PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 119 (133) (2026), 39–49 DOI: https://doi.org/10.2298/PIM2633039

CHARACTERISTIC FUNCTIONS OF (r, n)-FREE AND (f, g)-ELEMENTS OF FINITE CYCLIC MODULE

Himangshu Hazarika and Dhiren Kumar Basnet

Abstract. Let $\mathfrak{C}_Q$ be a cyclic group of order Q and n is a divisor of Q, while r is a divisor of Q/n; then under some restrictions, an element $\alpha \in \mathfrak{C}_Q$ is called (r, n)-free. Similarly, if $f, g \in \mathbb{F}_q[x]$ are divisors of $x^m - 1$, then under special conditions, an element $\alpha \in \mathbb{F}_{q^m}$ is called (f, g)-free element. We generalize the notions (r, n)-free and (f, g)-free elements to that of a finite cyclic module and establish characteristic functions for these elements.

1. Introduction

The problem of constructing an algorithm to find a primitive element of a finite field is one of the major open problems in finite field theory. Hence, researchers focus on relatively unchallenging problem, i.e., to create an algorithm to find an element of higher multiplicative order. This problem becomes more useful as the elements of higher multiplicative order may replace primitive elements in various applications. One of the notable work of Gao [**2**], who established algorithm for elements of higher order in $\mathbb{F}_{q^m}$ with $m^{\log_q m/(4\log_q(2\log_q m))-1/2}$ as the lower bound of the order. Later Popovych estimated lower bounds on elements of higher multiplicative orders of finite fields in [**3**]. Then Cohen, Kapetanakis and Reis defined (r, n)-free elements for finite fields and studied various properties of (r, n)-free elements in [**1**]. They provided the characteristic function for the (r, n)-free elements, which is an extension of Vinogradov's formula for the characteristic function for primitive elements, wherefrom we generalise the notions of (r, n)-free and (f, g)-free elements to that of a finite cyclic module. Next we find the characteristic functions and prove some results for (r, n)-free and (f, g)-free elements of a finite cyclic module.

We begin this article with the preparation Section 2 consisting of basic materials. Next we study finite cyclic R-module in Section 3. Then we establish some results with additive module in Section 4. In Section 5 we define (f, g)-free elements and provide some properties. Finally, in Section 6, we define (f, g)-freeness of elements through polynomial values and establish some additional results.

2020 *Mathematics Subject Classification:* 11T30; 11A07; 11T23.
Key words and phrases: finite fields, character sums, elliptic curves.
Communicated by Stevan Pilipović.

2. Preliminaries

DEFINITION 2.1. If $n \mid q^m - 1$, then an element $\alpha \in \mathbb{F}_{q^m}$ is called *n-primitive* element, if it is of order $(q^m - 1)/n$. So primitive elements are nothing but 1-primitive elements.

The characteristic function of n-free elements is given by Carlitz in [**4**], as following.

LEMMA 2.1. *If M is a divisor of $q^m - 1$, the characteristic function for the set of elements with multiplicative order M in $\mathbb{F}_{q^m}$ is*

$$\Psi_M(\alpha) = \frac{M}{q^m - 1} \sum_{d|M} \frac{\mu(d)}{d} \sum_{\mathrm{ord}(\kappa)|\frac{d(q^m-1)}{M}} \kappa(\alpha),$$

where the sum runs over all the characters κ such that $\mathrm{ord}(\kappa)$ *divides $d(q^m-1)/M$.*

For a multiplicative cyclic group, Cohen et al. provided the following result.

LEMMA 2.2. [**1**, Lemma 2.5] *For positive integers r and n,*

$$T(r,n) := \sum_{l|r} \frac{|\mu(l_{(n)})|}{\phi(l_{(n)})} \phi(l) = \gcd(r,n)\, W(\gcd(r, r_{(n)})),$$

where $W(k)$ is the number of square-free divisors of k and $x_{(y)} = \frac{x}{\gcd(x,y)}$.

2.1. (r,n)-free elements. The following concepts are provided by Cohen, Kapetanakis and Reis in [**1**].

DEFINITION 2.2. Let $\mathfrak{C}_Q$ denote a multiplicative cyclic group of order Q. Let n be a divisor of Q and r be a divisor of Q/n. Then an element $\alpha \in \mathfrak{C}_Q$ is called (r,n)-free if the following hold:

(i) α is in the subgroup $\mathfrak{C}_{Q/n}$, i.e., $\mathrm{ord}(\alpha) \mid \frac{Q}{n}$;
(ii) α is r-free in $\mathfrak{C}_{Q/n}$, i.e., if $\alpha = \beta^a$ with $\beta \in \mathfrak{C}_{Q/n}$ and $a \mid r$, then $a = 1$.

LEMMA 2.3. [**1**, Lemma 3.3] *Let n be a divisor of Q and r be a divisor of Q/n. An element $\alpha \in \mathfrak{C}_Q$ is (r,n)-free if and only if $\alpha = \beta^n$ for some $\beta \in \mathfrak{C}_Q$, but α is not of the form β_0^{np} where $\beta_0 \in \mathfrak{C}_Q$, for every prime divisor p of r. In particular, $\alpha \in \mathfrak{C}_Q$ is (r,n)-free if and only if* $\gcd\left(rn, \frac{Q}{\mathrm{ord}(\alpha)}\right) = n$.

3. Finite cyclic R-module

Let R be a Euclidean domain and $\mathbf{M}$ be a finite cyclic R-module, under the rule $r \circ \alpha$, where $r \in R$ and $\alpha \in \mathbf{M}$. Let $g \in \mathbf{M}$ be a generator of $\mathbf{M}$. Since $\mathbf{M}$ has similar properties as Abelian group, hence $\widehat{\mathbf{M}}$ can be defined as an R-module, under the rule, $r \circ \psi : \alpha \mapsto \psi(r \circ \alpha)$, for $\alpha \in \mathbf{M}$ and $\psi \in \widehat{\mathbf{M}}$. Note that, whenever a character sum runs through the divisors of orders of some element of R, or when a condition is applicable to all the members of a conjugacy class of $R/\sim$, we will consider just one representative, as an element of R will be treated as the same with its conjugates that hold the equivalence relation $r \sim s \Leftrightarrow r = us$, for some $u \in R^*$.

For $\alpha \in \mathbf{M}$, we have that the annihilator of α is an ideal of R, hence it has a unique generator. This annihilator is called the *order* of α and we denote it with $\mathrm{ord}(\alpha)$. We set $m := \mathrm{ord}(g)$.

For $d \in R$, the Euler function is defined as $\phi(d) = |(R/dR)^*|$. For $a, b \in R$, we denote $a_{(b)}$ as $a_{(b)} = \frac{a}{\gcd(a,b)}$.

LEMMA 3.1. *Let $r \in R$ and b be a divisor of m. An element $\alpha \in \mathbf{M}$ is of the form $r \circ \beta$ with $\mathrm{ord}(\beta) = b$ if and only if $\mathrm{ord}(\alpha) = b_{(n)}$, where $n = \gcd(r, m)$.*

PROOF. ($\Rightarrow$) Let $\alpha \in \mathbf{M}$ be of the form $r \circ \beta$ with $\mathrm{ord}(\beta) = b$. Then b is a generator of the ideal (annihilator of β) in R. Then $\alpha = r \circ \beta$ has order $\frac{b}{\gcd(b,r)} = \frac{b}{\gcd(b,n)} = b_{(n)}$.

($\Leftarrow$) Let $\mathrm{ord}(\alpha) = b_{(n)}$, where $n = \gcd(r, m)$. To show $\alpha \in \mathbf{M}$ is of the form $r \circ \beta$ with $\mathrm{ord}(\beta) = b$. Consider the set $A_b = \{r \circ \beta \mid \mathrm{ord}(\beta) = b\}$. Then the cardinality of the set is $\phi(b_{(n)})$. Now for any element δ of order b, the elements of A_b are $i \circ (r \circ \delta) = (ir) \circ \delta$, where $\gcd(i, b) = 1$. So we have, $(ir) \circ \delta = (jr) \circ \delta$ if and only if $i = j + yb_{(n)}$, for some $y \in R$, i.e., $i \equiv j \pmod{b_{(n)}}$. (This mod is analogous to *natural mod.*)

Therefore the cardinality of A_b is the number of in-congruent $x \pmod{b_{(n)}}$, as $x \in R$ such that $\gcd(x, b) = 1$. Since $b_{(n)}$ divides b, hence the cardinality is $\phi(b_{(n)})$. □

LEMMA 3.2. *For $n, r \in R$, we have*

$$T(r,n) := \sum_{t|r} \frac{|\mu(t_{(n)})|}{\phi(t_{(n)})}\, \phi(t) = |(R/\alpha R)|\, W(|(R/\beta R)|),$$

where $\alpha = \gcd(n, r)$, $\beta = \gcd(r, r_{(n)})$ and $W(a)$ denotes the number of square free divisors of a.

PROOF. We have $f_n(r) := \frac{|\mu(t_{(n)})|}{\phi(t_{(n)})}\phi(t)$ and $g_n(r) := |(R/\alpha R), W(|(R/\beta R)|)$, are multiplicative functions in R. Hence the same holds for $T(n, r)$ and thus it suffices to prove the equality $T(n, r) = g_n(r)$ in the case, where r is a prime power in R. We use $r = p^a$, where p is a prime in R and $a \in \mathbb{N}$, and write $n = p^b n_0$, where b is an integer with $b \geqslant 0$ and $\gcd(p, n_0) = 1$. Now we have the following cases

(i) If $b = 0$, then $\gcd(r, n) = 1$, $r_{(n)} = r$ i.e., $\alpha = 1$, $\beta = r$.

$$T(n,r) = \sum_{t|r} \frac{|\mu(t_{(n)})|}{\phi(t_{(n)})}\, \phi(t) = \phi(1) + \frac{|\mu(p)|}{\phi(p)}\phi(p) = 2,$$

$$g_n(r) = |(R/R)|\, W(|(R/p^a R)|) = W(|(R/pR)|^a) = W(|(R/pR)|) = 2.$$

(ii) If $0 < b \leqslant a$, then $\gcd(n, r) = p^b$ and $r_{(n)} = p^{a-b}$, i.e., $\alpha = p^b$ and $\beta = p^{a-b}$ if $b < a$, $\beta = 1$ if $b = a$. Then for $b < a$,

$$T(n,r) = \sum_{i=0}^{b} \phi(p^i) + \sum_{i=b+1}^{a} \frac{|\mu(p^{i-b})|}{\phi(p^{i-b})}\phi(p^i)$$

$$= \sum_{i=0}^{b} \phi(p^i) + \frac{1}{\phi(p)}\phi(p^{b+1}) = 2|(R/p^bR)|.$$

If $b = a$, then $T(n, r) = |(R/p^bR)|$. If $b < a$, then $\alpha = p^b$ and $\beta = p^{a-b}$. Hence

$$\begin{aligned} g_n(r) &= |(R/p^bR)|\, W(|(R/p^{a-b}R)|) = |(R/p^bR)|\, W(|(R/pR)|^{a-b}) \\ &= |(R/p^bR)|\, W(|(R/pR)|) = 2|(R/p^bR)|. \end{aligned}$$

Similarly, when $b = a$ then $\alpha = p^b$ and $\beta = 1$. In this case $g_n(r) = |(R/p^bR)|$.

(iii) If $b > a$, then $\gcd(n, r) = p^a$ and $r_{(n)} = 1$, i.e., $\alpha = p^a$, $\beta = 1$. Then $T(n, r) = \sum_{i=0}^{a} \frac{|\mu(i)|}{\phi(i)}\phi(p^i) = |(R/p^aR)|$. For $\alpha = p^a$, $\beta = 1$, $g_n(r) = |(R/p^aR)|$. □

Next we have the characteristic function for the set of elements in $\mathbf{M}$ of order n.

LEMMA 3.3. [**1**, Lemma 3.4] *If $n \mid m$, then the characteristic function for the set of elements in $\mathbf{M}$ of order n is*

$$\Lambda_n(\omega) = \frac{|(R/nR)|}{|\mathbf{M}|} \sum_{d|n} \frac{\mu(n)}{|(R/dR)|} \sum_{\mathrm{ord}(\chi)=d} \chi(\omega).$$

LEMMA 3.4. *For $r = m/n$ where $n \mid m$, the above function can be rewritten as*

$$\Lambda_n(\omega) = \frac{\phi(m/n)}{|\mathbf{M}|} \sum_{t|m} \frac{\mu(t_{(n)})}{\phi(t_{(n)})} \sum_{\mathrm{ord}(\chi)=t} \chi(\omega).$$

3.1. Generalized (r, n)-free elements.

DEFINITION 3.1. Let r and n be two divisors of m. An element $x \in \mathbf{M}$ is called (r, n)-free if $\mathrm{ord}(a) \mid \frac{m}{\gcd(r,n)}$ and if $x = d \circ y$ for some $y \in \mathbf{M}$ with $\mathrm{ord}(y) \mid \frac{m}{\gcd(r,n)}$ and $d | r_{(n)}$, implies $d = 1$.

LEMMA 3.5. *Let r, n be two divisors of m and $a \in \mathbf{M}$ such that* $\mathrm{ord}(a) \mid \frac{m}{\gcd(r,n)}$. *Then a is (r, n)-free if and only if* $\gcd(r, n) = \gcd\left(r, \frac{m}{\mathrm{ord}(a)}\right)$.

PROOF. Clearly it suffices to prove that $\gcd\left(r_{(n)}, \frac{m}{\gcd(r,n)\,\mathrm{ord}(a)}\right) = 1$. We take $b \in \mathbf{M}$ of order $\frac{m}{\gcd(r,m)}$. Then $a = k \circ b$ for some $k \in R$, while $\mathrm{ord}(a) = \left(\frac{m}{\gcd(r,n)\,\gcd(k,\, m/\gcd(r,n))}\right)$.

($\Rightarrow$) Let a be (r, n)-free such that $\gcd\left(r_{(n)}, \frac{m}{\gcd(r,n)\,\mathrm{ord}(a)}\right) \neq 1$. Then

$$\gcd\left(r_{(n)}, \gcd\left(k, \frac{m}{\gcd(r,n)}\right)\right) \neq 1, \quad \text{i.e.,} \quad \gcd\left(r_{(n)}, k, \frac{m}{\gcd(r,n)}\right) \neq 1,$$

i.e., $k = k_0k_1$ for some $k_0 \in R$ such that $k_0 \neq 1$ and $k_0 \mid \gcd\left(r_{(n)}, \frac{m}{\gcd(r,n)}\right)$.

Thus $a = k \circ b = (k_0k_1) \circ b = k_0 \circ (k_1 \circ b)$. Since a is (r, n)-free, this implies $k_0 = 1$, a contradiction.

($\Leftarrow$) Let $\gcd\left(r_{(n)}, \frac{m}{\gcd(r,n)\,\mathrm{ord}(a)}\right) = 1$. Take some $\beta \in \mathbf{M}$ such that $\mathrm{ord}(\beta) \mid \frac{m}{\gcd(r,\, n)}$ $a = d \circ \beta$ and $d \mid r_{(n)}$. It suffices to show that $d = 1$. First we have $\beta = i \circ b$, for some $i \in R$. It follows that $a = k \circ b = d \circ (i \circ b) = (di) \circ b$. Now $\mathrm{ord}(b) = \frac{m}{\gcd(r,\, n)}$

and $k \circ b = (di) \circ b$, where $b \in \mathbf{M}$ and $k, di \in R$. Since R is ED, there exists $t \in R$ such that $k = di + t\frac{m}{\gcd(r,n)}$. Since $d \mid di$ and $d \mid \frac{m}{\gcd(r,n)}$, hence $d \mid k$. We have $\gcd\left(r_{(n)}, \frac{m}{\gcd(r,n)\,\mathrm{ord}(a)}\right) = 1$ i.e., $\gcd\left(r_{(n)}, k, \frac{m}{\gcd(r,n)}\right) = 1$ and combining the facts that $d \mid k$ and $d \mid \frac{m}{\gcd(r,n)}$ we get $d = 1$. □

LEMMA 3.6. *Let $t \mid m$ and $x \in \mathbf{M}$. Then*

$$\sum_{\mathrm{ord}(\chi)\mid t} \chi(x) = \begin{cases} |(R/tR)|, & \text{if } t \mid \frac{m}{\mathrm{ord}(x)}, \\ 0, & \text{otherwise.} \end{cases}$$

This can be proved from orthogonality relations.

Finally, we define the characteristic function for the set of (r,n)-free elements in $\mathbf{M}$ by

$$\Lambda_{r,n}(x) = \frac{\phi(r_{(n)})}{|(R/rR)|} \sum_{t\mid r} \frac{\mu(t_{(n)})}{\phi(t_{(n)})} \sum_{\mathrm{ord}(\chi)=t} \chi(x), \quad x \in \mathbf{M},$$

as character sum expression.

We prove the following lemma to support our claim.

LEMMA 3.7. *Let $x \in \mathbf{M}$, then* $\Lambda_{r,n}(x) = \begin{cases} 1, & \text{if } x \text{ is } (r,n)\text{-free}, \\ 0, & \text{otherwise.} \end{cases}$

PROOF. Let $r = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be a prime factorisation of r in R and $e_i \geqslant 1$. It follows from the definition that ω is (r,n)-free if and only if it is $(p_i^{e_i}, n)$-free for each $i = 1, 2, \ldots, k$. Moreover we have $\Lambda_{e_1e_2,n}(\omega) = \Lambda_{e_1,n}(\omega)\Lambda_{e_2,n}(\omega)$. It follows that it suffices to restrict our case to $r = p^s$, where p is irreducible in R and $s \neq 0$.

Consider the case $p^s \nmid n$; then $\gcd(p^s, n) = p^t$, for some $0 \leqslant t < s$. So $p^s_{(n)} = p^{s-t}$. Further

$$\Lambda_{p^s,n}(\omega) = \frac{\phi(p^s_{(n)})}{|(R/p^sR)|} \sum_{i=0}^{s} \frac{\mu(p^i_{(n)})}{\phi(p^i_{(n)})} \sum_{\mathrm{ord}(\psi)=p^i} \psi(\omega).$$

Now

$$\begin{aligned} \sum_{i=0}^{s} \frac{\mu(p^i_{(n)})}{\phi(p^i_{(n)})} \sum_{\mathrm{ord}(\psi)=p^i} \psi(\omega) &= \sum_{i=0}^{t} \frac{\mu(p^i_{(n)})}{\phi(p^i_{(n)})} \sum_{\mathrm{ord}(\psi)=p^i} \psi(\omega) + \frac{\mu(p^{t+1}_{(n)})}{\phi(p^{t+1}_{(n)})} \sum_{\mathrm{ord}(\psi)=p^{t+1}} \psi(\omega) \\ &= \sum_{i=0}^{t} \sum_{\mathrm{ord}(\psi)=p^i} \psi(\omega) - \frac{1}{\phi(p)} \sum_{\mathrm{ord}(\phi)=p^{t+1}} \psi(\omega) \\ &= \sum_{\mathrm{ord}(\psi)\mid p^t} \psi(\omega) - \frac{1}{\phi(p)} \sum_{\mathrm{ord}(\psi)=p^{t+1}} \psi(\omega). \end{aligned}$$

Hence

$$\Lambda_{p^s,n}(\omega) = \frac{\phi(p^s_{(n)})}{|(R/p^sR)|} \left(\sum_{\mathrm{ord}(\psi)\mid p^t} \psi(\omega) - \frac{1}{\phi(p)} \sum_{\mathrm{ord}(\psi)=p^{t+1}} \psi(\omega) \right). \tag{3.1}$$

Let $\nu_p(g)$ stands for the exponent of the prime p in the prime factorisation of g. Now ω is (p^s,n)-free if and only if $t=\nu_p(m)-\nu_p(\mathrm{ord}(\omega))$. If ω is (p^s,n)-free, then the above equality and Lemma 3.6 imply that

$$\sum_{\mathrm{ord}(\chi)|p^t}\chi(\omega)=|(R/p^sR)| \quad \text{and} \quad \sum_{\mathrm{ord}(\chi)|p^{t+1}}\chi(\omega)=0,$$

which yield $\sum_{\mathrm{ord}(\chi)=p^{t+1}}\chi(\omega)=-|(R/p^sR)|$. Now, by (3.1), we have $\Lambda_{p^s,n}(\omega)=1$.

Assume that ω is not (p^s,n)-free. This means $t>\nu_p(m)-\nu_p(\mathrm{ord}(\omega))$ or $t<\nu_p(m)-\nu_p(\mathrm{ord}(\omega))$. For the case $t>\nu_p(m)-\nu_p(\mathrm{ord}(\omega))$, we have $p^t\nmid\frac{m}{\mathrm{ord}(\omega)}$. By Lemma 3.6, we have $\sum_{\mathrm{ord}(\chi)|p^t}\chi(\omega)=\sum_{\mathrm{ord}(\chi)=p^{t+1}}\chi(\omega)=0$. Hence from (3.1), $\Lambda_{p^s,n}=0$.

Finally if $t<\nu_p(m)-\nu_p(\mathrm{ord}(\omega))$, by Lemma 3.6, we have

$$\sum_{\mathrm{ord}(\chi)|p^t}\chi(\omega)=|(R/p^tR)| \quad \text{and} \quad \sum_{\mathrm{ord}(\chi)=p^{t+1}}\chi(\omega)=\phi(p^{t+1})=|(R/p^tR)|\Big(1-\frac{1}{|(R/pR)|}\Big).$$

Now, we discuss the case $p^s|n$, then $\gcd(p^s,n)=p^s$ and $p^s_{(n)}=1$.

$$\Lambda_{p^s,n}(\omega)=\frac{\phi(p^s_{(n)})}{|(R/p^tR)|}\sum_{i=0}^{s}\frac{\mu(p^i_{(n)})}{\phi(p^i_{(n)})}\sum_{\mathrm{ord}(\chi)=p^i}\chi(\omega)=\frac{1}{|(R/p^tR)|}\sum_{\mathrm{ord}(\chi)|p^s}\chi(\omega). \tag{3.2}$$

In this case ω is (p^s,n)-free if and only if $p^s|\frac{m}{\mathrm{ord}(\omega)}$. Along with this and from Lemma 3.6, we have that $\Lambda_{p^s,n}(\omega)=1$ if ω is (p^s,n)-free and $\Lambda_{p^s,n}(\omega)=0$, otherwise. □

4. Additive module

The additive group of $\mathbb{F}_{q^m}$ can be viewed as an $\mathbb{F}_q[x]$-module $\mathfrak{F}\circ\alpha:=\sum_{i=0}^{n}F_i\alpha^{q^i}$, where $\mathfrak{F}(x)=\sum_{i=0}^{n}F_ix^i\in\mathbb{F}_q[x]$. From the normal basis theorem, it is clear that the $\mathbb{F}_q[x]$-module is cyclic, and normal elements or free elements are generators of the module.

Throughout this section, $\mathrm{Ord}(\alpha)$ will denote the additive order of $\alpha\in\mathbb{F}_{q^m}$, i.e., $\mathrm{Ord}(\alpha)$ is the $\mathbb{F}_q$-order of α in $\mathbb{F}_q[x]$-module. For any element α in some extension of $\mathbb{F}_q$, $(x^m-1)\circ\alpha=\alpha^{q^m}-\alpha=0$ if and only if $\alpha\in\mathbb{F}_{q^m}$. If we set $I_\alpha=\{g(x)\in\mathbb{F}_q[x]\mid g\circ\alpha=0\}$, then I_α is an ideal of $\mathbb{F}_q[x]$ and hence generated by a polynomial, say $h_\alpha(x)$ (we require $h_\alpha(x)$ to be monic). Then $h_\alpha(x)$ is the $\mathbb{F}_q$-order of α. It is clear that $\mathrm{Ord}(\alpha)\in\mathbb{F}_q[x]$ and $\mathrm{Ord}(\alpha)\mid x^m-1$.

For $f,g\in\mathbb{F}_q[x]$, we denote $f_{(g)}$ as $f_{(g)}=\frac{f}{\gcd(f,g)}$.

If $f\in\mathbb{F}_q[x]$, $f=\sum_{i=0}^{s}a_ix^i$, we define $L_f(x)=\sum_{i=0}^{s}a_ix^{q^i}$ as q-associate of f. Also for $\alpha\in\mathbb{F}_{q^m}$, let $f\circ\alpha=L_f(\alpha)=\sum_{i=0}^{s}a_i\alpha^{q^i}$. For $f,g\in\mathbb{F}_q[x]$, the following hold: (i) $L_f(L_g(x))=L_{fg}(x)$, (ii) $L_f(x)+L_g(x)=L_{f+g}(x)$.

Lemma 4.1. *Let $f,g\in\mathbb{F}_q[x]$ be divisors of x^m-1. An element $\alpha\in\mathbb{F}_{q^m}$ is of the form $f\circ\beta$ with $\mathrm{Ord}(\beta)=g$ if and only if $\mathrm{Ord}(\alpha)=g_{(h)}$, where $h=\gcd(f,x^m-1)$.*

Proof is similar to that of Lemma 3.1.

LEMMA 4.2. *Let $f, g \in \mathbb{F}_{q^m}[x]$, then we have*

$$T(f,g) := \sum_{t|f} \frac{|\mu(t_{(g)})|}{\Phi(t_{(g)})}\,\Phi(t) = \Big|\frac{\mathbb{F}_q[x]}{l\mathbb{F}_q[x]}\Big|\,W\Big(\Big|\frac{\mathbb{F}_q[x]}{h\mathbb{F}_q[x]}\Big|\Big) = \big(q^{\deg(l)}\big)\,W\big(q^{\deg(h)}\big),$$

where $l = \gcd(f,g)$, $h = \gcd(f, f_{(g)})$, and $W(n)$ is the number of square free divisors of n.

Proof is similar to that of Lemma 3.2.

5. (f,g)-free element

DEFINITION 5.1. Let $f, g \in \mathbb{F}_q[x]$ be divisors of $x^m - 1$. An element $\alpha \in \mathbb{F}_{q^m}$ is called (f,g)-free if $\mathrm{Ord}(\alpha) \mid \frac{x^m-1}{\gcd(f,g)}$ and $\alpha = h \circ \beta$, for some $\beta \in \mathbb{F}_{q^m}$ with $\mathrm{Ord}(\beta) \mid \frac{x^m-1}{\gcd(f,g)}$ and $h \mid f_{(g)}$, imply $h = 1$.

We have the following.

LEMMA 5.1. *Let f, $g \in \mathbb{F}_q[x]$ be divisors of $x^m - 1$. Let $\alpha \in \mathbb{F}_{q^m}$ be such that $\mathrm{Ord}(\alpha) \mid \frac{x^m-1}{\gcd(f,g)}$. Then α is (f,g)-free if and only if $\gcd(f,g) = \gcd\big(f, \frac{x^m-1}{\mathrm{Ord}(\alpha)}\big)$.*

Proof is similar to that of Lemma 3.5.

LEMMA 5.2. *Let $t \mid x^m - 1$ and take some $\omega \in \mathbb{F}_{q^m}$. Then*

$$\sum_{\mathrm{Ord}(\psi)|t} \psi(\omega) = \begin{cases} |t\mathbb{F}_q[x]| \text{ or } q^{\deg(t)}, & \text{if } t \mid \frac{x^m-1}{\mathrm{Ord}(\omega)}, \\ 0, & \text{otherwise.} \end{cases}$$

DEFINITION 5.2. Now we define the function

$$\Omega_{f,g}(\omega) = \frac{\Phi(f_{(g)})}{q^{\deg(f)}} \sum_{h|f} \frac{\mu(h_{(g)})}{\Phi(h_{(g)})} \sum_{\mathrm{Ord}(\psi)=h} \psi(\omega), \quad \omega \in \mathbb{F}_{q^m}$$

as the characteristic function for (f,g)-free elements of $\mathbb{F}_{q^m}$.

The following lemma establishes the above definition.

LEMMA 5.3. *Let $\omega \in \mathbb{F}_{q^m}$, then $\Omega_{f,g}(\omega) = \begin{cases} 1, & \text{if } \omega \text{ is } (f,g)\text{-free}, \\ 0, & \text{otherwise.} \end{cases}$*

Proof is similar to that of Lemma 3.7.

6. (f,g)-freeness through polynomial values

For divisors f, F, g, G of $x^m - 1$ and polynomials $h, H \in \mathbb{F}_{q^m}[x]$, we study the number of pairs $(h(y), H(y))$ such that $h(y)$ is (f,g)-free and $H(y)$ is (F,G)-free with $y \in \mathbb{F}_{q^m}$. This number can be zero if $h(x)$ and $H(x)$ have certain additive dependence with respect to the polynomials f, F.

DEFINITION 6.1. Let $f, F \in \mathbb{F}_{q^m}[x]$ be divisors of $x^m - 1$ and let $h, H \in \mathbb{F}_{q^m}[x]$ be nonconstant polynomials. The pair (h, H) is (f, F)-independent if for every $t \mid f$ and $T \mid F$ with $l = \operatorname{lcm}(t, T) \neq 1$ (we choose t, T to be monic) and $1 \leqslant \deg(c) \leqslant \deg(t)$ and $1 \leqslant \deg(C) \leqslant \deg(T)$ with $\gcd(t, c) = \gcd(T, C) = 1$, the polynomial $L_{\frac{lc}{t}}(h(x)) + L_{\frac{lC}{T}}(H(x))$ is not of the form $L_l(g(x)) + k$, for some $g \in \mathbb{F}_q[x]$ and $k \in \mathbb{F}_{q^m}$.

PROPOSITION 6.1. *With the terms and conditions as above, if* $\mathfrak{G}(x) = L_{\frac{lc}{t}}(h(x)) + L_{\frac{lC}{T}}(H(x))$ *is not of the form* $L_l(g(x)) + k$ *for any* $g(x) \in \mathbb{F}_q[x]$ *and for any* $k \in \mathbb{F}_{q^m}$*, then* $\mathfrak{G}(x)$ *is definitely not of the form* $a(x)^p - a(x) + b$*, for any* $a(x) \in \mathbb{F}_q[x]$ *and* $b \in \mathbb{F}_{q^m}$*, where* $q = p^n$ *for some positive integer* n*.*

LEMMA 6.1. *Let* $f, F \in \mathbb{F}_{q^m}[x]$ *be divisors of* $x^m - 1$*. If the pair* (h, H) *is not* (f, F)*-independent, then there exist divisors* $r, R \in \mathbb{F}_{q^m}[x]$ *of* $x^m - 1$ *such that there is no element* $\theta \in \mathbb{F}_{q^m}$ *with* $h(\theta)$ *is* (f, r)*-free and* $H(\theta)$ *is* (F, R)*-free.*

PROOF. Since (h, H) is not (f, F)-independent, there exist some $t \mid f$ and $T \mid F$ with $l = \operatorname{lcm}(t, T) \neq 1$ and $1 \leqslant \deg(c) \leqslant \deg(t)$ and $1 \leqslant \deg(C) \leqslant \deg(T)$ with $\gcd(t, c) = \gcd(T, C) = 1$, such that for some $g \in \mathbb{F}_{q^m}[x]$ and $k \in \mathbb{F}_{q^m}[x]$

$$L_{\frac{lc}{t}}(h(x)) + L_{\frac{lC}{T}}(H(x)) = L_l(g(x)) + k.$$

Then for every $\theta \in \mathbb{F}_{q^m}$ we have $\left(\frac{lc}{t}\right) \circ h(\theta) + \left(\frac{lC}{T}\right) \circ H(\theta) = l \circ g(\theta) + k$. Then multiplying by $\frac{x^m-1}{l}$ we have

$$\frac{(x^m - 1)c}{t} \circ h(\theta) + \frac{(x^m - 1)C}{T} \circ H(\theta) = \left(\frac{x^m - 1}{l}\right) \circ k. \tag{6.1}$$

First we consider the case $t \neq T$ (we have already chosen t, T as monic). From (6.1), dividing by T and t we have

$$\frac{T(x^m - 1)c}{t} \circ h(\theta) = \frac{T(x^m - 1)}{l} \circ k \text{ and } \frac{t(x^m - 1)C}{T} \circ H(\theta) = \frac{t(x^m - 1)}{l} \circ k$$

respectively. Since right hand sides are inverses of one another, hence we have

$$\frac{\operatorname{Ord}(h(\theta))}{\gcd(\operatorname{Ord}(h(\theta)), \frac{x^m-1}{t}Tc)} = \frac{\operatorname{Ord}(H(\theta))}{\gcd(\operatorname{Ord}(H(\theta)), \frac{x^m-1}{T}tC)}$$
$$\Leftrightarrow t \gcd\left(T, \frac{x^m - 1}{\operatorname{Ord}(H(\theta))}tC\right) = T \gcd\left(t, \frac{x^m - 1}{\operatorname{Ord}(h(\theta))}Tc\right).$$

We divide both the parts of above by $\gcd(t, T)$ and get

$$t \gcd\left(T_{(t)}, \frac{x^m - 1}{\operatorname{Ord}(H(\theta))}t_{(T)}C\right) = T \gcd\left(t_{(T)}, \frac{x^m - 1}{\operatorname{Ord}(h(\theta))}T_{(t)}c\right).$$

Since $\gcd(t_{(T)}, T_{(t)}.c) = \gcd(T_{(t)}, t_{(T)}.C) = 1$, the above equation becomes

$$t \gcd\left(T_{(t)}, \frac{x^m - 1}{\operatorname{Ord}(H(\theta))}\right) = T \gcd\left(t_{(T)}, \frac{x^m - 1}{\operatorname{Ord}(h(\theta))}\right). \tag{6.2}$$

If possible let there exist some $\theta \in \mathbb{F}_{q^m}$, such that $h(\theta)$ is (f, r)-free and $H(\theta)$ is (F, R)-free, for some divisors $r, R \in \mathbb{F}_{q^m}[x]$ of $x^m - 1$. Using Lemma 5.1, we have

$\gcd\left(f, \frac{x^m-1}{\mathrm{Ord}(h(\theta))}\right) = \gcd(f,r)$. Then combining this with the fact that $t_{(T)}|f$, we have that $\gcd\left(t_{(T)}, \frac{x^m-1}{\mathrm{Ord}(h(\theta))}\right) = \gcd(t_{(T)}, r)$. Similarly we have

$$\gcd\left(T_{(t)}, \frac{x^m-1}{\mathrm{Ord}(H(\theta))}\right) = \gcd(T_{(t)}, R).$$

Then (6.2) gives

$$t\gcd(T_{(t)}, R) = T\gcd(t_{(T)}, r). \tag{6.3}$$

Since $t \neq T$, without loss of generality we assume that there is some non constant monic polynomial $d \in \mathbb{F}_{q^m}[x]$ such that $d|t_{(T)}$. Now we choose $R = T_{(t)}$ and $r = \frac{t_{(T)}}{d}$, then (6.3) yields $\frac{tT}{\gcd(t,T)} = \frac{tT}{d\ \gcd(t,T)}$, a contradiction.

Now we have the case $t = T$. In this case, (6.1) becomes

$$\frac{(x^m-1)c}{l} \circ h(\theta) + \frac{(x^m-1)C}{l} \circ H(\theta) = \frac{(x^m-1)}{l} \circ k.$$

Let us set $r = R = l$. In this case if $h(\theta)$ is (f,l)-free, then its $\mathbb{F}_q$-order divides $\frac{x^m-1}{l}$, hence $\frac{(x^m-1)c}{l} \circ h(\theta) = 0$. Similarly $\frac{(x^m-1)C}{l} \circ H(\theta) = 0$ and hence their sum must be zero i.e., $\frac{x^m-1}{l} \circ k = 0$. Then identical arguments lead us to (6.3),

$$t\gcd(T,R) = T\gcd(t,r).$$

Since $\mathrm{lcm}(t,T)$ is nonconstant monic polynomial in $\mathbb{F}_{q^m}[x]$, hence without loss of generality we may assume that there exists some nonconstant $e \in \mathbb{F}_{q^m}[x]$ such that $e \mid t$. Now we choose $R = T$ and $r = \frac{t}{e}$; then above yields $tT = \frac{tT}{e}$, a contradiction. □

THEOREM 6.1. *Let f, F, r, $R \in \mathbb{F}_{q^m}[x]$ be divisors of $x^m - 1$ and for h, $H \in \mathbb{F}_{q^m}[x]$, the pair (h,H) is (f,F)-independent. Let $D+1 \geqslant 1$ be the number of distinct roots of $h(x)+H(x)$ in its splitting field over $\mathbb{F}_q$. The number $\mathbf{N}_{h,H} = \mathbf{N}_{h,H}(f,F,r,R)$ of elements $\theta \in \mathbb{F}_{q^m}$ such that $h(\theta)$ is (f,r)-free and $H(\theta)$ is (F,R)-free satisfy*

$$\mathbf{N}_{h,H} = \frac{\Phi(f_{(r)})\Phi(F_{(R)})}{q^{\deg(f)}q^{\deg(F)}}\left(q + M(f,r,F,R)\right)$$

with $|M(f,r,F,R)| \leqslant Dq^{m/2}Q_{f,r}Q_{F,R}$, where $Q_{g,h} := \left|\frac{\mathbb{F}_q[x]}{\langle k\rangle}\right| W\left(\left|\frac{\mathbb{F}_q[x]}{\langle y\rangle}\right|\right)$ with $k = gcd(g,h)$, $y = \gcd(g, g_{(h)})$.

PROOF. By definition we have, $\mathbf{N}_{h,H} = \sum_{\omega\in\mathbb{F}_{q^m}} \Omega_{f,r}(h(\omega))\Omega_{F,R}(H(\omega))$. From the characteristic function Ω, for $A = \frac{\Phi(f_{(r)})\Phi(F_{(R)})}{q^{\deg(f)}q^{\deg(F)}}$ we have that

$$\begin{aligned}\mathbf{N}_{h,H}/A &= \sum_{\omega\in\mathbb{F}_{q^m}} \left(\sum_{t|f} \frac{\mu(t_{(r)})}{\Phi(t_{(r)})} \sum_{\mathrm{Ord}(\psi)=t} \psi(h(\omega))\right)\left(\sum_{T|F} \frac{\mu(T_{(R)})}{\Phi(T_{(R)})} \sum_{\mathrm{Ord}(\kappa)=T} \kappa(H(\omega))\right) \\ &= \sum_{T|F,\, t|f} \frac{\mu(t_{(r)})\mu(T_{(R)})}{\Phi(t_{(r)})\Phi(T_{(R)})} \sum_{\mathrm{Ord}(\kappa)=T,\mathrm{Ord}(\psi)=t} G_{h,H}(\psi,\kappa),\end{aligned}$$

where $G_{h,H} = \sum_{\omega \in \mathbb{F}_{q^m}} \psi(h(\omega))\kappa(H(\omega))$.

Fix $t \mid f$ and $T \mid F$ (we choose t, T to be monic); let ψ, κ be additive characters of $\mathbb{F}_q$-orders t and T respectively, and set $l = \mathrm{lcm}(t, T)$. Then

$$\psi(h(\omega))\kappa(H(\omega)) = \widetilde{\psi}\Big(\Big(\frac{cl}{t}\Big) \circ h(\omega) + \Big(\frac{Cl}{T}\Big) \circ H(\omega)\Big)$$

for some additive character $\widetilde{\psi}$ of $\mathbb{F}_q$-order l and some polynomials c, C such that $1 \leqslant \deg(c) \leqslant \deg(t)$ and $1 \leqslant \deg(C) \leqslant \deg(T)$ with $\gcd(t, c) = \gcd(T, C) = 1$.

Since the pair (h, H) is (f, F)-independent, the polynomial $\mathfrak{G}(x) = L_{\frac{cl}{t}}(h(x)) + L_{\frac{Cl}{T}}(H(x))$ is of the form $L_l(g(x)) + k$ if and only if $l = 1$ i.e., $t = T = 1$. Therefore from Weil's theorem we have $|G_{h,H}(\psi, \kappa)| \leqslant Dq^{m/2}$ whenever $(t, T) = (1, 1)$.

For $t = T = 1$, we observe that ψ and κ are just the trivial additive characters and so $G_{h,H}(\psi, \kappa) = q^m - \varepsilon$, where ε is the number of the roots of $h(x) + H(x)$ defined over $\mathbb{F}_{q^m}$. Since $\varepsilon \leqslant D + 1$, we have $|\mathbf{N}_{h,H}/A - q^m| \leqslant D + 1 + Dq^{m/2}E$ where

$$E = \sum_{\substack{t \mid f, T \mid F \\ (t,T) \neq (1,1)}} \frac{\mu(t_{(r)})\mu(T_{(R)})}{\Phi(t_{(r)})\Phi(T_{(R)})} \sum_{\substack{\mathrm{Ord}(\psi) = t \\ \mathrm{Ord}(\kappa) = T}} \mathbf{1} = T(f, r)T(F, R) - 1.$$

and where $T(f, g)$ is as in Lemma 4.2 and according to the Lemma 6.1, we have the equality $T(f, g) = Q_{f,g}$ and so

$$|\mathbf{N}_{h,H}/A - q^m| \leqslant D + 1 + Dq^{m/2}(Q_{f,r}Q_{F,R} - 1) < Dq^{m/2}Q_{f,r}Q_{F,R}$$

from where the result follows. □

Corollary 6.1. *Let f, F, r, R, h, H be as in the above theorem. If $q^{m/2} \geqslant DQ_{f,r}Q_{F,R}$, then $\mathbf{N}_{h,H} > 0$.*

Acknowlegement. The authors are grateful to Giorgos N. Kapetanakis for his valuable comments and suggestions.

References

1. S. D. Cohen, G. Kapetanakis, L. Reis, *The existence of $\mathbb{F}_q$-primitive points on curves using freeness*, C. R., Math., Acad. Sci. Paris **360** (2022), 641–652.
2. S. Gao, *Elements of provable high orders in finite fields*, Proc. Am. Math. Soc. **127** (1999), 1615–1623.
3. R. Popovych, *Elements of high order in finite fields of the form $\mathbb{F}_q[x]/(x^m - a)$*, Finite Fields Appl. **19** (2013), 86-92.
4. L. Carlitz, *Primitive roots in a finite field*, Trans. Am. Math. Soc. **73** (1952), 373–382.

Department of Mathematics
Tezpur College
Tezpur
India
himangshuhazarika10@gmail.com

Department of Mathematical Sciences
Tezpur University
Tezpur
India
dbasnet@tezu.ernet.in

(Received 06 03 2025)
(Revised 16 02 2026)