2006

Evalutaion of certain exponential sums of quadratic functions over a finite fields of odd characteristic

Sandra D. Draper
University of South Florida

Evaluation of Certain Exponential Sums of Quadratic Functions over a Finite Field of Odd Characteristic

by

Sandra D. Draper

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Arts
Department of Mathematics
College of Arts and Sciences
University of South Florida

Major Professor: Xiang–Dong Hou, Ph.D.
Brian Curtin, Ph.D.
Stephen Suen, Ph.D.

Date of Approval:
June 22, 2006

Keywords: Artin-Schreier Theorem, Gauss sum, law of quadratic reciprocity, Legendre symbol, quadratic form

Contents

List of Tables

Evaluation of Certain Exponential Sums of Quadratic Functions Over a Finite Field of Odd Characteristic

Sandra Draper

ABSTRACT

Let p be an odd prime, and define $f(x)$ as follows:

$$f(x) = \sum_{i=1}^{k} a_i x^{p^{\alpha_i}+1} \in \mathbb{F}_{p^n}[x]$$

where $0 \leq \alpha_1 < \alpha_2 < \cdots < \alpha_k = \alpha$. We consider the exponential sum

$$S(f,n) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n(f(x))},$$

where $\zeta_p = e^{2\pi i/p}$ and Tr_n is the trace from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$.

We provide necessary background from number theory and review the basic facts about quadratic forms over a finite field $\mathbb{F}_p$ through both the multivariable and single variable approach. Our main objective is to compute $S(f,n)$ explicitly. The sum $S(f,n)$ is determined by two quantities: the nullity and the type of the quadratic form $\mathrm{Tr}_n(f(x))$, denoted by $l_n(f)$ and $t_n(f)$, respectively. We give an effective algorithm for the computation of $l_n(f)$. Tables of numerical values of $l_n(f)$ are included. However, $t_n(f)$ is more subtle and more difficult to determine. Most of our investigation concerns $t_n(f)$.

We obtain "relative formulas" for $S(f,mn)$ in terms of $S(f,n)$ when $\nu_p(m) \leq \min\{\nu_p(\alpha_i) : i \leq 1 \leq k\}$, where ν_p is the p-adic order. The formulas are obtained in three separate cases, using different methods: (i) $m = q^s$, where q is a prime different from 2 and p; (ii) $m = 2^s$; and (iii) $m = p$. In case (i), we use a congruence relation resulting from a suitable action by the Galois group $\mathrm{Gal}(\mathbb{F}_{q^s n}/\mathbb{F}_{p^n})$. For case (ii), in addition to the congruence in case (i), a special partition of $\mathbb{F}_{p^{2n}}$ is needed. In case (iii), the congruence method does not work. However, the Artin-Schreier Theorem for the extension $\mathbb{F}_{p^{pn}}/\mathbb{F}_{p^n}$ allows us to compute the trace of $\mathbb{F}_{p^{pn}}/\mathbb{F}_{p^n}$ rather explicitly.

When $\nu_2(\alpha_1) = \nu_2(\alpha_2) = \cdots = \nu_2(\alpha_k) < \nu_2(n)$, we are able to determine $S(f,n)$ explicitly. As a special case, we have explicit formulas for $S(ax^{1+p^\alpha})$.

Most of the results of the thesis are new and generalize previous results by Carlitz, Baumert, McEliece, and Hou.

1. Introduction

Let p be a prime and n a positive integer. Let $\mathbb{F}_{p^n}$ denote the finite field with p^n elements. When $m \mid n$, the trace from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ is written as $\mathrm{Tr}_{n/m}$. We denote the $\mathrm{Tr}_{n/1}$ as Tr_n. Let $e_n(y) = e^{2\pi i \mathrm{Tr}_n(y)/p}$ for $y \in \mathbb{F}_{p^n}$. In 1979, Carlitz wrote a paper [3] evaluating the sum

$$\sum_{x \in \mathbb{F}_q} e_n(ax^3 + bx), \ a, b \in \mathbb{F}_q,$$

where $q = 2^n$. In 1980, Carlitz wrote another paper [4] evaluating the sum

$$\sum_{x \in \mathbb{F}_q} e_n(ax^{p+1} + bx), \ a, b \in \mathbb{F}_q,$$

where $q = p^n$ again, but p is an odd prime. A similar sum

$$\sum_{x \in \mathbb{F}_{p^n}} e_n(ax^{p^\alpha+1}), \quad a \in \mathbb{F}_{p^n}, \ \alpha \geq 0,$$

was also implied by the results of Baumert and McEliece [2]. Also see [7].

In 2005, Hou wrote a paper [8] for the $p = 2$ case, generalizing the result by Carlitz. More precisely, in [8], the polynomial $ax^3 + bx$ in [3] was replaced by a polynomial of the form $f(x) = \sum_{i=1}^{k} a_i x^{2^{\alpha_i}+1} + bx \in \mathbb{F}_{2^n}[x]$. Possible extension of the results of [8] for the case of $p = 2$ to the case of odd p presented the opportunity for this thesis.

This topic, evaluation of exponential sums, has applications in many areas within and outside mathematics. In number theory, exponential sums are a powerful tool to study the number of solutions of polynomial equations over finite fields, see [13, Chapter 6]. Exponential sums are also widely used in coding theory, information theory, cryptography and combinatorics. In fact, the sum $\sum_{x \in \mathbb{F}_{p^n}} e_n(ax^{p^\alpha+1})$ arose in the study of weights of irreducible cyclic codes (see Baumert and McEliece [2]) and the study of the cross-correlation function between two maximal linear sequences (see Helleseth [7]).

In this thesis, we always let p be a odd prime. We define $f(x)$ as follows:

$$f(x) = \sum_{i=1}^{k} a_i x^{p^{\alpha_i}+1} \in \mathbb{F}_{p^n}[x]$$

where $0 \leq \alpha_1 < \alpha_2 < \cdots < \alpha_k = \alpha$ are integers. We consider the sum

$$S(f, n) = \sum_{x \in \mathbb{F}_{p^n}} e_n(f(x))$$

as Hou did in his paper [8], where he handles the case of $p = 2$. The function $\mathrm{Tr}_n(f(x))$ is a quadratic form in the $\mathbb{F}_p$-coordinates of $x \in \mathbb{F}_{p^n}$ when $\mathbb{F}_{p^n}$ is identified with $\mathbb{F}_p^n$ as a $\mathbb{F}_p$-vector space. Thus, $S(f, n)$ is an exponential sum of a quadratic form over $\mathbb{F}_p$. The exponential sum of a quadratic form over $\mathbb{F}_p$ is completely determined by the nullity ($n -$ rank) and the type (discriminant) of the quadratic form. In Section 5, we will see that there is an effective method for computing the nullity. However, there is no direct way to identify the type of $\mathrm{Tr}_n(f(x))$ from $f(x)$. Most of our investigation is about the determination of the type of $\mathrm{Tr}_n(f(x))$.

Here is a briefly outline of the thesis. Section 2 contains some necessary theorems and information from number theory. Sections 3 and 4 discuss the quadratic forms on $\mathbb{F}_{p^n}$ using both the multivariable and single-variable approach. We may include a linear term to $f(x)$; the resulting sum will be $S(f+bx,n)$, $b \in \mathbb{F}_{p^n}$. In fact, $S(f+bx,n)$, as a function of b, is the "Fourier transform" of $\mathrm{Tr}_n(f(x))$. In Section 5, we show that $S(f+bx,n)$ follows from $S(f,n)$ in a straightforward way. In Section 6, the method for the computation of the nullity is shown. In Sections 7 through 9, we derive "relative" formulas for $S(f,mn)$ in terms of $S(f,n)$. Here, $S(f,mn)$ is the exponential sum of the same polynomial $f \in \mathbb{F}_{p^n}[x]$ over an extension field $\mathbb{F}_{p^{mn}}$. Three cases require different methods. In Section 7, we assume $m = q^s$ where q is a prime different from p and 2. We use a congruence relation resulting from a suitable action by the Galois group $\mathrm{Gal}(\mathbb{F}_{q^s n}/\mathbb{F}_{p^n})$ to determine the type of $\mathrm{Tr}_{q^s n}(f)$. In Section 8, We assume $m = 2^s$. In addition to the congruence in Section 7, a special partition of $\mathbb{F}_{p^{2n}}$ is needed. In Section 9, we assume $m = p$. In this case, the congruence method in the previous two sections does not work. However, the Artin-Schreier Theorem for the extension $\mathbb{F}_{p^{pn}}/\mathbb{F}_{p^n}$ allows us to compute the trace of $\mathbb{F}_{p^{pn}}/\mathbb{F}_{p^n}$ rather explicitly. We are able to express $S(f,pn)$ in terms of $S(f,n)$ under the condition that $\min\{\nu_p(\alpha_i) : i \le 1 \le k\} \ge 1$, where ν_p is the p-adic order.

In Section 10, we look at the case where $\nu_2(\alpha_1) = \nu_2(\alpha_2) = \cdots = \nu_2(\alpha_k) < \nu_2(n)$. An explicit formula for $S(f,n)$ is obtained. Section 11 handles the special case of $S(ax^{1+p^\alpha})$ which can be evaluated as a result of the previous section.

Tables of numerical values of certain nullities are included in Section 12.

2. Background from Number Theory

In this section, we collect some well-known facts from number theory to be used later.

Let p be an odd prime and $a \in \mathbb{Z}$. The Legendre symbol $(\frac{a}{p})$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a square in } \mathbb{F}_p^*, \\ -1 & \text{if } a \text{ is a nonresidue in } \mathbb{F}_p^*. \end{cases}$$

Theorem 2.1. (i) *We have*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)},$$
$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}.$$

(ii) *(The law of quadratic reciprocity) Let q be an odd prime with $q \neq p$. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}.$$

For the proof of Theorem 2.1, see [11, §5.2]

Let $q = p^n$, where p is an odd prime and $n \in \mathbb{Z}^+$. Let $e_n : \mathbb{F}_q \to \mathbb{C}$ be the canonical additive character, i.e.,

$$e_n(y) = \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(y)}, \quad y \in \mathbb{F}_q,$$

where $\zeta_p = e^{2\pi i/p}$. Let $\eta : \mathbb{F}_q \to \mathbb{C}$ be the quadratic character of $\mathbb{F}_q$, i.e.,

$$\eta(y) = \begin{cases} 0 & \text{if } y = 0, \\ 1 & \text{if } y \text{ is a square in } \mathbb{F}_q^*, \\ -1 & \text{if } y \text{ is a nonsquare in } \mathbb{F}_q^*. \end{cases}$$

When $q = p$, $\eta(y)$ is the Legendre symbol $(\frac{y}{p})$. The Gauss quadratic sum on $\mathbb{F}_q$, denoted by $G(\eta)$, is defined as

$$G(\eta) = \sum_{y \in \mathbb{F}_q} \eta(y) e(y).$$

Lemma 2.2. (i) *We have*

$$G(\eta) = \sum_{y \in \mathbb{F}_q} e(y^2).$$

(ii) *For each $a \in \mathbb{F}_q^*$,*

$$\sum_{y \in \mathbb{F}_q} e(ay^2) = \eta(a) \sum_{y \in \mathbb{F}_q} e(y^2).$$

Proof. (i): We have

$$G(\eta) = \eta(0)e_n(0) + \sum_{y \in \mathbb{F}_q^*} \eta(y) e_n(y) = \sum_{y \in (F_q^*)^2} e_n(y) - \sum_{y \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^2} e_n(y). \tag{2.1}$$

On the other hand,

$$-1 = \sum_{y\in\mathbb{F}_q^*} e_n(y) = \sum_{y\in(F_q^*)^2} e_n(y) + \sum_{y\in\mathbb{F}_q^*\setminus(\mathbb{F}_q^*)^2} e_n(y). \tag{2.2}$$

Adding (2.1) and (2.2), we have

$$G(\eta) = 1 + 2\sum_{y\in(F_q^*)^2} e_n(y) = \sum_{y\in\mathbb{F}_q} e_n(y^2).$$

(ii): If a is a square in $\mathbb{F}_q^*$, say, $a = b^2$, $b \in \mathbb{F}_q^*$, then

$$\sum_{y\in\mathbb{F}_q} e_n(ay^2) = \sum_{y\in\mathbb{F}_q} e_n\big((by)^2\big) = \sum_{y\in\mathbb{F}_q} e_n(y^2).$$

If a is a non square in $\mathbb{F}_q^*$, then

$$\sum_{y\in\mathbb{F}_q} e_n(y^2) + \sum_{y\in\mathbb{F}_q} e_n(ay^2) = 2\sum_{y\in\mathbb{F}_q} e_n(y) = 0.$$

So,

$$\sum_{y\in\mathbb{F}_q} e_n(y^2) = -\sum_{y\in\mathbb{F}_q} e_n(ay^2) = \eta(a)\sum_{y\in\mathbb{F}_q} e_n(ay^2).$$

□

The Gauss quadratic sum is completely determined. We use g_p to denote the Gauss quadratic sum over $\mathbb{F}_p$, i.e.,

$$g_p = \sum_{y\in\mathbb{F}_p} \zeta_p^{y^2}.$$

It is easy to show that

$$g_p = \begin{cases} \pm p^{\frac{1}{2}} & \text{if } p \equiv 1 \pmod 4, \\ \pm p^{\frac{1}{2}} i & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

It took Gauss four years (1801 – 1805) to determine that signs in both cases above are positive, i.e.,

$$g_p = \left\{ \begin{array}{ll} p^{\frac{1}{2}} & \text{if } p \equiv 1 \pmod 4, \\ p^{\frac{1}{2}} i & \text{if } p \equiv -1 \pmod 4 \end{array} \right\} = i^{\frac{1}{4}(p-1)^2} p^{\frac{1}{2}}.$$

The Gauss quadratic sum $G(\eta)$ over $\mathbb{F}_q$ follows from the Davenport-Hasse Theorem on the Gauss sum of a lifted character [5]. We have

$$G(\eta) = (-1)^{n-1} g_p^n,$$

where $q = p^n$.

3. Quadratic Forms on $\mathbb{F}_p^n$, the Multivariable Approach

A quadratic form on $\mathbb{F}_q^n$ is a function $F : \mathbb{F}_q^n \to \mathbb{F}_q$ defined by a homogeneous polynomial in $(x_1, \ldots, x_n)$. When q is odd, a quadratic form on $\mathbb{F}_q^n$ can be written as

$$F(x_1, \ldots, x_n) = (x_1, \ldots, x_n)A(x_1, \ldots, x_n)^T,$$

where A is an $n \times n$ symmetric matrix over $\mathbb{F}_q$. The matrix A is called the matrix of F. Two quadratic forms $F(x) = xAx^T$ and $G(x) = xBx^T$, where $x = (x_1, \ldots, x_n)$, are called *equivalent* if there exists $P \in \mathrm{GL}(n, \mathbb{F}_q)$ such that $F(x) = G(xP)$, or equivalently, $A = PBP^T$. So, the classification of quadratic forms on $\mathbb{F}_q^n$ (q odd) under equivalence is the same as the classification $n \times n$ symmetric matrices over $\mathbb{F}_q$ under congruence. Congruence of symmetric matrices is denoted by $\cong$.

The classification of quadratic form over finite fields is well-known. When q is odd, the classification is simple and is given in the next theorem. When q is even, the classification is slightly involved, see [1, 6].

For the rest of this section q is a power of an odd prime p.

Theorem 3.1. *Let $x = (x_1, \ldots, x_n)$ and A be an $n \times n$ symmetric matrix over $\mathbb{F}_q^n$. Then every quadratic form $F(x) = xAx^T$ on $\mathbb{F}_p^n$ is equivalent to*

$$x_1^2 + \cdots + x_{r-1}^2 + dx_r^2,$$

where $0 \le r \le n$ and $d \in \mathbb{F}_q^*$. The integer r is called the rank *of F and is denoted by* $\operatorname{rank} F$. *The image of d in $\mathbb{F}_q^*/(\mathbb{F}_q^*)^2$, i.e. $d(\mathbb{F}_q^*)^2$, is called the* discriminant *of F. (Sometimes we simply say that the discriminant of F is d. If $r = 0$, the discriminant of F is defined to be 1.) Two quadratic forms are equivalent if and only if they have the same rank and discriminant.*

The proof of Theorem 3.1 will follow two lemmas.

Lemma 3.2. *Every element of $\mathbb{F}_q$ is a sum of two squares.*

Proof. The multiplicative group $\mathbb{F}_q^*$ contains $\frac{1}{2}(q-1)$ squares and $\frac{1}{2}(q-1)$ nonsquares. So, $\mathbb{F}_q$ has $\frac{1}{2}(q+1)$ squares (including 0). We claim that the set of squares in $\mathbb{F}_q$ is not closed under addition. Otherwise, the set of squares of $\mathbb{F}_q$ would be a subgroup of $(\mathbb{F}_q, +)$, which is impossible since $\frac{1}{2}(q+1)$ does not divide q. Thus, there exists a nonsquare $d \in \mathbb{F}_q$ such that $d = a^2 + b^2$ for some $a, b \in \mathbb{F}_q$.

Now let $x \in \mathbb{F}_q$ be arbitrary. If x is a square, say, $x = y^2$, then $x = y^2 + 0^2$. If x is a nonsquare, since $|\mathbb{F}_q^*/(\mathbb{F}_q^*)^2| = 2$, we must have $x = dy^2$ for some $y \in \mathbb{F}_q$. Then $x = (a^2 + b^2)y^2 = (ay)^2 + (by)^2$. □

Lemma 3.3. *Every $n \times n$ symmetric matrix of rank r over $\mathbb{F}_q$ is congruent to*

$$\begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & d & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}.$$

Proof. Let

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{12} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{bmatrix}$$

be an $n \times n$ symmetric matrix over $\mathbb{F}_q$. We may assume $A \neq 0$. By suitable permutations of rows and columns of A, we may assume that the first row of A is not all 0.

First, we show that A is congruent to a diagonal matrix. There are two cases for A, $a_{11} \neq 0$ or $a_{11} = 0$.

Case 1. Assume $a_{11} \neq 0$. Let

$$P = \begin{bmatrix} 1 & & & \\ -\frac{a_{12}}{a_{11}} & 0 & & \\ \vdots & & \ddots & \\ -\frac{a_{1n}}{a_{11}} & & & 0 \end{bmatrix} \in \mathrm{GL}(n, \mathbb{F}_q).$$

Then

$$PAP^T = \begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{bmatrix},$$

where A_1 is an $(n-1) \times (n-1)$ symmetric matrix over $\mathbb{F}_q$. Using induction on n, we may assume that A_1 is congruent to a diagonal matrix. So, A is congruent to a diagonal matrix.

Case 2. Assume $a_{11} = 0$. Then one of $a_{12}, \ldots, a_{1n}$ is nonzero, say, $a_{12} \neq 0$. Let

$$P = \begin{bmatrix} 1 & 1 & & \\ & 1 & & \\ & & \ddots & \\ & & \cdots & 1 \end{bmatrix} \in \mathrm{GL}(n, \mathbb{F}_q).$$

Then

$$PAP^T = \begin{bmatrix} 2a_{12} & * & \cdots & * \\ * & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ * & * & \cdots & * \end{bmatrix},$$

where $2a_{12} \neq 0$. Therefore, we are in case 1.

So we have proved that A is congruent to a diagonal matrix. We can use row and column permutations to move all non-zero diagonal entries of A to the first entries in the diagonal.

Then A has the form:

$$\begin{bmatrix} a_{11} & & & & & \\ & \ddots & & & & \\ & & a_{rr} & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix}, \qquad a_{11}, \ldots, a_{rr} \in \mathbb{F}_q^*.$$

There are two cases for each a_{ii}: it is either a square or a nonsquare in $\mathbb{F}_q^*$. Without loss of generality, we may assume that $a_{11}, \ldots, a_{ss}$ are squares and $a_{s+1,s+1}, \ldots, a_{rr}$ are nonsquares. So,

$$a_{ii} = \begin{cases} b_i^2 & \text{if } 1 \le i \le s, \\ d\, b_i^2 & \text{if } s+1 \le i \le r, \end{cases}$$

where $b_1, \ldots, b_r \in \mathbb{F}_q^*$ and $d \in \mathbb{F}_q^*$ is a nonsquare. Let

$$P = \begin{bmatrix} b_1 & & & & & \\ & \ddots & & & & \\ & & b_r & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{bmatrix}.$$

Then

$$PAP^T = \begin{bmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & d & & & & \\ & & & & \ddots & & & \\ & & & & & d & & \\ & & & & & & 0 & \\ & & & & & & & \ddots \\ & & & & & & & & 0 \end{bmatrix}. \tag{3.1}$$

By Lemma 3.2, $d = a^2 + b^2$, $a, b \in \mathbb{F}_q$. So,

$$\begin{bmatrix} d & \\ & d \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \cong \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}.$$

Therefore, the diagonal matrix in (3.1) is congruent to

$$\begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & d & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{bmatrix}$$

depending on whether $r - s$ is even or odd. □

Proof of Theorem 3.1. Let $F(x_1,\dots,x_n) = (x_1,\dots,x_n)A(x_1,\dots,x_n)^T$ be a quadratic form in $x_1,\dots,x_n$ over $\mathbb{F}_q$, where A is an $n\times n$ symmetric matrix over $\mathbb{F}_q$. By Lemma 3.2, there exists $Q \in \mathrm{GL}(n,\mathbb{F}_q)$ such that

$$QAQ^T = \left.\begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & d & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}\right\}{\scriptstyle r}, \qquad d \in \mathbb{F}_q^*.$$

Then

$$\begin{aligned} F(x_1,\dots,x_n) &\cong F((x_1,\dots,x_n)Q) \\ &= (x_1,\dots,x_n)QAQ^T(x_1,\dots,x_n)^T \\ &= x_1^2 + x_2^2 + \cdots + x_{r-1}^2 + dx_r^2. \end{aligned}$$

Let $G(x_1,\dots,x_n)$ be another quadratic form over $\mathbb{F}_q$ with rank r' and discriminant d'. If $r' = r$ and $\eta(d) = \eta(d')$, of course, $G \cong F$. On the other hand, if $G \cong F$, by the next theorem, we have

$$\begin{aligned} \eta(d)\, g_p^r\, p^{n-r} &= \sum_{(x_1,\dots,x_n)\in\mathbb{F}_p^n} \zeta_p^{F(x_1,\dots,x_n)} \\ &= \sum_{(x_1,\dots,x_n)\in\mathbb{F}_p^n} \zeta_p^{G(x_1,\dots,x_n)} \\ &= \eta(d') g_p^{r'} p^{n-r'}. \end{aligned}$$

It follows that $r = r'$ and $\eta(d) = \eta(d')$. □

Let F be a quadratic form on $\mathbb{F}_q^n$ with discriminant d. Then $\eta(d) \in \{\pm 1\}$ is called the *type* of F. So,

$$\text{type of } F = \begin{cases} 1 & \text{if the discriminant of } F \text{ is a square,} \\ -1 & \text{if the discriminant of } F \text{ is a nonsquare.} \end{cases}$$

Theorem 3.4. *Let F be a quadratic form on $\mathbb{F}_p^n$ with type t and rank r. Then*

$$\sum_{(x_1,\dots,x_n)\in\mathbb{F}_p^n} \zeta_p^{F(x_1,\dots,x_n)} = t\, g_p^r\, p^{n-r}.$$

Proof. We may assume $F(x_1,\dots,x_n)=x_1^2+\cdots+x_{r-1}^2+dx_r^2$, $0\le r\le n$, $d\in\mathbb{F}_q^*$. Then

$$\begin{aligned}
&\sum_{(x_1,\dots,x_n)\in\mathbb{F}_p^n}\zeta_p^{F(x_1,\dots,x_n)}\\
=&\Big(\sum_{x_1\in\mathbb{F}_p^n}\zeta_p^{x_1^2}\Big)\cdots\Big(\sum_{x_{r-1}\in\mathbb{F}_p^n}\zeta_p^{x_{r-1}^2}\Big)\Big(\sum_{x_r\in\mathbb{F}_p^n}\zeta_p^{dx_r^2}\Big)\Big(\sum_{x_{r+1}\in\mathbb{F}_p^n}1\Big)\cdots\Big(\sum_{x_n\in\mathbb{F}_p^n}1\Big)\\
=&\Big(\sum_{x\in\mathbb{F}_p}\zeta_p^{x^2}\Big)\Big(\sum_{x\in\mathbb{F}_p}\zeta_p^{x^2}\Big)\cdots\Big(\sum_{x\in\mathbb{F}_p}\zeta_p^{x^2}\Big)\Big(\sum_{x\in\mathbb{F}_p}\zeta_p^{dx^2}\Big)p^{n-r}\\
=&\Big(\sum_{x\in\mathbb{F}_p}\zeta_p^{x^2}\Big)^{r-1}\Big(\sum_{x\in\mathbb{F}_p}\zeta_p^{dx^2}\Big)p^{n-r}\\
=&g_p^{r-1}\eta(d)g_pp^{n-r}\qquad\text{(by Lemma 2.2 (ii)).}
\end{aligned}$$

□

4. Quadratic Forms on $\mathbb{F}_p^n$, the Single Variable Approach

In Section 3, quadratic forms on $\mathbb{F}_q^n$ are represented by homogeneous polynomials of degree 2 in $x_1, \ldots, x_n$; this way of representing quadratic forms is usually referred to as the multi-variable approach. However, since $\mathbb{F}_q^n$ is identified with the finite field $\mathbb{F}_{q^n}$, there is another way of representing quadratic forms of $\mathbb{F}_q^n$ which is called the single-variable approach.

Let $a \in \mathbb{F}_{q^n}^*$ and $\alpha \geq 0$. Let $\epsilon_1, \ldots, \epsilon_n$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and let $x = x_1\epsilon_1 + \cdots + x_n\epsilon_n$, $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$. Let $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$. Then

$$\begin{aligned}
\mathrm{Tr}(ax^{q^\alpha+1}) &= \mathrm{Tr}\Big[a\Big(\sum_{i=1}^n x_i\epsilon_i\Big)^{q^\alpha+1}\Big] \\
&= \mathrm{Tr}\Big[a\Big(\sum_{i=1}^n x_i\epsilon_i^{q^\alpha}\Big)\Big(\sum_{j=1}^n x_j\epsilon_j\Big)\Big] \\
&= \mathrm{Tr}\Big[a\sum_{i=1}^n \epsilon_i^{q^\alpha}\epsilon_j x_i x_j\Big] \\
&= \sum_{i,j} \mathrm{Tr}(a\epsilon_i^{q^\alpha}\epsilon_j)x_i x_j
\end{aligned}$$

is a quadratic form in $x_1, \ldots, x_n$ over $\mathbb{F}_q$. Therefore, if $a_1, \ldots, a_k \in \mathbb{F}_q$ and $\alpha_1, \ldots, \alpha_k \geq 0$, then

$$\mathrm{Tr}\Big(\sum_{i=1}^k a_i x^{q^{\alpha_i}+1}\Big) \tag{4.1}$$

is a quadratic form in $x_1, \ldots, x_n$ over $\mathbb{F}_q$.

On the other hand, every quadratic form on $\mathbb{F}_q^n$ (identified with $\mathbb{F}_{q^n}$) can be written in the form of (4.1). In fact, if n is odd, a basis of the $\mathbb{F}_q$-space of quadratic forms on $\mathbb{F}_q^n$ is given by

$$\mathrm{Tr}(ax^{q^i+1}), \quad 0 \leq i \leq \frac{n-1}{2},\ a \in A,$$

where A is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. If n is even, a basis of the $\mathbb{F}_q$-space of quadratic forms on $\mathbb{F}_q^n$ is given by

$$\mathrm{Tr}(ax^{q^i+1}), \quad 0 \leq i \leq \frac{n}{2},\ a \in A$$

and

$$\mathrm{Tr}(ax^{q^{n/2}+1}), \quad b \in B,$$

where A is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and B is a basis of $\mathbb{F}_{q^{n/2}}$ over $\mathbb{F}_q$. See [9] for details.

5. Computation of the Nullity

Let $F(x_1, \ldots, x_n) = (x_1, \ldots, x_n)A(x_1, \ldots, x_n)^T$ be a quadratic form on $\mathbb{F}_p^n$ where A is an $n \times n$ symmetric matrix over $\mathbb{F}_p$. For $z, x \in \mathbb{F}_p^n$, we have

$$F(x+z) - F(x) = xAz^T + zAx^T + zAz^T = 2zAx^T + zAz^T.$$

Thus, $zA = 0$ if and only if $F(x+z) - F(x)$ is constant for all $x \in \mathbb{F}_p^n$. So

$$n - \operatorname{rank} F = \dim_{\mathbb{F}_p}\{z \in \mathbb{F}_p^n : F(x+z) - F(x) = \text{constant for all } x \in \mathbb{F}_p^n\}.$$

The number $n - \operatorname{rank} F$ is called the nullity of F.

Consider

$$f(x) = \sum_{i=1}^{k} a_i x^{p^{\alpha_i}+1} + bx \in \mathbb{F}_{p^n}[x], \tag{5.1}$$

where $0 \le \alpha_1 \le \alpha_2 \le \cdots \le \alpha_k = \alpha$. In Section 4, we saw that every quadratic form on $\mathbb{F}_p^n$ (identified with $\mathbb{F}_{p^n}$) can be written as $\operatorname{Tr}_n(f(x))$ for some $f \in \mathbb{F}_{p^n}[x]$ of the form (5.1). Denote the nullity of $\operatorname{Tr}_n(f(x))$ by $l_n(f)$, i.e.

$$l_n(f) = \dim_{\mathbb{F}_p} L_n(f),$$

where

$$L_n(f) = \{z \in \mathbb{F}_{p^n} : \operatorname{Tr}_n(f(x+z) - f(x)) = \text{constant for all } x \in \mathbb{F}_{p^n}\}$$

which is called the null space of f. Let $t_n(f)$ denote the type of $\operatorname{Tr}_n(f(x))$. Then by Theorem 3.4, we have

$$S(f, n) = t_n(f) g_p^{n-l_n(f)} p^{l_n(f)}.$$

Thus, $S(f, n)$ is completely determined by $l_n(f)$ and $t_n(f)$.

There is an effective algorithm to compute $l_n(f)$. We have

$$
\begin{aligned}
&\mathrm{Tr}_n(f(x+z)-f(x))\\
&=\mathrm{Tr}_n\Big(\sum_{i=1}^{k}a_i(x+z)^{p^{\alpha_i+1}}-\sum_{i=1}^{k}a_ix^{p^{\alpha_i+1}}\Big)\\
&=\mathrm{Tr}_n\Big(\sum_{i=1}^{k}(a_i(x+z)^{p^{\alpha_i+1}}-a_ix^{p^{\alpha_i+1}})\Big)\\
&=\mathrm{Tr}_n\Big(\sum_{i=1}^{k}(a_i(x^{p^{\alpha_i+1}}+x^{p^{\alpha_i}}z+xz^{p^{\alpha_i}}+z^{p^{\alpha_i+1}})-a_ix^{p^{\alpha_i+1}})\Big)\\
&=\mathrm{Tr}_n\Big(\sum_{i=1}^{k}a_i(x^{p^{\alpha_i}}z+xz^{p^{\alpha_i}}+z^{p^{\alpha_i+1}})\Big)\\
&=\mathrm{Tr}_n\Big(\sum_{i=1}^{k}a_iz^{p^{\alpha_i+1}}+\sum_{i=1}^{k}a_i(x^{p^{\alpha_i}}z+xz^{p^{\alpha_i}})\Big)\\
&=\mathrm{Tr}_nf(z)+\mathrm{Tr}_n\Big(\sum_{i=1}^{k}(a_ix^{p^{\alpha_i}}z+a_ixz^{p^{\alpha_i}})\Big)\\
&=\mathrm{Tr}_nf(z)+\mathrm{Tr}_n\Big(\sum_{i=1}^{k}(a_ix^{p^{\alpha_i}}z)^{p^{-\alpha_i}}+a_ixz^{p^{\alpha_i}})\Big)\\
&=\mathrm{Tr}_nf(z)+\mathrm{Tr}_n\Big(\sum_{i=1}^{k}(a_i^{p^{-\alpha_i}}xz^{p^{-\alpha_i}}+a_ixz^{p^{\alpha_i}})\Big)\\
&=\mathrm{Tr}_nf(z)+\mathrm{Tr}_n\Big(x\sum_{i=1}^{k}(a_i^{p^{-\alpha_i}}z^{p^{-\alpha_i}}+a_iz^{p^{\alpha_i}})\Big)\\
&=\mathrm{Tr}_nf(z)+\mathrm{Tr}_n\Big(x^{p^\alpha}\sum_{i=1}^{k}(a_i^{p^{\alpha-\alpha_i}}z^{p^{\alpha-\alpha_i}}+a_i^{p^\alpha}z^{p^{\alpha+\alpha_i}})\Big)\\
&=\mathrm{Tr}_nf(z)+\mathrm{Tr}_n\Big(x^{p^\alpha}f^*(z)\Big),
\end{aligned}
\tag{5.2}
$$

where $p^{-\alpha_i}$ is a positive integer and $p^{-\alpha_i}p^{\alpha_i}\equiv 1 \pmod{p^n-1}$, and

$$f^*(z)=\sum_{i=1}^{k}(a_i^{p^{\alpha-\alpha_i}}z^{p^{\alpha-\alpha_i}}+a_i^{p^\alpha}z^{p^{\alpha+\alpha_i}}).$$

Note that $f^*\in\mathbb{F}_{p^n}[x]$ is a p-polynomial with no repeated roots. Thus, $\mathrm{Tr}_n(f(x+z)-f(x))$ is constant for all $x\in\mathbb{F}_{p^n}$ if and only if z is a root of f^*. Therefore,

$$L_n(f)=\{z\in\mathbb{F}_{p^n}:f^*(z)=0\}$$

and

$$
\begin{aligned}
l_n(f)&=\dim_{\mathbb{F}_p}\{z\in\mathbb{F}_{p^n}:f^*(z)=0\}\\
&=\log_p|\,\{z\in\mathbb{F}_{p^n}:f^*(z)=0\}|\\
&=\log_p\deg(f^*,\ x^{p^n}-x).
\end{aligned}
\tag{5.3}
$$

Since $\alpha_k=\alpha$, then the degree of f^* is always $p^{2\alpha}$. Let

$$s=\min\{m:n\mid m,\ l_m(f)=2\alpha\}. \tag{5.4}$$

Thus, $\mathbb{F}_{p^s}$ is the splitting field of f^* over $\mathbb{F}_{p^n}$. It is then obvious that for all multiples m of n,

$$l_m(f) = l_{(m,s)}(f). \tag{5.5}$$

Therefore, we can compute the nullity $l_m(f)$ for all $0 < m \equiv 0 \pmod{n}$ using the following method. First, use (5.3) to compute $l_{in}(f)$ for $i = 1, 2, \ldots$ until $l_s(f) = 2\alpha$. Then $\mathbb{F}_{p^s}$ is the splitting field of f^* and $l_m(f)$ is given by (5.5).

Example 5.1. Let

$$f(x) = 2x^{3^1+1} + 2x^{3^2+1} + x^{3^3+1} \in \mathbb{F}_3[x].$$

Then we find that

$$f^*(x) = x^{3^0} + 2x^{3^1} + 2x^{3^2} + 2x^{3^4} + 2x^{3^5} + x^{3^6}.$$

We can then use *Mathematica* [15] to find that

$$\deg(f^*,\ x^{3^m} - x) = \begin{cases} 3^6 & \text{if } m = 26, \\ 1 & \text{if } 1 \le m < 26. \end{cases}$$

Thus, the splitting field of $\mathbb{F}_3$ is $\mathbb{F}_{3^{26}}$. So

$$l_m(f) = \begin{cases} 6 & \text{if } 26 \mid m, \\ 0 & \text{otherwise.} \end{cases}$$

Example 5.2. Let

$$f(x) = 3x^{7^1+1} + 3x^{7^2+1} + x^{7^3+1} \in \mathbb{F}_7[x].$$

Then we find that

$$f^*(x) = x^{7^0} + 3x^{7^1} + 3x^{7^2} + 3x^{7^4} + 3x^{7^5} + x^{7^6}.$$

We can then use *Mathematica* [15] to find that

$$\deg(f^*,\ x^{7^m} - x) = \begin{cases} 7^6 & \text{if } m = 175, \\ 7^5 & \text{if } m < 175,\ 25 \mid m, \\ 7^2 & \text{if } m < 175,\ 7 \mid m, \\ 7^1 & \text{if } m < 175,\ 25 \nmid m, 7 \nmid m. \end{cases}$$

The splitting field of f^* over $\mathbb{F}_7$ is $\mathbb{F}_{7^{175}}$. Write $m = 5^a 7^b m^*$, where $a, b \ge 0$ and $(5 \cdot 7, m^*) = 1$. Then for every $m > 0$,

$$l_m(f) = \begin{cases} 6 & \text{if } a \ge 2 \text{ and } b \ge 1, \\ 5 & \text{if } a \ge 2 \text{ and } b = 0, \\ 2 & \text{if } a \le 1 \text{ and } b \ge 1, \\ 1 & \text{if } a \le 1 \text{ and } b = 0. \end{cases}$$

In fact, we have computed the values of $l_m(f)$ with $p^n = 3,\ \alpha \le 4$, and $p^n = 5,\ \alpha \le 3$. The results are tabulated in Section 12.

6. $S(f+bx)$ Follows from $S(f)$

Let $f \in \mathbb{F}_{p^n}[x]$ be given in (5.1). Our main objective is to compute the sum $S(f,n)$. Let $b \in \mathbb{F}_{p^n}$. The sum

$$S(f+bx,n) = \sum_{x\in\mathbb{F}_{p^n}} e_n(f(x)+bx)$$

is also important. In fact, when viewed as a function of b, $S(f+bx,n)$ is the "Fourier transform" of $\mathrm{Tr}_n(f)$. However, we will see that the seemingly more general sum $S(f+bx,n)$ follows easily from $S(f,n)$. Hence, it suffices to determine $S(f,n)$.

Theorem 6.1. *Let $b \in \mathbb{F}_{p^n}$. Then*

$$S(f,n)\overline{S(f+bx,n)} = \begin{cases} p^{n+l_n(f)}e_n(f(x_0)) & \text{if } f^*(x) = b^{p^\alpha} \text{ has a solution } x_0 \in \mathbb{F}_p^n, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We have

$$\begin{aligned}
&S(f,n)\overline{S(f+bx,n)} \\
=&\sum_{x\in\mathbb{F}_{p^n}} e_n(f(x)) \sum_{y\in\mathbb{F}_{p^n}} \overline{e(f(y)+by)} \\
=&\sum_{x,y\in\mathbb{F}_{p^n}} e_n(f(x)-f(y)-by) \\
=&\sum_{x,y\in\mathbb{F}_{p^n}} e_n(f(x+y)-f(y)-by) \\
=&\sum_{x,y\in\mathbb{F}_{p^n}} e_n(f(x)+yf^*(x)^{p^{-\alpha}}-by) \quad \text{(by (5.2))} \\
=&\sum_{x\in\mathbb{F}_{p^n}} e_n(f(x)) \sum_{y\in\mathbb{F}_{p^n}} e_n[y(f^*(x)^{p^{-\alpha}}-b)] \\
=&p^n \sum_{\substack{x\in\mathbb{F}_{p^n} \\ f^*(x)=b^{p^{-\alpha}}}} e_n(f(x)).
\end{aligned}$$

If $f^*(x) = b^{p^{-\alpha}}$ has no solution in $\mathbb{F}_{p^n}$, then $S(f,n)\overline{S(f+bx,n)} = 0$. Thus, assume $f^*(x) = b^{p^\alpha}$ has a solution, $x_0 \in \mathbb{F}_{p^n}$. Then the solution set of $f^*(x) = b^{p^\alpha}$ is

$$x_0 + \{x \in \mathbb{F}_{p^n} : f^*(x) = 0\}$$

since $f^*(x)$ is a p-polynomial. The solution set can also be written as $x_0 + L_n(f)$ where $L_n(f)$ is the null space of f. Since $\mathrm{Tr}_n f(x)$ is a quadratic form on $\mathbb{F}_{p^n}$, it is constant on

$x_0 + L_n(f)$. So

$$\begin{aligned} S(f,n)\overline{S(f+bx,n)} &= p^n \sum_{\substack{x\in\mathbb{F}_{p^n} \\ f^*(x)=b^{p^{-\alpha}}}} e_n(f(x)) \\ &= p^n \sum_{x\in x_0+L_n(f)} e_n(f(x)) \\ &= p^n p^{l_n(f)} e_n(f(x_0)) \\ &= p^{n+l_n(f)} e_n(f(x_0)). \end{aligned}$$

□

Corollary 6.2.

$$S(f+bx,n) = \begin{cases} \overline{e(f(x_0))}S(f,n) & \text{if } f^*(x) = b^{p^\alpha} \text{ has a solution } x_0 \in \mathbb{F}_{p^n}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Since $S(f,n) \neq 0$, then by Theorem 6.1, we know that the only case we have to consider is when $f^*(x) = b^{p^\alpha}$ has a solution $x_0 \in \mathbb{F}_{p^n}$. Then by Theorem 6.1,

$$S(f+bx,n) = \frac{p^{n+l_n(f)}}{\overline{S(f,n)}}\overline{e(f(x_0))} = \frac{p^{n+l_n(f)}}{|S(f,n)|^2}\overline{e(f(x_0))}S(f,n).$$

Since $S(f,n) = t_n(f)g_p^{n-l_n(f)}p^{l_n(f)}$, we have $|S(f,n)|^2 = p^{n+l_n(f)}$. This yields the desired result. □

7. From $S(f,n)$ to $S(f,q^sn)$, $q \neq p,2$

In this section, assume that q is an odd prime such that $q \neq p$ and $s \geq 0$.

Theorem 7.1. *In the ring $\mathbb{Z}[\zeta_p]$, we have*

$$S(f,q^sn) \equiv \sum_{x \in \mathbb{F}_{p^n}} e_{q^sn}(f(x)) \pmod{q}.$$

Equivalently,

$$t_{q^sn}(f) g_p^{q^sn - l_{q^sn}(f)} p^{l_{q^sn}(f)} \equiv \left(\frac{q}{p}\right)^{s(n-l_n(f))} t_n(f) g_p^{n-l_n(f)} p^{l_n(f)} \pmod{q}.$$

Proof. Let $T(i) = \{x \in \mathbb{F}_{p^{q^sn}} \setminus \mathbb{F}_{p^n} : \mathrm{Tr}_{q^sn}(f(x)) = i\}$, $i \in \mathbb{F}_p$. We can then write

$$\begin{aligned} S(f,q^sn) &= \sum_{x \in \mathbb{F}_{p^{q^sn}} \setminus \mathbb{F}_{p^n}} e_{q^sn}(f(x)) + \sum_{x \in \mathbb{F}_{p^n}} e_{q^sn}(f(x)) \\ &= \sum_{i=0}^{p-1} |T(i)| \zeta_p^i + \sum_{x \in \mathbb{F}_{p^n}} e_{q^sn}(f(x)). \end{aligned}$$

The Galois group $\mathrm{Aut}(\mathbb{F}_{p^{q^sn}}/\mathbb{F}_{p^n})$ acts on $T(i)$. Take $x \in T(i)$ and take $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^{q^sn}}/\mathbb{F}_{p^n})$. Since $f \in \mathbb{F}_{p^n}[x]$, we have $\sigma(f(x)) = f(\sigma(x))$ for all $x \in \mathbb{F}_{p^{q^sn}}$. Thus,

$$\mathrm{Tr}_{q^sn}\big(f(\sigma(x))\big) = \mathrm{Tr}_{q^sn}\big(\sigma(f(x))\big) = \mathrm{Tr}_{q^sn}(f(x)) = i.$$

Secondly, note that since $x \notin \mathbb{F}_{p^n}$, then $\sigma(x) \notin \mathbb{F}_{p^n}$. (Otherwise, we would have $x = \sigma^{-1}\sigma(x) \in \mathbb{F}_{p^n}$.) Therefore, $\sigma(x) \in T(i)$.

$T(i)$ is a union of $\mathrm{Aut}(\mathbb{F}_{p^{q^sn}}/\mathbb{F}_{p^n})$-orbits of cardinality of q to positive powers. Recall that the cardinality of the orbit is the size of the group divided by the size of the stabilizer. Thus, since $|\mathrm{Aut}(\mathbb{F}_{p^{q^sn}}/\mathbb{F}_{p^n})| = q^s$, then the cardinality of every orbit must be q to some positive power. If the cardinality of the orbit is 1, then the element of that orbit is fixed by every automorphism, and that orbit is contained in the base field $\mathbb{F}_{p^n}$. But, the orbit is in $T(i)$, which is a contradiction as the orbit cannot be in $\mathbb{F}_{p^n}$. Thus, the cardinality of every orbit is equal to q^h, where $0 < h \leq s$. Thus, $T(i)$ is a union of $\mathrm{Aut}(\mathbb{F}_{p^{q^sn}}/\mathbb{F}_{p^n})$-orbits of size q^h where $0 < h \leq s$. So $|T(i)| \equiv 0 \pmod{q}$ for all $0 \leq i \leq p-1$. Therefore,

$$\sum_{x \in \mathbb{F}_{p^{q^sn}} \setminus \mathbb{F}_{p^n}} e_{q^sn}(f(x)) \equiv 0 \pmod{q}$$

which gives us

$$S(f,q^sn) \equiv \sum_{x \in \mathbb{F}_{p^n}} e_{q^sn}(f(x)) \pmod{q}.$$

For the equivalence in the second part of the theorem, since

$$S(f,q^sn) = t_{q^sn}(f) g_p^{q^sn - l_{q^sn}(f)} p^{l_{q^sn}(f)}$$

and

$$\sum_{x \in \mathbb{F}_{p^n}} e_{q^sn}(f(x)) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{q^s \mathrm{Tr}_n(f(x))} = \left(\frac{q}{p}\right)^{s(n-l_n(f))} t_n(f) g_p^{n-l_n(f)} p^{l_n(f)},$$

then

$$t_{q^sn}(f)g_p^{q^sn-l_{q^sn}(f)}p^{l_{q^sn}(f)} \equiv \big(\frac{q}{p}\big)^{s(n-l_n(f))}t_n(f)g_p^{n-l_n(f)}p^{l_n(f)} \pmod q.$$

□

Lemma 7.2. *We have*

$$p^{l_{q^sn}(f)-l_n(f)} \equiv 1 \pmod q$$

and

$$\frac{1}{2}[l_{q^sn}(f) - l_n(f)] \in \mathbb{Z}$$

.

Proof. Let $X = \{x \in \mathbb{F}_p^{q^sn} \setminus \mathbb{F}_{p^n} : f^*(x) = 0$. Then the Galois group $\mathrm{Aut}(\mathbb{F}_p^{q^sn}/\mathbb{F}_{p^n})$ acts on X and X is a union of $\mathrm{Aut}(\mathbb{F}_p^{q^sn}/\mathbb{F}_{p^n})$-orbits of cardinality > 1. Then,

$$p^{l_{q^sn}(f)} - p^{l_n(f)} = |X| \equiv 0 \pmod q$$

$$p^{l_n(f)}(p^{l_{q^sn}(f)-l_n(f)} - 1) \equiv 0 \pmod q$$

since p is a prime different from q and $l_n(f)$ is an integer, then $p^{l_{q^sn}(f)-l_n(f)}-1 \equiv 0 \pmod q$. Therefore,

$$p^{l_{q^sn}(f)-l_n(f)} \equiv 1 \pmod q.$$

To prove the second part of the lemma, begin with the equation from Theorem 7.1,

$$t_{q^sn}(f)g_p^{q^sn-l_{q^sn}(f)}p^{l_{q^sn}(f)} \equiv \big(\frac{q}{p}\big)^{s(n-l_n(f))}t_n(f)g_p^{n-l_n(f)}p^{l_n(f)} \pmod q. \tag{7.1}$$

Using the above equation and $p^{l_{q^sn}(f)-l_n(f)} \equiv 1 \pmod q$, we can simplify (7.1) to be

$$t_{q^sn}(f)g_p^{q^sn-l_{q^sn}(f)} \equiv \big(\frac{q}{p}\big)^{s(n-l_n(f))}t_n(f)g_p^{n-l_n(f)} \pmod q. \tag{7.2}$$

Assume to the contrary of $\frac{1}{2}[l_{q^sn}(f) - l_n(f)] \notin \mathbb{Z}$, i.e. $l_{q^sn}(f) - l_n(f)$ is odd. Then exactly one of $q^sn - l_{q^sn}(f)$ or $n - l_n(f)$ is odd. This is true as q^sn and n have the same parity, but $l_{q^sn}(f)$ and $l_n(f)$ have different parities. Also, since $g_p = p^{\frac{1}{2}}$ or $ip^{\frac{1}{2}}$, then $g_p^2 = \pm p$. Thus, since $q^sn - l_{q^sn}(f)$ or $n - l_n(f)$ is odd, then (7.2) has g_p to an even power on one side and g_p to an odd power on the other side. This gives us p to some power on one side and p to some power multiplied by g_p on the other side, respectively. Thus,

$$g_p p^a \equiv b \pmod q$$

for some $a, b \in \mathbb{Z},\ a \geq 0$. Let $\sigma \in \mathrm{Aut}(\mathbb{Q}(g_p)/\mathbb{Q})$ such that $\sigma(g_p) = -g_p$. Since $\mathbb{Q}(g_p) \subset (\zeta_p)$ and $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is Galois, we can extend σ to $\tau \in \mathrm{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. By applying τ to $g_p p^a \equiv b \pmod q$, we have

$$-g_p p^a \equiv b \pmod q.$$

By subtracting the two equations, the result is $2g_p p^a \equiv 0 \pmod q$, which is a contradiction. Thus, $\frac{1}{2}[l_{q^sn}(f) - l_n(f)] \in \mathbb{Z}$. □

Let $o_q(p)$ denote the multiplicative order of p in $\mathbb{Z}/q\mathbb{Z}$. Then, using the above equation $p^{l_{q^sn}(f)-l_n(f)} \equiv 1 \pmod q$, we find that $\frac{1}{o_q(p)}(l_{q^sn}(f) - l_n(f)) \in \mathbb{Z}$. Clearly

$$p^{\frac{1}{2}(l_{q^sn}(f)-l_n(f))} \equiv (-1)^{\frac{1}{o_q(p)}(l_{q^sn}(f)-l_n(f))} \pmod q.$$

Theorem 7.3. *We have*

$$t_{q^sn}(f) = t_n(f)\big(\frac{q}{p}\big)^{sl_n(f)}(-1)^{\frac{1}{4}(p-1)[l_{q^sn}(f)-l_n(f)]+\frac{1}{o_q(p)}[l_{q^sn}(f)-l_n(f)]}. \tag{7.3}$$

Proof. First, recall that $p^{\frac{1}{2}(q-1)} \equiv (\frac{p}{q}) \pmod q$ and note that $q^s - 1 \equiv s(q-1) \pmod 4$. We can start with (7.2)

$$t_{q^s n}(f) g_p^{q^s n - l_{q^s n}(f)} \equiv \big(\frac{q}{p}\big)^{s(n-l_n(f))} t_n(f) g_p^{n-l_n(f)} \pmod q$$

and simplify it to be

$$\begin{aligned} t_{q^s n}(f) g_p^{q^s n - n} &\equiv \big(\frac{q}{p}\big)^{s(n-l_n(f))} t_n(f) g_p^{l_{q^s n}(f) - l_n(f)} \pmod q \\ t_{q^s n}(f) g_p^{n(q^s-1)} &\equiv \big(\frac{q}{p}\big)^{s(n-l_n(f))} t_n(f) g_p^{l_{q^s n}(f) - l_n(f)} \pmod q. \end{aligned}$$

Recall that the Gauss sum is $g_p = i^{\frac{1}{4}(p-1)^2} p^{\frac{1}{2}}$. Then,

$$g_p^2 = \big(i^{\frac{1}{4}(p-1)^2} p^{\frac{1}{2}}\big)^2 = i^{\frac{1}{2}(p-1)^2} p = (-1)^{\frac{p-1}{2}} p.$$

Using this fact, then

$$\begin{aligned} g_p^{n(q^s-1)} &= [(-1)^{\frac{p-1}{2}} p]^{\frac{1}{2}n(q^s-1)} \\ &= (-1)^{\frac{1}{4}n(p-1)(q^s-1)} p^{\frac{1}{2}n(q^s-1)} \\ &= (-1)^{\frac{1}{4}n(p-1)s(q-1)} p^{\frac{1}{2}ns(q-1)} \\ &= (-1)^{\frac{1}{4}ns(p-1)(q-1)} p^{\frac{1}{2}(q-1)sn} \\ &= (-1)^{\frac{1}{4}ns(p-1)(q-1)} \big(\frac{p}{q}\big)^{sn} \pmod q. \end{aligned}$$

Also, simplify

$$\begin{aligned} g_p^{l_{q^s n}(f) - l_n(f)} &= [(-1)^{\frac{p-1}{2}} p]^{\frac{1}{2}[l_{q^s n}(f) - l_n(f)]} \\ &= (-1)^{\frac{1}{4}(p-1)[l_{q^s n}(f) - l_n(f)]} p^{\frac{1}{2}[l_{q^s n}(f) - l_n(f)]} \\ &= (-1)^{\frac{1}{4}(p-1)[l_{q^s n}(f) - l_n(f)]} (-1)^{\frac{1}{o_q(p)}(l_{q^s n}(f) - l_n(f))} \pmod q \\ &= (-1)^{\frac{1}{4}(p-1)[l_{q^s n}(f) - l_n(f)] + \frac{1}{o_q(p)}(l_{q^s n}(f) - l_n(f))} \pmod q \end{aligned}$$

Then, the above values can be substituted into

$$t_{q^s n}(f) g_p^{n(q^s-1)} \equiv \big(\frac{q}{p}\big)^{s(n-l_n(f))} t_n(f) g_p^{l_{q^s n}(f) - l_n(f)} \pmod q$$

as

$$\begin{aligned} & t_{q^s n}(f) (-1)^{\frac{1}{4}ns(p-1)(q-1)} \big(\frac{p}{q}\big)^{sn} \\ \equiv & \big(\frac{q}{p}\big)^{s(n-l_n(f))} t_n(f) (-1)^{\frac{1}{4}(p-1)[l_{q^s n}(f) - l_n(f)] + \frac{1}{o_q(p)}[l_{q^s n}(f) - l_n(f)]} \pmod q \end{aligned}$$

$$
\begin{aligned}
&t_{q^s n}(f)\\
\equiv\, & t_n(f)\Big(\frac{q}{p}\Big)^{s(n-l_n(f))}\Big(\frac{p}{q}\Big)^{-sn}\\
&\cdot(-1)^{\frac{1}{4}(p-1)[l_{q^s n}(f)-l_n(f)]+\frac{1}{o_q(p)}[l_{q^s n}(f)-l_n(f)]-\frac{1}{4}ns(p-1)(q-1)} \pmod q\\
=\, & t_n(f)\Big(\frac{q}{p}\Big)^{s(n-l_n(f))}\Big(\frac{p}{q}\Big)^{sn}(-1)^{\frac{1}{4}(p-1)[l_{q^s n}(f)-l_n(f)]-\frac{1}{4}ns(p-1)(q-1)+\frac{1}{o_q(p)}[l_{q^s n}(f)-l_n(f)]}\\
=\, & t_n(f)\Big(\frac{q}{p}\Big)^{s(n-l_n(f))}\Big(\frac{p}{q}\Big)^{sn}(-1)^{\frac{1}{4}(p-1)\Big([l_{q^s n}(f)-l_n(f)]-sn(q-1)\Big)+\frac{1}{o_q(p)}[l_{q^s n}(f)-l_n(f)]}\\
=\, & t_n(f)\Big(\frac{q}{p}\Big)^{-sl_n(f)}\Big(\frac{q}{p}\Big)^{sn}\Big(\frac{p}{q}\Big)^{sn}(-1)^{\frac{1}{4}(p-1)\Big([l_{q^s n}(f)-l_n(f)]-sn(q-1)\Big)+\frac{1}{o_q(p)}[l_{q^s n}(f)-l_n(f)]}\\
=\, & t_n(f)\Big(\frac{q}{p}\Big)^{sl_n(f)}\Big(\Big(\frac{q}{p}\Big)\Big(\frac{p}{q}\Big)\Big)^{sn}(-1)^{\frac{1}{4}(p-1)\Big([l_{q^s n}(f)-l_n(f)]-sn(q-1)\Big)+\frac{1}{o_q(p)}[l_{q^s n}(f)-l_n(f)]}.
\end{aligned}
$$

In the above equation, both sides are ± 1. Thus, the two sides are equal. We can use the law of quadratic reciprocity which states

$$\Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) = (-1)^{\frac{1}{4}(p-1)(q-1)}.$$

This allows us to further simplify our equation.

$$
\begin{aligned}
&t_{q^s n}(f)\\
=\, & t_n(f)\Big(\frac{q}{p}\Big)^{sl_n(f)}\Big(\Big(\frac{q}{p}\Big)\Big(\frac{p}{q}\Big)\Big)^{sn}(-1)^{\frac{1}{4}(p-1)\Big([l_{q^s n}(f)-l_n(f)]-sn(q-1)\Big)+\frac{1}{o_q(p)}[l_{q^s n}(f)-l_n(f)]}\\
=\, & t_n(f)\Big(\frac{q}{p}\Big)^{sl_n(f)}\Big((-1)^{\frac{1}{4}(p-1)(q-1)}\Big)^{sn}(-1)^{\frac{1}{4}(p-1)\Big([l_{q^s n}(f)-l_n(f)]-sn(q-1)\Big)+\frac{1}{o_q(p)}[l_{q^s n}(f)-l_n(f)]}\\
=\, & t_n(f)\Big(\frac{q}{p}\Big)^{sl_n(f)}(-1)^{\frac{1}{4}sn(p-1)(q-1)+\frac{1}{4}(p-1)\Big([l_{q^s n}(f)-l_n(f)]-sn(q-1)\Big)+\frac{1}{o_q(p)}[l_{q^s n}(f)-l_n(f)]}\\
=\, & t_n(f)\Big(\frac{q}{p}\Big)^{sl_n(f)}(-1)^{\frac{1}{4}(p-1)\Big(sn(q-1)+[l_{q^s n}(f)-l_n(f)]-sn(q-1)\Big)+\frac{1}{o_q(p)}[l_{q^s n}(f)-l_n(f)]}\\
=\, & t_n(f)\Big(\frac{q}{p}\Big)^{sl_n(f)}(-1)^{\frac{1}{4}(p-1)[l_{q^s n}(f)-l_n(f)]+\frac{1}{o_q(p)}[l_{q^s n}(f)-l_n(f)]}.
\end{aligned}
$$

□

Example 7.4. Let

$$f(x) = 2x^{3^1+1} + 2x^{3^2+1} + x^{3^3+1} \in \mathbb{F}_3[x]$$

as in Example 5.1. Then we found the nullity of $f(x)$ for every m to be

$$l_m(f) = \begin{cases} 6 & \text{if } 26 \mid m,\\ 0 & \text{otherwise.}\end{cases}$$

Since

$$S(f,1) = \sum_{x\in\mathbb{F}_3} e_1(f(x)) = \sum_{x\in\mathbb{F}_3} e_1(-x^2) = \eta(-1)\sum_{x\in\mathbb{F}_3} e_1(x^2) = -g_3,$$

we have $t_1(f) = -1$.

Now, let m be odd and not divisible by 3. Since m is not divisible by 26, then $l_m(f) = 0$ and it follows from (7.3) that

$$t_m(f) = -1.$$

Example 7.5. Let

$$f(x) = 3x^{7^1+1} + 3x^{7^2+1} + x^{7^3+1} \in \mathbb{F}_7[x]$$

as in Example 5.2. Then we found the nullity of $f(x)$ for every $m = 5^a 7^b m^*$, $(m^*,\, 5\cdot 7) = 1$, to be

$$l_m(f) = \begin{cases} 6 & \text{if } a \geq 2 \text{ and } b \geq 1, \\ 5 & \text{if } a \geq 2 \text{ and } b = 0, \\ 2 & \text{if } 0 \leq a \leq 1 \text{ and } b \geq 1, \\ 1 & \text{if } 0 \leq a \leq 1 \text{ and } b = 0. \end{cases}$$

Since

$$S(f,1) = \sum_{x\in\mathbb{F}_7} e_1(f(x)) = \sum_{x\in\mathbb{F}_7} 1 = 7,$$

we have $t_1(f) = 1$.

Now, let m be odd and not divisible by 7. Write $m = 5^a m^*$ where $(m^*, 2\cdot 5\cdot 7) = 1$. Note that $o_5(7) = 4$ and $(\frac{5}{7}) = -1$. It follows from (7.3) that

$$t_m(f) = \begin{cases} (-1)^a \left(\frac{m^*}{7}\right) & \text{if } a \leq 1, \\ (-1)^{a+1} \left(\frac{m^*}{7}\right) & \text{if } a \geq 2. \end{cases}$$

In the next section, we will revisit these examples and determine $t_m(f)$ for all even m not divisible by 7.

8. From $S(f,n)$ to $S(f,2^s n)$, $s>0$

To find $S(f,2^s n)$, if we use the congruence we used in the previous section, it would yield an answer for $t_{2^s n}(f)$ with congruence *modulo* 2. Since 1 and -1 are congruent (mod 2), that does not help us to determine the sign. In this case, instead of looking at $t_{2^s n}(f)$ modulo 2, we will look at $t_{2^s n}(f)$ modulo 4.

Let $T(i)=\{x\in\mathbb{F}_{p^{2^s n}}\setminus\mathbb{F}_{p^{2n}} : \mathrm{Tr}_{2^s n}(f(x))=i\}$. We can write

$$\begin{aligned} S(f,2^s n) &= \sum_{x\in\mathbb{F}_{p^{2^s n}}\setminus\mathbb{F}_{p^{2n}}} e_{2^s n}(f(x)) + \sum_{x\in\mathbb{F}_{p^{2n}}} e_{2^s n}(f(x)) \\ &= \sum_{i=0}^{p-1} |T(i)|\zeta_p^i + \sum_{x\in\mathbb{F}_{p^{2n}}} e_{2^s n}(f(x)). \end{aligned}$$

The Galois group $\mathrm{Aut}(\mathbb{F}_{p^{2^s n}}/\mathbb{F}_{p^n})$ acts on $T(i)$, and $T(i)$ is a union of $\mathrm{Aut}(\mathbb{F}_{p^{2^s n}}/\mathbb{F}_{p^n})$-orbits of cardinality of 2 to some power greater than or equal to 2. Recall that $\mathrm{Aut}(\mathbb{F}_{p^{2^s n}}/\mathbb{F}_{p^n})$ is cyclic with an order of 2^s. If $x\in\mathbb{F}_{p^{2^s n}}\setminus\mathbb{F}_{p^{2n}}$, then the stabilizer of x in $\mathrm{Aut}(\mathbb{F}_{p^{2^s n}}/\mathbb{F}_{p^n})$ does not contain $\mathrm{Aut}(\mathbb{F}_{p^{2^s n}}/\mathbb{F}_{p^{2n}})$ so the stabilizer of x must be properly contained in $\mathrm{Aut}(\mathbb{F}_{p^{2^s n}}/\mathbb{F}_{p^{2n}})$, i.e. contained in $\mathrm{Aut}(\mathbb{F}_{p^{2^s n}}/\mathbb{F}_{p^{4n}})$. (Note that all subgroups of a cyclic group of order 2^s form a chain.) Thus, the $\mathrm{Aut}(\mathbb{F}_{p^{2^s n}}/\mathbb{F}_{p^n})$-orbits have cardinality that is divisible by 4.

So $|T(i)|\equiv 0 \pmod 4$ for all $0\le i\le p-1$. Therefore,

$$\sum_{x\in\mathbb{F}_{p^{2^s n}}\setminus\mathbb{F}_{p^{2n}}} e_{2^s n}(f(x)) \equiv 0 \pmod 4.$$

This gives us

$$S(f,2^s n) = \sum_{x\in\mathbb{F}_{p^{2n}}} e_{2^s n}(f(x)) \pmod 4. \tag{8.1}$$

Consider the elements of $\mathbb{F}_{p^{2n}}$. For every $x\in\mathbb{F}_{p^{2n}}$, $x^{p^{2n}-1}=1$ if and only if $x\in\mathbb{F}_{p^n}$. So, we can partition $\mathbb{F}_{p^{2n}}$ into

$$\mathbb{F}_{p^{2n}} = \mathbb{F}_{p^n}\cup A\cup B,$$

where

$$\begin{aligned} A &= \{x\in\mathbb{F}_{p^{2n}}^* : x^{p^n-1}=-1\} \\ B &= \{x\in\mathbb{F}_{p^{2n}}^* : x^{p^n-1}\neq\pm 1\}. \end{aligned}$$

The set B can be partitioned even further into four-element subsets of the form $\{\pm x,\pm x^{p^n}\}$. Since $f(-x)=f(x)$ and $f(x^{p^n})=f(x)^{p^n}$, then $e_{2^s n}(f(x))$ is constant on $\{\pm x,\pm x^{p^n}\}$. We can then write

$$\sum_{x\in B} e_{2^s n}(f(x)) \equiv 0 \pmod 4. \tag{8.2}$$

Now, consider A. Choose $\beta\in\mathbb{F}_{p^n}$ such that β is a nonsquare. Also, let $x_0^2=\beta$ where $x_0\in\mathbb{F}_{p^{2n}}$. We then find that $x_0^{p^n-1}=-1$. Also, for every $y\in A$, y can be written as

$y = x_0 x$ where $x \in \mathbb{F}_{p^n}^*$, so A can be rewritten as $A = x_0 \mathbb{F}_{p^n}^*$. Recall that

$$f(x) = \sum_{i=1}^{k} a_i x^{p^{\alpha_i}+1}.$$

So,

$$\begin{aligned}
\sum_{x\in A} e_{2^s n}(f(x)) &= \sum_{x\in A} e_{2^s n}\Big(\sum_{i=1}^{k} a_i x^{p^{\alpha_i}+1}\Big) \\
&= \sum_{x\in \mathbb{F}_{p^n}^*} e_{2^s n}\Big(\sum_{i=1}^{k} a_i x_0^{p^{\alpha_i}+1} x^{p^{\alpha_i}+1}\Big) \\
&= \sum_{x\in \mathbb{F}_{p^n}^*} e_{2^s n}\Big(\sum_{i=1}^{k} a_i \beta^{\frac{1}{2}(p^{\alpha_i}+1)} x^{p^{\alpha_i}+1}\Big) \\
&= \sum_{x\in \mathbb{F}_{p^n}} e_{2^s n}\big(\tilde{f}(x)\big) - 1,
\end{aligned} \tag{8.3}$$

where

$$\tilde{f}(x) = \sum_{i=1}^{k} a_i \beta^{\frac{1}{2}(p^{\alpha_i}+1)} x^{p^{\alpha_i}+1} \in \mathbb{F}_{p^n}[x].$$

Notice that $\tilde{\tilde{f}}(x) = f(\beta x)$ when β is fixed. Combine (8.1) through (8.3). We have

$$\begin{aligned}
S(f, 2^s n) &\equiv \sum_{x\in \mathbb{F}_{p^{2n}}} e_{2^s n}(f(x)) \pmod 4 \\
&= \Big(\sum_{x\in \mathbb{F}_{p^n}} + \sum_{x\in A} + \sum_{x\in B}\Big) e_{2^s n}(f(x)) \\
&= \sum_{x\in \mathbb{F}_{p^n}} e_{2^s n}(f(x)) + \sum_{x\in \mathbb{F}_{p^n}} e_{2^s n}(\tilde{f}(x)) - 1 \pmod 4 \\
&= \Big(\frac{2}{p}\Big)^{s(n-l_n(f))} S(f, n) + \Big(\frac{2}{p}\Big)^{s(n-l_n(\tilde{f}))} S(\tilde{f}, n) - 1.
\end{aligned}$$

Since $S(f,n) = t_n(f) g_p^{n-l_n(f)} p^{l_n(f)}$, then $S(\tilde{f},n) = t_n(\tilde{f}) g_p^{n-l_n(\tilde{f})} p^{l_n(\tilde{f})}$ and $S(f, 2^s n) = t_{2^s n}(f) g_p^{2^s n - l_{2^s n}(f)} p^{l_{2^s n}(f)}$. By substituting these three values into the above equation, we have

$$\begin{aligned}
&t_{2^s n}(f) g_p^{2^s n - l_{2^s n}(f)} p^{l_{2^s n}(f)} \\
\equiv &\Big(\frac{2}{p}\Big)^{s(n-l_n(f))} t_n(f) g_p^{n-l_n(f)} p^{l_n(f)} + \Big(\frac{2}{p}\Big)^{s(n-l_n(\tilde{f}))} t_n(\tilde{f}) g_p^{n-l_n(\tilde{f})} p^{l_n(\tilde{f})} - 1 \pmod 4.
\end{aligned}$$

Since $\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}$ and $p \equiv (-1)^{\frac{1}{2}(p-1)} \pmod 4$, we can further simplify the above to

$$\begin{aligned}
&t_{2^s n}(f) (-1)^{\frac{1}{2}(p-1) l_{2^s n}(f)} g_p^{2^s n - l_{2^s n}(f)} \\
\equiv &(-1)^{\frac{1}{8}(p^2-1) s(n-l_n(f)) + \frac{1}{2}(p-1) l_n(f)} t_n(f) g_p^{n-l_n(f)} \\
&+ (-1)^{\frac{1}{8}(p^2-1) s(n-l_n(\tilde{f})) + \frac{1}{2}(p-1) l_n(\tilde{f})} t_n(\tilde{f}) g_p^{n-l_n(\tilde{f})} - 1 \pmod 4.
\end{aligned}$$

Theorem 8.1. *Let*

$$f(x) = \sum_{i=1}^{k} a_i x^{p^{\alpha_i}+1}$$

and

$$\tilde{f}(x) = \sum_{i=1}^{k} a_i \beta^{\frac{1}{2}(p^{\alpha_i})+1} x^{p^{\alpha_i}+1}$$

and let $s > 0$. Then $l_n(f) + l_n(\tilde{f}) + l_{2^s n}(f)$ is even. Moreover,

$$t_{2^s n}(f) = \begin{cases} t_n(f)t_n(\tilde{f}) & \text{if } l_n(f) \equiv l_n(\tilde{f}) \pmod 2, \\ t_n(f)t_n(\tilde{f})(-1)^{\frac{1}{8}(p^2-1)s} & \text{if } l_n(f) \not\equiv l_n(\tilde{f}) \pmod 2. \end{cases} \tag{8.4}$$

Proof. We begin the proof by showing that $l_n(f) + l_n(\tilde{f}) + l_{2^s n}(f)$ is even. Suppose to the contrary that $l_n(f) + l_n(\tilde{f}) + l_{2^s n}(f)$ is odd. Then, either one or all three terms in $l_n(f) + l_n(\tilde{f}) + l_{2^s n}(f)$ must be odd. This means that exactly one or three of $n - l_n(f)$, $n - l_n(\tilde{f})$, or $2^s n - l_{2^s n}(f)$ must be odd. Recall that $g_p^2 = i^{\frac{1}{2}(p-1)^2} p$ and that $p \equiv (-1)^{\frac{1}{2}(p-1)} \pmod 4$, so

$$\begin{aligned} g_p^2 &\equiv i^{\frac{1}{2}(p-1)^2}(-1)^{\frac{1}{2}(p-1)} \pmod 4 \\ &= i^{\frac{1}{2}(p-1)^2} i^{(p-1)} \\ &= i^{\frac{1}{2}(p-1)^2+(p-1)} \\ &= i^{\frac{1}{2}(p^2-1)} \\ &= 1. \end{aligned}$$

We use the above facts, in the equation

$$\begin{aligned} & t_{2^s n}(f)(-1)^{\frac{1}{2}(p-1)l_{2^s n}(f)} g_p^{2^s n - l_{2^s n}(f)} \\ \equiv\, & (-1)^{\frac{1}{8}(p^2-1)s(n-l_n(f))+\frac{1}{2}(p-1)l_n(f)} t_n(f) g_p^{n-l_n(f)} \\ & + (-1)^{\frac{1}{8}(p^2-1)s(n-l_n(\tilde{f}))+\frac{1}{2}(p-1)l_n(\tilde{f})} t_n(\tilde{f}) g_p^{n-l_n(\tilde{f})} - 1 \pmod 4. \end{aligned} \tag{8.5}$$

The above equation becomes

$$g_p \equiv u \pmod 4$$

for some $u \in \mathbb{Z}$ if only one of the three numbers $n - l_n(f)$, $n - l_n(\tilde{f})$, or $2^s n - l_{2^s n}(f)$ is odd; the above equation becomes

$$-1 \equiv v g_p \pmod 4$$

for some $v \in \mathbb{Z}$ if all three numbers $n - l_n(f)$, $n - l_n(\tilde{f})$, and $2^s n - l_{2^s n}(f)$ are odd. Let $\tau \in \mathrm{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ such that $\tau(g_p) = -g_p$. We can apply τ to both of the above cases. In the first case, we get

$$\begin{cases} g_p \equiv u \pmod 4, \\ -g_p \equiv u \pmod 4. \end{cases}$$

This implies $2g_p \equiv 0 \pmod 4$, which is a contradiction. For the second case, we have

$$\begin{cases} -1 \equiv v g_p \pmod 4, \\ -1 \equiv -v g_p \pmod 4. \end{cases}$$

This leads to $-2 \equiv 0 \pmod 4$ which is a contradiction as well. Therefore, $l_n(f) + l_n(\tilde{f}) + l_{2^s n}(f)$ is even.

To prove the second part of the theorem, we begin by assuming that

$$l_n(f) \equiv l_n(\tilde{f}) \pmod 2.$$

Since $l_n(f)$ and $l_n(\tilde{f})$ have the same parity, then $l_{2^s n}(f)$ is even. Consider

$$\begin{aligned}
&t_{2^s n}(f)(-1)^{\frac{1}{2}(p-1)l_{2^s n}(f)} g_p^{2^s n - l_{2^s n}(f)} \\
\equiv &(-1)^{\frac{1}{8}(p^2-1)s(n-l_n(f))+\frac{1}{2}(p-1)l_n(f)} t_n(f) g_p^{n-l_n(f)} \\
&+ (-1)^{\frac{1}{8}(p^2-1)s(n-l_n(\tilde{f}))+\frac{1}{2}(p-1)l_n(\tilde{f})} t_n(\tilde{f}) g_p^{n-l_n(\tilde{f})} - 1 \pmod 4.
\end{aligned}$$

Thus, since $g_p^2 \equiv 1 \pmod 4$, then $g_p^{2^s n - l_{2^s n}(f)} \equiv 1 \pmod 4$. We can use this and the assumption that $l_n(f) \equiv l_n(\tilde{f}) \pmod 2$ to continue with the above.

$$\begin{aligned}
&t_{2^s n}(f)(-1)^{\frac{1}{2}(p-1)l_{2^s n}(f)} \\
\equiv &(-1)^{\frac{1}{8}(p^2-1)s(n-l_n(f))+\frac{1}{2}(p-1)l_n(f)} t_n(f) g_p^{n-l_n(f)} \\
&+ (-1)^{\frac{1}{8}(p^2-1)s(n-l_n(f))+\frac{1}{2}(p-1)l_n(f)} t_n(\tilde{f}) g_p^{n-l_n(f)} - 1 \pmod 4 \\
\equiv &(t_n(f) + t_n(\tilde{f})) g_p^{n-l_n(f)} (-1)^{\frac{1}{8}(p^2-1)s(n-l_n(f))+\frac{1}{2}(p-1)l_n(f)} - 1 \pmod 4 \\
\equiv &(t_n(f) + t_n(\tilde{f}))\delta - 1 \pmod 4
\end{aligned}$$

where $\delta \in \{\pm 1, \pm g_p\}$. Since $\frac{1}{2}(g_p - 1)$ is integral over $\mathbb{Q}$, then $g_p \equiv 1 \pmod 2$. We can rewrite this to be $2g_p \equiv 2 \pmod 4$ and generalize it further to $2\delta \equiv 2 \pmod 4$. Returning to

$$t_{2^s n}(f) \equiv (t_n(f) + t_n(\tilde{f}))\delta - 1 \pmod 4,$$

recall that as $t_n(f)$ is the type of f, it is either -1 or 1. Then $t_n(f) + t_n(\tilde{f})$ can be either $0, 2$, or -2. If $t_n(f) + t_n(\tilde{f}) = 0$, then $t_{2^s n}(f) \equiv -1 \pmod 4$. If $t_n(f) + t_n(\tilde{f}) = 2$, then $t_{2^s n}(f) \equiv 2\delta - 1 \equiv 1 \pmod 4$. If $t_n(f) + t_n(\tilde{f}) = -2$, then $t_{2^s n}(f) \equiv -2\delta - 1 \equiv 1 \pmod 4$. Thus,

$$t_{2^s n}(f) = \left\{ \begin{array}{ll} -1 & \text{if } t_n(f) + t_n(\tilde{f}) = 0 \\ 1 & \text{if } t_n(f) + t_n(\tilde{f}) = \pm 2 \end{array} \right\} = t_n(f) t_n(\tilde{f}).$$

Now assume that $l_n(f) \not\equiv l_n(\tilde{f}) \pmod 2$. Since they have different parities but the sum is even, then $l_{2^s n}(f)$ is odd. Without loss of generality, assume that $n - l_n(f)$ is odd and $n - l_n(\tilde{f})$ is even. Then, we can simplify (8.5).

$$\begin{aligned}
&t_{2^s n}(f)(-1)^{\frac{1}{2}(p-1)l_{2^s n}(f)} g_p^{2^s n - l_{2^s n}(f)} \\
\equiv &(-1)^{\frac{1}{8}(p^2-1)s(n-l_n(f))+\frac{1}{2}(p-1)l_n(f)} t_n(f) g_p^{n-l_n(f)} \\
&+ (-1)^{\frac{1}{8}(p^2-1)s(n-l_n(\tilde{f}))+\frac{1}{2}(p-1)l_n(\tilde{f})} t_n(\tilde{f}) g_p^{n-l_n(\tilde{f})} - 1 \pmod 4
\end{aligned}$$

$$\begin{aligned}
&t_{2^s n}(f)(-1)^{\frac{1}{2}(p-1)} g_p \\
\equiv &(-1)^{\frac{1}{8}(p^2-1)s+\frac{1}{2}(p-1)l_n(f)} t_n(f) g_p + (-1)^{\frac{1}{2}(p-1)l_n(\tilde{f})} t_n(\tilde{f}) - 1 \pmod 4 \\
= &(-1)^{\frac{1}{8}(p^2-1)s+\frac{1}{2}(p-1)(l_n(\tilde{f}))+\frac{1}{2}(p-1)} t_n(f) g_p + (-1)^{\frac{1}{2}(p-1)l_n(\tilde{f})} t_n(\tilde{f}) - 1
\end{aligned}$$

$$\begin{aligned}
&t_{2^s n}(f)(-1)^{\frac{1}{2}(p-1)} g_p - (-1)^{\frac{1}{8}(p^2-1)s+\frac{1}{2}(p-1)l_n(\tilde{f})+\frac{1}{2}(p-1)} t_n(f) g_p \\
\equiv &(-1)^{\frac{1}{2}(p-1)l_n(\tilde{f})} t_n(\tilde{f}) - 1 \pmod 4
\end{aligned}$$

$$g_p(-1)^{\frac{1}{2}(p-1)} \left[t_{2^s n}(f) - t_n(f)(-1)^{\frac{1}{8}(p^2-1)s+\frac{1}{2}(p-1)l_n(\tilde{f})} \right] \equiv t_n(\tilde{f})(-1)^{\frac{1}{2}(p-1)l_n(\tilde{f})} - 1 \pmod 4$$

So,

$$t_{2^s n}(f) = \begin{cases} t_n(f)(-1)^{\frac{1}{8}(p^2-1)s+\frac{1}{2}(p-1)l_n(\tilde{f})} & \text{if } t_n(\tilde{f})(-1)^{\frac{1}{2}(p-1)l_n(\tilde{f})} = 1, \\ -t_n(f)(-1)^{\frac{1}{8}(p^2-1)s+\frac{1}{2}(p-1)l_n(\tilde{f})} & \text{if } t_n(\tilde{f})(-1)^{\frac{1}{2}(p-1)l_n(\tilde{f})} = -1 \end{cases}$$
$$= t_n(f)t_n(\tilde{f})(-1)^{\frac{1}{8}(p^2-1)s}.$$

Thus, result. □

Example 8.2. Let

$$f(x) = 2x^{3^1+1} + 2x^{3^2+1} + x^{3^3+1} \in \mathbb{F}_3[x]$$

as in Example 7.4 where $t_1(f) = -1$ and $l_1(f) = 0$. Choose $\beta = 2$ as the nonsquare in $\mathbb{F}_3$. Then

$$\tilde{f}(x) = 2x^{3^1+1} + x^{3^2+1} + 2x^{3^3+1}.$$

Since

$$S(\tilde{f}, 1) = \sum_{x\in\mathbb{F}_3} e_1(\tilde{f}(x)) = \sum_{x\in\mathbb{F}_3} e_1(-x^2) = \eta(-1) \sum_{x\in\mathbb{F}_3} = -g_3$$

then $t_1(\tilde{f}) = -1$. Also, $l_1(\tilde{f}) = 0$. By (8.4),

$$t_{2^s}(f) = 1, \quad \text{for } s > 0.$$

Let $m = 2^s 13^b m^*$ where $(m^*, 2 \cdot 3 \cdot 13) = 1$. Note that $o_{13}(3) = 3$. Then, by (7.3),

$$t_m(f) = \begin{cases} -1 & \text{if } b \geq 1, \\ 1 & \text{otherwise.} \end{cases}$$

Example 8.3. Let

$$f(x) = 3x^{7^1+1} + 3x^{7^2+1} + x^{7^3+1} \in \mathbb{F}_7[x]$$

as in Example 7.5 where $t_1(f) = 1$ and $l_1(f) = 1$. Choose $\beta = 3$ as the nonsquare in $\mathbb{F}_7$. Then

$$\tilde{f}(x) = 4x^{7^1+1} + 3x^{7^2+1} + 4x^{7^3+1}.$$

Since

$$S(\tilde{f}, 1) = \sum_{x\in\mathbb{F}_7} e_1(\tilde{f}(x)) = \sum_{x\in\mathbb{F}_7} e_1(4x^2) = g_7$$

then $t_1(\tilde{f}) = 1$. Also, $l_1(\tilde{f}) = 0$. By (8.4),

$$t_{2^s}(f) = 1, \quad \text{for } s > 0.$$

Let $m = 2^s 5^a m^*$ where $s > 0$ and $(m^*, 2 \cdot 5 \cdot 7) = 1$. Then, by (7.3),

$$t_m(f) = \begin{cases} (-1)^a \left(\frac{m^*}{7}\right) & \text{if } a \leq 1, \\ (-1)^{a+1} \left(\frac{m^*}{7}\right) & \text{if } a \geq 2. \end{cases}$$

.

9. From $S(f,n)$ to $S(f,pn)$

Note that both $S(f,n)$ and $S(f,p^n)$ contain a power of p. If we used the congruence method from the two previous sections, we would only get $0 \equiv 0 \pmod{p}$ which is useless. Therefore, to find a relative formula for $S(f,p^n)$ in terms of $S(f,n)$, we have to use a different method.

Let $b \in \mathbb{F}_{p^n}$ such that $\mathrm{Tr}_n(b) \neq 0$. Using the Artin-Schreier Theorem [10, Ch. 5, Prop. 7.8], [12, Ch. VI, Thm 6.4], we have $\mathbb{F}_{p^m} = \mathbb{F}_{p^n}(\epsilon)$ where $\epsilon^p = \epsilon + b$, and the roots of the irreducible polynomial $x^p - x - b$ are $\epsilon + j, j \in \mathbb{F}_p$. Then, for every integer $t \geq 0$, we have

$$\begin{aligned}\mathrm{Tr}_{pn/n}(\epsilon^t) &= \sum_{j\in\mathbb{F}_p} (\epsilon + j)^t \\ &= \sum_{j\in\mathbb{F}_p} \sum_{s=0}^{t} \binom{t}{s} j^s \epsilon^{t-s} \\ &= \sum_{s=0}^{t} \binom{t}{s} \epsilon^{t-s} \sum_{j\in\mathbb{F}_p} j^s\end{aligned}$$

According to [13, Lemma 7.3],

$$\sum_{j\in\mathbb{F}_p} j^s = \begin{cases} -1 & \text{if } s > 0 \text{ and } s \equiv 0 \pmod{(p-1)}, \\ 0 & \text{otherwise.}\end{cases}$$

So we have

$$\mathrm{Tr}_{pn/n}(\epsilon^t) = -\sum_{i>0} \binom{t}{i(p-1)} \epsilon^{t-i(p-1)}. \tag{9.1}$$

Lemma 9.1. *Let u, v be integers such that $0 \leq u, v \leq p-1$. Then*

$$\mathrm{Tr}_{pn/n}(\epsilon^{u+v}) = \begin{cases} 0 & \text{if } u+v \neq p-1, 2(p-1), \\ -1 & \text{if } u+v = p-1, 2(p-1).\end{cases}$$

If α is a positive integer, then

$$\begin{aligned}\mathrm{Tr}_{pn/n}(\epsilon^{u+vp^\alpha}) = &-\binom{v}{u+v-(p-1)} (b^{p^0} + \cdots + b^{p^{\alpha-1}})^{u+v-(p-1)} \\ &+ \begin{cases} 0 & \text{if } u+v \neq 2(p-1) \\ -1 & \text{if } u+v = 2(p-1).\end{cases}\end{aligned}$$

Proof. Write $u+v = u' + v'p$, where $0 \le u', v' \le p-1$. We now have

$$\begin{aligned}
\mathrm{Tr}_{pn/n}(\epsilon^{u+v}) &= -\sum_{i>0} \binom{u+v}{i(p-1)} \epsilon^{u+v-i(p-1)} \\
&= -\binom{u+v}{p-1}\epsilon^{u+v-(p-1)} - \binom{u+v}{2(p-1)}\epsilon^{u+v-2(p-1)} \\
&= -\binom{u'+v'p}{p-1}\epsilon^{u+v-(p-1)} - \binom{u'+v'p}{2(p-1)}\epsilon^{u+v-2(p-1)} \\
&= -\binom{u'+v'p}{p-1}\epsilon^{u+v-(p-1)} - \binom{u'+v'p}{(p-2)+p}\epsilon^{u+v-2(p-1)} \\
&= -\binom{u'}{p-1}\epsilon^{u+v-(p-1)} - \binom{u'}{p-2}\binom{v'}{1}\epsilon^{u+v-2(p-1)} \\
&= \begin{cases} -1 & \text{if } (u',v') = (p-1,0) \text{ or } (p-2,1), \text{ i.e. } u+v = p-1 \text{ or } 2(p-1) \\ 0 & \text{otherwise.} \end{cases}
\end{aligned}$$

Using (9.1) again as we prove the second part of the theorem,

$$\mathrm{Tr}_{pn/n}(\epsilon^{u+vp^\alpha}) = -\sum_{i>0} \binom{u+vp^\alpha}{i(p-1)} \epsilon^{u+vp^\alpha - i(p-1)}.$$

Write $i(p-q) = s + s_1 p + \cdots + s_{\alpha-1}p^{\alpha-1} + tp^\alpha$ where $0 \le s, s_1, \ldots, s_{\alpha-1}, p \le p-1$. By the Lucas Theorem [14],

$$\binom{u+vp^\alpha}{i(p-1)} \equiv \begin{cases} \binom{u}{s}\binom{v}{t} \pmod p & \text{if } s_1 = \cdots = s_{\alpha-1} = 0, \\ 0 \pmod p & \text{otherwise.} \end{cases}$$

So,

$$\begin{aligned}
&\mathrm{Tr}_{pn/n}(\epsilon^{u+vp^\alpha}) \\
&= - \sum_{\substack{0\le s,t\le p-1 \\ 0<s+tp^\alpha \equiv 0 \pmod{(p-1)}}} \binom{u+vp^\alpha}{s+tp^\alpha} \epsilon^{u+vp^\alpha-(s+tp^\alpha)} \\
&= - \sum_{\substack{0\le s\le u \\ 0\le t\le v \\ 0<s+t\equiv 0 \pmod{(p-1)}}} \binom{u}{s}\binom{v}{t} \epsilon^{u-s+(v-t)p^\alpha} \\
&= - \sum_{\substack{0\le s\le u \\ 0\le t\le v \\ u+v>s+t\equiv u+v \pmod{(p-1)}}} \binom{u}{s}\binom{v}{t} \epsilon^{s+tp^\alpha} \qquad (s\mapsto u-s,\ t\mapsto v-t).
\end{aligned}$$

Since $\epsilon^p = \epsilon + b$, then, by induction, we have $\epsilon^{p^\alpha} = \epsilon + b^{p^0} + \cdots + b^{p^{\alpha-1}}$. Thus,

$$\begin{aligned}
&\mathrm{Tr}_{pn/n}(\epsilon^{u+vp^\alpha}) \\
&= - \sum_{\substack{0\le s\le u\\ 0\le t\le v\\ u+v>s+t\equiv u+v \pmod{(p-1)}}} \binom{u}{s}\binom{v}{t}\epsilon^s(\epsilon + b^{p^0} + \cdots + b^{p^{\alpha-1}})^t \\
&= - \sum_{\substack{0\le s\le u\\ 0\le t\le v\\ u+v>s+t\equiv u+v \pmod{(p-1)}}} \binom{u}{s}\binom{v}{t}\sum_{\tau=0}^{t}\binom{t}{\tau}(\epsilon + b^{p^0} + \cdots + b^{p^{\alpha-1}})^{t-\tau}\epsilon^{s+\tau}
\end{aligned}$$

In the above sum, $s+\tau \le s+t \le u+v-(p-1) \le p-1$. Since $\mathrm{Tr}_{pn/n}(\epsilon^{u+vp^\alpha}) \in \mathbb{F}_{p^n}$, then we only have to sum the terms where $s+\tau = 0$ which is when $s = \tau = 0$. So,

$$\begin{aligned}
&\mathrm{Tr}_{pn/n}(\epsilon^{u+vp^\alpha}) \\
&= - \sum_{\substack{0\le t\le v\\ u+v>t\equiv u+v \pmod{(p-1)}}} \binom{v}{t}(\epsilon + b^{p^0} + \cdots + b^{p^{\alpha-1}})^t \\
&= -\binom{v}{u+v-(p-1)}(b^{p^0} + \cdots + b^{p^{\alpha-1}})^{u+v-(p-1)} + \begin{cases} 0 & \text{if } u+v \ne 2(p-1),\\ -1 & \text{if } u+v = 2(p-1).\end{cases}
\end{aligned}$$

Thus, result. □

Theorem 9.2. *Let f be as previously stated. Assume*

$$\nu_p(n) < \min\{\nu_p(\alpha_i) : 1 \le i \le k\}.$$

Then,

$$S(f, pn) = p^{\frac{1}{2}(p-3)(n+l_n(f))}|S(f,n)|^2\,\overline{S(f,n)}.$$

Moreover,

$$\begin{aligned} l_{pn}(f) &= p\,l_n(f),\\ t_{pn}(f) &= t_n(f).\end{aligned}$$

Proof. Let $v_p(n) = v$ and write $n = p^v n'$ where $p \nmid n'$. Choose $b \in \mathbb{F}_{p^{p^v}}$ such that $\mathrm{Tr}_{p^v}(b) \ne 0$. Then $\mathrm{Tr}_n(b) = \mathrm{Tr}_{p^v n'}(b) = n'\mathrm{Tr}_{p^v}(b) \ne 0$. Since $v_p(\alpha_i) > v$, we have

$$b^{p^0} + \cdots + b^{p^{\alpha_i-1}} = \mathrm{Tr}_{\alpha^i}(b) = 0. \tag{9.2}$$

(Note that if $\alpha_i = 0$ then $b^{p^0} + \cdots + b^{p^{\alpha-1}}$ is an empty sum.) Recall that

$$\mathrm{Tr}_{pn/n}(\epsilon^{u+vp^{\alpha_i}}) = \begin{cases} 0 & \text{if } u+v \ne p-1, 2(p-1)\\ -1 & \text{if } u+v = p-1, 2(p-1).\end{cases}$$

for all $1 \le i \le k$ and all $0 \le u, v \le p-1$. Let $x = x_0\epsilon^0 + \cdots + x_{p-1}\epsilon^{p-1} \in \mathbb{F}_{p^{pn}}$, where $x_u \in \mathbb{F}_{p^n}$, $0 \le u \le p-1$. Then

$$
\begin{aligned}
&\mathrm{Tr}_{pn}\big(f(x)\big)\\
&= \mathrm{Tr}_{pn}\Big(\sum_{i=1}^{k} a_i (x_0\epsilon^0 + \cdots + x_{p-1}\epsilon^{p-1})^{1+p^{\alpha_i}}\Big)\\
&= \mathrm{Tr}_{pn}\Big(\sum_{i=1}^{k} a_i \sum_{0\le u,v\le p-1} x_u x_v^{p^{\alpha_i}} \epsilon^{u+vp^{\alpha_i}}\Big)\\
&= \mathrm{Tr}_{n}\Big[\sum_{i=1}^{k} a_i \sum_{0\le u,v\le p-1} x_u x_v^{p^{\alpha_i}} \mathrm{Tr}_{pn/n}(\epsilon^{u+vp^{\alpha_i}})\Big]\\
&= -\mathrm{Tr}_{n}\Big[\sum_{i=1}^{k} a_i \sum_{\substack{0\le u,v\le p-1\\ u+v=p-1,\,2(p-1)}} x_u x_v^{p^{\alpha_i}}\Big]\\
&= -\mathrm{Tr}_{n}\Big[\sum_{i=1}^{k} a_i \Big(x_{p-1}^{1+p^{\alpha_i}} + x_0 x_{p-1}^{p^{\alpha_i}} + x_{p-1}x_0^{p^{\alpha_i}} + x_{\frac{1}{2}(p-1)}^{1+p^{\alpha_i}} + \sum_{u=1}^{\frac{1}{2}(p-3)} (x_u x_{p-1-u}^{p^{\alpha_i}} + x_{p-1-u}x_u^{p^{\alpha_i}})\Big)\Big]\\
&= -\mathrm{Tr}_{n}\Big[\sum_{i=1}^{k} a_i \Big(x_{p-1}^{1+p^{\alpha_i}} + x_0 x_{p-1}^{p^{\alpha_i}} + x_{p-1}x_0^{p^{\alpha_i}} + x_0^{1+p^{\alpha_i}} - x_0^{1+p^{\alpha_i}} + x_{\frac{1}{2}(p-1)}^{1+p^{\alpha_i}}\\
&\quad + \sum_{u=1}^{\frac{1}{2}(p-3)} (x_u x_{p-1-u}^{p^{\alpha_i}} + x_{p-1-u}x_u^{p^{\alpha_i}})\Big)\Big]\\
&= -\mathrm{Tr}_{n}\Big[\sum_{i=1}^{k} a_i \Big((x_0 + x_{p-1})^{1+p^{\alpha_i}} - x_0^{1+p^{\alpha_i}} + x_{\frac{1}{2}(p-1)}^{1+p^{\alpha_i}}\Big)\\
&\quad + \sum_{u=1}^{\frac{1}{2}(p-3)} \sum_{i=1}^{k} a_i (x_u x_{p-1-u}^{p^{\alpha_i}} + x_{p-1-u}x_u^{p^{\alpha_i}})\Big]\\
&= -\mathrm{Tr}_{n}\Big[f(x_0 + x_{p-1}) - f(x_0) + f(x_{\frac{1}{2}(p-1)}) + \sum_{u=1}^{\frac{1}{2}(p-3)} \sum_{i=1}^{k} (a_i x_u x_{p-1-u}^{p^{\alpha_i}} + a_i x_{p-1-u}x_u^{p^{\alpha_i}})\Big]\\
&= -\mathrm{Tr}_{n}\Big[f(x_0 + x_{p-1}) - f(x_0) + f(x_{\frac{1}{2}(p-1)}) + \sum_{u=1}^{\frac{1}{2}(p-3)} \sum_{i=1}^{k} (a_i x_u x_{p-1-u}^{p^{\alpha_i}} + a_i^{p^{-\alpha_i}} x_{p-1-u}^{p^{-\alpha_i}} x_u)\Big]\\
&= -\mathrm{Tr}_{n}\Big[f(x_0 + x_{p-1}) - f(x_0) + f(x_{\frac{1}{2}(p-1)}) + \sum_{u=1}^{\frac{1}{2}(p-3)} \sum_{i=1}^{k} x_u (a_i x_{p-1-u}^{p^{\alpha_i}} + a_i^{p^{-\alpha_i}} x_{p-1-u}^{p^{-\alpha_i}})\Big]\\
&= -\mathrm{Tr}_{n}\Big[f(x_0 + x_{p-1}) - f(x_0) + f(x_{\frac{1}{2}(p-1)}) + \sum_{u=1}^{\frac{1}{2}(p-3)} x_u \sum_{i=1}^{k} (a_i x_{p-1-u}^{p^{\alpha_i}} + a_i^{p^{-\alpha_i}} x_{p-1-u}^{p^{-\alpha_i}})\Big]\\
&= -\mathrm{Tr}_{n}\Big[f(x_0 + x_{p-1}) - f(x_0) + f(x_{\frac{1}{2}(p-1)}) + \sum_{u=1}^{\frac{1}{2}(p-3)} x_u f^*(x_{p-1-u})^{p^{-\alpha}}\Big].
\end{aligned}
$$

Then,

$$\begin{aligned}
&S(f,pn)\\
&= \sum_{(x_0,\ldots,x_{p-1})\in\mathbb{F}_{p^n}^p} e_n\Big[-f(x_0+x_{p-1})+f(x_0)-f(x_{\frac{1}{2}(p-1)})-\sum_{u=1}^{\frac{1}{2}(p-3)} x_u f^*(x_{p-1-u})^{p^{-\alpha}}\Big]\\
&= \overline{S(f,n)}^2 S(f,n)\prod_{n=1}^{\frac{1}{2}(p-3)}\Big(\sum_{x_u,x_{p-1-u}\in\mathbb{F}_{p^n}} e_n\big(-x_u f^*(x_{p-1-u})^{p^{-\alpha}}\big)\Big)\\
&= |S(f,n)|^2\,\overline{S(f,n)}\prod_{n=1}^{\frac{1}{2}(p-3)} p^{l_n(f)+n}\\
&= p^{\frac{1}{2}(p-3)(n+l_n(f))}|S(f,n)|^2\,\overline{S(f,n)}.
\end{aligned}$$

Since $S(f,pn)=t_{pn}g_p^{pn-l_pn(f)}p^{l_{pn}(f)}$, then

$$t_{pn}(f)g_p^{pn-l_{pn}(f)}p^{l_{pn}(f)} = p^{\frac{1}{2}(p-3)(n+l_n(f))}|S(f,n)|^2\,\overline{S(f,n)}$$

Consider the two sides separately. The left-hand side equals

$$\begin{aligned}
&t_{pn}(f)(i^{\frac{1}{4}(p-1)^2}p^{\frac{1}{2}})^{pn-l_{pn}(f)}p^{l_{pn}(f)}\\
=&\,t_{pn}(f)i^{\frac{1}{4}(p-1)^2(pn-l_{pn}(f))}p^{\frac{1}{2}(pn-l_{pn}(f)+l_{pn}(f))}\\
=&\,t_{pn}(f)i^{\frac{1}{4}(p-1)^2(pn-l_{pn}(f))}p^{\frac{1}{2}(pn+l_{pn}(f))}.
\end{aligned}$$

When we look at the right-hand side, we get

$$\begin{aligned}
&p^{\frac{1}{2}(p-3)(n+l_n(f))}|S(f,n)|^2\,\overline{S(f,n)}\\
=&\,p^{\frac{1}{2}(p-3)(n+l_n(f))}|t_n(f)g_p^{n-l_n(f)}p^{l_n(f)}|^2\,\overline{t_n(f)g_p^{n-l_n(f)}p^{l_n(f)}}\\
=&\,p^{\frac{1}{2}(p-3)(n+l_n(f))}p^{n+l_n(f)}t_n(f)(i^{\frac{-1}{4}(p-1)^2}p^{\frac{1}{2}})^{n-l_n(f)}p^{l_n(f)}\\
=&\,t_n(f)p^{\frac{1}{2}(p-3)(n+l_n(f))}p^{n+l_n(f)}i^{\frac{-1}{4}(p-1)^2(n-l_n(f))}p^{\frac{1}{2}(n-l_n(f))+l_n(f)}\\
=&\,t_n(f)p^{\frac{1}{2}p(n+l_n(f))-\frac{3}{2}(n+l_n(f))}p^{n+l_n(f)}i^{-\frac{1}{4}(p-1)^2(n-l_n(f))}p^{\frac{1}{2}(n+l_n(f))}\\
=&\,t_n(f)p^{\frac{1}{2}p(n+l_n(f))}i^{-\frac{1}{4}(p-1)^2(n-l_n(f))}.
\end{aligned}$$

This yields

$$t_{pn}(f)i^{\frac{1}{4}(p-1)^2(pn-l_{pn}(f))}p^{\frac{1}{2}(pn+l_{pn}(f))} = t_n(f)p^{\frac{1}{2}p(n+l_n(f))}i^{-\frac{1}{4}(p-1)^2(n-l_n(f))}.$$

Thus, $l_{pn}(f)=p\,l_n(f)$. We can then simplify further

$$\begin{aligned}
t_{pn}(f) &= t_n(f)i^{-\frac{1}{4}(p-1)^2[(n-l_n(f))+(pn-l_{pn}(f))]}\\
&= t_n(f)i^{-\frac{1}{4}(p-1)^2[(n-l_n(f))+p(n-l_n(f))]}\\
&= t_n(f)i^{-\frac{1}{4}(p-1)^2[(p+1)(n-l_n(f))]}\\
&= t_n(f).
\end{aligned}$$

Thus, result. □

10. When $\nu_2(\alpha_1) = \nu_2(\alpha_2) = \cdot\ \cdot\ \cdot = \nu_2(\alpha_k)$

Lemma 10.1. *Let $\alpha_1, \ldots, \alpha_k \geq 0$ be integers. Then*

$$\gcd(p^{\alpha_1} + 1, \ldots, p^{\alpha_k} + 1) > 2 \Leftrightarrow \nu_2(\alpha_1) = \cdots = \nu_2(\alpha_k) < \infty.$$

When $\nu_2(\alpha_1) = \cdots = \nu_2(\alpha_k) < \infty$,

$$\gcd(p^{\alpha_1} + 1, \ldots, p^{\alpha_k} + 1) = p^{\gcd(\alpha_1, \ldots, \alpha_k)} + 1.$$

Proof. It is sufficient to prove the lemma with $k = 2$.

($\Leftarrow$) Since $\frac{\alpha_i}{(\alpha_1, \alpha_2)}$, $i = 1, 2$, are odd, $p^{(\alpha_1, \alpha_2)} + 1 \mid p^{\alpha_i} + 1$ for $i = 1, 2$. Thus, $p^{(\alpha_1, \alpha_2)} + 1 \mid (p^{\alpha_1} + 1, p^{\alpha_2} + 1)$. Also, since

$$\begin{aligned} \frac{1}{2}(p^{\alpha_1} + 1, p^{\alpha_2} + 1) &\mid \frac{1}{2}\Big(\frac{1}{2}(p^{2\alpha_1} - 1), \frac{1}{2}(p^{2\alpha_2} - 1)\Big) \\ &= \frac{1}{4}(p^{2(\alpha_1, \alpha_2)} - 1) \\ &= \frac{p^{(\alpha_1, \alpha_2)} + 1}{2} \cdot \frac{p^{(\alpha_1, \alpha_2)} + 1}{2} \end{aligned}$$

and since $(\frac{p^{\alpha_1} + 1}{2}, \frac{p^{(\alpha_1, \alpha_2)} - 1}{2}) = 1$, we have $\frac{1}{2}(p^{\alpha_1} + 1, p^{\alpha_2} + 1) \mid \frac{1}{2}(p^{(\alpha_1, \alpha_2)} + 1)$ which is $(p^{\alpha_1} + 1, p^{\alpha_2} + 1) \mid p^{(\alpha_1, \alpha_2)} + 1$. Thus, $(p^{\alpha_1} + 1, p^{\alpha_2} + 1) = p^{(\alpha_1, \alpha_2)} + 1$.

($\Rightarrow$) Clearly, $\alpha_i > 0$ for every $1 \leq i \leq k$. Assume to the contrary that $\nu(\alpha_1) > \nu(\alpha_2)$. Suppose that $\alpha_1 = 2^i \alpha_1'$ and $\alpha_2 = 2^j \alpha_2'$ where $i > j$ and α_1' and α_2' are odd. Then,

$$\begin{aligned} (p^{\alpha_1} + 1, p^{\alpha_2} + 1) &\mid (p^{2^i \alpha_1' \alpha_2'} + 1, p^{2\alpha_2} - 1) \\ &\mid (p^{2^i \alpha_1' \alpha_2'} + 1, p^{2^i \alpha_1 \alpha_2} - 1) \\ &= 2 \end{aligned}$$

which is a contradiction. Thus, we have proven the lemma. □

Lemma 10.2. *Let $\alpha, \beta \geq 0$ be integers. Then*

$$(p^{\alpha} + 1, p^{\beta} - 1) = \begin{cases} p^{(\alpha, \beta)} + 1 & \text{if } \nu_2(\beta) > \nu_2(\alpha), \\ 2 & \text{if } \nu_2(\beta) \leq \nu_2(\alpha). \end{cases}$$

Proof. Since $(0, m) = m$, then if any α or β is 0, the conclusion is obvious. Thus, assume $\alpha, \beta > 0$.

First assume $\nu_2(\beta) > \nu_2(\alpha)$. Recall that ν_2 is the 2-adic order function. Since $\frac{\alpha}{(\alpha,\beta)}$ is odd, then $p^{(\alpha,\beta)}+1 \mid p^\alpha+1$. Since $\frac{\alpha}{(\alpha,\beta)}$ is even, then $p^{(\alpha,\beta)}+1 \mid p^\beta-1$. Thus, $p^{(\alpha,\beta)}+1 \mid (p^\alpha+1, p^\beta-1)$. Note that

$$\begin{aligned}\frac{1}{2}(p^\alpha+1,p^\beta-1) &\mid \frac{1}{2}(p^{2\alpha}-1,p^\beta-1)\\ &= \frac{1}{2}(p^{(2\alpha,\beta)}-1)\\ &= \frac{1}{2}(p^{2(\alpha,\beta)}-1)\\ &= \frac{1}{2}(p^{(\alpha,\beta)}-1)(p^{(\alpha,\beta)}+1).\end{aligned}$$

Since $(\frac{1}{2}(p^\alpha+1), \frac{1}{2}(p^{(\alpha,\beta)}-1)) = 1$ this implies that $\frac{1}{2}(p^\alpha+1,p^\beta-1) \mid p^{(\alpha,\beta)}+1$. For each $x \in \mathbb{Z}$ and an odd integer $k>0$, we have $\nu_2(1+x^k) = \nu_2(1+x)$. By this we get $\nu_2(p^\alpha+1) = \nu_2(p^{(\alpha,\beta)}+1)$ and $\nu_2(p^\beta-1) \geq \nu_2(p^\alpha+1)$. Then $\nu_2(p^\alpha+1,p^\beta-1) = \nu_2(p^{(\alpha,\beta)}+1)$. Then, using $\frac{1}{2}(p^\alpha+1,p^\beta-1) \mid p^{(\alpha,\beta)}+1$, we get $(p^\alpha+1,p^\beta-1) \mid p^{(\alpha,\beta)}+1$. Thus, $(p^\alpha+1,p^\beta-1) \mid p^{(\alpha,\beta)}+1$.

For the second part, assume that $\nu_2(\beta) \leq \nu_2(\alpha)$. Then,

$$\begin{aligned}\Big(\frac{p^\alpha+1}{2}\cdot\frac{p^\beta-1}{2},\frac{p^\beta-1}{2}\Big) &\mid \frac{1}{2}(p^{2\alpha-1},p^\beta-1)\\ &= \frac{1}{2}(p^{(2\alpha,\beta)}-1)\\ &= \frac{1}{2}(p^{(\alpha,\beta)}-1)\\ &= \Big(\frac{p^\alpha-1}{2},\frac{p^\beta-1}{2}\Big).\end{aligned}$$

Since $(\frac{p^\alpha+1}{2}, \frac{p^\alpha-1}{2}) = 1$, then $(\frac{p^\alpha+1}{2}, \frac{p^\beta-1}{2}) = 1$ which gives us

$$(p^\alpha+1, p^\beta-1) = 2.$$

This completes the proof. □

Theorem 10.3. *Let f be as previously stated. Assume that $\nu_2(\alpha_1) = \cdots = \nu_2(\alpha_k) = \nu$ and that $\nu_2(n) > \nu$. Then $2^{\nu+1} \mid l_n(f)$ and*

$$t_n(f) = (-1)^{(\frac{1}{4}(p-1)^2 2^\nu+1)\frac{n-l_n(f)}{2^{\nu+1}}} = \begin{cases}(-1)^{(\frac{1}{4}(p-1)^2+1)\frac{n-l_n(f)}{2^{\nu+1}}} & \text{if } \nu=0,\\ (-1)^{\frac{n-l_n(f)}{2^{\nu+1}}} & \text{if } \nu>0.\end{cases}$$

Proof. Using the two lemmas above, we have

$$\begin{aligned}\gcd(p^{\alpha_1}+1,\ldots,p^{\alpha_k}+1,p^n-1) &= (p^{\gcd(\alpha_1,\ldots,\alpha_k)}+1,p^n-1)\\ &= p^{\gcd(\alpha_1,\ldots,\alpha_k,n)}+1\\ &\equiv 0 \pmod{(p^{2^\nu}+1)}.\end{aligned} \tag{10.1}$$

Let $q = p^{2^\nu}+1$. Then $2^{\nu+1}$ is the multiplicative order of $p \pmod q$, namely, $o_q(p) = 2^{\nu+1}$. Since $2^{\nu+1} \mid n$, then $q \mid p^n-1$.

First we need to show that $2^{\nu+1} \mid l_n(f)$. To do that, we show that $\{x \in \mathbb{F}_{p^n} : f^*(x) = 0\}$ is a vector space over $\mathbb{F}_{p^{2^{\nu+1}}}$. Let $x \in \mathbb{F}_{p^n}$ such that $f^*(x) = 0$. Also, let $y \in \mathbb{F}_{p^{2^{\nu+1}}}$. Then,

we want to show that $f^*(xy) = 0$. Using the definition of f^*, we have

$$f^*(yx)^{p^{-\alpha}} = \sum_{i=1}^{k} (a_i y^{p^{\alpha_i}} x^{p^{\alpha_i}} + a_i^{p^{-\alpha_i}} y^{p^{-\alpha_i}} x^{p^{-\alpha_i}}).$$

We claim that $y^{p^{\pm\alpha_i}} = y^{p^\alpha}$ for all $1 \le i \le k$. By equation (10.1), $p^{\alpha_i} \equiv -1 \pmod q$ which implies that $p^{\pm\alpha_i} \equiv -1 \pmod q$. Then, $p^\alpha \equiv -1 \equiv p^{\pm\alpha_i} \pmod q$. This leads to $p^{\alpha \mp \alpha_i} \equiv 1 \pmod q$ for all $1 \le i \le k$. Since $o_q(p) = 2^{\nu+1}$, then $\alpha \mp \alpha_i \equiv 0 \pmod{2^{\nu+1}}$. Thus, $y^{p^{\alpha \mp \alpha_i}} = y$ which implies that $y^{p^\alpha} = y^{p^{\pm\alpha}}$. Then $f^*(yx)^{p^{-\alpha}}$ becomes

$$\begin{aligned} f^*(yx)^{p^{-\alpha}} &= \sum_{i=1}^{k} (a_i y^{p^\alpha} x^{p^{\alpha_i}} + a_i^{p^{-\alpha_i}} y^{p^\alpha} x^{p^{-\alpha_i}}) \\ &= y^{p^\alpha} \Big(\sum_{i=1}^{k} (a_i x^{p^{\alpha_i}} + a_i^{p^{-\alpha_i}} x^{p^{-\alpha_i}}) \Big) \\ &= y^{p^\alpha} f^*(x)^{p^{-\alpha}} = 0. \end{aligned}$$

Thus, $f^*(yx) = 0$. So, we have proved that $2^{\nu+1} \mid l_n(f)$.

Now, choose $z \in \mathbb{F}_{p^n}^*$ such that $o(z) = q$. Since $p^{\alpha_i} + 1 \equiv 0 \pmod q$ for all $1 \le i \le k$, we have $f(yx) = f(x)$ for all $y \in \langle z \rangle$. So,

$$\begin{aligned} t_n(f) g_p^{n - l_n(f)} p^{l_n(f)} &= S(f, n) \\ &= 1 + \sum_{x \in \mathbb{F}_{p^n}^*} e_n(f(x)) \\ &= 1 + \sum_{x \in \mathbb{F}_{p^n}^* / \langle z \rangle} \sum_{y \in \langle z \rangle} e_n(f(xy)) \\ &= 1 + \sum_{x \in \mathbb{F}_{p^n}^* / \langle z \rangle} e_n(f(x)) \cdot q \\ &= 1 + q \sum_{x \in \mathbb{F}_{p^n}^* / \langle z \rangle} e_n(f(x)) \\ &\equiv 1 \pmod q. \end{aligned}$$

In the above, $p^{l_n(f)} \equiv 1 \pmod q$ since $o_q(p) = 2^{\nu+1} \mid l_n(f)$. Also,

$$\begin{aligned} g_p^{2^{\nu+1}} &= \left[i^{\frac{1}{4}(p-1)^2} p^{\frac{1}{2}} \right]^{2^{\nu+1}} = i^{\frac{1}{4}(p-1)^2 2^\nu 2} p^{\frac{1}{2}(2^\nu 2)} \\ &= (-1)^{\frac{1}{4}(p-1)^2 2^\nu} p^{2^\nu} \equiv (-1)^{\frac{1}{4}(p-1)^2 2^\nu + 1} \pmod q; \end{aligned}$$

hence,

$$g_p^{n - l_n(f)} = g_p^{2^{\nu+1} \frac{n - l_n(f)}{2^{\nu+1}}} \equiv (-1)^{(\frac{1}{4}(p-1)^2 2^\nu + 1) \frac{n - l_n(f)}{2^{\nu+1}}} \pmod q.$$

This leads to

$$t_n(f) = (-1)^{(\frac{1}{4}(p-1)^2 2^\nu + 1) \frac{n - l_n(f)}{2^{\nu+1}}}.$$

□

Corollary 10.4. *Assume $p \equiv -1 \pmod 4$, $\alpha_1, \ldots, \alpha_k$ are all odd and n is even. Then $t_n(f) = 1$.*

Proof. This follows immediately from Theorem 10.3. □

Example 10.5. Let $f(x) = 2x^{3^1+1} + x^{3^3+1} \in \mathbb{F}_3[x]$. Then $f^*(x) = x^{3^0} + 2x^{3^2} + 2x^{3^4} + x^{3^6}$. The splitting field of f^* over $\mathbb{F}_3$ is $\mathbb{F}_{3^{12}}$ and

$$l_{2^a 3^b m^*}(f) = \begin{cases} 6 & \text{if } a \geq 2,\ b \geq 1 \\ 4 & \text{if } a = 1,\ b \geq 1 \text{ or } a \geq 2,\ b = 0, \\ 2 & \text{if } a = 1,\ b = 0 \text{ or } a = 0,\ b \geq 1, \\ 1 & \text{if } a, b = 0. \end{cases}$$

where $(m^*, 2 \cdot 3) = 1$. By Corollary 10.4, for even n,

$$t_n(f) = 1.$$

11. The Formula for $S(ax^{1+p^\alpha})$

Theorem 10.3 helps to provide a proof for the evaluation of the sum of $S(ax^{p^\alpha+1}, n)$, a special case of the sum in Theorem 10.3

Corollary 11.1. *Let $a \in \mathbb{F}_{p^n}^*$ and let $\alpha \geq 0$.*

(i) *If $\nu_2(n) \leq \nu_2(\alpha)$,*

$$S(ax^{p^\alpha+1}, n) = \eta(a)(-1)^{n-1} i^{\frac{1}{4}(p-1)^2 n} p^{\frac{1}{2}n}.$$

(ii) *If $\nu_2(n) = \nu_2(\alpha) + 1$,*

$$S(ax^{p^\alpha+1}, n) = \begin{cases} p^{\frac{1}{2}[n+(2\alpha,n)]} & \text{if } a^{\frac{(p^\alpha-1)(p^n-1)}{p^{(2\alpha,n)}-1}} = -1, \\ -p^{\frac{1}{2}n} & \text{otherwise.} \end{cases}$$

(iii) *If $\nu_2(n) > \nu_2(\alpha) + 1$,*

$$S(ax^{p^\alpha+1}, n) = \begin{cases} -p^{\frac{1}{2}[n+(2\alpha,n)]} & \text{if } a^{\frac{(p^\alpha-1)(p^n-1)}{p^{(2\alpha,n)}-1}} = 1, \\ p^{\frac{1}{2}n} & \text{otherwise.} \end{cases}$$

Proof. We first need to determine $l_n(f)$. We claim that

$$l_n(f) = \begin{cases} (2\alpha, n) & \text{if } a^{\frac{(p^\alpha-1)(p^n-1)}{p^{(2\alpha,n)}-1}} = (-1)^{\frac{p^n-1}{p^{(2\alpha,n)}-1}} \\ 0 & \text{otherwise.} \end{cases} \tag{11.1}$$

Note that $f^*(x) = a^{p^\alpha} x^{p^{2\alpha}} + ax = a^{p^\alpha} x(x^{p^{2\alpha}-1} + a^{1-p^\alpha})$. So, if $f^*(x) = 0$ has a solution in $\mathbb{F}_{p^n}^*$, the number of solutions will be $(p^{2\alpha} - 1, p^n - 1) = p^{(2\alpha,n)} - 1$. So,

$$l_n(f) = \begin{cases} (2\alpha, n) & \text{if } f^*(x) = 0 \text{ has a solution in } \mathbb{F}_{p^n}^*, \\ 0 & \text{otherwise.} \end{cases}$$

Notice that $f^*(x) = 0$ has a solution in $\mathbb{F}_{p^n}^*$ if and only if $-a^{p^\alpha-1} = x^{p^{2\alpha}-1}$ for some $x \in \mathbb{F}_{p^n}^*$. This happens if and only if

$$\left(-a^{p^\alpha-1}\right)^{\frac{p^n-1}{(p^{2\alpha}-1,p^n-1)}} = 1,$$

$$\left(-a^{p^\alpha-1}\right)^{\frac{p^n-1}{p^{(2\alpha,n)}-1}} = 1,$$

$$(-1)^{\frac{p^n-1}{p^{(2\alpha,n)}-1}} \left(a^{p^\alpha-1}\right)^{\frac{p^n-1}{p^{(2\alpha,n)}-1}} = 1,$$

$$(-1)^{\frac{p^n-1}{p^{(2\alpha,n)}-1}} a^{\frac{(p^\alpha-1)(p^n-1)}{p^{(2\alpha,n)}-1}} = 1,$$

$$a^{\frac{(p^\alpha-1)(p^n-1)}{p^{(2\alpha,n)}-1}} = (-1)^{\frac{p^n-1}{p^{(2\alpha,n)}-1}}.$$

This yields (11.1).

(i) Since $\nu_2(n) \le \nu_2(\alpha)$, we can use Lemma 10.2 which says $(p^\alpha+1, p^n-1) = 2$. Then, $x \mapsto x^{p^\alpha+1}$ is a 2-to-1 map from $\mathbb{F}_{p^n}^*$ to $(\mathbb{F}_{p^n}^*)^2$. Thus,

$$\begin{aligned}
&S(ax^{p^\alpha+1}, n)\\
=&1 + \sum_{x\in\mathbb{F}_{p^n}^*} e_n(ax^{p^\alpha+1}) = 1 + 2\sum_{x\in(\mathbb{F}_{p^n}^*)^2} e_n(ax)\\
=&1 + \sum_{x\in\mathbb{F}_{p^n}^*} e_n(ax^2) = \sum_{x\in\mathbb{F}_{p^n}} e_n(ax^2) = \eta(a)\sum_{x\in\mathbb{F}_{p^n}} e_n(x^2)\\
=&\eta(a)(-1)^{n-1}g_p^n \qquad \text{(by the Davenport-Hasse theorem [5], [13, §5.2])}\\
=&\eta(a)(-1)^{n-1}i^{\frac{1}{4}(p-1)^2 n}p^{\frac{1}{2}n}.
\end{aligned}$$

(ii) Since $\nu_2(n) = \nu_2((2\alpha, n))$, then $\frac{p^n-1}{p^{(2\alpha,n)}-1}$ is odd. By (11.1),

$$l_n(f) = \begin{cases} (2\alpha, n) & \text{if } a^{\frac{(p^\alpha-1)(p^n-1)}{p^{(2\alpha,n)}-1}} = -1,\\ 0 & \text{otherwise.}\end{cases}$$

We can then use Theorem 10.3,

$$t_n(f) = (-1)^{(\frac{1}{4}(p-1)^2\alpha+1)\frac{n-l_n(f)}{2^{\nu_2(\alpha)+1}}}.$$

If $l_n(f) = (2\alpha, n)$, then $\frac{n-l_n(f)}{2^{\nu_2(\alpha)+1}}$ is even since $\nu_2(n-(2\alpha,n)) > \nu_2(n) = \nu_2(\alpha)+1$. So, $t_n(f) = 1$; hence

$$S(ax^{p^\alpha+1}, n) = g_p^{n-l_n(f)}p^{l_n(f)} = i^{\frac{1}{4}(p-1)^2(n-(2\alpha,n))}p^{\frac{1}{2}[n+(2\alpha,n)]} = p^{\frac{1}{2}[n+(2\alpha,n)]}$$

since $\nu_2(n+(2\alpha,n)) \ge 2$. If $l_n(f) = 0$, then $\frac{n-l_n(f)}{2^{\nu_2(\alpha)+1}}$ is odd and $t_n(f) = -(-1)^{\frac{1}{4}(p-1)^2\alpha}$. So,

$$\begin{aligned}
S(ax^{p^\alpha+1}, n) &= -(-1)^{\frac{1}{4}(p-1)^2\alpha}g_p^n = -(-1)^{\frac{1}{4}(p-1)^2\alpha}i^{\frac{1}{4}(p-1)^2 n}p^{\frac{1}{2}n}\\
&= -(-1)^{\frac{1}{4}(p-1)^2(\alpha\frac{n}{2})}p^{\frac{1}{2}n} = -p^{\frac{1}{2}n}
\end{aligned}$$

since $\nu_2(\alpha+\frac{n}{2}) > \nu_2(\alpha) \ge 0$. To summarize, we have

$$S(ax^{p^\alpha+1}, n) = \begin{cases} p^{\frac{1}{2}[n+(2\alpha,n)]} & \text{if } a^{\frac{(p^\alpha-1)(p^n-1)}{p^{(2\alpha,n)}-1}} = -1,\\ -p^{\frac{1}{2}n} & \text{otherwise.}\end{cases}$$

(iii) In this case, $\frac{p^n-1}{p^{(2\alpha,n)}-1}$ is even. By (11.1),

$$l_n(f) = \begin{cases} (2\alpha, n) & \text{if } a^{\frac{(p^\alpha-1)(p^n-1)}{p^{(2\alpha,n)}-1}} = 1,\\ 0 & \text{otherwise.}\end{cases}$$

By Theorem 10.3,

$$t_n(f) = (-1)^{(\frac{1}{4}(p-1)^2\alpha+1)\frac{n-l_n(f)}{2^{\nu_2(\alpha)+1}}}.$$

The conclusion follows the same way as in (ii). □

12. Tables of Numerical Results

Let

$$f(x) = \sum_{i=1}^{k} a_i x^{p^{\alpha_i}+1} \in \mathbb{F}_{p^n}[x], \qquad 0 \le \alpha_1 < \cdots < \alpha_k,$$

where $a_k \in \mathbb{F}_{p^n}^*$ and let $0 < m \equiv 0 \pmod{n}$. Since $\mathrm{Tr}_m(a_k^{-1} f) = a_k^{-1}\mathrm{Tr}_m(f)$, then $l_m(f) = l_m(a_k^{-1} f)$, where $a_k^{-1} f$ is monic. Thus, when we compute $l_m(f)$ with $a_k \in \mathbb{F}_p^*$, we can assume that $a_k = 1$.

We have two tables for $l_m(f)$ in this section. Table 1 gives the values for $l_m(f)$ where $p^n = 3$ and $\alpha \le 4$. Table 2 gives the values for $l_m(f)$ where $p^n = 5$ and $\alpha \le 3$. Both tables were computed using *Mathematica* [15]. In both tables, the first column contains the values for a_i where $0 \le i \le k$ of $f(x)$ as defined above. The next column is the integer s such that $\mathbb{F}_{p^s}$ is the splitting field for $f^*(x)$. The last column lists all the pairs $(m, l_m(f))$ such that $m \mid s$. The values of $l_m(f)$ for arbitrary m's follows from (5.5).

The tables begin on the next page.

TABLE 1. Values of $l_m(f)$ with $p^n = 3$, $\alpha \leq 4$

$a_0, \ldots, a_k$	s	$(m, l_m(f)),\ m \mid s$
1	1	(1,0)
0 1	4	(1,0) (2,0) (4,2)
1 1	6	(1,0) (2,1) (3,0) (6,2)
2 1	3	(1,1) (3,2)
0 0 1	8	(1,0) (2,0) (4,0) (8,4)
1 0 1	12	(1,0) (2,0) (3,0) (4,2) (6,0) (12,4)
2 0 1	6	(1,1) (2,2) (3,2) (6,4)
0 1 1	18	(1,0) (2,1) (3,0) (6,3) (9,0) (18,4)
1 1 1	12	(1,1) (2,1) (3,2) (4,3) (6,2) (12,4)
2 1 1	5	(1,0) (5,4)
0 2 1	9	(1,1) (3,3) (9,4)
1 2 1	12	(1,0) (2,1) (3,0) (4,3) (6,2) (12,4)
2 2 1	10	(1,0) (2,0) (5,0) (10,4)
0 0 0 1	12	(1,0) (2,0) (3,0) (4,2) (6,0) (12,6)
1 0 0 1	18	(1,0) (2,1) (3,0) (6,3) (9,0) (18,6)
2 0 0 1	9	(1,1) (3,3) (9,6)
0 1 0 1	8	(1,0) (2,0) (4,2) (8,6)
1 1 0 1	30	(1,1) (2,1) (3,2) (5,1) (6,2) (10,5) (15,2) (30,6)
2 1 0 1	30	(1,0) (2,1) (3,0) (5,4) (6,2) (10,5) (15,4) (30,6)
0 2 0 1	12	(1,1) (2,2) (3,2) (4,4) (6,4) (12,6)
1 2 0 1	13	(1,0) (13,6)
2 2 0 1	26	(1,0) (2,0) (13,0) (26,6)
0 0 1 1	30	(1,0) (2,1) (3,0) (5,0) (6,2) (10,5) (15,0) (30,6)
1 0 1 1	12	(1,1) (2,1) (3,2) (4,3) (6,2) (12,6)
2 0 1 1	28	(1,0) (2,0) (4,0) (7,0) (14,0) (28,6)
0 1 1 1	24	(1,1) (2,1) (3,2) (4,1) (6,2) (8,5) (12,2) (24,6)
1 1 1 1	36	(1,0) (2,1) (3,0) (4,3) (6,3) (9,0) (12,5) (18,4) (36,6)
2 1 1 1	7	(1,0) (7,6)
0 2 1 1	13	(1,0) (13,6)
1 2 1 1	20	(1,0) (2,0) (4,2) (5,4) (10,4) (20,6)
2 2 1 1	18	(1,1) (2,2) (3,3) (6,5) (9,4) (18,6)
0 0 2 1	15	(1,1) (3,2) (5,5) (15,6)
1 0 2 1	28	(1,0) (2,0) (4,0) (7,0) (14,0) (28,6)
2 0 2 1	12	(1,0) (2,1) (3,0) (4,3) (6,2) (12,6)
0 1 2 1	24	(1,0) (2,1) (3,0) (4,1) (6,2) (8,5) (12,2) (24,6)
1 1 2 1	14	(1,0) (2,0) (7,0) (14,6)
2 1 2 1	36	(1,1) (2,1) (3,3) (4,3) (6,3) (9,4) (12,5) (18,4) (36,6)
0 2 2 1	26	(1,0) (2,0) (13,0) (26,6)
1 2 2 1	18	(1,1) (2,2) (3,2) (6,5) (9,2) (18,6)
2 2 2 1	20	(1,0) (2,0) (4,2) (5,0) (10,4) (20,6)

TABLE 1. Continued

$a_0, \ldots, a_k$	s	$(m, l_m(f)),\ m \mid s$
0 0 0 0 1	16	(1,0) (2,0) (4,0) (8,0) (16,8)
1 0 0 0 1	24	(1,0) (2,0) (3,0) (4,0) (6,0) (8,4) (12,0) (24,8)
2 0 0 0 1	12	(1,1) (2,2) (3,2) (4,4) (6,4) (12,8)
0 1 0 0 1	90	(1,0) (2,1) (3,0) (5,0) (6,3) (9,0) (10,5) (15,0) (18,4) (30,7) (45, 0) (90,8)
1 1 0 0 1	84	(1,1) (2,1) (3,2) (4,1) (6,2) (7,1) (12,2) (14,1) (21,2) (28,7) (42, 2) (84,8)
2 1 0 0 1	52	(1,0) (2,0) (4,2) (13,0) (26,6) (52,8)
0 2 0 0 1	45	(1,1) (3,3) (5,5) (9,4) (15,7) (45,8)
1 2 0 0 1	84	(1,0) (2,1) (3,0) (4,1) (6,2) (7,0) (12,2) (14,1) (21,0) (28,7) (42, 2) (84,8)
2 2 0 0 1	52	(1,0) (2,0) (4,2) (13,6) (26,6) (52,8)
0 0 1 0 1	36	(1,0) (2,0) (3,0) (4,2) (6,0) (9,0) (12,6) (18,0) (36,8)
1 0 1 0 1	24	(1,1) (2,2) (3,2) (4,2) (6,4) (8,6) (12,4) (24,8)
2 0 1 0 1	10	(1,0) (2,0) (5,4) (10,8)
0 1 1 0 1	36	(1,1) (2,1) (3,3) (4,3) (6,3) (9,6) (12,5) (18,6) (36,8)
1 1 1 0 1	41	(1,0) (41,8)
2 1 1 0 1	42	(1,0) (2,1) (3,0) (6,2) (7,6) (14,7) (21,6) (42,8)
0 2 1 0 1	36	(1,0) (2,1) (3,0) (4,3) (6,3) (9,0) (12,5) (18,6) (36,8)
1 2 1 0 1	82	(1,0) (2,0) (41,0) (82,8)
2 2 1 0 1	42	(1,1) (2,1) (3,2) (6,2) (7,1) (14,7) (21,2) (42,8)
0 0 2 0 1	18	(1,1) (2,2) (3,3) (6,6) (9,4) (18,8)
1 0 2 0 1	24	(1,0) (2,0) (3,0) (4,2) (6,0) (8,6) (12,4) (24,8)
2 0 2 0 1	20	(1,0) (2,0) (4,0) (5,0) (10,0) (20,8)
0 1 2 0 1	41	(1,0) (41,8)
1 1 2 0 1	60	(1,0) (2,1) (3,0) (4,3) (5,4) (6,2) (10,5) (12,4) (15,4) (20,7) (30, 6) (60,8)
2 1 2 0 1	78	(1,1) (2,1) (3,2) (6,2) (13,1) (26,7) (39,2) (78,8)
0 2 2 0 1	82	(1,0) (2,0) (41,0) (82,8)
1 2 2 0 1	60	(1,1) (2,1) (3,2) (4,3) (5,1) (6,2) (10,5) (12,4) (15,2) (20,7) (30, 6) (60,8)
2 2 2 0 1	78	(1,0) (2,1) (3,0) (6,2) (13,6) (26,7) (39,6) (78,8)
0 0 0 1 1	42	(1,0) (2,1) (3,0) (6,2) (7,0) (14,7) (21,0) (42,8)
1 0 0 1 1	78	(1,1) (2,1) (3,2) (6,2) (13,1) (26,7) (39,2) (78,8)
2 0 0 1 1	60	(1,0) (2,0) (3,0) (4,2) (5,4) (6,0) (10,4) (12,4) (15,4) (20,6) (30, 4) (60,8)
0 1 0 1 1	39	(1,1) (3,2) (13,7) (39,8)
1 1 0 1 1	72	(1,0) (2,1) (3,0) (4,1) (6,3) (8,5) (9,0) (12,3) (18,4) (24,7) (36, 4) (72,8)
2 1 0 1 1	52	(1,0) (2,0) (4,2) (13,6) (26,6) (52,8)
0 2 0 1 1	80	(1,0) (2,0) (4,0) (5,0) (8,0) (10,0) (16,0) (20,0) (40,0) (80,8)
1 2 0 1 1	30	(1,0) (2,0) (3,0) (5,0) (6,0) (10,4) (15,0) (30,8)
2 2 0 1 1	36	(1,1) (2,2) (3,3) (4,4) (6,5) (9,4) (12,7) (18,6) (36,8)
0 0 1 1 1	12	(1,1) (2,1) (3,2) (4,3) (6,2) (12,8)
1 0 1 1 1	41	(1,0) (41,8)
2 0 1 1 1	78	(1,0) (2,1) (3,0) (6,2) (13,0) (26,7) (39,0) (78,8)
0 1 1 1 1	60	(1,0) (2,1) (3,0) (4,3) (5,0) (6,2) (10,5) (12,4) (15,0) (20,7) (30, 6) (60,8)
1 1 1 1 1	40	(1,0) (2,0) (4,0) (5,4) (8,4) (10,4) (20,4) (40,8)

TABLE 1. Continued

$a_0, \ldots, a_k$	s	$(m, l_m(f)),\ m \mid s$
2 1 1 1 1	9	(1,1) (3,3) (9,8)
0 2 1 1 1	28	(1,0) (2,0) (4,2) (7,0) (14,0) (28,8)
1 2 1 1 1	18	(1,1) (2,2) (3,2) (6,5) (9,2) (18,8)
2 2 1 1 1	80	(1,0) (2,0) (4,0) (5,0) (8,0) (10,0) (16,0) (20,0) (40,0) (80,8)
0 0 2 1 1	41	(1,0) (41,8)
1 0 2 1 1	36	(1,0) (2,1) (3,0) (4,3) (6,3) (9,0) (12,7) (18,4) (36,8)
2 0 2 1 1	90	(1,1) (2,1) (3,3) (5,1) (6,3) (9,4) (10,5) (15,3) (18,4) (30,7) (45, 4) (90,8)
0 1 2 1 1	82	(1,0) (2,0) (41,0) (82,8)
1 1 2 1 1	24	(1,1) (2,1) (3,2) (4,3) (6,2) (8,7) (12,4) (24,8)
2 1 2 1 1	84	(1,0) (2,1) (3,0) (4,1) (6,2) (7,0) (12,2) (14,1) (21,0) (28,7) (42, 2) (84,8)
0 2 2 1 1	30	(1,1) (2,2) (3,2) (5,5) (6,4) (10,6) (15,6) (30,8)
1 2 2 1 1	28	(1,0) (2,0) (4,2) (7,6) (14,6) (28,8)
2 2 2 1 1	40	(1,0) (2,0) (4,0) (5,0) (8,0) (10,0) (20,0) (40,8)
0 0 0 2 1	21	(1,1) (3,2) (7,7) (21,8)
1 0 0 2 1	78	(1,0) (2,1) (3,0) (6,2) (13,6) (26,7) (39,6) (78,8)
2 0 0 2 1	60	(1,0) (2,0) (3,0) (4,2) (5,0) (6,0) (10,4) (12,4) (15,0) (20,6) (30, 4) (60,8)
0 1 0 2 1	80	(1,0) (2,0) (4,0) (5,0) (8,0) (10,0) (16,0) (20,0) (40,0) (80,8)
1 1 0 2 1	15	(1,0) (3,0) (5,4) (15,8)
2 1 0 2 1	36	(1,1) (2,2) (3,2) (4,4) (6,5) (9,2) (12,7) (18,6) (36,8)
0 2 0 2 1	78	(1,0) (2,1) (3,0) (6,2) (13,0) (26,7) (39,0) (78,8)
1 2 0 2 1	72	(1,1) (2,1) (3,3) (4,1) (6,3) (8,5) (9,4) (12,3) (18,4) (24,7) (36, 4) (72,8)
2 2 0 2 1	52	(1,0) (2,0) (4,2) (13,0) (26,6) (52,8)
0 0 1 2 1	12	(1,0) (2,1) (3,0) (4,3) (6,2) (12,8)
1 0 1 2 1	82	(1,0) (2,0) (41,0) (82,8)
2 0 1 2 1	39	(1,1) (3,2) (13,7) (39,8)
0 1 1 2 1	28	(1,0) (2,0) (4,2) (7,0) (14,0) (28,8)
1 1 1 2 1	18	(1,1) (2,2) (3,3) (6,5) (9,6) (18,8)
2 1 1 2 1	80	(1,0) (2,0) (4,0) (5,0) (8,0) (10,0) (16,0) (20,0) (40,0) (80,8)
0 2 1 2 1	60	(1,1) (2,1) (3,2) (4,3) (5,5) (6,2) (10,5) (12,4) (15,6) (20,7) (30, 6) (60,8)
1 2 1 2 1	40	(1,0) (2,0) (4,0) (5,0) (8,4) (10,4) (20,4) (40,8)
2 2 1 2 1	18	(1,0) (2,1) (3,0) (6,3) (9,0) (18,8)
0 0 2 2 1	82	(1,0) (2,0) (41,0) (82,8)
1 0 2 2 1	36	(1,1) (2,1) (3,3) (4,3) (6,3) (9,4) (12,7) (18,4) (36,8)
2 0 2 2 1	90	(1,0) (2,1) (3,0) (5,4) (6,3) (9,0) (10,5) (15,4) (18,4) (30,7) (45, 4) (90,8)
0 1 2 2 1	30	(1,1) (2,2) (3,2) (5,1) (6,4) (10,6) (15,2) (30,8)
1 1 2 2 1	28	(1,0) (2,0) (4,2) (7,0) (14,6) (28,8)
2 1 2 2 1	40	(1,0) (2,0) (4,0) (5,0) (8,0) (10,0) (20,0) (40,8)
0 2 2 2 1	41	(1,0) (41,8)
1 2 2 2 1	24	(1,0) (2,1) (3,0) (4,3) (6,2) (8,7) (12,4) (24,8)
2 2 2 2 1	84	(1,1) (2,1) (3,2) (4,1) (6,2) (7,1) (12,2) (14,1) (21,2) (28,7) (42, 2) (84,8)

TABLE 2. Values of $l_m(f)$ with $p^n = 5$, $\alpha \leq 3$

$a_0, \ldots, a_k$	s	$(m, l_m(f)),\ m \mid s$
1	1	(1,0)
0 1	4	(1,0) (2,0) (4,2)
1 1	10	(1,0) (2,1) (5,0) (10,2)
2 1	6	(1,0) (2,0) (3,0) (6,2)
3 1	3	(1,0) (3,2)
4 1	5	(1,1) (5,2)
0 0 1	8	(1,0) (2,0) (4,0) (8,4)
1 0 1	20	(1,0) (2,0) (4,2) (5,0) (10,0) (20,4)
2 0 1	12	(1,0) (2,0) (3,0) (4,0) (6,0) (12,4)
3 0 1	6	(1,0) (2,0) (3,2) (6,4)
4 0 1	10	(1,1) (2,2) (5,2) (10,4)
0 1 1	30	(1,0) (2,1) (3,0) (5,0) (6,3) (10,2) (15,0) (30,4)
1 1 1	12	(1,0) (2,0) (3,2) (4,2) (6,2) (12,4)
2 1 1	13	(1,0) (13,4)
3 1 1	5	(1,1) (5,4)
4 1 1	24	(1,0) (2,0) (3,0) (4,0) (6,0) (8,0) (12,0) (24,4)
0 2 1	26	(1,0) (2,0) (13,0) (26,4)
1 2 1	20	(1,0) (2,1) (4,3) (5,0) (10,2) (20,4)
2 2 1	30	(1,1) (2,1) (3,1) (5,2) (6,3) (10,2) (15,2) (30,4)
3 2 1	13	(1,0) (13,4)
4 2 1	15	(1,0) (3,2) (5,0) (15,4)
0 3 1	13	(1,0) (13,4)
1 3 1	20	(1,1) (2,1) (4,3) (5,2) (10,2) (20,4)
2 3 1	30	(1,0) (2,1) (3,2) (5,0) (6,3) (10,2) (15,2) (30,4)
3 3 1	26	(1,0) (2,0) (13,0) (26,4)
4 3 1	30	(1,0) (2,0) (3,0) (5,0) (6,2) (10,0) (15,0) (30,4)
0 4 1	15	(1,1) (3,3) (5,2) (15,4)
1 4 1	12	(1,0) (2,0) (3,0) (4,2) (6,2) (12,4)
2 4 1	26	(1,0) (2,0) (13,0) (26,4)
3 4 1	10	(1,0) (2,1) (5,0) (10,4)
4 4 1	24	(1,0) (2,0) (3,0) (4,0) (6,0) (8,0) (12,0) (24,4)
0 0 0 1	12	(1,0) (2,0) (3,0) (4,2) (6,0) (12,6)
1 0 0 1	30	(1,0) (2,1) (3,0) (5,0) (6,3) (10,2) (15,0) (30,6)
2 0 0 1	18	(1,0) (2,0) (3,0) (6,0) (9,0) (18,6)
3 0 0 1	9	(1,0) (3,0) (9,6)
4 0 0 1	15	(1,1) (3,3) (5,2) (15,6)
0 1 0 1	8	(1,0) (2,0) (4,2) (8,6)
1 1 0 1	126	(1,0) (2,0) (3,0) (6,0) (7,0) (9,0) (14,0) (18,0) (21,0) (42,0) (63, 0) (126,6)
2 1 0 1	30	(1,0) (2,1) (3,2) (5,0) (6,3) (10,4) (15,2) (30,6)
3 1 0 1	30	(1,1) (2,1) (3,1) (5,4) (6,3) (10,4) (15,4) (30,6)
4 1 0 1	63	(1,0) (3,0) (7,0) (9,0) (21,0) (63,6)
0 2 0 1	12	(1,0) (2,0) (3,2) (4,2) (6,4) (12,6)

TABLE 2. Continued

$a_0, \ldots, a_k$	s	$(m, l_m(f)),\ m \mid s$
1 2 0 1	21	(1,0) (3,0) (7,0) (21,6)
2 2 0 1	130	(1,1) (2,1) (5,2) (10,2) (13,1) (26,5) (65,2) (130,6)
3 2 0 1	130	(1,0) (2,1) (5,0) (10,2) (13,4) (26,5) (65,4) (130,6)
4 2 0 1	42	(1,0) (2,0) (3,0) (6,0) (7,0) (14,0) (21,0) (42,6)
0 3 0 1	20	(1,0) (2,0) (4,2) (5,0) (10,0) (20,6)
1 3 0 1	65	(1,1) (5,2) (13,5) (65,6)
2 3 0 1	24	(1,0) (2,0) (3,0) (4,0) (6,2) (8,0) (12,2) (24,6)
3 3 0 1	24	(1,0) (2,0) (3,2) (4,0) (6,2) (8,0) (12,2) (24,6)
4 3 0 1	130	(1,0) (2,1) (5,0) (10,2) (13,0) (26,5) (65,0) (130,6)
0 4 0 1	20	(1,1) (2,2) (4,4) (5,2) (10,4) (20,6)
1 4 0 1	78	(1,0) (2,0) (3,2) (6,2) (13,0) (26,4) (39,2) (78,6)
2 4 0 1	62	(1,0) (2,0) (31,0) (62,6)
3 4 0 1	31	(1,0) (31,6)
4 4 0 1	78	(1,0) (2,0) (3,0) (6,2) (13,4) (26,4) (39,4) (78,6)
0 0 1 1	50	(1,0) (2,1) (5,0) (10,5) (25,0) (50,6)
1 0 1 1	52	(1,0) (2,0) (4,2) (13,4) (26,4) (52,6)
2 0 1 1	12	(1,0) (2,0) (3,2) (4,0) (6,2) (12,6)
3 0 1 1	65	(1,1) (5,2) (13,5) (65,6)
4 0 1 1	78	(1,0) (2,0) (3,0) (6,2) (13,4) (26,4) (39,4) (78,6)
0 1 1 1	24	(1,0) (2,0) (3,2) (4,0) (6,2) (8,4) (12,2) (24,6)
1 1 1 1	60	(1,0) (2,1) (3,0) (4,3) (5,0) (6,3) (10,2) (12,5) (15,0) (20,4) (30, 4) (60,6)
2 1 1 1	130	(1,1) (2,1) (5,2) (10,2) (13,1) (26,5) (65,2) (130,6)
3 1 1 1	7	(1,0) (7,6)
4 1 1 1	62	(1,0) (2,0) (31,0) (62,6)
0 2 1 1	63	(1,0) (3,0) (7,0) (9,0) (21,0) (63,6)
1 2 1 1	20	(1,1) (2,1) (4,3) (5,4) (10,4) (20,6)
2 2 1 1	120	(1,0) (2,1) (3,0) (4,1) (5,0) (6,1) (8,1) (10,2) (12,1) (15,0) (20, 2) (24,5) (30,2) (40,2) (60,2) (120,6)
3 2 1 1	30	(1,0) (2,0) (3,2) (5,0) (6,4) (10,0) (15,4) (30,6)
4 2 1 1	31	(1,0) (31,6)
0 3 1 1	30	(1,1) (2,1) (3,1) (5,2) (6,3) (10,2) (15,2) (30,6)
1 3 1 1	60	(1,0) (2,0) (3,2) (4,2) (5,0) (6,2) (10,0) (12,4) (15,2) (20,4) (30, 2) (60,6)
2 3 1 1	42	(1,0) (2,0) (3,0) (6,0) (7,0) (14,0) (21,0) (42,6)
3 3 1 1	130	(1,0) (2,1) (5,0) (10,2) (13,0) (26,5) (65,0) (130,6)
4 3 1 1	124	(1,0) (2,0) (4,0) (31,0) (62,0) (124,6)
0 4 1 1	124	(1,0) (2,0) (4,0) (31,0) (62,0) (124,6)
1 4 1 1	24	(1,0) (2,0) (3,0) (4,2) (6,0) (8,2) (12,2) (24,6)
2 4 1 1	78	(1,0) (2,0) (3,0) (6,2) (13,0) (26,4) (39,0) (78,6)
3 4 1 1	124	(1,0) (2,0) (4,0) (31,0) (62,0) (124,6)
4 4 1 1	30	(1,1) (2,2) (3,3) (5,2) (6,4) (10,4) (15,4) (30,6)
0 0 2 1	24	(1,0) (2,0) (3,2) (4,0) (6,2) (8,0) (12,2) (24,6)

TABLE 2. Continued

$a_0, \ldots, a_k$	s	$(m, l_m(f)),\ m \mid s$
1 0 2 1	63	(1,0) (3,0) (7,0) (9,0) (21,0) (63,6)
2 0 2 1	60	(1,1) (2,1) (3,1) (4,3) (5,2) (6,3) (10,2) (12,5) (15,2) (20,4) (30, 4) (60,6)
3 0 2 1	124	(1,0) (2,0) (4,0) (31,0) (62,0) (124,6)
4 0 2 1	60	(1,0) (2,1) (3,0) (4,1) (5,0) (6,1) (10,2) (12,5) (15,0) (20,2) (30, 2) (60,6)
0 1 2 1	40	(1,0) (2,1) (4,1) (5,0) (8,5) (10,2) (20,2) (40,6)
1 1 2 1	120	(1,1) (2,1) (3,1) (4,1) (5,2) (6,1) (8,1) (10,2) (12,1) (15,2) (20, 2) (24,5) (30,2) (40,2) (60,2) (120,6)
2 1 2 1	52	(1,0) (2,0) (4,2) (13,0) (26,4) (52,6)
3 1 2 1	39	(1,0) (3,2) (13,4) (39,6)
4 1 2 1	30	(1,0) (2,0) (3,0) (5,0) (6,2) (10,0) (15,0) (30,6)
0 2 2 1	130	(1,1) (2,1) (5,2) (10,2) (13,1) (26,5) (65,2) (130,6)
1 2 2 1	30	(1,0) (2,1) (3,2) (5,0) (6,5) (10,2) (15,2) (30,6)
2 2 2 1	52	(1,0) (2,0) (4,2) (13,4) (26,4) (52,6)
3 2 2 1	62	(1,0) (2,0) (31,0) (62,6)
4 2 2 1	63	(1,0) (3,0) (7,0) (9,0) (21,0) (63,6)
0 3 2 1	63	(1,0) (3,0) (7,0) (9,0) (21,0) (63,6)
1 3 2 1	126	(1,0) (2,0) (3,0) (6,0) (7,0) (9,0) (14,0) (18,0) (21,0) (42,0) (63, 0) (126,6)
2 3 2 1	20	(1,0) (2,1) (4,3) (5,0) (10,2) (20,6)
3 3 2 1	78	(1,0) (2,0) (3,0) (6,2) (13,4) (26,4) (39,4) (78,6)
4 3 2 1	15	(1,1) (3,3) (5,4) (15,6)
0 4 2 1	78	(1,0) (2,0) (3,0) (6,2) (13,0) (26,4) (39,0) (78,6)
1 4 2 1	62	(1,0) (2,0) (31,0) (62,6)
2 4 2 1	60	(1,0) (2,0) (3,2) (4,2) (5,0) (6,2) (10,0) (12,4) (15,4) (20,2) (30, 4) (60,6)
3 4 2 1	10	(1,1) (2,2) (5,2) (10,6)
4 4 2 1	124	(1,0) (2,0) (4,0) (31,0) (62,0) (124,6)
0 0 3 1	24	(1,0) (2,0) (3,0) (4,0) (6,2) (8,0) (12,2) (24,6)
1 0 3 1	60	(1,1) (2,1) (3,1) (4,1) (5,2) (6,1) (10,2) (12,5) (15,2) (20,2) (30, 2) (60,6)
2 0 3 1	124	(1,0) (2,0) (4,0) (31,0) (62,0) (124,6)
3 0 3 1	60	(1,0) (2,1) (3,2) (4,3) (5,0) (6,3) (10,2) (12,5) (15,2) (20,4) (30, 4) (60,6)
4 0 3 1	126	(1,0) (2,0) (3,0) (6,0) (7,0) (9,0) (14,0) (18,0) (21,0) (42,0) (63, 0) (126,6)
0 1 3 1	40	(1,1) (2,1) (4,1) (5,2) (8,5) (10,2) (20,2) (40,6)
1 1 3 1	15	(1,0) (3,2) (5,0) (15,6)
2 1 3 1	78	(1,0) (2,0) (3,0) (6,2) (13,0) (26,4) (39,0) (78,6)
3 1 3 1	52	(1,0) (2,0) (4,2) (13,4) (26,4) (52,6)
4 1 3 1	120	(1,0) (2,1) (3,0) (4,1) (5,0) (6,1) (8,1) (10,2) (12,1) (15,0) (20, 2) (24,5) (30,2) (40,2) (60,2) (120,6)
0 2 3 1	130	(1,0) (2,1) (5,0) (10,2) (13,4) (26,5) (65,4) (130,6)
1 2 3 1	126	(1,0) (2,0) (3,0) (6,0) (7,0) (9,0) (14,0) (18,0) (21,0) (42,0) (63, 0) (126,6)
2 2 3 1	31	(1,0) (31,6)
3 2 3 1	52	(1,0) (2,0) (4,2) (13,0) (26,4) (52,6)
4 2 3 1	30	(1,1) (2,1) (3,3) (5,2) (6,5) (10,2) (15,4) (30,6)
0 3 3 1	126	(1,0) (2,0) (3,0) (6,0) (7,0) (9,0) (14,0) (18,0) (21,0) (42,0) (63, 0) (126,6)

TABLE 2. Continued

$a_0, \ldots, a_k$	s	$(m, l_m(f)),\ m \mid s$
1 3 3 1	30	(1,0) (2,1) (3,0) (5,0) (6,3) (10,4) (15,0) (30,6)
2 3 3 1	78	(1,0) (2,0) (3,2) (6,2) (13,0) (26,4) (39,2) (78,6)
3 3 3 1	20	(1,1) (2,1) (4,3) (5,2) (10,2) (20,6)
4 3 3 1	63	(1,0) (3,0) (7,0) (9,0) (21,0) (63,6)
0 4 3 1	39	(1,0) (3,2) (13,4) (39,6)
1 4 3 1	124	(1,0) (2,0) (4,0) (31,0) (62,0) (124,6)
2 4 3 1	10	(1,1) (2,2) (5,4) (10,6)
3 4 3 1	60	(1,0) (2,0) (3,0) (4,2) (5,0) (6,2) (10,0) (12,4) (15,0) (20,2) (30, 4) (60,6)
4 4 3 1	31	(1,0) (31,6)
0 0 4 1	25	(1,1) (5,5) (25,6)
1 0 4 1	78	(1,0) (2,0) (3,2) (6,2) (13,0) (26,4) (39,2) (78,6)
2 0 4 1	130	(1,0) (2,1) (5,0) (10,2) (13,0) (26,5) (65,0) (130,6)
3 0 4 1	12	(1,0) (2,0) (3,0) (4,0) (6,2) (12,6)
4 0 4 1	52	(1,0) (2,0) (4,2) (13,0) (26,4) (52,6)
0 1 4 1	24	(1,0) (2,0) (3,0) (4,0) (6,2) (8,4) (12,2) (24,6)
1 1 4 1	31	(1,0) (31,6)
2 1 4 1	14	(1,0) (2,0) (7,0) (14,6)
3 1 4 1	130	(1,0) (2,1) (5,0) (10,2) (13,4) (26,5) (65,4) (130,6)
4 1 4 1	60	(1,1) (2,1) (3,3) (4,3) (5,2) (6,3) (10,2) (12,5) (15,4) (20,4) (30, 4) (60,6)
0 2 4 1	126	(1,0) (2,0) (3,0) (6,0) (7,0) (9,0) (14,0) (18,0) (21,0) (42,0) (63, 0) (126,6)
1 2 4 1	62	(1,0) (2,0) (31,0) (62,6)
2 2 4 1	30	(1,0) (2,0) (3,2) (5,0) (6,4) (10,0) (15,2) (30,6)
3 2 4 1	120	(1,1) (2,1) (3,1) (4,1) (5,2) (6,1) (8,1) (10,2) (12,1) (15,2) (20, 2) (24,5) (30,2) (40,2) (60,2) (120,6)
4 2 4 1	20	(1,0) (2,1) (4,3) (5,0) (10,4) (20,6)
0 3 4 1	30	(1,0) (2,1) (3,2) (5,0) (6,3) (10,2) (15,4) (30,6)
1 3 4 1	124	(1,0) (2,0) (4,0) (31,0) (62,0) (124,6)
2 3 4 1	65	(1,1) (5,2) (13,5) (65,6)
3 3 4 1	21	(1,0) (3,0) (7,0) (21,6)
4 3 4 1	60	(1,0) (2,0) (3,0) (4,2) (5,0) (6,2) (10,0) (12,4) (15,0) (20,4) (30, 2) (60,6)
0 4 4 1	124	(1,0) (2,0) (4,0) (31,0) (62,0) (124,6)
1 4 4 1	30	(1,1) (2,2) (3,1) (5,2) (6,4) (10,4) (15,2) (30,6)
2 4 4 1	124	(1,0) (2,0) (4,0) (31,0) (62,0) (124,6)
3 4 4 1	39	(1,0) (3,2) (13,4) (39,6)
4 4 4 1	24	(1,0) (2,0) (3,0) (4,2) (6,0) (8,2) (12,2) (24,6)

References

[1] C. Arf, *Untersuchungen über quadratische Formen in Körpern der Charakteristik* 2, J. Reine Angew. Math. **183** (1941), 148 – 167.

[2] L. Baumert and R. McEliece, *Weights of irreducible cyclic codes*, Inform. Control **20** (1972), 158 – 175.

[3] L. Carlitz, *Explicit evaluation of certain exponential sums*, Math. Scand. **44** (1979), 5 – 16.

[4] L. Carlitz, *Evaluation of some exponential sums over a finite field*, Math. Nachr. **96** (1980), 319 – 339.

[5] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1935), 151 – 182.

[6] L. E. Dickson, *Linear Groups*, Dover, New York, 1958.

[7] T. Helleseth, *Some results about the cross-correlation function between two maximal linear sequences*, Discrete Math. **16** (1976), 209 – 232.

[8] X. Hou, *Explicit evaluation of certain exponential sums of binary quadratic functions*, preprint.

[9] X. Hou, *Lectures on Finite Fields*, preprint.

[10] T. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.

[11] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York, 1982.

[12] S. Lang, *Algebra*, Addison-Wesley, Reading, MA, 1993.

[13] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[14] E. Lucas, *Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. France **6** (1877 – 1878), 49 – 54.

[15] Wolfram Research, Inc., Mathematica, Version 5.1, Champaign, IL, 2004.