ARTIN-SCHREIER CURVES AND WEIGHTS OF 2-D CYCLIC CODES

CEM GÜNERİ

ABSTRACT. Let $\mathbb{F}_q$ be the finite field with q elements of characteristic p, $\mathbb{F}_{q^m}$ be the extension of degree $m > 1$ and $f(x)$ be a polynomial over $\mathbb{F}_{q^m}$. We determine a necessary and sufficient condition for $y^q - y = f(x)$ to have the maximum number of affine $\mathbb{F}_{q^m}$-rational points. Then we study the weights of 2-D cyclic codes. For this, we give a trace representation of the codes starting with the zeros of the dual 2-D cyclic code. This leads to a relation between the weights of codewords and a family of Artin-Schreier curves. We give a lower bound on the minimum distance for a large class of 2-D cyclic codes. Then we look at some special classes that are not covered by our main result and obtain similar minimum distance bounds.

1. INTRODUCTION

One of the applications of algebraic curves over finite fields in coding theory in recent years has been in the weight computations of certain cyclic codes. In this method, a cyclic code under consideration is represented as the trace of another code over an extension field and then the codewords of the cyclic code are related to a family of algebraic curves using the additive form of Hilbert's Theorem 90 (see [3], [15] and [17]). In [6], we used this idea to determine when a family of Artin-Schreier (A-S) curves has a member with the maximum possible number of affine rational points.

This article consists of two parts both of which heavily depend on the main results of [6]. The first part is on A-S curves. Namely, we determine a necessary and sufficient condition for an A-S curve to have the maximum number of affine rational points. The second part is on two-dimensional (2-D) cyclic codes and their weight analysis. These codes are generalizations of ordinary cyclic codes and, naturally, more complicated to deal with. The first attempts to build a general theory of such codes dates back to 70's, in particular to the works of Ikai, et al ([8]) and Imai ([9]). We extend the method applied to cyclic codes, which is mentioned above, to "square" 2-D cyclic codes by introducing a trace representation for such codes. As we will see, the main difference compared to cyclic codes is that the weight

1991 *Mathematics Subject Classification.* 94B27, 14G50, 11T71.

Key words and phrases. Artin-Schreier curve, 2-D cyclic code, trace code, Delsarte's theorem, Hilbert's Theorem 90.

of a single codeword is determined by more than one curve from a family of A-S curves.

There is another lower bound on the minimum distance of 2-D cyclic codes due to Jensen (see [10], [13]). He utilizes the concatenated structure of 2-D cyclic codes to come up with this bound. We leave the comparison of the two bounds to a future work.

In Section 2, we recall results on A-S families from [6] and use these to draw new conclusions about A-S curves. In Section 3, we define and state basic properties of 2-D cyclic codes, without proofs. We introduce the trace representation for 2-D cyclic codes in Section 4. In Section 5, we use this representation to state a general lower bound on the minimum distance. The final section is devoted to some special classes of codes which are not in the scope of our general bound from Section 5. We state similar minimum distance bounds for these special classes of codes and in one case we determine the complete weight enumerator. We explain our discussions with examples throughout and in some of the examples, we show possible improvements to our general bounds using specific arguments.

2. Artin-Schreier Curves

Unless otherwise stated $\mathbb{F}_q = \mathbb{F}_{p^l}$, with $l \geq 1$, is the finite field of characteristic p with q elements and $\mathbb{F}_{q^m}$ is the degree m extension of $\mathbb{F}_q$ where $m > 1$.

In [6] we studied the family $\mathcal{F} = \{y^q - y = \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s};\ \lambda_j \in \mathbb{F}_{q^m},\ i_j > 0\}$. We call the member with $\lambda_i = 0$, for all $i = 1, 2, \ldots, s$, the trivial one. It is easy to see that the number of affine $\mathbb{F}_{q^m}$-rational points of a nontrivial member in $\mathcal{F}$ is divisible by q and bounded by q^{m+1} (Proposition 4.1 in [6]).

Definition 2.1. 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 $q^{r+1}b \equiv b \ mod\ c$. *The q-cyclotomic coset containing b mod c* is the set

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

where each $q^i b$ is reduced mod c.

Here are the results from [6] which we will use in this section.

Theorem 2.2. *Let $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ be as before. Consider the family of curves*

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

Let B_j denote the q-cyclotomic coset mod $q^m - 1$ containing the exponent i_j and let $|B_j| = \delta_j \leq m$, for all j. We have the following:

(i) $\mathcal{F}$ has no nontrivial member with q^{m+1} affine $\mathbb{F}_{q^m}$-rational points if and only if $B_i \cap B_j = \emptyset$ for all $i \neq j$, $i, j \in \{1, 2, \ldots, s\}$, and $\delta_j = m$ for all j.

(ii) If there exists β distinct q-cyclotomic cosets $B_1, B_2, \ldots, B_\beta$ 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. See Theorem 4.4 and Corollary 4.5 in [6]. □

So, for $\mathcal{F}$ to have a nontrivial member with q^{m+1} affine $\mathbb{F}_{q^m}$-rational points, either two of the exponents should be in the same q-cyclotomic coset mod q^m-1 or the cardinality of one of the cyclotomic cosets should be a proper divisor of $m = [\mathbb{F}_{q^m} : \mathbb{F}_q]$. However, the theorem does not immediately indicate which member curves could achieve this upper bound. We want to answer the following question here:

Question: Given $X: \ y^q - y = \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}$, where λ_j's are in $\mathbb{F}_{q^m}$ and the q-cyclotomic cosets mod q^m-1 of i_j's are distinct. What are the necessary and sufficient conditions for X to have q^{m+1} affine $\mathbb{F}_{q^m}$-rational points?

Let $\#_{\mathbb{F}_{q^m}}(X)$ denote the number of affine $\mathbb{F}_{q^m}$-rational points of X. Note that $\#_{\mathbb{F}_{q^m}}(X) = q^{m+1}$ is equivalent to $\mathrm{tr}(\lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) = 0, \forall x \in \mathbb{F}_{q^m}$, by Hilbert's Theorem 90, where tr denotes the trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Hence, the above question can be restated as, with the same assumptions on the exponents, when is it true that $\mathrm{tr}(\lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) = 0$ for all x in $\mathbb{F}_{q^m}$?

Proposition 2.3. *Let $\lambda_j \in \mathbb{F}_{q^m}$ and i_j be positive integers, for $j = 1, 2, \ldots, s$. Assume that the q-cyclotomic cosets containing i_j's are distinct. Then $\mathrm{tr}(\lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) = 0$ for all x in $\mathbb{F}_{q^m}$ if and only if $\mathrm{tr}(\lambda_j x^{i_j}) = 0$ for all x in $\mathbb{F}_{q^m}$ and for all $j = 1, 2, \ldots, s$.*

Proof. One implication is immediate by linearity of the trace. For the other implication, note that the assertion is equivalent to

$$\begin{array}{c} \#_{\mathbb{F}_{q^m}}(y^q - y = \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) = q^{m+1} \\ \Updownarrow \\ \#_{\mathbb{F}_{q^m}}(y^q - y = \lambda_j x^{i_j}) = q^{m+1}, \text{ for all } j = 1, 2, \ldots, s. \end{array}$$

We need to prove the upper to lower implication. For this, we proceed by induction on s. If $s = 1$ there is nothing to prove. Assume the validity of the assertion up to s and consider the family $\mathcal{F} = \{y^q - y = \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s};\ \lambda_j \in \mathbb{F}_{q^m}\}$. By Theorem 2.2(ii), and using its notation, $\mathcal{F}$ has $q^{ms-\sum_{j=1}^{s}\delta_j} - 1$ nontrivial members with q^{m+1} affine rational points over $\mathbb{F}_{q^m}$. The subfamily $\mathcal{F}_1 = \{y^q - y = \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_{s-1} x^{i_{s-1}};\ \lambda_j \in \mathbb{F}_{q^m}\}$ contains $q^{m(s-1)-\sum_{j=1}^{s-1}\delta_j} - 1$ of these members in $\mathcal{F}$, and the subfamily $\mathcal{F}_2 = \{y^q - y = \lambda_s x^{i_s};\ \lambda_s \in \mathbb{F}_{q^m}\}$ has $q^{m-\delta_s} - 1$ of them. Furthermore, $\left(q^{m(s-1)-\sum_{j=1}^{s-1}\delta_j} - 1\right)\left(q^{m-\delta_s} - 1\right)$ curves in $\mathcal{F}$, which are distinct from those

in $\mathcal{F}_1$ and $\mathcal{F}_2$, with q^{m+1} points are obtained by "combining" q^{m+1} point curves in $\mathcal{F}_1$ and $\mathcal{F}_2$. By this, we mean creating polynomials in x in the form $\lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}$ by taking the first $s-1$ coefficients from the members with q^{m+1} points in $\mathcal{F}_1$ and λ_s with the same property from $\mathcal{F}_2$. The resulting polynomials do produce curves with q^{m+1} points indeed by linearity of the trace map. In this way, we exhaust all the $q^{ms-\sum_{j=1}^{s}\delta_j}-1$ nontrivial members of $\mathcal{F}$. Since the induction hypothesis applies to $\mathcal{F}_1$ and $\mathcal{F}_2$, we are done. □

By this proposition, the question posed reduces to the question: For which values $a \in \mathbb{F}_{q^m}$ and $i \in \mathbb{Z}^+$ do we have $\mathrm{tr}(ax^i) = 0$ for all x in $\mathbb{F}_{q^m}$? The following result of Gillot (Proposition 1.2 in [4]) answers this question. We present an alternative proof which depends on Theorem 2.2.

Proposition 2.4. *Let $a \in \mathbb{F}_{q^m}^*$ and i be a positive integer. Denote by B the q-cyclotomic coset containing i mod q^m-1 and let $\delta \leq m$ be the cardinality of B. Then $\mathrm{tr}(ax^i) = 0$ for all $x \in \mathbb{F}_{q^m}$ if and only if $\delta < m$ and $\mathrm{tr}_{q^m q^\delta}(a) = 0$, where $\mathrm{tr}_{q^m q^\delta}$ is the trace map from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_{q^\delta}$.*

Proof. Note that δ is a divisor of m. Hence, $\mathbb{F}_{q^\delta}$ is a subfield of $\mathbb{F}_{q^m}$ and $\mathrm{tr}_{q^m q^\delta}$ makes sense.
($\Rightarrow$) By the first part of Theorem 2.2, $\delta \neq m$ and by the second part of the same theorem, there exists $q^{m-\delta}$ a's in $\mathbb{F}_{q^m}$ such that $\mathrm{tr}(ax^i) = 0$ for all $x \in \mathbb{F}_{q^m}$. The number of elements in the kernel of $\mathrm{tr}_{q^m q^\delta}$ is also $q^{m-\delta}$ and for any b in this kernel, we have

$$\mathrm{tr}(bx^i) = \mathrm{tr}_{q^\delta q}(\mathrm{tr}_{q^m q^\delta}(bx^i)) = \mathrm{tr}_{q^\delta q}(x^i \mathrm{tr}_{q^m q^\delta}(b)) = 0.$$

Note that the second equality holds since $x^i \in \mathbb{F}_{q^\delta}$ for any $x \in \mathbb{F}_{q^m}$, by $|B| = \delta$, and $\mathrm{tr}_{q^m q^\delta}$ is an $\mathbb{F}_{q^\delta}$-linear map. Therefore, a must be in the kernel of $\mathrm{tr}_{q^m q^\delta}$.
($\Leftarrow$) By assumption on $|B|$, $x^i \in \mathbb{F}_{q^\delta}$ for any x in $\mathbb{F}_{q^m}$. Reading the above equalities from right to left, replacing b by a, proves the claim. □

Now, the following answers our question.

Theorem 2.5. *Let $X: \; y^q - y = \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}$, where λ_j's are in $\mathbb{F}_{q^m}$. Let B_j denote the q-cyclotomic coset containing i_j mod q^m-1, for all j, and assume that B_j's are pairwise disjoint. Then the following are equivalent:*
(i) $\#_{\mathbb{F}_{q^m}}(X) = q^{m+1}$,
(ii) $|B_j| = \delta_j < m$ and $\mathrm{tr}_{q^m q^{\delta_j}}(\lambda_j) = 0$, for all $j = 1, 2, \ldots, s$.

Proof. Immediate from Propositions 2.3 and 2.4. □

We finish this section with a characterization of (Hasse-Weil) maximal (Theorem V.2.3, Definition V.3.2 in [16]) and q^{m+1}-optimal A-S curves whose x-degree is relatively prime to the characteristic of the base field (also see Corollary 4.7 in [6]).

Corollary 2.6. *Let m be even, $X : y^q - y = f(x)$, where $f(x)$ is a constant-free polynomial over $\mathbb{F}_{q^m}$ for which the exponents of x are in different q-cyclotomic cosets mod $q^m - 1$ and $\gcd(\deg(f), q) = 1$. Then X is maximal and q^{m+1}-optimal if and only if X is of the form $y^q - y = ax^{q^{\frac{m}{2}}+1}$ for some $a \in \mathbb{F}_{q^m}$ with $\mathrm{tr}_{q^m q^{\frac{m}{2}}}(a) = 0$.*

Proof. ($\Rightarrow$) X has one point at infinity and hence the number of projective $\mathbb{F}_{q^m}$-rational points is $q^{m+1}+1$. By assumption on $\deg(f)$, the genus of X is $\frac{(q-1)(\deg(f)-1)}{2}$ (Proposition VI.4.1 in [16]). Therefore, Hasse-Weil bound on the number of projective rational points is $q^m + 1 + (q-1)(\deg(f)-1)q^{\frac{m}{2}}$. Equating these two numbers, both of which are met by X, gives $\deg(f) = q^{\frac{m}{2}}+1$. Note that the cardinality of the q-cyclotomic coset containing $\deg(f)$ is $\frac{m}{2}$. If $f(x) = bx^r + ax^{q^{\frac{m}{2}}+1}$ for some $b \in \mathbb{F}_{q^m}^*$ and $r < q^{\frac{m}{2}} + 1$ then, in order to be q^{m+1}-optimal, cardinality of the cyclotomic coset containing r must be a proper divisor of m (Theorem 2.5). But this number must also be greater than $\frac{m}{2}$, which is impossible. Therefore $f(x) = ax^{q^{\frac{m}{2}}+1}$ for some $a \in \mathbb{F}_{q^m}$, and the condition on a follows from Theorem 2.5.
($\Leftarrow$) The assumption on a and the exponent $q^{\frac{m}{2}} + 1$ of x guarantees that such a curve is q^{m+1}-optimal. Using the genus formula and the Hasse-Weil bound above, together with the fact that X has one point at infinity, we see that X is also maximal. □

3. Definition and Basic Properties of 2-D Cyclic Codes

For the proofs of the results in this section and for further properties of 2-D cyclic codes, we refer the interested reader to [7], [8], [9] and [14].

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.

Definition 3.1. 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 $\mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1)$:

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

Under this identification, we can think of a 2-D linear code C as a subset of $\mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1)$. It is easy to see that 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 $\mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1)$. In short, we have two ways to represent a 2-D cyclic code: The matrix representation and the polynomial representation.

We assume, from now on, that both n_1 and n_2 are relatively prime to p. In fact, both of these numbers will be $q^m - 1$ for some $m > 1$ in our considerations starting with the next section. 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.

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

We define *the $\mathbb{F}_q$-conjugacy class containing* (α_1^i, α_2^j) to be

$$S = [(\alpha_1^i, \alpha_2^j)] = \{(\alpha_1^i, \alpha_2^j), (\alpha_1^{iq}, \alpha_2^{jq}), \ldots, (\alpha_1^{iq^{\delta-1}}, \alpha_2^{jq^{\delta-1}})\},$$

where δ is the least common multiple of the degrees of α_1^i and α_2^j over $\mathbb{F}_q$. 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.

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

$$I(U) = \{f(x,y) \in \mathbb{F}_q[x,y];\ f(a) = 0,\ \forall a \in U\}. \tag{1}$$

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. 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

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

is called *the zero set of the 2-D cyclic code* $\tilde{J}$. 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 it is either a single $\mathbb{F}_q$-conjugacy class or a finite union of $\mathbb{F}_q$-conjugacy classes. Also note that $Z_{\bar{\mathbb{F}}_q}(J)$ would be another way to denote $Z(\tilde{J})$, due to obvious reasons, where $\bar{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$.

Proposition 3.2. *Let U be a subset of Ω. Then*

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

Another way to state Proposition 3.2 is that every subset U of Ω is the zero set of the 2-D cyclic code $\tilde{I}(U)$ that it defines. Note that since a 2-D cyclic code is an ideal in $\mathbb{F}_q[x,y]/(x^{n_1}-1, y^{n_2}-1)$, we can describe it by giving a finite number of generating polynomials. The following result says that there is another way to describe a 2-D cyclic code.

Proposition 3.3. *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 $\tilde{J}$.*

In other words we have $\tilde{I}(Z(\tilde{J})) = \tilde{J}$, which comes from the fact that $J \subset \mathbb{F}_q[x,y]$ is a radical ideal. This can be proved by Seidenberg's Lemma 92 (Proposition 8.14 in [1]). Besides describing the code, the zero set also gives us the dimension of the code.

Theorem 3.4. *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*

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

We now state the result that relates the code to its dual.

Proposition 3.5. *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 3.6. *The dimension of a 2-D cyclic code is equal to the number of zeros of its dual code.*

We finish with two more definitions for the sake of completeness.

Definition 3.7. 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 3.8. 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 3.9. 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 the rest of the paper, we will always have this kind of choice on our basic sets and, unless otherwise stated, the choice will be made with respect to the second coordinates.

4. Trace Representation of 2-D Cyclic Codes

Recall that $q = p^l$ for some $l \geq 1$, where p is prime, and consider q^m with $m > 1$. Let α be a primitive element of $\mathbb{F}_{q^m}$ throughout, unless otherwise stated. Consider the sets

$$\Omega = \{(\alpha^i, \alpha^j);\ 0 \leq i, j \leq q^m - 2\} = \mathbb{F}_{q^m}^* \times \mathbb{F}_{q^m}^*, \tag{3}$$

$$U = [(\alpha^{i_1}, \alpha^{j_1})] \cup [(\alpha^{i_2}, \alpha^{j_2})] \cup \ldots \cup [(\alpha^{i_s}, \alpha^{j_s})], \tag{4}$$

where i_γ, j_γ are in the set $\{0, 1, \ldots, q^m - 2\}$.

We know that the zero (resp. nonzero) set or a basic zero (resp. basic nonzero) set determine the 2-D cyclic code uniquely. 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:

$$Z(C) = \Omega - U^{-1} = \bar{U}^{-1} \tag{5}$$

If C' denotes the dual of C, then we have the following easy consequences:

$$\begin{aligned} NZ(C) &= \Omega - \bar{U}^{-1} = U^{-1} \\ Z(C') &= U \\ NZ(C') &= \Omega - U = \bar{U} \end{aligned} \tag{6}$$

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 the previous section.

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

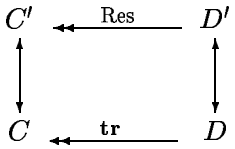
$$C = C_{\bar{U}^{-1}} = \tilde{I}(\bar{U}^{-1}) = I(\bar{U}^{-1})/(x^{q^m-1} - 1, y^{q^m-1} - 1).$$

For simplicity we will denote C and C' as I and I', respectively, in the polynomial representation. 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

$$Z(D') = \{(\alpha^{i_1},\alpha^{j_1}),(\alpha^{i_2},\alpha^{j_2}),\ldots,(\alpha^{i_s},\alpha^{j_s})\}. \tag{7}$$

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. Note that D' restricts to C' and hence we get the following familiar diagram from Delsarte's Theorem (Theorem VIII 1.2 in [16]):

(8)



Note that **tr** is defined by applying the trace map, tr, 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

$$a(\alpha^{i_\gamma},\alpha^{j_\gamma}) = \sum_{i,j=0}^{q^m-2} a_{i,j}(\alpha^{i_\gamma})^i(\alpha^{j_\gamma})^j = 0, \quad \gamma = 1,2,\ldots,s. \tag{9}$$

When the s equations in (9) are translated to the matrix notation, we get

$$(a_{i,j})\cdot v_\gamma = 0,\ \gamma = 1,2,\ldots,s.$$

Here $(a_{i,j}) \in D'$ is the corresponding coefficient matrix (codeword) for an arbitrary polynomial in J' and it is in the form

$$(a_{i,j}) \quad = \quad \begin{pmatrix} a_{0,0} & \cdots & a_{0,q^m-2} \\ a_{1,0} & \cdots & a_{1,q^m-2} \\ \vdots & \ddots & \vdots \\ a_{q^m-2,0} & \cdots & a_{q^m-2,q^m-2} \end{pmatrix}.$$

On the other hand v_γ is defined as

$$v_\gamma \quad = \quad \begin{pmatrix} (\alpha^{i_\gamma})^0(\alpha^{j_\gamma})^0 & \cdots & (\alpha^{i_\gamma})^0(\alpha^{j_\gamma})^{q^m-2} \\ (\alpha^{i_\gamma})^1(\alpha^{j_\gamma})^0 & \cdots & (\alpha^{i_\gamma})^1(\alpha^{j_\gamma})^{q^m-2} \\ \vdots & \ddots & \vdots \\ (\alpha^{i_\gamma})^{q^m-2}(\alpha^{j_\gamma})^0 & \cdots & (\alpha^{i_\gamma})^{q^m-2}(\alpha^{j_\gamma})^{q^m-2} \end{pmatrix}. \tag{10}$$

Therefore $\{v_1,v_2,\ldots,v_s\}$ is contained in D, which is the dual of D'. Observe that the $\mathbb{F}_{q^m}$-dimension of D is s, by Corollary 3.6 and (7).

Proposition 4.1. *$\{v_1,v_2,\ldots,v_s\}$ forms a basis for D.*

Proof. 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:

$$A = \mathbb{F}_{q^m}^* = \{\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{q^m-2}\}. \tag{11}$$

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. What we understand from this notation is that one substitutes the elements of A for x, following the order of elements in (11). If we put the above representations of each row in v_γ together, we get the following representation for v_γ:

$$v_\gamma = \begin{pmatrix} x^{j_\gamma} \\ \alpha^{i_\gamma} x^{j_\gamma} \\ \vdots \\ (\alpha^{i_\gamma})^{q^m-2} x^{j_\gamma} \end{pmatrix}_{x\in A}, \qquad \gamma = 1, 2, \ldots, s \tag{12}$$

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

$$v_\gamma = \left((\alpha^{i_\gamma})^\delta x^{j_\gamma}\right)_{x\in A, \delta\in\mathcal{I}}, \qquad \gamma = 1, 2, \ldots, s \tag{13}$$

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. Suppose there exist $\mu_1, \mu_2, \ldots, \mu_s$ in $\mathbb{F}_{q^m}$ such that

$$\mu_1 v_1 + \mu_2 v_2 + \cdots + \mu_s v_s = \vec{0}. \tag{14}$$

This means

$$\begin{pmatrix} \mu_1 x^{j_1} + \mu_2 x^{j_2} + \cdots + \mu_s x^{j_s} \\ \mu_1 \alpha^{i_1} x^{j_1} + \mu_2 \alpha^{i_2} x^{j_2} + \cdots + \mu_s \alpha^{i_s} x^{j_s} \\ \vdots \\ \mu_1 (\alpha^{i_1})^{q^m-2} x^{j_1} + \mu_2 (\alpha^{i_2})^{q^m-2} x^{j_2} + \cdots + \mu_s (\alpha^{i_s})^{q^m-2} x^{j_s} \end{pmatrix}_{x\in A} = \vec{0}. \tag{15}$$

Suppose that the j_γ's are all distinct. Then the first row in (15) gives

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

This polynomial expression has distinct exponents and its degree is the maximum of $\{j_1, \ldots, j_s\}$. This degree is strictly less than $q^m - 1$ (cf. (3)). 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 (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:

$$\begin{array}{c} \mu_1 + \mu_2 + \cdots + \mu_c = 0 \\ \mu_1\alpha^{i_1} + \mu_2\alpha^{i_2} + \cdots + \mu_c\alpha^{i_c} = 0 \\ \vdots \\ \mu_1(\alpha^{i_1})^{q^m-2} + \mu_2(\alpha^{i_2})^{q^m-2} + \cdots + \mu_c(\alpha^{i_c})^{q^m-2} = 0 \end{array} \tag{16}$$

Since α is primitive in $\mathbb{F}_{q^m}$, the equalities in (16) are equivalent to

$$\mu_1 x^{i_1} + \mu_2 x^{i_2} + \cdots + \mu_c x^{i_c} = 0, \quad \text{forall } x \in A = \mathbb{F}_{q^m}^*. \tag{17}$$

Note that the exponents in (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 (4).

By the above observation on $i_1, \ldots, i_c$, (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. □

Remark 4.2. It is important to note that an analogue of the representations in (12) and (13) can also be obtained vertically. For this, we look at the columns of v_γ in (10). 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

$$v_\gamma = \left(x^{i_\gamma} \quad , \quad \alpha^{j_\gamma}x^{i_\gamma} \quad , \quad \ldots \quad , \quad (\alpha^{j_\gamma})^{q^m-2}x^{i_\gamma}\right)_{x\in A}, \quad \gamma = 1, 2, \ldots, s \tag{18}$$

and the short vertical representation is

$$v_\gamma = \left((\alpha^{j_\gamma})^\delta x^{i_\gamma}\right)_{x\in A, \delta\in\mathcal{I}}, \qquad \gamma = 1, 2, \ldots, s \tag{19}$$

Note that δ indexes the columns of v_γ this time.

Theorem 4.3. *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 $\gamma = 1, 2, \ldots, s$:*

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

$$= \left\{ \left(\lambda_1 (\alpha^{j_1})^\delta x^{i_1} + \lambda_2 (\alpha^{j_2})^\delta x^{i_2} + \cdots + \lambda_s (\alpha^{j_s})^\delta x^{i_s} \right)_{x \in A, \delta \in \mathcal{I}} \right\}$$

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

Proof. This is a direct consequence of Proposition 4.1 combined with the fact that $C = \mathbf{tr}(D)$ and the notations introduced in (12), (13), (18) and (19). □

Note that the order of representations for D and C in Theorem 4.3, after the first one, 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 4.4. *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*

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

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

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

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 $(\mu_1, \mu_2, \ldots, \mu_s)$ 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. □

5. Minimum Distance Bound

Consider the code C in the horizontal representation in Theorem 4.3. 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 and it is

$$(20)\quad q^m - 1 - \frac{1}{q}\left(\#_{\mathbb{F}_{q^m}}(y^q - y = f(x)) - q\right) = q^m - \frac{\#_{\mathbb{F}_{q^m}}(y^q - y = f(x))}{q},$$

where $f(x)$ is what is in the trace function corresponding to this row. 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. In particular, for the $(r+1)^{st}$ row for any $r \in \{0, 1, \ldots, q^m - 2\}$, we have $f(x) = \mu_1(\alpha^{i_1})^r x^{j_1} + \cdots + \mu_s(\alpha^{i_s})^r x^{j_s}$. Note that q points corresponding to $x = 0$ on the curve must be subtracted in the formula since we evaluate trace on $\mathbb{F}_{q^m}^*$. Therefore, the whole weight enumerator of C is related to the following family:

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

Using Theorem 2.2, we have the following criteria for rows in codewords of C to be zero:

Proposition 5.1. *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*

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

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 (8) 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 3.6, 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 also injective.

(ii) Recall that the weight of a row in v is given by the formula (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 pairwise non-conjugate with respect to $\mathbb{F}_q$ (cf. Remark 3.9), we can use Theorem 2.2. Note that some of the j_γ's may be the same and therefore we cannot conclude that the curve in the formula (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 5.1 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 4.3 makes it clear that answering this question in the generality of Proposition 5.1 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.

Theorem 5.2. *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*

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

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

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

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

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 3.6.

(ii) We adopt the notation of Proposition 5.1. 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

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

Since the j_γ's are all distinct, the polynomial expression of degree $j_s < q^m-1$ (see (3)) is 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 affine $\mathbb{F}_{q^m}$-rational points on any member of $\mathcal{F}$ is divisible by q and cannot be q^{m+1} by our hypothesis (cf. Theorem 2.2). 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. Letting N be this number we see that the minimal possible weight in a row of v is, by (20), $q^m - \frac{N}{q}$. Repeating this minimal weight in each row gives the lowest possible nonzero weight that can occur in C. $\square$

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 5.2. If we attempt to use the Hasse-Weil-Serre (H-W-S) bound (Theorem V.3.1 in [16]) 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 Section 3 in [6]). The following is a case when we are able to overcome these difficulties.

Corollary 5.3. *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 $\dim_{\mathbb{F}_q}(C) = sm$ and if d denotes the minimum distance of C, we have

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

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. The dimension of C is found as in Theorem 5.2. 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 5.2 and we only need to show that the number N is what we assert it is. Note that our family is $\mathcal{F} = \{y^q - y = \sum_\gamma \lambda_\gamma x^{r_\gamma p^{\eta_\gamma}};\ \lambda_\gamma \in \mathbb{F}_{q^m}\}$. It is known that such curves are all Artin-Schreier (A-S) and the biggest genus in $\mathcal{F}$ is $\frac{(q-1)(r-1)}{2}$ (Remark 3.2 in [6]). Therefore, the corresponding H-W-S bound is indeed a universal bound on the family of curves; i.e., it bounds the number of affine rational points of every curve in the family. Note that the bound we use in the formula is one less than the H-W-S bound, which is due to the fact that there is only one rational point at infinity for all the curves in $\mathcal{F}$ and we only consider affine rational points in our considerations. □

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, which is $q^m - \frac{N}{q}$) in each row whereas this is not necessarily the case in reality. Finding a way to use the relations among the coefficients of rows in the representations of Theorem 4.3 could clearly imrove the bound.

We look at some examples now. One can use Macaulay2 ([5]) to compute actual minimum distances if the finite field is not too big. For the Macaulay2 routine, which is based on our representations in Theorem 4.3, we refer to [7]. In the examples we will try to show some ideas to improve the estimates and even compute the weight enumerators in some cases.

Example 5.4. 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 6.2.

Example 5.5. 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 5.3. 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 hypotheses of Corollary 5.3 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.

Example 5.6. 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 the code over $\mathbb{F}_8$ such that $\mathbf{tr}(D) = C$, we have the following representation (cf. Theorem 4.3):

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

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 the tables for such curves in [15], 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 5.7. Two things make it possible to find the exact minimum distance in Example 5.6. The first is the knowledge that N of Corollary 5.3 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 the 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.

6. Special Classes of 2-D Cyclic Codes

Our goal in this section is to investigate special classes of codes which are not covered by Corollary 5.3. In order to stay out of the scope of Corollary 5.3, 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 6.1. *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 C is of dimension $2m$ over $\mathbb{F}_q$ and 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

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

Proof. Since α is primitive in $\mathbb{F}_{q^m}$ 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 and the dimension of C is $2m$. We know that $C=\mathbf{tr}(D)$ for a code D over $\mathbb{F}_{q^m}$ and $\mathbf{tr}$ is injective (cf. Proposition 5.1). 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 5.1. In fact, by Theorem 4.3, we have the following short horizontal representations for these codewords:

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

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

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

$$q^m-\frac{\#_{\mathbb{F}_{q^m}}\left(y^q-y=(\lambda_1(\alpha^{i_1})^\delta+\lambda_2(\alpha^{i_2})^\delta)x\right)}{q}$$

for some $\delta\in\mathcal{I}$. Since the curve in the formula is a rational curve, provided that the coefficient of x 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

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

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 $(\lambda_1, \lambda_2) \in \mathbb{F}_{q^m}^* \times \mathbb{F}_{q^m}^*$). 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. This means the corresponding codewords in C will have the same number of zero rows and hence their weight will be $\left(q^m - 1 - \frac{q^m-1}{\theta}\right)(q^m - q^{m-1})$. All the remarkaining $(q^m-1)^2 - \theta \cdot (q^m-1)$ 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 6.2. Refer back to the code C of Example 5.4. 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 4.4). 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 5.4 is 42.

Remark 6.3. Theorem 6.1 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 [2]).

Observe that what made it possible to obtain the weight enumerator in Theorem 6.1 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 6.4. *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

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

where d is the minimum distance of C, N is the maximum of $\{q, 2q, \ldots, (q^m-1)q\}$ 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 $\mathbb{F}_q$. 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

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

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

By Proposition 5.1, 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 6.1. For the remaining nonzero rows, we choose the lowest possible weight. This means, the highest number of affine $\mathbb{F}_{q^m}$-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 2.2, $\mathcal{F}$ 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 6.5. 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 6.6. *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 $j_\gamma = r_\gamma p^{\eta_\gamma}$ $(\gamma = 1, 2)$, 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 $r = max\{r_1, r_2\}$. If r_1 and r_2 are distinct, then

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

where d is the minimum distance of C, N is the maximum of $\{q, 2q, \ldots, (q^m-1)q\}$ 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 and C have dimension $3m$ over $\mathbb{F}_q$. A nonzero codeword v in C is of the form

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

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 the 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 $\frac{q^m-1}{\theta}$ total zero rows. It can be shown, as it was done in the proof of Theorem 6.1, 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 $\frac{q^m-1}{\theta}$. 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 6.7. 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 6.8. 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 6.7, 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 6.9. *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

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

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

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

Example 6.10. 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 6.11. 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 5.6. Namely, the codewords in C are of the form

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

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 5.6, 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, the tables in [15] show that 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 6.12. 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 6.11, 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.

Acknowledgements

The results on 2-D cyclic codes (sections 4, 5, and 6) have appeared in the author's doctoral dissertation, which was written under the supervision of R.F. Lax at Louisiana State University. The author appreciates his guidance. Also, thanks to M. Zieve for pointing out Corollary 2.6.

References

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

[2] R. Calderbank and W. M. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc.* **18** (1986), 97-122.

[3] G. van der Geer and M. van der Vlugt, Weight distributions for a certain class of codes and maximal curves, *Discrete Math.* **106/107** (1992), 209–218.

[4] V. Gillot, Bounds for exponential sums over finite fields, *Finite Fields Appl.* **1** (1995), 421–436.

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

[6] C. Guneri, A bound on the number of rational points of certain Artin-Schreier families, *Comm. Algebra* **30** (2002), 4251–4265.

[7] C. Guneri, Artin-Schreier families and 2-D cyclic codes, PhD Thesis Louisiana State University (2001).

[8] T. Ikai, H. Kosako and Y. Kojima, Two-dimensional cyclic codes, *Electronics and Communications in Japan* **57-A** (1975), 27– 35.

[9] H. Imai, A theory of two-dimensional cyclic codes, *Information and Control* **34** (1977), 1–21.
[10] J. M. Jensen, The concatenated structure of cyclic and abelian codes, *IEEE Trans. Inform. Theory* **31** (1985), 788–793.
[11] R. Lidl and H. Niederreiter, Finite Fields, Encyc. Math. Appl. **20**, Cambridge University Press (1997).
[12] J. H. van Lint, Introduction to Coding Theory, Springer-Verlag, (1999).
[13] R. E. Sabin, On minimum distance bounds for abelian codes, *Appl. Algebra Engrg. Comm. Comput.* **3** (1992), 183–197.
[14] K. Saints, Algebraic methods for the encoding and decoding problems for multidimensional cyclic codes and algebraic-geometric codes, PhD Thesis Cornell University (1995).
[15] R. Schoof, Families of curves and weight distribution of codes, *Bull. Amer. Math. Soc.* **32** (1995), 171–183.
[16] H. Stichtenoth, Algebraic Function Fields and Codes, Universitext Springer-Verlag (1993).
[17] J. Wolfmann, New bounds on cyclic codes from algebraic curves, *Lecture Notes in Comput. Sci.* **388** (1989), 47–62.

SABANCI UNIVERSITY, FENS, TUZLA 34956, ISTANBUL TURKEY
E-mail address: guneri@sabanciuniv.edu