World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:19, No:2, 2025

Existence of Rational Primitive Normal Pairs with Prescribed Norm and Trace

Soniya Takshak, R. K. Sharma

Abstract—Let q be a prime power and n be a positive integer, $\mathbb{F}_q$ stands for the finite field of q elements, and $\mathbb{F}_{q^n}$ denotes the extension of $\mathbb{F}_q$ of degree n. Also, $\mathbb{F}_q^*$ represents the multiplicative group of non-zero elements of $\mathbb{F}_q$, and the generators of $\mathbb{F}_q^*$ are called primitive elements. A normal element of a finite field $\mathbb{F}_{q^n}$ is an element α such that the set of α and its all conjugates in $\mathbb{F}_{q^n}$ forms a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Primitive normal elements have several applications in coding theory and cryptography. So, establishing the existence of primitive normal elements under certain conditions is theoretically essential and a genuine issue. In this article, we provide a sufficient condition for the existence of a primitive normal element α in $\mathbb{F}_{q^n}$ of a prescribed primitive norm and non-zero trace over $\mathbb{F}_q$ such that $f(\alpha)$ is also primitive, where $f(x)$ is a rational function of degree sum m over $\mathbb{F}_{q^n}$. Particularly, for the rational functions of degree sum 4 over $\mathbb{F}_{q^n}$, where $\mathbb{F}_q$ is the field of characteristic 11 and n is greater than or equal to 7, we demonstrated that there are only 3 exceptional pairs (q, n) for which such kind of primitive normal elements may not exist. In general, we show that such elements always exist except for finitely many choices of (q, n). We used additive and multiplicative character sums as important tools to arrive at our conclusion.

Keywords—Finite Field, Primitive Element, Normal Element, norm, trace, character.

I. Introduction

THERE are two well-known concepts related to the elements of finite fields, namely, the trace and the norm. For $\alpha \in \mathbb{F}_{q^n}$, the trace of α over $\mathbb{F}_q$ is defined as $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i}$, and the norm of α over $\mathbb{F}_q$ is defined as $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \prod_{i=0}^{n-1} \alpha^{q^i}$.

In [1], Sharma et al. proved the existence of primitive normal pairs $(\alpha, f(\alpha))$ in $\mathbb{F}_{q^n}$ where $f(x)$ is a polynomial of degree m. In this article, we generalize $f(x)$ to a rational function of degree sum m and relax the normality condition on $f(\alpha)$. Here degree sum of a rational function $f = f_1/f_2$ is defined to be the sum of the degrees of f_1 and f_2. In our context, we define a pair $(\alpha, \beta) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ to be a primitive normal pair when α is primitive and normal both, but β is primitive only.

For a positive integer m, let $S_{q^n}(m)$ denote the set of rational functions $f(x) = \frac{f_1(x)}{f_2(x)} \in \mathbb{F}_{q^n}(x)$ of degree sum m, which are non-exceptional. Here, by the non-exceptional functions we mean that $f(x) \neq \lambda x^r h(x)^s$ for $\lambda \in \mathbb{F}_{q^n}^*$, any integer r, and $h(x) \in \mathbb{F}_{q^n}(x)$, and $s|(q^n - 1)$ such that $s > 1$. For primitive element a and non-zero element b in $\mathbb{F}_q$, let $T_{m,a,b}$ denote the set of pairs (q, n) such that for each $f \in S_{q^n}(m)$, there exists a primitive normal pair $(\alpha, f(\alpha))$ in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ with $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = a$ and $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = b$.

Soniya Takshak and R. K. Sharma are with the Department of Mathematics, Indian Institute of Technology Delhi, New Delhi, 110016, India (e-mail: sntakshak9557@gmail.com, rksharmaiitd@gmail.com).

This article is organized in the following manner: Section II contains some basic results and notations. A sufficient condition for the existence of primitive normal element α with prescribed norm and trace, such that $f(\alpha)$ is also primitive, is obtained in Section III. Further, in Section IV, we improved the sufficient condition with the help of the sieving technique. At last, we provide a numerical example of the rational functions of degree sum 4 over $\mathbb{F}_{q^n}, q = 11^k$, in Section V.

II. Preliminaries

Let $q = p^k$, where p is a prime and k is a positive integer. We denote an algebraic closure of $\mathbb{F}_p$ by $\mathbb{F}$ and the set of positive integers by $\mathbb{N}$. Next, $W(\lambda)$ represents the number of square-free divisors of λ, where λ is a positive integer or a polynomial. For primary results related to e-free elements, g-free elements, and characters the reader is referred to [2].

Similar to Cohen and Huczynska [3], [4], the characteristic function for the subset of e-free elements of $\mathbb{F}_{q^n}^*$, where e is a divisor of $q^n - 1$, can be provided as follows,

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

where $\theta(e) := \frac{\phi(e)}{e}$, μ denotes the Möbius function, and χ_d denotes a multiplicative character of order d.

Analogously, the characteristic function for the set of g-free elements of $\mathbb{F}_{q^n}^*$, where g is a factor of $(x^n - 1)$, is as follows,

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

where $\Theta(g) := \frac{\Phi_q(g)}{q^{deg(g)}}$, ψ_h is any additive character of order h, and μ' is analogous to the Möbius function, with $\mu'(h) = (-1)^s$, when h is a product of s distinct monic irreducible polynomials, otherwise 0.

We also need two characteristic functions, η_a and τ_b, for the set of elements of prescribed norm and trace, respectively. For $a \in \mathbb{F}_q^*$, the characteristic function for the set of elements in $\mathbb{F}_{q^n}$ of norm a, is given by

$$\eta_a : \alpha \mapsto \frac{1}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} \chi(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) a^{-1}),$$

where $\widehat{\mathbb{F}_q^*}$ is the set of multiplicative characters over $\mathbb{F}_q^*$. Similarly, the characteristic function for the set of elements in $\mathbb{F}_{q^n}$ of trace b, is given by

$$\tau_b : \alpha \mapsto \frac{1}{q} \sum_{\psi \in \widehat{\mathbb{F}_q}} \psi(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) - b),$$

where $\widehat{\mathbb{F}_q}$ is the set of additive characters over $\mathbb{F}_q$.

We will use Lemma 1 and Lemma 2 to prove this article's sufficient condition (Lemma 4).

Lemma 1. [5] *Let $f(x)$ be a rational function over $\mathbb{F}_{q^n}$. Let $f(x) = \prod_{j=1}^{k} f_j(x)^{r_j}$, where $f_j(x)$ are irreducible polynomials over $\mathbb{F}_{q^n}$ and r_j are nonzero integers. Let χ be a multiplicative character of square-free order d of $\mathbb{F}_{q^n}$, where $d|q^n-1$. Suppose $f(x) \neq cg(x)^d$ for any rational function $g(x)$ in $\mathbb{F}_{q^n}(x)$ and $c \in \mathbb{F}_{q^n}^*$. Then*

$$\left| \sum_{\alpha \in \mathbb{F}_{q^n}, f(\alpha) \neq \infty} \chi(f(\alpha)) \right| \leq (\sum_{j=1}^{k} deg(f_j) - 1) q^{n/2}.$$

Lemma 2. [6] *Let χ be a multiplicative character of order r and ψ be a nontrivial additive character of $\mathbb{F}_{q^n}$. Let f and g be rational functions over $\mathbb{F}_{q^n}$. We write $f(x) = \prod_{j=1}^{k} f_j(x)^{r_j}$, where $f_j(x)$ are irreducible polynomials over $\mathbb{F}_{q^n}$ and r_j are nonzero integers. Let g is not of the form $h^{q^n} - h$, for any $h \in \mathbb{F}(x)$. Then*

$$\left| \sum_{\substack{\alpha \in \mathbb{F}_{q^n}, \\ f(\alpha) \neq 0, \infty, \\ g(\alpha) \neq \infty}} \chi(f(\alpha))\psi(g(\alpha)) \right| \leq (N_1 + N_2 + N_3 + N_4 - 1) q^{n/2},$$

where $N_1 = \sum_{j=1}^{k} deg(f_j)$, $N_2 = max(deg(g), 0)$, N_3 is the degree of the denominator of $g(x)$ and N_4 is the sum of the degrees of irreducible factors of the denominator of $g(x)$, which are different from $f_j(x), j = 1, 2, \ldots, k$.

III. Sufficient Condition

Whenever α is a primitive element in $\mathbb{F}_{q^n}$, the norm of α is a primitive element in $\mathbb{F}_q$. That is, if α is (q^n-1)-free in $\mathbb{F}_{q^n}$, then $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ is $(q-1)$-free in $\mathbb{F}_q$. Moreover, Lemma 3 deals with the general case. We have changed the notations according to our article.

Lemma 3. [1] *Let l be a divisor of $q^n - 1, \sigma = gcd(l, q-1)$, and R_l is the largest divisor of l such that $gcd(\sigma, R_l) = 1$. Then $\alpha \in \mathbb{F}_{q^n}^*$ is l-free if and only if $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ is σ-free in $\mathbb{F}_q^*$, and α is R_l-free.*

Let l_1, l_2 divide $(q^n - 1)$, and $g(x)$ divides $x^n - 1$. Let $\sigma = \gcd(l_1, q-1)$ and R_{l_1} be the largest divisor of l_1 in such a manner that $\gcd(\sigma, R_{l_1}) = 1$. It is evident from Lemma 3 that if $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ is σ-free and α is R_{l_1}-free, then α will be l_1-free. Furthermore, the non-zero value of $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ implies that α is $(x-1)$-free. Next, S_g is the highest degree polynomial dividing $g(x)$ such that $\gcd(S_g, x-1) = 1$. Now, to show that α is l_1-free and g-free, we need to show that α is R_{l_1}-free and S_g-free.

For $f \in S_{q^n}(m)$, a σ-free element $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q^*$, let $N_{f,a,b}(R_{l_1}, l_2, S_g)$ represents the number of elements $\alpha \in \mathbb{F}_{q^n}$ such that α is R_{l_1}-free and S_g-free with $f(\alpha)$ is l_2-free, such that $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = a, Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = b$. For easy notation, we set $R \coloneqq R_{q^n-1}, S \coloneqq S_{x^n-1}$ and $N_{f,a,b} \coloneqq N_{f,a,b}(R, q^n - 1, S)$. Hence to prove that $(q, n) \in T_{m,a,b}$, it is required to show that $N_{f,a,b} > 0$ for every $f \in S_{q^n}(m)$. In Lemma 4, we prove a sufficient condition such that $N_{f,a,b}(R_{l_1}, l_2, S_g)$ is positive. Consequently, Corollary 1 provides the sufficient condition on q and n such that $(q, n) \in T_{m,a,b}$.

Lemma 4. *Let q, m, and n are in $\mathbb{N}$ and q be a prime power such that $q^{\frac{n}{2}-2} > (m+1)W(R_{l_1})W(l_2)W(S_g)$. Then $N_f(R_{l_1}, l_2, S_g) > 0$, where l_1, l_2 divide $q^n - 1$ and $g(x)|x^n - 1$.*

Proof: Let V_1 be the set containing zeros and poles of $f(x)$ in $\mathbb{F}_{q^n}$ and $V = V_1 \cup \{0\}$. Then

$$\begin{aligned} &N_{f,a,b}(R_{l_1}, l_2, S_g) \\ &\quad = \sum_{\substack{\alpha \in \mathbb{F}_{q^n} \\ \alpha \notin V}} \rho_{R_{l_1}}(\alpha)\rho_{l_2}(f(\alpha))\kappa_{S_g}(\alpha)\eta_a(\alpha)\tau_b(\alpha) \\ &\quad = \frac{\theta(l_1)\theta(l_2)\Theta(g)}{q(q-1)} \sum_{\substack{d_1 | R_{l_1}, d_2 | l_2, \\ h | S_g}} \frac{\mu(d_1)\mu(d_2)\mu^{'}(h)}{\phi(d_1)\phi(d_2)\Phi_q(h)} \\ &\qquad \sum_{\substack{\chi_{d_1}, \chi_{d_2}, \\ \psi_h}} \chi_{d_1,d_2,h,a,b} \end{aligned}$$

where

$$\begin{aligned} \chi_{d_1,d_2,h,a,b} = \sum_{\chi \in \widehat{\mathbb{F}_q^*}} \sum_{\psi \in \widehat{\mathbb{F}_q}} \sum_{\substack{\alpha \in \mathbb{F}_{q^n} \\ \alpha \notin V}} &\chi_{d_1}(\alpha)\chi_{d_2}(f(\alpha))\psi_h(\alpha) \\ &\chi(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)a^{-1})\psi(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) - b) \end{aligned}$$

For multiplicative character χ_{q-1} of order $q-1$ in $\widehat{\mathbb{F}_q^*}$ and canonical additive character ψ_0 in $\widehat{\mathbb{F}_q}$, we have

$$\begin{aligned} &\chi_{d_1,d_2,h,a,b} \\ &\quad = \sum_{j=1}^{q-1} \sum_{c \in \mathbb{F}_q} \chi_{q-1}(a^{-j})\psi_0(-cb) \sum_{\substack{\alpha \in \mathbb{F}_{q^n} \\ \alpha \notin V}} \chi_{d_1}(\alpha)\chi_{d_2}(f(\alpha)) \\ &\qquad \psi_h(\alpha)\chi_{q-1}^j(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha))\psi_0(cTr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)) \\ &\quad = \sum_{j=1}^{q-1} \sum_{c \in \mathbb{F}_q} \chi_{q-1}(a^{-j})\psi_0(-cb) \sum_{\substack{\alpha \in \mathbb{F}_{q^n} \\ \alpha \notin V}} \chi_{d_1}(\alpha)\chi_{d_2}(f(\alpha)) \\ &\qquad \psi_h(\alpha)\tilde{\chi}^j(\alpha)\tilde{\psi_0}(c\alpha) \end{aligned}$$

where $\tilde{\chi} = \chi_{q-1} \circ N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ and $\tilde{\psi_0} = \psi_0 \circ Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}$. It is clear that $\tilde{\chi}$ is a multiplicative character in $\widehat{\mathbb{F}_{q^n}^*}$ and $\tilde{\psi_0}$ is a canonical additive character in $\widehat{\mathbb{F}_{q^n}}$. Since the order of $\tilde{\chi}$ is $q-1$, there exists a multiplicative character χ_{q^n-1} in $\widehat{\mathbb{F}_{q^n}^*}$ such that $\tilde{\chi} = \chi_{q^n-1}^{(q^n-1)/(q-1)}$ and $\chi_{d_j}(\alpha) = \chi_{q^n-1}(\alpha^{n_j})$, for some $n_j \in \{1, 2, \ldots, q^n - 2\}, j = 1, 2$. Moreover, there exists

$y' \in \mathbb{F}_{q^n}$ such that $\psi_h(\alpha) = \tilde{\psi_0}(y'\alpha)$. Therefore

$$\begin{aligned}
&\chi_{d_1,d_2,h,a,b} \\
&= \sum_{j=1}^{q-1} \sum_{c\in\mathbb{F}_q} \chi_{q-1}(a^{-j})\psi_0(-cb) \\
&\quad \sum_{\substack{\alpha\in\mathbb{F}_{q^n}\\ \alpha\notin V}} \chi_{q^n-1}(\alpha^{n_1+\frac{(q^n-1)j}{(q-1)}} f(\alpha)^{n_2})\tilde{\psi_0}((y'+c)\alpha) \\
&= \sum_{j=1}^{q-1} \sum_{c\in\mathbb{F}_q} \chi_{q-1}(a^{-j})\psi_0(-cb) \\
&\quad \sum_{\substack{\alpha\in\mathbb{F}_{q^n}\\ \alpha\notin V}} \chi_{q^n-1}(F_j(\alpha))\tilde{\psi_0}(G_c(\alpha))
\end{aligned}$$

where $F_j(x) = x^{n_1+\frac{(q^n-1)j}{(q-1)}} f(x)^{n_2},\ j = 1, 2, \cdots, q-1$ and $G_c(x) = (y'+c)x,\ c \in \mathbb{F}_q$. If $G_c(x) \neq H(x)^{q^n} - H(x)$, for any $H(x) \in \mathbb{F}(x)$ then lemma 2 provides

$$|\chi_{d_1,d_2,h,a,b}| \leq (m+1)(q-1)q^{n/2+1}.$$

Also when $G_c(x) = H(x)^{q^n} - H(x)$, it is possible to write $(y'+c)x = H(x)^{q^n} - H(x)$, for some $H(x) \in \mathbb{F}(x)$, only when $y'+c = 0$. Since $\psi_h(h(\alpha)) = 1$, we get $\tilde{\psi_0}(y'h(\alpha)) = 1$. Thus $y'+c = 0$ implies $\tilde{\psi_0}(-ch(\alpha)) = 1$. Since c is an element of $\mathbb{F}_q$, and $x^n - 1$ is the $\mathbb{F}_q$-order of $\tilde{\psi_0}$, therefore $x^n - 1 | ch(x)$. This implies $c = 0$, which further implies $y' = 0$. Hence $h = 1$. Therefore, when $G_c(x) = H(x)^{q^m} - H(x)$, the following two cases arise.

Case 1. If $F_j(x) \neq \lambda H(x)^{q^n-1}$ for any $\lambda \in \mathbb{F}_{q^n}^*$ and $H(x) \in \mathbb{F}_{q^n}(x)$, then we get the following bound using Lemma 1

$$|\chi_{d_1,d_2,h,a,b}| \leq m(q-1)q^{n/2+1} + m < (m+1)(q-1)q^{n/2+1}.$$

Case 2. If $F_j(x) = \lambda H(x)^{q^n-1}$ for some $\lambda \in \mathbb{F}_{q^n}^*$ and $H(x) \in \mathbb{F}_{q^n}(x)$, then $d_1 = d_2 = 1$. For this

$$x^{n_1+\frac{(q^n-1)j}{q-1}} f(x)^{n_2} = \lambda H(x)^{q^n-1}. \tag{1}$$

We can write $f(x)$ in the product form as $f(x) = \omega x^r \prod_{i=1}^{k} f_i(x)^{s_i}$, where $\omega \in \mathbb{F}_{q^n}^*, r, s_i$ are integers and $f_i(x)$ is an irreducible polynomial, $i = 1, 2, \ldots, k$. Comparing powers of $f_i(x)$ on both sides, we get

$$s_i n_2 = s_i'(q^n - 1)$$

where s_i' represents the multiplicity of $f_i(x)$ in $H(x)$. Let $s = \frac{q^n-1}{\gcd(q^n-1, n_2)}$, then s divides s_i. Therefore, $f(x) = \omega x^r g(x)^s$ for some $g(x) \in \mathbb{F}_{q^n}(x)$. Since $f(x) \in S_{q^n}(m)$, we get $s = 1$. Hence $q^n - 1 | n_2$ and this implies $n_2 = 0$. Now equation (1) becomes

$$x^{n_1+\frac{(q^n-1)j}{q-1}} = \lambda H(x)^{q^n-1}$$

This implies $H(x) = x^t$, for some $t \in \mathbb{N}$, and $n_1 + \frac{(q^n-1)j}{q-1} = t(q^n-1)$. Hence $n_1 = (t - \frac{j}{q-1})(q^n-1) \geq (t-1)(q^n-1)$, and this implies $t = 1$ (since $0 \leq n_1 \leq q^n - 2$). Thus $n_1 = (1 - \frac{j}{q-1})(q^n-1)$. Since $\chi_{d_1} = \chi_{q^n-1}^{n_1}$, there exists $t' \in \mathbb{N}$ such that $n_1 = \frac{t'(q^n-1)}{d_1}$. This implies $(q-1-j)d_1 = t'(q-1)$. Since $\gcd(d_1, q-1) = 1$, we get $d_1 | t'$. Hence $q^n - 1 | n_1$, and this implies $n_1 = 0$. Thus we get $n_1 = n_2 = 0$, and hence $d_1 = d_2 = 1$. Consequently, we get $(d_1, d_2, h) = (1, 1, 1)$, whenever $G_c(x) = H(x)^{q^m} - H(x)$ and $F_j(x) = \lambda H(x)^{q^n-1}$ for some $H(x) \in \mathbb{F}_{q^n}(x)$. Hence

$$\begin{aligned}
&\chi_{1,1,1,a,b} \\
&= \sum_{j=1}^{q-1} \sum_{c\in\mathbb{F}_q} \chi_{q-1}(a^{-j})\psi_0(-cb) \sum_{\substack{\alpha\in\mathbb{F}_{q^n}\\ \alpha\notin V}} \chi_{q^n-1}(\alpha^{\frac{(q^n-1)j}{(q-1)}}) \\
&\quad \tilde{\psi_0}(c\alpha) \\
&= \sum_{j=1}^{q-1} \sum_{c\in\mathbb{F}_q^*} \chi_{q-1}(a^{-j})\psi_0(-cb) \sum_{\substack{\alpha\in\mathbb{F}_{q^n}\\ \alpha\notin V}} \chi_{q^n-1}(\alpha^{\frac{(q^n-1)j}{(q-1)}}) \\
&\quad \tilde{\psi_0}(c\alpha) + \sum_{j=1}^{q-2} \chi_{q-1}(a^{-j}) \sum_{\substack{\alpha\in\mathbb{F}_{q^n}\\ \alpha\notin V}} \chi_{q^n-1}(\alpha^{\frac{(q^n-1)j}{(q-1)}}) \\
&\quad + \chi_{q-1}(a^{-(q-1)}) \sum_{\substack{\alpha\in\mathbb{F}_{q^n}\\ \alpha\notin V}} \chi_{q^n-1}(\alpha^{q^n-1}) \\
&= A + B + (q^n - |V|)
\end{aligned}$$

where

$$A = \sum_{j=1}^{q-1} \sum_{c\in\mathbb{F}_q^*} \chi_{q-1}(a^{-j})\psi_0(-cb) \sum_{\substack{\alpha\in\mathbb{F}_{q^n}\\ \alpha\notin V}} \chi_{q^n-1}(\alpha^{\frac{(q^n-1)j}{(q-1)}})\tilde{\psi_0}(c\alpha)$$

and $B = \sum_{j=1}^{q-2} \chi_{q-1}(a^{-j}) \sum_{\substack{\alpha\in\mathbb{F}_{q^n}\\ \alpha\notin V}} \chi_{q^n-1}(\alpha^{\frac{(q^n-1)j}{(q-1)}})$.

As it is not possible to write cx in the form of $H(x)^{q^m} - H(x)$ for any $c \in \mathbb{F}_q^*$ and $H(x) \in \mathbb{F}(x)$, so we get $|A| \leq (q-1)^2 q^{\frac{n}{2}}$ using Lemma 2. Now we determine an upper bound for B.

$$B = \sum_{j=1}^{q-2} \chi_{q-1}(a^{-j}) \left\{ \sum_{\alpha\in\mathbb{F}_{q^n}^*} \chi_{q^n-1}^{\frac{(q^n-1)j}{(q-1)}}(\alpha) - \sum_{\alpha\in V_1} \chi_{q^n-1}^{\frac{(q^n-1)j}{(q-1)}}(\alpha) \right\}$$

$$|B| \leq (q-2)(|V|-1).$$

Thus

$$|\chi_{1,1,1,a,b} - (q^n - |V|)| \leq (q-2)(|V|-1) + (q-1)^2 q^{\frac{n}{2}}$$

Therefore

$$\begin{aligned}
&N_{f,a,b}(R_{l_1}, l_2, S_g) \\
&\geq \frac{\theta(l_1)\theta(l_2)\Theta(g)}{q(q-1)} \{q^n - (q-1)(|V|-1) - 1 - (q-1)^2 q^{\frac{n}{2}} \\
&\quad + (q-1)(m+1)q^{\frac{n}{2}+1}(W(R_{l_1})W(l_2)W(S_g) - 1)\} \\
&\geq \frac{\theta(l_1)\theta(l_2)\Theta(g)}{q(q-1)} \{q^n - 1 - (q-1)\{(|V|-1) - (q-1)q^{\frac{n}{2}} \\
&\quad + (m+1)q^{\frac{n}{2}+1}(W(R_{l_1})W(l_2)W(S_g) - 1)\}\} \\
&\geq \frac{\theta(l_1)\theta(l_2)\Theta(g)}{q(q-1)} \{q^n - 1 - (q-1)\{(m-1) - (q-1)q^{\frac{n}{2}} \\
&\quad + (m+1)q^{\frac{n}{2}+1}(W(R_{l_1})W(l_2)W(S_g) - 1)\}\}.
\end{aligned}$$

Hence $N_{f,a,b}(R_{l_1}, l_2, S_g) > 0$, whenever

$$q^{\frac{n}{2}-2} > (m+1)W(R_{l_1})W(l_2)W(S_g).$$

■

Corollary 1. *For any $f(x) \in S_{q^n}(m)$, any primitive element $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q^*$, the pair $(q,n) \in T_{m,a,b}$ if*

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

Clearly, (2) can not be used to discuss the cases when $n < 5$. However, when n is 1 or 2, the primitive normal pairs become just the primitive pairs. Therefore $n \geq 3$ can be assumed, but inequality (2) does not settle the case when n is 3 and 4. From now on, we assume that $n \geq 5$. Lemma 5 and 6 provide upper bounds for $W(x^n-1)$ and $W(\mathcal{M})$, respectively. We will use these results in the rest of the article.

Lemma 5. [7] *Let $n \in \mathbb{N}$, and q be a prime power. Then*

$$W(x^n-1) \leq 2^{\frac{1}{2}(n+gcd(n,q-1))}.$$

Particularly, $W(x^n-1) \leq 2^n$, and equality holds only when $n|(q-1)$. Furthermore, $W(x^n-1) \leq 2^{3n/4}$ if $n \nmid (q-1)$.

Lemma 6. *[4] Let $\mathcal{M} \in \mathbb{N}$, and ν be a positive real number. Then*

$$W(\mathcal{M}) \leq \mathcal{C} \cdot \mathcal{M}^{1/\nu},$$

where $\mathcal{C} = \prod_{j=1}^{s} \frac{2}{p_j^{1/\nu}}$ and $p_1, p_2, \ldots, p_s$ are the primes smaller than 2^ν that divide $\mathcal{M}$.

Since R is the largest divisor of q^n-1, which is coprime to $q-1$, $R = \frac{q^n-1}{(q-1)\text{gcd}(n,q-1)}$. Next, S is the largest divisor of x^n-1 coprime to $x-1$. Therefore, $W(S) = W(x^n-1)/2$. We propose Proposition 1, which shows that $T_{m,a,b}$ is non-empty except for finitely many choices of (q,n), although the proof is similar to [1, Proposition 3.1].

Proposition 1. *Let q be a prime power and $n \geq 5$, then $(q,n) \in T_{m,a,b}$ except for finitely many pairs (q,n).*

IV. Sieving Result

Condition (2) is further improved in Theorem 1, and the proof is alike [8, Theorem 3.4].

Theorem 1. *Suppose $l'|R$ and $p_1', p_2', \ldots, p_r'$ are the remaining primes dividing R, and $l|q^n-1$ and $p_1, p_2, \ldots, p_s$ are the remaining primes dividing q^n-1. Also, let $E|S$ and $P_1, P_2, \ldots, P_t$ are the remaining irreducible polynomials that divide S. Take $\delta = 1 - \sum_{i=1}^{r} \frac{1}{p_i'} - \sum_{i=1}^{s} \frac{1}{p_i} - \sum_{i=1}^{t} \frac{1}{q^{deg(P_i)}}$ and $\Delta = \frac{r+s+t-1}{\delta} + 2$. Assume $\delta > 0$, then $N_{f,a,b} > 0$ if*

$$q^{\frac{n}{2}-2} > (m+1)\Delta W(l')W(l)W(E). \quad (3)$$

V. Working Example

This section demonstrates a numerical example of the above results by working with the rational functions with degree sum 4. From Lemma 5 and 6, inequality (2) becomes equivalent to

$$q^{n/2-2} > 5\mathcal{C}^2 q^{2n/\nu} 2^{n-1}. \quad (4)$$

For simplicity of the calculations, we assume that $q = 11^k$. First, we discuss the case when $n \geq 7$ and prove Lemma 7.

Lemma 7. *Let $q = 11^k$, and $k, n \in \mathbb{N}$ such that $n \geq 7$. Then $(q,n) \in T_{4,a,b}$ except possibly $(11,7), (11,8), (11,10)$.*

Proof: Let $\nu = 10$ in Lemma 6, and then we have $\mathcal{C} \leq 1.11 \times 10^9$. Hence inequality (4) becomes $q^{n/2-2} > 5 \times (1.11 \times 10^9)^2 q^{2n/10} 2^{n-1}$, which is true when $k \geq 198$ and $n \geq 7$. For $k \leq 197$, we find the values of n_k such that this inequality is satisfied for $n \geq n_k$. Now for these values of k and n_k, we check inequality (5)

$$q^{n/2-2} > 5 \times (1.11 \times 10^9)^2 q^{2n/10} W(x^n-1)/2. \quad (5)$$

The above inequality (5) is valid for $n_k = 7$ when $k \geq 13$, and for other values of n_k when $1 \leq k \leq 12$, which are tabulated in Table I. Further, we verify $q^{n/2-2} > 5W(R)W(q^n-1)W(S)$ for these values and find the following exceptions.

$$q = 11 \text{ and } n = 7, 8, 9, 10, 12, 14, 15, 16, 20, 24$$

$$q = 11^2 \text{ and } n = 7, 8, 9, 10, 12$$

$$q = 11^3 \text{ and } n = 7, 8$$

For the above exceptional values of q and n, we select l', l, and E as listed in the Appendix such that inequality (3) is satisfied. Hence we can say that the only exceptional pairs are $(11,7), (11,8), (11,10)$. ■

TABLE I
Values of n_k When $1 \leq k \leq 12$

k	1	2	3	4	5	6	7	8	9	10	11	12
n_k	49	31	20	16	12	11	10	9	9	9	8	8

For $n = 5$, if we choose $\nu = 21.6$ then Lemma 6 provides $\mathcal{C} \leq 1.27 \times 10^{4994}$. Now inequality (4) is satisfied when $k \geq 259012$ and $n = 5$. For $n = 6$, we assume $\nu = 14$ and check that inequality (4) is true when $k \geq 926$. For the remaining values of k, when n is 5 and 6, we have to check the inequality (2), which requires the exact calculation of $W(q^n-1)$. These computations demand a large amount of time and memory. So we omit these cases here and propose the following conjecture for $n \geq 7$.

Conjecture 1. *Let $q = 11^k, k \in \mathbb{N}$ and $n \geq 7$. Assume $f(x) \in S_{q^n}(4)$. Then $(q,n) \in T_{4,a,b}$ unless $(11,7), (11,8)$ and $(11,10)$.*

Remark 1. *For $q = 11^k, k \in \mathbb{N}, n = 5, 6$, we verified inequality (3) for $k \leq 25$. These computations suggest that all the pairs (q,n) are in $T_{4,a,b}$ except possibly $(11,5), (11^2,5), (11^3,5), (11^4,5), (11,6), (11^2,6), (11^3,6)$.*

APPENDIX

TABLE II

PAIRS (q,n) SATISFYING $q^{\frac{n}{2}-2} > 5\Delta W(l')W(l)W(E)$

(q,n)	l'	l	E	Δ
$(11,9)$	1	2	1	21.9622513324522
$(11,12)$	6	30	1	74.5523562157433
$(11,14)$	6	6	1	18.6785777285348
$(11,15)$	7	2	$x+2$	65.2353275170198
$(11,16)$	2	6	$x+1$	50.1051340406700
$(11,20)$	6	6	x^2+3x+2	227.333807794329
$(11,24)$	6	6	$x+1$	388.277468595869
$(11^2,7)$	43	2	1	20.0438499599651
$(11^2,8)$	17	2	1	49.3288379439818
$(11^2,9)$	3	6	1	43.3670106551059
$(11^2,10)$	61	6	1	24.5843102799047
$(11^2,12)$	7	6	1	130.480024911173
$(11^3,7)$	43	10	1	22.6388740148260
$(11^3,8)$	6	6	1	57.4446091126709

ACKNOWLEDGMENT

This work has been supported by CSIR, New Delhi, Govt. of India, under Grant F. No. 09/086(1328)/2018-EMR-1.

REFERENCES

[1] A. K. Sharma, M. Rani, and S. K. Tiwari, *Primitive normal pairs with prescribed norm and trace*, Finite Fields Their Appl., vol. 78, pp. 101976, 2022.
[2] Anju, and R. K. Sharma, *Existence of some special primitive normal elements over finite fields*, Finite Fields Appl., vol. 46, pp. 280-303, 2017.
[3] S. D. Cohen, and S. Huczynska, *The primitive normal basis theorem-without a computer*, J. Lond. Math. Soc., vol. 67, no. 1, pp. 41-56, 2003.
[4] S. D. Cohen, and S. Huczynska, *The strong primitive normal basis theorem*, Acta Arith., vol. 143, no. 4, pp. 299-332, 2010.
[5] T. Cochrane and C. Pinner, *Using Stepanov's method for exponential sums involving rational functions*, Journal of Number Theory, vol. 116, no. 2, pp. 270-292, 2006.
[6] L. Fu, and D. Q. Wan, *A class of incomplete character sums*, Quart. J. Math., vol. 65, pp. 1195-1211, 2014.
[7] H. W. Lenstra, Jr. and R. J. Schoof, *Primitive normal bases for finite fields*, Math. Comp., vol. 48, pp. 217-231, 1987.
[8] A. Gupta, R. K. Sharma, and S. D. Cohen, *Some Special Primitive Elements with Prescribed Trace over Finite Fields*, Finite Fields Appl., vol. 54, pp. 1-18, 2018.

Soniya Takshak received her M.Sc. degree from University of Rajasthan, India. She is pursuing her Ph.D. degree under the guidance of Prof. R. K. Sharma from Indian Institute of Technology, Delhi. Her research interests are Finite Fields and Cryptography. Particularly, she has been working on primitive elements and primitive polynomials.

R. K. Sharma is professor of mathematics at the Indian Institute of Technology, Delhi. Earlier, he was in the faculty of mathematics at IIT Kharagpur. He has guided 34 Ph.D. theses and more than 78 M.Tech. projects. His main area of research is Algebra and Cryptography. He has published more than 153 research papers in international journals. He has participated in several conferences, including the coveted International Congress of Mathematicians (ICM) 1994, in Zurich, Switzerland. He has traveled widely and delivered invited talks at several places. He was a postdoctoral fellow in France and Germany for 3 years. Several students are working with him on sponsored projects.