http://ijgt.ui.ac.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. x No. x (202x), pp. xx-xx.
© 2022 University of Isfahan
www.ui.ac.ir

EXISTENCE OF RATIONAL PRIMITIVE NORMAL PAIRS OVER FINITE FIELDS

RAJENDRA KUMAR SHARMA*, SONIYA TAKSHAK, AMBRISH AWASTHI AND HARIOM SHARMA

Abstract. For a finite field $\mathbb{F}_{q^n}$ and a rational function $f = \frac{f_1}{f_2} \in \mathbb{F}_{q^n}(x)$, we present a sufficient condition for the existence of a primitive normal element $\alpha \in \mathbb{F}_{q^n}$ in such a way $f(\alpha)$ is also primitive in $\mathbb{F}_{q^n}$, where $f(x)$ is a rational function in $\mathbb{F}_{q^n}(x)$ of degree sum m (degree sum of $f(x) = \frac{f_1(x)}{f_2(x)}$ is defined to be the sum of the degrees of $f_1(x)$ and $f_2(x)$). Additionally, for rational functions of degree sum 4, we proved that there are only 37 and 16 exceptional values of (q, n) when $q = 2^k$ and $q = 3^k$ respectively.

1. Introduction

Let $\mathbb{F}_q$ denotes a finite field of $q = p^k$ elements. We call an element $\alpha \in \mathbb{F}_q$ to be *primitive* if it is a generator of the multiplicative cyclic group $\mathbb{F}_q^*$ consisting of non-zero elements of $\mathbb{F}_q$. Primitive elements have several applications in cryptography and coding theory[14]. A *normal element* of a finite field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is an element $\alpha \in \mathbb{F}_{q^n}$ such that $\{\alpha, \alpha^q \cdots \alpha^{q^n-1}\}$ forms a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. If α is both primitive and normal element of $\mathbb{F}_{q^n}$, then α is called a *primitive normal element*. For every q and n, the field $\mathbb{F}_{q^n}$ has a normal element over $\mathbb{F}_q$ [13].

Existence of primitive pairs $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q$, is a fascinating problem. If α and $f(\alpha)$ both are primitive in $\mathbb{F}_q$, a pair $(\alpha, f(\alpha))$ in $\mathbb{F}_q \times \mathbb{F}_q$ is said to be a *primitive pair*, where $f(x) \in \mathbb{F}_q(x)$ is a rational function. Another interesting problem is the existence of primitive normal pairs defined as $(\alpha, f(\alpha))$ in $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$, such that α is both primitive as well as normal and $f(\alpha)$ is primitive.

Communicated by Victor Bovdi.

MSC(2010): Primary: 12E20; Secondary: 11T23.

Keywords: Finite Field, Primitive Element, Normal Element, Character.

Article Type: Research Paper.

Received: 10 March 2022, Accepted: 04 July 2022.

*Corresponding author.

http://dx.doi.org/10.22108/IJGT.2022.133016.1784 .

For all field extensions $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$, Lenstra and Schoof [12] proved the existence of primitive normal elements. Cohen and Huczynska [6] provided the first proof of the above result which was computer-free. Kapetanakis [11] studied the existence of primitive pairs of the form $(\alpha, f(\alpha) = \frac{a\alpha+b}{c\alpha+d})$, where both α and $f(\alpha)$ are normal elements. Anju and Sharma [1] also studied the existence problem of primitive normal pairs $(\alpha, f(\alpha) = \frac{a\alpha^2+b\alpha+c}{d\alpha+e})$ in $\mathbb{F}_{q^n}$, by taking $f(x) = \frac{ax^2+bx+c}{dx+e} \in \mathbb{F}_{q^n}(x)$. Sharma et al. [17] further generalized $f(x)$ to $\frac{ax^2+bx+c}{dx^2+ex+f}$ and studied the existence of primitive pairs $(\alpha, f(\alpha) = \frac{a\alpha^2+b\alpha+c}{d\alpha^2+e\alpha+f})$ in $\mathbb{F}_{2^k}$. Recently, Carvalho et. al [2] studied the existence of pairs $(\alpha, f(\alpha) = \frac{f_1(\alpha)}{f_2(\alpha)})$, where α is both primitive and normal and $f(\alpha)$ is primitive. But they considered $f(x) = \frac{f_1(x)}{f_2(x)}$ to be a rational function such that there exists at least one monic irreducible polynomial $g \in \mathbb{F}_q[x]$ other than x and a positive integer n with $gcd(n, q-1) = 1, g^n | f_1 f_2$ but $g^{n+1} \nmid f_1 f_2$. In this article we prove the existence of such elements for more general rational functions(discussed in [8]) as detailed below. Clearly, the family of rational functions considered by Carvalho et. al is properly contained in the family which we are discussing in this article. For example, $\frac{(x-2)^2}{(x+2)^3} \in \mathbb{F}_7[x]$ is a rational function that does not belong to the family considered by Carvalho et. al. Also, existence of primitive pairs $(\alpha, f(\alpha))$ such that both α and $f(\alpha)$ are normal have been discussed in [15], where the class of functions used is a subclass of our function class.

If $f = \frac{f_1}{f_2} \in \mathbb{F}_{q^n}(x)$ then *degree sum* of f is defined to be $degsum(f) = deg(f_1) + deg(f_2)$, where, $deg(f_i), i = 1, 2$ are the degrees of polynomials $f_1(x)$ and $f_2(x)$ respectively. Next, we can consider $f_2(x)$ to be monic as $f_1(x)$ and $f_2(x)$ can be divided by the leading coefficient of $f_2(x)$. Further, we impose some restrictions on the rational function $f(x)$ and call that $f(x)$ is an exceptional function whenever $f = cx^j g^d$ for some $c \in \mathbb{F}_{q^n}, j \in \mathbb{Z}$(the set of integers), $g \in \mathbb{F}_{q^n}(x)$ and $d > 1$ is a divisor of $q^n - 1$ or $f(x) = x^j$ for some $j \in \mathbb{Z}$ such that $gcd(q^n - 1, j) \neq 1$. For $m_1, m_2 \in \mathbb{N} \cup \{0\}, S_{q,n}(m_1, m_2)$ denote the set of rational functions $f(x) = \frac{f_1(x)}{f_2(x)} \in \mathbb{F}_{q^n}(x)$ with $deg(f_1) \leq m_1$ and $deg(f_2) \leq m_2$, which are non-exceptional. Let T_{m_1,m_2} denote the set of pairs (q, n) such that for each $f \in S_{q,n}(m_1, m_2)$ there exist a primitive normal pair $(\alpha, f(\alpha)), \alpha \in \mathbb{F}_{q^n}$. Define $S_{q,n}(m) = \cup_{m_1+m_2=m} S_{q,n}(m_1, m_2)$ and $T_m = \cap_{m_1+m_2=m} T_{m_1,m_2}$.

The article is organized as follows. A sufficient condition for the existence of primitive pairs $(\alpha, f(\alpha))$ in $\mathbb{F}_{q^n}$ with α normal over $\mathbb{F}_q$ has been obtained in section 3. Further, in section 4, we discussed the case when the degree sum of $f(x)$ is 4, that is, $m = 4$.

2. Preliminaries

$\mathbb{F}_q$ denotes a finite field with $q = p^k$ elements and $\mathbb{F}$ denotes the algebraic closure of $\mathbb{F}_{q^n}$ throughout the article. For primary results related to finite fields and characters reader is referred to [13].

Definition 2.1. *Let $s|q^n - 1$. An element $w \in \mathbb{F}_{q^n}^*$ is s- free, whenever $w = v^d$, for some $v \in \mathbb{F}_{q^n}^*$ and $d|s$ implies $d = 1$. Hence an element in $\mathbb{F}_{q^n}^*$ is primitive if and only if it is $(q^n - 1)$-free.*

Given any $\gamma \in \mathbb{F}_{q^n}$ and $f(x) = \sum_{i=0}^{r} a_i x^i \in \mathbb{F}_q[x]$. An action of $\mathbb{F}_q[x]$ over $\mathbb{F}_{q^n}$ can be defined by $f \circ \gamma = \sum_{i=0}^{n} a_i \gamma^{q^i}$. Then the additive group of $\mathbb{F}_{q^n}$ can be considered as an $\mathbb{F}_q[x]$ module.

http://dx.doi.org/10.22108/IJGT.2022.133016.1784

Definition 2.2. *Given $\beta \in \mathbb{F}_{q^n}$, the least degree unique polynomial $g(x) \in \mathbb{F}_q[x]$ such that $g(x)|x^n-1$ and $g \circ \beta = 0$ is said to be the $\mathbb{F}_q$ order of β and is denoted by $O(\beta)$.*

If $O(\beta)$ is g then there exist $\alpha \in \mathbb{F}_{q^n}$ such that $\beta = h \circ \alpha$ and $h(x)|(x^n-1)$.

Definition 2.3. *For a divisor $g(x)$ of (x^n-1), $\beta \in \mathbb{F}_{q^n}^*$ is said to be a $g-$ free element if for any $h(x)|g(x)$ and $\alpha \in \mathbb{F}_{q^n}, \beta = h(x) \circ \alpha$ implies $h(x) = 1$. Clearly, β is normal over $\mathbb{F}_q$ if and only if it is (x^n-1) free.*

Let $\widehat{\mathbb{F}_{q^n}}$ denotes the set of all additive characters of $\mathbb{F}_{q^n}$ and set of multiplicative characters of $\mathbb{F}_{q^n}^*$ are denoted by $\widehat{\mathbb{F}_{q^n}^*}$. An action of $\mathbb{F}_q[x]$ over $\widehat{\mathbb{F}_{q^n}}$ can be defined by

$$(\psi \circ f)(\beta) = \psi \circ f(\beta),$$

for any $\psi \in \widehat{\mathbb{F}_{q^n}}$, $f \in \mathbb{F}_q[x]$ and $\beta \in \mathbb{F}_{q^n}$. Then $\widehat{\mathbb{F}_{q^n}}$ is an $\mathbb{F}_q[x]$ module.

Definition 2.4. *Let g be a unique monic polynomial of the smallest degree such that $g|x^n-1$. Then g is said to be the $\mathbb{F}_q$ order of any additive character ψ_g of $\mathbb{F}_{q^n}$ if and only if $\psi_g \circ g$ is the trivial additive character of $\mathbb{F}_{q^n}$.*

Since $\widehat{\mathbb{F}_{q^n}^*}$ is a cyclic group[13], $\phi(d)$ provides the number of multiplicative characters of order d of $\mathbb{F}_{q^n}$, where $d|q^n-1$. Analogously, $\Phi_q(g)$ provides the number of additive characters ψ_g, where $\Phi(g) = |(\mathbb{F}_q[x]/g\mathbb{F}_q[x])^*|$.

Like Cohen and Huczynska [6, 7], the characteristic function for the subset of s-free elements $(s|q^n-1)$ of $\mathbb{F}_{q^n}^*$ is given by

$$\rho_s : \alpha \mapsto \theta(s) \sum_{d|s} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d} \chi_d(\alpha),$$

where $\theta(s) := \frac{\phi(s)}{s}$, μ denotes the Möbius function, and χ_d is any multiplicative character of order d. Analogously, the characteristic function for the set of g free elements, $g|(x^n-1)$, is given by,

$$K_g : \alpha \longmapsto \lambda(g) \sum_{h|g} \frac{\mu'(h)}{\Phi_q(h)} \sum_{\psi_h} \psi_h(\alpha),$$

where $\lambda(g) \coloneqq \frac{\Phi_q(g)}{q^{deg(g)}}$, μ' denotes the analogue of the Möbius function, given as

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

We will use the following Lemmas to prove the results in the next section.

Lemma 2.5. [3] *Let $F(x) \in \mathbb{F}_q(x)$ be a rational function. Write $F(x) = \prod_{j=1}^{k} F_j(x)^{r_j}$, where $F_j(x) \in \mathbb{F}_q[x]$ are irreducible polynomials and r_j are nonzero integers. Let χ be a multiplicative character of*

$\mathbb{F}_q^*$ of precise square-free order d(a divisor of $q-1$). Suppose that $F(x)$ is not of the form $cG(x)^d$ for some rational function $G(x) \in \mathbb{F}_q(x)$ and $c \in \mathbb{F}_q*$. Then we have

$$\left| \sum_{\alpha \in \mathbb{F}_q, F(\alpha) \neq \infty} \chi(F(\alpha)) \right| \leq \Big(\sum_{j=1}^{k} deg(F_j) - 1 \Big) q^{1/2},$$

Lemma 2.6. [9, Theorem 5.6] *Let χ be a multiplicative character of order r and ψ be a non-trivial additive character of $\mathbb{F}_{q^n}$. Let f and g be rational functions in $\mathbb{F}_{q^n}(x)$. Write $f(x) = \prod_{j=1}^{k} f_j(x)^{r_j}$, where $f_j(x) \in \mathbb{F}_{q^n}[x]$ are irreducible polynomials and r_j are nonzero integers. Suppose that $g \neq h^{q^n} - h$, for any $h \in \mathbb{F}(x)$. Then*

$$\left| \sum_{\alpha \in \mathbb{F}_{q^n}, f(\alpha) \neq 0, \infty, g(\alpha) \neq \infty} \chi(f(\alpha)) \psi(g(\alpha)) \right| \leq (M_1 + M_2 + M_3 + M_4 - 1) q^{n/2},$$

where $M_1 = \sum_{j=1}^{r} deg(f_j)$, $M_2 = max(deg(g), 0)$, M_3 is the degree of the denominator of $g(x)$ and M_4 is the sum of the degrees of those irreducible polynomials dividing the denominator of g, but distinct from $f_j(x) (j = 1, 2, \ldots, r)$.

3. Sufficient Condition for the Existence of Primitive Normal Pairs

Let $q = p^k$ and l_1, l_2 denote positive integers dividing $q^n - 1$. Suppose $N_f(l_1, l_2, g)$ is the number of pairs $(\alpha, f(\alpha))$ such that α is l_1-free, $f(\alpha)$ is l_2-free and α is g free. Hence in order to prove that $(q, n) \in T_m$, we need to show that $N_f(q^n - 1, q^n - 1, x^n - 1) > 0$ for every $f \in \mathbb{F}_{q^n}(x)$. If $n = 1$ and $q = 2^k$, then $(q, n) \in T_m$ (refer [8]) as primitive normal pairs become just the primitive pairs, and the problem is reduced to the existence problem of primitive pairs. If $n = 2$ and $q = 2^k$, then every primitive element of $\mathbb{F}_{q^2}$ is a normal element and the reader is again referred to [8]. Hence we assume that $n \geq 3$.

Let $\Omega_q(g)$ and $\omega(l)$ denote the number of monic irreducible divisors of g, and the number of prime divisors of l respectively. Also, $W(l)$ and $W(g)$ are the number of square free divisors of l and g. Define $\theta(l_1, l_2) = \theta(l_1)\theta(l_2)$. We start our discussion by proving a sufficient condition for the existence of l_1-free and g-free element $\alpha \in \mathbb{F}_{q^n}$ such that $f(\alpha)$ is l_2-free.

Lemma 3.1. *Let q, m and $n \geq 3$ are natural numbers and q be a prime power such that $q^{\frac{n}{2}} > (m+1)W(l_1)W(l_2)W(g)$. Then $N_f(l_1, l_2, g) > 0$, where $l_1, l_2 | q^n - 1$ and $g | x^n - 1$.*

Proof. Let R_1 be the set containing zeros and poles of $f(x)$ in $\mathbb{F}_{q^n}$ and $R = R_1 \cup \{0\}$. Then

$$N_f(l_1, l_2, g) = \sum_{\alpha \in \mathbb{F}_{q^n} \setminus R} \rho_{l_1}(\alpha) \rho_{l_2}(f(\alpha)) K_g(\alpha)$$

$$N_f(l_1, l_2, g) = \theta(l_1, l_2)\lambda(g) \sum_{d_1 | l_1, d_2 | l_2, h | g} \frac{\mu(d_1)\mu(d_2)\mu^{'}(h)}{\phi(d_1)\phi(d_2)\Phi_q(h)} \sum_{\chi_{d_1}, \chi_{d_2}, \psi_h} \chi_f(\chi_{d_1}, \chi_{d_2}, \psi_h) \tag{3.1}$$

http://dx.doi.org/10.22108/IJGT.2022.133016.1784

where $\chi_f(\chi_{d_1}, \chi_{d_2}, \psi_h) = \sum_{\alpha \in \mathbb{F}_{q^n} \setminus R} \chi_{d_1}(\alpha)\chi_{d_2}(f(\alpha))\psi_h(\alpha)$.
Since $d_1, d_2 | (q^n - 1)$, there exist n_1, n_2 in the set $\{0, 1, \ldots, q^n - 2\}$ such that $\chi_{d_i}(\alpha) = \chi_{q^n-1}(\alpha^{n_i})$ for $i \in \{1, 2\}$, and $\psi_h(\alpha) = \psi_{x^n-1}(y_1\alpha)$ for some $y_1 \in \mathbb{F}_{q^n}$[13]. Hence

$$\chi_f(\chi_{d_1}, \chi_{d_2}, \psi_h) = \sum_{\alpha \in \mathbb{F}_{q^n} \setminus R} \chi_{q^n-1}(F(\alpha))\psi_{x^n-1}(G(\alpha))$$

where $F(x) = x^{n_1}(f(x))^{n_2}$ for $n_1, n_2 \in \{1, 2, \ldots, q^n - 2\}$ and $G(x) = y_1 x \in \mathbb{F}_{q^n}(x)$. Here, if $G(x)$ is not of the form $h(x)^{q^n} - h(x)$, for any $h(x) \in \mathbb{F}(x)$ then from lemma 2.6

$$|\chi_f(\chi_{d_1}, \chi_{d_2}, \psi_h)| \leq (m + 1)q^{n/2}.$$

Clearly, it is possible to write $y_1 x = h(x)^{q^n} - h(x)$, for some $h(x) \in \mathbb{F}(x)$, if and only if $y_1 = 0$. Hence in this case,

$$\chi_f(\chi_{d_1}, \chi_{d_2}, \psi_h) = \sum_{\alpha \in \mathbb{F}_{q^n} \setminus R} \chi_{q^n-1}(F(\alpha)).$$

If $F(x) \neq yh(x)^{q^n-1}$ for any $y \in \mathbb{F}_{q^n}$ and $h(x) \in \mathbb{F}_{q^n}(x)$ then using Lemma 2.5 we obtain

$$|\chi_f(\chi_{d_1}, \chi_{d_2}, \psi_h)| \leq mq^{n/2} + m < (m + 1)q^{n/2}.$$

Now if $F = yh(x)^{q^n-1}$ for some $y \in \mathbb{F}_{q^n}$ and $h \in \mathbb{F}_{q^n}(x)$ then following [8], we have f is exceptional. Now referring previous computations, we get

$$|\chi_f(\chi_{d_1}, \chi_{d_2}, \psi_h)| < (m + 1)q^{\frac{n}{2}}$$

when $(\chi_{d_1}, \chi_{d_2}, \psi_h) \neq (\chi_1, \chi_1, \psi_1)$. Therefore,

$$\begin{aligned} N_f(l_1, l_2, g) &\geq \theta(l_1, l_2)\lambda(g)\{q^n - |R| - (m + 1)q^{\frac{n}{2}}(W(l_1)W(l_2)W(g) - 1)\} \\ &\geq \theta(l_1, l_2)\lambda(g)\{q^n - (m + 1) - (m + 1)q^{\frac{n}{2}}(W(l_1)W(l_2)W(g) - 1)\}. \end{aligned}$$

Hence $N_f(l_1, l_2, g) > 0$ if $q^n > (m + 1) + (m + 1)q^{\frac{n}{2}}(W(l_1)W(l_2)W(g) - 1)$ i.e.

$$q^{\frac{n}{2}} > (m + 1)W(l_1)W(l_2)W(g). \tag{3.2}$$

□

From the above lemma we have $N_f(q^n - 1, q^n - 1, x^n - 1) > 0$ if

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

3.1. **Sieving Results.** In this section, we state some results related to the sieving technique. Condition (3.2) is further improved in the next theorem, and the proof is similar to [10, Theorem 3.4].

Theorem 3.2. *Suppose $l | q^n - 1$ and $p_1, p_2, \ldots, p_s$ are the irreducible primes dividing $q^n - 1$. Also, let $E | x^n - 1$ and $P_1, P_2, \ldots, P_t$ are the remaining irreducible polynomials dividing $x^n - 1$. Set $\delta = 1 - 2\sum_{i=1}^{s} \frac{1}{p_i} - \sum_{i=1}^{t} \frac{1}{q^{deg(P_i)}}$ and $S = \frac{2s+t-1}{\delta} + 2$. Assume $\delta > 0$, then $(q, n) \in T_m$ if*

$$q^{\frac{n}{2}} > (m + 1)SW(l)^2 W(E) \tag{3.3}$$

http://dx.doi.org/10.22108/IJGT.2022.133016.1784

In particular, when $l = q^n - 1$ and $E = x^{n'} - 1$, we get

$$q^{\frac{n}{2}} > (m+1)W(q^n-1)^2 W(x^{n'}-1). \tag{3.4}$$

More improvement in the condition has been done in [5]. However, in our case the proof follows on the lines of [16], for which notations and conventions are quoted below.

"Let $Rad(q^n-1) = kPL$, where k is the product of smallest prime divisors of q^n-1, L is the product of large prime divisors of q^n-1 denoted by $L = l_1 \cdot l_2 \cdots l_t$, and the rest of the prime divisors of q^n-1 lie in P and denoted by $p_1, p_2, \ldots, p_r$. Similarly, $Rad(x^n-1) = gGH$, where g is the product of irreducible factors of x^n-1 of least degree. Irreducible factors of large degree are factors of H which are denoted by $h_1, h_2, \ldots, h_u$ and the rest of the factors lie in G and are denoted by $g_1, g_2, \ldots, g_s$"[16].

The Modified Prime Sieve:

Theorem 3.3. *Let $n, q \in \mathbb{N}$ such that q is a prime power and $n \geq 3$. Using the above notations, let $Rad(q^n-1) = kPL, Rad(x^n-1) = gGH, \delta = 1 - 2\sum_{i=1}^{r}\frac{1}{p_i} - \sum_{i=1}^{s}\frac{1}{q^{deg(g_i)}}, \epsilon_1 = \sum_{i=1}^{t}\frac{1}{l_i}, \epsilon_2 = \sum_{i=1}^{u}\frac{1}{q^{deg(h_i)}}$ and $\delta\theta(k)^2\lambda(g) - (2\epsilon_1+\epsilon_2) > 0$. Then*

$$\begin{aligned} q^{\frac{n}{2}} > \Bigg[& (m+1)\theta(k)^2\lambda(g)W(k)^2W(g)(2r+s-1+2\delta) + (m-1)(t-\epsilon_1) \\ & + \left(\frac{2m(t-\epsilon_1)+(m+1)(u-\epsilon_2)}{q^{\frac{n}{2}}}\right)\Bigg] / [\delta\theta(k)^2\lambda(g) - (2\epsilon_1+\epsilon_2)] \end{aligned} \tag{3.5}$$

implies $(q,n) \in T_m$.

4. When $f(x)$ is a rational function of degree sum 4

In this section, we demonstrate the application of above results by working with the rational functions of degree sum 4. By choosing rational functions of degree sum 4, and following the steps used for computations in [1], we get the results stated in Theorem 4.1 and found that the results in [1] for $q = 2^k$ are applicable for more general rational functions as stated below.

Theorem 4.1. *Let $\mathbb{F}_{q^n}$ be a finite extension of $\mathbb{F}_q$ of degree $n \geq 3$, where $q = 2^k$. Suppose that $f(x) \in S_{q,n}(4)$. Then $\mathbb{F}_{q^n}$ contains a primitive normal pair $(\alpha, f(\alpha))$ with the following possible exceptions* $(2,2), (2,3), (2,4), (2,5), (2,7), (2,6), (2,8), (2,9), (2,10), (2,12), (2,14), (2,15), (2,16), (2,18), (2,20), (2,24), (4,2), (4,3), (4,4), (4,5), (4,6), (4,7), (4,8), (4,9), (4,10), (4,12), (8,2), (8,3), (8,4), (8,7), (16,2), (16,3), (16,4), (16,5), (16,6), (32,2), (64,2)$.

Note: $(2,11)$ is an exception in [1] but not in Theorem 4.1, because it satisfies the modified prime sieve (refer Table 4.1a).

For more precise demonstration, we consider $q = 3^k$ and $f \in S_{q,n}(4), n \geq 3$ and proved the following Theorem.

Theorem 4.2. *Let $\mathbb{F}_{q^n}$ be a finite extension of $\mathbb{F}_q$ of degree $n \geq 3$, where $q = 3^k$. Suppose that $f(x) \in S_{q,n}(4)$. Then $\mathbb{F}_{q^n}$ contains a primitive normal pair $(\alpha, f(\alpha))$ with the following possible exceptions* $(3,3),(3,4),(3,5),(3,6),(3,7),(3,8),(3,9),(3,10),(3,12),(3,16),(9,3),(9,4),(9,6),(9,8),(27,4),(81,3)$.

To proceed further, first we assume $n = n'3^j$, where $j \geq 0$ is an integer and $\gcd(3, n') = 1$. We split the discussion depending upon the values of n', the one when $n'|q-1$ and the other when $n' \nmid q-1$. Throughout the remaining part of the article, let $\omega = \omega(q^n - 1)$ unless otherwise specified.

Case A. $\mathbf{n'|q-1}$

We know that whenever $n'|q-1, x^{n'} - 1$ is a product of n' distinct linear factors in $\mathbb{F}_q$[13]. We will use this fact further to calculate the value of S used in theorem 3.2. The proof of the following lemma follows from the idea of [4, Lemma 6.2].

Lemma 4.3. *Let m be an even positive integer. Then $W(m) < 11.25m^{1/5}$.*

Lemma 4.4. *Let $q = 3^k$, for some positive integer k and $n'|q-1$. If $n' \geq 25$ then $(q,n) \in T_4$.*

Proof. Using Lemma 4.3, we get $W(q^n - 1) \leq 11.25q^{n/5}$. If we take $E = 1$, we see that, $(q,n) \in T_4$ if $q^{n/10} > 633S$. Let us first suppose that $n' = q-1$, then $S = q^2 - 2q + 2 < q^2$, and inequality (3.3) is satisfied if

$$q^{\frac{q-1}{10}-2} > 633$$

Which holds if $q \geq 81$. Now, if $q \geq 81$ and $25 \leq n' \leq \frac{q-1}{2}$ then $S < q$. Hence $(q,n) \in T_4$ if $q^{\frac{n'}{10}-1} > 633$. Clearly for $n' \geq 25$, $q^{\frac{n'}{10}-1} > 633$ holds for all $q \geq 81$ and for $(27,26)$, (3.4) is satisfied. Hence the proof follows. □

We discuss the remaining values of n' below. In the subsequent discussion, Table no. 3 and 4 can be accessed from the Appendix.

(**1**) If $\mathbf{n' = 1}$. Hence, $n = 3^j$ for some $j \geq 1$. Taking $E = x - 1$ and $l = q^n - 1$, we get $S = 1$, now $(q,n) \in T_4$ if

$$q^{\frac{3^j}{10}} > 1266 \tag{4.1}$$

We observe that (4.1) is true for $q \geq 3^{22}$ if $j \geq 1$ and it fails for $q = 3, 9, j = 1, 2, 3; q = 3^3, 3^4, 3^5, 3^6, 3^7$, $j = 1, 2; q = 3^8, 3^9, 3^{10}, 3^{11}, j = 1$. Now, we calculate the value of ω for the remaining pairs (q,n) for which (4.1) is not true and got that (3.4) is satisfied, except for $(3,3),(3,9),(9,3),(9,9),(27,3),(81,3)$, $(3^6,3)$. For these values of (q,n), we checked (3.3) for different values of l and E, and got it verified except $(3,3),(3,9),(9,3),(81,3)$. (refer Table 3)

(**2**) If $\mathbf{n' = 2}$. Hence, $n = 2\cdot 3^j$ for some $j \geq 1$. Similar to above step if we choose $E = 1$ and $l = q^n - 1$, we get $W(E) = 1$ and $S = 2 + \frac{q}{q-2} \leq 5$, now $(q,n) \in T_4$ if

$$q^{\frac{2\cdot 3^j}{10}} > 633 \times 5 \tag{4.2}$$

Now (4.2) is true for $q \geq 3^{13}$ and fails for $q = 3^2, 3^3, 3^4$ when $j = 1, 2$ and for $3^k, 5 \leq k \leq 12$ when $j = 1$. Now we calculate the value of ω for the remaining pairs (q,n) for which (4.2) does

not hold and determine whether (3.4) is satisfied or not, and found that only possible exceptions are $(3,6),(3,18),(9,6)$ and $(27,6)$.

Now, for these possible exceptions, we choose other values of l, E and verified that the inequality (3.3) is true except $(3,6),(9,6)$. (refer Table 3)

(**3**) If $\mathbf{n'=4}$. Hence, $n=4\cdot 3^j$ for some $j\geq 0$. Taking $E=1$ and $l=q^n-1$, we get $S=2+\frac{3q}{q-4}\leq 7.4$, now $(q,n)\in T_4$ if

$$(q)^{\frac{4\cdot 3^j}{10}} > 633\times 7.4 \tag{4.3}$$

It is clear that (4.3) holds for $q\geq 3^{19}$, and does not hold for $q=9, j=0,1,2$; $q=3^4,3^6, j=0,1$ and $q=3^k, k=6,8,10,12,14,16,18, j=0$. Now for these values, we evaluate the exact value of ω and see that the inequality (3.4) is valid except $(9,12),(3^4,4),(3^6,4)$. For these, we checked (3.3) for different values of l and E, and got it verified as described in Table 3.

For $5\leq n'\leq 24$ such that $\gcd(n',3)=1$, we follow the same procedure of $n'=4$ and get two exceptions $(9,4),(9,8)$, when $n'|q-1$. (refer Table 3)

Hence all the exceptions are $(3,3),(3,6),(3,9),(9,3),(9,4),(9,6),(9,8),(81,3)$, when $n'|q-1$.

Theorem 4.5. *Let $\mathbb{F}_{q^n}$ be a finite extension of $\mathbb{F}_q$ of degree $n\geq 3$, where $q=3^k, k\in\mathbb{N}$. Assume $f(x)\in S_{q,n}(4)$. If $n'|q-1$, then there exists a primitive normal pair $(\alpha, f(\alpha))$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ unless (q,n) is one of the pairs $(3,3),(3,6),(3,9),(9,3),(9,4),(9,6),(9,8),(81,3)$.*

Case B. $\mathbf{n'\nmid q-1}$

Let the order of q mod n' be v'. Then x^n-1 is a product of irreducible polynomials having degree less than or equal to v'. Particularly, $v'\geq 2$ if $n'\nmid q-1$. Let N' denotes the number of distinct irreducible factors of x^n-1 over $\mathbb{F}_q$ having degree less than v'. Suppose $\rho(q,n)$ represents the following ratio

$$\rho(q,n)=\frac{N'}{n}.$$

It is clear that $n\rho(q,n)=n'\rho(q,n')$. The following upper bounds for $\rho(q,n')$ will be used further.

Lemma 4.6. [4] *Suppose $q=3^k$, for some positive integer k and n is an integer such that n' does not divide $q-1$. If E is the product of irreducible factors of x^n-1 of degrees less than v', then $S<n'$.*

Lemma 4.7. [6] *Assume that $n'>3$. Then the following bounds hold, where $n_1=\gcd(n',q-1)$.*
(1) *For $n'=2n_1(q$ odd$)$; $\rho=1/2$; for $n'=4n_1(q\equiv 1(\mathrm{mod}4))$; $\rho=3/8$; for $n'=6n_1(q\equiv 1(\mathrm{mod}6))$; $\rho=13/36$; otherwise $\rho(q,n')\leq 1/3$.*
(2) *$\rho(3,16)=5/16$; otherwise, $\rho(3,n')\leq 1/4$.*

Lemma 4.8. *Suppose $m=q^n-1$, where q is odd, then $W(m)<245m^{1/7}$.*

We divide our further discussion into two parts depending upon the values of q, when $q=3$ and $q>3$. First, we note that $n'=1$ and 2 divides $q-1$ for all $q=3^k$ which we have discussed in case A. Since $n'=3$ is not possible, we need to discuss when $n'>3$.

When $\mathbf{q=3}$: Let us first suppose that $n'=16$. Then $x^{n'}-1$ can be written as a product of two

linear, three quadratic and two quartic factors over $\mathbb{F}_q$. Because $n \geq n'$, first we consider that $n > n'$, then $n = 16 \cdot 3^r, r \geq 1$. Let $l = q^n - 1$ and $E = x + 1$. Then $\delta = 1 - \frac{1}{3} - \frac{3}{9} - \frac{2}{81} = \frac{25}{81}$ and $S = \frac{91}{5} = 18.2$. From (3.3) and lemma 4.3, to get $N_f(q^n - 1, q^n - 1, x^n - 1) > 0$, it is enough to show that $3^{\frac{16 \cdot 3^r}{10}} > 633 \times 18.2 \times 2$. This holds when $r \geq 2$. For $r = 1$, we have $\omega = 12$ which implies (3.3) holds. Now suppose $n = n'$, we got that (3.3) does not hold and hence we consider $(3, 16)$ to be an exception.

Now if $n' \neq 16$, then by Lemma 4.7, $\rho \leq 1/4$. By using Lemma 4.6 and Lemma 4.8, inequality (3.3) is satisfied if $3^{3n/14} > 300125n2^{n/4}$. This holds for $n \geq 295$. Now suppose that $n \leq 294$. But then $\omega \leq 69$ and $3^{n/2} > 5n2^{2\omega+n/4}$ holds for $n \geq 274$. Repeating this process multiple times, we can consider $n \leq 232$. For remaining (q, n), we calculated the exact value of ω and checked $3^{n/2} > 5n2^{2\omega+n/4}$ holds for all (q, n) except the pairs for which $4 \leq n \leq 25$, and $n = 30, 32, 34, 36, 42, 48, 54$. By taking other suitable choices of l and E for each of these, we see that (3.3) is satisfied except $n = 4, 5, 7, 8, 10, 11, 12, 13, 16$ (refer Table 4).

Hence all (q, n) with $q = 3$ and n such that $n' \nmid q-1$ are in T_4 except $(3, 4), (3, 5), (3, 7), (3, 8), (3, 10)$, $(3, 11), (3, 12), (3, 13), (3, 16)$.

When q > 3 : From lemma 4.7 we divide the discussion into four parts:

1. $n' = 2n_1 (q$ is odd $)$
2. $n' = 4n_1 (q \equiv 1 \bmod 4)$
3. $n' = 6n_1 (q \equiv 1 \bmod 6)$
4. $n' \neq 2n_1, 4n_1, 6n_1$

Let E is the product of irreducible factors of $x^n - 1$ having degree less than v'. Then for $N_A(q^n - 1, q^n - 1, x^n - 1) > 0$, using lemma 4.8 it is sufficient to show that

$$q^{n/2} > 5S(245)^2 q^{2n/7} 2^{n\rho(q,n')} \tag{4.4}$$

1. When $\mathbf{n' = 2n_1}$, by Lemma 4.7 $\rho = 1/2$ and hence (4.4) is equivalent to $q^{3n/14} > 300125n2^{n/2}$. This holds for $q = 9$ when $n \geq 142$, while for $q \geq 27$ it is true when $n \geq 46$. Note that, for $q = 9$, only possible value of n' is 16. Hence the possible exceptions are $(9, 16), (9, 48)$. Further, when $q \geq 27$, and $q^n < 27^{46}$, we checked $q^{n/2} > 5n2^{2\omega+n/2}$ along with above two exceptions. This holds except $(9, 16), (27, 4), (27, 12), (243, 4)$.

2. When $\mathbf{n' = 4n_1} (q \equiv 1 \bmod 4)$, by Lemma 4.7 $\rho = 3/8$ and (4.4) is equivalent to $q^{3n/14} > 300125n2^{3n/8}$. This holds for $q = 9$ when $n \geq 81$, while for $q \geq 81$ it is true when $n \geq 24$. clearly, for $q = 9$, only possible value of n' is 32. Therefore possible exception is $(9, 32)$. Further, when $q \geq 81$, and $q^n < 81^{24}$, we verified that the condition $q^{n/2} > 5n2^{2\omega+3n/8}$ holds for all values of (q, n) along with $(9, 32)$.

3. When $\mathbf{n' = 6n_1} (q \equiv 1 \bmod 6)$, by Lemma 4.7 $\rho = 13/36$. This case is not possible as $3^k \not\equiv 1 \bmod 6$ for any value of k.

4. When $\mathbf{n' \neq 2n_1, 4n_1, 6n_1}$, $\rho(q, n') \leq 1/3$ and (4.4) is equivalent to $q^{3n/14} > 300125n2^{n/3}$. This holds for $q \geq 9$ when $n \geq 71$. Now for $q^n < 9^{71}$, we calculate the value of ω and check whether $q^{n/2} >$

$5n2^{2\omega+n/3}$ is true and got it verified except $(9,5),(9,7),(9,10),(9,11),(9,14),(9,15),(27,5),(27,8),(27,10),(81,6)$.

Now, by taking other suitable values of l and E, the possible exceptions of above four cases satisfy (3.3) except $(27,4)$. (refer Table 4). Hence all (q,n) with $q \geq 9$, and n such that $n' \nmid q-1$ are in T_4 except $(27,4)$.

Now we apply the modified prime sieve and see that the pairs $(3,11)$ and $(3,13)$ satisfy inequality (3.5) (refer Table 4.1a). Hence all the exceptions are $(3,4),(3,5),(3,7),(3,8),(3,10),(3,12),(3,16)$ and $(27,4)$ when $n' \nmid q-1$.

Theorem 4.9. *Let $\mathbb{F}_{q^n}$ be a finite extension of $\mathbb{F}_q$ of degree $n \geq 3$, where $q = 3^k$. Assume $f(x) \in S_{q,n}(4)$. If $n' \nmid q-1$, then there exists a primitive normal pair $(\alpha, f(\alpha))$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ unless (q,n) is one of the pairs $(3,4),(3,5),(3,7),(3,8),(3,10),(3,12),(3,16),(27,4)$.*

Now Theorem 4.2 is the conclusion of Theorem 4.5 and Theorem 4.9 collectively.

TABLE 4.1A. The pairs satisfying modified prime sieve.

(q,n)	g	G	H	k	P	L	δ	R'
(2,11)	$x+1$	1	$x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$	1	23	89	0.9130434	41
(3,11)	$x-1$	$x^5-x^3+x^2-x-1$	$x^5+x^4-x^3+x^2-1$	2	23	3851	0.90892825	194
(3,13)	$x-1$	$x^9-x^8+x^7-x^6+x^4+x^3-1$	x^3-x^2-x-1	2	1	797161	0.88888	254

where, R' denotes the numerical value of R.H.S. of inequality (3.5).

4.1. **Remark.** We further investigated the pairs posing as exceptional pairs with the help of SAGEMATH [18] and found that $(2,2),(2,3),(2,4),(3,3)$ and $(3,4)$ are genuine exceptions. In support, we provide a list of counter-examples for each of these pairs in the Table (4.2b). The rational functions $f(x) \in S_{q,n}(4)$ provided in Table (4.2b) will never give the primitive element $f(\alpha)$ for every primitive normal element α of the field $\mathbb{F}_{q^n}$. For the rest of the exceptional pairs mentioned in Theorems 4.1 and 4.2, we checked for a large number of rational functions of degree sum 4 and did not find any counter example.

http://dx.doi.org/10.22108/IJGT.2022.133016.1784

TABLE 4.2B. Counter examples to show genuine exceptions.

Sr. No.	(q,n)	counter-example $f(x) \in S_{q,n}(4)$
1	(2,2)	$\frac{(g+1)x^2+(g+1)x+g+1}{x^2+gx+g+1}$
2	(2,3)	$\frac{gx^2+(g^2+g+1)x+g+1}{x^2+(g^2+1)x+g^2+1}$
3	(2,4)	$\frac{(g^3+1)x^2+g^3+g}{x^2+(g^3+g)x+g^3+g+1}$
4	(3,3)	$\frac{(2g^2+1)x^2+(g+2)x+2g^2+2g+1}{x^2+(g^2+1)x+g^2+2g+2}$
5	(3,4)	$\frac{(g^3+2g^2)x^2+g^3x}{x^2+(2g^3+g^2+g+1)x+g^3+2}$

where g is the primitive element of the $\mathbb{F}_{q^n}$.

Acknowledgments

The authors are thankful to the referee for his/her comments and suggestions for better presentation of the paper. Prof. R. K. Sharma is the ConsenSys Blockchain Chair Professor at IIT Delhi. He is grateful to ConsenSys AG for that privilege. He is also thankful to the DST SERB MATRICS grant. Ms. Soniya Takshak is CSIR research fellow under Grant F. No. 09/086(1328)/2018-EMR-1. She is thankful for the same.

REFERENCES

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

[2] Cícero Carvalho, João Paulo Guardieiro, Victor G. L. Neumann and Guilherme Tizziotti, On the existence of pairs of primitive and normal elements over finite fields, *Bull. Braz. Math. Soc. (N.S.)*, **53** (2022) 677699.

[3] Todd Cochrane and Christopher Pinner, Using stepanov's method for exponential sums involving rational functions, *Journal of Number Theory*, **116** no. 2 (2006) 270–292.

[4] S. D. Cohen, Pair of primitive elements in fields of even order, *Finite Fields Appl.*, **28** (2014) 22–42.

[5] S. D. Cohen and Anju Gupta, Primitive element pairs with a prescribed trace in the quartic extension of a finite field, *J. Algebra Appl.*, **20** (2021) 14 pp.

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

[7] S. D. Cohen and S. Huczynska, The strong primitive normal basis theorem, *Acta Arith.*, **143** (2010) 299–332.

[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** (2021) 237–246.

[9] L. Fu and D. Q.Wan, A class of incomplete character sums, *Quart. J. Math.*, **65** (2014) 1195–1211.

[10] A. Gupta, R. K. Sharma and S. D. Cohen, Some special primitive elements with prescribed trace over finite fields, *Finite Fields Appl.*, (2018) **54** 1–18.

[11] G. Kapetanakis, Normal bases and primitive elements over finite fields, *Finite Fields Appl.*, **26** (2014) 123–143.

[12] H. W. Lenstra and R. J. Schoof, Primitive normal bases for finite fields, *Mathematics of Computation*, **48** no. 177 (1987) 217–231.

[13] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 2nd edition, (1997).

[14] Christof Paar and Jan Pelzl, *Public-Key Cryptosystems Based on the Discrete Logarithm Problem*, Springer Berlin Heidelberg, Berlin, Heidelberg, (2010) 205–238.

[15] A. K. Sharma, M. Rani and Sh. K. Tiwari, Primitive normal values of rational functions over finite fields, https://doi.org/10.1142/S0219498823501529, (2021).

[16] Hariom Sharma and R. K. Sharma, Existence of primitive normal pairs with one prescribed trace over finite fields, *Designs, Codes and Cryptography*, **89**, no. 12 (2021).

[17] R. K. Sharma, A. Awasthi and A. Gupta, Existence of pair of primitive elements over finite fields of characterisitc 2, *Journal of Number Theory*, **193** (2018) 386–394.

[18] SageMath, the Sage Mathematics Software System (Version 9.2), *The Sage Developers*, (2020), https://www.sagemath.org.

Rajendra Kumar Sharma
Department of Mathematics, Indian Institute of Technology, Hauz Khas, 110016, New Delhi, India
Email: rksharmaiitd@gmail.com

Soniya Takshak
Department of Mathematics, Indian Institute of Technology, Hauz Khas, 110016, New Delhi, India
Email: sntakshak9557@gmail.com

Ambrish Awasthi
Scientific Analysis Group, Defence Research and Development Organisation, Metcalfe House, 110054, Delhi, India
Email: ambrishawasthi@yahoo.com

Hariom Sharma
S. S. Govt. P.G. College, Tigaon, Faridabad, 121101, Haryana, India
Email: hariomsharma638@gmail.com

http://dx.doi.org/10.22108/IJGT.2022.133016.1784

Appendix

1. Pairs for which condition $\mathbf{q^{\frac{n}{2}} > 5SW(l)^2W(E)}$ is true.

Table 3: Case A $n'|q-1$.

Sr. No.	(q,n)	l	s	E	t	S
1	(9,9)	2	5	$x-1$	0	24.59
2	(27,3)	2	1	1	1	6.96
3	$(3^6,3)$	2	5	$x-1$	0	24.59
4	(3,18)	2	5	$x+1$	1	155.5
5	(27,6)	2	5	$x+1$	1	29.67
6	$(9,12)$	10	5	$x+1$	3	81.671
7	$(3^4,4)$	2	4	$x+1$	3	27.8952
8	$(3^6,4)$	2	6	$x+1$	3	177.36
9	$(3^4,5)$	2	4	$x+2$	4	31.521

Table 4: Case B $n' \nmid q-1$.

Sr. No.	(q,n)	l	s	E	t	S
1	(3,11)	2	2	1	3	12.809
2	(3,13)	2	1	$x+2$	4	7.8696
3	(3,14)	2	2	$x+1$	3	11.25
4	(3,15)	22	2	$x+2$	1	6.7998
5	(3,17)	2	2	$x+2$	1	6.005
6	(3,19)	2	2	$x+2$	1	6.00504
7	(3,20)	10	3	$x+1$	6	39.95
8	(3,21)	26	2	$x+2$	1	6.013
9	(3,22)	46	3	$x+1$	5	18.2125
10	(3,23)	94	1	$x+2$	2	5.00004
11	(3,24)	70	4	$x+1$	4	108.79525
12	(3,25)	22	2	$x+2$	2	7.0604
13	(3,28)	10	4	$x+1$	6	29.34
14	(3,30)	14	6	$x+1$	3	71.5862
15	(3,32)	10	4	$x+1$	8	116.0279
16	(3,34)	206	4	$x+1$	3	17.22
17	(3,36)	70	6	$x+1$	2	63.22
18	(3,42)	14	6	$x+1$	3	32.6217
19	(3,48)	910	8	$x+1$	6	273.1065
20	(9,5)	2	2	1	3	11.2366
21	(9,7)	2	2	$x+2$	2	7.04149
22	(9,10)	2	4	$x+1$	5	55.762
23	(9,11)	2	4	$x+2$	2	12.2318
24	(9,14)	10	4	$x+1$	5	16.8363
25	(9,15)	2	7	$x+2$	2	62.287346
26	(9,16)	10	4	x^2+2	10	160.6409

http://dx.doi.org/10.22108/IJGT.2022.133016.1784

Sr. No.	(q,n)	l	s	E	t	S
27	(27,5)	2	3	$x+2$	1	11.03757
28	(27,8)	2	6	$x+1$	4	352.4595
29	(27,10)	2	7	$x+1$	3	69.6650104
30	(27,12)	10	7	$x+1$	2	47.08966
31	(81,6)	2	6	$x+1$	1	169.58
32	(243,4)	10	3	$x+1$	2	10.97932

http://dx.doi.org/10.22108/IJGT.2022.133016.1784