5-29-2009

Certain Diagonal Equations over Finite Fields

Christopher Sze
University of South Florida

Certain Diagonal Equations over Finite Fields

by

Christopher Sze

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Arts
Department of Mathematics and Statistics
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:
May 29, 2009

Keywords: irreducible polynomial, Gaussian sum, planar function, Hasse-Weil bound, elliptic curve

Dedication

To the memory of my mother

Virginia Sze

Table of Contents

Certain Diagonal Equations over Finite Fields

Christopher Sze

Abstract

Let $\mathbb{F}_{q^t}$ be the finite field with q^t elements and let $\mathbb{F}_{q^t}^*$ be its multiplicative group. We study the diagonal equation $ax^{q-1} + by^{q-1} = c$ where $a, b, c \in \mathbb{F}_{q^t}^*$. This equation can be written as $x^{q-1} + \alpha y^{q-1} = \beta$, where $\alpha, \beta \in \mathbb{F}_{q^t}^*$. Let $N_t(\alpha, \beta)$ denote the number of solutions $(x, y) \in \mathbb{F}_{q^t}^* \times \mathbb{F}_{q^t}^*$ of $x^{q-1} + \alpha y^{q-1} = \beta$ and $I(r; a, b)$ be the number of monic irreducible polynomials $f \in \mathbb{F}_q[x]$ of degree r with $f(0) = a$ and $f(1) = b$. We show that $N_t(\alpha, \beta)$ can be expressed in terms of $I(r; a, b)$, where $r \mid t$ and $a, b \in \mathbb{F}_q^*$ are related to α and β. A recursive formula for $I(r; a, b)$ will be given and we illustrate this by computing $I(r; a, b)$ for $2 \leq r \leq 4$. We also show that $N_3(\alpha, \beta)$ can be expressed in terms of the number of monic irreducible cubic polynomials over $\mathbb{F}_q$ with prescribed trace and norm. Consequently, $N_3(\alpha, \beta)$ can be expressed in terms of the number of rational points on a certain elliptic curve. We give a proof that given any $a, b \in \mathbb{F}_q^*$ and integer $r \geq 3$, there always exists a monic irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree r such that $f(0) = a$ and $f(1) = b$. We also use the result on $N_2(\alpha, \beta)$ to construct a new family of planar functions.

1 Introduction

Let $\mathbb{F}_q$ be the finite field with q elements and let t be a positive integer. The multiplicative group of $\mathbb{F}_{q^t}$ is denoted by $\mathbb{F}_{q^t}^*$. The purpose of this thesis is to study the number of solutions $(x, y) \in \mathbb{F}_{q^t}^* \times \mathbb{F}_{q^t}^*$ of the equation

$$ax^{q-1} + by^{q-1} = c, \tag{1.1}$$

where $a, b, c \in \mathbb{F}_{q^t}^*$. Equation (1.1) is equivalent to

$$x^{q-1} + \alpha y^{q-1} = \beta, \tag{1.2}$$

where $\alpha = \frac{b}{a}$, $\beta = \frac{c}{a} \in \mathbb{F}_{q^t}^*$. Let $N_t(\alpha, \beta)$ denote the number of solutions $(x, y) \in \mathbb{F}_{q^t}^* \times \mathbb{F}_{q^t}^*$ of (1.2). The number $N_t(\alpha, \beta)$ is related to the number of rational points on the projective Fermat curve

$$\mathcal{C} : \qquad x^{q-1} + \alpha y^{q-1} - \beta z^{q-1} = 0 \tag{1.3}$$

over $\mathbb{F}_{q^t}$. The number of rational points on C is given by

$$|\mathcal{C}(\mathbb{F}_{q^t})| = N_t(\alpha, \beta) + k(q - 1), \tag{1.4}$$

where k is the number of elements in the multiset $\{-\alpha, \beta, \beta/\alpha\}$ which are $(q-1)$st powers in $\mathbb{F}_{q^t}$. Equation (1.4) was stated in [23].

Equation (1.2) is a special diagonal equation. In general, the number of solutions of a diagonal equation can be expressed in terms of Gaussian sums and estimates for the number of solutions can be obtained thereafter. However, the exact number of solutions of a diagonal equation is not known except in some special cases. Wolfmann [29] determined the number of solutions of

$$a_1x_1^d + \cdots + a_sx_s^d = b$$

over $\mathbb{F}_{p^{2m}}$ where d is a "special" divisor of $p^{2m}-1$, meaning that $d \mid p^r+1$ for some $r \mid m$. Assume $q^t = p^{2m}$ (i.e., $t \mid 2m$ and $q = p^{\frac{2m}{t}}$). Then

$$(p^r+1, q-1) = \begin{cases} p^{(r,\frac{2m}{t})}+1 & \text{if } \nu_2\Big(\dfrac{2m}{t}\Big) > \nu_2(r), \\ 2 & \text{if } \nu_2\Big(\dfrac{2m}{t}\Big) \le \nu_2(r) \text{ and } p > 2, \\ 1 & \text{if } \nu_2\Big(\dfrac{2m}{t}\Big) \le \nu_2(r) \text{ and } p = 2, \end{cases}$$

where ν_2 is the 2-adic order; see [5, Lemma 2.6] and [17, Lemma 5.3]. Thus, $q-1$ is not a special divisor of $p^{2m}-1$ except when $q = 2, 2^2$ or 3. Hence, in general, equation (1.2) is not covered the result of [29].

The focus of this thesis is the number $N_t(\alpha,\beta)$. Let $I(r;a,b)$ denote the number of monic irreducible polynomials $f \in \mathbb{F}_q[x]$ of degree r such that $f(0) = a$ and $f(1) = b$. We shall see that $N_t(\alpha,\beta)$ can be expressed in terms of $I(r;a,b)$ where $r \mid t$ and $a,b \in \mathbb{F}_q^*$ are related to α and β. This reduces our problem to finding $I(r;a,b)$. The problem of counting (monic) irreducible polynomials with prescribed values resembles that of counting (monic) irreducible polynomials with prescribed coefficients; the latter is a well studied topic in finite fields, see for example [4, 12, 13, 25, 28, 30], but the former, to our knowledge, has not attracted much attention. Here arises a natural question: Is $I(r;a,b)$ always positive? Namely, given $r > 0$ and $a,b \in \mathbb{F}_q^*$, does there always exist a monic irreducible polynomial $f \in \mathbb{F}_q[x]$ such that $f(0) = a$ and $f(1) = b$? The answer is obviously negative for $r = 1,2$, and is obviously positive for $r = 3$. We are able to prove that $I(r;a,b) > 0$ for all $r \ge 4$ and $a,b \in \mathbb{F}_q^*$.

In Chapter 2 we will present preliminary results on Gaussian sums and Möbius

Inversion; these are the basic tools of our investigation. In Chapter 3 we look at the diagonal equations in general and give the number of solutions in terms of Gaussian sums. In Chapter 4, we consider our main problem, and we shall express $N_t(\alpha, \beta)$ in terms of $I(r; a, b)$. We will give a recursive formula for $I(r; a, b)$ and computations of $I(r; a, b)$ for small values of r in Chapter 5. In Chapter 6, we will derive another formula for $N_3(\alpha, \beta)$ using a different perspective. This new formula allows us to relate $N_3(\alpha, \beta)$ to the number of irreducible cubics over $\mathbb{F}_q$ with prescribed trace and norm and further allows us to relate $N_3(\alpha, \beta)$ to a certain elliptic curve. In Chapter 7, we give a proof that asserts the positivity of $I(r; a, b)$, for $t \geq 3$. In the last chapter we will discuss some application to planar functions which are also known as perfect linear functions. We will use the result on $N_2(\alpha, \beta)$ to construct a new family of planar functions.

2 Preliminary Results

2.1 Characters

Let G be a finite abelian group written multiplicatively. A *character* of G is a map χ from G into the multiplicative group of complex numbers of absolute value 1 such that

$$\chi(g_1g_2) = \chi(g_1)\chi(g_2) \quad \text{for all } g_1, g_2 \in G.$$

Equivalently, a character of a finite abelian group G is a homomorphism $\chi : G \to \mathbb{C}^*$. If 1_G is the identity element in G, then $\chi(1_G) = 1$. If $g \in G$, then $\chi(g)$ is a $|G|$th root of unity and $\chi(g^{-1}) = (\chi(g))^{-1} = \overline{\chi(g)}$, where the bar denotes complex conjugation.

For any finite abelian group G, we have the *trivial* character χ_0 defined by $\chi_0(g) = 1$ for all $g \in G$. For each character χ of G, there is associated the *conjugate character* $\overline{\chi}$ defined by $\overline{\chi}(g) = \overline{\chi(g)}$ for all $g \in G$. Given the characters $\chi_1, \ldots, \chi_n$, we define the product $\chi_1 \cdots \chi_n$ by $(\chi_1 \cdots \chi_n)(g) = \chi_1(g) \cdots \chi_n(g)$. The set $G^\wedge$ of characters of G forms an abelian group under multiplication of characters and $|G| = |G^\wedge|$. In fact, $G \cong G^\wedge$ although the isomoprhism is not canonical.

Let $\mathbb{F}_q$ be the finite field with q elements. Then $\mathbb{F}_q$ and $\mathbb{F}_q^*$ are finite abelian groups under addition and multiplication, respectively. Consider first the additive group of $\mathbb{F}_q$. Let $q = p^n$, where p is a prime. Let $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p$ be the absolute trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. Then the *canonical additive character* of $\mathbb{F}_q$, denoted by χ_1, is given by

$$\chi_1(c) = e^{2\pi i \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(c)/p} \qquad \text{for all } c \in \mathbb{F}_q. \tag{2.1}$$

For each $b \in \mathbb{F}_q$, the function χ_b defined by

$$\chi_b(c) = \chi_1(bc) \qquad \text{for all } c \in \mathbb{F}_q$$

is also an additive character of $\mathbb{F}_q$ and all additive characters of $\mathbb{F}_q$ are found in this manner. Now, let us consider the multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$. The characters of $\mathbb{F}_q^*$ are called the *multiplicative characters* of $\mathbb{F}_q$. Let g be a fixed primitive element of $\mathbb{F}_q$. Then for each $j = 0, 1, \ldots, q-2$, the function ψ_j defined by

$$\psi_j(g^k) = e^{2\pi ijk/(q-1)} \qquad \text{for } k = 0, 1, \ldots, q-2$$

is a multiplicative character of $\mathbb{F}_q$ and all multiplicative characters of $\mathbb{F}_q$ are obtained in this way. Furthermore, the set of all multiplicative characters of $\mathbb{F}_q$ forms a cyclic group of order $q-1$.

Let q be odd and η be the function on $\mathbb{F}_q^*$ defined by

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

Then η is a multiplicative character of $\mathbb{F}_q$ called the *quadratic character* of $\mathbb{F}_q$. For convenience, we define $\eta(0) = 0$.

We have the following identities involving the additive and multiplicative characters of $\mathbb{F}_q$. If χ_a and χ_b are additive characters of $\mathbb{F}_q$ we have

$$\sum_{c \in \mathbb{F}_q} \chi_a(c)\overline{\chi_b(c)} = \begin{cases} 0 & \text{if } a \neq b, \\ q & \text{if } a = b. \end{cases}$$

In particular,

$$\sum_{c \in \mathbb{F}_q} \chi_a(c) = 0 \qquad \text{for } a \neq 0.$$

Moreover, if $c, d \in \mathbb{F}_q$ then

$$\sum_{b \in \mathbb{F}_q} \chi_b(c)\overline{\chi_b(d)} = \begin{cases} 0 & \text{if } c \neq d, \\ q & \text{if } c = d. \end{cases} \tag{2.2}$$

For multiplicative characters ψ and τ of $\mathbb{F}_q$ we have

$$\sum_{c \in \mathbb{F}_q^*} \psi(c)\overline{\tau(c)} = \begin{cases} 0 & \text{if } \psi \neq \tau, \\ q-1 & \text{if } \psi = \tau. \end{cases}$$

In particular,

$$\sum_{c \in \mathbb{F}_q^*} \psi(c) = 0 \qquad \text{for } \psi \neq \psi_0. \tag{2.3}$$

Furthermore, if $c, d \in \mathbb{F}_q^*$ then

$$\sum_{\psi} \psi(c)\overline{\psi(d)} = \begin{cases} 0 & \text{if } c \neq d, \\ q-1 & \text{if } c = d, \end{cases} \tag{2.4}$$

where the sum is over all multiplicative characters ψ of $\mathbb{F}_q$.

Characters are used to find expressions for the number of solutions of equations in a finite abelian group G. Let $f(x_1, \dots, x_n) = b$ be an equation in n indeterminates over G. Let $N(b)$ be the number of $(x_1, \dots, x_n) \in G^n$ such that $f(x_1, \dots, x_n) = b$. Then

$$N(b) = \frac{1}{|G|} \sum_{x_1 \in G} \cdots \sum_{x_n \in G} \sum_{\chi \in G^\wedge} \chi(f(x_1, \dots, x_n))\overline{\chi(b)}. \tag{2.5}$$

2.2 Gaussian Sums

Let ψ be a multiplicative and χ be an additive character of $\mathbb{F}_q$. The *Gaussian sum* $G(\psi, \chi)$ is defined by

$$G(\psi, \chi) = \sum_{c \in \mathbb{F}_q^*} \psi(c)\chi(c).$$

Let χ_0 and ψ_0 be the trivial additive and multiplicative characters of $\mathbb{F}_q$ respectively. The Gaussian sum $G(\psi, \chi)$ satisfies

$$G(\psi, \chi) = \begin{cases} q-1 & \text{if } \psi = \psi_0, \chi = \chi_0, \\ -1 & \text{if } \psi = \psi_0, \chi \neq \chi_0, \\ 0 & \text{if } \psi \neq \psi_0, \chi = \chi_0, \end{cases} \tag{2.6}$$

and

$$|G(\psi, \chi)| = q^{1/2} \qquad \text{if } \psi \neq \psi_0, \chi \neq \chi_0. \tag{2.7}$$

The Gaussian sums for the finite field $\mathbb{F}_q$ also have the following properties:

(i) $G(\psi, \chi_{ab}) = \overline{\psi(a)} G(\psi, \chi_b)$ for $a \in \mathbb{F}_q^*, b \in \mathbb{F}_q$;

(ii) $G(\psi, \overline{\chi}) = \psi(-1) G(\psi, \chi)$;

(iii) $G(\overline{\psi}, \chi) = \psi(-1) \overline{G(\psi, \chi)}$;

(iv) $G(\psi, \chi) G(\overline{\psi}, \chi) = \psi(-1) q$ for $\psi \neq \psi_0$ and $\chi \neq \chi_0$;

(v) $G(\psi^p, \chi_b) = G(\psi, \chi_{\sigma(b)})$ for $b \in \mathbb{F}_q$, where p is the characteristic of $\mathbb{F}_q$ and $\sigma(b) = b^p$.

Let ψ be a multiplicative character of $\mathbb{F}_q$. By (2.2) we have, for any $c \in \mathbb{F}_q^*$

$$\begin{aligned} \psi(c) &= \frac{1}{q} \sum_{d \in \mathbb{F}_q^*} \psi(d) \sum_{b \in \mathbb{F}_q} \chi_b(c) \overline{\chi_b(d)} \\ &= \frac{1}{q} \sum_{b \in \mathbb{F}_q} \chi_b(c) \sum_{d \in \mathbb{F}_q^*} \psi(d) \overline{\chi_b}(d) \\ &= \frac{1}{q} \sum_{\chi} G(\psi, \overline{\chi}) \chi(c), \end{aligned}$$

where the last sum is extended over all additive characters χ of $\mathbb{F}_q$. Similarly, if χ is an additive character of $\mathbb{F}_q$, then by (2.4), we get, for any $c \in \mathbb{F}_q^*$

$$\begin{aligned}
\chi(c) &= \frac{1}{q-1} \sum_{d \in \mathbb{F}_q^*} \chi(d) \sum_{\psi} \psi(c)\overline{\psi(d)} \\
&= \frac{1}{q-1} \sum_{\psi} \psi(c) \sum_{d \in \mathbb{F}_q^*} \overline{\psi}(d)\chi(d) \\
&= \frac{1}{q-1} \sum_{\psi} G(\overline{\psi}, \chi)\psi(c),
\end{aligned} \tag{2.8}$$

where the sum is extended over all multiplicative characters ψ of $\mathbb{F}_q$.

2.3 Möbius Inversion

A *partially ordered set* $(S, \leq)$ is an ordered pair consisting of a set S and a binary relation $\leq$ on S that is reflexive, transitive and anti-symmetric. An *interval* of a partially ordered set $(S, \leq)$ is given by $[x, y] = \{z \in S : x \leq z \leq y\}$. We say that a partially ordered set is *locally finite* if every interval has a finite number of elements.

Let $(S, \leq)$ be a locally finite partially ordered set. The *Möbius function* of $(S, \leq)$ is an integer valued function of two variables on S defined by

$$\mu(x, y) = 0 \qquad \text{if } x \not\leq y,$$

and by

$$\sum_{z \in [x,y]} \mu(x, z) = \delta(x, y) \qquad \text{if } x \leq y,$$

where δ is the Kronecker delta function.

Theorem 2.1 (Möbius Inversion Formula [1])**.** *Let $(S, \leq)$ be a locally finite partially ordered set with Möbius function μ. Let A be an abelian group and $N_= : S \to A$ be a function. Let $l, m \in S$ be fixed and for $x \in S$ define*

$$N_{\geq}(x) = \sum_{y \in [x,m]} N_=(y)$$

and

$$N_{\leq}(x) = \sum_{y \in [l,x]} N_{=}(y).$$

Then

$$N_{=}(x) = \sum_{y \in [x,m]} \mu(x,y) N_{\geq}(y) \quad \textit{for all } x \in S \textit{ with } x \leq m$$

and

$$N_{=}(x) = \sum_{y \in [l,x]} \mu(y,x) N_{\leq}(y) \quad \textit{for all } x \in S \textit{ with } x \geq l.$$

Example 2.2. [*Classical Möbius function*] Let $\mathbb{Z}^+$ be the set of all positive integers. Then $(\mathbb{Z}^+, |)$ is a locally finite partially ordered set, where $x \mid y$ means x divides y. The Möbius function is given by

$$\mu(x,y) = \mu\left(\frac{y}{x}\right) = \begin{cases} 1 & \text{if } \dfrac{y}{x} = 1, \\ (-1)^k & \text{if } \dfrac{y}{x} \text{ is a product of } k \text{ distinct primes,} \\ 0 & \text{if } \dfrac{y}{x} \text{ is divisible by a square of a prime.} \end{cases}$$

Example 2.3. [*Partitions of a set* [1]] Let S_n be a finite set consisting of n elements. Let $\{\pi_1, \pi_2, \ldots\}$ be a partition of S_n into subsets of S_n. The sets π_i are called *blocks* of the partition. Let $\mathcal{P}$ be the set of all partitions of S_n and let $\pi, \sigma \in \mathcal{P}$. We write $\pi \leq \sigma$ to mean that π is a refinement of σ. Then $(\mathcal{P}, \leq)$ is a locally finite partially ordered set. Then the Möbius function is given by

$$\mu(\pi, \sigma) = (-1)^{r(\pi) - r(\sigma)} \prod_{i=1}^{r(\sigma)} (n_i - 1)! \tag{2.9}$$

where $r(\pi)$ denotes the number of blocks of π and the ith block of σ (for some fixed order) is the union of exactly n_i blocks of π.

3 Diagonal Equations

A *diagonal equation* over $\mathbb{F}_q$ is an equation of the form

$$a_1 x_1^{k_1} + \ldots + a_n x_n^{k_n} = b, \tag{3.1}$$

where $k_1, \ldots, k_n$ are positive integers, $a_1, \ldots, a_n \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. In this chapter, we will use Gaussian sums to express the number of solutions of diagonal equations.

Let N be the number of solutions of (3.1) in $\mathbb{F}_q^n$. By (2.5) we have

$$N = \frac{1}{q} \sum_{c_1,\ldots,c_n \in \mathbb{F}_q} \sum_{\chi} \chi(a_1 c_1^{k_1} + \cdots + a_n c_n^{k_n}) \overline{\chi}(b),$$

where χ runs through all the additive character of $\mathbb{F}_q$. Rearranging and separating the trivial character χ_0, we get

$$\begin{aligned} N &= \frac{1}{q} \sum_{s \in \mathbb{F}_q} \overline{\chi_s}(b) \sum_{c_1,\ldots,c_n \in \mathbb{F}_q} \chi_s(a_1 c_1^{k_1}) \cdots \chi_s(a_n c_n^{k_n}) \\ &= \frac{1}{q}(q^n) + \frac{1}{q} \sum_{s \in \mathbb{F}_q^*} \overline{\chi_s}(b) \sum_{c_1,\ldots,c_n \in \mathbb{F}_q} \chi_s(a_1 c_1^{k_1}) \cdots \chi_s(a_n c_n^{k_n}) \\ &= q^{n-1} + \frac{1}{q} \sum_{s \in \mathbb{F}_q^*} \overline{\chi_s}(b) \left(\sum_{c_1 \in \mathbb{F}_q} \chi_{a_1 s}(c_1^{k_1}) \right) \cdots \left(\sum_{c_n \in \mathbb{F}_q} \chi_{a_n s}(c_n^{k_n}) \right). \end{aligned}$$

We look at the sum $\displaystyle\sum_{c_i \in \mathbb{F}_q} \chi_{a_i s}(c_i^{k_i})$. By (2.8),

$$\chi_{a_i s}(c_i^{k_i}) = \frac{1}{q-1} \sum_{\psi} G(\overline{\psi}, \chi_{a_i s}) \psi(c_i^{k_i}),$$

where the sum is over all multiplicative characters ψ of $\mathbb{F}_q$. We have

$$\begin{aligned}\sum_{c_i\in\mathbb{F}_q}\chi_{a_is}(c_i^{k_i}) &= 1+\sum_{c_i\in\mathbb{F}_q^*}\chi_{a_is}(c_i^{k_i})\\ &= 1+\frac{1}{q-1}\sum_{c_i\in\mathbb{F}_q^*}\sum_{\psi}G(\overline{\psi},\chi_{a_is})\psi(c_i^{k_i})\\ &= 1+\frac{1}{q-1}\sum_{\psi}G(\overline{\psi},\chi_{a_is})\sum_{c_i\in\mathbb{F}_q^*}\psi^{k_i}(c_i).\end{aligned}$$

By (2.3),

$$\sum_{c_i\in\mathbb{F}_q^*}\psi^{k_i}(c_i)=\begin{cases}q-1 & \text{if } \psi^{k_i}=\psi_0,\\ 0 & \text{if } \psi^{k_i}\neq\psi_0,\end{cases}$$

where ψ_0 is the trivial multiplicative character of $\mathbb{F}_q$. Now let $d_i=\gcd(k_i,q-1)$. Then ψ^{k_i} is trivial if and only if $o(\psi)\mid d_i$, where $o(\psi)$ is the order of ψ. Let λ_i be a multiplicative character of order d_i. Since $\overline{\lambda_i}$ is of order d_i, then the characters whose order divides d_i are exactly given by $\overline{\lambda_i}^{j_i}$, for $j_i=0,1,\ldots,d_i-1$. Hence,

$$\begin{aligned}\sum_{c_i\in\mathbb{F}_q}\chi_{a_is}(c_i^{k_i}) &= 1+\frac{1}{q-1}\sum_{j_i=0}^{d_i-1}G(\lambda_i^{j_i},\chi_{a_is})\sum_{c_i\in\mathbb{F}_q^*}\overline{\lambda_i}^{j_i}(c_i)\\ &= 1+\sum_{j_i=0}^{d_i-1}G(\lambda_i^{j_i},\chi_{a_is})\end{aligned}$$

Finally, by (2.6) and property (i) of Gaussian sums we get

$$\begin{aligned}\sum_{c_i\in\mathbb{F}_q}\chi_{a_is}(c_i^{k_i}) &= \sum_{j_i=1}^{d_i-1}G(\lambda_i^{j_i},\chi_{a_is})\\ &= \sum_{j_i=1}^{d_i-1}\overline{\lambda_i}^{j_i}(a_i)G(\lambda_i^{j_i},\chi_s)\end{aligned}$$

Therefore,

$$\begin{aligned}
N &= q^{n-1} + \frac{1}{q} \sum_{s \in \mathbb{F}_q^*} \overline{\chi_s}(b) \left(\sum_{j_1=1}^{d_1-1} \overline{\lambda_1}^{j_1}(a_1) G(\lambda_1^{j_1}, \chi_s) \right) \cdots \left(\sum_{j_n=1}^{d_n-1} \overline{\lambda_n}^{j_n}(a_n) G(\lambda_n^{j_n}, \chi_s) \right) \\
&= q^{n-1} + \frac{1}{q} \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} \overline{\lambda_1}^{j_1}(a_1) \ldots \overline{\lambda_n}^{j_n}(a_n) \sum_{s \in \mathbb{F}_q^*} \overline{\chi_s}(b) G(\lambda_1^{j_1}, \chi_s) \ldots G(\lambda_n^{j_n}, \chi_s).
\end{aligned}$$

For the inner sum, we have

$$\begin{aligned}
\sum_{s \in \mathbb{F}_q^*} \overline{\chi_s}(b) G(\lambda_1^{j_1}, \chi_s) \ldots G(\lambda_n^{j_n}, \chi_s) &= G(\lambda_1^{j_1}, \chi_1) \cdots G(\lambda_n^{j_n}, \chi_1) \sum_{s \in \mathbb{F}_q^*} \overline{\chi_b}(a) \overline{\lambda_1}^{j_1}(a) \cdots \overline{\lambda_n}^{j_n}(a) \\
&= G(\lambda_1^{j_1}, \chi_1) \cdots G(\lambda_n^{j_n}, \chi_1) G(\overline{\lambda_1}^{j_1} \cdots \overline{\lambda_n}^{j_n}, \overline{\chi_b}).
\end{aligned}$$

Thus,

$$\begin{aligned}
N &= q^{n-1} + \frac{1}{q} \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} \overline{\lambda_1}^{j_1}(a_1) G(\lambda_1^{j_1}, \chi_1) \cdots \overline{\lambda_n}^{j_n}(a_n) G(\lambda_n^{j_n}, \chi_1) G(\overline{\lambda_1}^{j_1} \cdots \overline{\lambda_n}^{j_n}, \overline{\chi_b}) \\
&= q^{n-1} + \frac{1}{q} \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} G(\lambda_1^{j_1}, \chi_{a_1}) \cdots G(\lambda_n^{j_n}, \chi_{a_n}) G(\overline{\lambda_1}^{j_1} \cdots \overline{\lambda_n}^{j_n}, \overline{\chi_b}).
\end{aligned} \tag{3.2}$$

4 The Main Problem

Let $\mathbb{F}_q$ be the finite field with q elements and let t be a positive integer. Consider the equation

$$x^{q-1} + \alpha y^{q-1} = \beta, \tag{4.1}$$

where $\alpha, \beta \in \mathbb{F}_{q^t}^*$. We want to know the number of solutions $(x, y) \in \mathbb{F}_{q^t}^* \times \mathbb{F}_{q^t}^*$ of (4.1). Let

$$N_t(\alpha, \beta) = \left|\{(x, y) \in \mathbb{F}_{q^t}^* \times \mathbb{F}_{q^t}^* : x^{q-1} + \alpha y^{q-1} = \beta\}\right|$$

and for $a, b \in \mathbb{F}_q^*$ and $r \geq 1$, let

$$I(r; a, b) = \left|\{f \in \mathbb{F}_q[x] : f \text{ monic, irr. deg } f = r, f(0) = a, f(1) = b\}\right|.$$

We give a formula for $N_t(\alpha, \beta)$ in terms of $I(r; a, b)$ where $r \mid t$ and $a, b \in \mathbb{F}_q^*$ are related to α and β. For any integer s, let $\mathbb{F}_{q^t}^{*(s)}$ be the group defined by

$$\mathbb{F}_{q^t}^{*(s)} = \{x^s : x \in \mathbb{F}_{q^t}^*\}.$$

We denote the norm function from $\mathbb{F}_{q^t}$ to $\mathbb{F}_q$ by $\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}$.

Theorem 4.1. *For $\alpha, \beta \in \mathbb{F}_{q^t}^*$,*

$$N_t(\alpha, \beta) = (q-1)^2 \sum_{\substack{r \mid t \\ \alpha, \beta \in \mathbb{F}_{q^t}^{*(q-1, t/r)}}} r \sum_{\substack{a, b \in \mathbb{F}_q^* \\ a^{t/r} = \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha) \\ b^{t/r} = \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\beta)}} I(r; a, b).$$

Proof. Put $\mathcal{X} = \{(x, y) \in \mathbb{F}_{q^t}^{*(q-1)} \times \mathbb{F}_{q^t}^{*(q-1)} : x + \alpha y = \beta\}$. Then we have

$$N_t(\alpha, \beta) = (q-1)^2 |\mathcal{X}|. \tag{4.2}$$

Let

$$\mathcal{U} = \{u \in \mathbb{F}_{q^t}^* : \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(u) = \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha),\ \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(u+1) = \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\beta)\}.$$

We claim that the mapping

$$\begin{array}{rccc} \phi: & \mathcal{X} & \longrightarrow & \mathcal{U} \\ & (x, y) & \longmapsto & \dfrac{\alpha y}{x} \end{array}$$

is a bijection. Let $x + \alpha y = \beta$. Then

$$\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}\left(\frac{\alpha y}{x}\right) = \left(\frac{\alpha y}{x}\right)^{(q^t-1)/(q-1)} = \alpha^{(q^t-1)/(q-1)} = \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha).$$

Similarly,

$$\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}\left(\frac{\alpha y}{x} + 1\right) = \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}\left(\frac{\beta}{x}\right) = \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\beta).$$

This shows that ϕ is well-defined. Let $x_1 + \alpha y_1 = \beta = x_2 + \alpha y_2$ and $\frac{\alpha y_1}{x_1} = \frac{\alpha y_2}{x_2}$, then clearly $(x_1, y_1) = (x_2, y_2)$. Thus ϕ is one-to-one. To show that ϕ is onto, let $u \in \mathcal{U}$. Then $\frac{\beta}{1+u}, \frac{\beta u}{\alpha(1+u)} \in \mathbb{F}_{q^t}^{*(q-1)}$ since

$$\left(\frac{\beta}{1+u}\right)^{(q^t-1)/(q-1)} = \frac{\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\beta)}{\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(1+u)} = 1$$

and

$$\left(\frac{\beta u}{\alpha(1+u)}\right)^{(q^t-1)/(q-1)} = \frac{\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\beta)\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(u)}{\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha)\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(1+u)} = 1.$$

Furthermore,

$$\frac{\beta}{1+u} + \alpha\left(\frac{\beta u}{\alpha(1+u)}\right) = \beta.$$

Therefore we have shown that ϕ is a bijection with inverse

$$\begin{aligned}\phi^{-1}:\ \mathcal{U} &\longrightarrow \qquad \mathcal{X} \\ u &\longmapsto \frac{\beta}{1+u}\Big(1,\ \frac{u}{\alpha}\Big).\end{aligned}$$

Hence,

$$|\mathcal{X}| = |\mathcal{U}|. \tag{4.3}$$

Let $\mathcal{U}_r = \{u \in \mathcal{U} : [\mathbb{F}_q(u) : \mathbb{F}_q] = r\}$. Then $|\mathcal{U}| = \sum_{r|t} |\mathcal{U}_r|$. Let $u \in \mathbb{F}_{q^t}$ such that $[\mathbb{F}_q(u) : \mathbb{F}_q] = r$ and let $f \in \mathbb{F}_q[x]$ be the minimal polynomial of u over $\mathbb{F}_q$. We have

$$\begin{aligned}\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(u) &= \mathrm{N}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_{q^r}}(u)) \\ &= \mathrm{N}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(u^{t/r}) \\ &= [(-1)^r f(0)]^{t/r}.\end{aligned}$$

Similarly, since $f(x-1)$ is the minimal polynomial of $u+1$ over $\mathbb{F}_q$ we have

$$\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(u) = [(-1)^r f(-1)]^{t/r}.$$

Let

$$\mathcal{I}_r = \{f \in \mathbb{F}_q[x] : f \text{ monic, irr. deg } f = r, f(0)^{t/r} = \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha), f(1)^{t/r} = \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\beta)\}. \tag{4.4}$$

Then it is clear that the mapping

$$\begin{aligned}\mathcal{U}_r &\longrightarrow \mathcal{I}_r \\ u &\longmapsto (-1)^r f(-x),\end{aligned}$$

where f is the minimal polynomial of u over $\mathbb{F}_q$, is onto and r-to-1. So $|\mathcal{U}_r| = r|\mathcal{I}_r|$. From (4.4) we see that $\mathcal{I}_r = \emptyset$ unless $\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha), \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\beta) \in \mathbb{F}_q^{*(t/r)}$.

We first claim that $\mathbb{F}_q^{*(t/r)} = \mathbb{F}_q^{*(q-1,t/r)}$, where $(q-1, t/r) = \gcd(q-1, t/r)$. Clearly, $\mathbb{F}_q^{*(t/r)} \subset \mathbb{F}_q^{*(q-1,t/r)}$. If $\alpha \in \mathbb{F}_q^{*(q-1,t/r)}$, then $\alpha = x^{a(q-1)+b(t/r)}$ for some $x \in \mathbb{F}_q^*$ and integers a, b. And so $\alpha = x^{b(t/r)} \in \mathbb{F}_q^{*(t/r)}$. Next, we show that $\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q^{*(t/r)}$ if and only if $\alpha \in \mathbb{F}_{q^t}^{*(q-1,t/r)}$.

$$
\begin{aligned}
\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q^{*(t/r)} &\Longleftrightarrow \alpha^{\frac{q^t-1}{q-1}} \in \mathbb{F}_q^{*(t/r)} = \mathbb{F}_q^{*(q-1,t/r)} \\
&\Longleftrightarrow \left(\alpha^{\frac{q^t-1}{q-1}}\right)^{\frac{q-1}{(t/r,q-1)}} = 1 \\
&\Longleftrightarrow \alpha^{\frac{q^t-1}{(t/r,q-1)}} = 1 \\
&\Longleftrightarrow \alpha \in \mathbb{F}_{q^t}^{*(q-1,t/r)}.
\end{aligned}
$$

Therefore, $\mathcal{I}_r = \emptyset$ unless $\alpha, \beta \in \mathbb{F}_{q^t}^{*(q-1,t/r)}$. And so we get

$$
\begin{aligned}
|\mathcal{U}| &= \sum_{r|t} |\mathcal{U}_r| \\
&= \sum_{\substack{r|t \\ \alpha,\beta \in \mathbb{F}_{q^t}^{*(q-1,t/r)}}} r|\mathcal{I}_r| \\
&= \sum_{\substack{r|t \\ \alpha,\beta \in \mathbb{F}_{q^t}^{*(q-1,t/r)}}} r \sum_{\substack{a,b \in \mathbb{F}_q^* \\ a^{t/r} = \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha) \\ b^{t/r} = \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\beta)}} I(r; a, b).
\end{aligned} \tag{4.5}
$$

The conclusion follows from (4.2), (4.3), and (4.5).

■

5 Number of Irreducible Polynomials with Prescribed Values

In this chapter, we give a recursive formula for $I(r; a, b)$. We also give explicit formulas for $I(r; a, b)$ for $r = 2, 3, 4$.

5.1 A Recursive Formula for $I(r; a, b)$

For integer $r > 0$ and $a, b \in \mathbb{F}_q^*$, let

$$\mathcal{I}(r; a, b) = \{f \in \mathbb{F}_q[x] : f \text{ monic, irr. deg } f = r, f(0) = a, f(1) = b\}.$$

So $I(r; a, b) = |\mathcal{I}(r; a, b)|$. If $f \in \mathcal{I}(1; a, b)$, then $f = (b - a)x + a$. So

$$I(1; a, b) = \begin{cases} 1 & \text{if } b - a = 1, \\ 0 & \text{otherwise.} \end{cases} \tag{5.1}$$

For integer $i > 0, \lambda \geq 0$ and $\boldsymbol{a} = (a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$, let

$$\begin{aligned} \mathcal{I}^\lambda(i; \boldsymbol{a}) = \{f_1 \cdots f_\lambda : f_1, \ldots, f_\lambda \in \mathbb{F}_q[x] \text{ monic, irr. of deg } i, \\ (f_1 \cdots f_\lambda)(0) = a, (f_1 \cdots f_\lambda)(1) = b\} \end{aligned}$$

and let $I^\lambda(i;\boldsymbol{a}) = |\mathcal{I}^\lambda(i;\boldsymbol{a})|$. We define $I^0(i;\boldsymbol{a}) = 1$, and write $I^1(i;\boldsymbol{a}) = I(i;\boldsymbol{a})$. We have

$$\begin{aligned} q^{r-2} &= \big|\big\{f \in \mathbb{F}_q[x] : f \text{ monic of deg } r,\ f(0) = a,\ f(1) = b\big\}\big| \\ &= \sum_{1\lambda_1+\cdots+r\lambda_r=r} \sum_{\substack{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_r \in \mathbb{F}_q^*\times\mathbb{F}_q^* \\ \boldsymbol{a}_1\cdots\boldsymbol{a}_r=(a,b)}} \prod_{i=1}^{r} I^{\lambda_i}(i;\boldsymbol{a}_i). \end{aligned}$$

And so

$$I(r;a,b) = q^{r-2} - \sum_{1\lambda_1+\cdots+(r-1)\lambda_{r-1}=r} \sum_{\substack{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{r-1} \in \mathbb{F}_q^*\times\mathbb{F}_q^* \\ \boldsymbol{a}_1\cdots\boldsymbol{a}_{r-1}=(a,b)}} \prod_{i=1}^{r-1} I^{\lambda_i}(i;\boldsymbol{a}_i). \tag{5.2}$$

In the following Lemma, we will express $I^\lambda(i;\boldsymbol{a})$ in terms of $I(i;\boldsymbol{a}')$ where $\boldsymbol{a}' \in \mathbb{F}_q^* \times \mathbb{F}_q^*$.

A *partition of an integer* $\lambda \geq 0$ is a sequence of integers $\tau = (\tau_1,\ldots,\tau_k)$ such that $\tau_1 \geq \cdots \geq \tau_k \geq 1$ and $\tau_1 + \cdots + \tau_k = \lambda$. We write $\tau \vdash \lambda$ to mean that τ is a partition of λ. For $\tau = (\tau_1,\ldots,\tau_k) \vdash \lambda$, let

$$n_s(\tau) = |\{j : \tau_j = s\}|, \qquad 1 \leq s \leq \lambda.$$

Lemma 5.1. *For $i > 0$, $\lambda \geq 0$ and $\boldsymbol{a} \in \mathbb{F}_q^* \times \mathbb{F}_q^*$, we have*

$$I^\lambda(i;\boldsymbol{a}) = \sum_{\tau=(\tau_1,\ldots,\tau_k)\vdash\lambda} \frac{1}{n_1(\tau)!\cdots n_\lambda(\tau)!} \sum_{\substack{\boldsymbol{a}_1,\ldots,\boldsymbol{a}_k \in \mathbb{F}_q^*\times\mathbb{F}_q^* \text{ distinct} \\ \boldsymbol{a}_1^{\tau_1}\cdots\boldsymbol{a}_k^{\tau_k}=\boldsymbol{a}}} \prod_{j=1}^{k} \binom{I(i;\boldsymbol{a}_j)+\tau_j-1}{\tau_j}. \tag{5.3}$$

Proof. Since the elements of $\mathcal{I}^\lambda(i;\boldsymbol{a})$ are products of λ irreducible polynomials, we partition $\mathcal{I}^\lambda(i;\boldsymbol{a})$ by looking at the images of 0 and 1 under each irreducible factor and group the elements of $\mathcal{I}^\lambda(i;\boldsymbol{a})$ having the same set of images, counting multiplicities.

So for each $\tau = (\tau_1, \ldots, \tau_k) \vdash \lambda$, let

$$\mathcal{I}_\tau^\lambda(i;\boldsymbol{a}) = \big\{ f_1 \cdots f_\lambda : \exists\ \boldsymbol{a}_1, \ldots, \boldsymbol{a}_k \in \mathbb{F}_q^* \times \mathbb{F}_q^* \text{ distinct such that } \boldsymbol{a}_1^{\tau_1} \cdots \boldsymbol{a}_k^{\tau_k} = \boldsymbol{a} \\ \text{and } f_s \in \mathcal{I}(i;\boldsymbol{a}_j) \text{ for } \tau_1 + \cdots + \tau_{j-1} < s \leq \tau_1 + \cdots + \tau_j \big\}.$$

Then we have

$$\mathcal{I}^\lambda(i;\boldsymbol{a}) = \dot{\bigcup_{\tau \vdash \lambda}} \mathcal{I}_\tau^\lambda(i;\boldsymbol{a}). \tag{5.4}$$

Now fix $\tau = (\tau_1, \ldots, \tau_k) \vdash \lambda$. For $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k \in \mathbb{F}_q^* \times \mathbb{F}_q^*$, let

$$\mathcal{J}(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k) = \big\{ (g_1, \ldots, g_k) : g_j \text{ is a product of } \tau_j \text{ (not necessarily distinct)} \\ \text{elements of } \mathcal{I}(i;\boldsymbol{a}_j) \big\}.$$

Then

$$|\mathcal{J}(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k)| = \prod_{j=1}^k \binom{I(i;\boldsymbol{a}_j) + \tau_j - 1}{\tau_j}. \tag{5.5}$$

Moreover, the mapping

$$\begin{array}{rccc} \psi : & \dot{\bigcup\limits_{\substack{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k \in \mathbb{F}_q^* \times \mathbb{F}_q^* \text{ distinct} \\ \boldsymbol{a}_1^{\tau_1} \cdots \boldsymbol{a}_k^{\tau_k} = \boldsymbol{a}}}} \mathcal{J}(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k) & \longrightarrow & \mathcal{I}_\tau^\lambda(i;\boldsymbol{a}) \\ & (g_1, \ldots, g_k) & \longmapsto & g_1 \cdots g_k \end{array}$$

is $n_1(\tau)! \cdots n_\lambda(\tau)!$-to-1 and onto. Hence

$$\begin{aligned} |\mathcal{I}_\tau^\lambda(i;\boldsymbol{a})| &= \frac{1}{n_1(\tau)! \cdots n_\lambda(\tau)!} \sum_{\substack{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k \in \mathbb{F}_q^* \times \mathbb{F}_q^* \text{ distinct} \\ \boldsymbol{a}_1^{\tau_1} \cdots \boldsymbol{a}_k^{\tau_k} = \boldsymbol{a}}} |\mathcal{J}(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k)| \\ &= \frac{1}{n_1(\tau)! \cdots n_\lambda(\tau)!} \sum_{\substack{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k \in \mathbb{F}_q^* \times \mathbb{F}_q^* \text{ distinct} \\ \boldsymbol{a}_1^{\tau_1} \cdots \boldsymbol{a}_k^{\tau_k} = \boldsymbol{a}}} \prod_{j=1}^k \binom{I(i;\boldsymbol{a}_j) + \tau_j - 1}{\tau_j}. \end{aligned} \tag{5.6}$$

The conclusion follows from (5.4) and (5.6).

■

With this Lemma, (5.2) becomes a recursive formula for $I(r;a,b)$. However, in the inner sum of (5.3), the requirement that $\boldsymbol{a}_1,\dots,\boldsymbol{a}_k$ be distinct is difficult to implement in actual computation. We shall use a Möbius inversion to waive this requirement.

Fix $\tau=(\tau_1,\dots,\tau_k)\vdash\lambda$ and let

$$\mathcal{A}=\{(\boldsymbol{a}_1,\dots,\boldsymbol{a}_k):\boldsymbol{a}_1,\dots,\boldsymbol{a}_k\in\mathbb{F}_q^*\times\mathbb{F}_q^*,\ \boldsymbol{a}_1^{\tau_1}\cdots\boldsymbol{a}_k^{\tau_k}=\boldsymbol{a}\}.$$

For each $(\boldsymbol{a}_1,\dots,\boldsymbol{a}_k)\in\mathcal{A}$ we define an equivalence relation on the set $\{1,\dots,k\}$ as follows: $i\sim j$ if and only if $\boldsymbol{a}_i=\boldsymbol{a}_j$. We denote the induced partition on $\{1,\dots,k\}$ by $\pi(\boldsymbol{a}_1,\dots,\boldsymbol{a}_k)$. Let $\mathcal{P}_k$ be the set of all partitions of $\{1,\dots,k\}$. For $\pi,\sigma\in\mathcal{P}_k$, we write $\pi\le\sigma$ to mean that π is a refinement of σ. Then $(\mathcal{P}_k,\le)$ is a partially ordered set whose smallest element is $\pi_0=\big\{\{1\},\dots,\{k\}\big\}$. For $\pi\in\mathcal{P}_k$, put

$$\mathcal{A}_\pi=\{(\boldsymbol{a}_1,\dots,\boldsymbol{a}_k)\in\mathcal{A}:\pi(\boldsymbol{a}_1,\dots,\boldsymbol{a}_k)=\pi\}.$$

Let $\pi_1,\dots,\pi_l$ be the blocks of $\pi\in\mathcal{P}_k$. We have

$$\begin{aligned}
&\sum_{\sigma\ge\pi}\ \sum_{(\boldsymbol{a}_1,\dots,\boldsymbol{a}_k)\in\mathcal{A}_\pi}|\mathcal{J}(\boldsymbol{a}_1,\dots,\boldsymbol{a}_k)|\\
=&\sum_{\substack{(\boldsymbol{a}_1,\dots,\boldsymbol{a}_k)\in\mathcal{A}\\ \pi(\boldsymbol{a}_1,\dots,\boldsymbol{a}_k)\ge\pi}}|\mathcal{J}(\boldsymbol{a}_1,\dots,\boldsymbol{a}_k)|\\
=&\sum_{\substack{\boldsymbol{a}_1,\dots,\boldsymbol{a}_l\in\mathbb{F}_q^*\times\mathbb{F}_q^*\\ \boldsymbol{a}_1^{\sum_{j_1\in\pi_1}\tau_{j_1}}\cdots\boldsymbol{a}_l^{\sum_{j_l\in\pi_l}\tau_{j_l}}=\boldsymbol{a}}}\ \prod_{s=1}^{l}\prod_{j\in\pi_s}\binom{I(i;\boldsymbol{a}_s)+\tau_j-1}{\tau_j}.
\end{aligned}$$

By the Möbius inversion formula,

$$\begin{aligned}
&\sum_{(\boldsymbol{a}_1,\dots,\boldsymbol{a}_k)\in\mathcal{A}_{\pi_0}}|\mathcal{J}(\boldsymbol{a}_1,\dots,\boldsymbol{a}_k)|\\
=&\sum_{\pi=\{\pi_1,\dots,\pi_l\}\in\mathcal{P}_k}\mu(\pi)\sum_{\substack{\boldsymbol{a}_1,\dots,\boldsymbol{a}_l\in\mathbb{F}_q^*\times\mathbb{F}_q^*\\ \boldsymbol{a}_1^{\sum_{j_1\in\pi_1}\tau_{j_1}}\cdots\boldsymbol{a}_l^{\sum_{j_l\in\pi_l}\tau_{j_l}}=\boldsymbol{a}}}\ \prod_{s=1}^{l}\prod_{j\in\pi_s}\binom{I(i;\boldsymbol{a}_s)+\tau_j-1}{\tau_j},
\end{aligned}$$

where $\mu(\pi)=\mu(\pi_0,\pi)$ and μ is the Möbius function of $(\mathcal{P}_k,\leq)$. By (2.9),

$$\mu(\pi)=\mu(\pi_0,\pi)=(-1)^{k-l}\prod_{s=1}^{l}(|\pi_s|-1)!.$$

But

$$A_{\pi_0}=\{(\boldsymbol{a}_1,\dots,\boldsymbol{a}_k):\boldsymbol{a}_1,\dots,\boldsymbol{a}_k\in\mathbb{F}_q^*\times\mathbb{F}_q^*\,\text{distinct},\boldsymbol{a}_1^{\tau_1}\cdots\boldsymbol{a}_k^{\tau_k}=\boldsymbol{a}\}.$$

And so by (5.5),

$$\sum_{(\boldsymbol{a}_1,\dots,\boldsymbol{a}_k)\in\mathcal{A}_{\pi_0}}|\mathcal{J}(\boldsymbol{a}_1,\dots,\boldsymbol{a}_k)|=\sum_{\substack{\boldsymbol{a}_1,\dots,\boldsymbol{a}_k\in\mathbb{F}_q^*\times\mathbb{F}_q^*\,\text{distinct}\\ \boldsymbol{a}_1^{\tau_1}\cdots\boldsymbol{a}_k^{\tau_k}=\boldsymbol{a}}}\prod_{j=1}^{k}\binom{I(i;\boldsymbol{a}_j)+\tau_j-1}{\tau_j}.$$

Hence, we can write (5.3) as

$$\begin{aligned}I^\lambda(i;\boldsymbol{a})=&\sum_{\tau=(\tau_1,\dots,\tau_k)\vdash\lambda}\frac{1}{n_1(\tau)!\cdots n_\lambda(\tau)!}\sum_{\pi=\{\pi_1,\dots,\pi_l\}\in\mathcal{P}_k}\mu(\pi)\\ &\cdot\sum_{\substack{\boldsymbol{a}_1,\dots,\boldsymbol{a}_l\in\mathbb{F}_q^*\times\mathbb{F}_q^*\\ \boldsymbol{a}_1^{\sum_{j_1\in\pi_1}\tau_{j_1}}\cdots\boldsymbol{a}_l^{\sum_{j_l\in\pi_l}\tau_{j_l}}=\boldsymbol{a}}}\prod_{s=1}^{l}\prod_{j\in\pi_s}\binom{I(i;\boldsymbol{a}_s)+\tau_j-1}{\tau_j}.\end{aligned}\tag{5.7}$$

5.2 The Case $r=2$

In this section we will find an expression for $I(2;a,b)$ and consequently, for $N_2(\alpha,\beta)$. Let $f\in\mathbb{F}_q[x]$ be monic with $\deg f=2, f(0)=a, f(1)=b$. Then f is of the form

$$f=x^2+(b-a-1)x+a.$$

We find conditions such that f is irreducible.

We first assume that q is odd. Then f is irreducible if and only if $(b-a-1)^2-4a$ is a nonsquare in $\mathbb{F}_q$. Let η be the quadratic character of $\mathbb{F}_q$. Note that we define

$\eta(0) = 0$. Then

$$\eta((b-a-1)^2 - 4a) = \begin{cases} 1 & \text{if } (b-a-1)^2 - 4a \text{ is a square in } \mathbb{F}_q^*, \\ -1 & \text{if } (b-a-1)^2 - 4a \text{ is a nonsquare in } \mathbb{F}_q^*. \end{cases}$$

Thus,

$$I(2;a,b) = \begin{cases} \frac{1}{2}\big[1 - \eta\big((b-a-1)^2 - 4a\big)\big] & \text{if } (b-a-1)^2 - 4a \neq 0, \\ 0 & \text{if } (b-a-1)^2 - 4a = 0. \end{cases} \tag{5.8}$$

If q is even, then $f = x^2 + (b-a-1)x + a \in \mathbb{F}_q[x]$ is reducible if and only if $b-a-1 = 0$ or there exists $\gamma \in \mathbb{F}_q$ such that $\gamma^2 + (b-a-1)\gamma + a = 0$. When $b - a - 1 \neq 0$,

$$\begin{aligned} \gamma^2 + (b-a-1)\gamma + a = 0 &\Longleftrightarrow \left(\tfrac{\gamma}{b-a-1}\right)^2 + \left(\tfrac{\gamma}{b-a-1}\right) = \tfrac{a}{(b-a-1)^2} \\ &\Longleftrightarrow \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\tfrac{a}{(b-a-1)^2}\right) = 0, \end{aligned}$$

by [22, Theorem 2.25]. Therefore f is irreducible if and only if $b-a-1 \neq 0$ and $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{a}{(b-a-1)^2}\right) = 1$. Now let χ_1 be the canonical additive character of $\mathbb{F}_q$. Then by (2.1),

$$\begin{aligned} \chi_1\left(\frac{a}{(b-a-1)^2}\right) &= (-1)^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{a}{(b-a-1)^2}\right)} \\ &= \begin{cases} 1 & \text{if } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\tfrac{a}{(b-a-1)^2}\right) = 0, \\ -1 & \text{if } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\tfrac{a}{(b-a-1)^2}\right) = 1. \end{cases} \end{aligned}$$

Hence,

$$I(2;a,b) = \begin{cases} \frac{1}{2}\left[1 - \chi_1\left(\frac{a}{(b-a-1)^2}\right)\right] & \text{if } b-a-1 \neq 0, \\ 0 & \text{if } b-a-1 = 0. \end{cases} \tag{5.9}$$

We shall use Theorem 4.1 together with (5.8) and (5.9) to determine $N_2(\alpha,\beta)$.

Let $a = \mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha)$ and $b = \mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta)$. By Theorem 4.1,

$$\frac{N_2(\alpha,\beta)}{(q-1)^2} = 2I(2;a,b) + \sum_{\substack{a_1,b_1\in\mathbb{F}_q^* \\ a_1^2=a,\, b_1^2=b}} I(1;a_1,b_1).$$

Using (5.1),

$$\begin{aligned}\sum_{\substack{a_1,b_1\in\mathbb{F}_q^* \\ a_1^2=a,\, b_1^2=b}} I(1;a_1,b_1) &= \left|\left\{a_1\in\mathbb{F}_q^* : a_1^2=a,\ (a_1+1)^2=b\right\}\right| \\ &= \begin{cases} 1 & \text{if } (b-a-1)^2-4a=0, \\ 0 & \text{otherwise.}\end{cases}\end{aligned} \tag{5.10}$$

Combining (5.10) with (5.8) and (5.9), we get, if q is odd,

$$\frac{N_2(\alpha,\beta)}{(q-1)^2} = 1-\eta\big((b-a-1)^2-4a\big). \tag{5.11}$$

If q is even,

$$\frac{N_2(\alpha,\beta)}{(q-1)^2} = \begin{cases} 1-\chi_1\left(\dfrac{a}{(b-a-1)^2}\right) & \text{if } b-a-1\neq 0, \\ 1 & \text{if } b-a-1=0.\end{cases}$$

5.3 The Case $r=3$

Let $f\in\mathbb{F}_q[x]$ be monic with $\deg f=3$, $f(0)=a$, $f(1)=b$. Then

$$f = x^3+cx^2+(b-a-c-1)x+a,$$

for some $c \in \mathbb{F}_q$. Now f is irreducible if and only if $f(x) \neq 0$ for all $x \in \mathbb{F}_q \setminus \{0,1\}$. Let

$$\begin{aligned} V(a,b) &= \left\{ \frac{-1}{x^2-x}\big(x^3+(b-a-1)x+a\big) : x \in \mathbb{F}_q \setminus \{0,1\} \right\} \\ &= \left\{ -x+\frac{a}{x}-\frac{b}{x-1}-1 : x \in \mathbb{F}_q \setminus \{0,1\} \right\}. \end{aligned} \tag{5.12}$$

Then f is irreducible if and only if $c \notin V(a,b)$. Therefore

$$I(3;a,b) = q - |V(a,b)|. \tag{5.13}$$

To determine $N_3(\alpha,\beta)$, let $a = \mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\alpha)$ and $b = \mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\beta)$. By Theorem 4.1 and (5.13),

$$\begin{aligned} \frac{N_3(\alpha,\beta)}{(q-1)^2} &= 3I(3;a,b) + \sum_{\substack{a_1,b_1 \in \mathbb{F}_q^* \\ a_1^3=a,\, b_1^3=b}} I(1;a_1,b_1) \\ &= 3\big(q-|V(a,b)|\big) + \Big|\Big\{a_1 \in \mathbb{F}_q^* : a_1^3 = a,\ (a_1+1)^3 = b\Big\}\Big|. \end{aligned} \tag{5.14}$$

We determine $\Big|\Big\{a_1 \in \mathbb{F}_q^* : a_1^3 = a,\ (a_1+1)^3 = b\Big\}\Big|$ in (5.14) in the next lemma.

Lemma 5.2. *Let $a, b \in \mathbb{F}_q^*$.*

(i) When $p \neq 3$,

$$\begin{aligned} &\Big|\Big\{a_1 \in \mathbb{F}_q^* : a_1^3 = a,\ (a_1+1)^3 = b\Big\}\Big| \\ &= \begin{cases} 2 & \text{if } a=1,\ b=-1 \text{ and } 3 \mid q-1, \\ 1 & \text{if } b-a+2 \neq 0 \text{ and } 3(2a+b-1)(a+2b+1) = (b-a+2)^2(b-a-1), \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

(ii) When $p = 3$,

$$\left|\left\{a_1 \in \mathbb{F}_q^* : a_1^3 = a,\ (a_1+1)^3 = b\right\}\right| = \begin{cases} 1 & \textit{if } b = a+1, \\ 0 & \textit{if } b \neq a+1. \end{cases}$$

Proof. (i) Let $a, b \in \mathbb{F}_q^*$ and $A = \left|\left\{a_1 \in \mathbb{F}_q^* : a_1^3 = a,\ (a_1+1)^3 = b\right\}\right|$. If $a_1 \in A$, then $3a_1^2 + 3a_1 + 1 = b - a$. So $a_1^2 + a_1 + 1 = \frac{1}{3}(b - a + 2)$.

If $b - a + 2 = 0$, then $a_1^3 = 1$. So $a = 1$ and $b = -1$. It follows that a_1 is a primitive cube root of unity. But $\mathbb{F}_q^*$ has a primitive cube root of unity if and only if $3 \mid q - 1$. And so if $a = 1, b = -1$ and $3 \mid q - 1$ then $|A| = 2$.

If $b - a + 2 \neq 0$, we have

$$a_1 - 1 = \frac{a_1^3 - 1}{a_1^2 + a_1 + 1} = \frac{3(a-1)}{b - a + 2}.$$

So

$$a_1 = \frac{2a + b - 1}{b - a + 2}.$$

If $a_1 = \frac{2a+b-1}{b-a+2}$, the equation $a_1^2 + a_1 + 1 = \frac{1}{3}(b - a + 2)$ becomes equivalent to

$$3(2a + b - 1)(a + 2b + 1) = (b - a + 2)^2(b - a - 1). \tag{5.15}$$

Thus, if (5.15) is satisfied then $|A| = 1$.

(ii) Obvious.

∎

5.4 The Case $r = 4$

In this section we will present an explicit formula for $I(4; a, b)$. Using (5.2) we have

$$\begin{aligned} I(4; a, b) = {} & q^2 - I^4(1; a, b) - \sum_{\substack{\boldsymbol{a}_1, \boldsymbol{a}_2 \in \mathbb{F}_q^* \times \mathbb{F}_q^* \\ \boldsymbol{a}_1 \cdot \boldsymbol{a}_2 = (a,b)}} I^2(1; \boldsymbol{a}_1) I(2; \boldsymbol{a}_2) \\ & - I^2(2; a, b) - \sum_{\substack{\boldsymbol{a}_1, \boldsymbol{a}_2 \in \mathbb{F}_q^* \times \mathbb{F}_q^* \\ \boldsymbol{a}_1 \cdot \boldsymbol{a}_2 = (a,b)}} I(1; \boldsymbol{a}_1) I(3; \boldsymbol{a}_2). \end{aligned} \tag{5.16}$$

In (5.16), we shall use (5.7) to compute $I^2(1; \boldsymbol{a}), I^2(2; a, b)$ and $I^4(1; a, b)$. Note that for $i = 1, 2$, then $I(i; \boldsymbol{a}) = 0$ or 1 and so the binomial coefficient in (5.7) is simplified to

$$\binom{I(i; \boldsymbol{a}_s) + \tau_j - 1}{\tau_j} = I(i; \boldsymbol{a}_s).$$

Performing the computations, we get

$$\begin{aligned} I^4(1; a, b) = {} & \frac{1}{24} \sum_{\boldsymbol{a}_1 \cdots \boldsymbol{a}_4 = (a,b)} I(1; \boldsymbol{a}_1) I(1; \boldsymbol{a}_2) I(1; \boldsymbol{a}_3) I(1; \boldsymbol{a}_4) \\ & + \frac{1}{4} \sum_{\boldsymbol{a}_1^2 \boldsymbol{a}_2 \boldsymbol{a}_3 = (a,b)} I(1; \boldsymbol{a}_1) I(1; \boldsymbol{a}_2) I(1; \boldsymbol{a}_3) + \frac{1}{8} \sum_{\boldsymbol{a}_1^2 \boldsymbol{a}_2^2 = (a,b)} I(1; \boldsymbol{a}_1) I(1; \boldsymbol{a}_2) \\ & + \frac{1}{3} \sum_{\boldsymbol{a}_1^3 \boldsymbol{a}_2 = (a,b)} I(1; \boldsymbol{a}_1) I(1; \boldsymbol{a}_2) + \frac{1}{4} \sum_{\boldsymbol{a}_1^4 = (a,b)} I(1; \boldsymbol{a}_1). \end{aligned} \tag{5.17}$$

Each sum in (5.17) represents the number of solutions of a rational equation or some polynomial equations. And so (5.17) can be written as

$$\begin{aligned} I^4(1; a, b) = {} & \frac{1}{24} \left| \left\{ (a_1, a_2, a_3) : a_i \in \mathbb{F}_q^*,\ (1 + a_1)(1 + a_2)(1 + a_3) \left(1 + \tfrac{a}{a_1 a_2 a_3}\right) = b \right\} \right| \\ & + \frac{1}{4} \left| \left\{ (a_1, a_2) \in \mathbb{F}_q^* \times \mathbb{F}_q^* :\ (1 + a_1)^2 (1 + a_2) \left(1 + \tfrac{a}{a_1^2 a_2}\right) = b \right\} \right| \\ & + \frac{1}{8} \left| \left\{ (a_1, a_2) \in \mathbb{F}_q^* \times \mathbb{F}_q^* : a_1^2 a_2^2 = a,\ (1 + a_1)^2 (1 + a_2)^2 = b \right\} \right| \\ & + \frac{1}{3} \left| \left\{ a_1 \in \mathbb{F}_q^* :\ (1 + a_1)^3 \left(1 + \tfrac{a}{a_1^3}\right) = b \right\} \right| + \frac{1}{4} \left| \left\{ a_1 \in \mathbb{F}_q^* : a_1^4 = a,\ (1 + a_1)^4 = b \right\} \right|. \end{aligned} \tag{5.18}$$

Next, for $i = 1, 2$, $\boldsymbol{a} \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ we have

$$I^2(i;\boldsymbol{a}) = \frac{1}{2}\sum_{\boldsymbol{a}_1\boldsymbol{a}_2=\boldsymbol{a}} I(i;\boldsymbol{a}_1)I(i;\boldsymbol{a}_2) + \frac{1}{2}\sum_{\boldsymbol{a}_1^2=\boldsymbol{a}} I(i;\boldsymbol{a}_1). \tag{5.19}$$

Let $i = 1$ and $\boldsymbol{a} = (a, b)$ in (5.19). Then by (5.10),

$$\sum_{\boldsymbol{a}_1^2=\boldsymbol{a}} I(1;\boldsymbol{a}_1) = \begin{cases} 1 & \text{if } (b-a-1)^2 - 4a = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Now

$$\begin{aligned} \sum_{\boldsymbol{a}_1\boldsymbol{a}_2=\boldsymbol{a}} I(1;\boldsymbol{a}_1)I(1;\boldsymbol{a}_2) &= \left|\left\{a_1 \in \mathbb{F}_q^* :\ (1+a_1)\left(1+\tfrac{a}{a_1}\right) = b\right\}\right| \\ &= \left|\left\{a_1 \in \mathbb{F}_q^* : a_1^2 - (b-a-1)a_1 + a = 0\right\}\right| \\ &= \begin{cases} 1 + \eta\big((b-a-1)^2 - 4a\big) & \text{if } q \text{ is odd,} \\ 1 + \chi_1\left(\dfrac{a}{(b-a-1)^2}\right) & \text{if } q \text{ is even and } b-a-1 \neq 0, \\ 1 & \text{if } q \text{ is even and } b-a-1 = 0. \end{cases} \end{aligned}$$

Hence, if q is odd, then

$$I^2(1;\boldsymbol{a}) = \begin{cases} 1 & \text{if } \eta\big((b-a-1)^2 - 4a\big) = 0 \text{ or } 1, \\ 0 & \text{if } \eta\big((b-a-1)^2 - 4a\big) = -1, \end{cases}$$

and so

$$\begin{aligned} \sum_{\substack{\boldsymbol{a}_1,\boldsymbol{a}_2\in\mathbb{F}_q^*\times\mathbb{F}_q^* \\ \boldsymbol{a}_1\boldsymbol{a}_2=(a,b)}} I^2(1;\boldsymbol{a}_1)I(2;\boldsymbol{a}_2) = \Bigg|\Bigg\{&(a_1, b_1) \in \mathbb{F}_q^* \times \mathbb{F}_q^* : \eta\left((b_1 - a_1 - 1)^2 - 4a_1\right) = 0 \text{ or } 1; \\ &\eta\left(\left(\tfrac{b}{b_1} - \tfrac{a}{a_1} - 1\right)^2 - 4\tfrac{a}{a_1}\right) = -1\Bigg\}\Bigg|. \end{aligned} \tag{5.20}$$

Now if q is even, then

$$I^2(1;\boldsymbol{a}) = \begin{cases} 0 & \text{if } b-a-1 \neq 0 \text{ and } \chi_1\Big(\dfrac{a}{(b-a-1)^2}\Big) = -1, \\ \\ 1 & \text{otherwise.} \end{cases}$$

and so we have

$$\sum_{\substack{\boldsymbol{a}_1,\boldsymbol{a}_2 \in \mathbb{F}_q^* \times \mathbb{F}_q^* \\ \boldsymbol{a}_1\boldsymbol{a}_2=(a,b)}} I^2(1;\boldsymbol{a}_1)I(2;\boldsymbol{a}_2) = \Big|\Big\{(a_1,b_1) \in \mathbb{F}_q^* \times \mathbb{F}_q^* : b_1 - a_1 - 1 = 0 \text{ or } \chi_1\Big(\tfrac{a_1}{(b_1-a_1-1)^2}\Big) = 1;$$

$$\chi_1\left(\frac{\frac{a}{a_1}}{(\frac{b}{b_1} - \frac{a}{a_1} - 1)^2}\right) = -1\Big\}\Big|. \tag{5.21}$$

Now let $i=2$ and $\boldsymbol{a} = (a,b)$ in (5.19). Then

$$I^2(2;a,b) = \frac{1}{2}\sum_{\boldsymbol{a}_1\boldsymbol{a}_2=(a,b)} I(2;\boldsymbol{a}_1)I(2;\boldsymbol{a}_2) + \frac{1}{2}\sum_{\boldsymbol{a}_1^2=(a,b)} I(2;\boldsymbol{a}_1).$$

When q is odd, we have

$$\begin{aligned} &I^2(2;a,b) = \\ &\frac{1}{2}\Big|\Big\{(a_1,b_1) \in \mathbb{F}_q^* \times \mathbb{F}_q^* : \eta\big((b_1-a_1-1)^2-4a_1\big) = -1,\ \eta\Big(\Big(\tfrac{b}{b_1} - \tfrac{a}{a_1} - 1\Big)^2 - 4\tfrac{a}{a_1}\Big) = -1\Big\}\Big| \\ &+ \frac{1}{2}\big|\big\{(a_1,b_1) \in \mathbb{F}_q^* \times \mathbb{F}_q^* : a_1^2 = a,\ b_1^2 = b,\ \eta\big((b_1-a_1-1)^2 - 4a_1\big) = -1\big\}\big|. \end{aligned} \tag{5.22}$$

When q is even, we have

$$I^2(2;a,b) =$$
$$\frac{1}{2}\left|\left\{(a_1,b_1)\in\mathbb{F}_q^*\times\mathbb{F}_q^* : \chi_1\left(\frac{a_1}{(b_1-a_1-1)^2}\right)=-1,\ \chi_1\left(\frac{\frac{a}{a_1}}{(\frac{b}{b_1}-\frac{a}{a_1}-1)^2}\right)=-1\right\}\right|$$
$$+\begin{cases}\frac{1}{2} & \text{if } \chi_1\left(\dfrac{a_1}{(b_1-a_1-1)^2}\right)=-1,\\ 0 & \text{otherwise.}\end{cases} \tag{5.23}$$

The last sum in (5.16) is given by

$$\sum_{\substack{\boldsymbol{a}_1,\boldsymbol{a}_2\in\mathbb{F}_q^*\times\mathbb{F}_q^*\\ \boldsymbol{a}_1\cdot\boldsymbol{a}_2=(a,b)}} I(1;\boldsymbol{a}_1)I(3;\boldsymbol{a}_2) = \sum_{a_1\in\mathbb{F}_q^*,\, a_1\neq -1}\left(q-\left|V\left(\tfrac{a}{a_1},\tfrac{b}{a_1+1}\right)\right|\right), \tag{5.24}$$

where $V\left(\frac{a}{a_1},\frac{b}{a_1+1}\right)$ is defined in (5.12).

Now, Equation (5.16) combined with (5.18) and (5.20)–(5.24), is the most explicit formula for $I(4;a,b)$ that this method can offer.

6 $N_3(\alpha, \beta)$ and Elliptic Curves

In a recent paper [23], Moisio found a formula for $N_3(\alpha, \beta)$ in terms of the number of rational points on a projective cubic curve. Let $a = \mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\alpha)$ and $b = \mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\beta)$. Let $\mathcal{A}$ be the affine cubic curve defined by

$$\mathcal{A}: \quad ax^2y + axy^2 + x^2 + ay^2 + (a+1-b)xy + x + y = 0$$

and let $\bar{\mathcal{A}}$ be the projective closure of $\mathcal{A}$. Moisio [23, Theorem 2] proved that

$$\frac{N_3(\alpha, \beta)}{(q-1)^2} = |\bar{\mathcal{A}}(\mathbb{F}_q)|,$$

where $\bar{\mathcal{A}}(\mathbb{F}_q)$ denotes the set of rational points on $\bar{\mathcal{A}}$ over $\mathbb{F}_q$. In this chapter, we will derive another formula for $N_3(\alpha, \beta)$ in terms of the number of rational points on a different (and simpler) projective cubic.

We first define a few terms. For $a, b \in \mathbb{F}_q^*$, $a' \in \mathbb{F}_q$ and integer $r \geq 1$, let

$$\begin{aligned}
S_r(a, b) &= \{u \in \mathbb{F}_{q^r}^* : \mathrm{N}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(u) = a,\ \mathrm{N}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(u+1) = b\}, \\
T_r(a', b) &= \{u \in \mathbb{F}_{q^r}^* : \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(u) = a',\ \mathrm{N}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(u) = b\}, \\
J(r; a', b) &= \big|\{x^r - a'x^{r-1} + \cdots + (-1)^r b \in \mathbb{F}_q[x] \text{ is irreducible}\}\big|.
\end{aligned}$$

Remark. Let γ be a primitive element of $\mathbb{F}_{q^r}$ and assume that $a = \mathrm{N}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\gamma^i)$, $b = \mathrm{N}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\gamma^j)$. Then $|S_r(a, b)|$ is the *cyclotomic number* $(i, j)_{q-1}$ over $\mathbb{F}_{q^r}$; see [22, p.247]. Cyclotomic numbers are closely related to Jacobi sums; see [2, §11.6].

Throughout this chapter, let $a = \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha)$, $b = \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\beta)$. By (4.2) and (4.3),

$$\frac{N_3(\alpha,\beta)}{(q-1)^2} = |S_3(a,b)|. \tag{6.1}$$

Our method in this chapter consists of two steps: First we prove a peculiar connection between $S_3(a,b)$ and $T_3(b-a-1,ab)$ (Theorem 6.1). Then we use a result of Moisio [24] to express $T_3(b-a-1,ab)$ in terms of the number of rational points on a projective cubic.

Theorem 6.1. *Let $a,b \in \mathbb{F}_q^*$. The mapping*

$$\begin{array}{rccc} \psi: & S_3(a,b) & \longrightarrow & T_3(b-a-1,ab) \\ & u & \longmapsto & u+u^{1+q} \end{array}$$

is onto. More precisely, for each $v \in T_3(b-a-1,ab)$,

$$|\psi^{-1}(v)| = \begin{cases} q+1 & \text{if } a=1 \text{ and } v=-1, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. First we show that if $u \in S_3(a,b)$, then $u+u^{1+q}$ indeed belongs to $T_3(b-a-1,ab)$. Clearly,

$$\mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(u+u^{1+q}) = \mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}\big(u(1+u)^q\big) = \mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(u)\,\mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(1+u) = ab.$$

We also have

$$\begin{aligned} b &= \mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(u+1) = (u+1)^{1+q+q^2} \\ &= u^{1+q+q^2} + u^{1+q} + u^{q+q^2} + u^{q^2+1} + u^1 + u^q + u^{q^2} + 1 \\ &= \mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(u) + 1 + \mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(u+u^{1+q}) \\ &= a + 1 + \mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(u+u^{1+q}). \end{aligned}$$

So $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(u+u^{1+q}) = b-a-1$.

Now let $\alpha \in \mathbb{F}_{q^3}^*$ such that $\mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\alpha) = a$. Then $u \in \mathbb{F}_{q^3}^*$ satisfies $\mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(u) = a$ if and only if $u = \alpha x^{q-1}$ for some $x \in \mathbb{F}_{q^3}^*$.

For $v \in T_3(b-a-1, ab)$, let $u \in \psi^{-1}(v)$ such that $\mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(u) = a$. Hence we can write $u = \alpha x^{q-1}$, for some $x \in \mathbb{F}_{q^3}^*$. We claim that $u = \alpha x^{q-1} \in \psi^{-1}(v)$ if and only if $x \in \mathbb{F}_{q^3}^*$ is a solution of

$$\alpha^{1+q} x^{q^2} + \alpha x^q - vx = 0. \tag{6.2}$$

First assume $\alpha x^{q-1} \in \psi^{-1}(v)$. Then $\alpha x^{q-1} + (\alpha x^{q-1})^{1+q} = v$ and so $\alpha x^q + \alpha^{1+q} x^{q^2} = vx$. Next, we assume $x \in \mathbb{F}_{q^3}^*$ is a solution of (6.2). Then we have

$$\psi(\alpha x^{q-1}) = \alpha x^{q-1} + (\alpha x^{q-1})^{1+q} = v.$$

It remains to show that $u \in S_3(a, b)$. We only need to show that $\mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(u+1) = b$. We have

$$\begin{aligned} \mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(u+1) &= \mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(u) + \mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(u + u^{1+q}) + 1 \\ &= a + b - a - 1 + 1 \\ &= b. \end{aligned}$$

This proves the claim.

The number of solutions $x \in \mathbb{F}_{q^3}$ of (6.2) is $q^{3-\mathrm{rank}\, A}$, where

$$A = \begin{bmatrix} v & -\alpha & -\alpha^{1+q} \\ -\alpha^{q+q^2} & v^q & -\alpha^q \\ -\alpha^{q^2} & -\alpha^{q^2+1} & v^{q^2} \end{bmatrix};$$

see [16, Proposition 2.1]. We have

$$
\begin{aligned}
\det A &= v^{1+q+q^2} - \alpha^{1+q+q^2} - \alpha^{2(1+q+q^2)} - \alpha^{1+q+q^2}(v^1 + v^q + v^{q^2}) \\
&= \mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(v) - \mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\alpha) - \mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\alpha)^2 - \mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\alpha)\,\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(v) \\
&= ab - a - a^2 - a(b-a-1) \\
&= 0.
\end{aligned}
$$

So $\operatorname{rank} A = 1$ or 2. It is easy to see that

$$
\operatorname{rank} A = \begin{cases} 1 & \text{if } a = 1 \text{ and } v = -1, \\ 2 & \text{otherwise.} \end{cases}
$$

Hence the number of $x \in \mathbb{F}_{q^3}^*$ of (6.2) is

$$
\begin{cases} q^2 - 1 & \text{if } a = 1 \text{ and } v = -1, \\ q - 1 & \text{otherwise.} \end{cases} \tag{6.3}
$$

Now suppose $x \in \mathbb{F}_{q^3}^*$ is a solution of (6.2). Then for $\epsilon \in \mathbb{F}_q^*$, $x\epsilon$ is also a solution since

$$
\alpha^{1+q}(x\epsilon)^{q^2} + \alpha(x\epsilon)^q - v(x\epsilon) = \epsilon(\alpha^{1+q}x^{q^2} + \alpha x^q - vx).
$$

Therefore, for $v \in T_3(b-a-1, ab)$, the number of $u = \alpha x^{q-1} \in \psi^{-1}(v)$ is

$$
\begin{cases} q + 1 & \text{if } a = 1 \text{ and } v = -1, \\ 1 & \text{otherwise.} \end{cases}
$$

■

If $a = 1$ and $v = -1 \in T_3(b-a-1, ab)$, then $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(-1) = b-2$ and $\mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(-1) = b$, which imply $b = -1$. We have the following corollary.

Corollary 6.2. *Let $a, b \in \mathbb{F}_q^*$. Then*

$$|S_3(a,b)| = \begin{cases} |T_3(b-a-1,ab)| + q & \text{if } a = 1 \text{ and } b = -1, \\ |T_3(b-a-1,ab)| & \text{otherwise.} \end{cases} \tag{6.4}$$

Combining (6.4) and (6.1), we arrive at a new formula for $N_3(\alpha, \beta)$:

$$\frac{N_3(\alpha,\beta)}{(q-1)^2} = \begin{cases} |T_3(b-a-1,ab)| + q & \text{if } a = 1 \text{ and } b = -1, \\ |T_3(b-a-1,ab)| & \text{otherwise,} \end{cases} \tag{6.5}$$

where $a = \mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\alpha)$ and $b = \mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\beta)$.

Moisio [24] studied the number of irreducible polynomials over finite fields with prescribed trace and norm. The number $|T_3(b-a-1,ab)|$ in (6.5) is subject to further interpretations by the results of [24].

For $c \in \mathbb{F}_q^*$, let $\mathcal{B}_c$ be the affine cubic curve defined by

$$\mathcal{B}_c : \quad y^2 + cy + xy = x^3$$

and let $\bar{\mathcal{B}}_c$ denote the projective closure of $\mathcal{B}_c$. By Theorems 3.2 and 5.1 of [24], we have

$$|T_3(b-a-1,ab)| = \begin{cases} \left|\bar{\mathcal{B}}_c(\mathbb{F}_q)\right|, \text{ where } c = \dfrac{ab}{(b-a-1)^3}, & \text{if } b-a-1 \neq 0, \\ q + 1 + \dfrac{1}{q} \displaystyle\sum_{x \in \mathbb{F}_{q^3}} e(\alpha\beta x^{(3,q-1)}) & \text{if } b-a-1 = 0, \end{cases} \tag{6.6}$$

where e is the canonical additive character of $\mathbb{F}_{q^3}$.

We can also write

$$\begin{aligned}|T_3(b-a-1,ab)| &= \left|T_3(b-a-1,ab)\cap(\mathbb{F}_{q^3}\setminus\mathbb{F}_q)\right| + \left|T_3(b-a-1,ab)\cap\mathbb{F}_q\right| \\ &= 3J(3;b-a-1,ab) + \left|\{v\in\mathbb{F}_q : 3v=b-a-1,\ v^3=ab\}\right| \\ &= \begin{cases} 3J(3;b-a-1,ab)+1 & \text{if } (b-a-1)^3=27ab, \\ 3J(3;b-a-1,ab) & \text{otherwise.}\end{cases}\end{aligned} \tag{6.7}$$

If $(b-a-1)^3=27ab$ and char $\mathbb{F}_q\neq 3$, by Corollary 5.2 of [24],

$$J(3;b-a-1,ab)=\left\lfloor \tfrac{1}{3}(q+1)\right\rfloor,$$

so

$$|T_3(b-a-1,ab)| = 3\left\lfloor \tfrac{1}{3}(q+1)\right\rfloor + 1.$$

This is also true when char $\mathbb{F}_q=3$ since in (6.6), we have $\sum_{x\in\mathbb{F}_{q^3}} e(\alpha\beta x)=0$ and $3\left\lfloor \tfrac{1}{3}(q+1)\right\rfloor+1=q+1$. Thus (6.7) can be made a little more explicit:

$$|T_3(b-a-1,ab)| = \begin{cases} 3\lfloor\frac{1}{3}(q+1)\rfloor+1 & \text{if } (b-a-1)^3=27ab, \\ 3J(3;b-a-1,ab) & \text{otherwise.}\end{cases} \tag{6.8}$$

By (6.5) and (6.8) we obtain the following formula for $N_3(\alpha,\beta)$:

$$\frac{N_3(\alpha,\beta)}{(q-1^2)} = \begin{cases} 3\lfloor\frac{1}{3}(q+1)\rfloor+q+1 & \text{if } (a,b)=(1,-1), \\ 3\lfloor\frac{1}{3}(q+1)\rfloor+1 & \text{if } (a,b)\neq(1,-1) \text{ and } (b-a-1)^3=27ab, \\ 3J(3;b-a-1,ab) & \text{otherwise,}\end{cases}$$

where $a=\mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\alpha)$ and $b=\mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\beta)$.

7 Positivity of $I(t; a, b), t \geq 3$

In this chapter, we want to determine if $I(t; a, b)$ is positive with $a, b \in \mathbb{F}_q^*$ and integer $t > 0$. Namely, given a,b and t, does there exist a monic irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree t such that $f(0) = a$ and $f(1) = b$? By (5.1), (5.8) and (5.9), we see that for $t = 1, 2$, we have $I(t; a, b) = 0$ or 1 depending on certain conditions on a and b. When $t = 3$, then by (5.13), $I(3; a, b) \geq 2$ since $|V(a, b)| \leq q - 2$. We will prove that $I(t; a, b) > 0$ for $t \geq 4$. Our proof is based on the relation between $I(t; a, b)$ and an estimate for $N_t(\alpha, \beta)$.

In some sense, the positivity of $I(t; a, b)$ ($t \geq 3$) is comparable with the Hansen-Mullen conjecture for irreducible polynomials [13] (proved by Wan [28] and Ham and Mullen [12]) which postulates that a prescribed degree and one prescribed coefficient can always be achieved by a monic irreducible polynomial in $\mathbb{F}_q[x]$ excluding two obvious non attainable cases.

We first look at $N_t(\alpha, \beta) = \left|\left\{(x, y) \in \mathbb{F}_{q^t}^* \times \mathbb{F}_{q^t}^* : x^{q-1} + \alpha y^{q-1} = \beta\right\}\right|$, where $\alpha, \beta \in \mathbb{F}_{q^t}^*$. The number of solutions of a diagonal equation can be expressed in terms of Gaussian sums and is given in (3.2). But note than in this expression, we considered all solutions in $\mathbb{F}_q^n$. For nonzero solutions, the computation is similar.

We now consider the solutions $(x, y) \in \mathbb{F}_{q^t}^* \times \mathbb{F}_{q^t}^*$ of the diagonal equation $x^{q-1} + \alpha y^{q-1} = \beta$. Let χ_1 be the canonical additive character of $\mathbb{F}_{q^t}$ and let λ be a multiplicative character of order $q-1$ of $\mathbb{F}_{q^t}$. Then

$$\begin{aligned}
N_t(\alpha,\beta) &= \frac{1}{q^t}\sum_{x,y\in\mathbb{F}_{q^t}^*}\sum_{s\in\mathbb{F}_{q^t}}\chi_s(x^{q-1}+\alpha y^{q-1})\overline{\chi_s}(\beta) \\
&= \frac{(q^t-1)^2}{q^t}+\frac{1}{q^t}\sum_{s\in\mathbb{F}_{q^t}^*}\overline{\chi_s}(\beta)\sum_{x,y\in\mathbb{F}_{q^t}^*}\chi_s(x^{q-1})\chi_s(\alpha y^{q-1}) \\
&= \frac{(q^t-1)^2}{q^t}+\frac{1}{q^t}\sum_{j=0}^{q-2}\sum_{k=0}^{q-2}G(\lambda^j,\chi_1)G(\lambda^k,\chi_\alpha)G(\lambda^{-j-k},\overline{\chi_\beta}) \\
&= \frac{(q^t-1)^2}{q^t}+\frac{1}{q^t}\sum_{j=0}^{q-2}\sum_{k=0}^{q-2}\lambda^j(-\beta)\lambda^k\left(-\frac{\beta}{\alpha}\right)G(\lambda^j,\chi_1)G(\lambda^k,\chi_1)G(\lambda^{-j-k},\chi_1).
\end{aligned} \tag{7.1}$$

Observe that by (2.6) and (2.7),

$$\begin{aligned}
&|G(\lambda^j,\chi_1)G(\lambda^k,\chi_1)G(\lambda^{-j-k},\chi_1)| \\
&= \begin{cases} 1 & \text{if } j,k,-j-k \text{ are all} \equiv 0 \pmod{(q-1)}, \\ q^t & \text{if exactly one of } j,k,-j-k \text{ is} \equiv 0 \pmod{(q-1)}, \\ q^{\frac{3}{2}t} & \text{if none of } j,k,-j-k \text{ is} \equiv 0 \pmod{(q-1)}. \end{cases}
\end{aligned}$$

Thus

$$\begin{aligned}
N_t(\alpha,\beta) &\geq \frac{(q^t-1)^2}{q^t}-\frac{1}{q^t}\left[1+3(q-2)q^t+(q-2)(q-3)q^{\frac{3}{2}t}\right] \\
&= q^t+4-3q-(q^2-5q+6)q^{\frac{t}{2}}.
\end{aligned}$$

And so we have the following lemma.

Lemma 7.1. *Let $\alpha,\beta\in\mathbb{F}_{q^t}^*$. Then we have*

$$N_t(\alpha,\beta)\geq q^t+4-3q-(q^2-5q+6)q^{\frac{t}{2}}.$$

Remark. Lemma 7.1 also follows from the Hasse-Weil bound ([27, Theorem V.2.3]). Since the genus of $\mathcal{C}$ in (1.3) is $\frac{1}{2}(q-2)(q-3)$ ([11, p.199]), the Hasse-Weil bound gives $|\mathcal{C}(\mathbb{F}_{q^t})| \geq q^t + 1 - (q-2)(q-3)q^{\frac{t}{2}}$. Thus by (1.4),

$$N_t(\alpha, \beta) \geq |\mathcal{C}(\mathbb{F}_{q^t})| - 3(q-1) \geq q^t + 4 - 3q - (q^2 - 5q + 6)q^{\frac{t}{2}}.$$

We now prove the positivity of $I(t; a, b)$ for $t \geq 4$ in the next theorem.

Theorem 7.2. *For $a, b \in \mathbb{F}_q^*$ and $t \geq 4$ we have $I(t; a, b) > 0$.*

Proof. If $q = 2$, then $a = b = 1$. Every irreducible polynomial $f \in \mathbb{F}_2[x]$ with $\deg f > 1$ must have $f(0) = 1$ and $f(1) = 1$. Thus, $I(t; 1, 1) > 0$ for $t \geq 2$. Henceforth we assume $q \geq 3$.

Let $\alpha, \beta \in \mathbb{F}_{q^t}^*$ such that $a = \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha)$ and $b = \mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\beta)$. By Theorem 4.1,

$$\begin{aligned}
tI(t; a, b) &= \frac{N_t(\alpha, \beta)}{(q-1)^2} - \sum_{r \mid t,\, r<t} r \sum_{\substack{a_1, b_1 \in \mathbb{F}_q^* \\ a_1^{t/r} = a,\, b_1^{t/r} = b}} I(r; a_1, b_1) \\
&\geq \frac{1}{(q-1)^2}\left[q^t + 4 - 3q - (q^2 - 5q + 6)q^{\frac{t}{2}}\right] - \sum_{r \mid t,\, r<t} r\left(\frac{t}{r}\right)^2 q^{r-2} \\
&\geq \frac{1}{(q-1)^2}\left[q^t + 4 - 3q - (q^2 - 5q + 6)q^{\frac{t}{2}}\right] - t^2 q^{-2} \sum_{r \leq \lfloor \frac{t}{2} \rfloor} q^r \\
&= \frac{1}{(q-1)^2}\left[q^t + 4 - 3q - (q^2 - 5q + 6)q^{\frac{t}{2}}\right] - t^2 q^{-2} \cdot \frac{q^{\lfloor \frac{t}{2} \rfloor + 1} - 1}{q-1} \\
&\geq \frac{1}{(q-1)^2}\left[q^t + 4 - 3q - (q^2 - 5q + 6)q^{\frac{t}{2}}\right] - \frac{t^2 q^{\lfloor \frac{t}{2} \rfloor}}{q(q-1)} \\
&\geq \frac{1}{(q-1)^2}\left[q^t + 4 - 3q - (q^2 - 5q + 6)q^{\frac{t}{2}}\right] - \frac{t^2 q^{\frac{t}{2}}}{(q-1)^2} \\
&= \frac{1}{(q-1)^2}\left[q^{\frac{t}{2}}(q^{\frac{t}{2}} - q^2 + 5q - 6 - t^2) + 4 - 3q\right].
\end{aligned}$$

Let $A(q, t) = q^{\frac{t}{2}} - q^2 + 5q - 6 - t^2$. Then

$$\begin{cases}
\dfrac{\partial A}{\partial q} = \dfrac{t}{2} q^{\frac{t}{2} - 1} - 2q + 5, \\
\dfrac{\partial A}{\partial t} = \dfrac{1}{2} q^{\frac{t}{2}} \ln q - 2t.
\end{cases}$$

We have $A(5,4) = 3$, $A(3,8) = 17$ and

$$\frac{\partial A}{\partial q} > 0, \quad \frac{\partial A}{\partial t} > 0 \qquad \text{for } q \geq 5,\ t \geq 4 \text{ or } q \geq 3,\ t \geq 8.$$

So when $q \geq 5$, $t \geq 4$ or $q \geq 3$, $t \geq 8$, we have $A(q,t) \geq 3$ and consequently

$$tI(t; a, b) \geq \frac{1}{(q-1)^2}(q^{\frac{t}{2}} \cdot 3 + 4 - 3q) > 0.$$

For $3 \leq q < 5$ and $4 \leq t < 8$, the positivity of $I(t; a, b)$ is checked directly using a computer.

$\blacksquare$

8 Applications to Planar Functions

A function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is called *planar* if for every $u \in \mathbb{F}_q^*$,

$$x \longmapsto f(x+u) - f(x)$$

is a permutation of $\mathbb{F}_q$. Planar functions were introduced by Dembowski and Ostrom [7] to describe certain affine planes. For further results on planar functions and related topics, see [6], [14], [18], [21]. Recently, planar functions have found important applications in cryptography where they are called *perfect nonlinear functions*; see [26]. Constructions of perfect nonlinear functions and their close relatives *almost perfect nonlinear functions* have been attracting much attention for the past decade, see [3], [8], [9], [10], [15], [19].

Observe that planar functions exist only when q is odd.

Lemma 8.1. *Let p be an odd prime and n be a positive integer. Let*

$$f(x) = x^{p^m+1} + \beta x^2 \in \mathbb{F}_{p^n}[x],$$

where $m > 0$ and $\beta \in \mathbb{F}_{p^n}^*$. Let $t = \frac{n}{(m,n)}$ and $q = p^{(m,n)} = p^{\frac{n}{t}}$ (so $q^t = p^n$). Then f is a planar function on $\mathbb{F}_{q^t}$ if and only if $N_t(1, -2\beta) = 0$, i.e., if and only if $x^{q-1} + y^{q-1} = -2\beta$ has no solution $(x, y) \in \mathbb{F}_{q^t}^* \times \mathbb{F}_{q^t}^*$.

Proof. Let $u \in \mathbb{F}_{q^t}$. Since $f(u)$ is constant, then $f(x+u) - f(x)$ is a permutation of

$\mathbb{F}_{q^t}$ if and only if $f(x+u)-f(x)-f(u)$ is a permutation of $\mathbb{F}_{q^t}$. We have

$$\begin{aligned} f(x+u)-f(x)-f(u) &= ux^{p^m}+u^{p^m}x+2\beta ux \\ &= ux(x^{p^m-1}+u^{p^m-1}+2\beta). \end{aligned}$$

Now $f(x+u)-f(x)-f(u)$ is a p-polynomial. By [22, Theorem 7.9], it is a permutation of $\mathbb{F}_{q^t}$ if and only if $x=0$ is its only root, i.e., if and only if

$$x^{p^m-1}+u^{p^m-1}\neq -2\beta \qquad \text{for all } x,u\in\mathbb{F}_{q^t}^*.$$

But $\mathbb{F}_{q^t}^{*(p^m-1)}=\mathbb{F}_{q^t}^{*(p^m-1,q^t-1)}=\mathbb{F}_{q^t}^{*(p^{(m,n)}-1)}$. And so $f(x+u)-f(x)-f(u)$ is a permutation of $\mathbb{F}_{q^t}$ if and only if

$$x^{q-1}+u^{q-1}\neq -2\beta \qquad \text{for all } x,u\in\mathbb{F}_{q^t}^*.$$

Therefore, f is a planar function on $\mathbb{F}_{q^t}$ if and only if $N_t(1,-2\beta)=0$.

■

In Lemma 8.1, if $t=1$, then $f(x)=(\beta+1)x^2$ on $\mathbb{F}_q$, which is not interesting; if $t\geq 3$, we know from chapter 7 that $N_t(1,-2\beta)>0$, so Lemma 8.1 does not produce any planar function. The only interesting case in this Lemma is when $t=2$. Let $t=2$ and let $b=\mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta)$. Then $\mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(-2\beta)=4b$. By (5.11) we have

$$\begin{aligned} \frac{N_2(1,-2\beta)}{(q-1)^2} &= 1-\eta\big((4b-2)^2-4\big) \\ &= 1-\eta\big(b(b-1)\big). \end{aligned}$$

Combining the above equation and Lemma 8.1, we have the following proposition.

Proposition 8.2. *Let p be an odd prime and let n,m be positive integers such that $(m,n)=\frac{n}{2}$. Put $q=p^{\frac{n}{2}}$ (so $p^n=q^2$). Let $f(x)=x^{p^m+1}+\beta x^2\in\mathbb{F}_{q^2}[x]$, where $\beta\in\mathbb{F}_{q^2}^*$. Then f is a planar function on $\mathbb{F}_{q^2}$ if and only if $\eta\big(b(b-1)\big)=1$, where $b=N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta)$.*

Suppose f satisfy the assumptions in Proposition 8.2. We know that f is a planar function on $\mathbb{F}_{q^2}$ if and only if $N_2(1,-2\beta)=0$. We count the number of β so that f is planar. Write $H=\mathbb{F}_{q^2}^{*(q-1)}$. Then

$$\{\beta' \in \mathbb{F}_{q^2}^* : N_2(1,\beta')>0\} = \mathbb{F}_{q^2}^* \cap (H+H) = H(1+H\backslash\{-1\}).$$

Let q be odd and $x,y \in H\backslash\{-1\}$. We have

$$\begin{aligned}
\frac{1+y}{1+x} \in H &\iff \left(\frac{1+y}{1+x}\right)^{q+1} = 1 \\
&\iff (1+y)^{q+1} = (1+x)^{q+1} \\
&\iff (1+y)(1+y^q) = (1+x)(1+x^q) \\
&\iff 2+y+y^q = 2+x+x^q \\
&\iff y+y^{-1} = x+x^{-1} \\
&\iff (y-x)(xy-1) = 0 \\
&\iff y = x \text{ or } y = x^{-1}.
\end{aligned}$$

Therefore, if $x \neq 1$, then there are precisely two $y \in H$ ($y=x$ or x^{-1}) such that $H(1+x)=H(1+y)$. If $x=1$, then there is exactly one $y \in H$ ($y=x$) such that $H(1+x)=H(1+y)$. Thus,

$$|H(1+H\backslash\{-1\})| = |H|\left(\frac{1}{2}(|H|-2)+1\right) = \frac{1}{2}|H|^2 = \frac{1}{2}(q+1)^2.$$

Hence the number of β in Proposition 8.2 so that f is a planar function is

$$q^2-1-\frac{1}{2}(q+1)^2 = \frac{1}{2}(q+1)(q-3).$$

References

[1] E. A. Bender and J. R. Goldman, *On the applications of Möbius inversion in combinatorial analysis*, Amer. Math. Monthly **82** (1975), 789 – 803.

[2] B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi Sums*, John Wiley, New York, 1998.

[3] L. Budaghyan, C. Carlet, G. Leander, *Two classes of quadratic APN binomials inequivalent to power functions*, IEEE Trans. Inform. Theory **54** (2008), 4218 – 4229.

[4] S. D. Cohen, *Primitive polynomials with a prescribed coefficient*, Finite Fields Appl. **12** (2006), 425 – 491.

[5] R. S. Coulter, *Explicit evaluations of some Weil sums*, Acta Arith. **83** (1998), 241 – 251.

[6] R. S. Coulter, R. W. Matthews, *Planar functions and planes of Lenz-Barlotti class II*, Des. Codes Cryptogr. **10** (1997), 167 – 184.

[7] P. Dembowski and T. G. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z. **103** (1968), 239 – 258.

[8] H. Dobbertin, *Almost perfect nonlinear power functions on $GF(2^n)$: the Welsh case*, IEEE Trans. Infor. Theory **45** (1999), 1271-1275.

[9] H. Dobbertin, *Almost perfect nonlinear power functions on $GF(2^n)$: a new case for n divisible by 5*, Finite Fields and Applications, Springer, Berlin, 2001, 113-121.

[10] T. Helleseth, C. Rong, D. Sandberg, *New families of almost perfect nonlinear power mappings*, IEEE Trans. Inform. Theory **45** (1999), 474-485.

[11] W. Fulton, *Algebraic Curves*, Addison-Wesley, Reading MA, 1989.

[12] K. H. Ham and G. L. Mullen, *Distribution of irreducible polynomials of small degrees over finite fields*, Math. Comp. **67** (1998), 337 – 341.

[13] T. Hansen and G. L. Mullen, *Primitive polynomials over finite fields*, Math. Comp. **59** (1992), 639 – 643, S47 – S50.

[14] T. Helleseth, H. D. L. Hollmann, A. Kholosha, Z. Wang, Q. Xiang, *Proofs of two conjectures on ternary weakly regular bent functions*, IEEE Trans. Inform. Theory, to appear.

[15] H. D. L. Hollmann and Q. Xiang, *A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences*, Finite Fields Appl. **7** (2001), 253 – 286.

[16] X. Hou, *Solution to a problem of S. Payne*, Proc. Amer. Math. Soc. **132** (2004), 1 – 6.

[17] X. Hou, *Explicit evaluation of certain exponential sums of binary quadratic functions*, Finite Fields Appl. **13** (2007), 843 – 868.

[18] X. Hou, *On the dual of a Coulter-Matthews bent function*, Finite Fields Appl. **14** (2008), 505 – 514.

[19] X. Hou, G. L. Mullen, J. A. Sellers, J. L. Yucas, *Reversed Dickson polynomials over finite fields*, preprint.

[20] X. Hou and C. Sze *On certain diagonal equations over finite fields*, Finite Fields Appl., to appear.

[21] W.M. Kantor, *Commutative semifields and symplectic spreads*, J. Algebra **270** (2003), 96 - 114.

[22] R. Lidl and H. Neiderreiter, *Finite Fields*, Cambridge Univ. Press, Cambridge, UK, 1997.

[23] M. Moisio, *On the number of rational points on some families of Fermat curves over finite fields*, Finite Fields Appl. **13** (2007), 546 – 562.

[24] M. Moisio, *Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm*, Acta Arith. **132** (2008), 329 – 350.

[25] H. Niederreiter, *An enumeration formula for certain irreducible polynomials with an application to the construction of irreducible polynomials over the binary field*, Appl. Algebra Engrg. Comm. Comput. **1** (1990), 119 – 124.

[26] K. Nyberg, *Perfect nonlinear S-boxes*, Advances in cryptology – EUROCRYPT '91 (Brighton, 1991), 378 – 386, Lecture Notes in Comput. Sci., 547, Springer, Berlin, 1991.

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

[28] D. Wan, *Generators and irreducible polynomials over finite fields*, Math. Comp. **66** (1997), 1195 – 1212.

[29] J. Wolfmann, *The number of solutions of certain diagonal equations over finite fields*, J. Number Theory **42** (1992), 247 – 257.

[30] J. L. Yucas, *Irreducible polynomials over finite fields with prescribed trace/prescribed constant term*, Finite Fields Appl. **12** (2006), 211 – 221.