) = u^p - u$. Define

$$\begin{aligned} z \;=\; & \beta^{p^{-1}}\lambda_d^{p^{-1}} x^{r_d p^{i_d - 1}} + \beta^{p^{-2}}\lambda_d^{p^{-2}} x^{r_d p^{i_d - 2}} + \cdots + \beta^{p^{-i_d}}\lambda_d^{p^{-i_d}} x^{r_d} \\ & + \beta^{p^{-1}}\lambda_{d-1}^{p^{-1}} x^{r_{d-1} p^{i_{d-1} - 1}} + \beta^{p^{-2}}\lambda_{d-1}^{p^{-2}} x^{r_{d-1} p^{i_{d-1} - 2}} + \cdots + \beta^{p^{-i_{d-1}}}\lambda_{d-1}^{p^{-i_{d-1}}} x^{r_{d-1}} \\ & \vdots \\ & + \beta^{p^{-1}}\lambda_1^{p^{-1}} x^{r_1 p^{i_1 - 1}} + \beta^{p^{-2}}\lambda_1^{p^{-2}} x^{r_1 p^{i_1 - 2}} + \cdots + \beta^{p^{-i_1}}\lambda_1^{p^{-i_1}} x^{r_1} \end{aligned}$$

Note that z is in $\mathbb{F}_{q^m}(x)$ since p^{th} roots exist in $\mathbb{F}_{q^m}$ and hence all the coefficients in z are elements of $\mathbb{F}_{q^m}$. Also note that z gives the following nice reduction:

$$\beta f(x) - (z^p - z) = \beta^{p^{-i_1}}\lambda_1^{p^{-i_1}} x^{r_1} + \beta^{p^{-i_2}}\lambda_2^{p^{-i_2}} x^{r_2} + \cdots + \beta^{p^{-i_d}}\lambda_d^{p^{-i_d}} x^{r_d}$$

Let $r = \max\{r_1, r_2, \ldots, r_d\}$ and observe that r is the degree of the above expression and it is relatively prime to p. If v_∞ is the valuation corresponding to the place at infinity of the rational function field, we have

$$\begin{aligned} \infty = v_\infty(0) &= v_\infty\big(\beta f(x) - (u^p - u)\big) \\ &= v_\infty\big(\beta f(x) - (z^p - z) + (z^p - z) - (u^p - u)\big) \\ &= v_\infty\big(\beta f(x) - (z^p - z) - \big((u - z)^p - (u - z)\big)\big) \\ &= v_\infty\big(\beta^{p^{-i_1}}\lambda_1^{p^{-i_1}} x^{r_1} + \cdots + \beta^{p^{-i_d}}\lambda_d^{p^{-i_d}} x^{r_d} - \big((u - z)^p - (u - z)\big)\big) \end{aligned}$$

Using the fact that r is relatively prime to p and Lemma III.7.7 in [29], we can show that the last expression above is at most $-r$, which is a contradiction since $\infty \not< -r$. This proves that $t^q - t - f(x)$ is irreducible over $\mathbb{F}_{q^m}(x)$ and hence the function field F is A-S.

The genus of F is the sum of genera of the degree p intermediate fields. The form of these intermediate fields is given in (1.6) and following the same reduction procedure above, they can be reduced to the form

$$y_\mu^p - y_\mu = f_\mu(x), \ \forall \mu \in \mathbb{F}_{q^m}^*,$$

where the degree of $f_\mu(x)$ is r for every μ. Therefore, by Proposition 1.21, the genus for each of these fields is $\frac{(p-1)(r-1)}{2}$. Since there are $\frac{q-1}{p-1}$ of these the result follows. □

A genus formula similar to that of Proposition 1.22 is not easy to write if the r_i's are not distinct. This is because the reduction argument we apply to degree p intermediate fields may cancel some terms with the same r_j exponent and there are many possibilities of such cancellations for different intermediate fields.

1.4 Artin-Schreier Families and Cyclic Codes

Our purpose in this section is to use the method described in Section 1.2 to come up with an upper bound on the number of rational points of some family of curves. These results will be used in our arguments concerning two-dimensional cyclic codes in Chapter 3.

Consider the family

$$\mathcal{F} = \{y^q - y = \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s};\ \lambda_j \in \mathbb{F}_{q^m},\ i_j > 0\}. \qquad (1.7)$$

We will refer to the right hand side of a curve in $\mathcal{F}$ as $f(x)$ as before. Note that $f(x)$ doesn't have a nonzero constant term for any choice of $\lambda_1, \lambda_2, \ldots, \lambda_s$ in $\mathbb{F}_{q^m}$. Even though we will call $\mathcal{F}$ an A-S family, note that not every curve in $\mathcal{F}$ is necessarily A-S (i.e., elementary abelian p-extension). This is because $t^q - t - f(x)$ may not be irreducible over $\mathbb{F}_{q^m}(x)[t]$ for every $f(x)$ that appears in $\mathcal{F}$.

The well-known Hasse-Weil-Serre (H-W-S) bound implies that for a curve $X \in \mathcal{F}$, the number of projective $\mathbb{F}_{q^m}$-rational points is bounded by

$$q^m + 1 + g_X[2\sqrt{q^m}],$$

where g_X is the genus of $X \in \mathcal{F}$, which may differ among the members of $\mathcal{F}$. Since the curves in our family have only one point at infinity, the H-W-S bound on their affine $\mathbb{F}_{q^m}$-rational points would be one less than the above bound.

Now we will state another bound on this family which holds for any curve in $\mathcal{F}$, independent of the genus, and which is tighter than H-W-S when g_X is big.

Proposition 1.23. *For any $X \in \mathcal{F}$, the number of affine $\mathbb{F}_{q^m}$-rational points is divisible by q and it is at most q^{m+1}.*

Proof. For $a \in \mathbb{F}_{q^m}$, if $\beta \in \mathbb{F}_{q^m}$ is a root of $y^q - y - f(a) \in \mathbb{F}_{q^m}[y]$ then all the elements in $\{\beta + \mathbb{F}_q\} \subset \mathbb{F}_{q^m}$ are also roots of this polynomial. Therefore if we look at the number of affine $\mathbb{F}_{q^m}$-rational points of a curve in $\mathcal{F}$, this number will be divisible by q and it is at most $q \cdot q^m = q^{m+1}$ if $y^q - y - f(a)$ has a root in $\mathbb{F}_{q^m}$ for every $a \in \mathbb{F}_{q^m}$. □

Remark 1.24. For the A-S members of $\mathcal{F}$, one can give a simple function field theoretic proof of this fact using the knowledge of ramifications in such curves, which we described in Section 1.3.

A natural question one might ask is when does a family like $\mathcal{F}$ contain a curve that attains the bound q^{m+1}. We will answer this question in the next theorem but before that, we need the following definition.

Definition 1.25. Let $q = p^l$ be a prime power, where $l \geq 1$, and c be a positive integer that is not divisible by p. If $0 \leq b < c$ is an integer, then let r be the smallest number such that $q^{r+1}b \equiv b \bmod c$. *The q-cyclotomic coset containing b*

mod c is the set

$$B = \{b, qb, q^2b, \ldots, q^rb\},$$

where each q^ib is reduced mod c.

As a convention, we take the q-cyclotomic coset containing c mod c as the singleton $\{0\}$. The following is the main theorem of this section.

Theorem 1.26. *Let* $\mathbb{F}_q$ *and* $\mathbb{F}_{q^m}$ *be as before. Consider the family of curves*

$$\mathcal{F} = \{y^q - y = \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s};\ \lambda_j \in \mathbb{F}_{q^m},\ i_j > 0\}.$$

We have the following:

(i) If $i_1, i_2, \ldots, i_s$ *are chosen so that the* q*-cyclotomic cosets,* B_j*, mod* $q^m - 1$ *containing* i_j $(j = 1, 2, \ldots, s)$ *are all distinct with cardinality* $m = [\mathbb{F}_{q^m} : \mathbb{F}_q]$*, then no curve in* $\mathcal{F}$*, except the "trivial" one obtained by letting* $\lambda_j = 0$ *for all* $j \in \{1, 2, \ldots, s\}$*, has* q^{m+1} *affine* $\mathbb{F}_{q^m}$*-rational points.*

(ii) Otherwise, i.e., if either two i_j*'s are in the same* q*-cyclotomic coset mod* $q^m - 1$ *or* $|B_j| < m$ *for some* $j \in \{1, 2, \ldots, s\}$*, there exists a "nontrivial" curve in* $\mathcal{F}$ *with* q^{m+1} *affine* $\mathbb{F}_{q^m}$*-rational points.*

Proof. Observe that we can assume $i_s < q^m$ since otherwise one can use the fact that $x^{q^m} = x$ in $\mathbb{F}_{q^m}$ to reduce the degree.

(i) Let α be a primitive element of $\mathbb{F}_{q^m}$ and consider $\alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_s}$ in $\mathbb{F}_{q^m}$. The assumption on the $|B_j|$'s implies that each α^{i_j} has m distinct $\mathbb{F}_q$-conjugates and hence they have degree m over $\mathbb{F}_q$ (i.e., $[\mathbb{F}_q(\alpha^{i_j}) : \mathbb{F}_q] = m$ for all $j = 1, 2, \ldots, s$). Let I be the cyclic code over $\mathbb{F}_q$ defined by

$$I = (f_{\alpha^{i_1}}(t) f_{\alpha^{i_2}}(t) \ldots f_{\alpha^{i_s}}(t)) \subset \mathbb{F}_q[t]/(t^{q^m-1} - 1),$$

where $f_{\alpha^{i_j}}(t)$ (for all j) is the minimal polynomial of α^{i_j} over $\mathbb{F}_q$. Since the q-cyclotomic cosets mod $q^m - 1$ are all distinct, the α^{i_j}'s are not $\mathbb{F}_q$-conjugate to

each other and hence we have the following diagram from Delsarte's Theorem

$$\begin{array}{ccc} I & \xleftarrow{\text{Res}} & J \\ \updownarrow & & \updownarrow \\ I^{\perp} & \xleftarrow{\mathbf{tr}} & J^{\perp} \end{array} \tag{1.8}$$

where $J = ((t-\alpha^{i_1})(t-\alpha^{i_2})\dots(t-\alpha^{i_s})) \subset \mathbb{F}_{q^m}[t]/(t^{q^m-1}-1)$. Note that $\mathbf{tr}$ is defined as

$$\mathbf{tr}(w) = \big(\mathrm{tr}(w_1), \mathrm{tr}(w_2), \dots, \mathrm{tr}(w_{q^m-1})\big), \ \forall w = (w_1, \dots, w_{q^m-1}) \in J^{\perp},$$

where tr is the trace mapping from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$.

Observe that for any codeword $b(t) = \sum_{i=0}^{q^m-2} b_i t^i$ in J, $b(\alpha^{i_j}) = 0$, for all $j = 1, 2, \dots, s$. These equalities can also be written as:

$$\begin{aligned} (b_0, b_1, \dots, b_{q^m-2}) \cdot (1, (\alpha^{i_1})^1, \dots, (\alpha^{i_1})^{q^m-2}) &= 0 \\ (b_0, b_1, \dots, b_{q^m-2}) \cdot (1, (\alpha^{i_2})^1, \dots, (\alpha^{i_2})^{q^m-2}) &= 0 \\ &\vdots \\ (b_0, b_1, \dots, b_{q^m-2}) \cdot (1, (\alpha^{i_s})^1, \dots, (\alpha^{i_s})^{q^m-2}) &= 0 \end{aligned}$$

for any $b(t) \in J$. Remembering the vector representation of cyclic codes, the above equalities mean that the following vectors are codewords in $J^{\perp}$:

$$\left.\begin{aligned} v_1 &= (1, (\alpha^1)^{i_1}, \dots, (\alpha^{q^m-2})^{i_1}) \\ v_2 &= (1, (\alpha^1)^{i_2}, \dots, (\alpha^{q^m-2})^{i_2}) \\ &\vdots \\ v_s &= (1, (\alpha^1)^{i_s}, \dots, (\alpha^{q^m-2})^{i_s}) \end{aligned}\right\} \in J^{\perp}. \tag{1.9}$$

The generator polynomial of J reveals that the $\mathbb{F}_{q^m}$-dimension of $J^{\perp}$ is s (cf. Remark 1.4). We want to show that $\{v_1, v_2, \dots, v_s\} \subset J^{\perp}$ forms an $\mathbb{F}_{q^m}$-basis for the dual code $J^{\perp}$.

Since α is a primitive element in $\mathbb{F}_{q^m}$, $1, \alpha, \ldots, \alpha^{q^m-2}$ are all the elements in $\mathbb{F}_{q^m}^*$. Therefore, as in [9] and [25], we have the following alternative representation for the v_j's:

$$v_j = (x^{i_j})_{x \in \mathbb{F}_{q^m}^*}, \ j = 1, 2, \ldots, s. \tag{1.10}$$

Here $(x^{i_j})_{x \in \mathbb{F}_{q^m}^*}$ denotes a vector of length $q^m - 1$ in which the coordinates are obtained by letting x take every value in $\mathbb{F}_{q^m}^*$ following the order

$$\mathbb{F}_{q^m}^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{q^m-2}\}$$

of elements. Hence, any $\mathbb{F}_{q^m}$-linear combination of the v_j's will be in the form

$$\sum_{j=1}^{s} \lambda_j v_j = (\lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s})_{x \in \mathbb{F}_{q^m}^*}, \ \lambda_j \in \mathbb{F}_{q^m}. \tag{1.11}$$

This means that for some $\lambda_1 \ldots, \lambda_s \in \mathbb{F}_{q^m}$,

$$\sum_{j=1}^{s} \lambda_j v_j = \vec{0} \ \Leftrightarrow \ \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s} = 0, \ \forall x \in \mathbb{F}_{q^m}^*.$$

However, a polynomial of degree $i_s < q^m$, which vanishes at $x = 0$, can't vanish on $\mathbb{F}_{q^m}^*$ unless all the coefficients are zero, since the exponents are all distinct. This proves that $\{v_1, v_2, \ldots, v_s\}$ forms an $\mathbb{F}_{q^m}$-basis for $J^\perp$. Therefore $J^\perp$ is of the form

$$J^\perp = < v_1, v_2, \ldots, v_s > = \{\sum_{j=1}^{s} \lambda_j v_j; \ \lambda_j \in \mathbb{F}_{q^m}\}, \tag{1.12}$$

or

$$J^\perp = \{(\lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s})_{x \in \mathbb{F}_{q^m}^*}; \ \lambda_j \in \mathbb{F}_{q^m}\}, \tag{1.13}$$

which gives the following representation for $I^\perp$ by Delsarte's Theorem:

$$I^\perp = \{\left(\mathrm{tr}(\lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s})\right)_{x \in \mathbb{F}_{q^m}^*}; \ \lambda_j \in \mathbb{F}_{q^m}\}. \tag{1.14}$$

Note that $\mathbf{tr}$ is an $\mathbb{F}_q$-linear map from $J^\perp$ onto $I^\perp$. If we view $J^\perp$ as an $\mathbb{F}_q$-vector space, its dimension is ms, which is also the dimension of $I^\perp$ over $\mathbb{F}_q$, since $\deg(f_{\alpha^{ij}}(t)) = m$ for all $j = 1, 2, \ldots, s$. Therefore $\mathbf{tr}$ must have a trivial kernel. Equivalently, if v' is an arbitrary codeword in $I^\perp$, then $v' = \mathbf{tr}(v)$ for some $v \in J^\perp$ and

$$|v'| = 0 \Leftrightarrow |v| = 0. \tag{1.15}$$

However, by (1.14),

$$v' = \left(\mathrm{tr}(\lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s})\right)_{x \in \mathbb{F}_{q^m}^*}$$

for some λ_j's in $\mathbb{F}_{q^m}$ and its weight, by Hilbert's Theorem 90, can be written as

$$|v'| = q^m - 1 - \frac{1}{q}\left(\#_{\mathbb{F}_{q^m}}(y^q - y = \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) - q\right). \tag{1.16}$$

Here, $\#_{\mathbb{F}_{q^m}}(y^q - y = \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s})$ denotes the number of affine $\mathbb{F}_{q^m}$-rational points of the curve in paranthesis. Combining (1.15) with (1.16), we see that

$$\#_{\mathbb{F}_{q^m}}(y^q - y = \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) = q^{m+1}$$

$$\Updownarrow$$

$$\lambda_j = 0 \ \textit{for all} \ j = 1, 2, \ldots, s.$$

This proves part (i).

(ii) If i_j and $i_{j'}$ are in the same q-cyclotomic coset mod $q^m - 1$, then in the diagram (1.8) from Delsarte's Theorem, we have the same ideals J and $J^\perp$ as before but I will have one less polynomial factor in its generator since α^{i_j} and $\alpha^{i_{j'}}$ share the same minimal polynomial over $\mathbb{F}_q$. This will reduce the dimension of $I^\perp$ whereas the dimension of $J^\perp$ is still the same. Therefore the surjective $\mathbb{F}_q$-linear map $\mathbf{tr}$ will have a nontrivial kernel, meaning that for some s-tuple $(\mu_1, \mu_2, \ldots, \mu_s) \neq \vec{0}$,

the curve

$$y^q - y = \mu_1 x^{i_1} + \mu_2 x^{i_2} + \cdots + \mu_s x^{i_s}$$

will have q^{m+1} affine $\mathbb{F}_{q^m}$-rational points.

On the other hand, if one of the q-cyclotomic cosets, say B_j, has cardinality $\delta < m$, then this means that $\deg(f_{\alpha^{i_j}}(t)) = \delta$ and again even though J and $J^\perp$ stay the same as in diagram (1.8), the dimension of $I^\perp$ goes down. Then **tr** has a nontrivial kernel and we get the same conclusion. □

We have an immediate corollary coming from the proof of Theorem 1.26, which gives the number of member curves with q^{m+1} rational points in the family $\mathcal{F}$.

Corollary 1.27. *Consider the family $\mathcal{F}$. If there exists β distinct q-cyclotomic cosets mod $q^m - 1$ for the exponents $i_1, i_2, \ldots, i_s$ with cardinalities*

$$|B_j| = \delta_j \leq m, \ j = 1, 2, \ldots, \beta,$$

then $\mathcal{F}$ has $q^{ms - \sum_{j=1}^{\beta} \delta_j}$ members with q^{m+1} affine $\mathbb{F}_{q^m}$-rational points, including the trivial member.

Proof. Remember again the diagram (1.8) from Delsarte's Theorem. J and $J^\perp$ are the same as they were in that diagram, but I is

$$I = (f_1(t) f_2(t) \ldots f_\beta(t)) \subset \mathbb{F}_q[t]/(t^{q^m - 1} - 1),$$

where each $f_j(t)$ is the common minimal polynomial over $\mathbb{F}_q$ of all the powers of α that are in the same q-cyclotomic coset B_j. Then the dimension of $I^\perp$ over $\mathbb{F}_q$ is $\sum_{j=1}^{\beta} \delta_j$ and hence the $\mathbb{F}_q$-dimension of $ker(\mathbf{tr})$ is $ms - \sum_{j=1}^{\beta} \delta_j$. This means that there are $q^{ms - \sum_{j=1}^{\beta} \delta_j}$ s-tuples $(\lambda_1, \lambda_2, \ldots, \lambda_s)$ over $\mathbb{F}_{q^m}$ which produce curves with q^{m+1} affine $\mathbb{F}_{q^m}$-rational points. □

The next corollary is a special case of Theorem 1.26.

Corollary 1.28. *Consider $\mathbb{F}_{q^{\tilde{p}}}$ over $\mathbb{F}_q$, where $\tilde{p}$ is prime. Consider the family $\mathcal{F}$ over $\mathbb{F}_{q^{\tilde{p}}}$ and adopt the meanings of the B_j's from Theorem 1.26. Then the following are equivalent:*

(i) There exists no nontrivial curve in $\mathcal{F}$ with $q^{\tilde{p}+1}$ affine $\mathbb{F}_{q^{\tilde{p}}}$-rational points.

(ii) $B_j \cap B_{j'} = \emptyset$ for all $j \neq j'$ and $qi_j \not\equiv i_j \bmod q^{\tilde{p}} - 1$ for any $j = 1, 2, \ldots, s$.

Proof. Note that the cardinality of a q-cyclotomic coset has to be a divisor of $[\mathbb{F}_{q^{\tilde{p}}} : \mathbb{F}_q] = \tilde{p}$, but the only divisors of $\tilde{p}$ are one and itself. Observe that a q-cyclotomic coset, B_j, having cardinality one means $qi_j \equiv i_j \bmod q^{\tilde{p}} - 1$. □

Our final corollary on A-S families will also be a special case of Theorem 1.26. We state certain families that are similar to Hermitian curves in their appearance and in the sense that they, too, produce maximal curves, i.e., curves that achieve the Hasse-Weil bound. Note that every nontrivial member in the following family is truly an A-S curve.

Corollary 1.29. *Suppose m is even and consider the family*

$$\tilde{\mathcal{F}} = \{y^q - y = \lambda x^{q^{\frac{m}{2}}+1};\ \lambda \in \mathbb{F}_{q^m}\}.$$

Then $\tilde{\mathcal{F}}$ has $q^{\frac{m}{2}}$ curves, including the trivial one, with q^{m+1} affine rational points over $\mathbb{F}_{q^m}$. For any even positive integer m, the number q^{m+1} is equal to the Hasse-Weil bound for a nontrivial member of $\tilde{\mathcal{F}}$.

Proof. Note that we can obtain $\tilde{\mathcal{F}}$ by letting the coefficients $\lambda_j = 0$ for $j = 1, \ldots, s-1$ and choosing $i_s = q^{\frac{m}{2}} + 1$ in the family $\mathcal{F}$ of Theorem 1.26. Note also that the q-cyclotomic coset containing the exponent $q^{\frac{m}{2}} + 1 \bmod q^m - 1$ has cardinality $\frac{m}{2} < m$ and hence there exist curves with q^{m+1} rational points in $\tilde{\mathcal{F}}$ and their number is, by Corollary 1.27, $q^{\frac{m}{2}}$. On the other hand the genus of any nontrivial curve in $\tilde{\mathcal{F}}$ is $g = \dfrac{q^{\frac{m}{2}}(q-1)}{2}$ by Proposition 1.21, and the Hasse-Weil bound on

the affine rational points is

$$q^m + 2gq^{\frac{m}{2}} = q^m + q^{\frac{m}{2}}(q-1)q^{\frac{m}{2}} = q^{m+1}.$$

□

We would like to remark that in Example 1.3 of [7], the author studies maximal curves similar to those in Corollary 1.29.

Observe that all the results we have had so far say whether an A-S family has a nontrivial member with q^{m+1} affine rational points or not. This is important information for the estimates on minimum distances of certain 2-D cyclic codes, as we will see in Chapter 3. We try to get some conclusions from our analysis so far to answer the same question for a single curve in the family.

Proposition 1.30. *Consider the curve X given by*

$$y^q - y = \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}$$

over $\mathbb{F}_{q^m}$, where λ_j's are nonzero. Suppose we have the following:

(a) The exponents $i_1, \ldots, i_s$ have distinct q-cyclotomic cosets mod $q^m - 1$,

(b) The q-cyclotomic cosets of the first $s-1$ exponents, mod $q^m - 1$, have cardinality $m = [\mathbb{F}_{q^m} : \mathbb{F}_q]$.

Then X doesn't have q^{m+1} affine $\mathbb{F}_{q^m}$-rational points.

Proof. Note that if the q-cyclotomic coset of i_s also has cardinality m, then the result trivially follows by Theorem 1.26(i). Therefore, let's suppose this is not the case and assume that the cardinality is δ . Consider the family obtained by letting the λ_j's take all possible values in $\mathbb{F}_{q^m}$:

$$\mathcal{F}_1 = \{y^q - y = \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s};\ \lambda_j \in \mathbb{F}_{q^m}\}.$$

By Theorem 1.26 and Corollary 1.27, we know that there are $q^{m-\delta}$ curves with q^{m+1} affine rational points in $\mathcal{F}_1$. Also consider the family

$$\mathcal{F}_2 = \{y^q - y = \lambda x^{i_s};\ \lambda \in \mathbb{F}_{q^m}\}.$$

This also has $q^{m-\delta}$ curves with q^{m+1} affine rational points. Observe that $\mathcal{F}_2 \subset \mathcal{F}_1$ and therefore if $\lambda_j \neq 0$ for some $j \in \{1, 2, \ldots, s-1\}$, which is the case for X, then such a curve doesn't have q^{m+1} affine rational points over $\mathbb{F}_{q^m}$. □

Remark 1.31. Since we arrive at our conclusions mainly from Theorem 1.26, which is about a family of curves, it is in general more difficult to say, using this idea, whether a given curve achieves the q^{m+1} points than to say it doesn't.

Example 1.32. The following table shows "good" families of A-S curves.

Table 3. "Good" Artin-Schreier Families

Family	q	g	# of pts. achieved
$\mathcal{F}_1 = \{y^2 + y = \lambda x^5\}$	16	2	33
$\mathcal{F}_2 = \{y^2 + y = \lambda x^9\}$	64	4	129
$\mathcal{F}_3 = \{y^3 - y = \lambda x^4\}$	9	3	28
$\mathcal{F}_4 = \{y^3 - y = \lambda x^{10}\}$	81	9	244
$\mathcal{F}_5 = \{y^4 + y = \lambda x^5\}$	16	6	65
$\mathcal{F}_6 = \{y^8 + y = \lambda x^9\}$	64	28	513
$\mathcal{F}_7 = \{y^9 - y = \lambda x^{10}\}$	81	36	730

For our considerations, a good family is one in which there is a nontrivial member with "a lot of " rational points. Having "a lot of" rational points on a curve will mean achieving the best known number of rational points for the given genus and the finite field. Observe that, naturally, Corollary 1.29 provides all of the families in Table 3. Also observe that all of the A-S families we are dealing with have one

point at infinity and we added this point to q^{m+1} in order to achieve the results above. One can use the tables in [10] for the latest improvements on this problem. Note that nontrivial curves in each of the families above are truly A-S curves and in particular, the ones in $\mathcal{F}_3$, $\mathcal{F}_5$, $\mathcal{F}_6$ and $\mathcal{F}_7$ are Hermitian curves.

We finish this section with some words on curves of the form $y^q - y = f(x)$, where $f(x)$ has a nonzero constant term. The following simple observation shows that whether such a curve has q^{m+1} points or not is also related to the same question about the types of curves we have looked at so far, i.e., curves with constant-free polynomials $f(x)$ on the right hand side.

Proposition 1.33. *Let X and Y be curves over $\mathbb{F}_{q^m}$ given, respectively, by the equations*

$$y^q - y = \lambda_0 + \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}$$

and

$$y^q - y = \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s},$$

where λ_i's are nonzero and $i_s < q^m - 1$. Then X has q^{m+1} affine $\mathbb{F}_{q^m}$-rational points if and only if $tr(\lambda_0) = 0$ and Y has q^{m+1} affine $\mathbb{F}_{q^m}$-rational points.

Proof. The curve Y has q^{m+1} points if and only if

$$\mathrm{tr}(\lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) = 0, \ \forall x \in \mathbb{F}_{q^m}.$$

If $\mathrm{tr}(\lambda_0)$ is also zero, then using the linearity of trace, we get

$$\mathrm{tr}(\lambda_0 + \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) = 0, \ \forall x \in \mathbb{F}_{q^m}.$$

This implies that X has q^{m+1} points.

Conversely, suppose X has q^{m+1} points. This means

$$\mathrm{tr}(\lambda_0 + \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) = 0, \ \forall x \in \mathbb{F}_{q^m}.$$

If $x = 0$, then we get $\mathrm{tr}(\lambda_0) = 0$. This gives us the following using the linearity of trace:

$$\begin{aligned}\mathrm{tr}(\lambda_0 + \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) &= \mathrm{tr}(\lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) \\ &= 0, \ \forall x \in \mathbb{F}_{q^m}.\end{aligned}$$

This means the curve Y has q^{m+1} affine points over $\mathbb{F}_{q^m}$. $\square$

There is another way to prove this simple result via a family of curves in the form X. It follows the same steps that we had in Theorem 1.26.

With the above proposition, we can state results about families where the members are allowed to have nonzero constants on the right hand side. For instance, combining Proposition 1.33 with Corollary 1.29, we can say that the family

$$\{y^q - y = \lambda_0 + \lambda_1 x^{q^{\frac{m}{2}}+1};\ \lambda_0, \lambda_1 \in \mathbb{F}_{q^m}\}$$

has $q^{m-1} \cdot q^{\frac{m}{2}}$ curves with q^{m+1} affine $\mathbb{F}_{q^m}$-rational points. Note that q^{m-1} is the number of elements in $\mathbb{F}_{q^m}$ with trace zero and $q^{\frac{m}{2}}$ is the number of curves in the family of Corollary 1.29 with q^{m+1} points.

Chapter 2. Two-Dimensional (2-D) Cyclic Codes

2.1 Definition of 2-D Cyclic Codes

We continue our discussion on coding theory with two-dimensional (2-D) cyclic codes. These are generalizations of cyclic codes, which we described in Section 1.1. For more information on the theory of 2-D cyclic codes, we refer to [13], [14], [15] and [24]. This chapter is an attempt to clearly summarize some of the results that we need from the theory of 2-D cyclic codes. As before, $\mathbb{F}_q$ denotes a characteristic $p > 0$ finite field with q elements.

Consider the set

$$\mathbb{F}_q^{n_1 \times n_2} = \left\{ \begin{pmatrix} a_{0,0}, a_{0,1}, \ldots, a_{0,n_2-1} \\ a_{1,0}, a_{1,1}, \ldots, a_{1,n_2-1} \\ \vdots \\ a_{n_1-1,0}, \ldots, a_{n_1-1,n_2-1} \end{pmatrix} ; \; a_{i,j} \in \mathbb{F}_q \right\},$$

where n_1 and n_2 are two positive integers. Note that $\mathbb{F}_q^{n_1 \times n_2}$ is an $n_1 n_2$-dimensional vector space over $\mathbb{F}_q$ whose elements are written in $n_1 \times n_2$ matrix notation.

A k-dimensional subspace C of $\mathbb{F}_q^{n_1 \times n_2}$ is called a 2-D linear code of area $n_1 \times n_2$ over $\mathbb{F}_q$, and denoted as an $(n_1 \times n_2, k)$ code. Note that the term area is used instead of the term length of Chapter 1.

Definition 2.1. For a 2-D linear code $C \subset \mathbb{F}_q^{n_1 \times n_2}$ if $(a_{i,j})$ is in C implies that $(a_{i+s,j+t})$ is also in C for all s and t, where $i+s$ and $j+t$ are taken mod n_1 and n_2, respectively, then C is called *a 2-D cyclic code of area* $n_1 \times n_2$.

In other words, a 2-D linear code is 2-D cyclic if it is closed under row and column shifts. Note that the dual of a 2-D cyclic code is also 2-D cyclic.

As in the case of cyclic codes, we have an alternative representation for 2-D cyclic codes as ideals in certain rings. For this, observe the following $\mathbb{F}_q$-vector space isomorphism between $\mathbb{F}_q^{n_1 \times n_2}$ and $\mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1)$:

$$\begin{array}{ccc} \mathbb{F}_q^{n_1 \times n_2} & \overset{1\text{-}1}{\longleftrightarrow} & \mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1) \\ (a_{i,j}) & \longleftrightarrow & \displaystyle\sum_{i=0}^{n_1-1}\sum_{j=0}^{n_2-1} a_{i,j}x^i y^j \end{array}$$

Under this identification, codewords of C get sent to polynomials in $\mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1)$ and in this way, we can think of a 2-D linear code C as a subset of $\mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1)$.

Proposition 2.2. *A 2-D linear code C in $\mathbb{F}_q^{n_1 \times n_2}$ is 2-D cyclic if and only if C is an ideal in $\mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1)$.*

Proof. Being closed under a row shift (resp., a column shift) in $\mathbb{F}_q^{n_1 \times n_2}$ is equivalent to being closed under multiplication by x (resp., by y) in $\mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1)$. □

In short, we have two ways to represent a 2-D cyclic code: The matrix representation and the polynomial representation. The context will make it clear which one is being considered.

2.2 Zeros of 2-D Cyclic Codes and Seidenberg's Lemma 92

We assume, from now on, that n_1 and n_2 are relatively prime to p, which is the characteristic of $\mathbb{F}_q$. In fact, for our results in Chapter 3, we will take both of these numbers to be $q^m - 1$ for some $m > 1$.

Let α_1 be a primitive n_1^{th} root of unity and α_2 be a primitive n_2^{th} root of unity. We take both of these elements in the smallest extension $\mathbb{F}_{q^s}$ of $\mathbb{F}_q$ such that n_1

and n_2 divide $q^s - 1$. Consider the following set.

$$\Omega = \{(\alpha_1^i, \alpha_2^j);\ 0 \leq i \leq n_1 - 1,\ 0 \leq j \leq n_2 - 1\}$$

Remark 2.3. Note that if a polynomial $f(x, y) \in \mathbb{F}_q[x, y]$ vanishes at (α_1^i, α_2^j) for some i and j, then f also vanishes at

$$(\alpha_1^{iq}, \alpha_2^{jq}), (\alpha_1^{iq^2}, \alpha_2^{jq^2}), \ldots, (\alpha_1^{iq^{m-1}}, \alpha_2^{jq^{m-1}}), \tag{2.1}$$

where m is the least common multiple of $[\mathbb{F}_q(\alpha_1^i) : \mathbb{F}_q]$ and $[\mathbb{F}_q(\alpha_2^j) : \mathbb{F}_q]$. These two numbers are the degrees of α_1^i and α_2^j over $\mathbb{F}_q$, respectively. The pairs in (2.1), obtained from (α_1^i, α_2^j), are called $\mathbb{F}_q$-conjugates of (α_1^i, α_2^j) and together with (α_1^i, α_2^j), they form what we call the $\mathbb{F}_q$-conjugacy class of (α_1^i, α_2^j) in Ω. Our notation will be $[(\alpha_1^i, \alpha_2^j)]$ for an $\mathbb{F}_q$-conjugacy class. It is clear that Ω is a disjoint union of such $\mathbb{F}_q$-conjugacy classes. From now on, we will use the letter U only for either a single class or a finite union of $\mathbb{F}_q$-conjugacy classes in Ω.

Definition 2.4. For $U \subset \Omega$, *the ideal corresponding to* U is defined as

$$I(U) = \{f(x, y) \in \mathbb{F}_q[x, y];\ f(a) = 0,\ \forall a \in U\}. \tag{2.2}$$

Note that $x^{n_1} - 1$ and $y^{n_2} - 1$ are in $I(U)$ for any $U \subset \Omega$. Therefore, $I(U)/(x^{n_1} - 1, y^{n_2} - 1) \subset \mathbb{F}_q[x, y]/(x^{n_1} - 1, y^{n_2} - 1)$ is a 2-D cyclic code, which we will denote as $\tilde{I}(U)$. In this way, we associate a 2-D cyclic code to a subset of Ω. We can also do the opposite.

Definition 2.5. Let $\tilde{J} = J/(x^{n_1} - 1, y^{n_2} - 1) \subset \mathbb{F}_q[x, y]/(x^{n_1} - 1, y^{n_2} - 1)$ be a 2-D cyclic code. Then

$$Z(\tilde{J}) = \{(\gamma, \beta) \in \mathbb{F}_{q^s}^2;\ f(\gamma, \beta) = 0,\ \forall f \in J\} \tag{2.3}$$

is called *the zero set of the 2-D cyclic code* $\tilde{J}$.

Remark 2.6. Note that since $x^{n_1} - 1$ and $y^{n_2} - 1$ are in J, the zero set $Z(\tilde{J})$ is a subset of Ω and, by (2.1), it is either a single $\mathbb{F}_q$-conjugacy class or a finite union of $\mathbb{F}_q$-conjugacy classes.

Example 2.7. Let $q = 2$, $n_1 = 3$, and $n_2 = 5$. If we fix a primitive element α in $\mathbb{F}_{16}$, which satisfies $\alpha^4 + \alpha + 1 = 0$, then we can take $\alpha_1 = \alpha^5$, which is a primitive cube root of unity, and $\alpha_2 = \alpha^3$, which is a primitive 5^{th} root of unity. Then Ω is

$$\Omega = \{(\alpha_1^i, \alpha_2^j);\ 0 \le i \le 2,\ 0 \le j \le 4\}.$$

Define C in the polynomial representation as the binary 2-D cyclic code $\tilde{I} = I/(x^3 - 1, y^5 - 1) \subset \mathbb{F}_2[x, y]/(x^3 - 1, y^5 - 1)$ of area 3×5, where I is given with the generator polynomials

$$f_1(x, y) = (x + 1)(y^4 + y^3 + y^2 + y + 1) \quad \text{and} \quad f_2(x, y) = (x^2 + x + 1)(y + 1).$$

Note that $f_1(x, y)$ is zero if and only if $x = 1$ or $y = \alpha_2^j$ for $j = 1, 2, 3, 4$. On the other hand, $f_2(x, y)$ is zero if and only if $x = \alpha_1^i$ for $i = 1, 2$ or $y = 1$. Hence, the zero set of C is

$$\begin{aligned} Z(C) &= \{(1,1), (\alpha_1, \alpha_2), (\alpha_1^2, \alpha_2^2), (\alpha_1, \alpha_2^4), \\ &\quad (\alpha_1^2, \alpha_2^3), (\alpha_1, \alpha_2^2), (\alpha_1^2, \alpha_2^4), (\alpha_1, \alpha_2^3), (\alpha_1^2, \alpha_2)\} \\ &= [(1,1)] \cup [(\alpha_1, \alpha_2)] \cup [(\alpha_1, \alpha_2^2)]. \end{aligned}$$

As noted in Remark 2.6, the zero set is a union of finitely many (three) $\mathbb{F}_2$-conjugacy classes.

Note that since a 2-D cyclic code is an ideal in $\mathbb{F}_q[x, y]/(x^{n_1} - 1, y^{n_2} - 1)$, one can define it by giving a (finite) set of generator polynomials. This is what we did in Example 2.7. We want to show that a 2-D cyclic code can also be described by means of its zero set. For this, we need some preliminary work.

Definition 2.8. Let $J \subset k[x_1, x_2, \ldots, x_n]$ be an ideal, where k is an arbitrary field. J is called a *zero-dimensional ideal* if the set

$$Z_{\bar{k}}(J) = \{(a_1, a_2, \ldots, a_n) \in \bar{k}^n;\ f(a_1, a_2, \ldots, a_n) = 0,\ \forall f \in J\}$$

is finite, where $\bar{k}$ denotes the algebraic closure of k.

Note that $Z_{\bar{k}}(J)$ is the analog of Definition 2.5 for arbitrary polynomial ideals. In fact, if $\tilde{J} = J/(x^{n_1} - 1, y^{n_2 - 1})$ is a 2-D cyclic code over $\mathbb{F}_q$, then its zero set, $Z(\tilde{J})$, is just $Z_{\bar{\mathbb{F}}_q}(J)$. Similarly, we can define the ideal corresponding to a subset Z of $\bar{k}^n$ as the set $I(Z)$ of polynomials in $k[x_1, x_2, \ldots, x_n]$ all of which vanish on Z. Then Hilbert's Nullstellensatz (see [1] or [3]) states that for an ideal $J \subset k[x_1, x_2, \ldots, x_n]$, one has

$$I(Z_{\bar{k}}(J)) = \sqrt{J},$$

where $\sqrt{J}$ is the radical of J. In general, not every ideal is equal to its radical, i.e., a radical ideal. However, for certain zero-dimensional ideals this is true.

Theorem 2.9. (Seidenberg's Lemma 92) *Let k be a perfect field and J be a zero-dimensional ideal in $k[x_1, x_2, \ldots, x_n]$. Then, J is radical if and only if it contains a univariate, square-free polynomial in each of the variables $x_1, x_2, \ldots, x_n$.*

Proof. See [27] or Proposition 8.14 in [3]. □

Assume for the rest of the chapter that Ω is a disjoint union of l $\mathbb{F}_q$-conjugacy classes, $S_1, S_2, \ldots, S_l$, where S_γ is defined as

$$S_\gamma = [(\alpha_1^{i_\gamma}, \alpha_2^{j_\gamma})], \quad \gamma = 1, 2, \ldots, l. \tag{2.4}$$

Lemma 2.10. $\tilde{I}(S_\gamma) = I(S_\gamma)/(x^{n_1} - 1, y^{n_2} - 1) \subset \mathbb{F}_q[x, y]/(x^{n_1} - 1, y^{n_2} - 1)$ *is a maximal ideal for every γ.*

Proof. Recall that α_1 and α_2 were chosen in $\mathbb{F}_{q^s}$, which is the smallest extension of $\mathbb{F}_q$ that contains primitive n_1^{th} and n_2^{th} roots of unity. Note that $I(S_\gamma) \subset \mathbb{F}_q[x, y]$

is the contraction of the maximal ideal $\mathcal{M} = \left(x - \alpha_1^{i_\gamma}, y - \alpha_2^{j_\gamma}\right) \subset \mathbb{F}_{q^s}[x,y]$, i.e., $\mathcal{M}^c = \mathcal{M} \cap \mathbb{F}_q[x,y] = I(S_\gamma)$. Consider the Galois group $G = \mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q)$, which is generated by the Frobenius automorphism $\phi : a \to a^q$. Note that ϕ can be thought as an automorphism of $\mathbb{F}_{q^s}[x,y]$ since it induces

$$\begin{aligned} \mathbb{F}_{q^s}[x,y] &\longrightarrow \mathbb{F}_{q^s}[x,y] \\ \sum_{i,j} a_{ij}x^i y^j &\mapsto \sum_{i,j} \phi(a_{ij})x^i y^j \end{aligned}$$

When G is viewed as a finite subgroup of the automorphism group of $\mathbb{F}_{q^s}[x,y]$, $\mathbb{F}_q[x,y]$ becomes the ring of G-invariants,

$$\text{i.e., } \mathbb{F}_q[x,y] = \{f \in \mathbb{F}_{q^s}[x,y];\ \phi(f) = f\}.$$

Then, by Exercise 12 on page 68 of [2], $\mathbb{F}_{q^s}[x,y]$ is an integral ring extension over $\mathbb{F}_q[x,y]$. It follows from Corollary 5.8 in [2], and the fact that $\mathcal{M}$ is maximal in $\mathbb{F}_{q^s}[x,y]$, that $I(S_\gamma)$ is maximal in $\mathbb{F}_q[x,y]$. Therefore, $\tilde{I}(S_\gamma)$ is maximal, too.□

Proposition 2.11. *Let U be a subset of Ω. Then*

$$U = Z(\tilde{I}(U)) = Z_{\bar{\mathbb{F}}_q}(I(U)).$$

Proof. Note that it is enough to prove this for a single $\mathbb{F}_q$-conjugacy class. This is because of the following two formulas:

$$\begin{aligned} I(S_1 \cup S_2) &= I(S_1) \cap I(S_2) \\ Z_{\bar{\mathbb{F}}_q}(I_1 \cap I_2) &= Z_{\bar{\mathbb{F}}_q}(I_1) \cup Z_{\bar{\mathbb{F}}_q}(I_2) \end{aligned}$$

So let $S = [(\alpha_1^{i_\gamma}, \alpha_2^{j_\gamma})] \subset \Omega$ be an $\mathbb{F}_q$-conjugacy class. We showed in the proof of Lemma 2.10 how to view $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ as a finite subgroup of the automorphisms of $\mathbb{F}_{q^s}[x,y]$, which yielded the fact that $\mathbb{F}_{q^s}[x,y]$ is integral over $\mathbb{F}_q[x,y]$. Combining this with Exercise 13 on page 68 of [2], we see that all the prime ideals in $\mathbb{F}_{q^s}[x,y]$

that contract to $I(S)$ are

$$(x-\alpha_1^i, y-\alpha_2^j), (x-\alpha_1^{iq}, y-\alpha_2^{jq}), \ldots, (x-\alpha_1^{iq^{\delta-1}}, y-\alpha_2^{jq^{\delta-1}}),$$

where $\delta = |S|$. Now we can prove our assertion for S.

The fact that $S \subset Z_{\bar{\mathbb{F}}_q}(I(S))$ is trivial. Note that $k = \mathbb{F}_q$ is a perfect field and since n_1 and n_2 are relatively prime to $p = char(\mathbb{F}_q)$, $I(S)$ contains square-free univariate polynomials $x^{n_1} - 1$ and $y^{n_2} - 1$ in the variables x and y. Because of the same reason, i.e., $I(S)$ having $x^{n_1} - 1$ and $y^{n_2} - 1$ in it, $I(S)$ is a zero-dimensional ideal. Therefore, by Seidenberg's Lemma 92, $I(S)$ is a radical ideal. Now we show the inclusion $Z_{\bar{\mathbb{F}}_q}(I(S)) \subset S$.

Suppose that there exists $P = (\alpha_1^{i'}, \alpha_2^{j'})$ in $Z_{\bar{\mathbb{F}}_q}(I(S))$ that is not in S. Then $I(P)$ contains $I(Z_{\bar{\mathbb{F}}_q}(I(S)))$, which is simply $I(S)$ since $I(S)$ is radical and Hilbert's Nullstellensatz states that $I(Z_{\bar{\mathbb{F}}_q}(I(S))) = \sqrt{I(S)}$. But $I(S)$ is maximal in $\mathbb{F}_q[x, y]$ (cf. Lemma 2.10). Since $I(P)$ is not the whole ring $\mathbb{F}_q[x, y]$, this implies that $I(P) = I(S)$. Then, using the fact that $I(P)$ is the contraction of $(x-\alpha_1^{i'}, y-\alpha_2^{j'}) \subset \mathbb{F}_{q^s}[x, y]$, we get $(x - \alpha_1^{i'}, y - \alpha_2^{j'})$ in the list of prime ideals that contract to $I(S)$, which is a contradiction. □

Another way to state Proposition 2.11 is that every subset U, in the sense of Remark 2.3, of Ω is the zero set of the 2-D cyclic code $\tilde{I}(U)$ that it defines. We are now ready to state the following characterization result for 2-D cyclic codes.

Proposition 2.12. *Let $\tilde{J} = J/(x^{n_1} - 1, y^{n_2} - 1) \subset \mathbb{F}_q[x, y]/(x^{n_1} - 1, y^{n_2} - 1)$ be a 2-D cyclic code. The zero set $Z(\tilde{J})$ uniquely determines $\tilde{J}$.*

Proof. We can easily show that J is a radical ideal following the argument in the proof of Proposition 2.11. Combining this with the Nullstellensatz, we have

$$I(Z(\tilde{J})) = I(Z_{\bar{\mathbb{F}}_q}(J)) = J. \tag{2.5}$$

Therefore, the ideal corresponding to the zero set $Z(\tilde{J})$ of $\tilde{J}$ is J and the corresponding 2-D cyclic code is $\tilde{J}$ itself. On the other hand if $Z' = Z(J')$ is another subset of Ω, which is the zero set of another 2-D cyclic code $\tilde{J'} = J'/(x^{n_1}-1, y^{n_2}-1)$ by Proposition 2.11, then the ideal corresponding to Z' is J' and the corresponding 2-D cyclic code is $\tilde{J'}$. Therefore $Z(\tilde{J})$ uniquely determines $\tilde{J}$. □

We finish this section with another useful result which will be used in the next section.

Proposition 2.13. *Let k be a perfect field and $I \subset k[x_1, x_2, \ldots, x_n]$ be a zero-dimensional radical ideal. Then*

$$|Z_{\bar{k}}(I)| = \dim_k\big(k[x_1, x_2, \ldots, x_n]/I\big).$$

Proof. See Theorem 8.32 in [3]. □

2.3 The Dimension and The Dual Code

Recall that in the case of cyclic codes, we were able to relate the dimension of a code to the number of zeros of its dual cyclic code (Remark 1.4(ii)). In this section, we show that the same relation also holds for a 2-D cyclic code and its dual. We start with a couple of preliminary observations, which are not only interesting but also useful in proving the relation between a 2-D cyclic code and its dual.

Proposition 2.14. $\tilde{I}(S_\gamma) = I(S_\gamma)/(x^{n_1}-1, y^{n_2}-1) \subset \mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1)$ *are all the maximal ideals in the ring* $\mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1)$.

Proof. Recall that the fact that $\tilde{I}(S_\gamma)$ is maximal was shown in Lemma 2.10. Now we prove there is no other maximal ideal.

If we temporarily denote the ring $\mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1)$ as R, the Chinese Remainder Theorem gives us

$$R\Big/\bigcap_{\gamma}\tilde{I}(S_\gamma) \cong \prod_{\gamma} R/\tilde{I}(S_\gamma), \tag{2.6}$$

which implies another isomorphism:

$$\mathbb{F}_q[x,y]\Big/\bigcap_{\gamma} I(S_\gamma) \cong \prod_{\gamma} \mathbb{F}_q[x,y]/I(S_\gamma). \tag{2.7}$$

By Proposition 2.13, the $\mathbb{F}_q$-dimension of each factor in the product in (2.7) is $|Z_{\mathbb{F}_q}(I(S_\gamma))| = |Z(\tilde{I}(S_\gamma))| = |S_\gamma|$. Hence the total dimension on the right hand side in (2.7) is $|\Omega| = n_1 n_2$, which is also the $\mathbb{F}_q$-dimension of the right hand side in (2.6). If there were another maximal ideal $\tilde{M} = M/(x^{n_1}-1, y^{n_2}-1)$ of $R = \mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1)$, then we would have had

$$R\Big/\Big(\bigcap_{\gamma}\tilde{I}(S_\gamma) \bigcap \tilde{M}\Big) \cong \prod_{\gamma} R/\tilde{I}(S_\gamma) \times R/\tilde{M}.$$

Arguing as above, we see that the $\mathbb{F}_q$-dimension on the right hand side of this new isomorphism would be $n_1 n_2 + \dim_{\mathbb{F}_q}(R/\tilde{M})$, which is strictly bigger than $n_1 n_2$ since $\tilde{M}$ is a maximal ideal and hence can't be equal to R, whereas the $\mathbb{F}_q$-dimension of the left hand side is less than or equal to $n_1 n_2 = \dim_{\mathbb{F}_q}(R)$. Therefore, the $\tilde{I}(S_\gamma)$'s are all the maximal ideals of $R = \mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1)$. □

Corollary 2.15.

$$\prod_{\gamma=1}^{l} I(S_\gamma) = 0 \quad mod \ \ (x^{n_1}-1, y^{n_2}-1).$$

Proof. By the isomorphism in (2.6) and dimension computations following (2.6) in the above proof, we have $\bigcap_\gamma \tilde{I}(S_\gamma) = 0$. This means $\bigcap_\gamma I(S_\gamma) = 0 \bmod (x^{n_1}-1, y^{n_2}-1)$. Since $I(S_\gamma)$ is maximal for each γ, intersection is the same as product. □

Remark 2.16. There is an alternative proof of Corollary 2.15. We will use R to denote $\mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1)$ again. Suppose that there is an infinite sequence, $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \ldots$, of descending ideals in R. If we look at the zero sets of all the ideals in the sequence, the first thing to note would be that one zero set is strictly contained in the next. Otherwise, by taking the corresponding ideals of these zero sets, and using the fact that ideals of R are radical by Theorem 2.9, we would show that two ideals in the sequence are the same. Hence we get an infinite sequence of ascending sets in Ω, which is itself a finite set. Therefore, R satisfies the descending chain condition on ideals and such rings are called Artin rings. On the other hand, R is isomorphic to the group algebra $\mathbb{F}_q[\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}]$, which is semisimple since $p = char(\mathbb{F}_q)$ doesn't divide $|\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}|$, the order of the group (cf. Theorem 5.3 in [16]). Combining this with the fact that R is Artinian implies that the radical of R is trivial. Here we use the Theorem on page 203 and Proposition 4.4 of [16]. But in an Artin ring prime ideals are maximal and hence the intersection of all the maximal ideals in R, i.e., $\tilde{I}(S_\gamma)$'s, is zero.

The following is the analogue of Remark 1.4 for 2-D cyclic codes.

Theorem 2.17. *Let U be a subset of Ω and let $\bar{U}$ denote $\Omega - U$. Consider the 2-D cyclic code $C_U = \tilde{I}(U) = I(U)/(x^{n_1}-1, y^{n_2}-1)$ corresponding to U. The dimension of C_U is given by*

$$\dim_{\mathbb{F}_q}(C_U) = |\bar{U}|.$$

Proof. We know that $I(U)$ is a zero-dimensional radical ideal in $\mathbb{F}_q[x,y]$. Then, by Proposition 2.13, we have

$$|Z_{\bar{\mathbb{F}}_q}(I(U))| = |Z(\tilde{I}(U))| = \dim_{\mathbb{F}_q}\big(\mathbb{F}_q[x,y]/I(U)\big).$$

On the other hand, we have the following standard isomorphism:

$$\mathbb{F}_q[x,y]/I(U) \cong \mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1) \Big/ I(U)/(x^{n_1}-1, y^{n_2}-1)$$

Therefore, the dimension of the code $\tilde{I}(U)$ is given by

$$\begin{aligned}
\dim(\tilde{I}(U)) &= \dim_{\mathbb{F}_q}\big(I(U)/(x^{n_1}-1, y^{n_2}-1)\big) \\
&= \dim_{\mathbb{F}_q}\big(\mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1)\big) - \dim_{\mathbb{F}_q}\big(\mathbb{F}_q[x,y]/I(U)\big) \\
&= n_1 n_2 - |Z_{\mathbb{F}_q}(I(U))| \\
&= n_1 n_2 - |U| \\
&= |\bar{U}|
\end{aligned}$$

□

Remark 2.18. This theorem also has an alternative, but longer, proof which can be found in [13].

In order to say that this theorem relates the dimension of a 2-D cyclic code to the number of zeros of its dual, we need to determine the zero set for the dual code. This is what we will do in the remaining part of this section.

Consider the following subsets of Ω:

$$U = \bigcup_{\gamma=1}^{r} S_\gamma \quad \text{and} \quad \bar{U} = \bigcup_{\gamma=r+1}^{l} S_\gamma,$$

where

$$S_\gamma = [(\alpha_1^{i_\gamma}, \alpha_2^{j_\gamma})], \quad \gamma = 1, 2, \ldots, l.$$

Let C_U be the 2-D cyclic code with the ideal representation $\tilde{I}(U) = I(U)/(x^{n_1} - 1, y^{n_2} - 1)$ and consider $C_{\bar{U}}$ with the ideal representation $\tilde{I}(\bar{U}) = I(\bar{U})/(x^{n_1} - 1, y^{n_2} - 1)$. The following shows that the product of the ideals $I(U)$ and $I(\bar{U})$ is

zero mod $(x^{n_1}-1, y^{n_2}-1)$.

$$\begin{aligned} I(U)\cdot I(\bar{U}) &= I(\bigcup_{\gamma=1}^{r} S_\gamma)\cdot I(\bigcup_{\gamma=r+1}^{l} S_\gamma) \\ &= \bigcap_{\gamma=1}^{r} I(S_\gamma)\cdot \bigcap_{\gamma=r+1}^{l} I(S_\gamma) \\ &= \prod_{\gamma=1}^{r} I(S_\gamma)\cdot \prod_{\gamma=r+1}^{l} I(S_\gamma) \\ &= \prod_{\gamma=1}^{l} I(S_\gamma) \\ &= 0 \qquad \text{mod } (x^{n_1}-1, y^{n_2}-1). \end{aligned}$$

Note that the last equality comes from Corollary 2.15. Hence for any $a(x,y) \in I(U)$ and $b(x,y) \in I(\bar{U})$, we have

$$a(x,y)b(x,y) = 0 \qquad mod\ (x^{n_1}-1, y^{n_2}-1). \tag{2.8}$$

Equation (2.8) implies that if we carry out the product mod $(x^{n_1}-1, y^{n_2}-1)$ and combine the same terms together, the coefficient of each term must be zero. In particular, the coefficient of the term $x^d y^e$ must be zero, where d (resp., e) is the x-degree (resp., y-degree) of $b(x,y)$. This coefficient is the following:

$$\begin{array}{ll} a_{0,0}b_{d,e} + a_{0,1}b_{d,e-1} + \cdots + a_{0,e}b_{d,0} & + \\ a_{1,0}b_{d-1,e} + a_{1,1}b_{d-1,e-1} + \cdots + a_{1,e}b_{d-1,0} & + \\ \vdots & \vdots \\ a_{d,0}b_{0,e} + a_{d,1}b_{0,e-1} + \cdots + a_{d,e}b_{0,0} & \end{array}$$

Note that we do not have a coefficient $a_{i,j}$ of $a(x,y)$ with $i > d$ or $j > e$ above since for a term in $a(x,y)$ with such a coefficient to contribute to the coefficient of $x^d y^e$ in the product, $b(x,y)$ would have to have a term with x-degree higher than d or y-degree higher than e.

Define the reciprocal polynomial of $b(x,y)$ as

$$\begin{aligned} b^*(x,y) &= x^d y^e b(x^{-1},y^{-1}) \\ &= b_{d,e} + b_{d,e-1}y + \cdots + b_{d,0}y^e + \\ &\quad b_{d-1,e}x + b_{d-1,e-1}xy + \cdots + b_{d-1,0}xy^e + \\ &\quad \vdots \\ &\quad b_{0,e}x^d + b_{0,e-1}x^d y + \cdots + b_{0,0}x^d y^e \end{aligned}$$

Note that the coefficient of the term $x^d y^e$ in the product $a(x,y)b(x,y) \bmod (x^{n_1}-1, y^{n_2}-1)$ is the inner product of the matrices corresponding to $a(x,y)$ and $b^*(x,y)$ and this is known to be zero, i.e., $(a_{i,j}) \cdot (b^*_{i,j}) = 0$. Therefore, the following set of polynomials is contained in the dual of $C_U = \tilde{I}(U)$.

$$J = \{b^*(x,y);\ b(x,y) \in I(\bar{U})\}$$

Lemma 2.19. *Let* $\bar{U}^{-1} = \{(\mu_1^{-1}, \mu_2^{-1});\ (\mu_1,\mu_2) \in \bar{U}\}$. *Then* $J = I(\bar{U}^{-1})$.

Proof. One inclusion is because if $b(x,y)$ vanishes on $\bar{U}$, then $b^*(x,y)$ vanishes on $\bar{U}^{-1}$. For the other inclusion, let $f(x,y)$ vanish on $\bar{U}^{-1}$. Then $f^*(x,y)$ vanishes on $\bar{U}$ and hence it is in $I(\bar{U})$. But then $(f^*)^*(x,y) = f(x,y)$ is in J. □

So, $J = I(\bar{U}^{-1})$ and the corresponding 2-D cyclic code $\tilde{J} = I(\bar{U}^{-1})/(x^{n_1}-1, y^{n_2}-1)$ is contained in the dual of C_U. However, the dimension of the dual is

$$n_1 n_2 - \dim(C_U) = n_1 n_2 - |\bar{U}| = |\Omega - \bar{U}| = |U| = |U^{-1}| = \dim(\tilde{J}).$$

Therefore, the dual of C_U is $\tilde{J}$. We state this in the following proposition.

Proposition 2.20. *For the 2-D cyclic code* $C_U = \tilde{I}(U) = I(U)/(x^{n_1}-1, y^{n_2}-1)$, *its dual code is the 2-D cyclic code* $C_{\bar{U}^{-1}} = \tilde{I}(\bar{U}^{-1}) = I(\bar{U}^{-1})/(x^{n_1}-1, y^{n_2}-1)$, *which has the zero set*

$$Z(C_U^{\perp}) = Z(C_{\bar{U}^{-1}}) = \bar{U}^{-1} = \Omega - U^{-1},$$

where

$$U^{-1} = \{(\mu_1^{-1}, \mu_2^{-1});\ (\mu_1, \mu_2) \in U\}.$$

Corollary 2.21. *The dimension of a 2-D cyclic code is equal to the number of zeros of its dual code.*

Proof. By Theorem 2.17, Proposition 2.20 and the fact that $|\bar{U}| = |\bar{U}^{-1}|$. □

We finish with two more definitions which are going to be used in the next chapter.

Definition 2.22. Let C_U be the 2-D cyclic code of area $n_1 \times n_2$ with the zero set $U \subset \Omega$. Then *the nonzero set of* C_U is

$$NZ(C_U) = \Omega - U = \bar{U}.$$

Definition 2.23. If the zero set of a 2-D cyclic code C is the union of the $\mathbb{F}_q$-conjugacy classes $S_\gamma = [(\alpha_1^{i_\gamma}, \alpha_2^{j_\gamma})]$, where γ is in some index set $\mathcal{I}$, then the set

$$\{(\alpha_1^{i_\gamma}, \alpha_2^{j_\gamma});\ \gamma \in \mathcal{I}\}$$

is called *a basic zero set of* C and denoted $BZ(C)$. Similarly, one can define *a basic nonzero set of* C and denote it by $BNZ(C)$.

Since the zero set of a 2-D cyclic code uniquely determines the code, so does the nonzero set, a basic zero set and a basic nonzero set. Note, however, that zero and nonzero sets are unique whereas there can be different choices of basic zero and basic nonzero sets. This can simply be achieved by choosing different representatives from the $\mathbb{F}_q$-conjugacy classes.

Remark 2.24. Let $(\alpha_1^{i_1}, \alpha_2^{j_1})$ and $(\alpha_1^{i_2}, \alpha_2^{j_2})$ be representatives of two distinct classes in a basic set (zero or nonzero) and suppose that $\alpha_2^{j_1}$ and $\alpha_2^{j_2}$ are $\mathbb{F}_q$-conjugate. Then, one can find another pair in the class of $(\alpha_1^{i_2}, \alpha_2^{j_2})$ whose second

coordinate is $\alpha_2^{j_1}$ and replace $(\alpha_1^{i_2}, \alpha_2^{j_2})$ in the basic set with this new pair. This means that we can choose a basic set for our codes in which any two members have second coordinates that are not $\mathbb{F}_q$-conjugate. Note that the second coordinates in the basic set can be equal among some of the members. Also observe that we can easily make the same choice with respect to the first coordinates of pairs in the basic set. In Chapter 3, we will always have this kind of choice on our basic sets and unless otherwise stated, the choice will be with respect to the second coordinates.

Example 2.25. Consider the code C from Example 2.7. We found that the zero set was

$$Z(C) = [(1,1)] \cup [(\alpha_1, \alpha_2)] \cup [(\alpha_1, \alpha_2^2)].$$

Therefore, one can write the following basic zero set for C:

$$BZ(C) = \{(1,1), (\alpha_1, \alpha_2), (\alpha_1, \alpha_2^2)\}.$$

Note that the second coordinates in the second and the third pairs are $\mathbb{F}_2$-conjugate. This can be avoided by choosing (α_1^2, α_2) to be the representative of the $\mathbb{F}_2$-conjugacy class containing (α_1, α_2^2). Then, the following would be our choice for a basic zero set:

$$\{(1,1), (\alpha_1, \alpha_2), (\alpha_1^2, \alpha_2)\}.$$

The dual of C has the zero set $\Omega - Z(C)^{-1}$ by Proposition 2.20. Since $Z(C)^{-1} = Z(C)$, this set is simply the nonzero set of C and it is the union of two $\mathbb{F}_2$-conjugacy classes:

$$Z(C^\perp) = [(1, \alpha_2)] \cup [(\alpha_1, 1)]$$

Obviously, the following could be a choice for the basic zero set of $C^\perp$, which is also a choice for a basic nonzero set for C by the above observation.

$$BZ(C^\perp) = BNZ(C) = \{(1, \alpha_2), (\alpha_1, 1)\}$$

In this example, it is easy to see that $g_1(x,y) = (x+1)(y+1)$ and $g_2(x,y) = (x^2+x+1)(y^4+y^3+y^2+y+1)$ are generating polynomials for the ideal corresponding to $C^{\perp}$ in the polynomial representation.

Chapter 3. Weights of 2-D Cyclic Codes via Family of Curves

3.1 Trace Representation of 2-D Cyclic Codes

We will give several representations for a 2-D cyclic code starting from the zero set of its dual. Note that this set is the same as the inverse set of the nonzero set of the code itself (cf. Proposition 2.20). Our codes will be "square" codes, i.e., codewords will be square matrices. This section will be the basis for our analysis in the later sections of this chapter.

Unless otherwise stated, we will have the following assumptions in this chapter: $q = p^l$ for some $l \geq 1$, where p is prime, and consider q^m with $m > 1$. Let α be a primitive element of $\mathbb{F}_{q^m}$. Consider the following sets

$$\Omega = \{(\alpha^i, \alpha^j);\ 0 \leq i, j \leq q^m - 2\} = \mathbb{F}_{q^m}^* \times \mathbb{F}_{q^m}^*, \tag{3.1}$$

$$U = [(\alpha^{i_1}, \alpha^{j_1})] \cup [(\alpha^{i_2}, \alpha^{j_2})] \cup \ldots \cup [(\alpha^{i_s}, \alpha^{j_s})], \tag{3.2}$$

where i_γ, j_γ are in the set $\{0, 1, \ldots, q^m - 2\}$. Note that we adopt the notation of Chapter 2 and hence, $[(\alpha^{i_\gamma}, \alpha^{j_\gamma})]$ is the $\mathbb{F}_q$-conjugacy class containing $(\alpha^{i_\gamma}, \alpha^{j_\gamma})$ for every γ.

By Proposition 2.12, we know that the zero set determines the 2-D cyclic code uniquely. We also noted in Chapter 2 that the same thing is true for the nonzero set, a basic zero set or a basic nonzero set. We define C to be the 2-D cyclic code of area $(q^m - 1) \times (q^m - 1)$ over $\mathbb{F}_q$ which has the following zero set:

$$Z(C) = \Omega - U^{-1} = \bar{U}^{-1} \tag{3.3}$$

If C' denotes the dual of C, then we have the following easy consequences from Proposition 2.20 and Definition 2.22:

$$\begin{aligned} NZ(C) &= \Omega - \bar{U}^{-1} = U^{-1} \\ Z(C') &= U \\ NZ(C') &= \Omega - U = \bar{U} \end{aligned} \tag{3.4}$$

We also have the polynomial representation for these two codes, as ideals in $\mathbb{F}_q[x,y]/(x^{q^m-1}-1, y^{q^m-1}-1)$, and the corresponding notations which were also introduced in Chapter 2.

$$C' = C_U = \tilde{I}(U) = I(U)/(x^{q^m-1}-1, y^{q^m-1}-1),$$

$$C = C_{\bar{U}^{-1}} = \tilde{I}(\bar{U}^{-1}) = I(\bar{U}^{-1})/(x^{q^m-1}-1, y^{q^m-1}-1).$$

For simplicity, we will denote C and C' as I and I', respectively, in the polynomial representation. Our analysis will be on the weights of C. The method we employ will be that of Section 1.4, which is based on Delsarte's Theorem and Hilbert's Theorem 90.

Let D' be the 2-D cyclic code of area $(q^m-1) \times (q^m-1)$ defined over $\mathbb{F}_{q^m}$ by the zero set

$$Z(D') = \{(\alpha^{i_1}, \alpha^{j_1}), (\alpha^{i_2}, \alpha^{j_2}), \ldots, (\alpha^{i_s}, \alpha^{j_s})\}. \tag{3.5}$$

It is worth noting that there is a unique basic zero set for D' and it is equal to the above zero set. This is because each pair in $Z(D')$ has a singleton $\mathbb{F}_{q^m}$-conjugacy class that consists only of that pair. Let D be the dual of D' and denote these codes as J and J', respectively, in the polynomial representation.

Lemma 3.1. *The restriction of D' to $\mathbb{F}_q$ is C'.*

Proof. We need to show that $J' \cap \mathbb{F}_q[x,y]/(x^{q^m-1}-1, y^{q^m-1}-1) = I'$ in the polynomial representation. If $f(x,y)$ is in the intersection, then it vanishes on $Z(D')$ of (3.5) and since it has coefficients in $\mathbb{F}_q$, it vanishes on $U = Z(C')$. Therefore, $f(x,y)$ is in I'. The opposite inclusion is also easy since polynomials in I' have coefficients in $\mathbb{F}_q$ and they vanish on $U \supset Z(D')$. □

Since D' restricts to C' over $\mathbb{F}_q$, we get the the following familiar diagram from Delsarte's Theorem:

$$\begin{array}{ccc} C' & \xleftarrow{\text{Res}} & D' \\ \updownarrow & & \updownarrow \\ C & \xleftarrow{\mathbf{tr}} & D \end{array} \tag{3.6}$$

Note that **tr** is defined by applying the trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ on each of the entries in the codewords (matrices) of D.

If $a(x,y)$ is an arbitrary codeword (in the polynomial representation) in J', then it vanishes on the elements of $Z(D')$. Hence we have

$$a(\alpha^{i_\gamma}, \alpha^{j_\gamma}) = \sum_{i,j=0}^{q^m-2} a_{i,j}(\alpha^{i_\gamma})^i(\alpha^{j_\gamma})^j = 0, \quad \forall \gamma = 1,2,\ldots,s;\ \forall a(x,y) \in J'. \tag{3.7}$$

When the s equations in (3.7) are translated to the matrix notation, we get

$$\begin{pmatrix} a_{0,0} & \cdots & a_{0,q^m-2} \\ a_{1,0} & \cdots & a_{1,q^m-2} \\ \vdots & \ddots & \vdots \\ a_{q^m-2,0} & \cdots & a_{q^m-2,q^m-2} \end{pmatrix} \cdot \begin{pmatrix} (\alpha^{i_\gamma})^0(\alpha^{j_\gamma})^0 & \cdots & (\alpha^{i_\gamma})^0(\alpha^{j_\gamma})^{q^m-2} \\ (\alpha^{i_\gamma})^1(\alpha^{j_\gamma})^0 & \cdots & (\alpha^{i_\gamma})^1(\alpha^{j_\gamma})^{q^m-2} \\ \vdots & \ddots & \vdots \\ (\alpha^{i_\gamma})^{q^m-2}(\alpha^{j_\gamma})^0 & \cdots & (\alpha^{i_\gamma})^{q^m-2}(\alpha^{j_\gamma})^{q^m-2} \end{pmatrix} = 0$$

for every $\gamma \in \{1,2,\ldots,s\}$ and for every $(a_{i,j})$ in D', which are the corresponding coefficient matrices (codewords) of polynomials in J'. Therefore, if we define v_γ for

every $\gamma = 1, 2, \ldots, s$ as the $(q^m - 1) \times (q^m - 1)$ matrix

$$v_\gamma = \begin{pmatrix} (\alpha^{i_\gamma})^0(\alpha^{j_\gamma})^0 & \ldots & (\alpha^{i_\gamma})^0(\alpha^{j_\gamma})^{q^m-2} \\ (\alpha^{i_\gamma})^1(\alpha^{j_\gamma})^0 & \ldots & (\alpha^{i_\gamma})^1(\alpha^{j_\gamma})^{q^m-2} \\ \vdots & \ddots & \vdots \\ (\alpha^{i_\gamma})^{q^m-2}(\alpha^{j_\gamma})^0 & \ldots & (\alpha^{i_\gamma})^{q^m-2}(\alpha^{j_\gamma})^{q^m-2} \end{pmatrix}, \tag{3.8}$$

then $\{v_1, v_2, \ldots, v_s\}$ is contained in D, which is the dual of D'. Observe that the $\mathbb{F}_{q^m}$-dimension of D is s, by Corollary 2.21 and (3.5).

Since α is a primitive element in $\mathbb{F}_{q^m}$, we can list all the elements of the multiplicative group $\mathbb{F}_{q^m}^*$, which will also be denoted by A, as follows:

$$A = \mathbb{F}_{q^m}^* = \{\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{q^m-2}\}. \tag{3.9}$$

Therefore, one can represent the first row of v_γ as $\left(x^{j_\gamma}\right)_{x \in A}$, the second row as $\left(\alpha^{i_\gamma} x^{j_\gamma}\right)_{x \in A}$, and do this for all the remaining rows of v_γ. For the meaning of the above notations of rows, we refer to (1.10) in Section 1.4. If we put the above representations of each row in v_γ together, we get the following representation for v_γ:

$$v_\gamma = \begin{pmatrix} x^{j_\gamma} \\ \alpha^{i_\gamma} x^{j_\gamma} \\ \vdots \\ (\alpha^{i_\gamma})^{q^m-2} x^{j_\gamma} \end{pmatrix}_{x \in A}, \qquad \gamma = 1, 2, \ldots, s \tag{3.10}$$

We will call this the horizontal representation. The following will be the short horizontal representation for these codewords:

$$v_\gamma = \left((\alpha^{i_\gamma})^\delta x^{j_\gamma}\right)_{x \in A, \delta \in \mathcal{I}}, \qquad \gamma = 1, 2, \ldots, s \tag{3.11}$$

where $\mathcal{I} = \{0, 1, \ldots, q^m - 2\}$. In other words, δ indexes the rows, i.e., $\delta = 0$ gives the first row, $\delta = 1$ gives the second row, and so on.

It is important to note that an analogue of the representations in (3.10) and (3.11) can also be obtained vertically. For this, we look at the columns of v_γ in (3.8). The first column is $\left(x^{i_\gamma}\right)_{x\in A}$, the second column is $\left(\alpha^{j_\gamma}x^{i_\gamma}\right)_{x\in A}$, etc. Hence, the vertical representation can be obtained by putting representations of columns together as

$$v_\gamma = \left(x^{i_\gamma} \quad , \quad \alpha^{j_\gamma}x^{i_\gamma} \quad , \quad \dots \quad , \quad (\alpha^{j_\gamma})^{q^m-2}x^{i_\gamma} \right)_{x\in A}, \qquad \gamma = 1, 2, \dots, s \quad (3.12)$$

and the short vertical representation is

$$v_\gamma = \left((\alpha^{j_\gamma})^\delta x^{i_\gamma}\right)_{x\in A, \delta\in\mathcal{I}}, \qquad \gamma = 1, 2, \dots, s \quad (3.13)$$

Note that δ indexes the columns of v_γ this time.

Proposition 3.2. *The set $\{v_1, v_2, \dots, v_s\}$ is an $\mathbb{F}_{q^m}$-basis for the code D.*

Proof. We saw that these matrices are codewords of D and the $\mathbb{F}_{q^m}$-dimension of D is s. So we need to show that this set is $\mathbb{F}_{q^m}$-linearly independent. Suppose there exists $\mu_1, \mu_2, \dots, \mu_s$ in $\mathbb{F}_{q^m}$ such that

$$\mu_1 v_1 + \mu_2 v_2 + \cdots + \mu_s v_s = \vec{0}. \quad (3.14)$$

Using the horizontal representations for each v_γ in (3.10), this means

$$\begin{pmatrix} \mu_1 x^{j_1} + \mu_2 x^{j_2} + \cdots + \mu_s x^{j_s} \\ \mu_1 \alpha^{i_1} x^{j_1} + \mu_2 \alpha^{i_2} x^{j_2} + \cdots + \mu_s \alpha^{i_s} x^{j_s} \\ \vdots \\ \mu_1 (\alpha^{i_1})^{q^m-2} x^{j_1} + \mu_2 (\alpha^{i_2})^{q^m-2} x^{j_2} + \cdots + \mu_s (\alpha^{i_s})^{q^m-2} x^{j_s} \end{pmatrix}_{x\in A} = \vec{0}. \quad (3.15)$$

Suppose that the j_γ's are all distinct. Then the first row in (3.15) gives

$$\mu_1 x^{j_1} + \mu_2 x^{j_2} + \cdots + \mu_s x^{j_s} = 0, \quad \forall x \in A = \mathbb{F}_{q^m}^*.$$

This polynomial expression has distinct exponents and its degree is $\max\{j_1, \ldots, j_s\}$. This degree is strictly less than $q^m - 1$, by (3.1). Therefore the polynomial can vanish on all of $\mathbb{F}_{q^m}^*$ if and only if it is zero, i.e., all the coefficients are zero. This would imply the linear independence of our set.

Now suppose some of the j_γ's are equal. Let's assume, without loss of generality, $j_1 = j_2 = \cdots = j_c$ for some $c \leq s$. There might be other groups of j_γ's that are equal to each other, but the following argument can easily be applied to handle them, too. Since the polynomial expressions in each row in (3.15) are of degree strictly less than $q^m - 1$, the only way they can vanish on $\mathbb{F}_{q^m}^*$ is if the coefficients of the terms are zero. We list the coefficients of the term of degree j_1 in each row:

$$\begin{aligned} \mu_1 + \mu_2 + \cdots + \mu_c &= 0 \\ \mu_1\alpha^{i_1} + \mu_2\alpha^{i_2} + \cdots + \mu_c\alpha^{i_c} &= 0 \\ &\vdots \\ \mu_1(\alpha^{i_1})^{q^m-2} + \mu_2(\alpha^{i_2})^{q^m-2} + \cdots + \mu_c(\alpha^{i_c})^{q^m-2} &= 0 \end{aligned} \tag{3.16}$$

Since α is primitive in $\mathbb{F}_{q^m}$, the equalities in (3.16) are equivalent to

$$\mu_1 x^{i_1} + \mu_2 x^{i_2} + \cdots + \mu_c x^{i_c} = 0, \ \forall x \in \mathbb{F}_{q^m}^*. \tag{3.17}$$

Note that the exponents in (3.17) are all distinct. Otherwise, we would have had $(\alpha^{i_\gamma}, \alpha^{j_\gamma}) = (\alpha^{i_{\gamma'}}, \alpha^{j_{\gamma'}})$ for some $\gamma \neq \gamma'$ with $\gamma, \gamma' \leq c$. This would contradict the fact that these two pairs are representatives of distinct $\mathbb{F}_q$-conjugacy classes in (3.2).

By the above observation on $i_1, \ldots, i_c$, (3.17) holds if and only if $\mu_1 = \cdots = \mu_c = 0$ again due to the degree of the polynomial expression we have. This finishes the proof. □

Theorem 3.3. *With the notations and definitions so far, we have the following representations for the code D over $\mathbb{F}_{q^m}$ and the code C over $\mathbb{F}_q$, where λ_γ runs*

through $\mathbb{F}_{q^m}$ *for every* $\gamma = 1, 2, \ldots, s$*:*

$$
\begin{aligned}
D &= \left\{ \sum_{\gamma=1}^{s} \lambda_\gamma v_\gamma \right\} \\
&= \left\{ \begin{pmatrix} \lambda_1 x^{j_1} + \cdots + \lambda_s x^{j_s} \\ \lambda_1 \alpha^{i_1} x^{j_1} + \cdots + \lambda_s \alpha^{i_s} x^{j_s} \\ \vdots \\ \lambda_1 (\alpha^{i_1})^{q^m-2} x^{j_1} + \cdots + \lambda_s (\alpha^{i_s})^{q^m-2} x^{j_s} \end{pmatrix}_{x \in A} \right\} \qquad (3.18) \\
&= \left\{ \left(\lambda_1 (\alpha^{i_1})^{\delta} x^{j_1} + \cdots + \lambda_s (\alpha^{i_s})^{\delta} x^{j_s} \right)_{x \in A, \delta \in \mathcal{I}} \right\} \\
&= \left\{ \left(\lambda_1 x^{i_1} + \cdots + \lambda_s x^{i_s} \ , \ \lambda_1 \alpha^{j_1} x^{i_1} + \cdots + \lambda_s \alpha^{j_s} x^{i_s} \ , \cdots \right)_{x \in A} \right\} \\
&= \left\{ \left(\lambda_1 (\alpha^{j_1})^{\delta} x^{i_1} + \lambda_2 (\alpha^{j_2})^{\delta} x^{i_2} + \cdots + \lambda_s (\alpha^{j_s})^{\delta} x^{i_s} \right)_{x \in A; \delta \in \mathcal{I}} \right\}
\end{aligned}
$$

$$
\begin{aligned}
C &= \left\{ \sum_{\gamma=1}^{s} \mathbf{tr}(\lambda_\gamma v_\gamma) \right\} \\
&= \left\{ \begin{pmatrix} \mathrm{tr}\left(\lambda_1 x^{j_1} + \cdots + \lambda_s x^{j_s}\right) \\ \mathrm{tr}\left(\lambda_1 \alpha^{i_1} x^{j_1} + \cdots + \lambda_s \alpha^{i_s} x^{j_s}\right) \\ \vdots \\ \mathrm{tr}\left(\lambda_1 (\alpha^{i_1})^{q^m-2} x^{j_1} + \cdots + \lambda_s (\alpha^{i_s})^{q^m-2} x^{j_s}\right) \end{pmatrix}_{x \in A} \right\} \qquad (3.19) \\
&= \left\{ \left(\mathrm{tr}\left(\lambda_1 (\alpha^{i_1})^{\delta} x^{j_1} + \cdots + \lambda_s (\alpha^{i_s})^{\delta} x^{j_s}\right) \right)_{x \in A, \delta \in \mathcal{I}} \right\} \\
&= \left\{ \left(\mathrm{tr}\left(\lambda_1 x^{i_1} + \cdots + \lambda_s x^{i_s}\right) \ , \ \mathrm{tr}\left(\lambda_1 \alpha^{j_1} x^{i_1} + \cdots + \lambda_s \alpha^{j_s} x^{i_s}\right) \ , \cdots \right)_{x \in A} \right\} \\
&= \left\{ \left(\mathrm{tr}\left(\lambda_1 (\alpha^{j_1})^{\delta} x^{i_1} + \lambda_2 (\alpha^{j_2})^{\delta} x^{i_2} + \cdots + \lambda_s (\alpha^{j_s})^{\delta} x^{i_s}\right) \right)_{x \in A, \delta \in \mathcal{I}} \right\}
\end{aligned}
$$

Proof. This is a direct consequence of Proposition 3.2 combined with the fact that $C = \mathbf{tr}(D)$ and the notations introduced in (3.10), (3.11), (3.12) and (3.13). □

Note that the order of representations, after the first one, in (3.18) and (3.19) is horizontal, short horizontal, vertical and short vertical. Recall that our goal is to

investigate weights of C. We finish this section by stating the first remark on the weights of two different codes. This is an easy observation provided by two different ways of looking at codewords: horizontally and vertically. We will continue more detailed discussion of weights in the following sections.

Corollary 3.4. *Consider the code C of area $(q^m-1)\times(q^m-1)$ over $\mathbb{F}_q$ whose dual has as a basic zero set*

$$BZ(C^\perp)=\{(\alpha^{i_1},\alpha^{j_1}),(\alpha^{i_2},\alpha^{j_2}),\dots,(\alpha^{i_s},\alpha^{j_s})\}.$$

Let $\tilde{C}$ be the code of same area over $\mathbb{F}_q$ for which the dual has as a basic zero set

$$BZ(\tilde{C}^\perp)=\{(\alpha^{j_1},\alpha^{i_1}),(\alpha^{j_2},\alpha^{i_2}),\dots,(\alpha^{j_s},\alpha^{i_s})\}.$$

Then the weight enumerators of C and $\tilde{C}$ are the same.

Proof. Consider the horizontal representation of the codeword c in C determined by the s-tuple $(\mu_1,\mu_2,\dots,\mu_s)$ in $\mathbb{F}_{q^m}^s$ and the vertical representation of the codeword $\tilde{c}$ in $\tilde{C}$ which is also determined by the same s-tuple. Rows in c are identical to columns in $\tilde{c}$ and hence these codewords have the same weight. □

Remark 3.5. By this observation, we need to keep the following in mind for the rest of the chapter: Any statement made on the weights of a certain 2-D cyclic code C remains true for another 2-D cyclic code $\tilde{C}$ whose defining set is obtained from C's by switching x and y coordinates.

3.2 General Lower Bound on the Minimum Distance

Note that we didn't need any assumption on the set U of (3.2) in order to get the representations for the codes C and D in Theorem 3.3. In this section, with convenient assumptions on U, we will state a lower bound for the minimum distance

of C. Recall that one assumption we always make is that of Remark 2.23, which is easy to achieve as we observed in that remark.

Consider the code C in the horizontal representation in (3.19). If $c \in C$ is a nonzero codeword corresponding to the s-tuple $(\mu_1, \mu_2, \ldots, \mu_s) \in \mathbb{F}_{q^m}^s$, then the weight of any of its rows is given by Hilbert's Theorem 90, as was the case in Section 1.4, and it is

$$q^m - 1 - \frac{1}{q}\left(\#_{\mathbb{F}_{q^m}}(y^q - y = f(x)) - q\right) = q^m - \frac{\#_{\mathbb{F}_{q^m}}(y^q - y = f(x))}{q}, \qquad (3.20)$$

where $f(x)$ is what is in the trace function corresponding to this row. In particular, for the $(r+1)^{st}$ row for any $r \in \{0, 1, \ldots, q^m - 2\}$, we have

$$f(x) = \mu_1(\alpha^{i_1})^r x^{j_1} + \cdots + \mu_s(\alpha^{i_s})^r x^{j_s}.$$

In other words, the weight of a codeword in C is determined by the number of affine $\mathbb{F}_{q^m}$-rational points on $q^m - 1$ curves in the form $y^q - y = f(x)$, where $f(x)$ is determined by the particular row. Therefore, the whole weight enumerator of C is related to the following family from Section 1.4:

$$\mathcal{F} = \{y^q - y = \lambda_1 x^{j_1} + \lambda_2 x^{j_2} + \cdots + \lambda_s x^{j_s};\ \lambda_j \in \mathbb{F}_{q^m}\}.$$

Proposition 3.6. *Let C be the 2-D cyclic code of area $(q^m - 1) \times (q^m - 1)$ over $\mathbb{F}_q$ whose dual has as a basic zero set*

$$BZ(C^\perp) = \{(\alpha^{i_1}, \alpha^{j_1}), (\alpha^{i_2}, \alpha^{j_2}), \ldots, (\alpha^{i_s}, \alpha^{j_s})\}.$$

Assume that the q-cycloctomic coset mod $q^m - 1$ of each j_γ has cardinality $m = [\mathbb{F}_{q^m} : \mathbb{F}_q]$. Then we have

(i) The mapping **tr** *of the diagram (3.6) is an $\mathbb{F}_q$-vector space isomorphism.*

(ii) Let v be a codeword in C and $v' \in D$ be the unique codeword with $\mathbf{tr}(v') = v$. Then, a row in v is identically zero if and only if the same row in v' is identically zero.

Proof. (i) The fact that **tr** is surjective is known from Delsarte's Theorem. $\mathbb{F}_q$-linearity of the ordinary trace map implies the $\mathbb{F}_q$-linearity of the mapping **tr**. The cardinality of the $\mathbb{F}_q$-conjugacy class for each element in $BZ(C^{\perp})$ is m by the assumption made in the statement. Therefore, by Corollary 2.21, the $\mathbb{F}_q$-dimension of C is sm. The $\mathbb{F}_{q^m}$-dimension of D is s and hence over $\mathbb{F}_q$, it is sm dimensional, too. Therefore, **tr** is injective. Combined with the above observations, this shows that **tr** is an $\mathbb{F}_q$-vector space isomorphism between the codes D and C of the diagram (3.6).

(ii) Recall that the weight of a row in v is given by the formula (3.20). Since the q-cyclotomic coset mod $q^m - 1$ containing each j_γ has cardinality m and we choose j_γ's to be not $\mathbb{F}_q$-conjugate (cf. Remark 2.24), we can use Theorem 1.26. Note that since some of the j_γ's may be the same, we can't conclude that the curve in the formula (3.20) has q^{m+1} rational points if and only if every $\lambda_\gamma = 0$. However, we can say that there are q^{m+1} affine $\mathbb{F}_{q^m}$-rational points on $y^q - y = f(x)$ if and only if $f(x) \equiv 0$ on $\mathbb{F}_{q^m}$, which is enough for our statement to be true. □

The hypothesis of Proposition 3.6 gives us a bit of control on the behavior of the **tr** map. Namely, a nonzero row in $v' \in D$ will not be mapped to a zero row under **tr**. In order to say something effective about the minimum distance of C, we need to know the maximum possible number of zero rows in a codeword of C, which is equivalent to the same question about D. However, a quick look at the representations of Theorem 3.3 makes it clear that answering this question in the generality of Proposition 3.6 is fairly difficult due to the complexity of the system of equations one has to deal with. One additional assumption will avoid any of these zero row considerations and provide us a minimum distance bound. This is what we do in the next theorem.

Theorem 3.7. *Let C be the 2-D cyclic code of area $(q^m-1)\times(q^m-1)$ over $\mathbb{F}_q$ whose dual has as a basic zero set*

$$BZ(C^{\perp})=\{(\alpha^{i_1},\alpha^{j_1}),(\alpha^{i_2},\alpha^{j_2}),\ldots,(\alpha^{i_s},\alpha^{j_s})\}.$$

Assume that the j_γ's are distinct and the q-cyclotomic coset mod q^m-1 containing each j_γ has cardinality $m=[\mathbb{F}_{q^m}:\mathbb{F}_q]$. Then

(i) $\dim_{\mathbb{F}_q}(C)=sm$.

(ii) If d denotes the minimum distance of C, we have

$$d\geq(q^m-1)\left(q^m-\frac{N}{q}\right),$$

where N is in the set $\{q,2q,\ldots,(q^m-1)q\}$ and it is the tightest upper bound that applies to the number of affine $\mathbb{F}_{q^m}$-rational points of all the curves in the family $\mathcal{F}=\{y^q-y=\lambda_1x^{j_1}+\lambda_2x^{j_2}+\cdots+\lambda_sx^{j_s};\ \lambda_\gamma\in\mathbb{F}_{q^m}\}$.

Proof. (i) The $\mathbb{F}_q$-conjugacy class of each $(\alpha^{i_\gamma},\alpha^{j_\gamma})$ has cardinality m by the assumption on j_γ's. The result follows from Corollary 2.21.

(ii) We adopt the notation of Proposition 3.6. Note that the hypotheses of this proposition are satisfied. Hence, if $v\in C$ is a nonzero codeword, then it is the image under $\mathbf{tr}$ of a unique codeword v' in D, where both codewords are determined by a nontrivial s-tuple $(\lambda_1,\ldots,\lambda_s)$. Furthermore, a row in v is identically zero if and only if the same row in v' is identically zero. The rows of v' are in the form

$$\left(\lambda_1(\alpha^{i_1})^\delta x^{j_1}+\cdots+\lambda_s(\alpha^{i_s})^\delta x^{j_s}\right)_{x\in\mathbb{F}_{q^m}^*},\ \delta=0,1,\ldots,q^m-2.$$

Since the j_γ's are all distinct, the polynomial expression of degree $j_s<q^m-1$ (see (3.1)) can be identically zero on $\mathbb{F}_{q^m}^*$ if and only if every $\lambda_\gamma=0$. Therefore, a nontrivial codeword in D, and hence in C, will not have an identically zero row under our hypothesis.

We know that the number of $\mathbb{F}_{q^m}$-rational points on any member of $\mathcal{F}$ is divisible by q and can't be q^{m+1} by our hypothesis (cf. Theorem 1.26). What we want to understand is the lowest possible weight in a row of v. This is equivalent to asking what is the maximum number of affine $\mathbb{F}_{q^m}$-rational points that a nontrivial member of the family $\mathcal{F} = \{y^q - y = \lambda_1 x^{j_1} + \lambda_2 x^{j_2} + \cdots + \lambda_s x^{j_s};\ \lambda_j \in \mathbb{F}_{q^m}\}$ can have. Let N be this number, which has to be a member of the set $\{q, 2q, \ldots, (q^m - 1)q\}$ by the above explanation. Then, the minimal possible weight in a row of v is, by (3.20), $q^m - \frac{N}{q}$. Repeating this minimal weight in each row gives the lowest possible weight that can occur in C. □

There are couple of things that need to be addressed about this theorem. The main difficulty is the determination of the number N if the family we are dealing with is as general as it is in Theorem 3.7. If we attempt to use the Hasse-Weil-Serre (H-W-S) bound in place of N, then we need to be careful since the genus varies among the members of the family. To guarantee that the bound applies to all the curves in $\mathcal{F}$, we should compute the H-W-S bound that corresponds to the highest genus in $\mathcal{F}$. However, the genus computation for the members and the determination of the highest genus in the family might also be troublesome (see the end of Section 1.3 for possible difficulties). The following corollary is an example of a case when we are able to overcome these difficulties.

Corollary 3.8. *Let C be the 2-D cyclic code of area $(q^m - 1) \times (q^m - 1)$ over $\mathbb{F}_q$ whose dual has as a basic zero set*

$$BZ(C^{\perp}) = \{(\alpha^{i_1}, \alpha^{j_1}), (\alpha^{i_2}, \alpha^{j_2}), \ldots, (\alpha^{i_s}, \alpha^{j_s})\}.$$

Assume that the q-cyclotomic coset containing each j_γ has cardinality $m = [\mathbb{F}_{q^m} : \mathbb{F}_q]$. For every $\gamma = 1, 2, \ldots, s$, write j_γ as $j_\gamma = r_\gamma p^{\eta_\gamma}$, where p doesn't divide r_γ. Suppose the r_γ's are all distinct and let $r = \max\{r_1, r_2, \ldots, r_s\}$. Then

(i) $\dim_{\mathbb{F}_q}(C) = sm$.

(ii) If d *denotes the minimum distance of* C*, we have*

$$d \geq (q^m - 1)\left(q^m - \frac{N}{q}\right),$$

where N *is the maximum of the set* $\{q, 2q, \ldots, (q^m - 1)q\}$ *that is less than or equal to*

$$q^m + \frac{(q-1)(r-1)}{2}[2\sqrt{q^m}].$$

Proof. (i) As in Theorem 3.7.

(ii) Note that we require the r_γ's to be distinct, which guarantees that the j_γ's will be distinct. Therefore, everything follows as it did in Theorem 3.7 and we only need to show that the number N is what we assert it is. Note that our family is $\mathcal{F} = \{y^q - y = \sum_\gamma \lambda_\gamma x^{r_\gamma p^{n_\gamma}};\ \lambda_\gamma \in \mathbb{F}_{q^m}\}$. By Proposition 1.22, we know that the curves we are dealing with in this case are all Artin-Schreier and the biggest genus is $\frac{(q-1)(r-1)}{2}$. Therefore, the corresponding H-W-S bound is indeed a universal bound on the family of curves, i.e., it bounds the number of rational points of every curve in the family. □

Note that two things might cause this bound to be ineffective. First of all, the N we find by the universal H-W-S bound may not be a good estimate for the largest number of $\mathbb{F}_{q^m}$-rational points in the family. For instance, if the universal H-W-S bound is greater than or equal to q^{m+1}, then N will be $(q^m - 1)q$ and hence the minimal weight we find for each row will be $q^m - \frac{N}{q} = q^m - (q^m - 1) = 1$. Therefore, we would conclude $d \geq q^m - 1$, which is the number of rows. This is already known since the assumptions we made guarantee that a nonzero codeword in C doesn't have a zero row. Therefore, to get more meaningful estimates for d we should look at examples where the universal H-W-S bound is as small as possible compared to q^{m+1}. Secondly, we repeat the same highest number N (or the smallest weight

$q^m - \frac{N}{q}$) in each row whereas this is not necessarily the case in reality. This is caused by our inability to use the relations among the coefficients of rows in the representations given in Theorem 3.3. Therefore, the bound has a chance to be reasonable for small genus and small finite field $\mathbb{F}_{q^m}$.

In most of the remaining examples, we find the actual minimum distance using Macaulay2 ([12]). In fact, a short routine we wrote in the program (see the Appendix) can compute the weight enumerator for small extensions $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ and small number of basic zeros in the set $BZ(C^\perp)$.

Example 3.9. Consider $\mathbb{F}_9$ over $\mathbb{F}_3$ and let α be a primitive element in $\mathbb{F}_9$ which satisfies $\alpha^2 + \alpha - 1 = 0$. Let C be the 2-D cyclic code over $\mathbb{F}_3$ of area 8×8 whose dual has as a basic zero set

$$BZ(C^\perp) = \{(\alpha, \alpha), (\alpha, \alpha^2)\}.$$

Note that the cardinality of $Z(C^\perp)$ is 4 and hence C has dimension 4 over $\mathbb{F}_3$. The number N is a multiple of 3 that is less than $3 \cdot 9 = 27$ and $r = 2$. The universal H-W-S bound is $9 + [2\sqrt{9}] = 15$. Hence $N = 15$. Therefore our estimate for the minimum distance of C is $d \geq 8 \cdot 4 = 32$. The actual minimum distance is 42. For this example, we don't need Macaulay2 to obtain the actual minimum distance. We will compute the complete weight enumerator in Example 3.14.

Example 3.10. Consider $\mathbb{F}_8$ over $\mathbb{F}_2$ and let α be a primitive element in $\mathbb{F}_8$ which satisfies $\alpha^3 + \alpha + 1 = 0$. Let C be the 2-D cyclic code over $\mathbb{F}_2$ of area 7×7 whose dual has as a basic zero set

$$BZ(C^\perp) = \{(\alpha, \alpha), (\alpha^3, \alpha^5)\}.$$

The cardinality of $Z(C^\perp)$ is 6 and therefore C has dimension 6 over $\mathbb{F}_2$. N is a multiple of 2 that is less than $2 \cdot 8 = 16$ and $r = 5$. The universal H-W-S bound is

$8 + 2[2\sqrt{8}] = 18$. Therefore, $N = 14$ and our estimate for the minimum distance of C is $d \geq 7 \cdot 1 = 7$. Observe that this is just the number of rows and what is happening here is exactly what we mentioned in the paragraph that follows Corollary 3.8 and the cause for this poor estimate is the fact that the universal H-W-S bound is too big. However, we can do a little bit better if we just choose a different second representative in $BZ(C^{\perp})$. Namely, replace (α^3, α^5) with (α^6, α^3) and observe that all the hypothesis of Corollary 3.8 are still satisfied. Then $r = 3$ and the universal H-W-S bound is $8 + [2\sqrt{8}] = 13$. Since N has to be a multiple of 2, $N = 12$. Then our estimate becomes $d \geq 7 \cdot 2 = 14$. The actual minimum distance of C is 24.

As seen in these two examples, even with very small codes our estimate is not very effective. However, as the following example will show, if the basic set is nice and we know more about the family of curves in the problem, we can do better.

Example 3.11. Consider $\mathbb{F}_8$ over $\mathbb{F}_2$ and let α be a primitive element in $\mathbb{F}_8$ which satisfies $\alpha^3 + \alpha + 1 = 0$. Let C be the 2-D cyclic code over $\mathbb{F}_2$ of area 7×7 whose dual has as a basic zero set

$$BZ(C^{\perp}) = \{(\alpha, \alpha), (\alpha^3, \alpha^3)\}.$$

The cardinality of $Z(C^{\perp})$ is 6 and therefore C has dimension 6 over $\mathbb{F}_2$. N is a multiple of 2 that is less than $2 \cdot 8 = 16$ and $r = 3$. The universal H-W-S bound is $8 + [2\sqrt{8}] = 13$ and hence $N = 12$. Our estimate on the minimum distance is $d \geq 7 \cdot 2 = 14$. Note that for an arbitrary codeword in D, where D is defined as in Section 3.1, we have the following representation (cf. Theorem 3.3):

$$\left(\lambda_1(\alpha)^{\delta} x + \lambda_2(\alpha^3)^{\delta} x^3\right)_{x \in \mathbb{F}_8^*, \delta = 0, 1, \cdots, 6}, \quad \lambda_1, \lambda_2 \in \mathbb{F}_8.$$

Let v' be the codeword in D which is obtained by the coefficients $(\mu_1, \mu_2) \neq (0,0)$ in $(\mathbb{F}_8)^2$. For every δ, i.e., for every row, if we replace $\alpha^\delta x$ by x_δ, it changes the order of elements in the corresponding row but certainly doesn't change the set of elements of $\mathbb{F}_8$ that appears in that row. After this modification, we get the matrix

$$M = \left(\mu_1 x_\delta + \mu_2 x_\delta^3\right)_{x_\delta \in \mathbb{F}_8^*, \delta = 0,1,\cdots,6}.$$

If $v = \mathbf{tr}(v')$ is the codeword obtained from $v' \in D$, then its weight is the same as the weight of $\mathbf{tr}(M)$, by the above observation. The curves corresponding to the rows of $\mathbf{tr}(M)$ are the same and given by the equation $Y^2 + Y = \mu_1 X + \mu_2 X^3$. Using Table 1 and Proposition 1.16 of Chapter 1, we see that there is a choice of (μ_1, μ_2) for which $N = 12$ affine $\mathbb{F}_8$-rational points is achieved. Therefore, for such a choice of (μ_1, μ_2) we get a codeword in C of weight 14. Since we already showed $d \geq 14$ by our general bound, $d = 14$.

Remark 3.12. Two things make it possible to find the exact minimum distance in Example 3.11. The first is the knowledge that N of Corollary 3.8 is exactly the maximum rational points that appear in the corresponding family of curves. The second is the convenience of the basic set which guarantees the existence of a codeword for which the same lowest possible weight is repeated in every row. Therefore, we can get the minimum distance of similar binary 2-D cyclic codes where α is a primitive element of the extension $\mathbb{F}_{2^n}$ that is dealt with in the problem. The importance of the basic set is justified if we look at the binary code of same area whose dual has as a basic zero set $\{(\alpha, \alpha), (\alpha, \alpha^3)\}$, instead. Note that the family of curves we deal with is the same and we will have a good bound, $N = 12$, for the family again. Our estimate is $d \geq 14$ but the actual minimum distance of this code is 24.

3.3 Special Classes of 2-D Cyclic Codes

Our goal in this section is to investigate special classes of codes which are not covered by Theorem 3.7. In order to stay out of the scope of Theorem 3.7, we will allow some (or all) of the second coordinates of pairs in the basic set to be the same. Therefore we will no longer have the comfort of knowing that a nonzero codeword can't have an identically zero row.

We start with codes with two basic nonzeros. This will be followed by considerations of certain cases of three and four basic nonzeros.

Theorem 3.13. *Let C be the code over $\mathbb{F}_q$ of area $(q^m-1)\times(q^m-1)$ whose dual has as a basic zero set*

$$BZ(C^{\perp}) = \{(\alpha^{i_1}, \alpha), (\alpha^{i_2}, \alpha)\}.$$

Then we have

(i) $\dim(C) = 2m$.

(ii) If θ denotes the order of $\alpha^{i_2-i_1}$ in the multiplicative group $\mathbb{F}_{q^m}^*$, then the weights and their frequencies for C are given in the following table:

Table 4. Weights of C

weight	*frequency*
$(q^m-1-\frac{q^m-1}{\theta})(q^m-q^{m-1})$	$\theta\cdot(q^m-1)$
$(q^m-1)(q^m-q^{m-1})$	$q^{2m}-\theta\cdot(q^m-1)-1$

Proof. (i) α is primitive in $\mathbb{F}_{q^m}$ and hence its degree over $\mathbb{F}_q$ is m. Therefore, the cardinality of the $\mathbb{F}_q$-conjugacy classes for both pairs in $BZ(C^{\perp})$ is m.

(ii) We know that $C = \mathbf{tr}(D)$ and $\mathbf{tr}$ is injective (cf. Proposition 3.6). Therefore, for a nonzero codeword v in C, there exists a unique codeword v' in D such that $v = \mathbf{tr}(v')$ and a row in v is zero if and only if the same row in v' is zero, again by

Proposition 3.6. In fact, by Theorem 3.3, we have the following short horizontal representations for these codewords:

$$v' = \Big(\big(\lambda_1(\alpha^{i_1})^\delta + \lambda_2(\alpha^{i_2})^\delta\big)x \Big)_{x\in A, \delta\in\mathcal{I}}$$

$$v = \Big(\mathrm{tr}\big[\big(\lambda_1(\alpha^{i_1})^\delta + \lambda_2(\alpha^{i_2})^\delta\big)x\big] \Big)_{x\in A, \delta\in\mathcal{I}},$$

where λ_1, λ_2 are in $\mathbb{F}_{q^m}$. Note that the weight of a row in v is

$$q^m - \frac{\#_{\mathbb{F}_{q^m}}(y^q - y = (\ )x)}{q},$$

where the empty parenthesis in the formula is the coefficient determined by the row number. Since the curve in the formula is a rational curve, provided that the coefficient mentioned above is nonzero, it has q^m affine $\mathbb{F}_{q^m}$-rational points and hence when a row of v is nonzero, it has weight $q^m - q^{m-1}$. However, there may be zero rows in v and these are the same as the zero rows of v'. Observe that v' can also be written as

$$v' = \Big(\big(\lambda_1 + \lambda_2(\alpha^{i_2-i_1})^\delta\big)(\alpha^{i_1})^\delta x \Big)_{x\in A, \delta\in\mathcal{I}}$$

and a row is zero if and only if $\lambda_1 + \lambda_2(\alpha^{i_2-i_1})^\delta = 0$.

If $\lambda_1 = 0$ and $\lambda_2 \neq 0$, then no row in the corresponding codeword $v' \in D$ is zero. Therefore, $q^m - 1$ codewords in C obtained with such coefficients will have rational curves corresponding to each row, meaning that their weight will be $(q^m - 1)(q^m - q^{m-1})$. The same thing happens when $\lambda_2 = 0$ and $\lambda_1 \neq 0$.

Now assume that both coefficients are nonzero. Let θ be the order of $\alpha^{i_2-i_1}$ in $\mathbb{F}_{q^m}^*$. For any nonzero $\lambda_2 \in \mathbb{F}_{q^m}$, there exists a unique nonzero $\lambda_1 \in \mathbb{F}_{q^m}$ such that $\lambda_1 + \lambda_2(\alpha^{i_2-i_1})^\delta = 0$ for one and only one δ in the set $\{0, 1, \ldots, \theta - 1\}$. This means that for each $\lambda_2 \in \mathbb{F}_{q^m}^*$, there exists θ choices of $\lambda_1 \in \mathbb{F}_{q^m}^*$ satisfying the equality for some $\delta \in \{0, 1, \ldots, \theta - 1\}$ (i.e., $\theta \cdot (q^m - 1)$ pairs $(\lambda_1, \lambda_2) \in (\mathbb{F}_{q^m}^*)^2$).

Note that this unique zero row is repeated with period θ and hence all of these codewords will have total of $\frac{q^m-1}{\theta}$ zero rows. That means the corresponding codewords in C will have the same number of zero rows and hence their weight will be $(q^m-1-\frac{q^m-1}{\theta})(q^m-q^{m-1})$. All the remaining $(q^m-1)^2-\theta\cdot(q^m-1)$ choices of (λ_1,λ_2) in this case lead to words with no zero rows and hence codewords with weight $(q^m-1)(q^m-q^{m-1})$ in C. $\square$

Example 3.14. Refer back to the code C of Example 3.9. The weight enumerator of C is the same as that of the 2-D cyclic code $\tilde{C}$, whose dual has as a basic zero set $BZ(\tilde{C}^{\perp})=\{(\alpha,\alpha),(\alpha^2,\alpha)\}$ (cf. Corollary 3.4). The order of $\alpha^{2-1}=\alpha$ in $\mathbb{F}_9^*$ is 8 and hence the nonzero weights of $\tilde{C}$ are $7\cdot 6=42$ and $8\cdot 6=48$ with frequencies 64 and 16, respectively. Hence, the minimum distance of C in Example 3.9 is indeed 42.

Remark 3.15. Theorem 3.13 produces two-weight codes over any field $\mathbb{F}_q$. These types of codes are interesting for Graph Theorists and Finite Geometers due to their connection with the so-called strongly regular graphs and certain sets in projective spaces (see [4]). We must note that one needs two-weight codes to be projective in order to establish the connection with these subjects. A projective code over $\mathbb{F}_q$ is a code for which the columns of the generator matrix are mutually $\mathbb{F}_q$-linearly independent. This is equivalent to saying that the dual code has minimum distance at least equal to three.

Example 3.16. Let C_1 be the 2-D cyclic code over $\mathbb{F}_2$ of area 7×7 whose dual has $\{(\alpha,\alpha),(\alpha^2,\alpha)\}$ as a basic zero set, where α is a primitive element of $\mathbb{F}_8$. Let C_2 be the 2-D cyclic code over $\mathbb{F}_2$ of area 15×15 whose dual has $\{(\beta,\beta),(\beta^2,\beta)\}$ as a basic zero set, where β is a primitive element of $\mathbb{F}_{16}$. Both of these codes are projective by the MacWilliams Identity.

Observe that what made it possible to obtain the weight enumerator in Theorem 3.13 was the second coordinates in the dual's basic zero set, which produced rational curves in our argument. We now give a minimum distance bound on other codes with two basic nonzeros.

Proposition 3.17. *Let C be the code over $\mathbb{F}_q$ of area $(q^m-1)\times(q^m-1)$ whose dual has as a basic zero set*

$$BZ(C^{\perp}) = \{(\alpha^{i_1}, \alpha^j), (\alpha^{i_2}, \alpha^j)\}.$$

Let $1 \neq j = rp^\eta$, where p doesn't divide r and assume that the q-cyclotomic coset containing j mod q^m-1 has cardinality m. Then

$$d \geq (q^m - 1 - \frac{q^m-1}{\theta})(q^m - \frac{N}{q}),$$

where d is the minimum distance of C, N is the maximum of the set $\{q, 2q, \ldots, (q^m-1)q\}$ which is less than or equal to

$$q^m + \frac{(q-1)(r-1)}{2}[2\sqrt{q^m}],$$

and θ is the order of $\alpha^{i_2-i_1}$ in the multiplicative group $\mathbb{F}_{q^m}^*$.

Proof. Note that both C over $\mathbb{F}_q$ and D over $\mathbb{F}_{q^m}$ have dimension $2m$ over $\mathbb{F}_q$, where the meanings of D is as in Section 3.1. If $v' \in D$ is the nonzero codeword obtained from $\lambda_1, \lambda_2 \in \mathbb{F}_{q^m}$ and $v = \mathbf{tr}(v') \in C$, then they are of the form

$$v' = \left((\lambda_1(\alpha^{i_1})^\delta + \lambda_2(\alpha^{i_2})^\delta)x^j\right)_{x\in A, \delta\in\mathcal{I}}$$

$$v = \left(\mathrm{tr}\left[(\lambda_1(\alpha^{i_1})^\delta + \lambda_2(\alpha^{i_2})^\delta)x^j\right]\right)_{x\in A, \delta\in\mathcal{I}}.$$

By Proposition 3.6, a row in v is zero if and only if the same row in v' is zero. The maximum number of zero rows in a codeword of D is $\frac{q^m-1}{\theta}$, following a similar argument to that we had in the proof of Theorem 3.13. For the remaining nonzero

rows, we choose the lowest possible weight. This means, the highest number of $\mathbb{F}_{q^m}$-rational points among the nontrivial members of the family $\mathcal{F} = \{y^q - y = \lambda x^j;\ \lambda \in \mathbb{F}_{q^m}\}$. By Theorem 1.26, $\mathcal{F}$ doesn't have a nontrivial curve with q^{m+1} points. The universal H-W-S bound for this family is

$$q^m + \frac{(q-1)(r-1)}{2}[2\sqrt{q^m}].$$

This is because every nontrivial curve in $\mathcal{F}$ is Artin-Schreier with the genus $g = \frac{(q-1)(r-1)}{2}$. Hence the result follows. □

Example 3.18. Consider $\mathbb{F}_{16}$ over $\mathbb{F}_2$ and let α be a primitive element in $\mathbb{F}_{16}$ which satisfies $\alpha^4 + \alpha + 1 = 0$. Let C be the 2-D cyclic code over $\mathbb{F}_2$ of area 15×15 whose dual has as a basic zero set

$$BZ(C^\perp) = \{(\alpha, \alpha^3), (\alpha^6, \alpha^3)\}.$$

Note that the cardinality of $Z(C^\perp)$ is 8 and hence C has dimension 8 over $\mathbb{F}_2$. The number N is a multiple of 2 that is less than $2 \cdot 16 = 32$ and $r = 3$. The universal H-W-S bound is $16 + [2\sqrt{16}] = 24$. Hence $N = 24$. On the other hand, the order of $\alpha^{6-1} = \alpha^5$ in $\mathbb{F}_{16}^*$ is 3. Therefore our estimate for the minimum distance of C is $d \geq (15 - 5) \cdot 4 = 40$. The actual minimum distance is 60.

This doesn't look like a good estimate but compared to examples of Section 3.2, it isn't terribly bad considering the size of the code C to the sizes of the examples in Section 3.2. In the next example our estimate is as good as it can be.

Example 3.19. Consider $\mathbb{F}_9$ over $\mathbb{F}_3$ and let α be a primitive element in $\mathbb{F}_9$ which satisfies $\alpha^2 + \alpha - 1 = 0$. Let C be the 2-D cyclic code over $\mathbb{F}_3$ of area 8×8 whose dual has as a basic zero set

$$BZ(C^\perp) = \{(\alpha, \alpha^2), (\alpha^5, \alpha^2)\}.$$

Note that the cardinality of $Z(C^{\perp})$ is 4 and hence C has dimension 4 over $\mathbb{F}_3$. The number N is a multiple of 3 that is less than $3 \cdot 9 = 27$ and $r = 2$. The universal H-W-S bound is $9 + [2\sqrt{9}] = 15$. Hence $N = 15$. The order of $\alpha^{5-1} = \alpha^4$ in $\mathbb{F}_9^*$ is 2. Therefore our estimate for the minimum distance of C is $d \geq (8-4) \cdot 4 = 16$. This is the actual minimum distance of C.

We now move on to codes with three basic nonzeros. Our choice of a nonzero set will be explained after the following proposition.

Proposition 3.20. *Let C be the code over $\mathbb{F}_q$ of area $(q^m-1) \times (q^m-1)$ whose dual has as a basic zero set*

$$BZ(C^{\perp}) = \{(\alpha^{i_1}, \alpha^{j_1}), (\alpha^{i_2}, \alpha^{j_2}), (\alpha^{i_3}, \alpha^{j_2})\}.$$

Let $j_\gamma = r_\gamma p^{n_\gamma}$ $(\gamma = 1, 2)$, where p doesn't divide r_γ and suppose that the q-cyclotomic coset containing j_γ mod $q^m - 1$ has cardinality m. Let $r = max\{r_1, r_2\}$. If r_1 and r_2 are distinct, then

$$d \geq (q^m - 1 - \frac{q^m - 1}{\theta})(q^m - \frac{N}{q}),$$

where d is the minimum distance of C, N is the maximum of the set $\{q, 2q, \ldots, (q^m - 1)q\}$ which is less than or equal to

$$q^m + \frac{(q-1)(r-1)}{2}[2\sqrt{q^m}],$$

and θ is the order of $\alpha^{i_3 - i_2}$ in the multiplicative group $\mathbb{F}_{q^m}^*$.

Proof. Both D, which is as in Section 3.1, and C have dimension $3m$ over $\mathbb{F}_q$. A nonzero codeword v in C is of the form

$$v = \left(\mathrm{tr}\left[\lambda_1(\alpha^{i_1})^\delta x^{j_1} + (\lambda_2(\alpha^{i_2})^\delta + \lambda_3(\alpha^{i_3})^\delta)x^{j_2}\right]\right)_{x \in A, \delta \in \mathcal{I}},$$

and it is the image under **tr** of a unique codeword in D, which is

$$v' = \left(\lambda_1(\alpha^{i_1})^\delta x^{j_1} + \left(\lambda_2(\alpha^{i_2})^\delta + \lambda_3(\alpha^{i_3})^\delta\right)x^{j_2}\right)_{x\in A,\delta\in\mathcal{I}},$$

where $\lambda_1, \lambda_2, \lambda_3$ are in $\mathbb{F}_{q^m}$. We get a zero row in v if and only if the same row in v' is zero. So, we look at the maximum possible number of zero rows in a nonzero codeword of D. If we choose λ_i's as

$$\lambda_1 = 0 \quad \text{and} \quad \lambda_2 = -\lambda_3(\alpha^{i_3-i_2})^\delta,$$

for some δ in $\{0, 1, \ldots, \theta-1\}$, then the row corresponding to this δ value will be zero and there will be $\dfrac{q^m-1}{\theta}$ total zero rows. It can be shown, as it was done in the proof of Theorem 3.13, that two distinct δ values in $\{0, 1, \ldots, \theta-1\}$ can't yield two zero rows. Therefore, the maximum number of zero rows in a codeword of D, and hence in a codeword of C, is $\dfrac{q^m-1}{\theta}$. The fact that the H-W-S bound is a universal bound follows by the assumption that r_1 and r_2 are distinct. Therefore, repeating the minimum possible weight in the remaining nonzero rows finishes the proof. □

Remark 3.21. Note that if we assume all of the second coordinates in the basic set are equal, then we run into difficulty of determining how many times the set of equations of the form

$$\lambda_1(\alpha^{i_1})^\delta + \lambda_2(\alpha^{i_2})^\delta + \lambda_3(\alpha^{i_3})^\delta = 0, \quad \delta = 0, 1, \ldots, q^m-2$$

are satisfied for $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{F}_{q^m}^3$.

Example 3.22. Consider $\mathbb{F}_8$ over $\mathbb{F}_2$ and let α be a primitive element in $\mathbb{F}_8$ which satisfies $\alpha^3 + \alpha + 1 = 0$. Let C be the 2-D cyclic code over $\mathbb{F}_2$ of area 7×7 whose dual has as a basic zero set

$$BZ(C^\perp) = \{(\alpha, \alpha), (\alpha, \alpha^3), (\alpha^3, \alpha^3)\}.$$

Note that the cardinality of $Z(C^{\perp})$ is 9 and hence C has dimension 9 over $\mathbb{F}_2$. The number N is a multiple of 2 that is less than $2 \cdot 8 = 16$ and $r = 3$. The universal H-W-S bound is $8 + [2\sqrt{8}] = 13$. Hence $N = 12$. The order of $\alpha^{3-1} = \alpha^2$ in $\mathbb{F}_8^*$ is 7. Therefore our estimate for the minimum distance of C is $d \geq (7-1) \cdot 2 = 12$. The actual minimum distance of C is 14.

Finally, we look at codes with four basic nonzeros. Due to reasons similar to those of Remark 3.21, we restrict our attention to the case below. Since the proof is very similar to the ones we have given so far, we omit it and just give examples.

Proposition 3.23. *Let C be the code over $\mathbb{F}_q$ of area $(q^m - 1) \times (q^m - 1)$ whose dual has as a basic zero set*

$$BZ(C^{\perp}) = \{(\alpha^{i_1}, \alpha^{j_1}), (\alpha^{i_2}, \alpha^{j_1}), (\alpha^{i_3}, \alpha^{j_2}), (\alpha^{i_4}, \alpha^{j_2})\}.$$

Let $j_\gamma = r_\gamma p^{\eta_\gamma}$ $(\gamma = 1, 2)$, where p doesn't divide r_γ and suppose that the q-cyclotomic coset containing j_γ mod $q^m - 1$ has cardinality m. Let $r = max\{r_1, r_2\}$, θ be the order of $\alpha^{i_2 - i_1}$ in $\mathbb{F}_{q^m}^*$, and assume this is the same as the order of $\alpha^{i_4 - i_3}$. If r_1 and r_2 are distinct, then

$$d \geq (q^m - 1 - \frac{q^m - 1}{\theta})(q^m - \frac{N}{q}),$$

where d is the minimum distance of C, N is the maximum of the set $\{q, 2q, \ldots, (q^m - 1)q\}$ which is less than or equal to

$$q^m + \frac{(q-1)(r-1)}{2}[2\sqrt{q^m}].$$

Example 3.24. Consider $\mathbb{F}_9$ over $\mathbb{F}_3$ and let α be a primitive element in $\mathbb{F}_9$ which satisfies $\alpha^2 + \alpha - 1 = 0$. Let C be the 2-D cyclic code over $\mathbb{F}_3$ of area 8×8 whose dual has as a basic zero set

$$BZ(C^{\perp}) = \{(\alpha, \alpha), (\alpha^2, \alpha), (\alpha, \alpha^2), (\alpha^2, \alpha^2)\}.$$

Note that the cardinality of $Z(C^{\perp})$ is 8 and hence C has dimension 8 over $\mathbb{F}_3$. The number N is a multiple of 3 that is less than $3 \cdot 9 = 27$ and $r = 2$. The universal H-W-S bound is $9 + [2\sqrt{9}] = 15$. Hence $N = 15$. The order of $\alpha^{2-1} = \alpha$ in $\mathbb{F}_9^*$ is 8. Therefore our estimate for the minimum distance of C is $d \geq (8-1) \cdot 4 = 28$. The actual minimum distance of C is 32.

Example 3.25. Consider $\mathbb{F}_{16}$ over $\mathbb{F}_2$ and let α be a primitive element in $\mathbb{F}_{16}$ which satisfies $\alpha^4 + \alpha + 1 = 0$. Let C be the 2-D cyclic code over $\mathbb{F}_2$ of area 15×15 whose dual has as a basic zero set

$$BZ(C^{\perp}) = \{(\alpha, \alpha), (\alpha^3, \alpha), (\alpha, \alpha^3), (\alpha^3, \alpha^3)\}.$$

Note that the cardinality of $Z(C^{\perp})$ is 12 and hence C has dimension 12 over $\mathbb{F}_2$. The number N is a multiple of 2 that is less than $2 \cdot 16 = 32$ and $r = 3$. The universal H-W-S bound is $16 + [2\sqrt{16}] = 24$. Hence $N = 24$. The order of $\alpha^{3-1} = \alpha^2$ in $\mathbb{F}_{16}^*$ is 15. Therefore our estimate for the minimum distance of C is $d \geq (15-1) \cdot 4 = 56$.

We now show how one can say more about the minimum distance of this code using an argument similar to that of Example 3.11. Namely, the codewords in C are of the form

$$\Big(\mathrm{tr}\big[(\lambda_1(\alpha)^{\delta} + \lambda_2(\alpha^3)^{\delta})x + (\lambda_3(\alpha)^{\delta} + \lambda_4(\alpha^3)^{\delta})x^3\big]\Big)_{x \in \mathbb{F}_{16}^*, \delta = 0,1,\ldots,14} \quad \lambda_\gamma \in \mathbb{F}_{16}.$$

Consider the codeword $v \in C$ which is obtained by choosing $\lambda_2 = \lambda_3 = 0$ and $(\lambda_1, \lambda_4) \neq (0,0)$. Following the steps in Example 3.11, we can show that such a codeword has the lowest possible weight of $16 - 12 = 4$ repeated in all 15 rows. This shows the existence of a codeword of weight 60 in C and hence gives us $56 \leq d \leq 60$. On the other hand, by Table 1 of Chapter 1, all possible weights for the rows of a codeword in C are even and hence we conclude $d = 56, 58$ or 60. The actual minimum distance is 60.

Once again, this shows the possible improvements we can make on the general bounds of our results when we look at specific examples.

Example 3.26. Consider $\mathbb{F}_8$ over $\mathbb{F}_2$ and let α be a primitive element in $\mathbb{F}_8$ which satisfies $\alpha^3 + \alpha + 1 = 0$. Let C be the 2-D cyclic code over $\mathbb{F}_2$ of area 7×7 whose dual has as a basic zero set

$$BZ(C^{\perp}) = \{(\alpha, \alpha), (\alpha^3, \alpha), (\alpha, \alpha^3), (\alpha^3, \alpha^3)\}.$$

Note that the cardinality of $Z(C^{\perp})$ is 12 and hence C has dimension 12 over $\mathbb{F}_2$. The number N is a multiple of 2 that is less than $2 \cdot 8 = 16$ and $r = 3$. The universal H-W-S bound is $8 + [2\sqrt{8}] = 13$ and hence $N = 12$. The order of $\alpha^{3-1} = \alpha^2$ in $\mathbb{F}_8^*$ is 7. Therefore our estimate on the minimum distance of C is $d \geq (7-1) \cdot 2 = 12$. Using the argument in Example 3.25, we can prove the existence of a codeword of weight 14 and we can show that the weights of codewords are even. Therefore, we end up with $d = 12$ or 14. The actual minimum distance is 14.

Remark 3.27. Jensen gave a lower bound for the minimum distance of multi-dimensional cyclic codes based on decomposing such a code as the direct sum of concatenated codes (see [17] for details). Using the algorithm of Sabin ([23]), one can show that the code C of Example 3.26 decomposes as $A_1 \square B \bigoplus A_2 \square B$, where A_1 is the binary $[7, 3, 4]$ cyclic code with the generator polynomial $x^4 + x^2 + x + 1$, A_2 is the binary $[7, 3, 4]$ cyclic code with the generator polynomial $x^4 + x^3 + x^2 + 1$, and B is the cyclic code over $\mathbb{F}_8$ with zeros $1, \alpha, \alpha^2, \alpha^3, \alpha^5$, where α is a primitive element of $\mathbb{F}_8$. The minimum distance of B is 6 and the Jensen bound here gives that the minimum distance of C is at least 12, which is the same lower bound as we found in Example 3.26.

References

[1] Adams W. and Loustaunau, P., *An Introduction to Grobner Bases*, AMS, 1994.

[2] Atiyah, M. F. and Macdonald, I. G., *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[3] Becker, T. and Weispfenning, V., *Grobner Bases*, Springer-Verlag, 1993.

[4] Calderbank, R. and Kantor, W. M., *The Geometry of Two-Weight Codes*, Bull. London Math. Soc. **18** (1986), 97-122.

[5] Delsarte, P., *On Subfield Subcodes of Reed-Solomon Codes*, IEEE Trans. Inform. Theory **21** (1975), 575–576.

[6] Fulton, W., *Algebraic Curves: An Introduction to Algebraic Geometry*, Addison-Wesley, 1989.

[7] Garcia, A., *On Goppa Codes and Artin-Schreier Extensions*, Comm. Algebra **20** (1992), 3683–3689.

[8] Garcia, A. and Stichtenoth, H., *Elementary Abelian p-Extensions of Algebraic Function Fields*, Manuscripta Math. **72** (1991), 67–79.

[9] van der Geer, G. and van der Vlugt, M., *Reed-Muller Codes and Supersingular Curves. I*, Compositio Math. **84** (1992), 333–367.

[10] van der Geer, G. and van der Vlugt, M., *Tables of Curves With Many Points*, available at http://www.science.uva.nl/∼ geer, (July 2000).

[11] Goppa, V.D., *Codes on Algebraic Curves*, Soviet Math. Dokl. **24** No.1 (1981), 170–172.

[12] Grayson, D. R. and Stillman, M. E., *Macaulay 2, a software for research in algebraic geometry*, available at http://www.math.uiuc.edu/Macaulay2.

[13] Ikai, T., Kosako, H. and Kojima, Y., *Two-Dimensional Cyclic Codes*, Electronics and Communications in Japan (4) **57-A** (1975), 27– 35.

[14] Ikai, T., Kosako, H. and Kojima, Y., *Basic Theory of Two-Dimensional Cyclic Codes: Periods of Ideals and Fundamental Theorems*, Electronics and Communications in Japan (3) **59-A** (1976), 31–38.

[15] Imai, H., *A Theory of Two-Dimensional Cyclic Codes*, Information and Control **34** (1977), 1–21.

[16] Jacobson, N., *Basic Algebra II*, Freeman, 1989.

[17] Jensen, J. M., *The Concatenated Structure of Cyclic and Abelian Codes*, IEEE Trans. Inform. Theory **31** (1985), 788–793.

[18] Lang, S., *Algebra*, Addison-Wesley, 1965.

[19] Lidl, R. and Niederreiter, H., *Introduction to Finite Fields and Their Applications*, Cambridge University Press, 2000.

[20] van Lint, J. H., *Introduction to Coding Theory*, Springer-Verlag, 1999.

[21] MacWilliams, F. J., *A Theorem on the Distribution of Weights in a Systematic Code*, Bell Syst. Tech. J. **42** (1963), 79–94.

[22] Pless, V., *Introduction to the Theory of Error-Correcting Codes*, Wiley-Interscience, 1998.

[23] Sabin, R. E., *On Minimum Distance Bounds for Abelian Codes*, Appl. Algebra Engrg. Comm. Comput. **3** (1992), 183–197.

[24] Saints, K., *Algebraic Methods for The Encoding and Decoding Problems for Multidimensional Cyclic Codes and Algebraic-Geometric Codes*, PhD Thesis Cornell University (1995).

[25] Schoof, R., *Families of Curves and Weight Distribution of Codes*, Bulletin of Amer. Math. Soc. (2) **32** (1995), 171–183.

[26] Schoof, R., *Nonsingular Plane Cubic Curves over Finite Fields*, J. Combin. Theory Ser. A **46** (1987), 183–211.

[27] Seidenberg, A., *Constructions in Algebra*, Trans. Amer. Math. Soc. **197** (1974), 272–313.

[28] Silverman, J. H., *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[29] Stichtenoth, H., *Algebraic Function Fields and Codes*, Springer-Verlag, 1993.

[30] Tate, J. T., *The Arithmetic of Elliptic Curves*, Invent. Math. **23** (1974), 179–206.

[31] Tate, J. T., *Endomorphisms of Abelian Varieties over Finite Fields*, Invent. Math. **2** (1966), 134–144.

[32] Waterhouse, W. C., *Abelian Varieties over Finite Fields*, Ann. Sci. École Norm. Sup. **2** (1969), 521–560.

[33] Wolfmann, J., *The Number of Points of Certain Algebraic Curves over Finite Fields*, Comm. Algebra **17** (1989), 2055-2060.

Appendix. Macaulay2 Routine

We present our Macaulay2 routine which can be used for weight computations of 2-D cyclic codes in Proposition 3.23. Obvious modifications can be done to apply it in other cases. We would like to note that the following code takes $q = p$ for some prime p and it computes the weights of the codewords corresponding to $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) \in (\mathbb{F}_{p^m})^4$, where none of the λ_γ's is zero. Note that $f(t)$ is a primitive polynomial of degree m over $\mathbb{F}_p$. Hence, $k = \mathbb{F}_{p^m}$. For the ease of the reader, we give the exact Macaulay2 syntax for this input. For instance, i1: is what is used by Macaulay2 as an input prompt in the first line.

i1: $k = GF(ZZ/p[t]/(f(t)))$

i2: $R = k[x, y]$

i3: $a = 0;$

i4: while $a < p\hat{}m - 1$ do(

$b = 0;$

while $b < p\hat{}m - 1$ do(

$c = 0;$

while $c < p\hat{}m - 1$ do(

$d = 0;$

while $d < p\hat{}m - 1$ do(

weight=0;

$\delta = 0;$

while $\delta < p\hat{}m - 1$ do(

I=ideal$(y\hat{}p - y - (t\hat{}(a + i_1 * \delta) + t\hat{}(b + i_2 * \delta)) * x\hat{}j_1 + (t\hat{}(c + i_3 * \delta) + t\hat{}(d +$

$i_4 * \delta)) * x\hat{}j_2, x\hat{}(p\hat{}m) - x, y\hat{}(p\hat{}m) - y);$

count=#flatten(entries(basis(R/I)));

rowweight=$p\hat{}m$ − count/p;

weight=weight+rowweight;

$\delta = \delta + 1$);

<< weight;

$d = d + 1$);

$c = c + 1$);

$b = b + 1$);

$a = a + 1$);

Vita

Cem Guneri was born on September 25 1973, in Elazig, Turkey. He finished his undergraduate studies at the Middle East Technical University, Ankara, on January 1995. In August 1996, he came to Louisiana State University to pursue graduate studies in mathematics. He earned a master of science degree in mathematics from Louisiana State University in May 1998. He is currently a candidate for the degree of Doctor of Philosophy in mathematics, which will be awarded in August 2001.

DOCTORAL EXAMINATION AND DISSERTATION REPORT

Candidate: Cem Guneri

Major Field: Mathematics

Title of Dissertation: Artin-Schreier Families and 2-D Cyclic Codes

Approved:

Robert F. Lax
Major Professor and Chairman

Dean of the Graduate School

EXAMINING COMMITTEE:

William A. Adkins

Robert Perlis

Date of Examination:

June 26, 2001