ARS COMBINATORIA 163 (2025) 69–82

Ars Combinatoria
www.combinatorialpress.com/ars

Combinatorial Press

# Primitive normal pairs with prescribed traces over finite fields

Shikhamoni Nath[1], Arpan Chandra Mazumder[1], Dhiren Kumar Basnet[1,] ✉

[1] *Department of Mathematical Sciences, Tezpur University, Tezpur, Assam, 784028, India*

ABSTRACT

Let $q$ be a positive integral power of some prime $p$ and $\mathbb{F}_{q^m}$ be a finite field with $q^m$ elements for some $m \in \mathbb{N}$. Here we establish a sufficient condition for the existence of primitive normal pairs of the type $(\epsilon, f(\epsilon))$ in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ with two prescribed traces, $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(f(\epsilon)) = b$, where $f(x) \in \mathbb{F}_{q^m}(x)$ is a rational function with some restrictions and $a, b \in \mathbb{F}_q^*$. Furthermore, for $q = 5^k$, $m \geq 9$ and rational functions with degree sum 4, we explicitly find at most 13 fields in which the desired pair may not exist.

*Keywords:* finite fields, primitive elements, normal elements, additive and multiplicative characters, trace

*2020 Mathematics Subject Classification.* 12E20, 11T23.

## 1. Introduction

Given a prime power $q$ and a positive integer $m$, we denote the finite field with $q$ elements by $\mathbb{F}_q$ and its extension field of degree $m$ by $\mathbb{F}_{q^m}$. The multiplicative group $\mathbb{F}_{q^m}^*$ is a cyclic group and a generator of this group is called a *primitive* element of $\mathbb{F}_{q^m}$. For an element $\epsilon \in \mathbb{F}_{q^m}$, the elements $\epsilon, \epsilon^q, \epsilon^{q^2}, \ldots, \epsilon^{q^{m-1}}$ are called conjugates of $\epsilon$ with respect to $\mathbb{F}_q$. Sum of all these conjugates is called the trace of $\epsilon$ over $\mathbb{F}_q$ and is denoted by $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\epsilon)$. Further, an element $\epsilon \in \mathbb{F}_{q^m}$ for which the set $\{\epsilon, \epsilon^q, \epsilon^{q^2}, \ldots, \epsilon^{q^{m-1}}\}$ forms a basis of $\mathbb{F}_{q^m}(\mathbb{F}_q)$, when considered as a vector space, is called a *normal* element. An element that is simultaneously primitive and normal is referred to as a primitive normal

✉ Corresponding author.
*E-mail address:* shikha@tezu.ernet.in (S. Nath).

Received 19 September 2024; Accepted 02 May 2025; Published Online 28 June 2025.

DOI: 10.61091/ars163-05

© 2025 The Author(s). Published by Combinatorial Press. This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).

element. Existence of such elements is firstly given by the following theorem.

**Theorem 1.1** (Primitive normal basis theorem). *In the finite field $\mathbb{F}_{q^m}$, there always exists some element which is simultaneously primitive and normal.*

Lenstra and Schoof proved this result in [14]. Later, Cohen and Huczynska [10] presented a modified proof of this result with the help of sieving techniques.

In 1985, Cohen [8] proved the existence of consecutive pairs of primitive elements of the type $(\epsilon, \epsilon^{-1})$ in $\mathbb{F}_q$. After that, it was further developed in [1, 9, 12], among others. Similar studies on primitive normal pairs emerged following the development of the primitive normal basis theorem; they can be studied from [3, 13, 17] etc. and the references therein.

In 2001, Chou and Cohen [5] studied existence of primitive pair $(\epsilon, \epsilon^{-1})$ in $\mathbb{F}_q$ such that both have trace zero over $\mathbb{F}_p$. Cao and Wang [2] proved that, for any prime power $q$ and any positive integer $m$, there exists an element $\epsilon \in \mathbb{F}_{q^m}$ such that $\epsilon + \epsilon^{-1}$ is a primitive element of $\mathbb{F}_{q^m}$ and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\epsilon) = a$, $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\epsilon^{-1}) = b$ for any prescribed $a, b \in \mathbb{F}_q^*$. In [6], Choudhary et al. discussed the existence of primitive pairs $(\epsilon, f(\epsilon))$ with two prescribed traces, where $f$ is a rational function with some restrictions. Recently Sharma et al. [16] considered rational functions $f$ with some minor restrictions over $\mathbb{F}_{q^m}$ for some prime power $q$ and $m \in \mathbb{N}$ and provided a sufficient condition for the existence of primitive normal pair of the form $(\epsilon, f(\epsilon))$ over $\mathbb{F}_q$.

Inspired by all these results, we are presenting a sufficient condition for the existence of primitive normal pair $(\epsilon, f(\epsilon))$ in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ such that $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(f(\epsilon)) = b$, where $f(x) \in \mathbb{F}_{q^m}(x)$ is a rational function with some restrictions and $a, b \in \mathbb{F}_q^*$. The kind of rational functions we will study in this paper are defined below:

**Definition 1.2.** The set $\mathcal{R}_{q^m}^n$ consists of rational functions of the simplest form $f = \frac{f_1}{f_2}$ of degree sum $n = \deg(f_1) + \deg(f_2)$, such that

(i) $f \neq cx^j h^d$ for any $c \in \mathbb{F}_{q^m}^*$, any $j \in \mathbb{Z}$, any $h \in \mathbb{F}_{q^m}(x)$ and any divisor $d$ other than 1 of $q^m - 1$.

(ii) There exists at least one monic irreducible factor $g$ of $f_2$ in $\mathbb{F}_{q^m}[x]$ with multiplicity $r$ such that $q^m \nmid r$.

We will use the notations $\deg(f_1) = n_1$ and $\deg(f_2) = n_2$ throughout. We also note that the second condition of the above definition implies that $n_2 > 0$. This type of rational function is popularly known as Cohen's kind of rational function [12] which also includes Carvalho's kind of rational function [3].

In Section 3, we derive a sufficient condition for the existence of desired primitive normal pairs. In Section 4, we use a sieving inequality to improve the sufficient condition for more efficient results. In Section 5, we study the application of our results over fields of characteristic 5 and for rational functions of degree sum 4 and prove the following:

**Theorem 1.3.** *Let $q = 5^k, m \geq 9$ and $f \in \mathcal{R}_{q^m}^n$. Then, for any $a, b \in \mathbb{F}_q^*$, there exists an element $\epsilon \in \mathbb{F}_{q^m}$ with $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\epsilon) = a$, $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(f(\epsilon)) = b$ and $(\epsilon, f(\epsilon))$ is a primitive normal pair in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ unless $(q, m)$ is one of the 13 pairs: $(5, 9)$, $(5, 10)$, $(5, 11)$,*

$(5,12)$, $(5,14)$, $(5,16)$, $(5,18)$, $(5,20)$, $(5,24)$, $(5^2,9)$, $(5^2,10)$, $(5^2,12)$, $(5^2,24)$.

Now, we present some notations that are significant to this article. We indicate the algebraic closure of $\mathbb{F}_q$ by $\mathbb{F}$. Let $\mathcal{A}_p^n$ be the set of pairs $(q,m)$ such that there exists an element $\epsilon \in \mathbb{F}_{q^m}$ with $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(f(\epsilon)) = b$, where $f(x) \in \mathcal{R}_{q^m}^n$ and $a, b \in \mathbb{F}_q^*$. For each $n \in \mathbb{N}$, we denote the number of prime divisors of $n$ and the number of square-free divisors of $n$ by $w(n)$ and $W(n)$, respectively. Additionally, for $r(x) \in \mathbb{F}_q[x]$, we indicate the number of square-free and monic irreducible $\mathbb{F}_q$-divisors of $r$ by $W(r)$ and $w(r)$, respectively.

## 2. Preliminaries

In this section, we review a few definitions, lemmas and notations that will be used in proving a sufficient condition for the existence of primitive normal pairs of our interest.

**Definition 2.1** (Characters)**.** Let $G$ be a finite abelian group. Then, a character $\chi$ of $G$ is a homomorphism from $G$ to the group $S^1 := \{z \in \mathbb{C} : |z| = 1\}$. The characters of $G$ form a group under multiplication called the *dual group* or *character group* of $G$, which is denoted by $\widehat{G}$. It is well known that $\widehat{G}$ is isomorphic to $G$. Also, $\chi_1$ denotes the trivial character of $G$ defined as $\chi_1(a) = 1$, for all $a \in G$.

A character of a group $G$ of order $d$ is denoted by $\chi_d$. We also denote all the characters of order $d$ by $(d)$.

Corresponding to two different abelian group structures present in a finite field $\mathbb{F}_{q^m}$ i.e., $(\mathbb{F}_{q^m}, +)$ and $(\mathbb{F}_{q^m}^*, \cdot)$; two types of characters can be formed. We refer to them as additive character denoted by $\psi$ and multiplicative character denoted by $\chi$, respectively. Multiplicative characters are extended from $\mathbb{F}_{q^m}^*$ to $\mathbb{F}_{q^m}$ by the rule $\chi(0) = \begin{cases} 0 & \text{if } \chi \neq \chi_1, \\ 1 & \text{if } \chi = \chi_1. \end{cases}$

The additive character $\bar{\psi}(\epsilon) = e^{2\pi i \,\mathrm{Tr}(\epsilon)/p}$, for all $\epsilon \in \mathbb{F}_q$, where Tr is the absolute trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$, is called the canonical additive character of $\mathbb{F}_q$ and every additive character $\psi_\alpha$ for $\alpha \in \mathbb{F}_q$ can be expressed in terms of the canonical additive character $\bar{\psi}$ as $\psi_\alpha(\beta) = \bar{\psi}(\alpha\beta)$ for all $\beta \in \mathbb{F}_q$.

**Definition 2.2.** ($e$-free element) For any divisor $e$ of $q^m - 1$, an element $\epsilon \in \mathbb{F}_{q^m}$ is called $e$-free if $\epsilon \neq \beta^d$ for any $\beta \in \mathbb{F}_{q^m}$ and for any divisor $d$ of $e$ other than 1.

An element $\epsilon \in \mathbb{F}_{q^m}^*$ is primitive if and only if it is $(q^m - 1)$-free. The characteristic function for $e$-free elements of $\mathbb{F}_{q^m}^*$ is defined as follows:

$$\rho_e : \mathbb{F}_{q^m}^* \to \{0,1\}; \epsilon \mapsto \theta(e) \sum_{d|e} \frac{\mu(d)}{\phi(d)} \sum_{(d)} \chi_d(\epsilon), \tag{1}$$

where $\theta(e) := \frac{\phi(e)}{e}$ and $\phi, \mu$ denote the Euler's totient function and Mobius function respectively.

The additive group of $\mathbb{F}_{q^m}$ is a $\mathbb{F}_q[x]$-module under the rule $f \circ \alpha = \sum_{i=0}^{n} a_i \alpha^{q^i}$; for $\alpha \in \mathbb{F}_{q^m}$ and $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}_q[x]$. For $\alpha \in \mathbb{F}_{q^m}$, the $\mathbb{F}_q$-order of $\alpha$ is the monic $\mathbb{F}_q$-divisor $g$ of $x^m - 1$ of minimal degree such that $g \circ \alpha = 0$.

Similarly, for $\psi \in \widehat{\mathbb{F}_{q^m}}$, the $\mathbb{F}_q$-order of $\psi$ is the monic divisor $g$ of $x^m - 1$ of minimal degree such that $\psi \circ g$ is the trivial character, where $(\psi \circ g)(\beta) = \psi(g \circ \beta)$.

**Definition 2.3.** ($g$-free element) Let $g$ divides $x^m - 1$ and $\epsilon \in \mathbb{F}_{q^m}$. If $\epsilon \neq h \circ \gamma$ for any $\gamma \in \mathbb{F}_{q^m}$ and for any divisor $h$ of $g$ other than 1, then $\epsilon$ is called a $g$-free element.

An element $\epsilon \in \mathbb{F}_{q^m}$ is normal if and only if it is $(x^m - 1)$-free. The characteristic function for $g$-free elements of $\mathbb{F}_{q^m}$ is defined as follows:

$$\eta_g : \mathbb{F}_{q^m} \to \{0, 1\}; \epsilon \mapsto \Theta(g) \sum_{h|g} \frac{\mu'(g)}{\Phi(g)} \sum_{(h)} \psi_h(\epsilon), \tag{2}$$

where $\Theta(g) := \frac{\Phi(g)}{q^{\deg(g)}}$ and $\Phi(g) = |(\frac{\mathbb{F}_q[x]}{<g>})^*|$ and the function $\mu'$ is given by:

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

We shall also need characteristic function for prescribed values of trace. For each $a \in \mathbb{F}_q$ the characteristic function for the elements $\epsilon \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\epsilon) = a$, is defined as follows:

$$\tau_a : \mathbb{F}_{q^m} \to \{0, 1\}; \epsilon \mapsto \frac{1}{q} \sum_{\psi \in \widehat{\mathbb{F}_q}} \psi(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\epsilon) - a). \tag{3}$$

The following lemmas will be handy while finding sufficient conditions. The first result was given by Weil [18] as described in [7] at (1.1) to (1.3).

**Lemma 2.4.** *Let $f(x) \in \mathbb{F}_{q^m}(x)$ be a rational function. Write $f(x) = \prod_{j=1}^{k} f_j(x)^{r_j}$, where $f_j(x) \in \mathbb{F}_{q^m}[x]$ are irreducible polynomials and $r_j$ are nonzero integers. Let $\chi$ be a nontrivial multiplicative character of $\mathbb{F}_{q^m}$ of squarefree order $d$ (a divisor of $q^m - 1$). Suppose that $f(x)$ is not of the form $cg(x)^d$ for any rational function $g(x) \in \mathbb{F}_{q^m}(x)$ and $c \in \mathbb{F}_{q^m}^*$. Then we have,*

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

**Lemma 2.5.** [4] *Let $\chi$ and $\psi$ be two nontrivial multiplicative and additive characters of the field $\mathbb{F}_{q^m}$, respectively. Let $f, g$ be rational functions in $\mathbb{F}_{q^m}(x)$, where $f \neq \beta h^r$ and $g \neq h^p - h + \beta$, for any $h \in \mathbb{F}_{q^m}(x)$ and any $\beta \in \mathbb{F}_{q^m}$, and $r$ is the order of $\chi$. Then*

$$\left| \sum_{\alpha \in \mathbb{F}_{q^m} \setminus S} \chi(f(\alpha)) \psi(g(\alpha)) \right| \leq [\deg(g_\infty) + l_0 + l_1 - l_2 - 2] q^{m/2},$$

*where $S$ denotes the set of all poles of $f$ and $g$, $g_\infty$ denotes the pole divisor of $g$, $l_0$ denotes the number of distinct zeroes and finite poles of $f$ in the algebraic closure $\mathbb{F}$ of $\mathbb{F}_q$, $l_1$ denotes the number of distinct poles of $g$ (including infinite pole) and $l_2$ denotes the number of finite poles of $f$, that are also zeroes or poles of $g$.*

Using these, we can now proceed to find all the pairs $(q, m)$, for which there exists a rational function $f \in \mathcal{R}_{q^m}^n$ of degree sum $n$ such that $(\epsilon, f(\epsilon))$ is a primitive normal pair with $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(f(\epsilon)) = b$ for some prescribed values $a, b \in \mathbb{F}_q^*$. Let $\mathcal{A}_p^n$ denotes the set of all such pairs $(q, m)$, where $q$ is power some prime $p$. If $(q, m) \notin \mathcal{A}_p^n$, we refer to such pair as an exceptional pair.

## 3. A sufficient condition for elements in $\mathcal{A}_p^n$

Let $e_1$, $e_2$ be two divisors of $q^m - 1$ and $g_1$, $g_2$ be two divisors of $x^m - 1$. We denote the number of $\epsilon \in \mathbb{F}_{q^m}$ such that $\epsilon$ is both $e_1$-free and $g_1$-free and $f(\epsilon)$ is both $e_2$-free and $g_2$-free with $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(f(\epsilon)) = b$, where $a, b \in \mathbb{F}_q^*$ and $f(x) \in \mathcal{R}_{q^m}^n$ by $N_{f,a,b}(e_1, e_2, g_1, g_2)$. Since the trace of an element is nonzero if and only if it is $(x-1)-$free, therefore to show that an element is $g_i-$free, for $i = 1, 2$, it is enough to prove that the element is $L_{g_i}-$free, where $L_{g_i}$ is the largest divisor of $g_i$ such that $(x-1) \nmid L_{g_i}$. Let $S$ be the set containing all zeros and poles of $f(x)$ along with 0. Now, using the characteristic functions (1), (2), and (3), we get,

$$\begin{aligned} N_{f,a,b}(e_1, e_2, L_{g_1}, L_{g_2}) &= \sum_{\epsilon \in \mathbb{F}_{q^m} \setminus S} \rho_{e_1}(\epsilon)\rho_{e_2}(f(\epsilon))\eta_{L_{g_1}}(\epsilon)\eta_{L_{g_2}}(f(\epsilon))\tau_a(\epsilon)\tau_b(f(\epsilon)) \\ &= \frac{\theta(e_1)\theta(e_2)\Theta(L_{g_1})\Theta(L_{g_2})}{q^2} \sum_{\substack{d_1|e_1, d_2|e_2 \\ t_1|L_{g_1}, t_2|L_{g_2}}} \frac{\mu(d_1)\mu(d_2)\mu'(t_1)\mu'(t_2)}{\phi(d_1)\phi(d_2)\Phi(t_1)\Phi(t_2)} \\ &\quad \times \sum_{\substack{\chi_{d_1}, \chi_{d_2} \\ \psi_{t_1}, \psi_{t_2}}} \chi_{f,a,b}(d_1, d_2, t_1, t_2), \end{aligned}$$

where,

$$\begin{aligned} \chi_{f,a,b}(d_1, d_2, t_1, t_2) &= \sum_{\epsilon \in \mathbb{F}_{q^m} \setminus S} \chi_{d_1}(\epsilon)\chi_{d_2}(f(\epsilon))\psi_{t_1}(\epsilon)\psi_{t_2}(f(\epsilon)) \sum_{\psi \in \widehat{\mathbb{F}_q}} \psi(\mathrm{Tr}(\epsilon) - a) \\ &\quad \times \sum_{\tilde{\psi} \in \widehat{\mathbb{F}_q}} \tilde{\psi}(\mathrm{Tr}(f(\epsilon)) - b), \\ &= \sum_{\epsilon \in \mathbb{F}_{q^m} \setminus S} \chi_{d_1}(\epsilon)\chi_{d_2}(f(\epsilon))\psi_{t_1}(\epsilon)\psi_{t_2}(f(\epsilon)) \\ &\quad \times \sum_{u_1 \in \mathbb{F}_q} \bar{\psi}(\mathrm{Tr}(u_1\epsilon) - u_1 a) \sum_{u_2 \in \mathbb{F}_q} \bar{\psi}(\mathrm{Tr}(u_2 f(\epsilon)) - u_2 b). \end{aligned}$$

Here we have considered $u_1, u_2 \in \mathbb{F}_q$, such that $\psi(\beta) = \bar{\psi}(u_1\beta)$ and $\tilde{\psi}(\beta) = \bar{\psi}(u_2\beta)$ for

all $\beta \in \mathbb{F}_{q^m}$. Let us denote $\bar{\psi}(\mathrm{Tr}(\epsilon)) = \psi'(\epsilon), \forall \epsilon \in \mathbb{F}_{q^m}$, which is an additive character of $\mathbb{F}_{q^m}$. Then the above equation takes the form,

$$\begin{aligned}\chi_{f,a,b}(d_1,d_2,t_1,t_2) = &\sum_{u_1,u_2\in\mathbb{F}_q} \bar{\psi}(-u_1a-u_2b)\\ &\times \sum_{\epsilon\in\mathbb{F}_{q^m}\setminus S} \chi_{d_1}(\epsilon)\chi_{d_2}(f(\epsilon))\psi_{t_1}(\epsilon)\psi_{t_2}(f(\epsilon))\psi'(u_1\epsilon+u_2\epsilon).\end{aligned}$$

There exist, $v_1, v_2 \in \mathbb{F}_{q^m}$, such that $\psi_{t_1}(\epsilon) = \psi'(v_1\epsilon)$ and $\psi_{t_2}(\epsilon) = \psi'(v_2 f(\epsilon))$. Moreover we consider $\chi_{d_1} = \chi_{q^m-1}^{m_1}$ and $\chi_{d_2} = \chi_{q^m-1}^{m_2}$ for some multiplicative character $\chi_{q^m-1}$ of order $q^m-1$, where $m_1 \in \{0,1,\ldots,q^m-2\}$ and $m_2 = \frac{q^m-1}{d_2}$. Then we get,

$$\begin{aligned}\chi_{f,a,b}(d_1,d_2,t_1,t_2) = &\sum_{u_1,u_2\in\mathbb{F}_q} \bar{\psi}(-u_1a-u_2b)\\ &\times \sum_{\epsilon\in\mathbb{F}_{q^m}\setminus S} \chi_{q^m-1}(\epsilon^{m_1}f(\epsilon)^{m_2})\psi'(v_1\epsilon+v_2f(\epsilon)+u_1\epsilon+u_2f(\epsilon))\\ = &\sum_{u_1,u_2\in\mathbb{F}_q} \bar{\psi}(-u_1a-u_2b) \sum_{\epsilon\in\mathbb{F}_{q^m}\setminus S} \sum \chi_{q^m-1}(F_1(\epsilon))\psi'(F_2(\epsilon)),\end{aligned}$$

where,

$$\begin{aligned}F_1(x) =& x^{m_1}f(x)^{m_2},\\ F_2(x) =& (u_1+v_1)x + (u_2+v_2)f(x).\end{aligned}$$

*Case I.* $F_2(x) \neq r(x)^p - r(x) + \beta$ for any $r(x) \in \mathbb{F}_{q^m}(x)$, $\beta \in \mathbb{F}_{q^m}$ and $F_1(x) = x^{m_1}f(x)^{m_2} \neq \beta(h(x))^{q^m-1}$ for any $h(x) \in \mathbb{F}_{q^m}(x)$.

In this case, we can use Lemma 2.5 to derive the following :

$$|\chi_{f,a,b}(d_1,d_2,t_1,t_2)| \leq q^2(2n+1)q^{m/2} + q^2(|S|-1).$$

*Case II.* $F_2(x) = h(x)^p - h(x) + \beta$ for some $h(x) \in \mathbb{F}_{q^m}(x), \beta \in \mathbb{F}_{q^m}$.

For $F_2(x) = h(x)^p - h(x) + \beta$ for some $h(x) \in \mathbb{F}_{q^m}(x), \beta \in \mathbb{F}_{q^m}$; we can show that $g_1 = g_2 = 1$. For this let us consider $f(x) = c_1x^j\frac{f_1}{f_2}$ and $h(x) = c_2x^k\frac{h_1}{h_2}$, where $c_1 \in \mathbb{F}_{q^m}^*, c_2 \in \mathbb{F}_{q^m}^*, j,k \in \mathbb{Z}$ and $f_1, f_2 \in \mathbb{F}_{q^m}[x]$, $h_1, h_2 \in \mathbb{F}_{q^m}[x]$ are monic polynomials such that $x$ divides none of them and $\gcd(f_1,f_2) = 1, \gcd(h_1,h_2) = 1$. Then

$$(u_1+v_1)x + (u_2+v_2)f(x) = h(x)^p - h(x) + \beta.$$

Setting $(u_1+v_1) = k_1$ and $(u_2+v_2) = k_2$ we get,

$$(k_1xf_2 + k_2c_1x^jf_1)h_2^p = (c_2^px^{kp}h_1^p - c_2x^kh_1h_2^{p-1} + \beta h_2^p)f_2. \tag{4}$$

Let $k_2 \neq 0$, then from (4), we get $f_2|h_2^p$, since $(f_1,f_2) = 1$. Also, since $\gcd(h_2^p, c_2^px^{kp}h_1^p - c_2x^kh_1h_2^{p-1} + \beta h_2^p) = 1$, it will imply $h_2^p|f_2$. This further gives us $f_2 = h_2^p$, which creates contradiction due to coprimality restrictions i.e., $\gcd(f_1,f_2) = 1, \gcd(h_1,h_2) = 1$. Therefore, we must have $k_2 = 0$ i.e., $u_2 + v_2 = 0$.

So,

$$k_1 x h_2^p = c_2^p x^{kp} h_1^p - c_2 x^k h_1 h_2^{p-1} + \beta h_2^p, \tag{5}$$

i.e., $h_2$ divides $c_2^p x^{kp} h_1^p - c_2 x^k h_1 h_2^{p-1} + \beta h_2^p$. This gives a contradiction since $\gcd(h_2, c_2^p x^{kp} h_1^p - c_2 x^k h_1 h_2^{p-1}) = 1$. Therefore, $k_1 = 0$ i.e., $u_1 + v_1 = 0$.

Let us take $\psi_{t_1}$ to be an additive character of $\mathbb{F}_q$-order $t_1$. Then we will have,

$$\psi_{t_1}(t_1 \circ \alpha) = 0 \implies \psi'(v_1 t_1 \circ \alpha) = 0 \implies \psi'(-u_1 t_1 \circ \alpha) = 0, \forall \alpha \in \mathbb{F}_{q^m}.$$

Since $u_1 \in \mathbb{F}_q$ and $\mathbb{F}_q$-order of $\psi'$ is $x - 1$, we must have $x - 1 | (-u_1 t_1)$. Therefore, we get $u_1 = 0$. This further implies $v_1 = 0$, since $k_1 = 0$.

Similarly, from $k_2 = 0$, it can be shown that $u_2 = v_2 = 0$. With this, we arrive at the conclusion that, if $F_2(x) = h(x)^p - h(x) + \beta$ for some $h(x) \in \mathbb{F}_{q^m}(x)$ and $\beta \in \mathbb{F}_{q^m}$, then $t_1 = t_2 = 1$.

Let $F_1(x) = x^{m_1} f(x)^{m_2} \neq \beta(h(x))^{q^m - 1}$ for any $h(x) \in \mathbb{F}_{q^m}(x)$ and $\beta \in \mathbb{F}_{q^m}$. In this case, we use Lemma 2.4 to prove that

$$|\chi_{f,a,b}(d_1, d_2, t_1, t_2)| \leq q^2 n q^{m/2} = n q^{\frac{m}{2}+2}.$$

In case $F_1(x) = x^{m_1} f(x)^{m_2} = \beta(h(x))^{q^m - 1}$, for some $h(x) \in \mathbb{F}_{q^m}(x)$ and $\beta \in \mathbb{F}_{q^m}$, then $f(x) \notin \mathcal{R}_{q^m}^n$ due to violation of the first criterion in the definition.

*Case III.* $F_2(x) = h(x)^p - h(x) + \beta$ and $F_1(x) = x^{m_1} f(x)^{m_2} = \beta(h(x))^{q^m - 1}$, for some $h(x) \in \mathbb{F}_{q^m}(x)$ and $\beta \in \mathbb{F}_{q^m}$.

When $F_1(x) = x^{m_1} f(x)^{m_2} = \beta(h(x))^{q^m - 1}$ for some $h(x) \in \mathbb{F}_{q^m}(x)$, we can prove that $d_1 = d_2 = 1$. One can refer to [16] for the proof. So here we have

$$(d_1, d_2, t_1, t_2) = (1, 1, 1, 1).$$

Summarizing all the above cases, we observe that

$$|\chi_{f,a,b}(d_1, d_2, h_1, h_2)| \leq (2n + 1) q^{\frac{m}{2}+2},$$

where $(d_1, d_2, h_1, h_2) \neq (1, 1, 1, 1)$. Now,

$$\begin{aligned} N_{f,a,b}(e_1, e_2, L_{g_1}, L_{g_2}) \geq & \frac{\kappa}{q^2} [(q^m - (2n + 1) q^{\frac{m}{2}+2})(W(e_1) W(e_2) W(L_{g_1}) W(L_{g_2}) - 1)], \\ \geq & \kappa q^{\frac{m}{2}} [q^{\frac{m}{2}-2} - (2n + 1) W(e_1) W(e_2) W(L_{g_1}) W(L_{g_2})], \end{aligned}$$

where $\kappa = \theta(e_1)\theta(e_2)\Theta(L_{g_1})\Theta(L_{g_2})$.

To show that there exists an element $\epsilon \in \mathbb{F}_{q^m}$ such that for preassigned $a, b \in \mathbb{F}_q^*$, and a rational function $f(x) \in \mathcal{R}_{q^m}^n$, $(\epsilon, f(\epsilon))$ is a primitive normal pair with $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(f(\epsilon)) = b$, it is enough to show that $N_{f,a,b}(q^m - 1, q^m - 1, x^m - 1, x^m - 1) > 0$, which is evident if

$$q^{\frac{m}{2}-2} > (2n + 1) W(q^m - 1)^2 W(x^m - 1)^2. \tag{6}$$

## 4. The prime sieve

We will use the following two lemmas to deduce a sieving inequality that will help to improve the sufficient condition (6).

**Lemma 4.1.** *Let $d$ be a divisor of $q^m-1$ and $p_1,p_2,\dots,p_r$ are the remaining distinct primes dividing $q^m-1$. Furthermore, let $g$ be a divisor of $x^m-1$ and $g_1,g_2,\dots,g_s$ are the remaining distinct irreducible polynomials dividing $x^m-1$. Then*

$$N_{f,a,b}(q^m-1,q^m-1,x^m-1,x^m-1) \geq \sum_{i=1}^{r} N_{f,a,b}(p_i d,d,g,g)+\sum_{i=1}^{r} N_{f,a,b}(d,p_i d,g,g)$$
$$+\sum_{i=1}^{s} N_{f,a,b}(d,d,g_i g,g)+\sum_{i=1}^{s} N_{f,a,b}(d,d,g,g_i g)-(2r+2s-1)N_{f,a,b}(d,d,g,g).$$

**Lemma 4.2.** *Let $d,m,q\in\mathbb{N}, g\in\mathbb{F}_q[x]$ be such that $q$ is a prime power, $m\geq 5, d|q^m-1$, and $g|x^m-1$. Let $e$ be a prime number that divides $q^m-1$ but not $d$ and $h$ be any irreducible polynomial dividing $x^m-1$ but not $g$. Then we have the following bounds:*

$$\begin{aligned}
|N_{f,a,b}(ed,d,g,g)-\theta(e)N_{f,a,b}(d,d,g,g)| &\leq (2n+1)\theta(e)\theta(d)^2\Theta(g)^2W(d)^2W(g)^2q^{\frac{m}{2}},\\
|N_{f,a,b}(d,ed,g,g)-\theta(e)N_{f,a,b}(d,d,g,g)| &\leq (2n+1)\theta(e)\theta(d)^2\Theta(g)^2W(d)^2W(g)^2q^{\frac{m}{2}},\\
|N_{f,a,b}(d,d,hg,g)-\Theta(h)N_{f,a,b}(d,d,g,g)| &\leq (2n+1)\Theta(h)\theta(d)^2\Theta(g)^2W(d)^2W(g)^2q^{\frac{m}{2}},\\
|N_{f,a,b}(d,d,g,hg)-\Theta(h)N_{f,a,b}(d,d,g,g)| &\leq (2n+1)\Theta(h)\theta(d)^2\Theta(g)^2W(d)^2W(g)^2q^{\frac{m}{2}}.
\end{aligned}$$

Using Lemma 4.1 and Lemma 4.2, we deduce the following:

**Theorem 4.3.** *Let $d,m,q\in\mathbb{N}, g\in\mathbb{F}_q[x]$ be such that $q$ is a prime power, $m\geq 5, d|q^m-1$ and $g|x^m-1$. Let $d$ be a divisor of $q^m-1$ and $p_1,p_2,\dots,p_r$ be the remaining distinct primes dividing $q^m-1$. Furthermore, let $g$ be a divisor of $x^m-1$ such that $g_1,g_2,\dots,g_s$ are the remaining distinct irreducible factors of $x^m-1$. Define:*

$$l:=1-2\sum_{i=1}^{r}\frac{1}{p_i}-\sum_{i=1}^{s}\frac{1}{q^{\deg(g_i)}},\qquad l>0,$$

*and*

$$L:=\frac{2(r+s)-1}{l}+2.$$

*Then $N_{f,a,b}(q^m-1,q^m-1,x^m-1,x^m-1)>0$ if*

$$q^{\frac{m}{2}-2}>(2n+1)W(d)^2W(g)^2L. \tag{7}$$

**Proof.** For our convenience, let us denote $N_{f,a,b}(q^m-1,q^m-1,x^m-1,x^m-1)$ by $N$.

Then from Lemma 4.1 and 4.2, we have

$$\begin{aligned}
N \geq & \sum_{i=1}^{r}\{N_{f,a,b}(p_i d,d,g,g)-\theta(p_i)N_{f,a,b}(d,d,g,g)\}\\
&+\sum_{i=1}^{r}\{N_{f,a,b}(d,p_i d,g,g)-\theta(p_i)N_{f,a,b}(d,d,g,g)\}\\
&+\sum_{i=1}^{s}\{N_{f,a,b}(d,d,g_i g,g)-\Theta(g_i)N_{f,a,b}(d,d,g,g)\}\\
&+\sum_{i=1}^{s}\{N_{f,a,b}(d,d,g,g_i g)-\Theta(g_i)N_{f,a,b}(d,d,g,g)\}\\
&+\left\{2\sum_{i=1}^{r}\theta(p_i)+2\sum_{i=1}^{s}\Theta(g_i)\right\}N_{f,a,b}(d,d,g,g)-(2r+2s-1)N_{f,a,b}(d,d,g,g)\\
=&\sum_{i=1}^{r}\{N_{f,a,b}(p_i d,d,g,g)-\theta(p_i)N_{f,a,b}(d,d,g,g)\}\\
&+\sum_{i=1}^{r}\{N_{f,a,b}(d,p_i d,g,g)-\theta(p_i)N_{f,a,b}(d,d,g,g)\}\\
&+\sum_{i=1}^{s}\{N_{f,a,b}(d,d,g_i g,g)-\Theta(g_i)N_{f,a,b}(d,d,g,g)\}\\
&+\sum_{i=1}^{s}\{N_{f,a,b}(d,d,g,g_i g)-\Theta(g_i)N_{f,a,b}(d,d,g,g)\}+lN_{f,a,b}(d,d,g,g)\\
\geq&\theta(d)^2\Theta(g)^2 l[\{-(2n+1)W(d)^2W(g)^2q^{\frac{m}{2}}L\}+\{q^{m-2}-(n+1)+(2n+1)q^{\frac{m}{2}}\}].
\end{aligned}$$

Therefore, when $l>0$, then $N_{f,a,b}(q^m-1,q^m-1,x^m-1,x^m-1)>0$ if

$$q^{\frac{m}{2}-2}>(2n+1)W(d)^2W(g)^2L. \tag{8}$$

□

## 5. Numerical computations

In this section, we particularly study the case when finite fields are of characteristic 5 and rational functions are of degree sum 4 and try to determine pairs $(q,m)\in\mathcal{A}_5^4$. For large calculations, we use sagemath [15].

The following lemma will be used extensively throughout the process.

**Theorem 5.1** ([16], Lemma 2.4). *Let $\nu>0$ be a real number and $t$ be a positive integer. Then $W(t)<Dt^{1/\nu}$, where $D=\frac{2^r}{(p_1p_2\ldots p_r)^{\frac{1}{\nu}}}$ and $p_1,p_2,\ldots,p_r$ are primes $\leq 2^\nu$ that divide $t$.*

**Remark 5.2.** For large values of $q$ and $m$, calculation of $W(q^m-1)$ is very time consuming. So, using the above lemma, we find an upper bound for the term $W(q^m-1)$ as follows:

$$W(q^m-1) \leq D(q^m-1)^{\frac{1}{\nu}} < D(q^m)^{\frac{1}{\nu}}.$$

Also, since $x^m-1$ can have atmost $m$ linear factors in $\mathbb{F}_q[x]$. So,

$$W(x^m-1) \leq 2^m.$$

Using these two observations, we rewrite our sufficient condition (6) as:

$$q^{\frac{m}{2}-2} > (2n+1)D^2 q^{\frac{2m}{\nu}} 2^{2m}. \tag{9}$$

In our case, $n=4, m \geq 5, q=5^k$ for some positive integer $k$. We choose $\nu = 21.57$. Then we get $D \leq 1.52 \times 10^{4906}$. For these values, (9) holds for $k \geq 385897$ and $m \geq 5$.

**Table 1.** Values of $\nu$ and $m_k$ corresponding to $k$

| $\nu$ | $k$ | $m_k$ |
|---|---|---|
| 13.7 | 1379,1380, ...,385896 | 6 |
| 11.3 | 212, 213, ..., 1378 | 7 |
| 10.1 | 84, 85, ..., 211 | 8 |
| 9.52 | 48,49, ..., 83 | 9 |
| 9.2 | 33,34, ...,47 | 10 |
| 8.9 | 26,27,..., 32 | 11 |
| 8.7 | 21,22, ..., 25 | 12 |
| 8.6 | 18,19,20 | 13 |
| 8.5 | 16,17 | 14 |
| 8.5 | 14,15 | 15 |
| 8.4 | 13 | 16 |
| 8.4 | 12 | 17 |
| 8.5 | 11 | 18 |
| 8.4 | 10 | 19 |
| 8.4 | 9 | 21 |
| 8.5 | 8 | 24 |
| 8.4 | 7 | 28 |
| 8.5 | 6 | 36 |
| 8.8 | 5 | 52 |
| 9.4 | 4 | 99 |
| 11.3 | 3 | 520 |

Now, for $3 \leq k \leq 385897$, we present a Table 1 that shows suitable values of $\nu$ and an integer $m_k$ corresponding to each value of $k$ such that for all $m \geq m_k$ and that particular $\nu$, (9) holds.

Analyzing the values of $m_k$ and corresponding range of $k$ from Table 1, we observe that (9) holds for all $k \geq 48$ and $m \geq 9$. Based on this, we claim the following:

**Lemma 5.3.** *For $k \geq 3$, and $m \geq 9$, $(q, m) \in \mathcal{A}_5^4$.*

**Proof.** Since for $3 \leq k \leq 47$, (9) holds for all $m \geq m_k$, so for $9 \leq k < m_k$, we first check the following inequality,

$$q^{\frac{m}{2}-2} > (2n+1)D^2 q^{\frac{2m}{\nu}} (W(x^m-1))^2. \tag{10}$$

This inequality reduces the number of possible exceptional pairs to 220. For all these possibilities, we can find suitable values of $d$ and $g$ ( as defined in Theorem 4.3), so that (7) holds. □

We study the pairs for $k = 1$ and $k = 2$ separately. Let us consider $m = m'5^j$ for $j \geq 0$ such that $\gcd(5, m') = 1$. Then, we can divide our discussion into the following two cases:
(i) $m' | q^2 - 1$,
(ii) $m' \nmid q^2 - 1$.
*Case I.* First, let us consider the pairs $(q, m)$, where $m' | q^2 - 1$ and $k = 1$.
Then possible values of $m'$ are 1, 2, 3, 4, 6, 8, 12, 24. Since $W(x^m - 1) = W(x^{m'} - 1)$, we can rewrite (9) as

$$q^{\frac{m'5^j}{2}-2} > (2n+1)D^2 q^{\frac{2m'5^j}{\nu}} 2^{2m'}. \tag{11}$$

Then (11) holds when,
(i) $m' = 1$ and $j \geq 4$,
(ii) $m' = 2$ ,3, 4, 6 and $j \geq 3$,
(iii) $m' = 8$ ,12, 24 and $j \geq 2$.
Therefore $(5, m) \in \mathcal{A}_5^4$ unless $m = 10$, 12, 15, 20, 24, 25, 30, 40, 50, 60, 75, 100, 120, 125, 150. For these pairs, we directly check sufficient condition (6) and reduce the list of possible exceptional values of $m$ to 10, 12, 15, 20, 24, 30. Again for these values of $m$, we try to find suitable $d$ and $g$ ( as defined in Theorem 4.3) for which (7) is satisfied ( see Table 2). But for the pairs $(5, 10)$, $(5, 12)$, $(5, 20)$, $(5, 24)$, we could not find such $d$ and $g$. So in this case, these are the possible exceptional pairs.
Now let $k = 2$ and $m' \nmid q^2 - 1$.
Then possible values of $m'$ are 1, 2, 3, 4, 6, 8, 12, 13, 16, 24, 26, 39, 48, 52, 76, 104, 156, 208, 312, 624. We find out that (11) holds when,
(i) $m' = 1$ ,2, 3 and $j \geq 3$,
(ii) $m' = 4$, 6, 8, 12, 13, 16 and $j \geq 2$,
(iii) $m' = 24$, 26, 39, 48, 52, 76, 104, 156, 208, 312, 624 and $j \geq 1$.
Therefore $(25, m) \in \mathcal{A}_5^4$ unless $m = 10$, 12, 13, 15, 16, 20, 24, 25, 26, 30, 39, 40, 48, 50, 52, 60, 65, 75, 76, 80, 104, 156, 208, 312, 624. We reduce these exceptions by removing the pairs $(25, m)$ that satisfy (6). This leaves us with possible exceptional values of $m = 10, 12, 13, 15, 16, 24, 48$. For these pairs, we try to find $d$ and $g$(as defined in Theorem (4.3)) such that (7) holds( see Table 2). Since we fail to find such $d$ and $g$ for $m = 10, 12, 24$; so $(25, 10), (25, 12), (25, 24)$ adds up to the list of exceptional pairs.
Here $g' = (x+1)(x+2)(x+3)(x+4)(x+\beta)(x+\beta+1)(x+\beta+2)(x+\beta+3)(x+\beta+4)(x+2\beta)(x+2\beta+1)(x+2\beta+2)(x+2\beta+3)(x+2\beta+4)$, with $\beta$ as an generating element of the field.

**Table 2.** Pairs $(q, m)$ when $k = 1, 2$, for which Theorem 7 holds for the above choices of $d$, $r$, $g$, and $s$

| SL No. | $(q, m)$ | $d$ | $r$ | $g$ | $s$ | $l$ | $L$ |
|---|---|---|---|---|---|---|---|
| 1 | (5,13) | 2 | 1 | $(x+4)$ | 3 | 0.990 | 9.07 |
| 2 | (5,15) | 2 | 5 | $(x+4)$ | 1 | 0.633 | 19.37 |
| 3 | (5,21) | 2 | 4 | $(x+4)$ | 4 | 0.850 | 19.65 |
| 4 | (5,22) | 6 | 4 | $(x+1)$ | 5 | 0.480 | 37.04 |
| 5 | (5,30) | 462 | 7 | $(x+1)$ | 3 | 0.298 | 65.71 |
| 6 | (5,80) | 66 | 12 | $(x+1)(x+2)(x+3)(x+4)$ | 4 | 0.466 | 68.50 |
| 7 | $(5^2, 11)$ | 6 | 4 | $(x+4)$ | 2 | 0.883 | 14.46 |
| 8 | $(5^2, 13)$ | 6 | 3 | $(x+4)$ | 6 | 0.980 | 19.34 |
| 9 | $(5^2, 14)$ | 6 | 5 | $(x+1)$ | 5 | 0.692 | 29.45 |
| 10 | $(5^2, 15)$ | 6 | 9 | $(x+4)$ | 2 | 0.231 | 93.03 |
| 11 | $(5^2, 18)$ | 42 | 8 | $(x+1)$ | 9 | 0.216 | 155.00 |
| 12 | $(5^2, 21)$ | 6 | 10 | $(x+4)$ | 8 | 0.348 | 102.67 |
| 13 | $(5^2, 36)$ | 546 | 12 | $(x+1)(x+2)(x+3)(x+4)$ | 16 | 0.095 | 579.62 |
| 14 | $(5^2, 48)$ | 9282 | 10 | $g'$ | 22 | 0.066 | 716.32 |

Before moving to the second case, let us recall the following lemmas.

**Lemma 5.4** ([11], Lemma 6.1). *Suppose $q = 5^k, m' > 4$ and $\bar{m} = \gcd(q-1, m')$. If $M'$ denotes the number of distinct irreducible factors of $x^{m'} - 1$ over $\mathbb{F}_q$, $e$ is the order of $q(\mod m')$ and $\delta(q, m) = \frac{M'}{e}$; Then, the following hold.*

- $\delta(q, m) \leq \frac{1}{2}$, *for* $m = 2\bar{m}$,
- $\delta(q, m) \leq \frac{3}{8}$, *for* $m = 4\bar{m}$,
- $\delta(q, m) \leq \frac{13}{36}$, *for* $m = 6\bar{m}$,
- $\delta(q, m) \leq \frac{1}{3}$, *otherwise.*

**Lemma 5.5** ([16], Lemma 5.3). *Assume that $q = p^k, k \in \mathbb{N}$ and $m = m'p^j, j \geq 0$ is a positive integer such that $m' \nmid q - 1$ and $\gcd(m', p) = 1$. Let $e(> 2)$ denote the order of $q \mod m'$. Then $d = q^m - 1$ and $g$ as the product of the irreducible factors of $x^{m'} - 1$ of degree less than $e$. Then, in the notation of Theorem 4.3, we have $L \leq 2m'$.*

Since $m' \nmid q^2 - 1$ implies $m' \nmid q - 1$ and $e > 2$, we can transform (9) using the above two lemmas as follows:

$$q^{\frac{m'5^j}{2}-2} > 9D^2 q^{\frac{2m'5^j}{\nu}} 2^{2m'\delta(q,m')} 2m',$$

which is also true if

$$q^{\frac{m}{2}-2} > 18D^2 q^{\frac{2m}{\nu}} 2^{2m\delta(q,m')} m. \tag{12}$$

Now, we can proceed to the second case.

*Case II.* $m' \nmid q^2 - 1$. Let $k = 1$. Then possible values of $m'$ are 5, 7, 9, 10, 11, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23. Out of these only 16 is there, such that $16 = 4.\bar{m}$. So

for others, we can rewrite (13) as

$$5^{\frac{m}{2}-2} > 18D^2m5^{\frac{2m}{\nu}}2^{\frac{2m}{3}}. \tag{13}$$

For $\nu = 11.3$, (13) holds for $m \geq 1566$. So we list out the possible exceptional values of $m$ in this case to be $m = 9$, 10, 11, 13, 14, 15, 17, 18, 20, 21, 22, 23, 25, 35, 45, 50, 55, 65, 70, 75, 85, 90, 95, 100, 105, 110, 115, 125, 175, 225, 250, 275, 325, 350, 375, 425, 450, 475, 500, 525, 550, 575, 625, 875, 1125, 1250, 1375. Out of them $m = 9$, 10, 11, 13, 14, 15, 18, 20, 21, 22 don't satisfy (6). For these values, we try to calculate $d$ and $g$ so that condition (7) is satisfied ( see Table 2). For $m = 9$, 10, 11, 14, 18 and 20, we fail to do so. Therefore, they also belong to the list of exceptional values of $m$.

The case $m' = 16$ is handled separately. For this (11) takes the form

$$5^{\frac{m}{2}-2} > 18D^2m5^{\frac{2m}{\nu}}2^{\frac{3m}{4}}. \tag{14}$$

For $\nu = 11.3$, (14) holds for $m \geq 342$. This leaves us with $m = 16$, 80. But for $m = 16$, neither (6) holds, nor can we find any $d$ and $g$ to satisfy (7). So $(5, 16)$ is also a possible exceptional pair. With this, we exhaust the case for $k = 1$.

For $k = 2$, there is no $m'$ such that $m' = 2\bar{m}, 4\bar{m}$ or $6\bar{m}$. So here we can rewrite (11) as

$$(25)^{\frac{m}{2}-2} > 18D^2m(25)^{\frac{2m}{\nu}}2^{\frac{2m}{3}}. \tag{15}$$

With $\nu = 11.3$, (15) holds for all $m \geq 159$.

Therefore, we need to check for $m \in \{9, 10, .., 158\}\backslash\{12, 13, 16, 24, 26, 39, 48, 52, 78, 104, 156\}$. Out of these, for $m = 9$, 10, 11, 14, 15, 18, 21 and 36, (6) do not hold. So we search for $d$ and $g$ so that (7) holds for them. But for $m = 9$, 10, we could not find such $d$ and $g$, so $(25, 9)$, $(25, 10)$ are added up to the list of possible exceptional pairs.

In summarizing the discussions in this section, we obtain the proof of Theorem 1.3.

## Funding

The first author is supported by NFOBC fellowship (NBCFDC Ref. No. 231610154828). The Second author is supported by DST INSPIRE Fellowship, under grant no. DST/INSPIRE Fellowship/2021/IF210206.

## References

[1] A. Booker, S. Cohen, N. Sutherland, and T. Trudgian. Primitive values of quadratic polynomials in a finite field. *Mathematics of Computation*, 88(318):1903–1912, 2019. http://dx.doi.org/10.1090/mcom/3390.

[2] X. Cao and P. Wang. Primitive elements with prescribed trace. *Applicable Algebra in Engineering, Communication and Computing*, 25:339–345, 2014. https://doi.org/10.1016/j.ffa.2022.102094.

[3] C. Carvalho, J. P. Guardieiro, V. G. Neumann, and G. Tizziotti. On the existence of pairs of primitive and normal elements over finite fields. *Bulletin of the Brazilian Mathematical Society, New Series*:1–23, 2021. https://doi.org/10.1007/s40863-021-00224-5.

[4] F. Castro and C. Moreno. Mixed exponential sums over finite fields. *Proceedings of the American Mathematical Society*, 128(9):2529–2537, 2000. https://doi.org/10.1090/S0002-9939-00-05441-1.

[5] W.-S. Chou and S. D. Cohen. Primitive elements with zero traces. *Finite Fields and Their Applications*, 7(1):125–141, 2001. https://doi.org/10.1006/ffta.2000.0284.

[6] A. Choudhary and R. Sharma. Existence of primitive pairs with two prescribed traces over finite fields. *Journal of Algebra and Its Applications*, 23(14):2450245, 2024. https://doi.org/10.1142/S0219498824502451.

[7] T. Cochrane and C. Pinner. Using stepanov's method for exponential sums involving rational functions. *Journal of Number Theory*, 116(2):270–292, 2006. https://doi.org/10.1016/j.jnt.2005.04.001.

[8] S. D. Cohen. Pairs of primitive roots. *Mathematika*, 32(2):276–285, 1985. https://doi.org/10.1112/S0025579300011050.

[9] S. D. Cohen. Pairs of primitive elements in fields of even order. *Finite Fields and Their Applications*, 28:22–42, 2014. https://doi.org/10.1016/j.ffa.2014.01.012.

[10] S. D. Cohen and S. Huczynska. The primitive normal basis theorem–without a computer. *Journal of the London Mathematical Society*, 67(1):41–56, 2003. https://doi.org/10.1112/S0024610702003782.

[11] S. D. Cohen and S. Huczynska. The strong primitive normal basis theorem. *Acta Arithmetica*, 143:299–332, 2010. https://doi.org/10.4064/aa143-4-1.

[12] S. D. Cohen, H. Sharma, and R. Sharma. Primitive values of rational functions at primitive elements of a finite field. *Journal of Number Theory*, 219:237–246, 2021. https://doi.org/10.1016/j.jnt.2020.09.017.

[13] G. Kapetanakis. Normal bases and primitive elements over finite fields. *Finite Fields and Their Applications*, 26:123–143, 2014. https://doi.org/10.1016/j.ffa.2013.12.002.

[14] H. W. Lenstra Jr and R. Schoof. Primitive normal bases for finite fields. *Mathematics of Computation*:217–231, 1987.

[15] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*. 2020. https://www.sagemath.org.

[16] A. K. Sharma, M. Rani, and S. K. Tiwari. Primitive normal values of rational functions over finite fields. *Journal of Algebra and Its Applications*, 22(07):2350152, 2023. https://doi.org/10.1142/S0219498823501529.

[17] H. Sharma and R. K. Sharma. Existence of primitive normal pairs with one prescribed trace over finite fields. *Designs, Codes and Cryptography*, 89:2841–2855, 2021. https://doi.org/10.1007/s10623-021-00956-7.

[18] A. Weil. On some exponential sums. *Proceedings of the National Academy of Sciences*, 34(5):204–207, 1948.