Palestine Journal of Mathematics

Vol 13(4)(2024) , 1252–1265

PAIR OF PRIMITIVE ELEMENTS IN QUADRATIC FORM WITH PRESCRIBED TRACE OVER A FINITE FIELD

Himangshu Hazarika and Dhiren Kumar Basnet

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 12E20; Secondary 11T23.

Keywords and phrases: Finite field; primitive element; free element; normal basis; character; Trace.

The authors would like to thank the reviewers and editor for their constructive comments and valuable suggestions that improved the quality of our paper.

Corresponding Author: Himangshu Hazarika

Abstract *In this paper, we establish a sufficient condition for the existence of primitive element $\alpha \in \mathbb{F}_{q^m}$ such that $f(\alpha)$ is also primitive element of $\mathbb{F}_{q^m}$ and $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \beta$, for any prescribed $\beta \in \mathbb{F}_q$, where $f(x) = ax^2 + bx + c \in \mathbb{F}_{q^m}[x]$ such that $b^2 - 4ac \neq 0$. We conclude that, for $m \geq 5$ there is only one exceptional pair (q, m) which is $(2, 6)$.*

1 Introduction

In the area of Finite Fields, a crucial focus lies on primitive elements and prescribed trace, gaining increased significance with the substantial advancements in technology. The theory surrounding primitive elements with a specified trace has garnered attention due to its distinctive application in combinatorics, coding theory, cryptology, and the mathematical study of electrical circuits. The similar work have been done in [12].

L. Carlitz established the primary idea behind our techniques in his articles [15, 16], which was later developed by Devenport in the late 60's. In 1987, Lenstra and Schoof developed the technique in, which is popularly known as Lenstra-Schoof method.

These techniques find application in the area of irreducible polynomials over finite fields. Given that irreducible polynomials serve as the foundation for constructing extended finite fields, these methods prove highly effective in the context of finite fields. Our results incorporate Vinogradov's formula, specifically for desired primitive pairs and primitive-normal pairs, where the second element of the pair is expressed in terms of a prescribed polynomial. Employing the characteristic function and leveraging the properties of characters, we establish a sufficient condition for the existence of the desired special elements. This systematic approach narrows down our results to a relatively small number of possible exceptional pairs. For the remaining pairs, we delve into further study using modified methods involving character sum estimates. If necessary, we individually compute and estimate the final results.

Exponential sums are key tools for studying finite field theory. One of the important aspects of studying exponential sums for finite fields is observing the special group homomorphisms namely characters.

In order to characterise the elements and their polynomial forms of the finite fields with desired properties such as primitiveness, freeness; characters *and* character sums *become vital tools. In addition to characterizing these elements, we can also provide estimates for the number of special elements in finite fields possessing the desired properties. For a thorough exploration of character theory, readers keen on delving into the subject are recommended to consult classic textbooks such as [13, 17]. This section commences with the definition of a character.*

Definition 1.1. Let $\mathbf{G}$ be a finite abelian group. A character χ of the group $\mathbf{G}$ is a homomorphism from $\mathbf{G} \to \mathbb{S}^1$, where $\mathbb{S}^1 := \{z \in \mathbb{C} : |z| = 1\}$ is the multiplicative group of complex numbers of

unit modulus, i.e. $\chi(a_1a_2) = \chi(a_1)\chi(a_2)$, for all $a_1, a_2 \in \mathbf{G}$. The characters of $\mathbf{G}$ form a group under under multiplication defined by $(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a)$, called *dual group* or *character group* of $\mathbf{G}$, which is isomorphic to the abelian group $\mathbf{G}$ and is denoted by $\widehat{\mathbf{G}}$. If the order of an element (i.e. a character) of the group $\widehat{\mathbf{G}}$ is d, then characters of order d is denoted by (d). The special character $\chi_1 : \mathbf{G} \to \mathbb{S}^1$ defined as $\chi_1(a) = 1$, for all $a \in \mathbf{G}$ is called the *trivial character* of $\mathbf{G}$.

In our research, characters will play a crucial role in characterizing the elements of finite fields $\mathbb{F}_{q^m}$ with specific properties. Sums of combinations of characters will prove highly valuable for computation and further estimation, making such character sums indispensable. When estimating the desired properties of elements, if we focus solely on the sum of values of a single character, this sum is referred to as a character sum*. On the other hand, if we involve one or more characters and combine them with other function values, the sum is termed an* exponential sum*. We commence our theorems with the orthogonality relations of characters.*

Theorem 1.2. *[13, Theorem 5.4]* (Orthogonality relations) *For any nontrivial character χ of a finite abelian group $\mathbf{G}$, and any nontrivial element $\alpha \in \mathbf{G}$, the following hold:*

$$\sum_{\alpha\in\mathbf{G}} \chi(\alpha) = 0 \text{ and } \sum_{\chi\in\widehat{\mathbf{G}}} \chi(\alpha) = 0.$$

The following theorem is fundamental yet crucial for estimating elements with desired properties in a finite field.

Theorem 1.3. *[13, Theorem 5.5] The number of characters of a finite abelian group $\mathbf{G}$ is same as the order of the group $\mathbf{G}$.*

In the upcoming subsections, we introduce characters, character sums, and bounds on character sums for certain functions over finite fields. These bounds play a crucial role in the computation and estimation of specific types of elements within finite fields.

1.1 Characters of finite field

In the finite field $\mathbb{F}_{q^m}$ we have two associate finite abelian groups, which are (i) the multiplicative group *which is denoted by $\mathbb{F}_{q^m}^*$, and (ii)* the additive group *which is denoted by $\mathbb{F}_{q^m}$. Hence we have two characters, namely* multiplicative characters *of $\mathbb{F}_{q^m}^*$ and* additive characters *of $\mathbb{F}_{q^m}$. Multiplicative characters can be extended from $\mathbb{F}_{q^m}^*$ to $\mathbb{F}_{q^m}$ by the rule*

$$\chi(0) = \begin{cases} 0 \text{ if } \chi \neq \chi_1 \\ 1 \text{ if } \chi = \chi_1, \end{cases}$$

where χ_1 denotes the trivial multiplicative character. We denote the trivial additive character by ψ_1.

For a fixed primitive element α of $\mathbb{F}_{q^m}$, for $\mathrm{e}^{(2\pi\iota nk/q^m-1)}$, $n = 0, 1, ..., q^m - 2$; the multiplicative characters of $\mathbb{F}_{q^m}^*$ are obtained as $\chi_n(\alpha^k) = \mathrm{e}^{2\pi\iota nk/q^m-1}$ for $0 \leq k \leq q^m - 2$. Since $\widehat{\mathbb{F}_{q^m}^*} \cong \mathbb{F}_{q^m}^*$, hence $\widehat{\mathbb{F}_{q^m}^*}$ is cyclic. The generators of this group are denoted by χ_g and termed as generator characters*, which are defined by $\chi(\alpha) = \chi_g(\alpha^n)$, for some $1 \leq n \leq q^m - 2$, for any nontrivial character χ of $\widehat{\mathbb{F}_{q^m}^*}$. Further, for any divisor d of $q^m - 1$, there are exactly $\phi(d)$ characters of order d in $\widehat{\mathbb{F}_{q^m}^*}$ and the characters of order are denoted by (d).*

Consider the additive group $\mathbb{F}_{q^m}$. Let p be the characteristic of the finite field $\mathbb{F}_{q^m}$, then $\mathbb{F}_p$ is the prime subfield of $\mathbb{F}_{q^m}$. Let $\mathbf{T} : \mathbb{F}_{q^m} \to \mathbb{F}_p$ be the absolute trace function from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_p$ defined as $\mathbf{T}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + ... + \alpha^{q^{m-1}}$, for $\alpha \in \mathbb{F}_{q^m}$, i.e. sum of conjugates of α with respect to $\mathbb{F}_p$. Then for all $\alpha \in \mathbb{F}_{q^m}$ the function ψ_0 defined as

$$\psi_0(\alpha) = \mathrm{e}^{2\pi\iota\mathbf{T}(\alpha)/p}$$

is an additive character of $\mathbb{F}_{q^m}$. It is trivial that for different additive characters ψ_b of $\mathbb{F}_{q^m}$, we have $\psi_b(\alpha) = \psi_1(b\alpha)$, hence we conclude that all additive characters of $\mathbb{F}_{q^m}$ can be expressed

in terms of ψ_0. The character ψ_0 is called the canonical additive character *of $\mathbb{F}_{q^m}$. For $b = 0$, we have the trivial additive character ψ_1.*

Let $\mathbb{F}_q$ be a finite field of order q and $\mathbb{F}_{q^s}$ be its extended field of order q^s, with $s \geq 1$. For a multiplicative character χ of $\mathbb{F}_q^*$, we have the character $\chi^{(s)}$ defined by $\chi^{(s)}(\alpha) := \chi\left(N_{\mathbb{F}_{q^s}|\mathbb{F}_q}(\alpha)\right)$, for all $\alpha \in \mathbb{F}_{q^s}^*$. Here $N_{\mathbb{F}_{q^s}|\mathbb{F}_q}$ is the norm function *from $\mathbb{F}_{q^s}$ to $\mathbb{F}_q$. Then $\chi^{(s)} \in \widehat{\mathbb{F}_{q^s}^*}$ is called the* lifted character *of χ. Similarly, for an additive character ψ of $\mathbb{F}_q$, we have the lifted character $\psi^{(s)} \in \widehat{\mathbb{F}_{q^s}}$ as $\psi^{(s)}(\alpha) := \chi\left(Tr_{\mathbb{F}_{q^s}|\mathbb{F}_q}(\alpha)\right)$, for all $\alpha \in \mathbb{F}_{q^s}$. Here $Tr_{\mathbb{F}_{q^s}|\mathbb{F}_q}$ is the* trace function *from $\mathbb{F}_{q^s}$ to $\mathbb{F}_q$.*

In this paper, we employ both additive and multiplicative characters of finite fields to effectively articulate the characteristic functions of elements possessing desired properties. Utilizing these characteristic functions, we aim to compute character sums within certain bounds, or at the very least, make estimations that contribute to establishing our results. We initiate our exploration with the following definition provided by Gauss, while Hecke introduced Gaussian sums for algebraic number fields.

Definition 1.4. For multiplicative character χ and additive character ψ of $\mathbb{F}_{q^m}$, the *Gaussian sum* $\mathbb{G}(\psi, \chi)$ is defined by

$$\mathbb{G}(\psi, \chi) = \sum_{\alpha \in \mathbb{F}_{q^m}^*} \psi(\alpha)\chi(\alpha).$$

The absolute value of the Gaussian sum is at most $q^m - 1$. If $\chi \neq \chi_1$ and $\psi \neq \psi_1$ then $|\mathbb{G}(\psi, \chi)| = q^{m/2}$. This is one of the major tool for the estimation of number of special elements of a finite field with desired properties.

Theorem 1.5. *[13, Theorem 5.11] Let χ be a nontrivial multiplicative character and ψ be a nontrivial additive character of $\mathbb{F}_{q^m}$. Then* $\left| \sum_{\alpha \in \mathbb{F}_{q^m}^*} \chi(\alpha)\psi(\alpha) \right| = q^{m/2}$.

The following theorem is called Weil's theorem

Theorem 1.6. *[13, Theorem 5.38] Let ψ be a non trivial additive character of $\mathbb{F}_{q^m}$ and $f(x) \in \mathbb{F}_{q^m}[x]$ be of degree $n \geq 1$ such that* $\gcd(n, q^m - 1) = 1$. *Then*

$$\left| \sum_{\alpha \in \mathbb{F}_{q^m}} \psi(f(\alpha)) \right| \leq (n-1)q^{m/2}.$$

A corresponding theorem for multiplicative characters is presented as follows.

Theorem 1.7. *[13, Theorem 5.41] Consider the multiplicative character χ of $\mathbb{F}_{q^m}$ of order $d > 1$ and let $g(x) \in \mathbb{F}_{q^m}[x]$ be a monic polynomial of positive degree such that $g(x) \neq h(x)^d$ for any $h(x) \in \mathbb{F}_{q^m}[x]$. If g has n distinct roots in its splitting field, then for any $c \in \mathbb{F}_{q^m}$,*

$$\left| \sum_{\alpha \in \mathbb{F}_{q^m}} \chi(cg(\alpha)) \right| \leq (n-1)q^{m/2}.$$

The Theorems 1.6 and 1.7 were proved by Weil [14] on the basis of his proof of the Riemann hypothesis for curves over finite fields. Later, Stepanov established an elementary method, that was developed by Schmidt, to prove similar theorems. This method is known as the Stepanov-Schmidt method.

Continuing, we now delve into the definition of the Kloosterman sum. *This sum, introduced by Kloosterman, originated in connection with a problem involving the representation of integers by a quadratic form.*

Definition 1.8. Let ψ be a nontrivial additive character of $\mathbb{F}_{q^m}$ and $a, b \in \mathbb{F}_{q^m}$. Then the sum

$$K(\psi; a, b) = \sum_{\alpha \in \mathbb{F}_{q^m}^*} \psi(a\alpha + b\alpha^{-1})$$

is called the Kloosterman sum.

Following Lemma is an important bound on Kloosterman sum.

Lemma 1.9. *[13, Theorem 5.45] For a nontrivial additive character ψ of $\mathbb{F}_{q^m}$, the Kloosterman sum $K(\psi; a, b)$ has the bound as follows*

$$|K(\psi; a, b)| \leq 2q^{m/2},$$

where $a, b \in \mathbb{F}_{q^m}$ are not both zero.

Hasse observed that the bound in Lemma 1.9 would follow from the Riemann hypothesis for curves over finite fields. More expressive this hypothesis was provided by Weil and later he showed the bounds for Kloosterman sums in [14]. Weil's proof of Lemma 1.9 was developed by Carlitz and Uchiyama [9] who extended the result by considering the case of fields of even characteristic, which was not treated by Weil.

In our results, We will also use hybrid character sums*, that is character sums that contains both additive and multiplicative characters. The next theorem is one such estimate.*

Theorem 1.10. *[4, Corollary 2.3] Consider any two nontrivial multiplicative characters χ_1, χ_2 of the finite field $\mathbb{F}_{q^m}$. Again let $f_1(x), f_2(x) \in \mathbb{F}_{q^m}[x]$ be two monic pairwise co-prime polynomials such that atleast one of $f_i(x)$ is not of the form $g(x)^{ord(\chi_i)}$ for $i = 1, 2$, where $g(x) \in \mathbb{F}_{q^m}[x]$ is of degree atleast 1. Then*

$$\left| \sum_{\alpha \in \mathbb{F}_{q^m}} \chi_1(f_1(\alpha))\chi_2(f_2(\alpha)) \right| \leq (n_1 + n_2 - 1)q^{m/2},$$

where n_1 and n_2 are the degrees of largest square-free divisors of f_1, f_2 respectively.

The following result by Fu and Wan, which is a special case of [5, Theorem 5.5].

Lemma 1.11. *Let $f_1(x), f_2(x), \ldots, f_k(x) \in \mathbb{F}_{q^m}[x]$ be distinct irreducible polynomials over $\mathbb{F}_{q^m}$. Let $\chi_1, \chi_2, \ldots, \chi_k$ be multiplicative characters and ψ be a non-trivial additive character of $\mathbb{F}_{q^m}$. Then*

$$\left| \sum_{\substack{\alpha \in \mathbb{F}_{q^m} \\ f_i(\alpha) \neq 0}} \chi_1(f_1(\alpha))\chi_2(f_2(\alpha)) \ldots \chi_k(f_k(\alpha))\psi(\alpha) \right| \leq n\, q^{m/2},$$

where $n = \sum_{j=1}^{k} deg(f_j)$.

The following theorem provides us with an estimate for hybrid character sums with rational functions. The theorem was given by Castro and Moreno in [10]. The complete proof of the Theorem was given by Cochrane and Pinner in [11] by using elementary Stepanov-Schmidt method.

Theorem 1.12. *Let χ and ψ be two nontrivial additive and multiplicative characters of the finite field $\mathbb{F}_{q^m}$ respectively. Let $\mathbf{F}$ and $\mathbf{G}$ be rational functions in $\mathbb{F}_{q^m}[x]$, where $\mathbf{F} \neq x\mathbf{H}^n$ and $\mathbf{G} \neq \mathbf{H}^p - \mathbf{H} + \beta$, for any $\mathbf{H} \in \mathbb{F}_{q^m}[x]$, any $\beta \in \mathbb{F}_{q^m}$ and n is the order of χ. Then*

$$\left| \sum_{\alpha \in \mathbb{F}_{q^m} \setminus \mathfrak{S}} \chi(\mathbf{F}(\alpha))\psi(\mathbf{G}(\alpha)) \right| \leq [deg(\mathbf{G}_\infty) + k_0 + k_1 - k_2 - 2]q^{m/2},$$

where $\mathfrak{S}$ denotes the set of all poles of $\mathbf{F}$ and $\mathbf{G}$, $\mathbf{G}_\infty$ denotes the pole divisor of $\mathbf{G}$, k_0 denotes the number of distinct zeroes and finite poles of $\mathbf{F}$ in the algebraic closure $\overline{\mathbb{F}_{q^m}}$ of $\mathbb{F}_{q^m}$, k_1 denotes the number of distinct zeroes and poles of $\mathbf{G}$ (including the infinite pole) and k_2 denotes the number of finite poles of $\mathbf{F}$, that are also zeroes or poles of $\mathbf{G}$.

1.2 characteristic functions of e-free and g-free elements

We begin this section with some preliminary concepts of finite fields. As we know the multiplicative group $\mathbb{F}_{q^m}^*$ is being considered as $\mathbb{Z}$-module with respect to the rule $z \circ \alpha := \alpha^z$, for $z \in \mathbb{Z}$ and $\alpha \in \mathbb{F}_{q^m}^*$; and the additive group $\mathbb{F}_{q^m}$ is being considered as an $\mathbb{F}_q[x]$-module, with respect to the rule $f \circ \alpha := \sum_{i=0}^{n} f_i \alpha^{q^i}$, where $f(x) = \sum_{i=0}^{n} f_i x \in \mathbb{F}_q[x]$ and $\alpha \in \mathbb{F}_{q^m}$. Given that every finite field contains primitive and normal elements, both modules are cyclic, and their generators are primitive and normal elements, respectively. Our results and estimations regarding elements with desired properties are rooted in these modules.

Let ord(α) *denotes the multiplicative order of an element $\alpha \in \mathbb{F}_{q^m}^*$. Then it follows that α is primitive element of $\mathbb{F}_{q^m}$ if and only if $ord(\alpha) = q^m - 1$. Now we have the definition of* e-free *elements.*

Definition 1.13. Let $e|q^m - 1$, then an element $\alpha \in \mathbb{F}_{q^m}$ is called e-free, if $d|e$ and $\alpha = y^d$, for some $y \in \mathbb{F}_{q^m}$ implies $d = 1$.

From the definition it is clear that an element $\alpha \in \mathbb{F}_{q^m}$ is primitive if and only if it is $(q^m - 1)$-free element. The radical of a natural number r is denoted by r_0, where $r = r_0 p^k$ such that $\gcd(r_0, p) = 1$. *It is clear from the definition that $q^m - 1$ can be freely replaced by the radical q_0.*

Now we have the characteristic function for e-free elements.

Definition 1.14. For any $e|q^m - 1$, the characteristic function for the subset of e-free elements of $\mathbb{F}_{q^m}$ is defined as follows:

$$\rho_e : \mathbb{F}_{q^m} \to \mathbb{S}^1; \alpha \mapsto \theta(e) \sum_{d|e} \left(\frac{\mu(d)}{\phi(d)} \sum_{(d)} \chi_d(\alpha) \right), \tag{1.1}$$

where $\theta(e) := \frac{\phi(e)}{e}$, μ is the Möbius function and χ_d stands for any character of $\widehat{\mathbb{F}_{q^m}^*}$ of order d.

For e-free elements, Cohen and Huczynska introduced the "integral" notation for weighted sums in [6, 7] as follows

$$\int_{d|e} \chi_d := \sum_{d|e} \frac{\mu(d)}{\phi(d)} \sum_{(d)} \chi_d.$$

Then the characteristic function (1.1) *becomes*

$$\rho_e : \alpha \mapsto \theta(e) \int_{d|e} \chi_d(\alpha). \tag{1.2}$$

The additive group $\mathbb{F}_{q^m}$ can be seen as $\mathbb{F}_q[x]$-module with respect to the rule $f \circ \alpha := \sum_{i=0}^{n} f_i \alpha^{q^i}$, where $f(x) = \sum_{i=0}^{n} f_i x \in \mathbb{F}_q[x]$ and $\alpha \in \mathbb{F}_{q^m}$. Then the $\mathbb{F}_q$-order *of an additive character $\chi_g \in \widehat{\mathbb{F}_{q^m}}$ is the monic $\mathbb{F}_q$-divisor g of $x^m - 1$ of minimal degree such that $\chi_g \circ g$ is the trivial character of $\widehat{\mathbb{F}_{q^m}}$. It is well-known that there are $\Phi(g)$ characters ψ_g, where $\Phi(g) = |(\mathbb{F}_q[x]/g\mathbb{F}_q[x])^*|$ is the analogue of the Euler's phi function over $\mathbb{F}_q[x]$. Now we have the definition of g-free element.*

Definition 1.15. For $g|x^m - 1$, an element $\alpha \in \mathbb{F}_{q^m}$ is called g-free element if $\alpha = h \circ \beta$ for some $\beta \in \mathbb{F}_{q^m}$ and $h|g$ implies $h = 1$.

From the definition it is obvious that an element $\alpha \in \mathbb{F}_{q^m}$ is normal if and only if it is $(x^m - 1)$-free. From the definition, it is clear that $x^m - 1$ can be freely replaced by the radical $g_0 := x^{m_0} - 1$, where m_0 is such that $m = m_0 p^a$, here a is a non-negative integer and $\gcd(m_0, p) = 1$.

Now we have the characteristic function for g-free *elements as follows*

Definition 1.16. For any $g|x^m-1$, the characteristic function for the subset of g-free elements of $\mathbb{F}_{q^m}$ is defined as follows:

$$\eta_g : \mathbb{F}_{q^m} \to \mathbb{S}^1; \alpha \mapsto \Theta(g)\sum_{f|g}\left(\frac{\mu'(f)}{\Phi(f)}\sum_{(f)}\psi_f(\alpha)\right), \tag{1.3}$$

where $\Theta(g) := \frac{\Phi(g)}{q^{deg(g)}}$, ψ_f stands for any character of $\widehat{\mathbb{F}_{q^m}}$ of $\mathbb{F}_q$-order f and μ' is the analogue Möbius function defined as follows

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

We use the "integral" notation for weighted sum of additive characters as follows

$$\int_{f|g}\psi_f := \sum_{f|g}\frac{\mu'(f)}{\Phi(f)}\sum_{(f)}\psi_f.$$

Then the characteristic function given by (1.3), for the set of g-free elements in $\mathbb{F}_{q^m}$, for any $g|x^m-1$, is given by

$$\eta_g : \alpha \mapsto \Theta(g)\int_{f|g}\psi_f(\alpha). \tag{1.4}$$

The above characteristic functions are derived form of the Vinogradov's formula [8, page 183]. Throughout our paper, we will use all these notations, unless or otherwise explicitly stated.

Following the Vinogradov's formula, the characteristic function of the set of elements $\alpha \in \mathbb{F}_{q^m}$ with $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \beta \in \mathbb{F}_q$ is given by

$$\Gamma_\beta : \alpha \mapsto \frac{1}{q}\sum_{\psi\in\widehat{\mathbb{F}_{q^m}}}\psi(Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)-\beta).$$

in which the sum runs over all additive characters ψ of $\mathbb{F}_{q^m}$, i.e., all elements of $\widehat{\mathbb{F}_{q^m}}$.

Since every additive character ψ of $\mathbb{F}_q$ can be obtained by the canonical additive character ψ_0 of $\mathbb{F}_q$ as $\psi(\alpha) = \psi_0(u\alpha)$, where u is some element of $\mathbb{F}_q$.

$$\begin{aligned}\Gamma_\beta(\alpha) &= \tfrac{1}{q}\sum_{u\in\mathbb{F}_q}\psi_0(Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(u\alpha)-u\beta) \\ &= \tfrac{1}{q}\sum_{u\in\mathbb{F}_q}\widehat{\psi_0}(u\alpha)\psi_0(u\beta),\end{aligned} \tag{1.5}$$

where $\widehat{\psi_0}$ is the additive character of $\mathbb{F}_{q^m}$ defined by $\widehat{\psi_0}(\alpha) = \psi_0(Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha))$.

2 Existence of primitive pairs with prescribed trace

In this section we establish a sufficient condition for every $\beta \in \mathbb{F}_q$, the existence of a primitive pair $(\alpha, f(\alpha)) \in \mathbb{F}_{q^m}$ such that $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \beta$. Take r_1, r_2 such that $r_1, r_2|q^m-1$. Define $\mathfrak{T}(r_1, r_2)$ to be the number of $\alpha \in \mathbb{F}_{q^m}$ such that α is r_1-free and $f(\alpha)$ is r_2-free, where $f(x) = ax^2+bx+c$ and $a, b, c \in \mathbb{F}_{q^m}$, $b^2-4ac \neq 0$ and $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \beta \in \mathbb{F}_q$. Hence it is sufficient to show that $\mathfrak{T}(q^m-1, q^m-1) > 0$ for every $\beta \in \mathbb{F}_q$.

We use the notation $\omega(n)$ to denote the number of prime divisors of n. For calculations we use $W(n) := 2^{\omega(n)}$.

Theorem 2.1. *Let $\beta \in \mathbb{F}_q$ and $r_1, r_2|q^m-1$. Then $\mathfrak{T}(r_1, r_2) > 0$ if $q^{m/2-1} > 2W(r_1)W(r_2)$.*

In particular if $q^{m/2-1} > 2W(q^m-1)^2$, then $\mathfrak{T}(q^m-1, q^m-1) > 0$.

Proof. By definition $\mathfrak{T}(r_1, r_2) = \sum_{\alpha \in \mathbb{F}_{q^m}^*} \sigma_{r_1}(\alpha)\sigma_{r_2}(f(\alpha))\Gamma(\alpha)$. Now

$$\mathfrak{T}(r_1, r_2) = \frac{\theta(r_1)\theta(r_2)}{q} \sum_{\substack{d_2|r_2 \\ d_1|r_1}} \frac{\mu(d_1)\mu(d_2)}{\phi(d_1)\phi(d_2)} \sum_{\chi_{d_1}, \chi_{d_2}} S(\chi_{d_1}, \chi_{d_2}), \tag{2.1}$$

where

$$S(\chi_{d_1}, \chi_{d_2}) = \sum_{u \in \mathbb{F}_q} \psi_0(-\beta u) \sum_{\alpha \in \mathbb{F}_{q^m}^*} \chi_{d_1}(\alpha)\chi_{d_2}(a\alpha^2 + b\alpha + c)\widehat{\psi_0}(u\alpha).$$

Now, we have $\chi_{d_1}(x) = \chi_{q^m-1}(x^{m_i}) = \chi(x^{m_i})$ for $0 \le m_i \le q^m - 2$.

$$\begin{aligned} S(\chi_{d_1}, \chi_{d_2}) &= \sum_{u \in \mathbb{F}_q} \psi_0(-\beta u) \sum_{\alpha \in \mathbb{F}_{q^m}^*} \chi(\alpha^{m_1}(a\alpha^2 + b\alpha + c)^{m_2})\widehat{\psi_0}(u\alpha) \\ &= \sum_{u \in \mathbb{F}_q} \psi_0(-\beta u) \sum_{\alpha \in \mathbb{F}_{q^m}^*} \chi(F(\alpha))\widehat{\psi_0}(u\alpha), \end{aligned}$$

where $F(x) = x^{m_1}(ax^2 + bx + c)^{m_2} \in \mathbb{F}_{q^m}[x]$, $0 \le m_1, m_2 \le q^m - 2$.

If $F(x) \ne yH^{q^m-1}$ for any $y \in \mathbb{F}_{q^m}$ and $H \in \mathbb{F}_{q^m}[x]$, then by following the [4, Lemma 2.2] we have

$$\left| \sum_{\alpha \in \mathbb{F}_{q^m}^*} \chi(F(\alpha))\psi_0(u\alpha) \right| \le (0 + 3 + 1 - 0 - 2)q^{m/2} = 2q^{m/2}.$$

Then we have

$$\begin{aligned} |S| &= \left| \sum_{u \in \mathbb{F}_q} \psi_0(-\beta u) \sum_{\alpha \in \mathbb{F}_{q^m}^*} \chi(F(\alpha))\widehat{\psi_0}(u\alpha) \right| \le \sum_{u \in \mathbb{F}_q} \left| \psi_0(-\beta u) \sum_{\alpha \in \mathbb{F}_{q^m}^*} \chi(F(\alpha))\widehat{\psi_0}(u\alpha) \right| \\ &= \sum_{u \in \mathbb{F}_q} |\psi_0(-\beta u)| \left| \sum_{\alpha \in \mathbb{F}_{q^m}^*} \chi(F(\alpha))\widehat{\psi_0}(u\alpha) \right| \le \sum_{u \in \mathbb{F}_q} |\psi_0(-\beta u)|\, 2q^{m/2} = 2q^{m/2+1}. \end{aligned}$$

Let $F = yH^{q^m-1}$ for some $y \in \mathbb{F}_{q^m}$ and $H \in \mathbb{F}_{q^m}[x]$. Then we have $x^{m_1}(ax^2 + bx + c)^{m_2} = yH^{q^m-1}$.

If $m_1 \ne 0$, then $(ax^2 + bx + c)^{m_2} = yx^{q^m-1-m_1}B^{q^m-1}$, where $B(x) = \frac{H(x)}{x}$. Comparing the degrees we have

$$q^m - 1 - m_1 + k(q^m - 1) \Rightarrow m_1 + 2m_2 = (k + 1)(q^m - 1), \tag{2.2}$$

where k is the degree of B.

Since $m_1 \ne q^m - 1$, hence we have $c = 0$. Then

$$\begin{aligned} (ax^2 + bx)^{m_2} &= yx^{q^m-1-m_1}B^{q^m-1} \\ \text{imples} \quad x^{m_2}(ax + b)^{m_2} &= yx^{q^m-1-m_1}B^{q^m-1}. \end{aligned} \tag{2.3}$$

If $m_2 \ne 0$, then we have

$$(ax + b)^{m_2} = yx^{q^m-1-m_1-m_2}B^{q^m-1}. \tag{2.4}$$

If $q^m - 1 \ne m_1 + m_2$, then $b = 0$, which is a contradiction. Hence $q^m - 1 = m_1 + m_2$. From (2.2), we have $m_2 + (q^m - 1) = (k + 1)(q^m - 1)$ i.e., $m_2 = k(q^m - 1)$, which is possible only if $k = 0$. Again from (2.3), we have $a = 0$, which is a contradiction. Hence m_2 must be zero and thus m_1 must be zero or $m_1 = m_2 = 0$, i.e. when $F = yH^{q^m-1}$, $(\chi_{d_1}, \chi_{d_2}) = (\chi_1, \chi_2)$.

If $u \ne 0$, then $|S(\chi_{d_1}, \chi_{d_2})| = q - 1 \le 2q^{m/2+1}$.

Hence $|S(\chi_{d_1}, \chi_{d_2})| \le 2q^{m/2+1}$, when $(\chi_{d_1}, \chi_{d_2}, u) \ne (\chi_1, \chi_1, 0)$. Then we have

$$\mathfrak{T}(r_1, r_2) \ge \frac{\theta(r_1)\theta(r_2)}{q} \left(q^m - 1 - 2q^{m/2+1}(W(r_1)W(r_2) - 1) \right). \tag{2.5}$$

Hence $\mathfrak{T}(r_1, r_2) > 0$ i.e., the sufficient condition is

$$q^{m/2-1} > 2W(r_1)W(r_2).$$

This completes the proof. □

In particular if

$$q^{m/2-1} > 2W(q^m - 1)^2, \tag{2.6}$$

then $\mathfrak{T}(q^m - 1, q^m - 1) > 0$.

3 Prime Sieving in the Estimation

We begin this section with the following Lemma.

Lemma 3.1. *Let* $r|q^m - 1$ *and* p *any prime dividing* $q^m - 1$ *but not* r.

$$|\mathfrak{T}(pr, r) - \mathfrak{T}(r, r)| \leq \frac{2\theta(r)^2\theta(p)}{q} W(r)^2 q^{m/2+1}$$

and

$$|\mathfrak{T}(r, pr) - \mathfrak{T}(r, r)| \leq \frac{2\theta(r)^2\theta(p)}{q} W(r)^2 q^{m/2+1}.$$

This proof is identical with [1, Lemma 3.2], hence we omit the proof.

3.1 Sieving inequality

Lemma 3.2. *[3, Sieve Inequality] Let* r *be a divisor of* $q^m - 1$ *and* $p_1, p_2, \ldots, p_n$ *be the distinct primes dividing* $q^m - 1$ *but not* r. *Abbreviate* $\mathfrak{T}(q^m - 1, q^m - 1)$ *to* $\mathfrak{T}$. *Then*

$$\mathfrak{T} \geq \sum_{i=1}^{n} \mathfrak{T}(p_i r, r) + \sum_{i=1}^{n} \mathfrak{T}(r, p_i r) - (2n - 1)\mathfrak{T}(r, r). \tag{3.1}$$

Applying the sieving inequality we have the following Lemma.

Lemma 3.3. *With all the assumptions as in Lemma 3.2, define*

$$\Delta := 1 - 2\sum_{i=1}^{n} \frac{1}{p_i}$$

and

$$\Lambda := \frac{2n + k - 1}{\Delta} + 2.$$

Suppose $\Delta > 0$. *Then a sufficient condition for the existence of a primitive element* α *for which* $a\alpha^2 + b\alpha + c$ *is also primitive in* $\mathbb{F}_{q^m}$ *with* $b^2 - 4ac \neq 0$ *and* $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \beta$ *is*

$$q^{m/2-1} > 2W(d)^2\Lambda. \tag{3.2}$$

Proof. A key step is to write (3.1) in the equivalent form

$$\mathfrak{T} \geq \frac{\theta(r)^2}{q} \left(\sum_{i=1}^{n} 2\theta(p_i) \left(-2q^{m/2+1} W(r)^2 \right) + \Delta \left(q^m - 1 - 2q^{m/2+1}(W(r)^2 - 1) \right) \right). \tag{3.3}$$

Then

$$\mathfrak{T} \geq \frac{\theta(r)^2}{q} \Delta \left[\left(\frac{2\sum_{i=1}^{n} \theta(p_i)}{\Delta} + 1 \right) \{-2q^{m/2+1} W(r)^2\} + \{q^m - 1 + 2q^{m/2+1}\} \right].$$

Since $\Delta = 2\sum_{i=1}^{n}\theta(p_i) - (2n-1)$ and $\Lambda = \left(\frac{2\sum_{i=1}^{n}\theta(p_i)}{\Delta} + 1\right)$, we have

$$\mathfrak{T} \geq \frac{\theta(r)^2}{q}\Delta\left[-2\Lambda q^{m/2+1}W(r)^2 + q^m - 1 + 2q^{m/2+1}\right].$$

We already have $\Delta > 0$, hence $\mathfrak{T} > 0$ if $q^{m/2-1} > q^{-m/2-1} - 2 + 2W(r)^2\Lambda$ i.e., if $q^{m/2-1} > 2W(r)^2\Delta$. That is it is sufficient if

$$q^{m/2-1} > 2W(r)^2\Lambda,$$

giving us our sufficient condition.

□

4 Some estimates for existence of primitive pair with prescribed trace

For the remaining part of the article we are going to denote by $\mathfrak{T}$, the set of all pairs (q,m) for which $\mathbb{F}_{q^m}$ contains primitive pair $(\alpha, f(\alpha))$ with a prescribed trace. First we have the following Lemma from [2].

Lemma 4.1. *For any $n, \alpha \in \mathbb{N}$, $W(n) \leq B_{\alpha,n}n^{1/\alpha}$, where $B_{\alpha,n} = \frac{2^\alpha}{(p_1p_2\ldots p_k)^{1/\alpha}}$ and $p_1, p_2, \ldots, p_k$ are primes $\leq 2^\alpha$ that divide n and W denotes the same as described before.*

From this, we have the following lemma:

Lemma 4.2. *With the same meaning of W as mentioned above, we have*

- *For $\alpha = 6$, $W(n) < 37.4683n^{1/6}$,*
- *For $\alpha = 8$, $W(n) < 4514.7n^{1/8}$,*
- *For $\alpha = 14$, $W(n) < (5.09811 \times 10^{67})n^{1/14}$.*

Lemma 4.3. *Let N be a positive integer such that $\omega(N) \geq 85$, i.e. $N > 2.41 \times 10^{179}$. Then $W(N) < N^{1/7}$.*

Proof. The product of first 85 primes exceeds $M = 2.41 \times 10^{179}$. We write $N = n_1n_2$, a product of coprime integers, where all primes dividing n_1 are amongst the least 85 primes dividing N and those dividing n_2 are larger primes. Hence $n_1 > M$ and $n_1^{1/7} > M^{1/7} > 4.23 \times 10^{25}$, where as $W(n_1) = 2^85 < 1.93 \times 10^{25}$. Since $\mathfrak{p}^{1/7} > 2$ for all primes $\mathfrak{p} > 435$ (85^{th} prime), the result follows. □

Theorem 4.4. *Let q be some prime power, i.e. $q = p^s$, where p is any prime and s is a positive integer. Then $(q,m) \in \mathfrak{T}$ when $q \geq 16$ and $m \geq 29$.*

Proof. From the Lemma 4.2 we have $W(n) < 4514.7n^{1/8}$. Using this in the condition $q^{m/2-1} > 2W(q^m-1)^2$, we have a sufficient condition as $q^{m/4-1} > 2.03825 \times 10^7$. When $q \geq 16$, then the condition holds for $m \geq 29$. □

For the remaining cases i.e. q=2, 3, 4, 5, 7, 8, 9, 11, 13, the condition holds for m= 102, 64, 53, 46, 39, 37, 35, 33, 31 respectively. We check the pairs by further calculation.

4.1 Estimates for fields of odd characteristic

Let q be a odd prime power. As already discussed in Theorem 4.4, $m \geq 29$ for $q \geq 16$, in this section we assume that $m \leq 28$. We use the notation ω to denote $\omega(q^m-1)$ throughout this chapter. We begin with the following theorem.

Theorem 4.5. *Suppose $\mathbb{F}_{q^m}$ be a field of odd characteristic and $m \geq 5$ is a positive integer. Then there exists a primitive element $\alpha \in \mathbb{F}_{q^m}$ such that $a\alpha^2 + b\alpha + c$ is also primitive in $\mathbb{F}_{q^m}$ with $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \beta$ for any prescribed $\beta \in \mathbb{F}_q$, unless (q,m) is one of the pairs* (3,5), (3,6), (3,7), (3,8), (3,12), (5,5), (5,6), (5,8), (7,5), (7,6), (7,7), (9,5), (9,6), (11,5), (11,6), (13,5), (13,6), (17,6), (19,5), (19,6), (23, 6), (25,5), (29,6), (31,5), (31,6) and (37,5).

Proof. At first we assume that $\omega \geq 85$. Then from the sufficient condition (2.6), applying the Lemma 4.3, we have the inequality as $q^{\frac{3m}{14}-1} > 2$. Which holds unless $q \leq 16411$ if $m = 5$ or $q \leq 13$ if $m = 6$, this implies that $\omega < 85$.

Next we assume that $21 \leq \omega \leq 84$. Then as in Lemma 3.2, let r be the divisor of $q^m - 1$, whose prime factors are atleast 21 primes dividing $q^m - 1$ and hence $r \leq 63$. In Lemma 3.3 when $r = 63$, we have $\Delta > 0.373307$ and hence $\Lambda < 336.845$. Thus $2 \times W(r)^2 \times \Lambda < 2.96292 \times 10^{15}$. Now the sufficient condition is $q^m > (2 \times W(r)^2 \times \Lambda)^{\frac{2m}{m-2}}$, which becomes $q^m > (2 \times W(r)^2 \times \Lambda)^{\frac{10}{3}}$ (as $m \geq 5$). Hence the inequality becomes $q^m > 3.73594 \times 10^{51}$. In fact when $\omega \geq 33$, then $q^m - 1$ is the product of atleast first 33 primes, i.e. $q^m > 7.2 \times 10^{52}$. So $(q, m) \in \mathfrak{T}$ when $\omega \geq 33$ or $q > (3.73 \times 10^{51})^{1/m}$. When $m = 5$, $q > 2.06291 \times 10^{10}$.

Then we assume $4 \leq \omega \leq 32$ and $q < 2.06291 \times 10^{10}$. Then proceeding as above we assume $\omega(r) = 6$, $r = 26$ then $\Delta > 0.0626089$ and hence $\Lambda < 816.581$. Hence $2 \times W(r)^2 \times \Lambda < 6.68943 \times 10^{22}$, i.e. the sufficient condition is $q^m > 5.60424 \times 10^{22}$. When $\omega \geq 18$, then $q^m > 1.17288 \times 10^{23}$. We conclude that $(q, m) \in \mathfrak{T}$ when $\omega \geq 18$ or $q > (5.64024 \times 10^{22})^{1/m}$. Finally $q > 35503$ when $m = 5$.

In the next stage our range for ω is $4 \leq \omega \leq 17$ and $q < 35503$. We take $\omega(r) = 5$ and then $r = 12$, then $\Delta > 0.139272$ and hence $\Lambda < 167.144$. Hence $2 \times W(r)^2 \times \Lambda < 342311$ i.e. $q^m > 2.80588 \times 10^{18}$. In fact when $\omega \geq 16$, then $q^m > 3.25891 \times 10^{19}$. From which we have $(q, m) \in \mathfrak{T}$, when $\omega \geq 16$ or $q > (2.80588 \times 10^{18})^{1/m}$. Finally $q > 4894$ when $m = 5$.

Then we assume $4 \leq \omega \leq 15$ and $q < 4894$. Then proceeding as above we take $\omega(r) = 5$, $r = 10$, so $\Delta > 0.210906$ and hence $\Lambda < 92.0875$. Hence $2 \times W(r)^2 \times \Lambda < 188595$, i.e. the sufficient condition is $q^m > 3.84682 \times 10^{17}$. When $\omega \geq 15$, then $q^m > 6.14889 \times 10^{17}$. We conclude that $(q, m) \in \mathfrak{T}$, when $\omega \geq 15$ or $q > (3.84682 \times 10^{17})^{1/m}$. Finally $q > 3289$ when $m = 5$.

Next we take $4 \leq \omega \leq 14$, then repeating the above process with $\omega(r) = 4$, $r = 10$, we have $\Delta > 0.0716411$ and $\Lambda < 267.211$. Hence the inequality is $2 \times W(r)^2 \times \Lambda < 136812$. The condition holds when $q > (1.31951 \times 10^{17})^{1/m}$. Then the condition holds when $m = 5$, $q > 2655$, when $m = 6$, $q > 714$; when $m = 7$, $q > 279$; when $m = 8$, $q > 138$; when $m = 9$, $q > 80$; when $m = 10$, $q > 52$; when $m = 11$, $q > 36$; when $m = 12$, $q > 27$; when $m = 13$, $q > 21$; when $m = 14$, $q > 17$; when $m = 15$, $q > 13$ and when $m = 16$, $q > 11$.

By calculation we have, if $\omega \leq 3$, then the pairs satisfy (2.6) with $r = q^m - 1$.

Applying the Prime Sieve technique with appropriate choice of r from the factors of $q^m - 1$ in (3.2) as some of the calculations shown in Table 1, for $m \geq 5$, $(q, m) \in \mathfrak{T}$ except possibly one of the pairs (3, 5), (3, 6), (3, 7), (3, 8), (3, 12), (5, 5), (5, 6), (5, 8), (7, 5), (7, 6), (7, 7), (9, 5), (9, 6), (11, 5), (11, 6), (13, 5), (13, 6), (17, 6), (19, 5), (19, 6), (23, 6), (25, 6), (29, 6), (31, 5), (31, 6) and (37, 7).

Hence the proof is complete. □

Table 1 illustrates some of the calculations to show that pairs (q, m) satisfying the condition $q^{m/2-1} > 2 \times W(r)^2 \times \Lambda$.

(q, m)	primes of $q^m - 1$	$\omega(d)$	Δ	Λ	$q^{m/2-1}$	$2 \times W(r)^2 \times \Lambda$
(17, 5)	2, 88741	1	0.999977	3.00002	70.0928	24.00002
(23, 5)	2, 11, 292561	1	0.818175	5.6667	110.304	45.3336
(27, 5)	2, 11, 13, 4561	1	0.663897	9.53129	140.296	76.2503
(29, 5)	2, 7, 732541	1	0.714283	6.20002	156.17	49.6
(41, 5)	2, 5, 579281	1	0.599997	7.00003	262.528	56.00002
(43, 5)	2, 3, 7, 3500201	2	0.714285	6.2	281.97	198.4
(47, 5)	2, 11, 23, 31, 14621	1	0.666572	12.5015	322.216	100.012
(61, 5)	2, 3, 5, 131, 21491	2	0.58464	10.5523	476.425	337.674
(25, 6)	2, 3, 7, 13, 31, 601	2	0.492561	16.2104	625	518.733

(q, m)	primes of $q^m - 1$	$\omega(d)$	Δ	Λ	$q^{m/2-1}$	$2 \times W(r)^2 \times \Lambda$
(27, 6)	2, 7, 13, 19, 37, 757	1	0.39848	24.6426	729	197.141
(37, 6)	2, 3, 7, 19, 31, 43, 67	2	0.468144	21.2249	1369	679.197
(41, 6)	2, 3, 5, 7, 547, 1723	2	0.309469	24.6194	1681	787.821
(43, 6)	2, 3, 7, 11, 13, 139, 631	2	0.361063	26.9264	1849	861.645
(61, 6)	2, 3, 5, 7, 13, 31, 97, 523	3	0.471481	21.08888	3721	2699.37
(5, 7)	2, 19531	1	0.999898	3.0001	55.9017	24
(9, 7)	2, 547, 1093	1	0.994514	5.01655	243	40.1324
(11, 7)	2, 5, 43, 45319	1	0.553444	11.0343	401.312	88.2744
(19, 7)	2, 3, 701, 70841	2	0.997119	5.00867	1573.56	160.277
(7, 8)	2, 3, 5, 1201	2	0.598335	7.01391	343	224.445
(9, 8)	2, 5, 17, 41, 193	1	0.42321	18.5403	729	148.322
(11, 8)	2, 3, 5, 61, 7321	2	0.56694	10.8193	1331	346.218
(3, 9)	2, 13, 757	1	0.843512	5.55656	46.7654	44.4525
(5, 9)	2, 19, 31, 829	1	0.827807	8.04005	279.508	64.3204
(3, 10)	2, 11, 61	1	0.785395	5.81973	81	46.5578
(5, 10)	2, 3, 11, 71, 521	2	0.786174	8.35992	625	267.517
(3, 11)	2, 23, 3851	1	0.912524	5.27858	140.296	42.3006
(5, 12)	2, 3, 7, 13, 31, 601	2	0.492596	16.2104	3125	518.733
(3, 13)	2, 797161	1	0.999997	3	420.888	24
(3, 14)	2, 547, 1093	1	0.994514	5.01655	729	40.1332
(3, 15)	2, 11, 13, 4561	1	0.663897	9.53129	1262.67	76.2503

Table 1. Some illustrations to verify the pairs for the fields of odd characteristic.

4.2 Estimates for fields of even characteristic

For the fields of even characteristic we use the following lemma.

Lemma 4.6. *[2] For any odd positive integer n, $W(n) < 6.46n^{1/5}$, where W has the same meaning as mentioned above.*

Now we have the following Theorem.

Theorem 4.7. *Let $\mathbb{F}_{q^m}$ be a field of even characteristic and $m \geq 5$. Then there exists a primitive pair $(\alpha, f(\alpha))$ (where $f(x) = ax^2 + bx + c$, with $b^2 \neq 4ac$), with $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \beta$, for any prescribed $\beta \in \mathbb{F}_q$, unless (q, m) is one of the pairs* (2, 6), (2, 8), (2, 9), (2, 10), (2, 11), (2, 12), (4, 5), (4, 6), (4, 7), (4, 8), (8, 5), (8, 6), (8, 8), (16, 5) and (16, 6).

Proof. We will treat Mersenne primes differently. Here we will use the concept of radical of m i.e. m', where m' is such that $m = 2^k m'$ and $\gcd(2, m') = 1$.

Applying Lemma 4.6 on the inequality (3.2), we have the modified inequality as $q^{\frac{3m}{10}-1} > 84$.

We already have that the condition is satisfied, when $q \geq 16$ and $m \geq 29$. Now from the above modified inequality, we have the following conditions where the inequality is satisfied.

- When $q \geq 16$, condition holds for $m \geq 9$.
- When $q = 8$, condition holds for $m \geq 11$.
- When $q = 4$, condition holds for $m \geq 14$.
- When $q = 2$, condition holds for $m \geq 25$.

For the remaining pairs we calculate the exact ω and take $r = q^m - 1$, then all the pairs (q, m) satisfy the condition except the following (2, 6), (2, 8), (2, 9), (2, 10), (2, 11), (2, 12),(2, 14), (2,

(q,m)	prime factors of q^m-1	$\omega(d)$	Δ	Λ	$q^{\frac{m}{2}-1}$	$2\times W(r)^2\times\Lambda$
(2, 14)	3, 43, 127	1	0.93744	5.19918	64	41.5934
(2 ,15)	7, 31, 151	1	0.922239	5.25295	90.5097	42.0236
(2, 16)	3, 15, 17, 257	1	0.474571	12.5358	128	100.286
(2, 18)	3, 7, 19, 73	1	0.581625	10.5966	256	84.7728
(2, 20)	3, 5, 11, 31, 41	1	0.304885	24.9595	512	199.676
(2, 24)	3, 5, 7, 13, 17, 241	2	0.434494	18.1107	2048	579.542
(4, 9)	3, 7, 19, 73	1	0.581625	10.5966	128	84.7728
(4, 10)	3, 5, 11, 31, 41	1	0.304885	24.9595	256	199.676
(4, 12)	3, 5, 7, 13, 17, 241	2	0.434494	18.1107	1024	579.542
(8, 10)	3, 7, 11, 31, 151, 331	1	0.448664	22.0596	4096	176.477
(16, 7)	3, 5, 29, 43, 113, 127	1	0.451076	21.9523	1024	175.618
(32, 6)	3, 7, 11, 31, 151, 331	1	0.448664	22.0596	1024	176.477
(64, 5)	3, 7, 11, 31, 151, 331	1	0.448664	22.0596	512	176.477
(64, 6)	3, 5, 7, 11, 13, 19, 37, 73, 109	2	0.355376	32.9531	4096	1054.52
(128, 5)	31, 71, 127, 122921	1	0.956067	7.22976	1448.5	57.8381
(256, 5)	3, 5, 11, 17, 19, 31, 41, 61681	2	0.587206	17.3268	4096	554.458

Table 2. Some illustrations to verify the pairs for the fields of even characteristic.

15), (2, 16), (2, 18), (2, 20), (2, 24), (4, 5), (4, 6), (4, 7), (4, 8), (4, 9), (4, 10), (4, 12), (8, 5),(8, 6), (8, 8), (8, 10), (16, 5), (16, 6), (16, 7), (32, 6), (64, 5), (64, 6), (128, 5), (256, 5).

Then by using appropriate values of r in the modified prime sieving condition (3.2) as shown in Table 2, we have the following possible exceptional pairs : (2, 6), (2, 8), (2, 9), (2, 10), (2, 11), (2, 12), (4, 5), (4, 6), (4, 7), (4, 8), (8, 5), (8, 6), (8, 8), (16, 5), (16, 6).

This completes the proof.

□

Table 2 illustrates some of the calculations to show the pairs (q,m) satisfying the condition $q^{\frac{m}{2}-1}>2\times W(r)^2\times\Lambda$.

For Mersenne primes i.e., primes of the form 2^n-1, we have the following theorem.

Theorem 4.8. *If 2^m-1 is a Mersenne prime such that $2^m-1>13$, then the pairs $(2,m)\in\mathfrak{T}$.*

Proof. If 2^m-1 is a Mersenne prime i.e. $m=3,5,7,13,17,19$ etc., then every $\alpha\in\mathbb{F}_{2^m}^*$ is a primitive element other than 1. Also if $\alpha\in\mathbb{F}_{2^m}^*$, then degree of the minimal polynomial of α over $\mathbb{F}_2$ is greater than 3. Hence $a\alpha^2+b\alpha+c\neq 0,1$. Thus $a\alpha^2+b\alpha+c$ is also primitive. Moreover the trace map $Tr_{\mathbb{F}_{2^m}}$ is onto and inverse image of every element in $\mathbb{F}_2$ contains 2^m-1 elements in $\mathbb{F}_{2^m}$ and atleast three of them are primitive, hence the result.

□

5 Estimation with programming

Proposition 5.1. *Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_{q^m}$ be the extension field of degree m. For $m\geq 5$ there always exists a primitive pair $(\alpha,f(\alpha))$ and $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)=\beta$, for any prescribed $\beta\in\mathbb{F}_q$, where $f(x)=ax^2+bx+c\in\mathbb{F}_{q^m}[x]$ such that $b^2-4ac\neq 0$; with the only exceptional pair (q,m) which is $(2,6)$.*

We examine the exceptional pairs of the above theorems by using the following algorithm and try to establish the exact exceptional pair (2, 6). We have the field $\mathbb{F}_{2^6}\cong\frac{\mathbb{Z}_2[x]}{<y(x)>}$, where $y(x)=x^6+x^4+x^3+x+1$. For this field the quadratic polynomial is $f(x)=\alpha x^2+(\alpha^5+\alpha^4+\alpha+1)$.

For the remaining pairs we give the following proposition.

Proposition 5.2. *For the fields $\mathbb{F}_{q^m}$, where $m=3,4$, by sufficient amount of calculation using the algorithm, we have the pairs (3, 3), (5, 3), (6, 3), (3, 4) as the only possible exceptional pairs.*

Among the pairs (3, 3) is an exceptional pair, where $\mathbb{F}_{3^3} \cong \frac{\mathbb{Z}_3[x]}{<x^3+2x+1>}$ *and the quadratic polynomial is* $f(x) = \alpha x^2 + (\alpha+1)x + (2\alpha^2+2)$ *(*α *is a primitive root of* $\mathbb{F}_{3^3}$*).*

5.1 Algorithm for the programming

We propose the following algorithm to do the computations in SAGEMATH.

Algorithm *Check if* (q, m) *is exceptional pair or not*

```
Input : F_{q^m}  =  GF(q, m)
def is_primitive (b, q, m, F_{q^m}) :
    if b == 0 :
        return false
    if multiplicative_order(b) == q^m − 1 :
        return true
        else next b
def prescribed_trace (b, n, m, F_{q^m}) :
    Tr(b) = Sum([b ∧ (q ∧ i) for i in [0 . . . m − 1]])
    T = store Tr(b) for all b ∈ F_{q^m}
    if T = GF(q, 1)
        return true and proceed
    else next b
def check_coeffs (coefs, q, m, F_{q^m}, alpha) :
    a = coefs[0]
    b = coefs[1]
    c = coefs[2]
    if b ∧ 2 == 4 ∗ a ∗ c :
        return true
    for i in xrange (1, q ∧ m) :
        if gcd(i, q ∧ m − 1) == 1
        if is_primitive (a ∗ alpha ∧ (2 ∗ i) + b ∗ alpha ∧ i + c, q, m, F_{q^m}) :
        reuturn true
def check_pair (q, m) :
F_{q^m}. < alpha > = GF(q ∧ m, modulus = "primitive") :
    print "The Modulus is", F_{q^m}.modulus() :
    for C1 in xrange(1, q ∧ m) :
        for C2 in xrange(0, q ∧ m) :
        for C3 in xrange(0, q ∧ m) :
        coefs = [list(F_{q^m})[C1], list(F_{q^m})[C2], list(F_{q^m})[C3]]
        if check_coefs (coefs, q, m, F_{q^m}, alpha) == false
        print coefs
        return false
```

6 Conclusion remarks

The main objective of this paper is to determine the possible exceptional pairs of the given special form to determine exact exceptional pairs. Also, some new codes was algorithm was introduced to find the primitive normal elements in quadratic form with prescribed trace. Therefore, the outcomes of this research exhibit variability, significance, making it both compelling and conducive to further exploration in future studies.

References

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

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

[3] *T. Garefalakis, and G. Kapetanakis,* On the existence of primitive completely normal bases of finite fields, *J. Pure Appl. Algebra,* **223(3)**, *909–921, (2018).*

[4] *D. Wan,* Generators and irreducible polynomials over finite fields, *Math. Comput.,* **66(219)**, *1195–1212, (1997).*

[5] *L. Fu, and D. Q. Wan,* A class of incomplte character sums, *Q. J. Math.,* **65(4)**, *1195–1211, (2014).*

[6] *S. D. Cohen, and S. Huczynska,* The primitive normal basis theorem– without a computer, *J. Lond. Math. Soc. (2).,* **67(1)**, *41–56, (2003).*

[7] *S. D. Cohen, and S. Huczynska,* The strong primitive normal basis theorem, *Acta Arith.,* **143(4)**, *299–332, (2010).*

[8] *G. L. Mullen, and D. Panario,* Handbook of Finite Fields, *CRC Press, Boca Raton, (2013).*

[9] *L. Carlitz, and S. Uchiyama,* Bounds for exponential sums, *Duke Math. J.,***24**, *37–41, (1957).*

[10] *F. N. Castro, and C. J. Moreno,* Mixed exponential sums over finite fields, *Proc. Amer. Math. Soc.,* **128(9)**, *2529–2537, (2000).*

[11] *T. Cochrane, and C. Pinner,* Using Stepanov's method for exponential sums involving rational functions, *J. Number Theory.,* **116(2)**, *270–292, (2006).*

[12] *Kolo F. Soro, Eric D. Akeke and Konan M. Kouakou* A*n application of young tableaux to cryptography, Palest. J. Math.,***12(2)**, *524–529, (2023).*

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

[14] *A. Weil,* On some exponential sums, *Proc. Natl. Acad. Sci. U.S.A.,* **34**, *204–207, (1948).*

[15] *L. Carlitz,* Primitive roots in a finite fields, *Trans. Amer. Math. Soc.,* **73(3)**, *314–318, (1952).*

[16] *L. Carlitz,* Some problems involving primitive roots in a finite filed, *Proc. Natl. Acad. Sci. U.S.A.,* **38(4)**, *314–318, (1952).*

[17] *B. Huppert,* Charater theory of finite fields, *Walter de Gruyter, Berlin, New York , (1998).*

Author information

Himangshu Hazarika, Department of Mathematics, Tezpur College, India.
E-mail: himangshuhazarika10@gmail.com

Dhiren Kumar Basnet, Department of Mathematical Sciences, Tezpur University, India.
E-mail: dbasnet@tezu.ernet.in

Received: 2023-12-22
Accepted: 2024-05-05