ON THE EXISTENCE OF PRIMITIVE NORMAL ELEMENTS OF RATIONAL FORM OVER FINITE FIELDS OF EVEN CHARACTERISTIC

HIMANGSHU HAZARIKA, DHIREN KUMAR BASNET, AND GIORGOS KAPETANAKIS

Abstract. Let q be an even prime power and $m \geq 2$ an integer. By $\mathbb{F}_q$, we denote the finite field of order q and by $\mathbb{F}_{q^m}$ its extension degree m. In this paper we investigate the existence of a primitive normal pair $(\alpha, f(\alpha))$, with $f(x) = \dfrac{ax^2+bx+c}{dx+e} \in \mathbb{F}_{q^m}(x)$, where the rank of the matrix $F = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_{q^m})$ is 2. Namely, we establish sufficient conditions to show that nearly all fields of even characteristic possess such elements, except for $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ if $q = 2$ and m is odd, and then we provide an explicit list of possible and genuine exceptional pairs (q, m).

1. Introduction

Given an even prime power q and an integer $m \geq 2$, we denote by $\mathbb{F}_q$, the finite field of order q and by $\mathbb{F}_{q^m}$ its extension field of degree m. A generator of the (cyclic) multiplicative group $\mathbb{F}_{q^m}^*$ is called *primitive*. It is well-known that, for any finite field $\mathbb{F}_q$, there are $\phi(q-1)$ primitive elements, where ϕ is Euler's phi-function. Further, an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$ of the form $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\}$ is called a *normal basis* and α is called *normal* or *free*.

The readers are referred to [12] and the references therein for the existence of both primitive and free elements. The simultaneous occurrence of primitive and free elements in $\mathbb{F}_{q^m}$ is given by the following theorems.

Theorem 1.1 (Primitive normal basis theorem, [5]). *For any prime power q and positive integer m, the finite field $\mathbb{F}_{q^m}$ contains some element which is simultaneously primitive and free.*

At first, this result was proved by Lenstra and Schoof in [11]. Later on, by implementing a sieving technique that was initially introduced by Cohen [16], Cohen and Huczynska [5] provided a computer-free proof.

Theorem 1.2 (Strong primitive normal basis theorem [6]). *In $\mathbb{F}_{q^m}$, there exists some element α such that both α and α^{-1} are primitive and free, unless (q, m) is $(2, 3), (2, 4), (3, 4), (4, 3)$ or $(5, 4)$.*

2010 *Mathematics Subject Classification.* 12E20, 11T23.

Key words and phrases. Finite field, Primitive element, Normal element, Normal basis, Character.

This work was funded by the Council of Scientific and Industrial Research, New Delhi, Government of India's research grant no. 09/796(0099)/2019-EMR-I.

Tian and Qi were the first to provide this result in [13], for $m \geq 32$. Later on Cohen and Huczynska [6] completed the proof up to the above form, again by using their sieving technique.

The next theorems, which extend to rational functions, were given by Kapetanakis [9, 10] by employing the aforementioned sieving technique.

Theorem 1.3 ([9]). *For odd prime power $q \geq 23$, an integer $m \geq 17$ and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_q)$, with the condition that if A has exactly two non-zero entries and q is odd, then the quotient of these entries is a square in $\mathbb{F}_{q^m}$. Then there exists some $\alpha \in \mathbb{F}_{q^m}$ such that both α and $\frac{a\alpha+b}{c\alpha+d}$ are simultaneously primitive and normal.*

Theorem 1.4 ([10]). *Let q be a prime power, $n \geq 2$ an integer and some matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_q)$, where $M \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ if $q = 2$ and m is odd. There exists some primitive $\alpha \in \mathbb{F}_{q^m}$ such that α and $\frac{a\alpha+b}{c\alpha+d}$ are both simultaneously normal elements of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.*

The existence of a primitive element $\alpha \in \mathbb{F}_q$ such that $f(\alpha)$ is also primitive for an arbitrary quadratic in $\mathbb{F}_q[x]$ has been completely resolved in [2].

Theorem 1.5 ([2]). *For all $q > 211$, there always exists an element $\alpha \in \mathbb{F}_{q^m}$ such that α and $f(\alpha)$ are both primitive, where $f(x) = ax^2 + bx + c$ with $b^2 - 4ac \neq 0$.*

In this paper, we extend of Theorem 1.3. We solve the existence question for elements α of $\mathbb{F}_{q^m}$ that both α and $f(\alpha)$ are simultaneously primitive and normal over $\mathbb{F}_q$, where $f(x) = \frac{ax^2+bx+c}{dx+e} \in \mathbb{F}_{q^m}(x)$ such that the $F = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_{q^m})$ has rank 2. For $a = 0$, the results are already discussed in [12], hence throughout this paper we assume $a \neq 0$. We call the pair (q, m) a *primitive normal* pair if the field $\mathbb{F}_{q^m}$ contains such elements. In particular, we prove the following results, where m' is odd such that $m = 2^k m'$, $k \geq 0$.

Theorem 1.6. *For the finite field $\mathbb{F}_{q^m}$ of even characteristic, suppose m' is such that $m' | q-1$. Then there exists an element α in $\mathbb{F}_{q^m}$, such that both α and $f(\alpha)$ are simultaneously primitive normal in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, where $f(x) = \frac{ax^2+bx+c}{dx+e}$, with $a, b, c, d, e \in \mathbb{F}_{q^m}$, $a \neq 0$, and $dx + e \neq 0$ unless (q, m) is one of the pairs $(2, 2)$, $(2, 4)$, $(2, 8)$, $(2, 16)$, $(4, 2)$, $(4, 3)$, $(4, 4)$, $(4, 6)$, $(4, 8)$, $(4, 12)$, $(8, 2)$, $(8, 4)$, $(8, 7)$, $(8, 8)$, $(8, 14)$, $(16, 2)$, $(16, 3)$, $(16, 4)$, $(16, 5)$, $(16, 6)$, $(16, 15)$, $(32, 2)$, $(64, 2)$, $(64, 4)$, $(128, 2)$, $(256, 2)$, $(512, 2)$ or $(1024, 2)$.*

Theorem 1.7. *Let $\mathbb{F}_{q^m}$ be a finite field of even characteristic and $m' \nmid q - 1$. Then there exists an element α in $\mathbb{F}_{q^m}$, such that both α and $f(\alpha)$ are simultaneously primitive normal in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, where $f(x) = \frac{ax^2+bx+c}{dx+e}$, with $a, b, c, d, e \in \mathbb{F}_{q^m}$, $a \neq 0$, and $dx + e \neq 0$ unless (q, m) is one of the pairs $(2, 3)$, $(2, 5)$, $(2, 6)$, $(2, 7)$, $(2, 9)$, $(2, 10)$, $(2, 11)$, $(2, 12)$, $(2, 13)$, $(2, 14)$, $(2, 15)$, $(2, 18)$, $(2, 20)$, $(2, 21)$, $(2, 24)$, $(2, 30)$, $(4, 5)$, $(4, 7)$, $(4, 9)$, $(4, 10)$, $(8, 3)$, $(8, 5)$, $(8, 6)$ or $(32, 3)$.*

In addition, we employ explicit computational methods and show that the pairs $(2, 2)$, $(2, 3)$, $(2, 4)$, $(2, 5)$, $(2, 6)$, $(4, 2)$ and $(4, 6)$ appearing above are genuine exceptions, while,

based on computational evidence, we conjecture, that they are actually the only genuine exceptions, see Conjecture 6.1.

This work is heavily influenced by the the work of Lenstra and Schoof [11], while character sums plays a very crucial role. Further, we adjust the sieving technique, provided by Cohen and Huczynska [5, 6], in our setting.

In Section 3, we estimate a lower bound for existence of primitive normal pair. Then in Section 4, by using "the prime sieve technique", we weaken the sufficient condition for more efficient results. In Section 5, we apply the existence conditions on fields of even characteristic for each and every possible case and complete the proofs of Theorems 1.6 and 1.7. In Section 6, we employ computers to further investigate the actual situation with the pairs posing as possible exceptions on Theorems 1.6 and 1.7. We conclude this work with the statement of two related conjectures in Section 7.

2. Preliminaries

Under the rule $f \circ \alpha = \sum_{i=1}^{n} a_i \alpha^{q^i}$ and $f = \sum_{i=1}^{n} a_i x^i \in \mathbb{F}_q[x]$ for $\alpha \in \mathbb{F}_{q^m}$; the additive group of $\mathbb{F}_{q^m}$ is an $\mathbb{F}_q[x]$-module. The $\mathbb{F}_q$-order of $\alpha \in \mathbb{F}_{q^m}$, is the monic $\mathbb{F}_q$-divisor g of $x^m - 1$ of minimal degree such that $g \circ \alpha = 0$, which we define as *Order of* α and denote by $\mathrm{Ord}(\alpha)$. It is clear that the free elements of $\mathbb{F}_{q^m}$ are exactly those of Order $x^m - 1$.

The multiplicative order for $\alpha \in \mathbb{F}_{q^m}^*$ is denoted by $\mathrm{ord}(\alpha)$ and α is primitive if and only if $\mathrm{ord}(\alpha) = q^m - 1$. Furthermore, it follows from the definitions that $q^m - 1$ and $x^m - 1$ can be freely replaced by their radicals q_0 and $f_0 := x^{m_0} - 1$ respectively, where m_0 is such that $m = m_0 p^a$, where a is a non negative integer and $\gcd(m_0, p) = 1$.

Throughout this section we present a couple of functions that characterize primitive and free elements. To represent those functions, the idea of character of finite abelain group is necessary.

Definition 2.1. Let G be a finite abelian group. A character χ of G is a group homomorphism from G into 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, that is denoted by $\widehat{G}$ and is isomorphic to G. The character χ_0 defined as $\chi_0(a) = 1$ for all $a \in G$ is called the *trivial character* of G.

In a finite field $\mathbb{F}_{q^m}$, the additive group $\mathbb{F}_{q^m}$ and the multiplicative group $\mathbb{F}_{q^m}^*$ are abelian groups. Throughout this paper we call the characters of the additive group $\mathbb{F}_{q^m}$ *additive characters* and the characters of $\mathbb{F}_{q^m}^*$ *multiplicative characters*. Multiplicative characters are extended from $\mathbb{F}_{q^m}^*$ to $\mathbb{F}_{q^m}$ by the rule $\chi(0) = \begin{cases} 0, & \text{if } \chi \neq \chi_0, \\ 1, & \text{if } \chi = \chi_0. \end{cases}$ Furter, since $\widehat{\mathbb{F}_{q^m}^*} \cong \mathbb{F}_{q^m}^*$, $\widehat{\mathbb{F}_{q^m}^*}$ is cyclic and for any divisor d of $q^m - 1$ there are exactly $\phi(d)$ characters of order d in $\widehat{\mathbb{F}_{q^m}^*}$.

Let $e | q^m - 1$, then $\alpha \in \mathbb{F}_{q^m}$ is called *e-free* if $d|e$ and $\alpha = \beta^d$, for some $\beta \in \mathbb{F}_{q^m}$ implies $d = 1$. Furthermore α is primitive if and only if $\alpha = \beta^d$, for some $\beta \in \mathbb{F}_{q^m}$ and $d | q^m - 1$ implies $d = 1$.

For any $e|q^m-1$, following Cohen and Huczynska [5, 6], we express the characteristic function for the subset of e-free elements of $\mathbb{F}_{q^m}^*$ 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 is the Möbius function and χ_d stands for any multiplicative character of order d. For any $e|q^m-1$, we use "integral" notation due to Cohen and Huczynska [5, 6], for weighted sums as follows

$$\int_{d|q^m-1}\chi_d := \sum_{d|q^m-1}\frac{\mu(d)}{\phi(d)}\sum_{\chi_d}\chi_d.$$

Then the characteristic function for the subset of e-free elements of $\mathbb{F}_{q^m}^*$ becomes,

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

Again, for any monic $\mathbb{F}_q$-divisor g of x^m-1, a typical additive character ψ_g of $\mathbb{F}_q$-*order* g is one such that $\psi_g \circ g$ is the trivial character of $\mathbb{F}_{q^m}$ and g is of minimal degree satisfying this property. 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 function over $\mathbb{F}_q[x]$.

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

$$\kappa_g : \alpha \mapsto \Theta(g)\sum_{f|g}(\frac{\mu'(f)}{\Phi(f)}\sum_{\psi_f}\psi_f(\alpha)),$$

where $\Theta(g) := \frac{\Phi(g)}{q^{deg(g)}}$, the sum runs over all additive characters ψ_f of $\mathbb{F}_q$-order g and μ' is the analogue of the Möbius function which is 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

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

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

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

>From [13], we have the following about the typical additive character. Let λ be the canonical additive character of $\mathbb{F}_q$. Thus for $\alpha \in \mathbb{F}_q$ this character is defined as $\lambda(\alpha) = \exp^{2\pi i Tr(\alpha)/p}$, where $Tr(\alpha)$ is the absolute trace of α over $\mathbb{F}_p$.

Now let ψ_0 be the canonical additive character of $\mathbb{F}_{q^m}$, which is simply the lift of λ to $\mathbb{F}_{q^m}$, i.e., $\psi_0(\alpha) = \lambda(Tr(\alpha))$, $\alpha \in \mathbb{F}_{q^m}$. Now for any $\delta \in \mathbb{F}_{q^m}$, let ψ_δ be the character defined

by $\psi_\delta(\alpha) = \psi_0(\delta\alpha)$, $\alpha \in \mathbb{F}_{q^m}$. Define the subset Δ_g of $\mathbb{F}_{q^m}$ as the set of δ for which ψ_δ has $\mathbb{F}_q$-order g. So we may also write ψ_{δ_g} for ψ_δ, where $\delta_g \in \Delta_g$. So with the help of this we can express any typical additive character ψ_g in terms of ψ_{δ_g} and further we can express this in terms of canonical additive character ψ_0.

In the following sections we will encounter various character sums and a calculation, or at least an estimation, for them will be necessary. The following lemmas are well-established and provide such results.

Lemma 2.1 ([12], Theorem 5.4 - Orthogonality relations)**.** *For any nontrivial character χ of a finite abelian group G and any nontrivial element $\alpha \in G$, the following hold:*

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

.

Lemma 2.2 ([14], Corollary 2.3)**.** *Take two nontrivial multiplicative characters χ_1, χ_2 of $\mathbb{F}_{q^m}$. Let $f_1(x)$ and $f_2(x)$ be two monic co-prime polynomials in $\mathbb{F}_{q^m}[x]$, such that none of $f_i(x)$ is of the form $g(x)^{ord(\chi_i)}$ for $i = 1, 2$; where $g(x) \in \mathbb{F}_{q^m}[x]$ with degree at least 1. Then*

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

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

Lemma 2.3 ([7], Theorem 5.6)**.** *Let χ and ψ be two non-trivial multiplicative and additive characters of the field $\mathbb{F}_{q^m}$ respectively. Let $\mathfrak{F}, \mathfrak{G}$ be rational functions in $\mathbb{F}_{q^m}(x)$, where $\mathfrak{F} \neq \beta\mathfrak{H}^n$ and $\mathfrak{G} \neq \mathfrak{H}^p - \mathfrak{H} + \beta$, for any $\mathfrak{H} \in \mathbb{F}_{q^m}(x)$ and any $\beta \in \mathbb{F}_{q^m}$, and n is the order of χ. Then*

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

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

Lemma 2.4 ([7])**.** *Let $f_1(x)$, $f_2(x)$, ..., $f_s(x) \in \mathbb{F}_{q^m}[x]$ be distinct irreducible polynomials. Let χ_1, χ_2, ..., χ_s be multiplicative characters and ψ be a non trivial additive character of $\mathbb{F}_{q^m}$, then*

$$\left| \sum_{y \in \mathbb{F}_{q^m} f_t(y) \neq 0} \chi_1(f_1(y))\chi_2(f_2(y)) \dots \chi_s(f_s(y))\psi(y) \right| \leq kq^{m/2},$$

where $k = \sum_{i=1}^{s} deg(f_i)$.

Definition 2.2. For a non-trivial additive character ψ of the finite field $\mathbb{F}_{q^m}$, the sum

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

where $a, b \in \mathbb{F}_{q^m}$ is called a *Kloosterman sum.*

Lemma 2.5 ([3], Theorem 5.45)**.** *If the finite field $\mathbb{F}_{q^m}$ has a non-trivial additive character ψ and $a, b \in \mathbb{F}_{q^m}$ are not both zero, then the Kloosterman sum satisfies*

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

3. A lower bound for $\mathfrak{M}(e_1, e_2, g_1, g_2)$

In this section, we try to estimate the number of the elements $\alpha \in \mathbb{F}_{q^m}$ such that both α and $f(\alpha)$ are simultaneously primitive normal elements in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. We consider q an even prime power, i.e. $q = 2^k$, where k is a positive integer. Take e_1, e_2 such that $e_1, e_2 | q^m - 1$ and g_1, g_2 such that $g_1, g_2 | x^m - 1$. Let $\mathfrak{M}(e_1, e_2, g_1, g_2)$ be the number of $\alpha \in \mathbb{F}_{q^m}$, such that α is both e_1-free and g_1-free and $f(\alpha)$ is e_2-free, g_2-free; where $f(x) = \dfrac{ax^2 + bx + c}{dx + e}$ and the matrix $M = \begin{pmatrix} a & b, & c \\ 0 & d & e \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_{q^m})$ is of rank 2. In particular, for our purposes, it suffices to prove that $\mathfrak{M}(e_1, e_2, g_1, g_2) > 0$.

For convenience, we use the notations $\omega(n)$ and g_d to denote number of prime divisors of n and the number of monic irreducible factors of g over $\mathbb{F}_q$ respectively. Furthermore, we write $W(n) := 2^{\omega(n)}$ and $\Omega(g) := 2^{g_d}$.

Theorem 3.1. *Let $f(x) = \dfrac{ax^2 + bx + c}{dx + e} \in \mathbb{F}_{q^m}(x)$ such that the matrix $M = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix}$ $\in M_{2\times 3}(\mathbb{F}_{q^m})$ is of rank 2 and $f(x) \neq yx$, yx^2 for any $y \in \mathbb{F}_{q^m}$. Suppose e_1, e_2 divide $q^m - 1$ and g_1, g_2 divide $x^m - 1$. If $M \neq \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ when $q = 2$, m is odd and*

$$q^{\frac{m}{2}} > 4W(e_1)W(e_2)\Omega(g_1)\Omega(g_2), \tag{3.1}$$

then $\mathfrak{M}(e_1, e_2, g_1, g_2) > 0$.

In particular, if

$$q^{m/2} > 4W(q^m - 1)^2\Omega(x^m - 1)^2, \tag{3.2}$$

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

Proof. First we establish the result for $d \neq 0$. >From the definition we have,

$$\mathfrak{M}(e_1, e_2, g_1, g_2) = \theta(e_1)\theta(e_2)\Theta(g_1)\Theta(g_2) \sum_{\substack{d_1|e_1 \\ d_2|e_2}} \sum_{\substack{h_1|g_1 \\ h_2|g_2}} S(\chi_{d_1}, \chi_{d_2}, \psi_{h_1}, \psi_{h_2}), \tag{3.3}$$

where

$$S(\chi_{d_1}, \chi_{d_2}, \psi_{h_1}, \psi_{h_2}) = \sum_{\alpha \in \mathbb{F}_{q^m}} \chi_{d_1}(\alpha)\chi_{d_2}(f(\alpha))\psi_{h_1}(\alpha)\psi_{h_2}(f(\alpha))$$

As there exists some l_1, $l_2 \in \{0, 1, \ldots, q^m - 2\}$, such that $\chi_{l_i}(\alpha) = \chi_{q^m-1}(\alpha^{l_i})$, for $i = 1, 2$ and $\psi_{h_i}(\alpha) = \psi_{x^m-1}(\beta_i\alpha)$, for some $\beta_i \in \mathbb{F}_{q^m}$ for $i = 1, 2$, we have the following expression:

$$\begin{aligned} S(\chi_{d_1}, \chi_{d_2}, \psi_{h_1}, \psi_{h_2}) &= \sum_{\alpha\in\mathbb{F}_{q^m}} \chi_{q^m-1}(\alpha^{l_1} (f(\alpha))^{l_2})\psi_{x^m-1}((\beta_1\alpha) + \beta_2 f(\alpha)) \\ &= \sum_{\alpha\in\mathbb{F}_{q^m}} \chi_{q^m-1}(\mathfrak{F}(\alpha))\psi_{x^m-1}(\mathfrak{G}(\alpha)), \end{aligned}$$

where $\mathfrak{F}(x) = x^{l_1}(\frac{ax^2+bx+c}{dx+e})^{l_2}$ and $\mathfrak{G}(x) = \beta_1 x + \beta_2(\frac{ax^2+bx+c}{dx+e})$, for some l_1, $l_2 \in \{0, 1, \ldots, q^m - 2\}$ and β_1, $\beta_2 \in \mathbb{F}_{q^m}$.

If $\mathfrak{F} \neq \beta\mathfrak{H}^{q^m-1}$ and $\mathfrak{G} \neq \mathfrak{H}^p - \mathfrak{H} + \beta$, for any $\mathfrak{H} \in \mathbb{F}_{q^m}(x)$ and $\beta \in \mathbb{F}_{q^m}$, then Lemma 2.3 implies

$$|S(\chi_{d_1}, \chi_{d_2}, \psi_{h_1}, \psi_{h_2})| \leq 4q^{m/2}, \tag{3.4}$$

unless all the four characters are trivial.

Now we consider the case $\mathfrak{F} = \beta\mathfrak{H}^{q^m-1}$, for some $\mathfrak{H} \in \mathbb{F}_{q^m}(x)$ and $\beta \in \mathbb{F}_{q^m}$. Then $\mathfrak{H} = \frac{\mathfrak{H}_1}{\mathfrak{H}_2}$, for some $\mathfrak{H}_1$, $\mathfrak{H}_2$ coprime polynomials over $\mathbb{F}_{q^m}$. It follows that $x^{l_1}(ax^2 + bx + c)^{l_2}\mathfrak{H}_2^{q^m-1} = \beta(dx + e)^{l_2}\mathfrak{H}_1^{q^m-1}$, and this implies $\mathfrak{H}_2^{q^m-1}|(dx + e)^{l_2}$, hence $\mathfrak{H}_2$ is constant. Then comparing the degrees of both sides we have $l_1 + 2l_2 = l_2 + k_1(q^m - 1)$, where k_1 is the degree of $\mathfrak{H}_1$ and this gives $l_1 = 0$ or 1 i.e. $\mathfrak{H}_1(x) = a'x + b'$. When $k_1 = 1$ then l_1 must be non-zero, otherwise $l_2 = q^m - 1$, a contradiction. Now,

$$(ax^2 + bx + c)^{l_2} = \beta(dx + e)^{l_2}\mathfrak{B}^{q^m-1}x^{q^m-1-l_1}, \tag{3.5}$$

where $\mathfrak{B}(x) = \mathfrak{H}_1(x)/x \in \mathbb{F}_q[x]$, a constant polynomial. Comparing both sides we have $c = 0$. After putting this in the equation, this is possible only if $\gcd(dx + e, ax + b) = x + \frac{c}{d}$ and $q^m - 1 = l_1 + l_2$. In this case $f(x) = \frac{a}{d}x$, which is a contradiction. Hence $k_1 = 0$ and $l_1 = l_2 = 0$.

Next, let $\beta_1 = 0$ and $\beta_2 \neq 0$. Then,

$$\begin{aligned} |S(\chi_{d_1}, \chi_{d_2}, \psi_{h_1}, \psi_{h_2})| &= \left|\sum_{\alpha\neq-\frac{e}{d}} \psi_{x^m-1}\left(\frac{\beta_2(a\alpha^2 + b\alpha + c)}{d\alpha + e}\right)\right| \\ &= \left|\sum_{y\neq0} \psi_{x^m-1}\left(\frac{\beta_2}{d^2}ay + \left(\frac{\beta_2}{d^2}\right)(e^2 - de + cd^2)y^{-1}\right)\right|. \end{aligned}$$

By Lemma 2.5, we have

$$|S(\chi_{d_1}, \chi_{d_2}, \psi_{h_1}, \psi_{h_2})| \leq 2q^{m/2} < 4q^{m/2}.$$

Similarly, if $\beta_1 \neq 0$ and $\beta_2 = 0$, by applying Lemma 2.1, we have

$$|S(\chi_{d_1}, \chi_{d_2}, \psi_{h_1}, \psi_{h_2})| = \left|\sum_{\alpha\in\mathbb{F}_{q^m}} \psi_{x^m-1}(\beta_1\alpha)\right| \leq 1 < 4q^{m/2}.$$

If both β_1 and β_2 are non-zero, then we can proceed as follows:

$$\begin{aligned}|S(\chi_{d_1},\,\chi_{d_2},\psi_{h_1},\psi_{h_2})| &= \left|\sum_{\alpha\neq-\frac{e}{d}}\psi_{q^m-1}\left(\beta_1\alpha\,+\,\frac{\beta_2(a\alpha^2+b\alpha+c)}{d\alpha+e}\right)\right| \\ &= \left|\sum_{y\neq 0}\psi_{q^m-1}\left(\left(\frac{\beta_1}{d}+\frac{\beta_2 a}{d^2}\right)y\,+\,\left(\frac{\beta_2 ae^2}{d^2}-\frac{be}{d}+c\right)y^{-1}+\left(\frac{\beta_2 b}{d}-\frac{\beta_1 e}{d}\right)\right)\right| \\ &= \left|\sum_{y\neq 0}\psi_{q^m-1}\left(\left(\frac{\beta_1}{d}+\frac{\beta_2 a}{d^2}\right)y\,+\,\left(\frac{\beta_2 ae^2}{d^2}-\frac{be}{d}+c\right)y^{-1}\right)\right|\end{aligned}$$

Lemma 2.5 yields

$$|S(\chi_{d_1},\,\chi_{d_2},\psi_{h_1},\psi_{h_2})| \leq 2q^{m/2}\,<\,4q^{m/2}.$$

If $\mathfrak{G}=\mathfrak{H}^p-\mathfrak{H}+\beta$ for some $\mathfrak{H}\in\mathbb{F}_{q^m}(x)$ and for some $\beta\in\mathbb{F}_{q^m}$, then we write $\mathfrak{H}=\frac{H_1}{H_2}$, where H_1 and H_2 are co-prime polynomials. Continuing this, we have the following.

$$\frac{\beta_1 x(dx+e)+\beta_2(ax^2+bx+c)}{dx+e}=\frac{H_1^p-H_1H_2^{p-1}+\beta H_2^p}{H_2^p}.$$

Immediately from the restriction on the rational polynomial $\frac{ax^2+bx+c}{dx+e}$ we get $(dx+e)$ is co-prime to $\beta_1 x(dx+e)+\beta_2(ax^2+bx+c)$ and hence H_2^p is co-prime to $H_1^p-H_1H_2^{p-1}+\beta H_2^p$. Then $dx+e=H_2^p$, which is a contradiction as $d\neq 0$. It follows that $\mathfrak{G}=0$, i.e. $\beta_1=\beta_2=0$.

Additionally if at least one of l_1, l_2 is non-zero, then $x^{l_1}(ax^2+bx+c)^{l_2}(dx+e)^{q^m-1-l_2}$ has at most 4 distinct roots and is not of the form $\beta\mathfrak{H}^{q^m-1}$, for $\mathfrak{H}\in\mathbb{F}_{q^m}(x)$ and $\beta\in\mathbb{F}_{q^m}$. Then from Equation (3.5) we have

$$S(\chi_{d_1},\chi_{d_2},\psi_{h_1},\psi_{h_2})=\sum_{\alpha\neq-\frac{e}{d}}\chi_{q^m-1}\left(\alpha^{l_1}(a\alpha^2+b\alpha+c)^{l_2}(dx+e)^{q^m-1-l_2}\right).$$

>From Lemma 2.5 we have the bound $|S(\chi_{d_1},\chi_{d_2},\psi_{h_1},\psi_{h_2})|\leq 2q^{m/2}<4q^{m/2}$.

In all of the above cases, Equation (3.3) gives $\mathfrak{M}(e_1,e_2,g_1,g_2)>0$ if

$$q^m>1+4q^{m/2}\left(W(e_1)W(e_2)\Omega(g_1)\Omega(g_2)-1\right),$$

hence a sufficient condition is (3.1). This concludes the $d\neq 0$ case.

Next, we deal with the case $d=0$. Then $f(x)=\frac{ax^2+bx+c}{e}=\frac{a}{e}x^2+\frac{b}{e}x+\frac{c}{e}=a_1x^2+b_1+c_1$ and

$$\mathfrak{M}(e_1,e_2,g_1,g_2)=\theta(e_1)\theta(e_2)\Theta(g_1)\Theta(g_2)\int\limits_{\substack{d_1|e_1h_1|g_1\\ d_2|e_2\,h_2|g_2}}\int S(\chi_{d_1},\chi_{d_2},\psi_{h_1},\psi_{h_2}). \tag{3.6}$$

Where

$$\begin{aligned} S(\chi_{d_1}, \chi_{d_2}, \psi_{h_1}, \psi_{h_2}) &= \sum_{\alpha \in \mathbb{F}_{q^m}} \chi_{d_1}(\alpha)\chi_{d_2}(f(\alpha))\psi_{h_1}(\alpha)\psi_{h_2}(f(\alpha)) \\ &= \sum_{\alpha \in \mathbb{F}_{q^m}} \chi_{d_1}(\alpha)\chi_{d_2}(f(\alpha))\psi_{h_1}(\alpha)\psi'_{h_2}(\alpha) \\ &= \sum_{\alpha \in \mathbb{F}_{q^m}} \chi_{d_1}(\alpha)\chi_{d_2}(f(\alpha))(\psi_{h_1}\psi'_{h_2})(\alpha), \end{aligned}$$

and $\psi'_{h_2}(x) = \psi_{h_2}(f(x))$ for all $x \in \mathbb{F}_{q^m}$.

Now, if $(\chi_{d_1}, \chi_{d_2}, (\psi_{h_1}\psi'_{h_2}) = \psi_h) \neq (\chi_0, \chi_0, \psi_0)$, then we consider following cases.

- If $\psi_{h_1}\psi'_{h_2} = \psi_h$ is non trivial character, then applying Lemma 2.4 we have
$$|S(\chi_{d_1}, \chi_{d_2}, \psi_{h_1}, \psi_{h_2})| = |S(\chi_{d_1}, \chi_{d_2}, \psi_h)| \leq 3q^{m/2} < 4q^{m/2}.$$
- If $\psi_{h_1}\psi'_{h_2} = \psi_h$ is the trivial character ψ_0, then following Lemma 2.3, we have
$$|S(\chi_{d_1}, \chi_{d_2}, \psi_{h_1}, \psi_{h_2})| = |S(\chi_{d_1}, \chi_{d_2}, \psi_0)| \leq 2q^{m/2} < 4q^{m/2}.$$
- Finally, if $\chi_{d_1} = \chi_{d_2} = \chi_0$ then $|S(\chi_{d_1}, \chi_{d_2}, \psi_{h_1}, \psi_{h_2})| = |S(\chi_0, \chi_0, \psi_h)| = 0$.

Hence $|S(\chi_{d_1}, \chi_{d_2}, \psi_{h_1}, \psi_{h_2})| < 4q^{m/2}$ if $(\chi_{d_1}, \chi_{d_2}, \psi_h) \neq (\chi_0, \chi_0, \psi_0)$, where $\psi_h = \psi_{h_1}\psi'_{h_2}$. Then, from Equation (3.6) we have that a sufficient condition for $\mathfrak{M}(e_1, e_2, g_1, g_2) > 0$ is given by (3.1).

In particular setting $e_1 = e_2 = q^m - 1$ and $g_1 = g_2 = x^m - 1$, we obtain the sufficient condition (3.2).

Finally, we briefly consider the case $c_1 = 0$ i.e. $c = 0$. Then $f(x) = a_1x^2 + b_1x = x(a_1x + b_1)$, where $a_1, b_1 \in \mathbb{F}_{q^m}$ with $b_1 \neq 0$. This time we have

$$\mathfrak{M}(e_1, e_2, g_1, g_2) = \theta(e_1)\theta(e_2)\Theta(g_1)\Theta(g_2) \int\limits_{\substack{d_1|e_1 \\ d_2|e_2}} \int\limits_{\substack{h_2|g_2 \\ h_1|g_1}} S(\chi_{d_1}, \chi_{d_2}, \psi_{h_1}, \psi_{h_2}),$$

where

$$S(\chi_{d_1}, \chi_{d_2}, \psi_{h_1}, \psi_{h_2}) = \sum_{\alpha \in \mathbb{F}_{q^m}} \chi_{d_1}(\alpha)\chi_{d_2}(\alpha(a_1\alpha + b_1))\psi_h(\alpha) = \sum_{\alpha \in \mathbb{F}_{q^m}} \chi_{d_3}(\alpha)\chi_{d_2}(a_1\alpha + b_1)\psi_h(\alpha).$$

with $\chi_{d_3} = \chi_{d_1}\chi_{d_2}$. Now, from Lemma 2.4.

$$|S(\chi_{d_1}, \chi_{d_2}, \psi_{h_1}, \psi_{h_2})| = \left| \sum_{\alpha \in \mathbb{F}_{q^m}} \chi_{d_3}(\alpha)\chi_{d_2}(a_1\alpha + b_1)\psi_h(\alpha) \right| \leq 2q^{m/2} < 4q^{m/2}$$

and the conditions (3.1) and (3.2) follow as before. □

Note: If $q = 2$ and m is odd then for the matrix $M = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, the elements α and $f(\alpha)$ are not simultaneously normal. Again, for m odd this case is trivially true. Hence we exclude this matrix from our claim.

In the next section, we apply the results on primes dividing $q^m - 1$ and irreducible polynomials dividing $x^m - 1$ for enhanced results. As already mentioned, this technique was first introduced by Cohen and Huczynska in [5, 6].

4. The prime sieve technique

We begin this section with the sieving inequality, as established by Kapetanakis in [10], which we adjust properly.

Lemma 4.1 (Sieving Inequality)**.** *Let d be a divisor of q^m-1 and $p_1,p_2,\ldots,p_n$ be the remaining distinct primes dividing q^m-1. Furthermore, let g be a divisor of x^m-1 such that $g_1,g_2,\ldots,g_k$ are the remaining distinct irreducible factors of x^m-1. Abbreviate $\mathfrak{M}(q^m-1,q^m-1,x^m-1,x^m-1)$ to $\mathfrak{M}$. Then*

$$\mathfrak{M}\geq\sum_{i=1}^{n}\mathfrak{M}(p_id,d,g,g)+\sum_{i=1}^{n}\mathfrak{M}(d,p_id,g,g)+\sum_{i=1}^{k}\mathfrak{M}(d,d,g_ig,g)+\sum_{i=1}^{k}\mathfrak{M}(d,d,g,g_ig)-(2n+2k-1)\mathfrak{M}(d,d,g,g). \tag{4.1}$$

Theorem 4.2. *With the assumptions of Lemma 4.1, define*

$$\vartheta:=1-2\sum_{i=1}^{n}\frac{1}{p_i}-2\sum_{i=1}^{k}\frac{1}{q^{\deg(g_i)}}$$

and

$$\mathfrak{S}:=\frac{2n+2k-1}{\vartheta}+2.$$

Suppose $\vartheta>0$. Then a sufficient condition for the existence of an element $\alpha\in\mathbb{F}_{q^m}$ such that both α and $f(\alpha)=\dfrac{a\alpha^2+b\alpha+c}{d\alpha+e}$ are simultaneously primitive normal over $\mathbb{F}_{q^m}$, where the matrix $M=\begin{pmatrix}a&b&c\\0&d&e\end{pmatrix}$ is of rank 2 and if $(q,m)=(2,odd)$ then $M\neq\begin{pmatrix}1&1&0\\0&1&0\end{pmatrix}$ is

$$q^{m/2}>4W(d)^2\Omega(g)^2\mathfrak{S}. \tag{4.2}$$

Proof. A key step is to write (4.1) in the equivalent form

$$\begin{aligned}\mathfrak{M}\geq{}&\sum_{i=1}^{n}\left(\mathfrak{M}(p_id,d,g,g)-\left(1-\frac{1}{p_i}\right)\mathfrak{M}(d,d,g,g)\right)\\&+\sum_{i=1}^{n}\left(\mathfrak{M}(d,dp_i,g,g)-\left(1-\frac{1}{p_i}\right)\mathfrak{M}(d,d,g,g)\right)\\&+\sum_{i=1}^{k}\left(\mathfrak{M}(d,d,g_ig,g)-\left(1-\frac{1}{q^{\deg(g_i)}}\right)\mathfrak{M}(d,d,g,g)\right)\\&+\sum_{i=1}^{k}\left(\mathfrak{M}(d,d,g,g_ig)-\left(1-\frac{1}{q^{\deg(g_i)}}\right)\mathfrak{M}(d,d,g,g)\right)+\vartheta\mathfrak{M}(d,d,g,g).\end{aligned} \tag{4.3}$$

On the right side of (4.3), since $\vartheta>0$, we can bound the last term below using (3.1). Thus

$$\vartheta\mathfrak{M}(d,d,g,g)\geq\vartheta\theta^2(d)\Theta^2(g)q^{\frac{m}{2}}(q^{\frac{m}{2}}-4W^2(d)\Omega^2(g)). \tag{4.4}$$

Moreover, since $\theta(p_i d) = \theta(p_i)\theta(d) = \left(1 - \frac{1}{p_i}\right)$ and $\Theta(g_i g) = \Theta(g_i)\Theta(g) = \left(1 - \frac{1}{q^{\deg(g_i)}}\right)$ we have from (3.3),

$$\mathfrak{M}(p_i d, d, g, g) - \left(1 - \frac{1}{p_i}\right)\mathfrak{M}(d, d, g, g) = \left(1 - \frac{1}{p_i}\right)\theta^2\Theta^2 \sum_{\substack{d_1|d \\ d_2|d}} \sum_{\substack{h_1|g \\ h_2|g}} S(\chi_{p_i d_1}, \chi_{d_2}, \psi_{h_1}, \psi_{h_2}).$$

and

$$\mathfrak{M}(d, d, g_i g, g) - \left(1 - \frac{1}{q^{\deg(g_i)}}\right)\mathfrak{M}(d, d, g, g) = \left(1 - \frac{1}{q^{\deg(g_i)}}\right)\theta^2\Theta^2 \sum_{\substack{d_1|d \\ d_2|d}} \sum_{\substack{h_1|g \\ h_2|g}} S(\chi_{d_1}, \chi_{d_2}, \psi_{g_i h_1}, \psi_{h_2}).$$

Hence, as for (3.1),

$$\begin{aligned} \left|\mathfrak{M}(p_i d, d, g, g) - \left(1 - \frac{1}{p_i}\right)\mathfrak{M}(d, d, g, g)\right| &\leq 4\left(1 - \frac{1}{p_i}\right)\theta^2(d)\Theta^2(g)\big(W(p_i d) - W(p_i)\big)W(d) \\ &= 4\left(1 - \frac{1}{p_i}\right)\theta^2(d)W^2(d). \end{aligned} \tag{4.5}$$

$$\begin{aligned} \left|\mathfrak{M}(d, d, g_i g, g) - \left(1 - \frac{1}{q^{\deg(g_i)}}\right)\mathfrak{M}(d, d, g, g)\right| &\leq 4\left(1 - \frac{1}{p_i}\right)\theta^2(d)\Theta^2(g)\big(\Omega(g_i g) - \Omega(g_i)\big)\Omega(g) \\ &= 4\left(1 - \frac{1}{q^{\deg(g_i)}}\right)\Theta^2(g)\Omega^2(g). \end{aligned} \tag{4.6}$$

Similarly,

$$\left|\mathfrak{M}(d, d, g, g) - \left(1 - \frac{1}{p_i}\right)\mathfrak{M}(d, p_i d, g, g)\right| \leq 4\left(1 - \frac{1}{p_i}\right)\theta^2(d)\Theta^2(g)W^2(d) \tag{4.7}$$

and

$$\left|\mathfrak{M}(d, d, g_i g, g) - \left(1 - \frac{1}{q^{\deg(g_i)}}\right)\mathfrak{M}(d, d, g, g)\right| \leq 4\theta^2(d)\left(1 - \frac{1}{q^{\deg(g_i)}}\right)\Theta^2(g)\Omega^2(g). \tag{4.8}$$

Inserting (4.4), (4.5), (4.7) and (4.8) in (4.3) and cancelling the common factor $\theta^2(d)\Theta^2(g)$, we obtain (4.2) as a condition for $\mathfrak{M}$ to be positive (since ϑ is positive). This completes the proof. □

We conclude our paper by discussing all the possible cases for fields of characteristic 2.

5. Some estimations for fields of even characteristic

The prime purpose of this section is to analyse the conditions (3.2) and (4.2) for the existence of elements of desired properties in fields of even characteristic. Towards that, we express the pairs (q, m) with the desired properties with extending and developing the techniques employed in [13], [14] and [7] by the functions presented earlier, leading us to character sums. We have already defined such pairs (q, m) as *primitive normal* pair.

Also, it is worth mentioning that due to the complexity of the character sums and their fragile behaviour on fields of different orders, it is necessary to distinguish a few cases depending on the order of the prime subfield. Henceforth, we assume that $q = 2^k$, where k is a positive integer.

From now on we use the concept of the radical of m i.e. m' and the radical of x^m-1 which is $x^{m'}-1$. Where m' is such that $m=2^k m'$, where $\gcd(2,m')=1$ and k is a non-negative integer. In fact, when $m'=1$, trivially k is positive.

We split our computations in two cases:

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

Notice that, in the former case, $x^{m'}-1$ splits at most into a product of m' linear factors over $\mathbb{F}_q$. The following result is inspired from Lemma 6.1 of Cohen's work [4].

Lemma 5.1. *For $q=2^k$, where $k\geq 1$, let $d=q^m-1$ and let $g|x^m-1$ with $g_1,g_2,\ldots,g_r$ be the remaining distinct irreducible polynomials dividing x^m-1. Furthermore, let us write $\vartheta := 1-\sum_{i=1}^{r}\frac{1}{q^{deg(g_i)}}$ and $\mathfrak{S} := \frac{r-1}{\vartheta}+2$, with $\vartheta>0$. Let $m=m'\,2^k$, where k is a non-negative integer and $\gcd(m',2)=1$. If $m'|q-1$, then*

$$\mathfrak{S}=\frac{2q^2-6q+aq+4}{aq-2q+2},$$

where $m'=\frac{q-1}{a}$. In particular, $\mathfrak{S}<2q^2$.

We also need the following. We use this result in the next case and all the subsequent cases, unless stated otherwise.

Lemma 5.2 (Lemma 6.2, [4])**.** *For any odd positive integer n, $W(n)<6.46\,n^{1/5}$, where W has same meaning as stated earlier.*

From Theorem 4.2 it is clear that some concepts regarding the factorization of x^m-1 can be used in order to effectively use the results of the previous section. Such as if $m'|q-1$, then $x^{m'}-1$ splits into m' distinct linear polynomials. Throughout this section we use prime sieve technique result to establish the rest.

Lemma 5.3. *For $f(x)\in\mathbb{F}_{q^m}(x)$, such that $f(x)=x$ or $f(x)=x^2$, we have $\mathfrak{M}(q^m-1,q^m-1,x^m-1,x^m-1)>0$.*

Proof. The proof follows from Lemma 4.1 of [11]. Since q is even, q^m-1 is odd, hence both α and $f(\alpha)$ are simultaneously primitive. Similarly, since m' is odd, α and $f(\alpha)$ are simultaneously normal. □

5.1. **Proof of Theorem 1.6.** Taking $g=1$ in Inequality (4.2) and applying Lemma 5.2, we have the sufficient condition

$$q^{\frac{m}{10}}>334\,q^2.$$

Then for $m'=q-1$, the inequality transforms to

$$q^{\frac{q-1}{10}-2}>334,$$

which holds for $q\geq 64$.

Next, we consider $q=32$ and $m=m'=q-1=31$. Then, by factorizing, $\omega(27^{26}-1)=12$ and the pair $(q,m)=(32,31)$ satisfies the condition (4.2). Hence $\mathbb{F}_{32^{31}}$ contains an element α such that both α and $f(\alpha)$ are simultaneously primitive normal with the given conditions.

In order to reduce our calculations, we now consider the range $19 \leq m' < \frac{q-1}{3}$, for $q \geq 64$. Then, by Lemma 5.1 we have $\mathfrak{S} < (2q+2)$. Hence Inequality (4.2) is satisfied if $q^{\frac{m'-1}{10}} > 167(2q+2)$ and this holds for $m' \geq 19$.

When $m' = \frac{q-1}{3}$, then $\mathfrak{S} \leq q$ and then the condition becomes $q^{\frac{m'-1}{10}-1} > 167$ and this holds for $m' \geq 19$. Since $m' = 19 \neq \frac{q-1}{3}$ for any $q = 2^k$, we may leave this case.

Next, we investigate all cases with $m' < 19$. In the next part, we set $d = q^m - 1$, $g = 1$ unless mentioned otherwise.

Case 1, $m' = 1$**:** Then $m = 2^j$. Initially we take $j \geq 2$. To check the condition we take $g = X + 1$. In that case $\vartheta = 1$ and $\mathfrak{S} = 1$. Then the inequality becomes

$$q^{\frac{2^j}{10}} > 334.$$

For $q = 2$, the condition holds for $j \geq 7$. Again for $q = 4$, $j \geq 6$; for $8 \leq q \leq 32$, $j \geq 5$; for $64 \leq q \leq 2^{10}$, $j \geq 4$; for $2^{11} \leq q \leq 2^{20}$, $j \geq 3$ and for $q \geq 2^{21}$ the condition holds for $j \geq 2$. So we calculate the rest of the pairs (q, m) by calculating $\omega = \omega(q^m - 1)$, i.e., the number of distinct prime divisors of $q^m - 1$. Hence it suffices to check that $q^{m/2} > 4 \cdot W(q^m - 1)^2 \cdot 2^2$, where $W(q^m - 1) = 2^\omega$. The pairs $(2, 4), (2, 8), (2, 16), (4, 4), (4, 8), (8, 4), (8, 8), (16, 4), (32, 4), (64, 4), (128, 4), (512, 4)$ do not satisfy the condition. We take taking $g = 1$ and appropriate value of d and we apply the sieve condition 4.2 to verify $(128, 4), (512, 4)$ as primitive normal pairs and declare the rest as possibly exceptional pairs.

Now we discuss the case when $m = 2$. Then any pair $(q, 2)$ is primitive normal pair if and only if it is a primitive pair, i.e., there exists α in $\mathbb{F}_{q^2}$ such that both α and $f(\alpha)$ are simultaneously primitive elements of $\mathbb{F}_{q^2}$. For all q such that $q^2 - 1$ is a Mersenne prime (the primes which are of the form $2^j - 1$ for some positive integer j are called *Mersenne primes*) except $(2, 2)$, all the elements of $\mathbb{F}_{q^2}^*$ are primitive except the identity and hence pairs $(q, 2)$ are primitive normal pairs. However, $(2, 2)$ does not fit into this category as $\mathbb{F}_4 \cong \frac{\mathbb{Z}_2[x]}{<x^2+x+1>}$ and the primitive elements of $\mathbb{F}_4$ are roots of $f(x) = x^2 + x + 1$, i.e., $f(\alpha) = 0$ is not primitive when α is primitive.

Next, we employ the sufficient condition $q^{1/5} > 668$, which holds for $q \geq 2^{47}$ and for the remaining pairs we use sieve condition (4.2) to test the existence of the property. When $d = q^2 - 1$ and $g = x + 1$, the condition holds for all $q = 2^k$, where $k = 13, 17$ and $k \geq 19$. Again choosing appropriate d as in Table 1, we conclude that among the above pairs; $(2^{11}, 2), (2^{12}, 2), (2^{14}, 2), (2^{15}, 2), (2^{16}, 2), (2^{18}, 2)$ are primitive normal pairs and the rest are possible exceptions.

Summing up, we have the following possibly exceptional pairs: $(2, 2)$, $(2, 4)$, $(2, 8)$, $(2, 16)$, $(4, 2)$, $(4, 4)$, $(4, 8)$, $(8, 2)$, $(8, 4)$, $(8, 8)$, $(16, 2)$, $(16, 4)$, $(32, 2)$, $(64, 2)$, $(64, 4)$, $(128, 2)$, $(256, 2)$, $(512, 2)$ and $(1024, 2)$.

Case 2, $m' = 3$**:** In this case, m is of the form $m = 3 \cdot 2^j$, where j is a positive integer and $q = 2^{2k}$ for some $k \geq 1$. For $q = 4$, take $g = x^{m'} - 1$ so that $\mathfrak{S} = 1$ and the sufficient condition is $4^{\frac{3.2^j}{10}} > 167 \times (2^3)^2$, which holds for $j \geq 5$. Hence the pairs under the above condition are primitive normal pairs except $(4, 3), (4, 6), (4, 12), (4, 24)$ and $(4, 48)$. After employing the sieving condition (4.2), see Table 1, we conclude that $(4, 24), (4, 48)$ are primitive normal pairs and $(4, 3), (4, 6), (4, 12)$ are possible exceptional pairs.

Then we take $g = 1$. For $q = 16$, $\mathfrak{G} \leq 22$ the sufficient condition is $q^{\frac{3.2^j}{10}} > 3672.8$, which holds for $j \geq 4$.

For $q = 64, 256$, $\mathfrak{G} < 7.51$ and $m'|q-1$, the condition holds for $j \geq 3$. Again for $1024 \leq q \leq 2^{16}$, $\mathfrak{G} < 7.029$ and we need to check $q^{\frac{3.2^j}{10}} > 1251.95$, which holds when $j \geq 2$. For $2^{18} \leq q \leq 2^{34}$, $\mathfrak{G} < 7.0001$ and the condition holds for $j \geq 1$; and for $q \geq 2^{35}$ such that $m'|q-1$ the condition holds for $j \geq 0$.

We calculate the remaining pairs by taking $g = x^3 - 1$ and using $W(q^m - 1)$, $\Omega(x^3 - 1)$. So the condition is $q^{m/2} > 4 \cdot W(q^m - 1)^2 \cdot (2^3)^2$, which all but the pairs $(16, 3), (16, 6), (64, 3), (64, 6), (256, 3), (1024, 3), (2^{12}, 3), (2^{16}, 3), (2^{20}, 3)$ fail to satisfy. Now we choose suitable values of g and d to declare $(16, 12)$, $(16, 24)$, $(64, 3)$, $(256, 3)$, $(1024, 3)$, $(2^{12}, 3)$, $(2^{16}, 3)$ and $(2^{20}, 3)$ as primitive normal pairs, as shown in Table 1.

So, we have the following pairs as possible exceptional pairs: $(4, 3)$, $(4, 6)$, $(4, 12)$, $(16, 3)$ and $(16, 6)$.

From now on assume $m = m'2^j$ with $j \geq 0$.

Case 3, $m' = 5$**:** Here $m = 5 \cdot 2^j$, with non-negative integer j. As there are 5 distinct factors of $x^{m'} - 1$, so by calculation we have $\vartheta > 0$ if $q \geq 16$. Then $\mathfrak{G} < 26$ for $q = 16$ and the sufficient condition is $q^{\frac{5.2^j}{10}} > 4340.09$ which holds for $j \geq 3$.

For $q = 256$, $\mathfrak{G} \leq 11.7627$, and sufficient condition is $q^{\frac{5.2^j}{10}} > 1963$. This holds when $j \geq 2$. Again, $4096 \leq q \leq 2^{20}$ and $m'|q-1$, the condition is $q^{\frac{5.2^j}{10}} > 1843.57$ and holds for $j \geq 1$. When $q \geq 2^{21}$ and $m'|q-1$ the condition holds for $j \geq 0$.

Taking $g = x^5 - 1$, we check the remaining pairs for the inequality $q^{m/2} > 4 \cdot 2^{2\omega} \cdot (2^5)^2$ and have the following as possible exceptional pairs $(16, 5), (16, 10), (256, 5), (2^{12}, 5)$. Then we choose proper d and g, and verify condition (4.2) and have $(16, 10), (256, 5), (2^{12}, 5)$ are primitive normal pairs. Then the pair $(16, 5)$ is a possible exception.

Case 4, $m' = 7$**:** Here $m = 7 \cdot 2^j$, with non-negative integer j. Let $g = x^{m'} - 1$ for $q = 8$, then $\vartheta = 1$ and $\mathfrak{G} = 1$. Then the sufficient condition is $q^{\frac{7.2^j}{10}} > 2736128$ which holds for $j \geq 4$.

For $q = 64$, take $g = 1$ and $\mathfrak{G} \leq 18.64$, then sufficient condition $q^{\frac{7.2^j}{10}} > 3112.8$ holds for $j \geq 2$. Again, $q = 512, 2^{12}, 2^{15}$, $\mathfrak{G} < 15.3655$ and the condition holds for $j \geq 1$. For $q \geq 2^{16}$, whenever $m'|q-1$ the condition holds for $j \geq 0$.

Taking $g = x^7 - 1$, we check the remaining pairs for the inequality $q^{m/2} > 4 \cdot 2^{2\omega} \cdot (2^7)^2$. After a calculation, we conclude that all the pairs are primitive normal pairs except the pairs $(8, 7)$ $(8, 14)$.

Case 5, $m' = 9$**:** Here $m = 9 \cdot 2^j$, with non-negative integer j. As $m' = 9$, there are 9 distinct factors of $x^{m'} - 1$. When $g = 1$ we have $\vartheta > 0$ if $q \geq 32$. Then $\mathfrak{G} < 38.2667$ for $q = 64$ and the sufficient condition is $q^{\frac{9.2^j}{10}} > 6387.72$ which holds for $j \geq 2$.

For $q = 2^{12}$, sufficient condition holds for $j \geq 1$. When $q \geq 2^{13}$ and $m'|q-1$ the condition holds for $j \geq 0$.

Taking $g = x^9 - 1$, we check the remaining pairs for the inequality $q^{m/2} > 4 \cdot 2^{2\omega} \cdot (2^9)^2$ and take pair $(64, 9)$, which does not satisfy the inequality. After calculating with suitable values of d and g, as shown in Table 1, we conclude that $(64, 9)$ is also a primitive normal pair, i.e., all the pairs are primitive normal.

Case 6, $m' = 11$**:** Here $m = 11 \cdot 2^j$, with non-negative integer j. As there are 11 distinct factors of $x^{m'} - 1$, so by calculation for $g = 1$ we have $\vartheta > 0$ if $q \geq 32$.

For $q = 2^{10}$, $\mathfrak{S} < 27.3585$ and sufficient condition $q^{\frac{11.2^j}{10}} > 4566.86$ holds for $j \geq 1$. When $q \geq 2^{11}$ and $m'|q-1$ the condition holds for $j \geq 0$.

Taking $g = x^{11} - 1$, we check the remaining pairs for the inequality $q^{m/2} > 4 \cdot 2^{2\omega} \cdot (2^{11})^2$, then we have 3 possible exceptional pairs. By calculating with suitable values of d and $g = x^{m'} - 1$, we conclude that all the pairs are primitive normal.

Case 7, $m' = 13$**:** Here $m = 13 \cdot 2^j$, with non-negative integer j. As there are 13 distinct factors of $x^{m'} - 1$, by calculation, we have $\vartheta > 0$ if $q \geq 32$. For $q \geq 64$ and $m'|q-1$, take $g = 1$ then $\mathfrak{S} < 44.1053$ and the sufficient condition holds for $j \geq 0$. We conclude that all the pairs are primitive normal.

Case 8, $m' = 15$**:** Here $m = 15 \cdot 2^j$, with non-negative integer j. As $m' = 15$, there are 15 distinct factors of $g = x^{m'} - 1$. For $q = 16$, the sufficient condition for existence of primitive normal element is $q^{15.2^j/10} > 167 \cdot (2^{15})^2$. This condition holds for $j \geq 3$.

For $q = 256$, and $g = 1$ we have $\mathfrak{S} < 56.882$ and the sufficient condition $q^{\frac{15.2^j}{10}} > 9446.06$ holds for $j \geq 1$. When $q > 256$ and $m'|q-1$ the condition holds for $j \geq 0$.

Taking $g = x^{15} - 1$, we check the remaining pairs on the inequality $q^{m/2} > 4 \cdot 2^{2\omega} \cdot (2^{15})^2$ and we obtain $(16, 15), (16, 30), (256, 15)$ as possible exceptional pairs. By calculating with compatible values of d, g in the prime sieve condition (4.2), we get that $(16, 30), (256, 15)$ are primitive normal pairs. Hence we declare $(16, 15)$ as an exceptional pair.

Case 9, $m' = 17$**:** Here $m = 17 \cdot 2^j$, with non-negative integer j. As there are 17 distinct factors of $x^{m'} - 1$, by calculation, for $g = 1$, we have $\vartheta > 0$ if $q \geq 64$.

When $q \geq 64$, the sufficient condition is $q^{\frac{17.2^j}{10}} > 12085.5$ which holds for $j \geq 0$ whenever $m'|q-1$. Hence we have that all the pairs of this case are primitive normal.

For each of the individual pairs (q, m) listed above that do not satisfy the sufficient condition based on Lemma 5.2, we can test them further by means of the sufficient condition (4.2) after factorising completely $x^m - 1$ and $q^m - 1$ and making a choice of polynomial divisor g of $x^m - 1$ and factor d of $q^m - 1$. In practice, the best choice is to choose $p_1, \ldots, p_n$ and sometimes, the "largest" irreducible factors $g_1, \ldots, g_k$ of $x^m - 1$ to ensure that ϑ is positive (and not too small). Here the multiplicative aspect of the sieve is more significant. Table 1 summarizes the pairs in which the test yielded some positive conclusion. This concludes the proof.

5.2. **Proof of Theorem 1.7.** For our next main theorem, we need the following well-known facts, see [12, Theorem 2.47]. Let u be the order of q mod m'. Then $x^{m'} - 1$ is a product of irreducible polynomial factors of degree less than or equal to u in $\mathbb{F}_q[x]$; in particular, $u \geq 2$ if $m' \nmid q - 1$. Let M be the number of distinct irreducible polynomials of $x^m - 1$ over $\mathbb{F}_q$ of degree less than u. Let $\sigma(q, m)$ denotes the ratio

$$\sigma(q, m) := \frac{M}{m},$$

where $m\sigma(q, m) = m'\sigma(q, m')$.

From Proposition 5.3 of [5], we deduce the following bounds.

Lemma 5.4. *Suppose $q = 2^k$. Then the following hold.*

(q,m)	d	n	g	k	$\mathfrak{S}$	$q^{m/2}$	$4W(d)^2\Omega^2(g)\Lambda$
(128,4)	3	5	$x+1$	0	21.9523	16384	1404.95
(512,4)	15	6	$x+1$	0	32.9531	262144	8435.99
$(2^{11},2)$	3	3	$x+1$	0	7.6329	2048	488.506
$(2^{12},2)$	15	4	$x+1$	0	18.1107	4096	1159.08
$(2^{14},2)$	3	5	$x+1$	0	21.9523	16384	1404.95
$(2^{15},2)$	3	5	$x+1$	0	22.0596	32768	1411.81
$(2^{16},2)$	3	4	$x+1$	0	16.7511	65536	1072.07
$(2^{18},2)$	15	6	$x+1$	0	32.9531	262144	8435.99
(4,24)	15	7	x^3-1	0	34.2484	1.6777×10^7	140283
(4,48)	15	10	x^3-1	0	50.3795	2.81475×10^{14}	206354
(16,12)	15	7	x^3-1	0	34.2484	1.6777×10^7	140283
(16,24)	15	10	x^3-1	0	50.3795	2.81475×10^{14}	206354
(64,3)	3	3	$x+1$	2	19.3369	512	309.39
(256,3)	15	4	$x+1$	2	28.2612	4096	452.179
(1024,3)	3	5	x^3-1	0	22.0596	32768	22589
$(2^{12},3)$	15	6	x^3-1	0	32.9531	262144	134976
$(2^{16},3)$	15	7	x^3-1	0	34.2484	1.67772×10^7	140281
$(2^{20},3)$	15	9	x^3-1	0	82.2883	1.07374×10^9	337053
(16,10)	3	6	x^5-1	0	60.7588	1.04858×10^6	995472
(256,5)	3	6	x^5-1	0	60.7588	1.04858×10^6	995472
$(2^{12},5)$	15	9	x^5-1	0	87.8157	1.07374×10^9	5.75509×10^6
(8,28)	15	10	x^7-1	0	49.0678	4.39805×10^8	5.14313×10^7
(8,56)	15	15	x^7-1	0	106.643	1.93428×10^{25}	1.11828×10^8
(64,9)	3	5	x^9-1	0	17.4747	1.34218×10^8	7.32942×10^7
(16,30)	15	13	$x^{15}-1$	0	293.517	1.15292×10^{18}	2.01703×10^{13}
(256,15)	15	13	$x^{15}-1$	0	293.517	1.15292×10^{18}	2.01703×10^{13}

TABLE 1. Pairs (q,m) appearing in the proof of Theorem 1.6, in which the corresponding test yielded a positive conclusion.

- $\sigma(2,3)=\frac{1}{3}$; $\sigma(2,5)=\frac{1}{5}$; $\sigma(2,9)=\frac{2}{9}$; $\sigma(2,21)=\frac{4}{21}$ *otherwise* $\sigma(2,m)\le\frac{1}{6}$.
- $\sigma(4,9)=\frac{1}{3}$; $\sigma(4,45)=\frac{11}{45}$; *otherwise* $\sigma(4,m)\le\frac{1}{5}$.
- $\sigma(8,3)=\sigma(8,21)=\frac{1}{3}$; *otherwise* $\sigma(8,m)\le\frac{1}{5}$.
- *If* $q\ge16$, *then* $\sigma(q,m)\le\frac{1}{3}$.

In, to develop suitable sufficient conditions, we need Lemma 7.2 from [4].

Lemma 5.5. *Assume that* $q=2^k$ *and* m *is a positive integer such that* $m'\nmid q-1$. *Let* $u(>1)$ *stand for the order of* $q \mod m'$. *Let* g *be the product of the irreducible factors of* $x^{m'}-1$ *of degree less than* u. *Then, in the notation of Lemma* 5.1, *we have* $\mathfrak{S}\le m'$.

We need few more conditions, which we can derive from Lemma 4.2 of [8].

Lemma 5.6. *For any* $n,\alpha\in\mathbb{N}$, $W(n)\le b_{\alpha,n}n^{1/\alpha}$, *where* $b_{\alpha,n}=\frac{2^s}{(p_1p_2\cdots p_s)^{1/\alpha}}$ *and* p_1, p_2, …, p_s *are the primes* $\le2^\alpha$ *that divide* n *and* W *has the same meaning as before.*

From these we immediately derive the lemma below.

Lemma 5.7. *For $n \in \mathbb{N}$ and*

(i) $\alpha = 6$, $W(n) < 37.4683\, n^{1/6}$,
(ii) $\alpha = 8$, $W(n) < 4514.7\, n^{1/8}$,
(iii) $\alpha = 14$, $W(n) < (5.09811 \times 10^{67}) n^{1/14}$,

where W has the same meaning as earlier.

Lemma 5.8. *Let $q = 2$, $M \neq \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ and $m' \nmid q - 1$, then there exists an element $\alpha \in \mathbb{F}_{q^m}$ such that α, $f(\alpha)$ are simultaneously primitive and normal over $\mathbb{F}_q$, i.e., (q, m) are primitive normal pairs except, possibly, the pairs $(2,3)$, $(2,5)$, $(2,6)$, $(2,7)$, $(2,9)$, $(2,10)$, $(2,11)$, $(2,12)$, $(2,14)$, $(2,15)$, $(2,18)$, $(2,21)$, $(2,24)$, $(2,30)$.*

Proof. First, let $m' = 3$. Then $x' - 1$ can be factorised into one linear and one quadratic factor. Then the condition becomes $2^{m/10} > 2672$, which holds for $m \geq 114$. Next let $m = 96$. Then $\omega = 12$ and the condition is $q^{m/2} > 2^{2\omega+6}$, which holds. But the remaining pairs $(2,3), (2,6), (2,12), (2,24), (2,48)$ do not satisfy the above condition. We perform further research on these pairs by taking compatible d and g in the sieve condition (4.2) as demonstrated in Table 2 and conclude that $(2,48)$ is primitive normal pair and $(2,3), (2,6), (2,12), (2,24)$ are possible exceptional pairs.

Again, if $m' = 5$, then $x' - 1$ can be factorised into one linear and one fourth degree polynomial. Then the condition becomes $2^{m/10} > 2672$, which holds for $m \geq 114$. Thus, for the remaining pairs a condition is $q^{m/2} > 2^{2\omega+6}$ and by calculating $\omega(q^m - 1) = \omega$, we have the following exceptional pairs $(2,5), (2,10), (2,20), (2,40)$. Again from Table 2 we can conclude that the only possible exceptional pairs are $(2,5), (2,10), (2,20)$.

For $m' = 9$, $x' - 1$ is a product of one linear, one quadratic and one sextic polynomial and the condition is $2^{m/10} > 10688$, which holds for $m \geq 134$. For the remaining the pairs we use the condition $q^{m/2} > 2^{2\omega+8}$ and by calculating the value of ω, we have the following exceptional pairs $(2,9), (2,18), (2,36)$. From Table 2, we can conclude that $(2,36)$ is a primitive normal pair and hence final possible exceptional pairs are $(2,9)$ and $(2,18)$.

Now, for $m' = 21$, $x' - 1$ is a product of one linear, one quadratic, two cubic and two distinct sextic polynomials. Then the condition is $2^{m/10} > 684032$ and the condition holds for $m \geq 194$. For the remaining pairs we use the condition $q^{m/2} > 2^{2\omega+14}$ and by calculating the value of $\omega(q^m - 1) = \omega$, we have the following exceptional pairs $(2,21), (2,42)$, from which we can declare the pair $(2,42)$ as primitive normal pair from Table 2. Hence the ony possible exceptional pair is $(2,21)$.

For the remaining pairs i.e. $q = 2$, $m' \nmid q - 1$ and $m' \neq 3$, 5, 9, 21, we consider two cases, viz. (i) m is odd and (ii) m is even.

Case (i): m is odd. We apply Lemma 5.5 to obtain the condition $q^{m/2} > 4 \cdot 2^{2\omega} \cdot 2^{2m\sigma(q,m)} \cdot m$. Then by Lemmas 5.4 and 5.7, the condition transforms to $2^{m/42} > 1.03991 \cdot 10^{136}.m$, which holds for $m \geq 19577$. Let $m \leq 19576$, then $\omega \leq 1620$, and, by applying these on the condition $2^{m/6} > m2^{2\omega+2}$, we conclude that the condition holds for $m \geq 19538$. Maintaining the flow we have that the condition holds for $m \geq 19333$.

For the remaining pairs we calculate the exact value of ω and able to detect 37 pairs where $m = 7$, 11, 13, 15, 17, 19, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 51, 53, 55, 57, 59, 65, 67, 69, 71, 73, 75, 77, 79, 81, 135, 165 and 225; which don't satisfy the condition. Again for

$d = q^m - 1$ and $g = x^{m'} - 1$, applying the prime sieve we are able to declare 20 of them as primitive normal pairs. Then by choosing compatible d and g (as shown in Table 2) we are able to determine another 13 pairs $(2, 17)$, $(2, 19)$, $(2, 23)$, $(2, 25)$, $(2, 27)$, $(2, 29)$, $(2, 31)$, $(2, 33)$, $(2, 35)$, $(2, 39)$, $(2, 45)$, $(2, 51)$ as primitive normal pairs. Hence, we conclude that following are the possible exceptional pairs $(2, 7)$, $(2, 11)$, $(2, 13)$, $(2, 15)$.

Case (ii): m is even. Once again, we shall break this discussion into two parts.

$4 \mid m$: Then by Lemma 5.7, $W(q^m - 1) < 37.4683\, q^{m/6}$ and for $4|m$, $\sigma(q, m) \leq m/24$. Then to show $\mathfrak{M}(q^m - 1, q^m - 1, x^m - 1, x^m - 1) > 0$ it is sufficient to show $2^{m/12} > 5615.49\, m$, which holds for $m \geq 248$. Then we calculate the exact value of ω and check the condition $2^{5m/12} > 2^{2\omega+2}$, for $m \leq 143$ and identify the pairs $(2, 28)$, $(2, 44)$, $(2, 52)$, $(2, 56)$, $(2, 60)$ which do not satisfy the condition. But from Table 2, we can conclude that all of them are primitive normal pairs. Hence in this particular case all pairs (q, m) are primitive normal pairs.

$4 \nmid m$: From Lemma 5.7, $W(q^m - 1) < 4514.7\, q^{m/8}$ and in this case $\sigma(q, m) \leq m/12$. Now, a sufficient condition for the existence of a primitive normal pair is $2^{m/12} > 8.153 \times 10^7$, which holds for $m \geq 420$. For the remaining pairs we use the prime sieve condition (4.2) for $d = q^m - 1$ and $g = x^{m'} - 1$ and identify the pairs $(2, 14)$, $(2, 22)$, $(2, 30)$, $(2, 70)$ which fail to satisfy the condition. Again, by observing the condition (4.2) for appropriate values of d and g we are able to identify the pairs $(2, 22), (2, 70)$ as primitive normal pairs; the calculations are listed in Table 2. Hence the only possible exceptional pairs are $(2, 14)$ and $(2, 30)$.

The proof is now complete. □

The following lemma is derived from Lemma 5.6.

Lemma 5.9. *For $n \in \mathbb{N}$, $W(n) < 1.10992 \cdot 10^9\, n^{1/10}$ and $W(n) < 4.24455 \cdot 10^{14}\, n^{1/11}$.*

Lemma 5.10. *For $q = 4$ and $m' \nmid q - 1$, all the pairs (q, m) are primitive normal pairs, except for the possible exceptional pairs $(4, 5), (4, 7), (4, 9), (4, 10)$.*

Proof. We shall start this discussion with the case $m' = 45$. In this case $x^{m'}$ is a product of 3 linear, 6 quadratic, 2 cubic and 4 sextic factors. Let g be the product of the linear factors, then $\vartheta = 0.5927$ and $\mathfrak{S} = 20.56$. After this, the sufficient condition becomes $4^{m/10} > 167 \cdot (2^3)^2 \cdot 20.56$, which holds for $m \geq 90$. When $m = 45$, then $\omega = \omega(4^m - 1) = 11$ and the pair $(4, 45)$ satisfies the condition $4^{m/2} > 2^{2\omega+8} \cdot 20.56$. Hence $(4, 45)$ is also a primitive normal pair.

Now we are heading towards the next case, which is $m' = 9$. Then $x^{m'} - 1$ is a product of 3 linear and 2 cubic factors. Now we take g as the product of three linear factors, then $\vartheta = 0.9375$ and $\mathfrak{S} = 5.5$. These yield the condition $4^{m/10} > 167 \cdot (2^3)^2 \cdot 5.5$, which holds for $m \geq 144$.

For the remaining pairs we verify the sufficient condition $4^{m/2} > 2^{2\omega+8} \cdot 5.5$ by calculating the exact value of ω. After this, we can conclude that the pairs $(4, 36), (4, 72)$ are primitive normal. From Table 2, we conclude that $(4, 18)$ is also a primitive normal pair, thus the only possible exceptional pair is $(4, 9)$.

Next we have the case $q = 4$, $m' \nmid q - 1$ and $m' \neq 9, 45$. At first we consider m even. In this case $\sigma(q, m) \leq m/10$ and by Lemma 5.9, $W(q^m - 1) < 1.10992 \cdot 10^9\, q^{m/10}$. Hence a sufficient condition for our purpose is $4^{m/5} > 4.83296 \cdot 10^{18}\, m$, which holds for $m \geq 174$. For

the remaining pairs we use the condition $4^{2m/5} > 2^{2\omega+2}\, m$ and calculate $\omega = \omega(4^m - 1)$ explicitly. Among the remaining pairs, $(4, 10), (4, 14), (4, 20), (4, 22), (4, 28), (4, 30)$ do not satisfy the condition. Again for appropriate values of d and g, $(4, 14), (4, 20), (4, 22), (4, 28), (4, 30)$ satisfy the sieve condition as given in Table 2. Hence the only possible exceptional pair is $(4, 10)$.

Now, we consider the case m odd. Here $\sigma(q, m) = 1/5$ and from Lemma 5.9 we have $W(q^m - 1) < 4.24455 \cdot 10^{14}\, q^{m/11}$. Then the sufficient condition is $4^{m/11} > 7.20647 \cdot 10^{29}\, m$, which holds for $m \geq 597$. Afterwards, we use the condition $4^{3m/10} > 2^{2\omega+2}\, m$ to test the remaining pairs by calculating the $\omega = \omega(q^m - 1)$. The pairs $(4, 5)$, $(4, 7)$, $(4, 11)$, $(4, 13)$, $(4, 15)$, $(4, 25)$, $(4, 27)$, $(4, 29)$, $(4, 33)$, $(4, 35)$ and $(4, 39)$ do not satisfy the condition. Now we take $d = q^m - 1$ and $g = x^m - 1$ in the prime sieve condition (4.2) and detect $(4, 27), (4, 29), (4, 33)$ and $(4, 39)$ as primitive normal pairs. Again, by choosing compatible values of d and g in condition (4.2) (as shown in Table 2) we conclude that all of the remaining pairs are primitive normal pairs. This concludes the proof. □

Lemma 5.11. *Let $q = 8$ and $m' \nmid q - 1$, then all the pairs (q, m) are primitive normal pairs, unless (q, m) is one of the pairs $(8, 3), (8, 5)$ and $(8, 7)$.*

Proof. We begin our discussion with $m' = 3$. Then $x^{m'} - 1$ is a product of a linear and a quadratic polynomial. If we take g to be the linear polynomial, then $\vartheta = 0.96875$ and $\mathfrak{S} < 3.04$. It follows that a sufficient condition for the existence of primitive normal pair is $8^{m/10} > 167 \cdot 2^2 \cdot 3.04$ and this holds for all $m \geq 48$. For the remaining pairs we use the condition $8^{m/2} > 2^{2\omega+4} \cdot 3.04$ by explicitly calculating the value of ω. Then the pairs $(8, 3), (8, 6), (8, 12)$ are the ones which fail to satisfy the inequality. By choosing appropriate values of d and g in condition (4.2), as shown in Table 2, we conclude that $(8, 3)$ is the only possible exceptional pair.

For the next stage we choose $m' = 21$, that is, $x^{m'} - 1$ is product of one linear, one quadratic, two cubic and two sextic polynomials. We choose g as the product of the linear and the quadratic factor. Then $\vartheta = 0.992172$ and $\mathfrak{S} < 9.06$ which yields the sufficient condition $8^{m/10} > 167 \cdot (2^4)^2 \cdot 9.06$, which holds for $m \geq 84$. Then the condition $8^{m/2} > 2^{2\omega+10} \cdot 9.06$ comes into play to detect the primitive normal pairs by taking the exact value of ω. From this, we declare that the remaining pairs $(8, 21), (8, 42)$ are also primitive normal pairs.

Now, we are heading for the final stage, i.e., $q = 8$, $m' \nmid q - 1$ and $m' \neq 3, 21$. Form Lemmas 5.4 and 5.6, we have $\sigma(q, m) \leq 1/5$ and $W(q^m - 1) < 37.4683 q^{m/6}$. It follows that for the existence of primitive normal pairs, a sufficient condition is $8^{m/30} > 5616m$, which holds for $m \geq 202$.

For the remaining pairs, we use the condition $8^{11m/30} > 2^{2\omega+2} m$ by determining the value of ω. For $m \leq 201$, $\omega \leq 85$ this holds for $m \geq 164$. Next we take $m \leq 163$ and then $\omega \leq 72$. For these the condition holds for $m \geq 140$. Now repeating the above process we get that the condition holds for $m \geq 92$ and among the remaining pairs $(8, 5), (8, 9), (8, 10), (8, 11), (8, 15), (8, 20)$ are the ones which fail to satisfy the condition. Then choosing appropriate value of l and $g = x^{m'} - 1$ in condition (4.2) we are able to declare all but the pair $(8, 5)$ as primitive normal pairs.

Our proof is now complete. □

Lemma 5.12. *Let $q \geq 16$ and $m' \nmid q - 1$, then all the pairs (q, m) are primitive normal pairs, unless $(q, m) = (32, 3)$.*

Proof. We shall break the discussion into 4 cases (I–IV). Lemma 5.4 implies, that $\vartheta(q,m) \leq \frac{1}{3}$ in all four cases. Furthermore, we take g to be the product of irreducible polynomials dividing $x^m - 1$ of degree less than u.

Case I: $q = 16$**;** For this case we apply Lemma 5.7 i.e. $W(q^m - 1) < 4514.7q^{m/8}$. Then to show $\mathfrak{M}(q^m-1, q^m-1, x^m-1, x^m-1) > 0$ it is sufficient to show that $16^{m/12} > 8.15265 \cdot 10^7 m$, which holds for $m \geq 110$. We use the condition $16^{m/2} > 2^{2\omega+2}m$ to test the remaining pairs by plotting value of ω and conclude that the pairs $(16,7)$, $(16,9)$, $(16,11)$, $(16,13)$, $(16,14)$, $(16,18)$ and $(16,21)$ fail to satisfy the condition. Further, we choose compatible l and $g = x^{m'} - 1$ in condition (4.2) and conclude that all of them, except $(16,7)$, are primitive normal pairs. Finally, from Table 2, we obtain $(16,7)$ is also a primitive normal pair.

Case II: $q = 32$**;** From Lemma 5.7 we have $W(q^m - 1) < 37.4683q^{m/2}$ and proceeding as above with the sufficient condition $32^{m/30} > 1403.87m$, which is true for all $m \geq 103$. For rest of the pairs we use the condition $32^{11m/30} > 2^{2\omega+2}m$, which proves that all the pairs (q,m) are primitive normal pairs unless (q,m) is one of the pairs $(32,3), (32,5), (32,6), (32,9), (32,10)$, $(32,12)$. Furthermore applying the prime sieve condition (4.2) for compatible l and $g = x^{m'} - 1$, we confirm that all of them are primitive normal pairs except $(32,3)$.

Case III: $q = 64$**;** Using Lemma 5.7 we have $W(q^m - 1) < 37.4683q^{m/2}$ and for $\mathfrak{M}(q^m - 1, q^m - 1, x^m - 1, x^m - 1) > 0$ the sufficient condition is $64^{m/18} > 5601.03m$, which is true for all $m \geq 49$. We use the condition $64^{7m/18} > 2^{2\omega+2}m$, to investigate the existence of the property in the rest of the pairs and conclude that all the pairs (q,m) are primitive normal pairs unless (q,m) is $(64,5)$ or $(64,10)$. Later applying the prime sieve condition (4.2) for compatible l and $g = x^{m'} - 1$, we confirm that all of them are primitive normal pairs.

Case IV: $q \geq 128$**;** Lemma 5.7 yields $W(q^m - 1) < 37.4683q^{m/2}$ and for $\mathfrak{M}(q^m - 1, q^m - 1, x^m - 1, x^m - 1) > 0$ it is sufficient to show that $q^{m/6} > 1403.87 \cdot 2^{2m/3}m$, which is true for all $q \geq 128$ and $m \geq 18$. We use the condition $q^{m/2} > 2^{2\omega+2+2m/3}m$, to test the existence of the property in rest of the pairs (149 in total) and all the pairs (q,m) are primitive normal pairs except $(128,3)$. Then, from Table 2, we confirm that all of them are primitive normal pairs. This concludes our proof. □

As an immediate consequence of the above results, we obtain Theorem 1.7.

6. A few computational results

In this section we comment on the situation with the possible exceptional pairs that appear in Theorems 1.6 and 1.7. In particular, we wrote a script in SageMath, with the purpose of explicitly verifying whether the pairs in question are, in fact, genuine exceptions.

For every pair (q,m), our script first fixes a primitive element $\alpha \in \mathbb{F}_{q^m}$ and then for every quintuple $a,b,c,d,e \in \mathbb{F}_{q^m}$ with $a \neq 0$ and $dx + e \neq 0$, it checks whether there exists some power α^i with $\gcd(i, q^m - 1) = 1$ of α (hence a primitive element), such that α^i is normal over $\mathbb{F}_q$ and $\dfrac{a\alpha^2 + b\alpha + c}{d\alpha + e}$ is primitive and normal over $\mathbb{F}_q$. For the primitivity check, we just compute the corresponding multiplicative order and for the normality check, we use [12, Theorem 2.39]. If this search is successful for every valid quintuple, then the pair (q,m) is not an exception, while if it fails, even for one valid quintuple, the pair (q,m) is a genuine exception.

(q,m)	d	n	g	k	Λ	$q^{m/2}$	$3W(d)^2\Omega(g)\Lambda$
(2,48)	105	6	$x+1$	1	70.8428	1.67772^7	72543
(2,40)	3	6	1	2	82.1256	1.04858×10^6	21031.1
(2,36)	15	6	x^9-1	0	32.9531	262144	134976
(2,42)	3	5	$x^{21}-1$	0	15.9379	2.09751×10^6	16320.4
(2,17)	q^m-1	0	$x+1$	2	5.04762	362.039	323.048
(2,19)	q^m-1	0	$x+1$	1	3.00001	724.077	192.001
(2,23)	47	1	$x+1$	2	7.00984	2896.31	448.63
(2,25)	31	2	$x+1$	2	10.0408	5792.62	642.611
(2,27)	7	2	$x+1$	3	22.3926	11585.2	1433.13
(2,29)	233	2	$x^{29}-1$	0	5.00834	23170.5	1282.14
(2,31)	q^m-1	0	$x+1$	6	19.6	46341	1254.4
(2,33)	7	2	$x+1$	4	35.7918	92681.9	2290.68
(2,35)	31	3	$x+1$	5	47.4422	185364	3036.3
(2,39)	7	3	$(x+1)(x^2+x+1)$	3	13.3057	741455	3406.26
(2,45)	7	5	$(x+1)(x^2+x+1)$	6	32.9687	5.93164×10^6	8439.99
(2,51)	7	4	$x^{51}-1$	0	9.14684	4.74531×10^7	9.59166×10^6
(2,28)	3	5	$x+1$	2	66.6522	16384	4265.74
(2,44)	3	6	$x^{11}-1$	0	24.8377	4.1943×10^6	6358.45
(2,52)	3	6	$x^{13}-1$	0	22.0983	6.71089×10^7	5657.16
(2,56)	15	6	x^7-1	0	16.988	2.68435×10^8	17395.6
(2,60)	15	9	$x^{15}-1$	0	82.2883	1.07374×10^9	5.39285^6
(2,22)	3	3	$x^{11}-1$	0	7.6329	2048	1954.02
(2,70)	3	8	$x^{35}-1$	0	24.8631	3.43597×10^{10}	1.62943×10^6
(4,18)	15	6	$(x+1)(x^2+x+1)$	1	42.1079	262144	42.1079
(4,14)	3	5	$x+1$	2	35.4555	16384	2269.15
(4,20)	3	6	x^5-1	0	60.7588	1.04858×10^6	15554.3
(4,22)	3	6	$x^{11}-1$	0	24.8377	4.1943×10^6	6358.45
(4,28)	3	7	x^7-1	0	40.9888	2.68435×10^8	41972.5
(4,30)	15	9	$x^{15}-1$	0	82.2883	1.07374×10^9	5.39285×10^6
(4,11)	3	3	$x^{11}-1$	0	7.6329	2048	1954.02
(4,13)	3	2	$x^{13}-1$	0	5.00293	8192	1280.75
(4,15)	3	5	$(x+1)(x^2+x+1)$	3	44.2638	32768	11332.7
(4,25)	3	6	$x^{25}-1$	0	16.8495	3.35544×10^7	17253.9
(4,35)	33	7	$x+1$	5	31.9641	3.43596×10^{10}	2045.7
(8,6)	3	3	$x+1$	1	14.7186	512	235.498
(8,12)	15	6	x^3-1	0	32.9531	262144	33744
(16,7)	3	5	$x+1$	2	30.8825	16384	1976.48
(128,3)	7	2	x^3-1	0	5.06649	1448.15	1297.02

TABLE 2. Pairs (q,m) appearing in the proof of Theorem 1.7, in which the corresponding test yielded a positive conclusion.

Unfortunately, the extremely high number of such quintuples, even for "small" numbers, seems to create an impenetrable obstacle for a complete solution, with the exception of the pairs $(2,2)$ and $(2,3)$. On the other hand we managed to examine a respectable number of quintuples for all the other pairs and collected useful data.

In Table 3 we present the pairs (q,m), for which we found counter examples, while in Table 4, we present those for which we did not find counter examples.

(q,m)	f	counter-example	checked/exceptional 5-ples
$(2,2)$	x^2+x+1	$(\alpha,0,0,\alpha,\alpha)$	720/252
$(2,3)$	x^3+x+1	$(\alpha,0,0,\alpha,\alpha^2+\alpha)$	28224/8295
$(2,4)$	x^4+x+1	$(\alpha,0,0,0,\alpha^3+\alpha^2)$	64513/22109
$(2,5)$	x^5+x^2+1	$(\alpha,0,\alpha,0,\alpha)$	53345/52
$(2,6)$	$x^6+x^4+x^3+x+1$	$(\alpha,0,0,\alpha^2,\alpha^5+\alpha^4+\alpha+1)$	21857/77
$(4,2)$	x^4+x+1	$(\alpha,0,\alpha,\alpha,\alpha^3+\alpha^2)$	266115/1985
$(4,3)$	$x^6+x^4+x^3+x+1$	$(\alpha,0,0,\alpha,\alpha)$	47708/152

Notes:

(1) α is a root of $f \in \mathbb{F}_q[x]$.
(2) For the pairs $(2,2)$ and $(2,3)$ the search was exhaustive.

TABLE 3. Results of the computer test, where counter-examples were found.

Due to the large number of quintuples that we checked, without finding any counter-example, for the pairs (q,m) that appear in Table 4, we believe that the only genuine exceptions to the problem we considered in this paper are the pairs that appear in Table 3. In other words, based on our computational evindence, we state the following.

Conjecture 6.1. *Let $\mathbb{F}_{q^m}$ be a finite field of even characteristic. Then there exists an element α in $\mathbb{F}_{q^m}$, such that both α and $f(\alpha)$ are simultaneously primitive normal in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, where $f(x)=\dfrac{ax^2+bx+c}{dx+e}$, with $a,b,c,d,e \in \mathbb{F}_{q^m}$, $a \neq 0$, and $dx+e \neq 0$ unless (q,m) is one of the pairs $(2,2)$, $(2,3)$, $(2,4)$, $(2,5)$, $(2,6)$, $(4,2)$ or $(4,6)$, with these pairs being genuine exceptions.*

7. Some conjectures on rational functions

The following conjectures are extensions of the theorems given by Cohen, H. Sharma and R. Sharma in [15]. For a finite field $\mathbb{F}_{q^m}$ and a rational function $f(x) \in \mathbb{F}_{q^m}(x)$, we denote by $\deg(f)$ the sum of the degrees of f_1 and f_2, if $f(x)=f_1/f_2$ and f_1, f_2 are relatively prime polynomials. The following conjectures are based on the results obtained during various experiments performed on similar rational forms as in this paper, some of which are studied briefly and will be discussed extensively in our next papers. Due to significantly large number of finite fields and very fragile behavior of its properties, a large scale analysis is required to establish our claims and this will be the focus of our subsequent study.

Conjecture 7.1. *Take $f \in \mathbb{F}_{q^m}(x)$ and write $f=f_1/f_2$, where f_1, f_2 are relatively prime polynomials over $\mathbb{F}_{q^m}$. Let $n>2$ be the degree of f, such that $n=n_1+n_2$, where n_1, n_2 are degrees of f_1 and f_2 respectively. Then there exist an element $\alpha \in \mathbb{F}_{q^m}$ such that both α and*

(q,m)	checked 5-ples	(q,m)	checked 5-ples
$(2,7)$	11400	$(2,8)$	9067
$(2,10)$	12894	$(2,11)$	6504
$(2,12)$	1830	$(2,13)$	4765
$(2,14)$	2584	$(2,15)$	2003
$(2,16)$	2993	$(2,18)$	1104
$(2,20)$	1460	$(2,21)$	575
$(2,24)$	829	$(2,30)$	371
$(4,4)$	78278	$(4,5)$	25982
$(4,6)$	16072	$(4,7)$	19732
$(4,8)$	24391	$(4,9)$	4892
$(4,10)$	12001	$(4,12)$	4399
$(8,2)$	244944	$(8,3)$	163528
$(8,4)$	64654	$(8,5)$	67844
$(8,6)$	37279	$(8,7)$	11706
$(8,8)$	16416	$(8,14)$	1177
$(16,2)$	202189	$(16,3)$	79012
$(16,4)$	70934	$(16,5)$	28604
$(16,6)$	21965	$(16,15)$	235
$(32,2)$	189487	$(32,3)$	126253
$(64,2)$	133395	$(64,4)$	42129
$(128,2)$	163368	$(256,2)$	141196
$(512,2)$	135355	$(1024,2)$	106349

TABLE 4. Results of the computer test, where counter-examples were not found.

$f(\alpha)$ are simultaneously primitive normal elements of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ if

$$q^{m/2} > (2n-2)W(q^m-1)^2\Omega(x^m-1)^2,$$

provided the followings hold:

(i) *$f(x)$ is not of the form $ax^ig^h(x)$, where i is an integer, $1 \neq h \mid q^m-1$ and $a \in \mathbb{F}_{q^m}^*$.*
(ii) *If $n_1 \neq n_2$, then $p \nmid n_2$, where p is the characteristic of $\mathbb{F}_{q^m}$.*

Further, one can apply the prime sieve, see Section 4, to improve the above bound, leading to the next conjecture.

Conjecture 7.2. *The sufficient condition for existence of an element α in $\mathbb{F}_{q^m}$ such that (q,m) is a primitive normal pair is $q^{m/2} > (2n-2)W(d)^2\Omega(g)^2\mathfrak{S}$.*

REFERENCES

[1] Anju and R.K.Sharma, Existence of some special primitive normal elements over finite fields, *Finite Fields Appl.* **46** (2017) 280-303.
[2] A.R. Booker, S.D. Cohen, N. Sutherland and T. Trudgian, Primitive values of quadratic polynomials in a finite field, *Math. Comp.* **88** (318) (2019) 1903-1912.
[3] L.Carlitz, Primitive roots in a finite fields, *Trans. Amer. Math. Soc.* **73**(3) (1952) 314-318.
[4] S.D.Cohen, Pair of primitive elements in fields of even order, *Finite Fields Appl.* **28** (2014) 22-42.

[5] S.D.Cohen and S.Huczynska, The primitive normal basis theorem– without a computer, *J. Lond. Math. Soc.* **67**(1) (2003) 41-56.
[6] S.D.Cohen and S.Huczynska, The strong primitive normal basis theorem, *Acta. Arith.* **143**(4) (2010) 299-332.
[7] L.Fu and D.Q.Wan, A class of incomplete character sums, *Q.J.Math.Soc* **65**, (2014) 195-211.
[8] T.Garefalakis and G.Kapetanakis, On the existence of primitive completely normal bases of finite fields, *J. Pure Appl. Algebra* **223**(3) (2018) 909-921.
[9] G. Kapetanakis, An extension of the (strong) primitive normal basis theorem , *Appl. Algebra Eng. Commun. Comput.,* **25** (2013) 311-337.
[10] G. Kapetanakis, Normal bases and primitive elements over finite fields, *Finite Fields Appl.* **26**(2014) 123-143.
[11] H.W.Lenstra,Jr. and R.J.Schoof, Primitive Normal Bases for Finite Fields, *Math. Comp.* **48** (1987) 217-231.
[12] R. Lidl and H. Niederreiter, *Finite Fields* 2nd edn. (Cambridge University Press, Cambridge, 1997).
[13] T. Tian and W.F. Qi, Primitive normal elements and its inverse in finite fields, *Acta. Math. Sinica*(Chin. Ser.) **49**(3) (2006) 657-668.
[14] D. Wan, Generators and irreducible polynomials over finite fields, *Math. Comp.* **66**(219) (1997) 1195-1212.
[15] S.D. Cohen, H. Sharma and R. Sharma, Primitive values of rational functions at primitive elements of a finite field, arXiv:1909.13074v1 [math.NT] 28 Sep, 2019.
[16] S.D. Cohen, Kloosterman sums and primitive elements in Galois fields, *Acta Arithmetica* **XCIV**(2) (2000) 173-201.
[17] F.N. Castro, C.J. Moreno, Mixed exponential sums over finite fields, *Proc. Am. Math. Soc.* **128**(9) (2000) 2529-2537.
[18] S.D. Cohen, Consecutive primitive roots in a finite field, *Proc. Am. Math. Soc.* **93**(2) (1985) 189-197.
[19] H. Davenport, Bases for finite fields, *J. Lond. Math. Soc.* **43** (1968) 21-39.
[20] P.P. Wang, X.W. Cao and R.Q .Feng, On the existence of some specific elements in finite fields of characteristic 2, *Finite Fields Appl.* **18**(4) (2012) 800-8013.
[21] L. Carlitz, Some problems involving primitive roots in a finite filed, *Proc. Natl. Acad. Sci. USA,* **38**(4) (1952) 314-318.
[22] W.S. Chou, S.D. Cohen, Primitive elements with zero traces, *Finite Fields Appl.,* **7** (2001) 125-141.
[23] G.James and M.Liebeck, *Representations and Characters of Groups*, 2nd edn. (Cambridge University Press, Cambridge, 2001).
[24] L.B. He, W.B. Han,. Research on primitive elements in the form $\alpha + \alpha^{-1}$ over $\mathbb{F}_q$, *J. Inf. Eng. Univ.,* **4**(2) (2003) 97-98.
[25] G.B. Agnew, R.C. Mullin, I.M. Onyszchuk, and S.A. Vanstone. An implementation for a fast public key cryptosystem, *J. Cryptol.,* **3** (1991) 63-79.

Department of Mathematical Sciences, Tezpur University, Assam, India
Email address: diku_95@tezu.ernet.in

Department of Mathematical Sciences, Tezpur University, Assam, India
Email address: dbasnet@tezu.ernet.in

Department of Mathematics and Applied Mathematics, University of Crete, Voutes Campus, 70013 Heraklion, Greece
Email address: gnkapet@gmail.com