ON THE MINIMUM DISTANCE OF CYCLIC CODES

by

LEYLA IŞIK

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

Sabancı University
Fall 2010

ON THE MINIMUM DISTANCE OF CYCLIC CODES

APPROVED BY

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

Prof. Dr. Henning Stichtenoth ....

Prof. Dr. Alev Topuzoğlu ....

Assoc. Prof. Dr. Wilfried Meidl ....

Assoc. Prof. Dr. Albert Levi ....

DATE OF APPROVAL: February 4, 2011

ON THE MINIMUM DISTANCE OF CYCLIC CODES

Leyla Işık

Mathematics, Master Thesis, 2011

Thesis Supervisor: Assoc. Prof. Dr. Cem Güneri

Keywords: Finite fields, cyclic codes, trace representations, permutation polynomials.

Abstract

Estimation of the minimum distance of cyclic codes is a classical problem in coding theory. Using the trace representation of cyclic codes and Hilbert's Theorem 90, Wolfmann found a general estimate for the minimum distance of cyclic codes in terms of the number of rational points on certain Artin-Schreier curves. In this thesis, we try to understand if Wolfmann's bound can be improved by modifying equations of the Artin-Schreier curves by the use of monomial and some nonmonomial permutation polynomials. Our experiments show that an improvement is possible in some cases.

DEVİRSEL KODLARIN MİNİMUM UZAKLIĞI

Leyla Işık

Matematik, Yüksek Lisans Tezi, 2011

Tez Danışmanı: Doç. Dr. Cem Güneri

Anahtar Kelimeler: Sonlu cisimler, devirsel kodlar, iz gösterimleri, permütasyon polinomları

Özet

Devirsel kodların minimum uzaklıklarını sınırlama, kodlama teorisinin klasik problemlerinden biridir. Wolfmann, iz gösterimleri ve Hilbert 90 Teoremini kullanarak, devirsel kodların minimum uzaklıkları için bazı Artin-Schreier eğrilerinin rasyonel nokta sayıları cinsinden alt sınır buldu. Bu tezde Artin-Schreier eğrilerinin denklemleri değiştirilerek Wolfmann'ın sınırının iyileştirilip iyileştirilemeyeceği anlaşılmaya çalışıldı. Deneylerimiz iyileştirmenin bazı durumlarda mümkün olduğunu gösterdi.

Anneme

Acknowledgements

I would like to express my deep and sincere gratitude to my advisor, Assoc. Prof. Dr. Cem Güneri, who gave me the opportunity to work in this study. This thesis would not have been possible without his support and guidance. Also his wide knowledge and logical way of thinking have been of great value for me.

My special gratitude is due to my family members, especially my parents, for their loving support throughout this thesis.

I finally thank all my friends at office and dormitory for their kindness and helping me get through the difficult times.

Table of Contents

1

Cyclic Codes and Permutation Polynomials

We introduce the preliminaries in coding theory and permutation polynomials in this chapter. Section 1 and 2 introduce cyclic codes and their trace representation. The trace representation yields a relation with algebraic curves which we outline. We refer to [4], [5], [2], [6] for further details on cyclic codes and their relation to algebraic curves. In Section 3, we prove a result of Zieve [7] which will be used to produce permutation polynomials other than monomials.

1.1 Cyclic Codes

Let $\mathbb{F}_q$ denote the finite field with q elements, where $q = p^s$ for a prime number p and a nonnegative integer s. A subset C of $\mathbb{F}_q^n$ is called a *q-ary code of length n.* Elements of C are called *codewords.*

For $x = (x_1, x_2, ..., x_n),\ \ y = (y_1, y_2, ..., y_n) \in \mathbb{F}_q^n,$ define

$$d(x, y) := \big|\{1 \le i \le n;\ x_i \ne y_i\}\big|.$$

The function d defines a metric on $\mathbb{F}_q^n$, which is called the *Hamming distance.* Using the Hamming distance, we define the *minimum distance* $d(C)$ of C as

$$d_{min} := \min\{d(x, y)|\ x, y \in C, x \ne y\}.$$

The *weight* of an element $x = (x_1, x_2, ..., x_n) \in \mathbb{F}_q^n$ is defined as

$$wt(x) = d(x, 0) := \big|\{1 \le i \le n;\ x_i \ne 0\}\big|.$$

Throughout this thesis, we will consider *linear codes.* This means that $C \subseteq \mathbb{F}_q^n$ will be an $\mathbb{F}_q$-subspace. We will use the term “code” for linear codes. The dimension of C as an $\mathbb{F}_q$-vector space is called the *dimension* of the code. The length, dimension and the minimum distance are three important parameters of a code. We denote a code of length n, dimension k and minimum distance d as $[n, k, d]$ code.

Proposition 1.1. *For a linear code C, the minimum distance is equal to the minimum nonzero weight in C.*

Proof. It follows from the definitions that $w(x) = d(0, x)$ and that $d(x, y) = w(x - y)$. Let c be a codeword of minimum nonzero weight. Then $w(c) = d(0, c)$ and since 0 is a codeword we have $d_{min} \leq w_{min}$. On the other hand, if c_1 and c_2 are codewords at minimum distance, we have $d(c_1, c_2) = w(c_1 - c_2)$ and since $c_1 - c_2$ is again a codeword we get $w_{min} \leq d_{min}$. Therefore, $d(C)$ is the minimal weight of C. □

Definition 1.2. A $[n, k]$-code C over $\mathbb{F}_q$ is called *cyclic* if $(c_0, c_1, ..., c_{n-1}) \in C$ implies that $(c_{n-1}, c_0, ..., c_{n-2}) \in C$.

It is useful to represent codewords as polynomials. The codeword

$$c := (c_0, c_1, ..., c_{n-1})$$

is represented by the polynomial

$$c(x) := c_0 + c_1 x + ... + c_{n-1} x^{n-1}.$$

Note that this assignment yields a map

$$\begin{aligned} \varphi : \mathbb{F}_q^n &\rightarrow \mathbb{F}_q[x]/(x^n - 1) \\ (a_0, a_1, ..., a_{n-1}) &\mapsto \sum_{i=0}^{n-1} a_i x^i \end{aligned}$$

where $\sum_{i=0}^{n-1} a_i x^i$ denotes a coset representative.

Proposition 1.3. *φ is an $\mathbb{F}_q$-linear isomorphism.*

Proof. Let $a = (a_0, a_1, ..., a_{n-1}),\ b = (b_0, b_1, ..., b_{n-1}) \in \mathbb{F}_q^n$ and $k \in \mathbb{F}_q$. Then we have the following

$$\begin{aligned} \varphi(ka + b) &= \sum_{i=0}^{n-1} (ka_i + b_i) x^i \\ &= \Big\{ \sum_{i=0}^{n-1} k a_i x^i \Big\} + \Big\{ \sum_{i=0}^{n-1} b_i x^i \Big\} \\ &= k \sum_{i=0}^{n-1} a_i x^i + \sum_{i=0}^{n-1} b_i x^i \\ &= k\varphi(a) + \varphi(b). \end{aligned}$$

Therefore φ is a $\mathbb{F}_q$-linear map. It is easily seen that $Ker(\varphi) = \{a \in \mathbb{F}_q^n | \ a_0 + a_1 x + ... + a_{n-1} x^{n-1}\} = \{0\}$. This shows that φ is one-to-one. Also φ is surjective since for each polynomial with degree less than n there is an n-tuple vector which is obtained by the coefficients of that polynomial. Hence we have proved our assertion. □

Theorem 1.4. *A linear code $C \subseteq \mathbb{F}_q^n$ is cyclic if and only if C is an ideal of $\mathbb{F}_q[x]/(x^n-1)$.*

Proof. ($\Leftarrow$) If C is an ideal and $(a_0, a_1, ..., a_{n-1}) \in C$, then also

$$x(a_0 + a_1x + ... + a_{n-1}x^{n-1}) = a_0x + a_1x^2 + ... + a_{n-2}x^{n-1} + a_{n-1} \ \in C.$$

This implies $(a_{n-1}, a_0, ..., a_{n-2}) \in C$.
($\Rightarrow$) If $(a_0, a_1, ..., a_{n-1}) \in C$ implies $(a_{n-1}, a_0, ..., a_{n-2}) \in C$, then for every codeword $a(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} \in C$ we have $xa(x) \in C$, hence also $x^2a(x) \in C$, $x^3a(x) \in C$, so on. Therefore $b(x)a(x) \in C$ for any polynomial $b(x)$; that is C is an ideal. □

Definition 1.5. If C is an $[n,k]$ code we define the *dual code* $C^\perp$ by

$$C^\perp = \{u \in \mathbb{F}_q^n |\ u \cdot v = 0,\ \forall v \in C\},$$

where $\cdot$ denotes the usual inner product on $\mathbb{F}_q^n$.

Note that $C^\perp$ is also a linear code whose dimension is $n - \dim(C)$.

Proposition 1.6. *If C is cyclic then the dual code $C^\perp$ is also cyclic.*

Proof. Note that the shift operator

$$\begin{aligned} s : C &\rightarrow C \\ (c_0, c_1, ..., c_{n-1}) &\mapsto (c_{n-1}, c_0, ..., c_{n-2}) \end{aligned}$$

on a cyclic code C is a bijection. Let $(d_0, d_1, ..., d_{n-1}) \in C^\perp$. Then,

$$(d_0, d_1, ..., d_{n-1}) \cdot (c_0, c_1, ..., c_{n-1}) = 0, \text{ for any } (c_0, c_1, ..., c_{n-1}) \in C.$$

This implies that $(d_{n-1}, d_0, ..., d_{n-2}) \cdot (c_{n-1}, c_0, ..., c_{n-2}) = 0$. Since s is a bijection this means $(d_{n-1}, d_0, ..., d_{n-2})$ is orthogonal to every codeword in C. □

Next, we analyze the polynomial representation of a cyclic code. Note that $\mathbb{F}_q[x]/(x^n - 1)$ is a principal ideal ring. Hence, any cyclic code C in $\mathbb{F}_q[x]/(x^n-1)$ has a unique monic polynomial (codeword) $g(x)$ of lowest degree such that C is generated by $g(x)$ as an ideal. This polynomial is called the *generator polynomial* of C. Note that the generator polynomial $g(x)$ of a cyclic code C of length n must divide the polynomial $x^n - 1$ in $\mathbb{F}_q[x]$. Hence one can list all q-ary cyclic codes of length n by listing all possible divisors of $x^n - 1$.

Proposition 1.7. *Let C be a cyclic code of length n over $\mathbb{F}_q$ with the generator polynomial $g(x)$. If $\deg(g(x)) = k$, then $\dim(C) = n - k$.*

Proof. Note that

$$\begin{aligned} C =< g(x) > &= \{m(x)g(x) \mid m(x) \in \mathbb{F}_q[x]\ ,\ \deg(m(x)) < n-k\} \\ &= \big\{(m_0 + m_1x + ... + m_{n-k-1}x^{n-k-1})g(x) \mid m_i \in \mathbb{F}_q\big\} \\ &= \big\{m_0g(x) + m_1xg(x) + ... + m_{n-k-1}x^{n-k-1}g(x) \mid m_i \in \mathbb{F}_q\big\} \\ &= span_{\mathbb{F}_q}\{g(x), xg(x), ..., x^{n-k-1}g(x)\} \end{aligned}$$

Since the degrees of the polynomials in the spanning set are different, this set is $\mathbb{F}_q$-independent. Thus $\{g(x), xg(x), ..., x^{n-k-1}g(x)\}$ is a basis for C. □

Remark 1.8. We will assume throughout that $n = q^m - 1$ for some $m > 1$. This implies that the polynomial $x^n - 1$ is separable. In particular, the generator polynomial $g(x)$ of a q-ary cyclic code C of length n is also separable since $g(x)$ divides $x^n - 1$. In this case, we have $\dim C = n - k$ and $\dim C^{\perp} = k$, where k is the number of roots of $g(x)$. Note that the cyclic code $\widetilde{C}$ of length n whose generator polynomial is $\frac{x^n-1}{g(x)}$ is not $C^{\perp}$ but it can be obtained from $C^{\perp}$ by a change of coordinates of codewords (see [4], page 84). In this case, the two codes $\widetilde{C}$ and $C^{\perp}$ are said to be *equivalent*. Hence the weights in $\widetilde{C}$ and $C^{\perp}$ are identical.

Let $\mathbb{F}_{q^m}$ denote the degree m extension of $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^m}$ be a primitive element. This means that α generates the multiplicative group $\mathbb{F}_{q^m}^*$ or equivalently α is a primitive n^{th} root of unity. Note that the roots of $g(x)$ are powers of α. Suppose that $g(x)$ factors into irreducible polynomials over $\mathbb{F}_q$ as

$$g(x) = m_{\alpha^{i_1}}(x) \cdots m_{\alpha^{i_s}}(x), \tag{1.1}$$

where $m_{\alpha^{i_j}}(x) \in \mathbb{F}_q[x]$ denotes the minimal polynomial of α^{i_j} over $\mathbb{F}_q$. In this case, the other roots of $g(x)$ are obtained from $\alpha^{i_1}, ..., \alpha^{i_s}$ by raising to q^{th} powers. Namely, the roots of $g(x)$ are

$$\begin{matrix} \alpha^{i_1}, & \alpha^{qi_1}, & \dots & ,\alpha^{q^{d_1-1}i_1} \\ & & \vdots & \\ \alpha^{i_s}, & \alpha^{qi_s}, & \dots & ,\alpha^{q^{d_s-1}i_s} \end{matrix} \tag{1.2}$$

where $d_j = \deg(m_{\alpha^{i_j}})$ for all $1 \leq j \leq s$. It's clear that the generator polynomial $g(x)$ of C, hence the code C itself, can be described by listing all the roots of $g(x)$ as in (1.2) or just one root of each irreducible factor.

Definition 1.9. Let C be a q-ary cyclic code of length $n = q^m - 1$ with the generator polynomial as in (1.1). Then:

(i) The set $Z(C)$ defined by (1.2) is called the *zero set* of C,

(i) *A basic zero set* of C is defined by

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

Note that one can write different basic zero sets for C by changing the roots of each irreducible factor in the generator polynomial.

A classical problem in coding theory is to determine the minimum distance of a given family of codes. This is in general a difficult problem. Therefore one is also satisfied if one can find general bounds. In the case of cyclic codes, the following bound is simple and very well-known.

Theorem 1.10 (BCH Bound)**.** *Let C be a cyclic code of length n over $\mathbb{F}_q$ and α be a primitive n^{th} root of unity. If $Z(C)$ contains $\delta - 1$ consecutive powers $\alpha^b, \alpha^{b+1}, ..., \alpha^{b+\delta-2}$ of α, then $d(C) \geq \delta$.*

We need a well-known fact for the proof of the BCH bound. Let $\alpha_1, ..., \alpha_s$ be elements in a field $\mathbb{F}$. The $s \times s$ matrix $V = [v_{i,j}]$, where $v_{i,j} = \alpha_j^{i-1}$ is called a *Vandermonde matrix.*

$$V = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_s \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_s^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{s-1} & \alpha_2^{s-1} & \dots & \alpha_s^{s-1} \end{pmatrix}$$

Lemma 1.11. *We have* $\det(V) = \prod_{1 \leq i < j \leq s} (\alpha_j - \alpha_i)$*. In particular, V is nonsingular if the elements $\alpha_1, ..., \alpha_s$ are distinct.*

Proof of Theorem 1.10. Let $c(x)$ be a nonzero codeword in C of weight w, and let

$$c(x) = \sum_{j=1}^{w} c_{i_j} x^{i_j}\ , \qquad c_{i_j} \neq 0 \ \ \forall j.$$

Assume to the contrary that $w < \delta$. By assumption $c(\alpha^l) = 0$ for $b \leq l \leq b + \delta - 2$,

$$\begin{aligned} c(\alpha^b) &= c_{i_1}\alpha^{bi_1} + c_{i_2}\alpha^{bi_2} + ... + c_{i_w}\alpha^{bi_w} = 0 \\ c(\alpha^{b+1}) &= c_{i_1}\alpha^{(b+1)i_1} + c_{i_2}\alpha^{(b+1)i_2} + ... + c_{i_w}\alpha^{(b+1)i_w} = 0 \\ &\vdots \\ c(\alpha^{b+\delta-2}) &= c_{i_1}\alpha^{(b+\delta-2)i_1} + c_{i_2}\alpha^{(b+\delta-2)i_2} + ... + c_{i_w}\alpha^{(b+\delta-2)i_w} = 0. \end{aligned}$$

Then we have $Au = 0$, where

$$A = \begin{pmatrix} \alpha^{bi_1} & \alpha^{bi_2} & \dots & \alpha^{bi_w} \\ \alpha^{(b+1)i_1} & \alpha^{(b+1)i_2} & \dots & \alpha^{(b+1)i_w} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(b+w-1)i_1} & \alpha^{(b+w-1)i_2} & \dots & \alpha^{(b+w-1)i_w} \end{pmatrix}$$

and

$$u = \begin{pmatrix} c_{i_1} \\ c_{i_2} \\ \vdots \\ c_{i_w} \end{pmatrix}.$$

Since $u \neq 0$, A is a singular matrix and hence $\det A = 0$. But $\det A = \alpha^{(i_1+i_2+\ldots+i_w)b} \det V$, where V is the Vandermonde matrix

$$V = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_w} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{i_1(w-1)} & \alpha^{i_2(w-1)} & \dots & \alpha^{i_w(w-1)} \end{pmatrix}$$

Since α^{i_j} are distinct, $\det V \neq 0$ and this yields a contradiction. □

1.2 Trace Representation of Cyclic Codes and Wolfmann's Bound

We start by introducing an important function.

Definition 1.12. The map defined by

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$$
$$a \mapsto a + a^q + \ldots + a^{q^{m-1}}$$

is called the *trace map.*

We will denote this map simply by Tr unless otherwise stated. It is easy to see that the trace map is an $\mathbb{F}_q$-linear surjection. The following theorem is important and will be useful for our purposes.

Theorem 1.13 (Hilbert's Theorem 90)**.** *For $m > 1$ and $a \in \mathbb{F}_{q^m}$, we have that*

$$Tr(a) = 0 \text{ if and only if there exists } b \in \mathbb{F}_{q^m} \text{ such that } b^q - b = a.$$

Proof. ($\Leftarrow$) If there exists $b \in \mathbb{F}_{q^m}$ with $b^q - b = a$ then

$$\begin{aligned} Tr(a) &= Tr(b^q - b) \\ &= (b^q - b) + (b^q - b)^q + ... + (b^q - b)^{q^{m-1}} \\ &= b^{q^m} - b = 0, \quad \text{since } b \in \mathbb{F}_{q^m}. \end{aligned}$$

($\Rightarrow$) Let $a \in \mathbb{F}_{q^m}$ with $Tr(a) = 0$ and let b be a root of the polynomial

$$f(x) = x^q - x - a \ \in \mathbb{F}_{q^m}[x]$$

in some extension of $\mathbb{F}_q$. The same calculation above shows that such b is an element of $\mathbb{F}_{q^m}$. □

There are two common ways to construct a code over $\mathbb{F}_q$ from a given code over $\mathbb{F}_{q^m}$.

Definition 1.14. Let D be a linear code of length n over $\mathbb{F}_{q^m}$.

(*i*) The *restriction* of D to $\mathbb{F}_q$ is defined by

$$\begin{aligned} D|_{\mathbb{F}_q} &:= \{c = (c_1, ..., c_n) \in D \mid c_i \in \mathbb{F}_q \text{ for all } i\} \\ &= D \cap \mathbb{F}_q^n. \end{aligned}$$

(*ii*) The *trace code* of D is defined by

$$Tr(D) := \big\{\big(Tr(c_1), ..., Tr(c_n)\big) \mid (c_1, ..., c_n) \in D\big\}.$$

Note that both the restriction and the trace codes are $\mathbb{F}_q$-linear. The following theorem relates these two codes in a nontrivial way.

Theorem 1.15 (Delsarte)**.** *For any code C over $\mathbb{F}_{q^m}$, we have $(C|_{\mathbb{F}_q})^\perp = Tr(C^\perp)$.*

Proof. Let $\cdot$ denote the canonical inner product on both $\mathbb{F}_q^n$ and $\mathbb{F}_{q^m}^n$. In order to prove $(C|_{\mathbb{F}_q})^\perp \supseteq Tr(C^\perp)$ we need to show that

$$u \cdot Tr(v) = 0 \ \text{ for all } u \in C|_{\mathbb{F}_q} \ \text{ and } \ v \in C^\perp. \tag{1.3}$$

Write $u = (u_1, ..., u_n)$ and $v = (v_1, ..., v_n)$; then

$$u \cdot Tr(v) = \sum_{i=1}^{n} u_i \cdot Tr(v_i) = Tr\big(\sum_{i=1}^{n} u_i v_i\big) = Tr\big(u \cdot v\big) = Tr(0) = 0.$$

Here we obtained the result by using $\mathbb{F}_q$-linearity of the trace and the fact that $u \cdot v = 0$ (since $u \in C$ and $v \in C^\perp$). Therefore we have proved (1.3). Now we show that $(C|_{\mathbb{F}_q})^\perp \subseteq Tr(C^\perp)$. This statement is equivalent to

$$Tr(C^\perp)^\perp \subseteq C|_{\mathbb{F}_q}. \tag{1.4}$$

Suppose to the contrary that (1.4) does not hold. Then there exists some $a \in Tr(C^\perp)^\perp \backslash C$, hence an element $b \in C^\perp$ with $a \cdot b \neq 0$. Since $Tr : \mathbb{F}_{q^m} \to \mathbb{F}_q$ is not the zero map, there is an element $\gamma \in \mathbb{F}_{q^m}$ such that $Tr\big(\gamma(a \cdot b)\big) \neq 0$. Then we obtain

$$a \cdot Tr(\gamma b) = Tr(a \cdot \gamma b) = Tr\big(\gamma(a \cdot b)\big) \neq 0.$$

But also we know $a \cdot Tr(\gamma b) = 0$ because $a \in Tr(C^\perp)^\perp$ and $\gamma b \in C^\perp$. So we get a contradiction and this gives (1.4). □

Next, we present a trace representation for an arbitrary cyclic code. We denote by $\Big(Tr\big(a(x)\big)\Big)_{x \in \mathbb{F}^*_{q^m}}$ a vector of length $q^m - 1$ over $\mathbb{F}_q$ which is defined by

$$\Big(Tr\big(a(x)\big)\Big)_{x \in \mathbb{F}^*_{q^m}} = \Big(Tr\big(a(\alpha^0)\big), Tr\big(a(\alpha^1)\big), ..., Tr\big(a(\alpha^{q^m-2})\big)\Big).$$

Theorem 1.16. *Let $m > 1$ and C be a q-ary cyclic code of length $n = q^m - 1$. Let α be a primitive element of $\mathbb{F}_{q^m}$ and $\{\alpha^{i_1}, \alpha^{i_2}, ..., \alpha^{i_s}\}$ be a basic zero set of the code C, where $i_j > 0$ for all j. Then*

$$C^\perp = \big\{\big(Tr(\lambda_1 x^{i_1} + \lambda_2 x^{i_2} + ... + \lambda_s x^{i_s})\big)_{x \in \mathbb{F}^*_{q^m}} \mid \lambda_1, ..., \lambda_s \in \mathbb{F}_{q^m}\big\}.$$

Proof. We know that C is an ideal in $\mathbb{F}_q[x]/(x^n - 1)$ and

$$C = \big\langle m_{\alpha^{i_1}}(x) m_{\alpha^{i_2}}(x) \cdots m_{\alpha^{i_s}}(x)\big\rangle,$$

where $m_{\alpha^{i_j}}(x)$ is the minimal polynomial of α^{i_j} over $\mathbb{F}_q$, for all j. Let D be the code over $\mathbb{F}_{q^m}$ of the same length with the zero set $Z(D) = \{\alpha^{i_1}, \alpha^{i_2}, ..., \alpha^{i_s}\}$, i.e.

$$D = \big\langle (x - \alpha^{i_1})(x - \alpha^{i_2}) \cdots (x - \alpha^{i_s})\big\rangle \subset \mathbb{F}_{q^m}[x]/(x^n - 1).$$

Then $C = D|_{\mathbb{F}_q}$ and by Delsarte's Theorem we have $C^\perp = Tr(D^\perp)$.

Let $d(x) = \sum_{i=0}^{n-1} d_i x^i$ be any codeword in D. Then we have $d(\alpha^{i_j}) = 0$, for all $j = 1, ..., s$. We can also write these equalities by using the usual inner product in n-space as follows:

$$\big(d_0, d_1, ..., d_{n-1}\big) \cdot \big(1, (\alpha^{i_1})^1, ..., (\alpha^{i_1})^{n-1}\big) = 0$$

$$\big(d_0, d_1, ..., d_{n-1}\big) \cdot \big(1, (\alpha^{i_2})^1, ..., (\alpha^{i_2})^{n-1}\big) = 0$$

$$\vdots$$

$$\big(d_0, d_1, ..., d_{n-1}\big) \cdot \big(1, (\alpha^{i_s})^1, ..., (\alpha^{i_s})^{n-1}\big) = 0.$$

By vector representation of cyclic codes, this implies that the following vectors are codewords in $D^{\perp}$:

$$\begin{aligned} u_1 &= (1, (\alpha^1)^{i_1}, ..., (\alpha^{n-1})^{i_1}) \\ u_2 &= (1, (\alpha^1)^{i_2}, ..., (\alpha^{n-1})^{i_2}) \\ &\vdots \\ u_s &= (1, (\alpha^1)^{i_s}, ..., (\alpha^{n-1})^{i_s}). \end{aligned}$$

The generator polynomial of D yields that the $\mathbb{F}_{q^m}$-dimension of $D^{\perp}$ is s. We want to show that $\{u_1, ..., u_s\}$ forms an $\mathbb{F}_{q^m}$-basis for $D^{\perp}$. Since α is a primitive element of $\mathbb{F}_{q^m}$, $1, \alpha, \alpha^q, ..., \alpha^{q^m-2}$ are all elements in $\mathbb{F}^*_{q^m}$. So, we can represent each u_j in a different way as follows;

$$u_j = (x^{i_j})_{x \in \mathbb{F}^*_{q^m}}, \qquad j = 1, 2, ..., s$$

The notation here is similar to the one introduced before the statement of this theorem. Suppose that $\sum_{j=1}^{s} \delta_j u_j = 0$ for some $\delta_j \in \mathbb{F}_{q^m}$. This means that

$$\delta_1 x^{i_1} + \delta_2 x^{i_2} + ... + \delta_s x^{i_s} = 0 \qquad \text{for all } \ x \in \ \mathbb{F}_{q^m}.$$

Since $i_j < q^m$ for all j, this is possible if $\delta_1 = ... = \delta_s = 0$. This proves that $\{u_1, ..., u_s\}$ forms a basis for $D^{\perp}$. Therefore $D^{\perp}$ is of the form

$$D^{\perp} = \langle u_1, ..., u_s \rangle = \{ \sum_{j=1}^{s} \lambda_j u_j \mid \ \ \lambda_j \in \mathbb{F}_{q^m} \},$$

or

$$D^{\perp} = \{ (\lambda_1 x^{i_1} + ... + \lambda_s x^{i_s})_{x \in \mathbb{F}^*_{q^m}} \ : \ \lambda_1, ..., \lambda_s \in \mathbb{F}_{q^m} \}$$

Hence,

$$C^{\perp} = Tr(D^{\perp}) = \{ \big(Tr(\lambda_1 x^{i_1} + ... + \lambda_s x^{i_s}) \big)_{x \in \mathbb{F}^*_{q^m}} \ : \ \lambda_1, ..., \lambda_s \in \mathbb{F}_{q^m} \}.$$

□

Consider a codeword c of the cyclic code C in Theorem 1.16.
Suppose that

$$c = \Big(Tr(\lambda_1 x^{i_1} + ... + \lambda_s x^{i_s}) \Big)_{x \in \mathbb{F}^*_{q^m}}$$

for some $\lambda_1, ..., \lambda_s \in \mathbb{F}_{q^m}$. Set $f(x) := \lambda_1 x^{i_1} + ... + \lambda_s x^{i_s}$. By Hilbert's Theorem 90, we have that for any $x_0 \in \mathbb{F}_{q^m}$ with $Tr(f(x_0)) = 0$, there exists $y_0 \in \mathbb{F}_{q^m}$ such that

$$y_0^q - y_0 = f(x_0).$$

Note that for any $a \in \mathbb{F}_q$, we also have

$$\begin{aligned}(y_0 + a)^q - (y_0 + a) &= y_0^q - y_0 + (a^q - a)\\ &= y_0^q - y_0\\ &= f(x_0).\end{aligned}$$

Therefore, for each $x_0 \in \mathbb{F}_{q^m}$ with $Tr(f(x_0)) = 0$, there exist q distinct $y_0 \in \mathbb{F}_{q^m}$ with

$$y_0^q - y_0 = f(x_0).$$

Hence,

$$\begin{aligned} w(c) &= (q^m - 1) - \big|\{x_0 \in \mathbb{F}_{q^m}^* \ ; \ Tr(f(x_0)) = 0\}\big| \\ &= (q^m - 1) - \tfrac{N-q}{q} \\ &= q^m - \tfrac{N}{q} \end{aligned} \tag{1.5}$$

where N denotes the number of solutions $(x_0, y_0) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$ to the equation

$$y^q - y = f(x). \tag{1.6}$$

An equation of the form (1.6) is said to define an *Artin-Schreier (A-S) curve* over $\mathbb{F}_{q^m}$ and N is called the *number of affine* $\mathbb{F}_{q^m}$*- rational points* of this curve. Hence, weights of codewords in C are related to the number of affine $\mathbb{F}_{q^m}$- rational points of members in the following Artin-Schreier family $\mathcal{F}$ consisting of equations of the form

$$y^q - y = \lambda_1 x^{i_1} + ... + \lambda_s x^{i_s}$$

where $\lambda_1, ..., \lambda_s$ are arbitrary elements in $\mathbb{F}_{q^m}$.

Theorem 1.17. *Let X be an A-S curve over $\mathbb{F}_{q^m}$ defined by $y^q - y = f(x)$, where $f(x) \in \mathbb{F}_{q^m}[x]$ and $\big(\deg(f), q\big) = 1$.*

(*i*) *The genus of X is*

$$g = \frac{1}{2}(q-1)\big(\deg(f) - 1\big). \quad \text{(See [2], Example 2.4.)}$$

(*ii*) *(Hasse-Weil). The number N of affine $\mathbb{F}_{q^m}$-rational points of X satisfies*

$$N \leq q^m + 2gq^{\frac{m}{2}}. \quad \text{(See [5], Theorem 5.2.3.)}$$

Using the trace representation and the Hasse-Weil Theorem, we obtain the following bound on the minimum distance.

Theorem 1.18 (Wolfmann, [6])**.** *Let C be a q-ary cyclic code of length $n = q^m - 1$ whose dual's basic zero set is*

$$BZ(C^\perp) = \{\alpha^{i_1}, \cdots, \alpha^{i_s}\},$$

where α is a primitive n^{th} root of unity and $1 \leq i_1 < ... < i_s$ are integers that are relatively prime to q. Then,

$$d(C) \geq q^m - q^{m-1} - (q-1)(i_s - 1)q^{\frac{m}{2}-1}.$$

Proof. Let w be any nonzero weight in C. Then by (1.5) and (1.6), we have

$$w = q^m - \frac{N}{q},$$

where N is the number of affine $\mathbb{F}_{q^m}$-rational points of the curve defined by

$$y^q - y = f(x) = \lambda_1 x^{i_1} + ... + \lambda_s x^{i_s}. \tag{1.7}$$

By Hasse-Weil bound

$$N \leq q^m + 2gq^{\frac{m}{2}}.$$

Hence

$$q^m - \frac{N}{q} \geq q^m - q^{m-1} - 2gq^{\frac{m}{2}-1}.$$

To estimate the minimal weight (minimum distance), we consider the curve in the form (1.7) with the largest genus. The largest genus is (by Theorem 1.17 (i))

$$\frac{(q-1)(i_s-1)}{2}.$$

Hence, the result follows. □

Example 1.19. Let $q^m = 2^5$ and ξ be a primitive element of $\mathbb{F}_{32}$. When we factor $x^{31}-1$ into irreducible polynomials over $\mathbb{F}_2$, we get the following irreducible polynomials and corresponding roots in $\mathbb{F}_{32}$.

$$\begin{aligned}
x+1 &: 1 \\
x^5+x^2+1 &: \xi, \xi^2, \xi^4, \xi^8, \xi^{16} \\
x^5+x^3+1 &: \xi^{15}, \xi^{23}, \xi^{27}, \xi^{29}, \xi^{30} \\
x^5+x^3+x^2+x+1 &: \xi^7, \xi^{14}, \xi^{19}, \xi^{25}, \xi^{28} \\
x^5+x^4+x^2+x+1 &: \xi^5, \xi^9, \xi^{10}, \xi^{18}, \xi^{20} \\
x^5+x^4+x^3+x+1 &: \xi^{11}, \xi^{13}, \xi^{21}, \xi^{22}, \xi^{26} \\
x^5+x^4+x^3+x^2+1 &: \xi^3, \xi^6, \xi^{12}, \xi^{17}, \xi^{24}.
\end{aligned}$$

Let C be the binary code of length 31 whose generator polynomial is

$$g(x) = (x^5 + x^3 + 1)(x^5 + x^3 + x^2 + x + 1)(x^5 + x^4 + x^2 + x + 1)(x^5 + x^4 + x^3 + x + 1).$$

Then, $C^{\perp}$ is equivalent to the cyclic code $\widetilde{C}$ with the generator polynomial $h(x) = (x + 1)(x^5 + x^2 + 1)(x^5 + x^4 + x^3 + x^2 + 1)$, and $BZ(\widetilde{C}) = \{1, \xi, \xi^3\}$ (cf. Remark 1.8). Then by Theorem 1.18, we get the following inequality.

$$\begin{aligned} d(C) \geq & 2^5 - 2^4 - (2-1)(3-1)2^{\frac{5}{2}-1} \\ \sim & 16 - 2(2,8) \\ \sim & 10,4. \end{aligned}$$

Hence $d(C) \geq 11$. On the other hand we get $d(C) \geq 7$ by applying the BCH Bound, since $Z(C)$ contains 6 consecutive powers $\xi^{18}, \xi^{19}, ..., \xi^{23}$. So, Wolfmann's bound performs better than the BCH bound in this example.

Next let $q^m = 3^3$ and ζ be a primitive element of $\mathbb{F}_{27}$. In this case we have 10 irreducible factors of $x^{26} - 1$ over $\mathbb{F}_3$ and corresponding roots in $\mathbb{F}_{27}$ as follows:

$$\begin{aligned} x + 1 &: 2 \\ x + 2 &: 1 \\ x^3 + 2x + 1 &: \zeta, \zeta^3, \zeta^9 \\ x^3 + 2x + 2 &: \zeta^{14}, \zeta^{16}, \zeta^{22} \\ x^3 + x^2 + 2 &: \zeta^4, \zeta^{10}, \zeta^{12} \\ x^3 + x^2 + x + 2 &: \zeta^2, \zeta^6, \zeta^{18} \\ x^3 + x^2 + 2x + 1 &: \zeta, \zeta^3, \zeta^9 \\ x^3 + 2x^2 + 1 &: \zeta^{17}, \zeta^{23}, \zeta^{25} \\ x^3 + 2x^2 + x + 1 &: \zeta^5, \zeta^{15}, \zeta^{19} \\ x^3 + 2x^2 + 2x + 2 &: \zeta^8, \zeta^{20}, \zeta^{24} \end{aligned}$$

Let C be the 3-ary cyclic code of length 26 with the generator polynomial

$$g(x) = (x + 1)(x + 2)(x^3 + 2x + 2)(x^3 + x^2 + 2x + 1)(x^3 + 2x^2 + 1)(x^3 + 2x^2 + 2x + 2)$$

Arguing as above, we obtain

$$\begin{aligned} d(C) \geq & 3^3 - 3^2 - (3-1) \cdot (5-1)3^{\frac{3}{2}-1} \\ \geq & 5. \end{aligned}$$

For the same code, the BCH bound yields $d(C) \geq 6$ since there are 5 consecutive powers $\zeta^{20}, \zeta^{21}, ..., \zeta^{24}$ in $Z(C)$. This time the BCH bound performs better than Wolfmann's bound.

1.3 Permutation Polynomials Over Finite Fields

Definition 1.20. A polynomial $f \in \mathbb{F}_q[x]$ is said to be a *permutation polynomial* if the associated function $f : c \mapsto f(c)$ from $\mathbb{F}_q$ into $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$.

The following statement characterizes permutation monomials. The proof is immediate.

Proposition 1.21. *The monomial x^n is a permutation polynomial of $\mathbb{F}_q$ if and only if* $\gcd(n, q-1) = 1$.

Permutation polynomials other than monomials are not as easy to find. We will use the following theorem of Zieve ([7], Theorem 1.2) in the next chapter. Note that μ_d denotes the set of d^{th} roots of unity in the algebraic closure of $\mathbb{F}_q$.

Theorem 1.22. *Let d, r be positive integers and $d|(q-1)$. Assume that $q = q_0^m$ satisfies $q_0 \equiv 1$ (mod d) and $d|m$. Let $h \in \mathbb{F}_{q_0}[x]$. Then $f(x) := x^r h(x^{(q-1)/d})$ permutes $\mathbb{F}_q$ if and only if* $\gcd(r, (q-1)/d) = 1$ *and h has no roots in μ_d.*

We need the following lemma and corollary in order to prove this theorem.

Lemma 1.23. *Let d, r be positive integers with $d|(q-1)$, and let $h \in \mathbb{F}_q[x]$. Then $f(x) := x^r h(x^{(q-1)/d})$ permutes $\mathbb{F}_q$ if and only if both*

(1) $\gcd(r, (q-1)/d) = 1$ *and*

(2) $x^r h(x)^{(q-1)/d}$ *permutes μ_d.*

Proof. ($\Rightarrow$) Let $(q-1)/d = s$. Firstly, we want to show that if f permutes $\mathbb{F}_q$ then $\gcd(r, s) = 1$. Let $\beta \in \mu_s$ be a primitive s^{th} root of unity and assume that $\gcd(r, s) = k > 1$. Then we have

$$f(\beta^{\frac{s}{k}} x) = \beta^{\frac{sr}{k}} f(x) = f(x),$$

unless $k = 1$, $\beta^{\frac{s}{k}} \neq 1$. Hence we obtain $f(\beta^{\frac{s}{k}} x) = f(x)$ with $\beta^{\frac{s}{k}} x \neq x$. Therefore f is not one-to-one and this contradicts the assumption that f permutes $\mathbb{F}_q$.

Observe that

$$\begin{array}{rccc} \varphi : & \mathbb{F}_q^* & \longrightarrow & \mu_d \\ & x & \longmapsto & x^s \end{array} \tag{1.8}$$

is a multiplicative homomorphism since $(x^s)^d = x^{q-1} = 1$. We have $\mathrm{Ker}(\varphi) = \{x \in \mathbb{F}_q^* \mid x^s = 1\} = \mu_s$, and hence

$$\mathbb{F}_q^*/\mu_s \simeq \mu_d.$$

In particular, $\mu_d = (\mathbb{F}_q^*)^s$. Set $g(x) = x^r h(x)^s$ and note that for $\gamma \in \mu_d$, we have

$$g(\gamma)^d = \gamma^{rd} h(\gamma)^{sd} = h(\gamma)^{q-1} = 1, \tag{1.9}$$

unless $h(\gamma) = 0$. Let $\gamma = \delta^s$ for $\delta \in \mathbb{F}_q^*$ and note that if $h(\gamma) = h(\delta^s) = 0$, then $f(\delta) = 0$ for $\delta \neq 0$. However, $f(0) = 0$ as well, and this contradicts the assumption that f permutes $\mathbb{F}_q^*$. So, $h(\gamma) \neq 0$ for any $\gamma \in \mu_d$ and by (1.8), g sends μ_d to μ_d.

It is left to show that g permutes μ_d. We have $f(x)^s = x^{rs} h(x^s)^s = g(x^s)$ and since $f(x)$ takes all values in $\mathbb{F}_q^*$ then $g(x^s) = f(x)^s$ also takes all values in $(\mathbb{F}_q^*)^s = \mu_d$. Hence $g(x)$ is onto on μ_d.

($\Leftarrow$) Note that

$$f(x)^s = x^{rs} h(x^s)^s = g(x^s).$$

Hence, $Im(f(x)^s) = Im(g(x^s))$. Since $(\mathbb{F}_q^*)^s = \mu_d$ and g permutes μ_d, we obtain that $Im(f(x)^s) = \mu_d$. This implies that $Im(f(x))$ consists of the s^{th} roots of elements in μ_d and there are $ds = q-1$ such roots. Hence, $|Im(f(x))| = q-1$, which means f is a permutation polynomial of $\mathbb{F}_q$. □

Corollary 1.24. *Choose $d, r, n > 0$ with $d|(q-1)$, and let $h \in \mathbb{F}_q[x]$. Assume $h(\zeta)^{(q-1)/d} = \zeta^n$ for all $\zeta \in \mu_d$. Then $f(x) := x^r h(x^{(q-1)/d})$ permutes $\mathbb{F}_q$ if and only if $gcd(r+n, d) = gcd(r, (q-1)/d) = 1$*

Proof. ($\Rightarrow$) Suppose $f(x) := x^r h(x^{(q-1)/d})$ permutes $\mathbb{F}_q$. Then by the above lemma we know that $\gcd(r, \frac{q-1}{d}) = 1$. We also know by the same lemma that $g(x) = x^r h(x)^s$ permutes μ_d. By assumption, we have

$$g(\zeta) = \zeta^r h(\zeta)^s = \zeta^{r+n}, \quad \text{for any } \zeta \in \mu_d.$$

So, for $g(x)$ to permute μ_d we must have $gcd(r+n, d) = 1$.

($\Leftarrow$) It is enough to show that $g(x) = x^r h(x)^s$ permutes μ_d. Let ζ be any element in μ_d. Then $g(\zeta) = \zeta^r h(\zeta)^s = \zeta^{r+n}$ permutes μ_d since $\gcd(r+n, d) = 1$. □

Now, we can prove Theorem 1.22.

Proof of Theorem 1.22. ($\Leftarrow$) Since $q_0 \equiv 1 \pmod{d}$, we have

$$\frac{q_0^d - 1}{q_0 - 1} = \sum_{i=0}^{d-1} q_0^i = \underbrace{q_0^{d-1} + q_0^{d-2} + \ldots + 1}_{1+1+\ldots+1=d.1} \equiv 0 \pmod{d}. \tag{1.10}$$

Since $d \mid m$, we can write $m = de$, for $e \in \mathbb{Z}^+$. Then,

$$q_0^m - 1 = q_0^{de} - 1 = (q_0^d - 1)(q_0^{(e-1)d} + q_0^{(e-2)d} + \ldots + q_0 + 1).$$

Hence, $(q_0^d - 1) \mid (q_0^m - 1) = q - 1$ and this implies $(q_0^d - 1)/d \mid (q_0^m - 1)/d = (q-1)/d$. We know $(q_0 - 1) \mid (q_0^d - 1)/d$ follows from (1.10). Then the hypothesis $d \mid (q_0 - 1)$ implies $d \mid (q - 1/d)$. Since $\gcd(r, (q-1)/d) = 1$, this yields $\gcd(r, d) = 1$.

Let $\zeta \in \mu_d$. Since $d \mid q_0 - 1$, we have $\zeta^{q_0 - 1} = 1$. So $\zeta^{q_0} = \zeta$ and this means $\zeta \in \mathbb{F}_{q_0}$. Therefore, we conclude that $h(\zeta) \in \mathbb{F}_{q_0}$. Now, suppose ζ is not a root of $h(x)$. By previous computations we know $(q_0 - 1) | (q-1)/d$, which yields $h(\zeta)^{(q-1)/d} = 1$. By Corollary 1.24 with $n = d$, we have $h(\zeta)^{(q-1)/d} = \zeta^d = 1$ for every $\zeta \in \mu_d$. Also, we have $\gcd(r, d) = 1$. Then $\gcd(r + d, d) = 1$ and the result follows from Corollary 1.24.
($\Rightarrow$) It follows from Lemma 1.23 that $\gcd(r, s) = 1$. The same lemma also implies that $g(x) = x^r h(x)^s$ permutes μ_d. Suppose that $h(\gamma) = 0$ for some $\gamma \in \mu_d$. Then,

$$g(\gamma) = \gamma^r h(\gamma)^s = 0,$$

which contradicts the permutation property of $g(x)$. So, h can not have a root in μ_d.

Example 1.25. Let $q = 64$ and ξ be a primitive element in $\mathbb{F}_{64}$ which is a root of

$$x^6 + x^4 + x^3 + x + 1 \quad \text{(minimal polynomial)}.$$

Consider $q_0 = 4$ and $m = 3$ in Theorem 1.22. It is easy to see that $d = 3$ since d should satisfy $d|3$ and also $4 \equiv 1 \pmod{d}$. Now we need to select $h(x) \in \mathbb{F}_4[x]$ such that h has no root in $\mu_3 = \{1, \xi^{21}, \xi^{42}\}$. The polynomial $h(x) = x^2 + x + \xi^{21}$ satisfies this condition. If we pick r with $\gcd(r, 21) = 1$, then by Theorem 1.22 we obtain the following 36 permutation polynomials over $\mathbb{F}_{64}$:

$$\begin{array}{ccc}
x^{43} + x^{22} + \xi^{21}x & x^{43} + \xi^{21}x^{22} + x & \xi^{21}x^{43} + x^{22} + x \\
x^{44} + x^{23} + \xi^{21}x^{2} & x^{44} + \xi^{21}x^{23} + x^{2} & \xi^{21}x^{44} + x^{23} + x^{2} \\
x^{46} + x^{25} + \xi^{21}x^{4} & x^{46} + \xi^{21}x^{25} + x^{4} & \xi^{21}x^{46} + x^{25} + x^{4} \\
x^{47} + x^{26} + \xi^{21}x^{5} & x^{47} + \xi^{21}x^{26} + x^{5} & \xi^{21}x^{47} + x^{26} + x^{5} \\
x^{50} + x^{29} + \xi^{21}x^{8} & x^{50} + \xi^{21}x^{29} + x^{8} & \xi^{21}x^{50} + x^{29} + x^{8} \\
x^{52} + x^{31} + \xi^{21}x^{10} & x^{52} + \xi^{21}x^{31} + x^{10} & \xi^{21}x^{52} + x^{31} + x^{10} \\
x^{53} + x^{32} + \xi^{21}x^{11} & x^{53} + \xi^{21}x^{32} + x^{11} & \xi^{21}x^{53} + x^{32} + x^{11} \\
x^{55} + x^{34} + \xi^{21}x^{13} & x^{55} + \xi^{21}x^{34} + x^{13} & \xi^{21}x^{55} + x^{34} + x^{13} \\
x^{58} + x^{37} + \xi^{21}x^{16} & x^{58} + \xi^{21}x^{37} + x^{16} & \xi^{21}x^{58} + x^{37} + x^{16} \\
x^{59} + x^{38} + \xi^{21}x^{17} & x^{59} + \xi^{21}x^{38} + x^{17} & \xi^{21}x^{59} + x^{38} + x^{17} \\
x^{61} + x^{40} + \xi^{21}x^{19} & x^{61} + \xi^{21}x^{40} + x^{19} & \xi^{21}x^{61} + x^{40} + x^{19} \\
x^{62} + x^{41} + \xi^{21}x^{20} & x^{62} + \xi^{21}x^{41} + x^{20} & \xi^{21}x^{62} + x^{41} + x^{20}
\end{array}$$

2

Improvements on Wolfmann's Bound

In this chapter we use permutation polynomials to modify Artin-Schreier curves related to weights of codewords in cyclic codes. Our hope is to lower the genus of the related curves, improve the Hasse-Weil bound and hence improve the Wolfmann's minimum distance estimate in some cases. We carry out some experiments using the computer algebra software Magma [1]. Section 1 explains the method and presents an example in which the related Magma code is provided Section 2 has some examples where the performance of the method is given. We finish with concluding remarks in Section 3.

2.1 Substitution / Reduction Method

Let C be a q-ary cyclic code of length $n = q^m - 1$. For a primitive element α of $\mathbb{F}_{q^m}$, let

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

where $0 < i_1 < ... < i_s$. Then, an arbitrary codeword $c \in C$ has the form

$$c = \big(Tr(\lambda_1 x^{i_1} + ... + \lambda_s x^{i_s})\big)_{x \in \mathbb{F}_{q^m}^*} \tag{2.1}$$

for some $\lambda_1, ..., \lambda_s \in \mathbb{F}_{q^m}$. (cf. Theorem 1.16). Recall that the weight of c is related to the Artin-Schreier curve defined by

$$y^q - y = \lambda_1 x^{i_1} + ... + \lambda_s x^{i_s}. \qquad \big(\text{cf. (1.5) and (1.6)}\big)$$

Moreover, Wolfmann's bound (Theorem 1.18) estimates the weight $w(c)$ in terms of the degree i_s of the polynomial

$$f_c(x) = \lambda_1 x^{i_1} + ... + \lambda_s x^{i_s}. \tag{2.2}$$

If $p(x) \in \mathbb{F}_{q^m}[x]$ is a permutation polynomial with $p(0) = 0$, then $p(x)$ permutes the elements of $\mathbb{F}_{q^m}^*$. Hence, if we substitute $p(x)$ in place of x in the trace representation (2.1), the resulting vector of length n will be different than c but its weight will be the same as $w(c)$. What we do by this substitution is nothing but shuffling the coordinates of c.

Let us denote the polynomial $f_c\big(p(x)\big)$ by $\overline{f_c}(x)$. Clearly $\deg \overline{f_c}(x) > \deg f_c(x)$ if $\deg p(x) > 1$. Let $\widetilde{f_c}(x)$ be the polynomial obtained from $\overline{f_c}(x)$ by reduction modulo $x^n - 1$. Note that the value sets of $\widetilde{f_c}(x)$ and $\overline{f_c}(x)$ are identical on $\mathbb{F}_{q^m}^*$. Therefore, the vector

$$\widetilde{c} = \big(Tr(\widetilde{f_c}(x))\big)_{x \in \mathbb{F}_{q^m}^*}$$

also has the same weight as c. Hence one can estimate the weight of the codeword $c \in C$ by the degrees of $f_c(x)$, $\overline{f_c}(x)$ and $\widetilde{f_c}(x)$. Our hope is that after this reduction, we get

$$\deg \widetilde{f_c}(x) < \deg f_c(x),$$

hence Wolfmann's estimate for $w(c)$ gets better. If such a decrease in degree can be achieved for the trace representation of each codeword $c \in C$, then the minimum distance of the code $d(C)$ can be estimated by a better lower bound than the original bound. We call this method the *substitution - reduction method.*

Let us present this idea by using the following example.

Example 2.1. Let $q^m = 2^6$ and $n = 63$. Let α be a primitive element of $\mathbb{F}_{64}$. Irreducible factors and corresponding roots for $x^{63} - 1$ are as follows :

$$\begin{array}{lcl}
x+1 & : & 1 \\
x^2+x+1 & : & \alpha^{21}, \alpha^{42}, \\
x^3+x+1 & : & \alpha^{9}, \alpha^{18}, \alpha^{36}, \\
x^3+x^2+1 & : & \alpha^{27}, \alpha^{45}, \alpha^{54}, \\
x^6+x+1 & : & \alpha^{5}, \alpha^{10}, \alpha^{17}, \alpha^{20}, \alpha^{34}, \alpha^{40}, \\
x^6+x^3+1 & : & \alpha^{7}, \alpha^{14}, \alpha^{28}, \alpha^{35}, \alpha^{49}, \alpha^{56}, \\
x^6+x^4+x^2+x+1 & : & \alpha^{15}, \alpha^{30}, \alpha^{39}, \alpha^{51}, \alpha^{57}, \alpha^{60}, \\
x^6+x^4+x^3+x+1 & : & \alpha, \alpha^{2}, \alpha^{4}, \alpha^{8}, \alpha^{16}, \alpha^{32}, \\
x^6+x^5+1 & : & \alpha^{23}, \alpha^{29}, \alpha^{43}, \alpha^{46}, \alpha^{53}, \alpha^{58}, \\
x^6+x^5+x^2+x+1 & : & \alpha^{11}, \alpha^{22}, \alpha^{25}, \alpha^{37}, \alpha^{44}, \alpha^{50}, \\
x^6+x^5+x^3+x^2+1 & : & \alpha^{31}, \alpha^{47}, \alpha^{55}, \alpha^{59}, \alpha^{61}, \alpha^{62}, \\
x^6+x^5+x^4+x+1 & : & \alpha^{13}, \alpha^{19}, \alpha^{26}, \alpha^{38}, \alpha^{41}, \alpha^{52}, \\
x^6+x^5+x^4+x^2+1 & : & \alpha^{3}, \alpha^{6}, \alpha^{12}, \alpha^{24}, \alpha^{33}, \alpha^{48}.
\end{array} \tag{2.3}$$

Let C be the binary cyclic code of length 63 whose dual's generator polynomial is

$$h(x) = x^6 + x^4 + x^2 + x + 1.$$

This implies that for $c \in C$, we have

$$c = \big(Tr(\lambda x^{15})\big)_{x \in \mathbb{F}_{64}^*} \tag{2.4}$$

for some $\lambda \in \mathbb{F}_{64}$. With our notation before this example,

$$f_c(x) = \lambda x^{15}.$$

In Example 1.25, we listed some nonmonomial permutation polynomials of $\mathbb{F}_{64}$ which are obtained from Zieve's result. We try each of these permutation polynomials $p(x)$ in our substitution and obtain

$$\widetilde{f_c}(x) = f_c\big(p(x)\big) \pmod{x^{63} - 1}.$$

For each $f_c(x)$ of $\deg(f_c(x)) = 15$ (i.e. $\lambda \neq 0$), the permutation polynomial

$$p(x) = x^{59} + x^{38} + \alpha^{21} x^{17} \in \mathbb{F}_{64}[x]$$

yields $\widetilde{f_c}(x)$ with

$$\deg(\widetilde{f_c}(x)) = 3 < 15 = \deg(f_c(x)).$$

Hence, for all nonzero codewords $c \in C$, Wolfmann's estimate for the weight becomes

$$\begin{aligned} w(c) &\geq 64 - 32 - (3-1)2^{3-1} \\ &= 32 - 8 \\ &= 24 \end{aligned}$$

With the original trace representation (2.4), we had

$$\begin{aligned} w(c) &\geq 64 - 32 - 14 \cdot 4 \\ &= -24 \end{aligned}$$

for all nonzero codewords of C. Hence, substitution/reduction method enables us to conclude

$$d(C) \geq 24.$$

The Magma code that we use to obtain nonmonomial permutation polynomials of $\mathbb{F}_{64}$ in Example 1.25 and to implement substitution/reduction in this example is given below. Part I of the code determines the permutation polynomials and Part II applies substitution / reduction.

```
$Fq := GF(q,m);$
$R < x > := PolynomialRing(Fq);$
$e := PrimitiveElement(Fq);$
$n := q^m - 1;$
$i := 0;$
$S := [\,];$
$I := ideal < R \mid x^n - 1 >;$
$Q < y > := R/I;$
$F := map < R \to Q \mid x :\to x >;$

I
    $h := func < x \mid x^2 + x + e^{21} >;$
    $g := h(x^{21});$
    for $r$ in $[1..n]$ do;
        $if$ $\gcd(r, 21)$ eq 1 then;
            $i := i + 1;$
            $m := (x^r) * g;$
            $s_i := F(m);$
            $Append(\ S, s_i);$
        end if
    end for;

$l := |S|;$

II
    for a,b in $Fq$ do;
        $f := func < x \mid a * x^{23} + b * x^{15} >;$
        $d :=$ deg$(f(x));$
        $u := [a, b];$
        $P := 0;$
        for $i$ in $[1..l]$ do;
            $p_i := S[i];$
            $z := f(p_i);$
            $redz := F(z);$
            $k :=$ deg$(redz);$
            if $k$ $lt$ $d$ then;
                $d := k;$
                $P := p_i;$
            end if;
        end for;

        if $d$ $lt$ deg$(f(x))$ $then;$
            Write("outcome.txt", $f(x)$);
            Write("outcome.txt", deg$(f(x))$);
            Write("outcome.txt", $P$));
            Write("outcome.txt", $d$);
        end if;
    end for;
```

2.2 Examples

We use the substitution / reduction method on certain cyclic codes defined over $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_5$. The length of our codes are determined by the extensions of the fields in which we can find permutation polynomials provided by Zieve's result (Theorem 1.22). We use both monomial and nonmonomial permutation polynomials in the examples. The codes we present have duals with 1 or 2 elements in the basic zero set so that the trace representations contain only 1 or 2 terms and, hence, the computations are feasible.

In the tables, we present the codes by the polynomial $f(x)$ that appear in their trace representations $\big($cf. (2.2)$\big)$. Note that these polynomials also describe the basic zero set of the dual codes. The polynomial obtained after substitution / reduction is denoted by $\widetilde{f}(x)$ as in Section 2.1.

Cyclic Codes over $\mathbb{F}_2$ of Length 63:

Let α be a primitive element of $\mathbb{F}_{64}^*$. The irreducible factors of $x^{63} - 1$ over $\mathbb{F}_2$ were listed in Example 2.1. Monomial pemutations of $\mathbb{F}_{64}$ are obtained by Proposition 1.21 and Zieve type permutations of $\mathbb{F}_{64}$ were listed in Example 2.1.

Case 1 :One Basic Zero for the Dual Code

	Zieve polynomial	$\deg(\widetilde{f})$	monomial	$\deg(\widetilde{f})$
$C_1 : f(x) = \lambda x^{27}$	$x^{47} + x^{26} + \alpha^{21}x^5$	9	x^5	9
$C_2 : f(x) = \lambda x^{15}$	$x^{59} + x^{38} + \alpha^{21}x^{17}$	3	x^{17}	3
$C_3 : f(x) = \lambda x^{23}$	-	-	x^{11}	1
$C_4 : f(x) = \lambda x^{31}$	-	-	x^{61}	1
$C_5 : f(x) = \lambda x^{13}$	-	-	x^{34}	1
$C_6 : f(x) = \lambda x^{5}$	-	-	x^{38}	1

Table 1

For the code C_1, whose dual's basic zero set is $BZ(C_1^\perp) = \{\alpha^{27}\}$ and the dual generator polynomial is $h(x) = x^3 + x^2 + 1$, Wolfmann's bound is

$$d(C_1) \geq 32 - 26 \cdot 4.$$

Since the right-hand side is negative, this estimate is useless. After substitution/reduction by the polynomial $x^{47} + x^{26} + \alpha^{21}x^5$ and by the polynomial x^5, the degree of the resulting polynomial $\widetilde{f}(x)$ in the trace representation decreases to 9. Hence, Wolfmann's bound becomes

$$d(C_1) \geq 32 - 8 \cdot 4 = 0.$$

Let us note that there are other monomial and Zieve permutation polynomials that lower the degree to 9 but we do not write them in the table. Although we achieve the aimed decrease in the degree, the new Wolfmann bound is not useful either.

Wolfmann's bounds for the other five codes before and after substitution/reduction are as follows :

	before	after
C_2	$d(C_2) \geq -24$	$d(C_2) \geq 24$
C_3	$d(C_3) \geq -56$	$d(C_3) \geq 32$
C_4	$d(C_4) \geq -88$	$d(C_4) \geq 32$
C_5	$d(C_5) \geq -16$	$d(C_5) \geq 32$
C_6	$d(C_6) \geq 16$	$d(C_6) \geq 32$

Table 2

Observe that the Zieve permutation does not yield any decrease in $\deg(f)$ for C_3, C_4, C_5 and C_6 whereas monomial permutations do.

Note that Table 1 also implies that codes C_3, C_4, C_5 and C_6 are all equivalent to the binary cyclic code C of length 63 whose dual's basic zero set is $BZ(C^\perp) = \{\alpha\}$. Hence, these codes are also equivalent to each other.

Case 2 : Two Basic Zeros for the Dual Code

		Zieve polynomial	$\deg(\widetilde{f})$	**monomial**	$\deg(\widetilde{f})$
$C_1 : f(x) = \lambda_1 x^{27} + \lambda_2 x^{21}$	$\lambda_1 \neq 0, \lambda_2 \neq 0$	$x^{52} + x^{31} + \alpha^{21}x^{10}$	21	x^{10}	21
	$\lambda_1 \neq 0, \lambda_2 = 0$	$x^{52} + x^{31} + \alpha^{21}x^{10}$	9	x^5	9
	$\lambda_1 = 0, \lambda_2 \neq 0$	-	-	-	-
$C_2 : f(x) = \lambda_1 x^{27} + \lambda_2 x^{15}$	$\lambda_1 \neq 0, \lambda_2 \neq 0$	$x^{47} + x^{26} + \alpha^{21}x^5$	12	x^5	12
	$\lambda_1 \neq 0, \lambda_2 = 0$	$x^{47} + x^{26} + \alpha^{21}x^5$	9	x^5	9
	$\lambda_1 = 0, \lambda_2 \neq 0$	$x^{59} + x^{38} + \alpha^{21}x^{17}$	3	x^{17}	3
$C_3 : f(x) = \lambda_1 x^{31} + \lambda_2 x^9$	$\lambda_1 \neq 0, \lambda_2 \neq 0$	-	-	x^{43}	10
	$\lambda_1 \neq 0, \lambda_2 = 0$	-	-	x^{61}	1
	$\lambda_1 = 0, \lambda_2 \neq 0$	-	-	-	-
$C_4 : f(x) = \lambda_1 x^{27} + \lambda_2 x^{23}$	$\lambda_1 \neq 0, \lambda_2 \neq 0$	-	-	x^{47}	10
	$\lambda_1 \neq 0, \lambda_2 = 0$	$x^{47} + x^{26} + \alpha^{21}x^5$	9	x^5	9
	$\lambda_1 = 0, \lambda_2 \neq 0$	-	-	x^{11}	1

Table 3

For C_2, the dual has $BZ(C_2^{\perp}) = \{\alpha^{15}, \alpha^{27}\}$ and $h(x) = (x^6 + x^4 + x^2 + x + 1)(x^3 + x^2 + 1)$. The codewords with both λ_1, λ_2 nonzero in the trace representation have corresponding polynomials with the degrees lowered to 12 after sunbstitution/reduction with Zieve and monomial permutation polynomials. Polynomials corresponding to $(\lambda_1 \neq 0, \lambda_2 = 0)$ and $(\lambda_1 = 0, \lambda_2 \neq 0)$ reduce to degrees 9 and 3, respectively, with both types of permutation polynomials. Since we should take the maximum degree into account in Wolfmann's bound (cf. Theorem 1.18), we conclude

$$d(C_2) \geq 32 - 26 \cdot 4 = -48.$$

before substitution/reduction and

$$d(C_2) \geq 32 - 11 \cdot 4 = -12.$$

after substitution/reduction. So, our improvement in degrees do not yield anything useful for the minimum distance estimate.

The same is the case for the remaining 3 codes, i.e. we are able to lower the polynomials degrees but the improvement is not good enough to say anything useful about the minimum distances. Therefore, we do not write a table for Wolfmann's bound in these examples.

Cyclic codes over $\mathbb{F}_3$ of length 80:

Let β be a primitive element of $\mathbb{F}_{81}^*$. Irreducible factors of $x^{80} - 1$ and the corresponding roots over $\mathbb{F}_3$ are listed below.

$x+1$	:	2	$x^4+x^3+x^2+x+1$	:	$\beta^{16},\beta^{32},\beta^{48},\beta^{64}$
$x+2$	:	1	$x^4+x^3+x^2+2x+2$	:	$\beta^{7},\beta^{21},\beta^{29},\beta^{63}$
x^2+1	:	β^{20},β^{60}	$x^4+x^3+2x^2+2x+2$	:	$\beta^{17},\beta^{51},\beta^{59},\beta^{73}$
x^2+x+2	:	β^{50},β^{70}	x^4+2x^3+2	:	$\beta,\beta^{3},\beta^{9},\beta^{27}$
x^2+2x+2	:	β^{10},β^{30}	x^4+2x^3+2	:	$\beta,\beta^{3},\beta^{9},\beta^{27}$
x^4+x+2	:	$\beta^{53},\beta^{71},\beta^{77},\beta^{79}$	x^4+2x^3+2	:	$\beta,\beta^{3},\beta^{9},\beta^{27}$
x^4+2x+2	:	$\beta^{13},\beta^{31},\beta^{37},\beta^{39}$	x^4+2x^3+2	:	$\beta,\beta^{3},\beta^{9},\beta^{27}$
x^4+x^2+2	:	$\beta^{25},\beta^{35},\beta^{65},\beta^{75}$	x^4+2x^3+2	:	$\beta,\beta^{3},\beta^{9},\beta^{27}$
x^4+x^2+x+1	:	$\beta^{22},\beta^{34},\beta^{38},\beta^{66}$	x^4+2x^3+x+1	:	$\beta^{44},\beta^{52},\beta^{68},\beta^{76}$
x^4+x^2+2x+1	:	$\beta^{26},\beta^{62},\beta^{74},\beta^{78}$	$x^4+2x^3+x^2+1$	:	$\beta^{2},\beta^{6},\beta^{18},\beta^{54}$
x^4+2x^2+2	:	$\beta^{5},\beta^{15},\beta^{45},\beta^{55}$	$x^4+2x^3+x^2+x+2$	:	$\beta^{23},\beta^{47},\beta^{61},\beta^{69}$
x^4+x^3+2	:	$\beta^{41},\beta^{43},\beta^{49},\beta^{67}$	$x^4+2x^3+x^2+2x+1$	:	$\beta^{8},\beta^{24},\beta^{56},\beta^{72}$
x^4+x^3+2x+1	:	$\beta^{4},\beta^{12},\beta^{28},\beta^{36}$	$x^4+2x^3+2x^2+x+2$	:	$\beta^{11},\beta^{19},\beta^{33},\beta^{57}$
$x^4+x^3+x^2+1$	:	$\beta^{14},\beta^{42},\beta^{46},\beta^{58}$			

Zieve type permutations of $\mathbb{F}_{81}$ are as follows :

$x^{41}+\beta^{10}x$	$x^{61}+\beta^{10}x^{21}$	$\beta^{10}x^{41}+x$	$\beta^{10}x^{61}+x^{21}$
$x^{43}+\beta^{10}x^{3}$	$x^{63}+\beta^{10}x^{23}$	$\beta^{10}x^{43}+x^{3}$	$\beta^{10}x^{63}+x^{23}$
$x^{47}+\beta^{10}x^{7}$	$x^{67}+\beta^{10}x^{27}$	$\beta^{10}x^{47}+x^{7}$	$\beta^{10}x^{67}+x^{27}$
$x^{49}+\beta^{10}x^{9}$	$x^{69}+\beta^{10}x^{29}$	$\beta^{10}x^{49}+x^{9}$	$\beta^{10}x^{69}+x^{29}$
$x^{51}+\beta^{10}x^{11}$	$x^{71}+\beta^{10}x^{31}$	$\beta^{10}x^{51}+x^{11}$	$\beta^{10}x^{71}+x^{31}$
$x^{53}+\beta^{10}x^{13}$	$x^{73}+\beta^{10}x^{33}$	$\beta^{10}x^{53}+x^{13}$	$\beta^{10}x^{73}+x^{33}$
$x^{57}+\beta^{10}x^{17}$	$x^{77}+\beta^{10}x^{37}$	$\beta^{10}x^{57}+x^{17}$	$\beta^{10}x^{77}+x^{37}$
$x^{59}+\beta^{10}x^{19}$	$x^{79}+\beta^{10}x^{39}$	$\beta^{10}x^{59}+x^{19}$	$\beta^{10}x^{79}+x^{39}$

Case 1 : One Basic Zero for the Dual Code

	Zieve polynomial	$\deg(\widetilde{f})$	**monomial**	$\deg(\widetilde{f})$
$C_1 : f(x)=\lambda x^{44}$	$x^{41}+\beta^{10}x$	4	x^{11}	4
$C_2 : f(x)=\lambda x^{41}$	-	-	x^{41}	1
$C_3 : f(x)=\lambda x^{26}$	-	-	x^{37}	2
$C_4 : f(x)=\lambda x^{23}$	-	-	x^{7}	1

Table 4

We list the performance of Wolfmann's bound before and after substitution / reduction below.

	before	after
C_1	$d(C_1) \geq -204$	$d(C_1) \geq 36$
C_2	$d(C_2) \geq -186$	$d(C_2) \geq 54$
C_3	$d(C_3) \geq -96$	$d(C_3) \geq 48$
C_4	$d(C_4) \geq -78$	$d(C_4) \geq 54$

Table 5

Case 2: Two Basic Zeros for the Dual Code

		Zieve polynomial	deg($\widetilde{f}$)	monomial polynomial	deg($\widetilde{f}$)
$C_1 : f(x) = \lambda_1 x^{53} + \lambda_2 x^{25}$	$\lambda_1 \neq 0, \lambda_2 \neq 0$	$x^{77} + \beta^{10} x^{37}$	45	x^{77}	5
	$\lambda_1 \neq 0, \lambda_2 = 0$	$x^{77} + \beta^{10} x^{37}$	41	x^{77}	1
	$\lambda_1 = 0, \lambda_2 \neq 0$	$-$	-	x^{13}	5
$C_2 : f(x) = \lambda_1 x^{53} + \lambda_2 x^{26}$	$\lambda_1 \neq 0, \lambda_2 \neq 0$	$x^{77} + \beta^{10} x^{37}$	42	x^{77}	2
	$\lambda_1 \neq 0, \lambda_2 = 0$	$x^{77} + \beta^{10} x^{37}$	41	x^{77}	1
	$\lambda_1 = 0, \lambda_2 \neq 0$	-	-	x^{37}	2
$C_3 : f(x) = \lambda_1 x^{50} + \lambda_2 x^{10}$	$\lambda_1 \neq 0, \lambda_2 \neq 0$	$x^{53} + \beta^{10} x^{13} - x^{41} + \beta^{10} x$	10	$-$	$-$
	$\lambda_1 \neq 0, \lambda_2 = 0$	-	-	x^{13}	10
	$\lambda_1 = 0, \lambda_2 \neq 0$	-	-	-	-

Table 6

Here is the table showing Wolfmann's bounds for these codes.

	before	after
C_1	$d(C_1) \geq -258$	$d(C_1) \geq 30$
C_2	$d(C_2) \geq -258$	$d(C_2) \geq 48$
C_3	$d(C_3) \geq -240$	$d(C_3) \geq 0$

Table 7

Cyclic Codes over $\mathbb{F}_5$ of Length 624:

The irreducible factors of $x^{624} - 1$ over $\mathbb{F}_5$ are listed below.

$x+1$ $x+2$ $x+3$ $x+4$

x^2+2 x^2+3 x^2+x+1 x^2+x+2

x^2+2x+3 x^2+2x+4 x^2+3x+3 x^2+3x+4

x^2+4x+1 x^2+4x+2 x^4+2 x^4+3

x^4+x+4 x^4+2x+4 x^4+3x+4 x^4+4x+4

x^4+x^2+2 x^4+x^2+x+1 x^4+x^2+2x+2 x^4+x^2+2x+3

x^4+x^2+3x+2 x^4+x^2+3x+3 x^4+x^2+4x+1 x^4+2x^2+3

x^4+2x^2+2x+1 x^4+2x^2+2x+3 x^4+2x^2+3x+1 x^4+2x^2+3x+3

x^4+3x^2+3 x^4+3x^2+x+1 x^4+3x^2+x+3 x^4+3x^2+4x+1

x^4+3x^2+4x+3 x^4+4x^2+2 x^4+4x^2+x+2 x^4+4x^2+x+3

x^4+4x^2+2x+1 x^4+4x^2+3x+1 x^4+4x^2+4x+2 x^4+4x^2+4x+3

x^4+x^3+4 x^4+x^3+x+3 x^4+x^3+2x+3 x^4+x^3+2x+4

x^4+x^3+3x+2 x^4+x^3+4x+1 x^4+x^3+4x+2 $x^4+x^3+x^2+1$

$x^4+x^3+x^2+x+3$ $x^4+x^3+x^2+x+4$ $x^4+x^3+x^2+2x+4$ $x^4+x^3+x^2+3x+3$

$x^4+x^3+x^2+4x+2$ $x^4+x^3+2x^2+2$ $x^4+x^3+2x^2+x+2$ $x^4+x^3+2x^2+x+3$

$x^4+x^3+2x^2+2x+1$ $x^4+x^3+2x^2+2x+2$ $x^4+x^3+2x^2+3x+4$ $x^4+x^3+2x^2+4x+4$

$x^4+x^3+3x^2+1$ $x^4+x^3+3x^2+3$ $x^4+x^3+3x^2+2x+1$ $x^4+x^3+3x^2+4x+2$

$x^4+x^3+3x^2+4x+4$ $x^4+x^3+4x^2+2$ $x^4+x^3+4x^2+x+1$ $x^4+x^3+4x^2+x+4$

$x^4+x^3+4x^2+4x+1$ $x^4+x^3+4x^2+4x+3$ x^4+2x^3+4 x^4+2x^3+x+3

x^4+x^3+x+4 x^4+2x^3+2x+1 x^4+2x^3+2x+2 x^4+2x^3+3x+3

x^4+2x^3+4x+2 $x^4+2x^3+x^2+2$ $x^4+2x^3+x^2+2x+1$ $x^4+2x^3+x^2+2x+3$

$x^4+2x^3+x^2+3x+1$ $x^4+2x^3+x^2+3x+4$ $x^4+2x^3+2x^2+1$ $x^4+2x^3+2x^2+3$

$x^4+2x^3+2x^2+x+1$ $x^4+2x^3+2x^2+2x+2$ $x^4+2x^3+2x^2+2x+4$ $x^4+2x^3+3x^2+2$

$x^4+2x^3+3x^2+x+1$ $x^4+2x^3+3x^2+x+2$ $x^4+2x^3+3x^2+2x+4$ $x^4+2x^3+3x^2+3x+2$

$x^4+2x^3+3x^2+3x+3$ $x^4+2x^3+3x^2+4x+4$ $x^4+2x^3+4x^2+1$ $x^4+2x^3+4x^2+x+4$

$x^4+2x^3+4x^2+2x+2$ $x^4+2x^3+4x^2+3x+3$ $x^4+2x^3+4x^2+3x+4$ $x^4+2x^3+4x^2+4x+3$

x^4+3x^3+4 x^4+3x^3+x+2 x^4+3x^3+2x+3 x^4+3x^3+3x+1

x^4+3x^3+3x+2 x^4+3x^3+4x+3 x^4+3x^3+4x+4 $x^4+3x^3+x^2+2$

$x^4+3x^3+x^2+2x+1$ $x^4+3x^3+x^2+2x+4$ $x^4+3x^3+x^2+3x+1$ $x^4+3x^3+x^2+3x+3$

$x^4+3x^3+2x^2+1$ $x^4+3x^3+2x^2+3$ $x^4+3x^3+2x^2+3x+2$ $x^4+3x^3+2x^2+3x+4$

$x^4+3x^3+2x^2+4x+1$ $x^4+3x^3+3x^2+2$ $x^4+3x^3+3x^2+x+4$ $x^4+3x^3+3x^2+2x+2$

$x^4+3x^3+3x^2+2x+3$ $x^4+3x^3+3x^2+3x+4$ $x^4+3x^3+3x^2+4x+1$ $x^4+3x^3+3x^2+4x+2$

$x^4+3x^3+4x^2+1$ $x^4+3x^3+4x^2+x+3$ $x^4+3x^3+4x^2+2x+3$ $x^4+3x^3+4x^2+2x+4$

$x^4+3x^3+4x^2+3x+2$ $x^4+3x^3+4x^2+4x+4$ x^4+4x^3+4 x^4+4x^3+x+1

x^4+4x^3+x+2 x^4+4x^3+2x+2 x^4+4x^3+3x+3 x^4+4x^3+3x+4

x^4+4x^3+4x+3 $x^4+4x^3+x^2+1$ $x^4+4x^3+x^2+x+2$ $x^4+4x^3+x^2+2x+3$

$x^4+4x^3+x^2+3x+4$ $x^4+4x^3+x^2+4x+3$ $x^4+4x^3+x^2+4x+4$ $x^4+4x^3+2x^2+2$

$x^4+4x^3+2x^2+x+4$ $x^4+4x^3+2x^2+2x+4$ $x^4+4x^3+2x^2+3x+1$ $x^4+4x^3+2x^2+3x+2$

$x^4+4x^3+2x^2+4x+2$ $x^4+4x^3+2x^2+4x+3$ $x^4+4x^3+3x^2+1$ $x^4+4x^3+3x^2+3$

$x^4+4x^3+3x^2+x+2$ $x^4+4x^3+3x^2+x+4$ $x^4+4x^3+3x^2+3x+1$ $x^4+4x^3+4x^2+2$

$x^4+4x^3+4x^2+x+1$ $x^4+4x^3+4x^2+x+3$ $x^4+4x^3+4x^2+4x+1$ $x^4+4x^3+4x^2+4x+4$

Monomial permutations of $\mathbb{F}_{625}$ are obvious and Zieve type permutations of $\mathbb{F}_{625}$ are listed below:

$2x^{313} + x$

$2x^{317} + x^{5}$

$2x^{319} + x^{7}$

$2x^{323} + x^{11}$

$2x^{329} + x^{17}$

$2x^{331} + x^{19}$

$2x^{335} + x^{23}$

$2x^{337} + x^{25}$

$2x^{341} + x^{29}$

$2x^{343} + x^{31}$

$2x^{347} + x^{35}$

$2x^{349} + x^{37}$

$2x^{353} + x^{41}$

$2x^{355} + x^{43}$

$2x^{359} + x^{47}$

$2x^{361} + x^{49}$

$2x^{365} + x^{53}$

$2x^{367} + x^{55}$

$2x^{371} + x^{59}$

$2x^{373} + x^{61}$

$2x^{379} + x^{67}$

$2x^{383} + x^{71}$

$2x^{385} + x^{73}$

$2x^{389} + x^{77}$

$2x^{391} + x^{79}$

$2x^{395} + x^{83}$

$2x^{397} + x^{85}$

$2x^{401} + x^{89}$

$2x^{407} + x^{95}$

$2x^{409} + x^{97}$

$2x^{413} + x^{101}$

$2x^{415} + x^{103}$

$2x^{419} + x^{107}$

$2x^{421} + x^{109}$

$2x^{425} + x^{113}$

$2x^{427} + x^{115}$

$2x^{431} + x^{119}$

$2x^{433} + x^{121}$

$2x^{437} + x^{125}$

$2x^{439} + x^{127}$

$2x^{443} + x^{131}$

$2x^{445} + x^{133}$

$2x^{449} + x^{137}$

$2x^{451} + x^{139}$

$2x^{457} + x^{145}$

$2x^{461} + x^{149}$

$2x^{463} + x^{151}$

$2x^{467} + x^{155}$

$2x^{469} + x^{157}$

$2x^{473} + x^{161}$

$2x^{475} + x^{163}$

$2x^{479} + x^{167}$

$2x^{485} + x^{173}$

$2x^{487} + x^{175}$

$2x^{491} + x^{179}$

$2x^{493} + x^{181}$

$2x^{497} + x^{185}$

$2x^{499} + x^{187}$

$2x^{503} + x^{191}$

$2x^{505} + x^{193}$

$2x^{509} + x^{197}$

$2x^{511} + x^{199}$

$2x^{515} + x^{203}$

$2x^{517} + x^{205}$

$2x^{521} + x^{209}$

$2x^{523} + x^{211}$

$2x^{527} + x^{215}$

$2x^{529} + x^{217}$

$2x^{535} + x^{223}$

$2x^{539} + x^{227}$

$2x^{541} + x^{229}$

$2x^{545} + x^{233}$

$2x^{547} + x^{235}$

$2x^{551} + x^{239}$

$2x^{553} + x^{241}$

$2x^{557} + x^{245}$

$2x^{563} + x^{251}$

$2x^{565} + x^{253}$

$2x^{569} + x^{257}$

$2x^{571} + x^{259}$

$2x^{575} + x^{263}$

$2x^{577} + x^{265}$

$2x^{581} + x^{26}$

$2x^{583} + x^{271}$

$2x^{587} + x^{275}$

$2x^{589} + x^{277}$

$2x^{593} + x^{281}$

$2x^{595} + x^{283}$

$2x^{599} + x^{287}$

$2x^{601} + x^{289}$

$2x^{605} + x^{293}$

$2x^{607} + x^{295}$

$2x^{613} + x^{301}$

$2x^{617} + x^{305}$

$2x^{619} + x^{307}$

$2x^{623} + x^{311}$

$x^{313} + 2x$

$x^{317} + 2x^{5}$

$x^{319} + 2x^{7}$

$x^{323} + 2x^{11}$

$x^{329} + 2x^{17}$

$x^{331} + 2x^{19}$

$x^{335} + 2x^{23}$

$x^{337} + 2x^{25}$

$x^{341} + 2x^{29}$

$x^{343} + 2x^{31}$

$x^{347} + 2x^{35}$

$x^{349} + 2x^{37}$

$x^{353} + 2x^{41}$

$x^{355} + 2x^{43}$

$x^{359} + 2x^{47}$

$x^{361} + 2x^{49}$

$x^{365} + 2x^{53}$

$x^{367} + 2x^{55}$

$x^{371} + 2x^{59}$

$x^{373} + 2x^{61}$

$x^{379} + 2x^{67}$

$x^{383} + 2x^{71}$

$x^{385} + 2x^{73}$

$x^{389} + 2x^{77}$

$x^{391} + 2x^{79}$

$x^{395} + 2x^{83}$

$x^{397} + 2x^{85}$

$x^{401} + 2x^{89}$

$x^{407} + 2x^{95}$

$x^{409} + 2x^{97}$

$x^{413} + 2x^{101}$

$x^{415} + 2x^{103}$

$x^{419} + 2x^{107}$

$x^{421} + 2x^{109}$

$x^{425} + 2x^{113}$

$x^{427} + 2x^{115}$

$x^{431} + 2x^{119}$

$x^{433} + 2x^{121}$

$x^{437} + 2x^{125}$

$x^{439} + 2x^{127}$

$x^{443} + 2x^{131}$

$x^{445} + 2x^{133}$

$x^{449} + 2x^{137}$

$x^{451} + 2x^{139}$

$x^{457} + 2x^{145}$

$x^{461} + 2x^{149}$

$x^{463} + 2x^{151}$

$x^{467} + 2x^{155}$

$x^{469} + 2x^{157}$

$x^{473} + 2x^{161}$

$x^{475} + 2x^{163}$

$x^{479} + 2x^{167}$

$x^{485} + 2x^{173}$

$x^{487} + 2x^{175}$

$x^{491} + 2x^{179}$

$x^{493} + 2x^{181}$

$x^{497} + 2x^{185}$

$x^{499} + 2x^{187}$

$x^{503} + 2x^{191}$

$x^{505} + 2x^{193}$

$x^{509} + 2x^{197}$

$x^{511} + 2x^{199}$

$x^{515} + 2x^{203}$

$x^{517} + 2x^{205}$

$x^{521} + 2x^{209}$

$x^{523} + 2x^{211}$

$x^{527} + 2x^{215}$

$x^{529} + 2x^{217}$

$x^{535} + 2x^{223}$

$x^{539} + 2x^{227}$

$x^{541} + 2x^{229}$

$x^{545} + 2x^{233}$

$x^{547} + 2x^{235}$

$x^{551} + 2x^{239}$

$x^{553} + 2x^{241}$

$x^{557} + 2x^{245}$

$x^{563} + 2x^{251}$

$x^{565} + 2x^{253}$

$x^{569} + 2x^{257}$

$x^{571} + 2x^{259}$

$x^{575} + 2x^{263}$

$x^{577} + 2x^{265}$

$x^{581} + 2x^{269}$

$x^{583} + 2x^{271}$

$x^{587} + 2x^{275}$

$x^{589} + 2x^{277}$

$x^{593} + 2x^{281}$

$x^{595} + 2x^{283}$

$x^{599} + 2x^{287}$

$x^{601} + 2x^{289}$

$x^{605} + 2x^{293}$

$x^{607} + 2x^{295}$

$x^{613} + 2x^{301}$

$x^{617} + 2x^{305}$

$x^{619} + 2x^{307}$

$x^{623} + 2x^{311}$

Case 1 : One Basic Zero for the Dual Code

	Zieve polynomial	deg($\widetilde{f}$)	monomial poynomial	deg($\widetilde{f}$)
$C_1 : f(x) = \lambda x^{64}$	$2x^{361} + x^{49}$	16	x^{49}	16
$C_2 : f(x) = \lambda x^{474}$	$2x^{443} + x^{131}$	6	x^{79}	6
$C_3 : f(x) = \lambda x^{242}$	$2x^{517} + x^{205}$	2	x^{49}	2
$C_4 : f(x) = \lambda x^{212}$	$2x^{365} + x^{53}$	4	x^{53}	4
$C_5 : f(x) = \lambda x^{374}$	$2x^{463} + x^{151}$	2	x^{307}	2
$C_6 : f(x) = \lambda x^{108}$	$2x^{341} + x^{29}$	12	x^{29}	12
$C_7 : f(x) = \lambda x^{222}$	$2x^{409} + x^{97}$	6	x^{149}	6
$C_8 : f(x) = \lambda x^{164}$	$2x^{449} + x^{137}$	4	x^{137}	4
$C_9 : f(x) = \lambda x^{56}$	$2x^{379} + x^{67}$	8	x^{67}	8
$C_{10} : f(x) = \lambda x^{36}$	$2x^{347} + x^{35}$	12	x^{35}	12
$C_{11} : f(x) = \lambda x^{368}$	$2x^{329} + x^{17}$	16	x^{17}	16
$C_{12} : f(x) = \lambda x^{158}$	$2x^{547} + x^{235}$	2	x^{79}	2

Table 8

Wolfmann's bound for these codes are as follows:

	before	after
C_1	$d(C_1) \geq -760$	$d(C_1) \geq 200$
C_2	$d(C_2) \geq -8960$	$d(C_2) \geq 400$
C_3	$d(C_3) \geq -4320$	$d(C_3) \geq 480$
C_4	$d(C_4) \geq -3720$	$d(C_4) \geq 440$
C_5	$d(C_5) \geq -6960$	$d(C_5) \geq 480$
C_6	$d(C_6) \geq -1640$	$d(C_6) \geq 280$
C_7	$d(C_7) \geq -3920$	$d(C_7) \geq 400$
C_8	$d(C_8) \geq -2760$	$d(C_8) \geq 440$
C_9	$d(C_9) \geq -600$	$d(C_9) \geq 360$
C_{10}	$d(C_{10}) \geq -200$	$d(C_{10}) \geq 280$
C_{11}	$d(C_{11}) \geq -5840$	$d(C_{11}) \geq 200$
C_{12}	$d(C_{12}) \geq -2640$	$d(C_{12}) \geq 480$

Table 9

Case 2 : Two Basic Zeros for the Dual Code

		Zieve polynomial	deg($\widetilde{f}$)	**monomial**	deg($\widetilde{f}$)
$C_1 : f(x) = \lambda_1 x^{242} + \lambda_2 x^{64}$	$\lambda_1 \neq 0, \lambda_2 \neq 0$	$2x^{517} + x^{205}$	16	x^{49}	16
	$\lambda_1 \neq 0, \lambda_2 = 0$	$2x^{517} + x^{205}$	2	x^{49}	2
	$\lambda_1 = 0, \lambda_2 \neq 0$	$2x^{361} + x^{49}$	16	x^{49}	16
$C_2 : f(x) = \lambda_1 x^{218} + \lambda_2 x^{82}$	$\lambda_1 \neq 0, \lambda_2 \neq 0$	$2x^{491} + x^{179}$	22	x^{23}	22
	$\lambda_1 \neq 0, \lambda_2 = 0$	$2x^{385} + x^{73}$	2	x^{229}	2
	$\lambda_1 = 0, \lambda_2 \neq 0$	$2x^{605} + x^{293}$	2	x^{137}	2
$C_3 : f(x) = \lambda_1 x^{374} + \lambda_2 x^{124}$	$\lambda_1 \neq 0, \lambda_2 \neq 0$	$2x^{463} + x^{151}$	4	x^{307}	4
	$\lambda_1 \neq 0, \lambda_2 = 0$	$2x^{463} + x^{151}$	2	x^{307}	2
	$\lambda_1 = 0, \lambda_2 \neq 0$	$2x^{463} + x^{151}$	4	x^{151}	4

Table 10

Here are the Wolfmann's bound for these codes.

	before	after
C_1	$d(C_1) \geq -4320$	$d(C_1) \geq 200$
C_2	$d(C_2) \geq -3840$	$d(C_2) \geq 80$
C_3	$d(C_3) \geq -6960$	$d(C_3) \geq 440$

Table 11

2.3 Conclusions

The examples in Section 2.2 indicate that by the substitution / reduction method, one can improve Wolfmann's bound in some cases. Note that if the length of the cyclic code (equivalently, the extension of the base field) is small, then it is sometimes difficult to obtain improvements or useful estimates. This was witnessed for the binary cyclic codes of length 63 whose duals have two basic nonzeros.

There are two constraints that limit the experiments. Firstly, it is not possible to obtain Zieve type permutation on any finite field. Therefore we restricted our attention to the cases investigated in Section 2.2. Secondly, if the field size (code length) is too big then Magma code slows down and we do not get results.

Bibliography

[1] W. Bosma, J. Cannon, C. Playoust, The Magma Algebra System I. the user language, J. Symbolic Comput., vol. 24, 235-265, 1997.

[2] C. Güneri, F. Özbudak, Artin-Schreier extensions and their applications, Topics in Geometry, Coding Theory and Cryptography (A. Garcia, H. Stichtenoth eds), Springer Algebr. Appl., vol. 6, 105-133, 2007.

[3] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge, 1997.

[4] J. van Lint, *Introduction to Coding Theory*, Springer-Verlag GTM, vol. 86, 1999.

[5] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag GTM, vol. 254, 2009.

[6] J. Wolfmann, New bounds on cyclic codes from algebraic curves, in: Lecture Notes in Computer Science, vol. 388, 47-62, 1989.

[7] M. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$, Proc. Amer. Math. Soc., vol. 137, 2209-2216, 2009.