Existence of Primitive Normal Pairs with One Prescribed Trace over Finite Fields

Hariom Sharma, R. K. Sharma

Department of Mathematics, Indian Institute of Technology Delhi, New Delhi, 110016, India

Abstract

Given $m, n, q \in \mathbb{N}$ such that q is a prime power and $m \geq 3$, $a \in \mathbb{F}_q$, we establish a sufficient condition for the existence of primitive pair $(\alpha, f(\alpha))$ in $\mathbb{F}_{q^m}$ such that α is normal over $\mathbb{F}_q$ and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^{-1}) = a$, where $f(x) \in \mathbb{F}_{q^m}(x)$ is a rational function of degree sum n. Further, when $n = 2$ and $q = 5^k$ for some $k \in \mathbb{N}$, such a pair definitely exists for all (q, m) apart from at most 20 choices.

Keywords: Finite Fields, Characters, Primitive element, Normal element
2010 Math. Sub. Classification: 12E20, 11T23 [1]

1 Introduction

Given the positive integers m and q such that q is a prime power, $\mathbb{F}_q$ denotes the finite field of order q and $\mathbb{F}_{q^m}$ be the extension of $\mathbb{F}_q$ of degree m. A generator of the cyclic multiplicative group $\mathbb{F}_{q^m}^*$ is known as a *primitive element* of $\mathbb{F}_{q^m}$. For a rational function $f(x) \in \mathbb{F}_{q^m}(x)$ and $\alpha \in \mathbb{F}_{q^m}$, we call a pair $(\alpha, f(\alpha))$ a *primitive pair* in $\mathbb{F}_{q^m}$ if both α and $f(\alpha)$ are primitive elements of $\mathbb{F}_{q^m}$. Further, α is *normal* over $\mathbb{F}_q$ if the set $\{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}\}$ forms a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Also, the *trace* of α over $\mathbb{F}_q$, denoted by $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ is given by $\alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}$.

[1]emails: hariomsharma638@gmail.com (Hariom), rksharmaiitd@gmail.com (Rajendra)

Primitive normal elements play a vital role in coding theory and cryptography [1]. Therefore, study of existence of such elements is an active area of research. We refer to [12] for the existence of primitive and normal elements in finite fields. Existence of both primitive and normal elements simultaneously was first established by Lenstra and Schoof in [11]. Later on, by using sieving techniques, Cohen and Huczynska [7] provided a computer-free proof of it. In 1985, Cohen studied the existence of primitive pair $(\alpha, f(\alpha))$ in $\mathbb{F}_q$ for the rational function $f(x) = x + a, a \in \mathbb{F}_q$. Many more researchers worked in this direction and proved the existence of primitive pair for more general rational function [8, 2, 14, 3]. Additionally, in the fields of even order, Cohen[5] established the existence of primitive pair $(\alpha, f(\alpha))$ in $\mathbb{F}_{q^n}$ such that α is normal over $\mathbb{F}_q$, where $f(x) = \frac{x^2+1}{x}$. Similar result has been obtained in [2] for the rational function $f(x) = \frac{ax^2+bx+c}{dx+e}$. Another interesting problem is to prove the existence of primitive pair with prescribed traces which have been discussed in [13, 10, 15].

In this article, we consider all the conditions simultaneously and prove the existence of primitive pair $(\alpha, f(\alpha))$ in $\mathbb{F}_{q^m}$ such that α is normal over $\mathbb{F}_q$ and for prescribed $a \in \mathbb{F}_q$, $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^{-1}) = a$, where $f(x)$ is more general rational function. To proceed further, we shall use some basic terminology and conventions used in [8]. To say that a non zero polynomial $f(x) \in \mathbb{F}_{q^m}[x]$ has *degree* $n \geq 0$ we mean that $f(x) = a_n x^n + \cdots + a_0$, where $a_n \neq 0$ and write it as $\deg(f) = n$. Next, for a rational function $f(x) = f_1(x)/f_2(x) \in \mathbb{F}_{q^m}(x)$, we always assume that f_1 and f_2 are coprime and degree sum of $f = \deg(f_1) + \deg(f_2)$. Also, we can divide each of f_1 and f_2 by the leading coefficient of f_2 and suppose that f_2 is monic. Further, we say that a rational function $f \in \mathbb{F}_{q^m}(x)$ is exceptional if $f = cx^i g^d$ for some $c \in \mathbb{F}_{q^m}, i \in \mathbb{Z}$(set of integers) and $d > 1$ divides $q^m - 1$ or $f(x) = x^i$ for some $i \in \mathbb{Z}$ such that $\gcd(q^m - 1, i) \neq 1$.

Finally, we introduce some sets which have an important role in this article. For $n_1, n_2 \in \mathbb{N}$, $S_{q,m}(n_1, n_2)$ will be used to denote the set of non exceptional rational functions $f = f_1/f_2 \in \mathbb{F}_{q^m}(x)$ with $\deg(f_1) \leq n_1$ and $\deg(f_2) \leq n_2$, and T_{n_1,n_2} as the set of pairs $(q, m) \in \mathbb{N} \times \mathbb{N}$ such that for any given $f \in S_{q,m}(n_1, n_2)$ and prescribed $a \in \mathbb{F}_q$, $\mathbb{F}_{q^m}$ contains a normal element α with $(\alpha, f(\alpha))$ a primitive pair and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^{-1}) = a$. Define $S_{q,m}(n) = \bigcup\limits_{n_1+n_2=n} S_{q,m}(n_1, n_2)$ and $T_n = \bigcap\limits_{n_1+n_2=n} T_{n_1,n_2}$. By [4], for $m \leq 2$, there does not exist any primitive element α such that $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^{-1}) = 0$. Therefore, we shall assume $m \geq 3$ throughout the article.

In this paper, for $n \in \mathbb{N}$, we take $f(x) \in S_{q,m}(n)$ a general rational function of degree sum n and $a \in \mathbb{F}_q$, and prove the existence of normal element α such that $(\alpha, f(\alpha))$ is a primitive pair in $\mathbb{F}_{q^m}$ and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^{-1}) = a$. To be more precise, in section 3, we obtain a sufficient condition for the existence of such elements in $\mathbb{F}_{q^m}$. In section 4, we further improve the condition by proving a generalization of sieving technique due to Anju and Cohen[6]. In section 5, we demonstrate the application of the results of section 3 and section 4 by working with the finite fields of characteristic 5 and $n = 2$. More precisely, we get a subset of T_2.

2 Preliminaries

In this section, we provide some preliminary notations, definitions and results which are required further in this article. Throughout this article, $m \geq 3$ is an integer, q is an arbitrary prime power and $\mathbb{F}_q$ is a finite field of order q. For each $k(>1) \in \mathbb{N}$, $\omega(k)$ denotes the number of prime divisors of k and $W(k)$ denotes the number of square free divisors of k. Also for $g(x) \in \mathbb{F}_q[x]$, $\Omega_q(g)$ and $W(g)$ denote the number of monic irreducible(over $\mathbb{F}_q$) divisors of g and number of square free divisors of g respectively, i.e., $W(k) = 2^{\omega(k)}$ and $W(g) = 2^{\Omega_q(g)}$.

For a finite abelian group G, a homomorphism χ from G into the multiplicative group $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ is known as a character of G. The set of all characters of G forms a group under multiplication, which is isomorphic to G and is denoted by $\widehat{G}$. Further, the character χ_0, defined as $\chi_0(g) = 1$ for all $g \in G$ is called the trivial character of G. The order of a character χ is the smallest positive integer r such that $\chi^r = \chi_0$. For a finite field $\mathbb{F}_{q^m}$, the characters of the additive group $\mathbb{F}_{q^m}$ and the multiplicative group $\mathbb{F}_{q^m}^*$ are called additive characters and multiplicative characters respectively. A multiplicative character $\chi \in \widehat{\mathbb{F}}_{q^m}^*$ is extended from $\mathbb{F}_{q^m}^*$ to $\mathbb{F}_{q^m}$ by the rule $\chi(0) = \begin{cases} 0 & \text{if } \chi \neq \chi_0 \\ 1 & \text{if } \chi = \chi_0 \end{cases}$. For more fundamentals on characters, primitive elements and finite fields, we refer the reader to [12].

For a divisor u of $q^m - 1$, an element $w \in \mathbb{F}_{q^m}^*$ is *u-free*, if $w = v^d$, where $v \in \mathbb{F}_{q^m}$ and $d|u$ implies $d = 1$. It is easy to observe that an element in $\mathbb{F}_{q^m}^*$ is $(q^m - 1)$-*free* if and only if it is primitive. A special case of [16, Lemma 10], provides an interesting result.

Lemma 2.1. *Let u be a divisor of q^m-1, $\xi \in \mathbb{F}_{q^m}^*$. Then*

$$\sum_{d|u} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d} \chi_d(\xi) = \begin{cases} \frac{u}{\phi(u)} & \text{if } \xi \text{ is } u\text{-free}, \\ 0 & \text{otherwise.} \end{cases}$$

where $\mu(\cdot)$ is the Möbius function and $\phi(\cdot)$ is the Euler function, χ_d runs through all the $\phi(d)$ multiplicative characters over $\mathbb{F}_{q^m}^*$ with order d.

Therefore, for each divisor u of q^m-1,

$$\rho_u : \alpha \mapsto \theta(u) \sum_{d|u} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d} \chi_d(\alpha), \tag{2.1}$$

gives a characteristic function for the subset of *u-free* elements of $\mathbb{F}_{q^m}^*$, where $\theta(u) = \frac{\phi(u)}{u}$.
Also, for each $a \in \mathbb{F}_q$,

$$\tau_a : \alpha \mapsto \frac{1}{q} \sum_{\psi \in \widehat{\mathbb{F}}_q} \psi(\operatorname{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) - a)$$

is a characterstic function for the subset of $\mathbb{F}_{q^m}$ consisting elements with $\operatorname{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = a$. From [12, Theorem 5.7] every additive character ψ of $\mathbb{F}_q$ can be obtained by $\psi(a) = \psi_0(ua)$, where ψ_0 is the canonical additive character of $\mathbb{F}_q$ and u is an element of $\mathbb{F}_q$ corresponding to ψ. Thus

$$\begin{aligned} \tau_a(\alpha) &= \frac{1}{q} \sum_{u \in \mathbb{F}_q} \psi_0(\operatorname{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(u\alpha) - ua) \\ &= \frac{1}{q} \sum_{u \in \mathbb{F}_q} \hat{\psi}_0(u\alpha)\psi_0(-ua), \end{aligned} \tag{2.2}$$

where $\hat{\psi}_0$ is the additive character of $\mathbb{F}_{q^m}$ defined by $\hat{\psi}_0(\alpha) = \psi_0(\operatorname{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha))$. In particular, $\hat{\psi}_0$ is the canonical additive character of $\mathbb{F}_{q^m}$.

The additive group of $\mathbb{F}_{q^m}$ is an $\mathbb{F}_q[x]$-module under the rule $f \ o \ \alpha = \sum_{i=1}^{k} a_i \alpha^{q^i}$; for $\alpha \in \mathbb{F}_{q^m}$ and $f(x) = \sum_{i=1}^{k} a_i x^i \in \mathbb{F}_q[x]$. For $\alpha \in \mathbb{F}_{q^m}$, the $\mathbb{F}_q$-order of α is the unique monic polynomial g of least degree such that $g \ o \ \alpha = 0$. Observe that g is a factor of $x^m - 1$. Similarly, by defining the action of $\mathbb{F}_q[x]$ over $\widehat{\mathbb{F}}_{q^m}$ by the rule $\psi \ o \ f(\alpha) = \psi(f \ o \ \alpha)$, where $\psi \in \widehat{\mathbb{F}}_{q^m}, \alpha \in \mathbb{F}_{q^m}$ and

$f \in \mathbb{F}_q[x]$, $\widehat{\mathbb{F}}_{q^m}$ becomes an $\mathbb{F}_q[x]$-module, and the unique monic polynomial g of least degree such that $\psi \; o \; g = \chi_0$ is called the $\mathbb{F}_q$-order of ψ. Further there are $\Phi_q(g)$ characters of $\mathbb{F}_q$-order g, where $\Phi_q(g)$ is the analogue of Euler's phi-function on $\mathbb{F}_q[x]$(see [12]).

Similar to above, for $g|x^m - 1$ an element $\alpha \in \mathbb{F}_{q^m}$ is g-$free$, if $\alpha = h \; o \; \beta$, where $\beta \in \mathbb{F}_{q^m}$ and $h|g$ implies $h = 1$. It is straightforward that an element in $\mathbb{F}_{q^m}$ is $(x^m - 1)$-$free$ if and only if it is normal. Also, for $g|x^m - 1$ an expression for the characteristic function for g-$free$ elements is given by

$$\kappa_g : \alpha \mapsto \Theta(g) \sum_{h|g} \frac{\mu'(d)}{\Phi_q(h)} \sum_{\psi_h} \psi_h(\alpha), \tag{2.3}$$

where $\Theta(g) = \frac{\Phi_q(g)}{q^{deg(g)}}$, the internal sum runs over all characters ψ_h of $\mathbb{F}_q$-order h and μ' is the analogue of the Möbius function defined as

$$\mu'(g) = \begin{cases} (-1)^s & \text{if g is a product of } s \text{ distinct monic irreducible polynomials,} \\ 0 & \text{otherwise.} \end{cases}$$

Following results of D. Wang and L. Fu will play a vital role in our next section.

Lemma 2.2. [9, Theorem 4.5] *Let $f(x) \in \mathbb{F}_{q^d}(x)$ be a rational function. Write $f(x) = \prod_{j=1}^k f_j(x)^{n_j}$, where $f_j(x) \in \mathbb{F}_{q^d}[x]$ are irreducible polynomials and n_j are non zero integers. Let χ be a multiplicative character of $\mathbb{F}_{q^d}$. Suppose that the rational function $\prod_{i=0}^{d-1} f(x^{q^i})$ is not of the form $h(x)^{ord(\chi)}$ in $\mathbb{F}_{q^d}(x)$, where ord(χ) is the order of χ, then we have*

$$\Big| \sum_{\alpha \in \mathbb{F}_q, f(\alpha) \neq 0, f(\alpha) \neq \infty} \chi(f(\alpha)) \Big| \leq (d \sum_{j=1}^k \deg(f_j) - 1) q^{\frac{1}{2}}.$$

Lemma 2.3. [9, Theorem 4.6] *Let $f(x), g(x) \in \mathbb{F}_{q^m}(x)$ be rational functions. Write $f(x) = \prod_{j=1}^k f_j(x)^{n_j}$, where $f_j(x) \in \mathbb{F}_{q^m}[x]$ are irreducible polynomials and n_j are non zero integers. Let $D_1 = \sum_{j=1}^k \deg(f_j)$, let $D_2 = max(\deg(g), 0)$, let D_3 be the degree of denominator of $g(x)$, and let D_4 be the sum of degrees of those irreducible polynomials dividing denominator* *of g but distinct from $f_j(x)(j=1,2,\cdots,k)$. Let χ be a multiplicative character of $\mathbb{F}_{q^m}$, and let ψ be a non trivial additive character of $\mathbb{F}_{q^m}$. Suppose $g(x)$ is not of the form $r(x)^{q^m}-r(x)$ in $\mathbb{F}_{q^m}(x)$. Then we have the estimate*

$$\Big|\sum_{\alpha\in\mathbb{F}_{q^m},f(\alpha)\neq 0,\infty g(\alpha)\neq\infty}\chi(f(\alpha))\psi(g(\alpha))\Big|\leq(D_1+D_2+D_3+D_4-1)q^{\frac{m}{2}}.$$

3 Sufficient condition

Let $l_1,l_2\in\mathbb{N}$ be such that $l_1,l_2|q^m-1$. Also, $a\in\mathbb{F}_q$, $f(x)\in S_{q,m}(n)$ and $g|x^m-1$, then $N_{f,a,n}(l_1,l_2,g)$ denote the number of elements $\alpha\in\mathbb{F}_{q^m}$ such that α is both l_1-*free* and g-$free$, $f(\alpha)$ is l_2-*free* and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^{-1})=a$.

We now prove one of the sufficient condition as follows.

Theorem 3.1. *Let m,n and $q\in\mathbb{N}$ such that q is a prime power and $m\geq 3$. Suppose that*

$$q^{\frac{m}{2}-1}>(n+2)W(q-1)^2W(x^m-1). \tag{3.1}$$

Then $(q,m)\in T_n$.

Proof. To prove the result, it is enough to show that $N_{f,a,n}(q^m-1,q^m-1,x^m-1)>0$ for every $f(x)\in S_{q,m}(n)$ and prescribed $a\in\mathbb{F}_q$. Let $f(x)\in S_{q,m}(n)$ be any rational function and $a\in\mathbb{F}_q$. Let U_1 be the set of zeros and poles of $f(x)$ in $\mathbb{F}_{q^m}$ and $U=U_1\cup\{0\}$. Assume l_1,l_2 be divisors of q^m-1 and g be a divisor of x^m-1. Then by definition

$$N_{f,a,n}(l_1,l_2,g)=\sum_{\alpha\in\mathbb{F}_{q^m}\setminus U}\rho_{l_1}(\alpha)\rho_{l_2}(f(\alpha))\tau_a(\alpha^{-1})\kappa_g(\alpha)$$

now using (2.1), (2.2) and (2.3),

$$N_{f,a,n}(l_1,l_2,g)=\frac{\theta(l_1)\theta(l_2)\Theta(g)}{q}\sum_{\substack{d_1|l_1,d_2|l_2\\ h|g}}\frac{\mu(d_1)}{\phi(d_1)}\frac{\mu(d_2)}{\phi(d_2)}\frac{\mu'(h)}{\Phi_q(h)}\sum_{\chi_{d_1},\chi_{d_2},\psi_h}\chi_{f,a}(d_1,d_2,h), \tag{3.2}$$

where $\chi_{f,a}(d_1,d_2,h)=\sum\limits_{u\in\mathbb{F}_q}\psi_0(-au)\sum\limits_{\alpha\in\mathbb{F}_{q^m}\setminus U}\chi_{d_1}(\alpha)\chi_{d_2}(f(\alpha))\psi_h(\alpha)\hat{\psi}_0(u\alpha^{-1})$.

Since ψ_h is an additive character of $\mathbb{F}_{q^m}$ and $\hat{\psi}_0$ is canonical additive character of $\mathbb{F}_{q^m}$, therefore there exists $v \in \mathbb{F}_{q^m}$ such that $\psi_h(\alpha) = \hat{\psi}_0(v\alpha)$. Hence $\chi_{f,a}(d_1, d_2, h) = \sum_{u \in \mathbb{F}_q} \psi_0(-au) \sum_{\alpha \in \mathbb{F}_{q^m} \setminus U} \chi_{d_1}(\alpha)\chi_{d_2}(f(\alpha))\hat{\psi}_0(v\alpha + u\alpha^{-1})$.

At this point, we claim that if $(d_1, d_2, h) \neq (1, 1, 1)$, where third 1 denotes the unity of $\mathbb{F}_q[x]$, then $|\chi_{f,a}(d_1, d_2, h)| \leq (n+2)q^{\frac{m}{2}+1}$. To see the claim, first suppose $d_2 = 1$, then $\chi_{f,a}(d_1, d_2, h) = \sum_{u \in \mathbb{F}_q} \psi_0(-au) \sum_{\alpha \in \mathbb{F}_{q^m} \setminus U} \chi_{d_1}(\alpha)\hat{\psi}_0(v\alpha + u\alpha^{-1})$. Here, if $vx + ux^{-1} \neq r(x)^{q^m} - r(x)$ for any $r(x) \in \mathbb{F}_{q^m}(x)$ then by Lemma 2.3 $|\chi_{f,a}(d_1, d_2, h)| \leq 2q^{\frac{m}{2}+1} + (|U| - 1)q \leq (n + 2)q^{\frac{m}{2}+1}$. Also, if $vx + ux^{-1} = r(x)^{q^m} - r(x)$ for some $r(x) \in \mathbb{F}_{q^m}(x)$ then following [Comm. Anju], it is possible when $u = v = 0$, which implies, $|\chi_{f,a}(d_1, d_2, h)| \leq |U|q < (n + 2)q^{\frac{m}{2}+1}$.

Now suppose $d_2 > 1$. Let d be the least common multiple of d_1 and d_2. Then [12] suggests that there exists a character χ_d of order d such that $\chi_{d_2} = \chi_d^{d/d_2}$. Also, there is an integer $0 \leq k < q^m - 1$ such that $\chi_{d_1} = \chi_d^k$. Consequently, $\chi_{f,a}(d_1, d_2, h) = \sum_{u \in \mathbb{F}_q} \psi_0(-au) \sum_{\alpha \in \mathbb{F}_{q^m} \setminus U} \chi_d(\alpha^k f(\alpha)^{d/d_2})\hat{\psi}_0(v\alpha + u\alpha^{-1})$. At this moment, first suppose $vx+ux^{-1} \neq r(x)^{q^m} - r(x)$ for any $r(x) \in \mathbb{F}_{q^m}(x)$. Then Lemma 2.3 implies that $|\chi_{f,a}(d_1, d_2, h)| \leq (n+2)q^{\frac{m}{2}+1}$. Also, if $vx+ux^{-1} = r(x)^{q^m} - r(x)$ for some $r(x) \in \mathbb{F}_{q^m}(x)$, then following [15] we get $u = v = 0$. Therefore, $\chi_{f,a}(d_1, d_2, h) = \sum_{u \in \mathbb{F}_q} \psi_0(-au) \sum_{\alpha \in \mathbb{F}_{q^m} \setminus U} \chi_d(\alpha^k f(\alpha)^{d/d_2})$. Here, if $x^k f(x)^{d/d_2} \neq r(x)^d$ for any $r(x) \in \mathbb{F}_{q^m}(x)$, then using Lemma 2.2 we get $|\chi_{f,a}(d_1, d_2, h)| \leq nq^{\frac{m}{2}+1} < (n+2)q^{\frac{m}{2}+1}$. However, $x^k f(x)^{d/d_2} = r(x)^d$ for some $r(x) \in \mathbb{F}_{q^m}(x)$ gives that f is exceptional(see [8]).

Hence, from the above discussion along with (3.2), we get

$$\begin{aligned}
N_{f,a,n}(l_1, l_2, g) &\geq \frac{\theta(l_1)\theta(l_2)\Theta(g)}{q}(q^m - |U| - ((n+2)q^{\frac{m}{2}+1})(W(l_1)W(l_2)W(g) - 1)) \\
&\geq \frac{\theta(l_1)\theta(l_2)\Theta(g)}{q}(q^m - (n+1) - ((n+2)q^{\frac{m}{2}+1})(W(l_1)W(l_2)W(g) - 1)) \\
&\geq \frac{\theta(l_1)\theta(l_2)\Theta(g)}{q}(q^m - (n+2)q^{\frac{m}{2}+1}W(l_1)W(l_2)W(g)) \qquad (3.3)
\end{aligned}$$

Thus, if $q^{\frac{m}{2}-1} > (n + 2)W(l_1)W(l_2)W(g)$, then $N_{f,a,n}(l_1, l_2, g) > 0$ for all $f(x) \in S_q(n)$ and prescribed $a \in \mathbb{F}_q$. The result now follows by taking $l_1 = l_2 = q^m - 1$ and $g = x^m - 1$. □

4 Sieving Results

Here, we state some results, their proofs have been omitted as they follow on the lines of the results in [10] and have been used frequently in [13, 8, 10, 14, 2].

Lemma 4.1. *Let k and P be co-prime positive integers and $g, G \in \mathbb{F}_q[x]$ be co-prime polynomials. Also, let $\{p_1, p_2, \cdots, p_r\}$ be the collection of all prime divisors of P, and $\{g_1, g_2, \cdots, g_s\}$ contains all the irreducible factors of G. Then*

$$N_{f,a,n}(kP, kP, gG) \geq \sum_{i=1}^{r} N_{f,a,n}(kp_i, k, g) + \sum_{i=1}^{r} N_{f,a,n}(k, kp_i, g) + \sum_{i=1}^{s} N_{f,a,n}(k, k, gg_i) - (2r + s - 1)N_{f,a,n}(k, k, g).$$

Lemma 4.2. *Let $l, m, q \in \mathbb{N}$, $g \in \mathbb{F}_q[x]$ be such that q is a prime power, $m \geq 3$ and $l | q^m - 1$, $g | x^m - 1$. Let c be a prime number which divides $q^m - 1$ but not l, and e be irreducible polynomial dividing $x^m - 1$ but not g. Then*

$$|N_{f,a,n}(cl, l, g) - \theta(c)N_{f,a,n}(l, l, g)| \leq (n + 2)\theta(c)\theta(l)^2\Theta(g)W(l)^2W(g)q^{\frac{m}{2}},$$

$$|N_{f,a,n}(l, cl, g) - \theta(c)N_{f,a,n}(l, l, g)| \leq (n + 2)\theta(c)\theta(l)^2\Theta(g)W(l)^2W(g)q^{\frac{m}{2}}$$

and

$$|N_{f,a,n}(l, l, eg) - \Theta(e)N_{f,a,n}(l, l, g)| \leq (n + 2)\theta(l)^2\Theta(e)\Theta(g)W(l)^2W(g)q^{\frac{m}{2}}.$$

Theorem 4.1. *Let $l, m, q \in \mathbb{N}$, $g \in \mathbb{F}_q[x]$ be such that q is a prime power, $m \geq 3$ and $l | q^m - 1$, $g | x^m - 1$. Also, let $\{p_1, p_2, \cdots p_r\}$ be the collection of primes which divides $q^m - 1$ but not l, and $\{g_1, g_2, \cdots g_s\}$ be the irreducible polynomials dividing $x^m - 1$ but not g. Suppose $\delta = 1 - 2\sum_{i=1}^{r} \frac{1}{p_i} - \sum_{i=1}^{s} \frac{1}{q^{\deg(g_i)}}$, $\delta > 0$ and $\Delta = \frac{2r+s-1}{\delta} + 2$. If $q^{\frac{m}{2}-1} > (n + 2)\Delta W(l)^2W(g)$ then $(q, m) \in T_n$.*

Now, we present a more effective sieving technique than Theorem 4.1, which is an extension of the result in [6]. For this, we adopt some notations and conventions from [6] as described. Let $\text{Rad}(q^m - 1) = kPL$, where k is the product of smallest prime divisors of $q^m - 1$, L is the product of large prime divisors of $q^m - 1$ denoted by $L = l_1 \cdot l_2 \cdots l_t$, and rest of the prime divisors of $q^m - 1$ lie in P and denoted by $p_1, p_2, \cdots, p_r$. Similarly, $\mathrm{Rad}(x^m - 1) = gGH$, where g is the product of irreducible factors of $x^m - 1$ of least degree, and irreducible factors of large degree are factors of H which are denoted by $h_1, h_2, \cdots, h_u$ and rest lie in G and denoted by $g_1, g_2, \cdots, g_s$.

Theorem 4.2. *Let $m, q \in \mathbb{N}$ such that q is a prime power and $m \geq 3$. Using above notations, let Rad$(q^m - 1) = kPL$, Rad$(x^m - 1) = gGH$, $\delta = 1 - 2\sum_{i=1}^{r} \frac{1}{p_i} - \sum_{i=1}^{s} \frac{1}{q^{\deg(g_i)}}$, $\epsilon_1 = \sum_{i=1}^{t} \frac{1}{l_i}$, $\epsilon_2 = \sum_{i=1}^{u} \frac{1}{q^{\deg(h_i)}}$ and $\delta\theta(k)^2\Theta(g) - (2\epsilon_1 + \epsilon_2) > 0$. Then*

$$q^{\frac{m}{2}-1} > (n+2)[\theta(k)^2\Theta(g)W(k)^2W(g)(2r+s-1+2\delta)+(t-\epsilon_1)+(2/(n+2))(u-\epsilon_2) + (n/(n+2))(1/q^{m/2})(t+u-\epsilon_1-\epsilon_2)]/[\delta\theta(k)^2\Theta(g) - (2\epsilon_1+\epsilon_2)] \quad (4.1)$$

implies $(q, m) \in T_n$.

Proof. Clearly,

$$N_{f,a,n}(q^m-1, q^m-1, x^m-1) = N_{f,a,n}(kPL, kPL, gGH) \geq N_{f,a,n}(kP, kP, gG) + N_{f,a,n}(L, L, H) - N_{f,a,n}(1,1,1). \quad (4.2)$$

Further, by Lemma 4.1

$$N_{f,a,n}(kP, kP, gG) \geq \delta N_{f,a,n}(k,k,g) + \sum_{i=1}^{r}\{N_{f,a,n}(kp_i, k, g) - \theta(p_i)N_{f,a,n}(k,k,g)\}$$
$$+\sum_{i=1}^{r}\{N_{f,a,n}(k, kp_i, g) - \theta(p_i)N_{f,a,n}(k,k,g)\} + \sum_{i=1}^{s}(N_{f,a,n}(k,k,gg_i) - \Theta(g_i)N_{f,a,n}(k,k,g))$$

.

Using (3.3) and Lemma 4.2, we get

$$N_{f,a,n}(kP, kP, gG) \geq \delta\theta(k)^2\Theta(g)\big(q^{m-1} - (n+2)W(k)^2W(g)q^{\frac{m}{2}}\big) - (n+2)\theta(k)^2\Theta(g)W(k)^2W(g)\big(\sum_{i=1}^{r} 2\theta(p_i) + \sum_{i=1}^{s}\Theta(g_i)\big)q^{\frac{m}{2}}$$

$$= \theta(k)^2\Theta(g)\big(\delta q^{m-1} - (n+2)(2r+s-1+2\delta)W(k)^2W(g)q^{\frac{m}{2}}\big). \quad (4.3)$$

Again, by Lemma 4.1

$$N_{f,a,n}(L,L,H)-N_{f,a,n}(1,1,1)\geq\sum_{i=1}^{t}N_{f,a,n}(l_i,1,1)+\sum_{i=1}^{t}N_{f,a,n}(1,l_i,1)$$
$$+\sum_{i=1}^{u}N_{f,a,n}(1,1,h_i)-(2t+u)N_{f,a,n}(1,1,1)$$

$$=\sum_{i=1}^{t}\{N_{f,a,n}(l_i,1,1)-\theta(l_i)N_{f,a,n}(1,1,1)\}+\sum_{i=1}^{t}\{N_{f,a,n}(1,l_i,1)-\theta(l_i)N_{f,a,n}(1,1,1)\}$$
$$+\sum_{i=1}^{u}\{N_{f,a,n}(1,1,h_i)-\Theta(h_i)N_{f,a,n}(1,1,1)\}-(2\epsilon_1+\epsilon_2)N_{f,a,n}(1,1,1) \quad (4.4)$$

By (3.2), for a prime divisor l of q^m-1, $|N_{f,a,n}(l,1,1)-\theta(l)N_{f,a,n}(1,1,1)|=\frac{\theta(l)}{\phi(l)q}|\sum\limits_{\chi_l}\chi_{f,a}(l,1,1)|$, where

$$|\chi_{f,a}(l,1,1)|=|\sum_{u\in\mathbb{F}_q}\psi_0(-au)\sum_{\alpha\in\mathbb{F}_{q^m}\setminus U}\chi_l(\alpha)\hat{\psi}_0(u\alpha^{-1}|\leq q^{\frac{m}{2}+1}+nq.$$

Hence, $|N_{f,a,n}(l,1,1)-\theta(l)N_{f,a,n}(1,1,1)|\leq\theta(l)(q^{\frac{m}{2}}+n)$. Similarly,

$$|\chi_{f,a}(1,l,1)|=|\sum_{u\in\mathbb{F}_q}\psi_0(-au)\sum_{\alpha\in\mathbb{F}_{q^m}\setminus U}\chi_l(f(\alpha))\hat{\psi}_0(u\alpha^{-1}|\leq(n+1)q^{\frac{m}{2}+1},$$

which further implies $|N_{f,a,n}(1,l,1)-\theta(l)N_{f,a,n}(1,1,1)|\leq(n+1)q^{\frac{m}{2}}$. Also, for an irreducible divisor h of x^m-1,

$$|\chi_{f,a}(1,1,h)|=|\sum_{u\in\mathbb{F}_q}\psi_0(-au)\sum_{\alpha\in\mathbb{F}_{q^m}\setminus U}\psi_h(\alpha)\hat{\psi}_0(u\alpha^{-1}|$$
$$=|\sum_{u\in\mathbb{F}_q}\psi_0(-au)\sum_{\alpha\in\mathbb{F}_{q^m}\setminus U}\hat{\psi}_0(v\alpha+u\alpha^{-1}|\leq 2q^{\frac{m}{2}+1}+nq.$$

Therefore, $|N_{f,a,n}(1,1,h)-\Theta(h)N_{f,a,n}(1,1,1)|\leq\Theta(h)(q^{\frac{m}{2}}+n)$. Using these bounds in (4.4), we have $N_{f,a,n}(L,L,H)-N_{f,a,n}(1,1,1)\geq-\sum\limits_{i=1}^{t}\theta(l_i)(q^{\frac{m}{2}}+$

$n) - \sum_{i=1}^{t} \theta(l_i)(n+1)q^{\frac{m}{2}} - \sum_{i=1}^{u} \Theta(h_i)(2q^{\frac{m}{2}} + n) - (2t+u)N_{f,a,n}(1,1,1)$. Now, $N_{f,a,n}(1,1,1) \leq q^{m-1}$ together with $\sum_{i=1}^{t} \theta(l_i) = (t - \epsilon_1)$ and $\sum_{i=1}^{u} = (u - \epsilon_2)$ implies

$$N_{f,a,n}(L,L,H) - N_{f,a,n}(1,1,1) \geq -\{(n+2)(t-\epsilon_1) + 2(u-\epsilon_2)\}q^{\frac{m}{2}} \\ - n(t+u-\epsilon_1-\epsilon_2) - (2\epsilon_1+\epsilon_2)q^{m-1}. \quad (4.5)$$

Now using (4.3) and (4.5) in (4.2) we get,

$$N_{f,a,n}(q^m-1, q^m-1, x^m-1) \geq \{\delta\theta(k)^2\Theta(g) - (2\epsilon_1+\epsilon_2)\}q^{m-1} - \theta(k)^2\Theta(g)(n+2) \\ (2r+s-1+2\delta)W(k)^2W(g)q^{\frac{m}{2}} - \{(n+2)(t-\epsilon_1) + 2(u-\epsilon_2)\}q^{\frac{m}{2}} - n(t+u-\epsilon_1-\epsilon_2)$$

$$= q^{\frac{m}{2}}\big[\big(\delta\theta(k)^2\Theta(g) - (2\epsilon_1+\epsilon_2)\big)q^{\frac{m}{2}-1} - (n+2)\{\theta(k)^2\Theta(g)(2r+s-1+2\delta)W(k)^2W(g) \\ - \{(t-\epsilon_1) + (2/(n+2))(u-\epsilon_2)\} - (n/(n+2))(1/q^{m/2})(t+u-\epsilon_1-\epsilon_2)\}\big]$$

Thus

$$q^{\frac{m}{2}-1} > (n+2)[\theta(k)^2\Theta(g)W(k)^2W(g)(2r+s-1+2\delta) + (t-\epsilon_1) + (2/(n+2))(u-\epsilon_2) \\ + (n/(n+2))(1/q^{m/2})(t+u-\epsilon_1-\epsilon_2)]/[\delta\theta(k)^2\Theta(g) - (2\epsilon_1+\epsilon_2)]$$

implies $N_{f,a,n}(q^m-1, q^m-1, x^m-1) > 0$ i.e., $(q,m) \in T_n$.

□

It is easy to observe that Theorem 4.1 is a special case of Theorem 4.2 and can be obtained by setting $t = u = \epsilon_1 = \epsilon_2 = 0$.

5 Working Example

However the results discussed above are applicable for arbitrary natural number n and the finite field $\mathbb{F}_{q^m}$ of any prime characteristic. Though to demonstrate the application of above results and make the calculations uncomplicated we assume that $q = 5^k$ for some $k \in \mathbb{N}$ and $n = 2$, and work on the set T_2. Precisely, in this section, we prove the following result.

Theorem 5.1. *Let $q = 5^k$ for some $k \in \mathbb{N}$ and $m \geq 3$ is an integer. Then $(q,m) \in T_2$ unless one of the following holds:*

1. $q = 5, 5^2, 5^3, 5^4, 5^5, 5^6, 5^8, 5^{10}$ *and* $m = 3$*;*

2. $q = 5, 5^2, 5^3, 5^4$ *and* $m = 4$*;*

3. $q = 5, 5^2$ *and* $m = 5, 6$;

4. $q = 5$ *and* $m = 7, 8, 10, 12$.

We shall divide it in two parts, in first part we shall work on $m \geq 5$ and in second we shall consider $m = 3, 4$. For further calculation work and to apply the previous results we shall need the following lemma which can also be developed from [5, Lemma 6.2].

Lemma 5.1. *Let* M *be a positive integer, then* $W(M) < 4515 \times M^{1/8}$.

5.1 Part 1.

In this part, we assume $m \geq 5$ and write $m = m'5^j$, where $j \geq 1$ is an integer and $5 \nmid m'$. Then $\Omega_q(x^m - 1) = \Omega_q(x^{m'} - 1)$ which further implies $W(x^m - 1) = W(x^{m'} - 1)$. Further, we shall divide the discussion in two cases.

- $m'|q-1$
- $m' \nmid q-1$

Case 1. $m|q-1$.
Clearly [12, Theorem 2.47] implies that $\Omega_q(x^{m'} - 1) = m'$. Let $l = q^m - 1$ and $g = 1$ in Theorem 4.1 then $\Delta = \frac{q^2+(a-3)q+2}{(a-1)q+1}$, where $a = \frac{q-1}{m'}$, which further implies $\Delta < q^2$. Hence $(q, m) \in T_2$ if $q^{\frac{m}{2}-3} > 4W(q^m - 1)^2$. However, by Lemma 5.1, it is sufficient if $q^{\frac{m}{4}-3} > 4 \cdot (4515)^2$, which holds for $q \geq 125$ and for all $m \geq 28$. In particular, for $q \geq 125$ and for all $m' \geq 28$. Next, we examine all the cases where $m' \leq 27$. For this we set $l = q^m - 1$ and $g = 1$ in Theorem 4.1 unless mentioned. Then $\delta = 1 - \frac{m'}{q}$ and $\Delta = 2 + \frac{(m'-1)q}{q-m'}$
1. $\underline{m' = 1.}$ Here $m = 5^j$ for some integer $j \geq 1$ and $\Delta = 2$. Then by Theorem 4.1 it is sufficient if $q^{\frac{m}{2}-1} > 4 \cdot 2 \cdot W(q^m - 1)^2$. Again Lemma 5.1 implies $(q, m) \in T_2$ if $q^{\frac{m}{4}-1} > 8 \cdot (4515)^2$ i.e., $q^{\frac{5^j}{4}-1} > 8 \cdot (4515)^2$, which holds for all choices of (q, m) except $(5, 5), (5, 5^2), (5^2, 5), (5^2, 5^2), (5^3, 5), (5^4, 5), \cdots, (5^{46}, 5)$ which are 48 in number. For these, we checked $q^{\frac{m}{2}-1} > 4 \cdot 2 \cdot W(q^m - 1)^2$ directly by factoring q^m-1 and got it verified except the pairs $(5, 5), (5^2, 5), (5^3, 5)$,

$(5^4, 5)$ and $(5^6, 5)$.

2. $\underline{m' = 2.}$ In this case, $m = 2 \cdot m^j$ for some $j \geq 1$ and $\Delta = 2 + \frac{q}{q-2} < 4$. Similar to the above case, it is sufficient if $q^{\frac{2 \cdot 5^j}{4} - 1} > 16 \cdot (4515)^2$, which is true except the 9 pairs $(5, 10), (5, 50), (5^2, 10), (5^3, 10), \cdots, (5^8, 10)$, and the verification of $q^{\frac{m}{2} - 1} > 4 \cdot 4 \cdot W(q^m - 1)^2$ for these pairs yield the only possible exceptions as $(5, 10)$ and $(5^2, 10)$.

Following the similar steps for the rest of the values of $m' \leq 27$ we get that there is no exception for many values of m'. Values of m' with possible exceptional pairs is as below.

3. $\underline{m' = 4.}$ $(5, 20)$.

4. $\underline{m' = 6.}$ $(5^2, 6), (5^4, 6)$ and $(5^6, 6)$.

5. $\underline{m' = 8.}$ $(5^2, 8)$.

Furthermore, for the pairs $(5^3, 5), (5^4, 5), (5^6, 5), (5^2, 10), (5, 20), (5^4, 6), (5^6, 6)$ and $(5^2, 8)$ Theorem 4.1 holds for some choice of l and g (see Table 1). Hence, only left **possible exceptions** in this case are $(5, 5), (5^2, 5), (5, 10)$ and $(5^2, 6)$.

Table 1

Sr. No.	(q, m)	l	r	g	s	$\delta >$	$\Delta <$	$4\Delta W(g) W(l)^2 <$
1	$(5^3, 5)$	2	5	1	1	0.705298	16.178405	518
2	$(5^4, 5)$	6	6	1	1	0.581729	22.628164	2897
3	$(5^6, 5)$	6	9	1	1	0.390631	48.079201	6155
4	$(5^2, 10)$	6	6	1	2	0.503329	27.828038	3562
5	$(5, 20)$	6	6	$x^2 + \beta^3 x + \beta$	2	0.183329	72.910743	18666
6	$(5^4, 6)$	6	6	1	6	0.476599	37.669274	4822
7	$(5^6, 6)$	6	9	1	6	0.330094	71.677019	9175
8	$(5^2, 8)$	6	4	1	8	0.401942	39.318735	5033

where β is a primitive element of $\mathbb{F}_5$.

Case 2. $m' \nmid q - 1$.

Let the order of $q \mod m'$ be denoted by b. Then $b \geq 2$ and degree of irreducible factors of $x^{m'} - 1$ over $\mathbb{F}_q$ is less than or equal to b. Let M denotes the number of distinct irreducible factors of $x^m - 1$ over $\mathbb{F}_q$ of degree less than b. Also let $\nu(q, m)$ denotes the ratio $\nu(q, m) = \frac{M}{m}$. Then, $m\nu(q, m) = m'\nu(q, m')$.

For the further progress, we need the following two results which are the directly implied by Proposition 5.3 of [7] and Lemma 7.2 of [5] respectively.

Lemma 5.2. *Let $k, m, q \in \mathbb{N}$ be such that $q = 5^k$ and $m' \nmid q-1$. In the notations of Theorem 4.1, let $l = q^m - 1$ and g is the product of irreducible factors of $x^m - 1$ of degree less than b, then $\Delta < m'$.*

Lemma 5.3. *Let $m' > 4$ and $m_1 = \gcd(q-1, m')$. Then following bounds hold.*

1. *For $m' = 2m_1$, $\nu(q, m') = \frac{1}{2}$;*
2. *for $m' = 4m_1, \nu(q, m') = \frac{3}{8}$;*
3. *for $m' = 6m_1, \nu(q, m') = \frac{13}{36}$;*
4. *otherwise, $\nu(q, m') \leq \frac{1}{3}$.*

At this point we note that $m' = 1, 2$ and 4 divide $q-1$ for any $q = 5^k$ and have been discussed in above case, whereas $m' = 5$ is not possible. Therefore, in this case we need to discuss $m' = 3$ and $m' \geq 6$.

First consider $m' = 3$. Then $m = 3 \cdot 5^j$ for some integer $j \geq 1$. Also, $m' \nmid q-1$ implies if $q = 5^k$ then k is odd and $x^{m'} - 1$ is the product of a linear factor and a quadratic factor. Thus, $W(x^m - 1) = W(x^{m'} - 1) = 2^2 = 4$ and (3.1) implies $(q, m) \in T_2$ if $q^{\frac{m}{2}-1} > 16 \cdot W(q^m - 1)^2$. By Lemma 5.1, it is sufficient if $q^{\frac{m}{4}-1} > 16 \cdot (4515)^2$, which hold for $q = 5$ and $m \geq 53$, $q = 125$ and $m \geq 21$, $q \geq 5^5$ and $m \geq 14$. Thus, only possible exceptions are $(5, 15)$ and $(125, 15)$. For these two possible exceptions we checked $q^{\frac{m}{4}-1} > 16 \cdot W(q^m - 1)^2$ directly by factoring $q^m - 1$ and got it verified for $(125, 15)$. Hence only possible exception for $m' = 3$ is $(5, 15)$.

Now suppose $m' \geq 6$. At this point, in Theorem 4.1 let $l = q^m - 1$ and g be the product of irreducible factors of $x^m - 1$ of degree less than b. Therefore, Lemma 5.2 along with Theorem 4.1 implies $(q, m) \in T_2$ if $q^{\frac{m}{2}-1} > 4 \cdot m' \cdot W(q^m - 1)^2 \cdot 2^{m'\nu(q,m')}$. By Lemma 5.1, it is sufficient if

$$q^{\frac{m}{4}-1} > 4 \cdot m \cdot (4515)^2 \cdot 2^{m\nu(q,m')}. \tag{5.1}$$

Further, we shall discuss it in four cases as follows.

1. $\underline{m' \neq 2m_1, 4m_1, 6m_1.}$

Here, Lemma 5.3 implies $\nu(q, m') = \frac{1}{3}$. Using this in (5.1) we get $(q, m) \in T_2$

if $q^{\frac{m}{4}-1} > 4 \cdot m \cdot (4515)^2 \cdot 2^{\frac{m}{3}}$, which holds for $q^m \geq 5^{145}$. Next, for $q^m \leq 5^{144}$, we verified $q^{\frac{m}{2}-1} > 4 \cdot m \cdot W(q^m-1)^2 \cdot 2^{\frac{m}{3}}$ by factoring $q^m - 1$ and got a list of 20 possible exception as follows.
$(5,6),(5,7),(5,9),(5,11),(5,12),(5,13),(5,14),(5,17),(5,18),(5,19),(5,21),(5,22),(5,27),(5,30),(5,36),(5^2,7),(5^2,9),(5^2,11),(5^3,6),(5^5,6)$.

2. $\underline{m' = 2m_1.}$
In this case, $\nu(q,m) = \frac{1}{2}$. Therefore, (5.1) implies $(q,m) \in T_2$ if $q^{\frac{m}{4}-1} > 4 \cdot m \cdot (4515)^2 \cdot 2^{\frac{m}{2}}$, which holds for $q = 5$ and $m \geq 466$ while for $q \geq 25$ it is sufficient that $m \geq 56$. Here, for $q = 5$, we have $m' = 8$ only. Thus possible exception for $q = 5$ are $(5,8),(5,40)$ and $(5,200)$. On the other hand, for $q \geq 25$ and $q^m < 25^{56}$ along with above three possible exceptions we checked $q^{\frac{m}{2}-1} > 4 \cdot m \cdot W(q^m-1)^2 \cdot 2^{\frac{m}{2}}$ and got it verified except $(5,8),(5,40)$ and $(5^3,8)$.

3. $\underline{m' = 4m_1.}$
Here, $\nu(q,m) = \frac{3}{8}$. Again, (5.1) gives $(q,m) \in T_2$ if $q^{\frac{m}{4}-1} > 4 \cdot m \cdot (4515)^2 \cdot 2^{\frac{3m}{8}}$, which is true for $q^m \geq 5^{176}$. On the other side, verification of $q^{\frac{m}{2}-1} > 4 \cdot m \cdot W(q^m-1)^2 \cdot 2^{\frac{3m}{8}}$ for $q^m < 5^{176}$ provides only possible exception as $(5,16)$.

4. $\underline{m' = 6m_1.}$
Similar to the above case, we have $\nu(q,m) = \frac{13}{36}$ and $q^{\frac{m}{4}-1} > 4 \cdot m \cdot (4515)^2 \cdot 2^{\frac{13m}{36}}$ holds for $q^m \geq 5^{164}$. Also, for $q^m < 5^{164}$, $q^{\frac{m}{2}-1} > 4 \cdot m \cdot W(q^m-1)^2 \cdot 2^{\frac{13m}{36}}$ holds for all (q,m) except $(5,24)$.

Table 2

Sr. No.	(q,m)	l	r	g	s	$\delta >$	$\Delta <$	$\frac{4\Delta W(g)}{W(l)^2} <$
1	$(5,11)$	2	1	1	3	0.799359	7.004009	225
2	$(5,13)$	2	1	1	4	0.795199	8.287731	266
3	$(5,14)$	2	4	$x+1$	3	0.059683	169.55170	5426
4	$(5,17)$	2	2	1	2	0.795110	8.288442	266
5	$(5,18)$	6	5	1	6	0.061578	245.59029	31436
6	$(5,19)$	2	3	1	3	0.789208	12.136745	389
7	$(5,21)$	2	4	1	5	0.689908	19.393614	621
8	$(5,22)$	2	5	$x+1$	5	0.014867	943.67119	30198
9	$(5,27)$	2	7	1	4	0.561470	32.277659	1033
10	$(5,30)$	6	9	$x+1$	3	0.110695	182.67531	23383
11	$(5,36)$	6	9	x^4-1	8	0.170222	148.86660	152440
12	$(5^2,7)$	2	4	1	3	0.219683	47.520125	1521
13	$(5^2,9)$	6	5	1	5	0.421578	35.208505	4507
14	$(5^2,11)$	2	5	1	3	0.176146	70.124930	2244
15	$(5^3,6)$	6	5	1	4	0.525578	26.734639	3423
16	$(5^5,6)$	6	9	10	4	0.390055	55.838482	7148
17	$(5,15)$	2	5	1	2	0.473298	25.241167	808
18	$(5,40)$	6	9	$x^2+\beta^3x+\beta$	4	0.088640	238.91192	61162
19	$(5^3,8)$	6	6	1	6	0.454072	39.438940	5049
20	$(5,16)$	6	4	$x+1$	7	0.038742	363.35624	46510
21	$(5,24)$	6	6	x^4-1	10	0.086200	245.61740	251513

Next, we refer to Table 2 to note that Theorem 4.1 holds for the pairs $(5,11)$, $(5,13)$, $(5,14)$, $(5,15)$, $(5,16)$, $(5,17)$, $(5,18)$, $(5,19)$, $(5,21)$, $(5,22)$, $(5,24)$, $(5,27)$, $(5,30)$, $(5,36)$, $(5,40)$, $(5^2,7)$, $(5^2,9)$, $(5^2,11)$, $(5^3,6)$, $(5^3,8)$, $(5^5,6)$. Thus, only left **possible exceptions** in the case $m' \nmid q-1$ are $(5,6)$,$(5,7)$, $(5,8)$, $(5,9)$, and $(5,12)$.

5.2 Part 2.

In this part we shall consider $m=3,4$. Following result will be required for further calculation, which follows on the lines of [6, Lemma 51].

Lemma 5.4. *Let $k \in \mathbb{N}$ such that $\omega(k) \geq 2828$. Then $W(k) < k^{\frac{1}{13}}$.*

Also, $W(x^m-1) \leq 16$. Now, first assume $\omega(q^m-1) \geq 2828$, then (3.1) and Lemma 5.4 together implies $(q,m) \in T_2$ if $q^{\frac{m}{2}-1} > 64 \cdot q^{\frac{2m}{13}}$ i.e., $q^{\frac{9m}{26}-1} > 64$ or $q^m > 64^{\frac{26m}{9m-26}}$, sufficient if $q^m > 64^{78}$, which is true for $\omega(q^m-1) \geq 2828$. To make further progress we follow [13]. Next, assume $88 \leq \omega(q^m-1) \leq 2827$. In Theorem 4.1, let $g = x^m - 1$ and l to be the product of least 88 primes dividing q^m-1 i.e., $W(l) = 2^{88}$. Then $r \leq 2739$ and δ will be at least its value when $\{p_1, p_2, \cdots, p_{2739}\} = \{461, 463, \cdots, 25667\}$. This gives $\delta > 0.0041806$ and $\Delta < 1.3101 \times 10^6$, hence $4\Delta W(g)W(l)^2 < 8.0309 \times 10^{60} = R$ (say). By Theorem 4.1 $(q,m) \in T_2$ if $q^{\frac{m}{2}-1} > R$ or $q^m > R^{\frac{2m}{m-2}}$. But $m \geq 3$ implies $\frac{2m}{m-2} \leq 6$. Therefore, if $q^m > R^6$ or $q^m > 2.6828 \times 10^{365}$ then $(q,m) \in T_2$. Hence, $\omega(q^m-1) \geq 152$ gives $(q,m) \in T_2$. Repeating this process of Theorem 4.1 for the values in Table 3 implies $(q,m) \in T_2$ if $q^{\frac{m}{2}-1} > 889903387$. Thus, for $m = 3$ it is sufficient if $q > (889903387)^2$ and for $m = 4$ we need $q > 889903387$. Hence, only possible exceptions are $(5,3), (5^2,3), \cdots, (5^{25},3)$ and $(5,4), (5^2,4), \cdots, (5^{12},4)$. However, Table 4 implies that Theorem 4.1 holds for $(5^9,3), (5^{11},3), (5^{12},3), (5^{13},3), \cdots, (5^{25},3)$ and $(5^6,4), (5^7,4), \cdots, (5^{12},4)$. Thus, only **possible exceptions** here are $(5,3), (5^2,3), \cdots, (5^8,3)$ and $(5^{10},3)$, and $(5,4), (5^2,4), \cdots, (5^5,4)$.

Table 3

Sr. No.	$a \leq \omega(q^m-1) \leq b$	$W(l)$	$\delta >$	$\Delta <$	$4\Delta W(g)$ $W(l)^2 <$
1	$a = 17, \quad b = 151$	2^{17}	0.0347407	7687.5008	8.4526×10^{15}
2	$a = 9, \quad b = 51$	2^9	0.0550187	1510.5788	2.5344×10^{10}
3	$a = 7, \quad b = 37$	2^7	0.0064402	9163.1796	9608289244
4	$a = 7, \quad b = 36$	2^7	0.0191790	2973.9903	3118453847
5	$a = 7, \quad b = 34$	2^7	0.0458469	1158.0218	1214272852
6	$a = 7, \quad b = 33$	2^7	0.0602354	848.6790	889903387

Table 4

Sr. No.	(q, m)	l	r	g	s	$\delta >$	$\Delta <$	$4\Delta W(g)$ $W(l)^2 <$
1	$(5^9, 3)$	2	7	1	2	0.801533	20.714128	663
2	$(5^{11}, 3)$	2	4	1	2	0.925433	11.725177	376
3	$(5^{12}, 3)$	6	9	1	3	0.330478	62.518314	8003
4	$(5^{13}, 3)$	2	4	1	2	0.910167	11.888295	381
5	$(5^{14}, 3)$	6	10	1	3	0.508443	45.269297	5795
6	$(5^{15}, 3)$	2	10	1	2	0.603902	36.773815	1177
7	$(5^{16}, 3)$	6	9	1	3	0.368379	56.291827	7206
8	$(5^{17}, 3)$	2	6	1	2	0.930565	15.970005	512
9	$(5^{18}, 3)$	6	12	1	3	0.499055	54.098369	6925
10	$(5^{19}, 3)$	2	5	1	2	0.924693	13.895837	445
11	$(5^{20}, 3)$	6	15	1	3	0.183646	176.24807	22560
12	$(5^{21}, 3)$	2	9	1	2	0.822416	25.102645	804
13	$(5^{22}, 3)$	6	10	1	3	0.522529	44.102865	5646
14	$(5^{23}, 3)$	2	7	1	2	0.920550	18.294603	586
15	$(5^{24}, 3)$	6	14	1	3	0.296682	103.11815	13200
16	$(5^{25}, 3)$	2	14	1	2	0.666688	45.498589	1456
17	$(5^6, 4)$	6	6	1	4	0.485944	32.867712	4208
18	$(5^7, 4)$	2	6	1	4	0.105913	143.62473	4596
19	$(5^8, 4)$	2	7	1	4	0.054494	313.95724	10047
20	$(5^9, 4)$	6	9	1	4	0.330476	65.544620	8390
21	$(5^10, 4)$	6	9	1	4	0.568640	38.930216	4984
22	$(5^11, 4)$	2	8	1	4	0.039829	479.03888	15330
23	$(5^12, 4)$	6	9	1	4	0.368379	59.006421	7553

Further, for all the left **possible exceptions** we checked Theorem 4.2 and got it verified in case of $(5^7, 3), (5^5, 4)$ and $(5, 9)$ for the values in Table 5.

Table 5

Sr. No.	(q, m)	k	P	L	f	G	H	$R' <$
1	$(5, 9)$	2	589	829	$x-1$	$x^2 + x + 1$	x^6+x^3+1	269
2	$(5^7, 3)$	2	229469719	519499	$x-1$	1	$x^2 + x + 1$	262
3	$(5^9, 4)$	6	216878233	9161	$x+1$	$x^2+x+\beta^3$	$x + \beta^3$	2788

Where, R' represent the right hand side value of (4.1). Hence, all the results from part 1 and part 2 collectively implies Theorem 5.1.

References

[1] G. B. Agnew, R. C. Mullin, I. M. Onyszchuk, and S. A. Vanstone. An implementation for a fast public-key cryptosystem. *J. Cryptology*, 3(2):63–79, 1991.

[2] Anju and R. K. Sharma. Existence of some special primitive normal elements over finite fields. *Finite Fields Appl.*, 46:280–303, 2017.

[3] A. Booker, S. D. Cohen, N. Sutherland, and T. Trudgian. Primitive values of quadratic polynomials in a finite field. *Math. Comp.*, 88(318):1903–1912, 2019.

[4] W. S. Chou and S. D. Cohen. Primitive elements with zero traces. *Finite Fields Appl.*, 7(1):125–141, 2001.

[5] S. D. Cohen. Pairs of primitive elements in fields of even order. *Finite Fields Appl.*, 28:22–42, 2014.

[6] S. D. Cohen and A. Gupta. Primitive element pairs with a prescribed trace in the quartic extension of a finite field. *J. Algebra Appl.*, 2020, DOI: https://doi.org/10.1142/S0219498821501681.

[7] S. D. Cohen and S. Huczynska. The primitive normal basis theorem–without a computer. *Lond. Math. Soc.*, 67(2):41–56, 2003.

[8] S. D. Cohen, H. Sharma, and R. Sharma. Primitive values of rational functions at primitive elements of a finite field. *J. Number Theory*, 219:237–246, 2021.

[9] L. Fu and D. Wan. A class of incomplete character sums. *Q. J. Math.*, (4):1195–1211, 2018.

[10] A. Gupta, R. K. Sharma, and S. D. Cohen. Primitive element pairs with one prescribed trace over a finite field. *Finite Fields Appl.*, 54:1–14, 2018.

[11] H. W. Lenstra Jr. and R. J. Schoof. Primitive normal bases for finite fields. *Math. Comp.*, 48(177):217–231, 1987.

[12] R. Lidl and H. Niederreiter. *Finite fields*, volume 20. Cambridge Univ. Press, Cambridge (UK), 1997.

[13] H. Sharma and R. K. Sharma. Existence of primitive pairs with prescribed traces over finite fields. *Comm. Algebra*, 2020, DOI: https://doi.org/10.1080/00927872.2020.1852243.

[14] R. K. Sharma, A. Awasthi, and A. Gupta. Existence of pair of primitive elements over finite fields of characteristic 2. *J. Number Theory*, 193:386–394, 2018.

[15] R. K. Sharma and A. Gupta. Pair of primitive elements with prescribed traces over finite fields. *Comm. Algebra*, 47:1278–1286, 2017.

[16] F. Shuqin and H. Wenbao. Character sums over galois rings and primitive polynomials over finite fields. *Finite Fields Appl.*, 10(1):36–52, 2004.