Proceedings of the Jangjeon Mathematical Society
29 (2026), No. 3, pp. 551 – 561

www.jangjeon.or.kr
http://dx.doi.org/10.17777/pjms2026.29.3.007

ON THE SUM OF ADDITIVE CHARACTERS OVER FINITE FIELDS

MAITHRI K, VADIRAJA BHATTA G. R.*, AND INDIRA K. P.

Abstract. In this paper, we study the sum of additive characters over finite fields, with a focus on those of specified $\mathbb{F}_q$-Order. We establish a general formula for these character sums, providing an additive analogue to classical results previously known for multiplicative characters. As an application, we derive a Möbius function $\mu(g)$ for polynomials $g \in \mathbb{F}_q[x]$, analogous to the integer Möbius function $\mu(n)$, and develop a characteristic function for k-normal elements. We also generalize several classical identities from the integer setting to the polynomial setting, highlighting the structural parallels between these two domains.

2010 Mathematics Subject Classification. 11T30, 11T06, 11T23, 12E20.

Keywords and phrases. r-primitive elements; k-normal elements; Multiplicative character; Additive characters.

1. Introduction

Let $\mathbb{F}_{q^m}$ be a finite field of order q^m, where $q = p^r$ for some prime p and positive integer r. The field $\mathbb{F}_{q^m}$ can be viewed as an m-dimensional vector space over its subfield $\mathbb{F}_q$. An element $\alpha \in \mathbb{F}_{q^m}$ is called *normal* over $\mathbb{F}_q$ if the set $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\}$ forms a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$; such a set is referred to as a *normal basis*.

The multiplicative group $\mathbb{F}_{q^m}^*$ is cyclic of order $q^m - 1$, and any generator of this group is called a *primitive element* of $\mathbb{F}_{q^m}$. Primitive elements always exist in any finite field. Both primitive and normal elements are of considerable interest in applications, particularly in cryptography. Elements that are simultaneously primitive and normal, known as *primitive normal elements* are especially useful due to their algebraic properties and efficiency in computational settings.

The existence of primitive normal elements has been studied extensively. Carlitz [1, 2] established their existence for sufficiently large values of q^m. Davenport [3] extended this result to the case where q is prime. A general proof covering all cases was later given by Lenstra and Schoof in 1987 [4].

Primitive elements in a finite field $\mathbb{F}_{q^m}$ have order $q^m - 1$. Building on this concept, G. Kapetanakis and L. Reis [5] generalized the idea and introduced r-primitive elements, which are elements of $\mathbb{F}_{q^m}$ of order $\frac{q^m-1}{r}$. In parallel, the concept of normal elements was extended to k-normal elements by S. Huczynsk et al. [6] in 2013. Subsequent research has focused on the existence of r-primitive and k-normal elements for various values of r and k [7, 8].

* Corresponding Author.

Further studies have been conducted on the behavior of the inverses of these elements [9], their properties with prescribed norm and trace [10], and on pairs of r-primitive and k-normal elements [11]. Additionally, research has explored arithmetic progressions of r-primitive and k-normal elements [12], [13].

The investigation of r-primitive and k-normal elements requires the use of characters over finite fields. The study of r-primitive elements typically involves multiplicative characters, while k-normal elements are studied using additive characters. Research has been done to study these additive characters and their properties in [16].

In this paper, we focus on the sum of additive characters and its applications. From this point forward, for any polynomial over the finite field $\mathbb{F}_q[x]$, we use the following notation: $\phi(f)$ represents the Euler's phi function of the polynomial f, which counts the number of polynomials in $\mathbb{F}_q[x]$ of degree less than that of f and relatively prime to f. The notation $\mu(f)$ is defined as $(-1)^r$ if f is the product of r distinct irreducible factors, and zero otherwise. Finally, $W(f)$ denotes the number of square-free divisors of f, and it is also equal to $2^{w(f)}$, where $w(f)$ is the number of irreducible factors of f.

In Section 2, we present the necessary background material. Section 3 establishes a general result on the sum of additive characters with a given $\mathbb{F}_q$-Order. As a consequence, we provide a formula for $\mu(g)$, where g is a polynomial, analogous to the classical Möbius function $\mu(n)$ for natural numbers. In Section 4, we apply the formula derived in Section 3 to construct a characteristic function for elements having specific $\mathbb{F}_q$-Order and hence for k-normal elements. Furthermore, we extend several identities, originally developed for natural numbers in [18] and [13], to the setting of polynomials.

2. Preliminary Definitions

Suppose α, along with all its conjugates, forms a basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, then α is referred to as a *normal element*. R. Lidl and H. Niederreiter [15] provided an equivalent condition for an element to be normal. Motivated by this, S. Huczyns et al. [6] defined k-normal element where the gcd will be of degree k. The normal element is 0-normal in this context.

Definition 2.1. [6] *Let $\alpha \in \mathbb{F}_{q^m}$ and $g_\alpha(x)$ be a polynomial $\sum_{i=0}^{m-1} \alpha^{q^i} x^{m-1-i} \in \mathbb{F}_{q^m}[x]$. If $gcd(x^m-1, g_\alpha(x))$ over $\mathbb{F}_{q^m}$ has degree k (where $0 \le k \le m-1$), then α is a k-normal element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.*

Similar to order of an element in a finite field $\mathbb{F}_q$, we have $\mathbb{F}_q$-Order which is defined with the help of linearized polynomials.

Definition 2.2. [15] *The polynomials*

$$l(x) = \sum_{i=0}^{n} \alpha_i x^i \quad \text{and} \quad L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$$

over $\mathbb{F}_{q^m}$ are called q-associates of each other. More specifically, $l(x)$ is the conventional q-associate of $L(x)$ and $L(x)$ is the linearized q-associate of $l(x)$.

Note that we use the notation $l \circ \alpha$ to represent $L(\alpha)$.

Definition 2.3. [6] *The $\mathbb{F}_q$-Order of an element γ is defined to be the (unique) monic polynomial $f(x) = \sum f_i x^i \in \mathbb{F}_q[x]$ of least degree such that $\sum f_i \gamma^{q^i} = 0$. It is also denoted by $Ord(\gamma)$.*

Analogous to the concept of $\mathbb{F}_q$-Order of elements in a finite field, the $\mathbb{F}_q$-Order of additive characters was introduced by Reis [16]. He also established a relationship between the $\mathbb{F}_q$-Order of an additive character and the $\mathbb{F}_q$-Order of the element that defines the character.

Definition 2.4. [16] *The $\mathbb{F}_q$-Order of and additive character $\chi \in \widehat{\mathbb{F}_{q^m}}$ is the unique monic polynomial in $f \in \mathbb{F}_q[x]$ of least degree such that $f \circ \chi = \chi_0$, that is $\chi(f \circ \gamma) = 1,\ \forall \gamma \in \mathbb{F}_{q^m}$.*

Definition 2.5. [14] *Let $a = a(x) \in \mathbb{F}_q[x], a \mid x^m - 1$ and let $A(x)$ be the linear polynomial corresponding to $a(x)$. Then*

$$c_a(\xi) = \sum_{a(x)} \chi(\xi) \quad (c_1(\xi) = 1)$$

the summation extending over all additive characters of $\mathbb{F}_q$-Order a. Also,

$$c'_a(\xi) = \sum_{d|a} c_D(\xi) = \sum_{A^*(\beta)=0} \chi_\beta(\xi).$$

Where the summation running over all the roots of $A^*(x)$ which is the linearized polynomial corresponding to $a^*(x)$.

Lemma 2.1. [14] *Let $a_1 \,|x^m - 1$ and $a_2| \, x^m - 1, (a_1, a_2) = 1$. Then,*

$$c_{a_1 a_2}(\xi) = c_{a_1}(\xi) c_{a_2}(\xi).$$

Lemma 2.2. [14] *Let u be an irreducible polynomial $\in \mathbb{F}_q[x],\ u^e \mid x^m - 1$. Let ξ belong to $K(x)$, where $K(x)$ corresponds to $k(x)$; also put $x^m - 1 = kl$. Then we have*

$$c_{u^e}(\xi) = \begin{cases} |u|^e - |u|^{e-1} & (u^e \mid l) \\ -|u|^{e-1} & \left(u^{e-1} \mid l, u^e \nmid l\right) \\ 0 & \left(u^{e-1} \nmid l\right) \end{cases}$$

where $|u| = q^{deg(u(x))}$.

Theorem 2.3. [**?**] *The sum S of k-th powers of primitive n-th roots of unity is given by $S = \mu(g)\frac{\phi(n)}{\phi(g)}$ where $g = \frac{n}{(k,n)}$.*

3. Sum of additive characters

In this section, we study sums of additive characters over finite fields. As mentioned earlier, we first examine these sums in the context of integers, and subsequently extend the analysis to the polynomial setting.

Theorem 3.1. *If α is primitive element in the field $\mathbb{F}_{q^m}$, then for a divisor d of $q^m - 1$,*

$$\sum_{(d)} \psi_d(\alpha^r) = \mu\left(\frac{d}{gcd(d,r)}\right) \frac{\phi(d)}{\phi\left(\frac{d}{gcd(d,r)}\right)},$$

where the summation runs over all the multiplicative character of order d.

Proof. Let α be a primitive element of the finite field $\mathbb{F}_{q^m}$. For any multiplicative character ψ of order d, the value $\psi(\alpha)$ is a primitive d-th root of unity. Consider the summation $\sum_{(d)} \psi_d(\alpha^r)$, where the sum runs over all multiplicative characters of order d. This summation represents the sum of the r-th powers of the primitive d-th roots of unity. From Theorem [**?**], it follows that

$$\sum_{(d)} \psi_d(\alpha^r) = \mu\left(\frac{d}{\gcd(d,r)}\right) \frac{\phi(d)}{\phi\left(\frac{d}{\gcd(d,r)}\right)}.$$

□

Motivated by this, an analogous result can also be formulated using additive characters. In the case of multiplicative characters, a primitive element is used, as every nonzero element of the field can be expressed as a power of such an element. For additive characters, we instead rely on the concept of a normal element, since any element β of the finite field can be written as $f \circ \alpha$ for some normal element α.

Lemma 2.2 gives the formula for sum of additive characters of an element of a finite field, where the sum is running over all the additive characters of $\mathbb{F}_q$-Order some power of an irreducible polynomial. Now, we prove the general case of this.

Theorem 3.2. *Let $x^m - 1 = f_1(x)f_2(x)$, $g(x)|x^m - 1$ and let $\alpha \in \mathbb{F}_{q^m}$ with $\mathbb{F}_q$-Order f_1, then $\sum_g \chi(\alpha) = \mu(d)\frac{\phi(g)}{\phi(d)}$, where $d(x) = \frac{g(x)}{gcd(g(x), f_2)}$ and the summation runs over all the additive characters of $\mathbb{F}_q$-Order g.*

Proof. Let $g = g_1^{e_1}(x)g_2^{e_2}(x)\dots g_k^{e_k}(x)$. Then

$$d = \frac{g}{\gcd(g, f_2)} = \frac{g_1^{e_1}g_2^{e_2}\dots g_k^{e_k}}{\gcd(g_1^{e_1}g_2^{e_2}\dots g_k^{e_k}, f_2)} = \frac{g_1^{e_1}g_2^{e_2}\dots g_k^{e_k}}{g_1^{l_1}g_2^{l_2}\dots g_k^{l_k}} = g_1^{e_1-l_1}g_2^{e_2-l_2}\dots g_k^{e_k-l_k}.$$

Moreover, by Lemma 2.1, we have

$$\sum_g \chi(\alpha) = \sum_{g_1^{e_1}} \chi(\alpha) \sum_{g_2^{e_2}} \chi(\alpha) \cdots \sum_{g_k^{e_k}} \chi(\alpha). \tag{1}$$

Case 1: $d = 1$

In this case, g divides f_2, that is, $g_i^{e_i} \mid f_2$ for all $1 \le i \le k$. By Lemma 2.2, it follows that

$$\sum_{g_i^{e_i}} \chi(\alpha) = |g_i|^{e_i} - |g_i|^{e_i-1} = \phi(g_i^{e_i}), \quad \text{for all } 1 \le i \le k.$$

Substituting into equation (1), we obtain

$$\sum_g \chi(\alpha) = \prod_{i=1}^{k} \phi(g_i^{e_i}) = \phi(g) = \mu(d)\frac{\phi(g)}{\phi(d)}.$$

Case 2: $d = g_1g_2\dots g_r$

By Lemma 2.2, we have

$$\sum_{g_i^{e_i}} \chi(\alpha) = -|g_i|^{e_i-1} = \mu(g_i)\frac{\phi(g_i^{e_i})}{\phi(g_i)} \quad \text{for } 1 \le i \le r,$$

and

$$\sum_{g_i^{e_i}} \chi(\alpha) = \phi(g_i^{e_i}) \quad \text{for } r+1 \le i \le k.$$

Substituting these into equation (1), it follows that

$$\sum_{g} \chi(\alpha) = \prod_{i=1}^{r} \mu(g_i)\frac{\phi(g_i^{e_i})}{\phi(g_i)} \prod_{i=r+1}^{k} \phi(g_i^{e_i}) = \mu(d)\frac{\phi(g)}{\phi(d)}.$$

Case 3: Suppose there exist an square factor in d.
Let $g_i^2|d$ for some i, $1 \le i \le k$, then by lemma 2.2, we have

$$\sum_{g_i^{e_i}} \chi(\alpha) = 0.$$

Substituting this into equation (1), it follows that

$$\sum_{g} \chi(\alpha) = 0 = \mu(d) = \mu(d)\frac{\phi(g)}{\phi(d)}.$$

□

Corollary 3.3. *Let α be a normal element in the field $\mathbb{F}_{q^m}$, $f(x) \in \mathbb{F}_q[x]$ and $g(x) \mid x^m - 1$, then $\sum_{g} \chi(f \circ \alpha) = \mu(d)\frac{\phi(g)}{\phi(d)}$, where $d = \frac{g}{gcd(g,f)}$.*

Remark 3.1. *It is well-known that for any positive integer n, sum of primitive n-th roots of unity is given by $\mu(n)$ i.e. $\sum_{n} \psi_n(\alpha) = \mu(n)$ where α is a primitive element. From the above result, we get that for any polynomial $g|x^m - 1$ over $\mathbb{F}_q[x]$, $\sum_{g} \chi(\alpha) = \mu(g)$, where α is a normal element.*

4. Applications of sum of additive characters

In this section, we establish some basic results on summations involving the Euler's totient function ϕ applied to polynomials, which will be utilized in the characteristic function for k-normal elements.

Lemma 4.1. *Let $f(x) \in \mathbb{F}_q[x]$ be a divisor of $x^m - 1$. For any square-free divisor $h(x)$ of f, $\sum_{\substack{g(x)|\frac{x^m-1}{f} \\ gcd(h,\frac{x^m-1}{fg})=1}} \phi(hg) = q^{deg(\frac{x^m-1}{f})}\phi(h)$.*

Proof. Let $x^m - 1 = \prod_{i=1}^{r} p_i^a(x)$, $f = \prod_{i=1}^{r} p_i^{b_i}(x)$ with $0 \le b_i \le a$, $h = \prod_{i=1}^{r} p_i^{c_i}(x)$ with $c_i =$ 0 or 1 and g is of the form $g = \prod_{i=1}^{r} p_i^{d_i}(x)$ with $0 \le d_i \le a - b_i$ and degree of

p_i be m_i.
Since $\gcd(h, \frac{x^m-1}{fg}) = 1$, if $c_i = 1$ then $d_i = a - b_i$. Let $S = \{i : c_i = 1\}, T = \{j : c_j = 0\}$.
Consider, $\phi(hg) = \prod_{i=1}^{r} \phi(p_i^{c_i+d_i}) = \prod_{i\in S} \phi(p_i^{1+a-b_i}) \prod_{j\in T} \phi(p_j^{d_j})$, then

$$\sum_{\substack{g|\frac{x^m-1}{f} \\ gcd(h,\frac{x^m-1}{fg})=1}} \phi(hg) = \prod_{i\in S} \phi(p_i^{1+a-b_i}) \sum_{\substack{j\in T \\ d_j=0}}^{a-b_j} \prod_{j} \phi(p_j^{d_j})$$

By interchanging summation and product and simplifying $\sum_{d_j=0}^{a-b_j} \phi(p_j^{d_j})$ we get,

$$\sum_{\substack{g|\frac{x^m-1}{f} \\ gcd(h,\frac{x^m-1}{fg})=1}} \phi(hg) = \prod_{i\in S} \phi(p_i^{1+a-b_i}) \prod_{j\in T} q^{m_j(a-b_j)} = \prod_{i\in S} q^{m_i(a-b_i)}(q^{m_i}-1) \prod_{j\in T} q^{m_j(a-b_j)}$$

Further by using the formula for Euler-phi function of a polynomial we get,

$$\sum_{\substack{g|\frac{x^m-1}{f} \\ gcd(h,\frac{x^m-1}{fg})=1}} \phi(hg) = \prod_{j=1}^{r} q^{m_j(a-b_j)} \prod_{i\in S}(q^{m_i} - 1) = q^{deg(\frac{x^m-1}{f})}\phi(h).$$

□

Remark 4.1. *Note that Lemmas 2.2 and 2.3 from* [18]*, originally stated for positive integers, can be extended to the polynomial setting by using Lemma 4.1.*

Lemma 4.2. *If u is an irreducible polynomial over $\mathbb{F}_q[x]$ of degree n, then $\sum_{i=0}^{l} \phi(u^i) = \frac{\phi(u^{l+1})}{\phi(u)}$ for any positive integer l.*

Proof.

$$\sum_{i=0}^{l} \phi(u^i) = 1 + \phi(u) + \phi(u^2) + \cdots + \phi(u^l)$$

$$= 1 + (q^n - 1) + (q^{2n} - q^n) + \cdots + (q^{ln} - q^{(l-1)n}) = q^{ln} = \frac{q^{ln}(q^n - 1)}{q^n - 1}$$

$$= \frac{q^{n(l+1)} - q^{ln}}{q^n - 1} = \frac{\phi(u^{l+1})}{\phi(u)}.$$

□

S. D. Cohen [18] provided a characteristic function for elements with a specific multiplicative order. Motivated by this, we derive a characteristic function for elements with a specific $\mathbb{F}_q$-Order. Let η_f be the characteristic

function for elements with $\mathbb{F}_q$-Order f. For any $f \in \mathbb{F}_q[x]$ dividing $x^m - 1$ and $\alpha \in \mathbb{F}_{q^m}$,

$$\eta_f(\alpha) = \begin{cases} 1 & \text{if } \mathbb{F}_q\text{-Order of } \alpha \text{ is } f \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 4.3. *Let $f(x)$ be a divisor of x^m-1 of degree n over $\mathbb{F}_q[x]$. Then, for any $\alpha \in \mathbb{F}_{q^m}$,*

$$\eta_f(\alpha) = \frac{\phi(f)}{q^m} \sum_{h|f} \frac{\mu(h)}{\phi(h)} \sum_{\substack{g|\frac{x^m-1}{f} \\ gcd(h,\frac{x^m-1}{fg})=1}} \sum_{hg} \chi(\alpha)$$

where the inner sum is running over all the additive characters of $\mathbb{F}_q$-Order hg.

Proof. Let $k(x)$ be the $\mathbb{F}_q$-Order of α.
Case 1: $k(x) = f(x)$
Then, by using theorem 3.2,

$$\eta_f(\alpha) = \frac{\phi(f)}{q^m} \sum_{h|f} \frac{\mu(h)}{\phi(h)} \sum_{\substack{g|\frac{x^m-1}{f} \\ gcd(h,\frac{x^m-1}{fg})=1}} \mu\left(\frac{gh}{\gcd(gh, \frac{x^m-1}{f})}\right) \frac{\phi(gh)}{\phi\left(\frac{gh}{\gcd(gh,\frac{x^m-1}{f})}\right)}$$

Since $\gcd(h, \frac{x^m-1}{fg}) = 1$, $\gcd(hg, \frac{x^m-1}{f}) = g$. Thus the above equation reduces to,

$$\eta_f(\alpha) = \frac{\phi(f)}{q^m} \sum_{h|f} \frac{\mu(h)}{\phi(h)} \sum_{\substack{g|\frac{x^m-1}{f} \\ gcd(h,\frac{x^m-1}{fg})=1}} \mu(h) \frac{\phi(gh)}{\phi(h)}$$

By using lemma 4.1, the above expression becomes

$$\begin{aligned} \eta_f(\alpha) &= \frac{\phi(f)}{q^m} \sum_{h|f} \frac{(\mu(h))^2}{(\phi(h))^2} q^{m-n} \phi(h) = \frac{\phi(f)}{q^m} q^{m-n} \sum_{h|f} \frac{(\mu(h))^2}{\phi(h)} \\ &= \frac{\phi(f)}{q^m} q^{m-n} \frac{q^n}{\phi(f)} = 1. \end{aligned}$$

Case 2: $k \mid f$ and $k \neq f$
Then, by theorem 3.2,
(2)

$$\eta_f(\alpha) = \frac{\phi(f)}{q^m} \sum_{h|f} \frac{\mu(h)}{\phi(h)} \sum_{\substack{g|\frac{x^m-1}{f} \\ gcd(h,\frac{x^m-1}{fg})=1}} \mu\left(\frac{gh}{\gcd(gh, \frac{x^m-1}{k})}\right) \frac{\phi(gh)}{\phi\left(\frac{gh}{\gcd(gh,\frac{x^m-1}{k})}\right)}$$

Let $x^m - 1 = (p_1(x)p_2(x)\dots p_r(x))^a$, $f = p_1^{b_1}p_2^{b_2}\dots p_r^{b_r}$, $k = p_1^{c_1}p_2^{c_2}\dots p_r^{c_r}$ and $h = p_1p_2\dots p_l$. Since $\gcd(h, \frac{x^m-1}{fg}) = 1$, $g = p_1^{a-b_1}\dots p_l^{a-b_l}p_{l+1}^{d_{l+1}}\dots p_r^{d_r}$. As $k \mid f, c_i \leq b_i \ \forall i$.

Let $S_h = \dfrac{\mu(h)}{\phi(h)} \sum_{\substack{g|\frac{x^m-1}{f} \\ \gcd(h,\frac{x^m-1}{fg})=1}} \mu\left(\dfrac{gh}{\gcd(gh,\frac{x^m-1}{k})}\right) \dfrac{\phi(gh)}{\phi\left(\frac{gh}{\gcd(gh,\frac{x^m-1}{k})}\right)}$.

Suppose $c_i < b_i\ \forall i$, then $\gcd(gh, \dfrac{x^m-1}{k}) = \gcd(p_1^{a-b_1+1}\dots p_l^{a-b_l+1}p_{l+1}^{d_{l+1}}\dots p_r^{d_r}, p_1^{a-c_1}\dots p_r^{a-c_r}) = p_1^{a-b_1+1}\dots p_l^{a-b_l+1}p_{l+1}^{d_{l+1}}\dots p_r^{d_r} = gh$.

Thus, by using lemma 4.1, $S_h = \dfrac{\mu(h)}{\phi(h)} \sum_{\substack{g|\frac{x^m-1}{f} \\ \gcd(h,\frac{x^m-1}{fg})=1}} \phi(gh) = \mu(h)q^{m-n}$.

Now, for any $u(x) \neq p_i,\ 1 \leq i \leq l, S_{uh} + S_h = 0$. Thus, $\eta_f = 0$.

Suppose, $c_1 = b_1, c_2 = b_2, \dots, c_i = b_i$ for $1 \leq i \leq l$, then
$\gcd(gh, \dfrac{x^m-1}{k}) = \gcd(p_1^{a-b_1+1}\dots p_l^{a-b_l+1}p_{l+1}^{d_{l+1}}\dots p_r^{d_r}, p_1^{a-c_1}\dots p_r^{a-c_r})$
$= p_1^{a-b_1}\dots p_i^{a-b_i}p_{i+1}^{a-b_{i+1}+1}\dots p_l^{a-b_l+1}p_{l+1}^{d_{l+1}}\dots p_r^{d_r} = \dfrac{gh}{p_1p_2\dots p_i}$.

Now, $S_h = \dfrac{\mu(h)}{\phi(h)} \sum_{\substack{g|\frac{x^m-1}{f} \\ \gcd(h,\frac{x^m-1}{fg})=1}} \mu(p_1p_2\dots p_i)\dfrac{\phi(gh)}{\phi(p_1p_2\dots p_i)}$

$= \dfrac{\mu(h)\mu(p_1p_2\dots p_i)}{\phi(h)\phi(p_1p_2\dots p_i)} \sum_{\substack{g|\frac{x^m-1}{f} \\ \gcd(h,\frac{x^m-1}{fg})=1}} \phi(gh)$.

By lemma 4.1, $S_h = \dfrac{\mu(h)\mu(p_1p_2\dots p_i)}{\phi(h)\phi(p_1p_2\dots p_i)}\phi(h)q^{m-n}$.

Now, for any $u(x) \neq p_j, 1 \leq j \leq l$, $S_{uh} = \dfrac{\mu(uh)\mu(p_1p_2\dots p_i)}{\phi(uh)\phi(p_1p_2\dots p_i)}\phi(uh)q^{m-n} = -S_h$. Thus, $S_h + S_{uh} = 0$. Thus $\eta_f = 0$.

Suppose, $c_1 = b_1, c_2 = b_2, \dots c_i = b_i$ for $l < i \leq r$, then $\gcd(gh, \dfrac{x^m-1}{k}) = \gcd(p_1^{a-b_1+1}\dots p_l^{a-b_l+1}p_{l+1}^{d_{l+1}}\dots p_r^{d_r}, p_1^{a-c_1}\dots p_r^{a-c_r}) = p_1^{a-b_1}\dots p_l^{a-b_l+1}p_{l+1}^{d_{l+1}}\dots p_r^{d_r} = \dfrac{gh}{p_1p_2\dots p_l}$. Further simplifying as above, we get $\eta_f = 0$.

Case 3: $k \nmid f$

Then there exists an irreducible polynomial $u(x)$ such that l is the highest power of u dividing k and u^l does not divide f.

Let a be the highest power of u dividing $x^m - 1$, r be the highest power of u dividing f and h, g be fixed with $u \nmid g$, h square-free. Let,

$$S_g = \mu\left(\frac{gh}{\gcd(gh, \frac{x^m-1}{k})}\right) \frac{\phi(gh)}{\phi\left(\frac{gh}{\gcd(gh, \frac{x^m-1}{k})}\right)}.$$

Consider the sum, $S = \sum_{i=0}^{a-r} S_{u^i g} = \sum_{i=0}^{a-r} \mu\left(\frac{u^i gh}{\gcd(u^i gh, \frac{x^m-1}{k})}\right) \frac{\phi(u^i gh)}{\phi\left(\frac{u^i gh}{\gcd(u^i gh, \frac{x^m-1}{k})}\right)}$.

Suppose $p \nmid h$ then, $\gcd(u^i gh, \frac{x^m-1}{k}) = u^i \gcd(gh, \frac{x^m-1}{k})$ for $0 \le i \le a-l$ and $\gcd(u^i gh, \frac{x^m-1}{k}) = u^{a-l} \gcd(gh, \frac{x^m-1}{k})$ for $a-l < i \le a-r$. Thus,

$$\begin{aligned} S =& \sum_{i=0}^{a-l} \mu\left(\frac{gh}{\gcd(gh, \frac{x^m-1}{k})}\right) \frac{\phi(u^i)\phi(gh)}{\phi\left(\frac{gh}{\gcd(gh, \frac{x^m-1}{k})}\right)} \\ &+ \sum_{j=a-l+1}^{l} \mu(u^{j-a+l}) \mu\left(\frac{gh}{\gcd(gh, \frac{x^m-1}{k})}\right) \frac{\phi(u^j)\phi(gh)}{\phi(u^{j-a+l})\phi\left(\frac{gh}{\gcd(gh, \frac{x^m-1}{k})}\right)} \\ &= \mu\left(\frac{gh}{\gcd(gh, \frac{x^m-1}{k})}\right) \frac{\phi(gh)}{\phi\left(\frac{gh}{\gcd(gh, \frac{x^m-1}{k})}\right)} \left[1 + \phi(u) + \phi(u^2) + \cdots + \phi(u^{a-l}) - \frac{\phi(u^{a-l+1})}{\phi(u)}\right] \end{aligned}$$

By lemma 4.2, we get $S = 0$.
Suppose $u \mid h$, as $\gcd(h, \frac{x^m-1}{fg}) = 1, u^{a-r}$ must divide g, but $u \nmid g, r = a$, a contradiction as r is the highest power of u dividing f and $r < l$.
Thus, $\eta_f = 0$.
Also, suppose $u \mid g$, then $g = u^j t$. Then we replace g by t and by same procedure as above we get $\eta_f = 0$. □

Theorem 4.4. *Consider the field $\mathbb{F}_{q^m}$, for any $\alpha \in \mathbb{F}_{q^m}$, and non-negative integer $k \le m$,*

$$\zeta_k(\alpha) := \sum_{\substack{f \mid x^m-1 \\ deg(f)=m-k}} \frac{\phi(f)}{q^m} \sum_{h \mid f} \frac{\mu(h)}{\phi(h)} \sum_{\substack{g \mid \frac{x^m-1}{f} \\ gcd(h, \frac{x^m-1}{fg})=1}} \sum_{hg} \chi(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is } k-\text{normal} \\ 0 & \text{otherwise} \end{cases}$$

is the characteristic function for k-normal elements.

We use the fact that an element $\alpha \in \mathbb{F}_{q^m}$ is k-normal if and only if degree of $\mathbb{F}_q$-Order of α is of degree $m-k$, and the theorem 4.3 for proving the above result.

We now present a result that relate the $\mathbb{F}_q$-Order, additive characters, and the Euler phi function, in analogy with the integer setting discussed in [13].

Proposition 4.5. *Consider the field $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, for any divisor g of x^m-1,*

$$\sum_{\substack{f \in \mathbb{F}_q[x] \\ deg(f)<m}} \mid \sum_{g} \chi(f \circ \alpha) \mid = q^{m-deg(g)} \phi(g) W(g),$$

where α is normal element over the field and inner sum is running over all the additive characters of $\mathbb{F}_q$-Order g.

Proof.

$$\sum_{\substack{f\in\mathbb{F}_q[x]\\ deg(f)<m}} |\sum_g \chi(f\circ\alpha)| = \sum_{\substack{f\in\mathbb{F}_q[x]\\ deg(f)<m}} |\mu(\frac{g}{\gcd(g,f)})| \frac{\phi(g)}{\phi(\frac{g}{\gcd(g,f)})}$$

$$= \phi(g) \sum_{\substack{f\in\mathbb{F}_q[x]\\ deg(f)<m}} \frac{\left(\mu(\frac{g}{\gcd(g,f)})\right)^2}{\phi(\frac{g}{\gcd(g,f)})}$$

$$= \phi(g) \sum_{d|g} \frac{\left(\mu(\frac{g}{d})\right)^2}{\phi(\frac{g}{d})} \sum_{\substack{h\in\mathbb{F}_q[x]\\ deg(h)<m-deg(d)\\ \gcd(h,\frac{g}{d})=1}} 1$$

By applying division algorithm for h and $\frac{g}{d}$, h is of the form $\frac{g}{d}s+t$ with $\gcd(k,t)=1$ and $deg(s)<m-deg(g)$, then

$$\sum_{\substack{h\in\mathbb{F}_q[x]\\ deg(h)<m-deg(d)\\ \gcd(h,\frac{g}{d})=1}} 1 = \sum_{\substack{\frac{g}{d}s+t\\ (\frac{g}{d},t)=1\\ deg(d)<m-deg(g)}} 1 = \phi\left(\frac{g}{d}\right) q^{m-deg(g)}$$

Thus, $\sum_{\substack{f\in\mathbb{F}_q[x]\\ deg(f)<m}} |\sum_g \chi(f\circ\alpha)| = \phi(g) \sum_{d|g} \frac{\left(\mu(\frac{g}{d})\right)^2}{\phi(\frac{g}{d})} \phi\left(\frac{g}{d}\right) q^{m-deg(g)}$

$= \phi(g) q^{m-deg(g)} \sum_{d|g} \left(\mu(\frac{g}{d})\right)^2 = \phi(g) q^{m-deg(g)} W(g).$ □

Conclusion

In this work, we explored the sum of additive characters over finite fields by organizing them according to their $\mathbb{F}_q$-Order. We derived a general formula for such sums, which serves as an additive analogue of known results involving multiplicative characters. As direct applications, we obtained a formula for the Möbius function of polynomials and constructed a characteristic function for k-normal elements. Additionally, several identities traditionally formulated for integers were successfully extended to the polynomial case, demonstrating the depth of analogy between number-theoretic and polynomial-theoretic structures. These results offer new tools and perspectives for further study in finite field theory and its applications in coding theory and cryptography.

References

[1] L. Carlitz, Primitive roots in a finite field, *Transactions of the American Mathematical Society*, vol. 73, no. 3, pp. 373–382, (1952).

[2] L. Carlitz, Some problems involving primitive roots in a finite field, *Proceedings of the National Academy of Sciences of the United States of America*, vol. 38, no. 4, pp. 314–318, (1952).

[3] H. Davenport, Bases for finite fields, *Journal of the London Mathematical Society*, vol. s1-43, pp. 21–39, (1968).

[4] H. W. Lenstra and R. J. Schoof, Primitive normal bases for finite fields, *Mathematics of Computation*, vol. 48, no. 177, pp. 217–231, (1987).
[5] G. Kapetanakis and L. Reis, Variations of the primitive normal basis theorem, *Designs, Codes and Cryptography*, vol. 87, (2019).
[6] D. Panario, D. Thomson, G. L. Mullen andS. Huczynska, Existence and properties of k-normal elements over finite fields, *Finite Fields and Their Applications*, vol. 24, pp. 170–183, (2013).
[7] D. Thomson and L. Reis, Existence of primitive 1-normal elements in finite fields, *Finite Fields and Their Applications*, vol. 51, pp. 238–269, (2018).
[8] J. Aguirre and V. Neumann, Existence of primitive 2-normal elements in finite fields, *Finite Fields and Their Applications*, vol. 73, p. 101864, 08 (2021).
[9] M. Rani, A. K. Sharma, S. K. Tiwari, and A. Panigrahi, "Inverses of r-primitive k-normal elements over finite fields," *The Ramanujan Journal*, vol. 63, 10 2023.
[10] A. K. Sharma, A. Panigrahi, M. Rani and S. K. Tiwari, On r-primitive k-normal elements with prescribed norm and trace over finite fields, *Finite Fields and Their Applications*, vol. 91, p. 102253, (2023).
[11] J. Aguirre and V. Neumann, Pairs of r-primitive and k-normal elements in finite fields, *Bulletin of the Brazilian Mathematical Society, New Series*, vol. 54, (2023).
[12] Abílio Lemos, Josimar J. R. Aguirre, S. Ribas and Victor G. L. Neumann, r-primitive k-normal elements in arithmetic progressions over finite fields, *Communications in Algebra*, vol. 52, no. 1, pp. 427–442, (2024).
[13] J. Sharma, R. Sarma, and S. Laishram, Arithmetic progressions of r-primitive elements in a field, *Boletim da Sociedade Brasileira de Matemática*, vol. 55, (2024).
[14] L. Carlitz, Sums of primitive roots of the first and second kind in a finite field, *Mathematische Nachrichten*, Vol. 12, no. 3-4, pp. 155–172, 1954.
[15] H. Niederreiter and R. Lidl, Finite Fields and Their Applications, Vol. 20 of *Encyclopedia Of Mathematics And Its Applications*. Cambridge University Press, (1996).
[16] L. Reis, A note on additive characters of finite fields, 05 (2020).
[17] M. Alizadeh, Some notes on the k-normal elements and k-normal polynomials over finite fields, *Journal of Algebra and its Applications*, vol. 16, no. 01, p. 1750006, (2017).
[18] S. Cohen, The orders of related elements of a finite field, *The Ramanujan Journal*, Vol. 7, pp. 169–183, (2003).

Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India.
Email address: maithri1499@gmail.com

Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India.
Email address: vadiraja.bhatta@manipal.edu

Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India.
Email address: indira.kp@manipal.edu