CHARACTER SUMS OF QUADRATIC FORMS OVER FINITE FIELDS AND THE NUMBER OF RATIONAL POINTS FOR SOME CLASSES OF ARTIN-SCHREIER TYPE CURVES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

AYHAN COŞGUN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
MATHEMATICS

JULY 2017

Approval of the thesis:

CHARACTER SUMS OF QUADRATIC FORMS OVER FINITE FIELDS AND THE NUMBER OF RATIONAL POINTS FOR SOME CLASSES OF ARTIN-SCHREIER TYPE CURVES

submitted by **AYHAN COŞGUN** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Mathematics Department, Middle East Technical University** by,

Prof. Dr. Gülbin Dural Ünver
Dean, Graduate School of **Natural and Applied Sciences** _____

Prof. Dr. Mustafa Korkmaz
Head of Department, **Mathematics** _____

Assoc. Prof. Dr. Ali Doğanaksoy
Supervisor, **Department of Mathematics, METU** _____

Examining Committee Members:

Prof. Dr. Hurşit Önsiper
Department of Mathematics, METU _____

Assoc. Prof. Dr. Ali Doğanaksoy
Department of Mathematics, METU _____

Assoc. Prof. Dr. Ömer Küçüksakallı
Department of Mathematics, METU _____

Assoc. Prof. Dr. Zülfükar Saygı
Department of Mathematics, TOBB ETU _____

Assist. Prof. Dr. Burcu Gülmez Temür
Department of Mathematics, Atılım University _____

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: AYHAN COŞGUN

Signature :

ABSTRACT

CHARACTER SUMS OF QUADRATIC FORMS OVER FINITE FIELDS AND THE NUMBER OF RATIONAL POINTS FOR SOME CLASSES OF ARTIN-SCHREIER TYPE CURVES

Coşgun, Ayhan
Ph.D., Department of Mathematics
Supervisor : Assoc. Prof. Dr. Ali Doğanaksoy

July 2017, 80 pages

Exponential sums of quadratic forms over finite fields have many applications to various areas such as coding theory and cryptography. As an example to these applications, there is an organic connection between exponential sums of quadratic forms and the number of rational points of algebraic curves defined over finite fields. This connection is central in the application of algebraic geometry to coding theory and cryptography. In this thesis, different facts and techniques of theory of finite fields are combined properly in order to improve and generalize some of the results in the existing literature on evaluation of exponential sums of certain quadratic forms. These evaluations also correspond to the Walsh-Hadamard transforms of Boolean functions in characteristic two. As a result of these evaluations, the number of rational points are computed for some classes of Artin-Schreier type curves over finite fields.

Keywords: Finite Fields, Exponential Sums, Quadratic Forms, Algebraic Curves, Artin-Schreier Type Curve, Rational Points, Boolean Functions, Gold Type Functions, Kasami-Welch Type Functions, Walsh-Hadamard Transform

ÖZ

SONLU CİSİMLER ÜZERİNDE KUADRATİK FORMLARIN KARAKTER TOPLAMLARI VE BAZI ARTIN-SCHREIER TİPİ EĞRİ SINIFLARININ RASYONEL NOKTA SAYILARI

Coşgun, Ayhan
Doktora, Matematik Bölümü
Tez Yöneticisi : Doç. Dr. Ali Doğanaksoy

Temmuz 2017 , 80 sayfa

Sonlu cisimler üzerinde kuadratik formların üstel toplamlarının kodlama teorisi ve kriptografi başta olmak üzere birçok alana uygulaması bulunmaktadır. Örneğin, kuadratik formların üstel toplamları ile yine sonlu cisimler üzerinde tanımlı cebirsel eğrilerin rasyonel nokta sayıları arasında organik bir bağlantı bulunmaktadır. Bu bağlantı, cebirsel geometrinin kodlama teorisi ve kriptografiye uygulanmasında temel teşkil etmektedir. Bu tezde, sonlu cisimler teorisinin farklı bilgileri ve teknikleri uygun bir şekilde bir araya getirilerek bazı kuadratik formların üstel toplamlarının hesaplanması üzerine literatürde var olan sonuçlar geliştirilmiş ve genelleştirilmiştir. Karakteristik iki olduğunda bu hesaplamalar aynı zamanda Boole fonksiyonlarının Walsh-Hadamard dönüşümlerine de denk gelmektedir. Bu hesaplamaların bir sonucu olarak, bazı Artin-Schreier tipi eğri sınıflarının rasyonel nokta sayısı bulunmuştur.

Anahtar Kelimeler: Sonlu Cisimler, Üstel Toplamlar, Kuadratik Formlar, Cebirsel Eğriler, Artin-Schreier Tipi Eğriler, Rasyonel Noktalar, Boole Fonksiyonları, Gold Tipi Fonksiyonlar, Kasami-Welch Tipi Fonksiyonlar, Walsh-Hadamard Dönüşümü

To my wife...

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my supervisor Assoc. Prof. Ali Doğanaksoy for his great support, help and compassion which rescued me in a very desperate situation about the thesis. I also would like to emphasize his fatherliness and friendship which motivated me and supplied energy for me during hard times. It was a great honor to work with him and being a student of him.

I also would like to thank Assoc. Prof. Zülfükar Saygı for his guidance and great contribution to the thesis. He showed endless patience towards my questions and welcomed them throughout the thesis.

I wish to thank committee members for their guidance and help.

My special appreciation goes to my wife Aynel for her endless love and patience. She always has been a source of energy of life for me and encouraged me about the thesis.

I am also grateful to my friends and old colleagues from Department of Mathematics for their support and friendship during my research assistantship, graduate and undergraduate education in the department. I especially thank to Fuat Erdem and Kamil Otal for their great effort to solve all my software problems including Latex errors.

Finally, I am very thankful to my dearest family members for their constant and endless support, love, sacrifice and prayers.

TABLE OF CONTENTS

ABSTRACT v

ÖZ vi

ACKNOWLEDGMENTS viii

TABLE OF CONTENTS ix

LIST OF TABLES xi

LIST OF FIGURES xii

LIST OF ABBREVIATIONS xiii

CHAPTERS

1 INTRODUCTION 1

2 DEFINITIONS AND PRELIMINARIES 3

2.1 Artin-Schreier Curves 4

2.2 Quadratic Forms 6

2.3 Linearized Polynomials 7

2.4 Outline of the Thesis 9

3 FURTHER RESULTS ON RATIONAL POINTS OF THE CURVE $y^{q^n} - y = \gamma x^{q^a+1} + \beta$ OVER $\mathbb{F}_{q^m}$ 11

3.1 Introduction 11

3.2 Preliminaries 17

3.3 Proof of Theorem 1 19

3.4 Analogous results for the finite fields having even characteristic 29

3.5 Examples of maximal and minimal curves 31

4 WALSH TRANSFORMS OF GOLD TYPE AND KASAMI-WELCH TYPE FUNCTIONS AND RATIONAL POINTS 33

4.1 Introduction 33

4.2 Preliminaries 36

4.3 When $\gcd(b-a,m)=\gcd(b+a,m)$ 38

4.4 When not necessarily $\gcd(b-a,m)=\gcd(b+a,m)$ 51

4.5 Rational Points of the Curve $y^{2^n}+y=\gamma x^{2^b+1}+\gamma x^{2^a+1}+\alpha x+\beta$ over $\mathbb{F}_{2^m}$ and Examples of Maximal and Minimal Curves Contained in This Class 65

5 CONCLUSION 69

5.1 Contributions of the Thesis 69

5.2 Future Study 70

REFERENCES 71

APPENDICES

A SOME RELATED PREVIOUS RESULTS 75

CURRICULUM VITAE 79

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

Figure 3.1 Extensions of $\mathbb{F}_{q_2}$. 14

LIST OF ABBREVIATIONS

p	A prime number
q	A power of a prime number
$\mathbb{F}_{q^m}$	Finite field with q^m elements
$\mathbb{F}_{q^m}[x]$	The polynomial ring over $\mathbb{F}_{q^m}$
$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_{q^n}}$	The relative trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_{q^n}$
$\mathrm{Tr}_{\mathbb{F}_{q^m}}$	The absolute trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_p$
ζ_p	The p-th root of unity $\left(e^{\frac{2\pi i}{p}}\right)$
$\chi_1(x)$	The canonical additive character of $\mathbb{F}_{q^m}$ at x
$f^W(\alpha)$	The Walsh-Hadamard transform of a Boolean function f at α
$r(Q)$	The dimension of the radical of a quadratic form Q
$\Lambda(Q)$	The invariant of a quadratic form Q
$R^*(x)$	The radical polynomial of a mentioned quadratic form Q
$L(x)$	A linearized polynomial over $\mathbb{F}_{q^m}$
$l(t)$	The q-associate of a linearized polynomial $L(x)$ over $\mathbb{F}_{q^m}$
$deg(f)$	Algebraic degree of a polynomial f
$\gcd(f,g)$	The greatest common divisor of f and g with respect to Euclidean division
$\lvert\mathcal{S}\rvert$	Cardinality of a set $\mathcal{S}$
$\mathbb{Z}$	The set of integers
$\mathfrak{X}$	An Artin-Schreier curve over $\mathbb{F}_{q^m}$
$g(\mathfrak{X})$	The genus of an Artin-Schreier curve $\mathfrak{X}$

CHAPTER 1

INTRODUCTION

Exponential sums are one of the powerful tools in both analytic and elementary number theory for solving a wide range of problems from the theory and applications. The study of exponential sums gains importance in modern number theory as most of the significant results have been acquired due to exponential sums and several problems in theory and applications can be reduced to evaluation of them. Analogously, the study of exponential sums over finite fields leads to fruitful results in various applications of finite fields. For instance, the nonlinearity and the Walsh spectrum of Boolean functions can be expressed by means of exponential sums and similarly the study of bentness of Boolean functions can be easily linked with the evaluation of exponential sums (see [35]). The special homomorphisms of finite fields called *characters* play a basic role in setting exponential sums for finite fields.

Algebraic curves over finite fields is an area where number theory and algebraic geometry meet and this area have attracted the interests of researchers of number theory and algebraic geometry since the seminal work of Hasse and Weil in the 1930s and 1940s. But after the papers of Goppa [24, 25, 26] in the period 1977-1982, where wonderful applications of algebraic curves over finite fields were explored, this area attracted new researchers such as coding theorists and algorithmically inclined mathematicians. Algebraic curves over finite fields have many applications to various areas such as coding theory, finite geometry, cryptography and low discrepancy point sets (see, for example [36, 37, 42, 43]). The number of rational points of algebraic curves is important for these applications. Indeed, the major reason why Goppa's work drew the attentions of coding theorsits is the applications of curves with many rational points to coding theory. There is a close connection between character sums and the number of points of curves defined over finite fields. Thus, evaluating the

related character sums is crucial and central in both theory of exponential sums and theory of algebraic curves over finite fields.

Before giving the outline of the thesis we need some mathematical concepts. We present some definitions and preliminaries in the next chapter and then give the outline of the thesis at the end of the chapter.

CHAPTER 2

DEFINITIONS AND PRELIMINARIES

Let p be a prime number. For positive integers e and m, let $q = p^e$ and let $\mathbb{F}_{q^m}$ denote the finite field with q^m elements. For any integer n dividing m, the *relative trace map* $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_{q^n}}$ from $\mathbb{F}_{q^m}$ to $\mathbb{F}_{q^n}$ is defined by

$$\begin{aligned} \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_{q^n}} : \mathbb{F}_{q^m} &\longrightarrow \mathbb{F}_{q^n} \\ x &\longmapsto x + x^{q^n} + x^{q^{2n}} + \cdots + x^{q^{m-n}}. \end{aligned} \tag{2.1}$$

In particular, the trace map $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_p}$ from $\mathbb{F}_{q^m}$ to the prime subfield $\mathbb{F}_p$ is called the *absolute trace* and we will denote it simply by $\mathrm{Tr}_{\mathbb{F}_{q^m}}$. Let $K = \mathbb{F}_{q^m}$ and $F = \mathbb{F}_{q^n}$. Then the trace map $\mathrm{Tr}_{K/F}$ satisfies the following properties (see [34, Theorems 2.23, 2.25 and 2.26]):

(i) $\mathrm{Tr}_{K/F}(x+y) = \mathrm{Tr}_{K/F}(x) + \mathrm{Tr}_{K/F}(y)$ for all $x, y \in K$;

(ii) $\mathrm{Tr}_{K/F}(cx) = c\mathrm{Tr}_{K/F}(x)$ for all $c \in F$ and $x \in K$;

(iii) $\mathrm{Tr}_{K/F}$ is a linear transformation from K onto F, where both K and F are viewed as vector spaces over F;

(iv) $\mathrm{Tr}_{K/F}(a) = \frac{m}{n}a$ for all $a \in F$;

(v) $\mathrm{Tr}_{K/F}\left(x^{q^n}\right) = \mathrm{Tr}_{K/F}(x)$ for all $x \in K$;

(vi) for any $x \in K$, we have $\mathrm{Tr}_{K/F}(x) = 0$ if and only if $x = \beta^{q^n} - \beta$ for some $\beta \in K$;

(vii) if E is an intermediate field between K and F, then

$$\mathrm{Tr}_{K/F}(x) = \mathrm{Tr}_{E/F}\left(\mathrm{Tr}_{K/E}(x)\right).$$

The ***canonical additive character*** χ_1 of $\mathbb{F}_{q^m}$ is defined by

$$\chi_1(x) = (\zeta_p)^{\mathrm{Tr}_{\mathbb{F}_{q^m}}(x)}$$

where $\zeta_p = e^{\frac{2\pi i}{p}}$ is the $p-th$ root of unity. Any additive character χ_c, for $c \in \mathbb{F}_{q^m}$, of $\mathbb{F}_{q^m}$ can be written in terms of χ_1 as $\chi_c(x) = \chi_1(cx)$. By the properties of trace function we have also $\chi_1(x+y) = \chi_1(x)\chi_1(y)$ and $\chi_1\left(x^{p^i}\right) = \chi_1(x)$ for all $x, y \in \mathbb{F}_{q^m}$ and $i \in \mathbb{Z}$. One of the useful properties of χ_1 is the following (see [34, Theorems 5.4] for proof). Let $\theta \in \mathbb{F}_{q^m}$, then

$$\sum_{x \in \mathbb{F}_{q^m}} \chi_1(\theta x) = \begin{cases} q^m & \text{if } \theta = 0, \\ 0 & \text{if } \theta \neq 0. \end{cases}$$

Let Ψ_1 be the canonical additive character of $\mathbb{F}_{q^n}$ for any n dividing m. Then by trace properties, for any $x \in \mathbb{F}_{q^n}$ and $\theta \in \mathbb{F}_{q^m}$ we have $\chi_1(\theta x) = \Psi_1\left(x\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_{q^n}}(\theta)\right)$ and we obtain the following result.

Lemma 1. *Let χ_1 be the canonical additive character of $\mathbb{F}_{q^m}$, $\theta \in \mathbb{F}_{q^m}$ and $n|m$. Then*

$$\sum_{x \in \mathbb{F}_{q^n}} \chi_1(\theta x) = \begin{cases} q^n & \textit{if } \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_{q^n}}(\theta) = 0, \\ 0 & \textit{if } \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_{q^n}}(\theta) \neq 0. \end{cases}$$

2.1 Artin-Schreier Curves

In this thesis, by an Artin-Schreier curve $\mathfrak{X}$ we mean a smooth, geometrically irreducible projective curve over a finite field $\mathbb{F}_{q^m}$ whose affine equation is given by

$$\mathfrak{X}: \quad y^{q^n} - y = F(x) \tag{2.2}$$

for some integer n and $F(x) \in \mathbb{F}_{q^m}[x]$. Artin-Schreier curves were studied by various authors in literature (see for instance [44, 31, 27, 12, 13, 14, 22, 39, 1]). There is a close connection between exponential sums and the number of points of curves defined over finite fields. Let N denote the number of solutions of the equation

$$y^{q^n} - y = F(x)$$

in $\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$ (i.e. the number of affine points of $\mathfrak{X}$). Let χ_1 be the canonical additive character of $\mathbb{F}_{q^m}$ and recall that $\chi_1(x) = \chi_1(x^{q^n})$ for all integers n and $x \in \mathbb{F}_{q^m}$.

Define $\varphi(x,y) = F(x) - y^{q^n} + y$. Thus,

$$N = |\{(x,y) \in \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} : \varphi(x,y) = 0\}|.$$

Then we have

$$\sum_{\theta \in \mathbb{F}_{q^m}} \chi_1(\theta\varphi(x,y)) = \begin{cases} q^m & \text{if } \varphi(x,y) = 0, \\ 0 & \text{if } \varphi(x,y) \neq 0. \end{cases}$$

Hence we get $\sum_{x,y \in \mathbb{F}_{q^m}} \sum_{\theta \in \mathbb{F}_{q^m}} \chi_1(\theta\varphi(x,y)) = Nq^m$. By changing the summation order we get

$$\begin{aligned} q^m N &= \sum_{\theta \in \mathbb{F}_{q^m}} \sum_{x,y \in \mathbb{F}_{q^m}} \chi_1(\theta\varphi(x,y)) \\ &= \sum_{\theta \in \mathbb{F}_{q^m}} \sum_{x \in \mathbb{F}_{q^m}} \chi_1(\theta F(x)) \sum_{y \in \mathbb{F}_{q^m}} \chi_1\left(\theta y - \theta y^{q^n}\right). \end{aligned} \tag{2.3}$$

The inner sum is

$$\sum_{y \in \mathbb{F}_{q^m}} \chi_1\left(\theta y - \theta y^{q^n}\right) = \sum_{y \in \mathbb{F}_{q^m}} \chi_1\left((\theta y)^{q^n}\right) \chi_1\left(-\theta y^{q^n}\right) = \sum_{y \in \mathbb{F}_{q^m}} \chi_1\left((\theta^{q^n} - \theta) y^{q^n}\right)$$

$$= \sum_{y \in \mathbb{F}_{q^m}} \chi_1\left((\theta^{q^n} - \theta) y\right) = \begin{cases} q^m & \text{if } \theta \in \mathbb{F}_{q^m} \cap \mathbb{F}_{q^n}, \\ 0 & \text{if } \theta \notin \mathbb{F}_{q^m} \cap \mathbb{F}_{q^n}. \end{cases}$$

Then by simplifying equation (2.3) we get

$$N = \sum_{\theta \in \mathbb{F}_{q^m} \cap \mathbb{F}_{q^n}} \sum_{x \in \mathbb{F}_{q^m}} \chi_1(\theta F(x)). \tag{2.4}$$

Therefore, we will deal with the character sums of the form (2.4) in this thesis in order to find the number of rational points of some Artin-Schreier type curves.

Let $N(\mathfrak{X})$ denote the number of $\mathbb{F}_{q^m}$-rational points of the curve $\mathfrak{X}$ and $g(\mathfrak{X})$ denote the genus of it. The Hasse–Weil inequality states that:

$$q^m + 1 - 2g(\mathfrak{X})\sqrt{q^m} \leq N(\mathfrak{X}) \leq q^m + 1 + 2g(\mathfrak{X})\sqrt{q^m}.$$

The curve $\mathfrak{X}$ is said to be *maximal* over $\mathbb{F}_{q^m}$ if the upper bound is attained and *minimal* over $\mathbb{F}_{q^m}$ if the lower bound is attained. Maximal curves provide the best algebraic geometry codes.

2.2 Quadratic Forms

In this section, we recall some basic facts about quadratic forms (see [34, Chapter 6] for example). Quadratic forms are functions of algebraic degree 2.

Definition 1. *For an integer $m \geq 2$, a map $Q : \mathbb{F}_{q^m} \longmapsto \mathbb{F}_q$ is called a **quadratic form** of dimension m over $\mathbb{F}_q$ if*

(i) $Q(ax) = a^2 Q(x)$ *for all* $a \in \mathbb{F}_q$ *and* $x \in \mathbb{F}_{q^m}$ *and*

(ii) the corresponding mapping $B_Q : \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} \longmapsto \mathbb{F}_q$ *given by* $B_Q(x,y) = Q(x+y) - Q(x) - Q(y)$ *is symmetric and bilinear.*

We define the *radical* of Q to be the radical of the bilinear form B_Q. More precisely,

$$rad\,(Q) = \{y \in K | B_Q(x,y) = 0 \text{ for all } x \in \mathbb{F}_{q^m}\}\,.$$

Then, we will denote the *dimension of the radical* (dimension as a vector space over $\mathbb{F}_q$) by $r\,(Q) = \dim rad\,(Q)$. There is another invariant associated to a quadratic form related to character sum of it. If $Q : \mathbb{F}_{p^m} \longmapsto \mathbb{F}_p$, then we have

$$\sum_{x \in \mathbb{F}_{p^m}} (\zeta_p)^{Q(x)} = \Lambda(Q) p^{\frac{1}{2}(m + r(Q))} \tag{2.5}$$

where $\Lambda(Q)$is uniquely determined according to type of the form and described as follows (for further details see [34, 28, 18, 15, 5]):

- if $p = 2$, then $\Lambda(Q)$ takes values in the set $\{-1, 0, +1\}$;
- if p is odd, then $\Lambda(Q)$ takes values in the set $\left\{-(\varsigma_p)^{m-rad(Q)}, +(\varsigma_p)^{m-rad(Q)}\right\}$;

where $\varsigma_p = i^{\frac{1}{4}(p-1)^2}$ is a complex number depending on p. We will call $\Lambda(Q)$ as *the invariant* of Q throughout the thesis. Hence, evaluating character sum of a quadratic form Q is the same with determining $r(Q)$ and $\Lambda(Q)$.

There are a few ways to represent a quadratic form . One of them is *the single variable approach* (or *polynomial representation*). Any quadratic form $Q : \mathbb{F}_{p^m} \longmapsto \mathbb{F}_p$ can be represented as

$$Q(x) = \mathrm{Tr}_{\mathbb{F}_{p^m}} \left(\sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} a_i x^{p^i+1} \right) \tag{2.6}$$

where $a_i \in \mathbb{F}_{p^m}$. If m is odd, the representation is unique, otherwise $a_{m/2}$ is unique only modulo $\mathbb{F}_{p^m}/\mathbb{F}_p$ (see [19]). Let $\mathfrak{c} = max\left\{0 \leq i \leq \lfloor \frac{m}{2} \rfloor : a_i \neq 0\right\}$ in the representation (2.6). The following is an another well-known fact and employed in many papers:

$$rad\,(Q) = \{x \in \mathbb{F}_{p^m} | R^*(x) = 0\}$$

and so

$$\dim rad\,(Q) = \log_p \left[deg\left(\gcd\left(R^*(x), x^{p^m} - x\right)\right)\right]$$

where

$$R^*(x) = \sum_{i=0}^{\mathfrak{c}} a_i \left(x^{p^{\mathfrak{c}+i}} + x^{p^{\mathfrak{c}-i}}\right)$$

is the *radical polynomial* of Q.

In literature, the character sums of the form

$$\sum_{x \in \mathbb{F}_{p^m}} \chi_1\left(F(x)\right) \tag{2.7}$$

where $F(x) \in \mathbb{F}_{p^m}[x]$, are called ***Weil sums***. The sum of $F(x) = \gamma x^{p^a+1} + \alpha x \in \mathbb{F}_{p^m}[x]$ is evaluated by Carlitz with $a = 1$ for $p = 2$ in [3] and for odd p in [4]. Then the evaluation for general a is carried out by Coulter in [11, 9, 10]. In [28], Hou evaluated the sum for a general $F(x) = \sum_{i=0}^{\mathfrak{c}} \gamma_i x^{p^{a_i}+1} + \alpha x \in \mathbb{F}_{p^m}[x]$ explicitly for $p = 2$ under some restrictions on a_i's. [18] is the extension of [28] to odd characteristics. Fitzgerald in [21] evaluated the sum for the binomial $F(x) = x^{2^b+1} + x^{2^a+1} \in \mathbb{F}_{2^m}[x]$ completely without any restrictions on m, a, and b.

2.3 Linearized Polynomials

A polynomial of the form

$$L(x) = \sum_{i=0}^{\mathfrak{c}} a_i x^{q^i} \in \mathbb{F}_{q^m}[x]$$

is called a ***linearized polynomial*** over $\mathbb{F}_{q^m}$. Its *q-associate* is defined as

$$l(t) = \sum_{i=0}^{\mathfrak{c}} a_i t^i \in \mathbb{F}_{q^m}[t]$$

and $L(x)$ is called the *inverse q-associate* of $l(t)$.

Let $A(x), B(x) \in \mathbb{F}_{q^m}[x]$ be linearized polynomials and $a(t), b(t) \in \mathbb{F}_{q^m}[t]$ be their q-associates. Then we define the right division "$|_r$" in $\mathbb{F}_{q^m}[x]$ by

$$A(x)|_r B(x) \quad \text{if and only if} \quad B(x) = C(x) \circ A(x)$$

for some linearized polynomial $C(x) \in \mathbb{F}_{q^m}[x]$

When, $m = 1$, in particular, we have

- q-associate of $A(x) \circ B(x)$ is $a(t)b(t)$ and inverse q-associate of $a(t)b(t)$ is $A(x) \circ B(x)$,
- $A(x)|_r B(x)$ if and only if $A(x)$ divides $B(x)$ in ordinary sense.

The following is a well-known fact about linearized polynomials and it provides convenience in the proofs of Lemma 7, Lemma 9 and Lemma 10 in Chapter 4. We give a proof here for completeness and refer to [34] for further details on linearized polynomials.

Proposition 1. *Suppose $L_1(x), L_2(x) \in \mathbb{F}_q[x]$ are two linearized polynomials over $\mathbb{F}_q$, and their q-associates are $l_1(t), l_2(t) \in \mathbb{F}_q[t]$ respectively. Then*

$$\gcd\left(L_1(x), L_2(x)\right) = \textit{the inverse q-associate of } \gcd\left(l_1(t), l_2(t)\right)$$

where $\gcd\left(L_1(x), L_2(x)\right)$ is the greatest common divisor of two polynomials $L_1(x)$ and $L_2(x)$ for Euclidean division.

Proof. Let $\gcd\left(L_1(x), L_2(x)\right) = A(x)$, $\gcd\left(l_1(t), l_2(t)\right) = b(t)$ and $B(x)$ be the inverse q-associate of $b(t)$. Then we will show that $A(x) = B(x)$.

- $B(x)$ divides $A(x)$:

Let $l_1(t) = c_1(t)b(t)$ and $l_2(t) = c_2(t)b(t)$ for some $c_1(t)$ and $c_2(t)$ in $\mathbb{F}_q[t]$. Then their inverse q-associates are $L_1(x) = C_1(x) \circ B(x)$ and $L_2(x) = C_2(x) \circ B(x)$

where $C_1(x)$, $C_2(x)$ are inverse q-associates of $c_1(t)$ and $c_2(t)$, respectively. So

$$B(x)|\gcd(L_1(x), L_2(x)) = A(x).$$

- $A(x)$ divides $B(x)$:

As $\gcd(L_1(x), L_2(x)) = A(x)$, we have $L_1(x) = D_1(x) \circ A(x)$ and $L_2(x) = D_2(x) \circ A(x)$ for some linearized polynomials $D_1(x), D_2(x) \in \mathbb{F}_q[x]$. Then their q-associates are $l_1(t) = d_1(t)a(t)$ and $l_2(t) = d_2(t)a(t)$ where $d_1(t)$, $d_2(t)$ are q-associates of $D_1(x)$ and $D_2(x)$, respectively. So $a(t)|\gcd(l_1(t), l_2(t)) = b(t)$. That is, $A(x)|B(x)$.

□

Now we are ready to give the outline of the thesis.

2.4 Outline of the Thesis

The thesis consists of five chapters including this chapter and the previous chapter Introduction.

In this thesis, we consider the Artin-Schreier curve over a finite field $\mathbb{F}_{q^m}$ whose affine equation is of the form

$$\mathfrak{X}: \quad y^{q^n} - y = \gamma_1 x^{q^b+1} + \gamma_2 x^{q^a+1} + \alpha x + \beta \tag{2.8}$$

for some integer n and $\gamma_1, \gamma_2, \alpha, \beta \in \mathbb{F}_{q^m}$.

In Chapter 3, we consider the case where $\gamma_1 = 0$ and $\alpha = 0$. Then, using the results of Coulter in [9, 11] we compute the number of rational points of the curve

$$\mathfrak{X}: \quad y^{q^n} - y = \gamma x^{q^a+1} + \beta. \tag{2.9}$$

in all characteristics. At the end of Chapter 3, we give new examples of maximal and minimal curves that are contained in the class of the curve (2.9).

In Chapter 4, we consider a binomial quadratic term in the curve (2.8) in even characteristic. Firstly, making use of the results in [21, 28] we evaluate the sum

$$\sum_{x\in\mathbb{F}_{2^m}} \chi_1\left(x^{2^b+1}+x^{2^a+1}+\alpha x\right)$$

which corresponds to the *Walsh transform* (see Definition 3 in Chapter 4) of the Gold type Boolean function $f(x)=\mathrm{Tr}_{\mathbb{F}_{2^m}}\left(x^{2^b+1}+x^{2^a+1}\right)$ at the point $\alpha\in\mathbb{F}_{q^m}$. Due to this evaluation we also correct a recent result in [41]. Then, we generalize these results to the evaluation of the sum

$$\sum_{x\in\mathbb{F}_{2^m}} \chi_1\left(\gamma x^{2^b+1}+\gamma x^{2^a+1}+\alpha x\right) \tag{2.10}$$

where the coefficient γ is taken arbitrarily from $\mathbb{F}_{2^m}\cap\mathbb{F}_{2^{b-a}}$ and without any restrictions on m, a, b and α. Finally, at the end of Chapter 4, using the sum (2.10) we compute the number of rational points of the curve (2.8) for the case $q=2$, $\gcd(m,n)=1$ and $\gamma_1=\gamma_2=\gamma\in\mathbb{F}_{2^m}\cap\mathbb{F}_{2^{b-a}}$. More precisely, we consider the curve

$$\mathfrak{X}: \quad y^{2^n}+y=\gamma x^{2^b+1}+\gamma x^{2^a+1}+\alpha x+\beta \tag{2.11}$$

with $\gamma\in\mathbb{F}_{2^m}\cap\mathbb{F}_{2^{b-a}}$ in Chapter 4. Furthermore, we give examples of maximal and minimal curves contained in the class of the curve (2.11).

We finish the thesis with Chapter 5 by giving some concluding remarks.

CHAPTER 3

FURTHER RESULTS ON RATIONAL POINTS OF THE CURVE $y^{q^n} - y = \gamma x^{q^a+1} + \beta$ OVER $\mathbb{F}_{q^m}$

3.1 Introduction

In this chapter we consider the class of Artin-Schreier type algebraic curves which are of the form (2.9). The number of rational points of these curves is determined in many cases in [40] (see also [12, 44]) and we improve these results by determining the number of rational points of these curves in some of the remaining cases for odd characteristic. Furthermore, we obtain analogous results for even characteristic. The results in this chapter are based on the publication [6].

Let p be a prime number. For positive integers e and m, let $q = p^e$ and let $\mathbb{F}_{q^m}$ denote the finite field with q^m elements.

Let n and a be positive integers and $\beta, \gamma \in \mathbb{F}_{q^m}$ with $\gamma \neq 0$. We consider the Artin-Schreier type curve $\mathfrak{X}$ of the form

$$\mathfrak{X}: \quad y^{q^n} - y = \gamma x^{q^a+1} + \beta. \tag{3.1}$$

Using [42, Proposition 6.4.1] we note that the genus of the curve $\mathfrak{X}$ in (3.1) is

$$g(\mathfrak{X}) = \frac{(q^n-1)q^a}{2}.$$

Let N denote the number of solutions of the equation

$$y^{q^n} - y = \gamma x^{q^a+1} + \beta$$

in $\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$. For the number $N(\mathfrak{X})$ of $\mathbb{F}_{q^m}$-rational points of $\mathfrak{X}$ we have

$$N(\mathfrak{X}) = 1 + N$$

since there is only one rational point at infinity. Hence determining $N(\mathfrak{X})$ is the same as determining N. This number is determined exactly in many cases in [40] for odd q and we have included these results in the Appendix A for the completeness of the chapter.

There is a close connection of the number of $\mathbb{F}_{q^m}$-rational points of $\mathfrak{X}$ to the weight distribution of some linear codes (see, for example [42] Section 9.2) and to cross-correlation of some sequences used in communication (see, for example [30]). Moreover, there are explicit maximal and minimal curves in the form of $\mathfrak{X}$ (see Section 3.5 below and the references therein). Although the form of $\mathfrak{X}$ is quite simple, it seems that finding its exact number of $\mathbb{F}_{q^m}$-rational points in some remaining cases is difficult (see the experimental results in the last part of Section 3.3 below).

Throughout the chapter we choose and fix q, m, n, a, γ and β as above. The integer n does not necessarily divide m. Besides this, our first observation shows that nothing changes in terms of the number of rational points of $\mathfrak{X}$ if we choose the integer n as a divisor of m.

Lemma 2. *Put $\delta = \gcd(m, n)$ and let $\mathfrak{X}_1$ and $\mathfrak{X}_2$ be the Artin-Schreier type curves given by*

$$\mathfrak{X}_1 : \quad y^{q^n} - y = \gamma x^{q^a+1} + \beta,$$

$$\mathfrak{X}_2 : \quad y^{q^\delta} - y = \gamma x^{q^a+1} + \beta.$$

Then, $N(\mathfrak{X}_1) = N(\mathfrak{X}_2)$.

Proof. The result follows easily by equation (2.4) as $\mathbb{F}_{q^m} \cap \mathbb{F}_{q^n} = \mathbb{F}_{q^{\gcd(m,n)}} = \mathbb{F}_{q^\delta}$.

□

Therefore, we will assume $n \mid m$ throughout the chapter. Moreover, we define non-

negative integers s, t and positive integers r, m_1, a_1 as follows:

$$\begin{aligned} m &= 2^s r m_1, \\ a &= 2^t r a_1, \end{aligned}$$

where $\gcd(m_1, a_1) = \gcd(2, r m_1 a_1) = 1$. Furthermore let u be the nonnegative integer and ρ, n_1, m_2 be the positive integers so that

$$n = 2^u \rho n_1 \quad \text{and} \quad m_1 = n_1 m_2$$

where $\gcd(2, \rho n_1) = 1$, $\rho | r$ and $n_1 | m_1$. Observe that if we fix m, a and n, then all of the parameters introduced here are uniquely determined. Also note that $u \leq s$ as $n|m$. Finally let

$$A = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_{q^n}}(\beta).$$

For the sake of simplicity we list all the notations used in this chapter:

- m, n and a are positive integers such that $n|m$.
- $m = 2^s r m_1$ and $a = 2^t r a_1$ such that $\gcd(2, r m_1 a_1) = 1$ and $\gcd(m_1, a_1) = 1$.
- $n = 2^u \rho n_1$ such that $\gcd(2, \rho n_1) = 1$, $\rho | r$ and $n_1 | m_1$ with $m_1 = n_1 m_2$.
- $A = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_{q^n}}(\beta)$.
- $q = p^e$ where p is a prime number.
- $q_1 = q^{2^t r}$.
- $q_2 = q^{2^t \rho}$.
- $q_3 = q^{\frac{n}{2^{u-t}}} = q^{2^t \rho n_1}$.
- $k = 2^{t+1} r$.
- $v = 2^{s-(t+1)}$.
- $B_1 = \gcd\left(2^{s-u} m_2, q_2 + 1\right)$.
- ω is a generator of $\mathbb{F}_{q^m}^* = \mathbb{F}_{q^m} \setminus \{0\}$.
- $\omega' = \omega^{\frac{q^m - 1}{q^n - 1}}$ generates $\mathbb{F}_{q^n}^* = \mathbb{F}_{q^n} \setminus \{0\}$.

- $\omega^{''} = \left(\omega^{'}\right)^{\frac{q^n-1}{q_3-1}}$ generates $\mathbb{F}_{q_3}^* = \mathbb{F}_{q_3} \setminus \{0\}$.
- $\mathbb{S} = \left\{0, 1, 2, \ldots, \frac{q^n-1}{q_3-1} - 1\right\}$.
- $\mathbb{S}_0 = \left\{ i \in \mathbb{S} : \left(\left(\omega^{'}\right)^i \gamma\right)^{\frac{q^m-1}{q_1+1}} = (-1)^v \right\}$.
- $A_i = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}\left(\left(\omega^{'}\right)^i A\right)$.
- $M_0 = |\{i \in \mathbb{S}_0 : A_i = 0\}|$.
- $\overline{M_0} = |\{i \in \mathbb{S} \setminus \mathbb{S}_0 : A_i = 0\}|$.
- h is the uniquely determined integer with $0 \leq h < q^m - 1$ such that $\gamma = \omega^h$.

We note that the finite fields $\mathbb{F}_{q^m}$, $\mathbb{F}_{q^n}$, $\mathbb{F}_{q_1}$, $\mathbb{F}_{q_2}$ and $\mathbb{F}_{q_3}$ form the lattice in Figure 3.1.

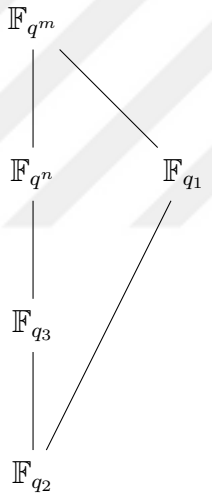

Figure 3.1: Extensions of $\mathbb{F}_{q_2}$.

For the finite fields having odd characteristic, N is determined explicitly in the following cases in [40]:

- for $s \leq t$,
- for $s \geq t + 1$ and $u \leq t$,
- for $t + 1 \leq u \leq s$ and $A = 0$.

It remains to consider the case $t+1 \leq u \leq s$ and $A \neq 0$. We have completed this case in this chapter except the subcase that $u \geq t+2$ with $h \equiv 0 \mod \left(\frac{q_1+1}{q_2+1}B_1\right)$. For this special subcase, we present some experimental results in the last part of Section 3.3 below. Moreover, we obtain analogous results for even q for all cases except the subcase that $u \geq t+2$ with $h \equiv 0 \mod \left(\frac{q_1+1}{q_2+1}B_1\right)$.

Here we note that in [40], the results were obtained by using some facts on quadratic forms and some properties of function fields. In this chapter, apart from the techniques in [40], we use also some explicit evaluations of Weil sums as in [9, 10, 11]. In particular, we use explicit evaluations of Weil sums for equation (3.5) in Section 3.3 in the proof of Theorem 1. We determined it explicitly in some cases using a specific subfield. It seems difficult to evaluate the corresponding exponential sum in (3.5) in all cases. For the subcase $u \geq t+2$ with $h \equiv 0 \mod \left(\frac{q_1+1}{q_2+1}B_1\right)$, it seems that new techniques are required to evaluate the corresponding Weil sums.

This chapter is organized as follows. We state our result for odd q in the rest of this section and then we compare our result with some known results. In Section 3.2 we present some preliminaries. Then we give the proof of our main result in odd characteristic and present some computational results in Section 3.3. In Section 3.4 we give our analogous results for even q and in Section 3.5 we give examples of maximal and minimal curves in the class of the curves considered in this chapter. In Appendix A we recall the number of rational points of the special curves obtained in [40].

Now we are ready to give our main result for the finite fields of odd characteristic.

Theorem 1. *Assume that q is odd, $t+1 \leq u \leq s$ and $A \neq 0$. Let l be the integer with $0 \leq l < q^n - 1$ such that $-A^{q^n - q^{\frac{n}{2}}} = \left(\omega^{'}\right)^l$ as $\omega^{'}$ is a generator of $\mathbb{F}_{q^n}^*$. Moreover, put $l^{'} = \dfrac{l}{q^{\frac{n}{2}}-1}$ and recall that $B_1 = \gcd\left(2^{s-u}m_2, q_2+1\right)$.*

- ***Case s=t+1 (=u):***

  If $h \not\equiv \frac{q_1+1}{2} \mod \left(\frac{q_1+1}{q_2+1}B_1\right)$, then

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

If $h \equiv \frac{q_1+1}{2} \mod \left(\frac{q_1+1}{q_2+1}B_1\right)$, *then*

$$N = \begin{cases} q^m + q^{\frac{m}{2}}\left[q^{\frac{(k+n)}{2}} + q^{\frac{n}{2}} + 1 - B_1(q^{\frac{k}{2}}+1)\left(\frac{q^{\frac{n}{2}}+1}{q_2+1}\right)\right] \\ \qquad\qquad \text{if } l'\frac{m_2}{B_1} \equiv B_2 \mod \left(\frac{q_2+1}{B_1}\right), \\ q^m + q^{\frac{m}{2}}\left[1 - B_1(q^{\frac{k}{2}}+1)\left(\frac{q^{\frac{n}{2}}+1}{q_2+1}\right)\right] \\ \qquad\qquad \text{if } l'\frac{m_2}{B_1} \not\equiv B_2 \mod \left(\frac{q_2+1}{B_1}\right), \end{cases}$$

where $B_2 = \dfrac{\frac{q_1+1}{2} - h}{\frac{q_1+1}{q_2+1}B_1}$.

- ***Case s* $\geq$ *t+2:***

  If $h \not\equiv 0 \mod \left(\frac{q_1+1}{q_2+1}B_1\right)$, *then*

  $$N = q^m - q^{\frac{m}{2}}.$$

  If $h \equiv 0 \mod \left(\frac{q_1+1}{q_2+1}B_1\right)$ *and* $u = t+1$, *then*

  $$N = \begin{cases} q^m - q^{\frac{m}{2}}\left[q^{\frac{(k+n)}{2}} + q^{\frac{n}{2}} + 1 - B_1(q^{\frac{k}{2}}+1)\left(\frac{q^{\frac{n}{2}}+1}{q_2+1}\right)\right] \\ \qquad\qquad \text{if } l'\frac{2^{s-u}m_2}{B_1} \equiv B_2 \mod \left(\frac{q_2+1}{B_1}\right), \\ q^m - q^{\frac{m}{2}}\left[1 - B_1(q^{\frac{k}{2}}+1)\left(\frac{q^{\frac{n}{2}}+1}{q_2+1}\right)\right] \\ \qquad\qquad \text{if } l'\frac{2^{s-u}m_2}{B_1} \not\equiv B_2 \mod \left(\frac{q_2+1}{B_1}\right), \end{cases}$$

  where $B_2 = \dfrac{-h}{\frac{q_1+1}{q_2+1}B_1}$.

In the following remark, we compare our results with the results in [12] and [44].

Remark 1. *The curve*

$$\mathfrak{X}: \quad y^{q^n} - y = \gamma x^{q^a+1} + \beta$$

is considered in [12] and [44] for some cases. We compare our main result and the main result of [9] with corresponding results given in [12, 44] below.

- *In [12], N is determined for the case where $n|a$ and $\beta = 0$. This is a special subcase of Theorem 13 and Theorem 14 given in the Appendix A.*
- *Using the results in [44], the case $u + 1 \leq s \leq t$ and the case $u \leq t$ with $s \geq t + 1$ can be obtained. The first case corresponds to a subcase of Theorem 13 and the second case coincides with Theorem 14 given in the Appendix A.*
- *The case $t + 1 \leq u \leq s$ is not considered in [12, 44]. Therefore, Theorem 15 given in the Appendix A (the main theorem of [40]) and Theorem 1 (the main result of this chapter) have no intersection with these two works.*

3.2 Preliminaries

In this section we give some preliminaries that we use in Section 3.3. Throughout this section we assume that q is odd.

Definition 2. *We define the function S: $\mathbb{F}_{q^n}^* \longrightarrow \left\{(-1)^{v+1}q^{\frac{(m+k)}{2}}, -(-1)^{v+1}q^{\frac{m}{2}}\right\}$ as follows:*

$$S(\theta) = \begin{cases} (-1)^{v+1}q^{\frac{(m+k)}{2}} & \text{if } (\theta\gamma)^{\frac{q^m-1}{q_1+1}} = (-1)^v \,, \\ -(-1)^{v+1}q^{\frac{m}{2}} & \text{if } (\theta\gamma)^{\frac{q^m-1}{q_1+1}} \neq (-1)^v \,. \end{cases}$$

The following lemma is a formulation of N in terms of Weil sums by rearranging the results found in [9]. So, it converts the problem of finding the number of rational points to the problem of evaluating certain exponential sums.

Lemma 3. $N = q^m + \sum_{\theta \in \mathbb{F}_{q^n}^*} \Psi_1(\theta A) S(\theta)$ *where Ψ_1 is the canonical additive character of $\mathbb{F}_{q^n}$.*

Proof. We have

$$N = \sum_{\theta \in \mathbb{F}_{q^n}} \sum_{x \in \mathbb{F}_{q^m}} \chi_1\left(\theta\left(\gamma x^{q^a+1} + \beta\right)\right) \tag{3.2}$$

by equation(2.4) where χ_1 is the canonical additive character of $\mathbb{F}_{q^m}$. As $\beta \in \mathbb{F}_{q^m}$ is a fixed element, equation (3.2) yields

$$N = q^m + \sum_{\theta \in \mathbb{F}_{q^n}^*} \chi_1(\beta\theta) \sum_{x \in \mathbb{F}_{q^m}} \chi_1\left(\theta\gamma x^{q^a+1}\right). \tag{3.3}$$

For the case $t+1 \leq u \leq s$, we have $q^a = p^{ea}$, $q^m = p^{em}$, and

$$d = \gcd(ea, em) = e\gcd(a, m) = e2^t r = e\frac{k}{2}$$

which gives

$$\frac{em}{d} = \frac{e2^s r m_1}{e2^t r} = 2^{s-t} m_1$$

is even. Hence by Theorem 2 of [9] we have

$$\sum_{x \in \mathbb{F}_{q^m}} \chi_1\left(\theta\gamma x^{q^a+1}\right) = S(\theta) = \begin{cases} q^{\frac{(m+k)}{2}} & \text{if } (\theta\gamma)^{\frac{q^m-1}{q_1+1}} = -1 \text{ with } s = t+1, \\ -q^{\frac{m}{2}} & \text{if } (\theta\gamma)^{\frac{q^m-1}{q_1+1}} \neq -1 \text{ with } s = t+1, \\ -q^{\frac{(m+k)}{2}} & \text{if } (\theta\gamma)^{\frac{q^m-1}{q_1+1}} = 1 \text{ with } s \geq t+2, \\ q^{\frac{m}{2}} & \text{if } (\theta\gamma)^{\frac{q^m-1}{q_1+1}} \neq 1 \text{ with } s \geq t+2. \end{cases}$$

Finally noting that $\chi_1(\theta\beta) = \Psi_1(\theta A)$ we complete the proof.

□

Remark 2. *Note that the function $S(\theta)$ in Lemma 3 depends on $\gcd(a, m) = 2^t r$ rather than the parameter a_1. Thus, the right hand side of equation (3.3) does not depend on a_1. That is, if all of the other parameters are fixed, the value of N does not change when a_1 is changed. But note that a_1 directly affects the genus of the curve given in (3.1).*

The exponential sum in Lemma 3 will be divided into two pieces (as in equation (3.5) below) due to two different conditions in the definition of the function S. The following lemma shows that the elements of $\mathbb{F}_{q_3}^*$ are independent of these two conditions and so the function S is constant on $\mathbb{F}_{q_3}^*$.

Lemma 4. *Let $t+1 \leq u \leq s$. Then $q_3 - 1$ divides $\dfrac{q^m-1}{q_1+1}$.*

Proof. The exponent $\frac{q^m-1}{q_1+1}$ in Lemma 3 has the following factorization for the case $t+1 \leq u \leq s$:

$$\begin{aligned} \frac{q^m-1}{q_1+1} &= \frac{q^{2^s r m_1}-1}{q^{2^t r}+1} \\ &= \frac{\left(q^{2^{s-1} r m_1}+1\right)\left(q^{2^{s-2} r m_1}+1\right)\cdots\left(q^{2^t r m_1}+1\right)\left(q^{2^t r m_1}-1\right)}{\left(q^{2^t r}+1\right)}. \end{aligned}$$

Since m_1 is odd, $\left(q^{2^t r m_1}+1\right)$ is divisible by $\left(q^{2^t r}+1\right)$. As $\left(q^{2^t r m_1}-1\right)$ is divisible by

$$\left(q^{\frac{n}{2^{u-t}}}-1\right)=\left(q^{2^t\rho n_1}-1\right)=q_3-1,$$

$\frac{q^m-1}{q_1+1}$ is also divisible by q_3-1.

□

This motivates us to work in the subfield $\mathbb{F}_{q_3}\subset\mathbb{F}_{q^n}$ instead of $\mathbb{F}_{q^n}$ itself. Note that for all $\theta\in\mathbb{F}_{q^n}^*$ we can write $\theta=\left(\omega^{''}\right)^j\left(\omega^{'}\right)^i$ for some $i\in\left\{0,1,2,\ldots,\frac{q^n-1}{q_3-1}-1\right\}$ and $j\in\{0,1,2,\ldots,q_3-2\}$ since we have the set equality

$$\mathbb{F}_{q^n}^*=\bigsqcup_{i=0}^{\frac{q^n-1}{q_3-1}-1}\bigsqcup_{j=0}^{q_3-2}\left\{\left(\omega^{''}\right)^j\left(\omega^{'}\right)^i\right\}. \tag{3.4}$$

3.3 Proof of Theorem 1

Now we will give a detailed proof of Theorem 1. Thus throughout this section we assume that q is odd.

Firstly, we will obtain exponential sums over $\mathbb{F}_{q_3}^*$ where the index of these sums runs through the whole subgroup $\mathbb{F}_{q_3}^*\subset\mathbb{F}_{q^n}^*$. Then, we will make use of the set equality (3.4) in order to formulate the number N in terms of some cardinalities.

We have $\mathbb{S}=\left\{0,1,2,\ldots,\frac{q^n-1}{q_3-1}-1\right\}$. Then for any $\theta=\left(\omega^{''}\right)^j\left(\omega^{'}\right)^i\in\mathbb{F}_{q^n}^*$ with $i\in\mathbb{S}$ and $j\in\{0,1,2,\ldots,q_3-2\}$ we have

$$(\theta\gamma)^{\frac{q^m-1}{q_1+1}}=\left(\left(\omega^{'}\right)^i\gamma\right)^{\frac{q^m-1}{q_1+1}}$$

since $\omega^{''}\in\mathbb{F}_{q_3}^*$ and q_3-1 divides $\frac{q^m-1}{q_1+1}$. So let

$$\mathbb{S}_0=\left\{i\in\mathbb{S}:\left(\left(\omega^{'}\right)^i\gamma\right)^{\frac{q^m-1}{q_1+1}}=(-1)^v\right\}.$$

Furthermore, define

$$A_i=\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}\left(\left(\omega^{'}\right)^iA\right)$$

for all $i \in \mathbb{S}$. Then by a simple observation we have $\Psi_1(\theta A) = \tau_1\left(\left(\omega''\right)^j A_i\right)$ where τ_1 is the canonical additive character of $\mathbb{F}_{q_3}$.

Therefore, by Lemma 3 and set equality (3.4), equation (3.3) becomes

$$N = q^m + (-1)^{v+1} q^{\frac{m}{2}} \left[\begin{array}{cc} q^{\frac{k}{2}} \sum\limits_{\substack{\theta \in \mathbb{F}_{q^n}^* \\ (\theta\gamma)^{\frac{q^m-1}{q_1+1}} = (-1)^v}} \Psi_1(\theta A) & - \sum\limits_{\substack{\theta \in \mathbb{F}_{q^n}^* \\ (\theta\gamma)^{\frac{q^m-1}{q_1+1}} \neq (-1)^v}} \Psi_1(\theta A) \end{array} \right] \tag{3.5}$$

$$= q^m + (-1)^{v+1} q^{\frac{m}{2}} \left[q^{\frac{k}{2}} \sum_{i \in \mathbb{S}_0} \sum_{j=0}^{q_3-2} \tau_1\left(\left(\omega''\right)^j A_i\right) - \sum_{i \in \mathbb{S} \setminus \mathbb{S}_0} \sum_{j=0}^{q_3-2} \tau_1\left(\left(\omega''\right)^j A_i\right) \right].$$

Now we define the cardinalities :

$$M_0 = |\{i \in \mathbb{S}_0 : A_i = 0\}| \text{ and } \overline{M_0} = |\{i \in \mathbb{S} \setminus \mathbb{S}_0 : A_i = 0\}|.$$

As ω'' is a generator of the multiplicative group $\mathbb{F}_{q_3}^*$, we have

$$\begin{aligned} \sum_{i \in \mathbb{S}_0} \sum_{j=0}^{q_3-2} \tau_1\left(\left(\omega''\right)^j A_i\right) &= M_0(q_3 - 1) + (|\mathbb{S}_0| - M_0)(-1) \\ &= q_3 M_0 - |\mathbb{S}_0|. \end{aligned} \tag{3.6}$$

Similarly,

$$\begin{aligned} \sum_{i \in \mathbb{S} \setminus \mathbb{S}_0} \sum_{j=0}^{q_3-2} \tau_1\left(\left(\omega''\right)^j A_i\right) &= \overline{M_0}(q_3 - 1) + \left(|\mathbb{S}| - |\mathbb{S}_0| - \overline{M_0}\right)(-1) \\ &= q_3 \overline{M_0} + |\mathbb{S}_0| - \frac{q^n - 1}{q_3 - 1}. \end{aligned} \tag{3.7}$$

Finally, putting (3.6) and (3.7) into (3.5) we get the following proposition.

Proposition 2. *We have*

$$N = q^m + (-1)^{v+1} q^{\frac{m}{2}} \left[q^{\frac{k}{2}} (q_3 M_0 - |\mathbb{S}_0|) - \left(q_3 \overline{M_0} + |\mathbb{S}_0| - \left(\frac{q^n - 1}{q_3 - 1} \right) \right) \right]. \tag{3.8}$$

In order to find N we need to compute the numbers M_0, $\overline{M_0}$ and $|\mathbb{S}_0|$ when v is even and when v is odd separately. Proposition 3 below shows that the sum of M_0 and $\overline{M_0}$ is fixed, and it is enough to find M_0 only.

Proposition 3. *We have* $M_0 + \overline{M_0} = \dfrac{q^n - q_3}{q_3(q_3-1)}$.

Proof. For all $\theta \in \mathbb{F}_{q^n}^*$ we have

$$\theta = \left(\omega^{''}\right)^j \left(\omega^{'}\right)^i$$

for some $i \in \mathbb{S}$ and $j \in \{0, 1, 2, \ldots, q_3 - 2\}$. Then, for a fixed

$$j \in \{0, 1, 2, \ldots, q_3 - 2\}$$

we have

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}(\theta A) = \left(\omega^{''}\right)^j \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}\left(\left(\omega^{'}\right)^i A\right) = \left(\omega^{''}\right)^j A_i = 0$$

if and only if $A_i = 0$. Therefore, there are $q_3 - 1$ choices for j. This gives the equality

$$\begin{aligned}\left|\left\{\theta A \in \mathbb{F}_{q^n}^* : \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}(\theta A) = 0\right\}\right| &= (q_3 - 1)\left|\{i \in \mathbb{S} : A_i = 0\}\right| \\ &= (q_3 - 1)\left(M_0 + \overline{M_0}\right).\end{aligned}$$

As $A \neq 0$, θA runs through $\mathbb{F}_{q^n}^*$. Then,

$$\left|\left\{\theta A \in \mathbb{F}_{q^n}^* : \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}(\theta A) = 0\right\}\right| = \left|\left\{z \in \mathbb{F}_{q^n} : \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}(z) = 0\right\}\right| - 1.$$

Since the polynomial $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}(z) = z + z^{q_3} + z^{\left(q_3{}^2\right)} + \cdots + z^{\left(\frac{q^n}{q_3}\right)}$ splits in $\mathbb{F}_{q^n}$, it has $\frac{q^n}{q_3}$ distinct roots in $\mathbb{F}_{q^n}$ (see [34, Theorem 2.25]). Thus,

$$\left|\left\{z \in \mathbb{F}_{q^n} : \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}(z) = 0\right\}\right| - 1 = \frac{q^n}{q_3} - 1.$$

Finally, we get $(q_3 - 1)\left(M_0 + \overline{M_0}\right) = \frac{q^n}{q_3} - 1$ which completes the proof.

□

The following proposition is another way of expressing M_0 in terms of the number of the roots of a polynomial in $\mathbb{F}_{q^n}^*$. If the cardinality in the following proposition can be evaluated, then the subcase which is not addressed in this chapter will be solved.

Proposition 4. *We have* $M_0 = \dfrac{\left|\left\{z \in \mathbb{F}_{q^n}^* : g(z) = \left((z^{q_3} - z)\,\frac{\gamma}{A}\right)^{\frac{q^m-1}{q_1+1}} - 1 = 0\right\}\right|}{(q_3-1)q_3}$.

Proof. Firstly,

$$\begin{aligned} M_0 &= \left|\left\{i \in \mathbb{S}_0 : \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}\left(\left(\omega^{'}\right)^i A\right) = 0\right\}\right| \\ &= \left|\left\{i \in \mathbb{S} : \left(\left(\omega^{'}\right)^i \gamma\right)^{\frac{q^m-1}{q_1+1}} = 1 \text{ and } \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}\left(\left(\omega^{'}\right)^i A\right) = 0\right\}\right|. \end{aligned}$$

As $\theta = \left(\omega^{''}\right)^j \left(\omega^{'}\right)^i$ for some $i \in \mathbb{S}$ and $j \in \{0, 1, 2, \ldots, q_3 - 2\}$ for all $\theta \in \mathbb{F}_{q^n}^*$, we have

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}(\theta A) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}\left(\left(\omega^{''}\right)^j \left(\omega^{'}\right)^i A\right) = 0$$

if and only if

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}\left(\left(\omega^{'}\right)^i A\right) = 0.$$

Also we have $(\theta\gamma)^{\frac{q^m-1}{q_1+1}} = \left(\left(\omega^{'}\right)^i \gamma\right)^{\frac{q^m-1}{q_1+1}}$. Thus, the integer j does not affect the set conditions above and there are $q_3 - 1$ free choices for j. That is,

$$\left|\left\{i \in \mathbb{S} : \left(\left(\omega^{'}\right)^i \gamma\right)^{\frac{q^m-1}{q_1+1}} = 1 \text{ and } \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}\left(\left(\omega^{'}\right)^i A\right) = 0\right\}\right|$$

$$= \frac{1}{q_3-1}\left|\left\{\theta \in \mathbb{F}_{q^n}^* : (\theta\gamma)^{\frac{q^m-1}{q_1+1}} = 1 \text{ and } \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}(\theta A) = 0\right\}\right|.$$

Moreover, we know that $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}(\theta A) = 0$ if and only if $\theta A = \sigma^{q_3} - \sigma$ for some $\sigma \in \mathbb{F}_{q^n}$ (see [34, Theorem 2.25]). This yields,

$$\frac{1}{q_3-1}\left|\left\{\theta \in \mathbb{F}_{q^n}^* : (\theta\gamma)^{\frac{q^m-1}{q_1+1}} = 1 \text{ and } \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}(\theta A) = 0\right\}\right|$$

$$= \frac{1}{q_3-1}\left|\left\{\tfrac{\sigma^{q_3}-\sigma}{A} : \sigma \in \mathbb{F}_{q^n} \text{ and } \left(\tfrac{\sigma^{q_3}-\sigma}{A}\gamma\right)^{\frac{q^m-1}{q_1+1}} = 1\right\}\right|$$

$$= \frac{1}{q_3-1}\left|\left\{\sigma^{q_3} - \sigma : \sigma \in \mathbb{F}_{q^n} \text{ and } \left(\tfrac{\sigma^{q_3}-\sigma}{A}\gamma\right)^{\frac{q^m-1}{q_1+1}} = 1\right\}\right|.$$

The polynomial $p(x) = x^{q_3} - x$ is constant on each coset of the quotient group $(\mathbb{F}_{q^n}/\mathbb{F}_{q_3}, +)$ and this means we have q_3 repeated values for $\sigma^{q_3} - \sigma$. In other words we have

$$\frac{1}{q_3 - 1}\left|\left\{\sigma^{q_3} - \sigma : \sigma \in \mathbb{F}_{q^n} \text{ and } \left(\tfrac{\sigma^{q_3}-\sigma}{A}\gamma\right)^{\frac{q^m-1}{q_1+1}} = 1\right\}\right|$$

$$= \frac{1}{(q_3-1)q_3}\left|\left\{z \in \mathbb{F}_{q^n} : g(z) = \left[(z^{q_3} - z)\,\tfrac{\gamma}{A}\right]^{\frac{q^m-1}{q_1+1}} - 1 = 0\right\}\right|$$

$$= \frac{1}{(q_3-1)q_3}\left|\left\{z \in \mathbb{F}^*_{q^n} : g(z) = \left[(z^{q_3} - z)\,\tfrac{\gamma}{A}\right]^{\frac{q^m-1}{q_1+1}} - 1 = 0\right\}\right|.$$

□

We continue our proof by considering our two cases.

Case s=t+1 (=u):

As $u = t + 1$ in this case, $u - t = 1$ and then $q_3 = q^{\frac{n}{2}}$. So,

$$\frac{q^n - 1}{q_3 - 1} = \frac{q^n - 1}{q^{\frac{n}{2}} - 1} = q^{\frac{n}{2}} + 1.$$

Before finding $|\mathbb{S}_0|$, we will firstly find the integers $i \in \mathbb{S}$ such that $A_i = 0$ in order to describe M_0 and $\overline{M_0}$. Note that by Proposition 3 we get $M_0 + \overline{M_0} = 1$. Now we will find the conditions when $\overline{M_0} = 1$ and when $M_0 = 1$.

We have

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^{\frac{n}{2}}}}\left(\left(\omega'\right)^i A\right) = A_i = \left(\omega'\right)^i A + \left(\left(\omega'\right)^i A\right)^{q^{\frac{n}{2}}} = 0$$

if and only if

$$\left(\omega'\right)^{i\left(q^{\frac{n}{2}}-1\right)} = -A^{q^n - q^{\frac{n}{2}}} = \left(\omega'\right)^l$$

or equivalently

$$l - i\left(q^{\frac{n}{2}} - 1\right) \equiv 0 \mod (q^n - 1). \tag{3.9}$$

As we have

$$i \in \mathbb{S} = \left\{0, 1, 2, \ldots, \tfrac{q^n-1}{q_3-1} - 1\right\} = \left\{0, 1, 2, \ldots, q^{\frac{n}{2}}\right\}$$

and $l \in \{0, 1, 2, \ldots, q^n - 2\}$, the inequality

$$1 - q^n < l - i\left(q^{\frac{n}{2}} - 1\right) < q^n - 1$$

holds for all $i \in \mathbb{S}$. That is, (3.9) is equivalent to $l - i\left(q^{\frac{n}{2}} - 1\right) = 0$. Thus, the only integer i such that $A_i = 0$ is $i = \dfrac{l}{q^{\frac{n}{2}} - 1} = l^{'}$ which lies in the set $\mathbb{S}$.

Then we get

$$M_0 = \begin{cases} 1 & \text{if } l^{'} \in \mathbb{S}_0 \\ 0 & \text{if } l^{'} \in \mathbb{S} \setminus \mathbb{S}_0 \end{cases} \text{ and } \overline{M_0} = \begin{cases} 0 & \text{if } l^{'} \in \mathbb{S}_0 \\ 1 & \text{if } l^{'} \in \mathbb{S} \setminus \mathbb{S}_0. \end{cases}$$

Now we will describe the set $\mathbb{S}_0$. This is the case where $v = 2^{s-(t+1)} = 2^0 = 1$. So,

$$\mathbb{S}_0 = \left\{ i \in \mathbb{S} : \left(\left(\omega^{'}\right)^i \gamma\right)^{\frac{q^m-1}{q_1+1}} = -1 \right\}.$$

Put $R = \dfrac{q^m - 1}{q^n - 1}$ from now on. Given $\gamma = \omega^h$ we have

$$\left(\left(\omega^{'}\right)^i \gamma\right)^{\frac{q^m-1}{q_1+1}} = -1$$

if and only if

$$h + iR \equiv \frac{q_1 + 1}{2} \mod (q_1 + 1) \tag{3.10}$$

where $\omega^{'} = \omega^R$. Note that

$$R \equiv m_2 \frac{q_1 + 1}{q_2 + 1} \mod (q_1 + 1).$$

So (3.10) is equivalent to

$$h + im_2 \frac{q_1 + 1}{q_2 + 1} \equiv \frac{q_1 + 1}{2} \mod (q_1 + 1). \tag{3.11}$$

As $\gcd\left(m_2 \frac{q_1+1}{q_2+1}, q_1 + 1\right) = \frac{q_1+1}{q_2+1} B_1$, there is no integer i satisfying (3.11) if

$$h \equiv \frac{q_1 + 1}{2} \mod \left(\frac{q_1 + 1}{q_2 + 1} B_1\right) \tag{3.12}$$

does not hold.

Assume that $h \equiv \frac{q_1+1}{2} \mod \left(\frac{q_1+1}{q_2+1}B_1\right)$ holds. Put

$$B_2 = \frac{\frac{q_1+1}{2} - h}{\frac{q_1+1}{q_2+1}B_1}.$$

Then (3.11) is equivalent to

$$i\frac{m_2}{B_1} \equiv B_2 \mod \left(\frac{q_2+1}{B_1}\right). \tag{3.13}$$

Note that i is uniquely determined modulo $\frac{q_2+1}{B_1}$ by (3.13). Thus, $\mathbb{S}_0$ will be explicitly

$$\mathbb{S}_0 = \left\{ i \in \mathbb{S} : i\frac{m_2}{B_1} \equiv B_2 \mod \left(\tfrac{q_2+1}{B_1}\right) \right\}$$

when (3.12) holds. So, putting

$$|\mathbb{S}_0| = \frac{q^{\frac{n}{2}}+1}{(q_2+1)/B_1} = \frac{q^{\frac{n}{2}}+1}{q_2+1}B_1$$

in the formula (3.8) we get the desired result explicitly for the case where (3.12) holds.

Now, assume that $h \not\equiv \frac{q_1+1}{2} \mod \left(\frac{q_1+1}{q_2+1}B_1\right)$. Then, there is no integer $i \in \mathbb{S}$ satisfying (3.11) and so satisfying (3.10). Thus,

$$\mathbb{S}_0 = \left\{ i \in \mathbb{S} : \left(\left(\omega'\right)^i \gamma\right)^{\frac{q^m-1}{q_1+1}} = -1 \right\} = \emptyset.$$

Therefore, $l' \notin \mathbb{S}_0$. Hence, by putting $|\mathbb{S}_0| = 0$, $M_0 = 0$ and $\overline{M_0} = 1$ in the formula (3.8) we find N explicitly for the case where (3.12) does not hold.

This completes the proof of the case $s = t + 1$.

Case s $\geq$ t+2 :

This time we will describe $\mathbb{S}_0$ firstly. This is the case where $v = 2^{s-(t+1)}$ is even in the formula (3.8). So,

$$\mathbb{S}_0 = \left\{ i \in \mathbb{S} : \left(\left(\omega'\right)^i \gamma\right)^{\frac{q^m-1}{q_1+1}} = 1 \right\}.$$

As $\gamma = \omega^h$, we have

$$\left(\left(\omega'\right)^i \gamma\right)^{\frac{q^m-1}{q_1+1}} = 1$$

if and only if

$$h + iR \equiv 0 \mod (q_1 + 1). \tag{3.14}$$

Note that

$$R \equiv 2^{s-u} m_2 \frac{q_1+1}{q_2+1} \mod (q_1 + 1)$$

in this case. So, (3.14) is equivalent to

$$h + i2^{s-u} m_2 \frac{q_1+1}{q_2+1} \equiv 0 \mod (q_1 + 1). \tag{3.15}$$

We have 2 cases again. Note that

$$\gcd\left(2^{s-u} m_2 \frac{q_1+1}{q_2+1}, q_1 + 1\right) = \frac{q_1+1}{q_2+1} B_1.$$

Hence if

$$h \equiv 0 \mod \left(\frac{q_1+1}{q_2+1} B_1\right) \tag{3.16}$$

does not hold, then there is no integer i satisfying (3.15).

Assume that $h \equiv 0 \mod \left(\frac{q_1+1}{q_2+1} B_1\right)$ holds and put

$$B_2 = \frac{-h}{\frac{q_1+1}{q_2+1} B_1}.$$

Then (3.15) is equivalent to

$$i \frac{2^{s-u} m_2}{B_1} \equiv B_2 \mod \left(\frac{q_2+1}{B_1}\right). \tag{3.17}$$

Hence, (3.17) determines i modulo $\frac{q_2+1}{B_1}$ again and we obtain

$$\mathbb{S}_0 = \left\{ i \in \mathbb{S} : i \frac{2^{s-u} m_2}{B_1} \equiv B_2 \mod \left(\tfrac{q_2+1}{B_1}\right) \right\}.$$

Therefore, $|\mathbb{S}_0| = \dfrac{|\mathbb{S}|}{(q_2+1)/B_1} = \dfrac{(q^n-1)B_1}{(q_3-1)(q_2+1)}$ in the formula (3.8).

For the assumption $u = t+1$, we will have $u - t = 1$ and so $q_3 = q^{\frac{n}{2^{u-t}}} = q^{\frac{n}{2}}$. This yields

$$\frac{q^n-1}{q_3-1} = \frac{q^n-1}{q^{\frac{n}{2}}-1} = q^{\frac{n}{2}}+1$$

again as above. By the same argument, the only integer $i \in \mathbb{S}$ such that $A_i = 0$ is $l' = \dfrac{l}{q^{\frac{n}{2}}-1}$. Hence

$$M_0 = \begin{cases} 1 & \text{if } l' \in \mathbb{S}_0 \\ 0 & \text{if } l' \in \mathbb{S} \setminus \mathbb{S}_0 \end{cases} \text{ and } \overline{M_0} = \begin{cases} 0 & \text{if } l' \in \mathbb{S}_0 \\ 1 & \text{if } l' \in \mathbb{S} \setminus \mathbb{S}_0. \end{cases}$$

Therefore, N is found for the case where $u = t+1$ and (3.16) holds.

Now, assume $h \not\equiv 0 \mod \left(\dfrac{q_1+1}{q_2+1}B_1\right)$. Then, there is no integer $i \in \mathbb{S}$ satisfying (3.15) and so satisfying (3.14). Thus, $\mathbb{S}_0 = \emptyset$. So we have $|\mathbb{S}_0| = 0$ and $M_0 = 0$ in the formula (3.8). By Proposition 3, $\overline{M_0} = \dfrac{\frac{q^n}{q_3}-1}{q_3-1}$. So N is found explicitly for the case (3.16) does not hold.

This completes the proof of Theorem 1.

We finish this section with some experimental results for the subcase that $s = u \geq t+2$ with $h \equiv 0 \mod \left(\frac{q_1+1}{q_2+1}B_1\right)$. Proposition 2 and Proposition 3 together show that the computation of N depends only on the computation of M_0 as $|\mathbb{S}_0|$ can be computed in each case. Therefore, in the experimental results below, we compute M_0 only.

Let $A = \left(\omega'\right)^c$ for some integer c such that $0 \leq c < q^n - 1$. Under the assumptions

- $s = u = t+2$
- $m_1 = 1$
- $B_1B_2 + c \equiv 0 \mod (q_2+1)$

we can show that $M_0 = 1$:

As $m_1 = 1$, we have $m_2 = 1$, $n_1 = 1$ and $q_2 = q_3$. Then we have

$$\mathbb{S}_0 = \left\{ i \in \mathbb{S} : i\frac{m_2}{B_1} \equiv B_2 \mod \left(\frac{q_2+1}{B_1}\right) \right\}$$

in this case (note that $s = u$). This yields that $i \in \mathbb{S}_0$ implies $i = f(q_2+1) + B_1B_2$ for some integer f. So $i + c \equiv 0 \mod (q_2+1)$. Then put $c_i = i + c \mod \left(\frac{q^n-1}{q_3-1}\right)$. Note that c_i is uniquely determined by the integer i as c is fixed. We have,

$$A_i = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}\left(\left(\omega^{'}\right)^i A\right) = 0$$

if and only if

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q_3}}\left(\left(\omega^{'}\right)^{c_i}\right) = 0.$$

That is,

$$\left(\omega^{'}\right)^{c_i} + \left(\omega^{'}\right)^{c_i q_3} + \left(\omega^{'}\right)^{c_i {q_3}^2} + \left(\omega^{'}\right)^{c_i {q_3}^3} = 0. \tag{3.18}$$

Put $z = \left(\omega^{'}\right)^{c_i(q_3-1)}$. Then $z^{\left({q_3}^2+1\right)} = 1$ as $c_i \equiv 0 \mod (q_2+1)$. Hence (3.18) is satisfied if and only if

$$1 + z + z^{(q_3+1)} + z^{\left({q_3}^2+q_3+1\right)} = (z+1)\left(z^{q_3}+1\right) = 0.$$

This happens only when

$$c_i \equiv \frac{q^n-1}{2(q_3-1)} \mod \left(\frac{q^n-1}{q_3-1}\right).$$

So $c_i = \dfrac{q^n-1}{2(q_3-1)}$ is determined uniquely. This yields that there is only one $i \in \mathbb{S}_0$ such that $A_i = 0$ and so $M_0 = 1$.

For the case $B_1B_2 + c \not\equiv 0 \mod (q_2+1)$, we have examples with $q = 3$ calculated in Magma. In each example, we find $M_0 = q_3 + 1$.

- If $q = 3$, $s = 2$, $u = 2$, $t = 2$, $\rho = 1$, $m = 4r$ and $n = 4\rho$, we have $M_0 = 4$ and $\overline{M_0} = 9$.

- If $q = 3$, $s = 2$, $u = 2$, $t = 2$, $\rho = 3$, $m = 4r$ and $n = 4\rho$, we have $M_0 = 28$ and $\overline{M_0} = 729$.

- If $q = 3$, $s = 2$, $u = 2$, $t = 2$, $\rho = 5$, $m = 4r$ and $n = 4\rho$, we have $M_0 = 244$ and $\overline{M_0} = 590049$.

3.4 Analogous results for the finite fields having even characteristic

Throughout this section we consider finite fields of characteristic 2. So we have $p = 2$ in this section. The following is analogous to Theorem 13 and Theorem 14 in the Appendix A.

Theorem 2. *Assume that $p = 2$ and $u \leq t$.*

- ***Case s $\leq$ t:***

$$N = q^m.$$

- ***Case t+1 $\leq$ s:***

If $(\gamma)^{\frac{q^m-1}{q_1+1}} \neq 1$, *then*

$$N = \begin{cases} q^m + (-1)^v q^{\frac{m}{2}}(q^n - 1) & \text{if } A = 0, \\ \\ q^m - (-1)^v q^{\frac{m}{2}} & \text{if } A \neq 0. \end{cases}$$

If $(\gamma)^{\frac{q^m-1}{q_1+1}} = 1$, *then*

$$N = \begin{cases} q^m - (-1)^v q^{\frac{m+k}{2}}(q^n - 1) & \text{if } A = 0, \\ \\ q^m + (-1)^v q^{\frac{m+k}{2}} & \text{if } A \neq 0. \end{cases}$$

The equation (3.3) in Section 3.2 is valid also for $p = 2$. So the proof of Theorem 2 can be obtained similarly using Weil sums evaluated in [11]. Furthermore, note that

the cases $t+1 \leq s$ and $s \leq t$ with $\frac{m}{n}$ is even are covered by the approach in [44]. This explains how we prove Theorem 2.

Next we present our results for the case $t+1 \leq u \leq s$ in Theorem 3 and Theorem 4 which are analogous versions of Theorem 15 in the Appendix A and Theorem 1 respectively. Then, we give a sketch of the proof for both, Theorem 3 and Theorem 4.

Theorem 3. *Assume that $p=2$, $t+1 \leq u \leq s$ and $A=0$. Recall that $B_1 = \gcd(2^{s-u}m_2, q_2+1)$.*

If $h \not\equiv 0 \mod \left(\frac{q_1+1}{q_2+1}B_1\right)$, *then*

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

If $h \equiv 0 \mod \left(\frac{q_1+1}{q_2+1}B_1\right)$, *then*

$$N = q^m + (-1)^{v+1} q^{\frac{m}{2}} \left[B_1 \frac{q^n-1}{q_2+1}(q^{\frac{k}{2}}+1) - (q^n-1) \right].$$

Theorem 4. *Assume that $p=2$, $t+1 \leq u \leq s$ and $A \neq 0$. Let l be the integer with $0 \leq l < q^n-1$ such that $-A^{q^n-q^{\frac{n}{2}}} = \left(\omega^{'}\right)^l$ as $\omega^{'}$ is a generator of $\mathbb{F}_{q^n}^*$. Moreover, put $l^{'} = \dfrac{l}{q^{\frac{n}{2}}-1}$ and recall that $B_1 = \gcd(2^{s-u}m_2, q_2+1)$.*

If $h \not\equiv 0 \mod \left(\frac{q_1+1}{q_2+1}B_1\right)$, *then*

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

If $h \equiv 0 \mod \left(\frac{q_1+1}{q_2+1}B_1\right)$ *and* $u = t+1$, *then*

$$N = \begin{cases} q^m + (-1)^{v+1} q^{\frac{m}{2}} \left[q^{\frac{(k+n)}{2}} + q^{\frac{n}{2}} + 1 - B_1(q^{\frac{k}{2}}+1)\left(\frac{q^{\frac{n}{2}}+1}{q_2+1}\right)\right] \\ \qquad \text{if } l^{'}\dfrac{2^{s-u}m_2}{B_1} \equiv B_2 \mod \left(\frac{q_2+1}{B_1}\right), \\ q^m + (-1)^{v+1} q^{\frac{m}{2}} \left[1 - B_1(q^{\frac{k}{2}}+1)\left(\frac{q^{\frac{n}{2}}+1}{q_2+1}\right)\right] \\ \qquad \text{if } l^{'}\dfrac{2^{s-u}m_2}{B_1} \not\equiv B_2 \mod \left(\frac{q_2+1}{B_1}\right), \end{cases}$$

where $B_2 = \dfrac{-h}{\frac{q_1+1}{q_2+1}B_1}$.

Proof. The proofs of Theorem 3 and Theorem 4 are the same with the proof of Theorem 1 with two small modifications. According to the results in [11], we only change the definitions of the set $\mathbb{S}_0$ defined in Section 3.1 and the function S given in Definition 2 as follows:

For $p = 2$, define

$$\mathbb{S}_0 = \left\{ i \in \mathbb{S} : \left(\left(\omega' \right)^i \gamma \right)^{\frac{q^m-1}{q_1+1}} = 1 \right\}$$

and

$$S(\theta) = \begin{cases} (-1)^{v+1} q^{\frac{(m+k)}{2}} & \text{if } (\theta\gamma)^{\frac{q^m-1}{q_1+1}} = 1 \, , \\ -(-1)^{v+1} q^{\frac{m}{2}} & \text{if } (\theta\gamma)^{\frac{q^m-1}{q_1+1}} \neq 1 \, . \end{cases}$$

Then, one can deduce that equation (3.8) is valid also for $p = 2$ by following the analogous steps in Section 3.2 and Section 3.3. Hence the proof of Theorem 3 and Theorem 4 can be similarly obtained using equation (3.8).

□

3.5 Examples of maximal and minimal curves

For the number $N(\mathfrak{X})$, the Hasse–Weil inequality states that:

$$q^m + 1 - 2g(\mathfrak{X})\sqrt{q^m} \leq N(\mathfrak{X}) \leq q^m + 1 + 2g(\mathfrak{X})\sqrt{q^m}.$$

Since the genus of the curve is $g(\mathfrak{X}) = \dfrac{(q^n-1)q^a}{2}$, we get

$$q^m + 1 - (q^n-1)q^a q^{\frac{m}{2}} \leq N(\mathfrak{X}) \leq q^m + 1 + (q^n-1)q^a q^{\frac{m}{2}}.$$

A class of maximal and minimal curves which follows from the results of Theorem 14 of the Appendix A is already given in both [12] and [44]. Now in the following corollary, we give our examples of maximal and minimal curves which are not covered in [12] and [44]. The following corollary is a result of Theorem 3 and Theorem 15 in the Appendix A.

Corollary 1. *Consider the curve*

$$\mathfrak{X}: \quad y^{q^n} - y = \gamma x^{q^a+1} + \beta$$

and let all other variables be given as in Section 3.1.

- ***Case p=2 :*** *Under the conditions*

  (i) $A = 0$,

  (ii) $h \equiv 0 \mod \left(\frac{q_1+1}{q_2+1} B_1\right)$,

  (iii) $a_1 = 1$ *and* $B_1 = q_2 + 1$,

  the curve $\mathfrak{X}$ *is maximal if* $s = t + 1$ *and minimal if* $s \geq t + 2$.

- ***Case p is odd :*** *Under the conditions*

  (i) $A = 0$,

  (ii) $h \equiv 0 \mod \left(\frac{q_1+1}{q_2+1} B_1\right)$,

  (iii) $a_1 = 1$ *and* $B_1 = q_2 + 1$,

  (iv) $s \geq t + 2$,

  the curve $\mathfrak{X}$ *is minimal.*

Example 1. *Let* $\underline{\beta = 0}, \underline{\gamma = 1}, \underline{q = 2^e}, \underline{m = 2^s\left(q^{2^t}+1\right)}, \underline{n = 2^u}, \underline{a = 2^t}$ *for some positive integers* e, s, t, u *with* $t + 1 \leq u \leq s$. *Hence the curve* $\mathfrak{X}$ *will be maximal when* $s = t + 1$ *and it will be minimal when* $s \geq t + 2$.

- *Choose* $e = s = u = t + 1 = 10000$. *Then* $\mathfrak{X}$ *is maximal.*
- *Choose* $e = u = t + 1 = 10000$ *and* $s = 50000$. *Then* $\mathfrak{X}$ *is minimal.*

CHAPTER 4

WALSH TRANSFORMS OF GOLD TYPE AND KASAMI-WELCH TYPE FUNCTIONS AND RATIONAL POINTS

4.1 Introduction

In this chapter, we evaluate the Walsh transforms of Gold type and Kasami-Welch type Boolean functions firstly. Then we use these results in order to compute the number of rational points of a class of Artin-Schreier type curves which have the form (2.11). The results of this chapter are based on the publication [7] and the submitted paper [8].

Definition 3. *Let f be a Boolean function $f : V_m \longrightarrow \mathbb{F}_2$, where V_m is a m-dimensional vector space over $\mathbb{F}_2$. The **Walsh transform** (or Walsh-Hadamard transform) of f at α is the function $f^W : V_m \longrightarrow \mathbb{Z}$ defined by*

$$f^W(\alpha) = \sum_{x \in V_m} (-1)^{f(x)+\langle \alpha, x \rangle} \tag{4.1}$$

where $\langle \alpha, x \rangle$ denotes an (non-degenerate) inner product on V_m.

We refer, for example, to [2] for more details on Walsh transform for Boolean functions. Let $K = \mathbb{F}_{2^m}$ denote the finite field of 2^m elements. When $V_m = K$, a natural choice for $\langle \alpha, x \rangle$ is $\mathrm{Tr}_K(\alpha x)$. Then equation (4.1) becomes

$$f^W(\alpha) = \sum_{x \in K} (-1)^{f(x)+\mathrm{Tr}_K(\alpha x)}. \tag{4.2}$$

The *Walsh spectrum* of a Boolean function $f : K \longrightarrow \mathbb{F}_2$ is defined to be the set

$$\left\{f^W(\alpha) : \alpha \in K\right\}.$$

When the spectrum is precisely $\left\{\pm 2^{\frac{m}{2}}\right\}$, f is called ***bent function***. For an integer $0 \leq r \leq m$, a function $f : K \longrightarrow \mathbb{F}_2$ is called **r-*plateaued*** (r-*partially bent*) if its Walsh spectrum is $\left\{0, \pm 2^{\frac{1}{2}(m+r)}\right\}$. Bent functions have significance due to their applications in cryptography and r-plateaued functions gain interest as they can be used to construct bent functions (see [32, 41] for instance).

Among the most famous examples of functions having 3-valued Walsh spectrum, we have Gold functions [23] $f(x) = \mathrm{Tr}_K\left(x^{2^a+1}\right)$, with a relatively prime to m and m odd. Gold [23] determined $f^W(\alpha)$ in terms of $f^W(1)$ and $f^W(1)$ is evaluated first in [16] and then in [32]. Furthermore, more general Gold functions are studied in the appendix of [16].

The other famous examples having 3-valued Walsh spectrum are Kasami-Welch functions [29] (see also [17]) $f(x) = \mathrm{Tr}_K\left(x^{4^a-2^a+1}\right)$, with the same hypothesis that a is relatively prime to m and m is odd. Both Gold and Kasami-Welch functions have the spectrum $\left\{0, \pm 2^{\frac{(m+1)}{2}}\right\}$ (i.e. they are 1-plateaued).

In this chapter, we deal with the Walsh transforms of Gold type and Kasami-Welch type functions firstly. Without loss of generality we assume $0 \leq a < b$ ($a = b$ is a trivial case) and by a Gold type function we mean

$$f(x) = \mathrm{Tr}_K\left(x^{2^a+1} + x^{2^b+1}\right), \tag{4.3}$$

and by a Kasami-Welch type function we mean

$$f(x) = \mathrm{Tr}_K\left(x^{\frac{2^{ta}+1}{2^a+1}}\right), t \text{ odd}. \tag{4.4}$$

Gold type functions were studied by various authors in literature. For instance, in [32], Lahtonen, McGuire and Ward give $f^W(0)$ for $f(x) = \mathrm{Tr}_K\left(x^{2^a+1} + x^{2^b+1}\right)$, where $\gcd(b-a, m) = \gcd(b+a, m) = 1$ and m odd. Then, using the results of Fitzgerald in [21], Roy [41] evaluated $f^W(\alpha)$

- for any $\alpha \in K$ with m odd,
- for $\alpha \in K$ with $\mathrm{Tr}_K(\alpha) = 0$ and m even,

and stated that the case

- $\mathrm{Tr}_K(\alpha) = 1$ with m even

is open. However, we observed that Roy's result for the case

- $\alpha \in K$ with $\mathrm{Tr}_K(\alpha) = 0$ and m even

does not hold for some α's. We give a counterexample for such an α in *Example 2* below in Section 4.3. In Corollary 2 in Section 4.3, we will complete the evaluation of $f^W(\alpha)$ by fixing the problem in the result of Roy and giving $f^W(\alpha)$ for the remaining open case $\mathrm{Tr}_K(\alpha) = 1$ with m even.

In Section 4.3 we consider a more general function $f(x) = \mathrm{Tr}_K\left(x^{2^a+1} + x^{2^b+1}\right)$ with the assumption that

$$\gcd(b-a, m) = \gcd(b+a, m) \text{ (not necessarily } = 1)$$

and generalize Roy's results by evaluating $f^W(\alpha)$ except a very particular case (see Theorem 6 and Theorem 7).

In Section 4.4, the condition

$$\gcd(b-a, m) = \gcd(b+a, m)$$

is removed. Theorem 10 completes the evaluation of $f^W(\alpha)$ without any restriction on m, a, b and α. Moreover, in the second result Theorem 11 of Section 4.4 we generalize the results found in Theorem 10. Let f_γ be the following function

$$f_\gamma(x) = \mathrm{Tr}_K\left(\gamma x^{2^a+1} + \gamma x^{2^b+1}\right), \tag{4.5}$$

where the coefficient γ is taken arbitrarily from $\mathbb{F}_{2^m} \cap \mathbb{F}_{2^{b-a}}$. Explicit evaluation of the Walsh transform of f_γ at $\alpha \in K$ is given in Theorem 11 without any restriction on m, a, b and α.

Kasami-Welch type functions, $f(x) = \mathrm{Tr}_K(x^c)$ where $c = \frac{2^{ta}+1}{2^a+1}$ and t is odd, were studied by Niho in his thesis [38]. In [32], Lahtonen, McGuire and Ward evaluated

$f^W(1)$ under certain conditions. In [33], Langevin, Leander and McGuire gave a counterexample to a conjecture of Niho [38] by determining the Walsh spectrum of f explicitly when $m = 25$, $a = 3$, $t = 19$ and when $m = 23$, $a = 1$, $t = 7$. Then, Roy in [41] generalized the related result in [32] when m is odd. We also give a generalization of Roy's result for m even with Theorem 8 in Section 4.3 below.

Eventually, in this chapter we improve and generalize the related results [32, 41] in literature.

The rest of the chapter is organized as follows. We introduce some notation and give some background in Section 4.2. In Section 4.3, the case where $\gcd(b-a,m) = \gcd(b+a,m)$ is analyzed. Finally, this condition is removed in Section 4.4.

4.2 Preliminaries

In this section we introduce our notation and present some background about quadratic forms that we use when proving our results in Section 4.3 and Section 4.4.

Let n be an arbitrary positive integer. Throughout the chapter $v_p(n)$ will denote the highest non-negative exponent v such that p^v divides n (that is, the p-adic valuation) and $\left(\frac{a}{n}\right)$ will denote the Jacobi symbol of a modulo n. For finite fields F and E, we will write $\mathrm{Tr}_{E/F}$ for the relative trace from E to F and for the absolute trace from E to $\mathbb{F}_2$ we will write Tr_E. As the characteristic is 2 in this chapter and the second root of unity is -1, we will use sometimes $(-1)^{\mathrm{Tr}_E(x)}$ for $\chi_{_E}(x)$ where $\chi_{_E}$ is the canonical additive character of a finite field E of characteristic 2. Furthermore, for the sake of simplicity we will put

- $d_1 = \gcd(b-a,m)$,
- $d_2 = \gcd(b+a,m)$,
- if $d_1 = d_2$ then $d = d_1 = d_2$,
- $e = \gcd(d_1,d_2)$,
- $\nu = max\{v_2(b-a), v_2(b+a)\}$,

- $S_n = \left\{x \in K : \mathrm{Tr}_{K/\mathbb{F}_{2^n}}(x) = 0\right\}$ for any n dividing m,

throughout the chapter.

Let

$$R(x) = \sum_{i=0}^{\mathfrak{c}} a_i x^{2^i} + \alpha,$$

where $a_i, \alpha \in K$. Let $Q : K \longrightarrow \mathbb{F}_2$ be the quadratic form given by

$$Q(x) = \mathrm{Tr}_K(xR(x)).$$

Then we have

$$\sum_{x \in K} (-1)^{Q(x)} = \Lambda(Q)\, 2^{\frac{1}{2}(m + r(Q))} \tag{4.6}$$

where $r(Q) = \dim rad(Q)$ is the dimension of the radical and $\Lambda(Q) \in \{-1, 0, +1\}$ is the invariant of Q.

Combining definition (4.2) and equation (4.6) above, we have that if

$$f(x) = \mathrm{Tr}_K\left(x \sum_{i=0}^{\mathfrak{c}} a_i x^{2^i}\right),$$

then

$$f^W(\alpha) = \Lambda(Q)\, 2^{\frac{1}{2}(m + r(Q))} \tag{4.7}$$

where $R(x) = \sum_{i=0}^{\mathfrak{c}} a_i x^{2^i} + \alpha$. Therefore, in order to evaluate $f^W(\alpha)$ it is enough to determine $\Lambda(Q)$ and $r(Q)$. Furthermore, quadratic functions are $r(Q)$-plateaued by equation (4.7).

Moreover, we remind the well-known fact

$$rad(Q) = \{x \in K | R^*(x) = 0\}$$

and so

$$\dim rad(Q) = \log_2\left[deg\left(\gcd\left(R^*(x), x^{2^m} + x\right)\right)\right]$$

where

$$R^*(x) = \sum_{i=0}^{\mathfrak{c}} a_i \left(x^{2^{\mathfrak{c}+i}} + x^{2^{\mathfrak{c}-i}} \right)$$

is the *radical polynomial* of Q.

It is easy to observe that $rad\,(Q)$ is independent of the affine part of Q, and this yields:

Lemma 5. *Define* $Q_1(x) = \mathrm{Tr}_K\,(xR_1(x))$ *and* $Q_2(x) = \mathrm{Tr}_K\,(xR_2(x))$ *where* $R_1(x) = \sum_{i=0}^{\mathfrak{c}} a_i x^{2^i} + \alpha_1 \in K[x]$ *and* $R_2(x) = \sum_{i=0}^{\mathfrak{c}} a_i x^{2^i} + \alpha_2 \in K[x]$. *Then*

$$r\,(Q_1) = r\,(Q_2)\,.$$

When $f(x) = \mathrm{Tr}_K \left(x^{2^a+1} + x^{2^b+1} \right)$, the dimension of the radical $r(f)$ is computed in [21] and we will use this result frequently in our proofs.

Theorem 5. (Theorem 1.5 (3) in [21]) *If* $f(x) = \mathrm{Tr}_K \left(x^{2^a+1} + x^{2^b+1} \right)$, $0 \le a < b$, *and* $\nu = max\,\{v_2(b-a), v_2(b+a)\}$, *then*

$$r(f) = \begin{cases} d_1 + d_2 - e, & \textit{if } v_2(m) \le \nu\,, \\ \\ d_1 + d_2, & \textit{if } v_2(m) > \nu. \end{cases}$$

Therefore by equation (4.7), Lemma 5 and [21, Theorem 1.5], it will be enough to determine the invariant $\Lambda(Q)$ of

$$Q(x) = \mathrm{Tr}_K \left(x^{2^a+1} + x^{2^b+1} + \alpha x \right)$$

in order to evaluate the Walsh transform of f at α.

4.3 When $\gcd\,(b-a, m) = \gcd\,(b+a, m)$

In this section, the function $f(x) = \mathrm{Tr}_K \left(x^{2^a+1} + x^{2^b+1} \right)$ with the assumption that

$$\gcd\,(b-a, m) = \gcd\,(b+a, m)$$

is considered.

Firstly, we will give a counterexample to the result in [41] and then present our main result in Theorem 6. Moreover, Theorem 7 and Corollary 2 solves an open problem of [41] and Theorem 8 generalizes a result of [41].

In the example below, we will see that the result in [41, Theorem 11] does not hold for some $\alpha \in K$.

Example 2. *Let $m = 2$, so $K = \mathbb{F}_4$. Also let $f(x) = \mathrm{Tr}_K\left(x^{2^0+1} + x^{2^1+1}\right)$. So, $a = 0$, $b = 1$ and $\gcd(b-a, m) = \gcd(b+a, m) = 1$. Then, by [21, Theorem 2.1] we have $f^W(0) = 0$. Therefore, we would have $f^W(\alpha) = 0$ for all $\alpha \in K$ with $\mathrm{Tr}_K(\alpha) = 0$ according to [41, Theorem 11].*

Now, let $\vartheta \in K = \mathbb{F}_4$ be the element such that $\vartheta^2 = \vartheta + 1$ (Note that $x^2 + x + 1$ is irreducible over $\mathbb{F}_2$). Then $\mathbb{F}_4 = \{0, 1, \vartheta, \vartheta + 1\}$.

For $\alpha = 1$ (so $\mathrm{Tr}_K(1) = 1 + 1^2 = 0$) we have

$$\begin{aligned} f^W(1) &= \sum_{x\in K} (-1)^{\mathrm{Tr}_K\left(x^2+x^3+x\right)} \\ &= (-1)^{\mathrm{Tr}_K\left(0^2+0^3+0\right)} + (-1)^{\mathrm{Tr}_K\left(1^2+1^3+1\right)} \\ &+ (-1)^{\mathrm{Tr}_K\left(\vartheta^2+\vartheta^3+\vartheta\right)} + (-1)^{\mathrm{Tr}_K\left((\vartheta+1)^2+(\vartheta+1)^3+(\vartheta+1)\right)} \\ &= (-1)^{\mathrm{Tr}_K(0)} + (-1)^{\mathrm{Tr}_K(1)} + (-1)^{\mathrm{Tr}_K(0)} + (-1)^{\mathrm{Tr}_K(0)} = 4 \end{aligned}$$

and so $f^W(1) \neq 0$.

The problem in the proof of [41, Theorem 11] is about the image $\mathrm{Im}(L)$ of L where

$$L(x) = x^{2^a} + x^{2^{-a}} + x^{2^b} + x^{2^{-b}}.$$

In [41, Theorem 7] it is shown that when $\gcd(b-a, m) = \gcd(b+a, m) = 1$ and m is odd, we have $\mathrm{Im}(L) = K_0$ where K_0 is the set of elements of K with absolute trace 0. The equality " $\mathrm{Im}(L) = K_0$" is assumed also in the proof of [41, Theorem 11], when m is even. However, the equality is not true for even m.

For any integer n dividing m, define the set

$$S_n = \left\{x \in K : \mathrm{Tr}_{K/\mathbb{F}_{2^n}}(x) = 0\right\}$$

from now on. In fact, we will see below in Lemma 7 that

$$\mathrm{Im}(L) = \begin{cases} S_d, & \text{if } m/d \text{ is odd}, \\ S_{2d}, & \text{if } m/d \text{ is even}. \end{cases}$$

Therefore, [41, Theorem 11] (where $d = 1$ and m is even) does not necessarily hold for an $\alpha \in K$ such that $Tr_{K/\mathbb{F}_{2^2}}(\alpha) = 1$ as in the Example 2, although we have still $Tr_K(\alpha) = 0$.

Before proving Lemma 7 we will present the following observation which will play a central role in its proof.

Lemma 6. *Assume* $\gcd(b-a, m) = \gcd(b+a, m)$. *Put* $d = \gcd(b-a, m)$ $(= \gcd(b+a, m))$ *and let* $\delta = \gcd(2d, m)$. *Then we have* $\delta \in \{d, 2d\}$ *and*

(i) $\delta = d \iff m/d$ *is odd* $\iff \delta | (b-a)$ *and* $\delta | (b+a)$,

(ii) $\delta = 2d \iff m/d$ *is even* $\iff \delta \nmid (b-a)$, $\delta \nmid (b+a)$ *and* $\delta | 2a$, $\delta | 2b$.

Proof. We have $\delta = \gcd(2d, m) = \begin{cases} d, & \text{if } m/d \text{ is odd}, \\ 2d, & \text{if } m/d \text{ is even}. \end{cases}$

If $\delta = d$, then $\delta | (b-a)$ and $\delta | (b+a)$ by assumption. So *(i)* is proved.

Assume $\delta = 2d$. So m/d is even and $v_2(m) > v_2(d)$. Then we get $v_2(b-a) = v_2(b+a) = v_2(d)$. Hence, $\delta \nmid (b-a)$ and $\delta \nmid (b+a)$.

Furthermore, $v_2(2b) > v_2(d)$ and $v_2(2a) > v_2(d)$ and this yields $v_2(2b) - v_2(d) = v_2(2b/d) \geq 1$ and $v_2(2a) - v_2(d) = v_2(2a/d) \geq 1$. Then, both $2b/d$ and $2a/d$ are even (note that d divides both $2b$ and $2a$). That is, $\delta = 2d$ divides both $2b$ and $2a$.

□

Now we are ready for the next lemma.

Lemma 7. *Let $L : K \longrightarrow K$ where $L(x) = x^{2^a} + x^{2^{-a}} + x^{2^b} + x^{2^{-b}}$. Under the notation of Lemma 6 we have*

$$\mathrm{Im}(L) = S_\delta.$$

Proof. Clearly $L : K \longrightarrow K$ is linear. We claim:

(1) $\mathrm{Im}(L) \subseteq S_\delta$.

(2) $\mathrm{Ker}(L) = \mathbb{F}_{2^\delta}$.

*Proof of **(1)** :* We will show that $\mathrm{Tr}_{K/\mathbb{F}_{2^\delta}}(L(x)) = 0$ for all $x \in K$.

$$\begin{aligned}\mathrm{Tr}_{K/\mathbb{F}_{2^\delta}}(L(x)) &= \mathrm{Tr}_{K/\mathbb{F}_{2^\delta}}\left(x^{2^a} + x^{2^{-a}} + x^{2^b} + x^{2^{-b}}\right) \\ &= \mathrm{Tr}_{K/\mathbb{F}_{2^\delta}}\left(x^{2^a} + x^{2^{m-a}} + x^{2^b} + x^{2^{m-b}}\right).\end{aligned}$$

Case (i): If $\delta = d$, $\delta | (b-a)$ by Lemma 6. Then

$$\left[x^{2^a}\right]^{\left(2^\delta\right)^{\frac{m+b-a}{\delta}}} = x^{2^{a+m+b-a}} = x^{2^{m+b}} = x^{2^b}$$

and

$$\left[x^{2^{m-a}}\right]^{\left(2^\delta\right)^{\frac{m-(b-a)}{\delta}}} = x^{2^{m-b}}$$

similarly. That is, $\mathrm{Tr}_{K/\mathbb{F}_{2^\delta}}\left(x^{2^a}\right) = \mathrm{Tr}_{K/\mathbb{F}_{2^\delta}}\left(x^{2^b}\right)$ and $\mathrm{Tr}_{K/\mathbb{F}_{2^\delta}}\left(x^{2^{m-a}}\right) = \mathrm{Tr}_{K/\mathbb{F}_{2^\delta}}\left(x^{2^{m-b}}\right)$.

Case (ii): If $\delta = 2d$, $\delta | 2b$ and $\delta | 2a$ by Lemma 6. Then

$$\left[x^{2^a}\right]^{\left(2^\delta\right)^{\frac{m-2a}{\delta}}} = x^{2^{m-a}} \text{ and } \left[x^{2^b}\right]^{\left(2^\delta\right)^{\frac{m-2b}{\delta}}} = x^{2^{m-b}}.$$

Thus, $\mathrm{Tr}_{K/\mathbb{F}_{2^\delta}}\left(x^{2^a}\right) = \mathrm{Tr}_{K/\mathbb{F}_{2^\delta}}\left(x^{2^{m-a}}\right)$ and $\mathrm{Tr}_{K/\mathbb{F}_{2^\delta}}\left(x^{2^b}\right) = \mathrm{Tr}_{K/\mathbb{F}_{2^\delta}}\left(x^{2^{m-b}}\right)$.

Therefore, in both cases we get $\mathrm{Tr}_{K/\mathbb{F}_{2^\delta}}(L(x)) = 0$ for all $x \in K$.

*Proof of **(2)** :*

$L(x) = x^{2^a} + x^{2^{-a}} + x^{2^b} + x^{2^{-b}} = 0$ if and only if $x^{2^{a+b}} + x^{2^{b-a}} + x^{2^{2b}} + x = 0$.

It will be sufficient to show that

$$\gcd\left(x^{2^{a+b}}+x^{2^{b-a}}+x^{2^{2b}}+x, x^{2^m}+x\right)=x^{2^\delta}+x.$$

The linearized polynomial $x^{2^{a+b}}+x^{2^{b-a}}+x^{2^{2b}}+x \in \mathbb{F}_2[x]$ has the 2-associate $x^{a+b}+x^{b-a}+x^{2b}+1$ which has the following factorization

$$x^{a+b}+x^{b-a}+x^{2b}+1=\left(x^{a+b}+1\right)\left(x^{b-a}+1\right).$$

Since $\gcd(b-a,m)=\gcd(b+a,m)=d$, we have

$$\gcd\left(x^{a+b}+1, x^m+1\right)=x^d+1 \text{ and } \gcd\left(x^{b-a}+1, x^m+1\right)=x^d+1.$$

Then

$$\begin{aligned}\gcd\left(x^{a+b}+x^{b-a}+x^{2b}+1, x^m+1\right) &= \begin{cases} x^d+1, & \text{if } m/d \text{ is odd}, \\ x^{2d}+1, & \text{if } m/d \text{ is even} \end{cases} \\ &= x^\delta+1\end{aligned}$$

and the result follows by Proposition 1.

Hence, $K/\mathrm{Ker}(L) \cong \mathrm{Im}(L)$ implies $|\mathrm{Im}(L)| = 2^{m-\delta}$ and then $\mathrm{Im}(L) = S_\delta$ as $|S_\delta| = 2^{m-\delta}$.

□

Now we present the main result of the section. The evaluation of $f^W(0)$ is already completed in [21]. We find $f^W(\alpha)$ in terms of $f^W(0)$ in some cases of our main result, and we give $f^W(0)$ in absolute value only.

Theorem 6. *Assume that* $\gcd(b-a,m)=\gcd(b+a,m)$, $0 \le a < b$, *and put* $d=\gcd(b-a,m)\,(=\gcd(b+a,m))$. *Let* $K=\mathbb{F}_{2^m}$, $E=\mathbb{F}_{2^\delta}$ *where* $\delta=\gcd(2d,m)$, *and* $f(x)=\mathrm{Tr}_K\left(x^{2^a+1}+x^{2^b+1}\right)$.

Case 1 : *"*$v_2(b-a)=v_2(b+a)=v_2(m)-1$*" does not hold:*

If $\mathrm{Tr}_{K/E}(\alpha)=0$, *then we choose* $\theta \in K$ *such that* $\theta^{2^a}+\theta^{2^{-a}}+\theta^{2^b}+\theta^{2^{-b}}=\alpha$ *(see Lemma 7 for existence of such* θ*). Then,*

$$f^W(\alpha) = \begin{cases} (-1)^{\mathrm{Tr}_K\left(\theta^{2^a+1}+\theta^{2^b+1}+\alpha\theta\right)} f^W(0), & \textit{if } \mathrm{Tr}_{K/E}(\alpha) = 0\,, \\ \\ 0, & \textit{otherwise}, \end{cases}$$

where $|f^W(0)| = 2^{\frac{1}{2}(m+\delta)}$.

Case 2 : *If* $v_2(b-a) = v_2(b+a) = v_2(m) - 1$*:*

In this case $[K : E]$ *is odd. Put* $\tau = \mathrm{Tr}_{K/E}(\alpha)$*. Then* $\mathrm{Tr}_{K/E}(\alpha+\tau) = \mathrm{Tr}_{K/E}(\alpha) + \tau\mathrm{Tr}_{K/E}(1) = \tau+\tau = 0$ *and hence we choose* $\theta \in K$ *such that* $\theta^{2^a}+\theta^{2^{-a}}+\theta^{2^b}+\theta^{2^{-b}} = \alpha+\tau$ *(see Lemma 7 for existence of such* θ*). Then,*

$$f^W(\alpha) = (-1)^{\mathrm{Tr}_K\left(\theta^{2^a+1}+\theta^{2^b+1}+\alpha\theta\right)} f^W(\tau).$$

Furthermore, if Ω *denotes the set of odd prime divisors of* $m/2d$ *with the property that*

$$min\left\{v_p(m), v_p(b-a)\right\} + min\left\{v_p(m), v_p(b+a)\right\}$$

is odd, then

$$f^W(\tau) = \begin{cases} \Lambda(g)\, 2^{\frac{1}{2}(m+2d)}, & \textit{if } v_2(m) - 1 > 0\,, \\ \prod_{p\in\Omega}\left(\frac{2}{p}\right)\Lambda(g)\, 2^{\frac{1}{2}(m+2d)}, & \textit{if } v_2(m) - 1 = 0\,, \end{cases}$$

where g *is the quadratic form* $g(x) = \mathrm{Tr}_E\left(x^{2^a+1} + x^{2^b+1} + x\tau\right)$ *and* $\Lambda(g)$ *denotes its invariant.*

Remark 3. *To avoid a very long and complicated statement in Theorem 6, we will continue the evaluation of* $\Lambda(g)$ *separately in Theorem 7.*

Proof. Firstly,

$$f^W(0) = \sum_{x\in K}(-1)^{f(x)} = \Lambda(f)\, 2^{\frac{1}{2}(m+r)}$$

where

$$r = deg\left(\gcd\left(x^{a+b} + x^{b-a} + x^{2b} + 1, x^m + 1\right)\right) = deg\left(x^\delta + 1\right) = \delta$$

by Proposition 1 and proof of Lemma 7. As the dimension of the radical does not depend on α, we have $f^W(\alpha) = 0$ or $|f^W(\alpha)| = 2^{\frac{1}{2}(m+\delta)}$. So it is left to determine the sign of $f^W(\alpha)$.

By [21, Theorem 2.1],

$$\text{invariant of } f = \Lambda(f) = 0$$

if and only if

$$v_2(b-a) = v_2(b+a) = v_2(m) - 1$$

Thus,

$$f^W(0) = 0 \quad \text{if and only if} \quad v_2(b-a) = v_2(b+a) = v_2(m) - 1.$$

Case 1 : When "$v_2(b-a) = v_2(b+a) = v_2(m) - 1$" does not hold.

In this case we are sure that $f^W(0) \neq 0$. Then, by [28, Proposition 3.2],

$$f^W(\alpha) = \begin{cases} (-1)^{f(x_0)} f^W(0), & \text{if } R^*(x) = \alpha^{2^b} \text{ has a solution } x_0 \in K, \\ 0, & \text{otherwise,} \end{cases}$$

where $R^*(x) = x^{2^{b+a}} + x^{2^{b-a}} + x^{2^{2b}} + x$ is the radical polynomial of $R(x) = x^{2^a} + x^{2^b}$.

We have

$$R^*(x) = \alpha^{2^b} \text{ for some } x_0 \in K \quad \textit{if and only if} \quad L(x_0) = \alpha \text{ for the same } x_0 \in K$$

$$\textit{if and only if} \quad \mathrm{Tr}_{K/E}(\alpha) = \tau = 0$$

by Lemma 7.

When $\tau = 0$, let $\theta \in K$ be such that $\alpha = \theta^{2^a} + \theta^{2^{-a}} + \theta^{2^b} + \theta^{2^{-b}}$ and observe that $\mathrm{Tr}_K(\alpha\theta) = \mathrm{Tr}_K\left(\theta^{2^a+1} + \theta^{2^{-a}+1} + \theta^{2^b+1} + \theta^{2^{-b}+1}\right) = 0$ as $\left(\theta^{2^{-t}+1}\right)^{2^t} = \theta^{2^t+1}$ for all integers t. Hence,

$$f(\theta) = \mathrm{Tr}_K\left(\theta^{2^a+1} + \theta^{2^b+1}\right) = \mathrm{Tr}_K\left(\theta^{2^a+1} + \theta^{2^b+1} + \alpha\theta\right)$$

and

$$f^W(\alpha) = \begin{cases} (-1)^{\mathrm{Tr}_K\left(\theta^{2^a+1}+\theta^{2^b+1}+\alpha\theta\right)} f^W(0), & \text{if } \tau = 0\,, \\ \\ 0, & \text{otherwise.} \end{cases}$$

Case 2 : $v_2(b-a) = v_2(b+a) = v_2(m) - 1$.

This is the case when $v_2(m/d) = 1$. So we have $\delta = 2d$.

We will use a similar idea as Roy used in [41]. For any element θ of K, we have

$$f^W(\alpha) = \chi_K\left(\theta^{2^a+1} + \theta^{2^b+1} + \alpha\theta\right) \sum_{x\in K} \chi_K\left(x^{2^a+1} + x^{2^b+1} + x\left(L(\theta) + \alpha\right)\right)$$

where $L(\theta) = \theta^{2^a} + \theta^{2^{-a}} + \theta^{2^b} + \theta^{2^{-b}}$.

Now, let $\tau = \mathrm{Tr}_{K/E}(\alpha) \in E$. Then we have

$$\mathrm{Tr}_{K/E}(\alpha + \tau) = \mathrm{Tr}_{K/E}(\alpha) + \tau \mathrm{Tr}_{K/E}(1).$$

The extension degree m/δ is odd in this case, and then $\mathrm{Tr}_{K/E}(1) = 1$. So,

$$\mathrm{Tr}_{K/E}(\alpha + \tau) = \tau + \tau = 0$$

Then, by Lemma 7 there exists $\theta \in K$ such that $L(\theta) = \alpha + \tau$. That is,

$$L(\theta) + \alpha = \tau.$$

Therefore,

$$\begin{aligned} f^W(\alpha) &= \chi_K\left(\theta^{2^a+1} + \theta^{2^b+1} + \alpha\theta\right) \sum_{x\in K} \chi_K\left(x^{2^a+1} + x^{2^b+1} + x\tau\right) \\ &= (-1)^{\mathrm{Tr}_K\left(\theta^{2^a+1}+\theta^{2^b+1}+\alpha\theta\right)} f^W(\tau) \end{aligned}$$

where $\theta \in K$ such that $\alpha + \tau = \theta^{2^a} + \theta^{2^{-a}} + \theta^{2^b} + \theta^{2^{-b}}$.

Let $\Lambda(h_\tau)$ denote the invariant of the quadratic form

$$h_\tau(x) = \mathrm{Tr}_K\left(x^{2^a+1} + x^{2^b+1} + x\tau\right).$$

So,

$$f^W(\tau) = \Lambda(h_\tau)\, 2^{\frac{1}{2}(m+2d)}.$$

It is left to relate $\Lambda(h_\tau)$ and $\Lambda(g)$. In literature, the relation between $\Lambda(h_\tau)$ and $\Lambda(g)$ is given in both [28] and [21] in a similar way. Note that we have $v_2(m) = v_2(2d)$. Let Ω denote the set of odd prime divisors of $m/2d$ with the property that $min\{v_p(m), v_p(b-a)\} + min\{v_p(m), v_p(b+a)\}$ is odd. Then, combining Lemma 5 and [21, Theorem 3.7] we get

$$\Lambda(h_\tau) = \Lambda(g) \begin{cases} +1, & \text{if } v_2(m) - 1 > 0\,, \\ \prod_{p\in\Omega}\left(\frac{2}{p}\right), & \text{if } v_2(m) - 1 = 0\,. \end{cases}$$

This result can also be observed by [28, Theorem 4.2].

This completes the proof of Theorem 6.

□

For the case $v_2(b-a) = v_2(b+a) = v_2(m) - 1$, the evaluation of $f^W(\alpha)$ depends on the evaluation of $\Lambda(g)$ according to Theorem 6.

Next we evaluate $\Lambda(g)$ when $v_2(b-a) = v_2(b+a) = v_2(m) - 1$, $\tau \in \mathbb{F}_{2^2}$ and d is odd.

Theorem 7. *Under the notation of Theorem 6, assume $v_2(b-a) = v_2(b+a) = v_2(m) - 1$, $\tau \in \mathbb{F}_{2^2}$ and d is odd. Then*

$$\Lambda(g) = \begin{cases} +1, & \textit{if } \tau = 1\,, \\ 0, & \textit{otherwise}. \end{cases}$$

Proof. By the assumptions we have $0 = v_2(d) = v_2(b-a) = v_2(b+a) = v_2(m) - 1$ and $\delta = 2d$. Let $\Lambda(h_\tau)$ denote the invariant of the quadratic form

$$h_\tau(x) = \mathrm{Tr}_{\mathbb{F}_4}\left(x^{2^a+1} + x^{2^b+1} + x\tau\right).$$

Since $v_2(2d) = 1 = v_2(2)$ we can apply the same method in the proof of Theorem 6. Let Ω denote the set of prime divisors of d with the property that $min\{v_p(2d), v_p(b-a)\} + min\{v_p(2d), v_p(b+a)\}$ is odd. But as $d|(b \pm a)$ we have

$$min\{v_p(2d), v_p(b-a)\} + min\{v_p(2d), v_p(b+a)\} = v_p(2d) + v_p(2d) = 2v_p(2d)$$

is always even and $\Omega = \emptyset$. Then, combining Lemma 5 and [21, Theorem 3.7] we get

$$\Lambda(g) = \Lambda(h_\tau).$$

Now, we will focus on $\Lambda(h_\tau)$. By equation (4.6),

$$\Lambda(h_\tau)\, 2^{\frac{1}{2}(2+r(h_\tau))} = \sum_{x\in\mathbb{F}_4} (-1)^{h_\tau(x)}.$$

As $\mathbb{F}_4 = \{0, 1, \vartheta, \vartheta+1\}$ where $\vartheta^2 = \vartheta + 1$, we are left to deal with 4 cases for τ.

(1) $\tau = 0$**:**

As $v_2(b-a) = v_2(b+a) = v_2(2) - 1$, we have $\Lambda(h_\tau) = \Lambda(h_0) = 0$ by [21, Theorem 2.1].

(2) $\tau = 1$**:**

- $h_\tau(0) = \mathrm{Tr}_{\mathbb{F}_4}(0) = 0$,
- $h_\tau(1) = \mathrm{Tr}_{\mathbb{F}_4}(1) = 0$,
- $h_\tau(\vartheta) = \mathrm{Tr}_{\mathbb{F}_4}\left(\vartheta^{2^a+1} + \vartheta^{2^b+1} + \vartheta\right) = \mathrm{Tr}_{\mathbb{F}_4}\left(\vartheta^{2^a+1} + \vartheta^{2^b+1}\right) + 1$,
- and

$$\begin{aligned} h_\tau(\vartheta+1) &= \mathrm{Tr}_{\mathbb{F}_4}\left((\vartheta+1)^{2^a+1} + (\vartheta+1)^{2^b+1} + (\vartheta+1)\right) \\ &= \mathrm{Tr}_{\mathbb{F}_4}\left(\vartheta^{2^a+1} + \vartheta^{2^b+1} + \vartheta^{2^a} + \vartheta^{2^b} + (\vartheta+1)\right) \\ &= \mathrm{Tr}_{\mathbb{F}_4}\left(\vartheta^{2^a+1} + \vartheta^{2^b+1}\right) + \mathrm{Tr}_{\mathbb{F}_4}(\vartheta) + \mathrm{Tr}_{\mathbb{F}_4}(\vartheta) + \mathrm{Tr}_{\mathbb{F}_4}(\vartheta+1) \\ &= \mathrm{Tr}_{\mathbb{F}_4}\left(\vartheta^{2^a+1} + \vartheta^{2^b+1}\right) + 1. \end{aligned}$$

Thus,

$$\sum_{x\in\mathbb{F}_4}(-1)^{h_\tau(x)} = 2 - 2(-1)^{\mathrm{Tr}_{\mathbb{F}_4}\left(\vartheta^{2^a+1}+\vartheta^{2^b+1}\right)}.$$

As $\vartheta^2 = \vartheta + 1$, we have

$$\vartheta^t = \begin{cases} 1 & \text{if } t \equiv 0 \mod 3\,, \\ \vartheta & \text{if } t \equiv 1 \mod 3\,, \\ \vartheta + 1 & \text{if } t \equiv 2 \mod 3\,. \end{cases}$$

Thus,

$$\mathrm{Tr}_{\mathbb{F}_4}\left(\vartheta^{2^t+1}\right) = \begin{cases} 0 & \text{if } t \text{ is odd,} \\ 1 & \text{if } t \text{ is even.} \end{cases}$$

In our case, we have $v_2(b+a) = v_2(d) = 0$ and so $b+a$ is odd. Then, one of a and b is odd and the other one is even. That is,

$$\mathrm{Tr}_{\mathbb{F}_4}\left(\vartheta^{2^a+1} + \vartheta^{2^b+1}\right) = 1 \tag{4.8}$$

for all such a and b. Finally we deduce that $\sum_{x\in\mathbb{F}_4}(-1)^{h_\tau(x)} = 4$ and $\Lambda(h_\tau) = +1$ for $\tau = 1$.

(3) $\tau = \vartheta$**:**

- $h_\tau(0) = \mathrm{Tr}_{\mathbb{F}_4}(0) = 0$,
- $h_\tau(1) = \mathrm{Tr}_{\mathbb{F}_4}(\vartheta) = 1$,
- $h_\tau(\vartheta) = \mathrm{Tr}_{\mathbb{F}_4}\left(\vartheta^{2^a+1} + \vartheta^{2^b+1} + (\vartheta+1)\right) = 1 + 1 = 0$,
- and

$$\begin{aligned} h_\tau(\vartheta+1) &= \mathrm{Tr}_{\mathbb{F}_4}\left((\vartheta+1)^{2^a+1} + (\vartheta+1)^{2^b+1} + (\vartheta+1)\vartheta\right) \\ &= \mathrm{Tr}_{\mathbb{F}_4}\left(\vartheta^{2^a+1} + \vartheta^{2^b+1} + \vartheta^{2^a} + \vartheta^{2^b} + 1\right) = 1, \end{aligned}$$

using equation (4.8). Then, $\sum_{x\in\mathbb{F}_4}(-1)^{h_\tau(x)} = 0$ and $\Lambda(h_\tau) = 0$ for $\tau = \vartheta$.

(4) $\tau = \vartheta + 1$**:**

- $h_\tau(0) = \mathrm{Tr}_{\mathbb{F}_4}(0) = 0$,
- $h_\tau(1) = \mathrm{Tr}_{\mathbb{F}_4}(\vartheta + 1) = 1$,
- $h_\tau(\vartheta) = \mathrm{Tr}_{\mathbb{F}_4}\left(\vartheta^{2^a+1} + \vartheta^{2^b+1} + \vartheta(\vartheta+1)\right) = 1 + 0 = 1$,
- and

$$\begin{aligned} h_\tau(\vartheta+1) &= \mathrm{Tr}_{\mathbb{F}_4}\left((\vartheta+1)^{2^a+1} + (\vartheta+1)^{2^b+1} + (\vartheta+1)^2\right) \\ &= \mathrm{Tr}_{\mathbb{F}_4}\left(\vartheta^{2^a+1} + \vartheta^{2^b+1} + \vartheta^{2^a} + \vartheta^{2^b} + \vartheta\right) = 0, \end{aligned}$$

using equation (4.8). Then, $\sum_{x\in\mathbb{F}_4}(-1)^{h_\tau(x)} = 0$ and $\Lambda(h_\tau) = 0$ for $\tau = \vartheta + 1$.

□

As a consequence, we can complete the evaluation of $f^W(\alpha)$ where f is as given in [41, Theorem 11]. The following corollary completely solves the open problem stated in [41] (see pages 901-903 of [41]), in particular in the paragraph before [41, Theorem 9] and in the Remark in page 903.

Corollary 2. *Under the notation of Theorem 6, with m even and $d = 1$, we have*

Case 1 : $v_2(m) > 1$

$$f^W(\alpha) = \begin{cases} (-1)^{\mathrm{Tr}_K\left(\theta^{2^a+1}+\theta^{2^b+1}+\alpha\theta\right)} f^W(0), & \textit{if } \tau = 0\,, \\ \\ 0, & \textit{otherwise}, \end{cases}$$

where $|f^W(0)| = 2^{\frac{1}{2}(m+2)}$.

Case 2 : $v_2(m) = 1$

$$f^W(\alpha) = \begin{cases} (-1)^{\mathrm{Tr}_K\left(\theta^{2^a+1}+\theta^{2^b+1}+\alpha\theta\right)} \prod_{p\in\Omega}\left(\frac{2}{p}\right) 2^{\frac{1}{2}(m+2)}, & \textit{if } \tau = 1\,, \\ \\ 0, & \textit{otherwise}, \end{cases}$$

where Ω denotes the set of odd prime divisors of $m/2$ with the property that

$$min\{v_p(m), v_p(b-a)\} + min\{v_p(m), v_p(b+a)\}$$

is odd.

The following is a related but a different result. It gives a generalization of one of the main results of [41] (see [41, Theorem 7]) for m even.

Theorem 8. *Let $K = \mathbb{F}_{2^m}$, m even, a be such that $\gcd(2^m - 1, 2^a + 1) = 1$. Let t be odd and $c = \frac{2^{ta}+1}{2^a+1}$ with a is a positive integer. If $f(x) = \mathrm{Tr}_K(x^c)$ on the field K, then*

$$f^W(1) = 2^{\frac{1}{2}(m+r(m))}$$

where $r(m) = \gcd((t-1)a, m) + \gcd((t+1)a, m) - \gcd(2a, m)$.

Proof. Since $\gcd(2^m - 1, 2^a + 1) = 1$, we have

$$\begin{aligned} f^W(1) = \sum_{x\in K} \chi_K\left(x^{\frac{2^{ta}+1}{2^a+1}} + x\right) &= \sum_{x\in K} \chi_K\left(x^{2^{ta}+1} + x^{2^a+1}\right) \\ &= \Lambda(Q)\, 2^{\frac{1}{2}(m+r(Q))} \end{aligned}$$

where $Q(x) = \mathrm{Tr}_K\left(x^{2^{ta}+1} + x^{2^a+1}\right)$. Denote $r(Q)$ by $r(m)$. Then

$$\gcd(2^m - 1, 2^1 + 1) = 1 \quad \text{if and only if} \quad v_2(m) \le v_2(a)$$

(see [28, Lemma 5.3]). So

$$v_2(m) \le v_2(a) \le v_2(ta + a)$$

and

$$v_2(m) \le v_2(a) \le v_2(ta - a)$$

as t is odd. Then, by [21, Theorem 1.5] we have

$$r(m) = \gcd(ta - a, m) + \gcd(ta + a, m) - \gcd(s, m)$$

where $s = \gcd(ta + a, ta - a) = 2a$.

Now, it is left to determine $\Lambda(Q)$. Combining [21, Theorem 3.7] and [21, Theorem 4.9] we obtain $\Lambda(Q) = 1$.

□

4.4 When not necessarily $\gcd(b-a,m) = \gcd(b+a,m)$

In this section, a different point of view rather than the approaches in Section 4.3 is applied in the proofs in order to remove the assumption

$$\gcd(b-a,m) = \gcd(b+a,m) \tag{4.9}$$

for the function $f(x) = \mathrm{Tr}_K\left(x^{2^a+1} + x^{2^b+1}\right)$.

One of the major effects of the removal of the condition (4.9) is the difficulty in determining the image of $L(x) = x^{2^a} + x^{2^{-a}} + x^{2^b} + x^{2^{-b}}$. Indeed, it is easy to observe $\mathrm{Im}(L) = \mathrm{Im}(R^*)$. This difficulty can be observed by comparing Lemma 8, 9, 10 of this section (where we find $\mathrm{Im}(R^*)$ instead) with Lemma 7 of Section 4.3. Especially in Lemma 10, some foresight is needed in order to determine a candidate set for the image of L (see the explanation below the equation (4.14)). Another effect of the removal of the condition (4.9) is the following. The idea mentioned in the proof of Case 2 of Theorem 6, which is similar to the one used in [41], will not work anymore when (4.9) is removed since the image of L in Lemma 10 is rather complicated than the one in Lemma 7. Instead, we will use another idea which is explained in details in the proof of Case 2 of Theorem 10 below.

We organized the rest of the section as follows. Firstly, before the statement of the main results we need the explicit image of a certain linearized polynomial which will play a central role in the proofs. Then we present the main result of the section in Theorem 10 and prove it by making use of the results [28, 21]. Finally, we present the second result Theorem 11 of the section which is a generalization of the results of Theorem 10.

For any quadratic form $f : K \longrightarrow \mathbb{F}_2$ (having an affine part or not), we have by Lemma 5 and equation (4.7) that the relation between $f^W(0)$ and $f^W(\alpha)$ depends

only on the relation between the invariants $\Lambda(f)$ and $\Lambda(Q)$, and this relation is given by [28, Proposition 3.2] unless $f^W(0) = 0$. Therefore, if $f^W(0) \neq 0$, we obtain the following useful result

$$f^W(\alpha) = \begin{cases} (-1)^{f(x_0)} f^W(0), & \text{if } R^*(x) = \alpha^{2^b} \text{ has a solution } x_0 \in K, \\ \\ 0, & \text{otherwise.} \end{cases} \tag{4.10}$$

Let

$$f(x) = \mathrm{Tr}_K\left(x^{2^a+1} + x^{2^b+1}\right).$$

Then, $R^*(x) = x^{2^{b+a}} + x^{2^{b-a}} + x^{2^{2b}} + x$ and

$$R^*(x_0) = \alpha^{2^b} \text{ for some } x_0 \in K \iff R^*\left((x_0)^{2^{-b}}\right) = \alpha \text{ for the same } x_0 \in K$$

$$\iff \alpha \in \mathrm{Im}(R^*) \text{ where } R^* : K \longrightarrow K.$$

So we need the image of $R^* : K \longrightarrow K$ explicitly. Firstly, the cardinality of the image can be observed easily. Since $\mathrm{Ker}(R^*) = rad(Q)$, $|\mathrm{Ker}(R^*)| = 2^{r(Q)}$. Then, $K/\mathrm{Ker}(R^*) \cong \mathrm{Im}(R^*)$ implies $|\mathrm{Im}(R^*)| = 2^{m-r(Q)}$. As $r(f) = r(Q)$, it is given in [21, Theorem 1.5] and we obtain

$$|\mathrm{Im}(R^*)| = \begin{cases} 2^{m-(d_1+d_2-e)}, & \text{if } v_2(m) \leq \nu, \\ \\ 2^{m-(d_1+d_2)}, & \text{if } v_2(m) > \nu. \end{cases}$$

We remind our notation for S_n for any integer n dividing m :

$$S_n = \left\{x \in K : \mathrm{Tr}_{K/\mathbb{F}_{2^n}}(x) = 0\right\}.$$

Lemma 8. $\mathrm{Im}(R^*) \subseteq S_{d_1} \cap S_{d_2}$

Proof. As $d_1 | (b-a)$ and $x^{2^{2b}} = \left(x^{2^{b+a}}\right)^{2^{b-a}}$, we have

$$\mathrm{Tr}_{K/\mathbb{F}_{2^{d_1}}}\left(x^{2^{2b}}\right) = \mathrm{Tr}_{K/\mathbb{F}_{2^{d_1}}}\left(x^{2^{b+a}}\right) \text{ and } \mathrm{Tr}_{K/\mathbb{F}_{2^{d_1}}}\left(x^{2^{b-a}}\right) = \mathrm{Tr}_{K/\mathbb{F}_{2^{d_1}}}(x).$$

Thus,

$$\mathrm{Tr}_{K/\mathbb{F}_{2^{d_1}}}\left(x^{2^{b+a}} + x^{2^{b-a}} + x^{2^{2b}} + x\right) = 0 \text{ for all } x \in K.$$

As $d_2|(b+a)$, by a similar observation we have

$$\mathrm{Tr}_{K/\mathbb{F}_{2^{d_2}}}\left(x^{2^{b+a}} + x^{2^{b-a}} + x^{2^{2b}} + x\right) = 0 \text{ for all } x \in K$$

and the result follows.

□

Now we are ready to give $\mathrm{Im}\,(R^*)$ explicitly when $v_2(m) \leq \nu$.

Lemma 9. $\mathrm{Im}\,(R^*) = S_{d_1} \cap S_{d_2}$ *when* $v_2(m) \leq \nu$.

Proof. It is enough to prove $|S_{d_1} \cap S_{d_2}| = 2^{m-(d_1+d_2-e)}$ as

$$|\mathrm{Im}\,(R^*)\,| = 2^{m-(d_1+d_2-e)}$$

when $v_2(m) \leq \nu$.

Let $G_1, G_2 : K \longrightarrow K$ be linearized polynomials given by

$$G_1(x) = x + x^{2^{d_1}} + x^{2^{2d_1}} + \cdots + x^{2^{(m/d_1-1)d_1}}$$

and

$$G_2(x) = x + x^{2^{d_2}} + x^{2^{2d_2}} + \cdots + x^{2^{(m/d_2-1)d_2}}.$$

So $G_1 = \mathrm{Tr}_{K/\mathbb{F}_{2^{d_1}}}(x)$, $G_2 = \mathrm{Tr}_{K/\mathbb{F}_{2^{d_2}}}(x)$ and both G_1 and G_2 split over $\mathbb{F}_{2^m}$. Then, $\gcd(G_1, G_2)$ splits over $\mathbb{F}_{2^m}$. That is,

$|S_{d_1} \cap S_{d_2}|$=the number of roots of $\gcd(G_1, G_2)$ = *deg* $(\gcd(G_1, G_2))$.

Let g_1 and g_2 denote the 2-associates of G_1 and G_2 respectively.

$$g_1(t) = 1 + t^{d_1} + t^{2d_1} + \cdots + t^{(m/d_1-1)d_1} = \frac{t^m - 1}{t^{d_1} - 1}$$

and

$$g_2(t) = 1 + t^{d_2} + t^{2d_2} + \cdots + t^{(m/d_2-1)d_2} = \frac{t^m - 1}{t^{d_2} - 1}.$$

Then,

$$\gcd(g_1, g_2) = \gcd\left(\frac{t^m - 1}{t^{d_1} - 1}, \frac{t^m - 1}{t^{d_2} - 1}\right) = \frac{(t^m - 1)\gcd\left(t^{d_1} - 1, t^{d_2} - 1\right)}{(t^{d_1} - 1)(t^{d_2} - 1)}$$

$$= \frac{(t^m - 1)(t^e - 1)}{(t^{d_1} - 1)(t^{d_2} - 1)} = \frac{t^{m+e} - t^m - t^e + 1}{t^{d_1+d_2} - t^{d_1} - t^{d_2} + 1}.$$

So $\textit{deg}\,(\gcd(g_1, g_2)) = m - (d_1 + d_2 - e)$ and this yields

$$\textit{deg}\,(\gcd(G_1, G_2)) = 2^{m-(d_1+d_2-e)}.$$

□

When $v_2(m) > \nu$, $\mathrm{Im}(R^*)$ is a proper subset of $S_{d_1} \cap S_{d_2}$ and determination of it requires some extra work.

Observe that $d_1 | \frac{m}{2}$ and $d_2 | \frac{m}{2}$ if $v_2(m) > \nu$. Let $r^*(t) \in \mathbb{F}_2[x]$ denote the 2-associate of $R^*(x)$. Then,

$$r^*(t) = t^{a+b} + t^{b-a} + t^{2b} + 1 = \left(t^{b+a} + 1\right)\left(t^{b-a} + 1\right).$$

Since $\gcd\left(t^{b-a} + 1, t^m + 1\right) = t^{d_1} + 1$, $\gcd\left(t^{b+a} + 1, t^m + 1\right) = t^{d_2} + 1$,

$$\left(t^{d_1} + 1\right) \mid \left(t^{m/2} + 1\right) \text{ and } \left(t^{d_2} + 1\right) \mid \left(t^{m/2} + 1\right),$$

we get

$$\gcd(r^*(t), t^m + 1) = \left(t^{d_1} + 1\right)\left(t^{d_2} + 1\right)$$

when $v_2(m) > \nu$. Thus,

$$\gcd\left(R^*(x), x^{2^m} + x\right) = \left(x^{2^{d_1}} + x\right) \circ \left(x^{2^{d_2}} + x\right).$$

Furthermore, we have

$$\begin{aligned} t^m+1 &= \left(t^{d_1}+1\right)\left(t^{d_2}+1\right)\frac{t^m+1}{\left(t^{d_1}+1\right)\left(t^{d_2}+1\right)} \\ &= \left(t^{d_1}+1\right)\left(t^{d_2}+1\right)\frac{\left(t^{m/2}+1\right)}{\left(t^{d_1}+1\right)}\frac{\left(t^{m/2}+1\right)}{\left(t^{d_2}+1\right)}. \end{aligned} \tag{4.11}$$

Let the inverse 2-associates of $\dfrac{\left(t^{m/2}+1\right)}{\left(t^{d_1}+1\right)}$ and $\dfrac{\left(t^{m/2}+1\right)}{\left(t^{d_2}+1\right)}$ be $L_1(x)$ and $L_2(x)$ respectively. Explicitly,

$$L_1, L_2 : K \longrightarrow K$$

where

$$L_1(x) = x + x^{2^{d_1}} + x^{2^{2d_1}} + \cdots + x^{2^{\frac{m}{2}-d_1}} \tag{4.12}$$

and

$$L_2(x) = x + x^{2^{d_2}} + x^{2^{2d_2}} + \cdots + x^{2^{\frac{m}{2}-d_2}}. \tag{4.13}$$

Finally, taking inverse 2-associates of each term in equation (4.11)

$$x^{2^m}+x = \gcd\left(R^*(x), x^{2^m}+x\right) \circ \left[\left(L_1 \circ L_2\right)(x)\right]. \tag{4.14}$$

As roots of $\gcd\left(R^*(x), x^{2^m}+x\right)$ are exactly $\mathrm{Ker}\left(R^*(x)\right)$ and $R^*(x)$ is an additive polynomial, equation (4.14) gives a clue about $\mathrm{Im}\left(R^*\right)$.

Lemma 10. $\mathrm{Im}\left(R^*\right) = \{x \in K : \left(L_1 \circ L_2\right)(x) = 0\}$ *when* $v_2(m) > \nu$.

Proof. Firstly, as $\dfrac{\left(t^{m/2}+1\right)}{\left(t^{d_1}+1\right)}\dfrac{\left(t^{m/2}+1\right)}{\left(t^{d_2}+1\right)}$ has degree $m-(d_1+d_2)$, we have

$$\textit{deg}\left(L_1 \circ L_2\right) = 2^{m-(d_1+d_2)}.$$

Then,

$$\left|\{x \in K : \left(L_1 \circ L_2\right)(x) = 0\}\right| \leq \textit{deg}\left(L_1 \circ L_2\right) = 2^{m-(d_1+d_2)}.$$

Therefore, it will be enough to show $\mathrm{Im}\left(R^*\right) \subseteq \{x \in K : \left(L_1 \circ L_2\right)(x) = 0\}$ as $\left|\mathrm{Im}\left(R^*\right)\right| = 2^{m-(d_1+d_2)}$.

Let $z = x^{2^{b+a}} + x^{2^{b-a}} + x^{2^{2b}} + x = \left(x^{2^{b-a}} + x\right) \circ \left(x^{2^{b+a}} + x\right)$ for some $x \in K$. Then,

$$(L_1 \circ L_2)(z) = L_1 \circ L_2 \circ \left(x^{2^{b-a}} + x\right) \circ \left(x^{2^{b+a}} + x\right)$$

has the 2-associate

$$\frac{(t^m+1)}{(t^{d_1}+1)(t^{d_2}+1)}\left(t^{b-a}+1\right)\left(t^{b+a}+1\right) = (t^m+1)\left[\frac{\left(t^{b-a}+1\right)\left(t^{b+a}+1\right)}{(t^{d_1}+1)(t^{d_2}+1)}\right].$$

Hence,

$$(L_1 \circ L_2)(z) = \left(x^{2^m} + x\right) \circ (G(x)) = 0$$

where $G(x)$ is the inverse 2-associate of $\frac{\left(t^{b-a}+1\right)\left(t^{b+a}+1\right)}{(t^{d_1}+1)(t^{d_2}+1)}$. This completes the proof.

□

The following result gives computation of Walsh transform of f when its domain is restricted to a special subfield and under some other conditions. It has an importance due to its role in proof of Theorem 10.

Theorem 9. *Let* $h_\theta(x) = \mathrm{Tr}_{\mathbb{F}_{2^{2e}}}\left(x^{2^a+1} + x^{2^b+1} + \theta x\right)$, $0 \le a < b$, *with* $\theta \in \mathbb{F}_{2^e}$ *and assume that* $v_2(b-a) = v_2(b+a) < v_2(m)$. *Then*

$$\Lambda(h_\theta) = \begin{cases} +1, & \text{if } \theta = 1\,, \\ \\ 0, & \text{otherwise}. \end{cases}$$

Proof. Put $\mu = v_2(b-a) = v_2(b+a)$ and observe that $v_2(d_1) = v_2(d_2) = v_2(e) = \mu$. Furthermore, we have

$$e|2a \quad \text{and} \quad e|2b.$$

Let $b-a = 2^\mu A$ and $b+a = 2^\mu B$ with $A = 2k+1$, $B = 2l+1$ for some $k, l \in \mathbb{Z}$. So $2b = 2^\mu(B+A)$, $2a = 2^\mu(B-A)$ and clearly $v_2(2b) > v_2(e)$, $v_2(2b) > v_2(e)$. Hence,

$$e|a \quad \text{and} \quad e|b.$$

On the other hand, $b = 2^{\mu}(l+k+1)$, $a = 2^{\mu}(l-k)$ and the parities of $(l+k+1)$ and $(l-k)$ are different. Hence, we have one of the following 2 cases:

$$\left\{ \begin{array}{c} v_2(e) < v_2(b) \\ \text{and} \\ v_2(e) = v_2(a) \end{array} \right\} \text{ or } \left\{ \begin{array}{c} v_2(e) < v_2(a) \\ \text{and} \\ v_2(e) = v_2(b) \end{array} \right\}.$$

That is,

$$\left\{ \begin{array}{c} b \equiv 0 \mod (2e) \\ \text{and} \\ a \equiv e \mod (2e) \end{array} \right\} \text{ or } \left\{ \begin{array}{c} a \equiv 0 \mod (2e) \\ \text{and} \\ a \equiv e \mod (2e) \end{array} \right\}.$$

This yields

$$x^{2^a+1} + x^{2^b+1} = x^{2^e+1} + x^{2^0+1} = x^{2^e+1} + x^2$$

for all $x \in \mathbb{F}_{2^{2e}}$. Then,

$$\mathrm{Tr}_{\mathbb{F}_{2^{2e}}}\left(x^{2^a+1} + x^{2^b+1} + \theta x\right) = \mathrm{Tr}_{\mathbb{F}_{2^{2e}}}\left(x^{2^e+1} + x^2 + \theta x\right)$$

$$= \mathrm{Tr}_{\mathbb{F}_{2^{2e}}}\left(x\left(x^{2^e} + x + \theta\right)\right) = \mathrm{Tr}_{\mathbb{F}_{2^e}}\left(\mathrm{Tr}_{\mathbb{F}_{2^{2e}}/\mathbb{F}_{2^e}}\left(x\left(x^{2^e} + x + \theta\right)\right)\right)$$

$$= \mathrm{Tr}_{\mathbb{F}_{2^e}}\left(\left(x^{2^e} + x + \theta\right)\mathrm{Tr}_{\mathbb{F}_{2^{2e}}/\mathbb{F}_{2^e}}(x)\right) = \mathrm{Tr}_{\mathbb{F}_{2^e}}\left(\left(x^{2^e} + x + \theta\right)\left(x^{2^e} + x\right)\right)$$

as $\left(x^{2^e} + x + \theta\right) \in \mathbb{F}_{2^e}$ for any $x \in \mathbb{F}_{2^{2e}}$. And this gives,

$$\sum_{x \in \mathbb{F}_{2^{2e}}} (-1)^{h_\theta(x)} = \sum_{x \in \mathbb{F}_{2^{2e}}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}}\left(\left(x^{2^e}+x+\theta\right)\left(x^{2^e}+x\right)\right)}.$$

Observe that the relative trace map

$$\begin{aligned} \mathrm{Tr}_{\mathbb{F}_{2^{2e}}/\mathbb{F}_{2^e}} : \mathbb{F}_{2^{2e}} &\longrightarrow \mathbb{F}_{2^e} \\ x &\longmapsto x^{2^e} + x \end{aligned}$$

maps $\mathbb{F}_{2^{2e}}$ onto $\mathbb{F}_{2^e}$ and $y = x^{2^e} + x$ runs through $\mathbb{F}_{2^e}$ exactly 2^e times when x runs through $\mathbb{F}_{2^{2e}}$ once. So

$$\begin{aligned}&\mathrm{Tr}_{\mathbb{F}_{2^e}}\left(\left(x^{2^e}+x+\theta\right)\left(x^{2^e}+x\right)\right) = \mathrm{Tr}_{\mathbb{F}_{2^e}}\left((y+\theta)\,y\right)\\ &= \mathrm{Tr}_{\mathbb{F}_{2^e}}\left(y^2+\theta y\right) = \mathrm{Tr}_{\mathbb{F}_{2^e}}\left(y+\theta y\right) = \mathrm{Tr}_{\mathbb{F}_{2^e}}\left(y(\theta+1)\right)\end{aligned}$$

and

$$\sum_{x\in\mathbb{F}_{2^{2e}}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}}\left(\left(x^{2^e}+x+\theta\right)\left(x^{2^e}+x\right)\right)} = 2^e \sum_{y\in\mathbb{F}_{2^e}} (-1)^{\mathrm{Tr}_{\mathbb{F}_{2^e}}(y(\theta+1))}$$

$$= \begin{cases} 2^{2e}, & \text{if } \theta = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore,

$$\Lambda\left(h_\theta\right) = \begin{cases} +1, & \text{if } \theta = 1\,, \\ 0, & \text{otherwise.} \end{cases}$$

□

Finally we are ready to present the main result of the section. The evaluation of $f^W(0)$ is already completed in [21]. $\Lambda\left(f\right)$ can be evaluated explicitly by combining [21, Theorem 3.7] and [21, Theorem 4.9]. Therefore, $f^W(\alpha)$ will be given in terms of $\Lambda\left(f\right)$ in some cases of the main result.

Theorem 10. *Let $K = \mathbb{F}_{2^m}$ and $f(x) = \mathrm{Tr}_K\left(x^{2^a+1} + x^{2^b+1}\right)$, $0 \le a < b$.*

Case 1 : *"$v_2(b-a) = v_2(b+a) = v_2(m) - 1$" does not hold:*

(a) $v_2(m) \le \nu$ **:**

If $\alpha \in S_{d_1} \cap S_{d_2}$, then we choose $y_0 \in K$ such that $R^*\left(y_0\right) = \alpha$ (see Lemma 9 for existence of such y_0). Then,

$$f^W(\alpha) = \begin{cases} (-1)^{f\left(y_0 2^b\right)} \Lambda(f)\, 2^{\frac{1}{2}(m+d_1+d_2-e)}, & \text{if } \alpha \in S_{d_1} \cap S_{d_2}, \\ 0, & \text{otherwise}. \end{cases}$$

(b) $v_2(m) > \nu$ ***:***

Let L_1 *and* L_2 *be given by equations (4.12) and (4.13) respectively. If* $(L_1 \circ L_2)(\alpha) = 0$*, then we choose* $y_0 \in K$ *such that* $R^*(y_0) = \alpha$ *(see Lemma 10 for existence of such* y_0*). Then,*

$$f^W(\alpha) = \begin{cases} (-1)^{f\left(y_0 2^b\right)} \Lambda(f)\, 2^{\frac{1}{2}(m+d_1+d_2)}, & \text{if } (L_1 \circ L_2)(\alpha) = 0\,, \\ 0, & \text{otherwise}. \end{cases}$$

Case 2 : $v_2(b-a) = v_2(b+a) = v_2(m) - 1$***:***

If $(L_1 \circ L_2)(\alpha+1) = 0$*, then we choose* $y_0 \in K$ *such that* $R^*(y_0) = \alpha + 1$ *(see Lemma 10 for existence of such* y_0*). Then,*

(a) $v_2(m) - 1 > 0$ ***:***

$$f^W(\alpha) = \begin{cases} (-1)^{f\left(y_0 2^b\right) + \mathrm{Tr}_K(y_0)} 2^{\frac{1}{2}(m+d_1+d_2)}, & \text{if } (L_1 \circ L_2)(\alpha+1) = 0\,, \\ 0, & \text{otherwise}. \end{cases}$$

(b) $v_2(m) = 1$ ***:***

Let Ω *denote the set of odd prime divisors of* $m/2e$ *with the property that*

$$min\left\{v_p(m), v_p(b-a)\right\} + min\left\{v_p(m), v_p(b+a)\right\}$$

is odd. Then,

$$f^W(\alpha) = \begin{cases} (-1)^{f\left(y_0{}^{2^b}\right)+\mathrm{Tr}_K(y_0)} \left[\prod_{p\in\Omega}\left(\frac{2}{p}\right)\right] 2^{\frac{1}{2}(m+d_1+d_2)}, \\ \qquad\qquad\qquad\qquad\qquad\qquad \textit{if } \left(L_1 \circ L_2\right)(\alpha+1) = 0, \\ \\ 0, \qquad\qquad\qquad\qquad\qquad\qquad \textit{otherwise}. \end{cases}$$

Proof. Firstly,

$$f^W(0) = \sum_{x\in K}(-1)^{f(x)} = \Lambda\left(f\right) 2^{\frac{1}{2}(m+r(f))}$$

where $r(f)$ is given by [21, Theorem 1.5] as

$$r(f) = \begin{cases} d_1 + d_2 - e, & \text{if } v_2(m) \leq \nu\ , \\ \\ d_1 + d_2, & \text{if } v_2(m) > \nu. \end{cases}$$

As $r\left(f\right) = r\left(Q\right)$ by Lemma 5, it is left to determine $\Lambda\left(Q\right)$ where

$$Q(x) = \mathrm{Tr}_K\left(x^{2^a+1} + x^{2^b+1} + \alpha x\right).$$

Furthermore, by [21, Theorem 2.1],

$$\Lambda\left(f\right) = 0 \iff v_2(b-a) = v_2(b+a) = v_2(m) - 1.$$

Thus,

$$f^W(0) = 0 \iff v_2(b-a) = v_2(b+a) = v_2(m) - 1.$$

Case 1 : "$v_2(b-a) = v_2(b+a) = v_2(m) - 1$" does not hold.

In this case we are sure that $f^W(0) \neq 0$. Then by equation(4.10),

$$f^W(\alpha) = \begin{cases} (-1)^{f(x_0)} f^W(0), & \text{if } R^*(x) = \alpha^{2^b} \text{ has a solution } x_0 \in K, \\ \\ 0, & \text{otherwise.} \end{cases}$$

Since we have

$$\begin{aligned} R^*(x_0) = \alpha^{2^b} \text{for some } x_0 \in K &\iff R^*(y_0) = \alpha \text{ with } y_0 = (x_0)^{2^{-b}} \\ &\iff \alpha \in \mathrm{Im}(R^*) \text{ where } R^* : K \longrightarrow K, \end{aligned}$$

the result follows by Lemma 9 and Lemma 10.

Case 2 : $v_2(b-a) = v_2(b+a) = v_2(m) - 1$.

In this case $f^W(0) = 0$ and we can not use [28, Proposition 3.2] to relate $\Lambda(f)$ and $\Lambda(Q)$.

The idea applied here is to use another quadratic form on K for which [28, Proposition 3.2] is applicable (i.e its Walsh transform at $0 \in K$ is not equal to 0) and the value of its Walsh transform at some point is equal to $f^W(\alpha)$. As f does not contain an affine part, we need to consider a quadratic form with affine part. The simplest case is the following. Let

$$g(x) = \mathrm{Tr}_K\left(x^{2^a+1} + x^{2^b+1} + x\right)$$

and observe that

$$g^W(\alpha+1) = \sum_{x \in K} \chi_K\left(x^{2^a+1} + x^{2^b+1} + \alpha x\right) = f^W(\alpha).$$

Then, if $g^W(0) \neq 0$ we can find $g^W(\alpha+1)$ in terms of $g^W(0)$.

In order to show $\Lambda(g) \neq 0$, we define another quadratic form on a special subfield where calculations are easier and relate the invariant of it to $\Lambda(g)$.

Let

$$h_1(x) = \mathrm{Tr}_{\mathbb{F}_{2^{2e}}}\left(x^{2^a+1} + x^{2^b+1} + x\right)$$

and $\Lambda(h_1)$ denote its invariant. Observe that $\Lambda(h_1) = +1$ by Theorem 9.

Note that we have $v_2(m) = v_2(2e)$. So the relation between $\Lambda(g)$ and $\Lambda(h_1)$ is determined similarly to the proof of Theorem 6 by combining Lemma 5 and [21,

Theorem 3.7]. Let Ω denote the set of odd prime divisors of $m/2e$ with the property that $min\{v_p(m), v_p(b-a)\} + min\{v_p(m), v_p(b+a)\}$ is odd. Then,

$$\Lambda(g) = \begin{cases} +1, & \text{if } v_2(m) - 1 > 0\,, \\ \prod_{p\in\Omega} \left(\frac{2}{p}\right), & \text{if } v_2(m) - 1 = 0\,. \end{cases}$$

Finally, as $g^W(0) \neq 0$ we get

$$g^W(\alpha+1) = \begin{cases} (-1)^{g(x_0)} g^W(0), & \text{if } R^*(x) = (\alpha+1)^{2^b} \text{ has a solution } x_0 \in K, \\ \\ 0, & \text{otherwise.} \end{cases}$$

Since we have

$$\begin{aligned} R^*(x_0) = (\alpha+1)^{2^b} \text{for some } x_0 \in K &\iff R^*(y_0) = \alpha + 1 \text{ with } y_0 = (x_0)^{2^{-b}} \\ &\iff (\alpha+1) \in \mathrm{Im}(R^*) \end{aligned}$$

and $g(x_0) = f(x_0) + \mathrm{Tr}_K(x_0) = f\left({y_0}^{2^b}\right) + \mathrm{Tr}_K(y_0)$ with $y_0 = (x_0)^{2^{-b}}$, the result follows by Lemma 10.

This completes the proof of Theorem 10.

□

Next, using the result in Theorem 10 we will evaluate $f_\gamma^W(\alpha)$ for any $\alpha \in K$ where

$$f_\gamma(x) = \mathrm{Tr}_K\left(\gamma x^{2^a+1} + \gamma x^{2^b+1}\right), \text{ with } \gamma \in \mathbb{F}_{2^{d_1}}.$$

Theorem 11. *Let $K = \mathbb{F}_{2^m}$ and $f(x) = \mathrm{Tr}_K\left(x^{2^a+1} + x^{2^b+1}\right)$, $0 \le a < b$. Let $f_\gamma(x) = \mathrm{Tr}_K\left(\gamma x^{2^a+1} + \gamma x^{2^b+1}\right)$,$0 \le a < b$, be given for any $\gamma \in \mathbb{F}_{2^{d_1}}$.*

Case 1 : *"$v_2(a) = v_2(b) < v_2(m)$" does not hold:*

For any $\gamma \in \mathbb{F}_{2^{d_1}}$ there exists $\Gamma \in \mathbb{F}_{2^{d_1}}$ such that $\gamma = \Gamma^{2^a+1}$ and

$$f_\gamma^W(\alpha) = f^W(\alpha/\Gamma)\,.$$

Case 2 : $v_2(a) = v_2(b) < v_2(m)$ ***:***

(a) $v_2(m) \leq \nu$ ***:***

If $\frac{\alpha}{\gamma^{2^{-b}}} \in S_{d_1} \cap S_{d_2}$*, then we choose* $y_0 \in K$ *such that* $R^*(y_0) = \frac{\alpha}{\gamma^{2^{-b}}}$ *(see Lemma 9 for existence of such* y_0*). Then,*

$$f_\gamma^W(\alpha) = \begin{cases} (-1)^{\left[\frac{m+d_1+d_2-e}{2^{\mu+1}} + f\left({y_0}^{2^b}\right)\right]} 2^{\frac{1}{2}(m+d_1+d_2-e)}, & \text{if } \frac{\alpha}{\gamma^{2^{-b}}} \in S_{d_1} \cap S_{d_2}, \\ 0, & \text{otherwise}, \end{cases}$$

where $\mu = v_2(a) = v_2(b)$*.*

(b) $v_2(m) > \nu$ ***:***

Let L_1 *and* L_2 *be given by equations (4.12) and (4.13) respectively. If* $(L_1 \circ L_2)\left(\frac{\alpha}{\gamma^{2^{-b}}}\right) = 0$*, then we choose* $y_0 \in K$ *such that* $R^*(y_0) = \frac{\alpha}{\gamma^{2^{-b}}}$ *(see Lemma 10 for existence of such* y_0*). Then,*

$$f^W(\alpha) = \begin{cases} (-1)^{\left[\frac{m+d_1+d_2}{2^{\mu+1}} + f\left({y_0}^{2^b}\right)\right]} 2^{\frac{1}{2}(m+d_1+d_2)}, & \text{if } (L_1 \circ L_2)\left(\frac{\alpha}{\gamma^{2^{-b}}}\right) = 0\ , \\ 0, & \text{otherwise}, \end{cases}$$

where $\mu = v_2(a) = v_2(b)$*.*

Proof. Firstly, we have

$$\begin{cases} v_2(b \pm a) = min\{v_2(b), v_2(a)\}, & \text{if } v_2(b) \neq v_2(a)\ , \\ v_2(b \pm a) > v_2(b) = v_2(a), & \text{if } v_2(b) = v_2(a). \end{cases}$$

Case 1 : "$v_2(a) = v_2(b) < v_2(m)$" does not hold.

In this case we have $v_2(d_1) \leq v_2(a)$. In order to see this, assume firstly $v_2(b) \neq v_2(a)$. Then, $v_2(d_1) \leq v_2(b-a) = min\{v_2(b), v_2(a)\}$. On the other hand, if $v_2(a) = v_2(b) \geq v_2(m)$ then $v_2(d_1) \leq v_2(m) \leq v_2(a)$.

As $v_2(d_1) \leq v_2(a)$, by [28, Lemma 5.3] we get

$$\gcd\left(2^a+1, 2^{d_1}-1\right) = 1.$$

Thus, the map

$$\begin{aligned} \mathbb{F}_{2^{d_1}} &\longrightarrow \mathbb{F}_{2^{d_1}} \\ x &\longmapsto x^{2^a+1} \end{aligned} \tag{4.15}$$

is a permutation on $\mathbb{F}_{2^{d_1}}$.

Let $\gamma \in \mathbb{F}_{2^{d_1}}^*$ and $\alpha \in K$ be given.Then there exists $\Gamma \in \mathbb{F}_{2^{d_1}}^*$ such that $\gamma = \Gamma^{2^a+1}$. Furthermore, we have $\Gamma^{2^a+1} = \Gamma^{2^b+1}$ for any $\Gamma \in \mathbb{F}_{2^{d_1}} \subseteq \mathbb{F}_{2^{b-a}}$.

Then,

$$\begin{aligned} f_\gamma^W(\alpha) &= \sum_{x\in K} \chi_K\left(\gamma x^{2^a+1} + \gamma x^{2^b+1} + \alpha x\right) \\ &= \sum_{x\in K} \chi_K\left(\Gamma^{2^a+1} x^{2^a+1} + \Gamma^{2^b+1} x^{2^b+1} + \alpha x\right) \\ &= \sum_{x\in K} \chi_K\left((\Gamma x)^{2^a+1} + (\Gamma x)^{2^b+1} + (\alpha/\Gamma)(\Gamma x)\right) \\ &= \sum_{x\in K} \chi_K\left(x^{2^a+1} + x^{2^b+1} + (\alpha/\Gamma)\, x\right) = f^W(\alpha/\Gamma) \end{aligned}$$

and the result follows by Theorem 10.

Case 2 : $v_2(a) = v_2(b) < v_2(m)$.

In this case $v_2(d_1) > v_2(a)$ and the above map (4.15) is not a permutation on $\mathbb{F}_{2^{d_1}}$.

Let

$$Q_\gamma(x) = f_\gamma(x) + \mathrm{Tr}_K(\alpha x) = \mathrm{Tr}_K\left(\gamma x^{2^a+1} + \gamma x^{2^b+1} + \alpha x\right)$$

and observe that the radical polynomial of Q_γ is equal to $\gamma R^*(x)$ where $R^*(x) =$

$x^{2^{b+a}} + x^{2^{b-a}} + x^{2^{2b}} + x$. Then, by [28, Theorem 5.1]

$$\Lambda(Q_\gamma) = \begin{cases} (-1)^{\frac{m+r(f_\gamma)}{2^{\mu+1}}}(-1)^{f_\gamma(x_0)}, & \text{if } \gamma R^*(x) = \alpha^{2^b} \text{ has a solution } x_0 \in K, \\ 0, & \text{otherwise,} \end{cases}$$

where $\mu = v_2(a) = v_2(b)$.

As $\mathrm{Ker}(\gamma R^*) = \mathrm{Ker}(R^*)$, we have

$$r(Q_\gamma) = r(f_\gamma) = r(f) = \begin{cases} d_1 + d_2 - e, & \text{if } v_2(m) \leq \nu\,, \\ d_1 + d_2, & \text{if } v_2(m) > \nu, \end{cases}$$

by [21, Theorem 1.5]. Furthermore,

$$\gamma R^*(x_0) = \alpha^{2^b} \text{for some } x_0 \in K \iff R^*(y_0) = \frac{\alpha}{\gamma^{2^{-b}}} \text{ with } y_0 = (x_0)^{2^{-b}}$$

$$\iff \frac{\alpha}{\gamma^{2^{-b}}} \in \mathrm{Im}(R^*),$$

and the result follows by Lemma 9 and Lemma 10.

□

4.5 Rational Points of the Curve $y^{2^n} + y = \gamma x^{2^b+1} + \gamma x^{2^a+1} + \alpha x + \beta$ over $\mathbb{F}_{2^m}$ and Examples of Maximal and Minimal Curves Contained in This Class

In this section we consider the curve (2.8) in even characteristic together with the assumptions $q = 2$, $\gcd(m, n) = 1$ and $\gamma_1 = \gamma_2 = \gamma \in \mathbb{F}_{2^m} \cap \mathbb{F}_{2^{b-a}}$. Without these assumptions it is much more difficult to find the number of rational points explicitly, at least requires new techniques, and this problem remains open in literature except very particular cases. We manage to evaluate the two-piece sum in equation (3.5) of Chapter 3 according to the sum $\sum_{x \in \mathbb{F}_{q^m}} \chi_1\left(\theta \gamma x^{q^a+1}\right)$ which is 2-valued. However, the Weil sum

$$\sum_{x\in\mathbb{F}_{2^m}} \chi_1\left(\gamma x^{2^b+1}+\gamma x^{2^a+1}+\alpha x\right)$$

corresponding to the curve (2.8) is 3-valued and much more complicated according to Theorem 10 and Theorem 11.

Let $\mathfrak{X}$ be the the Artin-Schreier type curve of the form

$$\mathfrak{X}: \quad y^{2^n}+y=\gamma x^{2^b+1}+\gamma x^{2^a+1}+\alpha x+\beta$$

with $\gcd(m,n)=1$ and $\gamma\in\mathbb{F}_{2^m}\cap\mathbb{F}_{2^{b-a}}$. If N denotes the number of solutions of the affine equation of $\mathfrak{X}$, for the number $N(\mathfrak{X})$ of $\mathbb{F}_{2^m}$-rational points of $\mathfrak{X}$ we have

$$N(\mathfrak{X})=1+N$$

since there is only one rational point at infinity. Since $f_\gamma^W(\alpha)$ is evaluated in Theorem 11 where $f_\gamma(x)=\mathrm{Tr}_K\left(\gamma x^{2^b+1}+\gamma x^{2^a+1}\right)$, it is enough to determine $N(\mathfrak{X})$ in terms of $f_\gamma^W(\alpha)$.

Theorem 12. $N(\mathfrak{X})=1+2^m+(-1)^{\mathrm{Tr}_K(\beta)}f_\gamma^W(\alpha)$

Proof. By equation (2.4) we get

$$\begin{aligned}
N&=\sum_{\theta\in\mathbb{F}_{2^{\gcd(m,n)}}}\sum_{x\in\mathbb{F}_{2^m}}\chi_1\left(\theta\left(\gamma x^{2^b+1}+\gamma x^{2^a+1}+\alpha x+\beta\right)\right)\\
&=\sum_{\theta\in\mathbb{F}_2}\chi_1(\theta\beta)\sum_{x\in\mathbb{F}_{2^m}}\chi_1\left(\theta\gamma x^{2^b+1}+\theta\gamma x^{2^a+1}+\theta\alpha x\right)\\
&=\sum_{\theta\in\mathbb{F}_2}(-1)^{\mathrm{Tr}_K(\theta\beta)}\,f_{\theta\gamma}^W(\theta\alpha)\\
&=2^m+(-1)^{\mathrm{Tr}_K(\beta)}f_\gamma^W(\alpha)
\end{aligned}$$

□

The Hasse-Weil inequality implies

$$2^m+1-2g(\mathfrak{X})\sqrt{2^m}\le N(\mathfrak{X})\le 2^m+1+2g(\mathfrak{X})\sqrt{2^m}.$$

By [42, Proposition 6.4.1] the genus of the curve $\mathfrak{X}$ is $g(\mathfrak{X})=\dfrac{(2^n-1)\,2^b}{2}$. Hence,

$$2^m+1-(2^n-1)\,2^b\sqrt{2^m}\le N(\mathfrak{X})\le 2^m+1+(2^n-1)\,2^b\sqrt{2^m}.$$

As $f_\gamma^W(\alpha) = \Lambda(Q_\gamma)\, 2^{\frac{1}{2}(m+r(Q_\gamma))}$ where

$$Q_\gamma(x) = \mathrm{Tr}_K\left(\gamma x^{2^a+1} + \gamma x^{2^b+1} + \alpha x\right)$$

and

$$r(Q_\gamma) = r(f_\gamma) = \begin{cases} d_1 + d_2 - e, & \text{if } v_2(m) \leq \nu\,, \\ \\ d_1 + d_2, & \text{if } v_2(m) > \nu, \end{cases}$$

we have the following corollary.

Corollary 3. *Under the conditions*

(i) m *is even,* $n = 1$*,*

(ii) $v_2(m) > \nu$*,*

(iii) $(b \pm a)|m$*,*

the curve $\mathfrak{X}$ *is maximal if* $(-1)^{\mathrm{Tr}_K(\beta)}\Lambda(Q_\gamma) = +1$ *and minimal if* $(-1)^{\mathrm{Tr}_K(\beta)}\Lambda(Q_\gamma) = -1$.

Example 3. *Let* $\underline{m = 1000}$*,* $\underline{n = 1}$ $\underline{b = 60}$ *and* $\underline{a = 40}$*. So we have* $v_2(b-a) = v_2(b+a) = v_2(m) - 1 > 0$ *and the condition "*$v_2(a) = v_2(b) < v_2(m)$*" does not hold. For* $\underline{\text{any}}$ *element* $\underline{\alpha \in \mathbb{F}_{2^m}}$*, choose* $\underline{\gamma = \alpha^{2^a+1}}$*. Then, combining Theorem 11 and Theorem 10 we have* $\Lambda(Q_\gamma) = +1$*. Thus, it is left to choose* $\beta \in \mathbb{F}_{2^m}$ *in order to make the curve* $\mathfrak{X}$ *maximal or minimal. When* $\mathrm{Tr}_K(\beta) = 0$*,* $\mathfrak{X}$ *is maximal and when* $\mathrm{Tr}_K(\beta) = 1$*,* $\mathfrak{X}$ *is minimal.*

- *Let* $\underline{\beta = 0}$*. Then* $\mathfrak{X}$ *is* ***maximal****.*
- *Let* $\underline{\beta \in \mathbb{F}_{2^3}}$ *be an element such that* $\underline{\beta^3 = \beta^2 + 1}$ *(*$x^3 + x^2 + 1$ *is irreducible over* $\mathbb{F}_2$*). Then,* $\mathrm{Tr}_{\mathbb{F}_{2^3}}(\beta) = \beta + \beta^2 + \beta^4 = \beta + \beta^2 + (\beta^2 + 1 + \beta) = 1$*. Thus,*

  $$\mathrm{Tr}_K(\beta) = \mathrm{Tr}_{\mathbb{F}_{2^3}}\left(\mathrm{Tr}_{K/\mathbb{F}_{2^3}}(\beta)\right) = \mathrm{Tr}_{\mathbb{F}_{2^3}}\left(\beta\,\mathrm{Tr}_{K/\mathbb{F}_{2^3}}(1)\right) = \mathrm{Tr}_{\mathbb{F}_{2^3}}(\beta) = 1.$$

  So $\mathfrak{X}$ *is* ***minimal****.*

CHAPTER 5

CONCLUSION

5.1 Contributions of the Thesis

Quadratic forms are among the most useful tools in finite geometry. In this thesis, we evaluate the exponential sums of certain quadratic forms over finite fields. There is a natural connection between these exponential sums and the number of rational points of algebraic curves defined over finite fields. Therefore we manage to compute the number of rational points of certain Artin-Schreier type curves. In both ways, this thesis contributed to the existing literature about quadratic forms and rational points.

- In Chapter 3, we compute the number of rational points of the curve (3.1) which is a general version of the curve considered in [44]. Thus, the results of this chapter improves the work done in [44].

  Secondly, Chapter 3 is a continuation of [40] and so we complete the work done in [40] by Chapter 3.

  Thirdly, if we neglect the linear term of Coulter's curve [12], the curve (3.1) is also a general version of Coulter's curve. Hence our results improve also the results of [12].

  Finally, we give *new* examples of maximal and minimal curves that are in the class of the curve (3.1).

- In Chapter 4, we evaluated the Walsh transform of a Gold type (4.3) and a Kasami-Welch type (4.4) Boolean functions without any restriction on m, a, b and α. The Walsh transforms of (4.3) and (4.4) were given in literature by [32, 41] in some restrictions on m, a, b and α. Therefore, by the results in Chapter 4 we improve the results of [32, 41] and furthermore correct a result in

[41].

Secondly, in Section 4.4 we generalize our own results by evaluating the Walsh transforms of (4.5).

Thirdly, in Section 4.5 we compute the number of rational points of the curve (2.11) which is considered in several contexts before (see [20, Section 4] for instance) when $n = 1$ and *except the coefficient* $\gamma \in \mathbb{F}_{2^m} \cap \mathbb{F}_{2^{b-a}}$. Then we give examples of maximal and minimal curves that are in the class of the curve (2.11).

5.2 Future Study

The majority of the problems in the cases that are not considered in this thesis remain open in literature. Thus, those cases may constitute the topic of our future studies.

- It seems difficult to evaluate the exponential sum in (3.5) in all cases. The subcase $u \geq t+2$ with $h \equiv 0 \mod \left(\frac{q_1+1}{q_2+1}B_1\right)$ is not considered in this thesis and it seems that new techniques are required to evaluate the sum. It will be one of our interests in future to investigate new techniques to evaluate the sum.

- The coefficient γ for the Gold type function f_γ (4.5) is restricted to be in $\mathbb{F}_{2^m} \cap \mathbb{F}_{2^{b-a}}$ and the Walsh transforms of f_γ are computed under this restriction. Apart from the techniques used in Chapter 4, some more powerful techniques are needed to remove this restriction and to evaluate the Walsh transforms of f_γ for any $\gamma \in \mathbb{F}_{2^m}$

- Moreover, the evaluation of exponential sum of a quadratic form that has more than two terms is open in general. There are some conjectures and some explicit evaluations in very particular cases, but there is not a specific method for the solution of problem in general.

REFERENCES

[1] N. Anbar, W. Meidl, Quadratic functions and maximal Artin–Schreier curves, *Finite Fields Appl.*, vol 30, pp. 49–71, 2014. https://doi.org/10.1016/j.ffa.2014.05.008

[2] C. Carlet, Boolean functions for cryptography and error correcting codes, In: Crama Y., Hammer P.L. (eds.) *Boolean Models and Methods in Mathematics, Computer Science, and Engineering,* Encyclopedia of Mathematics and Its Applications, Cambridge University Press, Cambridge, vol. 134, Chap. 8, pp. 257–397, 2010. http://dx.doi.org/10.1017/CBO9780511780448.011

[3] L. Carlitz, Explicit evaluation of certain exponential sums, *Math. Scand.*, vol 44, pp. 5–16, 1979. http://dx.doi.org/10.7146/math.scand.a-11793

[4] L. Carlitz, Evaluation of some exponential sums over a finite field, *Math. Nachr.*, vol 96, pp. 319–339, 1980. http://dx.doi.org/10.1002/mana.19800960125

[5] P. Charpin, E. Pasalic, C. Tavernier, On bent and semi-bent quadratic Boolean functions, *IEEE Trans. Inf. Theory*, vol 51, pp. 4286–4298, 2005. https://doi.org/10.1109/TIT.2005.858929

[6] A. Coşgun, F. Özbudak, Z. Saygı, Further Results on Rational points of the curve $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ over $\mathbb{F}_{q^m}$, *Des. Codes Cryptogr.*, vol. 79, no. 3, pp. 423–441, 2016. http://dx.doi.org/10.1007/s10623-015-0107-1

[7] A. Coşgun, F. Özbudak, A Correction and Improvements of Some Recent Results on Walsh Transforms of Gold Type and Kasami-Welch Type Functions, In: Duquesne S., Petkova-Nikova S. (eds.) *Arithmetic of Finite Fields, WAIFI 2016*, Lecture Notes in Computer Science, vol 10064, pp. 243–257. Springer, Cham, 2016. http://dx.doi.org/10.1007/978-3-319-55227-9_17

[8] A. Coşgun, Explicit Evaluation of Walsh Transforms of a Class of Gold Type Functions, *submitted*, 2017.

[9] R.S. Coulter, Explicit evaluations of some Weil sums, *Acta Arith.*, vol 83, pp. 241–251, 1998. http://eudml.org/doc/207121

[10] R.S. Coulter, Further evaluations of some Weil sums, *Acta Arith.*, vol 86, pp. 217–226, 1998. http://eudml.org/doc/207191

[11] R.S. Coulter, On the evaluation of a class of Weil sums in characteristic 2, *New Zealand J. Math.*, vol 28, pp. 171–184, 1999. http://www.thebookshelf.auckland.ac.nz/docs/NZJMaths/nzjmaths028/nzjmaths028-02-002.pdf

[12] R.S. Coulter, The number of rational points of a class of Artin–Schreier curves, *Finite Fields Appl.*, vol 8, pp. 397–413, 2002. https://doi.org/10.1006/ffta.2001.0348

[13] E. Çakçak, F. Özbudak, Some Artin–Schreier type function fields over finite fields with prescribed genus and number of rational places, *J. Pure Appl. Algebra*, vol 210(1), pp. 113–135, 2007. https://doi.org/10.1016/j.jpaa.2006.08.007

[14] E. Çakçak, F. Özbudak, Curves related to Coulter's maximal curves, *Finite Fields Appl.*, vol 14, pp. 209–220, 2008. https://doi.org/10.1016/j.ffa.2006.10.003

[15] A. Çeşmelioğlu, G. McGuire, W. Meidl, A construction of weakly and non-weakly regular bent functions, *J. Comb. Theory*, Ser. A 119, pp. 420–429, 2012. https://doi.org/10.1016/j.jcta.2011.10.002

[16] J.F. Dillon, H. Dobbertin, New cyclic difference sets with Singer parameters, *Finite Fields Appl.*, vol 10, pp. 342–389, 2004. https://doi.org/10.1016/j.ffa.2003.09.003

[17] H. Dobbertin, Another proof of Kasami's theorem, *Des. Codes Cryptogr.*, vol 17, pp. 177–180, 1999. http://dx.doi.org/10.1023/A:1026475109375

[18] S.D. Draper, Evalutaion of certain exponential sums of quadratic functions over a finite fields of odd characteristic, *Graduate Theses and Dissertations*, University of South Florida, 2006. http://scholarcommons.usf.edu/etd/2508

[19] R.W. Fitzgerald, Highly degenerate quadratic forms over finite fields of characteristic 2, *Finite Fields Appl.*, vol 11, pp. 165–181, 2005. https://doi.org/10.1016/j.ffa.2004.06.003

[20] R.W. Fitzgerald, Trace forms over finite fields of characteristic 2 with prescribed invariants, *Finite Fields Appl.*,, vol 15, pp. 69–81, 2009. https://doi.org/10.1016/j.ffa.2008.08.002

[21] R. Fitzgerald, Invariants of Trace Forms over Finite Fields of Characteristic 2, *Finite Fields Appl.*, vol 15, pp. 261–275, 2009. https://doi.org/10.1016/j.ffa.2008.12.005

[22] G. van der Geer, M. van der Vlugt, Reed–Muller codes and supersingular curves, *I, Compos. Math.*, vol 84, pp. 333–367, 1992. http://eudml.org/doc/90187

[23] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, *IEEE Trans. Inform. Theory*, vol 14, pp. 154–156, 1968. https://doi.org/10.1109/TIT.1968.1054106

[24] V.D. Goppa, Codes that are associated with divisors (Russian), *Peredači Informacii*, vol 13, pp. 33–39, 1977.

[25] V.D. Goppa, Codes on algebraic curves (Russian), *Dokl. Akad. Nauk SSSR*, vol 259, pp. 1289–1290, 1981.

[26] V.D. Goppa, Algebraic-geometric codes (Russian), . *Akad. Nauk SSSR Sere Mat.*, vol 46, pp. 762–781, 1982.

[27] A. Hefez, N. Kakuta, Polars of Artin–Schreier curves, *Acta Arith.*, vol 77, pp. 57–70, 1996. http://eudml.org/doc/206907

[28] X.D. Hou, Explicit Evaluation of Certain Exponential Sums of Binary Quadratic Functions, *Finite Fields Appl.*, vol 13, pp. 843–868, 2007. https://doi.org/10.1016/j.ffa.2006.09.009

[29] T. Kasami, The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. *Information and Control.*, vol 18, pp. 369–394, 1971. https://doi.org/10.1016/S0019-9958(71)90473-6

[30] A. Klapper, Cross-correlations of quadratic form sequences in odd characteristic, *Des. Codes Cryptogr.*, vol. 11, no. 3, pp. 289–305, 1997. http://dx.doi.org/10.1023/A:1008250313089

[31] G. Lachaud, Artin–Schreier curves, exponential sums, and the Carlitz–Uchiyama bound for geometric codes, *J. Number Theory*, vol 39 , pp. 18–40, 1991. https://doi.org/10.1016/0022-314X(91)90031-6

[32] J. Lahtonen, G. McGuire, H.N. Ward, Gold and Kasami-Welch functions, quadratic forms, and bent functions, *Adv. Math. Commun.*, vol 1, no. 2, pp. 243–250, 2007. http://dx.doi.org/10.3934/amc.2007.1.243

[33] P. Langevin, G. Leander, G. McGuire, A Counterexample to a Conjecture of Niho, *IEEE Transactions on Information Theory*, vol 53, no. 12, pp. 4785–4786, 2007. https://doi.org/10.1109/TIT.2007.909109

[34] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.

[35] S. Mesnager, *Bent Functions: Fundamentals and Results*, Springer, New York, 2016. https://dx.doi.org/10.1007/978-3-319-32595-8

[36] H. Niederreiter, C. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*, Cambridge Univ. Press, Cambridge, 2001.

[37] H. Niederreiter, C. Xing, *Algebraic Geometry in Coding Theory and Cryptography*, Princeton Univ. Press, Princeton, 2009.

[38] Y. Niho, Multi-valued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences, *Ph.D. thesis*, University of Southern California, Los Angeles, 1972. http://digitallibrary.usc.edu/cdm/ref/collection/p15799coll37/id/51150

[39] F. Özbudak, E. Saygı, Z. Saygı, Quadratic forms of codimension 2over finite fields containing $\mathbb{F}_4$ and Artin–Schreier type curves, *Finite Fields Appl.*, vol 18, pp. 396–433, 2012. http://dx.doi.org/10.1007/s12095-011-0051-5

[40] F. Özbudak, Z. Saygı, Rational points of the curve $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ over $\mathbb{F}_{q^m}$, In: G. Larcher, F. Pillichshammer, A. Winterhof, C. Xing (eds.) *Applied Algebra and Number Theory*, Cambridge Univ. Press, Cambridge, pp. 297–306, 2014. https://doi.org/10.1017/CBO9781139696456.018

[41] S. Roy, Generalization of some Results on Gold and Kasami-Welch Functions, *Finite Fields Appl.*, vol 18, pp. 894–903, 2012. https://doi.org/10.1016/j.ffa.2012.06.006

[42] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 2009.

[43] M.A. Tsfasman, S.G. Vladut, D. Nogin, *Algebraic Geometric Codes: Basic Notions*, American Mathematical Society, Providence, 2007.

[44] J. Wolfmann, The number of points on certain algebraic curves over finite fields. *Comm. Algebra*, vol 17, pp. 2055–2060, 1989. http://dx.doi.org/10.1080/00927878908823835

APPENDIX A

SOME RELATED PREVIOUS RESULTS

Here we recall some of the results obtained in [40] related to the results of Chapter 3 for completeness. Let p be odd and q, m, a, n, β, γ, A, N be defined as above in Section 3.1.

Let $N(m,n)$ denote the cardinality

$$N(m,n) = \left|\left\{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_{q^n}}\left(\gamma x^{q^a+1} + \beta\right) = 0\right\}\right|.$$

Therefore, we have $N = q^n N(m,n)$. The number $N(m,n)$ is computed in [40] instead of N.

Theorem 13. *Assume that $s \leq t$. Let η and η' denote the quadratic characters of $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$, respectively.*

- *If m/n is even and $A = 0$, then*

$$N(m,n) = \begin{cases} q^{m-n} - (q^n-1)\, q^{m/2-n} & \text{if } \eta\left((-1)^{m/2}\right)\eta'(\gamma) = 1, \\ q^{m-n} + (q^n-1)\, q^{m/2-n} & \text{if } \eta\left((-1)^{m/2}\right)\eta'(\gamma) = -1. \end{cases}$$

- *If m/n is even and $A \neq 0$, then*

$$N(m,n) = \begin{cases} q^{m-n} + q^{m/2-n} & \text{if } \eta\left((-1)^{m/2}\right)\eta'(\gamma) = 1, \\ q^{m-n} - q^{m/2-n} & \text{if } \eta\left((-1)^{m/2}\right)\eta'(\gamma) = -1. \end{cases}$$

- *If m/n is odd and $A = 0$, then*

$$N(m,n) = q^{m-n}.$$

- *If m/n is odd, $A \neq 0$ and n is even, then*

$$N(m,n) = \begin{cases} q^{m-n} + q^{(m-n)/2} & \text{if } (u_1,u_2) \in \{(1,1),(-1,-1)\}, \\ \\ q^{m-n} - q^{(m-n)/2} & \text{if } (u_1,u_2) \in \{(1,-1),(-1,1)\}, \end{cases}$$

where u_1 *and* u_2 *are the integers in the set* $\{-1, 1\}$ *given by*

$$u_1 = \eta\left((-1)^{m/2}\right)\eta'(\gamma) \text{ and } u_2 = \eta\left((-1)^{n/2}\right)\eta'(A).$$

- *If* m/n *is odd,* $A \neq 0$ *and* n *is odd, then*

$$N(m,n) = \begin{cases} q^{m-n} + q^{(m-n)/2} & \text{if } (u_1, u_2) \in \{(1,1),(-1,-1)\}, \\ \\ q^{m-n} - q^{(m-n)/2} & \text{if } (u_1, u_2) \in \{(1,-1),(-1,1)\}, \end{cases}$$

where u_1 *and* u_2 *are the integers in the set* $\{-1, 1\}$ *given by*

$$u_1 = \eta\left((-1)^{(m-1)/2}\right)\eta'(\gamma) \text{ and } u_2 = \eta\left((-1)^{(n-1)/2}\right)\eta'(A).$$

Theorem 14. *Assume that* $s \geq t+1$ *and* $u \leq t$. *Let* ω *be a generator of the multiplicative group* $\mathbb{F}_{q^m} \setminus \{0\}$ *and let* h *be the integer with* $0 \leq h < q^m - 1$ *such that* $\gamma = \omega^h$.

- *Case* $s = t+1$*: Put* $q_1 = q^{2^t r}$.

  If $h \not\equiv m_1 \frac{q_1+1}{2} \mod (q_1+1)$, *then*

$$N(m,n) = \begin{cases} q^{m-n} + q^{m/2-n} & \text{if } A \neq 0, \\ q^{m-n} - (q^n-1)q^{m/2-n} & \text{if } A = 0. \end{cases}$$

  If $h \equiv m_1 \frac{q_1+1}{2} \mod (q_1+1)$, *then for* $k = 2^{t+1}r$ *we have that*

$$N(m,n) = \begin{cases} q^{m-n} - q^{(m+k)/2-n} & \text{if } A \neq 0, \\ q^{m-n} + (q^n-1)q^{(m+k)/2-n} & \text{if } A = 0. \end{cases}$$

- *Case* $s \geq t+2$*: Put* $q_1 = q^{2^t r}$.

  If $h \not\equiv 0 \mod (q_1+1)$, *then*

$$N(m,n) = \begin{cases} q^{m-n} - q^{m/2-n} & \text{if } A \neq 0, \\ q^{m-n} + (q^n-1)q^{m/2-n} & \text{if } A = 0. \end{cases}$$

  If $h \equiv 0 \mod (q_1+1)$, *then for* $k = 2^{t+1}r$ *we have that*

$$N(m,n) = \begin{cases} q^{m-n} + q^{(m+k)/2-n} & \text{if } A \neq 0, \\ q^{m-n} - (q^n-1)q^{(m+k)/2-n} & \text{if } A = 0. \end{cases}$$

Theorem 15. *Assume that $t+1 \leq u \leq s$ and $A = 0$. Let ω be a generator of the multiplicative group $\mathbb{F}_{q^m} \setminus \{0\}$ and let h be the integer with $0 \leq h < q^m - 1$ such that $\gamma = \omega^h$.*

- *Case $s = t+1$: Put $B_1 = \gcd\left(m_2, q^{2^t\rho}+1\right)$.*

  If $h \equiv n_1 m_2 \frac{q^{2^t r}+1}{2} \mod \left(\frac{q^{2^t r}+1}{q^{2^t\rho}+1} B_1\right)$, then

  $$N(m,n) = q^{m-n} - (q^n-1)q^{\frac{m}{2}-n} + B_1 \frac{q^n-1}{q^{2^t\rho}+1}\left(q^{\frac{m}{2}+2^t r-n} + q^{\frac{m}{2}-n}\right).$$

  If $h \not\equiv n_1 m_2 \frac{q^{2^t r}+1}{2} \mod \left(\frac{q^{2^t r}+1}{q^{2^t\rho}+1} B_1\right)$, then

  $$N(m,n) = q^{m-n} - (q^n-1)q^{\frac{m}{2}-n}.$$

- *Case $s \geq t+2$: Put $B_1 = \gcd\left(2^{s-u} m_2, q^{2^t\rho}+1\right)$.*

  If $h \equiv 0 \mod \left(\frac{q^{2^t r}+1}{q^{2^t\rho}+1} B_1\right)$, then

  $$N(m,n) = q^{m-n} + (q^n-1)q^{\frac{m}{2}-n} - B_1 \frac{q^n-1}{q^{2^t\rho}+1}\left(q^{\frac{m}{2}+2^t r-n} + q^{\frac{m}{2}-n}\right).$$

  If $h \not\equiv 0 \mod \left(\frac{q^{2^t r}+1}{q^{2^t\rho}+1} B_1\right)$, then

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

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Coşgun, Ayhan
Nationality: Turkish (TC)
Date and Place of Birth: 24.05.1988, Balıkesir
Marital Status: Married

EDUCATION

Degree	Institution	Year of Graduation
B.S.	Department of Mathematics, METU	2011
High School	Gönen Anatolian High School	2006

PROFESSIONAL EXPERIENCE

Year	Place	Enrollment
2011 – 2016	Department of Mathematics, METU	Research Assistant

PUBLICATIONS

1. A. Coşgun, F. Özbudak, Z. Saygı, *Further Results on Rational points of the curve* $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ *over* $\mathbb{F}_{q^m}$, Des. Codes Cryptogr., vol. 79, no. 3, pp. 423–441, 2016.
   http://dx.doi.org/10.1007/s10623-015-0107-1

2. A. Coşgun, F. Özbudak, *A Correction and Improvements of Some Recent Re-*

sults on Walsh Transforms of Gold Type and Kasami-Welch Type Functions, In: Duquesne S., Petkova-Nikova S. (eds.) Arithmetic of Finite Fields, WAIFI 2016. Lecture Notes in Computer Science, vol 10064, pp. 243–257. Springer, Cham, 2016. http://dx.doi.org/10.1007/978-3-319-55227-9_17

CONFERENCE TALKS

- A. Coşgun, F. Özbudak, *A Correction and Improvements of Some Recent Results on Walsh Transforms of Gold Type and Kasami-Welch Type Functions*, International Workshop on the Arithmetic of Finite Fields (WAIFI 2016), Ghent, Belgium, July 13–15, 2016.